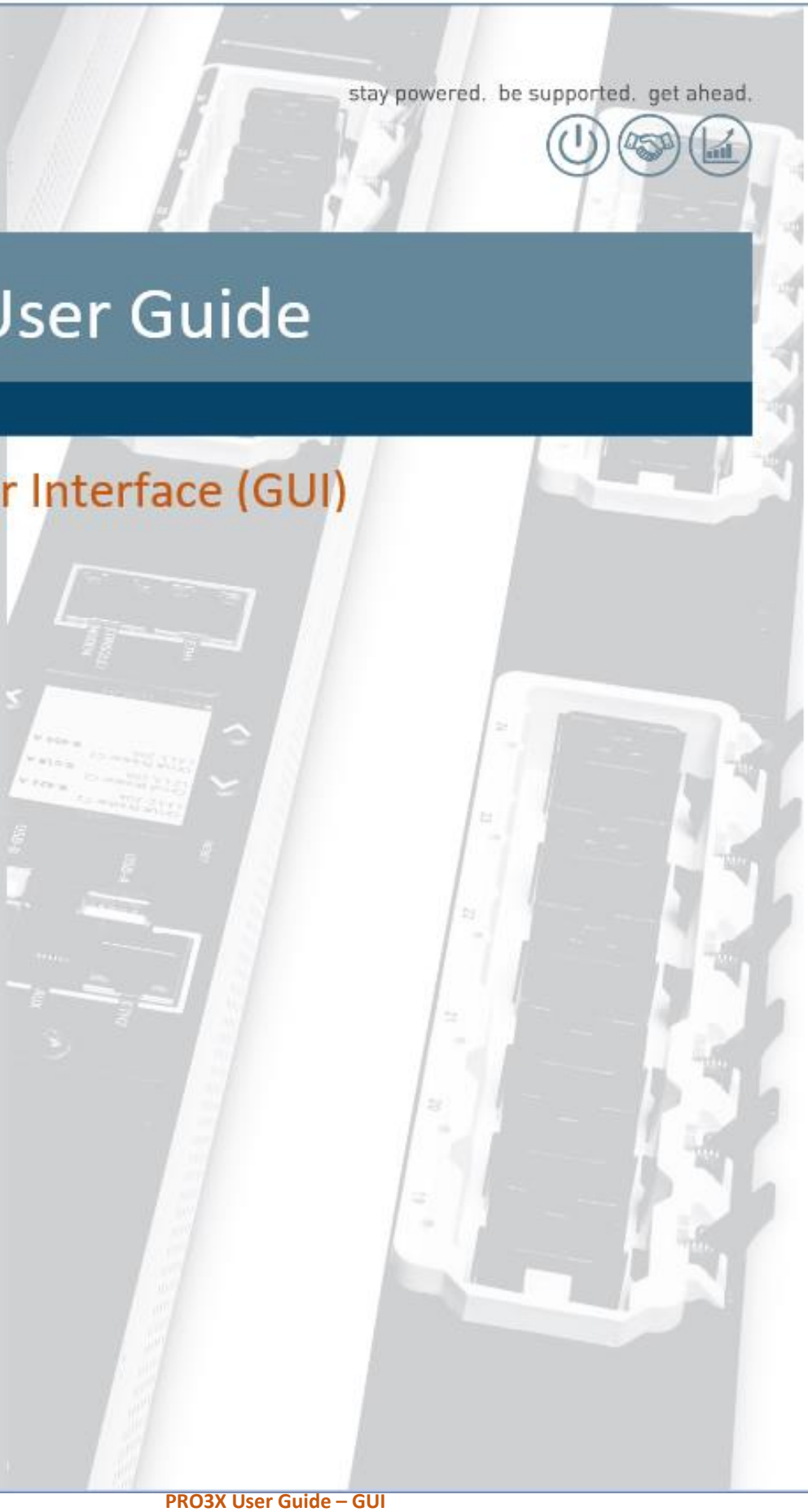
Server Technology
A brand of legrand

stay powered. be supported. get ahead.

PRO3X User Guide

Graphical User Interface (GUI)



1-800-835-1515
sales@servertech.com
www.servertech.com

Instructions
This symbol is intended to alert the user to the presence of important operating and maintenance (servicing) instructions in the literature accompanying the appliance.

Dangerous Voltage
This symbol is intended to alert the user to the presence of un-insulated dangerous voltage within the product's enclosure that may be of sufficient magnitude to constitute a risk of electric shock to persons.

Protective Grounding Terminal
This symbol indicates a terminal that must be connected to earth ground prior to making any other connections to the equipment.

Life-Support Policy

As a general policy, Server Technology® does not recommend the use of any of its products in the following situations:

- life-support applications where failure or malfunction of the Server Technology product can be reasonably expected to cause failure of the life-support device or to significantly affect its safety or effectiveness.
- direct patient care.

Server Technology will not knowingly sell its products for use in such applications unless it receives in writing assurances satisfactory to Server Technology that:

- the risks of injury or damage have been minimized,
- the customer assumes all such risks, and
- the liability of Server Technology is adequately protected under the circumstances.

The term life-support device includes but is not limited to neonatal oxygen analyzers, nerve stimulators (whether used for anesthesia, pain relief or other purposes), auto-transfusion devices, blood pumps, defibrillators, arrhythmia detectors and alarms, pacemakers, hemodialysis systems, peritoneal dialysis systems, neonatal ventilator incubators, ventilators (for adults or infants), anesthesia ventilators, infusion pumps, and any other devices designated as "critical" by the U.S. FDA.

Notices

301-4800-3 Rev B (091520)

1040 Sandhill Drive
Reno, Nevada 89521 USA

All Rights Reserved

The information in this document has been carefully checked and is believed to be accurate. However, changes are made periodically. These changes are incorporated in newer publication editions. Server Technology may improve and/or change products described in this publication at any time. Due to continuing system improvements, Server Technology is not responsible for inaccurate information which may appear in this manual. For the latest product updates, consult the Server Technology web site at www.servertech.com. In no event will Server Technology be liable for direct, indirect, special, exemplary, incidental, or consequential damages resulting from any defect or omission in this document, even if advised of the possibility of such damages.

In the interest of continued product development, Server Technology reserves the right to make improvements in this document and the products it describes at any time, without notices or obligation.

The Globe logo is a trademark of Server Technology, Inc., registered in the US. Use of the logos for commercial purposes without the prior written consent of Server Technology may constitute trademark infringement and unfair competition in violation of federal and state laws.

Server Technology, the Globe logo, Sentry, Switched CDU, CDU, PRO2, PIPS, POPS, PDU Power Pivot, and StartUp Stick are trademarks of Server Technology, Inc., registered in the US. EZip is a trademark of Server Technology.

Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Server Technology, Inc. disclaims any proprietary interest in trademarks and trade names other than its own.

Please Recycle
Shipping materials are recyclable. Please save them for later use, or dispose of them appropriately.

About Your User Guide

This user guide was designed for data center staff and administrators who monitor power, control outlet actions, and direct equipment operations in the data center network using the **Graphical User Interface (GUI**) on the PRO3X product group.

This guide is a detailed resource for the PRO3X GUI screens, descriptions, usage, step-by-step instructions, as well as providing screen examples and results to assist you with using the firmware's interface.

Contact Technical Support

Experience Server Technology's FREE Technical Support

Server Technology understands that there are often questions when installing and/or using a new product. Free Technical Support is provided from 8 a.m. to 5 p.m. Pacific Time, Monday through Friday.

Server Technology, Inc. (a brand of Legrand)

1040 Sandhill Road	Tel:	1-800-835-1515	Web:	www.servertech.com
Reno, Nevada 89521 USA	Fax:	775-284-2065	Email:	support@servertech.com

Safety Precautions

This section contains important safety/regulatory information that **must be reviewed** before installing and using the **PRO3X** PDU.

	Only for installation and use in a Restricted Access Location in accordance with the following installation and use instructions. **This equipment should only be installed by trained personnel.**	Destiné à l'installation et l'utilisation dans le cadre de Restricted Access Location selon les instructions d'installation et d'utilisation. **Cet équipement est uniquement destiné à être installé par personnel qualifié.**	Nur für Installation und Gebrauch in eingeschränkten Betriebszonen gemäß der folgenden Installations-und Gebrauchsanweisungen. **Dieses Gerät ist nur für den Einbau durch Personal vorgesehen.**
	This equipment is designed to be installed on a dedicated circuit. The power supply cord shall be a minimum of 1.5m (4.9ft) and a maximum of 4.5m (15ft). If using an extension power cord, the total length shall also be no more than the maximum allowed. The plug is considered the disconnect device and must be easily accessible.	Cet équipement a été conçu pour être installé que un circuit dédié. Le cordon d'alimentation doit être d'au moins 1,5M et un maximum de 4,5m. Si vous utilisez un cordon de rallonge, la longueur totale est également plus que le maximum autorise. La prise est considérée comme un dispositif de coupure et doit être facilement accessible.	Die Geräte sind für eine Installation an einer fest zugeordneten Leitung ausgelegt. Die Stromzuleitung hat eine Mindestlänge von 1,5m, und hochstens 4,5m. Sollten Sie ein Verlangerrungsnetzkabel, der Gesamtlange auch nicht mehr als die maximal zulassige sein. Der Stecker dient zur Trennung vom Netz und muss einfach erreichbar sein.
	The dedicated circuit must have circuit breaker or fuse protection. PDUs have been designed without a master circuit breaker or fuse to avoid becoming a single point of failure. It is the customer's responsibility to provide adequate protection for the dedicated power circuit. Protection of capacity equal to the current rating of the PDU must be provided and must meet all applicable codes and regulations. In North America, protection must have a 10,000A interrupt capacity.	Le circuit spécialisé doit avoir un disjoncteur ou une protection de fusible. PDUs ont été conçus sans disjoncteur général ni fusible pour éviter que cela devient un seul endroit de panne. C'est la responsabilité du client de fournir une protection adéquate pour le circuit-alimentation spécialisé. Protection de capacité équivalant à la puissance de l'équipement, et respectant tous les codes et normes applicables. Les disjoncteurs ou fusibles destinés à l'installation en Amérique du Nord doivent avoir une capacité d'interruption de 10.000 A.	Der feste Stromkreis muss mit einem Schutzschalter oder einem Sicherungsschutz versehen sein. PDUs verfügt über keinen Hauptschutzschalter bzw. über keine Sicherung, damit kein einzelner Fehlerpunkt entstehen kann. Der Kunde ist dafür verantwortlich, den Stromkreis sachgemäß zu schützen. Der Kapazitätsschutz entspricht der aktuellen Stromstärke der Geräte und muss alle relevanten Codes und Bestimmungen erfüllen. Für Installation in Nordamerika müssen Ausschalter bzw. Sicherung über 10.000 A Unterbrechungskapazität verfügen.
	Models with unterminated power cords: Input connector must be installed by qualified service personnel. Input connector rating must meet all applicable codes and regulations.	Modèles avec cordons d'alimentation non terminées: Le connecteur d'entrée doit être installé par un personnel qualifié. Entrée cote de raccordement doit respecter tous les codes et règlements électriques applicables.	Modelle mit nicht abgeschlossenen Netzkabel: Der Eingangsstecker darf nur von qualifiziertem Wartungspersonal installiert werden. Eingangsanschluss Bewertung müssen alle geltenden und verbindlichen Normen und Vorschriften entsprechen.
	Do not block venting holes when installing this product. Allow for maximum airflow at all times.	Ne bloquez pas les orifices d'aération lors de l'installation de ce produit. Permettre une circulation d'air maximale à tout moment.	Achten Sie darauf, dass keine Belüftungslöcher bei der Installation dieses Produkts. Damit für maximalen Luftstrom zu allen Zeiten.
	Installation Orientation: Vertical units are designed to be installed in vertical orientation.	Installation Orientation: Les unités vertical sont conçues pour être installées dans une orientation verticale.	Installationsausrichtung: Vertical Einheiten sind zur vertikalen Installation vorgesehen.
	Always disconnect the power supply cord before servicing to avoid electrical shock. For products with two input power cords, both must be disconnected before servicing.	Toujours débrancher le cordon d'alimentation avant de l'ouverture pour éviter un choc électrique. Pour les produits avec deux cordons d'alimentation d'entrée, les deux doivent être déconnectés avant l'entretien.	Trennen Sie das Netzkabel, bevor Sie Wartungsarbeiten Öffnung einen elektrischen Schlag zu vermeiden. Für Produkte mit zwei Eingangsstromkabel, sowohl, müssen vor der Wartung abgeschaltet werden.
	WARNING! High leakage current! Earth connection is essential before connecting supply!	ATTENTION! Haut fuite très possible! Une connection de masse est essentielle avant de connecter l'alimentation !	ACHTUNG! Hoher Ableitstrom! Ein Erdungsanschluss ist vor dem Einschalten der Stromzufuhr erforderlich!
	WARNING! Cx-xxE-x units double pole/neutral fusing	ATTENTION! Les unités Cx-xxE-x Double Pôle/Fusible sur le Neutre	ACHTUNG!: Cx-xxE-x Zweipolige bzw. Neutralleiter-Sicherung
	ATTENTION! Observe precautions for handling Electrostatic Sensitive Devices.	Attention ! Respecter les mesures de sécurité en manipulant des dispositifs sensibles aux décharges électrostatiques.	Achtung! Vorsichtshinweise zur Handhabung elektrostatisch empfindlicher Geräte beachten.
	Products rated for 240/415VAC may be fitted with a plug that is rated for a higher voltage. Caution must be taken to assure that the rating of the unit and the supply voltage match.	Les produits prévus pour 240/415VAC peut être équipé d'un bouchon qui est conçu pour une tension plus élevée. Des précautions doivent être prises pour assurer que la cote de l'unité et la tension d'alimentation correspond.	Produkte die für 240/415VAC zugelassen sind können mit einem Stecker der für eine höhere Spannung ausgestattet sein. Vorsicht ist geboten, um sicherzustellen, dass die erlaubten Betriebswerte des Gerätes und der Versorgungsspannung zueinander passen.

Attaching Safety Earth Ground Connection

Server Technology PDUs are supplied with an external safety ground connection to provide an alternate ground path for fault currents, and to maintain the same ground reference between it and the equipment rack.

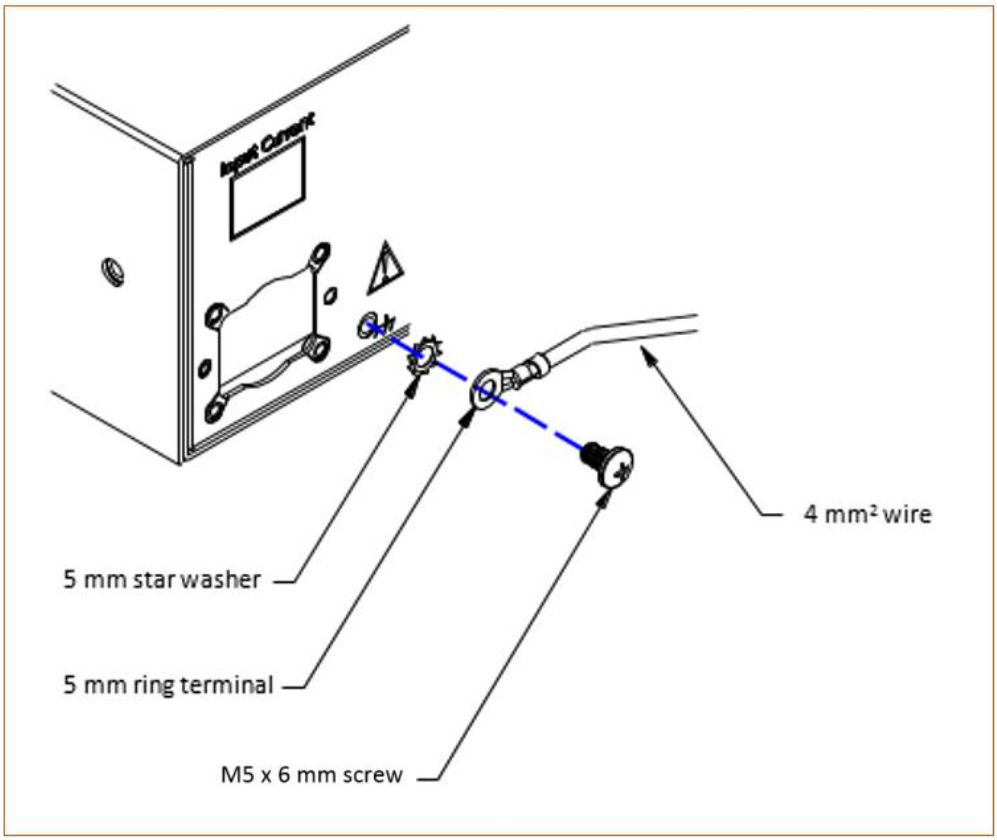
Note: The auxiliary external ground location may vary. Most PDUs will have it located near the power cord entry located near the ⏚ symbol.

User-Supplied Materials:

- One 5 mm internal (or external) tooth star washer;
- One 4.0 mm^2 (10 AWG) wire with 5 mm ring terminal;
- One metric M5 x 6 mm coarse pitch screw.

Instructions:

1. Connect one end of the ground wire to the equipment cabinet or local ground.
2. Locate the PDU external ground near the ⏚ symbol.
3. Connect the other end with a ring terminal and a M5 screw to the PDU external ground.
   To ensure proper grounding to chassis, use a star washer between ring terminal and PDU.



Using the Web Interface

This user guide explains how to use the screens and fields in the Web Graphical User Interface (GUI) to administer the PRO3X. Note that available screen functions may be dependent on model type.

Supported Web Browsers

- Internet Explorer® 11
- Firefox® 52 and later
- Safari® (Mac)
- Google® Chrome® 52 and later
- Android 4.2 and later
- iOS 7.0 and later

Login, Logout, and Password Change

The first time you log in to the PRO3X, use the factory default "admin" user credentials. For details, refer to the Quick Setup Guide accompanying the product.

After login, you can create user accounts for other users.

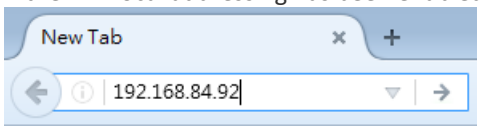
Login

You must enable JavaScript in the web browser for proper operation.

To log in to the web interface:

Open a browser and type the IP address of your PRO3X.

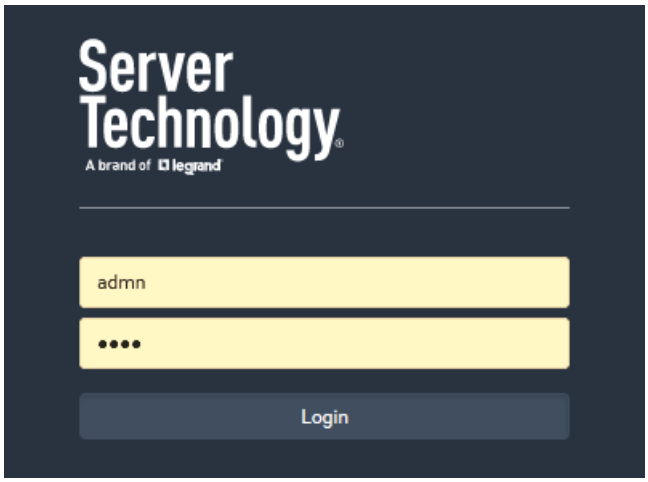
If the link-local addressing has been enabled, you can type *pdu.local* instead of an IP address.



Tip: You can also enter the desired page's URL so that you can immediately go to that page after login.

If any security alert message appears, accept it.

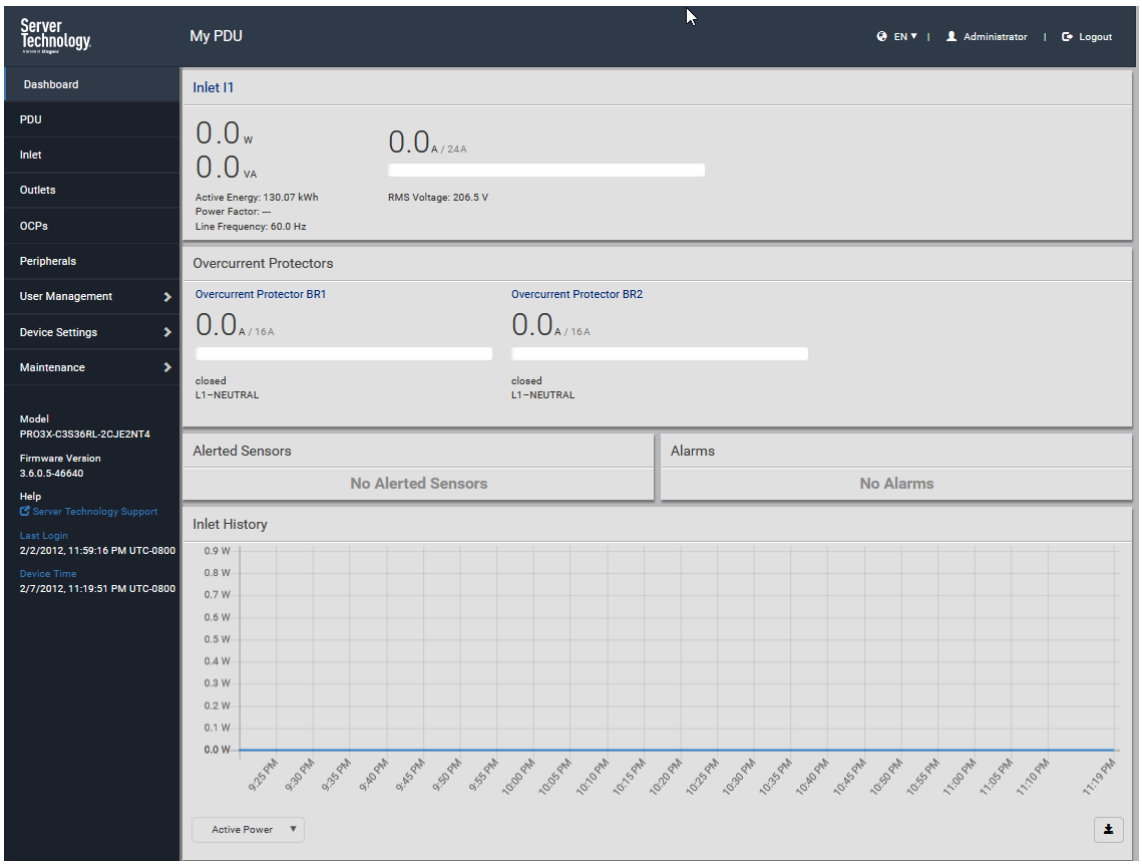
The login screen displays. Type your user name and password. User credentials are case sensitive.



(Optional) If a security agreement is displayed, accept it. Otherwise, you cannot log in.

Click Login or press Enter. The web interface of PRO3X opens.

Depending on your hardware configuration, your web interface shown onscreen may look slightly different from the image below.



Note: The address to access a link device in the Port Forwarding mode via non-standard ports is a combination of a protocol (http:// or https://), an IP address and a port number.

Changing Your Password

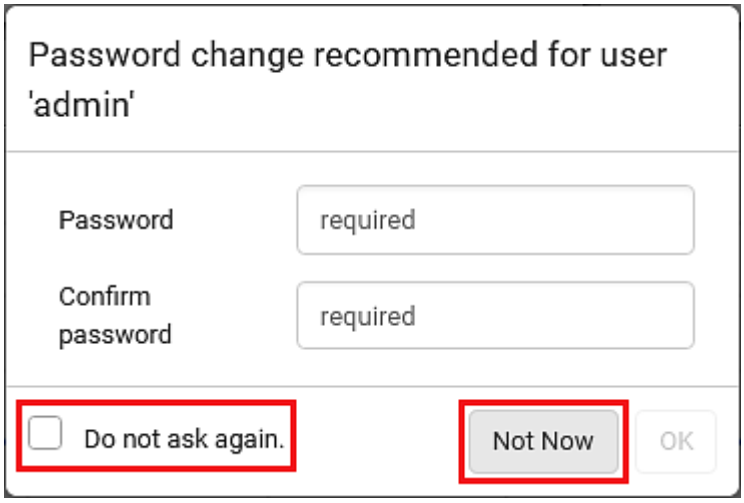
You need appropriate permissions to change your password. Refer to the following for details.

To change other users' passwords, Administrator Privileges are required instead.

Password change request on first login:

On *first login*, if you have both the Change Local User Management and Change Security Settings permissions, you can choose to either change your password or ignore it.

- *Not Now* ignores the request for this time only.
- *Do not ask again* ignores the request permanently. If you select this checkbox, then click *Not Now*.
- Or enter the new password and click Ok.



Users without permissions listed must change password.

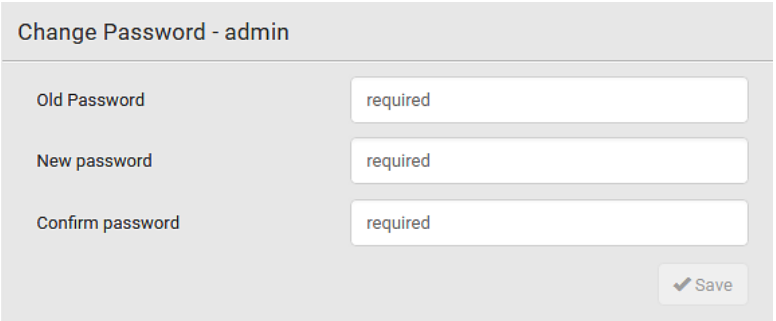
Note: This password change request also appears if the 'force password change' is enabled in the user account setting.

To change your password via the Change Password command:

You must have the Change Own Password permission to change your own password.

Choose User Management > Change Password.

First type the current password, and then the new password twice. Passwords are case sensitive. A password comprises 4 to 64 characters.



Remembering User Names and Passwords

PRO3X supports the password manager of common web browsers, including:

- Microsoft Internet Explorer®
- Mozilla Firefox®
- Google Chrome®

You can save the login name and password when these browsers ask whether to remember them.

For information on how to activate a web browser's password manager, see the user documentation accompanying your browser.

PRO3X does NOT support other browser password managers.

Logout

After finishing your tasks, you should log out to prevent others from accessing the PRO3X web interface.

To log out without closing the web browser:

Click "Logout" on the top-right corner.

-- OR --

Close the tab of PRO3X while there are other tabs available in the browser.

To log out by closing the web browser:

Click  on the top-right corner of the window.

-- OR --

Choose File > Close, or File > Exit.

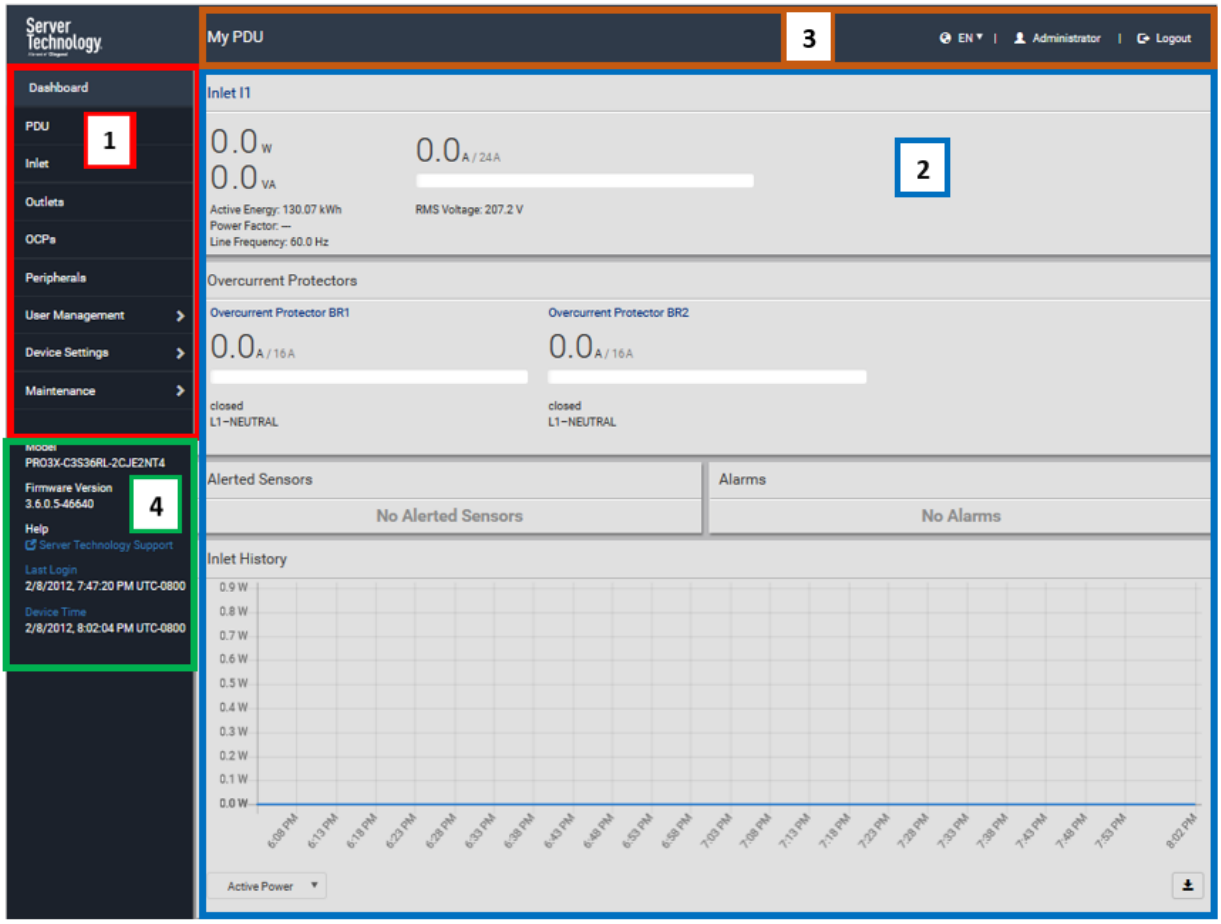
Web Interface Overview

The web interface consists of four areas as shown below.

Operation:

Click any menu or submenu item in the navigation area of 1.

The selected item's related data/setup page is opened in the area of 2. Then view/configure settings in the opened page.

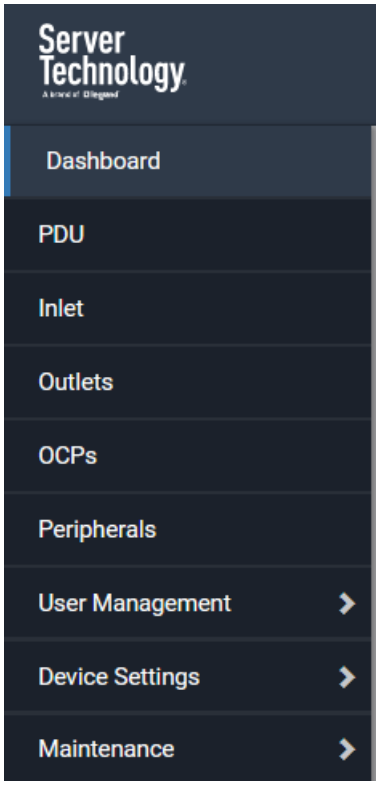


Number	Web Page Section
1	Navigation pane with menu and menu items.
2	Resulting data or setup page for the menu item you selected.
3	Device/Language/User Information header: Left side is the PRO3X device name. Right side shows the following: - Displayed language, which you can change. Default is English (EN). - Your login name, which you can click to view your current user account settings. - Logoff button.
4	General Information pane, top to bottom: - Your PRO3X model. - Current firmware version. - Server Technology support – link to the Technical Support page. - Date and time of your user account's last login – click to view your login history. - PRO3X system time, which is converted to the time zone of your computer or mobile device; click Device Time to open the Date/Time setup page.

To return to the main menu and the Dashboard page, click Server Technology at the top-left corner.

Menu

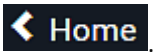
Depending on your model and hardware configuration, your PRO3X may show all or some of the menu items shown below.



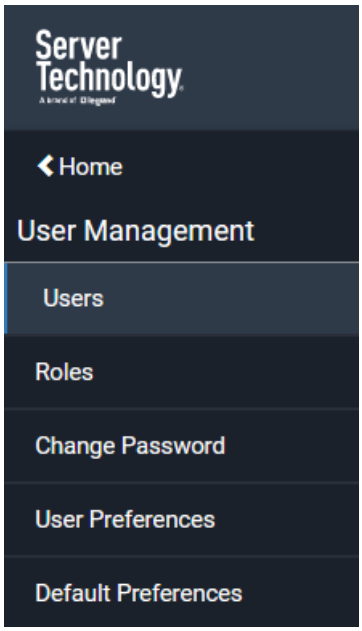
Menu Item	Description
Dashboard	Summary of the PRO3X status, including a list of alerted sensors and alarms, if any.
PDU	Device data and settings, such as the device name and MAC address.
Inlet	Inlet status and settings, such as inlet thresholds.
Outlets	Outlet status and settings, such as outlet thresholds.
Overcurrent Protectors (OCPs)	OCP status and settings, such as OCP thresholds. The OCPs menu item displays only when there are overcurrent protectors implements on your PDU model.
Peripherals	Status and settings of Server Technology environmental sensor packages, if connected.
User Management	Data and settings of user accounts and groups, such as password change.
Device Settings	Device-related settings, including network, security, system time, event rules, and more.
Maintenance	Device information and maintenance commands, such as firmware upgrade, device backup and reset.

If a menu item contains a submenu, the submenu is shown after clicking the menu item.

To return to the previous menu list, do any of the following:

Click the topmost link with the symbol **<**. For example, click 

.



Click 

at the top-left corner to return to the main menu.

Quick Access to a Specific Page

If you often visit a specific page in the PRO3X web interface, you can note down its URL or bookmark it with your web browser. Next time, you just enter its URL in the address bar of the browser prior to login. After login, the PRO3X immediately shows the wanted page rather than the Dashboard page.

Besides, you can also send the URL to other users so that they immediately see that page after login, using their own user credentials.

URL examples:

In the following examples, it is assumed that the IP address of PRO3X is 192.168.84.118.

Page Name	URL
Peripherals	https://192.168.84.118/#/peripherals
Event Log	https://192.168.84.118/#/maintenance/eventLog/0

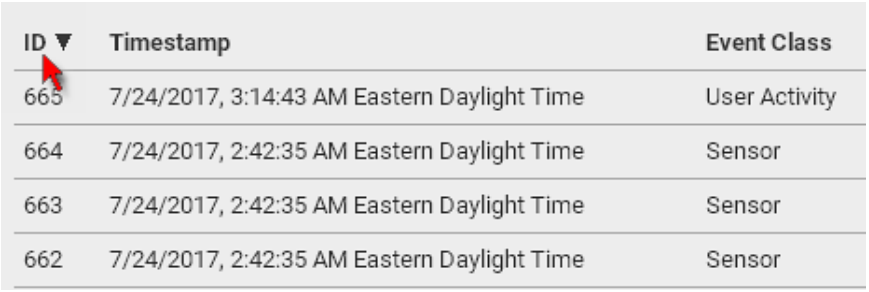
Sorting a List

If any list displays an arrow (▲ or ▼) in one of its column headers, you are allowed to resort the list by clicking any column header. The list will be resorted in the ascending or descending order based on the selected column.

Illustration -- Event Log:

By default, the Event Log is sorted in the descending order based on the ID column. Therefore, the arrow ▼ is displayed adjacent to the ID header.

To have it re-sorted in the ascending order based on the same column, click the ID header.

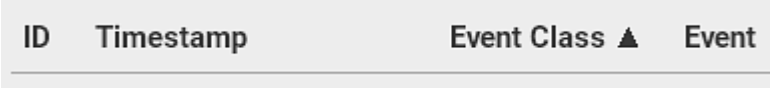


ID ▼	Timestamp	Event Class
665	7/24/2017, 3:14:43 AM Eastern Daylight Time	User Activity
664	7/24/2017, 2:42:35 AM Eastern Daylight Time	Sensor
663	7/24/2017, 2:42:35 AM Eastern Daylight Time	Sensor
662	7/24/2017, 2:42:35 AM Eastern Daylight Time	Sensor

The arrow turns to ▲, indicating the list is sorted in the "ascending" order.

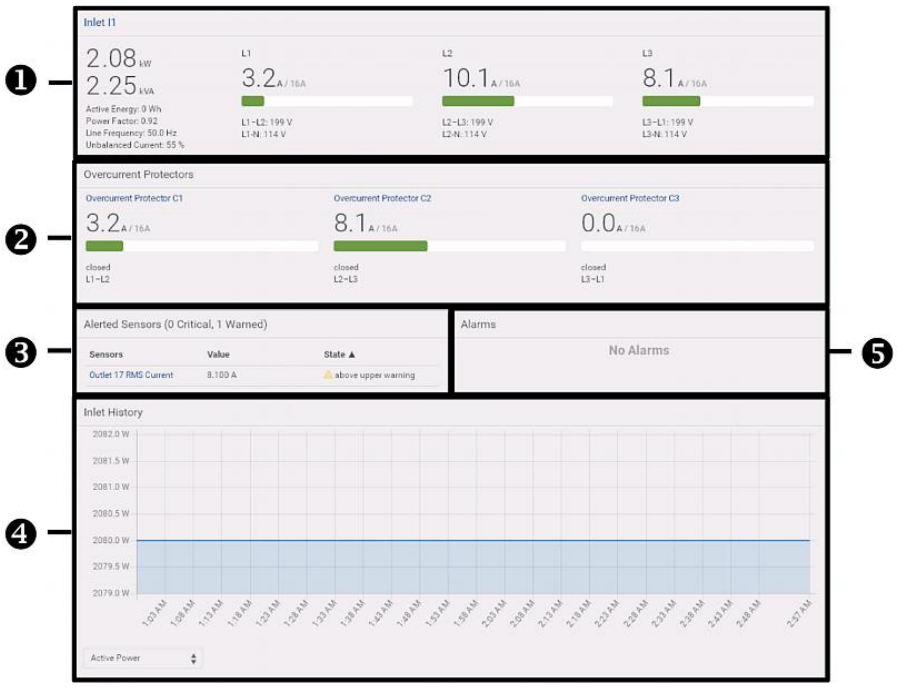
To resort the list based on a different column, click a different column header. In this example, the 'Event Class' column is clicked.

The arrow ▲ now appears adjacent to the selected column 'Event Class,' indicating the list is sorted in the ascending order based on that column.



Dashboard

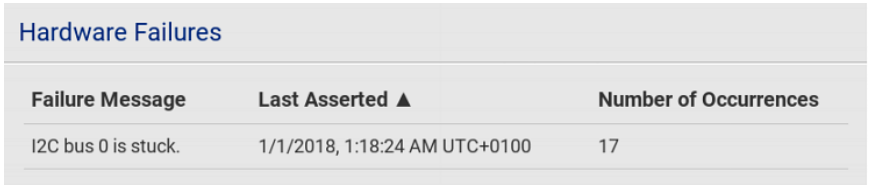
The Dashboard page contains four to five sections, depending on your PDU model.



Number	Section	Information Displayed
1	Inlet I1	▪ Overview of inlet power data ▪ A current bar per phase, which changes colors to indicate the RMS current state - green: normal - yellow: warning - red: critical
2	Overcurrent Protectors (OCPs)	This section is available only when your PRO3X has overcurrent protectors. ▪ Overview of each OCP's status ▪ A current bar per OCP, which changes colors to indicate the RMS current state - green: normal - yellow: warning - red: critical
3	Alerted Sensors	▪ When no sensors enter the alarmed state, this section shows the message "No Alerted Sensors." ▪ When any sensor enters the alarmed state, this section lists all of them.
4	Inlet History	The chart of the inlet's active power history is displayed by default. You can make it show a different data type.
5	Alarms	This section shows data only after you have set event rules requiring users to take the acknowledgement action. ▪ When there are no unacknowledged events, this section shows the message "No Alarms." ▪ When there are unacknowledged events, this section lists all of them.

The Hardware Failures section:

If PRO3X detects any internal hardware issues, a section labeled "Hardware Failures" will appear on the Dashboard page, listing all of current hardware issues.



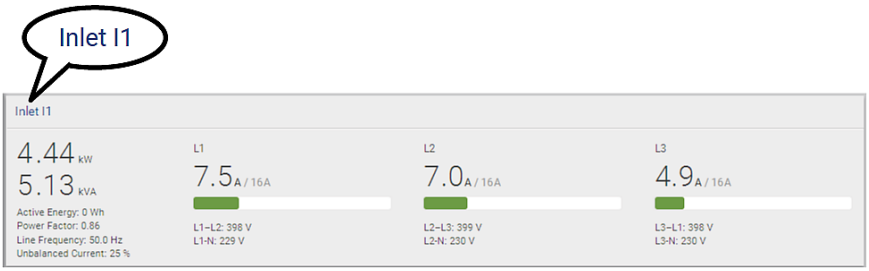
This section does NOT display as long as there are no hardware failures present.

Dashboard - Inlet I1

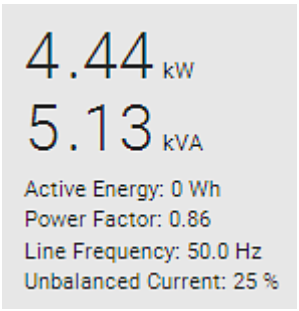
The number of phases shown in the Inlet section is model dependent.

Link to the Inlet page:

To view more information or configure the inlet(s), click this section's title 'Inlet I1' to go to the Inlet page.



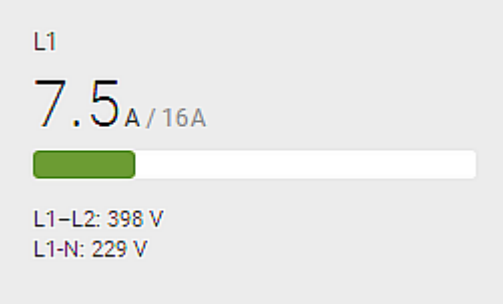
Left side - generic inlet power data:



The left side lists all or some of the following data. Available data is model dependent.

- Active power (kW or W)
- Apparent power (kVA or VA)
- Active energy (kWh or Wh)
- Power factor
- Line frequency (Hz)
- Unbalanced current (%) - *model dependent*

Right side - inlet's current and voltage:



The right side shows the current and voltage data per phase. For a single-phase device, it shows only one line, but for a three-phase device, it shows three lines (L1, L2 and L3).

Inlet data from top to bottom includes:

- RMS current (A) and rated current
- The smaller, gray text adjacent to RMS current is the rated current.
- A bar showing the RMS current level
- RMS voltage (V)

The RMS current bars automatically change colors to indicate the current status if the thresholds have been enabled.

Status	Bar colors
normal	
above upper warning	
above upper critical	

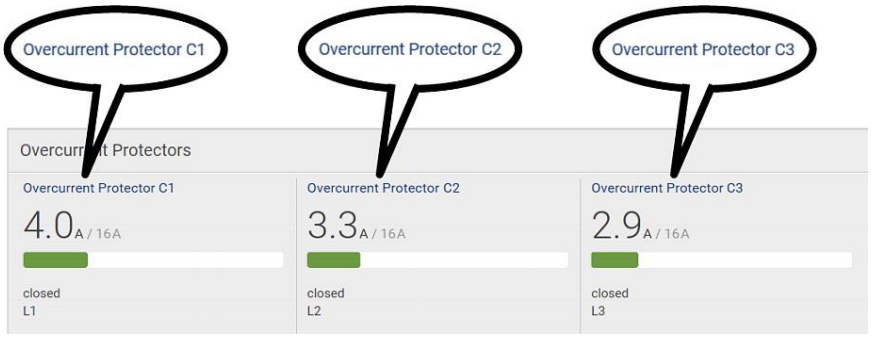
Note: The "below lower warning" and "below lower critical" states also show yellow and red colors respectively. However, it is not meaningful to enable the two thresholds for current levels.

Dashboard - OCP

Availability and total number of OCPs depend on the models.

Each OCP's link:

To view more information or configure individual OCPs, click the desired OCP's index number, which is C1, C2 and the like, to go to its setup page.



Each OCP's power data:

OCP data from top to bottom includes:

- RMS current (A), and rated current
- Smaller gray text adjacent to RMS current is each OCP's rated current, such as "16A" shown in the above diagram.
- A bar showing OCP current levels
- OCP status -- open or closed
- Associated line pair

The RMS current bars automatically change colors to indicate the current status if OCP thresholds have been enabled.

Status	Bar colors
normal	
above upper warning	
above upper critical	

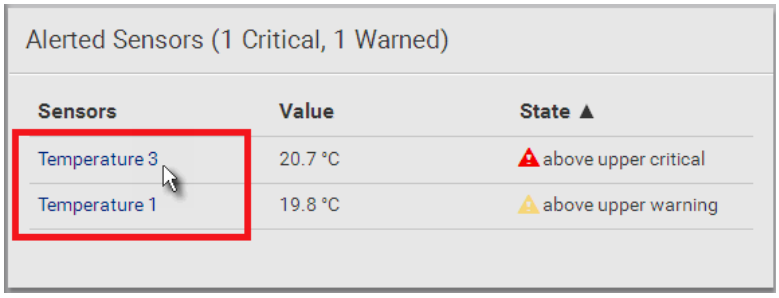
Note: The "below lower warning" and "below lower critical" states also show yellow and red colors respectively. However, it is not meaningful to enable the two thresholds for current levels.

Dashboard - Alerted Sensors

When any internal sensors or environmental sensor packages connected to the PRO3X enter an abnormal state, the Alerted Sensors section in the Dashboard show them for alerting users. This section also lists tripped circuit breakers or blown fuses, if available.

To view detailed information or configure each alerted sensor, you can click each sensor's name to go to individual sensor pages.

If wanted, you can resort the list by clicking the desired column header.



Summary in the section title:

Information in parentheses adjacent to the title is the total number of alerted sensors.

For example:

- **1 Critical**: 1 sensor enters the critical or alarmed state.
  - Numeric sensors enter the critical state.
  - State sensors enter the alarmed state.
- **1 Warned**: 1 'numeric' sensor enters the warning state.

List of alerted sensors:

Two icons are used to indicate various sensor states.

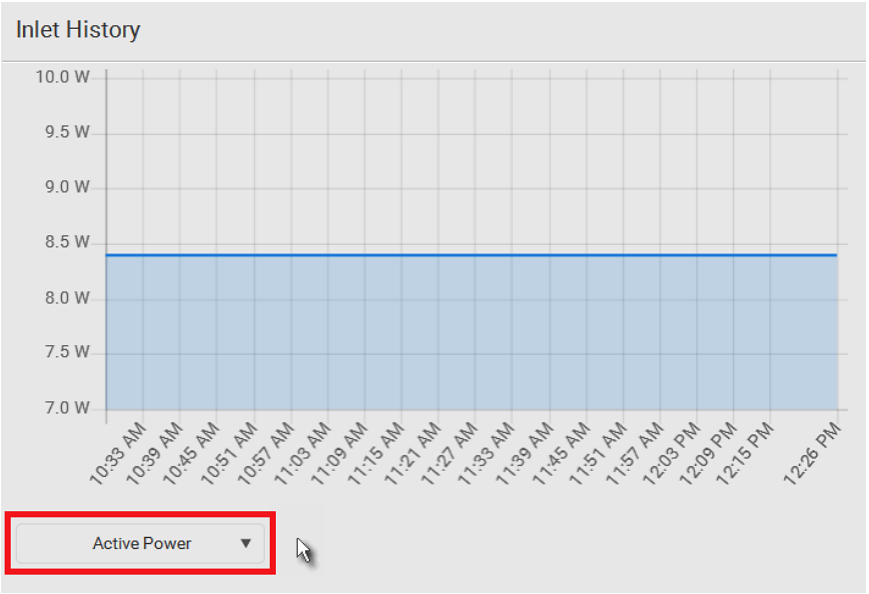
Icons	Sensor states
	Numeric sensors: ▪ above upper warning ▪ below lower warning
	Numeric sensors: ▪ above upper critical ▪ below lower critical
	State sensors: ▪ alarmed state

Dashboard - Inlet History

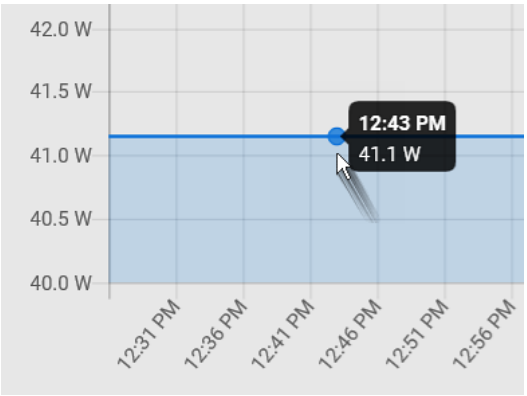
The inlet's power chart helps you observe whether there were abnormal events within the past tens of minutes. The default is to show the inlet's active power data.

You can have it show the chart of other inlet power data. Simply select a different data type by clicking the selector  below the diagram. Available data types include:

- RMS current
- RMS voltage
- Active power
- Apparent power

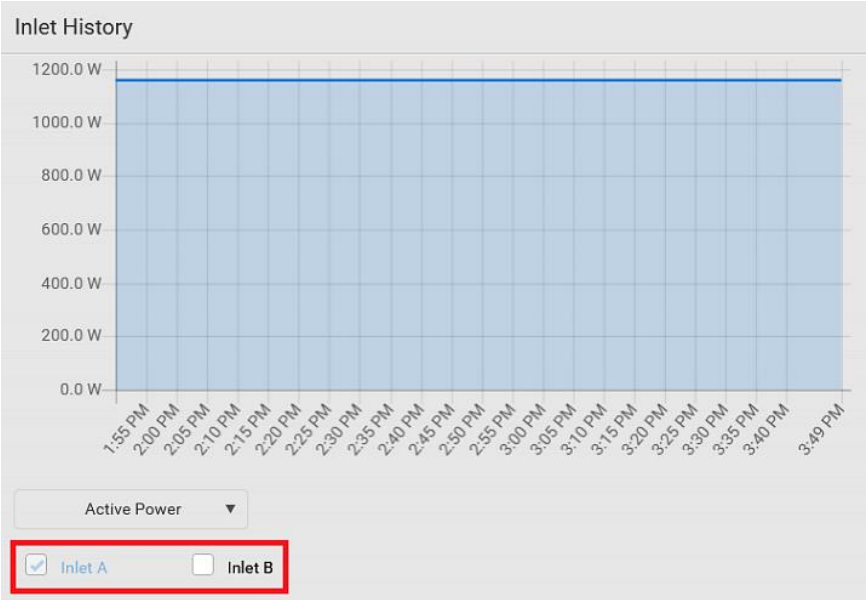


To retrieve the exact data at a particular time, hover your mouse over the data line in the chart. Both the time and data are displayed as illustrated below.



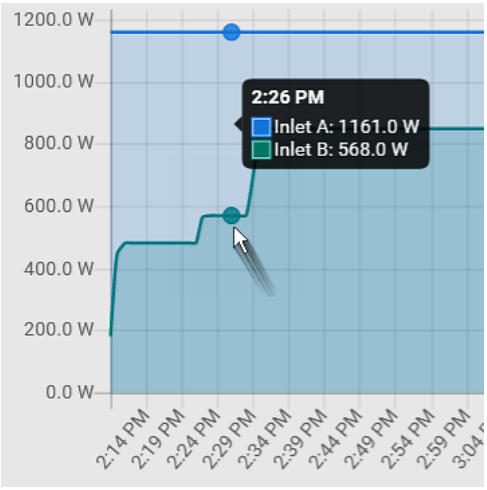
Inlet selection on multi-inlet models:

If your PDU is a multi-inlet model, you can have one or multiple inlets show their power charts by selecting the checkbox(es) of the desired inlet(s).



When multiple inlets are displayed in the chart, their colors differ. You can identify each inlet's data according to the colors of the selected inlet checkboxes.

When both inlets are shown in the chart, simply hover your mouse over either inlet's data line. Both inlets' values display simultaneously, marked with corresponding colors.



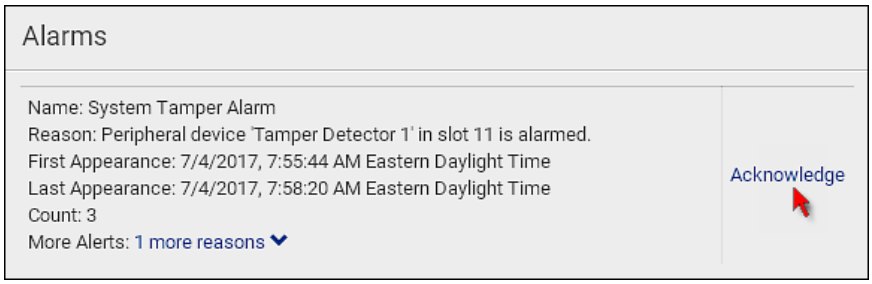
Dashboard - Alarms

If configuring any event rules which require users to take the acknowledgment action, the Alarms section will list any event which no one acknowledges yet since event occurrence.

Only users with the 'Acknowledge Alarms' permission can manually acknowledge an alarm.

To acknowledge an alarm:

Click Acknowledge, and that alarm then disappears from the Alarms section.



This table explains each column of the alarms list.

Field	Description
Name	Custom name of the Alarm action.
Reason	The first event that triggers the alert.
First Appearance	Date and time when the event indicated in the Reason column occurred for the first time.
Last Appearance	Date and time when the event indicated in the Reason column occurred for the last time.
Count	Number of times the event indicated in the Reason column has occurred.
More Alerts	This field appears only when there are more than one types of events triggering this alert. If there are other types of events (that is, other reasons) triggering the same alert, the total number of additional reasons is displayed. You can click it to view a list of all events.

The date and time shown on the PRO3X web interface are automatically converted to your computer's time zone. To avoid time confusion, it is suggested to apply the same time zone settings as those of PRO3X to your computer or mobile device.

Tip: You can also acknowledge all alarms by operating the LCD display.

PDU

The PRO3X device's generic information and PDU settings are available on the PDU page.

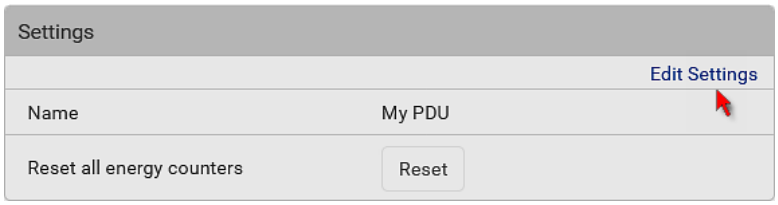
To open the PDU page, click 'PDU' in the Menu.

Device information shown:

Firmware version
Serial number
MAC address
Rating
Status of +12V Power Supply Sensor

To configure global settings:

Click Edit Settings.



In the Name field, type the name you prefer.

Click Save.

To view total active energy and power on multi-inlet models:

If your PRO3X is a multi-inlet model, a "Power" section for showing the data of total active energy and total active power is available on the PDU page.

For a regular PRO3X model with multiple inlets:

Total active energy = sum of all inlets' active energy values
Total active power = sum of all inlets' active power values

Sensor	Value	State
Active Power	16 W	normal
Active Energy	100243 Wh	normal

To configure the thresholds of total active energy and power:

For a multi-inlet model or an in-line monitor, a "Thresholds" section is available on the PDU page.

Time Units

If you choose to type a new value in the time-related fields, such as the "Idle timeout period" field, you must add a time unit after the numeric value. For example, you can type '15 s' for 15 seconds.

Note that different fields have different range of valid values.

Time units:

Unit	Time
ms	millisecond(s)
s	second(s)
min	minute(s)
h	hour(s)
d	day(s)

Setting Thresholds for Total Active Energy or Power

This section applies only to multi-inlet models, including in-line monitors.

Thresholds for total active energy and total active power are disabled by default. You can enable and set them so that you are alerted when the total active energy or total active power hits a certain level.

For a regular PRO3X model with multiple inlets:

- Total active energy = sum of all inlets' active energy values
- Total active power = sum of all inlets' active power values

For an in-line monitor with multiple inlets/outlets:

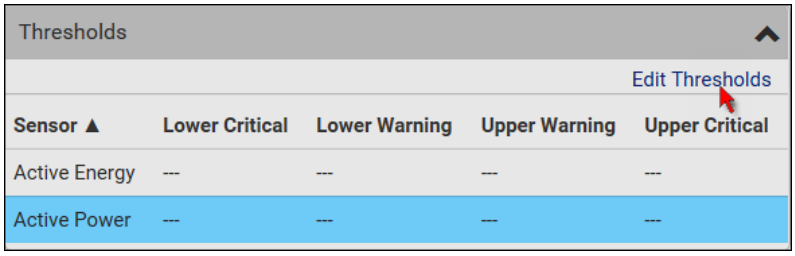
- Total active energy = sum of all outlets' active energy values
- Total active power = sum of all outlets' active power values

To configure thresholds for total active energy and/or power:

Click PDU. On the PDU page, you can also view the total active power and total active energy.

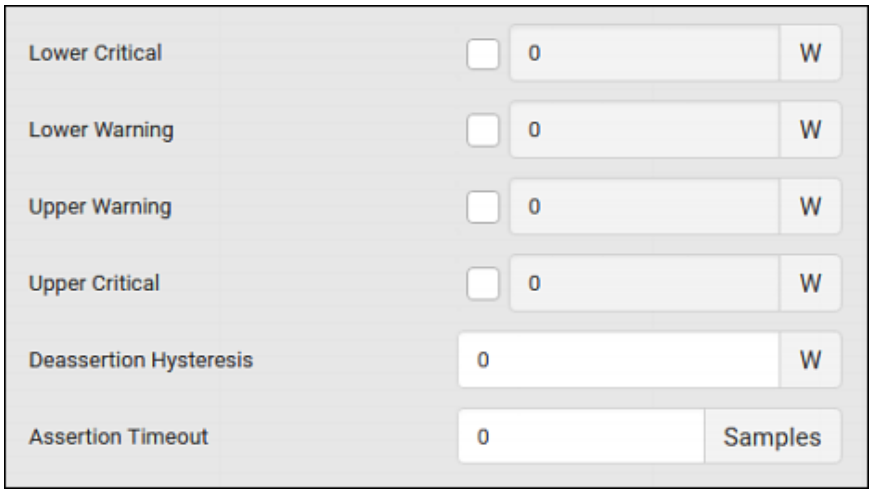
Click the Thresholds title bar at the bottom of the page to display thresholds.

Click the desired sensor **(**required), and then click Edit Thresholds.



Make changes as needed.

- To enable any threshold, select the corresponding checkbox.
- Type a new value in the accompanying text box.



Click Save.

+12V Power Supply Sensor

A PRO3X PDU's controller receives DC 12V power from its inlet. A sensor monitors the power supply status and indicates it on the PDU page.

State	Description
OK	The PRO3X controller is receiving power from its own inlet.
fault	The PRO3X controller cannot receive power from its own inlet because of a power failure on the inlet or a broken 12V power supply. Instead it is receiving power from another PRO3X PDU. After entering the fault state, this sensor is listed in the Alerted Sensors section of the Dashboard.
unavailable	The communication with the 12V power supply sensor is lost.

Alternatives for checking the 12V power supply status:

- Dot-matrix LCD panel.
- CLI command: `show pdu details`.

Inlet

You can view all inlet information, configure inlet-related settings, or reset the inlet active energy on the Inlet page. To open this page, click 'Inlet' in the Menu.

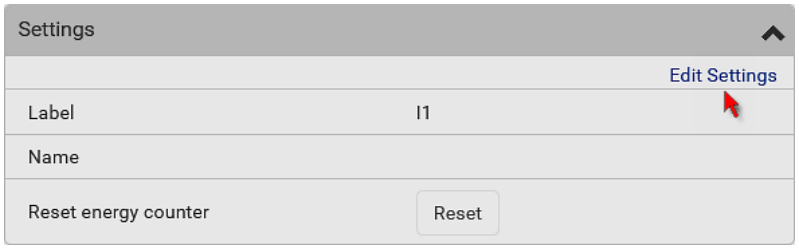
Inlet thresholds, once enabled, help you identify whether the inlet enters the warning or critical level. In addition, you can have PRO3X automatically generate alert notifications for any warning or critical status.

Generic inlet information shown:

- Inlet power overview, which is the same as *Dashboard - Inlet I1*
- A list of inlet sensors with more details. Number of available inlet sensors depends on the model.
- Sensors show both readings and states.
- Sensors in warning or critical states are highlighted in yellow or red.
- Inlet's power chart, which is the same as *Dashboard - Inlet History*

To customize the inlet's name:

Click Edit Settings.



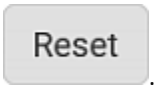
Type a name for the inlet. For example, you can name it to identify the power source.

Click Save. The inlet's custom name is displayed on the Inlet or Dashboard page, followed by its label in parentheses.

To reset the inlet's active energy counter:

Only users with the "Admin" role assigned can reset active energy readings.

The energy reset feature per inlet is especially useful when your PRO3X has more than one inlet.

Click 

.

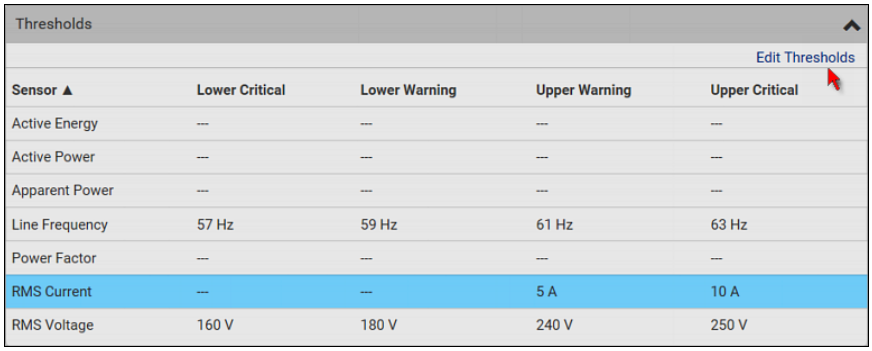
Click Reset on the confirmation message. This inlet's active energy reading is then reset to zero.

To configure inlet thresholds:

Per default, there are pre-defined RMS voltage and current threshold values in related fields. You can modify them to meet your needs.

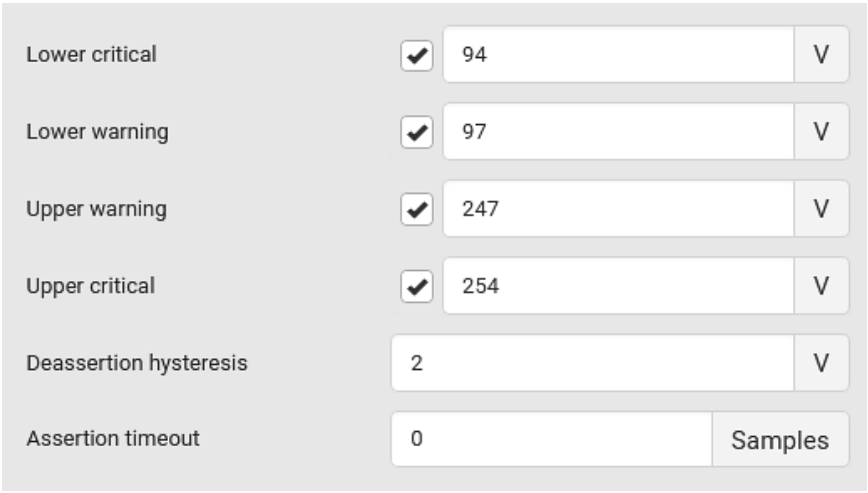
Click the Thresholds title bar at the bottom of the page to display inlet thresholds.

Click the desired sensor (required), and then click Edit Thresholds.



Make changes as needed.

- To enable any threshold, select the corresponding checkbox.
- Type a new value in the accompanying text box.



Click Save.

To configure residual current thresholds:

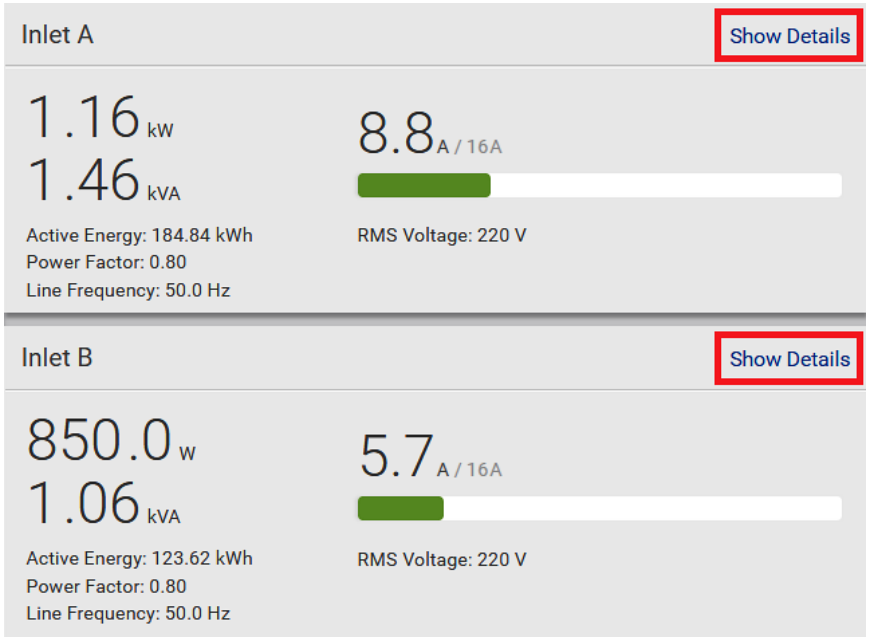
If your model supports residual current monitoring, a section titled "Residual Current Monitor" is displayed on the Inlet page.

Configuring a Multi-Inlet Model

If the PRO3X has more than one inlet, the Inlets page lists all inlets.

To view or configure each inlet:

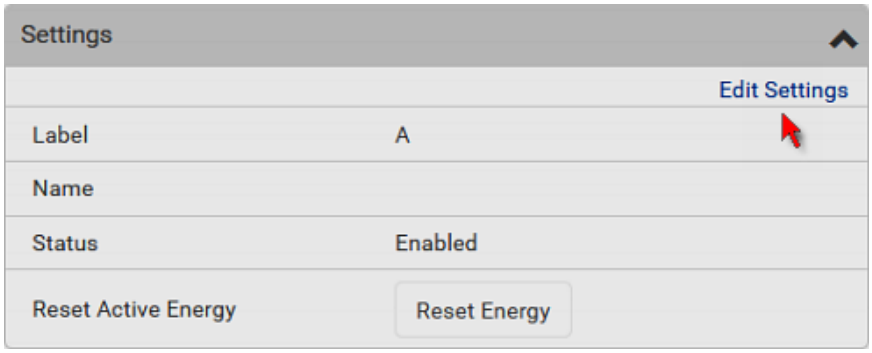
Click 'Show Details' of the desired inlet.



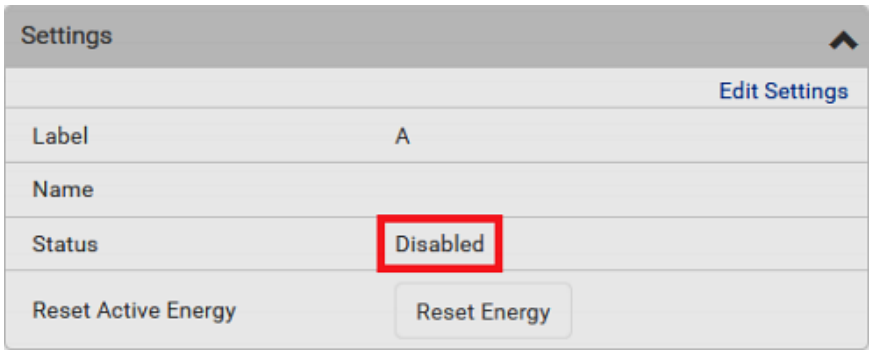
Now you can configure the selected inlet, such as enabling thresholds or resetting its energy. To disable the inlet, see the following instructions.

To disable one or multiple inlets:

On the individual inlet's data page, click Edit Settings.



Select the "Disable this inlet" checkbox.
Click Save. The inlet status now shows "Disabled."



To disable additional inlets, repeat the above steps.

If disabling an inlet will result in all inlets being disabled, a confirmation dialog appears, indicating that all inlets will be disabled. Then click Yes to confirm this operation or No to abort it.

After disabling any inlet, the following information or features associated with the disabled one are no longer available:

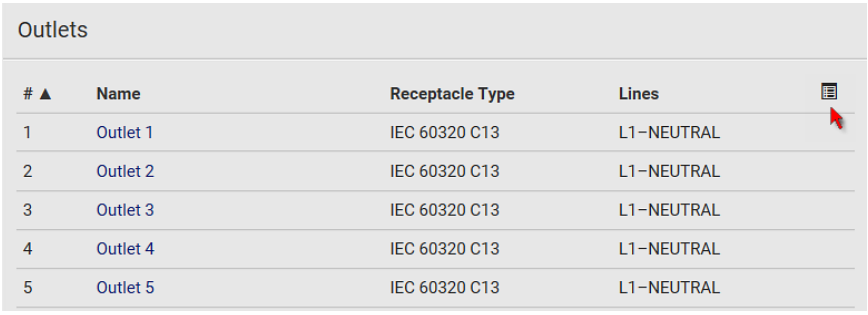
- Sensor readings, states, warnings, alarms or event notifications associated with the disabled inlet.
- Sensor readings, states, warnings, alarms or event notifications for all outlets and overcurrent protectors associated with the disabled inlet.
- The outlet-switching capability, if available, for all outlets associated with the disabled inlet.

Exception: All active energy sensors continue to accumulate data regardless of whether any inlet has been disabled.

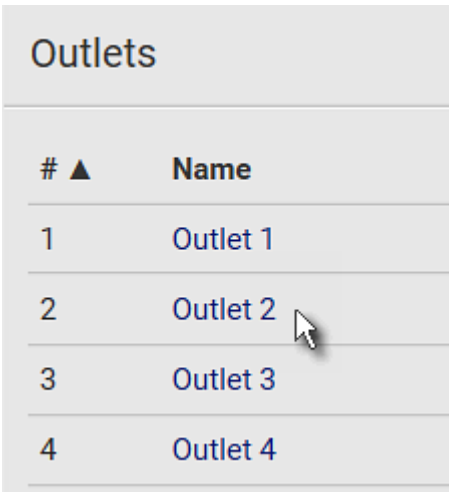
Warning: A disabled inlet, if remaining connected to a power source, continues to receive power from the connected power source and supplies power to the associated outlets and overcurrent protectors.

Outlets

The Outlets page shows a list of all outlets and their data, such as each outlet's associated lines. To open this page, click 'Outlets' in the Menu.



Go to an individual outlet's data/setup page by clicking an outlet's name.



If wanted, you can resort the list by clicking the desired column header. To show or hide specific columns on the outlets overview page:

Click  to show a list of outlet data types.

Select those you want to show, and deselect those you want to hide.

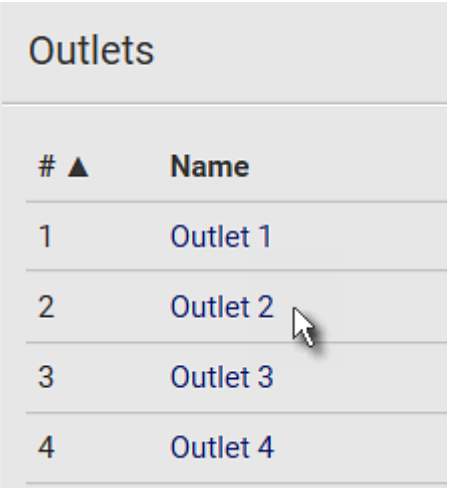
Available Data of the Outlets Overview Page

All of the following outlet data is displayed on the outlets overview page based on your selection. To show or hide specific data, click  .

- Receptacle type
- Lines associated with each outlet

Individual Outlet Pages

An outlet's data/setup page is opened after clicking the outlet's name on the Outlets overview page.

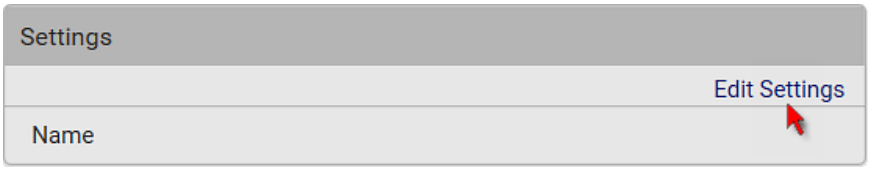


The individual outlet's page shows this outlet's detailed information.

In addition, you can perform the following operations on this outlet page.

To configure this outlet:

Click Edit Settings.



Specify the outlet name.

Type an outlet name up to 64 characters long.

Click Save. The outlet's custom name, if available, is displayed in the outlets list, following by its label in parentheses.

Other operations:

You can go to another outlet's data/setup page by clicking the outlet selector on the top-left corner.
You can go to the associated Inlet's or overcurrent protector's data pages by clicking the Inlet or Overcurrent Protector links in the Details section.

Detailed Information on Outlet Pages

Each outlet's data page has the Details section for showing general outlet information.

Details section:

Field	Description
Label	The physical outlet number
Receptacle type	This outlet's receptacle type
Lines	Lines associated with this outlet
Inlet	Inlet associated with this outlet
Overcurrent protector	This information is available only when your PRO3X has overcurrent protectors. Overcurrent protector associated with this outlet

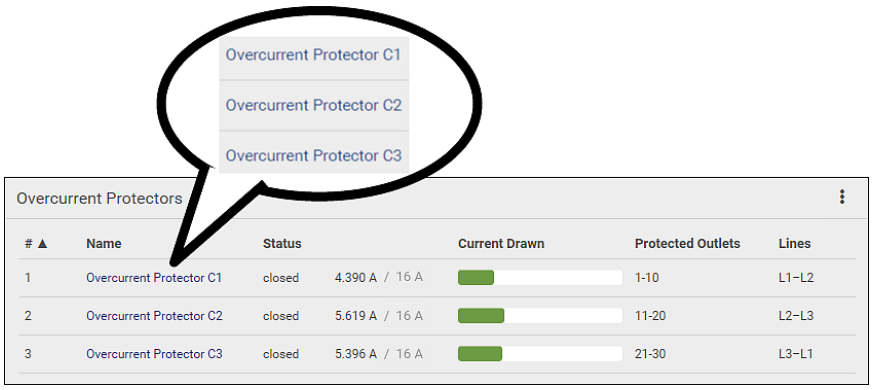
OCPs

The OCPs page is available only when you PRO3X has overcurrent protectors, such as circuit breakers.

The OCPs page lists all overcurrent protectors as well as their status. If any OCP trips or its current level enters the alarmed state, it is highlighted in red or yellow.

To open the OCPs page, click 'OCPs' in the Menu.

You can go to each OCP's data/setup page by clicking its name on this page.



If wanted, you can resort the list by clicking the desired column header.

Overcurrent protector overview:

OCP status - open (tripped) or closed

Current drawn, rated current and current bar

The smaller, gray text adjacent to "current drawn" is the rated current of each OCP.

The RMS current bars change colors to indicate the status if the OCP thresholds have been configured and enabled.

Status	Bar colors
normal	
above upper warning	
above upper critical	

Note: The "below lower warning" and "below lower critical" states also show yellow and red colors respectively. However, it is not meaningful to enable the two thresholds for current levels.

To configure current thresholds for multiple overcurrent protectors:

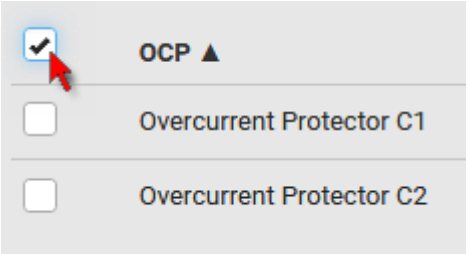
OCP thresholds, when enabled, help you identify the OCP whose RMS current enters the warning or critical level with the yellow or red color. In addition, you can have PRO3X automatically generate alert notifications for any warning or critical status.

Note: By default, upper thresholds of an OCP's RMS current have been configured. You can modify them as needed.

Click ⋮ > Threshold Bulk Setup.

Select one or multiple OCPs.

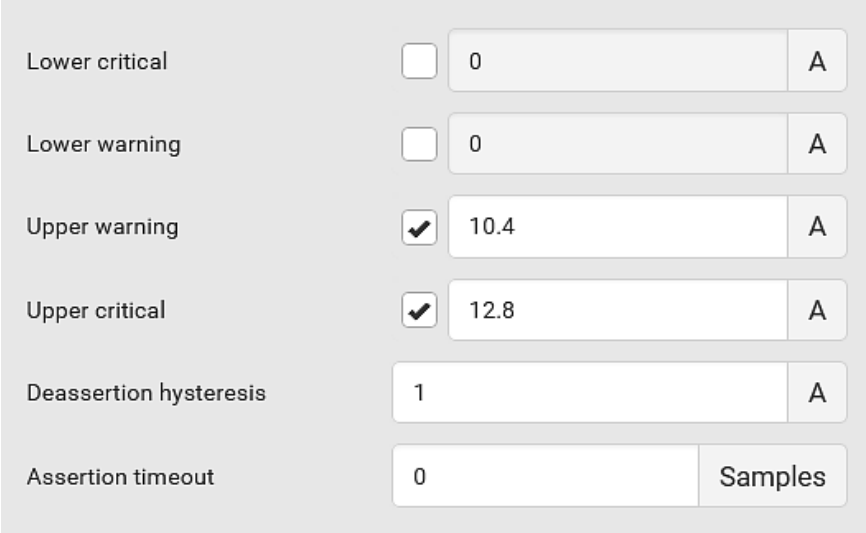
To select all OCPs, simply click the topmost checkbox in the header row.



Click Edit Thresholds.

Make changes as needed.

- To enable any threshold, select the corresponding checkbox.
- Type a new value in the accompanying text box.



Click Save.

Individual OCP Pages

An OCP's data/setup page is opened after clicking any OCP's name on the OCPs or Dashboard page.

General OCP information:

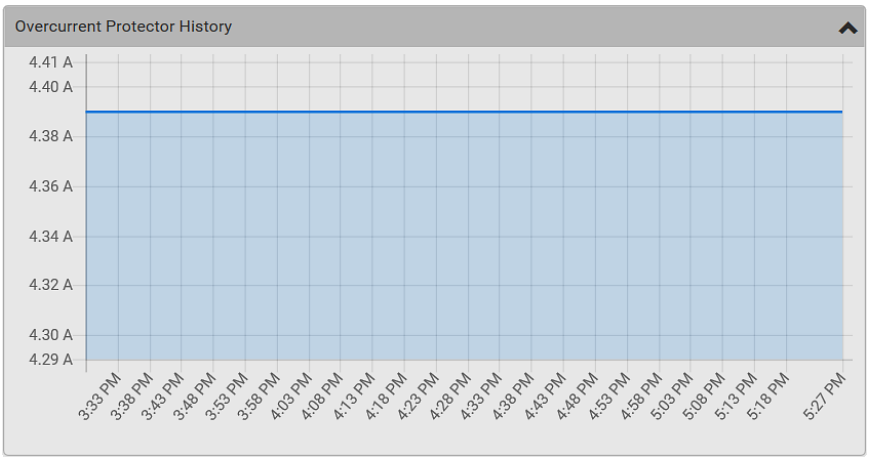
Field	Description
Label	This OCP's physical number.
Status	open or closed.
Type	This OCP's type.
Rating	This OCP's rated current.
Lines	Lines associated with this OCP.
Protected outlets	Outlets associated with this OCP.
Inlet	Inlet associated with this OCP. Note: This information is useful when your PDU has multiple inlets.
RMS current	This OCP's current state and readings, including current drawn and current remaining.

To customize this OCP's name:

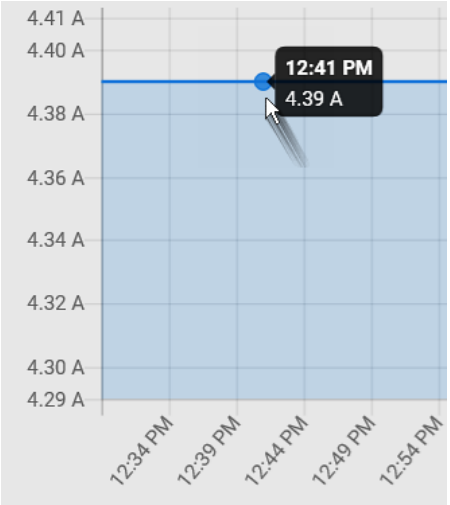
1. Click Edit Settings.
2. Type a name.
3. Click Save.

To view this OCP's RMS current chart:

This OCP's data chart is shown in the Overcurrent Protector History section.



To retrieve the exact data at a particular time, hover your mouse over the data line in the chart. Both the time and data are displayed as illustrated below.

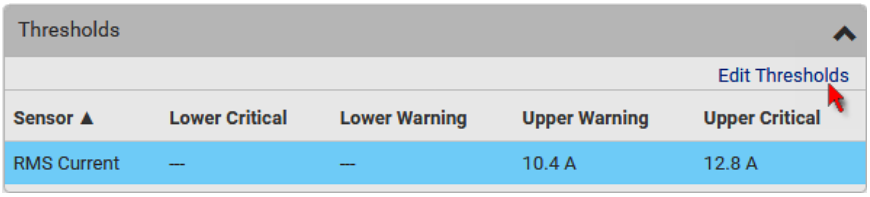


To configure this OCP's threshold settings:

By default, upper thresholds of an OCP's RMS current have been configured. You can modify them as needed.

Note: The threshold values set for an individual OCP will override the bulk threshold values stored on that particular OCP. Click the Thresholds title bar at the bottom of the page to display the threshold data.

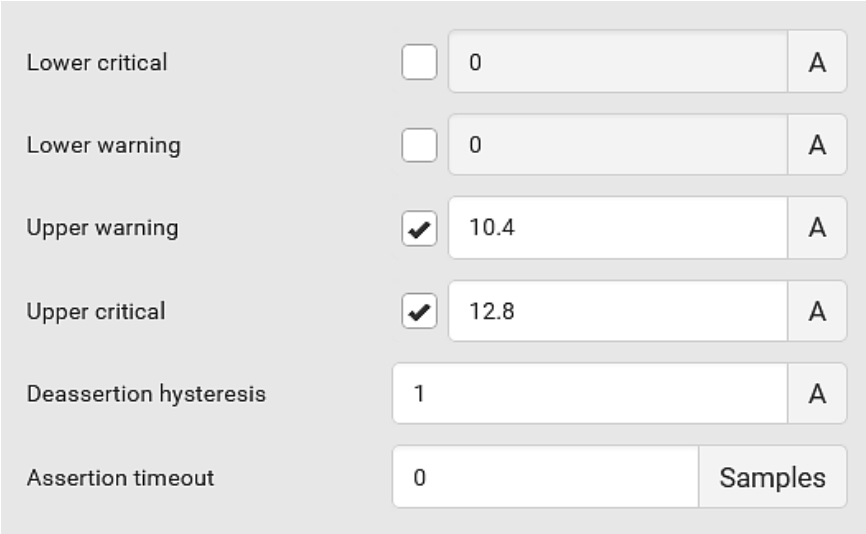
Click the RMS current sensor (required), and then click Edit Thresholds.



Make changes as needed.

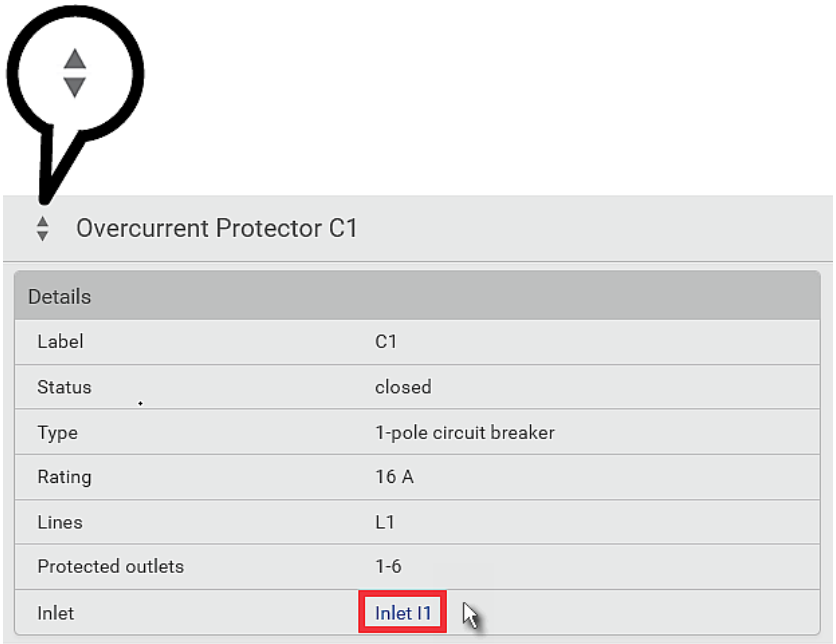
- To enable any threshold, select the corresponding checkbox.
- Type a new value in the accompanying text box.

Click Save.



Other operations:

You can go to another OCP's data/setup page by clicking the OCP selector  on the top-left corner.
You can go to the associated Inlet's data page by clicking the Inlet link in the Details section.



Peripherals

If there are Server Technology environmental sensor packages connected to the PRO3X, they are listed on the Peripherals page.

An environmental sensor package comprises one or some of the following sensors/actuators:

- Numeric sensors: Detectors that show both readings and states, such as temperature sensors.
- State sensors: Detectors that show states only, such as contact closure sensors.
- Actuators: An actuator controls a system or mechanism so it shows states only.

PRO3X communicates with *managed* sensors/actuators only and retrieves their data. It does not communicate with unmanaged ones.

When the number of "managed" sensors/actuators has not reached the maximum, PRO3X automatically brings newly-detected sensors/actuators under management by default.

One PRO3X can manage a maximum of 32 sensors/actuators.

Note: To disable the automatic management function, refer to the final table in this section. You need to manually manage a sensor/actuator only when it is not under management.

When any sensor/actuator is no longer needed, you can unmanage/release it.

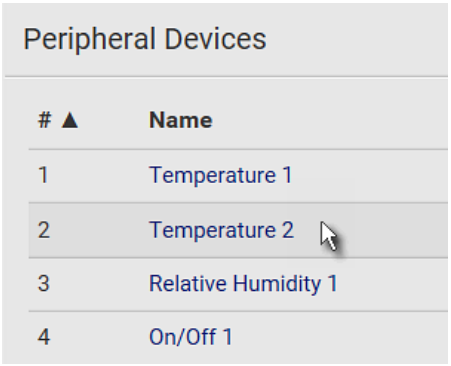
Open the Peripheral Devices page by clicking Peripherals in the Menu.

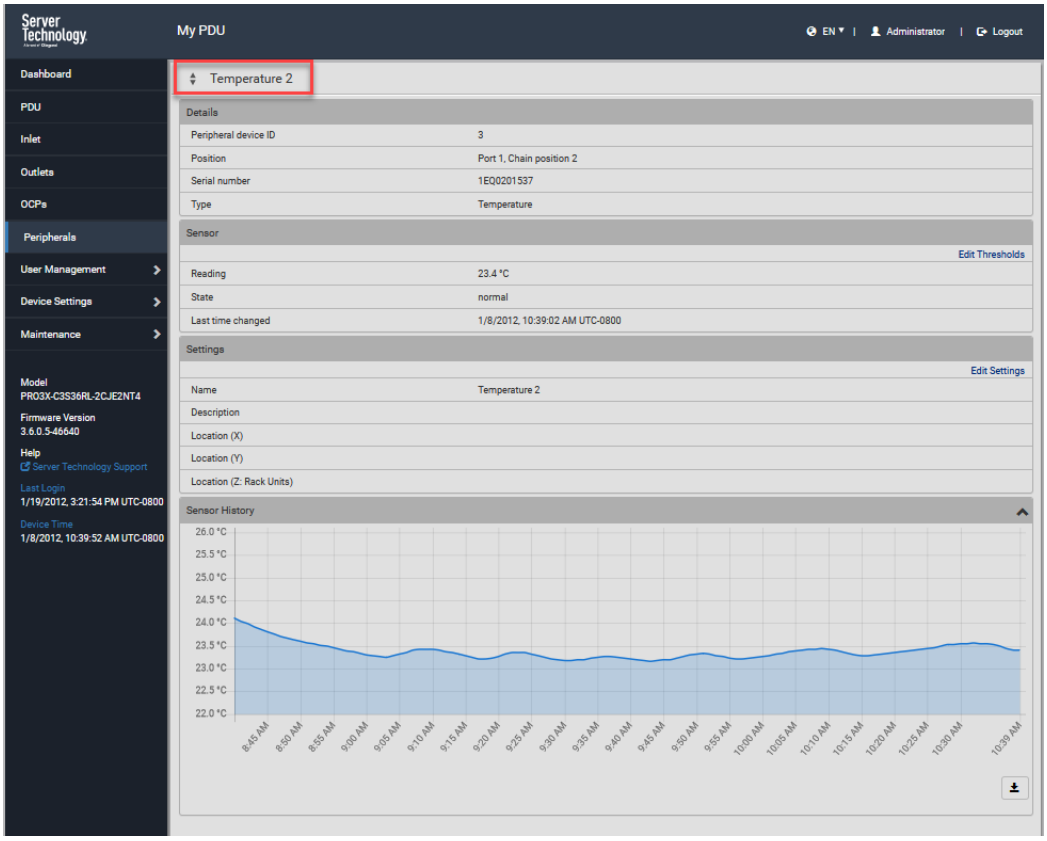
If wanted, you can resort the list by clicking the desired column header.

Peripheral Devices

# ▲	Name	Reading	State	Type	Serial Number	Position	Actuator
1	Temperature 1	24.7 °C	normal	Temperature	12A8600101	Port 1, Chain position 1	
2	Relative Humidity 1	26 %	normal	Humidity	12A8600101	Port 1, Chain position 1	
3	Temperature 2	24.4 °C	normal	Temperature	1EQ0201537	Port 1, Chain position 2, Channel 1	
4	Relative Humidity 2	24 %	normal	Humidity	1EQ0201537	Port 1, Chain position 2, Channel 1	
5	Temperature 3	24.4 °C	normal	Temperature	1JX0302612	Port 1, Chain position 3, Channel 1	
6	Absolute Humidity 1	5.9 g/m³	normal	Absolute Humidity	12A8600101	Port 1, Chain position 1	
7	Absolute Humidity 2	5.4 g/m³	normal	Absolute Humidity	1EQ0201537	Port 1, Chain position 2, Channel 1	

You can then go to an individual sensor's or actuator's data/setup page by clicking its name.





Sensor/actuator overview on this page:

If any sensor enters an alarmed state, it is highlighted in yellow or red. An actuator is never highlighted.

Column	Description
Name	By default the PRO3X assigns a name comprising the following two elements to a newly-managed sensor/actuator. ▪ Sensor/actuator type, such as "Temperature" or "Dry Contact." ▪ Sequential number of the same sensor/actuator type, like 1, 2, 3 and so on. You can customize the name.
Reading	Only managed 'numeric' sensors show this data, such as temperature and humidity sensors.
State	The data is available for all sensors and actuators.
Type	Sensor or actuator type.
Serial Number	This is the serial number printed on the sensor package's label. It helps to identify your Server Technology sensors/actuators.
Position	The data indicates where this sensor or actuator is located in the sensor chain.
Actuator	Indicates whether this sensor package is an actuator or not. If yes, the symbol ✔ is shown.

To release or manage sensors/actuators:

When the total of managed sensors/actuators reaches the maximum value, you cannot manage additional ones. The only way to manage any sensor/actuator is to release or replace the managed ones. To replace a managed sensor/actuator. To release any one, follow this procedure.

Click  to make checkboxes appear in front of sensors/actuators.

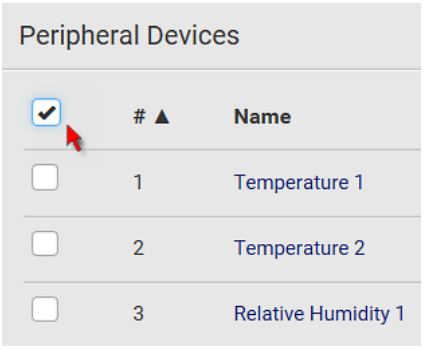
Tip: To perform the desired action on only one sensor/actuator, simply click that sensor/actuator without making the checkboxes appear.

Select multiple sensors/actuators.

To release sensors/actuators, you must select "managed" ones only.

To manage sensors/actuators, you must select "unmanaged" ones only.

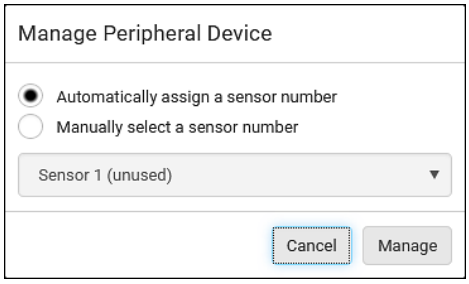
To select ALL sensors/actuators, select the topmost checkbox in the header row.



To release selected ones, click ⋮ > Release.

To manage them, click ⋮ > Manage.

The management action triggers a "Manage Peripheral Device" dialog. Simply click Manage if you are managing *multiple* sensors/actuators.



If you are managing only *one* sensor/actuator, you can choose to assign an ID number by selecting "Manually select a sensor number."

Now released sensors/actuators become "unmanaged." Managed ones show one of the managed states.

To configure sensor/actuator-related settings:

Click ⋮ > Peripheral Device Setup.

Now you can configure the fields.

Click ▼ to select an option.

Adjust the numeric values.

Select or deselect the checkbox.

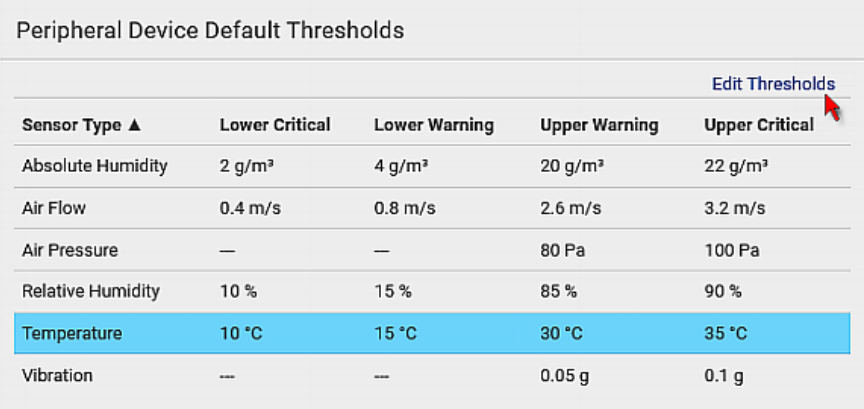
Click Save.

Field	Function	Note
Peripheral device Z coordinate format	Determines how to describe the vertical locations (Z coordinates) of Server Technology environmental sensor packages. ▪ Options: Rack units and Free-form	To specify the location of any sensor/actuators in the data center
Peripheral device auto management	Enables or disables the automatic management feature for Server Technology environmental sensor packages. ▪ The default is to enable it.	See How the Automatic Management Function Works
Altitude	Specifies the altitude of PRO3X above sea level when a Server Technology's differential air pressure sensor is attached. ▪ Range: -425 to 3000 meters (-1394 to 9842 feet) ▪ Note that it can be a negative value down to -425 meters (-1394 feet) because some locations are below the sea level.	▪ The device's altitude is associated with the altitude correction factor. See *Altitude Correction Factors* ▪ The default altitude measurement unit is meter. See *Setting Default Measurement Units* ▪ You can have the measurement unit vary between meter and foot according to user credentials. See *Setting Your Preferred Measurement Units*
Active powered dry contact limit	Determines the maximum number of "active" powered dry contact actuators that is permitted concurrently. ▪ Range: 0 to 24 ▪ Default: *1*	▪ An "active" actuator is the one that is turned ON, or, if with a door handle connected, is OPENED. ▪ This setting only applies to "powered dry contact" (PD) actuators rather than normal "dry contact" actuators. ▪ You need either 'Change Peripheral Device Configuration' privilege or 'Administrator Privileges' to change its upper limit. ▪

To configure default threshold settings:

Note that any changes made to default threshold settings not only re-determine the initial threshold values that will apply to newly-added sensors but also the threshold values of the already-managed sensors where default thresholds are being applied. Click ⋮ > Default Threshold Setup.

Click the desired sensor type (required), and then click Edit Thresholds.

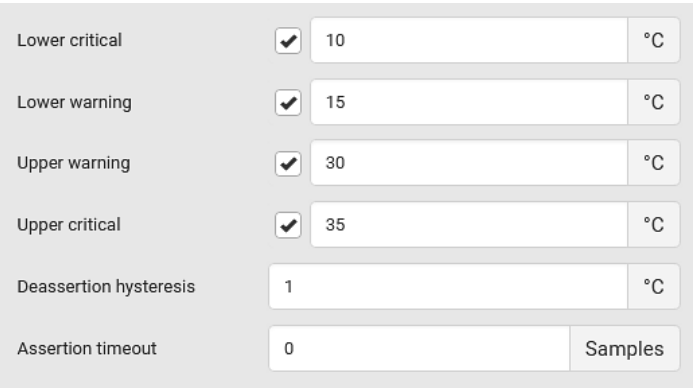


Sensor Type ▲	Lower Critical	Lower Warning	Upper Warning	Upper Critical
Absolute Humidity	2 g/m³	4 g/m³	20 g/m³	22 g/m³
Air Flow	0.4 m/s	0.8 m/s	2.6 m/s	3.2 m/s
Air Pressure	—	—	80 Pa	100 Pa
Relative Humidity	10 %	15 %	85 %	90 %
Temperature	10 °C	15 °C	30 °C	35 °C
Vibration	---	---	0.05 g	0.1 g

Make changes as needed.

- To enable any threshold, select the corresponding checkbox.
- Type a new value in the accompanying text box.

Click Save.



To turn on or off any actuator(s):

Select one or multiple actuators which are *in the same status* - on or off.

To select multiple actuators, click  to make checkboxes appear and then select desired actuators.

Click the desired button: TURN ON is **green**. TURN OFF is **red**.

Note: Per default you can turn on as many dry contact actuators as you want, but only one "powered dry contact" actuator can be turned on at the same time. To change this limitation of "powered dry contact" actuators, modify the active powered dry contact setting.

Confirm the operation when prompted.

Yellow- or Red-Highlighted Sensors

The PRO3X highlights those sensors that enter the abnormal state with a yellow or red color. Note that numeric sensors can change colors only after you have enabled their thresholds.

Tip: When an actuator is turned ON, it is also highlighted in red for drawing attention.

# ▲	Name	Reading	State	Type	Serial Number	Position	Actuator
1	Temperature 1	25.0 °C	above upper critical	Temperature	AEH2A51454	Port 1	
2	Absolute Humidity 1	10.8 g/m³	normal	Absolute Humidity	AEI1750551	Port 4	
3	Absolute Humidity 2	11.0 g/m³	above upper warning	Absolute Humidity	AEI2850240	Port 4	
4	Temperature 2	25.8 °C	above upper critical	Temperature	AEI2A50775	Port 1	
5	Relative Humidity 1	44 %	normal	Humidity	AEI2A50775	Port 1	

Sensor status	Color	States shown in the interface	Description
Unknown		unavailable	Sensor state or readings cannot be detected.
		unmanaged	Sensors are not being managed.
Normal		normal	▪ Numeric or state sensors are within the normal range. -- OR -- ▪ No thresholds have been enabled for numeric sensors.
Warning		above upper warning	Upper Warning threshold < "R" <= Upper Critical threshold
		below lower warning	Lower Critical threshold <= "R" < Lower Warning threshold
Critical		above upper critical	Upper Critical threshold < "R"
		below lower critical	"R" < Lower Critical threshold
Alarmed		alarmed	State sensors enter the abnormal state.
OCP alarm		Open	▪ Circuit breaker trips. -- OR -- ▪ Fuse blown.

In the table above, "R" represents any numeric sensor's reading. The symbol <= means "smaller than" or "equal to."

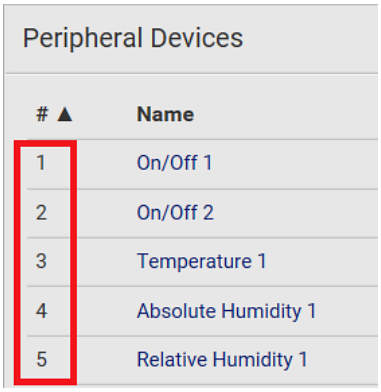
Managed vs. Unmanaged Sensors/Actuators

Managed sensors/actuators:

PRO3X communicates with managed sensors/actuators and retrieves their data.

Managed sensors/actuators are always listed on the Peripheral Devices page no matter they are physically connected or not.

They have an ID number as illustrated below.



They show one of the managed states.

For managed 'numeric' sensors, their readings are retrieved and displayed. If any numeric sensor is disconnected or its reading cannot be retrieved, it shows "unavailable" for its reading.

Unmanaged sensors/actuators:

PRO3X does NOT communicate with unmanaged sensors/actuators so their data is not retrieved.

Unmanaged sensors/actuators are listed only when they are physically connected to PRO3X.

They disappear when they are no longer connected.

They do *not* have an ID number.

They show the "unmanaged" state.

Sensor/Actuator States

An environmental sensor or actuator shows its real-time state after being managed.

Available sensor states depend on the sensor type -- numeric or state sensors. For example, a contact closure sensor is a state sensor so it switches between three states only -- *unavailable*, *alarmed* and *normal*.

Sensors will be highlighted in yellow or red when they enter abnormal states.

An actuator's state is marked in red when it is turned on.

Managed sensor states:

In the following table, "R" represents any numeric sensor's reading. The symbol <= means "smaller than" or "equal to."

State	Description
normal	▪ For numeric sensors, it means the readings are within the normal range. ▪ For state sensors, it means they enter the normal state.
below lower critical	"R" < Lower Critical threshold
below lower warning	Lower Critical threshold <= "R" < Lower Warning threshold
above upper warning	Upper Warning threshold < "R" <= Upper Critical threshold
above upper critical	Upper Critical threshold < "R"
alarmed	The state sensor enters the abnormal state.
unavailable	▪ Communication with the managed sensor is lost.

Managed actuator states:

State	Description
on	The actuator is turned on.
off	The actuator is turned off.
unavailable	▪ Communication with the managed actuator is lost.

Unmanaged sensor/actuator states:

State	Description
unmanaged	Sensors or actuators are physically connected to the PRO3X but not managed yet.

Note: Unmanaged sensors or actuators will disappear from the web interface after they are no longer physically connected to the PRO3X.

Finding the Sensor's Serial Number

A DPX environmental sensor package includes a serial number tag on the sensor cable.

The serial number for each sensor or actuator appears listed in the web interface after each sensor or actuator is detected by the PRO3X. Match the serial number from the tag to those listed in the sensor table.

Peripheral Devices

# ▲	Name	Reading	State	Type	Serial Number	Position	Actuator
1	On/Off 1		normal	Contact Closure	QLLemu0001	Port 1, Chain Position 1, Channel 1	
2	On/Off 2		normal	Contact Closure	QLLemu0001	Port 1, Chain Position 1, Channel 3	
3	Temperature 1	24.0 °C	normal	Temperature	QMTemu0005	Port 1, Chain Position 5	
4	Absolute Humidity 1	9.2 g/m³	normal	Absolute Humidity	QMSemu0004	Port 1, Chain Position 4	
5	Relative Humidity 1	42 %	normal	Humidity	QMSemu0004	Port 1, Chain Position 4	

Identifying the Sensor Position and Channel

The PRO3X can indicate where each sensor or actuator is connected on the Peripheral Devices page.

Peripheral Devices

# ▲	Name	Reading	State	Type	Serial Number	Position	Actuator
1	On/Off 1		normal	Contact Closure	QLLemu0001	Port 1, Chain Position 1, Channel 1	
2	On/Off 2		normal	Contact Closure	QLLemu0001	Port 1, Chain Position 1, Channel 3	
3	Temperature 1	24.0 °C	normal	Temperature	QMTemu0005	Port 1, Chain Position 5	
4	Absolute Humidity 1	9.2 g/m³	normal	Absolute Humidity	QMSemu0004	Port 1, Chain Position 4	
5	Relative Humidity 1	42 %	normal	Humidity	QMSemu0004	Port 1, Chain Position 4	

The following table displays sensor/actuator position examples:

Example	Physical position
Port 1	Connected to the sensor port #1.
Port 1, Channel 2	▪ Connected to the sensor port #1. ▪ The sensor/actuator is the 2nd channel of the sensor package.
Port 1, Chain Position 4	▪ Connected to the sensor port #1. ▪ The sensor/actuator is located in the 4th sensor package of the sensor chain.
Port 1, Chain Position 3, Channel 2	▪ Connected to the sensor port #1. ▪ The sensor/actuator is located in the 3rd sensor package of the sensor chain. ▪ It is the 2nd channel of the sensor package.
Port 1, Chain Position 1, Hub Port 2, Chain Position 3	▪ Connected to the sensor port #1. The hub's position in the sensor chain -- "Chain Position 1" The hub port where this particular sensor package is connected -- "Hub Port 2" ▪ The sensor/actuator is located in the 3rd sensor package of the sensor chain connected to the hub's port 2.

If a

How the Automatic Management Function Works

After enabling the automatic management function:

When the total number of managed sensors and actuators has not reached the upper limit yet, PRO3X automatically brings newly-connected environmental sensors and actuators under management after detecting them.

PRO3X can manage up to 32 sensors/actuators.

After disabling the automatic management function:

PRO3X no longer automatically manages any newly-added environmental sensors and actuators, and therefore neither ID numbers are assigned nor sensor readings or states are available for newly-added ones.

You must manually manage new sensors/actuators.

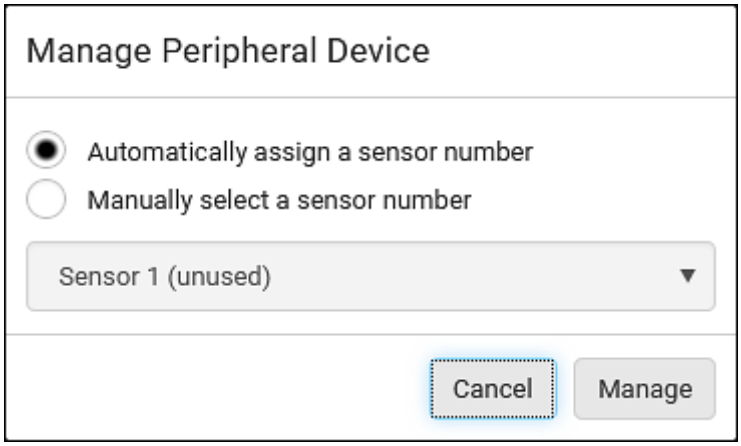
Managing One Sensor or Actuator

If you are managing only one sensor or actuator, you can assign the desired ID number to it. Note that you cannot assign ID numbers when managing multiple sensors/actuators at a time.

Tip: When the total of managed sensors/actuators reaches the maximum value, you cannot manage additional ones. The only way to manage any sensor/actuator is to release or replace the managed ones. To replace a managed one, assign an ID number to it by following the procedure below. To manage only one sensor/actuator:

From the list of "unmanaged" sensors/actuators, click the one you want to manage.

The Manage Peripheral Device dialog appears.



To let PRO3X randomly assign an ID number to it, select "Automatically assign a sensor number."

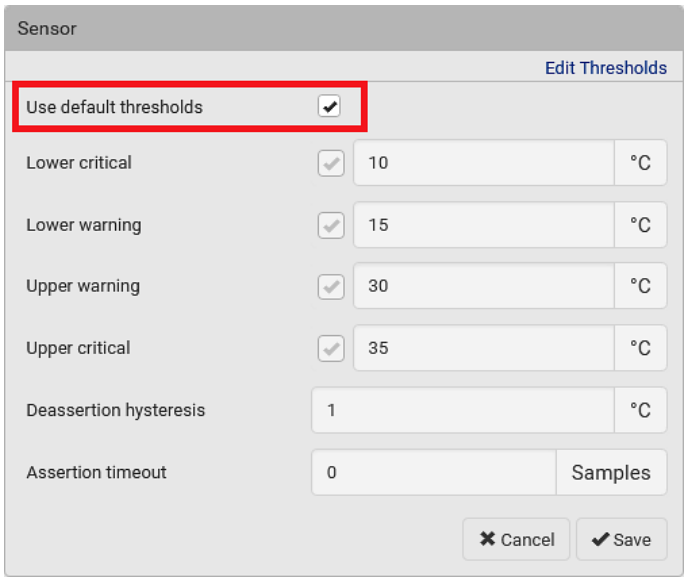
This method does not release any managed sensor or actuator.

To assign a desired ID number, select "Manually select a sensor number." Then click ▼ to select an ID number.

This method may release a managed sensor/actuator if the number you selected has been assigned to a specific sensor/actuator.

Click Manage.

Tip: The information in parentheses following each ID number indicates whether the number has been assigned to a sensor or actuator. If it has been assigned to a sensor or actuator, it shows the sensor package's serial number. Otherwise, it shows the word "unused."



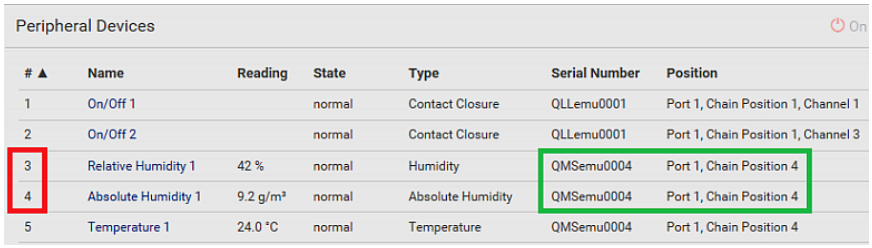
Special note for a Server Technology humidity sensor:

A Server Technology humidity sensor is able to provide two measurements - relative and absolute humidity values.

- A relative humidity value is measured in percentage (%).
- An absolute humidity value is measured in grams per cubic meter (g/m³).

However, only relative humidity sensors are "automatically" managed if the automatic management function is enabled. You must "manually" manage absolute humidity sensors as needed.

Note that relative and absolute values of the same humidity sensor do NOT share the same ID number though they share the same serial number and position.



Individual Sensor/Actuator Pages

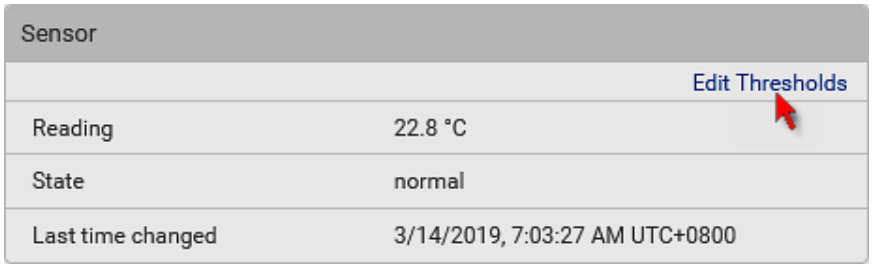
A sensor's or actuator's data/setup page is opened after clicking any sensor or actuator name on the Peripheral Devices page.

Note that only a numeric sensor has threshold settings, while a state sensor or actuator has no thresholds.

Threshold settings, if enabled, help you identify whether any numeric sensor enters the warning or critical level. In addition, you can have PRO3X automatically generate alert notifications for any warning or critical status.

To configure a numeric sensor's threshold settings:

Click Edit Thresholds.



Tip: The date and time shown on the PRO3X web interface are automatically converted to your computer's time zone. To avoid time confusion, it is suggested to apply the same time zone settings as those of PRO3X to your computer or mobile device.

Select or deselect 'Use default thresholds' according to your needs.

To have this sensor follow the default threshold settings configured for its own sensor type, select the 'Use default thresholds' checkbox.

The default threshold settings are configured on the Peripherals page.

To customize the threshold settings for this particular sensor, deselect the 'Use default thresholds' checkbox, and then modify the threshold fields below it.

Click Save.

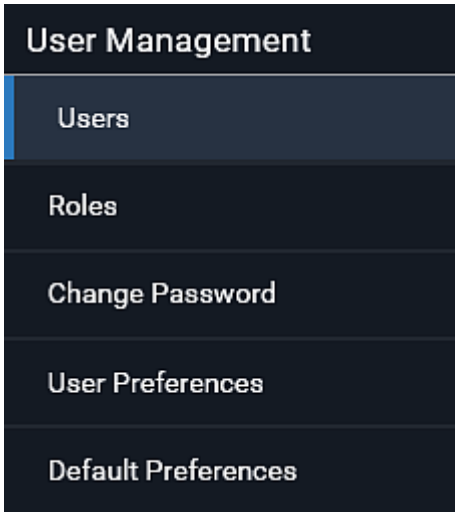
User Management

User Management menu deals with user accounts, permissions, and preferred measurement units on a per-user basis.

PRO3X is shipped with one built-in administrator account: **admin**, which is ideal for initial login and system administration. You cannot delete 'admin' or change its permissions, but you can and **should** change its password.

A "role" determines the tasks/actions a user is permitted to perform on the PRO3X so you must assign one or multiple roles to each user.

Click 'User Management' in the ***Menu***, and the following submenu displays.



Submenu command	Refer to...
Users	*Creating Users*
Roles	*Creating Roles*
Change Password	*Changing Your Password*
User Preferences	*Setting Your Preferred Measurement Units*
Default Preferences	*Setting Default Measurement Units*

Creating Users

All users must have a user account, containing the login name and password. Multiple users can log in simultaneously using the same login name.

To add users, choose User Management > Users >  .

Note that you must enter information in the fields showing the message 'required.'

User information:

Field/setting	Description
User name	The name the user enters to log in to the PRO3X. 4 to 32 characters, Case sensitive, Spaces are not permitted.
Full name	The user's first and last names.
Password, Confirm password	4 to 64 characters, Case sensitive, Spaces are permitted.
Telephone number	The user's telephone number
Email address	The user's email address, Up to 128 characters, Case sensitive
Enable	When selected, the user can log in to the PRO3X.
Force password change on next login	When selected, a password change request automatically appears the next time the user logs in.

SSH:

You need to enter the SSH public key only if the public key authentication for SSH is enabled. Open the SSH public key with a text editor. Copy and paste all content in the text editor into the SSH Public Key field.

SNMPv3:

The SNMPv3 access permission is disabled by default.

Field/setting	Description
Enable SNMPv3	Select this checkbox when intending to permit the SNMPv3 access by this user. *Note: The SNMPv3 protocol must be enabled for SNMPv3 access.*
Security level	Click the field to select a preferred security level from the list: ▪ None: No authentication and no privacy. This is the default. ▪ Authentication: Authentication and no privacy. ▪ Authentication & Privacy: Authentication and privacy.

Authentication Password: This section is configurable only when 'Authentication' or 'Authentication & Privacy' is selected.

Field/setting	Description
Same as user password	Select this checkbox if the authentication password is identical to the user's password. To specify a different authentication password, disable the checkbox.
Password, Confirm password	Type the authentication password if the 'Same as User Password' checkbox is deselected. The password must consist of 8 to 32 ASCII printable characters.

Privacy Password: This section is configurable only when 'Authentication & Privacy' is selected.

Field/setting	Description
Same as authentication password	Select this checkbox if the privacy password is identical to the authentication password. To specify a different privacy password, disable the checkbox.
Password, Confirm password	Type the privacy password if the 'Same as Authentication Password' checkbox is deselected. The password must consist of 8 to 32 ASCII printable characters.

Protocol:

This section is configurable only when 'Authentication' or 'Authentication & Privacy' is selected.

Field/setting	Description
Authentication	Click this field to select the desired authentication protocol. Two protocols are available: MD5 SHA-1 (default)
Privacy	Click this field to select the desired privacy protocol. Two protocols are available: DES (default) AES-128

Preferences:

This section determines the measurement units displayed in the web interface and command line interface for this user.

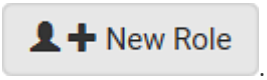
Field	Description
Temperature unit	Preferred units for temperatures -- °C (Celsius) or °F (Fahrenheit).
Length unit	Preferred units for length or height -- Meter or Feet.
Pressure unit	Preferred units for pressure -- Pascal or Psi. ▪ Pascal = one newton per square meter ▪ Psi = pounds per square inch

Note: Users can change the measurement units at any time by setting their own preferences.

Roles:

Select one or multiple roles to determine the user's permissions.

To select all roles, select the topmost checkbox in the header row. However, a user can have a maximum of 32 roles only.

If the built-in roles do not satisfy your needs, add new roles by clicking 

. This newly-created role will be then automatically assigned to the user account currently being created.

Built-in role	Description
Admin	Provide full permissions.
Operator	Provide frequently-used permissions, including: Acknowledge Alarms Change Own Password Change Pdu, Inlet, Outlet & Overcurrent Protector Configuration View Event Settings View Local Event Log

Note: With multiple roles selected, a user has the union of all roles' permissions.

Editing or Deleting Users

To edit or delete users, choose User Management > Users to open the Users page, which lists all users.

In the Enabled column:

✔: The user is enabled.

✖: The user is disabled.

If wanted, you can resort the list by clicking the desired column header.

To edit or delete a user account:

On the Users page, click the desired user. The Edit User page for that user opens.

Make changes as needed.

To change the password, type a new password in the Password and Confirm Password fields. If the password field is left blank, the password remains unchanged.

To delete this user, click 🗑, and confirm the operation.

Click Save.

To delete multiple user accounts:

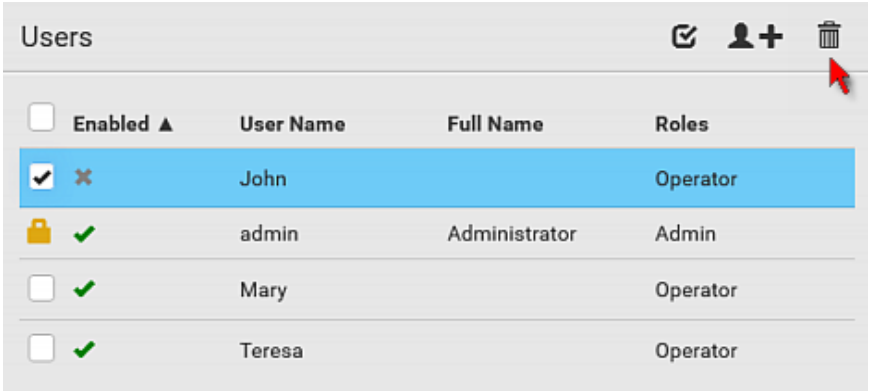
On the Users page, click to make checkboxes appear in front of user names.

Tip: To delete only one user, you can simply click that user without making the checkboxes appear. Refer to the above procedure.

Select one or multiple users.

To select all roles, except for the admin user, select the topmost checkbox in the header row.

Click .



Click Delete on the confirmation message.

Creating Roles

A role is a combination of permissions. Each user must have at least one role.

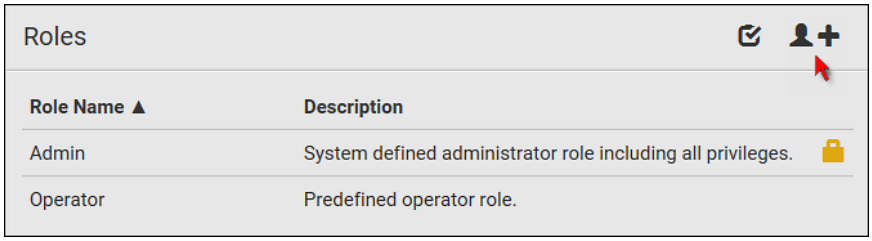
The PRO3X provides two built-in roles.

Built-in role	Description
Admin	Provide full permissions.
Operator	Provide frequently-used permissions, including: Acknowledge Alarms Change Own Password Change Pdu, Inlet, Outlet & Overcurrent Protector Configuration View Event Settings View Local Event Log

If the two do not satisfy your needs, add new roles. PRO3X supports up to 64 roles.

To create a role:

Choose User Management > Roles >  .



Assign a role name.

1 to 32 characters long

Case sensitive

Spaces are permitted

Type a description for the role in the Description field.

Select the desired privilege(s).

The 'Administrator Privileges' includes all privileges.

The 'Unrestricted View Privileges' includes all 'View' privileges.

If any privilege requires the argument setting, the symbol  displays in the rightmost edge of that privilege's row. To select such a privilege:

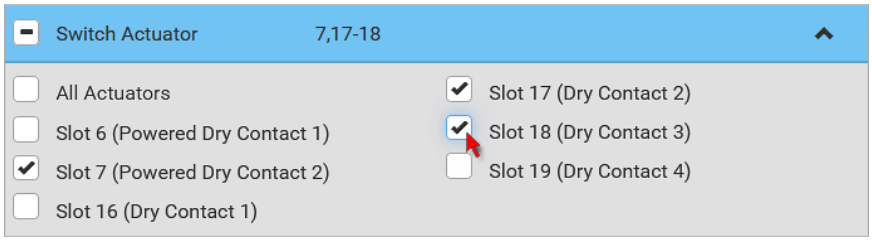
Click on that privilege's row to display a list of available arguments for that privilege.

Select the desired arguments.

To select all arguments, simply select the checkbox labeled 'All XXX'.

Tip: The other way to select all arguments is to select that privilege's checkbox while the arguments list is not expanded yet.

For example, you can specify the actuators that users can switch on/off as shown below. To select all actuators, select the 'All Actuators' checkbox instead.

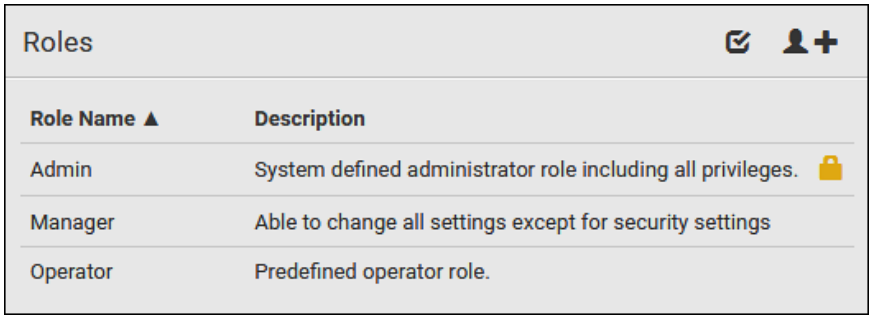


Click Save.

Editing or Deleting Roles

Choose User Management > Roles to open the Roles page, which lists all roles.

If wanted, you can resort the list by clicking the desired column header.



The Admin role is not user-configurable so the lock icon displays, indicating that you are not allowed to configure it.

To edit a role:

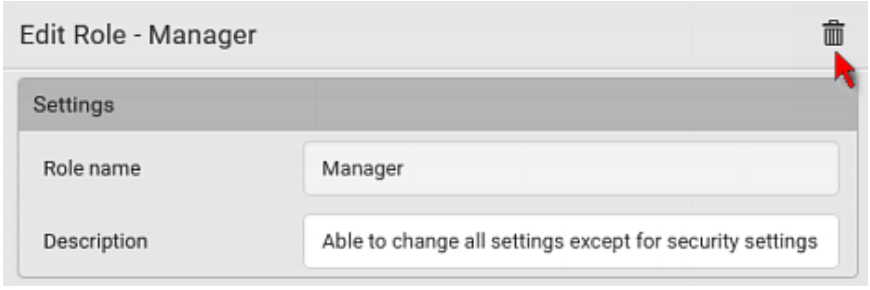
On the Roles page, click the desired role. The Edit Role page opens.

Make changes as needed.

The role name cannot be changed.

To delete this role, click , and confirm the operation.

Click Save.



To delete any roles:

On the Roles page, click  to make checkboxes appear in front of roles.

Tip: To delete only one role, you can simply click that role without making the checkboxes appear. Refer to the above procedure.

Select one or multiple roles.

To select all roles, except for the Admin role, select the topmost checkbox in the header row.

Click  on the top-right corner.

Click Delete on the confirmation message.

Setting Your Preferred Measurement Units

You can change the measurement units shown in the PRO3X user interface according to your own preferences regardless of the permissions you have.

Tip: Preferences can also be changed by administrators for specific users on the Edit User page.

Measurement unit changes only apply to the web interface and command line interface.

Setting your own preferences does not change the default measurement units. To select the measurement units you prefer:

Choose User Management > User Preferences.

Make changes as needed.

Field	Description
Temperature unit	Preferred units for temperatures -- °C (Celsius) or °F (Fahrenheit).
Length unit	Preferred units for length or height -- Meter or Feet.
Pressure unit	Preferred units for pressure -- Pascal or Psi. ▪ Pascal = one newton per square meter ▪ Psi = pounds per square inch

Click Save.

Setting Default Measurement Units

Default measurement units are applied to all PRO3X user interfaces across all users, including users accessing the PRO3X via external authentication servers.

The front panel display also shows the default measurement units.

Note: The preferred measurement units set by any individual user or by the administrator on a per-user basis will override the default units in the web interface and command line interface.

To set up default user preferences:

Click User Management > Default Preferences.

Make changes as needed.

Field	Description
Temperature unit	Preferred units for temperatures -- °C (Celsius) or °F (Fahrenheit).
Length unit	Preferred units for length or height -- Meter or Feet.
Pressure unit	Preferred units for pressure -- Pascal or Psi. ▪ Pascal = one newton per square meter ▪ Psi = pounds per square inch

Click Save.

User Interfaces Showing Default Units

Default measurement units will apply to the following user interfaces or data:

Web interface for "newly-created" local users when they have not configured their own preferred measurement units.

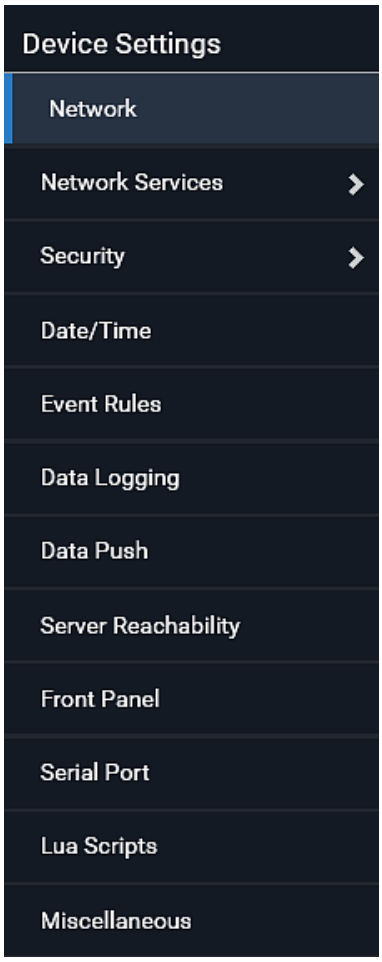
Web interface for users who are authenticated via LDAP/Radius servers.

The sensor report triggered by the "Send Sensor Report" action.

Front panel LCD display.

Device Settings

Click 'Device Settings' in the ***Menu*** and the following submenu displays.



Menu command	Submenu command	Refer to...
Network		Configuring Network Settings
Network Services	HTTP	Changing HTTP(S) Settings
	SNMP	Configuring SNMP Settings)
	SMTP Server	Configuring SMTP Settings)
	SSH	Changing SSH Settings
	Telnet	Changing Telnet Settings
	Modbus	Changing Modbus Settings
	Server Advertising	Enabling Service Advertising
Security	IP Access Control	Creating IP Access Control Rules
	Role Based Access Control	Creating Role Based Access Control Rules
	TLS Certificate	Setting Up a TLS Certificate
	Authentication	Setting Up External Authentication
	Login Settings	Configuring Login Settings
	Password Policy	Configuring Password Policy
	Service Agreement	Enabling the Restricted Service Agreement
Date/Time		Setting the Date and Time
Event Rules		Event Rules and Actions
Data Logging		Setting Data Logging
Data Push		Configuring Data Push Settings
Server Reachability		Monitoring Server Accessibility
Front Panel		Front Panel Settings
Serial Port		Configuring the Serial Port
Lua Scripts		Lua Scripts
Miscellaneous		Miscellaneous

Configuring Network Settings

Configure wired, wireless, and Internet protocol-related settings on the Network page after connecting the PRO3X to your network.

You can enable both the wired and wireless networking on PRO3X so that it has multiple IP addresses -- wired and wireless IP. For example, you can obtain one IPv4 and/or IPv6 address by enabling one Ethernet interface, and obtain one more IPv4 and/or IPv6 address by enabling/configuring the wireless interface. This also applies when PRO3X enters the port forwarding mode so that PRO3X has more than one IPv4 or IPv6 address in the port forwarding mode.

However, PRO3X in the BRIDGING mode obtains "only one" IP address for wired networking. Wireless networking is NOT supported in this mode.

Important: In the bridging mode, only the IP parameters of the BRIDGE interface function. The IP parameters of ETH1/ETH2 and WIRELESS interfaces do NOT function.

To set up the network settings:

Choose Device Settings > Network.

To use DHCP-assigned DNS servers and gateway instead of static ones, go to step 3. To manually specify DNS servers and default gateway, configure the Common Network Settings section.

Static routes and cascading mode are also in this section. You need to configure them only when there are such local requirements.

To configure IPv4/IPv6 settings for a *wired* network, click the ETH1/ETH2 or BRIDGE section.

If the device's cascading mode is set to 'Bridging', the BRIDGE section appears. Then you must click the BRIDGE section for IPv4/IPv6 settings.

To configure IPv4/IPv6 settings for a *wireless* network, click the WIRELESS section.

You must connect a USB wireless LAN adapter to the PRO3X for wireless networking.

Note: If the device's cascading mode is set to 'Bridging' or its role is set to 'link' in the port forwarding mode, the wireless settings will be disabled.

Click Save.

After enabling either or both Internet protocols:

After enabling IPv4 and/or IPv6, all but not limited to the following protocols will be compliant with the selected Internet protocol(s):

- LDAP
- NTP
- SMTP
- SSH
- Telnet
- FTP
- SSL/TLS
- SNMP
- SysLog

Note: PRO3X disables TLS 1.0 *and* 1.1 *by default. It enables only TLS* 1.2 *and* 1.3.

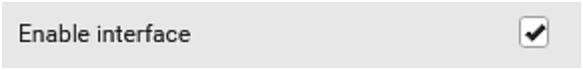
Wired Network Settings

On the Network page, click the ETH1/ETH2 section to configure IPv4/IPv6 settings.

If the device's cascading mode is set to 'Bridging', the BRIDGE section appears. Then you must click the BRIDGE section for IPv4/IPv6 settings.

Enable Interface:

Make sure the Ethernet interface is enabled, or all networking through this interface fails. This setting is available in the ETH1/ETH2 section, but not available in the BRIDGE section.



IPv4 settings:

Field/setting	Description
Enable IPv4	Enable or disable the IPv4 protocol.
IP auto configuration	Select the method to configure IPv4 settings. ▪ *DHCP*: Auto-configure IPv4 settings via DHCP servers. ▪ *Static*: Manually configure the IPv4 settings.
Preferred hostname	Enter the hostname you prefer for IPv4 connectivity

DHCP settings: Optionally specify the preferred hostname, which must meet the following requirements:

- Consists of alphanumeric characters and/or hyphens
- Cannot begin or end with a hyphen
- Cannot contain more than 63 characters
- Cannot contain punctuation marks, spaces, and other symbols

Static settings: Assign a static IPv4 address, which follows this syntax "IP address/prefix length".

Example: *192.168.84.99/24*

IPv6 settings:

Field/setting	Description
Enable IPv6	Enable or disable the IPv6 protocol.
IP auto configuration	Select the method to configure IPv6 settings. ▪ *Automatic*: Auto-configure IPv6 settings via DHCPv6. ▪ *Static*: Manually configure the IPv6 settings.
Preferred hostname	▪ Enter the hostname you prefer for IPv6 connectivity

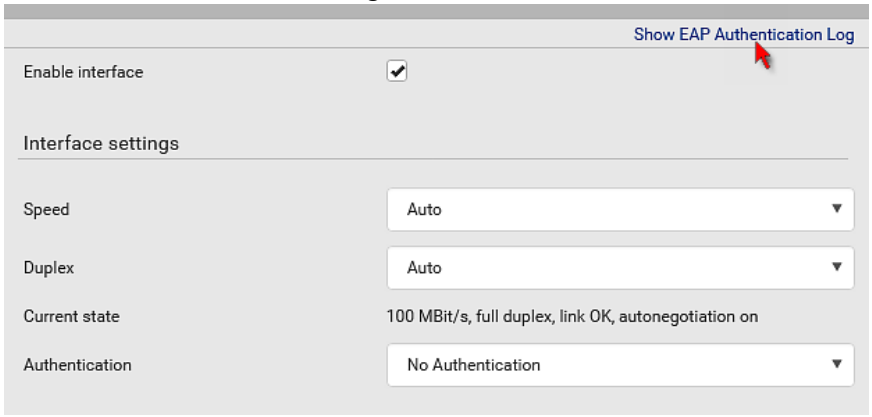
Automatic settings: Optionally specify the preferred hostname, which must meet the above requirements.

Static settings**:** Assign a static IPv6 address, which follows this syntax "IP address/prefix length".

Example: *fd07:2fa:6cff:1111::0/128*

(Optional) To view the diagnostic log for EAP authentication:

Click Show EAP Authentication Log.



Common Network Settings

Common Network Settings are OPTIONAL, not required. Therefore, leave them unchanged if there are no specific local networking requirements.

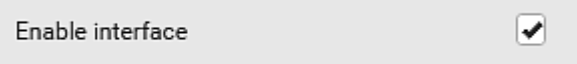
Field	Description
Cascading mode	Leave it to the default "None" unless you are establishing a cascading chain. For more information, refer to: ▪ Cascading Multiple PRO3X Devices for Sharing Ethernet Connectivity ▪ Setting the Cascading Mode
DNS resolver preference	Determine which IP address is used when the DNS resolver returns both IPv4 and IPv6 addresses. ▪ IPv4 address: Use the IPv4 addresses. ▪ IPv6 address: Use the IPv6 addresses.
DNS suffixes (optional)	Specify a DNS suffix name if needed.
First/Second/Third DNS server	Manually specify static DNS server(s). ▪ If any static DNS server is specified in these fields, it will override the DHCP-assigned DNS server. ▪ If DHCP (or Automatic) is selected for IPv4/IPv6 settings, and there are NO static DNS servers specified, the PRO3X will use DHCP-assigned DNS servers.
IPv4/IPv6 routes	You need to configure these settings only when your local network contains two subnets, and you want PRO3X to communicate with the other subnet. If so, make sure IP forwarding has been enabled in your network, and then you can click 'Add Route' to add static routes.

Ethernet Interface Settings

By default both ETH1 and ETH2 interfaces on PRO3X are enabled.

Enable Interface:

Make sure the Ethernet interface is enabled, or all networking through this interface fails. This setting is available in the ETH1/ETH2 section, but not available in the BRIDGE section.



Available settings for the CA Certificate:

Field/setting	Description
Enable verification of TLS certificate chain	Select this checkbox for the PRO3X to verify the validity of the TLS certificate that will be installed. ▪ For example, the PRO3X will check the certificate's validity period against the system time.
Browse...	Click this button to import a certificate file. Then you can: ▪ Click Show to view the certificate's content. ▪ Click Remove to delete the installed certificate if it is inappropriate.
Allow expired and not yet valid certificates	▪ Select this checkbox to make the authentication succeed regardless of the certificate's validity period. ▪ After deselecting this checkbox, the authentication fails whenever any certificate in the selected certificate chain is outdated or not valid yet.
Allow connection if system clock is incorrect	When this checkbox is deselected, and if the system time is incorrect, the installed TLS certificate is considered not valid yet and will cause the wireless network connection to fail. When this checkbox is selected, it will make the wireless network connection successful when the PRO3X system time is earlier than the firmware build before synchronizing with any NTP server. ▪ The incorrect system time issue may occur when the PRO3X has once been powered off for a long time.

Wireless Network Settings

Note: If the device's cascading mode is set to 'Bridging' or its role is set to “link” in the port forwarding mode, the wireless settings will be disabled.

By default the wireless interface is disabled. You should enable it if wireless networking is wanted.

On the Network page, click the WIRELESS section to configure wireless and IPv4/IPv6 settings.

Interface Settings:

Field/setting	Description
Enable interface	Enable or disable the wireless interface. When disabled, the wireless networking fails.
Hardware state	Check this field to ensure that the PRO3X has detected a wireless USB LAN adapter. If not, verify whether the USB LAN adapter is firmly connected or whether it is supported.
SSID	Type the name of the wireless access point (AP).
Force AP BSSID	If the BSSID is available, select this checkbox.
BSSID	Type the MAC address of an access point.
Enable High Throughput (802.11n)	Enable or disable 802.11n protocol.
Authentication	Select an authentication method. ▪ *No Authentication:* No authentication data is required. ▪ *PSK*: A Pre-Shared Key is required. *EAP:* Use Protected Extensible Authentication Protocol. Enter required authentication data in the fields that appear.
Pre-Shared Key	This field appears only when PSK is selected. Type the PSK string.
Outer authentication	This field appears when 'EAP' is selected. There are two authentication methods for EAP. ▪ *PEAP:* A TLS tunnel is established, and an inner authentication method can be specified for this tunnel. *TLS:* Authentication between the client and authentication server is performed using TLS certificates.
Inner authentication	This field appears when both 'EAP' and 'PEAP' are selected. ▪ *MS-CHAPv2:* Authentication based on the given password using MS-CHAPv2 protocol. *TLS:* Authentication between the client and authentication server is performed using TLS certificates.
Identity	This field appears when 'EAP' is selected. Type your user name.

Password	This field appears only when 'EAP', 'PEAP' and 'MS-CHAPv2' are all selected. Type your password.
Client certificate, Client private key, Client private key password	This field appears when 'EAP', 'PEAP' and 'TLS' are all selected. PEM encoded X.509 certificate and PEM encoded private key are required for certification-based authentication methods. Private key password is optional. ▪ PRO3X supports private keys of PKCS#1 and PKCS#8 formats. ▪ Client Private Key Password should be entered only when your private key is encrypted with a password. ▪ To view the uploaded certificate, click Show Client Certificate. To remove the uploaded certificate and private key, click 'Clear Key/Certificate selection'.
Client certificate, Client private key, Client private key password	This field appears when 'EAP', 'PEAP' and 'TLS' are all selected. PEM encoded X.509 certificate and PEM encoded private key are required for certification-based authentication methods. Private key password is optional. ▪ PRO3X supports private keys of PKCS#1 and PKCS#8 formats. ▪ Client Private Key Password should be entered only when your private key is encrypted with a password. ▪ To view the uploaded certificate, click Show Client Certificate. ▪ To remove the uploaded certificate and private key, click 'Clear Key/Certificate selection'.
RADIUS authentication server name	This field appears when 'EAP' is selected. Type the name of the RADIUS server if it is present in the TLS certificate. The name must match the fully qualified domain name (FQDN) of the host shown in the certificate.

Available Settings for the CA Certificate:

Field/setting	Description
Enable verification of TLS certificate chain	Select this checkbox for the PRO3X to verify the validity of the TLS certificate that will be installed. ▪ For example, the PRO3X will check the certificate's validity period against the system time.
Browse…	Click this button to import a certificate file. Then you can: ▪ Click Show to view the certificate's content. ▪ Click Remove to delete the installed certificate if it is inappropriate.
Allow expired and not yet valid certificates	▪ Select this checkbox to make the authentication succeed regardless of the certificate's validity period. ▪ After deselecting this checkbox, the authentication fails whenever any certificate in the selected certificate chain is outdated or not valid yet.
Allow connection if system clock is incorrect	When this checkbox is deselected, and if the system time is incorrect, the installed TLS certificate is considered not valid yet and will cause the wireless network connection to fail. When this checkbox is selected, it will make the wireless network connection successful when the PRO3X system time is earlier than the firmware build before synchronizing with any NTP server. ▪ The incorrect system time issue may occur when the PRO3X has once been powered off for a long time.

IPv4 settings:

Field/setting	Description
Enable IPv4	Enable or disable the IPv4 protocol.
IP auto configuration	Select the method to configure IPv4 settings. ▪ *DHCP*: Auto-configure IPv4 settings via DHCP servers. ▪ *Static*: Manually configure the IPv4 settings.
Preferred hostname	Enter the hostname you prefer for IPv4 connectivity

DHCP settings: Optionally specify the preferred hostname, which must meet the following requirements:

Consists of alphanumeric characters and/or hyphens

Cannot begin or end with a hyphen

Cannot contain more than 63 characters

Cannot contain punctuation marks, spaces, and other symbols

Static settings: Assign a static IPv4 address, which follows this syntax "IP address/prefix length".

Example: *192.168.84.99/24*

IPv6 settings:

Field/setting	Description
Enable IPv6	Enable or disable the IPv6 protocol.
IP auto configuration	Select the method to configure IPv6 settings. ▪ *Automatic*: Auto-configure IPv6 settings via DHCPv6. ▪ *Static*: Manually configure the IPv6 settings.
Preferred hostname	▪ Enter the hostname you prefer for IPv6 connectivity

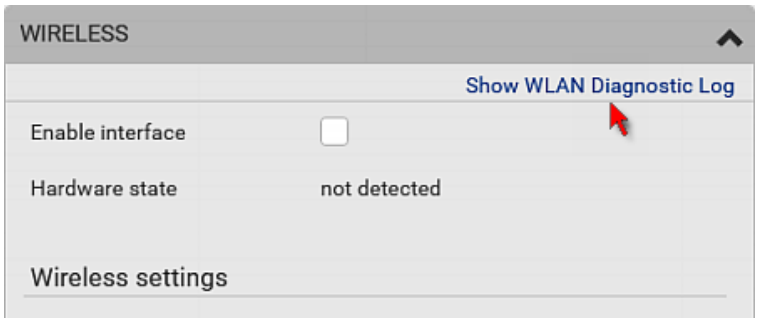
Automatic settings: Optionally specify the preferred hostname, which must meet the above requirements.

Static settings: Assign a static IPv6 address, which follows this syntax "IP address/prefix length".

Example: *fd07:2fa:6cff:1111::0/128*

(Optional) To view the wireless LAN diagnostic log:

Click Show WLAN Diagnostic Log.



Diagnostic Log for Network Connections

PRO3X provides a diagnostic log for inspecting connection errors that occurred during the EAP authentication or the wireless network connection. The information is useful for technical support.

Note that the diagnostic log shows data only after connection errors are detected.

Each entry in the log consists of:

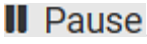
- ID number
- Date and time
- Description

To view the log:

Access the diagnostic log with either method below.

Choose Device Settings > Network > ETH1/ETH2 > Show EAP Authentication Log.

Choose Device Settings > Network > WIRELESS > Show WLAN Diagnostic Log.

The log is refreshed automatically at a regular interval of five seconds. To avoid any new events' interruption during data browsing, you can suspend the automatic update by clicking 

.

To restore automatic update, click 

. Those new events that have not been listed yet due to suspension will be displayed in the log now.

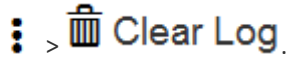
To go to other pages of the log, click the pagination bar at the bottom of the page.

When there are more than 5 pages and the page numbers listed does not show the desired one, click

to have the bar show the next or previous five page numbers, if available.

If wanted, you can resort the list by clicking the desired column header.

To clear the diagnostic log:

On the top-right corner of the log, click 

.

Click Clear Log on the confirmation message.

Static Route Examples

This section describes two static route examples: IPv4 and IPv6. Both examples assume that two network interface controllers (NIC) have been installed in one network server, leading to two available subnets, and IP forwarding has been enabled. All of the NICs and PRO3X devices in the examples use static IP addresses.

Most of local multiple networks are not directly reachable and require the use of a gateway. Therefore, we will select Gateway in the following examples. If your local multiple networks are directly reachable, you should select Interface rather than Gateway.

Note: If Interface is selected, you should select an interface name instead of entering an IP address.

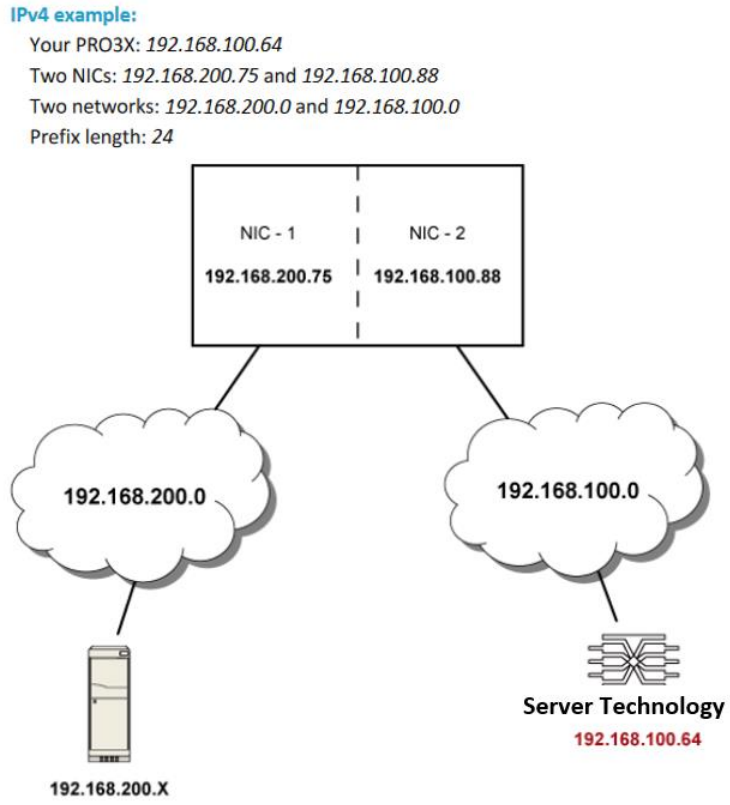
IPv4 example:

Your PRO3X: *192.168.100.64*

Two NICs: *192.168.200.75* and *192.168.100.88*

Two networks: *192.168.200.0* and *192.168.100.0*

Prefix length: *24*



In this example, NIC-2 (192.168.100.88) is the next hop router for your PRO3X to communicate with any device in the other subnet 192.168.200.0.

In the IPv4 "Static Routes" section, you should enter the data as shown below. Note that the address in the first field must be of the Classless Inter-Domain Routing (CIDR) notation.

IPv6 example:

Your PRO3X: *fd07:2fa:6cff:2405::30*

Two NICs: *fd07:2fa:6cff:1111::50* and *fd07:2fa:6cff:2405::80*

Two networks: *fd07:2fa:6cff:1111::0* and *fd07:2fa:6cff:2405::0*

Prefix length: *64*

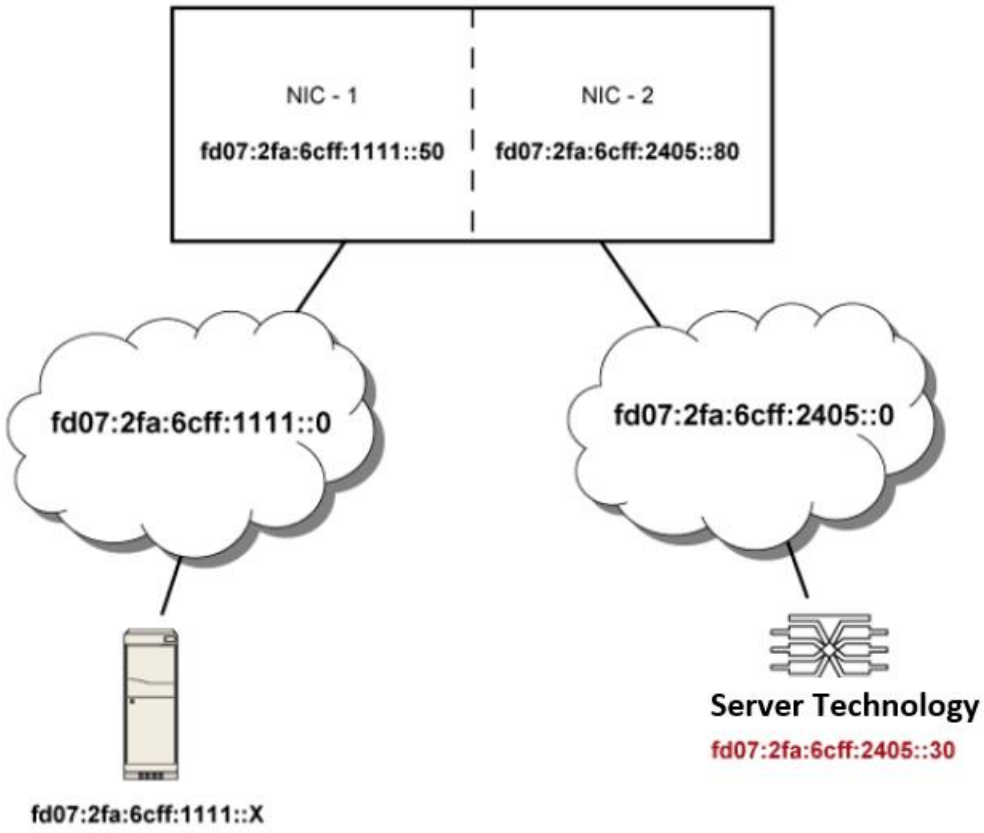
IPv6 example:

Your PRO3X: *fd07:2fa:6cff:2405::30*

Two NICs: *fd07:2fa:6cff:1111::50* and *fd07:2fa:6cff:2405::80*

Two networks: *fd07:2fa:6cff:1111::0* and *fd07:2fa:6cff:2405::0*

Prefix length: *64*

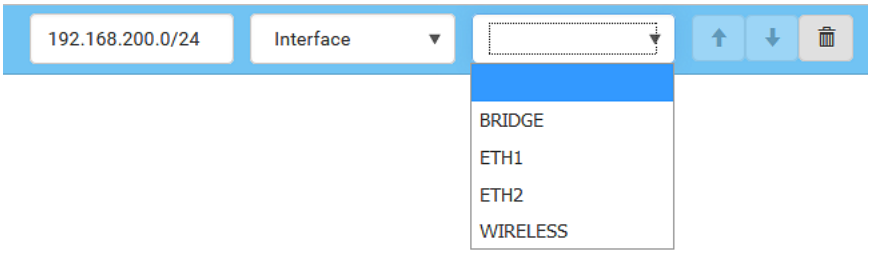


In this example, NIC-2 (fd07:2fa:6cff:2405::80) is the next hop router for your PRO3X to communicate with any device in the other subnet fd07:2fa:6cff:1111::0.

In the IPv6 "Static Routes" section, you should enter the data as shown below. Note that the address in the first field must be of the Classless Inter-Domain Routing (CIDR) notation.

Interface Names

When your local multiple networks are "directly reachable", you should select Interface for static routes. Then choose the interface where another network is connected.



Interface list:

Interface name	Description
BRIDGE	When another wired network is connected to the Ethernet port of your PRO3X, and your PRO3X has been set to the bridging mode, select this interface name instead of the Ethernet interface.
ETH1	When another wired network is connected to the ETH1 port of your PRO3X, select this interface name.
ETH2	When another wired network is connected to the ETH2 port of your PRO3X, select this interface name.
WIRELESS	When another wireless network is connected to your PRO3X, select this interface name.

Setting the Cascading Mode

A maximum of 16 PRO3X devices can be cascaded to share one Ethernet connection.

The cascading mode configured on the master device determines the Ethernet sharing method, which is either network bridging or port forwarding.

The cascading mode of all devices in the chain must be the same.

Only a user with the Change Network Settings permission can configure the cascading mode.

Note: PRO3X in the Port Forwarding mode does not support APIPA.

To configure the cascading mode:

Connect the device you will cascade to the LAN and find its IP address, or connect it to a computer.

Log in to the web interface. .

Choose Device Settings > Network.

Select the preferred mode in the Cascading Mode field.

Mode	Description
None	No cascading mode is enabled. This is the default.
Bridging	Each device in the cascading chain is accessed with a different IP address.
Port Forwarding	Each device in the cascading chain is accessed with the same IP address(es) but with a different port number assigned.

Tip: If selecting Port Forwarding, the Device Information page will show a list of port numbers for all cascaded devices. Choose Maintenance > Device Information > Port Forwarding.

For the Port Forwarding mode, one to two more fields have to be configured. Note that if either setting below is incorrectly configured, a networking issue occurs.

Field	Description
Port forwarding role (available on all cascaded devices)	*Master or link.* This is to determine which device is the master and which ones are link devices.
Downstream interface (available on the maser device only)	*USB or ETH1/ETH2.* This is to determine which port on the master device is connected to link 1. If ETH1 or ETH2 is selected as the downstream interface, make sure the selected Ethernet interface is enabled.

(Optional) Configure the network settings by clicking the BRIDGE, ETH1/ETH2, or WIRELESS section on the same page.

In the Bridging mode, each cascaded device can have different network settings. You may need to configure each device's network settings in the BRIDGE section.

In the Port Forwarding mode, all cascaded devices share the master device's network settings. You only need to configure the master device's network settings in the ETH1/ETH2 and/or WIRELESS section.

Tip: You can enable/configure multiple network interfaces in the Port Forwarding mode so that the cascading chain has multiple IP addresses.

Click Save.

Enable R/STP if a cascade loop is preferred:

You can "loop" a cascading chain to create network communication redundancy (Bridging mode only), but only when your network supports **R/STP** protocol.

Make sure that your network has R/STP enabled if using a cascade loop (Bridging mode) *or else network loops may occur*.

Overview of the Cascading Modes

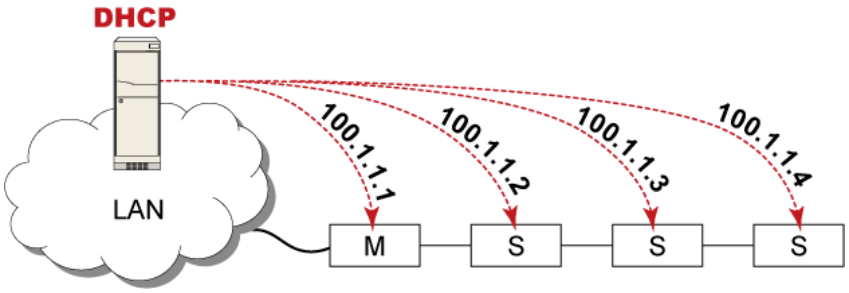
You must apply a cascading mode to the cascading chain.

There are two cascading modes: Bridging and Port Forwarding.

In the following illustration, it is assumed that users enable the DHCP networking for the cascading chain comprising four devices. In the diagrams, "M" is the master device and "S" is a link device.

Illustration:

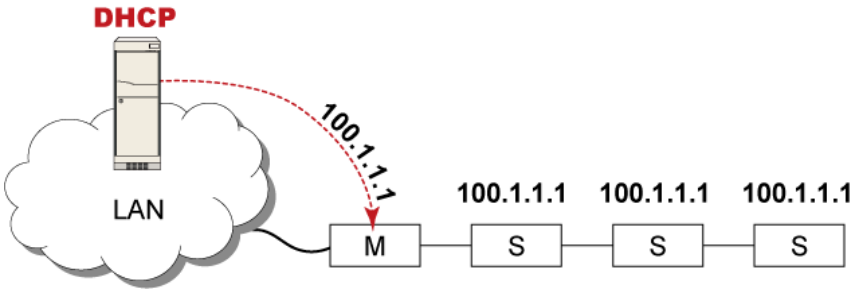
"Bridging" mode:



In this mode, the DHCP server communicates with every cascaded device respectively and assigns four *different* IP addresses. Each device has its own IP address.

The way to remotely access each cascaded device is completely the same as accessing a standalone device in the network.

"Port Forwarding" mode:



In this mode, the DHCP server communicates with the master device alone and assigns one IP address to the master device. All link devices share the same IP address as the master device.

You must specify a 5XXXX port number (where X is a number) when remotely accessing any link device with the shared IP address.

Comparison between cascading modes:

The Bridging mode supports the wired network only, while the Port Forwarding mode supports both wired and wireless networks.

Both cascading modes support a maximum of 16 devices in a chain.

Both cascading modes support both DHCP and static IP addressing.

In the Bridging mode, each cascaded device has a unique IP address.

In the Port Forwarding mode, all cascaded devices share the same IP address(es) as the master device.

In the Bridging mode, each cascaded device has only one IP address.

In the Port Forwarding mode, each cascaded device can have multiple IP addresses as long as the master device has multiple network interfaces enabled/configured properly.

For example:

When the master device has two Ethernet ports (ETH1/ETH2), you can enable ETH1, ETH2 and WIRELESS interfaces so that the Port-Forwarding chain has two wired IP addresses and one wireless IP address.

Port Number Syntax

In the Port Forwarding mode, all devices in the cascading chain share the same IP address(es). To access any cascaded device, you must assign an appropriate port number to it.

Master device: The port number is either *5NNXX* or the standard TCP/UDP port.

Link device: The port number is *5NNXX*.

5NNXX port number syntax:

NN is a two-digit number representing the network protocol as shown below:

Protocols	NN
HTTPS	00
HTTP	01
SSH	02
TELNET	03
SNMP	05
MODBUS	06

XX is a two-digit number representing the device position as shown below.

Position	XX	Position	XX
Master device	00	Link 8	08
Link 1	01	Link 9	09
Link 2	02	Link 10	10
Link 3	03	Link 11	11
Link 4	04	Link 12	12
Link 5	05	Link 13	13
Link 6	06	Link 14	14
Link 7	07	Link 15	15

For example, to access the Link 4 device via Modbus/TCP, the port number is 50604.

Tip: The full list of each cascaded device's port numbers can be retrieved from the web interface. Choose Maintenance > Device Information > Port Forwarding.

Standard TCP/UDP ports:

The master device can be also accessed through standard TCP/UDP ports as listed in the following table.

Protocols	Port Numbers
HTTPS	443
HTTP	80
SSH	22
TELNET	23
SNMP	161
MODBUS	502

In the Port Forwarding mode, the cascaded device does NOT allow you to modify the standard TCP/UDP port configuration, including HTTP, HTTPS, SSH, Telnet and Modbus/TCP.

Port Forwarding Examples

To access a cascaded device in the Port Forwarding mode, assign a port number to the IP address.

Master device: Assign proper 5NNXX port numbers or standard TCP/UDP ports.

Link device: Assign proper 5NNXX port numbers.

Assumption: *The Port Forwarding mode is applied to a cascading chain comprising three devices. The IP address is 192.168.84.77.*

Master device:

Position code for the master device is '00' so each port number is 5NN00 as listed below.

Protocols	Port numbers
HTTPS	50000
HTTP	50100
SSH	50200
TELNET	50300
SNMP	50500
MODBUS	50600

Examples using "5NN00" ports:

To access the master device via HTTPS, the IP address is:

https://192.168.84.77:50000/

To access the master device via HTTP, the IP address is:

http://192.168.84.77:50100/

To access the master device via SSH, the command is:

ssh -p 50200 192.168.84.77

Examples using standard TCP/UDP ports:

To access the master device via HTTPS, the IP address is:

https://192.168.84.77:443/

To access the master device via HTTP, the IP address is:

http://192.168.84.77:80/

To access the master device via SSH, the command is:

ssh -p 22 192.168.84.77

Link 1 device:

Position code for Link 1 is '01' so each port number is 5NN01 as shown below.

Protocols	Port numbers
HTTPS	50001
HTTP	50101
SSH	50201
TELNET	50301
SNMP	50501
MODBUS	50601

Examples:

To access Link 1 via HTTPS, the IP address is:

https://192.168.84.77:50001/

To access Link 1 via HTTP, the IP address is:

http://192.168.84.77:50101/

To access Link 1 via SSH, the command is:

ssh -p 50201 192.168.84.77

Link 2 device:

Position code for Link 2 is '02' so each port number is 5NN02 as shown below.

Protocols	Port numbers
HTTPS	50002
HTTP	50102
SSH	50202
TELNET	50302
SNMP	50502
MODBUS	50602

Examples:

To access Link 2 via HTTPS, the IP address is:

https://192.168.84.77:50002/

To access Link 2 via HTTP, the IP address is:

http://192.168.84.77:50102/

To access Link 2 via SSH, the command is:

ssh -p 50202 192.168.84.77

Adding, Removing, or Swapping Cascaded Devices

Change a device's cascading mode first before adding that device to a cascading chain, or before disconnecting that device from the chain.

If you only want to change the cascading mode of an existing chain, or swap the master and link device, always start from the link device.

Note: If the following procedures are not followed, a networking issue occurs. When a networking issue occurs, check the cascading connection and/or software settings of all devices in the chain.

To add a device to an existing chain:

Connect the device you will cascade to the LAN and find its IP address, or connect it to a computer.

Log in to this device and set its cascading mode to be the same as the existing chain's cascading mode.

(Optional) If this device will function as a link device, disconnect it from the LAN after configuring the cascading mode.

Connect this device to the chain, using either a USB or Ethernet cable.

To remove a device from the chain:

Log in to the desired cascaded device, and change its cascading mode to None.

Exception: If you are going to connect the removed device to another cascading chain, set its cascading mode to be the same as the mode of another chain.

Now disconnect it from the cascading chain.

To swap the master and link device:

In the Bridging mode, you can swap the master and link devices by simply disconnecting ALL cascading cables from them, and then reconnecting cascading cables. No changes to software settings are required.

In the Port Forwarding mode, you must follow the procedure below:

Access the link device that will replace the master device, and set its role to 'Master', and correctly set the downstream interface.

Access the master device, set its role to 'Link'.

Swap the master and link device now.

You must disconnect the LAN cable and ALL cascading cables connected to the two devices first before swapping them, and then reconnecting all cables.

To change the cascading mode applied to a chain:

Access the last link device, and change its cascading mode.

If the new cascading mode is 'Port Forwarding', you must also set its role to 'Link'.

Access the second to last, third to last and so on until the first link device to change their cascading modes one by one.

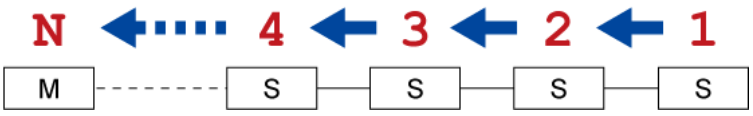
Access the master device, and change its cascading mode.

If the new cascading mode is 'Port Forwarding', you must also set its role to 'Master', and correctly select the downstream interface.

The following diagram indicates the correct sequence. 'N' is the final one.

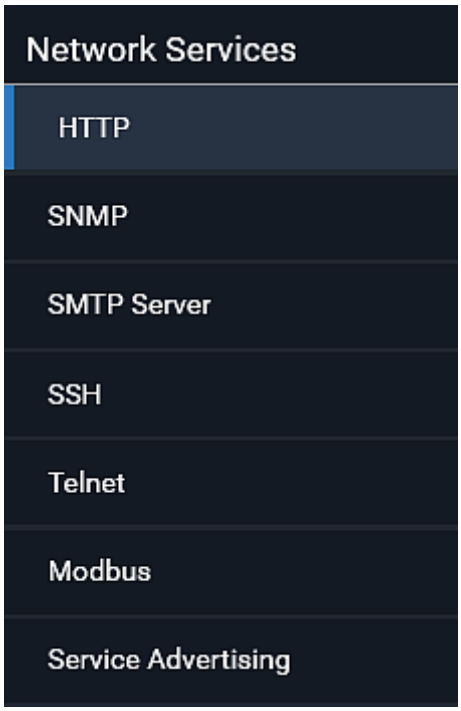
M = Master device

S = Link device



Configuring Network Services

PRO3X supports the following network communication services.



HTTPS and HTTP enable the access to the web interface. Telnet and SSH enable the access to the command line interface.

By default, SSH is enabled, Telnet is disabled, and all TCP ports for supported services are set to standard ports. You can change default settings if necessary.

Note: Telnet access is disabled by default because it communicates openly and is thus insecure.

Submenu command	Refer to
HTTP	*Changing HTTP(S) Settings*
SNMP	*Configuring SNMP Settings*
SMTP Server	*Configuring SMTP Settings*
SSH	*Changing SSH Settings*
Telnet	*Changing Telnet Settings*
Modbus	*Changing Modbus Settings*
Server Advertising	*Enabling Service Advertising*

Important: TLS is used instead of SSL 3.0 due to published security vulnerabilities in SSL 3.0. Make sure your network infrastructure, such as LDAP and mail services, uses TLS rather than SSL 3.0.

Changing HTTP(S) Settings

HTTPS uses Transport Layer Security (TLS) technology to encrypt all traffic to and from the PRO3X so it is a more secure protocol than HTTP. PRO3X disables TLS *1.0* and *1.1* by default. It enables only TLS *1.2* and *1.3.*

By default, any access to the PRO3X via HTTP is automatically redirected to HTTPS. You can disable this redirection if needed.

To change HTTP or HTTPS port settings:

Choose Device Settings > Network Services > HTTP.

Enable either or both protocols by selecting the corresponding 'Enable' checkbox.

To use a different port for HTTP or HTTPS, type a new port number.

Warning: Different network services cannot share the same TCP port.

To redirect the HTTP access to the PRO3X to HTTPS, select the "Redirect HTTP connections to HTTPS."

The redirection checkbox is configurable only when both HTTP and HTTPS have been enabled.

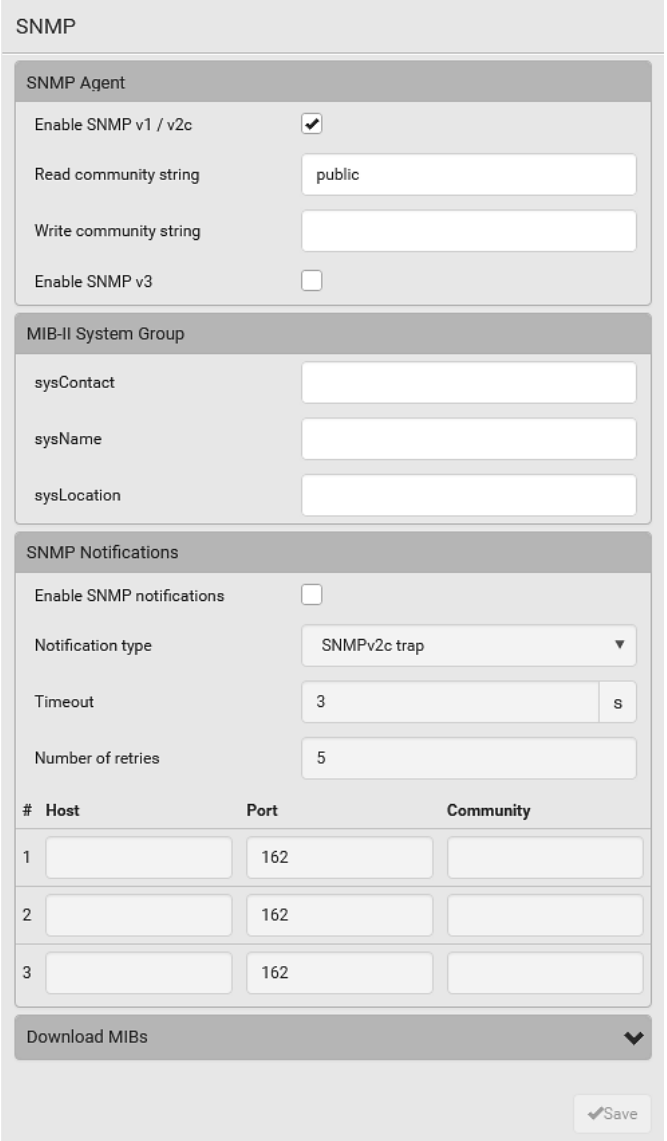
Special note for AES ciphers:

The PRO3X device's TLS-based protocols support AES 128- and 256-bit ciphers. The exact cipher to use is negotiated between PRO3X and the client (such as a web browser), which is impacted by the cipher priority of PRO3X and the client's cipher availability/settings.

Tip: To force PRO3X to use a specific AES cipher, refer to your client's user documentation for information on configuring AES settings. For example, you can enable a cipher and disable the other in the Firefox via the "about:config" command.

To configure SNMP communication:

Choose Device Settings > Network Services > SNMP.



Enable or disable "SNMP v1 / v2c" and/or "SNMP v3" by clicking the corresponding checkbox.
The SNMP v1/v2c read-only access is enabled by default. The default 'Read community string' is "public."
To enable read-write access, type the 'Write community string.' Usually the string is "private."
Enter the MIB-II system group information, if applicable.
sysContact - the contact person in charge of the system
sysName - the name assigned to the system
sysLocation - the location of the system

To configure SNMP notifications:

Select the 'Enable SNMP notifications' checkbox.

Select a notification type -- SNMPv2c trap, SNMPv2c inform, SNMPv3 trap, and SNMPv3 inform.

Specify the SNMP notification destinations and enter necessary information. For details, refer to:

SNMPv2c Notifications/SNMPv3 Notifications

Note: Any changes made to the 'SNMP Notifications' section on the SNMP page will update the settings of the System SNMP Notification Action, and vice versa. To add more than three SNMP destinations, you can create new SNMP notification actions.

You must download the SNMP MIB for your PRO3X to use with your SNMP manager.

Click the Download MIBs title bar to show the download links.

- Click the PDU2-MIB download link.
- Click Save.

Configuring SMTP Settings

The PRO3X can be configured to send alerts or event messages to a specific administrator by email.

To send emails, you have to configure the SMTP settings and enter an IP address for your SMTP server and a sender's email address.

If any email messages fail to be sent successfully, the failure event and reason are available in the event log.

To set SMTP server settings:

Choose Device Settings > Network Services > SMTP Server.

Enter the information needed.

Field	Description
IP address/host name	Type the name or IP address of the mail server.
Port	Type the port number. ▪ Default is 25
Sender email address	Type an email address for the sender.
Number of sending retries	Type the number of email retries. ▪ Default is 2 retries
Time between sending retries	Type the interval between email retries in minutes. ▪ Default is 2 minutes.
Server requires authentication	Select this checkbox if your SMTP server requires password authentication.
User name, Password	Type a user name and password for authentication after selecting the above checkbox. ▪ The length of user name and password ranges between 4 and 64. Case sensitive. ▪ Spaces are not allowed for the user name, but allowed for the password.
Enable SMTP over TLS (StartTLS)	If your SMTP server supports the Transport Layer Security (TLS), select this checkbox.

Settings for the CA Certificate:

Field/setting	Description
Browse...	Click this button to import a certificate file. Then you can: ▪ Click Show to view the certificate's content. ▪ Click Remove to delete the installed certificate if it is inappropriate.
Allow expired and not yet valid certificates	▪ Select this checkbox to make the authentication succeed regardless of the certificate's validity period. ▪ After deselecting this checkbox, the authentication fails whenever any certificate in the selected certificate chain is outdated or not valid yet.

Now that you have set the SMTP settings, you can test it to ensure it works properly.

Type the recipient's email address in the 'Recipient email addresses' field. Use a comma to separate multiple email addresses.

Click Send Test Email.

Check if the recipient(s) receives the email successfully.

Click Save.

Special note for AES ciphers:

The PRO3X device's TLS-based protocols support AES 128- and 256-bit ciphers. The exact cipher to use is negotiated between PRO3X and the client (such as a web browser), which is impacted by the cipher priority of PRO3X and the client's cipher availability/settings.

Tip: To force PRO3X to use a specific AES cipher, refer to your client's user documentation for information on configuring AES settings.

Changing SSH Settings

You can enable or disable the SSH access to the command line interface, change the TCP port, or set a password or public key for login over the SSH connection.

To change SSH settings:

Choose Device Settings > Network Services > SSH.

To enable or disable the SSH access, select or deselect the checkbox.

To use a different port, type a port number.

Select one of the authentication methods.

- *Password authentication only:* Enables the password-based login only.
- *Public key authentication only:* Enables the public key-based login only.
- *Password and public key authentication:* Enables both the password- and public key-based login. This is the default.

Click Save.

If the public key authentication is selected, you must enter a valid SSH public key for each user profile to log in over the SSH connection.

Changing Telnet Settings

You can enable or disable the Telnet access to the command line interface, or change the TCP port.

To change Telnet settings:

Choose Device Settings > Network Services > Telnet.

To enable the Telnet access, select the checkbox.

To use a different port, type a new port number.

Click Save.

Changing Modbus Settings

The PRO3X supports both the Modbus/TCP and Modbus Gateway features. Enable either or both Modbus features according to your needs.

Modbus/TCP Access:

You can enable or disable the Modbus/TCP access to PRO3X, set it to the read-only mode, or change the TCP port.

Choose Device Settings > Network Services > Modbus.

To enable the Modbus/TCP access, select the "Enable Modbus/TCP access" checkbox.

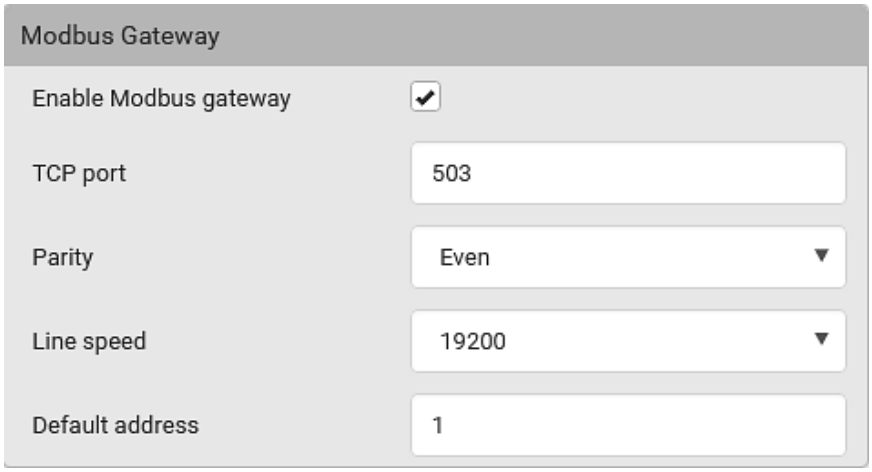
To use a different port, type a new port number.

To enable the Modbus read-only mode, select the checkbox of the "Enable read-only mode" field. To enable the read-write mode, deselect it.

Modbus Gateway:

If connecting the Modbus RTU devices to PRO3X and enabling the Modbus Gateway feature, the Modbus TCP clients on your network will be able to communicate with those Modbus RTU devices attached to PRO3X.

To allow the Modbus TCP clients on the network to communicate with the Modbus RTU devices connected to the PRO3X, select the 'Enable Modbus gateway' checkbox.



Now configure the fields shown.

Field	Description
TCP port	Use the default port 503, or assign a different port. Valid range is 1 to 65535. *Note: Port 502 is the default Modbus/TCP port for PRO3X, so you cannot use that port for the Modbus Gateway.*
Parity, Line speed	Use the default values, or update if the Modbus RTU devices are using different communication parameters.
Default address	If the Modbus TCP client does not support Modbus RTU unit identifier addressing, enter a Default Address. If you must provide a unit identifier address: ▪ Only one Modbus RTU device is supported. ▪ The unit identifier address you provide is applied to the Modbus RTU device connected to PRO3X. Note that each Modbus RTU device's unit identifier address must be unique. *Warning: If the connected Modbus RTU device's address does not match the address entered in this field, communications between the Modbus TCP clients and Modbus RTU device fail.*

Enabling Service Advertising

The PRO3X advertises all enabled services that are reachable using the IP network. This feature uses DNS-SD (Domain Name System-Service Discovery) and MDNS (Multicast DNS). The advertised services are discovered by clients that have implemented DNS-SD and MDNS.

The advertised services include the following:

- HTTP
- HTTPS
- Telnet
- SSH
- Modbus
- json-rpc
- SNMP

By default, this feature is enabled.

Enabling this feature also enables Link-Local Multicast Name Resolution (LLMNR) and/or MDNS, which are required for resolving APIPA host names.

The service advertisement feature supports both IPv4 and IPv6 protocols.

If you have set a preferred host name for IPv4 and/or IPv6, that host name can be used as the zero configuration .local host name, that is, *<preferred_host_name>.local*, where <preferred_host_name> is the preferred host name you have specified for PRO3X. The IPv4 host name is the first priority. If an IPv4 host name is not available, then use the IPv6 host name.

To enable or disable service advertising:

Choose Device Settings > Network Services > Service Advertising.

To enable the service advertising, select either or both checkboxes.

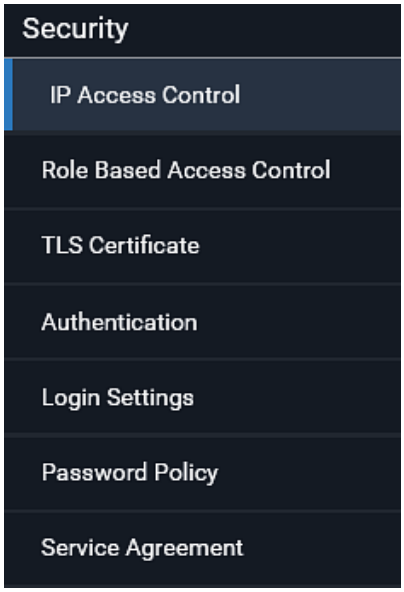
To advertise via MDNS, select the Multicast DNS checkbox.

To advertise via LLMNR, select the Link-Local Multicast Name Resolution checkbox.

Click Save.

Configuring Security Settings

The PRO3X provides tools to control access. You can enable the internal firewall, create firewall rules, and set login limitations. In addition, you can create and install the certificate or set up external authentication servers for access control. This product supports SHA-2 TLS certificates.



Submenu command	Refer to
IP Access Control	*Creating IP Access Control Rules*
Role Based Access Control	*Creating Role Based Access Control Rules*
TLS Certificate	*Setting Up a TLS Certificate*
Authentication	*Setting Up External Authentication*
Login Settings	*Configuring Login Settings*
Password Policy	*Configuring Password Policy*
Service Agreement	*Enabling the Restricted Service Agreement*

ADD a rule to the end of the list
▪ Click Append. ▪ Type an IP address and subnet mask in the IP/Mask field. ▪ Select an option in the Policy field. *Accept:* Accepts traffic from/to the specified IP address(es). *Drop:* Discards traffic from/to the specified IP address(es), without sending any failure notification to the source or destination host. *Reject:* Discards traffic from/to the specified IP address(es), and an ICMP message is sent to the source or destination host for failure notification.

Creating IP Access Control Rules

IP access control rules (firewall rules) determine whether to accept or discard traffic to/from the PRO3X, based on the IP address of the host sending or receiving the traffic.

When creating rules, keep these principles in mind:

Rule order is important.

When traffic reaches or is sent from the PRO3X, the rules are executed in numerical order. Only the first rule that matches the IP address determines whether the traffic is accepted or discarded. Any subsequent rules matching the IP address are ignored.

Prefix length is required.

When typing the IP address, you must specify it in the CIDR notation. That is, BOTH the address and the prefix length are included. For example, to specify a single address with the 24-bit prefix length, use this format:

x.x.x.x/24

/24 = the prefix length.

Note: Valid IPv4 addresses range from 0.0.0.0 through 255.255.255.255.

To configure IPv4 access control rules:

Choose Device Settings > Security > IP Access Control.

Select the 'Enable IPv4 access control' checkbox to enable IPv4 access control rules.

Determine the IPv4 default policy.

- *Accept:* Accepts traffic from all IPv4 addresses.
- *Drop:* Discards traffic from all IPv4 addresses, without sending any failure notification to the source host.
- *Reject:* Discards traffic from all IPv4 addresses, and an ICMP message is sent to the source host for failure notification.

Go to the Inbound Rules section or the Outbound Rules section according to your needs.

- Inbound rules control the data sent to the PRO3X.
- Outbound rules control the data sent from the PRO3X.

Create rules. Refer to the tables below for different operations.

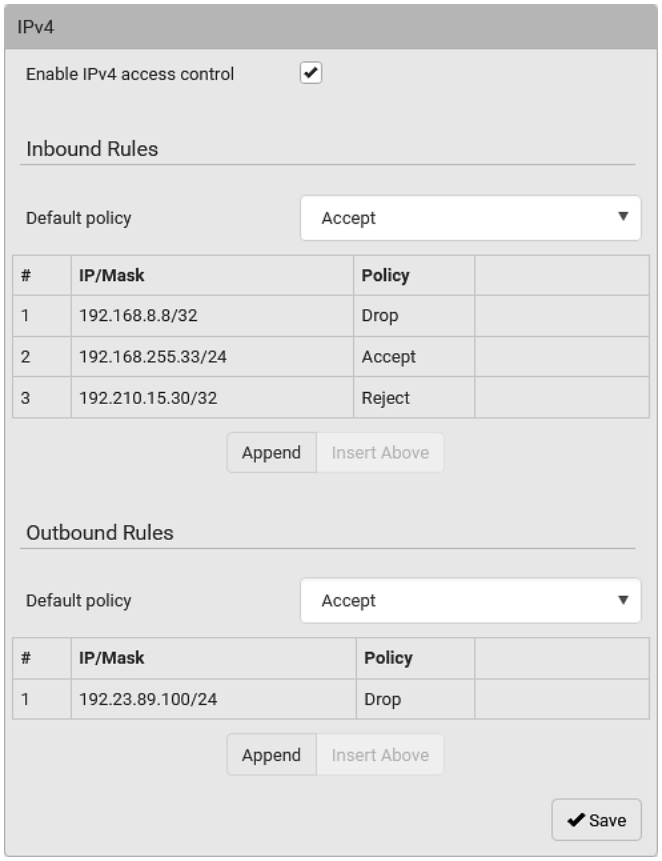
INSERT a rule between two rules

- Select the rule above which you want to insert a new rule. For example, to insert a rule between rules #3 and #4, select #4.
- Click *Insert Above*.
- Type an IP address and subnet mask in the IP/Mask field.
- Select *Accept*, *Drop* or *Reject* in the Policy field. Refer to the above table for details.

The system automatically numbers the rule.

When finished, the rules are listed.

You can select any existing rule and then click  or  to change its priority.



Click Save. The rules are applied.

To configure IPv6 access control rules:

On the same page, select the 'Enable IPv6 access control' checkbox to enable IPv6 access control rules.

Follow the same procedure as the above IPv4 rule setup to create IPv6 rules.

Make sure you click the Save button in the IPv6 section, or the changes made to IPv6 rules are not saved.

Editing or Deleting IP Access Control Rules

When an existing IP access control rule requires updates of IP address range and/or policy, modify them accordingly. Or you can delete any unnecessary rules.

To modify or delete a rule:

Choose Device Settings > Security > IP Access Control.

Go to the IPv4 or IPv6 section.

Select the desired rule in the list.

Ensure the IPv4 or IPv6 checkbox has been selected, or you may not edit or delete any rule.

Perform the desired action.

Make changes to the selected rule, and then click Save.

Click  to remove it.

To resort its order, click  or  .

Click Save.

- IPv4 rules: Make sure you click the Save button in the IPv4 section, or the changes made to IPv4 rules are not saved.
- IPv6 rules: Make sure you click the Save button in the IPv6 section, or the changes made to IPv6 rules are not saved.

Creating Role Based Access Control Rules

Role-based access control rules are similar to IP access control rules, except that they are applied to members of a specific role. This enables you to grant system permissions to a specific role, based on their IP addresses.

Same as IP access control rules, the order of role-based access control rules is important, since the rules are executed in numerical order.

To create IPv4 role-based access control rules:

Choose Device Settings > Security > Role Based Access Control.

Select the 'Enable role based access control for IPv4' checkbox to enable IPv4 access control rules.

Determine the IPv4 default policy.

Accept: Accepts traffic when no matching rules are present.

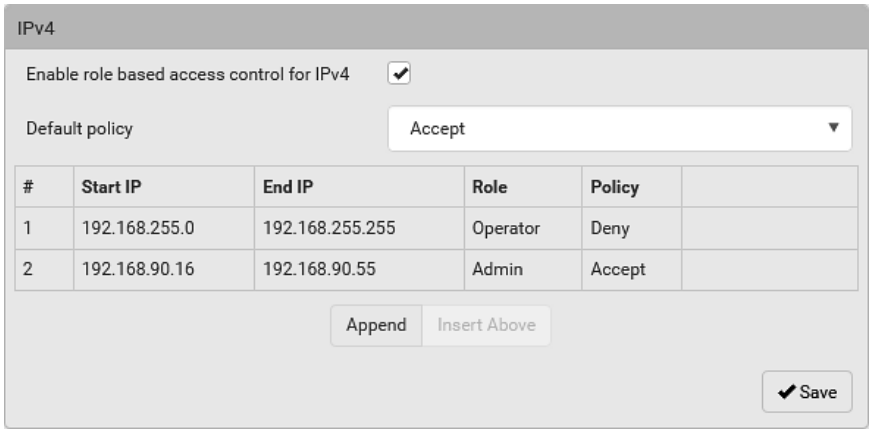
Deny: Rejects any user's login attempt when no matching rules are present.

Create rules. Refer to the tables below for different operations.

ADD a rule to the end of the list
▪ Click Append. ▪ Type a starting IP address in the Start IP field. ▪ Type an ending IP address in the End IP field. ▪ Select a role in the Role field. This rule applies to members of this role only. ▪ Select an option in the Policy field. *Accept:* Accepts traffic from the specified IP address range when the user is a member of the specified role. *Deny:* Rejects the login attempt of a user from the specified IP address range when that user is a member of the specified role.
INSERT a rule between two rules
▪ Select the rule above which you want to insert a new rule. For example, to insert a rule between rules #3 and #4, select #4. ▪ Click Insert Above. ▪ Type a starting IP address in the Start IP field. ▪ Type an ending IP address in the End IP field. ▪ Select a role in the Role field. This rule applies to members of this role only. ▪ Select Accept or Deny in the Policy field. Refer to the above table for details.

The system automatically numbers the rule.

When finished, the rules are listed on this page.



You can select any existing rule and then click  or  to change its priority. Click Save. The rules are applied.

Setting Up a TLS Certificate

Important: TLS is used instead of SSL 3.0 due to published security vulnerabilities in SSL 3.0. Make sure your network infrastructure, such as LDAP and mail services, uses TLS rather than SSL 3.0.

Having an X.509 digital certificate ensures that both parties in a TLS connection are who they say they are.

Besides, you can create or apply for a multi-domain certificate with subject alternative names.

To obtain a CA-signed certificate:

Create a Certificate Signing Request (CSR) on the PRO3X.

Submit it to a certificate authority (CA). After the CA processes the information in the CSR, it provides you with a certificate.

Import the CA-signed certificate onto the PRO3X.

Note: If you are using a certificate that is part of a chain of certificates, each part of the chain is signed during the validation process.

A CSR is not required in either scenario below:

Make the PRO3X create a *self-signed* certificate.

Appropriate, valid certificate and key files are already available, and you only need to import them.

Creating a CSR

Follow this procedure to create the CSR for your PRO3X.

Note that you must enter information in the fields showing the message 'required.'

To create a CSR:

Choose Device Settings > Security > TLS Certificate.

Provide the information requested.

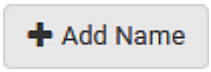
Field	Description
Country	The country where your company is located. Use the standard ISO country code, which comprises two uppercase letters. For a list of ISO codes, google ISO 3166 country codes.
State or province	The full name of the state or province where your company is located.
Locality	The city where your company is located.
Organization	The registered name of your company.
Organizational unit	The name of your department.
Common name	The fully qualified domain name (FQDN) of your PRO3X.
Email address	An email address where you or another administrative user can be reached.

Subject:

Warning: If you generate a CSR without values entered in the required fields, you cannot obtain third-party certificates.

Subject Alternative Names:

If you want a certificate to secure multiple hosts across different domains or subdomains, you can add additional DNS host names or IP addresses of the wanted hosts to this CSR so that a single certificate will be valid for all of them.

Click 

when there are more than one additional hosts to add.

Field	Do this
Key length	Select an available key length (bits). A larger key length enhances the security, but slows down the response of PRO3X. Only 2048 is available now.
Self-sign	For requesting a certificate signed by the CA, ensure this checkbox is NOT selected.
Challenge, Confirm challenge	Type a password. The password is used to protect the certificate or CSR. This information is optional. The value should be 4 to 64 characters long. Case sensitive.

Key Creation Parameters:

Click Create New TLS Key to create both the CSR and private key. This may take several minutes to complete.

Click Download Certificate Signing Request to download the CSR to your computer.

You are prompted to open or save the file. Click Save to save it onto your computer.

Submit it to a CA to obtain the digital certificate.

If the CSR contains incorrect data, click Delete Certificate Signing Request to remove, and then repeat the above steps to re-create it.

To store the newly-created private key on your computer, click Download Key in the **New TLS Certificate** section.

Note: The Download Key button in the Active TLS Certificate *section is for downloading the private key of the currently-installed certificate rather than the newly-created one.*

You are prompted to open or save the file. Click Save to save it onto your computer.

After getting the CA-signed certificate, install it.

Installing a CA-Signed Certificate

To get a certificate from a certificate authority (CA), first create a CSR and send it to the CA.

After receiving the CA-signed certificate, install it onto the PRO3X.

To install the CA-signed certificate:

Choose Device Settings > Security > TLS Certificate.

Click 

to navigate to the CA-signed certificate file.

Click Upload to install it.

To verify whether the certificate has been installed successfully, check the data shown in the Active TLS Certificate section.

Creating a Self-Signed Certificate

When appropriate certificate and key files for PRO3X are unavailable, the alternative, other than submitting a CSR to the CA, is to generate a self-signed certificate.

Note that you must enter information in the fields showing the message 'required.'

To create and install a self-signed certificate:

Choose Device Settings > Security > TLS Certificate.

Enter information.

Field	Description
Country	The country where your company is located. Use the standard ISO country code, which comprises two uppercase letters. For a list of ISO codes, google ISO 3166 country codes.
State or province	The full name of the state or province where your company is located.
Locality	The city where your company is located.
Organization	The registered name of your company.
Organizational unit	The name of your department.
Common name	The fully qualified domain name (FQDN) of your PRO3X.
Email address	An email address where you or another administrative user can be reached.
Key length	Select an available key length (bits). A larger key length enhances the security, but slows down the response of PRO3X. Only 2048 is available now.
Self-sign	Ensure this checkbox is selected, which indicates that you are creating a self-signed certificate.
Validity in days	This field appears after the Self-sign checkbox is selected. Type the number of days for which the self-signed certificate will be valid.

A password is not required for a self-signed certificate so the Challenge and Confirm Challenge fields disappear.

Click Create New TLS Key to create both the self-signed certificate and private key. This may take several minutes to complete.

Once complete, do the following:

Double check the data shown in the New TLS Certificate section.

If correct, click "Install Key and Certificate" to install the self-signed certificate and private key.

Tip: To verify whether the certificate has been installed successfully, check the data shown in the Active TLS Certificate section.

If incorrect, click "Delete Key and Certificate" to remove the self-signed certificate and private key, and then repeat the above steps to re-create them.

(Optional) To download the self-signed certificate and/or private key, click Download Certificate or Download Key in the New TLS Certificate section.

You are prompted to open or save the file. Click Save to save it onto your computer.

Note: The Download Key button in the Active TLS Certificate *section is for downloading the private key of the currently-installed certificate rather than the newly-created one.*

Installing or Downloading Existing Certificate and Key

You can download the already-installed certificate and private key from any PRO3X for backup or file transfer. For example, you can install the files onto a replacement PRO3X, add the certificate to your browser and so on.

If valid certificate and private key files are already available, you can install them on the PRO3X without going through the process of creating a CSR or a self-signed certificate.

Note: If you are using a certificate that is part of a chain of certificates, each part of the chain is signed during the validation process.

To download active key and certificate files from PRO3X:

Choose Device Settings > Security > TLS Certificate.

In the *Active TLS Certificate* section, click Download Key and Download Certificate respectively.

Note: The Download Key button in the New TLS Certificate section, if present, is for downloading the newly-created private key rather than the one of the currently-installed certificate.

You are prompted to open or save the file. Click Save to save it onto your computer.

To install available key and certificate files onto PRO3X:

Choose Device Settings > Security > TLS Certificate.

Select the "Upload key and certificate" checkbox at the bottom of the page.

The 'Key File' and 'Certificate file' buttons appear. Click each button to select the key and/or certificate file.

Click Upload. The selected files are installed.

To verify whether the certificate has been installed successfully, check the data shown in the Active TLS Certificate section.

Setting Up External Authentication

Important: TLS is used instead of SSL 3.0 due to published security vulnerabilities in SSL 3.0. Make sure your network infrastructure, such as LDAP and mail services, uses TLS rather than SSL 3.0.

For security purposes, users attempting to log in to PRO3X must be authenticated. PRO3X supports the following authentication mechanisms:

Local user database on the PRO3X

Lightweight Directory Access Protocol (LDAP)

Remote Access Dial-In User Service (Radius) protocol

By default, PRO3X is configured for local authentication. If you use this method, you only need to create user accounts.

If you prefer external authentication, you must provide PRO3X with information about the external Authentication and Authorization (AA) server.

If both local and external authentication is needed, create user accounts on the PRO3X in addition to providing the external AA server data.

When configured for external authentication, all PRO3X users must have an account on the external AA server. Local-authentication-only users will have no access to the PRO3X except for the admin, who always can access the PRO3X.

If the external authentication fails, an "Authentication failed" message is displayed. Details regarding the authentication failure are available in the event log.

Note that only users who have both the "Change Authentication Settings" and "Change Security Settings" permissions can configure or modify the authentication settings.

To enable external authentication:

Collect external AA server information. Enter required data for external AA server(s) on the PRO3X.

If both the external and local authentication is needed, or you have to return to the local authentication only, see Managing External Authentication Settings.

Special note about the AES cipher:

The PRO3X device's TLS-based protocols support AES 128- and 256-bit ciphers. The exact cipher to use is negotiated between PRO3X and the client (such as a web browser), which is impacted by the cipher priority of PRO3X and the client's cipher availability/settings.

Tip: To force PRO3X to use a specific AES cipher, refer to your client's user documentation for information on configuring AES settings

Gathering LDAP/Radius Information

It requires knowledge of your AA server settings to configure the PRO3X for external authentication. If you are not familiar with these settings, consult your AA server administrator for help.

Information needed for LDAP authentication:

The IP address or hostname of the LDAP server

Whether the Secure LDAP protocol (LDAP over TLS) is being used

If Secure LDAP is in use, consult your LDAP administrator for the CA certificate file.

The network port used by the LDAP server

The type of the LDAP server, usually one of the following options:

OpenLDAP

If using an OpenLDAP server, consult the LDAP administrator for the Bind Distinguished Name (DN) and password.

Microsoft Active Directory® (AD)

If using a Microsoft Active Directory server, consult your AD administrator for the name of the Active Directory Domain.

Bind Distinguished Name (DN) and password (if anonymous bind is NOT used)

The Base DN of the server (used for searching for users)

The login name attribute (or AuthorizationString)

The user entry object class

The user search subfilter (or BaseSearch)

Information needed for Radius authentication:

The IP address or host name of the Radius server

Authentication protocol used by the Radius server

Shared secret for a secure communication

UDP authentication port and accounting port used by the Radius server

Adding LDAP/LDAPS Servers

To use LDAP authentication, enable it and enter the information you have gathered.

Note that you must enter information in the fields showing the message 'required.'

To add LDAP/LDAPS servers:

Choose Device Settings > Security > Authentication.

Click New in the LDAP Servers section.

Enter information as shown in the following table:

Field/setting	Description
IP address / hostname	The IP address or hostname of your LDAP/LDAPS server. Without the encryption enabled, you can type either the domain name or IP address in this field, but you must type the fully qualified domain name if the encryption is enabled.
Copy settings from existing LDAP server	This checkbox appears only when there are existing AA server settings on the PRO3X. To duplicate any existing AA server's settings, refer to the duplicating procedure below.
Type of LDAP server	Choose one of the following options: • OpenLDAP • Microsoft Active Directory. Active Directory is an implementation of LDAP/LDAPS directory services by Microsoft for use in Windows environments.
Security	Determine whether you would like to use Transport Layer Security (TLS) encryption, which allows the PRO3X to communicate securely with the LDAPS server. Three options are available: • StartTLS • TLS • None
Port (None/StartTLS)	The default Port is 389. Either use the standard LDAP TCP port or specify another port.
Port (TLS)	Configurable only when "TLS" is selected in the Security field. The default is 636. Either use the default port or specify another one.
Enable verification of LDAP server certificate	Select this checkbox if it is required to validate the LDAP server's certificate by the PRO3X prior to the connection. If the certificate validation fails, the connection is refused.
CA certificate	Consult your AA server administrator to get the CA certificate file for the LDAPS server. Click  to select and install the certificate file. Click Show to view the installed certificate's content. Click Remove to delete the installed certificate if it is inappropriate.
Allow expired and not yet valid certificates	Select this checkbox to make the authentication succeed regardless of the certificate's validity period. After deselecting this checkbox, the authentication fails whenever any certificate in the selected certificate chain is outdated or not valid yet.
Anonymous bind	Use this checkbox to enable or disable anonymous bind.

	▪ To use anonymous bind, select this checkbox. When a Bind DN and password are required to bind to the external LDAP/LDAPS server, deselect this checkbox.
Bind DN	Required after deselecting the Anonymous Bind checkbox. Distinguished Name (DN) of the user who is permitted to search the LDAP directory in the defined search base.
Bind password, Confirm bind password	Required after deselecting the Anonymous Bind checkbox. Enter the Bind password.
Base DN for search	Distinguished Name (DN) of the search base, which is the starting point of the LDAP search. Example: `ou=dev,dc=example,dc=com`
Login Name Attribute	The attribute of the LDAP user class which denotes the login name. Usually it is the `uid`.
User entry object class	The object class for user entries. Usually it is `inetOrgPerson`.
User search subfilter	Search criteria for finding LDAP user objects within the directory tree.
Active Directory domain	The name of the Active Directory Domain. Example: `testradius.com`

To verify if the authentication configuration is set correctly, click Test Connection to check whether the PRO3X can connect to the new server successfully.

Tip: You can also test the connection on the Authentication page after finishing adding servers.

Click Add Server. The new LDAP server is listed on the Authentication page.

To add more servers, repeat the same steps.

In the Authentication Type field, select LDAP. Otherwise, the LDAP authentication does not work.

Click Save. The LDAP authentication is now in place.

To duplicate LDAP/LDAPS server settings:

If you have added any LDAP/LDAPS server to the PRO3X, and the server you will add shares identical settings with an existing one, the most convenient way is to duplicate that LDAP/LDAPS server's data and then revise the IP address/host name.

Repeat Steps 1 to 2 in the above procedure.

Select the "Copy settings from existing LDAP server" checkbox.

Click the "Select LDAP Server" field to select the LDAP/LDAPS server whose settings you want to copy.

Modify the IP Address/Hostname field.

Click Add Server.

Adding Radius Servers

To use Radius authentication, enable it and enter the information you have gathered.

Note that you must enter information in the fields showing the message 'required.'

To add Radius servers:

Choose Device Settings > Security > Authentication.

Click New in the Radius Servers section.

Field/setting	Description
IP address / hostname	The IP address or hostname of your Radius server.
Type of RADIUS authentication	Select an authentication protocol. • PAP (Password Authentication Protocol) • CHAP (Challenge Handshake Authentication Protocol) • MS-CHAPv2 (Microsoft Challenge Handshake Authentication Protocol) CHAP is generally considered more secure because the user name and password are encrypted, while in PAP they are transmitted in the clear. MS-CHAPv2 provides stronger security than the above two. Selecting this option will support both MS-CHAPv1 and MS-CHAPv2.
Authentication port, Accounting port	The defaults are standard ports -- 1812 and 1813. To use non-standard ports, type a new port number.
Timeout	This sets the maximum amount of time to establish contact with the Radius server before timing out. Type the timeout period in seconds.
Retries	Type the number of retries.
Shared secret, Confirm shared secret	The shared secret is necessary to protect communication with the Radius server.

Enter information.

To verify if the authentication configuration is set correctly, click Test Connection to check whether the PRO3X can connect to the new server successfully.

Tip: You can also test the connection on the Authentication page after finishing adding servers.

Click Add Server. The new Radius server is listed on the Authentication page.

To add more servers, repeat the same steps.

In the Authentication Type field, select Radius. **Otherwise**, the Radius authentication does not work.

Click Save. Radius authentication is now in place.

Managing External Authentication Settings

Choose Device Settings > Security > Authentication to open the Authentication page, where you can:

Enable both the external and local authentication.

Edit or delete a server.

Resort the access order of servers.

Test the connection to a server.

Disable external authentication without removing servers.

To test, edit or delete a server, or resort the server list:

Select a server in the list.

Access Order	IP Address / Hostname	Security	Port	LDAP Server Type
1	192.168.91.100	None	389	OpenLDAP
2	192.168.1.33	StartTLS	389	OpenLDAP
3	192.168.8.95	None	389	Microsoft Active Directory

Perform the desired action.

Click Edit to edit its settings, and click Modify Server to save changes.

Click Delete to delete the server, and then confirm the operation.

Click Test Connection to verify the connection to the selected server. User credentials may be required.

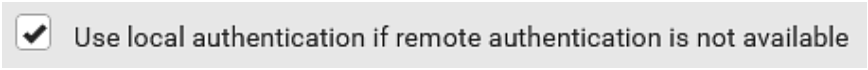
Click  or  to change the server order, which determines the access priority, and click Save Order to save the new sequence.

Note: Whenever PRO3X is successfully connected to one external authentication server, it STOPS trying access to remaining servers in the authentication list regardless of the user authentication result.

To enable both external and local authentication:

In the 'Authentication type' field, select the external authentication you want -- LDAP or RADIUS.

Select the following checkbox. Then the PRO3X always tries external authentication first. Whenever the external authentication fails, the PRO3X switches to local authentication.



Click Save.

To disable external authentication:

In the 'Authentication type' field, select Local.

Click Save.

Configuring Login Settings

Choose Device Settings > Security > Login Settings to open the Login Settings page, where you can:

Configure the user blocking feature.

Note: The user blocking function applies only to local authentication instead of external authentication through AA servers.

Determine the timeout period for any inactive user.

Prevent simultaneous logins using the same login name.

To configure user blocking:

To enable the user blocking feature, select the 'Block user on login failure' checkbox.

In the 'Block timeout' field, type a value or click  to select a time option. This setting determines how long the user is blocked.

If you type a value, the value must be followed by a time unit, such as '4 min.'

In the 'Maximum number of failed logins' field, type a number. This is the maximum number of login failure the user is permitted before the user is blocked from accessing the PRO3X.

Click Save.

Tip: If any user blocking event occurs, you can unblock that user manually by using the "unblock" CLI command over a local connection.

To set limitations for login timeout and use of identical login names:

In the "Idle timeout period" field, type a value or click  to select a time option. This setting determines how long users are permitted to stay idle before being forced to log out.

If you type a value, the value must be followed by a time unit, such as '4 min.'

Keep the idle timeout to 20 minutes or less if possible. This reduces the number of idle sessions connected, and the number of simultaneous commands sent to the PRO3X.

Select the 'Prevent concurrent login with same username' checkbox if intending to prevent multiple persons from using the same login name simultaneously.

Click Save.

Configuring Password Policy

Choose Device Settings > Security > Password Policy to open the Password Policy page, where you can:

Force users to use strong passwords.

Force users to change passwords at a regular interval -- that is, password aging.

Use of strong passwords makes it more difficult for intruders to crack user passwords and access the PRO3X.

To configure password aging:

Select the 'Enabled' checkbox of Password Aging.

In the 'Password aging interval' field, type a value or click  to select a time option. This setting determines how often users are requested to change their passwords.

If you type a value, the value must be followed by a time unit, such as '10 d.'

Click Save.

To force users to create strong passwords:

Select the 'Enabled' checkbox of Strong Passwords to activate the strong password feature. The following are the default settings:

Minimum length	= 8 characters
Maximum length	= 32 characters
At least one lowercase character	= Required
At least one uppercase character	= Required
At least one numeric character	= Required
At least one special character	= Required
Number of forbidden previous passwords	= 5

Note: The maximum password length accepted by PRO3X is 64 characters.

Make changes to the default settings as needed.

Click Save.

Enabling the Restricted Service Agreement

The restricted service agreement feature, if enabled, forces users to read a security agreement when they log in to the PRO3X.

Users must accept the agreement, or they cannot log in.

An event notifying you if a user has accepted or declined the agreement can be generated.

To enable the service agreement:

Click Device Settings > Security > Service Agreement.

Select the 'Enforce restricted service agreement' checkbox.

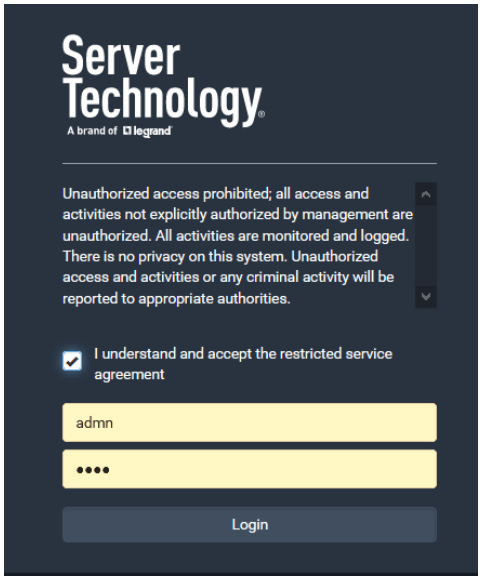
Edit or paste the content as needed.

A maximum of 10,000 characters can be entered.

Click Save.

Login manner after enabling the service agreement:

After the Restricted Service Agreement feature is enabled, the agreement's content is displayed on the login screen.



Do either of the following, or the login fails:

In the web interface, select the checkbox labeled "I understand and accept the restricted service agreement."

Tip: To select the agreement checkbox using the keyboard, first press Tab to go to the checkbox and then Enter.

In the CLI, type `y` when the confirmation message "I understand and accept the restricted service agreement" is displayed.

Setting the Date and Time

Set the internal clock on the PRO3X manually, or link to a Network Time Protocol (NTP) server.

Note: If you are using Sunbird's Power IQ to manage the PRO3X, you must configure Power IQ and the PRO3X to have the same date/time or NTP settings.

To set the date and time:

Choose Device Settings > Date/Time.

Click the 'Time zone' field to select your time zone from the list.

If the daylight saving time applies to your time zone, verify the 'Automatic daylight saving time adjustment' checkbox is selected.

If the daylight saving time rules are not available for the selected time zone, the checkbox is not configurable.

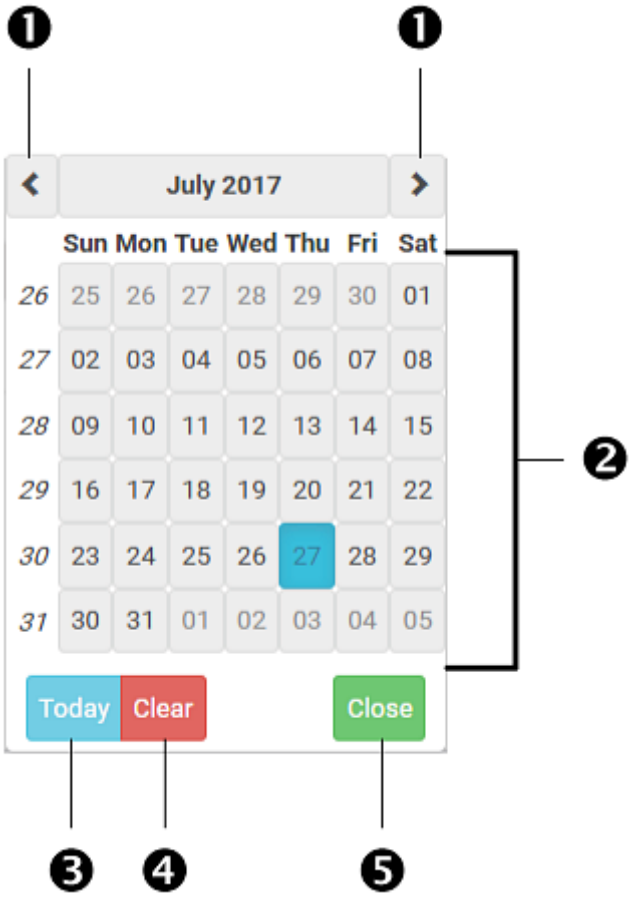
Select the method for setting the date and time.

Click Save.

PRO3X follows the NTP server sanity check per the IETF RFC.

Calendar

The calendar icon  in the Date field is a convenient tool to select a custom date. Click it and a calendar similar to the following appears.



Number	Item	Description
1	arrows	Switch between months.
2	dates (01-31)	All dates of the selected month. To select a date, simply click it.
3	Today	Select today's date.
4	Clear	Clear the entry, if any, in the Date field.
5	Close	Close the calendar.

Windows NTP Server Synchronization Solution

The NTP client on the PRO3X follows the NTP RFC so the PRO3X rejects any NTP servers whose root dispersion is more than one second. An NTP server with a dispersion of more than one second is considered an inaccurate NTP server by the PRO3X.

Note: For information on NTP RFC, visit **http://tools.ietf.org/html/rfc4330 - http://tools.ietf.org/html/rfc4330** *to refer to section 5.*

Windows NTP servers may have a root dispersion of more than one second, and therefore cannot synchronize with the PRO3X. When the NTP synchronization issue occurs, change the dispersion settings to resolve it.

To change the Windows NTP's root dispersion settings:

Access the registry settings associated with the root dispersion on the Windows NTP server.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config

AnnounceFlags must be set to 0x05 or 0x06.

0x05 = 0x01 (Always time server) and 0x04 (Always reliable time server)

0x06 = 0x02 (Automatic time server) and 0x04 (Always reliable time server)

Note: Do NOT use 0x08 (Automatic reliable time server) because its dispersion starts at a high value and then gradually decreases to one second or lower.

LocalClockDispersion must be set to 0.

Event Rules and Actions

A benefit of the product's intelligence is its ability to notify you of or react to a change in conditions. This event notification or reaction is an "event rule."

An event rule consists of two parts:

- Event: This is the situation where the PRO3X or a device connected to it meets a certain condition. For example, the inlet's voltage reaches the warning level.
- Action: This is the response to the event. For example, the PRO3X notifies the system administrator of the event via email.

If you want the PRO3X to perform one action at a regular interval instead of waiting until an event occurs, you can schedule that action. For example, you can make the PRO3X email the temperature report every hour.

Note that you need the Administrator Privileges to configure event rules.

To create an event rule:

Choose Device Settings > Event Rules.

If the needed action is not available yet, create it by clicking ➕ New Action.

Assign a name to this action.

Select the desired action and configure it as needed.

Click Create.

Click ➕ New Rule to create a new rule.

Assign a name to this rule.

Make sure the Enabled checkbox is selected, or the new event rule does not work.

In the Event field, select the event to which you want the PRO3X to react.

In the 'Available actions' field, select the desired action(s) to respond to the selected event.

Click Create.

To create a scheduled action:

If the needed action is not available yet, create it by clicking ➕ New Action. See above.

Note: When creating scheduled actions, available actions are less than usual because it is meaningless to schedule certain actions like "Alarm," "Log event message," "Send email," "Syslog message" and the like.

Click ➕ New Scheduled Action to schedule the desired action.

Assign a name to this scheduled action.

Make sure the Enabled checkbox is selected, or the PRO3X does not perform this scheduled action.

Set the interval time, which ranges from every minute to yearly.

In the 'Available actions' field, select the desired action(s).

Click Create.

Built-in Rules and Rule Configuration

PRO3X is shipped with four built-in event rules, which cannot be deleted. If the built-in event rules do not satisfy your needs, create new rules.

Built-in rules:

System Event Log Rule:

This causes ANY event occurred to the PRO3X to be recorded in the internal log. It is enabled by default.

System SNMP Notification Rule:

This causes SNMP traps or informs to be sent to specified IP addresses or hosts when ANY event occurs to the PRO3X. It is disabled by default.

Event rule configuration illustration:

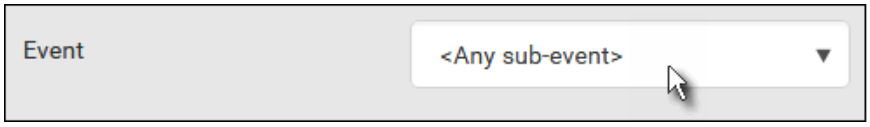
Choose Device Settings > Event Rules > 

.

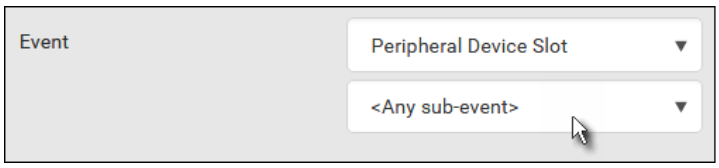
Click the Event field to select an event type.

<Any sub-event> means all events shown on the list.

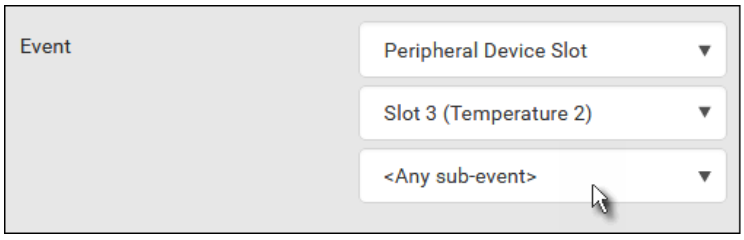
<Any Numeric Sensor> means all numeric sensors of the PRO3X, including internal and environmental sensors. <Any Numeric Sensor> is especially useful if you want to receive the notifications when any numeric sensor's readings pass through a specific threshold.



In this example, the Peripheral Device Slot is selected, which is related to the environmental sensor packages. Then a sensor ID field for this event type appears. Click this additional field to specify which sensor should be the subject of this event.



In this example, sensor ID 3 (Slot 3) is selected, which is a temperature sensor. Then a new field for this sensor appears. Click this field to specify the type of event(s) you want.



In this example, Numeric Sensor is selected because we want to select numeric-sensor-related event(s). Then a field for numeric-sensor-related events appears. Click this field to select one of the numeric-sensor-related events from the list.

Radio buttons for different events:

According to the event you select, the "Trigger condition" field containing three radio buttons may or may not appear.

Event Types	Radio Buttons
Numeric sensor threshold-crossing events, or the occurrence of the selected event -- true or false	Available radio buttons include "Asserted," "Deasserted" and "Both." ▪ Asserted: PRO3X takes the action only when the selected event occurs. That is, the status of the event transits from FALSE to TRUE. ▪ Deasserted: PRO3X takes the action only when the selected event disappears or stops. That is, the status of the selected event transits from TRUE to FALSE. Both: PRO3X takes the action both when the event occurs (asserts) and when the event stops/disappears (deasserts).
State sensor state change	Available radio buttons include "Alarmed/Open/On," "No longer alarmed/Closed/Off" and "Both." ▪ Alarmed/Open/On: PRO3X takes the action only when the chosen sensor enters the alarmed, open or on state. ▪ No longer alarmed/Closed/Off: PRO3X takes the action only when the chosen sensor returns to the normal, closed, or off state. Both: PRO3X takes the action whenever the chosen sensor switches its state.
Sensor availability	Available radio buttons include "Unavailable," "Available" and "Both." ▪ Unavailable: PRO3X takes the action only when the chosen sensor is NOT detected and becomes unavailable. ▪ Available: PRO3X takes the action only when the chosen sensor is detected and becomes available. Both: PRO3X takes the action both when the chosen sensor becomes unavailable or available.
Network interface link state	▪ Link state is up: PRO3X takes the action only when the network link state changes from down to up. ▪ Link state is down: PRO3X takes the action only when the network link state changes from up to down. Both: PRO3X takes the action whenever the network link state changes.
Function enabled or disabled	▪ Enabled: PRO3X takes the action only when the chosen function is enabled. ▪ Disabled: PRO3X takes the action only when the chosen function is disabled. Both: PRO3X takes the action when the chosen function is either enabled or disabled.
Restricted service agreement	▪ Accepted: PRO3X takes the action only when the specified user accepts the restricted service agreement. ▪ Declined: PRO3X takes the action only when the specified user rejects the restricted service agreement. Both: PRO3X takes the action both when the specified user accepts or rejects the restricted service agreement.
Server monitoring event	▪ Monitoring started: PRO3X takes the action only when the monitoring of any specified server starts. ▪ Monitoring stopped: PRO3X takes the action only when the monitoring of any specified server stops. Both: PRO3X takes the action when the monitoring of any specified server starts or stops.
Server reachability	▪ Unreachable: PRO3X takes the action only when any specified server becomes inaccessible. ▪ Reachable: PRO3X takes the action only when any specified server becomes accessible. Both: PRO3X takes the action when any specified server becomes either inaccessible or accessible.

Device connection or disconnection, such as a USB-cascaded link device	▪ Connected: PRO3X takes the action only when the selected device is physically connected to it. ▪ Disconnected: PRO3X takes the action only when the selected device is physically disconnected from it. Both: PRO3X takes the action both when the selected device is physically connected to it and when it is disconnected.
+12V Supply 1 Status	Available radio buttons include "Fault," "OK" and "Both." ▪ Fault: PRO3X takes the action only when the selected 12V power supply to the controller enters the fault state. ▪ OK: PRO3X takes the action only when the selected 12V power supply to the controller enters the OK state. Both: PRO3X takes the action whenever the selected 12 power supply's status changes.

Default Log Messages

These default log messages, shown in the table on the following pages, are recorded internally and emailed to specified recipients when PRO3X events occur (are TRUE) or, in some cases, stop or become unavailable (are FALSE).

Available Actions

The PRO3X comes with three built-in actions, which cannot be deleted. You can create additional actions for responding to different events.

Built-in actions:

System Event Log Action:

This action records the selected event in the internal log when the event occurs.

System SNMP Notification Action:

This action sends SNMP notifications to one or multiple IP addresses after the selected event occurs.

Note: No IP addresses are specified for this notification action by default so you must enter IP addresses before applying this action to any event rule. See **Editing or Deleting a Rule/Action**. *Any changes made to the 'SNMP Notifications' section on the SNMP page will update the settings of the System SNMP Notification Action, and vice versa.*

System Tamper Alarm:

This action causes the PRO3X to show the alarm for the tamper sensor, if any, on the Dashboard page until a person acknowledges it. By default, this action has been assigned to the built-in tamper detection event rules.

Actions you can create:

Choose Device Settings > Event Rules > ✚ New Action.

Click the Action field to select an action type from the list.

Below is the list of available actions.

Action	Function
Alarm	Requires the user to acknowledge the alert after it is generated. If needed, you can have the alert notifications regularly generated until a person takes the acknowledgment action.
Execute an action group	Creates a group of actions comprising existing actions.
Log event message	Records the selected events in the internal log.
Power control server	Available for outlet-switching capable models.
Send email	Emails a textual message.
Send sensor report	Reports the readings or status of the selected sensors, including internal or external sensors.
Send SMS message	Sends a message to a mobile phone.
Send SNMP notification	Sends SNMP traps or informs to one or multiple SNMP destinations.
Start/stop Lua script	If you are a developer who can create a Lua script, you can upload it to the PRO3X, and have the PRO3X automatically perform or stop the script in response to an event.
Switch outlet group	PRO3X-1000 does NOT support this feature.
Switch peripheral actuator	Switches on or off the mechanism or system connected to the specified actuator.
Syslog message	Makes the PRO3X automatically forward event messages to the specified syslog server.

Enter the information as needed and click Create.

Then you can assign the newly-created action to an event rule or schedule it.

Alarm

The Alarm is an action that requires users to acknowledge an alert. This helps ensure that the user is aware of the alert.

If the Alarm action has been included in a specific event rule and no one acknowledges that alert after it occurs, the PRO3X resends or regenerates an alert notification regularly until the alert is acknowledged or the maximum number of alert notifications is sent.

Operation:

Choose Device Settings > Event Rules > 

.

Select Alarm from the Action list.

In the Alarm Notifications list box, specify one or multiple ways to issue the alert notifications. Available methods vary, depending on how many notification-based actions have been created. Notification-based action types include:

Syslog message

Send email

Send SMS message

To enable the notification-resending feature, select the 'Enable re-scheduling of alarm notifications' checkbox.

In the 'Re-scheduling period' field, specify the time interval (in minutes) at which the alert notification is resent or regenerated regularly.

In the 'Re-scheduling limit' field, specify the maximum number of times the alert notification is resent. Values range from 1 to infinite.

(Optional) You can instruct the PRO3X to send the acknowledgment notification after the alarm is acknowledged in the 'Acknowledgment notifications' field. Available methods are identical to those for generating alarm notifications.

In the Available field, select desired methods one by one, or click Select All. See step 3 for details.

In the Selected field, click any method's  to remove unnecessary ones, or click Deselect All.

Action Group

You can create an action group that performs up to 32 actions. After creating such an action group, you can easily assign this set of actions to any event rule rather than selecting all needed actions one by one per rule.

If the needed action is not available yet, create it first.

Operation:

Choose Device Settings > Event Rules > ➕ New Action.

Select 'Execute an action group' from the Action list.

To select any action(s), select them one by one from the 'Available actions' list.

To select all available actions, click Select All.

To remove any action(s) from the 'Selected actions' field, click that action's ✖.

To remove all actions, click Deselect All.

Log an Event Message

The option 'Log event message' records the selected events in the internal log.

The default log message generated for each type of event is available in the section titled Default Log Messages.

Push Out Sensor Readings

You can configure the PRO3X to push sensor log to a remote server after a certain event occurs, including logs of internal sensors, environmental sensors and actuators.

Before creating this action, make sure that you have properly defined the destination servers and the data to be sent on the Data Push page.

Operation:

Choose Device Settings > Event Rules > ➕ New Action.

Select 'Push out sensor readings' from the Action list.

Select a server or host which receives the data in the Destination field.

If the desired destination is not available yet, go to the Data Push page to specify it.

Send Email

You can configure emails to be sent when an event occurs and can customize the message.

Messages consist of a combination of free text and PRO3X placeholders. The placeholders represent information which is pulled from the PRO3X and inserted into the message.

For example:

```
[USERNAME] logged into the device on [TIMESTAMP]
```

translates to

```
Mary logged into the device on 2012-January-30 21:00
```

Operation:

Choose Device Settings > Event Rules > ➕ New Action.

Select 'Send email' from the Action list.

In the 'Recipient email addresses' field, specify the email address(es) of the recipient(s). Use a comma to separate multiple email addresses.

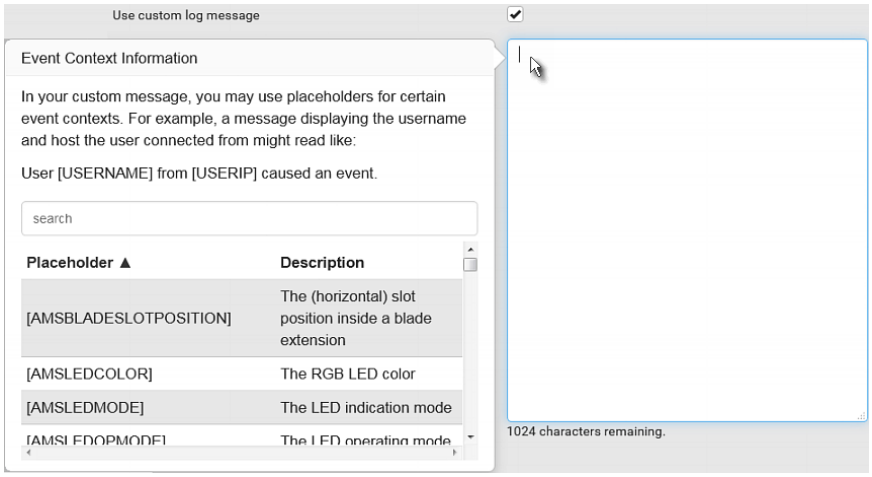
By default, the SMTP server specified on the SMTP Server page will be the SMTP server for performing this action. To use a different SMTP server, select the 'Use custom settings' radio button. The fields for customized SMTP settings appear.

Default messages are sent based on the event. If needed, you can customize the subject and messages sent via this email.

Select the 'Custom subject' checkbox, and enter the text you prefer as this email's subject.

Select the 'Use custom log message' checkbox, and then create a custom message up to 1024 characters in the provided field.

When clicking anywhere inside the text box, the Event Context Information displays, showing a list of placeholders and their definitions. Just scroll down to select the desired placeholder.



To start a new line in the text box, press Enter.

Note: In case you need to type any square brackets "[" and "]" in the custom message for non-placeholder words, always add a backslash in front of the square bracket. That is, \[or \]. Otherwise, the message sent will not display the square brackets.

Send Sensor Report

You may set the PRO3X so that it automatically reports the latest readings or states of one or multiple sensors by sending a message or email or simply recording the report in a log. These sensors can be either internal or environmental sensors listed below.

Inlet sensors, including RMS current, RMS voltage, active power, apparent power, power factor and active energy.

Overcurrent protector sensors, including RMS current and tripping state.

Peripheral device sensors, which can be any environmental sensor packages connected to the PRO3X, such as temperature or humidity sensors.

Operation:

Choose Device Settings > Event Rules > ➕ New Action.

Select 'Send sensor report' from the Action list.

In the 'Destination actions' section, select the method(s) to report sensor readings or states. The number of available methods varies, depending on how many messaging actions have been created.

The messaging action types include:

- Log event message
- Syslog message
- Send email
- Send SMS message

If no messaging actions are available, create them now.

To select any methods, select them one by one in the Available field.

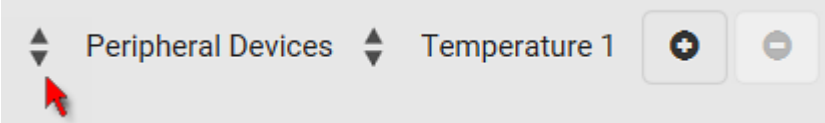
To add all available methods, simply click Select All.

To delete any methods, click a method's ✖ in the Selected field.

To remove all methods, simply click Deselect All.

In the 'Available sensors' field, select the desired target's sensor.

Click the first ▲▼ to select a target component from the list.



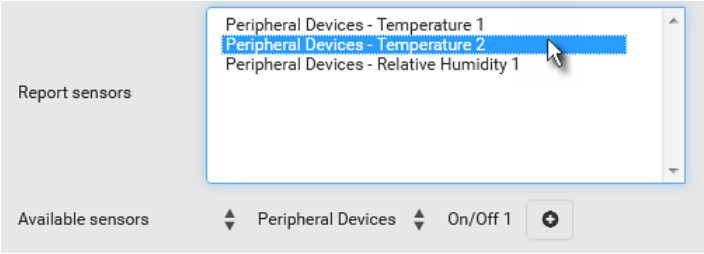
Click the second ▲▼ to select the specific sensor for the target from the list.

Click ⊕ to add the selected sensor to the Report Sensors list box.

For example, to monitor the current reading of the Inlet 1, select Inlet 1 from the left field, and then select RMS Current from the right field.

To report additional sensors simultaneously, repeat the above step to add more sensors.

To remove any sensor from the 'Report sensors' list box, select it and click  . To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.



To immediately send out the sensor report, click Send Report Now.

Tip: When intending to send a sensor report using custom messages, use the placeholder [SENSORREPORT] to report sensor readings.

Send SMS Message

You can configure SMS messages to be sent when an event occurs and can customize the message.

Only the 7-bit ASCII charset is supported for SMS messages. Messages consist of a combination of free text and PRO3X placeholders. The placeholders represent information which is pulled from the PRO3X and inserted into the message.

For example:

```
[USERNAME] logged into the device on [TIMESTAMP]
```

translates to

```
Mary logged into the device on 2012-January-30 21:00
```

Operation:

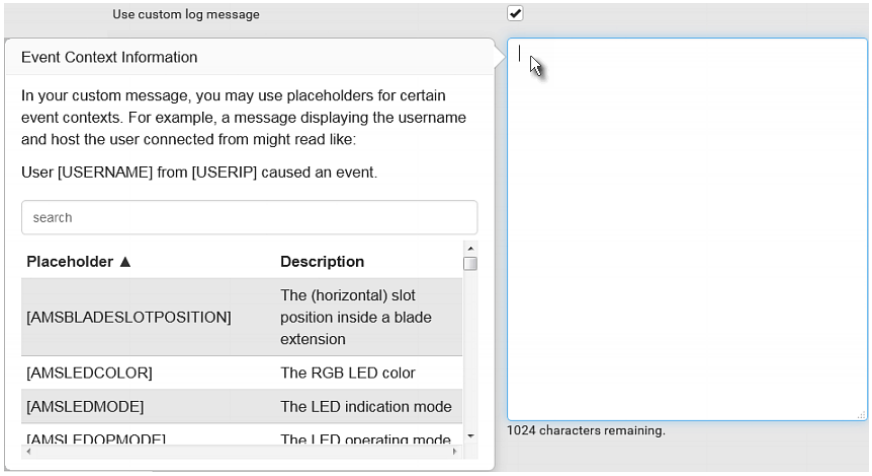
Choose Device Settings > Event Rules > ✚ New Action.

Select 'Send SMS message' from the Action list.

In the 'Recipient phone number' field, specify the phone number of the recipient.

Select the 'Use custom log message' checkbox, and then create a custom message in the provided text box.

When clicking anywhere inside the text box, the Event Context Information displays, showing a list of placeholders and their definitions. Just scroll down to select the desired placeholder.



To start a new line in the text box, press Enter.

Note: In case you need to type any square brackets "[" and "]" in the custom message for non-placeholder words, always add a backslash in front of the square bracket. That is, \[or \]. Otherwise, the message sent will not display the square brackets.

Send an SNMP Notification

This option sends an SNMP notification to one or multiple SNMP destinations.

Operation:

Choose Device Settings > Event Rules > 

.

Select 'Send SNMP notification' from the Action list.

Select the type of SNMP notification. See either procedure below according to your selection.

To send SNMP v2c notifications:

In the 'Notification type' field, select 'SNMPv2c trap' or 'SNMPv2c inform.'

For SNMP INFORM communications, leave the resend settings at their default or do the following:

- In the Timeout field, specify the interval of time, in seconds, after which a new inform communication is resent if the first is not received. For example, resend a new inform communication once every 3 seconds.
- In the 'Number of retries' field, specify the number of times you want to re-send the inform communication if it fails. For example, inform communications are re-sent up to 5 times when the initial communication fails.

In the Host fields, enter the IP address of the device(s) you want to access. This is the address to which notifications are sent by the SNMP system agent.

In the Port fields, enter the port number used to access the device(s).

In the Community fields, enter the SNMP community string to access the device(s). The community is the group representing the PRO3X and all SNMP management stations.

Tip: An SNMP v2c notification action permits only a maximum of three SNMP destinations. To assign more than three SNMP destinations to a specific rule, first create several SNMP v2c notification actions, each of which contains completely different SNMP destinations, and then add all of these SNMP v2c notification actions to the same rule.

To send SNMP v3 notifications:

In the 'Notification type' field, select 'SNMPv3 trap' or 'SNMPv3 inform.'

For SNMP TRAPs, the engine ID is prepopulated.

For SNMP INFORM communications, leave the resend settings at their default or do the following:

- In the Timeout field, specify the interval of time, in seconds, after which a new inform communication is resent if the first is not received. For example, resend a new inform communication once every 3 seconds.
- In the 'Number of retries' field, specify the number of times you want to re-send the inform communication if it fails. For example, inform communications are re-sent up to 5 times when the initial communication fails.

For both SNMP TRAPS and INFORMS, enter the following as needed and then click OK to apply the settings:

- Host name
- Port number
- User ID for accessing the host -- make sure the User ID has the SNMPv3 permission.
- Select the host security level

Security level	Description
"noAuthNoPriv"	Select this if no authorization or privacy protocols are needed.
"authNoPriv"	Select this if authorization is required but no privacy protocols are required. Select the authentication protocol - MD5 or SHA Enter the authentication passphrase and then confirm the authentication passphrase
"authPriv"	Select this if authentication and privacy protocols are required. Select the authentication protocol - MD5 or SHA Enter the authentication passphrase and confirm the authentication passphrase Select the Privacy Protocol - DES or AES Enter the privacy passphrase and then confirm the privacy passphrase

Start or Stop a Lua Script

If you have created or loaded a Lua script file into the PRO3X, you can have that script automatically run or stop in response to a specific event.

To automatically start or stop a Lua script:

Choose Device Settings > Event Rules > 

.

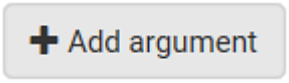
Select 'Start/stop Lua script' from the Action list.

In the Operation field, select 'Start script' or 'Stop script.'

In the Script field, select the script that you want it to be started or stopped when an event occurs.

No script is available if you have not created or loaded it into the PRO3X.

To apply different arguments than the default, do the following. Note that the newly-added arguments will override this script's default arguments.

Click 

.

Type the key and value.

Repeat the same steps to enter more arguments as needed.

To remove any existing argument, click adjacent to it.

Switch Peripheral Actuator

If you have any actuator connected to the PRO3X, you can set up the PRO3X so it automatically turns on or off the system controlled by the actuator when a specific event occurs.

Operation:

Choose Device Settings > Event Rules > 

.

Select 'Switch peripheral actuator' from the Action list.

In the Operation field, select an operation for the selected actuator(s).

Turn on: Turns on the selected actuator(s).

Turn off: Turns off the selected actuator(s).

To select the actuator(s) where this action will be applied, select them one by one from the 'Available actuators' list.

To add all actuators, click Select All.

To remove any selected actuator from the 'Selected actuators' field, click that actuator's  .

To remove all actuators, click Deselect All.

Syslog Message

Use this action to automatically forward event messages to the specified syslog server. Determine the syslog transmission mechanism you prefer when setting it up - UDP, TCP or TLS over TCP.

Transport protocols	Next steps
UDP	▪ In the 'UDP port' field, type an appropriate port number. Default is 514. ▪ Select the 'Legacy BSD syslog protocol' checkbox if applicable.
TCP	NO TLS certificate is required. Type an appropriate port number in the 'TCP port' field.
TCP+TLS	A TLS certificate is required. Do the following: a. Type an appropriate port number in the 'TCP port' field. Default is 6514. b. In the 'CA certificate' field, click  to select a TLS certificate. After importing the certificate, you may: Click Show to view its contents. Click Remove to delete it if it is inappropriate. c. Determine whether to select the 'Allow expired and not yet valid certificates' checkbox. To always send the event message to the specified syslog server as long as a TLS certificate is available, select this checkbox. To prevent the event message from being sent to the specified syslog server when any TLS certificate in the selected certificate chain is outdated or not valid yet, deselect this checkbox.

PRO3X may or may not detect the syslog message transmission failure. If yes, it will log this syslog failure as well as the failure reason in the event log.

Operation:

Choose Device Settings > Event Rules > ➕ New Action.

Select 'Syslog message' from the Action list.

In the 'Syslog server' field, specify the IP address to which the syslog is forwarded.

In the 'Transport protocol' field, select one of the syslog protocols: TCP, UDP or TCP+TLS. The default is UDP.

Scheduling an Action

An action can be regularly performed at a preset time interval instead of being triggered by a specific event. For example, you can make the PRO3X report the reading or state of a specific sensor regularly by scheduling the "Send sensor report" action.

When scheduling an action, make sure you have a minimum of 1-minute buffer between this action's creation and first execution time. Otherwise, the scheduled action will NOT be performed at the specified time when the buffer time is too short. For example, if you want an action to be performed at 11:00 am, you should finish scheduling it at 10:59 am or earlier.

If the needed action is not available yet, create it first.

Operation:

Choose Device Settings > Event Rules > ➕ New Scheduled Action.

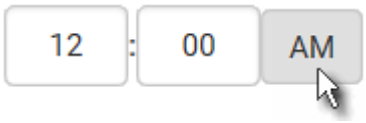
To select any action(s), select them one by one from the 'Available actions' list.

To select all available actions, click Select All.

To remove any action(s) from the 'Selected actions' field, click that action's ✖.

To remove all actions, click Deselect All.

Select the desired frequency in the 'Execution time' field, and then specify the time interval or a specific date and time in the field(s) that appear.

Execution time	Frequency settings
Minutes	Click the Frequency field to select an option. The frequency ranges from every minute, every 5 minutes, every 10 minutes and so on until every 30 minutes.
Hourly	Type a value in the Minute field, which is set to either of the following: ▪ The Minute field is set to 0 (zero). Then the action is performed at 1:00 am, 2:00 am, 3:00 am and so on. ▪ The Minute field is set to a non-zero value. For example, if it is set to 30, then the action is performed at 1:30 am, 2:30 am, 3:30 am and so on.
Daily	Type values or click ▲ ▼. The time is measured in 12-hour format so you must correctly specify AM or PM by clicking the AM/PM button.  For example, if you specify 01:30PM, the action is performed at 13:30 pm every day.
Weekly	Both the day and time must be specified for the weekly option. ▪ Days range from Sunday to Saturday. ▪ The time is measured in 12-hour format so you must correctly specify AM or PM by clicking the AM/PM button.
Monthly	Both the date and time must be specified for the monthly option. ▪ The dates range from 1 to 31. ▪ The time is measured in 12-hour format so you must correctly specify AM or PM by clicking the AM/PM button. Note that NOT every month has the date 31, and February in particular does not have the date 30 and probably even 29. Check the calendar when selecting 29, 30 or 31.
Yearly	This option requires three settings: ▪ Month - January through December. ▪ Day of month - 1 to 31. ▪ Time - the value is measured in 12-hour format so you must correctly specify AM or PM by clicking the AM/PM button.

Send Sensor Report Example

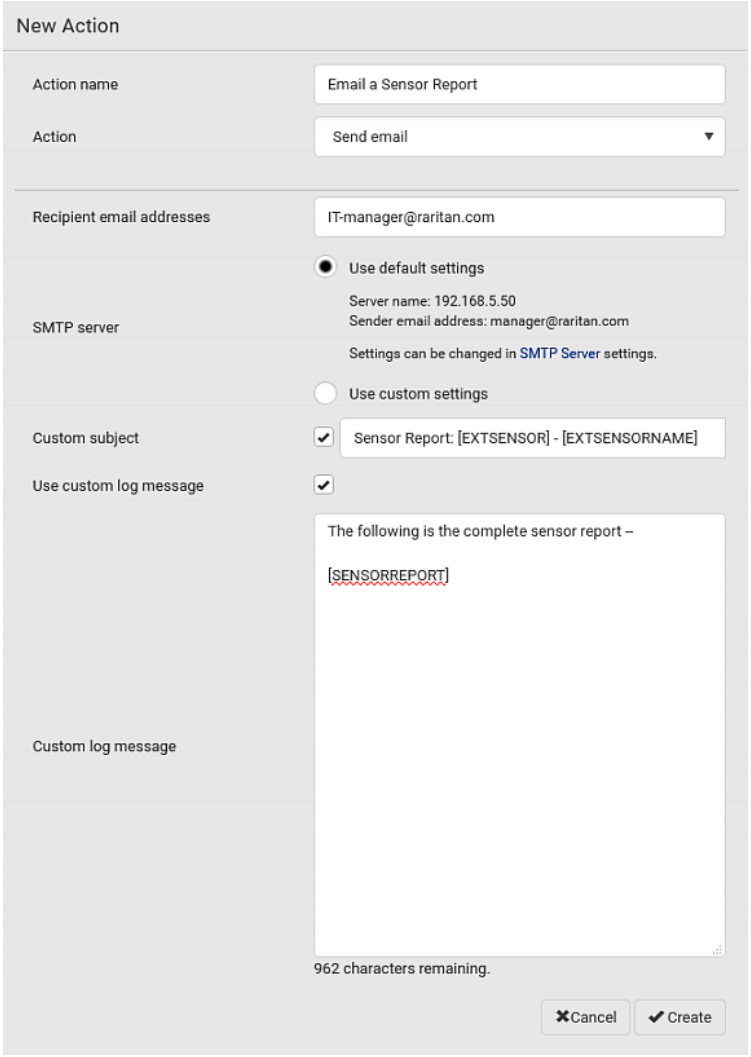
To create a scheduled action for emailing a temperature sensor report hourly, it requires:

- A 'Send email' action
- A 'Send sensor report' action
- A timer - that is, the scheduled action

Steps:

Click ➕ New Action to create a 'Send email' action that sends an email to the desired recipient(s). In this example, this action is named *Email a Sensor Report*.

If wanted, you can customize the subject and content of this email in this action.



Click ➕ New Action to create a 'Send sensor report' action that includes the 'Email a Sensor Report' action as its destination action.

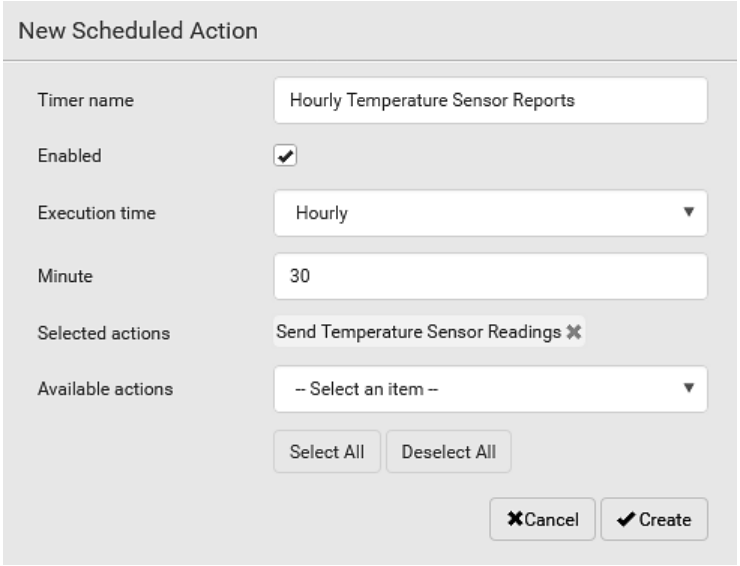
In this example, this action is named *Send Temperature Sensor Readings*.

You can specify more than one temperature sensor as needed in this action.

Click ➕ New Scheduled Action to create a timer for performing the 'Send Temperature Sensor Readings' action hourly.

In this example, the timer is named *Hourly Temperature Sensor Reports*.

To perform the specified action at 12:30 pm, 01:30 pm, 02:30 pm, and so on, select Hourly, and set the Minute to 30.



Then the PRO3X will send out an email containing the specified temperature sensor readings hourly every day.

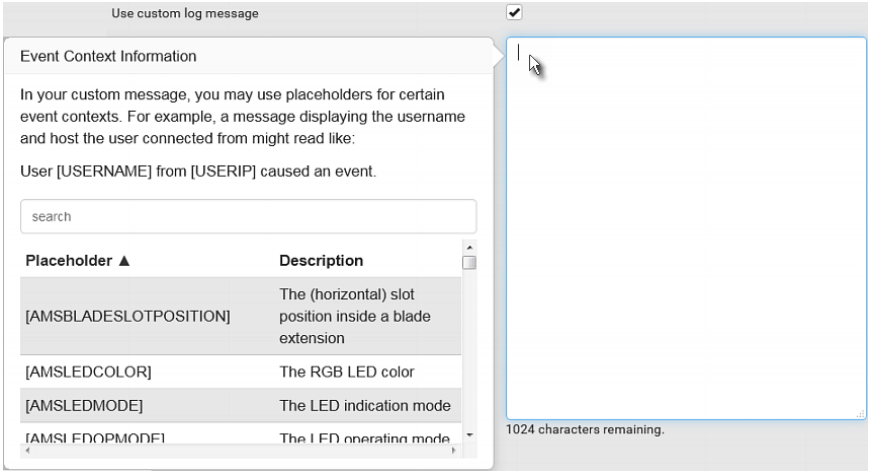
Whenever you want the PRO3X to stop sending the temperature report, simply deselect the Enabled checkbox in the timer.

Placeholders for Custom Messages

Actions of "Send email" and "Send SMS message" allow you to customize event messages.

When clicking anywhere inside the text box, the Event Context Information displays, showing a list of placeholders and their definitions. Simply drag the scroll bar and then click the desired placeholder to insert it into the custom message. Or you can type a keyword in the "search" box to quickly find the desired placeholder.

Note that available placeholders are model dependent.



If wanted, you can resort the list by clicking the desired column header.

To make the Event Context Information disappear, click anywhere inside the browser's window.

Editing or Deleting a Rule/Action

You can change the settings of an event rule, action or scheduled action, or delete them.

Exception: Some settings of the built-in event rules or actions are not user-configurable. Besides, you cannot delete built-in rules and actions.

To edit or delete an event rule, action or scheduled action:

Choose Device Settings > Event Rules.

Click the desired one in the list of rules, actions or scheduled actions. Its setup page opens.

Perform the desired action.

To modify settings, make necessary changes and then click Save.

To delete it, click Delete on the top-right corner. Then click Delete on the confirmation message.

Sample Event Rules

Sample PDU-Level Event Rule

In this example, we want the PRO3X to record the firmware upgrade failure in the internal log when it happens.

The event rule involves:

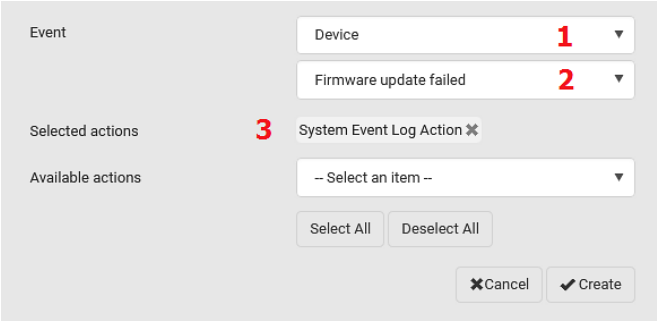
- Event: Device > Firmware update failed
- Action: System Event Log Action

To create this PDU-level event rule:

For an event at the PDU level, select "Device" in the Event field.

Select "Firmware update failed" so that the PRO3X responds to the event related to firmware upgrade failure.

To make PRO3X record the firmware update failure event in the internal log, select "System Event Log Action" in the 'Available actions' field.



Sample Outlet-Level Event Rule

In this example, we want the PRO3X to send SNMP notifications to the SNMP manager for any sensor change event of outlet 3.

The event rule involves:

Event: Outlet > Outlet 3 > Sensor > Any sub-event

Action: System SNMP Notification Action

To create this outlet-level event rule:

For an event at the outlet level, select "Outlet" in the Event field.

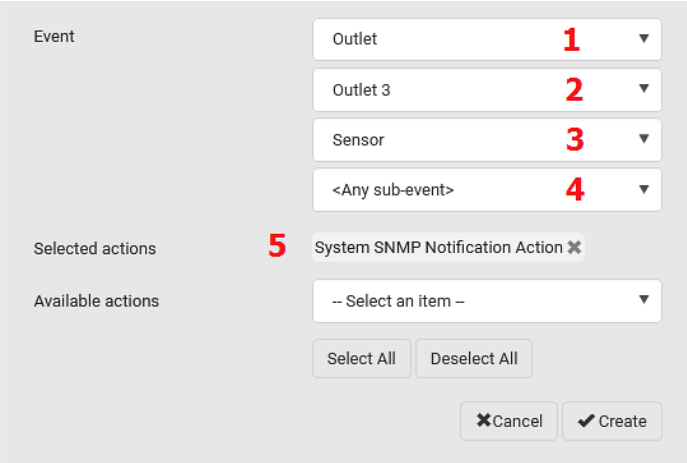
Select "Outlet 3" because that is the desired outlet.

Select "Sensor" to refer to sensor-related events.

Select "Any sub-event" to include all events related to all sensors of this outlet and all thresholds, such as current, voltage, upper critical threshold, upper warning threshold, lower critical threshold, lower warning threshold, and so on.

To make PRO3X send SNMP notifications, select "System SNMP Notification Action" in the 'Available actions' field.

Note: The SNMP notifications may be SNMP v2c or SNMP v3 traps/informs, depending on the settings for the System SNMP Notification Action.



Then the SNMP notifications are sent when:

Any numeric sensor's reading enters the warning or critical range.

Any sensor reading or state returns to normal.

Any sensor becomes unavailable.

The active energy sensor is reset.

Any state sensor changes its state.

For example, when the outlet 3's voltage exceeds the upper warning threshold, the SNMP notifications are sent, and when the voltage drops below the upper warning threshold, the SNMP notifications are sent again.

Sample Inlet-Level Event Rule

In this example, we want the PRO3X to send SNMP notifications to the SNMP manager for any sensor change event of the Inlet I1.

The event rule involves:

- Event: Inlet > Sensor > Any sub-event
- Action: System SNMP Notification Action

To create the above event rule:

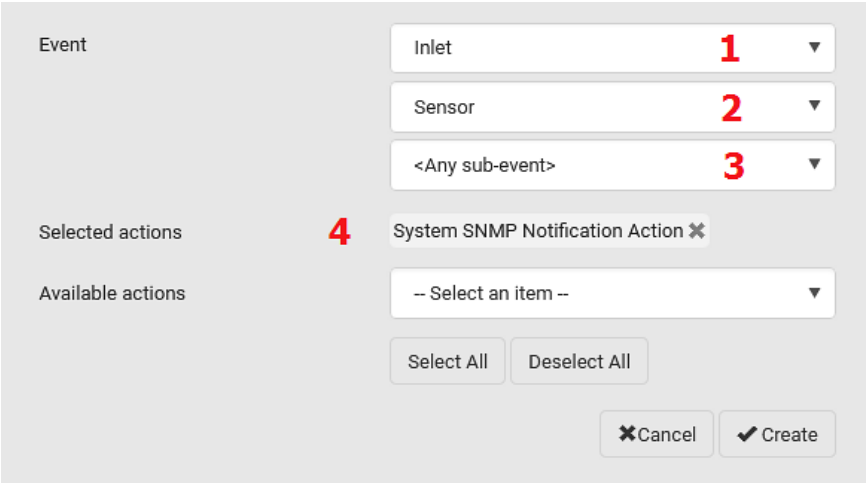
For an event at the inlet level, select "Inlet" in the Event field.

Select "Sensor" to refer to sensor-related events.

Select "Any sub-event" to include all events related to all sensors of this inlet and all thresholds, such as current, voltage, upper critical threshold, upper warning threshold, lower critical threshold, lower warning threshold, and so on.

To make the PRO3X send SNMP notifications, select "System SNMP Notification Action" in the 'Available actions' box.

Note: The SNMP notifications may be SNMP v2c or SNMP v3 traps/informs, depending on the settings for the System SNMP Notification Action.



Then the SNMP notifications are sent when:

Any numeric sensor's reading enters the warning or critical range.

Any sensor reading or state returns to normal.

Any sensor becomes unavailable.

The active energy sensor is reset.

For example, when the Inlet I1's voltage exceeds the upper warning threshold, the SNMP notifications are sent, and when the voltage drops below the upper warning threshold, the SNMP notifications are sent again.

A Note About Infinite Loop

You should avoid building an infinite loop when creating event rules.

The infinite loop refers to a condition where the PRO3X keeps busy because the action or one of the actions taken for a certain event triggers an identical or similar event which will result in an action triggering one more event.

Example 1

This example illustrates an event rule which continuously causes the PRO3X to send out email messages.

Event selected	Action included
Device > Sending SMTP message failed	Send email

Example 2

This example illustrates an event rule which continuously causes the PRO3X to send out SMTP messages when one of the selected events listed on the Device menu occurs. Note that <Any sub-event> under the Device menu includes the event "Sending SMTP message failed."

Event selected	Action included
Device > Any sub-event	Send email

Example 3

This example illustrates a situation where two event rules combined regarding the outlet state changes causes the PRO3X to continuously power cycle outlets 1 and 2 in turn.

Event selected	Action included
Outlet > Outlet 1 > Sensor > Outlet State > On/Off > Both (trigger condition)	Cycle Outlet 2 (Switch outlets --> Cycle Outlet --> Outlet 2)
Outlet > Outlet 2 > Sensor > Outlet State > On/Off > Both (trigger condition)	Cycle Outlet 1 (Switch outlets --> Cycle Outlet --> Outlet 1)

A Note about Untriggered Rules

In some cases, a measurement exceeds a threshold causing the PRO3X to generate an alert. The measurement then returns to a value within the threshold, but the PRO3X does not generate an alert message for the de-assertion event. Such scenarios can occur due to the hysteresis tracking the PRO3X uses.

Setting Data Logging

The PRO3X can store 120 measurements for each sensor in a memory buffer. This memory buffer is known as the data log. Sensor readings in the data log can be retrieved using SNMP.

You can configure how often measurements are written into the data log using the Measurements Per Log Entry field. Since the PRO3X internal sensors are measured every second, specifying a value of 60, for example, would cause measurements to be written to the data log once every minute. Since there are 120 measurements of storage per sensor, specifying a value of 60 means the log can store the last two hours of measurements before the oldest one in the log gets overwritten.

Whenever measurements are written to the log, three values for each sensor are written: the average, minimum and maximum values. For example, if measurements are written every minute, the average of all measurements that occurred during the preceding 60 seconds along with the minimum and maximum measurement values are written to the log.

Note: The PRO3X device's SNMP agent must be enabled for this feature to work. In addition, using an NTP time server ensures accurately time-stamped measurements.

By default, data logging is enabled. You must have the "Administrator Privileges" or "Change Pdu, Inlet, Outlet & Overcurrent Protector Configuration" permissions to change the setting.

To configure the data logging feature:

Choose Device Settings > Data Logging.

To enable the data logging feature, select the "Enable" checkbox in the General Settings section.

Type a number in the Measurements Per Log Entry field. Valid range is from 1 to 600. The default is 60.

Verify that all sensor logging is enabled. If not, click Enable All at the bottom of the page to have all sensors selected.

You can also click the topmost checkbox labeled "Logging Enabled" in the header row of each section to select all sensors of the same type.

If any section's number of sensors exceeds 35, the remaining sensors are listed on next page(s). If so, a pagination bar similar to the following diagram displays in this section, which you can click any button to switch between pages.

Click Save. This button is located at the bottom of the page.

Important: Although it is possible to selectively enable/disable logging for individual sensors on the PRO3X, it is NOT recommended to do so.

Configuring Data Push Settings

The data will be sent in JSON format using HTTP POST requests.

After configuring the destination and authentication settings, do either or both of the following:

To perform the data push after the occurrence of a certain event, create the data push action and assign it to an event rule.

To push the data at a regular interval, schedule the data push action.

To configure data push settings:

Choose Device Settings > Data Push.

To specify a destination, click 

.

Do the following to set up the URL field.

Click  to select *http* or *https*.

Type the URL or host name in the accompanying text box.

If selecting https, a CA certificate is required for making the connection. Click 

to install it. Then you can:

Click Show to view the certificate's content.

Click Remove to delete the installed certificate if it is inappropriate.

If the destination server requires authentication, select the 'Use authentication' checkbox, and enter the following data.

User name comprising up to 64 characters

Password comprising up to 128 characters

In the 'Entry type' field, determine the data that will be transmitted.

- *Sensor log:* Transmit the record of all logged sensors, including their sensor readings and/or status. Logged sensors refer to all internal and/or environmental sensors/actuators that you have selected on the Data Logging page.

Repeat the same steps for additional destinations. Up to 64 destinations are supported.

To immediately push out the data:

On the Data Push page, choose the one whose data you want to push out.

Click its 

.

To modify or delete data push settings:

On the Data Push page, click the one you want in the list.

Perform either action below.

To modify settings, make necessary changes and then click Save.

To delete it, click 

, and then confirm it on the confirmation message.

Data Push Format

Each push message contains exactly one JSON object. The data format is formally defined in IDL files, sharing several definitions from the JSON-RPC data model.

```
{
    "device": {
        "type": 0,              // Inlet sensor (see DeviceType enumeration)
        "label": "I1",          // Inlet label: I1
        "line": 0               // Power line; not applicable for inlet sensors
    },
    "id": "activePower",        // Sensor identification
    "readingtype": 0,           // Reading type: numeric
    "metadata": {
        "type": {
            "readingtype": 0,   // Reading type: numeric
            "type": 5,          // Sensor type: Active power
            "unit": 3           // Reading unit: Watt
        },
        "decdigits": 0,         // No decimal digits
        "accuracy": 1.0,        // Accuracy: 1 percent
        "resolution": 1.0,      // Reading resolution: 1 W
        "tolerance": 1.5,       // Reading tolerance: +/- 1.5 W
        "range": {
            "lower": 0.0,       // Minimum reading: 0 W
            "upper": 30000.0    // Maximum reading: 30 kW
        }
    }
}
```

Sensor Log

The root object of the message is a `SensorLogPushMessage` structure. It comprises a list of sensor descriptors and a list of log rows.

Sensor descriptors:

The sensor descriptor vector contains static information of all logged sensors, including:

The electrical component a sensor is associated with. For example, an inlet pole or an overcurrent protector.

The sensor's type. For example, RMS current or active energy.

Unit and range of the sensor's readings.

Log rows:

Each log row consists of a time stamp (accumulated seconds since 1/1/1970) and a list of log records -- one for each logged sensor.

The length and order of the record list is the same as the sensor descriptor vector.

Sensor Descriptors for Inlet Active Power

The following illustrates a descriptor for an inlet active power sensor.

The `metadata` field is relevant only to numeric sensors so the `readingtype` field is displayed twice in the illustration.

Note that a Server Technology-provided explanation, which is the comment beginning with // in each line, is added to the following illustration for you to understand it better.

Log Rows

The following illustrates log rows with only one sensor record shown.

The actual length and order of log rows will be the same as those of sensors descriptors.

Note that a Server Technology-provided explanation, which is the comment beginning with // in each line, is added to the following illustration for you to understand it better.

```
{
    "timestamp": 1334052852,            // Time stamp (seconds since 1/1/1970)
    "records": [
        {
            "available": true,          // This record is available
            "takenValidSamples": 60,    // Number of valid samples in this log period
            "state": 5,                 // Sensor was in normal range
            "minValue": 5800.0,         // Minimum sensor value: 5.8 kW
            "avgValue": 5900.0,         // Average sensor value: 5.9 kW
            "maxValue": 6100.0          // Maximum sensor value: 6.1 kW
        },
        {
            // [...] record for next sensor
        }
    ]
}
```

Monitoring Server Accessibility

You can monitor whether specific IT devices are alive by having the PRO3X continuously ping them. An IT device's successful response to the ping commands indicates that the IT device is still alive and can be remotely accessed.

This function is especially useful when you are not located in an area with Internet connectivity.

PRO3X can monitor any IT device, such as database servers, remote authentication servers, power distribution units (PDUs), and so on. It supports monitoring a maximum of 64 IT devices.

To perform this feature, you need the Administrator Privileges.

The default ping settings may not be suitable for monitoring devices that require high connection reliability so it is strongly recommended that you should adjust the ping settings for optimal results.

Tip: To make the PRO3X automatically log, send notifications or perform other actions for any server monitoring events, you can create event rules.

To add IT equipment for ping monitoring:

Choose Device Settings > Server Reachability.

Click + Monitor New Server.

By default, the "Enable ping monitoring for this server" checkbox is selected. If not, select it to enable this feature.

Configure the following.

Field	Description
IP address/hostname	IP address or host name of the IT equipment which you want to monitor.
Number of successful pings to enable feature	The number of successful pings required to declare that the monitored equipment is "Reachable." Valid range is 0 to 200.
Wait time after successful ping	The wait time before sending the next ping if the previous ping was successfully responded. Valid range is 5 to 600 (seconds).
Wait time after unsuccessful ping	The wait time before sending the next ping if the previous ping was not responded. Valid range is 3 to 600 (seconds).
Number of consecutive unsuccessful pings for failure	The number of consecutive pings without any response before the monitored equipment is declared "Unreachable." Valid range is 1 to 100.
Wait time before resuming pinging after failure	The wait time before the PRO3X resumes pinging after the monitored equipment is declared "Unreachable." Valid range is 1 to 1200 (seconds).
Number of consecutive failures before disabling feature (0 = unlimited)	The number of times the monitored equipment is declared "Unreachable" consecutively before the PRO3X disables the ping monitoring feature for it and shows "Waiting for reliable connection." Valid range is 0 to 100.

Click Create.

To add more IT devices, repeat the same steps.

Editing or Deleting Ping Monitoring Settings

You can edit the ping monitoring settings of any IT device or simply delete it if no longer needed.

To modify or delete any monitored IT device:

Choose Device Settings > Server Reachability.

Click the desired one in the list.

Perform the desired action.

To modify settings, make necessary changes and then click Save.

To delete it, click 

on the top-right corner.

Example: Ping Monitoring and SNMP Notifications

In this illustration, it is assumed that a significant PDU (IP address: 192.168.84.95) shall be monitored by your PRO3X to make sure that PDU is properly operating all the time, and the PRO3X must send out SNMP notifications (trap or inform) if that PDU is declared unreachable due to power or network failure. The prerequisite for this example is that the power sources are different between your PRO3X and the monitored PDU.

This requires the following two steps.

Step 1: Set up the ping monitoring for the target PDU

Choose Device Settings > Server Reachability.

Click 

.

Ensure the "Enable ping monitoring for this server" checkbox is selected.

Enter the data shown below.

Enter the server's data.

Field	Data entered
IP address/hostname	192.168.84.95

To make the PRO3X declare the accessibility of the monitored PDU every 15 seconds (3 pings * 5 seconds) when that PDU is accessible, enter the following data.

Field	Data entered
Number of successful pings to enable feature	3
Wait time after successful ping	5

To make the PRO3X declare the inaccessibility of the monitored PDU when that PDU becomes inaccessible for around 12 seconds (4 seconds * 3 pings), enter the following data.

Field	Data entered
Wait time after unsuccessful ping	4
Number of consecutive unsuccessful pings for failure	3

To make the PRO3X stop pinging the target PDU for 60 seconds (1 minute) after the PDU inaccessibility is declared, enter the following data. After 60 seconds, the PRO3X will re-ping the target PDU.

Field	Data entered
Wait time before resuming pinging after failure	60

The "Number of consecutive failures before disabling feature (0 = unlimited)" can be set to any value you want.

Click Create.

Step 2: Create an event rule to send SNMP notifications for the target PDU

Choose Device Settings > Event Rules.

Click 

.

Select the Enabled checkbox to enable this new rule.

Configure the following.

Field/setting	Data specified
Rule name	Send SNMP notifications for PDU (192.168.84.95) inaccessibility
Event	Choose Server Monitoring > 192.168.84.95 > Unreachable
Trigger condition	Select the Unreachable radio button

This will make the PRO3X react only when the target PDU becomes inaccessible.

Select the System SNMP Notification Action.

Front Panel Settings

You can set up the default mode of the front panel display, and front panel functions for actuator control, or RCM self-test.

Note that available front panel settings are model dependent.

- Actuator control -- available on all models.
- Default front panel mode setup -- available on all models.
- RCM self-test -- available on those PRO3X models which support residual current monitoring.

To configure the front panel settings:

Choose Device Settings > Front Panel.

Configure the following:

To configure the default view of the LCD display, select one mode below.

Mode	Data entered
Automatic mode	The LCD display cycles through both the inlet and overcurrent protector information. This is the default. Overcurrent protector information is available only when your PRO3X has overcurrent protectors.
Inlet overview	The LCD display cycles through the inlet information only.

To enable the front panel actuator-control function, select the 'Peripheral actuator control' checkbox.

- By default the front panel RCM self-test function, if available, is enabled.
- Click Save.

Configuring the Serial Port

You can change the bit rate of the serial port labeled CONSOLE / MODEM on the PRO3X. The default bit rate for console and modem operation is 115200 bps.

The PRO3X supports using the following devices via the serial interface:

- A computer for console management.
- An analog modem for remote dial-in and access to the CLI.
- A GSM modem for sending out SMS messages to a cellular phone.

Bit-rate adjustment may be necessary. Change the bit rate before connecting the supported device to the PRO3X through the serial port, or there are communication problems.

You can set diverse bit-rate settings for console and modem operations. Usually the PRO3X can detect the device type, and automatically apply the preset bit rate.

The PRO3X will indicate the detected device in the Port State section of the Serial Port page.

To configure serial port and modem settings, choose Device Settings > Serial Port.

To change the serial port's baud rate settings:

Click the 'Connected device' field to make the serial port enter an appropriate state.

Options	Description
Automatic detection	The PRO3X automatically detects the type of the device connected to the serial port. Select this option unless your PRO3X cannot correctly detect the device type.
Force console	The PRO3X attempts to recognize that the connected device is set for the console mode.
Force analog modem	The PRO3X attempts to recognize that the connected device is an analog modem.
Force GSM modem	The PRO3X attempts to recognize that the connected device is a GSM modem.

Click the 'Console baud rate' field to select the baud rate intended for console management.

Note: For a serial RS-232 or USB connection between a computer and the PRO3X, leave it at the default (115200 bps).

Click the 'Modem baud rate' field to select the baud rate for the modem connected to the PRO3X.

The following modem settings/fields appear in the web interface after the PRO3X detects the connection of an analog or GSM modem.

To configure the analog modem:

Select the 'Answer incoming calls' checkbox to enable the remote access via a modem. Otherwise, deselect it.

Type a value in the 'Number of rings before answering' field to determine the number of rings the PRO3X must wait before answering the call.

To configure the GSM modem:

Enter the SIM PIN code.

Select the 'Use custom SMS center number' checkbox if a custom SMS center will be used.

Enter the SMS center number in the 'SMS center' field.

If needed, click Advanced Information to view detailed information about the modem, SIM and mobile network.

To test whether the PRO3X can successfully send out SMS messages with the modem settings:

Enter the number of the recipient's phone in the Recipient Phone field.

Click Send SMS Test to send a test SMS message.

Lua Scripts

If you can write or obtain any Lua scripts, you can create or load them into the PRO3X to control its behaviors.

Note: Not all Lua script examples can apply to your PRO3X model. You should read each example's introduction before applying them.

You must have the Administrator Privileges to manage Lua scripts.

Writing or Loading a Lua Script

You can enter or load up to 4 scripts to the PRO3X.

Tip: If you can no longer enter or load a new script after reaching the upper limit, you can either delete any existing script or simply modify/replace an existing script's codes.

To write or load a Lua script:

Choose Device Settings > Lua Scripts > 

.

Type a name for this script. Its length ranges between 1 to 63 characters.

The name must contain the following characters only.

Alphanumeric characters

Underscore (_)

Minus (-)

Note: Spaces are NOT permitted.

Determine whether and when to automatically execute the loaded script.

Checkbox	Behavior when selected
Start automatically at system boot	Whenever the PRO3X reboots, the script is automatically executed.
Restart after termination	The script is automatically executed each time after 10 seconds since the script execution finishes.

(Optional) Determine the arguments that will be executed by default.

Click ➕ Add argument.

Type the key and value.

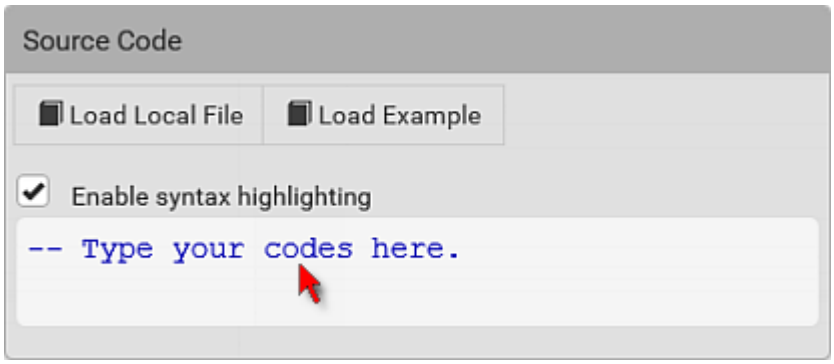
Repeat the same steps to enter more arguments as needed.

To remove any existing argument, click ➖ adjacent to it.

Note: The above default arguments will be overridden by new arguments specified with the "Start with Arguments" command or with any Lua-script-related event rule.

In the Source Code section, do one of the following. It is recommended to leave the Enable Syntax Highlighting checkbox selected unless you do not need different text colors to identify diverse code syntaxes.

To write a Lua script, type the codes in the Source Code section.



To load an existing Lua script file, click Load Local File.

To use a Lua script example, click Load Example.

Warning: The newly-loaded script will overwrite all existing codes in the Source Code section. Therefore, do not load a new script if the current script meets your needs.

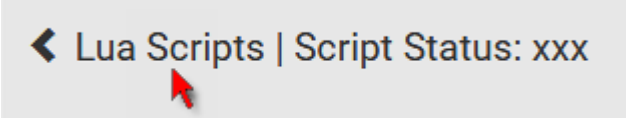
If you chose to load a script or example in the previous step, its codes are then displayed in the Source Code section. Double check the codes. If needed, modify the codes to meet your needs.

Click Create.

Next steps:

To execute the newly-added script immediately, click ▶ Start, or click ⋮ > Start with Arguments.

To add more scripts, first return to the scripts list by clicking "Lua Scripts" on the top (see below) or in the Menu, and then repeat the above steps.



Manually Starting or Stopping a Script

You can manually start or stop an existing Lua script at any time.

When starting a script, you can choose to start it either with its default arguments or with new arguments.

Tip: To have the PRO3X automatically start or stop a script in response to an event, create an event rule.

To manually start a script:

Choose Device Settings > Lua Scripts. The Lua scripts list displays.

Lua Scripts ✚ Create New Script

Name	State	Autostart	Restart
script-1	Terminated	yes	no
script-2	New	no	yes
script-3	Running	no	yes

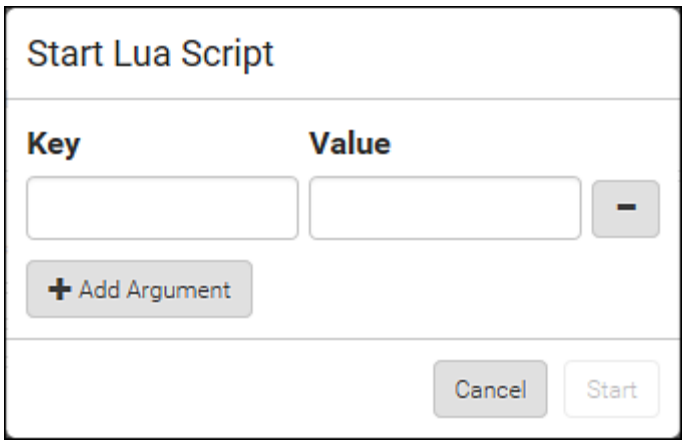
Click the desired script whose state is either 'Terminated' or 'New.'

To start with default arguments, click ▶ Start.

To start with new arguments, click ⋮ > Start with Arguments. Newly-assigned arguments will override default ones.

If you chose "Start With Arguments" in the above step, enter the key and value in the Start Lua Script dialog.

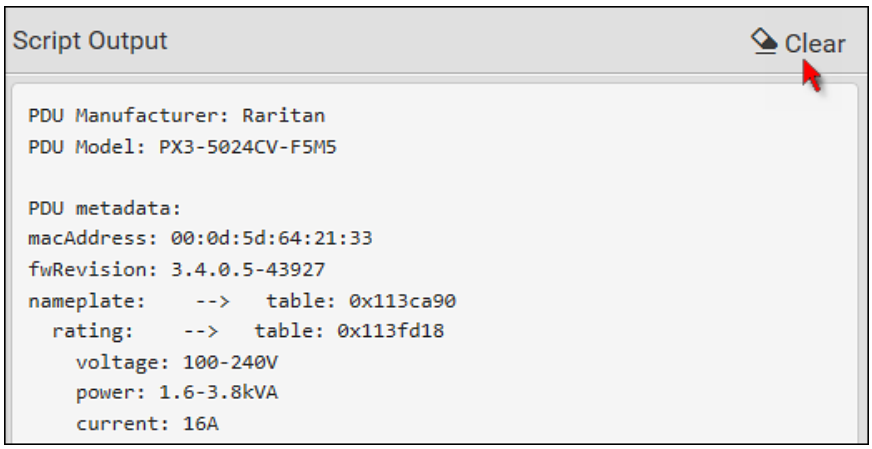
Click ✚ Add argument if needing additional arguments.



Click Start.

The script output will be shown in the Script Output section.

If needed, click Clear to delete the existing output data.



To manually stop a script:

To mannChoose Device Settings > Lua Scripts.

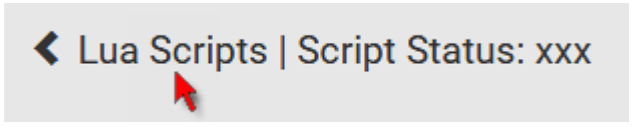
Click the desired script whose state is either 'Running' or 'Restarting.'

Click Stop on the top-right corner.

Click Stop on the confirmation message.

To return to the scripts list:

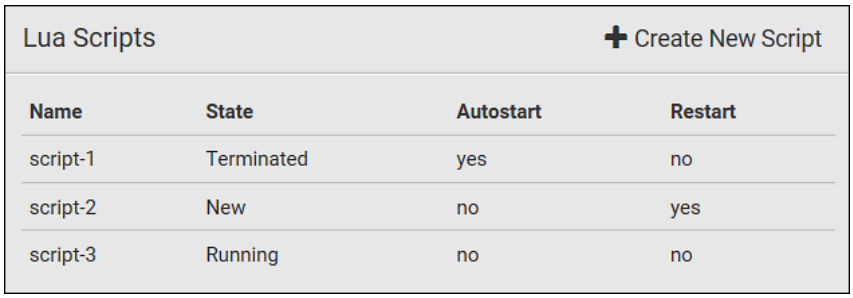
Click "Lua Scripts" on the top of the page.



Or click "Lua Scripts" in the Menu.

Checking Lua Scripts States

Choose Device Settings > Lua Scripts to show the scripts list, which indicates the current state and settings of each script.



State:

Four script states are available.

State	Description
New	The script is never executed since the device boot.
Running	The script is currently being executed.
Terminated	The script was once executed, but stops now.
Restarting	The script will be executed. Only the scripts with the "Restart" column set to "yes" will show this state.

Autostart:

This column indicates whether the checkbox labeled "Start automatically at system boot" is enabled.

Restart:

This column indicates whether the checkbox labeled "Restart after termination" is enabled.

Modifying or Deleting a Script

You can edit an existing script's codes or even replace it with a new script. Or you can remove an unnecessary script from the PRO3X.

To modify or replace a script:

Choose Device Settings > Lua Scripts.

Click the desired one in the scripts list.

Click ⋮ > Edit Script.

Make changes to the information shown, except for the script's name, which cannot be revised.

To replace the current script, click Load Local File or Load Example to select a new script.

To delete a script:

Choose Device Settings > Lua Scripts.

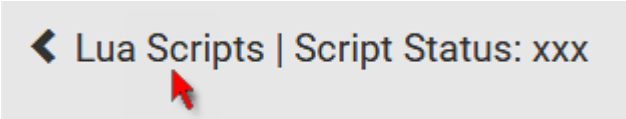
Click the desired one in the scripts list.

Click ⋮ > Delete.

Click Delete on the confirmation message.

To return to the scripts list:

Click "Lua Scripts" on the top of the page.



Or click "Lua Scripts" in the Menu.

Miscellaneous

If a Cisco® EnergyWise energy management architecture is implemented in your place, you can enable the Cisco EnergyWise endpoint implemented on the PRO3X so that this PRO3X becomes part of the Cisco EnergyWise domain.

In addition, if you have to prevent others from accessing your PRO3X via USB-A for security reasons, you can disable all of USB-A ports on the PRO3X. By default, USB-A ports are enabled.

Important: Disabling USB-A ports will disable all of 'USB-A' based features, such as wireless networking, USB cascading or pdView access using iOS mobile devices. Therefore, re-think about it before disabling USB-A.

To configure any of the above features, choose Device Settings > Miscellaneous.

To set the Cisco EnergyWise configuration:

Select the Enable EnergyWise checkbox.

Configure the following:

Field	Description
Domain name	Type the name of a Cisco EnergyWise domain where the PRO3X belongs ▪ Up to 127 printable ASCII characters are permitted. ▪ Spaces and asterisks are NOT acceptable.
Domain password	Type the authentication password (secret) for entering the Cisco EnergyWise domain ▪ Up to 127 printable ASCII characters are permitted. ▪ Spaces and asterisks are NOT acceptable.
Port	Type a User Datagram Protocol (UDP) port number for communications in the Cisco EnergyWise domain. ▪ Range from 1 to 65535. ▪ Default is 43440.
Polling interval	Type a polling interval to determine how often the PRO3X is queried in the Cisco EnergyWise domain. ▪ Range from 30 to 600 ms. ▪ Default is 180 ms.

Click Save in the *EnergyWise* section.

The PDU becomes a parent domain member.

All outlets become children of the PDU.

To disable the access to USB-A port(s):

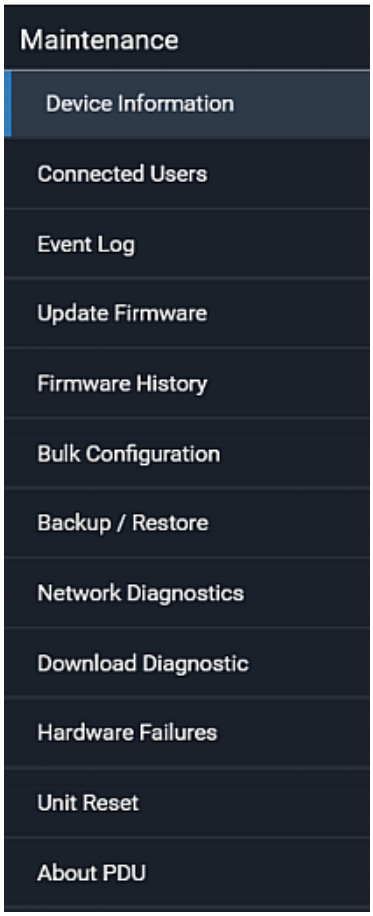
Deselect the Enable USB Host Ports checkbox.

Click Save in the USB Host Ports section.

Tip: After the Enable USB Host Ports checkbox is deselected, only the access to USB-A port(s) is prevented while the USB-B port works as normal. That is, users still can access the USB-B port, such as accessing CLI via USB-B. To disable the access to the USB-B port, you have to apply a mechanical method.

Maintenance

Click 'Maintenance' in the Menu, and the following submenu displays.



Submenu command	Refer to...
Device Information	*Device Information*
Connected Users	*Viewing Connected Users*
Event Log	*Viewing or Clearing the Local Event Log*
Update Firmware	*Updating the PRO3X Firmware*
Firmware History	*Viewing Firmware Update History*
Bulk Configuration	*Bulk Configuration*
Backup/Restore	*Backup and Restore of Device Settings*
Network Diagnostic	*Network Diagnostics*
Download Diagnostic	*Downloading Diagnostic Information*
Hardware Failures	*Hardware Issue Detection*
Unit Reset	▪ *Rebooting the PRO3X* ▪ *Resetting All Settings to Factory Defaults*
About PDU	*Retrieving Software Packages Information*

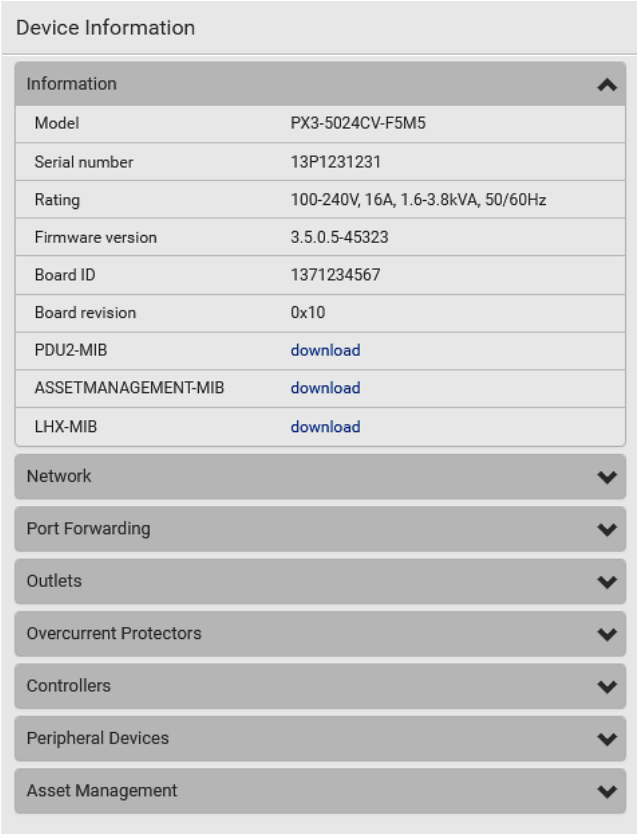
Device Information

Using the web interface, you can retrieve hardware and software information of components or peripheral devices connected to your PRO3X.

Tip: If the information shown on this page does not match the latest status, press F5 to reload it.

To display device information:

Choose Maintenance > Device Information.



Click the desired section's title bar to show that section's information. For example, click the Network section.

The number of available sections is model dependent.

Section title	Information shown
Information	General device information, such as model name, serial number, firmware version, hardware revision, MIB download link(s) and so on.
Network	The network information, such as the current networking mode, IPv4 and/or IPv6 addresses and so on. This tab also indicates whether the PRO3X is part of a cascading configuration.
Port Forwarding	If the port forwarding mode is activated, this section will show a list of port numbers for all cascaded devices.
Outlets	Each outlet's receptacle type, operating voltage and rated current.
Overcurrent Protectors	Each overcurrent protector's type, rated current and the outlets that it protects.
Controllers	Each inlet or outlet controller's serial number, board ID, firmware version and hardware version.
Inlets	Each inlet's plug type, rated voltage and current.
Peripheral Devices	Serial numbers, model names, position and firmware-related information of connected environmental sensor packages.

Identifying Cascaded Devices

This section explains how to identify a cascaded device on the Device Information page.

To identify the cascading status:

Choose Maintenance > Device Information.

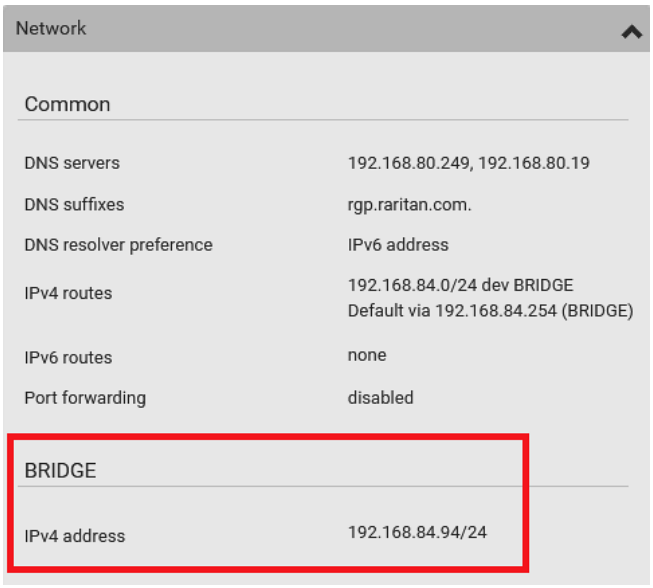
Click the Network title bar.

If the information shown on this page does not match the latest status, press F5 to reload it.

Cascading information in the Bridging mode:

The Common section contains two read-only fields for indicating the cascading status. Note that the cascading position is NOT available in the Bridging mode.

Fields	Description
Port forwarding	Indicates the Port Forwarding is disabled.
BRIDGE section	Indicates the device is in the Bridging mode and its IP address.

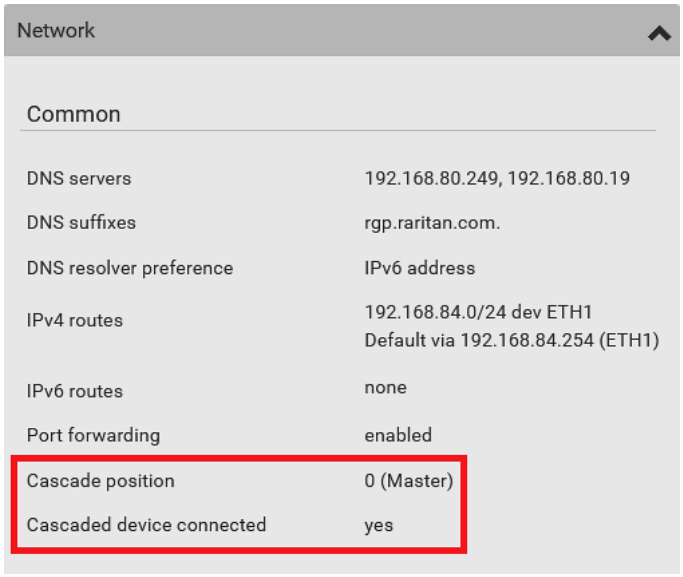


Cascading information in the Port Forwarding mode:

The Common section contains three read-only fields for indicating the cascading status.

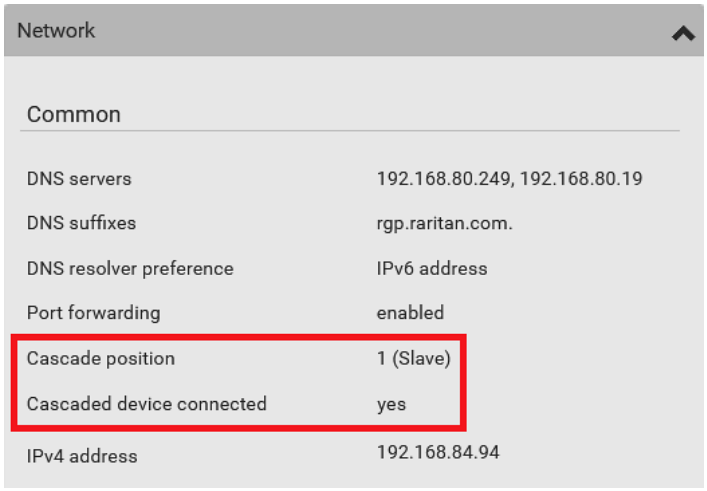
Fields	Description
Port forwarding	Indicates the Port Forwarding is enabled.
Cascade position	Indicates the position of the PRO3X in the cascading chain. ▪ 0 (zero) represents the master device. ▪ A non-zero number represents a link device. 1 is Link 1, 2 is Link 2, 3 is Link 3 and so on.
Cascaded device connected	Indicates whether a link device is detected on the USB-A or Ethernet port. ▪ yes: Connection to a link device is detected. ▪ no: NO connection to a link device is detected.

A master device shows *0* (zero) in the 'Cascade position' field and *yes* in the 'Cascaded device connected' field.



A link device in the middle position shows a non-zero number which indicates its exact position in the 'Cascade position' field and *yes* in the 'Cascaded device connected' field.

The following diagram shows 1, indicating it is the first link device - Link 1.



The final link device shows a non-zero number which indicates its position in the 'Cascade position' field and *no* in the 'Cascaded device connected' field.

The following diagram shows 2, indicating it is the second link device - Link 2. The 'Cascaded device connected' field shows *no*, indicating that it is the final one in the chain.

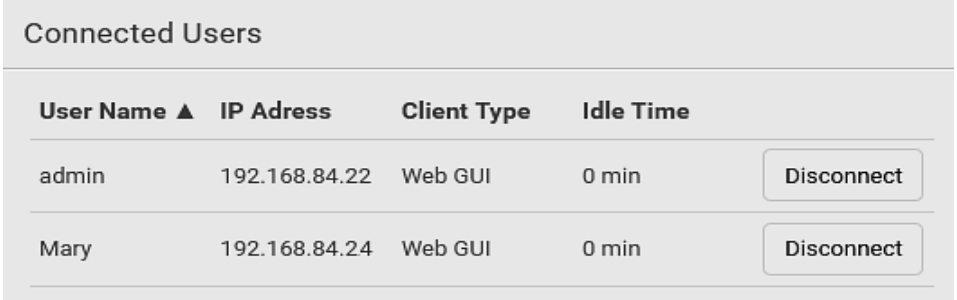
For a list of port numbers required for accessing each cascaded device in the Port Forwarding mode, click the Port Forwarding title bar on the same page.

Viewing Connected Users

You can check which users have logged in to the PRO3X and their status. If you have administrator privileges, you can terminate any user's connection to the PRO3X.

To view and manage connected users:

Choose Maintenance > Connected Users. A list of logged-in users displays.



If wanted, you can resort the list by clicking the desired column header.

Column	Description
User Name	The login name of each connected user.
IP Address	The IP address of each user's host. For the login via a local connection (serial RS-232 or USB), <local> is displayed instead of an IP address.
Client Type	The interface through which the user is being connected to the PRO3X. ▪ Web GUI: Refers to the web interface. ▪ CLI: Refers to the command line interface (CLI). The information in parentheses following "CLI" indicates how this user is connected to the CLI. - Serial: The local connection, such as the serial RS-232 or USB connection. - SSH: The SSH connection. - Telnet: The Telnet connection.
Idle Time	The length of time for which a user remains idle.

To disconnect any user, click the corresponding Disconnect.

Click Disconnect on the confirmation message.

The disconnected user is forced to log out.

Viewing or Clearing the Local Event Log

By default, the PRO3X captures certain system events and saves them in a local (internal) event log.

You can view over 2000 historical events that occurred on the PRO3X in the local event log. When the log size exceeds 256KB, each new entry overwrites the oldest one.

To display the local log:

Choose Maintenance > Event Log.

Each event entry consists of:

ID number of the event

Date and time of the event

> *Tip: The date and time shown on the PRO3X web interface are automatically converted to your computer's time zone. To avoid time confusion, it is suggested to apply the same time zone settings as those of PRO3X to your computer or mobile device.*

Event type

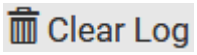
A description of the event

To view a specific type of events only, select the desired event type in the 'Filter event class' field.

The log is refreshed automatically at a regular interval of five seconds. To avoid any new events' interruption during data browsing, you can suspend the automatic update by clicking Pause.

To restore automatic update, click Resume. Those new events that have not been listed yet due to suspension will be displayed in the log now.

To clear the local log:

Click  on the top-right corner.

Click Clear Log on the confirmation message.

Updating the PRO3X Firmware

Firmware files are available on Server Technology's website ***Support page*** (***http://www.servertech.com/support/***).

When performing the firmware upgrade, the PRO3X keeps each outlet's power status unchanged so no server operation is interrupted. During and after the firmware upgrade, outlets that have been powered on prior to the firmware upgrade remain powered ON and outlets that have been powered off remain powered OFF.

You must be the administrator or a user with the Firmware Update permission to update the PRO3X firmware.

Before starting the upgrade, read the release notes downloaded from Server Technology's website ***Support page*** (***http://www.servertech.com/support/***). If you have any questions or concerns about the upgrade, contact Server Technology's Technical Support BEFORE upgrading.

On a multi-inlet PDU, all inlets must be connected to power for the PDU to successfully upgrade its firmware.

Note that firmware upgrade via iOS mobile devices, such as iPad, requires the use of iCloud Drive or a file manager app.

Warning: Do NOT perform the firmware upgrade over a wireless network connection.

To update the firmware:

Choose Maintenance > Update Firmware.

Click  to select an appropriate firmware file.

Click Upload. A progress bar appears to indicate the upload process.

Once complete, information of both installed and uploaded firmware versions as well as compatibility and signature-checking results are displayed.

If anything is incorrect, click Discard Upload.

To proceed with the update, click Update Firmware.

Warning: Do NOT power off the PRO3X during the update.

During the firmware update:

A progress bar appears on the web interface, indicating the update status.

The front panel display shows the firmware upgrade message.

The outlet LEDs flash if the relay boards are being updated. If the firmware update does not include the update of the relay board firmware, outlet LEDs do NOT flash.

No users can successfully log in to the PRO3X.

Other users' operation, if any, is forced to suspend.

When the update is complete, the PRO3X resets, and the Login page re-appears.

Other logged-in users are logged out when the firmware update is complete.

Important: If you are using the PRO3X with an SNMP manager, download its MIB again after the firmware update to ensure your SNMP manager has the correct MIB for the latest release you are using.

Alternatives:

To use a different method to update the firmware, refer to:

Firmware Update via SCP

Bulk Configuration or Firmware Upgrade via DHCP/TFTP

Firmware Upgrade via USB

Upgrade Guidelines for Existing Cascading Chains

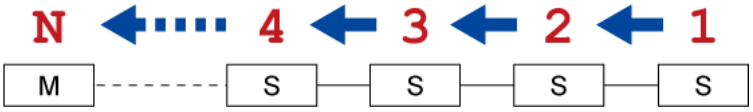
You must obey the following guidelines when upgrading a chain. Otherwise, a networking issue occurs.

Upgrade Sequence in an Existing Cascading Chain

Depending on the firmware version(s) of your cascading chain, there may or may not be limitations for the firmware upgrade sequence in the chain.

The upgrade must start from the last link device (S), then the second to last, the third to last, and so on until the master device (M).

Red numbers below represent the appropriate upgrade sequence. 'N' is the final one to upgrade.



A Note about Firmware Upgrade Time

The PDU firmware upgrade time varies from unit to unit, depending on various external and internal factors.

External factors include, but are not limited to: network throughput, firmware file size, and speed at which the firmware is retrieved from the storage location. Internal factors include: the necessity of upgrading the firmware on the microcontroller and the number of microcontrollers that require upgrade (which depends on the number of outlets). The microcontroller is upgraded only when required. Therefore, the length of firmware upgrade time ranges from approximately 3 minutes (without any microcontroller updated) to almost 7 minutes (with all microcontrollers for 48 outlets updated). Take the above factors into account when estimating the PDU's firmware upgrade time.

The time indicated in this note is for PRO3X web-interface-based upgrades. Upgrades through other management systems, such as Sunbird's Power IQ, may take additional time beyond the control of the PDU itself. This note does not address the upgrades using other management systems.

Viewing Firmware Update History

The firmware upgrade history is permanently stored on the PRO3X. It remains available even though you perform a device reboot or any firmware update.

To view the firmware update history:

Choose Maintenance > Firmware History.

Each firmware update event consists of:

Update date and time

Previous firmware version

Update firmware version

Update result

If wanted, you can resort the list by clicking the desired column header.

Bulk Configuration

The Bulk Configuration feature lets you save generic settings of a configured PRO3X device to your computer. You can use this configuration file to copy common settings to other PRO3X devices of the same model and firmware version.

A source device is the PRO3X device where the configuration file is downloaded/saved. A target device is the PRO3X device that loads the configuration file.

By default the configuration file downloaded from the source device contains settings based on the built-in bulk profile. The built-in bulk profile defines that all settings should be saved except for device-specific settings.

You can decide which settings are downloaded and which are not by creating your own bulk configuration profile.

Note that "device-specific" settings, such as the device's IP address or environmental sensor settings, will never be included into any profile you will create so they will never be downloaded from any source device.

When the date and time settings are included in the bulk configuration file, exercise caution when distributing that file to target devices located in a different time zone than the source device.

Tip: To back up or restore "all" settings, including device-specific ones, use the Backup/Restore feature instead.

Main bulk configuration procedure:

If you prefer customizing the bulk configuration file, create your own bulk configuration profile(s) first.

Perform the bulk configuration operation, which includes the following steps. Make sure the desired bulk configuration profile has been selected on the source device.

Save a bulk configuration file from the source device.

Perform bulk configuration on one or multiple target devices.

Note: On startup, PRO3X performs all of its functions, including event rules and logs, based on the new configuration you have copied instead of the previous configuration prior to the device reset. For example, the "Bulk configuration copied" event is logged only when the new configuration file contains the "Bulk configuration copied" event rule.

The last configuration-copying record:

If you once copied any bulk configuration or device backup file to the PRO3X, the last record similar to the following is displayed at the bottom of both the Bulk Configuration and Backup/Restore pages.

Last restore: 3/16/2019, 10:11:03 AM UTC+0800, status: OK

Tip: The date and time shown on the PRO3X web interface are automatically converted to your computer's time zone. To avoid time confusion, it is suggested to apply the same time zone settings as those of PRO3X to your computer or mobile device.

Alternatives:

To use a different bulk configuration method, refer to:

- Bulk Configuration via SCP
- Bulk Configuration or Firmware Upgrade via DHCP/TFTP
- Configuration or Firmware Upgrade with a USB Drive
- Raw Configuration Upload and Download

Tip: Both methods of uploading 'bulk configuration' file or 'raw configuration' file via SCP can serve the purpose of bulk configuration. The only difference is that you can configure device-specific *settings with the upload of raw configuration but not with the 'bulk configuration' file.*

Bulk Configuration Restrictions

Before performing bulk configuration, make sure your source and target devices are compatible devices for sharing general settings.

Restrictions for bulk configuration:

The target device must be running the same firmware version as the source device.

The target device must be of the same model type as the source device.

Bulk configuration is permitted if the differences between the target and source devices are only "mechanical" designs which are indicated in the model name's suffix.

For example, you can perform bulk configuration between PRO3X-4724-E2N1**K2** and PRO3X-4724-E2N1**K9** since the only difference between the two models is their chassis colors represented by K2 (blue) and K9 (gray).

Mechanical designs ignored by bulk configuration:

When the source and target devices share the same technical specifications but are only different with any "mechanical designs" which are indicated in the table below, the bulk configuration remains feasible.

These mechanical designs are represented by suffixes added to the model name of a PRO3X device. In the table, *x* represents a number. For example, A*x* can be A1, A2, A3, and so on.

Suffix	Mechanical design	Example
A*x*	The line cord's length in meters	A20 = 3.3 meters
B*x*	The line cord's color	B501 = bright red orange
C*x*	Cord types or options	C4 = power cord with the standard gauge
D*x*	Plug types or options	D1 = IP67 watertight plug
E*x*	Outlet types or options	E2 = *Locking* C13 or *Locking* C19
G*x*	Controller options	G0 = no controller
K*x*	Chassis colors	K6 = yellow
L*x*	The line cord's length in centimeters	
N*x*	Chassis dimensions or other mechanical changes	
O*x*	OCP brand options	
P*x*	Special requests for device painting or printing	
Q*x*	Special requests for physical placement arrangements	
U*x*	Different power plug brands	

Customizing Bulk Configuration Profiles

A bulk profile defines which settings are downloaded/saved from the source device and which are not. The default is to apply the built-in bulk profile, which downloads all settings from the source device except for device-specific data.

If the built-in profile does not meet your needs, you can create your own profile(s), and then apply the wanted profile before downloading/saving any settings from the source device.

To create new bulk profile(s):

Log in to the source PRO3X, whose settings you want to download.

Choose Maintenance > Bulk Configuration.

Click ➕ in the Bulk Profiles section.

In the 'Profile name' and 'Description' fields, enter information for identifying the new profile.

To make this new profile the default one for future bulk configuration operations, select the 'Select as default profile' checkbox.

After setting any profile as the default, the original default profile will no longer function as the default one.

Now decide which settings are wanted and which are not.

Click  of the setting which you want to configure.

When the pop-up menu appears, select one of the options.

Note that the two options 'Inherited' and 'Built-in' are mutually exclusive.

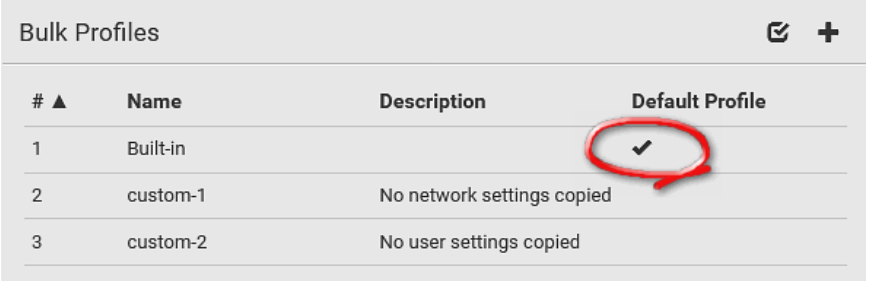
Option	Description
Excluded	The setting will *not* be downloaded.
Included	The setting will be downloaded.
Inherited	The setting will follow its parent setting (that is, the upper-level setting). ▪ If you select 'Excluded' for its upper-level setting, this setting will be also excluded. ▪ If you select 'Included' for its upper-level setting, this setting will be also included. The option inherited from its parent setting will be enclosed in parentheses.
Built-in	The setting will follow the same setting of the built-in profile. ▪ If 'Excluded' is selected in the built-in profile, this setting will be also excluded. ▪ If 'Included' is selected in the built-in profile, this setting will be also included. The option inherited from the built-in profile will be enclosed in parentheses. *Note: The option 'Built-in' is available in those settings whose corresponding settings in the built in profile have been set to a non-inherited option -- Excluded or Included.*

Click Save.

Repeat the same steps if you want to create more bulk profiles.

Performing Bulk Configuration

On the source device, make sure the wanted profile has been set as the default one. If not, start from step 1 below. If yes, go to step 2 directly.



Step 1: Select the desired bulk configuration profile (optional)

Log in to the source PRO3X, whose settings you want to copy.

Choose Maintenance > Bulk Configuration.

Click on the row of the wanted profile to open the Edit Bulk Profile page.

Select the 'Select as default profile' checkbox.

Click Save.

Step 2: Save a bulk configuration file

You must have the Administrator Privileges or "Unrestricted View Privileges" to download the configuration.

Log in to the source PRO3X if you have not yet.

Choose Maintenance > Bulk Configuration.

Check the 'Bulk format' field. If the chosen value does not match your need, change it.

Option	Description
Encrypted	▪ Partial content is base64 encoded. ▪ Its content is encrypted using the AES-128 encryption algorithm. ▪ The file is saved to the TXT format
Cleartext	▪ Content is displayed in clear text. ▪ The file is saved to the TXT format.

Click Download Bulk Configuration.

When prompted to open or save the configuration file, click Save.

Step 3: Perform bulk configuration

You must have the Administrator Privileges to upload the configuration.

Log in to the target PRO3X, which is of the same model and runs the same firmware as the source PRO3X.

Choose Maintenance > Bulk Configuration.

Click 

to select the configuration file.

Click 'Upload & Restore Bulk Configuration' to copy it.

A message appears, prompting you to confirm the operation and enter the admin password.

Enter the admin password, and click Restore.

Wait until the PRO3X resets and the login page re-appears.

Alternatives:

To use a different bulk configuration method, refer to:

- Bulk Configuration via SCP
- Bulk Configuration or Firmware Upgrade via DHCP/TFTP
- Configuration or Firmware Upgrade with a USB Drive
- Raw Configuration Upload and Download

Tip: Both methods of uploading 'bulk configuration' file or 'raw configuration' file via SCP can serve the purpose of bulk configuration. The only difference is that you can configure device-specific *settings with the upload of raw configuration but not with the 'bulk configuration' file.*

Modifying or Removing Bulk Profiles

You can modify or remove any bulk profile except for the built-in one.

Note that a profile that has been set as the default cannot be removed, either. To remove it, you have to remove its default setting first.

Choose Maintenance > Bulk Configuration. A list of profiles displays and then do one of the following.

To modify an existing profile:

Click on the row of the wanted profile in the list.

Change the settings you want.

Click Save.

To remove a single profile:

Click on the row of the wanted profile.

Click  on the top-right corner.

Click Delete on the confirmation message.

To remove one or multiple profiles:

Click  to make checkboxes appear in front of profiles.

Select one or multiple profiles.

To select ALL profiles, select the topmost checkbox in the header row.

Click  on the top-right corner.

Click Delete on the confirmation message.

Backup and Restore of Device Settings

Unlike the bulk configuration file, the backup file contains ALL device settings, including device-specific data like device names and all network settings. To back up or restore the settings of PRO3X, you should perform the Backup/Restore feature.

All PRO3X information is captured in the plain-TEXT-formatted backup file except for the device logs and TLS certificate.

Note: To perform bulk configuration among multiple PRO3X devices, use the Bulk Configuration feature instead.

To download a backup PRO3X file:

You must have the Administrator Privileges or "Unrestricted View Privileges" to download a backup file.

Choose Maintenance > Backup/Restore.

Check the 'Backup format' field. If the chosen value does not match your need, change it.

Option	Description
Encrypted	▪ Partial content is base64 encoded. ▪ Its content is encrypted using the AES-128 encryption algorithm. ▪ The file is saved to the TXT format
Cleartext	▪ Content is displayed in clear text. ▪ The file is saved to the TXT format.

Click Download Device Settings. Save the file onto your computer.

To restore the PRO3X using a backup file:

You must have the Administrator Privileges to restore the device settings.

Choose Maintenance > Backup/Restore.

Click 

to select the backup file.

Click 'Upload & Restore Device Settings' to upload the file.

A message appears, prompting you to confirm the operation and enter the admin password.

Enter the admin password, then click Restore.

Wait until the PRO3X resets and the Login page re-appears, indicating that the restore is complete.

Note: On startup, PRO3X performs all of its functions, including event rules and logs, based on the new configuration you have copied instead of the previous configuration prior to the device reset. For example, the "Bulk configuration copied" event is logged only when the new configuration file contains the "Bulk configuration copied" event rule.

The last configuration-copying record:

If you once copied any bulk configuration or device backup file to the PRO3X, the last record similar to the following is displayed at the bottom of both the Bulk Configuration and Backup/Restore pages.

Last restore: 3/16/2019, 10:11:03 AM UTC+0800, status: OK

Alternative:

To use a different method to perform backup/restore, refer to:

Backup and Restore via SCP

Network Diagnostics

PRO3X provides the following tools in the web interface for diagnosing potential networking issues.

Ping: The tool is useful for checking whether a host is accessible through the network or Internet.

Trace Route: The tool lets you find out the route over the network between two hosts or systems.

List TCP Connections: You can use this function to display a list of TCP connections.

Tip: These network diagnostic tools are also available through CLI.

Choose Maintenance > Network Diagnostics, and then perform any function below.

Ping:

Type values in the following fields.

Field	Description
Network host	The name or IP address of the host that you want to check.
Number of requests	A number up to 20. This determines how many packets are sent for pinging the host.

Click Run Ping to ping the host. The Ping results are then displayed.

Trace Route:

Type values in the following fields.

Field/setting	Description
Hostname	The IP address or name of the host whose route you want to check.
Timeout(s)	A timeout value in seconds to end the trace route operation.
Use ICMP packets	To use the Internet Control Message Protocol (ICMP) packets to perform the trace route command, select this checkbox.

Click Run. The Trace Route results are then displayed.

List TCP Connections:

Click the List TCP Connections title bar to show the list.

Downloading Diagnostic Information

Important: This function is for use by Field Engineers or when you are directed by Server Technology Technical Support.

You can download the diagnostic file from the PRO3X to a client machine. The file is compressed into a .tgz file and should be sent to Server Technology Technical Support for interpretation.

This feature is accessible only by users with Administrative Privileges or Unrestricted View Privileges.

To retrieve a diagnostic file:

Choose Maintenance > Download Diagnostic > 

.

The system prompts you to save or open the file. Save the file then.

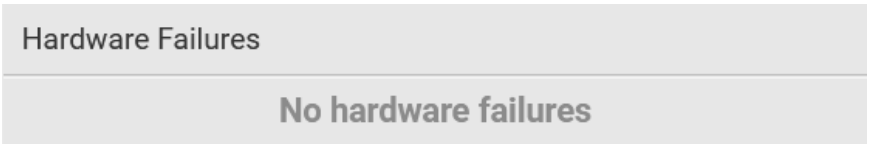
E-mail this file as instructed by Server Technology Technical Support.

Hardware Issue Detection

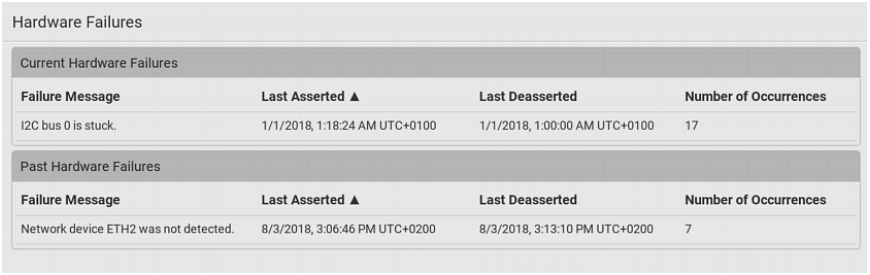
This page lists any internal hardware issues PRO3X has detected, including current events and historical records.

Choose Maintenance > Hardware Failures, and the page similar to either of the following diagrams opens.

NO hardware failures detected:



Hardware failure(s) detected:



Hardware Failure alerts on the Dashboard page:

Note that *current* hardware failure events, if any, will also display on the ***Dashboard***.

Hardware failure types:

Hardware issues	Description
Network device not detected	A specific networking interface of PRO3X is NOT detected.
I2C Bus stuck	A specific I2C bus is stuck, which affects the communication with sensors.
Link controller not reachable	Communication with a specific link controller fails.
Link controller malfunction	A specific link controller does not work properly.
Outlet power state inconsistent	The physical power state of a specific outlet is different from the chosen power state set by the software.

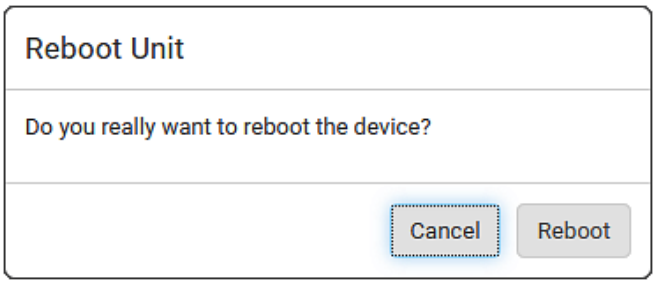
Rebooting the PRO3X

You can remotely reboot the PRO3X via the web interface.

Resetting the PRO3X does not interrupt the operation of connected servers because there is no loss of power to outlets. During and after the reboot, outlets that have been powered on prior to the reboot remain powered on, and outlets that have been powered off remain powered off.

To reboot the device:

Choose Maintenance > Unit Reset > Reboot Unit.



Click Reboot to restart the PRO3X.

A message appears, with a countdown timer showing the remaining time of the operation. It takes about one minute to complete.

When the restart is complete, the login page opens.

Tip: If you are not redirected to the login page after the restart is complete, click the text "this link" in the countdown message.

Note: Device reset will cause CLI communications over an "USB" connection to be lost. Therefore, re-connect the USB cable after the reset is complete.

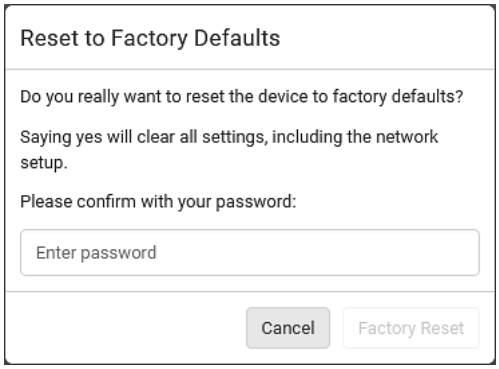
Resetting All Settings to Factory Defaults

You must have the Administrator Privileges to reset all settings of the PRO3X to factory defaults.

Important: Exercise caution before resetting the PRO3X to its factory defaults. This erases existing information and customized settings, such as user profiles, threshold values, and so on. Only active energy data and firmware upgrade history are retained.

To reset the device to factory defaults:

Choose Maintenance > Unit Reset > Reset to Factory Defaults.



Type your password and then click Factory Reset to reset the PRO3X to factory defaults.

A message appears, with a countdown timer showing the remaining time of the operation. It takes about two minutes to complete.

When the reset is complete, the login page opens.

Tip: If you are not redirected to the login page after the reset is complete, click the text "this link" in the countdown message.

Alternative:

There are two more methods to reset the device to factory defaults.

- Use the "mechanical" reset button
- Perform the CLI command

Note: Device reset will cause CLI communications over an "USB" connection to be lost. Therefore, re-connect the USB cable after the reset is complete.

Retrieving Software Packages Information

You can check the current firmware version and the information of all open source packages embedded in the PRO3X through the web interface.

To retrieve the embedded software packages information:

Choose Maintenance > About PDU. A list of open source packages is displayed.

You can click any link to access related information or download any software package.

Using SNMP

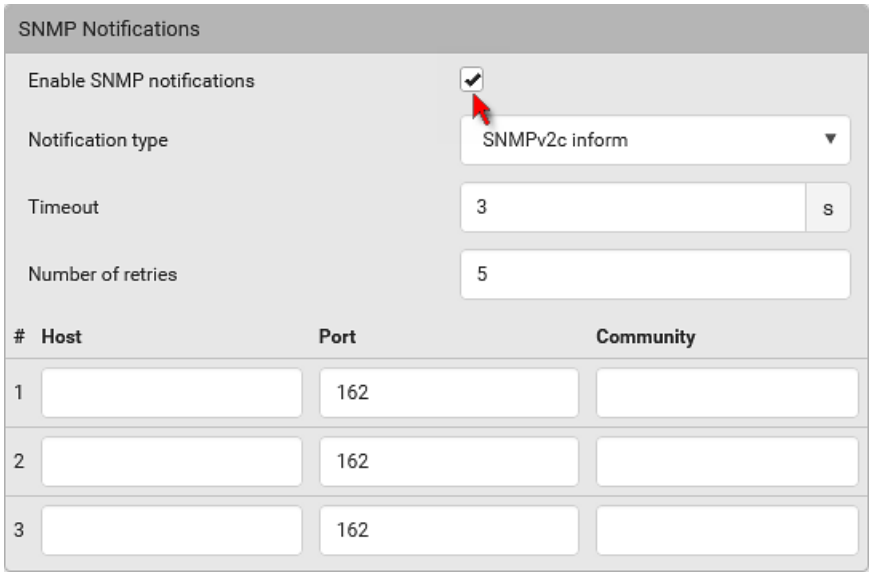
This SNMP section helps you set up the PRO3X for use with an SNMP manager. The PRO3X can be configured to send traps or informs to an SNMP manager, as well as receive GET and SET commands in order to retrieve status and configure some basic settings.

Enabling and Configuring SNMP

To communicate with an SNMP manager, you must enable SNMP protocols on the PRO3X. By default the "read-only" mode of SNMP v1/v2c is enabled.

The SNMP v3 protocol allows for encrypted communication. To take advantage of this, you must configure the users with the SNMP v3 access permission and set Authentication Pass Phrase and Privacy Pass Phrase, which act as shared secrets between SNMP and the PRO3X.

Important: You must download the SNMP MIB for your PRO3X to use with your SNMP manager.



To enable SNMP v1/v2c and/or v3 protocols:

Choose Device Settings > Network Services > SNMP.

In the SNMP Agent section, enable SNMP v1/v2c or SNMP v3, and configure related fields, such as the community strings.

If SNMP v3 is enabled, you must determine which users shall have the SNMP v3 access permission. See below.

To configure users for SNMP v3 access:

Choose User Management > Users.

Create or modify users to enable their SNMP v3 access permission.

If authentication and privacy is enabled, configure the SNMP password(s) in the user settings.

To enable SNMP notifications:

Choose Device Settings > Network Services > SNMP.

In the SNMP Notifications section, enable the SNMP notification feature, and configure related fields. For details, refer to:

SNMPv2c Notifications

SNMPv3 Notifications (Note: Any changes made to the 'SNMP Notifications' section on the SNMP page will update the settings of the System SNMP Notification Action, and vice versa.

SNMPv2c Notifications

Choose Device Settings > Network Services > SNMP.

In the SNMP Agent, make sure the Enable SNMP v1/v2c checkbox is selected.

In the SNMP Notifications section, make sure the 'Enable SNMP notifications' checkbox is selected.

Select 'SNMPv2c trap' or 'SNMPv2c inform' as the notification type.

Type values in the following fields.

Field	Description
Timeout	The interval of time, in seconds, after which a new inform communication is resent if the first is not received. ▪ For example, resend a new inform communication once every 3 seconds.
Number of retries	The number of times you want to resend the inform communication if it fails. ▪ For example, inform communications are resent up to 5 times when the initial communication fails.
Host	The IP address of the device(s) you want to access. This is the address to which notifications are sent by the SNMP agent. You can specify up to 3 SNMP destinations.
Port	The port number used to access the device(s).
Community	The SNMP community string to access the device(s). The community is the group representing the PRO3X and all SNMP management stations.

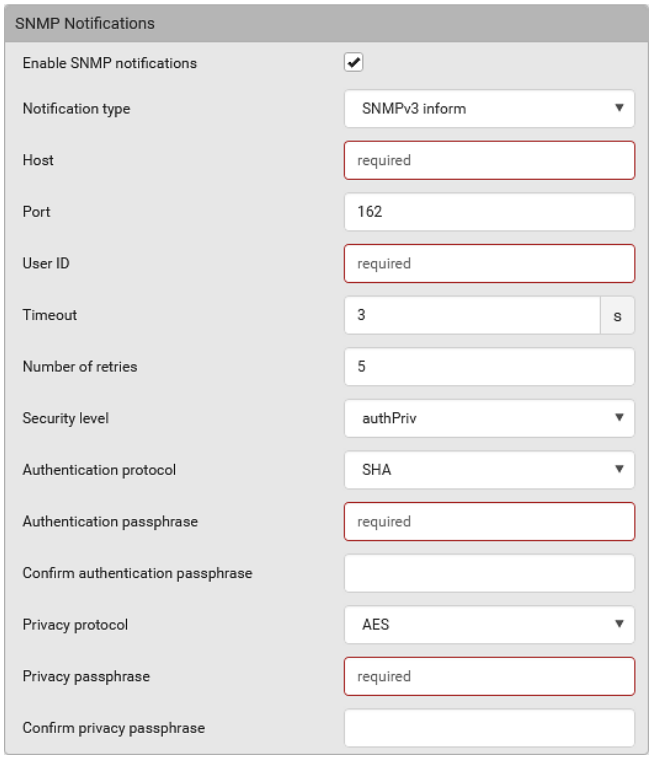
Click Save.

SNMPv3 Notifications

Choose Device Settings > Network Services > SNMP.

In the SNMP Agent, make sure the Enable SNMP v1/v2c checkbox is selected.

In the SNMP Notifications section, make sure the 'Enable SNMP notifications' checkbox is selected.



Select 'SNMPv3 trap' or 'SNMPv3 inform' as the notification type.

For SNMP TRAPs, the engine ID is prepopulated.

Type values in the following fields.

Click Save.

Field	Description
Host	The IP address of the device(s) you want to access. This is the address to which notifications are sent by the SNMP agent.
Port	The port number used to access the device(s).
User ID	User name for accessing the device. ▪ Make sure the user has the SNMP v3 access permission.
Timeout	The interval of time, in seconds, after which a new inform communication is resent if the first is not received. ▪ For example, resend a new inform communication once every 3 seconds.
Number of retries	Specify the number of times you want to resend the inform communication if it fails. ▪ For example, inform communications are resent up to 5 times when the initial communication fails.
Security level	Three types are available. ▪ noAuthNoPriv - neither authentication nor privacy protocols are needed. ▪ authNoPriv - only authentication is required. ▪ authPriv - both authentication and privacy protocols are required.
Authentication protocol, Authentication passphrase, Confirm authentication passphrase	The three fields are available when the security level is set to AuthNoPriv or authPriv. ▪ Select the authentication protocol - MD5 or SHA ▪ Enter the authentication passphrase
Privacy protocol, Privacy passphrase, Confirm privacy passphrase	The three fields are available when the security level is set to authPriv. ▪ Select the Privacy Protocol - DES or AES ▪ Enter the privacy passphrase and then confirm the privacy passphrase

Downloading SNMP MIB

You must download an appropriate SNMP MIB file for successful SNMP communications. Always use the latest SNMP MIB downloaded from the current firmware of your PRO3X.

You can download the MIBs from two different pages of the web interface.

MIB download via the SNMP page:

Choose Device Settings > Network Services > SNMP.

Click the Download MIBs title bar.

Select the desired MIB file to download.

PDU2-MIB: The SNMP MIB file for PRO3X management.

Click Save to save the file onto your computer.

MIB download via the Device Information page:

Choose Maintenance > Device Information.

In the Information section, click the desired download link:

PDU2-MIB

ASSETMANAGEMENT-MIB

Click Save to save the file onto your computer.

SNMP Gets and Sets

In addition to sending notifications, the PRO3X is able to receive SNMP get and set requests from third-party SNMP managers.

Get requests are used to retrieve information about the PRO3X, such as the system location, and the current on a specific outlet.

Set requests are used to configure a subset of the information, such as the SNMP system name.

Note: The SNMP system name is the PRO3X device name. When you change the SNMP system name, the device name shown in the web interface is also changed.

The PRO3X does NOT support configuring IPv6-related parameters using the SNMP set requests.

Valid objects for these requests are limited to those found in the SNMP MIB-II System Group and the custom PRO3X MIB.

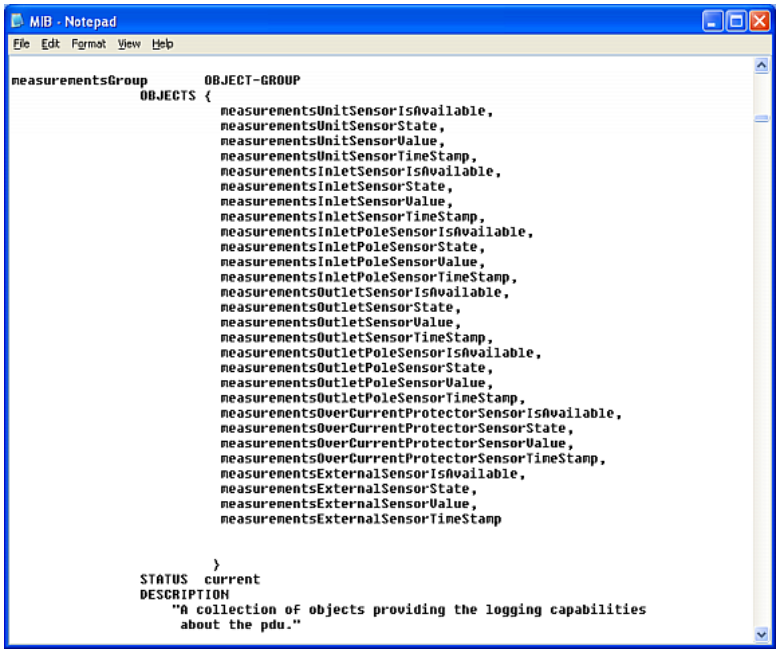
The PRO3X MIB

The SNMP MIB file is required for using your PRO3X with an SNMP manager. An SNMP MIB file describes the SNMP functions.

Layout

Opening the MIB reveals the custom objects that describe the PRO3X system at the unit level as well as at the individual-outlet level.

As standard, these objects are first presented at the beginning of the file, listed under their parent group. The objects then appear again individually, defined and described in detail.



For example, the measurementsGroup group contains objects for sensor readings of PRO3X as a whole. One object listed under this group, measurementsUnitSensorValue, is described later in the MIB as "The sensor value". pduRatedCurrent, part of the configGroup group, describes the PDU current rating.

SNMP Sets and Thresholds

Some objects can be configured from the SNMP manager using SNMP set commands. Objects that can be configured have a MAX-ACCESS level of "read-write" in the MIB.

These objects include threshold objects, which cause the PRO3X to generate a warning and send an SNMP notification when certain parameters are exceeded.

Note: When configuring the thresholds via SNMP set commands, ensure the value of upper critical threshold is higher than that of upper warning threshold.

Configuring NTP Server Settings

Using SNMP, you can change the following NTP server-related settings in the unitConfigurationTable:

Enable or disable synchronization of the device's date and time with NTP servers (synchronizeWithNTPServer)

Enable or disable the use of DHCP-assigned NTP servers if synchronization with NTP servers is enabled (useDHCPProvidedNTPServer)

Manually assign the primary NTP server if the use of DHCP-assigned NTP servers is disabled (firstNTPServerAddressType and firstNTPServerAddress)

Manually assign the secondary NTP server (optional) (secondNTPServerAddressType and secondNTPServerAddress)

When using the SNMP SET command to specify or change NTP servers, it is required that both the NTP server's address type and address be set in the command line simultaneously.

For example, the SNMP command to change the primary NTP server's address from IPv4 (192.168.84.84) to host name looks similar to the following:

```
snmpset -v2c -c private 192.168.84.84 firstNTPServerAddressType = dns
firstNTPServerAddress = "angu.pep.com"
```

A Note about Enabling Thresholds

When enabling previously-disabled thresholds via SNMP, make sure you set a correct value for all thresholds that are supposed to be enabled prior to actually enabling them. Otherwise, you may get an error message.

Appendix A: Regulatory Compliance

Product Safety

Units have been safety tested and certified to the following standards:

- USA/Canada UL 60950-1:2007 R10.14 and CAN/CSA 22.2 No. 60950-1-07 +A1+A2
- European Union EN 60950-1:2006 + A11 +A1 + A12 + A2

This product is also designed for Norwegian IT power system with phase-to phase voltage 230V.

Notifications

USA Notification

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at the user's own expense.

Modifications not expressly approved by the manufacturer could void the user's authority to operate the equipment under FCC rules.

Canadian Notification

This Class A digital apparatus complies meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe A respecte toutes les exigencies du Règlement sur le matériel brouilleur du Canada.

European Union Notification

WARNING: This equipment is compliant with Class A of CISPR 32. In a residential environment this equipment may cause radio interference.

Products with CE Marking comply with the EMC Directive (2014/30/EU), Low Voltage Directive (2014/35/EU) and RoHS 2 Directive (2011/65/EU) issued by the Commission of the European Community.

Compliance with the following harmonized standards demonstrate conformity with the EMC and Low Voltage Directives.

- EN 55032
- EN 55024
- EN 60950-1

Japanese Notification

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。
本製品に同梱または付属しております電源コードは、本製品専用です。本製品以外の製品ならびに他の用途に使用しないで下さい。

Chinese Notification

关于符合中国《电子信息产品污染控制管理办法》的声明

产品中有毒有害物质的名称及含量

部件名称 (Parts)	有毒有害物质或元素 (Hazardous Substance)					
	铅 (Pb)	汞 (Hg)	镉 (Cd)	六价铬 (Cr (VI))	多溴联苯 (PBB)	多溴二苯醚 (PBDE)
机箱子组件 (Chassis Subassembly)	O	O	O	O	O	O
印刷板组件 (PCAs)	X	O	O	O	O	O

O 表示该有毒有害物质在该部件所有均质材料中的含量均在 SJ/T 11363-2006 标准规定的限量要求以下。
Indicates that this hazardous substance contained in all homogeneous materials of this part is below the limit requirement in SJ/T 11363-2006.

X 表示该有毒有害物质至少在该部件的某一均质材料中的含量超出 SJ/T 11363-2006 标准 规定的限量要求。
Indicates that this hazardous substance contained in at least one of the homogeneous materials of this part is above the limit requirement in SJ/T 11363-2006.

Product Recycling

Recycling

Server Technology Inc. encourages the recycling of its products. Disposal facilities, environmental conditions and regulations vary across local, state and country jurisdictions, so Server Technology encourages consultation with qualified professional and applicable regulations and authorities within your region to ensure proper disposal.

Waste Electrical and Electronic Equipment (WEEE)

In the European Union, this label indicates that this product should not be disposed of with household waste. It should be deposited at an appropriate facility to enable recovery and recycling.

Appendix B: Product Support

Warranty

For Server Technology warranty information, visit our website www.servertech.com

Contact Technical Support

Experience Server Technology's FREE Technical Support

Server Technology understands that there are often questions when installing and/or using a new product. Free Technical Support is provided from 8 a.m. to 5 p.m. Pacific Time, Monday through Friday.

Server Technology, Inc. (a brand of Legrand)

1040 Sandhill Road	Tel:	1-800-835-1515	Web:	www.servertech.com
Reno, Nevada 89521 USA	Fax:	775-284-2065	Email:	support@servertech.com

Return Merchandise Authorization (RMA)

If you have a product that is not functioning properly and needs technical assistance or repair, see the Server Technology **Return Merchandise Authorization** process at: www.servertech.com

About Server Technology®

Server Technology, a brand of Legrand, is leading the engineering and manufacturing of customer-driven, innovative and exceptionally reliable power, access and control solutions for monitoring and managing critical IT assets for continual availability.

Server Technology's power strategy experts are trusted to provide Rack PDU solutions for data centers worldwide ranging from small technology startups to Fortune 100 powerhouses. Because power is all we do, Server Technology can be found in the best cloud and colocation providers, forward thinking labs, and telecommunications operations.

Server Technology customers consistently rank us as providing the highest quality PDUs, the best customer support, and most valuable innovation. We have over 12,000 PDU configurations to fit every data center need and most of our PDUs are shipped within 10 days.

Rack PDU Buying Guide
Find the best PDU for your data center
servertech.com/rack-pdu-buying-guide

Rack PDU Selector
Over 2000 standard configurations
servertech.com/product-selector

Build Your Own PDU
Build an HDOT or HDOT Cx PDU in 4 easy steps
byopdu.servertech.com

Speak to a Power Expert
Get free technical support
servertech.com/support

How to Buy
Tools to simplify the PDU buying process
servertech.com/how-to-buy

About Us
Stay Powered, Be Supported, Get Ahead
servertech.com/about-us

1-800-835-1515
sales@servertech.com
www.servertech.com

Server Technology®
A brand of legrand®