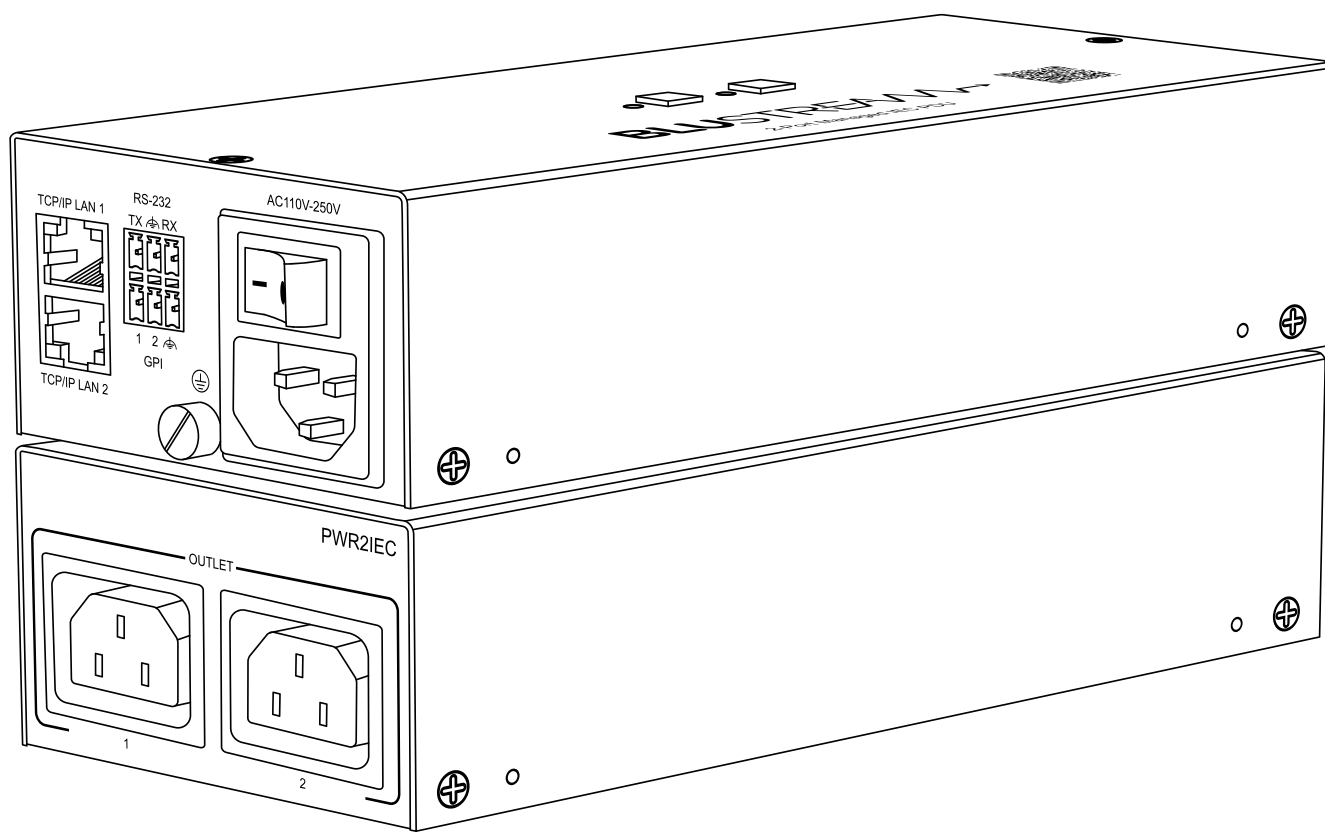




► PWR2IEC

User Manual

Thank you for purchasing this product.

For optimum performance and safety, please read these instructions carefully before connecting, operating or adjusting this product. Please keep this manual for future reference.



Surge Protection Device Recommended

This product contains sensitive electrical components that may be damaged by electrical spikes, surges, electric shock, lightning strikes, etc. Use of surge protection systems is highly recommended in order to protect and extend the life of your equipment.



Eco Friendly Packaging

This product has been packaged with fully recyclable materials, including compostable bags. Please help us to help the environment.

Safety and performance notice

Do not substitute or use any other power supply other than approved Blustream power supplies.

Do not disassemble the device for any reason. Doing so will void the manufacturer's warranty.

Contents

Introduction	03
Front Panel Description	04
Rear Panel Description	04
Resetting the PWR2IEC	05
Operation and Connections	05
Web GUI - Log In and Initialisation	06
Web GUI - Dashboard	08
Web GUI - Network	11
Web GUI - Schedule	14
Web GUI - Protocols	16
Web GUI - Email	37
Web GUI - Clock	42
Web GUI - RS-232	44
Web GUI - System	45
Web GUI - Security	49
Web GUI - Maintenance	53
Specifications	55
Package Contents	55
Maintenance	55
Communication Protocols and Commands	56
Certifications	59

Introduction

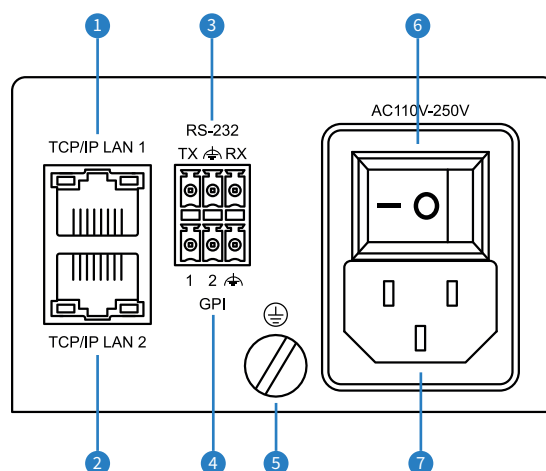
The PWR2IEC is an outlet-level metered and switched smart PDU. The unit features 1 x IEC C14 inlet for power (110-250V at up to 10A) and 2 x IEC C13 output outlets for supply to high-power consumption devices.

The PDU supports TCP/IP and RS-232 control, with a redundant TCP/IP port as a back-up. Front panel buttons for manual switching of power to individual outlets, and a single mains switch for overall system power. The PWR2IEC supports advanced power management features including scheduling, sequencing and power consumption. The GPI connections (x3) can also be used for automatic control of power to both inlet and individual outlet stages when triggered from 3rd party control platforms or BMS systems. Remote access and monitoring can be set-up and achieved via the web-GUI.

FEATURES:

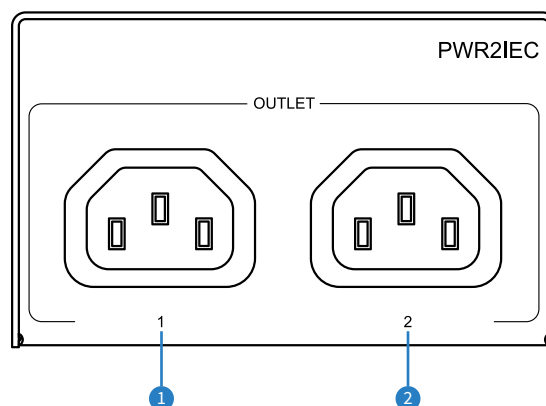
- Single C14 IEC inlet with 2 x C13 IEC outlets
- Products supports 110-250V AC power input up to 10A
- Monitoring and metering of Voltage, Current, Power, and Energy Consumption
- In-built self-healing through a 2-channel Watchdog, enabling adjustable ICMP or TCP monitoring per outlet, and automatic restarts to maintain uptime
- Overload Protection and Interference Filtering
- Advanced power management features including scheduling and power on/off sequencing
- Control via TCP/IP, RS-232, Front Panel buttons, or GPI's
- Dual TCP/IP network ports providing uninterrupted network service / access with SSL connectivity
- GPI's for automated switching of inlet, and individual power outlets
- Provides remote monitoring with password authentication through web-GUI
- Support multiple network and IoT protocols
- Wall / shelf mounting brackets included

Front Panel Description



- 1 TCP/IP Port LAN 1 — RJ45 port for network control
- 2 TCP/IP Port LAN 2 — RJ45 port for network control
- 3 RS-232 Serial Port — 3-pin Phoenix connector for serial control
- 4 GPIs — Phoenix connector triggers for individual outlets
- 5 Grounding Post
- 6 Power Switch
- 7 C14 IEC Power Connector

Rear Panel Description



- 1 C13 IEC Power Connector
- 2 C13 IEC Power Connector

Resetting the PWR2IEC

To reset the PWR2IEC back to factory defaults, press and hold outlet toggle buttons 1 & 2. Hold for at least 10 seconds before releasing.

The reset process takes approximately 30 seconds

Operation and Connections

Basic operation of the PWR2IEC can be achieved via the top panel. After connecting power to the rear of the unit, buttons 1-2 can be used to toggle the power outlets on or off.

For full configuration, the in-built Web GUI must be utilised.

Web GUI - Log In and Initialisation

The Web GUI allows for full configuration, ongoing maintenance and control of the PWR2IEC through a web portal. Connect a TCP/IP RJ45 socket from the local network, or directly from a computer, to the LAN 1 or LAN 2 port of the PWR2IEC in order to access the Web GUI.

By default, the PWR2IEC is set to obtain an IP address via DHCP; however, if a DHCP server (eg: network router) is not installed, the IP address will revert to below details:

Default IP Address is: **192.168.0.200**

Default Admin Username is: **blustream**

Default Admin Password is: **@Bls1234**

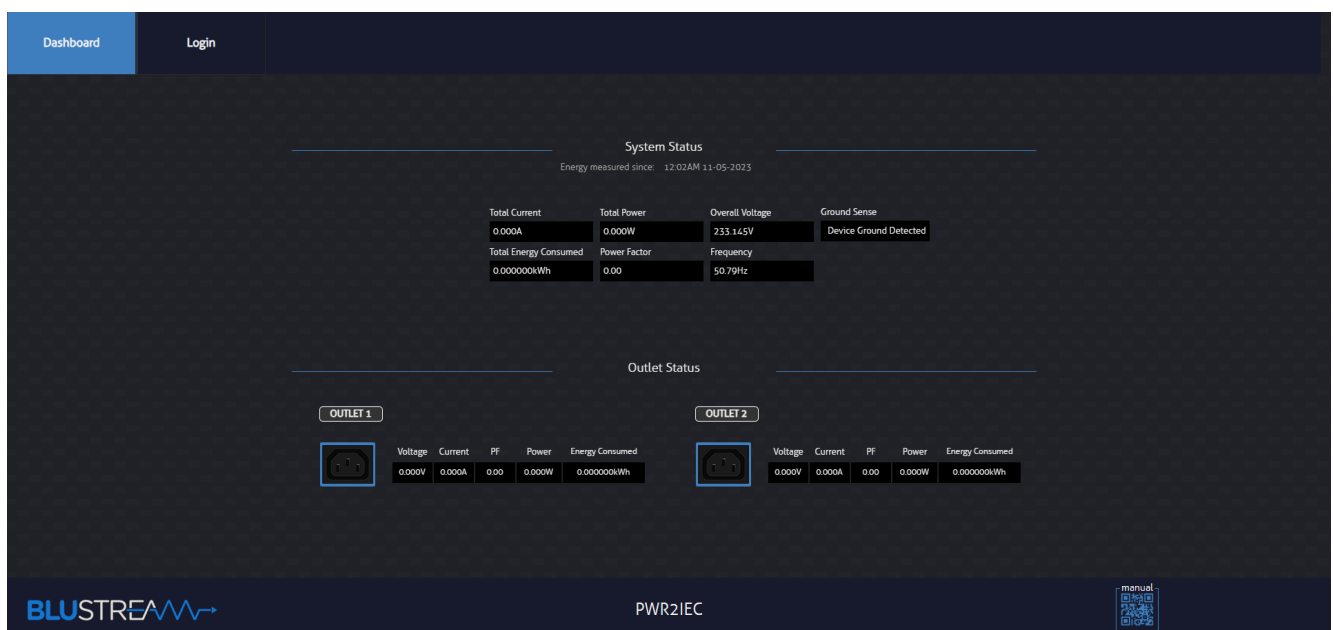
If the IP address of the PWR2IEC is not known, it can be found by:

- Using a 3rd party IP scanning tool
- Using an RS-232 connection and sending 'STATUS' command; this will return all settings of the XXXX
- Using the default mDNS hostname address
 - The PWR2IEC can be accessed via its mDNS hostname when the IP address is not known.
 - The default mDNS name is **pwr2iec.local**, which allows devices on the same local network to resolve the product's IP address without requiring a dedicated DNS server.

When initially accessing the Web GUI of the PWR2IEC, the Guest Dashboard page is shown as below.

Guest Dashboard Page:

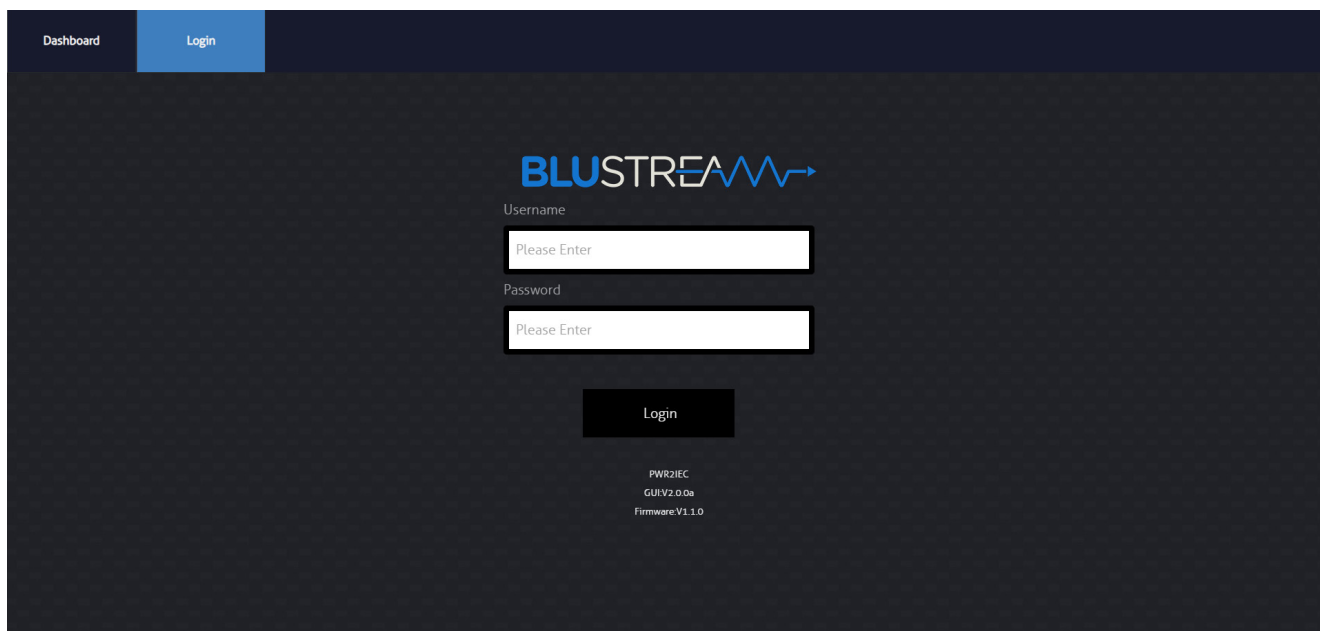
The Guest user is able to access the Dashboard page of the Web GUI without logging in. It provides a real time overview of the system and outlet status, including various metrics.



Login Page:

The Web GUI supports multiple users along with multiple user permissions as follows:

Administrator (Blustream)	The Administrator account allows full access to all functions and configuration of the device and is always enabled
User Accounts	User accounts can be utilised, each with individual login details and can be assigned permissions to specific areas and functions

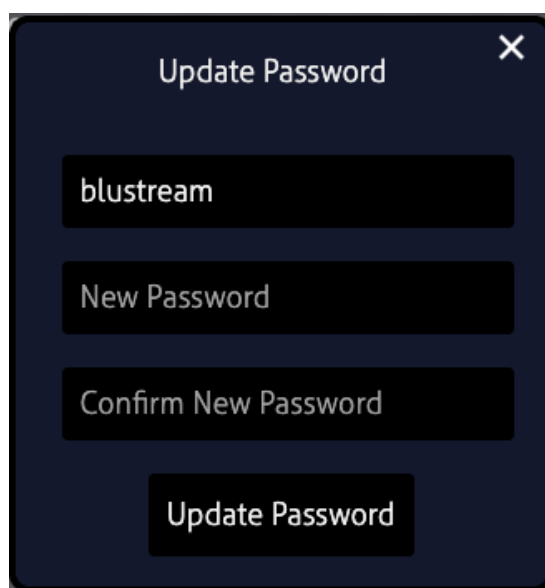


The screenshot shows the login interface of the Blustream PWR2IEC Web GUI. At the top, there is a dark blue navigation bar with 'Dashboard' and 'Login' tabs. The 'Login' tab is active. Below the navigation bar, the Blustream logo is centered. Under the logo, there are two input fields: 'Username' and 'Password', both with placeholder text 'Please Enter'. Below these fields is a 'Login' button. At the bottom of the login area, the following text is displayed: 'PWR2IEC', 'GUI V2.0.0a', and 'Firmware V1.1.0'.

Please note: The first time the Administrator logs into the Web GUI of the PWR2IEC the default password must be changed to a unique password. Please retain this password for future use. Forgetting the password will mean having to factory reset the device, losing all prior network and configuration settings.

New password regulations require passwords being set for products to be a minimum of 8 characters and contain a minimum of: 1 x uppercase letter, 1 x lowercase letter, 1 x symbol and 1 x number.

Passwords can be changed as required within the Web GUI of the device once logged in.



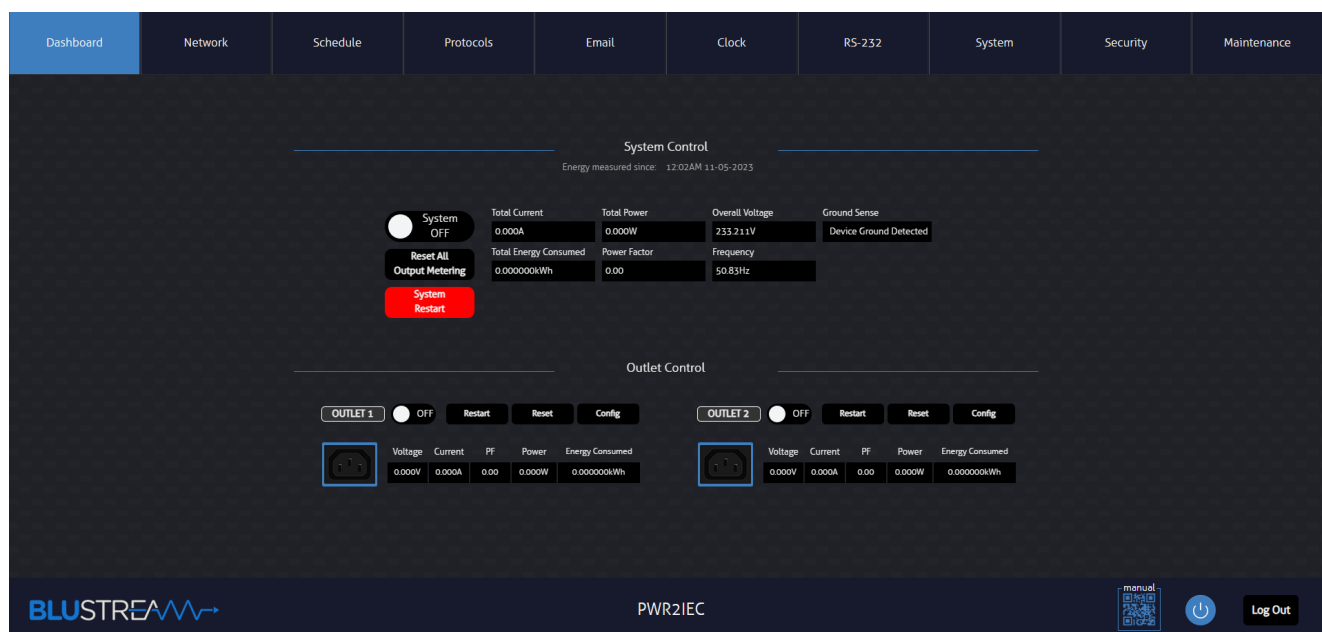
The screenshot shows a modal dialog box titled 'Update Password' with a close button (X) in the top right corner. The dialog contains three input fields: the first field is pre-filled with 'blustream', the second field is labeled 'New Password', and the third field is labeled 'Confirm New Password'. Below these fields is an 'Update Password' button.

Web GUI - Dashboard

Once logged in as the Administrator, the user will be directed to the Control page and additional pages become available from within the Web GUI. These can be navigated to by using the navigation bar at the top of the Web GUI and pressing the corresponding icon.

The buttons located at the bottom of the Web GUI provide access to product information, power on & off, and user logout.

The Dashboard page provides system level information, including power monitoring and ground status, and individual outlet information, providing real time status and power consumption data for each outlet.



System Control:

System ON / OFF

- Enable / disable power for all outputs. Does not power down the PWR2IEC

Reset All Output Metering

- Clear metering data for the system and all outlets

System Restart

- Cut power to each output individually then restart each output

Outlet Control:**Reset**

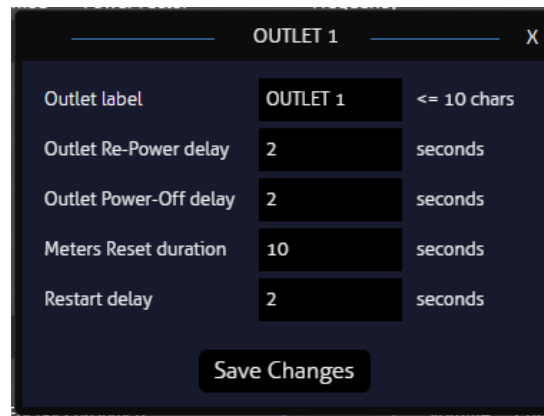
- Clear metering data for the selected outlet

Restart

- Power cycle the selected outlet. The duration of the power cycle is defined by Meters Reset Duration in the Config menu

Config

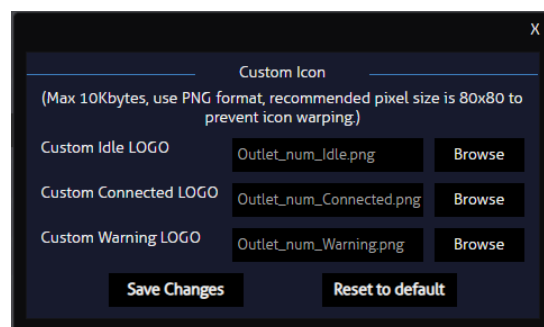
- Open a submenu to configure the selected outlet



- Outlet Label
 - Set the name of the outlet (maximum 10 alphanumeric characters)
- Outlet Re-Power Delay
 - Set a delay before the outlet is powered on when triggered
- Outlet Power-Off Delay
 - Set a delay before the outlet is powered off when triggered
- Meters Reset Duration
 - Set a delay when resetting the metering data
- Restart Delay
 - Set a delay when restarting the outlet
- Press Save Changes to apply any updated settings.

Clicking the IEC connector image allows the user to upload custom .png images for the device connected to the corresponding PWR2IEC outlet. Separate images can be assigned for the Idle, Connected, and Warning states.

Please note: Uploaded images must be in .png format, no larger than 10 KB in size, and should not exceed 80 x 80 pixels.



Outlet Control (continued)

The outlet icon and status indication will change based on the current operating state of the outlet. If custom images have been configured, the displayed icon will also update to match the outlet state.

Idle

- Indicates that no device is connected, or the connected device is not drawing power. The outlet icon is highlighted blue

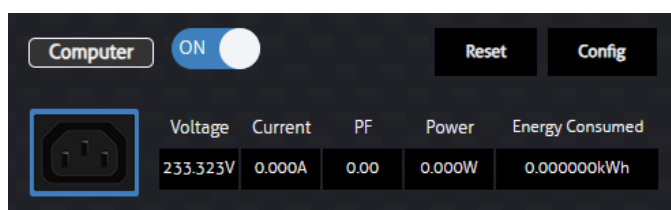
Connected

- Indicates that a device is connected and actively drawing power. The outlet icon is highlighted green

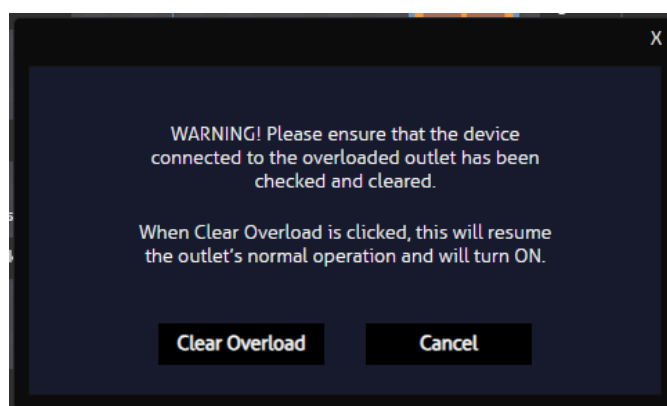
Warning

- Indicates that an abnormal voltage or overcurrent condition has been detected on the outlet
- When this occurs, the outlet is automatically powered off, and the icon is highlighted red
- When attempting to power the outlet back on, a warning dialog is displayed, allowing the warning state to be cleared and normal operation to resume
- Additional logic to handle overloaded outlets can be set on the System page of the Web GUI

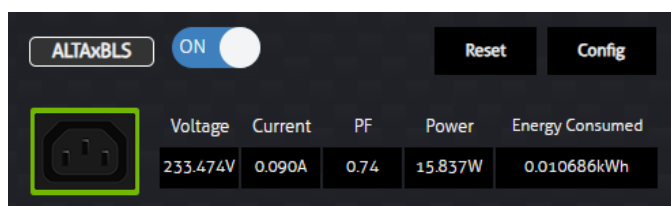
Outlet Idle State:



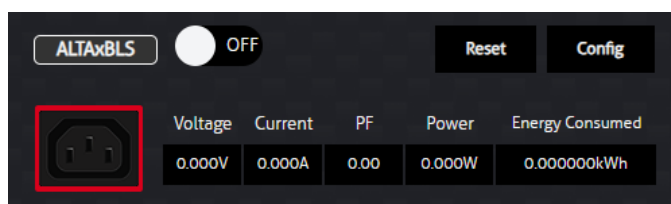
Outlet Warning Dialog:



Outlet Connected State:



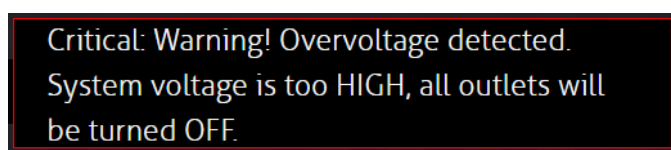
Outlet Warning State:



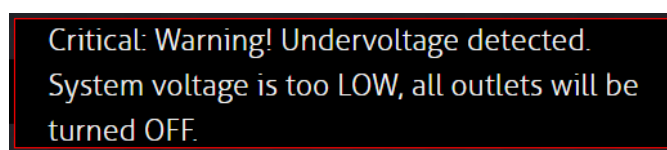
Additionally, the PWR2IEC features input power filtering and continuously monitors the incoming supply voltage for undervoltage and overvoltage conditions.

If an input voltage fault is detected, all outlets are automatically placed into a warning state and are powered off to protect connected equipment from potential damage. Once the input voltage returns to an acceptable operating range, the warning state can be cleared, allowing normal operation to resume.

Overvoltage Warning:



Undervoltage Warning:



Web GUI - Network

The Network page is used to configure the wired network interfaces, IPv4 and IPv6 addressing, Web GUI access, ICMP responses and mDNS discovery.

The PWR2IEC provides two independently configurable network interfaces. Each interface has a unique MAC address and can be connected to a separate network.

TCP/IP 1/2

MAC Address

- Displays the unique hardware address assigned to the selected TCP/IP interface

Use IPv4 DHCP

- Yes
 - Automatically obtains IPv4 addressing and network configuration settings from a DHCPv4 server
- Use Static IP
 - Allows IPv4 network settings to be configured manually

IPv4 Address

- Displays the current IPv4 address

IPv4 Netmask

- Displays the IPv4 subnet mask

IPv4 Gateway

- Displays the IPv4 default gateway

IPv4 DNS

- Displays the IPv4 address of the DNS server

Press Save Changes to apply any updated settings.

IPv6 Settings:

TCP/IP1 / TCP/IP2

- Select the interface to configure

Use IPv6 Protocol

- Enable / disable IPv6 communication on the selected interface

Use IPv6 Router Advertisement

- Enable / disable the use of IPv6 Router Advertisement (RA) information on the selected interface

IPv6 Settings

- DHCPv6
 - Automatically obtains IPv6 addressing and network configuration settings from a DHCPv6 server
- Manual
 - Allows IPv6 network settings to be configured manually

IPv6 Address

- Displays the current IPv6 address

IPv6 DNS Address 1

- Displays the IPv6 address of the preferred DNS server

IPv6 DNS Address 2

- Displays the IPv6 address of the secondary DNS server

IPv6 Gateway Address 1

- Displays the preferred IPv6 default gateway

IPv6 Gateway Address 2

- Displays the secondary IPv6 default gateway

Press Save Changes to apply any updated settings.

Web Server:

HTTP Server Port

- Set the TCP port used for unencrypted HTTP access to the Web GUI

HTTPS Server Port

- Set the TCP port used for encrypted HTTPS access to the Web GUI

TLS Versions

- Select the TLS (Transport Layer Security) version permitted for HTTPS connections

HTTP Server

- HTTP ONLY
 - Web GUI connections use unencrypted HTTP
- HTTPS ONLY
 - Web GUI connections use encrypted HTTPS

Reply ICMP PING

- Enable / disable whether the PWR2IEC responds to ICMP echo requests

Press Save Changes to apply any updated settings

Please note: Changing the HTTP or HTTPS mode or port may close the current Web GUI session.

mDNS:

mDNS is a protocol used in network environments to resolve hostnames to IP addresses within local networks without the need for a dedicated DNS server. The PWR2IEC can be accessed via the hostname if the IP address is not known.

By default, this is set to **pwr2iec.local**

mDNS On/Off

- Enable / disable mDNS advertisement

TCP/IP1 / TCP/IP2

- Select the network interface used for mDNS advertisement

Hostname

- Set the name advertised by the PWR2IEC through mDNS

Press Save Changes to apply any updated settings.

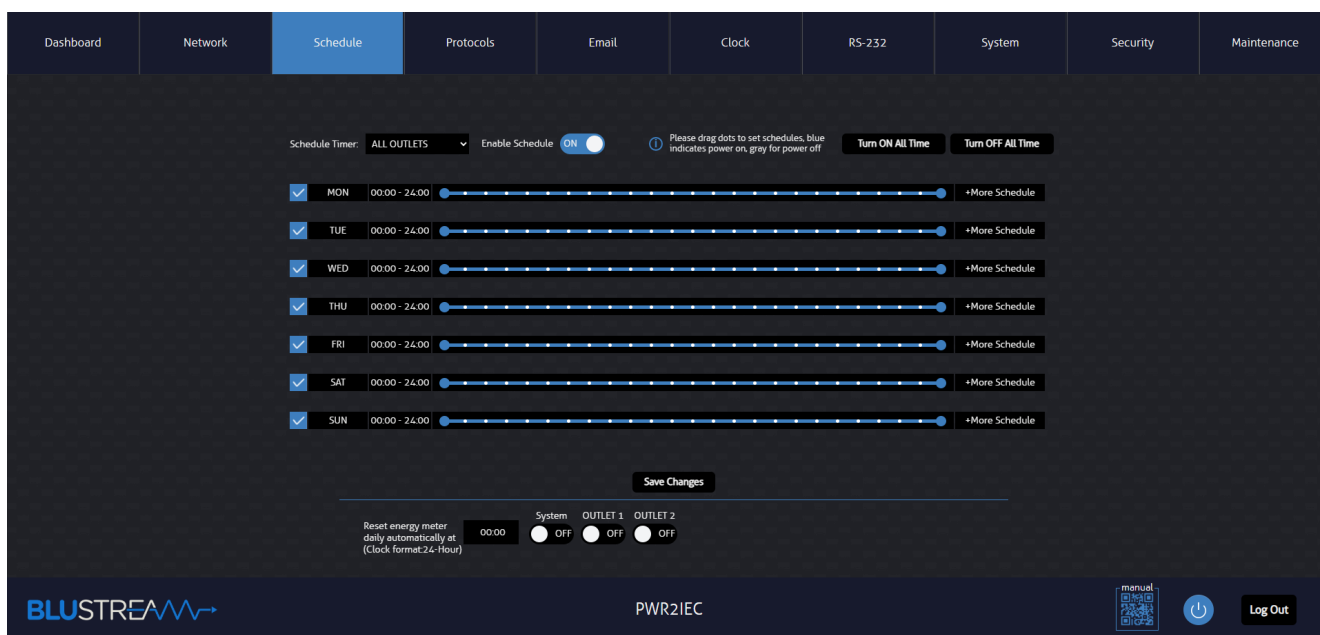
Web GUI - Schedule

The Schedule page allows for automatic control of the PWR2IEC outlets according to a weekly timetable. Scheduling can reduce power consumption when connected equipment is not required or periodically power cycling equipment that may become unresponsive after extended operation, such as satellite receivers.

Schedules operate across a seven-day week. Each day can contain one or more periods during which the selected outlet or outlets remain powered on.

The schedule page uses the PWR2IEC system clock. Before enabling a schedule, confirm that any time settings are configured correctly on the Clock page. An incorrect system clock will cause scheduled outlet events to occur at the wrong time.

Please note: The ALL OUTLETS schedule overrides the individual OUTLET 1 and OUTLET 2 schedules if a conflict occurs. For example, if the ALL OUTLETS schedule requires both outlets to be off while the OUTLET 1 schedule requires Outlet 1 to be on, the ALL OUTLETS schedule takes priority.



Schedule Timer

- Selects the outlet schedule to be viewed or configured

Enable Schedule

- Enable / disable scheduling for the selected schedule

Turn ON All Time

- Quickly configures the selected schedule so that the outlet remains powered on for the full 24-hour period on each day

Turn OFF All Time

- Quickly configures the selected schedule so that the outlet remains powered off for the full 24-hour period on each day

Web GUI - Schedule (continued)

Day Checkbox

- Enable / disable the configured time periods for that day

Time Interval

- Displays the start and end time of the scheduled on period
- The time display can be selected to enter the start and end times manually

Schedule Timeline

- The timeline represents the full 24-hour day. Drag the blue start and end markers along the timeline to define the period during which the selected outlet or outlets will be powered on:
 - Blue represents the period when the outlet is scheduled to be on
 - Grey represents the period the outlet is scheduled to be off
 - The left marker sets the scheduled on time
 - The right marker sets the scheduled off time

+More Schedule

- Adds another timeline to the selected day when equipment must turn on and off more than once during the same day. For example, an outlet could be scheduled to operate from 08:00 to 12:00 and again from 13:00 to 18:00
- After adding another period, set the start and end times using the new timeline controls or by manually entering the required times

- Press -Delete Schedule to remove added timelines

Press Save Changes to apply any updated settings.

Reset Energy Meter Daily Automatically At

- The metering displayed on the Dashboard can be reset automatically once per day, allowing data to be measured over a consistent daily period without requiring a manual reset. The energy meter reset function operates independently of the outlet power schedules
- Enter the reset time in 24-hour format, then select the meters to be reset

Web GUI - Protocols

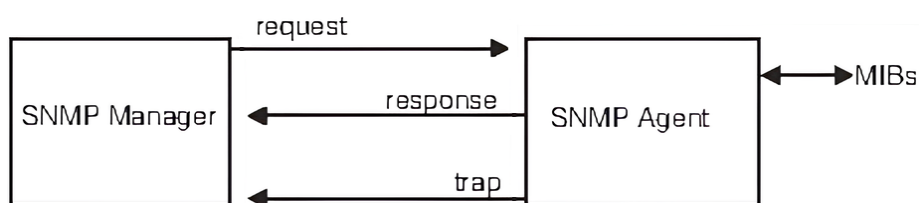
The Protocols page provides configuration and management of the communication services available on the PWR2IEC. These services allow the PWR2IEC to integrate with external control, monitoring, automation, and network management systems.

Each communication service includes a dedicated configuration page, enabling settings to be tailored to the requirements of the installation.

The following examples illustrate the configuration options available within the Protocols page.

SNMP (Simple Network Management Protocol):

SNMP is a widely used network management protocol that enables the monitoring and management of network devices. It allows external management systems to collect device information, monitor operational status, and receive notifications of events or faults.



The PWR2IEC includes an SNMP agent, which exposes device information through a Management Information Base (MIB). Network management software can communicate with the SNMP agent to retrieve status information, monitor device performance, and integrate the PWR2IEC into larger network management systems.

Enable SNMP V1 options	☒ SNMP GET ☒ SNMP SET
SNMP UDP port	161
sysContact(V1/V2C/V3)	
sysName(V1/V2C/V3)	
sysLocation(V1/V2C/V3)	
Enable SNMP V2C	☐ OFF
SNMP V1/V2C public community	public (Max 16 Chars)
SNMP V1/V2C private community	private (Max 16 Chars)
Enable SNMP V3	☐ OFF
SNMP V3 username	standard (Max 32 Chars)
SNMP V3 authorization algorithm	None
Set new authorization password	***** (8-32 Chars)
Repeat new authorization password	***** (8-32 Chars)
SNMP V3 private algorithm	None
Set new privacy password	***** (8-32 Chars)
Repeat new privacy password	***** (8-32 Chars)

SNMP (continued)

Enable SNMP V1 options

- SNMP GET
 - Enable / disable an SNMP manager to retrieve information from the PWR2IEC MIB
- SNMP SET
 - Enable / disable an SNMP manager to change supported values within the PWR2IEC MIB

SNMP UDP Port

- Set the UDP port used for SNMP requests. The default SNMP agent port is 161

sysContact / sysName / sysLocation

- SNMP system identification fields used to describe the device. These values are accessible through SNMP V1, V2C, and V3. Each field accepts a user-defined string of up to 255 characters

Enable SNMP V2C

- Enable / disable SNMP V2C communication

SNMP V1/V2C public community

- Set the community string used for read-only SNMP access

SNMP V1/V2C private community

- Set the community string used for read/write SNMP access

Please note: Both community strings accept up to 16 characters and must match the strings configured in the SNMP management system. Community strings act as credentials. Replace the default public and private values before connecting the PWR2IEC to a shared or accessible network.

Enable SNMP V3

- Enable / disable SNMP V3 communication. SNMP V3 supports username-based access with optional authentication and privacy protection

SNMP V3 Username

- Set the username used for SNMP V3 access

SNMP V3 Authorization Algorithm

- Set the algorithm used to authenticate SNMP V3 messages. Available options include:
 - None / MD5 / SHA1 / SHA2-25 / SHA2-384 / SHA2-512

Authorization Password

- Set new authorization password
- Repeat new authorization password

SNMP (continued)

SNMP V3 Privacy Algorithm

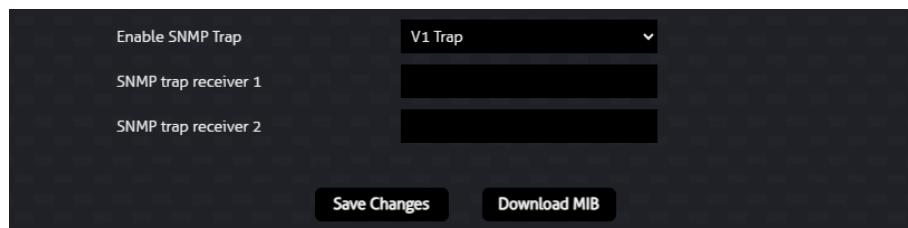
- Selects the encryption algorithm used to protect SNMP V3 communication. Available options include:
 - None / DES / AES / AES-128

Privacy Password

- Set new privacy password
- Repeat new privacy password

SNMP Traps:

SNMP traps are unsolicited event notifications sent by the PWR2IEC to an SNMP manager or trap receiver. Traps allow significant events to be reported immediately without waiting for the SNMP manager to poll the device. When a trap event occurs, the PWR2IEC sends the notification to the configured receiver addresses using the selected SNMP trap version.



Enable SNMP Trap

- Select the SNMP version used for trap notifications:
 - V1 Trap
 - V2C Trap
 - V3 Trap

SNMP Trap Receiver 1 and 2

- Set the IP addresses of up to two SNMP managers or trap receivers.
 - SNMP Trap Receiver 1
 - SNMP Trap Receiver 2

Select Save Changes to apply any updated settings.

Select Download MIB to download the PWR2IEC Management Information Base file. Import the MIB into a compatible SNMP management platform to identify the objects, values and commands supported by the PWR2IEC.

SNMP Example Setup:

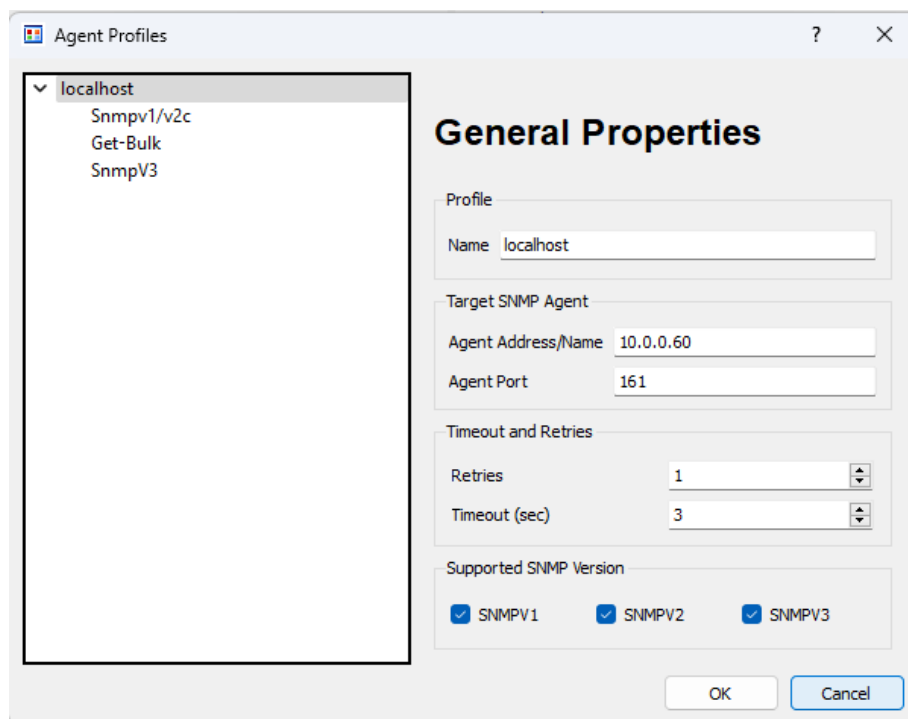
The following example demonstrates how to configure the PWR2IEC as an SNMP agent and verify communication using snmpB. Other compatible SNMP manager applications may also be used.

1. Complete the SNMP settings in the Web-GUI. Ensure that the SNMP trap receiver is set to the IP address of the device running the snmpB software.

Enable SNMP V1 options	☒ SNMP GET ☒ SNMP SET
SNMP UDP port	161
sysContact(V1/V2C/V3)	
sysName(V1/V2C/V3)	
sysLocation(V1/V2C/V3)	
Enable SNMP V2C	☐ OFF
SNMP V1/V2C public community	public (Max 16 Chars)
SNMP V1/V2C private community	private (Max 16 Chars)
Enable SNMP V3	☐ OFF
SNMP V3 username	standard (Max 32 Chars)
SNMP V3 authorization algorithm	None
Set new authorization password	***** (8-32 Chars)
Repeat new authorization password	***** (8-32 Chars)
SNMP V3 private algorithm	None
Set new privacy password	***** (8-32 Chars)
Repeat new privacy password	***** (8-32 Chars)
Enable SNMP Trap	V1 Trap
SNMP trap receiver 1	
SNMP trap receiver 2	
Save Changes Download MIB	

SNMP Example Setup (continued)

2. Open the snmpB software and navigate to Options > Manage Agent Profiles and create a new user. Set the Agent Address to the IP address of the PWR2IEC and the Agent Port to the SNMP UDP port defined in the Web GUI.

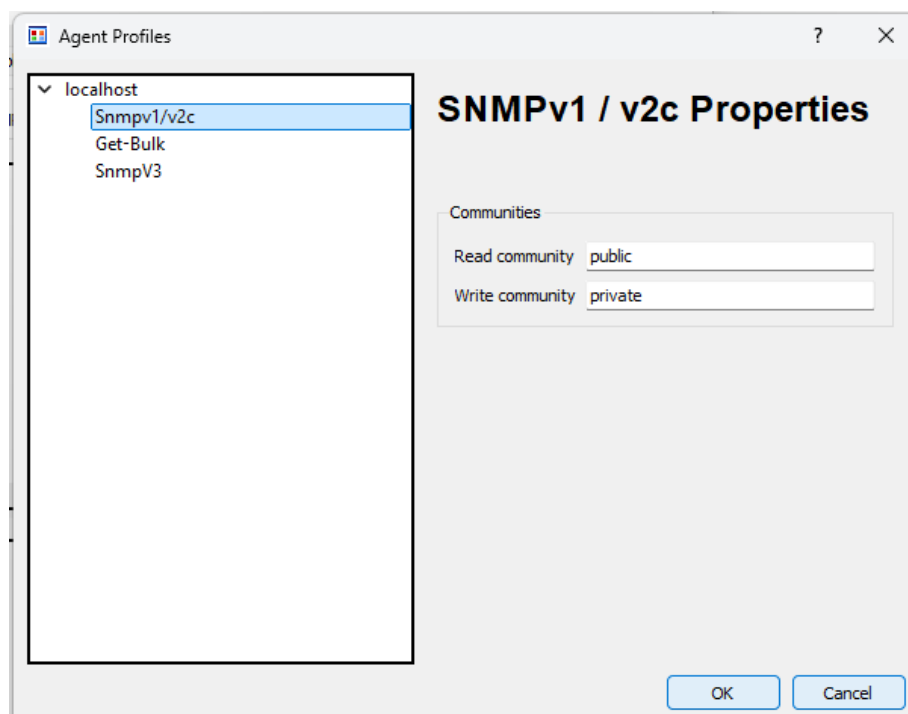


The 'Agent Profiles' dialog box is shown with the 'localhost' profile selected. The 'General Properties' section on the right contains the following fields:

- Profile:** Name: localhost
- Target SNMP Agent:** Agent Address/Name: 10.0.0.60, Agent Port: 161
- Timeout and Retries:** Retries: 1, Timeout (sec): 3
- Supported SNMP Version:** ☒ SNMPV1, ☒ SNMPV2, ☒ SNMPV3

Buttons at the bottom: OK, Cancel.

3. Set the Snmpv1 > v2c public and private communities to SNMP v2 public and private communities defined in the Web GUI.



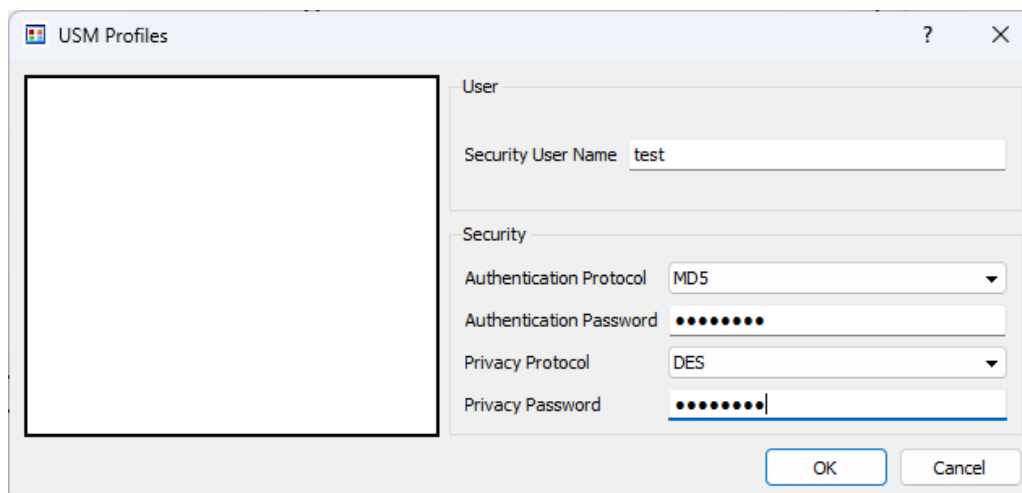
The 'Agent Profiles' dialog box is shown with the 'localhost' profile selected and 'Snmpv1/v2c' highlighted. The 'SNMPv1 / v2c Properties' section on the right contains the following fields:

- Communities:** Read community: public, Write community: private

Buttons at the bottom: OK, Cancel.

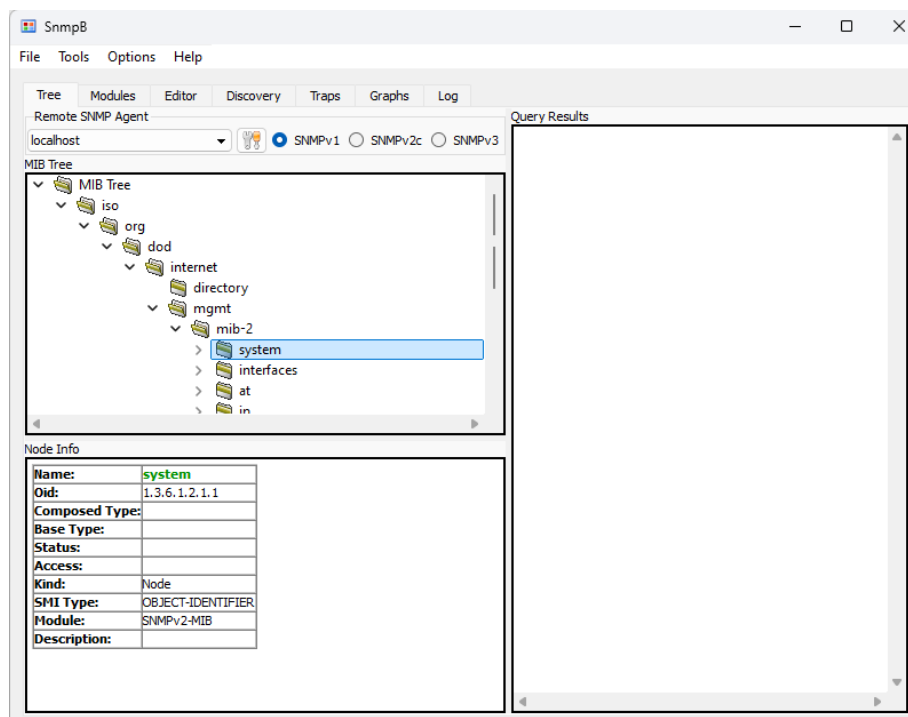
SNMP Example Setup (continued)

4. Navigate to Options > Manage SNMPv3 USM Profiles and configure the fields to match the settings defined under SNMPv3 in the Web GUI.



5. You can now verify if the software can communicate with the PWR2IEC.
On the main screen, with SNMPv1 selected, navigate through the MIB tree to find the system folder:

iso
 org
 dod
 internet
 mgmt
 mib-2

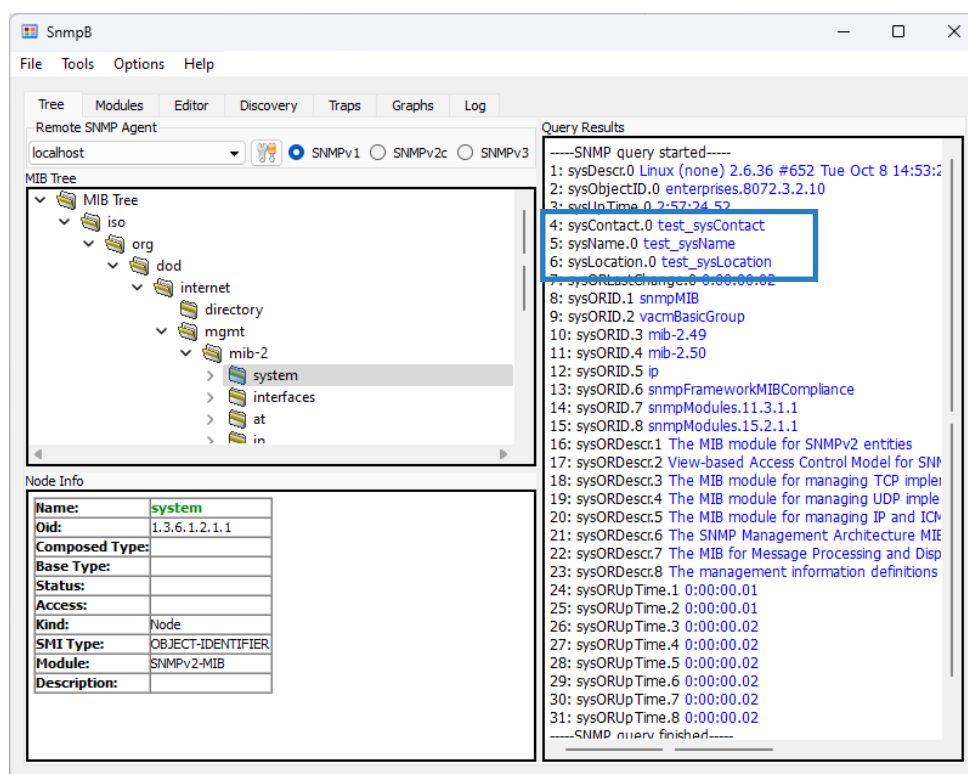


SNMP Example Setup (continued)

6. Right click on system and press 'Walk'.

Under Query Results, look for the labels defined for sysContact, sysName, sysLocation in the Web-GUI.

If they appear with the correct labels, then the SNMP protocol is working



Telnet:

The Telnet page configures Telnet access to the PWR2IEC. Telnet can be used with a standard terminal client or in raw mode for integration with 3rd party control systems, scripts, and custom applications.

Enable Telnet	☒	
Telnet TCP port	23	(Default: 23)
Raw mode	☒	
Active negotiation	☐	OFF
Activate echo	☒	
Push messages	☒	
Delay after 3 failed logins	☒	
Require login (Telnet)	☐	OFF
Use password	Local stored password	>> RADIUS settings
Local username	admin	(Max 12 Char.)
Local password	*****	(Max 8 Char.)
<button>Save Changes</button>		

Enable Telnet

- Enable / disable Telnet control of the PWR2IEC

Telnet TCP Port

- Set the TCP port to use for Telnet connections. The default port is 23

Raw Mode

- Controls how data is exchanged with the connected client:
 - When enabled, data is sent and received directly without standard Telnet negotiation or control sequences. Use this mode with custom scripts, control systems or applications that require a raw TCP connection
 - When disabled, standard Telnet protocol handling is used. Use this mode with a Telnet compatible terminal client

Active Negotiation

- Enable / disable active Telnet option negotiation when a client connects. This setting is normally disabled when Raw Mode is enabled

Activate Echo

- Enable / disable whether entered commands are echoed back to the connected terminal or console

Push Messages

- Enable / disable automatic status and notification messages within the active Telnet session

Delay After 3 Failed Logins

- Enable / disable a disconnect after three consecutive unsuccessful login attempts

Telnet (continued)

Require Login (Telnet)

- Enable / disable whether credentials are required when establishing a Telnet connection

Use Password

- Select the authentication source used when Require Login (Telnet) is enabled:
- Local stored password
 - Use the username and password configured on this page
- RADIUS Server password
 - Use the RADIUS authentication settings configured in the Security page

Local Username

- Set the username used for local Telnet authentication

Local Password

- Set the password used for local Telnet authentication

Select Save Changes to apply any updated settings.

Telnet Setup Example:

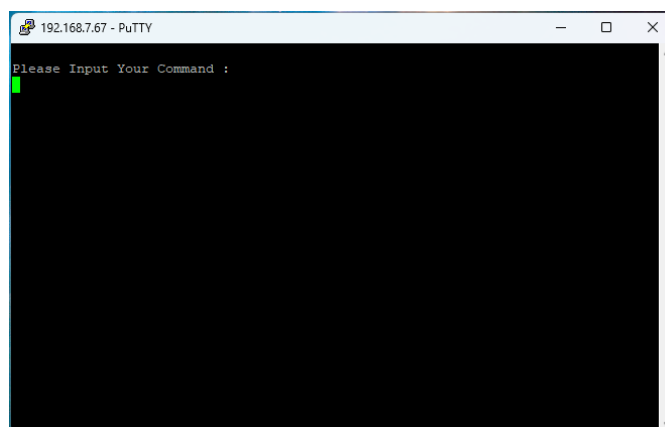
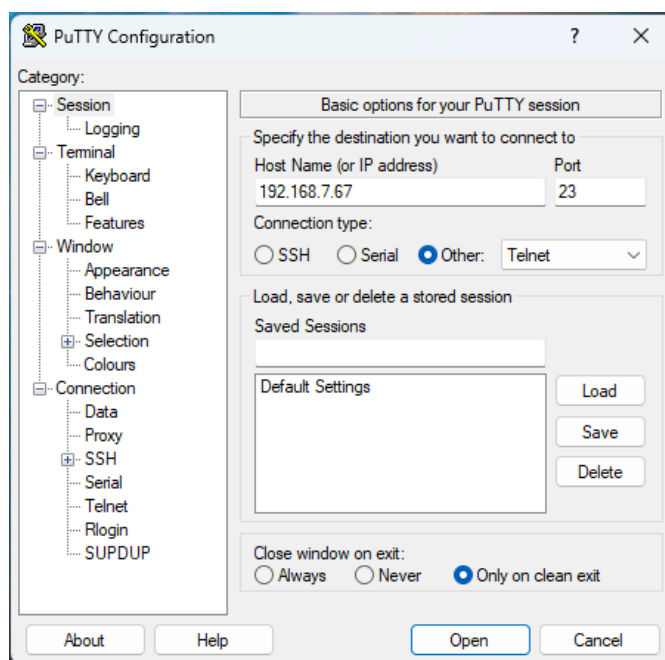
The following example demonstrates how to establish a Telnet connection to the PWR2IEC and send control commands using a terminal application. Telnet must be enabled before a client or 3rd party control system can connect.

Please note: Telnet is unencrypted. Use SSH where secure communication is required.

A Telnet connection can be made using a terminal application such as PuTTY, a command-line Telnet client, or a compatible 3rd party control system.

The controlling device must be connected to the same network as the PWR2IEC and must be able to reach its IP address.

1. Open PuTTY, enter the IP address of the PWR2IEC in the Host Name field, select Telnet as the connection type and open the connection.
2. If login authentication is enabled, enter the configured username and password.
3. Input the desired control command.



MQTT (Message Queuing Telemetry Transport):

The MQTT page configures the PWR2IEC as an MQTT client for integration with monitoring platforms, automation systems and 3rd party controllers. MQTT uses a lightweight publish/subscribe model in which clients exchange messages through a central broker rather than communicating directly with one another.

Enable MQTT

- Enable / disable MQTT communication.

Broker Status

- Displays the current connection state and activity

Broker Host

- Set the hostname or IP address of the MQTT broker

Broker TCP Port

- Set the TCP port used to connect to the MQTT broker. The default value is 1883

MQTT (continued)

Enable SSL/TLS

- Enable / disable SSL/TLS security for the connection between the PWR2IEC and MQTT broker
- When enabled, upload the certificate files required by the broker configuration

SSL CA File

- Select the CA (Certificate Authority) file used to verify the identity of the MQTT broker

SSL Certificate File

- Select the client certificate used by the PWR2IEC to authenticate with the MQTT broker when client certificate authentication is required

SSL Key File

- Select the private key associated with the uploaded client certificate

Please note: The required files depend on the broker's TLS configuration. The client certificate and key may not be required when the broker only requires server verification.

Use Credentials

- Enable / disable username and password authentication with the MQTT broker

Username

- Set the username for MQTT broker authentication

Password

- Set the password for MQTT broker authentication

Client ID for PWR2IEC Status

- Set a unique MQTT client identifier to be used for PWR2IEC status monitoring

Topic for PWR2IEC Status

- Set the topic used to publish PWR2IEC status and monitoring data
- 3rd party MQTT clients can subscribe to this topic

Client ID for PWR2IEC Control

- Set a unique MQTT client identifier to be used for PWR2IEC control monitoring

Topic for PWR2IEC Control

- Set the topic used to publish PWR2IEC control data
- 3rd party MQTT clients can subscribe to this topic

Client ID for PWR2IEC Feedback of Control Commands

- Set a unique MQTT client identifier to be used for publishing feedback in response to control commands

Topic for PWR2IEC Feedback of Control Commands

- Set the topic used to publish PWR2IEC control data
- 3rd party MQTT clients can subscribe to this topic

Please note: MQTT topics use a hierarchical structure, with each level normally separated by a forward slash. The topics entered into the PWR2IEC and 3rd party system must match exactly.

MQTT (continued)

Quality of Service (QoS)

- QoS 0 (at most once)
 - Sends the message without an acknowledgement. Delivery is not guaranteed
- QoS 1 (at least once)
 - Requires an acknowledgement. Delivery is assured, but duplicate messages may occur

Keep-Alive Ping Interval

- Set the maximum interval, in seconds, between MQTT control packets sent by the PWR2IEC. When no other packet needs to be sent, MQTT uses keep-alive messaging to confirm that communication with the broker remains available

Publish Device Data Summary Interval

- Set how frequently, in seconds, the PWR2IEC publishes its device summary data to the configured status topic
- Set to 0 to disable

Select Save Changes to apply any updated settings.

MQTT Setup Example:

The following example demonstrates how to connect the PWR2IEC to an MQTT broker and subscribe to its status topic using MQTTX and the HiveMQ public broker. Other compatible MQTT clients and brokers may also be used.

Please note: Use public brokers for testing only. Use a secured private broker for deployed systems.

1. Setup the MQTT tab with the public HiveMQ broker host and port, and set at least one client ID and topic:

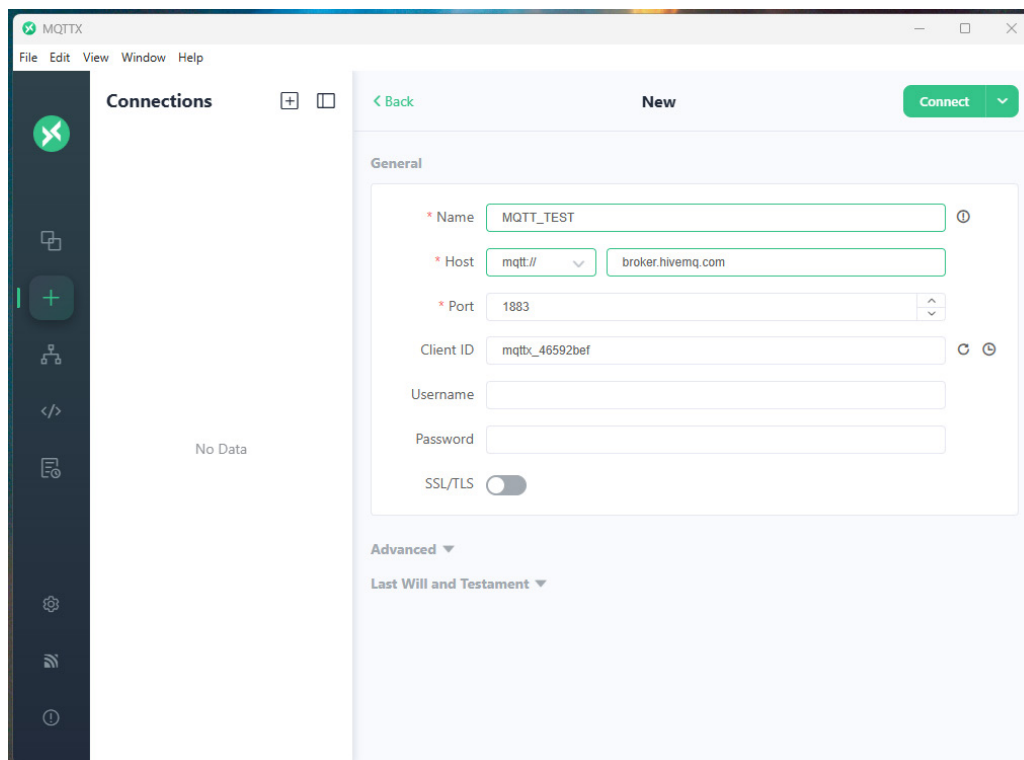
Host: broker.hivemq.com

TCP Port: 1883

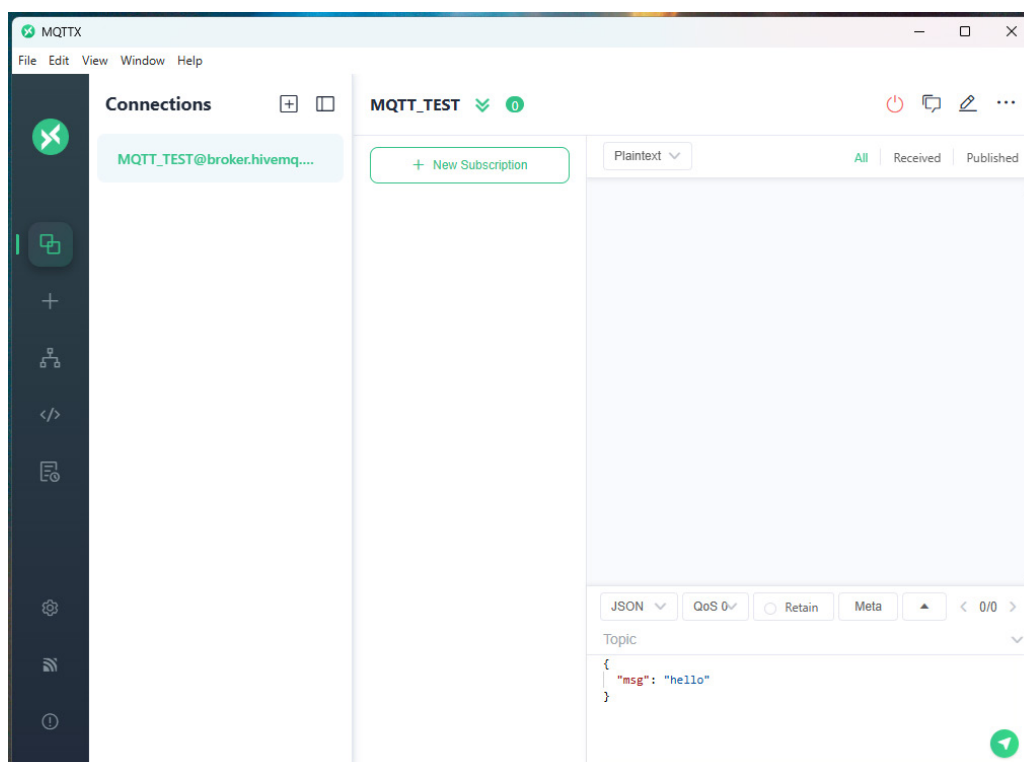
Enable MQTT	☒ ON	
Broker Status	Broker DNS ready, connected since 17s Last publish 7s ago, last incoming subscription 0s ago	
Broker Host	broker.hivemq.com	
Broker TCP Port	1883	(Default:1883.)
Enable SSL/TLS	☐ OFF	
SSL CA file	C://	Browse
SSL certificate file	C://	Browse
SSL Key file	C://	Browse
Use credentials	☐ OFF	
Username		
Password		
Client ID for PWR2IEC status	PWR2IEC-001-STATUS	Specify Client ID for monitoring status.
Topic for PWR2IEC status	blustream/pwr2iec/001/status	Use topic to monitor status of the PWR2IEC.
Client ID for PWR2IEC control	PWR2IEC-001-CONTROL	Specify Client ID for 3rd-party control.
Topic for PWR2IEC control	blustream/pwr2iec/001/control	Use topic to send commands to the PWR2IEC using 3rd party control.
Client ID for PWR2IEC feedback of control commands	PWR2IEC-001-FEEDBACK	Specify Client ID for control feedback.
Topic for PWR2IEC feedback of control commands	blustream/pwr2iec/001/feedback	Use topic to monitor control feedback from the PWR2IEC using 3rd party control.
Quality of Service (QoS)	☒ QoS 0 (at most once) ☐ QoS 1 (At least once)	
Keep-alive ping interval	60	seconds (Min.10 seconds)
Publish device data summary interval	10	seconds (0 for disabled)
Save Changes		

MQTT Setup Example (continued)

2. Open the MQTTX software and setup a new connection to the HiveMQ broker. Enter a unique connection name, the HiveMQ broker host and port, and a unique MQTT Client ID. The MQTTX client ID must be different from the client ID assigned to the PWR2IEC.
Press Connect once finished.

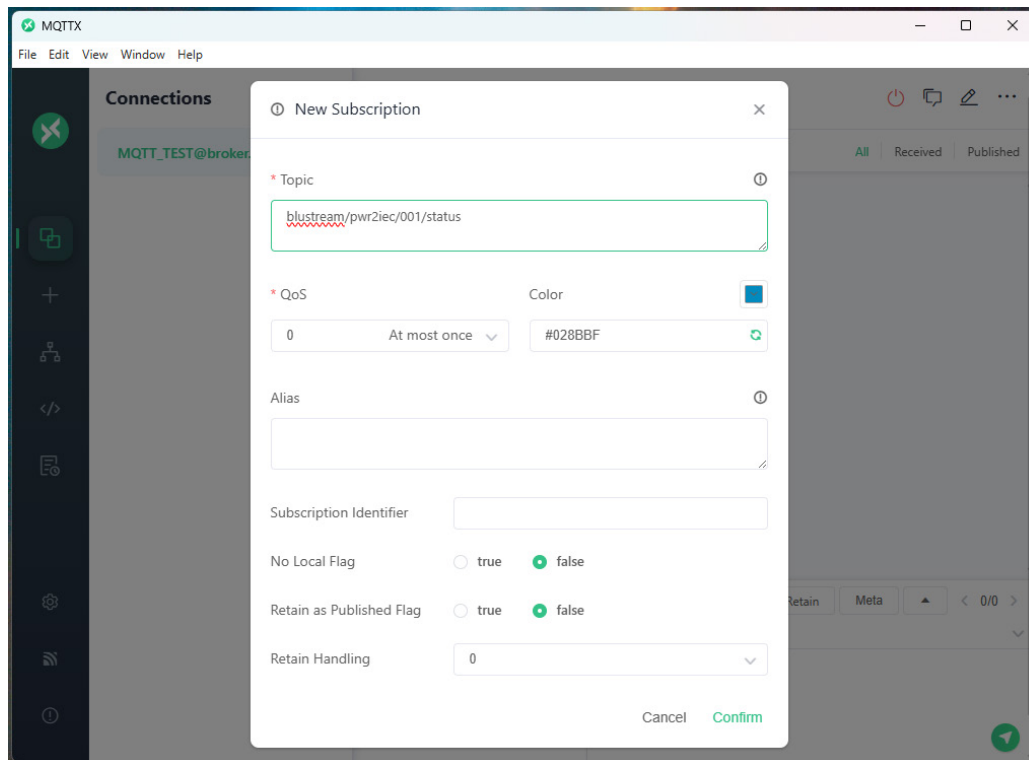


3. Once connected, press + New Subscription to subscribe to a topic.

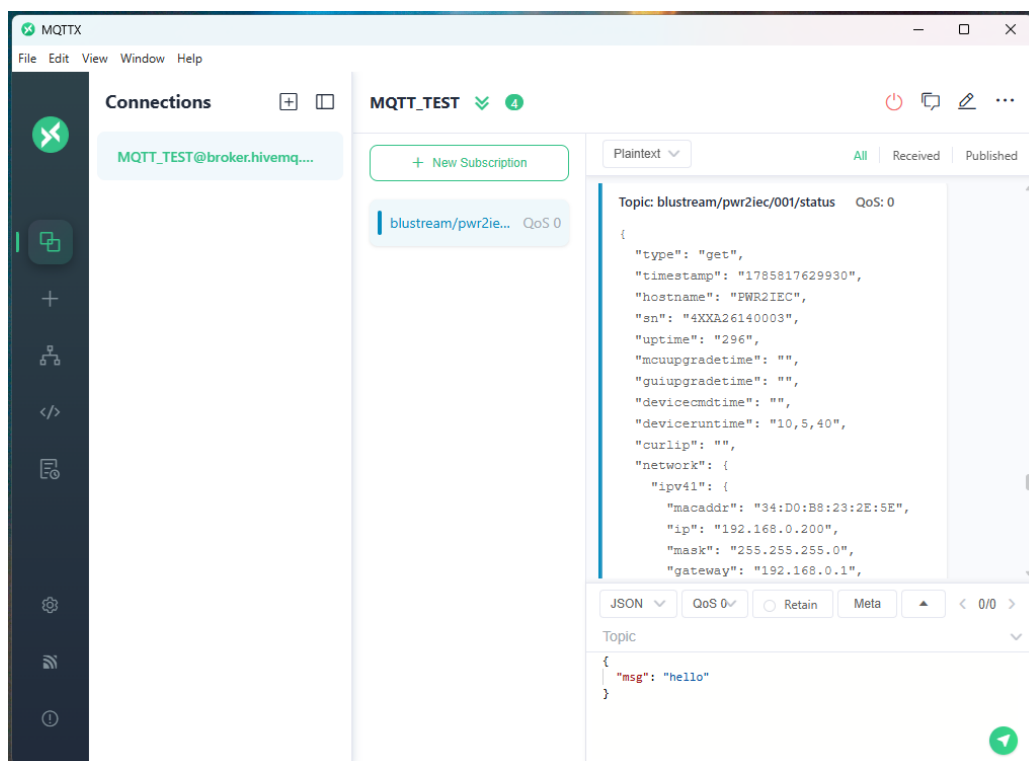


MQTT Setup Example (continued)

4. Create a new subscription using the topic configured in the PWR2IEC and select the same QoS level used by the PWR2IEC.



5. If the connection and topic are configured correctly, messages from the PWR2IEC will appear in MQTTX at the configured publish interval.



SSH (Secure Shell Protocol):

The SSH page configures secure, encrypted command-line access to the PWR2IEC. SSH provides confidentiality, connection integrity and authentication when sending commands across an IP network.

Enable SSH ☐ OFF

SSH TCP port (Default: 22)

Activate echo ☒ ON

Push messages ☒ ON

Require login (SSH) ☒ ON

Use password >> RADIUS settings

Local username (Max 12 Char.)

Local password (Max 8 Char.)

New SSH public key

Save Changes

Enable SSH

- Enable / disable SSH access to the PWR2IEC.

SSH TCP Port

- Set the TCP port used for SSH connections. The default port is 22.

Activate Echo

- Enable / disable whether entered commands are echoed back to the connected terminal or console.

Push Messages

- Enable / disable automatic status and notification messages within the active SSH session.

Require Login (SSH)

- Enable / disable whether authentication is required when establishing an SSH connection.

Use Password

- Select the authentication source used when Require Login (SSH) is enabled:
- Local stored password
 - Use the username and password configured on this page
- RADIUS Server password
 - Use the RADIUS authentication settings configured in the Security page

Local Username

- Set the username used for local SSH authentication

Local Password

- Set the password used for local SSH authentication

New SSH Public Key

- Allows an SSH public key to be entered for public key authentication

Select Save Changes to apply any updated settings.

SSH Setup Example:

The following example demonstrates how to establish an encrypted SSH connection to the PWR2IEC using a compatible terminal application with an SSH Key.

An SSH connection can be made using a terminal application, a command line SSH client, or a compatible 3rd party control system.

The client must be connected to the same network as the PWR2IEC and must be able to reach its IP address.

1. Generate a public / private SSH keypair. Copy the generated public key and paste it into the SSH public key field in the PWR2IEC Web GUI, then save the configuration. Store the private key in the appropriate location.
2. Open the terminal application and connect to the PWR2IEC via SSH.
3. The first time a connection is made, a security warning may be displayed for the host key. Confirm that the connection is being made to the correct device, then accept the host key to continue.
4. Enter the configured username and password when prompted, if password authentication is enabled.
5. Input the desired control command.

```

CA\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.26200.8875]
(c) Microsoft Corporation. All rights reserved.

C:\Users\DanielHenriksen>ssh pwr2iec-user@192.168.7.67

```

```

CA\WINDOWS\system32\cmd.exe - ssh pwr2iec-user@192.168.7.67
Microsoft Windows [Version 10.0.26200.8875]
(c) Microsoft Corporation. All rights reserved.

C:\Users\DanielHenriksen>ssh pwr2iec-user@192.168.7.67
The authenticity of host '192.168.7.67 (192.168.7.67)' can't be established.
ED25519 key fingerprint is SHA256:EPdv2eU0+9yd2S5Zvf8ZKgR6Bff0cAZZGTx6Xt5Cy4g.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? _

```

```

CA\WINDOWS\system32\cmd.exe - ssh pwr2iec-user@192.168.7.67
Microsoft Windows [Version 10.0.26200.8875]
(c) Microsoft Corporation. All rights reserved.

C:\Users\DanielHenriksen>ssh pwr2iec-user@192.168.7.67
The authenticity of host '192.168.7.67 (192.168.7.67)' can't be established.
ED25519 key fingerprint is SHA256:EPdv2eU0+9yd2S5Zvf8ZKgR6Bff0cAZZGTx6Xt5Cy4g.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.7.67' (ED25519) to the list of known hosts.
pwr2iec-user@192.168.7.67's password:

```

```

pwr2iec-user@192.168.7.67's password:
status
      PWR2IEC 2 Port IEC Power Controller
      FW Version: V1.1.0

Power  Key   Relay   TCP/IP   Baud   Current_Threshold   OverVoltage
old    Ground_Sense   ON      2       57600   10.9A              250V
ON     Device_Ground_Detected

Outlet Status Mode      PowerOnTime   PowerOffTime   PowerRestaTime   EL
1      ON      Idle      2s           2s           2s           10
2      ON      Connected 3s           3s           3s           10
SVS    ON      Normal

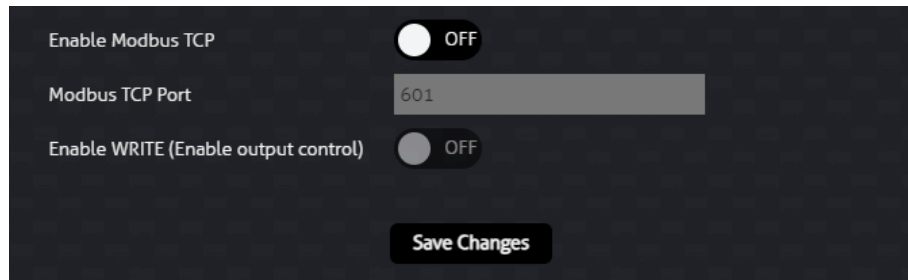
SafeMode RelayMode RelayVoltage StandbyMode OverloadRetryCNT
Outlet_Shutdown Push_Button Low_Voltage All_Standby_Mode 1

VoltMonitorMode VoltMonitorRetryTime
All_Outlets_Shutdown 3mins

```

Modbus:

The Modbus page configures Modbus TCP communication, allowing compatible control and monitoring systems to read PWR2IEC status information and, when explicitly enabled, control the outlets by writing to supported registers.



The image shows a dark-themed configuration window for Modbus. It contains three settings: 'Enable Modbus TCP' with a toggle switch set to 'OFF', 'Modbus TCP Port' with a text input field containing '601', and 'Enable WRITE (Enable output control)' with a toggle switch set to 'OFF'. At the bottom is a 'Save Changes' button.

Enable Modbus TCP

- Enable / disable the Modbus TCP server.

Modbus TCP Port

- Set the TCP port on which the PWR2IEC accepts Modbus connections.

Enable WRITE (Enable Output Control)

- Enable / disable whether Modbus clients can write to supported registers and operate the PWR2IEC outlets.

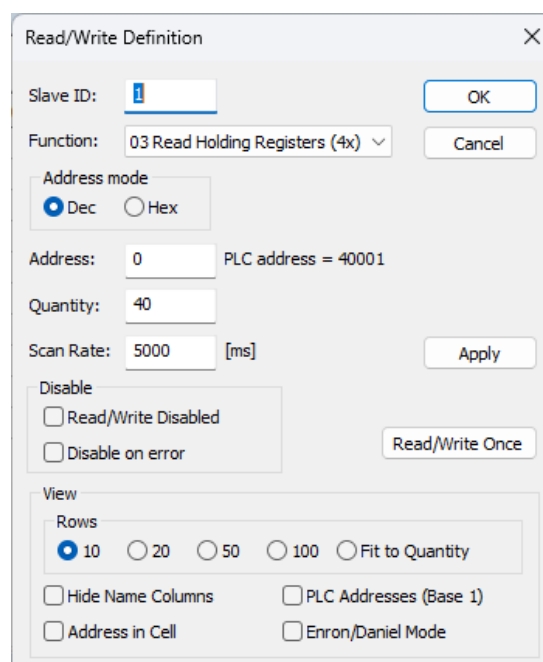
Please note: Enable WRITE only when remote outlet control is required. Standard Modbus TCP does not provide native encryption or authentication, so access should be restricted to trusted devices on a protected network. Disable WRITE when it is not required and do not expose the Modbus service to an open or public network

Select Save Changes to apply any updated settings.

Modbus Setup Example:

The following example demonstrates how to connect to the PWR2IEC and read register data using Modbus Poll. Other compatible Modbus TCP clients may also be used.

1. Open Modbus Poll, then select:
Setup > Read/Write Definition
Set Quantity to 40 and Scan Rate to 5000 ms



The image shows a 'Read/Write Definition' dialog box. It has fields for 'Slave ID' (set to 1), 'Function' (set to '03 Read Holding Registers (4x)'), 'Address' (set to 0, with 'PLC address = 40001' displayed next to it), 'Quantity' (set to 40), and 'Scan Rate' (set to 5000 [ms]). There are 'OK', 'Cancel', and 'Apply' buttons. Below these are checkboxes for 'Disable' (Read/Write Disabled, Disable on error) and a 'Read/Write Once' button. At the bottom, there are 'View' options: 'Rows' (10, 20, 50, 100, Fit to Quantity), 'Hide Name Columns', 'PLC Addresses (Base 1)', 'Address in Cell', and 'Enron/Daniel Mode'.

Modbus Setup Example (continued)

2. Select:
 Connection > Connect
 Enter the IP address of the PWR2IEC, set the server port to the Modbus TCP Port configured in the Web GUI, and set Connect Timeout to 5000 ms.

Connection Setup

Connection
 Modbus TCP/IP

Serial Settings
 COM1
 9600 Baud
 8 Data bits
 Even Parity
 1 Stop Bit

Mode
☒ RTU ☐ ASCII

Response Timeout
 1000 [ms]

Delay Between Polls
 20 [ms]

Remote Modbus Server
 IP Address or Node Name
 10.0.0.60

Server Port: 601 **Connect Timeout:** 5000 [ms] ☒ IPv4 ☐ IPv6

3. Open the connection. Once connected, Modbus Poll will begin reading the PWR2IEC registers and displaying the received data.

Modbus Poll - Mbpoll1

File Edit Connection Setup Functions Display View Window Help

05 06 15 16 17 22 23 TC

Tx = 94: Err = 7: ID = 1: F = 03: SR = 5000ms

	Name	00000	Name	00010	Name	00020	Name	00030
0	230	0		0		0		0
1	564	0		0		0		725
2	230	0		10		0		0
3	564	0		310		0		0
4	230	0		0		0		0
5	564	91		0		0		0
6	230	0		0		0		0
7	564	0		0		0		0
8	0	0		0		0		0
9	0	0		70		480		

For Help, press F1.

[10.0.0.60]: 601

	Voltage	Current	PF	Power	Energy Consumed
	230.564V	0.000A	0.00	0.000W	0.000000kWh

	Voltage	Current	PF	Power	Energy Consumed
	230.564V	0.000A	0.00	0.000W	0.000000kWh

Watchdog:

A Watchdog (IP Watchdog) is an automated monitoring tool that periodically sends network packets (pings) to a specific IP address to check if a device or network connection is operational. If the monitored target fails to respond within a set time or number of attempts, the Watchdog can take a specified action.

Each Outlet can have a separate Watchdog enabled.

The Recent Ping field will display the time in milliseconds it took the host to respond to the most recent ping.

Outlet 1 / 2

- Select the outlet for which the Watchdog settings are displayed and configured

Enable / Disable

- Enable / disable the Watchdog for the selected outlet

Watchdog Ping Configuration:

Ping Type

- ICMP
 - Send standard ICMP echo requests to test basic network availability. The target must be configured to respond to ICMP requests
- TCP
 - Attempt to connect to a specified TCP port. This can verify that a particular network service is available and is useful when ICMP responses are blocked
 - When TCP is selected, enter the port associated with the service being monitored

Watchdog Ping Configuration (continued)

Hostname (IP Address)

- Set the DNS hostname or IP address of the device to be monitored
- When using a hostname, the PWR2IEC must have access to a valid DNS server

TCP Port

- Set the destination TCP port to test when TCP is selected as the Ping Type. This field is not required for ICMP monitoring

Recent PING

- Displays the response time of the most recent successful check, measured in milliseconds

Watchdog Ping Cycle:

PING Interval

- Set the time between monitoring attempts
- A shorter interval detects failures more quickly but generates more network traffic

PING Retries

- Set the number of consecutive unsuccessful attempts permitted before the target is treated as unavailable and the selected Watchdog action is performed
- Set the interval and retry count high enough to avoid triggering an outlet action during brief network interruptions or while the monitored device is restarting

Watchdog Action:

One-Time Restart Mode

- Power cycle the selected outlet once when the target stops responding. No further restart is performed for the same outage until the target becomes reachable again and a later failure is detected

Two-Time Restart Outlet

- Power cycle the selected outlet when the target stops responding. If the target remains unavailable after the configured number of additional ping cycles, the outlet is restarted a second time. No further restart is performed until the target becomes reachable again

Watchdog Ping Cycle Attempts Between 2nd Outlet Restart

- Set how many complete ping cycles are performed before the second outlet restart
- Allow sufficient time for the connected device to finish restarting and restore network services before the second restart is attempted

Power Off Mode (Outlet Disabled)

- Turn the selected outlet off when the target is determined to be unavailable. The outlet remains off until it is turned on manually or by another supported control method

IP Master/Slave Mode 1 – Master Controls Slave Power

- Make the selected outlet follow the availability of the monitored target
 - If the target is available, the outlet powers on
 - If the target is unavailable the outlet powers off
- This mode can be used where the connected equipment should operate only while the monitored master device is available

Watchdog Action (continued)

IP Master/Slave Mode 2 – Automatic Failover

- Make the selected outlet operate inversely to the availability of the monitored target
 - If the target is available, the outlet powers off
 - If the target is unavailable the outlet powers on
- This mode can be used to power backup equipment automatically when the monitored primary device becomes unavailable

Log Only Mode (No Outlet Action)

- Record the Watchdog event without changing the power state of the selected outlet

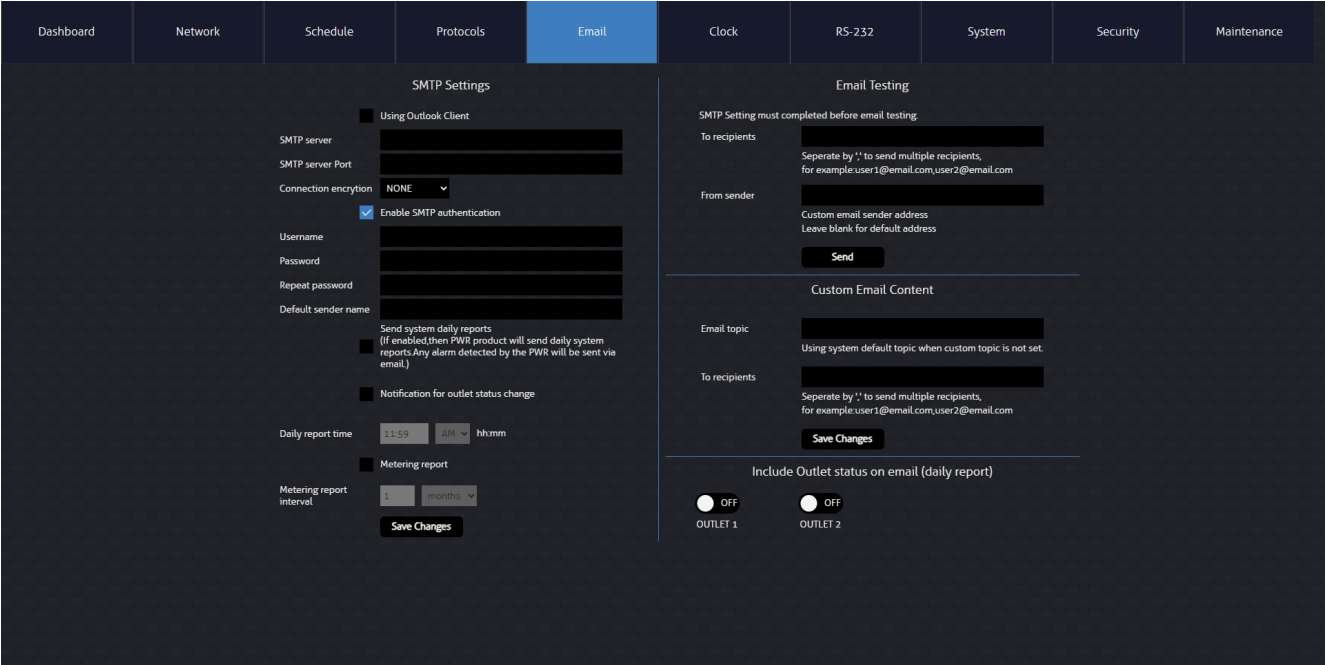
Treat Ping Requests as Unanswered When the Ethernet Link Is Down

- Determine whether loss of the PWR2IEC Ethernet link is counted as a failed monitoring attempt
 - If enabled, ping requests are treated as unanswered while the Ethernet link is down, allowing the configured Watchdog action to be triggered
 - If disabled, loss of the local Ethernet link is not treated as an unanswered target response

Select Save Changes to apply any updated settings.

Web GUI - Email

The Email page configures automatic email notifications, daily system reports and metering reports from the PWR2IEC. Email can be sent using either a conventional SMTP server or Microsoft Exchange Online using an application registered in Microsoft Entra ID. Email settings must be configured and saved before test messages, notifications or reports can be sent.



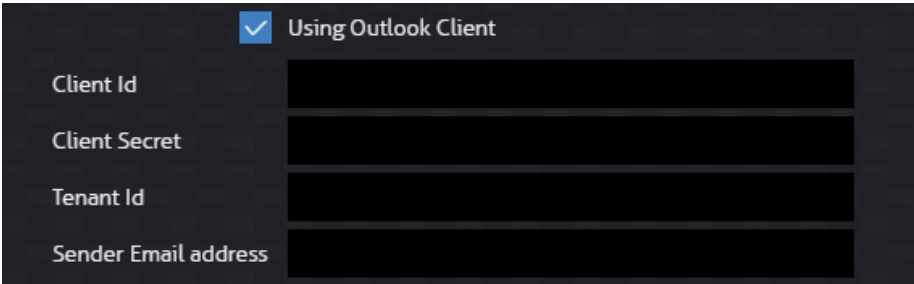
SMTP Settings:

Using Outlook Client

- Select the connection method used to send email:
 - When disabled, the PWR2IEC will use conventional SMTP server settings
 - When enabled, the PWR2IEC will use Microsoft Exchange Online with application credentials created through Microsoft Entra ID

Microsoft 365 / Exchange Online Settings

When Using Outlook Client is selected, the PWR2IEC uses OAuth application credentials to authenticate with Microsoft 365. This requires an application to be registered in Microsoft Entra ID and authorised to send email through Exchange Online. Microsoft supports OAuth client-credential authentication for applications that connect to SMTP services without an interactive user login.



Client ID

- Set the Application (client) ID assigned to the application registered in Microsoft Entra ID.
- The Client ID identifies the PWR2IEC email application to the Microsoft identity platform.

SMTP Settings (continued)

Client Secret

- Set the secret value created for the application under Certificates & secrets in Microsoft Entra ID.
- Enter the client secret value, not the secret ID.

Tenant ID

- Set the Directory (tenant) ID of the Microsoft Entra tenant containing the registered application and sender mailbox.

Sender Email Address

- Set the Microsoft 365 or Exchange Online mailbox from which PWR2IEC emails are sent.

Configuration of Microsoft Entra ID and Exchange Online should be completed by the organisation's Microsoft 365 administrator. Detailed Microsoft 365 configuration instructions are outside the scope of this manual.

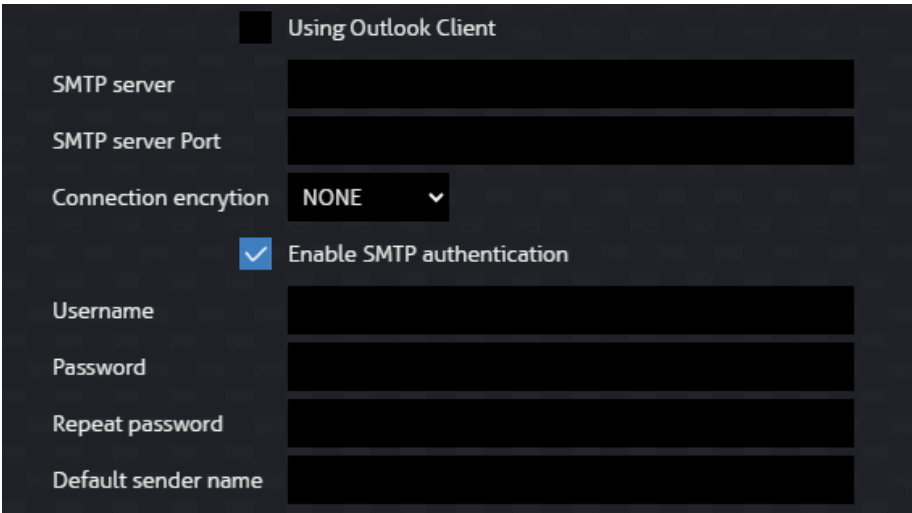
The general setup process includes:

- Registering an application in Microsoft Entra ID.
- Assigning the required Exchange Online email-sending permissions.
- Granting administrator consent for the application.
- Creating a Client Secret for authentication.
- Authorising the application to send email from the selected mailbox.
- Entering the resulting Client ID, Client Secret, Tenant ID and Sender Email Address into the PWR2IEC.
- Saving the settings and sending a test email to verify the configuration.

The required permissions and mailbox-access configuration may vary according to the organisation's Microsoft 365 security policies.

SMTP Server Settings

These fields are displayed when Using Outlook Client is disabled:



Using Outlook Client

SMTP server

SMTP server Port

Connection encryption **NONE** ▼

☒ Enable SMTP authentication

Username

Password

Repeat password

Default sender name

SMTP Server

- Set the hostname or IP address of the outgoing SMTP server.

SMTP Server Port

- Set the TCP port used to connect to the SMTP server.

SMTP Settings (continued)

Connection Encryption

- Select the encryption method used for the SMTP connection:
 - NONE / SSL/TLS / STARTTLS

Enable SMTP Authentication

- Enable / disable authentication with the SMTP server

Username

- Set the account name used to authenticate with the SMTP server

Password

- Set the password used for SMTP authentication

Repeat Password

- Set the password used for SMTP authentication

Default Sender Name

- Set the default sender identity displayed on emails generated by the PWR2IEC.

Send System Daily Reports

- Enable / disable automatic daily system reports.
 - When enabled, the PWR2IEC sends a report containing system information and the status of the outlets selected under Include Outlet Status on Email. Detected alarm conditions may also be included in the report.

Notification for Outlet Status Change

- Enable / disable email notifications when an outlet changes status.
 - This can be used to report changes caused by manual control, schedules, Watchdog actions or other supported control methods.

Daily Report Time

- Set the time at which the daily system report is sent; enter the required hour and minute, then select AM or PM.
- The PWR2IEC system clock must be configured correctly on the Clock page for reports to be sent at the intended time.

Metering Report

- Enable / disable automatic email reports containing energy-metering information.

Metering Report Interval

- Set how frequently the metering report is sent. Enter the interval value and select the corresponding time unit from the list.

Select Save Changes to apply any updated settings.

Email Testing:

The Email Testing section sends a test message using the currently saved email configuration.

To Recipients

- Set the email addresses that will receive the test message.
- Separate multiple recipient addresses using commas. For example: user1@example.com,user2@example.com

From Sender

- Set an optional sender address for the test message.

Send

- Send a test email using the saved connection and recipient settings.

Use this function to verify the server, authentication, sender and recipient configuration before enabling automatic reports or notifications.

Custom Email Content:

Email Topic

- Set a custom subject line for emails generated by the PWR2IEC.
- If this field is left blank, the system default subject is used.

To Recipients

- Set the recipients for automatic notifications and reports.
- Separate multiple recipient addresses using commas. For example: user1@example.com,user2@example.com

Select Save Changes to apply any updated settings.

Include Outlet Status on Email:

Select which outlet statuses are included in the daily system report. Each outlet can be enabled or disabled independently.

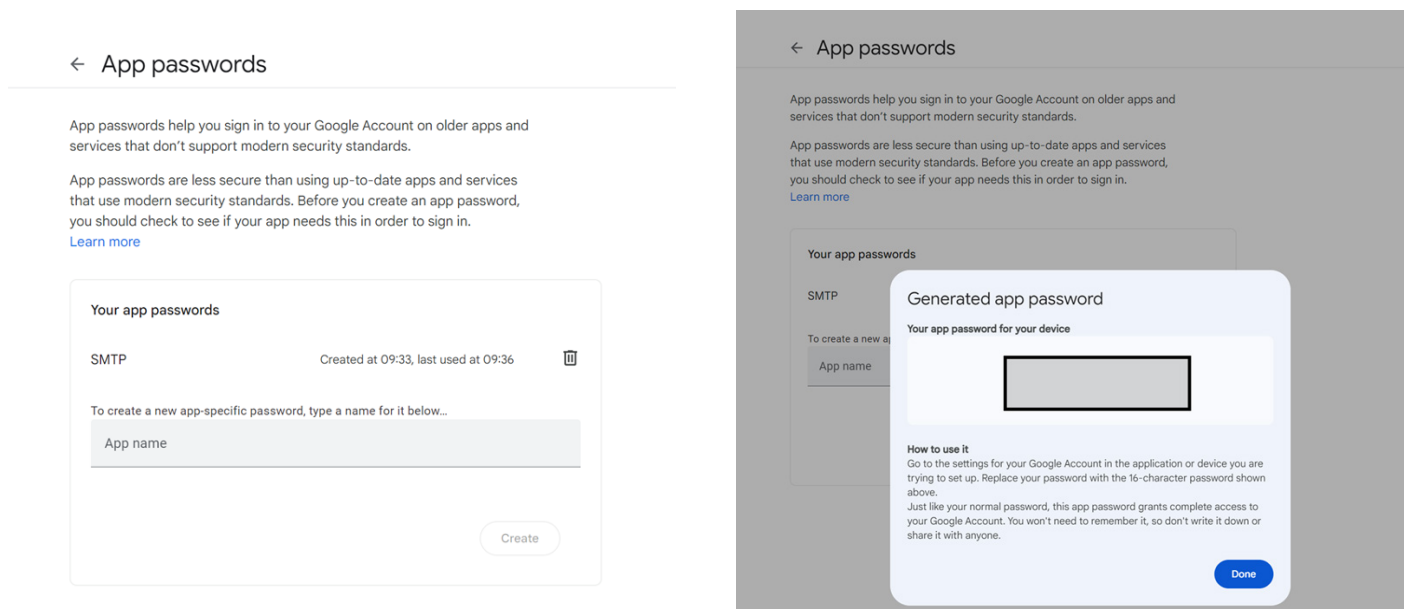
These options determine the outlet information included in the report. They do not enable or disable the outlets themselves.

SMTP Setup Example:

The following example demonstrates how to configure the PWR2IEC to send email notifications and reports using a conventional SMTP service. The available authentication methods and connection settings vary between SMTP providers. Confirm the required settings with the email provider or system administrator.

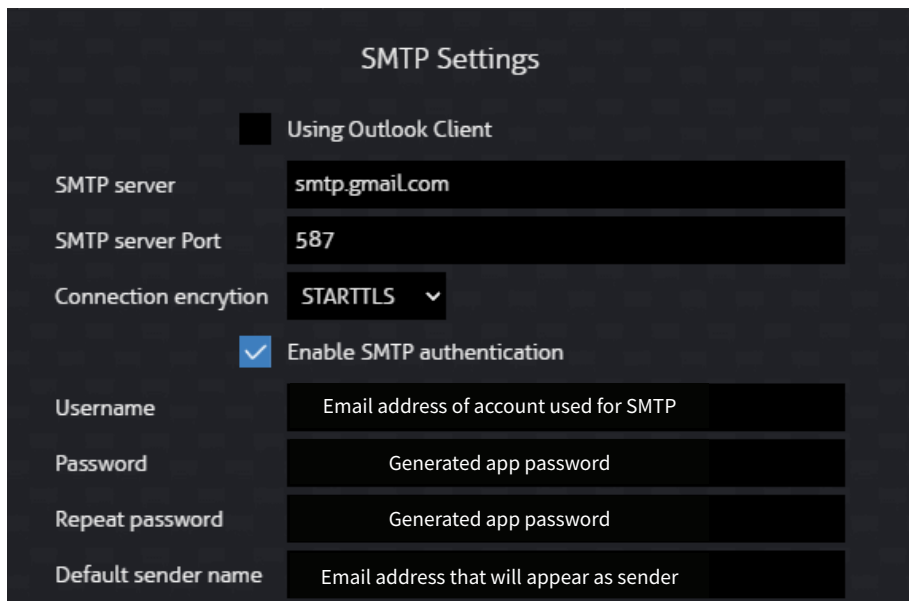
This example uses a Gmail account and Google's SMTP server; however, other compatible SMTP services may also be used. Gmail requires 2-Step Verification and a dedicated App Password for this configuration:

1. Enable and configure 2-Step Verification on the Google Account that will send emails from the PWR2IEC.
2. Create an App Password from the Google Account App Passwords page.



SMTP Setup Example (continued)

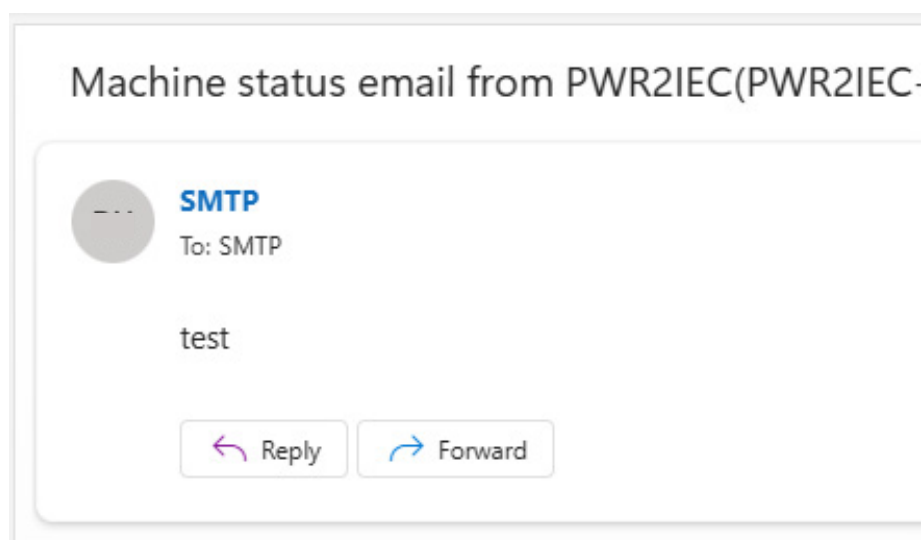
3. Configure the PWR2IEC using the relevant Gmail account information and generated App Password. For this example, use port 587 with STARTTLS. Gmail also supports port 465 with SSL/TLS.



The screenshot shows the 'SMTP Settings' window. At the top, there is a toggle for 'Using Outlook Client' which is currently turned off. Below this, the 'SMTP server' is set to 'smtp.gmail.com', the 'SMTP server Port' is '587', and the 'Connection encryption' is set to 'STARTTLS' with a dropdown arrow. A toggle for 'Enable SMTP authentication' is turned on. Below this, there are four input fields: 'Username' with the placeholder 'Email address of account used for SMTP', 'Password' with 'Generated app password', 'Repeat password' with 'Generated app password', and 'Default sender name' with 'Email address that will appear as sender'.

SMTP Settings	
☐ Using Outlook Client	
SMTP server	smtp.gmail.com
SMTP server Port	587
Connection encryption	STARTTLS
☒ Enable SMTP authentication	
Username	Email address of account used for SMTP
Password	Generated app password
Repeat password	Generated app password
Default sender name	Email address that will appear as sender

4. In the Email Testing section, enter a valid recipient address and select Send.
5. Confirm that the test email has been received. If it does not appear, check the recipient's junk or spam folder and verify the SMTP credentials and connection settings.



Web GUI - Clock

The Clock page configures the PWR2IEC system date and time. Accurate clock settings are required for scheduled outlet control, warning notifications, daily email reports, metering reports and logging.

The clock can be synchronised automatically using an NTP server or configured manually. An internal battery maintains the clock while the PWR2IEC is without mains power.

Please note: The PWR2IEC must be able to reach the configured NTP server through one of its network interfaces. Internet access is required when using a public NTP server.

Current Time

- Displays the current system time and date used by the PWR2IEC

NTP Settings:

Network Time Protocol, or NTP, allows the PWR2IEC to synchronise its clock automatically with a network time server.

Enable NTP Server

- Enable / disable NTP synchronisation. When disabled, the date and time can be entered under Manual Settings

Primary NTP Server

- Set the hostname or IP address of the preferred NTP server

Secondary NTP Server

- Set the hostname or IP address of an alternative NTP server. The secondary server may be used if the primary server is unavailable

Timezone

- Select the local time-zone offset applied to the time received from the NTP server
- NTP provides time in Coordinated Universal Time, or UTC. The selected time zone converts UTC to the required local time

Daylight Saving Time (DST)

- Apply a daylight-saving adjustment to the NTP server time
- Daylight Saving Time must be enabled or disabled manually when required for the installation location

Clock Format

- Select how the time is displayed:
 - 12-hour / 24-hour

Select Save Changes to apply any updated settings.

Manual Settings:

Manual settings are available when Enable NTP Server is disabled.

Set Date Manually

- Set the system date in the following format:
- dd-mm-yyyy

Set Time Manually

- Set the system time in hours and minutes
- When the 12-hour clock format is selected, use the adjacent AM/PM field to specify the required period

Clock Format

- Select how the time is displayed:
 - 12-hour / 24-hour

Select Save Changes to apply any updated settings.

After saving, check the Current Time display to confirm that the settings have been applied correctly.

Web GUI - RS-232

The RS-232 page configures the serial communication settings for the PWR2IEC. Commands can also be entered and transmitted out of the TX pin of the Phoenix serial port directly from this page, providing a convenient method of testing and troubleshooting. The RS-232 settings must match the baud rate, parity, character format and command ending requirements of the connected device.

Dashboard Network Schedule Protocols Email Clock RS-232 System Security Maintenance

RS-232

Character Set: ASCII Baud Rate: 57600

Command Ending: NULL Parity: None

RS-232 Command:

Test

Character Set

- Select the format used to enter and transmit the RS-232 command:
 - ASCII / HEX

Baud Rate

- Select the RS-232 baud rate:
 - 2400 / 4800 / 9600 / 19200 / 38400 / 57600 / 115200

Command Ending

- Select the terminating character or sequence appended to the command:
 - NULL (no command ending character is appended)
 - CR (Carriage Return 0x0D /r)
 - LF (Line Feed 0x0A /n)
 - CR+LF (Carriage Return 0x0D /r + Line Feed 0x0A /n)

Parity

- Select the parity setting used for RS-232 communication
 - Even / Odd

RS-232 Command

- Enter the ASCII command or hexadecimal data to be transmitted through the RS-232 port
- Select Test to transmit the entered command using the selected character set, baud rate, parity and command ending settings

Web GUI - System

The System page configures the PWR2IEC front-panel controls, external relay-control input, system behaviour, dashboard visibility, outlet protection and inlet voltage thresholds.

WARNING: Protection thresholds and recovery settings affect power supplied to connected equipment. Only adjust these settings where required for the installation and after confirming the electrical requirements of the connected devices.

The screenshot displays the 'System' configuration page of the PWR2IEC web interface. The top navigation bar includes links for Dashboard, Network, Schedule, Protocols, Email, Clock, RS-232, System (active), Security, and Maintenance.

Panel Lock: A toggle switch labeled 'Lock All Front Panel Buttons' is currently in the 'Unlock' position.

Relay Setting:

- Relay Enable:** A toggle switch is set to 'ON'.
- Relay Application mode:** A dropdown menu is set to 'Push Button mode'.
- Toggle by LOW voltage:** A dropdown menu is set to 'Toggle by LOW voltage'.
- Save Changes:** A button to save the relay settings.

System Setting:

- Device Name:** PWR2IEC
- Login Timeout:** 15 min (Default: 15 mins)
- Warning Beeper Time:** 10 seconds (Default: 10 seconds)
- Standby mode:** Radio buttons for 'All standby mode' (selected) and 'Sleep mode'.
- Save Changes:** A button to save system settings.
- Show Total Current:** ON
- Show Total Power:** ON
- Show Overall Voltage:** ON
- Show Energy Consumed:** ON
- Show PF(Power Factor):** ON
- Show Frequency:** ON
- Ground Sense:** ON
- System Power Switch:** ON
- Meter Reset Switch:** ON
- System Restart Switch:** ON
- Guest Control:** OFF (Switch of System Power/Reset/Restart)

Outlets Setting:

- Overload processing:** Radio buttons for 'Power off the overloaded outlet' (selected), 'Power off all outlets and set system to standby mode', and 'Auto recover 1 retries, in 3 mins (Default: 3 mins)'.
- Overcurrent Threshold:** System 10.9 A (max. 10.9A). OUTLET 1: 0 A. OUTLET 2: 0 A. (Default 0A, set 0 to follow by system overcurrent threshold)
- Instantaneous current delay mode:** OUTLET 1: No delay. OUTLET 2: No delay.
- Overvoltage and Undervoltage processing:** Radio buttons for 'Power off all outlets' (selected) and 'Outlets automatically recover 3 mins (Default: 3 mins) after the voltage input stabilises'.
- Save Changes:** A button to save outlet settings.
- Show Voltage:** ON
- Show Current:** ON
- Show PF(Power Factor):** ON
- Show Power:** ON
- Show Energy Consumed:** ON
- Guest Control:** OFF (Power/Reset/Config/Restart)

Inlet Setting:

- Undervoltage Threshold:** 189 V (Default: 189V/Min: 189V)
- Overvoltage Threshold:** 250 V (Default: 250V/Max: 264V)
- Save Changes:** A button to save inlet settings.

Panel Lock:

Lock All Front Panel Buttons

- Enable / disable the outlet buttons on the top panel
- Locking the front-panel buttons does not disable the PWR2IEC mains power switch

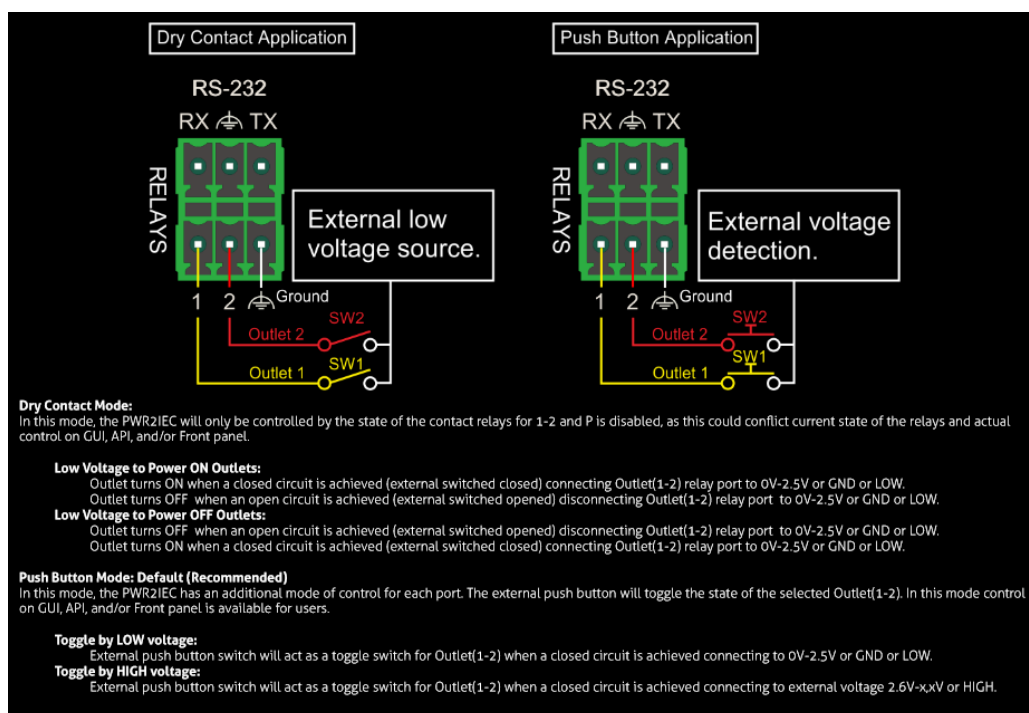
Relay Setting:

The Relay Setting section configures external control of Outlet 1 and Outlet 2 through the relay input connector. Each outlet has a dedicated input that can be connected to an external switch, relay contact or compatible voltage-control source.

Two application modes are available. Dry Contact Mode uses the maintained open or closed state of an external contact to determine the corresponding outlet's power state. In this mode, the physical contact controls the outlet directly, so control through the Web GUI, control commands and front panel is disabled to prevent the commanded outlet state from conflicting with the contact position.

Push Button Mode, which is the default and recommended setting, uses each valid input activation to toggle the corresponding outlet between on and off. As the input does not continuously determine the outlet state, control through the Web GUI, control commands and front panel remains available.

The selected trigger option determines whether the input responds to a low-voltage contact closure or a supported external high-voltage signal. Refer to the relay connection diagram and confirm the permitted input-voltage range before connecting external equipment.



Relay Setting (continued)

Relay Enable

- Enable / disable external relay control.

Relay Application Mode

Push Button Mode

- Use a momentary input to toggle the corresponding outlet between on and off
- The following trigger options are available:
 - Toggle by LOW voltage
 - Toggle by HIGH voltage
- Because Push Button Mode responds to each activation rather than continuously following the input state, outlet control remains available through the Web GUI, control commands and front panel

Dry Contact Mode

- Use a maintained open or closed contact to determine the corresponding outlet state
- The following trigger options are available
 - Low Voltage to Power ON Outlets
 - Low Voltage to Power OFF Outlets
- Because the maintained contact state determines the outlet state, control from the Web GUI, control commands and front panel may conflict with the physical input. Dry Contact Mode should be used where the external contact is intended as the primary source of outlet control

Select Save Changes to apply any updated settings.

System Setting:

Device Name

- Set the name used to identify the PWR2IEC

Login Timeout

- Set the period of Web GUI inactivity, in minutes, before the current user is automatically logged out

Warning Beeper Time

- Set how long, in seconds, the audible warning beeper operates when a warning or protection event is triggered

Standby Mode

- Determine how the PWR2IEC responds when the system power control is selected from the Web GUI
 - All Standby Mode turns off all outlets and disables normal Web GUI access while the system is in standby
 - Sleep Mode turns off all outlets while maintaining Web GUI access, allowing the system to be monitored or restored remotely

Select Save Changes to apply any updated settings.

Individual switches can be used to show or hide system information and controls on the Dashboard, including total current, total power, overall voltage, energy consumption, power factor, frequency, ground sense, system power, meter reset and system restart.

Guest Control

- Enable / disable whether the displayed System Power, Meter Reset and System Restart controls can be operated without logging into the PWR2IEC

Outlets Setting:

Overload Processing

- Determine how the PWR2IEC responds when an outlet overload is triggered:
 - Power Off the Overloaded Outlet
 - Power Off All Outlets and Set System to Standby Mode
 - Auto Recover: Turn off the affected outlet and then attempts to restore power automatically. The amount of retries autorecover duration can be set

Overcurrent Threshold

- System
 - Set the maximum combined system current at which an overcurrent event is triggered
- Outlet 1 / Outlet 2
 - Set an individual overcurrent threshold for each outlet
 - Entering 0 A causes that outlet to follow the system overcurrent threshold rather than using a separate outlet threshold

Instantaneous Current Delay Mode

- Set a short delay for each outlet before current protection is triggered, allowing a brief overcurrent to occur without immediately switching off the outlet
- Select No Delay where immediate current protection is required
- **WARNING:** Only add a delay if verified transient inrush current is causing unintended trips. Increasing the delay allows an overcurrent to persist for longer before protection is activated.

Overvoltage and Undervoltage Processing

- Determine how the PWR2IEC responds when the mains input voltage moves outside the configured inlet thresholds.
 - Power Off All Outlets
 - Outlets Automatically Recover: Turn off both outlets when an unsafe voltage condition is detected, then restores power automatically after the input voltage has stabilised for the configured number of minutes.

Select Save Changes to apply any updated settings.

Individual switches can be used to show or hide outlet information on the Dashboard, including voltage, current, power factor, power and accumulated energy consumption.

Guest Control

- Determine whether outlet power, meter reset, configuration and restart controls can be accessed without logging into the PWR2IEC

Inlet Setting:

Undervoltage Threshold

- Set the mains input voltage threshold for the PWR2IEC to detect an undervoltage condition
- **Please note:** For the regional version shown, the default and minimum threshold is 250V

Overvoltage Threshold

- Set the mains input voltage threshold for the PWR2IEC to detect an overvoltage condition
- **Please note:** For the regional version shown, the default and maximum threshold is 250V

WARNING: Do not change the inlet voltage thresholds beyond the operating limits of the connected equipment. Incorrect settings may reduce protection or cause unnecessary interruption of power.

Select Save Changes to apply any updated settings.

Web GUI - Security

The Security page manages access to the PWR2IEC. The Admin Credentials tab allows configuration of the administrator account and RADIUS authentication settings for supported services, including Telnet and SSH. The User Authorization tab allows additional user accounts to be added and their Web GUI access permissions to be configured.

Admin Credentials:

The Admin Credentials section allows the administrator username and password to be changed. Enter the current password, followed by the new username and/or password, then select Save Changes to apply any updated settings.

RADIUS (Remote Authentication Dial-In User Service):

Remote Authentication Dial-In User Service, or RADIUS, provides centralised authentication and authorization.

When enabled, the PWR2IEC operates as a RADIUS client, also known as a NAS (Network Access Server). It sends user credentials to a configured RADIUS server for authentication.

Please note: RADIUS configuration should normally be completed by the organisation's network or systems administrator.

Enable RADIUS Client

- Enable / disable RADIUS authentication

Authentication Protocol

- PAP
 - Use Password Authentication Protocol
- CHAP
 - Use Challenge-Handshake Authentication Protocol

Use Message Authentication

- Enable / disable the RADIUS Message-Authenticator attribute in authentication requests

Default Session Timeout

- Set the maximum permitted authenticated session duration, in seconds

Primary Server

- Set the IP address of the RADIUS server

RADIUS (continued)

New Shared Password

- Set the shared secret used to authenticate communication between the PWR2IEC and the RADIUS server
- The same shared secret must be configured for the PWR2IEC client entry on the RADIUS server

Repeat Password

- Enter the shared secret again

Timeout

- Set how long, in seconds, the PWR2IEC waits for a response from the RADIUS server before treating the request as unsuccessful or retrying it

Retries

- Set the number of times the PWR2IEC attempts to contact the RADIUS server after an authentication request receives no response

Select Save Changes to apply any updated settings.

RADIUS Setup Example:

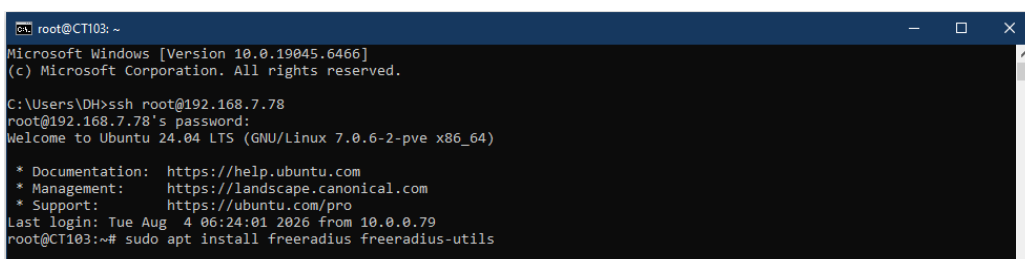
The following example uses FreeRADIUS on Ubuntu to demonstrate basic PWR2IEC RADIUS authentication. It is intended as a functional example only. Production RADIUS deployments should follow the organisation's security, redundancy, credential-management and network-access policies.

In this example, FreeRADIUS is installed on an Ubuntu server located on the same network as the PWR2IEC. The example uses:

- RADIUS username: pwr2iec-user
- RADIUS password: ExamplePassword1!
- Shared secret: ExampleRadiusSecret123!
- Authentication port: 1812/UDP

WARNING: Do not use these example passwords in a production installation. Replace the example addresses and credentials with values appropriate for your network.

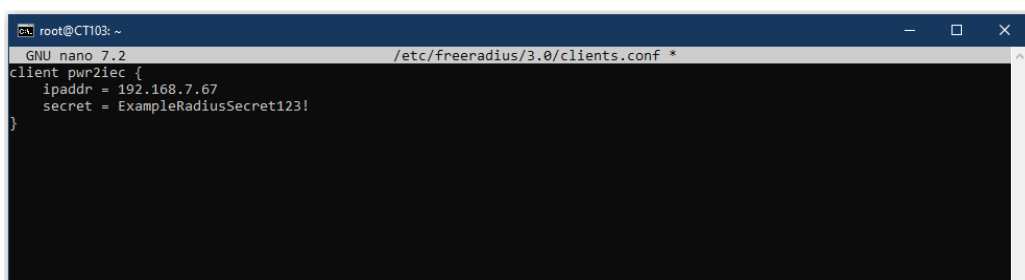
1. Install FreeRADIUS. FreeRADIUS normally uses UDP port 1812 for authentication and UDP port 1813 for accounting



```
root@CT103: ~  
Microsoft Windows [Version 10.0.19045.6466]  
(c) Microsoft Corporation. All rights reserved.  
  
C:\Users\DH>ssh root@192.168.7.78  
root@192.168.7.78's password:  
Welcome to Ubuntu 24.04 LTS (GNU/Linux 7.0.6-2-pve x86_64)  
  
 * Documentation:  https://help.ubuntu.com  
 * Management:    https://landscape.canonical.com  
 * Support:        https://ubuntu.com/pro  
Last login: Tue Aug  4 06:24:01 2026 from 10.0.0.79  
root@CT103:~# sudo apt install freeradius freeradius-utils
```

2. Add the PWR2IEC as a RADIUS client.

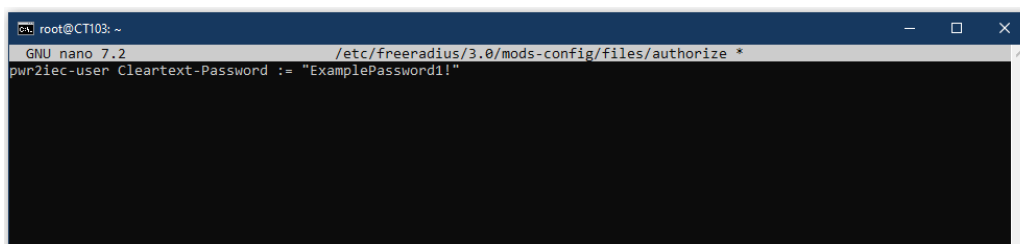
In this configuration ipaddr is the IP address of the PWR2IEC and secret is the shared secret used between the PWR2IEC and the RADIUS server.



```
root@CT103: ~  
GNU nano 7.2 /etc/freeradius/3.0/clients.conf *  
client pwr2iec {  
    ipaddr = 192.168.7.67  
    secret = ExampleRadiusSecret123!  
}
```

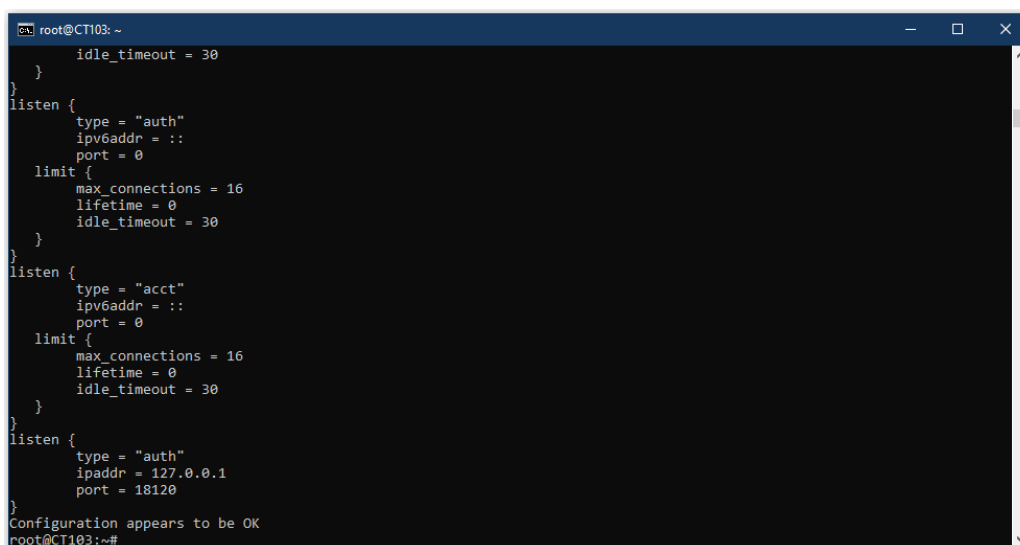
RADIUS Setup Example (continued)

3. Add a test user.



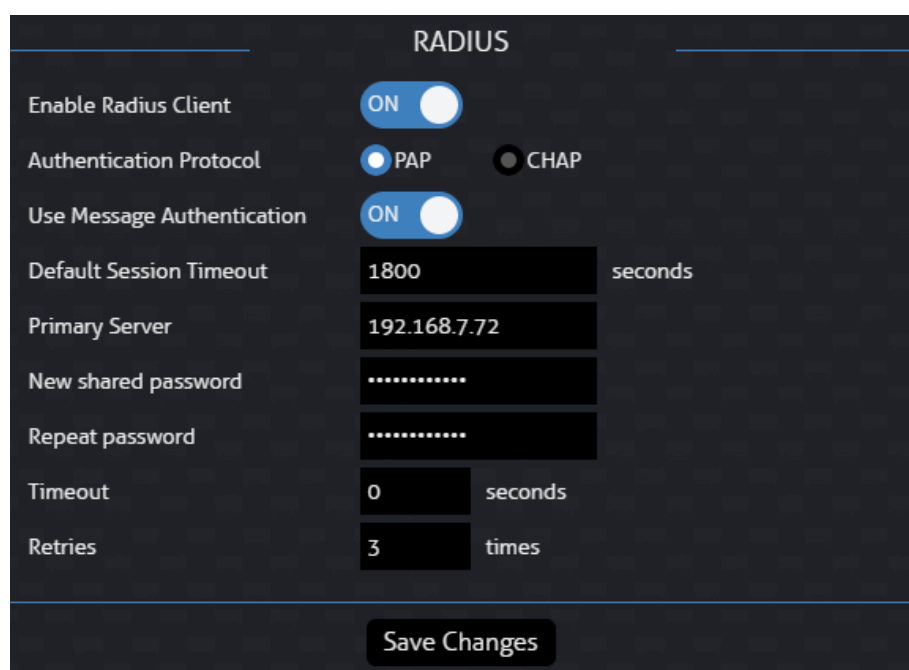
```
root@CT103: ~  
GNU nano 7.2 /etc/freeradius/3.0/mods-config/files/authorize *  
pwr2iec-user Cleartext-Password := "ExamplePassword1!"
```

4. Check the configuration. A successful check should end with a message indicating that the configuration is valid.



```
root@CT103: ~  
    idle_timeout = 30  
}  
}  
listen {  
    type = "auth"  
    ipv6addr = ::  
    port = 0  
    limit {  
        max_connections = 16  
        lifetime = 0  
        idle_timeout = 30  
    }  
}  
listen {  
    type = "acct"  
    ipv6addr = ::  
    port = 0  
    limit {  
        max_connections = 16  
        lifetime = 0  
        idle_timeout = 30  
    }  
}  
listen {  
    type = "auth"  
    ipaddr = 127.0.0.1  
    port = 18120  
}  
}  
Configuration appears to be OK  
root@CT103:~#
```

5. Restart the FreeRADIUS service:
6. Configure the PWR2IEC RADIUS settings. The Primary Server must be the IP address of the computer running FreeRADIUS. The Shared Password must exactly match the secret value entered in clients.conf.



RADIUS

Enable Radius Client	☒ ON
Authentication Protocol	☒ PAP ☐ CHAP
Use Message Authentication	☒ ON
Default Session Timeout	1800 seconds
Primary Server	192.168.7.72
New shared password	
Repeat password	
Timeout	0 seconds
Retries	3 times

Save Changes

RADIUS Setup Example (continued)

6. Test the RADIUS login

Attempt to log in to the RADIUS-enabled PWR2IEC service. In this example, SSH will be utilised:

Username: PWR2IEC-user

Password: ExamplePassword1!

If the credentials and shared secret are correct, FreeRADIUS returns an Access-Accept response.

```
(6) pap: Login attempt with password
(6) pap: Comparing with "known good" Cleartext-Password
(6) pap: User authenticated successfully
(6) [pap] = ok
(6) } # Auth-Type PAP = ok
(6) # Executing section post-auth from file /etc/freeradius/3.0/sites-enabled/default
(6) post-auth {
(6)   if (session-state:User-Name && reply:User-Name && request:User-Name && (reply:User-Name == request:User-Name)) {
(6)     if (session-state:User-Name && reply:User-Name && request:User-Name && (reply:User-Name == request:User-Name)) -> FALSE
(6)     update {
(6)       No attributes updated for RHS &session-state:
(6)     } # update = noop
(6)     [exec] = noop
(6)     policy remove_reply_message_if_eap {
(6)       if (&reply:EAP-Message && &reply:Reply-Message) {
(6)         if (&reply:EAP-Message && &reply:Reply-Message) -> FALSE
(6)       } else {
(6)         [noop] = noop
(6)       } # else = noop
(6)     } # policy remove_reply_message_if_eap = noop
(6)     if (EAP-Key-Name && &reply:EAP-Session-Id) {
(6)       if (EAP-Key-Name && &reply:EAP-Session-Id) -> FALSE
(6)     } # post-auth = noop
(6) Sent Access-Accept Id 167 from 192.168.7.72:1812 to 192.168.7.67:41209 length 38
(6) Finished request
(6) Waking up in 4.9 seconds.
(6) Cleaning up request packet ID 167 with timestamp +106279 due to cleanup_delay was reached
Ready to process requests
```

User Authorization:

The Web GUI supports up to 7 individual user accounts and a Guest account . Each user can be enabled or disabled and assigned specific access permissions.

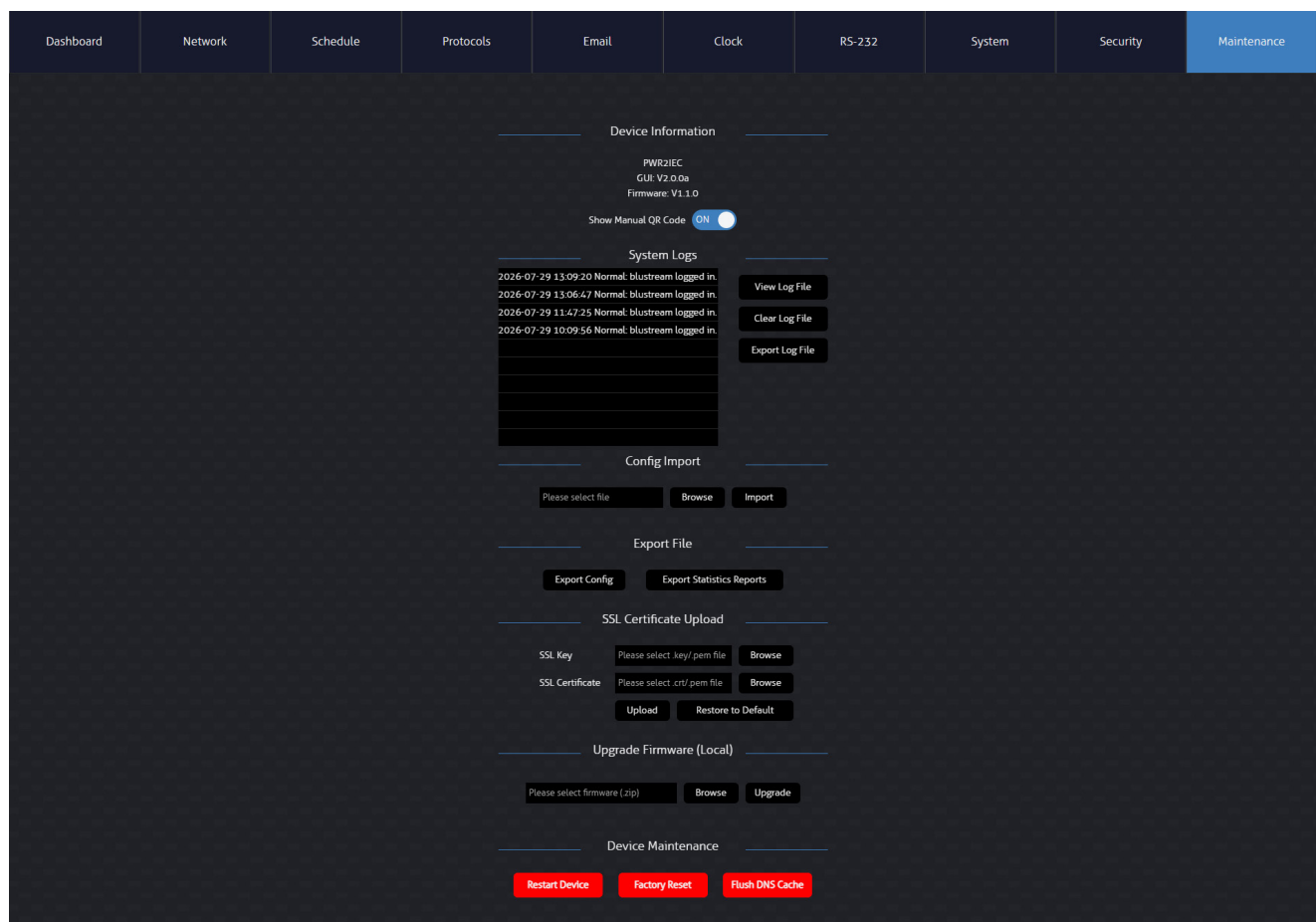
To configure a user account:

- Set the required user toggle to On
- Select the corresponding user from the User selection row
- Enter a unique username
- Create a password that meets the Web GUI password requirements
- Assign the required permissions by selecting the relevant checkboxes

Select Confirm to apply any updated settings.

Web GUI - Maintenance

The Maintenance page displays device and firmware information, provides access to system logs, and allows configuration files, certificates and firmware to be managed. The page also contains controls for restarting, resetting and clearing stored DNS information.



Device Information:

Displays the PWR2IEC model and the currently installed software versions:

Show Manual QR Code

- Enable / disable the manual QR code displayed at the bottom of the Web GUI

System Logs:

The System Logs section records device activity and configuration events, including user login activity.

View Log File

- Open the complete system log for viewing

Clear Log File

- Delete the entries currently stored in the system log

Export Log File

- Download the system log

Config Import:

Imports a previously exported PWR2IEC configuration file.

Select Browse, locate the required configuration file, then select Import to apply the settings to the PWR2IEC.

Export File:

Export Config

- Download a backup of the current PWR2IEC configuration. The exported file can be retained for recovery or imported into another compatible unit

Export Statistics Reports

- Download a snapshot report containing the currently recorded system, outlet and metering statistics

SSL Certificate Upload:

The SSL Certificate Upload section allows a custom certificate and corresponding private key to be installed for HTTPS access to the Web GUI.

Select Browse and locate the required private key and certificate files for SSL Key and SSL Certificate, respectively. Select Upload to install the files.

Select Restore to Default to remove the uploaded certificate and private key and restore the default certificate.

Upgrade Firmware (Local):

Allows the PWR2IEC firmware to be updated using a firmware package stored on the connected computer.

Download the latest compatible firmware package from the PWR2IEC product page.

Select Browse and locate the firmware .zip file.

Select Upgrade to begin the update.

Allow the upgrade to finish and the device to restart before reconnecting.

Please note: Only install firmware intended for the PWR2IEC. Do not disconnect mains power, close the browser or interrupt the network connection during the upgrade. Export the current configuration before updating in case the settings need to be restored.

After the update, return to Device Information and confirm that the expected firmware version is displayed.

Device Maintenance:

Restart Device

- Restart the PWR2IEC without intentionally deleting its saved configuration

Factory Reset

- Restore the PWR2IEC to its factory-default configuration, including its network and login settings

Flush DNS Cache

- Clear cached DNS records stored by the PWR2IEC

Specifications

- **Power Input ports:** 1 x C14 IEC 10A
- **Power Output ports:** 2 x C13 IEC 10A Total
- **GPI Control:** 1 x 3-Pin Phoenix connector
- **RS-232 serial port:** 1 x 3-Pin Phoenix connector
- **TCP/IP Control:** 2 x RJ45, female
- **Mounting:** wall / shelf mounting brackets included
- **Casing Dimensions (W x D x H):** 200mm x 85mm x 52mm
- **Shipping Weight:** 2.5kg
- **Operating Temperature:** 32°F to 104°F (0°C to 40°C)
- **Storage Temperature :** -4°F to 140°F (-20°C to 60°C)
- **Power Supply:** Internal 110-250V AC

NOTE: Specifications are subject to change without notice. Weights and dimensions are approximate.

Package Contents

- 1 x PWR2IEC
- 1 x Serial cable - DB9 to 3 pin Phoenix connector
- 1 x 3 pin 3.5mm Phoenix connector
- 4 x Rubber feet
- 6 x Cable management ties
- 1 x Wall / shelf mounting brackets
- IEC Inlet Power Cable(s)

Maintenance

Clean this unit with a soft, dry cloth. Never use alcohol, paint thinner or benzene to clean this unit.

Communication Protocols and Commands

The XXXX can be controlled with control commands via serial (RS-232) and TCP/IP (Telnet, SSH).

The default RS-232 communication settings are:

- **Baud rate:** 57600
- **Data bits:** 8
- **Stop bits:** 1
- **Parity bit:** none
- **Control Character:** CR+LF (Carriage Return 0x0D /r + Line Feed 0x0A /n)

The following pages list all available control commands.

Commonly Used Commands:

There are several commands that are commonly used for control and testing:

STATUS	Status will give feedback on the switcher such as outputs on, type of connection, etc.
PON	Power on
POFF	Power off
OUTLETxxON	Turn outlet xx on Example: OUTLET01ON (This would turn all outlets on)
OUTLETxxOFF	Turn outlet xx off Example: OUTLET00OFF (This would turn all outlets off)

Common Mistakes:

- Control Character
 - Serial terminal applications and control software vary in how they handle command termination. Some applications automatically append a Carriage Return CR and/or Line Feed LF character when transmitting a command. Other applications transmit the command string exactly as entered, requiring control characters to be added manually.
 - Blustream products require a Carriage Return (CR, 0D, /r) + Line Feed (LF, 0A, /n) at the end of each serial command. Commands that are not terminated with these characters will not be recognized.
 - Before troubleshooting serial communication issues, confirm how the application handles command termination and ensure that CR and LF characters are appended to every transmitted command.
- Spaces
 - Blustream commands do not require space between commands unless specified. There may be some applications that require spacing in order to work.
 - How the string should look is as follows: OUTON
 - How the string may look if spaces are required: OUT{Space}ON
- Baud rate, or other serial protocol settings, not set correctly

Communication Protocols and Commands (continued)

COMMAND	ACTION
?/HELP	Print Help Information
STATUS	Print System Status And Port Status
OUTLETSTATUS xx	Print Outlet xx ON/OFF xx = 0 All, 1 Outlet1, 2 Outlet2
CONNSTATUS xx	Print Outlet xx Idle/Connected/Overload/Abnormalvoltage xx = 0 All, 1 Outlet1, 2 Outlet2
ELESTA	Print All Outputs Electricity Level Information
FWVERSION	Print FW Version And GUI Version
DEVICENAME:xx	Set Device Name To xx
PON/OFF	Set System Power ON Or OFF
RELAY ON/OFF	Set System RELAY Control ON Or OFF
KEY ON/OFF	Set System Key Control ON Or OFF
RESET	Reset System To Default Setting(Type "Yes" To Confirm, "No" To Discard)
REBOOT	Set System Reboot And Apply New Config!!!
RESTA	Set System Restart
SETCURRENTTHRESHOLD xx	Set The System Current Threshold To xx(xx to one decimal place at most) xx = 0.0 : 10.9
OC DT xx	Print Outlet xx OverCurrent Delay Time xx = 0 All, 1 Outlet1, 2 Outlet2
OC DT xx DEL yy	Set Outlet xx OverCurrent Delay Time To ymys(Default: No Delay) xx = 0 All, 1 Outlet1, 2 Outlet2 yy = 0 No Delay, 1 100, 2 200, 3 300, 4 400, 5 500
SETOVERVOLTAGERESHOLD xx	Set The System OverVoltage Threshold To xxV(Default: 250V) xx = 198 : 264
SETUNDERVOLTAGERESHOLD xx	Set The System UnderVoltage Threshold To xxV(Default: 189V) xx = 189 : 249
SAFEMODE xx	Set The System Safe Mode To xx When Overloaded xx = 0 Outlet_Shutdown, 1 System_Shutdown, 2 Auto_Retry
OVERLOADRETRYCNT xx	Set The System Retry Number To xx When Overloaded(Default: 1) xx = 1 : 3
OVERLOADRETRYTIME xx	Set The System Retry Delay Time To xxmins When Overloaded(Default: 3mins) xx = 1 : 10
VOLTMONITORMODE xx	Set The System Voltage Monitor Mode To xx When Overvoltage Or Undervoltage xx = 0 All_Outlets_Shutdown, 1 Auto_Retry
VOLTMONITORRETRYTIME xx	Set The System Retry Delay Time To xxmins After the Voltage Input Stabilises(Default: 3mins) xx = 1 : 10
STANDBYMODE xx	Set The System Standby Mode To xx xx = 0 All_Standby_Mode, 1 Sleep_Mode
RELAYMODE xx	Set The System Relay Mode To xx xx = 0 Dry_Contact, 1 Push_Button
RELAYVOLTAGE xx	Set The System Relay Toggle Voltage To xx xx = 0 Low_Voltage, 1 High_Voltage
BEEPERTIME xx	Set The Buzzer Sound Time To xxs When Alarming(Default: 10 Seconds) xx = 0 : 9999

COMMAND	ACTION
OUTLETTIMEON xx:yy	Set Outlet xx Power_ON Delay To yys xx = 1 Outlet1, 2 Outlet2 yy = 2 : 9999
OUTLETTIMEOFF xx:yy	Set Outlet xx Power_OFF Delay To yys xx = 1 Outlet1, 2 Outlet2 yy = 0 : 9999
RESTADELAY xx:yy	Set Outlet xx Power_RESTA Delay To yys xx = 1 Outlet1, 2 Outlet2 yy = 2 : 9999
OUTLETELERESET xx:yy	Set Outlet xx Electrical Work Reset Duration To yys(Default: 10 Seconds) xx = 1 Outlet1, 2 Outlet2 yy = 0 : 9999
OUTLETTRESHOLD xx:yy	Set Outlet xx Current Threshold To xxA(Default: 0A) xx = 1 Outlet1, 2 Outlet2 yy = 0 : 10
ALLOUT ON/OFF	Set All Outlets ON/OFF
OUTLET xx ON/OFF/RESTA	Set Outlet xx ON/OFF/RESTA xx = 1 Outlet1, 2 Outlet2
RSALLOUTELE	Clean Up All Outlets Electrical Work
RSOUTELE xx	Clean Up The Outlet xx Electrical Work xx = 1 Outlet1, 2 Outlet2
SYS TIME	Get The Time For The System
RESYS TIME yyyy-mm-dd:hh:mm:ss	Set The Time For The System yyyy = Year, mm = Month, dd = Day, hh = Hour, mm = Minute, ss = Second
RS232OUT y:z:c:a	Send y Type Of Command a With Baud Rate z, Parity c To Output y=a: ASCII y=h: HEX z=1: 2400 z=2: 4800 z=3: 9600 z=4: 19200 z=5: 38400 z=6: 57600(Default) z=7: 115200 c=1: None c=2: Even c=3: Odd a=RS232 Command
RS232BAUD z	Set RS232 Baud Rate To xx z = 1 - 2400, 2 - 4800, 3 - 9600, 4 - 19200, 5 - 38400, 6 - 57600(Default), 7 - 115200
NET TCP/IP LIST	List Current TCP/IP Address
NET TCP/IP ENABLE xx	Set TCP/IP xx Enable(Only One Can Be Enabled) xx = 1 TCP/IP1, 2 TCP/IP2
NET TCP/IP1 DHCP ON/OFF	Set TCP/IP1 Auto IP(DHCP) ON Or OFF
NET TCP/IP1 IP xxx.xxx.xxx.xxx	Set TCP/IP1 IP Address
NET TCP/IP1 GW xxx.xxx.xxx.xxx	Set TCP/IP1 Gateway Address
NET TCP/IP1 SM xxx.xxx.xxx.xxx	Set TCP/IP1 Subnet Mask Address
NET TCP/IP2 DHCP ON/OFF	Set TCP/IP2 Auto IP(DHCP) ON Or OFF

Communication Protocols and Commands (continued)

COMMAND	ACTION
NET TCP/IP2 IP xxx.xxx. xxx.xxx	Set TCP/IP2 IP Address
NET TCP/IP2 GW xxx. xxx.xxx.xxx	Set TCP/IP2 Gateway Address
NET TCP/IP2 SM xxx. xxx.xxx.xxx	Set TCP/IP2 Subnet Mask Address
NET MDNS ON/OFF	Set mDNS ON/OFF
NET RB	Set Network Reboot And Apply New Config

Certifications

FCC Notice

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

Reorient or relocate the receiving antenna.

Increase the separation between the equipment and receiver.

Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

Consult the dealer or an experienced radio/TV technician for help.

CAUTION - changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Canada, Industry Canada (IC) Notices

This Class B digital apparatus complies with Canadian ICES-003.

Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Canada, avis d'Industry Canada (IC)

Cet appareil numérique de classe B est conforme aux normes canadiennes ICES-003.

Son fonctionnement est soumis aux deux conditions suivantes : (1) cet appareil ne doit pas causer d'interférence et (2) cet appareil doit accepter toute interférence, notamment les interférences qui peuvent affecter son fonctionnement.

Correct Disposal of this product

This marking indicates that this product should not be disposed with other household wastes. To prevent possible harm to the environment or human health from uncontrolled waste disposal, recycle it responsibly to promote the sustainable reuse of material resources. To return your used device, please use the return and collection systems or contact the retailer where the product was purchased. They can take this product for environmentally safe recycling.





www.blustream.com.au
www.blustream-us.com
www.blustream.co.uk