

**Server
Technology**[®]

A brand of **Legend**

stay powered. be supported. get ahead.



PRO3X User Guide

Command Line Interface (CLI)

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

301-9999-51 Rev A (041520)

Copyright © 2005-2020 Server Technology, Inc. All rights reserved.

1040 Sandhill Drive

Reno, Nevada 89521 USA

All Rights Reserved

This publication is protected by copyright and all rights are reserved. No part of it may be reproduced or transmitted by any means or in any form, without prior consent in writing from Server Technology.

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.



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 **Command Line Interface (CLI)** on the PRO3X product group.

This guide is a detailed resource for the PRO3X CLI commands, description, syntax, usage, parameters, variables, as well as providing command examples and results to assist you with using the firmware's interface.



stay powered.



be supported.



get ahead.

Contact Technical Support



be supported.

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 höchstens 4,5m. Sollten Sie ein Verlängerungsnetzkaabel, der Gesamtlänge auch nicht mehr als die maximal zulässige 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 équivalent 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

Using the PRO3X Command Line Interface (CLI)

	<p>ATTENTION! Observe precautions for handling Electrostatic Sensitive Devices.</p>	<p>Attention ! Respecter les mesures de sécurité en manipulant des dispositifs sensibles aux décharges électrostatiques.</p>	<p>Achtung! Vorsichtshinweise zur Handhabung elektrostatisch empfindlicher Geräte beachten.</p>
	<p>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.</p>	<p>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.</p>	<p>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.</p>

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.

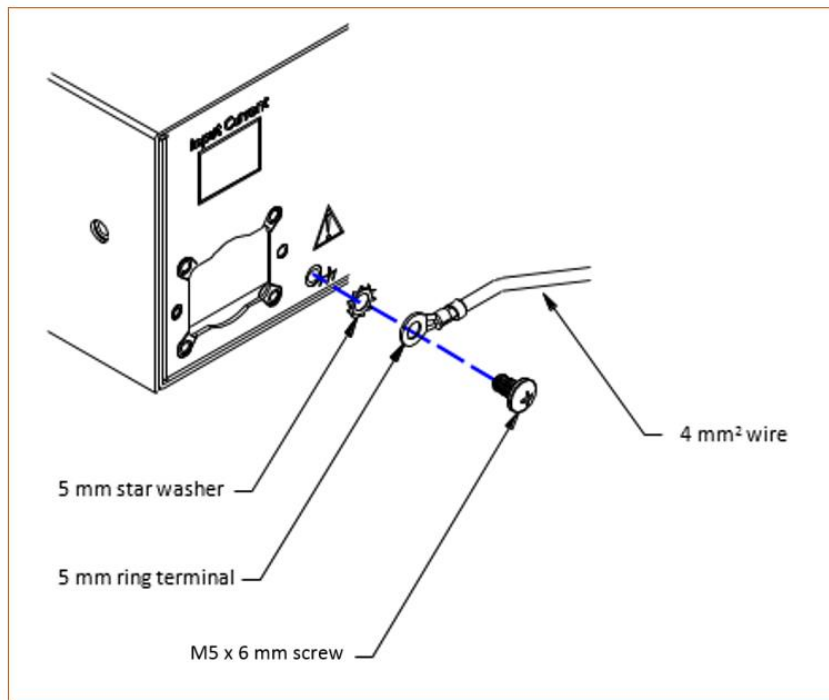
Note: The auxiliary external ground location may vary. Most PDUs will have it located near the power cord entry located near the  symbol.

User-Supplied Materials:

- One 5 mm internal (or external) tooth star washer;
- One 4.0 mm² (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 Command Line Interface

This user guide explains how to use the command line interface (CLI) to administer the PRO3X. Note that available CLI commands are model dependent. CLI commands are case sensitive.

About the Interface

The PRO3X provides a command line interface that enables data center administrators to perform some basic management tasks.

Using this interface, you can do the following:

- Reset the PRO3X
- Display the PRO3X and network information, such as the device name, firmware version, IP address, and so on
- Configure the PRO3X and network settings
- Troubleshoot network problems

You can access the interface over a local connection using a terminal emulation program such as HyperTerminal, or via a Telnet or SSH client such as PuTTY.

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

Logging in to CLI

Logging in via HyperTerminal over a local connection is a little different than logging in using SSH or Telnet.

If a security login agreement has been enabled, you must accept the agreement in order to complete the login. Users are authenticated first and the security banner is checked afterwards.

With HyperTerminal

You can use any terminal emulation programs for local access to the command line interface.

This section illustrates HyperTerminal, which is part of Windows operating systems prior to Windows Vista.

► **To log in using HyperTerminal:**

1. Connect your computer to the product via a local (USB or RS-232) connection.
2. Launch HyperTerminal on your computer and open a console window. When the window first opens, it is blank.

Make sure the COM port settings use this configuration:

- Bits per second = 115200 (115.2Kbps)
- Data bits = 8
- Stop bits = 1
- Parity = None
- Flow control = None

3. In the communications program, press Enter to send a carriage return to the PRO3X. The Username prompt appears.

Using the PRO3X Command Line Interface (CLI)

Username: _

4. Type a name and press Enter. The name is case sensitive. Then you are prompted to enter a password.

```
Username: admin
Password: _
```

5. Type a password and press Enter. The password is case sensitive.
After properly entering the password, the # or > system prompt appears.

Tip: The 'Last login' information, including the date and time, is also displayed if the same user account was used to log in to this product's web interface or CLI.

6. You are now logged in to the command line interface and can begin administering this product.

With SSH or Telnet

You can remotely log in to the command line interface (CLI) using an SSH or Telnet client, such as PuTTY.

Note: PuTTY is a free program you can download from the Internet. Refer to PuTTY's documentation for details on configuration.

► To log in using SSH or Telnet:

1. Ensure SSH or Telnet has been enabled.
2. Launch an SSH or Telnet client and open a console window. A login prompt appears.

```
login as: █
```

3. Type a name and press Enter. The name is case sensitive.

Note: If using the SSH client, the name must NOT exceed 25 characters. Otherwise, the login fails.

Then you are prompted to enter a password.

```
login as: admin
admin@192.168.84.88's password: █
```

4. Type a password and press Enter. The password is case sensitive.
5. After properly entering the password, the # or > system prompt appears..

Tip: The 'Last login' information, including the date and time, is also displayed if the same user account was used to log in to this product's web interface or CLI.

6. You are now logged in to the command line interface and can begin administering this product.

With an Analog Modem

The PRO3X supports remote access to the CLI via a connected analog modem. This feature is especially useful when the LAN access is not available.

▶ To connect to the PRO3X via the modem:

1. Make sure the PRO3X has an analog modem connected.
2. Make sure the computer you are using has an appropriate modem connected.
3. Launch a terminal emulation program, and configure its baud rate settings according to the baud rate set for the analog modem connected to the PRO3X.
4. Type the following AT command to make a connection with the PRO3X.

```
ATD<modem phone number>
```

5. The CLI login prompt appears after the connection is established successfully. Then type the user name and password to log in to the CLI.

▶ To disconnect from the PRO3X:

6. Return to the modem's command mode using the escape code +++.
7. After the OK prompt appears, type the following AT command to disconnect from the PRO3X.

```
ATH
```

Different CLI Modes and Prompts

Depending on the login name you use and the mode you enter, the system prompt in the CLI varies.

User Mode: When you log in as a normal user, who may not have full permissions to configure the PRO3X, the > prompt appears.

Administrator Mode: When you log in as an administrator, who has full permissions to configure the PRO3X, the # prompt appears.

Configuration Mode: You can enter the configuration mode from the administrator or user mode. In this mode, the prompt changes to **config:#** or **config:>** and you can change PRO3X device and network configurations.

Diagnostic Mode: You can enter the diagnostic mode from the administrator or user mode. In this mode, the prompt changes to **diag:#** or **diag:>** and you can perform the network troubleshooting commands, such as the ping command.

Closing the Local Connection

Close the window or terminal emulation program when you finish accessing the PRO3X over the local connection.

When accessing or upgrading multiple PRO3X devices, do not transfer the local connection cable from one device to another without closing the local connection window first.

The ? Command for Showing Available Commands

When you are not familiar with CLI commands, you can press the ? key at any time for one of the following purposes.

Show a list of main CLI commands available in the current mode.

Show a list of available commands or parameters for the command you type.

▶ **In the administrator mode:**

```
#          ?
```

▶ **In the configuration mode:**

```
config:#  ?
```

▶ **In the diagnostic mode:**

```
diag:#    ?
```

Press Enter after pressing the ? command, and a list of main commands for the current mode is displayed.

Querying Available Parameters for a Command

If you are not sure what commands or parameters are available for a particular type of CLI command or its syntax, you can have the CLI show them by adding a space and the help command (?) or list command (ls) to the end of that command. A list of available parameters and their descriptions will be displayed.

The following shows a few query examples.

▶ **To query available parameters for the "show" command:**

```
# show ?
```

▶ **To query available parameters for the "show user" command:**

```
# show user ?
```

▶ **To query available role configuration parameters:**

```
config:# role ?
```

▶ **To query available parameters for the "role create" command:**

```
config:# role create ?
```

Showing Information

You can use the show commands to view current settings or the status of the PRO3X device or part of it, such as the IP address, networking mode, firmware version, states or readings of internal or external sensors, user profiles, and so on.

Some "show" commands have two formats: one with the parameter "details" and the other without. The difference is that the command without the parameter "details" displays a shortened version of information while the other displays in-depth information.

After typing a "show" command, press Enter to execute it.

Note: Depending on your login name, the # prompt may be replaced by the > prompt.

Network Configuration

This command shows all network configuration and all network interfaces' information, such as the IP address, MAC address, the Ethernet interfaces' duplex mode, and the wireless interface's status/settings.

```
# show network
```

IP Configuration

This command shows the IP settings shared by all network interfaces, such as DNS and routes. Information shown will include both IPv4 and IPv6 configuration.

```
# show network ip common
```

To show the IP settings of a specific network interface, use the following command.

```
# show network ip interface <ETH>
```

Variables:

<ETH> is one of the network interfaces: *ETH1/ETH2*, *WIRELESS*, or *BRIDGE*. Note that you must choose/configure the bridge interface if your PRO3X is set to the bridging mode.

Note: 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.

Interface	Description
eth1	Show the IP-related configuration of the ETH1 interface.
eth2	Show the IP-related configuration of the ETH2 interface.
wireless	Show the IP-related configuration of the WIRELESS interface.
bridge	Show the IP-related configuration of the BRIDGE interface.
all	Show the IP-related configuration of all interfaces. <i>Tip: You can also type the command without adding this option "all" to get the same data. That is, show network ip interface.</i>

IPv4-Only or IPv6-Only Configuration

To show IPv4-only or IPv6-only configuration, use any of the following commands.

- ▶ To show IPv4 settings shared by all network interfaces, such as DNS and routes:

```
# show network ipv4 common
```

- ▶ To show IPv6 settings shared by all network interfaces, such as DNS and routes:

```
# show network ipv6 common
```

- ▶ To show the IPv4 configuration of a specific network interface:

```
# show network ipv4 interface <ETH>
```

- ▶ To show the IPv6 configuration of a specific network interface:

```
# show network ipv6 interface <ETH>
```

Variables:

<ETH> is one of the network interfaces: *ETH1/ETH2*, *WIRELESS*, or *BRIDGE*. Note that you must choose/configure the bridge interface if your PRO3X is set to the bridging mode.

Note: 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.

Interface	Description
eth1	Show the IPv4 or IPv6 configuration of the ETH1 interface.
eth2	Show the IPv4 or IPv6 configuration of the ETH2 interface.
wireless	Show the IPv4 or IPv6 configuration of the WIRELESS interface.
bridge	Show the IPv4 or IPv6 configuration of the BRIDGE interface.

Interface	Description
all	Show the IPv4 or IPv6 configuration of all interfaces. <i>Tip: You can also type the command without adding this option "all" to get the same data. That is, show network ipv4 interface.</i>

Network Interface Settings

This command shows the specified network interface's information which is NOT related to IP configuration. For example, the Ethernet port's LAN interface speed and duplex mode, or the wireless interface's SSID parameter and authentication protocol.

```
# show network interface <ETH>
```

Variables:

<ETH> is one of the network interfaces: *ETH1/ETH2*, *WIRELESS*, or *BRIDGE*. Note that you must choose/configure the bridge interface if your PRO3X is set to the bridging mode.

Note: 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.

Interface	Description
eth1	Show the ETH1 interface's non-IP settings.
eth2	Show the ETH2 interface's non-IP settings.
wireless	Show the WIRELESS interface's non-IP settings.
bridge	Show the BRIDGE interface's non-IP settings.
all	Show the non-IP settings of all interfaces. <i>Tip: You can also type the command without adding this option "all" to get the same data. That is, show network interface.</i>

Network Service Settings

This command shows the network service settings only, including the Telnet setting, TCP ports for HTTP, HTTPS, SSH and Modbus/TCP services, and SNMP settings.

```
# show network services <option>
```

Variables:

<option> is one of the options: *all, http, https, telnet, ssh, snmp, modbus* and *zeroconfig*.

Option	Description
all	Displays the settings of all network services, including HTTP, HTTPS, Telnet, SSH and SNMP. <i>Tip: You can also type the command without adding this option "all" to get the same data.</i>
http	Only displays the TCP port for the HTTP service.
https	Only displays the TCP port for the HTTPS service.
telnet	Only displays the settings of the Telnet service.
ssh	Only displays the settings of the SSH service.
snmp	Only displays the SNMP settings.
modbus	Only displays the settings of the Modbus/TCP service.
zeroconfig	Only displays the settings of the zero configuration advertising.

PDU Configuration

This command shows the PDU configuration, such as the device name, firmware version, model type and upper limit of active powered dry contact actuators.

```
# show pdu
```

To show detailed information, add the parameter "details" to the end of the command.

```
# show pdu details
```


Outlet Information

This command syntax shows the outlet information.

```
# show outlets <n>
```

To show detailed information, add the parameter "details" to the end of the command.

```
# show outlets <n> details
```

Variables:

<n> is one of the options: *all*, or a number.

Option	Description
all	Displays the information for all outlets. <i>Tip: You can also type the command without adding this option "all" to get the same data.</i>
A specific outlet number	Displays the information for the specified outlet only.

Displayed information:

Without the parameter **details** only the outlet name is displayed.

With the parameter **details** more outlet information is displayed in addition to the outlet name, such as the outlet rating.

Inlet Information

This command syntax shows the inlet information.

```
# show inlets <n>
```

To show detailed information, add the parameter "details" to the end of the command.

```
# show inlets <n> details
```

Variables:

<n> is one of the options: *all*, or a number.

Option	Description
all	Displays the information for all inlets. <i>Tip: You can also type the command without adding this option "all" to get the same data.</i>
A specific inlet number	Displays the information for the specified inlet only. An inlet number needs to be specified only when there are more than 1 inlet on your PDU.

Displayed information:

Without the parameter **details** only the inlet's name and RMS current are displayed.

With the parameter **details** more inlet information is displayed in addition to the inlet name and RMS current, such as the inlet's RMS voltage, active power and active energy.

Overcurrent Protector Information

This command is only available for models with overcurrent protectors for protecting outlets.

This command syntax shows the overcurrent protector information, such as a circuit breaker or a fuse.

```
# show ocp <n>
```

To show detailed information, add the parameter "details" to the end of the command.

```
# show ocp <n> details
```

Variables:

<n> is one of the options: *all*, or a number.

Option	Description
all	Displays the information for all overcurrent protectors. <i>Tip: You can also type the command without adding this option "all" to get the same data.</i>
A specific overcurrent protector number	Displays the information for the specified overcurrent protector only.

Using the PRO3X Command Line Interface (CLI)

Displayed information:

Without the parameter **details** only the overcurrent protector status and name are displayed.

With the parameter **details** more overcurrent protector information is displayed in addition to status, such as the rating and RMS current value.

Date and Time Settings

This command shows the current date and time settings on the PRO3X.

```
# show time
```

To show detailed information, add the parameter "details" to the end of the command.

```
# show time details
```

Default Measurement Units

This command shows the default measurement units applied to the PRO3X web and CLI interfaces across all users, especially those users authenticated through remote authentication servers.

```
# show user defaultPreferences
```

Note: If a user has set their own preferred measurement units or the administrator has changed any user's preferred units, the web and CLI interfaces show the preferred measurement units for that user instead of the default ones.

Environmental Sensor Information

This command syntax shows the environmental sensor's information.

```
# show externalsensors <n>
```

To show detailed information, add the parameter "details" to the end of the command.

```
# show externalsensors <n> details
```

```
# show externalsensors 2 details
External sensor 2 ('Temperature 2')
Sensor type: Temperature
Reading:      24.0 deg C (normal)

Serial number:      QMSemu0004
Description:        Not configured
Location:           X Not configured
                   Y Not configured
                   Z Not configured
Position:           Port 1, Chain Position 4
Using default thresholds: yes
```

Variables:

<n> is one of the options: *all*, or a number.

Option	Description
all	Displays the information of all environmental sensors. <i>Tip: You can also type the command without adding this option "all" to get the same data.</i>
A specific environmental sensor number*	Displays the information for the specified environmental sensor only.

* The environmental sensor number is the ID number assigned to the sensor, which can be found on the Peripherals page of the PRO3X web interface.

Displayed information:

Without the parameter **details** only the sensor ID, sensor type and reading are displayed.

Note: A state sensor displays the sensor state instead of the reading.

Using the PRO3X Command Line Interface (CLI)

With the parameter **details** more information is displayed in addition to the ID number and sensor reading, such as the serial number, sensor position, and X, Y, and Z coordinates.

Environmental Sensor Package Information

Different from the "show externalsensors" commands, which show the reading, status and configuration of an individual environmental sensor, the following command shows the information of all connected environmental sensor packages, each of which may contain more than one sensor or actuator.

```
# show peripheralDevicePackages
```

Information similar to the following is displayed. Peripheral Device Package refers to an environmental sensor package.

```
Peripheral Device Package 1
Serial Number: 1GE7A00022
Package Type: DX2-T1H1
Position: Port 1, Chain Position 1
Package State: operational
Firmware Version: 33.0
```

```
Peripheral Device Package 2
Serial Number: 1GE7A00021
Package Type: DX2-T3H1
Position: Port 1, Chain Position 2
Package State: operational
Firmware Version: 33.0
```

Actuator Information

This command syntax shows an actuator's information.

```
# show actuators <n>
```

To show detailed information, add the parameter "details" to the end of the command.

```
# show actuators <n> details
```

Variables:

<n> is one of the options: *all*, or a number.

Option	Description
all	Displays the information for all actuators. <i>Tip: You can also type the command without adding this option "all" to get the same data.</i>
A specific actuator number*	Displays the information for the specified actuator only.

* The actuator number is the ID number assigned to the actuator. The ID number can be found using the PRO3X web interface or CLI. It is an integer starting at 1.

Displayed information:

Without the parameter **details** only the actuator ID, type and state are displayed.

With the parameter **details** more information is displayed in addition to the ID number and actuator state, such as the serial number and X, Y, and Z coordinates.

Inlet Sensor Threshold Information

This command syntax shows the specified inlet sensor's threshold-related information.

```
# show sensor inlet <n> <sensor type>
```

To show detailed information, add the parameter "details" to the end of the command.

```
# show sensor inlet <n> <sensor type> details
```

Variables:

<n> is the number of the inlet whose sensors you want to query. For a single-inlet PDU, <n> is always 1.

<sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor
unbalancedCurrent	Unbalanced load sensor
lineFrequency	Line frequency sensor

Displayed information:

Without the parameter **details** only the reading, state, threshold, de-assertion hysteresis and assertion timeout settings of the specified inlet sensor are displayed.

With the parameter **details** more sensor information is displayed, including resolution and range.

If the requested sensor type is not supported, the "Sensor is not available" message is displayed.

► Additional sensors supported by specific models:

Specific PRO3X models support some or all of the following sensors. The CLI command(s) listed above can be also applied to the following sensors. Note that the measurement unit of current values in CLI is **A**, not mA.

Sensor type	Description
peakCurrent	Peak current sensor
reactivePower	Reactive power sensor
displacementPowerFactor	Displacement power factor sensor
residualCurrent	RCM current sensor <ul style="list-style-type: none"> ▪ For Type A, it is the sensor that detects residual AC current. ▪ For Type B, it is the sensor that detects both residual AC and DC current.
residualDCCurrent	RCM DC current sensor - detects residual DC current only. Available only on PDUs with RCM Type B.

Inlet Pole Sensor Threshold Information

This command syntax shows the specified inlet pole sensor's threshold-related information.

```
# show sensor inletpole <n> <p> <sensor type>
```

To show detailed information, add the parameter "details" to the end of the command.

```
# show sensor inletpole <n> <p> <sensor type> details
```

Variables:

<n> is the number of the inlet whose pole sensors you want to query. For a single-inlet PDU, <n> is always 1.

<p> is the label of the inlet pole whose sensors you want to query.

Pole	Label <p>	Current sensor	Voltage sensor
1	L1	L1	L1 - L2
2	L2	L2	L2 - L3
3	L3	L3	L3 - L1

<sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor

Displayed information:

Without the parameter **details** only the reading, state, threshold, de-assertion hysteresis and assertion timeout settings of the specified inlet pole sensor are displayed.

With the parameter **details** more sensor information is displayed, including resolution and range.

If the requested sensor type is not supported, the "Sensor is not available" message is displayed.

► Additional sensors supported by specific models:

Specific PRO3X models support some or all of the following sensors. The CLI command(s) listed above can be also applied to the following sensors. Note that the measurement unit of current values in CLI is **A**, not mA.

Sensor type	Description
peakCurrent	Peak current sensor
reactivePower	Reactive power sensor
displacementPowerFactor or	Displacement power factor sensor
residualCurrent	RCM current sensor <ul style="list-style-type: none"> ▪ For Type A, it is the sensor that detects residual AC current. ▪ For Type B, it is the sensor that detects both residual AC and DC current.
residualDCCurrent	RCM DC current sensor - detects residual DC current only. Available only on PDUs with RCM Type B.

Overcurrent Protector Sensor Threshold Information

This command is only available for models with overcurrent protectors for protecting outlets.

This command syntax shows the specified overcurrent protector sensor's threshold-related information.

```
# show sensor ocp <n> <sensor type>
```

To show detailed information, add the parameter "details" to the end of the command.

```
# show sensor ocp <n> <sensor type> details
```

Variables:

<n> is the number of the overcurrent protector whose sensors you want to query.

<sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor

Displayed information:

Without the parameter **details** only the reading, state, threshold, de-assertion hysteresis and assertion timeout settings of the specified overcurrent protector sensor are displayed.

With the parameter **details** more sensor information is displayed, including resolution and range.

Environmental Sensor Threshold Information

This command syntax shows the specified environmental sensor's threshold-related information.

```
# show sensor externalsensor <n>
```

To show detailed information, add the parameter "details" to the end of the command.

```
# show sensor externalsensor <n> details
```

```
External sensor 1 (Temperature):
Reading: 22.6 deg C
State: normal

Active Thresholds: Default thresholds

Default Thresholds for Temperature sensors:
Lower critical threshold: 10.0 deg C
Lower warning threshold: 15.0 deg C
Upper warning threshold: 30.0 deg C
Upper critical threshold: 35.0 deg C
Deassertion hysteresis: 1.0 deg C
Assertion timeout: 0 samples

Sensor Specific Thresholds:
Lower critical threshold: 10.0 deg C
Lower warning threshold: 15.0 deg C
Upper warning threshold: 30.0 deg C
Upper critical threshold: 35.0 deg C
Deassertion hysteresis: 1.0 deg C
Assertion timeout: 0 samples
```

Variables:

<n> is the environmental sensor number. The environmental sensor number is the ID number assigned to the sensor, which can be found on the Peripherals page of the PRO3X web interface.

Displayed information:

Without the parameter **details** only the reading, threshold, de-assertion hysteresis and assertion timeout settings of the specified environmental sensor are displayed.

With the parameter **details** more sensor information is displayed, including resolution and range.

Note: For a state sensor, the threshold-related and accuracy-related data is NOT available.

Environmental Sensor Default Thresholds

This command syntax shows a certain sensor type's default thresholds, which are the initial thresholds applying to the specified type of sensor.

```
# show defaultThresholds <sensor type>
```

To show detailed information, add the parameter "details" to the end of the command.

```
# show defaultThresholds <sensor type> details
```

Variables:

<sensor type> is one of the following numeric sensor types:

Sensor types	Description
absoluteHumidity	Absolute humidity sensors
relativeHumidity	Relative humidity sensors
temperature	Temperature sensors
airPressure	Air pressure sensors
airFlow	Air flow sensors
vibration	Vibration sensors
all	All of the above numeric sensors
	<i>Tip: You can also type the command without adding this option "all" to get the same data.</i>

Displayed information:

Without the parameter **details** only the default upper and lower thresholds, de-assertion hysteresis and assertion timeout settings of the specified sensor type are displayed.

With the parameter **details** the threshold range is displayed in addition to default thresholds settings.

Security Settings

This command shows the security settings of the PRO3X.

```
# show security
```

To show detailed information, add the parameter "details" to the end of the command.

```
# show security details
```

Displayed information:

Without the parameter **details** the information including IP access control, role-based access control, password policy, and HTTPS encryption is displayed.

With the parameter **details** more security information is displayed, such as user blocking time, user idle timeout and front panel permissions (if supported by your model).

Authentication Settings

▶ General authentication settings:

This command displays the authentication settings of the PRO3X, including both LDAP and Radius settings.

```
# show authentication
```

▶ One LDAP server's settings:

To show the configuration of a specific LDAP server, assign the desired LDAP server with its sequential number in the command. To get detailed information, add "details" to the end of the command.

```
# show authentication ldapServer <server_num>
```

-- OR --

```
# show authentication ldapServer <server_num>
```

▶ One Radius server's settings:

To show the configuration of a specific Radius server, assign the desired Radius server with its sequential number in the command. To get detailed information, add "details" to the end of the command.

```
# show authentication radiusServer <server_num>
```

-- OR --

```
# show authentication radiusServer <server_num> details
```

Variables:

<server_num> is the sequential number of the specified authentication server on the LDAP or Radius server list.

Displayed information:

Without specifying any server, PRO3X shows the authentication type and a list of both LDAP and Radius servers that have been configured.

When specifying a server, only that server's basic configuration is displayed, such as IP address and port number.

With the parameter "details" added, detailed information of the specified server is displayed, such as an LDAP server's bind DN and the login name attribute, or a Radius server's timeout and retries values.

Existing User Profiles

This command shows the data of one or all existing user profiles.

```
# show user <user_name>
```

To show detailed information, add the parameter "details" to the end of the command.

```
# show user <user_name> details
```

Variables:

<user_name> is the name of the user whose profile you want to query. The variable can be one of the options: *all* or a user's name.

Option	Description
all	This option shows all existing user profiles. <i>Tip: You can also type the command without adding this option "all" to get the same data.</i>
a specific user's name	This option shows the profile of the specified user only.

Displayed information:

Without the parameter **details** only four pieces of user information are displayed: user name, user "Enabled" status, SNMP v3 access privilege, and role(s).

With the parameter **details** more user information is displayed, such as the telephone number, e-mail address, preferred measurement units and so on.

Existing Roles

This command shows the data of one or all existing roles.

```
# show roles <role_name>
```

Using the PRO3X Command Line Interface (CLI)

Variables:

<role_name> is the name of the role whose permissions you want to query. The variable can be one of the following options:

Option	Description
all	This option shows all existing roles. <i>Tip: You can also type the command without adding this option "all" to get the same data.</i>
a specific role's name	This option shows the data of the specified role only.

Displayed information:

Role settings are displayed, including the role description and privileges.

Serial Port Settings

This command shows the baud rate setting of the serial port labeled CONSOLE / MODEM on the PRO3X.

```
# show serial
```

EnergyWise Settings

This command shows the PRO3X device's current configuration for Cisco® EnergyWise.

```
# show energywise
```

Asset Strip Settings

This command shows the asset strip settings, such as the total number of rack units (tag ports), asset strip state, numbering mode, orientation, available tags and LED color settings.

```
# show assetStrip <n>
```


Variables:

<n> is one of the options: *all*, or a number.

Option	Description
all	Displays all asset strip information. <i>Tip: You can also type the command without adding this option "all" to get the same data.</i>
A specific asset strip number	Displays the settings of the asset strip connected to the specified FEATURE port number. For the PRO3X device with only one FEATURE port, the valid number is always 1.

Rack Unit Settings of an Asset Strip

A rack unit refers to a tag port on the asset strips. This command shows the settings of a specific rack unit or all rack units on an asset strip, such as a rack unit's LED color and LED mode.

```
# show rackUnit <n> <rack_unit>
```

Variables:

<n> is the number of the FEATURE port where the selected asset strip is physically connected. For the PRO3X device with only one FEATURE port, the number is always 1.

<rack_unit> is one of the options: *all* or a specific rack unit's index number.

Option	Description
all	Displays the settings of all rack units on the specified asset strip. <i>Tip: You can also type the command without adding this option "all" to get the same data.</i>
A specific number	Displays the settings of the specified rack unit on the specified asset strip. Use the index number to specify the rack unit. The index number is available on the asset strip or the Asset Strip page of the web interface.

Event Log

The command used to show the event log begins with `show eventlog`. You can add either the *limit* or *class* parameters or both to show specific events.

▶ **Show the last 30 entries:**

```
# show eventlog
```

▶ **Show a specific number of last entries in the event log:**

```
# show eventlog limit <n>
```

▶ **Show a specific type of events only:**

```
# show eventlog class <event_type>
```

▶ **Show a specific number of last entries associated with a specific type of events only:**

```
# show eventlog limit <n> class <event_type>
```

Variables:

<n> is one of the options: *all* or a number.

Option	Description
all	Displays all entries in the event log.
An integer number	Displays the specified number of last entries in the event log. The number ranges between 1 to 10,000.

<event_type> is one of the following event types.

Event type	Description
all	All events.
device	Device-related events, such as system starting or firmware upgrade event.
userAdministration	User management events, such as a new user profile or a new role.
userActivity	User activities, such as login or logout.
pdu	Displays PDU-related events.
sensor	Internal or external sensor events, such as state changes of any sensors.

Event type	Description
serverMonitor	Server-monitoring records, such as a server being declared reachable or unreachable.
assetManagement	Asset management events, such as asset tag connections or disconnections.
lhx	Schroff® LHX/SHX heat exchanger events.
modem	Modem-related events.
timerEvent	Scheduled action events.
webcam	Events for webcam management, if available.
cardReader	Events for card reader management, if available.
energywise	Cisco EnergyWise-related events, such as enabling the support of the EnergyWise function.

Network Connections Diagnostic Log

This command shows the diagnostic log for both the EAP authentication and wireless LAN connection.

```
# show network diagLog
```

Server Reachability Information

This command shows all server reachability information with a list of monitored servers and status.

```
# show serverReachability
```

Server Reachability Information for a Specific Server

To show the server reachability information for a certain IT device only, use the following command.

```
# show serverReachability server <n>
```

To show detailed information, add the parameter "details" to the end of the command.

```
# show serverReachability server <n> details
```

Variables:

<n> is a number representing the sequence of the IT device in the monitored server list.

You can find each IT device's sequence number using the CLI command of `show serverReachability` as illustrated below.

#	IP address	Enabled	Status
1	192.168.84.126	Yes	Waiting for reliable connection
2	www.raritan.com	Yes	Waiting for reliable connection

Displayed information:

Without the parameter **details** only the specified device's IP address, monitoring enabled/disabled state and current status are displayed.

With the parameter **details** more settings for the specified device are displayed, such as number of pings and wait time prior to the next ping.

Command History

This command shows the command history for current connection session.

```
# show history
```

Displayed information:

A list of commands that were previously entered in the current session is displayed.

Reliability Data

This command shows the reliability data.

```
# show reliability data
```

Reliability Error Log

This command shows the reliability error log.

```
# show reliability errorlog <n>
```

Variables:

<n> is one of the options: 0 (zero) or any other integer number.

Option	Description
0	Displays all entries in the reliability error log. <i>Tip: You can also type the command without adding this option "0" to get all data.</i>
A specific integer number	Displays the specified number of last entries in the reliability error log.

Reliability Hardware Failures

This command shows a list of detected hardware failures.

```
# show reliability hwfailures
```

Examples

This section provides examples of the show command.

Example 1 - Basic Security Information

The diagram shows the output of the *show security* command.

```
# show security
IPv4 access control: Disabled

IPv6 access control: Disabled

Role based access control for IPv4: Disabled
Role based access control for IPv6: Disabled

Password aging: Disabled

Prevent concurrent user login: No

Strong passwords: Disabled

Restricted Service Agreement: disabled
```

Example 2 - In-Depth Security Information

More information is displayed when typing the *show security details* command.

```
# show security details
IPv4 access control: Disabled

IPv6 access control: Disabled

Role based access control for IPv4: Disabled
Role based access control for IPv6: Disabled

Password aging: Disabled

Prevent concurrent user login: No
Maximum number of failed logins: 3
User block time: 10 minutes

User idle timeout: 10 minutes

Strong passwords: Disabled

Restricted Service Agreement: disabled
Restricted Service Agreement Banner Content:
Unauthorized access prohibited; all access and activities not explicitly
authorized by management are unauthorized. All activities are monitored
and logged. There is no privacy on this system. Unauthorized access
and activities or any criminal activity will be reported to appropriate
authorities.

Front-Panel Permissions:
Switch Outlet: no
Switch Peripheral Actuator: no
```

Example 3 - Basic PDU Information

This example shows the output of the *show pdu* command.

```
# show pdu
PDU 'my PX'
Model: PX3-XXXX
Firmware Version: 2.X.0.5-40956
```

Example 4 - In-Depth PDU Information

More information is displayed when typing the `show pdu details` command. Displayed information varies depending on the model you purchased.

```
# show pdu details
PDU 'my PX'
Model:          PX3-XXXX
Firmware Version: 2.X.0.5-40956
Serial Number:  QGZ9792136
Board Revision:  0x01

Voltage rating:  200-240V
Current rating:  16A
Frequency rating: 50/60Hz
Power rating:    3.2-3.8kVA

Sensor data retrieval: Enabled
Measurements per log entry: 60

External sensor Z coordinate format: Rack units
Device altitude:          0 m
```

Clearing Information

You can use the clear commands to remove unnecessary data from the PRO3X.

After typing a "clear" command, press Enter to execute it.

Note: Depending on your login name, the # prompt may be replaced by the > prompt.

Clearing Event Log

This command removes all data from the event log.

```
#          clear eventlog

-- OR --

#          clear eventlog /y
```

If you entered the command without `/y`, a message appears, prompting you to confirm the operation. Type `y` to clear the event log or `n` to abort the operation.

If you type `y`, a message "Event log was cleared successfully" is displayed after all data in the event log is deleted.

Clearing Diagnostic Log for Network Connections

This command removes all data from the diagnostic log for both the EAP authentication and WLAN connection.

```
# clear networkDiagLog  
  
-- OR --  
  
# clear networkDiagLog /y
```

If you entered the command without "/y," a message appears, prompting you to confirm the operation. Type `y` to clear the log or `n` to abort the operation.

Configuring the PRO3X Device and Network

To configure the PRO3X device or network settings through the CLI, it is highly recommended to log in as the administrator so that you have full permissions.

To configure any settings, enter the configuration mode. Configuration commands are case sensitive so ensure you capitalize them correctly.

Entering Configuration Mode

Configuration commands function in configuration mode only.

► To enter configuration mode:

1. Ensure you have entered administrator mode and the # prompt is displayed.

Note: If you enter configuration mode from user mode, you may have limited permissions to make configuration changes.

2. Type `config` and press Enter.
3. The `config:#` prompt appears, indicating that you have entered configuration mode.

```
config:# _
```

4. Now you can type any configuration command and press Enter to change the settings.

Important: To apply new configuration settings, you must issue the "apply" command before closing the terminal emulation program. Closing the program does not save any configuration changes.

Quitting Configuration Mode

Both of "apply" and "cancel" commands let you quit the configuration mode. The difference is that "apply" saves all changes you made in the configuration mode while "cancel" aborts all changes.

► **To quit the configuration mode, use either command:**

```
config:#   apply
           -- OR --
config:#   cancel
```

The # or > prompt appears after pressing Enter, indicating that you have entered the administrator or user mode.

PDU Configuration Commands

One PDU configuration command begins with *pdu*. You can use the PDU configuration commands to change the settings that apply to the whole PRO3X device.

Configuration commands are case sensitive so ensure you capitalize them correctly.

Changing the PDU Name

This command changes the device name of PRO3X.

```
config:#   pdu name "<name>"
```

Variables:

<name> is a string comprising up to 64 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.

Enabling or Disabling Data Logging

This command enables or disables the data logging feature.

```
config:#   pdu dataRetrieval <option>
```

Variables:

<option> is one of the options: *enable* or *disable*.

Option	Description
enable	Enables the data logging feature.
disable	Disables the data logging feature.

Setting Data Logging Measurements Per Entry

This command defines the number of measurements accumulated per log entry.

```
config:# pdu measurementsPerLogEntry <number>
```

Variables:

<number> is an integer between 1 and 600. The default is 60 samples per log entry.

Specifying the Device Altitude

This command specifies the altitude of your PRO3X above sea level (in meters). You must specify the altitude of PRO3X above sea level if a differential air pressure sensor is attached. This is because the device's altitude is associated with the altitude correction factor.

```
config:# pdu deviceAltitude <altitude>
```

Variables:

<altitude> is an integer between -425 and 3000 meters.

Note that the lower limit "-425" is a negative value because some locations are below the seal level.

Setting the Z Coordinate Format for Environmental Sensors

This command enables or disables the use of rack units for specifying the height (Z coordinate) of environmental sensors.

```
config:# pdu externalSensorsZCoordinateFormat <option>
```

Variables:

<option> is one of the options: *rackUnits* or *freeForm*.

Option	Description
rackUnits	The height of the Z coordinate is measured in standard rack units. When this is selected, you can type a numeric value in the rack unit to describe the Z coordinate of any environmental sensors or actuators.

Option	Description
freeForm	Any alphanumeric string can be used for specifying the Z coordinate.

Enabling or Disabling Peripheral Device Auto Management

This command enables or disables the Peripheral Device Auto Management feature.

```
config:# pdu peripheralDeviceAutoManagement <option>
```

Variables:

<option> is one of the options: *enable* or *disable*.

Option	Description
enable	Enables the automatic management feature for environmental sensor packages.
disable	Disables the automatic management feature for environmental sensor packages.

Setting the Maximum Number of Active Powered Dry Contact Actuators

This command determines the upper limit of "active" powered dry contact actuators on one PRO3X device. You need either 'Change Peripheral Device Configuration' privilege or 'Administrator Privileges' to change its upper limit.

```
config:# pdu activePoweredDryContactLimit <number>
```

Variables:

<number> is the number representing the maximum number of active powered dry contact actuators. Its value ranges between 0 to 24.

Note: An "active" actuator is the one that is turned ON, or, if with a door handle connected, is OPENED.

Examples

This section illustrates several PDU configuration examples.

Example 1 - PDU Naming

The following command assigns the name "my PRO3X" to the PDU.

```
config:# pdu name "my pro3x"
```

Example 2 - Data Logging Enabled

The following command enables the data logging feature.

```
config:# pdu dataRetrieval enable
```

Network Configuration Commands

A network configuration command begins with *network*. A number of network settings can be changed through the CLI, such as the IP address, transmission speed, duplex mode, and so on.

Configuring IPv4 Parameters

An IPv4 configuration command begins with *network ipv4*.

Setting the IPv4 Configuration Mode

This command determines the IP configuration mode.

```
config:# network ipv4 interface <ETH> configMethod <mode>
```

Variables:

<ETH> is one of the network interfaces: *ETH1/ETH2*, *WIRELESS*, or *BRIDGE*. Note that you must choose/configure the bridge interface if your PRO3X is set to the bridging mode.

Note: 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.

Interface	Description
eth1	Determine the IPv4 configuration mode of the ETH1 interface (wired networking).
eth2	Determine the IPv4 configuration mode of the ETH2 interface (wired networking).
wireless	Determine the IPv4 configuration mode of the WIRELESS interface (that is, wireless networking).
bridge	Determine the IPv4 configuration mode of the BRIDGE interface (that is, bridging mode).

<mode> is one of the modes: *dhcp* or *static*.

Mode	Description
dhcp	The IPv4 configuration mode is set to DHCP.
static	The IPv4 configuration mode is set to static IP address.

Setting the IPv4 Preferred Host Name

After selecting DHCP as the IPv4 configuration mode, you can specify the preferred host name, which is optional. The following is the command:

```
config:# network ipv4 interface <ETH> preferredHostName <name>
```

Variables:

<ETH> is one of the network interfaces: *ETH1/ETH2*, *WIRELESS*, or *BRIDGE*. Note that you must choose/configure the bridge interface if your PRO3X is set to the bridging mode.

Note: 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.

Interface	Description
eth1	Determine the IPv4 preferred host name of the ETH1 interface (that is, wired networking).
eth2	Determine the IPv4 preferred host name of the ETH2 interface (that is, wired networking).
wireless	Determine the IPv4 preferred host name of the WIRELESS interface (that is, wireless networking).
bridge	Determine the IPv4 preferred host name of the BRIDGE interface (that is, bridging mode).

<name> is a host name which:

- 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

Using the PRO3X Command Line Interface (CLI)

Setting the IPv4 Address

After selecting the static IP configuration mode, you can use this command to assign a permanent IP address to the PRO3X.

```
config:# network ipv4 interface <ETH> address <ip address>
```

Variables:

<ETH> is one of the network interfaces: *ETH1/ETH2*, *WIRELESS*, or *BRIDGE*. Note that you must choose/configure the bridge interface if your PRO3X is set to the bridging mode.

Note: 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.

Interface	Description
eth1	Determine the IPv4 address of the ETH1 interface (that is, wired networking).
eth2	Determine the IPv4 address of the ETH2 interface (that is, wired networking).
wireless	Determine the IPv4 address of the WIRELESS interface (that is, wireless networking).
bridge	Determine the IPv4 address of the BRIDGE interface (that is, the bridging mode).

<ip address> is the IP address being assigned to your PRO3X. Its format is "IP address/prefix". For example, *192.168.84.99/24*.

Setting the IPv4 Gateway

After selecting the static IP configuration mode, you can use this command to specify the gateway.

```
config:# network ipv4 gateway <ip address>
```

Variables:

<ip address> is the IP address of the gateway. The value ranges from 0.0.0.0 to 255.255.255.255.

Setting IPv4 Static Routes

If the IPv4 network mode is set to static IP and your local network contains two subnets, you can configure static routes to enable or disable communications between the PRO3X and devices in the other subnet.

These commands are prefixed with *network ipv4 staticRoutes*.

Depending on whether the other network is directly reachable or not, there are two methods for adding a static route.

Using the PRO3X Command Line Interface (CLI)

Method 1: add a static route when the other network is NOT directly reachable:

```
network ipv4 staticRoutes add <dest-1> nextHop <hop>
```

▶ **Method 2: add a static route when the other network is directly reachable:**

```
network ipv4 staticRoutes add <dest-1> interface <ETH>
```

▶ **Delete an existing static route:**

```
network ipv4 staticRoutes delete <route_ID>
```

▶ **Modify an existing static route:**

```
network ipv4 staticRoutes modify <route_ID> dest <dest- 2> nextHop <hop>
```

--OR --

```
network ipv4 staticRoutes modify <route_ID> dest <dest-2> interface <ETH>
```

Variables:

<dest-1> is a combination of the IP address and subnet mask of the other subnet. The format is *IP address/subnet mask*.

<hop> is the IP address of the next hop router.

<ETH> is one of the interfaces: *ETH1/ETH2, WIRELESS* and *BRIDGE*. Type "bridge" only when your PRO3X is in the bridging mode.

<route_ID> is the ID number of the route setting which you want to delete or modify.

<dest-2> is a modified route setting that will replace the original route setting. Its format is *IP address/subnet mask*. You can modify either the IP address or the subnet mask or both.

Configuring IPv6 Parameters

An IPv6 configuration command begins with *network ipv6*.

Setting the IPv6 Configuration Mode

This command determines the IP configuration mode.

```
config:# network ipv6 interface <ETH> configMethod <mode>
```

Variables:

<ETH> is one of the network interfaces: *ETH1/ETH2*, *WIRELESS*, or *BRIDGE*. Note that you must choose/configure the bridge interface if your PRO3X is set to the bridging mode.

Note: 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.

Interface	Description
eth1	Determine the IPv6 configuration mode of the ETH1 interface (wired networking).
eth2	Determine the IPv6 configuration mode of the ETH2 interface (wired networking).
wireless	Determine the IPv6 configuration mode of the WIRELESS interface (that is, wireless networking).
bridge	Determine the IPv6 configuration mode of the BRIDGE interface (that is, bridging mode).

<mode> is one of the modes: *automatic* or *static*.

Mode	Description
automatic	The IPv6 configuration mode is set to automatic.
static	The IPv6 configuration mode is set to static IP address.

Setting the IPv6 Preferred Host Name

After selecting DHCP as the IPv6 configuration mode, you can specify the preferred host name, which is optional. The following is the command:

```
config:# network ipv6 interface <ETH> preferredHostName <name>
```

Using the PRO3X Command Line Interface (CLI)

Variables:

<ETH> is one of the network interfaces: *ETH1/ETH2*, *WIRELESS*, or *BRIDGE*. Note that you must choose/configure the bridge interface if your PRO3X is set to the bridging mode.

Note: 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.

Interface	Description
eth1	Determine the IPv6 preferred host name of the ETH1 interface (wired networking).
eth2	Determine the IPv6 preferred host name of the ETH2 interface (wired networking).
wireless	Determine the IPv6 preferred host name of the WIRELESS interface (that is, wireless networking).
bridge	Determine the IPv6 preferred host name of the BRIDGE interface (that is, bridging mode).

<name> is a host name which:

- 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

Setting the IPv6 Address

After selecting the static IP configuration mode, you can use this command to assign a permanent IP address to the PRO3X.

```
config:# network ipv6 interface <ETH> address <ip  
address>
```

Using the PRO3X Command Line Interface (CLI)

Variables:

<ETH> is one of the network interfaces: *ETH1/ETH2*, *WIRELESS*, or *BRIDGE*. Note that you must choose/configure the bridge interface if your PRO3X is set to the bridging mode.

Note: 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.

Interface	Description
eth1	Determine the IPv6 address of the ETH1 interface (wired networking).
eth2	Determine the IPv6 address of the ETH2 interface (wired networking).
wireless	Determine the IPv6 address of the WIRELESS interface (that is, wireless networking).
bridge	Determine the IPv6 address of the BRIDGE interface (that is, the bridging mode).

<ip address> is the IP address being assigned to your PRO3X. This value uses the IPv6 address format. Note that you must add /xx, which indicates a prefix length of bits such as /64, to the end of this IPv6 address.

Setting the IPv6 Gateway

After selecting the static IP configuration mode, you can use this command to specify the gateway.

```
config:# network ipv6 gateway <ip address>
```

Variables:

<ip address> is the IP address of the gateway. This value uses the IPv6 address format.

Setting IPv6 Static Routes

If the IPv6 network mode is set to static IP and your local network contains two subnets, you can configure static routes to enable or disable communications between the PRO3X and devices in the other subnet.

These commands are prefixed with *network ipv6 staticRoutes*.

Depending on whether the other network is directly reachable or not, there are two methods for adding a static route.

▶ **Method 1: add a static route when the other network is NOT directly reachable:**

```
network ipv6 staticRoutes add <dest-1> nextHop <hop>
```

▶ **Method 2: add a static route when the other network is directly reachable:**

```
network ipv6 staticRoutes add <dest-1> interface <ETH>
```

▶ **Delete an existing static route:**

```
network ipv6 staticRoutes delete <route_ID>
```

▶ **Modify an existing static route:**

```
network ipv6 staticRoutes modify <route_ID> dest <dest-2> nextHop <hop>
```

-- OR --

```
network ipv6 staticRoutes modify <route_ID> dest <dest-2> interface <ETH>
```

Variables:

<dest-1> is the IP address and prefix length of the subnet where the PRO3X belongs. The format is *IP address/prefix length*.

<hop> is the IP address of the next hop router.

<ETH> is one of the interfaces: *ETH1/ETH2*, *WIRELESS* and *BRIDGE*. Type "bridge" only when your PRO3X is in the bridging mode.

<route_ID> is the ID number of the route setting which you want to delete or modify.

<dest-2> is a modified route setting that will replace the original route setting. Its format is *IP address/prefix length*. You can modify either the IP address or the prefix length or both.

Configuring DNS Parameters

Use the following commands to configure static DNS-related settings.

▶ **Specify the primary DNS server:**

```
config:# network dns firstServer <ip address>
```

▶ **Specify the secondary DNS server:**

```
config:# network dns secondServer <ip address>
```

▶ **Specify the third DNS server:**

```
config:# network dns thirdServer <ip address>
```

▶ **Specify one or multiple optional DNS search suffixes:**

```
config:# network dns searchSuffixes <suffix1>
```

-- OR --

```
network dns searchSuffixes <suffix1>,<suffix2>,<suffix3>,...,<suffix6>
```

▶ **Determine which IP address is used when the DNS server returns both IPv4 and IPv6 addresses:**

```
config:# network dns resolverPreference <resolver>
```

Variables:

<ip address> is the IP address of the DNS server.

<suffix1>, <suffix2>, and the like are the DNS suffixes that automatically apply when searching for any device via PRO3X. You can specify up to 6 suffixes by separating them with commas.

<resolver> is one of the options: *preferV4* or *preferV6*.

Option	Description
preferV4	Use the IPv4 addresses returned by the DNS server.
preferV6	Use the IPv6 addresses returned by the DNS server.

Setting LAN Interface Parameters

A LAN interface configuration command begins with *network ethernet*.

Enabling or Disabling the LAN Interface

This command enables or disables the LAN interface.

```
config:# network ethernet <ETH> enabled <option>
```

Variables:

<ETH> is one of the options -- *eth1* or *eth2*.

Option	Description
eth1	ETH1 port
eth2	ETH2 port

<option> is one of the options: *true* or *false*.

Option	Description
true	The specified network interface is enabled.
false	The specified network interface is disabled.

Changing the LAN Interface Speed

This command determines the LAN interface speed.

```
config:# network ethernet <ETH> speed <option>
```

Variables:

<ETH> is one of the options -- *eth1* or *eth2*.

Option	Description
eth1	ETH1 port
eth2	ETH2 port

<option> is one of the options: *auto*, *10Mbps*, *100Mbps* or *1000Mbps*.

Option	Description
auto	System determines the optimum LAN speed through auto-negotiation.
10Mbps	The LAN speed is always 10 Mbps.
100Mbps	The LAN speed is always 100 Mbps.
1000Mbps	The LAN speed is always 1000 Mbps.

Changing the LAN Duplex Mode

This command determines the LAN interface duplex mode.

```
config:# network ethernet <ETH> duplexMode <mode>
```

Variables:

<ETH> is one of the options -- *eth1* or *eth2*.

Option	Description
eth1	ETH1 port
eth2	ETH2 port

<mode> is one of the modes: *auto*, *half* or *full*.

Option	Description
auto	The PRO3X selects the optimum transmission mode through auto-negotiation.
half	Half duplex: Data is transmitted in one direction (to or from the PRO3X) at a time.
full	Full duplex: Data is transmitted in both directions simultaneously.

Setting the Ethernet Authentication Method

This command sets the authentication method for the selected Ethernet interface to either none or Extensible Authentication Protocol (EAP).

```
config:# network ethernet <ETH> authMethod <method>
```

Variables:

<ETH> is one of the options -- *eth1* or *eth2*.

Option	Description
eth1	ETH1 port
eth2	ETH2 port

<method> is one of the authentication methods: *NONE* or *EAP*.

Method	Description
NONE	The authentication method is set to NONE.
EAP	The authentication method is set to EAP.

Setting Ethernet EAP Parameters

When the selected Ethernet interface's authentication method is set to EAP, you must configure EAP authentication parameters, including outer authentication, inner authentication, EAP identity, client certificate, client private key, password, CA certificate, and RADIUS authentication server.

▶ **Determine the outer authentication protocol:**

```
network ethernet <ETH> eapOuterAuthentication <outer_auth>
```

▶ **Determine the inner authentication protocol for authentication set to "EAP + PEAP":**

```
network ethernet <ETH> eapInnerAuthentication <inner_auth>
```

▶ **Set the EAP identity:**

```
config:# network ethernet <ETH> eapIdentity <identity>
```

▶ **Set the EAP password:**

```
config:# network ethernet <ETH> eapPassword
```

After performing the above command, the PRO3X prompts you to enter the password. Then type the password and press Enter.

▶ **Provide a client certificate for authentication set to "EAP + TLS" or "EAP + PEAP + TLS":**

```
config:# network ethernet <ETH> eapClientCertificate
```

After performing any certificate or private key commands, including commands for the client certificate, client private key, and CA certificate, the system prompts you to enter the contents of the wanted certificate or key.

▶ **Provide a client private key for authentication set to "EAP + TLS" or "EAP + PEAP + TLS":**

```
config:# network ethernet <ETH> eapClientPrivateKey
```

▶ **Provide a CA TLS certificate for EAP:**

```
config:# network ethernet <ETH> eapCACertificate
```

▶ **Enable or disable verification of the TLS certificate chain:**

```
network ethernet <ETH> enableCertVerification <option1>
```

▶ **Allow expired and not yet valid TLS certificates:**

```
network ethernet <ETH> allowOffTimeRangeCerts <option2>
```

▶ **Allow network connection with incorrect system time:**

Allow network connection with incorrect system time:

```
network ethernet <ETH> allowConnectionWithIncorrectClock <option3>
```

► **Set the RADIUS authentication server for EAP:**

```
config:# network ethernet <ETH> eapAuthServerName <FQDN>
```

Variables:

<ETH> is one of the options -- *eth1* or *eth2*.

Option	Description
eth1	ETH1 port
eth2	ETH2 port

<outer_auth> is one of the options: *PEAP* or *TLS*.

Option	Description
PEAP	Outer authentication is set to Protected Extensible Authentication Protocol (PEAP).
TLS	Outer authentication is set to TLS.

<inner_auth> is one of the options: *MS-CHAPv2* or *TLS*.

Option	Description
MSCHAPv2	Inner authentication is set to Microsoft's Challenge Authentication Protocol Version 2 (MS-CHAPv2).
TLS	Inner authentication is set to TLS.

<identity> is your user name for the EAP authentication.

<option1> is one of the options: *true* or *false*.

Option	Description
true	Enables the verification of the TLS certificate chain.
false	Disables the verification of the TLS certificate chain.

<option2> is one of the options: *true* or *false*.

Option	Description
true	Always make the network connection successful even though the TLS certificate chain contains any certificate which is outdated or not valid yet.
false	The network connection is NOT successfully established when the TLS certificate chain contains any certificate which is outdated or not valid yet.

<option3> is one of the options: *true* or *false*.

Option	Description
true	Make the network connection successful when the PRO3X system time is earlier than the firmware build before synchronizing with the NTP server, causing the TLS certificate to become invalid.
false	The network connection is NOT successfully established when the PRO3X finds that the TLS certificate is not valid due to incorrect system time.

<FQDN> is 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.

EAP CA Certificate Example

This section provides a CA certificate example for the Ethernet interface "ETH1". Your CA certificate contents should be different from the contents displayed in this example.

In addition, the procedure of uploading the client certificate and client private key in CLI is similar to the following example, except for the CLI command.

► To provide a CA certificate:

1. Make sure you have entered the configuration mode.
2. Type the following command for ETH1 and press Enter.

```
config:# network ethernet eth1 eapCACertificate
```

3. The system prompts you to enter the contents of the CA certificate.
4. Open a CA certificate using a text editor. You should see certificate contents similar to the following.

Using the PRO3X Command Line Interface (CLI)

```
--- BEGIN CERTIFICATE ---
MIICJTCCAfigAwIBAgIEMaYgRzALBqkqhkiG9w0BAQQwRTELMakGA1UEBhMCVVMx
NjA0BgNVBAAoTLU5hdGlvbmFsIEFlcm9uYXV0aWNzIGFuZCBTcGFjZSBBZG1pbmlz
dHJhdGlvbWAmFxE5NjA1MjgxmzQ5MDUrdMDgwMBcROUgWNTI4MTM0OTA1KzA4MDAw
ZzELMAkGA1UEBhMCVVMxNjA0BgNVBAAoTLU5hdGlvbmFsIEFlcm9uYXV0aWNzIGFu
ZCBTcGFjZSBBZG1pbmlzdHJhdGlvbWJgMAkGA1UEBRMCMTYwEwYDVQQDEwxdGV2
ZSBTY2hvY2gwWDALBqkqhkiG9w0BAQEDSQAwRgJBALrAwyYdgxmzNP/ts0Uyf6Bp
miJYktU/w4NG67ULa4B5CnEz7k57s9o3YY3LecETgQ5iQHmkwlyDTL2fTgVfw0C
AQOjgaswgagwZAYDVR0ZAQH/BFowWDBWMFQxCzAJBgNVBAYTAiVMTYwNAYDVQK
Ey1OYXRpb25hbCBBZjJvbmF1dG1jcyBhbmQGU3BhY2UgQWRtaW5pc3RyYXRpb24x
DTALBgNVBAMTBENSTDEwFwYDVR0BAQH/BA0wC4AJODMyOTcwODEwMBGGA1UdAgQR
MA8ECTgzMjk3MDgyM4ACBSAwDQYDVR0KBAYwBAMCBkAwCwYJKoZIhvcNAQEEA4GB
AH2y1VCEw/A4zaXzSYZJTUi3uawbbFiS2yxHvgf28+8Js0OHXk1H1w2d6qOHH21
X82tZXd/0JtG0g1T9usFFBDvYK800ebgz/P5ELJnBL2+atObEuJy1ZZ0pBDWINR3
WkDNLCGiTkCKp0F5EWIrVDwh54NNeVkcQRZita+z4IBO
--- END CERTIFICATE ---
```

5. Select and copy the contents as illustrated below, excluding the starting line containing "BEGIN CERTIFICATE" and the ending line containing "END CERTIFICATE."

```
MIICJTCCAfigAwIBAgIEMaYgRzALBqkqhkiG9w0BAQQwRTELMakGA1UEBhMCVVMxNjA0BgNVBAAoTLU5hdG
lvbmFsIEFlcm9uYXV0aWNzIGFuZCBTcGFjZSBBZG1pbmlzdHJhdGlvbWAmFxE5NjA1MjgxmzQ5MDUrdMDgw
MBcROUgWNTI4MTM0OTA1KzA4MDAwZzELMAkGA1UEBhMCVVMxNjA0BgNVBAAoTLU5hdGlvbmFsIEFlcm9uYX
V0aWNzIGFuZCBTcGFjZSBBZG1pbmlzdHJhdGlvbWJgMAkGA1UEBRMCMTYwEwYDVQQDEwxdGV2ZSBTY2hv
Y2gwWDALBqkqhkiG9w0BAQEDSQAwRgJBALrAwyYdgxmzNP/ts0Uyf6BpmiJYktU/w4NG67ULa4B5CnEz7
k57s9o3YY3LecETgQ5iQHmkwlyDTL2fTgVfw0CAQOjgaswgagwZAYDVR0ZAQH/BFowWDBWMFQxCzAJBgNV
BAYTAiVMTYwNAYDVQKQEy1OYXRpb25hbCBBZjJvbmF1dG1jcyBhbmQGU3BhY2UgQWRtaW5pc3RyYXRpb2
4xDTALBgNVBAMTBENSTDEwFwYDVR0BAQH/BA0wC4AJODMyOTcwODEwMBGGA1UdAgQRMA8ECTgzMjk3MDgy
M4ACBSAwDQYDVR0KBAYwBAMCBkAwCwYJKoZIhvcNAQEEA4GBAH2y1VCEw/A4zaXzSYZJTUi3uawbbFiS2
yxHvgf28+8Js0OHXk1H1w2d6qOHH21X82tZXd/0JtG0g1T9usFFBDvYK800ebgz/P5ELJnBL2+atObEuJy
1ZZ0pBDWINR3WkDNLCGiTkCKp0F5EWIrVDwh54NNeVkcQRZita+z4IBO
```

6. Paste the contents in the terminal.
7. Press Enter.
8. Verify whether the system shows the following command prompt, indicating the provided CA certificate is valid.

```
config:#
```

Removing the Uploaded Certificate or Private Key

The procedures of removing an existing client certificate, client private key or CA certificate in CLI are similar. This section illustrates such a procedure for the Ethernet interface "ETH1."

► **To remove a certificate or private key for ETH1:**

1. Make sure you have entered the configuration mode.
2. Type the appropriate command, depending on which file you want to remove, and press Enter.
 - *Client certificate:*

```
config:# network ethernet eth1 eapClientCertificate
```
 - *Client private key:*

```
config:# network ethernet eth1 eapClientPrivateKey
```
 - *CA certificate:*

```
config:# network ethernet eth1 eapCACertificate
```
3. The system prompts you to enter the contents of the chosen certificate or private key.
4. Press Enter without typing any data.
5. Verify whether the system shows the following command prompt, indicating the existing certificate or private key has been removed.

```
config:#
```

Setting Wireless Parameters

You must configure wireless parameters, including Service Set Identifier (SSID), authentication method, Pre-Shared Key (PSK), and Basic Service Set Identifier (BSSID) after the wireless networking mode is enabled.

A wireless configuration command begins with *network wireless*.

Note: If wireless networking mode is not enabled, the SSID, PSK and BSSID values are not applied until the wireless networking mode is enabled. In addition, a message appears, indicating that the active network interface is not wireless.

Setting the SSID

This command specifies the SSID string.

```
config:# network wireless SSID <ssid>
```

Variables:

<ssid> is the name of the wireless access point, which consists of:

- Up to 32 ASCII characters
- No spaces
- ASCII codes 0x20 ~ 0x7E

Enabling or Disabling 802.11n High Throughput

This command enables or disables the 802.11n high throughput protocol.

```
config:# network wireless enableHT <option>
```

Variables:

<option> is one of the options: *true* or *false*.

Option	Description
true	802.11n is enabled.
false	802.11n is disabled.

Setting the Wireless Authentication Method

This command sets the wireless authentication method to either PSK or Extensible Authentication Protocol (EAP).

```
config:# network wireless authMethod <method>
```

Variables:

<method> is one of the authentication methods: *PSK* or *EAP*.

Method	Description
PSK	The authentication method is set to PSK.
EAP	The authentication method is set to EAP.

Setting the PSK

If the Pre-Shared Key (PSK) authentication method is selected, you must assign a PSK passphrase by using this command.

```
config:# network wireless PSK <psk>
```

Variables:

<psk> is a string or passphrase that consists of:

- 8 to 63 characters
- No spaces
- ASCII codes 0x20 ~ 0x7E

Setting Wireless EAP Parameters

When the wireless authentication method is set to EAP, you must configure EAP authentication parameters, including outer authentication, inner authentication, EAP identity, client certificate, client private key, password, CA certificate, and RADIUS authentication server.

▶ **Determine the outer authentication protocol:**

```
config:# network wireless eapOuterAuthentication <outer_auth>
```

▶ **Determine the inner authentication protocol for authentication set to "EAP + PEAP":**

```
config:# network wireless eapInnerAuthentication <inner_auth>
```

▶ **Set the EAP identity:**

```
config:# network wireless eapIdentity <identity>
```

▶ **Set the EAP password:**

```
config:# network wireless eapPassword
```

After performing the above command, the PRO3X prompts you to enter the password. Then type the password and press Enter.

▶ **Provide a Client Certificate for authentication set to "EAP + TLS" or "EAP + PEAP + TLS":**

```
config:# network wireless eapClientCertificate
```

After performing any certificate or private key commands, including commands for the client certificate, client private key, and CA certificate, the system prompts you to enter the contents of the wanted certificate or key.

▶ **Provide a Client Private Key for authentication set to "EAP + TLS" or "EAP + PEAP + TLS":**

```
config:# network wireless eapClientPrivateKey
```

▶ **Provide a CA TLS certificate for EAP:**

```
config:# network wireless eapCACertificate
```

▶ **Enable or disable verification of the TLS certificate chain:**

```
config:# network wireless enableCertVerification <option1>
```

▶ **Allow expired and not yet valid TLS certificates:**

```
config:# network wireless allowOffTimeRangeCerts <option2>
```

► **Allow wireless network connection with incorrect system time:**

```
network wireless allowConnectionWithIncorrectClock <option3>
```

► **Set the RADIUS authentication server for EAP:**

```
config:# network wireless eapAuthServerName <FQDN>
```

Variables:

<outer_auth> is one of the options: *PEAP* or *TLS*.

Option	Description
PEAP	Outer authentication is set to Protected Extensible Authentication Protocol (PEAP).
TLS	Outer authentication is set to TLS.

<inner_auth> is one of the options: *MS-CHAPv2* or *TLS*.

Option	Description
MSCHAPv2	Inner authentication is set to Microsoft's Challenge Authentication Protocol Version 2 (MS-CHAPv2).
TLS	Inner authentication is set to TLS.

<identity> is your user name for the EAP authentication.

<option1> is one of the options: *true* or *false*.

Option	Description
true	Enables the verification of the TLS certificate chain.
false	Disables the verification of the TLS certificate chain.

<option2> is one of the options: *true* or *false*.

Option	Description
true	Always make the network connection successful even though the TLS certificate chain contains any certificate which is outdated or not valid yet.

Option	Description
false	The network connection is NOT successfully established when the TLS certificate chain contains any certificate which is outdated or not valid yet.

<option3> is one of the options: *true* or *false*.

Option	Description
true	Make the network connection successful when the PRO3X system time is earlier than the firmware build before synchronizing with the NTP server, causing the TLS certificate to become invalid.
false	The network connection is NOT successfully established when the PRO3X finds that the TLS certificate is not valid due to incorrect system time.

<FQDN> is 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.

Setting the BSSID

This command specifies the BSSID.

```
config:# network wireless BSSID <bssid>
```

Variables:

<bssid> is either the MAC address of the wireless access point or *none* for automatic selection.

Configuring the Cascading Mode

This command determines the cascading mode.

```
config:# network <mode> enabled <option1>
```

Variables:

<mode> is one of the following cascading modes.

Mode	Description
bridge	The Bridging mode, where each cascaded device is assigned a unique IP address.
portForwarding	The Port Forwarding mode, where every cascaded device in the chain shares the same IP address, with diverse port numbers assigned.

Important: When enabling either cascading mode, you must make sure the other cascading mode is disabled, or the preferred cascading mode may not be enabled successfully.

<option1> is one of the following options:

Option	Description
true	The selected cascading mode is enabled.
false	The selected cascading mode is disabled.

► **If Port Forwarding mode is enabled, you must configure two more settings to finish the configuration:**

On ALL cascaded devices, you must configure the 'role' setting one by one.

```
config:# network portForwarding role <option2>
```

On the master device, you must configure the 'downstream interface' setting.

```
config:# network portForwarding
masterDownstreamInterface <option3>
```

Variables:

<option2> is one of the following cascading roles:

Role	Description
master	The device is a master device.
link	The device is a link device.

<option3> is one of the following options:

Option	Description
ETH1/ETH2	ETH1/ETH2 port is the port where the 1st link device is connected.
Usb	USB port is the port where the 1st link device is connected.

Setting Network Service Parameters

A network service command begins with *network services*.

Setting the HTTP Port

The commands used to configure the HTTP port settings begin with *network services http*.

► **Change the HTTP port:**

```
config:# network services http port <n>
```

► **Enable or disable the HTTP port:**

```
config:# network services http enabled <option>
```

► **Enforce redirection from HTTP to HTTPS:**

```
config:# network services http enforceHttps <option>
```

Variables:

<n> is a TCP port number between 1 and 65535. The default HTTP port is 80.

<option> is one of the options: *true* or *false*.

Option	Description
true	<ul style="list-style-type: none"> ▪ The HTTP port is enabled. - OR - ▪ HTTP redirection to HTTPS is enabled.
false	<ul style="list-style-type: none"> ▪ The HTTP port is disabled. - OR - ▪ HTTP redirection to HTTPS is disabled.

Setting the HTTPS Port

The commands used to configure the HTTPS port settings begin with *network services https*.

▶ **Change the HTTPS port:**

```
config:# network services https port <n>
```

▶ **Enable or disable the HTTPS access:**

```
config:# network services https enabled <option>
```

Variables:

<n> is a TCP port number between 1 and 65535. The default HTTPS port is 443.

<option> is one of the options: *true* or *false*.

Option	Description
true	Forces any access to the PRO3X via HTTP to be redirected to HTTPS.
false	No HTTP access is redirected to HTTPS.

Changing the Telnet Configuration

You can enable or disable the Telnet service, or change its TCP port using the CLI commands.

A Telnet command begins with *network services telnet*.

Enabling or Disabling Telnet

This command enables or disables the Telnet service.

```
config:# network services telnet enabled <option>
```

Variables:

<option> is one of the options: *true* or *false*.

Option	Description
true	The Telnet service is enabled.
false	The Telnet service is disabled.

Changing the Telnet Port

This command changes the Telnet port.

```
config:# network services telnet port <n>
```

Variables:

<n> is a TCP port number between 1 and 65535. The default Telnet port is 23.

Changing the SSH Configuration

You can enable or disable the SSH service, or change its TCP port using the CLI commands.

An SSH command begins with *network services ssh*.

Enabling or Disabling SSH

This command enables or disables the SSH service.

```
config:# network services ssh enabled <option>
```

Variables:

<option> is one of the options: *true* or *false*.

Option	Description
true	The SSH service is enabled.
false	The SSH service is disabled.

Changing the SSH Port

This command changes the SSH port.

```
config:# network services ssh port <n>
```

Variables:

<n> is a TCP port number between 1 and 65535. The default SSH port is 22.

Determining the SSH Authentication Method

This command syntax determines the SSH authentication method.

```
config:# network services ssh authentication <auth_method>
```

Variables:

<option> is one of the options: *passwordOnly*, *publicKeyOnly* or *passwordOrPublicKey*.

Option	Description
passwordOnly	Enables the password-based login only.
publicKeyOnly	Enables the public key-based login only.
passwordOrPublicKey	Enables both the password- and public key-based login. This is the default.

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.

Setting the SNMP Configuration

You can enable or disable the SNMP v1/v2c or v3 agent, configure the read and write community strings, or set the MIB-II parameters, such as sysContact, using the CLI commands.

An SNMP command begins with *network services snmp*.

Enabling or Disabling SNMP v1/v2c

This command enables or disables the SNMP v1/v2c protocol.

```
config:# network services snmp v1/v2c <option>
```

Variables:

<option> is one of the options: *enable* or *disable*.

Option	Description
enable	The SNMP v1/v2c protocol is enabled.
disable	The SNMP v1/v2c protocol is disabled.

Enabling or Disabling SNMP v3

This command enables or disables the SNMP v3 protocol.

```
config:# network services snmp v3 <option>
```

Variables:

<option> is one of the options: *enable* or *disable*.

Option	Description
enable	The SNMP v3 protocol is enabled.
disable	The SNMP v3 protocol is disabled.

Setting the SNMP Read Community

This command sets the SNMP read-only community string.

```
config:# network services snmp readCommunity <string>
```

Variables:

<string> is a string comprising 4 to 64 ASCII printable characters.

The string CANNOT include spaces.

Setting the SNMP Write Community

This command sets the SNMP read/write community string.

```
config:# network services snmp writeCommunity <string>
```

Variables:

<string> is a string comprising 4 to 64 ASCII printable characters.

The string CANNOT include spaces.

Setting the sysContact Value

This command sets the SNMP MIB-II sysContact value.

```
config:# network services snmp sysContact <value>
```

Variables:

<value> is a string comprising 0 to 255 alphanumeric characters.

Setting the sysName Value

This command sets the SNMP MIB-II sysName value.

```
config:# network services snmp sysName <value>
```

Variables:

<value> is a string comprising 0 to 255 alphanumeric characters.

Setting the sysLocation Value

This command sets the SNMP MIB-II sysLocation value.

```
config:# network services snmp sysLocation <value>
```

Variables:

<value> is a string comprising 0 to 255 alphanumeric characters.

Changing the Modbus Configuration

You can enable or disable the Modbus agent, configure its read-only capability, or change its TCP port.

A Modbus command begins with *network services modbus*.

Enabling or Disabling Modbus

This command enables or disables the Modbus protocol.

```
config:# network services modbus enabled <option>
```

Variables:

<option> is one of the options: *true* or *false*.

Option	Description
true	The Modbus agent is enabled.
false	The Modbus agent is disabled.

Enabling or Disabling the Read-Only Mode

This command enables or disables the read-only mode for the Modbus agent.

```
config:# network services modbus readonly <option>
```

Variables:

<option> is one of the options: *true* or *false*.

Option	Description
true	The read-only mode is enabled.
false	The read-only mode is disabled.

Changing the Modbus Port

This command changes the Modbus port.

```
config:# network services modbus port <n>
```

Variables:

<n> is a TCP port number between 1 and 65535. The default Modbus port is 502.

Enabling or Disabling Service Advertising

This command enables or disables the zero configuration protocol, which enables advertising or auto discovery of network services.

```
config:# network services zeroconfig <method> <option>
```

Variables:

<method> is one of the options: *mdns* or *llmnr*.

Option	Description
mdns	Service advertisement via MDNS is enabled or disabled.
llmnr	Service advertisement via LLNMR is enabled or disabled.

<option> is one of the options: *enable* or *disable*.

Option	Description
enable	Service advertisement via the selected method (MDNS or LLMNR) is enabled.
disable	Service advertisement via the selected method (MDNS or LLMNR) is disabled.

Examples

This section illustrates several network configuration examples.

Example 1 - Wireless Networking Mode

The following command enables the wireless networking mode.

```
config:# network wireless enabled true
```

Example 2 - Enabling IPv6 Protocol on the Ethernet Interface

The following command enables the IPv6 protocol on the ETH1 interface.

```
config:# network ipv6 interface eth1 enabled true
```

Example 3 - Wireless Authentication Method

The following command sets the wireless authentication method to PSK.

```
config:# network wireless authMethod PSK
```

Example 4 - Static IPv4 Configuration

The following command enables the Static IPv4 configuration mode on the ETH1 interface.

```
network ipv4 interface eth1 configMethod static
```

Time Configuration Commands

A time configuration command begins with *time*.

Determining the Time Setup Method

This command determines the method to configure the system date and time.

```
config:# time method <method>
```

Variables:

<method> is one of the time setup options: *manual* or *ntp*.

Mode	Description
manual	The date and time settings are customized.
ntp	The date and time settings synchronize with a specified NTP server.

Setting NTP Parameters

A time configuration command for NTP-related parameters begins with *time ntp*.

► **Specify the primary time server:**

```
config:#  time ntp firstServer <first_server>
```

► **Specify the secondary time server:**

```
config:#  time ntp secondServer <second_server>
```

► **To delete the primary time server:**

```
config:#  time ntp firstServer ""
```

► **To delete the secondary time server:**

```
config:#  time ntp secondServer ""
```

Variables:

The <first_server> is the IP address or host name of the primary NTP server.

The <second_server> is the IP address or host name of the secondary NTP server.

Customizing the Date and Time

To manually configure the date and time, use the following CLI commands to specify them.

Note: You shall set the time configuration method to "manual" prior to customizing the date and time.

► **Assign the date:**

```
config:# time set date <yyyy-mm-dd>
```

► **Assign the time:**

```
config:# time set time <hh:mm:ss>
```

Variables:

Variable	Description
<yyyy-mm-dd>	Type the date in the format of yyyy-mm-dd. For example, type <i>2015-11-30</i> for November 30, 2015.
<hh:mm:ss>	Type the time in the format of hh:mm:ss in the 24-hour format. For example, type <i>13:50:20</i> for 1:50:20 pm.

Setting the Time Zone

The CLI has a list of time zones to configure the date and time for PRO3X.

```
config:# time zone
```

After a list of time zones is displayed, type the index number of the time zone or press Enter to cancel.

Example

► **To set the time zone:**

1. Type the time zone command as shown below and press Enter.

```
config:# time zone
```

2. The system shows a list of time zones. Type the index number of the desired time zone and press Enter.
3. Type `apply` for the selected time zone to take effect.

Setting the Automatic Daylight Savings Time

This command determines whether the daylight saving time is applied to the time settings.

```
config:#    time autoDST <option>
```

Variables:

<option> is one of the options: *enable* or *disable*.

Mode	Description
enable	Daylight savings time is enabled.
disable	Daylight savings time is disabled.

Examples

This section illustrates several time configuration examples.

Example 1 - Time Setup Method

The following command sets the date and time settings by using the NTP servers.

```
config:#    time method ntp
```

Example 2 - Primary NTP Server

The following command sets the primary time server to 192.168.80.66.

```
config:#    time ntp firstServer 192.168.80.66
```

Checking the Accessibility of NTP Servers

This command verifies the accessibility of NTP servers specified manually on your PRO3X and then shows the result.

To perform this command successfully, you must:

Own the "Change Date/Time Settings" permission.

Customize NTP servers.

This command is available either in the administrator/user mode or in the configuration mode. In the administrator/user mode:

```
#          check ntp
```

► **In the configuration mode:**

```
config#   check ntp
```

Security Configuration Commands

A security configuration command begins with *security*.

Firewall Control

You can manage firewall control features through the CLI. The firewall control lets you set up rules that permit or disallow access to the PRO3X from a specific or a range of IP addresses.

An IPv4 firewall configuration command begins with *security ipAccessControl ipv4*.

An IPv6 firewall configuration command begins with *security ipAccessControl ipv6*.

Modifying Firewall Control Parameters

There are different commands for modifying firewall control parameters.

IPv4 commands

► **Enable or disable the IPv4 firewall control feature:**

```
security ipAccessControl ipv4 enabled <option>
```

► **Determine the default IPv4 firewall control policy for inbound traffic:**

```
security ipAccessControl ipv4 defaultPolicyIn <policy>
```

► **Determine the default IPv4 firewall control policy for outbound traffic:**

```
security ipAccessControl ipv4 defaultPolicyOut <policy>
```

IPv6 commands

► **Enable or disable the IPv6 firewall control feature:**

```
security ipAccessControl ipv6 enabled <option>
```

► **Determine the default IPv6 firewall control policy for inbound traffic:**

```
security ipAccessControl ipv6 defaultPolicyIn <policy>
```

► **Determine the default IPv6 firewall control policy for outbound traffic:**

```
security ipAccessControl ipv6 defaultPolicyOut <policy>
```

Variables:

<option> is one of the options: *true* or *false*.

Option	Description
true	Enables the IP access control feature.
false	Disables the IP access control feature.

<policy> is one of the options: *accept*, *drop* or *reject*.

Option	Description
accept	Accepts traffic from all IP addresses.
drop	Discards traffic from all IP addresses, without sending any failure notification to the source host.
reject	Discards traffic from all IP addresses, and an ICMP message is sent to the source host for failure notification.

Tip: You can combine both commands to modify all firewall control parameters at a time.

Managing Firewall Rules

You can add, delete or modify firewall rules using the CLI commands.

An IPv4 firewall control rule command begins with *security ipAccessControl ipv4 rule*.

An IPv6 firewall control rule command begins with *security ipAccessControl ipv6 rule*.

Adding a Firewall Rule

Depending on where you want to add a new firewall rule in the list, the command for adding a rule varies.

IPv4 commands

▶ **Add a new rule to the bottom of the IPv4 rules list:**

```
security ipAccessControl ipv4 rule add <direction> <ip_mask> <policy>
```

▶ **Add a new IPv4 rule by inserting it above or below a specific rule:**

```
security ipAccessControl ipv4 rule add <direction> <ip_mask> <policy> <insert>  
<rule_number>
```

-- OR --

```
security ipAccessControl ipv4 rule add <direction> <insert> <rule_number>  
<ip_mask> <policy>
```

IPv6 commands

► Add a new rule to the bottom of the IPv6 rules list:

```
security ipAccessControl ipv6 rule add <direction> <ip_mask> <policy>
```

► Add a new IPv6 rule by inserting it above or below a specific rule:

```
security ipAccessControl ipv6 rule add <direction> <ip_mask> <policy> <insert>
<rule_number>
```

-- OR --

```
security ipAccessControl ipv6 rule add <direction> <insert> <rule_number>
<ip_mask> <policy>
```

Variables:

<direction> is one of the options: *in* or *out*.

Direction	Description
in	Inbound traffic.
out	Outbound traffic.

<ip_mask> is the combination of the IP address and subnet mask values (or prefix length), which are separated with a slash. For example, an IPv4 combination looks like this: *192.168.94.222/24*.

<policy> is one of the options: *accept*, *drop* or *reject*.

Policy	Description
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.

<insert> is one of the options: *insertAbove* or *insertBelow*.

Option	Description
insertAbove	Inserts the new rule above the specified rule number. Then: <i>new rule's number = the specified rule number</i>
insertBelow	Inserts the new rule below the specified rule number. Then: <i>new rule's number = the specified rule number + 1</i>

<rule_number> is the number of the existing rule which you want to insert the new rule above or below.

Modifying a Firewall Rule

Depending on what to modify in an existing rule, the command varies.

IPv4 commands

► Modify an IPv4 rule's IP address and/or subnet mask:

```
security ipAccessControl ipv4 rule modify <direction> <rule_number> ipMask
<ip_mask>
```

► Modify an IPv4 rule's policy:

```
security ipAccessControl ipv4 rule modify <direction> <rule_number> policy
<policy>
```

► Modify all contents of an existing IPv4 rule:

```
security ipAccessControl ipv4 rule modify <direction> <rule_number> ipMask
<ip_mask> policy <policy>
```

IPv6 commands▶ **Modify an IPv6 rule's IP address and/or prefix length:**

```
security ipAccessControl ipv6 rule modify <direction> <rule_number> ipMask
<ip_mask>
```

▶ **Modify an IPv6 rule's policy:**

```
security ipAccessControl ipv6 rule modify <direction> <rule_number> policy
<policy>
```

▶ **Modify all contents of an IPv6 existing rule:**

```
security ipAccessControl ipv6 rule modify <direction> <rule_number> ipMask
<ip_mask> policy <policy>
```

Variables:

<direction> is one of the options: *in* or *out*.

Direction	Description
in	Inbound traffic.
out	Outbound traffic.

<rule_number> is the number of the existing rule that you want to modify.

<ip_mask> is the combination of the IP address and subnet mask values (or prefix length), which are separated with a slash.

For example, an IPv4 combination looks like this: *192.168.94.222/24*.

<policy> is one of the options: *accept*, *drop* or *reject*.

Option	Description
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.

Deleting a Firewall Rule

The following commands remove a specific IPv4 or IPv6 rule from the list.

▶ IPv4 commands

```
security ipAccessControl ipv4 rule delete <direction> <rule_number>
```

▶ IPv6 commands

```
security ipAccessControl ipv6 rule delete <direction> <rule_number>
```

Variables:

<direction> is one of the options: *in* or *out*.

Direction	Description
in	Inbound traffic.
out	Outbound traffic.

<rule_number> is the number of the existing rule that you want to remove.

Restricted Service Agreement

The CLI command used to set the Restricted Service Agreement feature begins with `security restrictedServiceAgreement`,

Enabling or Disabling the Restricted Service Agreement

This command activates or deactivates the Restricted Service Agreement.

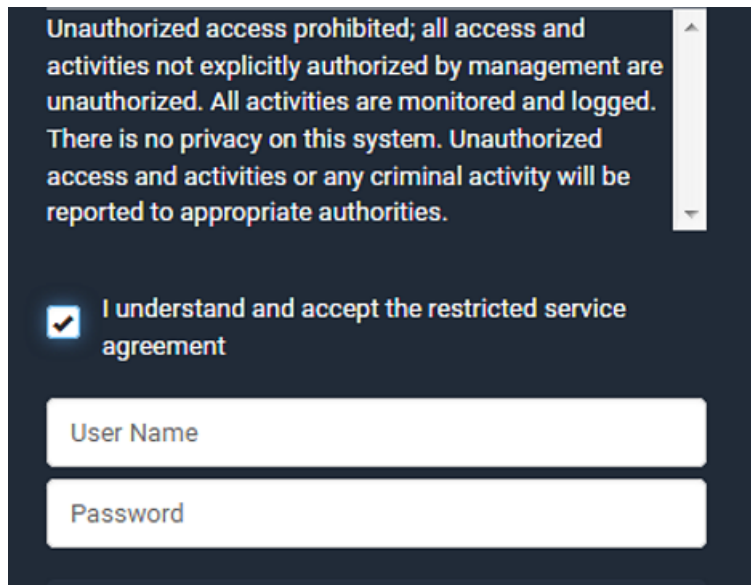
```
config:# security restrictedServiceAgreement enabled <option>
```

Variables:

<option> is one of the options: *true* or *false*.

Option	Description
true	Enables the Restricted Service Agreement feature.
false	Disables the Restricted Service Agreement feature.

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



The screenshot shows a dark-themed login interface. At the top, a white text box contains the following text: "Unauthorized access prohibited; all access and activities not explicitly authorized by management are unauthorized. All activities are monitored and logged. There is no privacy on this system. Unauthorized access and activities or any criminal activity will be reported to appropriate authorities." Below this text is a checkbox with a checkmark, labeled "I understand and accept the restricted service agreement". Underneath the checkbox are two input fields: "User Name" and "Password".

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.

Specifying the Agreement Contents

This command allows you to create or modify contents of the Restricted Service Agreement.

```
config:# security restrictedServiceAgreement bannerContent
```

After performing the above command, do the following:

1. Type the text comprising up to 10,000 ASCII characters when the CLI prompts you to enter the content.
2. To end the content:
 - a. Press Enter.
 - b. Type `--END--` to indicate the end of the content.
 - c. Press Enter again.

If the content is successfully entered, the CLI displays this message "Successfully entered Restricted Service Agreement" followed by the total number of entered characters in parentheses.

Note: The new content of Restricted Service Agreement is saved only after typing the `apply` command.

Example

The following example illustrates how to specify the content of the Restricted Service Agreement.

1. Type the following command and press Enter to start entering the content.

```
config:# security restrictedServiceAgreement bannerContent
```

2. Type the following content when the CLI prompts you to enter the content.

```
IMPORTANT!! You are accessing the PRO3X. If you are not the system administrator,  
do NOT operate it or change any settings without the permission of the system  
administrator.
```

3. Press Enter.

4. Type the following:

```
--END--
```

5. Press Enter again.

6. Verify that the message "Successfully entered Restricted Service Agreement" is displayed, indicating that the content input is successful.

Login Limitation

The login limitation feature controls login-related limitations, such as password aging, simultaneous logins using the same user name, and the idle time permitted before forcing a user to log out.

A login limitation command begins with *security loginLimits*.

You can combine multiple commands to modify various login limitation parameters at a time.

Single Login Limitation

This command enables or disables the single login feature, which controls whether multiple logins using the same login name simultaneously is permitted.

```
config:# security loginLimits singleLogin <option>
```

Variables:

<option> is one of the options: *enable* or *disable*.

Option	Description
enable	Enables the single login feature.
disable	Disables the single login feature.

Using the PRO3X Command Line Interface (CLI)

Password Aging

This command enables or disables the password aging feature, which controls whether the password should be changed at a regular interval:

```
config:# security loginLimits passwordAging <option>
```

Variables:

<option> is one of the options: *enable* or *disable*.

Option	Description
enable	Enables the password aging feature.
disable	Disables the password aging feature.

Password Aging Interval

This command determines how often the password should be changed.

```
config:# security loginLimits passwordAgingInterval <value>
```

Variables:

<value> is a numeric value in days set for the password aging interval. The interval ranges from 7 to 365 days.

Idle Timeout

This command determines how long a user can remain idle before that user is forced to log out of the PRO3X web interface or CLI.

```
config:# security loginLimits idleTimeout <value>
```

Variables:

<value> is a numeric value in minutes set for the idle timeout. The timeout ranges from 1 to 1440 minutes (24 hours).

User Blocking

There are different commands for changing different user blocking parameters. These commands begin with `security userBlocking`.

You can combine multiple commands to modify the user blocking parameters at a time. Determine the maximum number of failed logins before blocking a user:

```
security userBlocking maximumNumberOfFailedLogins <value1>
```

► **Determine how long a user is blocked:**

```
config:# security userBlocking blockTime <value2>
```

Variables:

<value1> is an integer between 3 and 10, or *unlimited*, which sets no limit on the maximum number of failed logins and thus disables the user blocking function.

<value2> is a numeric value ranging from 1 to 1440 minutes (one day), or *infinite*, which blocks the user all the time until the user is unblocked manually.

Strong Passwords

The strong password commands determine whether a strong password is required for login, and what a strong password should contain at least.

A strong password command begins with `security strongPasswords`.

You can combine multiple strong password commands to modify different parameters at a time.

Enabling or Disabling Strong Passwords

This command enables or disables the strong password feature.

```
config:# security strongPasswords enabled <option>
```

Variables:

<option> is one of the options: *true* or *false*.

Option	Description
true	Enables the strong password feature.
false	Disables the strong password feature.

Minimum Password Length

This command determines the minimum length of the password.

```
config:# security strongPasswords minLength <value>
```

Variables:

<value> is an integer between 8 and 32.

Maximum Password Length

This command determines the maximum length of the password.

```
config:# security strongPasswords maxLength <value>
```

Variables:

<value> is an integer between 16 and 64.

Lowercase Character Requirement

This command determines whether a strong password includes at least a lowercase character.

```
security strongPasswords enforceAtLeastOneLowerCaseCharacter <option>
```

Variables:

<option> is one of the options: *enable* or *disable*.

Option	Description
enable	At least one lowercase character is required.
disable	No lowercase character is required.

Uppercase Character Requirement

This command determines whether a strong password includes at least a uppercase character.

```
security strongPasswords enforceAtLeastOneUpperCaseCharacter <option>
```

Variables:

<option> is one of the options: *enable* or *disable*.

Option	Description
enable	At least one uppercase character is required.
disable	No uppercase character is required.

Numeric Character Requirement

This command determines whether a strong password includes at least a numeric character.

```
security strongPasswords enforceAtLeastOneNumericCharacter <option>
```

Variables:

<option> is one of the options: *enable* or *disable*.

Option	Description
enable	At least one numeric character is required.
disable	No numeric character is required.

Special Character Requirement

This command determines whether a strong password includes at least a special character.

```
security strongPasswords enforceAtLeastOneSpecialCharacter <option>
```

Variables:

<option> is one of the options: *enable* or *disable*.

Option	Description
enable	At least one special character is required.
disable	No special character is required.

Maximum Password History

This command determines the number of previous passwords that CANNOT be repeated when changing the password.

```
config:# security strongPasswords passwordHistoryDepth <value>
```

Variables:

<value> is an integer between 1 and 12.

Role-Based Access Control

In addition to firewall access control based on IP addresses, you can configure other access control rules that are based on both IP addresses and users' roles.

An IPv4 role-based access control command begins with *security roleBasedAccessControl ipv4*.

An IPv6 role-based access control command begins with *security roleBasedAccessControl ipv6*.

Modifying Role-Based Access Control Parameters

There are different commands for modifying role-based access control parameters.

IPv4 commands

► **Enable or disable the IPv4 role-based access control feature:**

```
security roleBasedAccessControl ipv4 enabled <option>
```

► **Determine the IPv4 role-based access control policy:**

```
security roleBasedAccessControl ipv4 defaultPolicy <policy>
```


IPv6 commands▶ **Enable or disable the IPv6 role-based access control feature:**

```
security roleBasedAccessControl ipv6 enabled <option>
```

▶ **Determine the IPv6 role-based access control policy:**

```
security roleBasedAccessControl ipv6 defaultPolicy <policy>
```

Variables:

<option> is one of the options: *true* or *false*.

Option	Description
true	Enables the role-based access control feature.
false	Disables the role-based access control feature.

<policy> is one of the options: *allow* or *deny*.

Policy	Description
allow	Accepts traffic from all IP addresses regardless of the user's role.
deny	Drops traffic from all IP addresses regardless of the user's role.

Tip: You can combine both commands to modify all role-based access control parameters at a time.

Managing Role-Based Access Control Rules

You can add, delete or modify role-based access control rules.

An IPv4 role-based access control command for managing rules begins with *security roleBasedAccessControl ipv4 rule*.

An IPv6 role-based access control command for managing rules begins with *security roleBasedAccessControl ipv6 rule*.

Adding a Role-Based Access Control Rule

Depending on where you want to add a new rule in the list, the command syntax for adding a rule varies.

IPv4 commands

▶ **Add a new rule to the bottom of the IPv4 rules list:**

```
security roleBasedAccessControl ipv4 rule add <start_ip> <end_ip> <role> <policy>
```

▶ **Add a new IPv4 rule by inserting it above or below a specific rule:**

```
security roleBasedAccessControl ipv4 rule add <start_ip> <end_ip> <role>
<policy> <insert> <rule_number>
```

IPv6 commands

▶ **Add a new rule to the bottom of the IPv6 rules list:**

```
security roleBasedAccessControl ipv6 rule add <start_ip> <end_ip> <role>
<policy>
```

▶ **Add a new IPv6 rule by inserting it above or below a specific rule:**

```
security roleBasedAccessControl ipv6 rule add <start_ip> <end_ip> <role>
<policy> <insert> <rule_number>
```

Variables:

<start_ip> is the starting IP address.

<end_ip> is the ending IP address.

<role> is the role for which you want to create an access control rule.

<policy> is one of the options: *allow* or *deny*.

Policy	Description
allow	Accepts traffic from the specified IP address range when the user is a member of the specified role
deny	Drops traffic from the specified IP address range when the user is a member of the specified role

<insert> is one of the options: *insertAbove* or *insertBelow*.

Option	Description
insertAbove	Inserts the new rule above the specified rule number. Then: <i>new rule's number = the specified rule number</i>
insertBelow	Inserts the new rule below the specified rule number. Then: <i>new rule's number = the specified rule number + 1</i>

<rule_number> is the number of the existing rule which you want to insert the new rule above or below.

Modifying a Role-Based Access Control Rule

Depending on what to modify in an existing rule, the command syntax varies.

IPv4 commands

► **Modify a rule's IPv4 address range:**

```
security roleBasedAccessControl ipv4 rule modify <rule_number> startIpAddress
<start_ip> endIpAddress <end_ip>
```

► **Modify an IPv4 rule's role:**

```
security roleBasedAccessControl ipv4 rule modify <rule_number> role <role>
```

► **Modify an IPv4 rule's policy:**

```
security roleBasedAccessControl ipv4 rule modify <rule_number> policy <policy>
```

► **Modify all contents of an existing IPv4 rule:**

```
security roleBasedAccessControl ipv4 rule modify <rule_number> startIpAddress
<start_ip> endIpAddress <end_ip> role <role> policy <policy>
```

IPv6 commands

▶ **Modify a rule's IPv6 address range:**

```
security roleBasedAccessControl ipv6 rule modify <rule_number> startIpAddress  
<start_ip> endIpAddress <end_ip>
```

▶ **Modify an IPv6 rule's role:**

```
security roleBasedAccessControl ipv6 rule modify <rule_number> role <role>
```

▶ **Modify an IPv6 rule's policy:**

```
security roleBasedAccessControl ipv6 rule modify <rule_number> policy <policy>
```

► Modify all contents of an existing IPv6 rule:

```
security roleBasedAccessControl ipv6 rule modify <rule_number>  
startIpAddress <start_ip> endIpAddress <end_ip> role <role> policy <policy>
```

Variables:

<rule_number> is the number of the existing rule that you want to modify.

<start_ip> is the starting IP address.

<end_ip> is the ending IP address.

<role> is one of the existing roles.

<policy> is one of the options: *allow* or *deny*.

Policy	Description
allow	Accepts traffic from the specified IP address range when the user is a member of the specified role
deny	Drops traffic from the specified IP address range when the user is a member of the specified role

Deleting a Role-Based Access Control Rule

These commands remove a specific rule from the list.

► IPv4 commands

```
security roleBasedAccessControl ipv4 rule delete <rule_number>
```

► IPv6 commands

```
security roleBasedAccessControl ipv6 rule delete <rule_number>
```

Variables:

<rule_number> is the number of the existing rule that you want to remove.

Enabling or Disabling Front Panel Actuator Control

The following CLI commands control whether you can turn on or off connected actuator(s) by operating the front panel LCD display.

► **To enable the front panel actuator control feature:**

```
config:# security frontPanelPermissions add switchActuator
```

► **To disable the front panel actuator control feature:**

```
config:# security frontPanelPermissions remove switchActuator
```

Tip: If your PRO3X supports multiple front panel permissions, you can combine them into one command by adding a semicolon (;) between different permissions. For example, the following CLI command enables both front panel actuator control and the internal beeper-muting functions simultaneously.

```
security frontPanelPermissions add switchActuator;muteBeeper
```

Enabling or Disabling Front Panel Beeper-Sound Control

The following CLI commands control whether you can mute the internal beeper by operating the front panel LCD display when the beeper sounds.

► **To enable the front panel beeper sound control feature:**

```
config:# security frontPanelPermissions add muteBeeper
```

► **To disable the front panel actuator control feature:**

```
config:# security frontPanelPermissions remove muteBeeper
```

Tip: If your PRO3X supports multiple front panel permissions, you can combine them into one command by adding a semicolon (;) between different permissions. For example, the following CLI command enables both front panel actuator control and the the internal beeper-muting functions simultaneously.

```
security frontPanelPermissions add switchActuator;muteBeeper
```

Examples

This section illustrates several security configuration examples.

Example 1 - IPv4 Firewall Control Configuration

The following command sets up two parameters of the IPv4 access control feature.

```
security ipAccessControl ipv4 enabled true defaultPolicyIn accept defaultPolicyOut accept
```

Results:

The IPv4 access control feature is enabled.

The default policy for inbound traffic is set to "accept."

The default policy for outbound traffic is set to "accept."

Example 2 - Adding an IPv4 Firewall Rule

The following command adds a new IPv4 access control rule and specifies its location in the list.

```
security ipAccessControl ipv4 rule add in 192.168.84.123/24 accept insertAbove 5
```

Results:

A new IPv4 firewall control rule is added to accept all packets sent from the IPv4 address 192.168.84.123.

The newly-added rule is inserted above the 5th rule. That is, the new rule becomes the 5th rule, and the original 5th rule becomes the 6th rule.

Example 3 - User Blocking

The following command sets up two user blocking parameters.

```
security userBlocking maximumNumberOfFailedLogins 5 blockTime 30
```

Results:

The maximum number of failed logins is set to 5.

The user blocking time is set to 30 minutes.

Example 4 - Adding an IPv4 Role-based Access Control Rule

The following command creates a new IPv4 role-based access control rule and specifies its location in the list.

```
security roleBasedAccessControl ipv4 rule add 192.168.78.50 192.168.90.100 admin deny  
insertAbove 3
```

Results:

A new IPv4 role-based access control rule is added, dropping all packets from any IPv4 address between 192.168.78.50 and 192.168.90.100 when the user is a member of the role "admin."

The newly-added IPv4 rule is inserted above the 3rd rule. That is, the new rule becomes the 3rd rule, and the original 3rd rule becomes the 4th rule.

Outlet Configuration Commands

An outlet configuration command begins with *outlet*. Such a command allows you to configure an individual outlet.

Changing the Outlet Name

This command names an outlet.

```
config:#    outlet <n> name "<name>"
```

Variables:

<n> is the number of the outlet that you want to configure.

<name> is a string comprising up to 64 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.

Example - Outlet Naming

The following command assigns the name "Win XP" to outlet 8.

```
config:#    outlet 8 name "Win XP"
```


Inlet Configuration Commands

An inlet configuration command begins with *inlet*. You can configure an inlet by using the inlet configuration command.

Changing the Inlet Name

This command syntax names an inlet.

```
config:#    inlet <n> name "<name>"
```

Variables:

<n> is the number of the inlet that you want to configure. For a single-inlet PDU, <n> is always 1. The value is an integer between 1 and 50.

<name> is a string comprising up to 64 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.

Enabling or Disabling an Inlet (for Multi-Inlet PDUs)

Enabling or disabling an inlet takes effect on a multi-inlet PDU only.

This command enables or disables an inlet.

```
config:#    inlet <n> enabled <option>
```

Variables:

<n> is the number of the inlet that you want to configure. For a single-inlet PDU, <n> is always 1. The value is an integer between 1 and 50.

<option> is one of the options: *true* or *false*.

Option	Description
true	The specified inlet is enabled.
false	The specified inlet is disabled.

Note: If performing this command causes all inlets to be disabled, a warning message appears, prompting you to confirm. When this occurs, press y to confirm or n to cancel the operation.

Example - Inlet Naming

The following command assigns the name "AC source" to the inlet 1. If your PRO3X contains multiple inlets, this command names the 1st inlet.

```
config:#  inlet 1 name "AC source"
```

Overcurrent Protector Configuration Commands

An overcurrent protector configuration command begins with *ocp*. The command configures an individual circuit breaker or fuse which protects outlets.

Changing the Overcurrent Protector Name

This command names a circuit breaker or a fuse which protects outlets on your PRO3X.

```
config:#  ocp <n> name "<name>"
```

Variables:

<n> is the number of the overcurrent protector that you want to configure. The value is an integer between 1 and 50.

<name> is a string comprising up to 64 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.

Example - OCP Naming

The command assigns the name "Email servers CB" to the overcurrent protector labeled 2.

```
config:#  ocp 2 name "Email servers CB"
```

User Configuration Commands

Most user configuration commands begin with *user* except for the password change command.

Creating a User Profile

This command creates a new user profile.

```
config:# user create <name> <option> <roles>
```

After performing the user creation command, the PRO3X prompts you to assign a password to the newly-created user. Then:

1. Type the password and press Enter.
2. Re-type the same password for confirmation and press Enter.

Variables:

<name> is a string comprising up to 32 ASCII printable characters. The <name> variable CANNOT contain spaces.

<option> is one of the options: *enable* or *disable*.

Option	Description
enable	Enables the newly-created user profile.
disable	Disables the newly-created user profile.

<roles> is a role or a list of comma-separated roles assigned to the specified user profile.

Modifying a User Profile

A user profile contains various parameters that you can modify.

Tip: You can combine all commands to modify the parameters of a specific user profile at a time.

Changing a User's Password

This command allows you to change an existing user's password if you have the Administrator Privileges.

```
config:# user modify <name> password
```

After performing the above command, PRO3X prompts you to enter a new password. Then:

1. Type a new password and press Enter.
2. Re-type the new password for confirmation and press Enter.

Variables:

<name> is the name of the user whose settings you want to change.

Example

The following procedure illustrates how to change the password of the user "May."

1. Verify that you have entered the configuration mode.
2. Type the following command to change the password for the user profile "May."

```
config:# user modify May password
```

3. Type a new password when prompted, and press Enter.
4. Type the same new password and press Enter. If the password change is completed successfully, the config:# prompt appears.

Modifying a User's Personal Data

You can change a user's personal data, including the user's full name, telephone number, and email address.

Various commands can be combined to modify the parameters of a specific user profile at a time.

► Change a user's full name:

```
config:# user modify <name> fullName "<full_name>"
```

► Change a user's telephone number:

```
config:# user modify <name> telephoneNumber "<phone_number>"
```

► Change a user's email address:

```
config:# user modify <name> emailAddress <email_address>
```

Variables:

<name> is the name of the user whose settings you want to change.

<full_name> is a string comprising up to 64 ASCII printable characters. The <full_name> variable must be enclosed in quotes when it contains spaces.

<phone_number> is the phone number that can reach the specified user. The <phone_number> variable must be enclosed in quotes when it contains spaces.

<email_address> is the email address of the specified user.

Enabling or Disabling a User Profile

This command enables or disables a user profile. A user can log in to the PRO3X only after that user's user profile is enabled.

```
config:# user modify <name> enabled <option>
```

Variables:

<name> is the name of the user whose settings you want to change.

<option> is one of the options: *true* or *false*.

Option	Description
true	Enables the specified user profile.
false	Disables the specified user profile.

Forcing a Password Change

This command determines whether the password change is forced when a user logs in to the specified user profile next time.

```
user modify <name> forcePasswordChangeOnNextLogin <option>
```

Variables:

<name> is the name of the user whose settings you want to change.

<option> is one of the options: *true* or *false*.

Option	Description
true	A password change is forced on the user's next login.
false	No password change is forced on the user's next login.

Modifying SNMPv3 Settings

There are different commands to modify the SNMPv3 parameters of a specific user profile. You can combine all of the following commands to modify the SNMPv3 parameters at a time.

▶ **Enable or disable the SNMP v3 access to PRO3X for the specified user:**

```
user modify <name> snmpV3Access <option1>
```

▶ **Determine the security level:**

```
user modify <name> securityLevel <option2>
```

▶ **Determine whether the authentication passphrase is identical to the password:**

```
user modify <name> userPasswordAsAuthenticationPassphrase <option3>
```

▶ **Determine the authentication passphrase:**

```
user modify <name> authenticationPassPhrase
```

After performing the above command, PRO3X prompts you to enter the authentication passphrase.

► **Determine whether the privacy passphrase is identical to the authentication passphrase:**

```
user modify <name>  
useAuthenticationPassPhraseAsPrivacyPassPhrase <option4>
```

► **Determine the privacy passphrase:**

```
user modify <name> privacyPassPhrase
```

After performing the above command, PRO3X prompts you to enter the privacy passphrase.

► **Determine the authentication protocol:**

```
user modify <name> authenticationProtocol <option5>
```

► **Determine the privacy protocol:**

```
user modify <name> privacyProtocol <option6>
```

Variables:

<name> is the name of the user whose settings you want to change.

<option1> is one of the options: *enable* or *disable*.

Option	Description
enable	Enables the SNMP v3 access permission for the specified user.
disable	Disables the SNMP v3 access permission for the specified user.

<option2> is one of the options: *noAuthNoPriv*, *authNoPriv* or *authPriv*.

Option	Description
noAuthNoPriv	No authentication and no privacy.
authNoPriv	Authentication and no privacy.
authPriv	Authentication and privacy.

<option3> is one of the options: *true* or *false*.

Option	Description
true	Authentication passphrase is identical to the password.
false	Authentication passphrase is different from the password.

<option4> is one of the options: *true* or *false*.

Option	Description
true	Privacy passphrase is identical to the authentication passphrase.
false	Privacy passphrase is different from the authentication passphrase.

<option5> is one of the options: *MD5* or *SHA-1*.

Option	Description
MD5	MD5 authentication protocol is applied.
SHA-1	SHA-1 authentication protocol is applied.

<option6> is one of the options: *DES* or *AES-128*.

Option	Description
DES	DES privacy protocol is applied.
AES-128	AES-128 privacy protocol is applied.

An authentication or privacy passphrase is a string comprising 8 to 32 ASCII printable characters.

Changing the Role(s)

This command changes the role(s) of a specific user.

```
config:# user modify <name> roles <roles>
```

Variables:

<name> is the name of the user whose settings you want to change.

<roles> is a role or a list of comma-separated roles assigned to the specified user profile.

Changing Measurement Units

You can change the measurement units displayed for temperatures, length, and pressure for a specific user profile. Different measurement unit commands can be combined so that you can set all measurement units at a time.

Note: The measurement unit change only applies to the web interface and command line interface.

► Set the preferred temperature unit:

```
config:# user modify <name> preferredTemperatureUnit <option1>
```

► Set the preferred length unit:

```
config:# user modify <name> preferredLengthUnit <option2>
```

► Set the preferred pressure unit:

```
config:# user modify <name> preferredPressureUnit <option3>
```

Variables:

<name> is the name of the user whose settings you want to change.

<option1> is one of the options: *C* or *F*.

Option	Description
C	This option displays the temperature in Celsius.
F	This option displays the temperature in Fahrenheit.

<option2> is one of the options: *meter* or *feet*.

Option	Description
meter	This option displays the length or height in meters.

Option	Description
feet	This option displays the length or height in feet.

<option3> is one of the options: *pascal* or *psi*.

Option	Description
pascal	This option displays the pressure value in Pascals (Pa).
psi	This option displays the pressure value in psi.

Specifying the SSH Public Key

If the SSH key-based authentication is enabled, specify the SSH public key for each user profile using the following procedure.

► To specify or change the SSH public key for a specific user:

1. Type the SSH public key command as shown below and press Enter.

```
config:# user modify <name> sshPublicKey
```
2. The system prompts you to enter the contents of the SSH public key. Do the following to input the contents:
 - a. Open your SSH public key with a text editor.
 - b. Copy all contents in the text editor.
 - c. Paste the contents into the terminal.
 - d. Press Enter.

► To remove an existing SSH public key:

1. Type the same command as shown above.
2. When the system prompts you to input the contents, press Enter without typing or pasting anything.

Example

The following procedure illustrates how to change the SSH public key for the user "assistant."

1. Verify that you have entered the configuration mode.
2. Type the following command and press Enter.

```
config:# user modify assistant sshPublicKey
```
3. You are prompted to enter a new SSH public key.
4. Type the new key and press Enter.

Deleting a User Profile

This command deletes an existing user profile.

```
config:# user delete <name>
```

Changing Your Own Password

Every user can change their own password via this command if they have the Change Own Password privilege. Note that this command does not begin with *user*.

```
config:# password
```

After performing this command, the PRO3X prompts you to enter both current and new passwords respectively.

Important: After the password is changed successfully, the new password is effective immediately no matter you type the command "apply" or not to save the changes.

Example

This procedure changes your own password:

1. Verify that you have entered the configuration mode.
2. Type the following command and press Enter.

```
config:# password
```

3. Type the existing password and press Enter when the following prompt appears.

```
Current password:
```

4. Type the new password and press Enter when the following prompt appears.

```
Enter new password:
```

5. Re-type the new password for confirmation and press Enter when the following prompt appears.

```
Re-type new password:
```

Setting Default Measurement Units

Default measurement units, including temperature, length, and pressure units, apply to the PRO3X user interfaces across all users except for those whose preferred measurement units are set differently by themselves or the administrator. Diverse measurement unit commands can be combined so that you can set all default measurement units at a time.

Note: The measurement unit change only applies to the web interface and command line interface.

▶ **Set the default temperature unit:**

```
user defaultpreferences preferredTemperatureUnit <option1>
```

▶ **Set the default length unit:**

```
user defaultpreferences preferredLengthUnit <option2>
```

▶ **Set the default pressure unit:**

```
user defaultpreferences preferredPressureUnit <option3>
```

Variables:

<option1> is one of the options: *C* or *F*.

Option	Description
C	This option displays the temperature in Celsius.
F	This option displays the temperature in Fahrenheit.

<option2> is one of the options: *meter* or *feet*.

Option	Description
meter	This option displays the length or height in meters.
feet	This option displays the length or height in feet.

<option3> is one of the options: *pascal* or *psi*.

Option	Description
pascal	This option displays the pressure value in Pascals (Pa).
psi	This option displays the pressure value in psi.

Examples

This section illustrates several user configuration examples.

Example 1 - Creating a User Profile

The following command creates a new user profile and sets two parameters for the new user.

```
config:# user create Mary enable admin
```

Results:

A new user profile "Mary" is created.

The new user profile is enabled.

The **admin** role is assigned to the new user profile.

Example 2 - Modifying a User's Roles

The following command assigns two roles to the user "Mary."

```
config:# user modify Mary roles admin, tester
```

Results:

The user Mary has the union of all privileges of "admin" and "tester."

Example 3 - Default Measurement Units

The following command sets all default measurement units at a time.

```
user defaultpreferences preferredTemperatureUnit F preferredLengthUnit feet  
preferredPressureUnit psi
```

Results:

The default temperature unit is set to Fahrenheit.

The default length unit is set to feet.

The default pressure unit is set to psi.

Role Configuration Commands

A role configuration command begins with *role*.

Creating a Role

This command creates a new role, with a list of semicolon-separated privileges assigned to the role.

```
role create <name> <privilege1>;<privilege2>;<privilege3>...
```

If a specific privilege contains any arguments, that privilege should be followed by a colon and the argument(s).

```
role create <name> <privilege1>:<argument1>,<argument2>...;
<privilege2>:<argument1>,<argument2>...;
<privilege3>:<argument1>,<argument2>...;
...
```

Variables:

<name> is a string comprising up to 32 ASCII printable characters.

<privilege1>, <privilege2>, <privilege3> and the like are names of the privileges assigned to the role. Separate each privilege with a semi-colon.

<argument1>, <argument2> and the like are arguments set for a particular privilege. Separate a privilege and its argument(s) with a colon, and separate arguments with a comma if there are more than one argument for a privilege.

All Privileges

This table lists all privileges. Note that available privileges vary according to the model you purchased.

Privilege	Description
acknowledgeAlarms	Acknowledge Alarms
adminPrivilege	Administrator Privileges
changeAssetStripConfiguration	Change Asset Strip Configuration
changeAuthSettings	Change Authentication Settings
changeDateTimeSettings	Change Date/Time Settings
changeExternalSensorsConfiguration	Change Peripheral Device Configuration
changeLhxConfiguration	Change LHX/SHX Configuration
changeModemConfiguration	Change Modem Configuration
changeNetworkSettings	Change Network Settings
changePassword	Change Own Password
changePduConfiguration	Change Pdu, Inlet, Outlet & Overcurrent Protector Configuration

Using the PRO3X Command Line Interface (CLI)

Privilege	Description
changeSecuritySettings	Change Security Settings
changeSnmpSettings	Change SNMP Settings
changeUserSettings	Change Local User Management
changeWebcamSettings	Change Webcam Configuration
clearLog	Clear Local Event Log
firmwareUpdate	Firmware Update
performReset	Reset (Warm Start)
switchActuator*	Switch Actuator
viewAuthSettings	View Authentication Settings
viewEventSetup	View Event Settings
viewEverything	Unrestricted View Privileges
viewLog	View Local Event Log
viewSecuritySettings	View Security Settings
viewSnmpSettings	View SNMP Settings
viewUserSettings	View Local User Management
viewWebcamSettings	View Webcam Snapshots and Configuration

* The "switchActuator" privilege requires an argument that is separated with a colon. The argument could be:

All actuators, that is,

```
switchActuator:all
```

An actuator's ID number. For example:

```
switchActuator:1
```

```
switchActuator:2
```

```
switchActuator:3
```

A list of comma-separated ID numbers of different actuators. For example:

```
switchActuator:1,3,6
```

Note: The ID number of each actuator is shown in the PRO3X web interface. It is an integer.

Modifying a Role

You can modify diverse parameters of an existing role, including its privileges.

► Modify a role's description:

```
config:#  role modify <name> description "<description>"
```

► Add more privileges to a specific role:

```
config:#  role modify <name> addPrivileges
          <privilege1>;<privilege2>;<privilege3>...
```

If a specific privilege contains any arguments, add a colon and the argument(s) after that privilege.

```
config:#  role modify <name> addPrivileges
          <privilege1>:<argument1>,<argument2>...;
          <privilege2>:<argument1>,<argument2>...;
          <privilege3>:<argument1>,<argument2>...;
          ...
```

► Remove specific privileges from a role:

```
config:#  role modify <name> removePrivileges
          <privilege1>;<privilege2>;<privilege3>...
```

If a specific privilege contains any arguments, add a colon and the argument(s) after that privilege.

```
config:#  role modify <name> removePrivileges
          <privilege1>:<argument1>,<argument2>...;
          <privilege2>:<argument1>,<argument2>...;
          <privilege3>:<argument1>,<argument2>...;
          ...
```

Note: When removing privileges from a role, make sure the specified privileges and arguments (if any) exactly match those assigned to the role. Otherwise, the command fails to remove specified privileges that are not available.

Variables:

<name> is a string comprising up to 32 ASCII printable characters.

<description> is a description comprising alphanumeric characters. The <description> variable must be enclosed in quotes when it contains spaces.

<privilege1>, <privilege2>, <privilege3> and the like are names of the privileges assigned to the role. Separate each privilege with a semi-colon.

<argument1>, <argument2> and the like are arguments set for a particular privilege. Separate a privilege and its argument(s) with a colon, and separate arguments with a comma if there are more than one argument for a privilege.

Deleting a Role

This command deletes an existing role.

```
config:#   role delete <name>
```

Example - Creating a Role

The following command creates a new role and assigns privileges to the role.

```
config:#   role create tester firmwareUpdate;viewEventSetup
```

Results:

A new role "tester" is created.

Two privileges are assigned to the role: firmwareUpdate (Firmware Update) and viewEventSetup (View Event Settings).

Authentication Commands

An authentication configuration command begins with *authentication*.

Determining the Authentication Method

You can choose to set the authentication type only, or both set the authentication type and determine whether to switch to local authentication in case the remote authentication is not available.

► Determine the authentication type only:

```
config:#   authentication type <option1>
```

► Determine the authentication type and enable/disable the option of switching to local authentication:

```
authentication type <option1> useLocalIfRemoteUnavailable <option2>
```

Note: You cannot enable or disable the option of switching to local authentication without determining the authentication type in the CLI. Therefore, always type "authentication type <option1>" when setting up "useLocalIfRemoteUnavailable".

Variables:

<option1> is one of the options: *local* , *ldap* or *radius*.

Option	Description
local	Enable Local authentication only.
ldap	Enable LDAP authentication.
radius	Enable Radius authentication.

<option2> is one of the options: *true* or *false*.

Option	Description
true	Remote authentication is the first priority. The device will switch to local authentication when the remote authentication is not available.
false	Always stick to remote authentication regardless of the availability of remote authentication.

LDAP Settings

All LDAP-related commands begin with *authentication ldap*.

If you enable LDAP authentication, you must add at least one LDAP server. Later you can modify or delete any existing LDAP server as needed.

Adding an LDAP Server

Adding an LDAP server requires the entry of quite a lot of parameters, such as the server's IP address, TCP port number, Base DN and so on.

You can repeat the following CLI command to add more than one LDAP server.

Tip: If any LDAP server's settings are identical to an existing LDAP server's, you can add it by just copying the existing one, instead of using the following command..

► **Add a new LDAP server:**

```
authentication ldap add <host> <port> <ldap_type> <security> <bind_type> <base_DN>
<login_name_att> <user_entry_class> "Optional Parameters"
```

*Note: "Optional Parameters" refer to one or multiple parameters listed in the section **Optional Parameters** (on page 124). They are required only when your server settings need to specify these parameters. For example, if setting the <bind_type> to "authenticatedBind", then you must add the parameter "bindDN" to this command.*

When the above command is successfully performed, a list of all LDAP servers, including the newly-added one, will be displayed, which is similar to the following diagram.

#	IP address	Server type
1	192.1.1.1	OpenLDAP
2	192.2.2.2	OpenLDAP

Variables:

<host> is the IP address or host name of the LDAP server.

<port> is the port number assigned for communication with the LDAP server.

<ldap_type> is one of the LDAP server types: *openldap* or *activeDirectory*.

Type	Description
openldap	OpenLDAP server
activeDirectory	Microsoft Active Directory

<security> is one of the security options: *none*, *startTls* or *tls*.

Type	Description
none	No security
startTls	StartTLS
tls	TLS

<bind_type> is one of the bind options: *anonymousBind*, or *authenticatedBind*.

Type	Description
anonymousBind	Enable the anonymous Bind. Bind DN and password are NOT required.
authenticatedBind	Enable the Bind with authentication. Bind DN and password are required.

<base_DN> is the base DN for search.
 <login_name_att> is the login name attribute.
 <user_entry_class> is the User Entry Object Class.

Optional Parameters

You can add one or multiple "optional parameters", such as specifying the Bind DN or certificate upload, to an LDAP-server-adding command as illustrated below. If adding multiple optional parameters, you must add them to the END of the command and separate them with a space.

- *Example 1 -- Specify an Active Directory Domain's name:*

```
authentication ldap add <host> <port> <ldap_type> <security> <bind_type> <base_DN>
<login_name_att> <user_entry_class> adDomain <AD_domain>
```

- *Example 2 -- Set up the bind DN:*

```
authentication ldap add <host> <port> <ldap_type> <security> <bind_type> <base_DN>
<login_name_att> <user_entry_class> bindDN <bind_DN>
```

► "Optional Parameters" table:

Parameters	To configure
userSearchSubfilter <filter>	User search subfilter
bindDN <bind_DN>	bind DN <ul style="list-style-type: none"> ▪ The system will prompt you to enter and re-confirm the bind password after adding this parameter to the command.
adDomain <AD_domain>	Active Directory Domain name
verifyServerCertificate <verify_cert>	Certificate verification setting <ul style="list-style-type: none"> ▪ After setting to true, the system will prompt you to upload a certificate.
allowExpiredCertificate <allow_exp_cert>	Whether to accept expired or not valid yet certificate.

Variables:

<filter> is the user search subfilter you specify.

<bind_DN> is bind DN.

<AD_domain> is the Active Directory Domain.

<verify_cert> is one of the options: *true* or *false*.

Option	Description
true	Enable the verification of the LDAP server certificate.
false	Disable the verification of the LDAP server certificate.

<allow_exp_cert> is one of the options: *true* or *false*.

Option	Description
true	Certificates that are either expired or not valid yet are all accepted.
false	Only valid certificates are accepted.

Illustrations of Adding LDAP Servers

This section shows several LDAP command examples. Those words highlighted in bold are required for their respective examples.

▶ **An OpenLDAP server:**

```
authentication ldap add op-ldap.raritan.com 389 openldap none anonymousBind
dc=raritan,dc=com uid inetOrgPerson
```

▶ **A Microsoft Active Directory server:**

```
authentication ldap add ac-ldap.raritan.com 389 activeDirectory none anonymousBind
dc=raritan,dc=com SAMAccountName user adDomain raritan.com
```

▶ **An LDAP server with a TLS certificate uploaded:**

- a. Enter the CLI command with the following two TLS-related options set and/or added:
 - <security> is set to *tls* or *startTls*.
 - The "verifyServerCertificate" parameter is added to the command and set to "true."

```
authentication ldap add ldap.raritan.com 389 openldap startTls ... inetOrgPerson
verifyServerCertificate true
```

- b. The system now prompts you to enter the certificate's content.
- c. Type or copy the certificate's content in the CLI and press Enter.

Note: The certificate's content is located between the line containing "BEGIN CERTIFICATE" and the line containing "END CERTIFICATE".

► **An LDAP server with the bind DN and bind password configured:**

- a. Enter the CLI command with the "bindDN" parameter and its data added.

```
authentication ldap add op-ldap.raritan.com 389 openldap none authenticatedBind  
cn=Manager,dc=raritan,dc=com uid inetOrgPerson bindDN user@raritan.com
```

- b. The system prompts you to specify the bind DN password.
- c. Type the password and press Enter.
- d. Re-type the same password.

Copying an Existing Server's Settings

If the server that you will add completely shares the same settings with any server that has been configured, use the following command.

► **Add an LDAP server by copying an existing server's settings:**

```
config:# authentication ldap addClone <server_num> <host>
```

Variables:

<host> is the IP address or host name of the LDAP server.

<server_num> is the sequential number of the specified server shown on the server list of the PRO3X.

Modifying an Existing LDAP Server

You can modify one or multiple parameters of an existing LDAP server, such as its IP address, TCP port number, Base DN and so on. Besides, you can also change the priority or sequence of existing LDAP servers in the server list.

► **Command syntax:**

A command to modify an existing LDAP server's settings looks like the following:

```
authentication ldap modify <server_num> "parameters"
```

Variables:

<server_num> is the sequential number of the specified server in the LDAP server list.

Replace "**parameters**" with one or multiple commands in the following table, depending on which parameter(s) you want to modify.

▶ A list of "parameters":

The following table provides a list of LDAP parameters:

Parameters	Description
host <host>	Change the IP address or host name. <ul style="list-style-type: none"> <host> is the new IP address.
port <port>	Change the TCP port number. <ul style="list-style-type: none"> <port> is the new TCP port number.
serverType <ldap_type>	Change the server type. <ul style="list-style-type: none"> <ldap_type> is the new type of the LDAP server. <ldap_type> values include: <code>openldap</code> and <code>activeDirectory</code>.
securityType <security>	Change the security type. <ul style="list-style-type: none"> <security> is the new security type. <security> values include: <code>none</code>, <code>startTls</code>, and <code>ssl</code>.
bindType <bind_type>	Change the bind type. <ul style="list-style-type: none"> <bind_type> is the new bind type. <bind_type> values include: <code>anonymousBind</code> and <code>authenticatedBind</code>.
searchBaseDN <base_DN>	Change the base DN for search. <ul style="list-style-type: none"> <base_DN> is the new base DN for search.
loginNameAttribute <login_name_att>	Change the login name attribute. <ul style="list-style-type: none"> <login_name_att> is the new login name attribute.
userEntryObjectClass <user_entry_class>	Change the user entry object class. <ul style="list-style-type: none"> <user_entry_class> is the new user entry class.
userSearchSubfilter <user_search_filter>	Change the user search subfilter. <ul style="list-style-type: none"> <user_search_filter> is the new user search subfilter.
adDomain <AD_domain>	Change the Active Directory Domain name. <ul style="list-style-type: none"> <AD_domain> is the new domain name of the Active Directory.
verifyServerCertificate <verify_cert>	Enable or disable the certificate verification. <ul style="list-style-type: none"> <verify_cert> enables or disables the certificate verification feature. Available values include: <code>true</code>, <code>false</code>
certificate	Re-upload a different certificate. <ol style="list-style-type: none"> First add the "certificate" parameter to the command, and press Enter. The system prompts you for the input of the certificate. Type or copy the content of the certificate in the CLI and press Enter.
allowExpiredCertificate <allow_exp_cert>	Determine whether to accept a certificate which is expired or not valid yet. <ul style="list-style-type: none"> <allow_exp_cert> determines whether to accept an expired or not valid yet certificate <allow_exp_cert> values include: <code>true</code>, and <code>false</code>

Using the PRO3X Command Line Interface (CLI)	
bindDN <bind_DN>	Change the bind DN. <ul style="list-style-type: none"> ▪ <bind_DN> is the new bind DN.
bindPassword	Change the bind DN password. <ol style="list-style-type: none"> First add the "bindPassword" parameter to the command, and press Enter. The system prompts you for the input of the password. Type the password and press Enter.
sortPosition <position>	Change the priority of the server (that is, resorting). <ul style="list-style-type: none"> ▪ <position> is the new sequential number of the server in the LDAP server list.

► **Examples:**

Change the IP address of the 1st LDAP server

```
authentication ldap modify 1 host 192.168.3.3
```

Change both the IP address and TCP port of the 1st LDAP server

```
authentication ldap modify 1 host 192.168.3.3 port 633
```

Change the IP address, TCP port and the type of the 1st LDAP server

```
authentication ldap modify 1 host 192.168.3.3 port 633 serverType activeDirectory
```

Removing an Existing LDAP Server

This command removes an existing LDAP server from the server list.

```
config:# authentication ldap delete <server_num>
```

Variables:

<server_num> is the sequential number of the specified server in the LDAP server list.

Radius Settings

All Radius-related commands begin with *authentication radius*.

If you enable Radius authentication, you must add at least one Radius server. Later you can modify or delete any existing Radius server as needed.

Adding a Radius Server

You can repeat the following commands to add Radius servers one by one.

▶ **Command syntax:**

```
authentication radius add <host> <rds_type> <auth_port> <acct_port> <timeout>
<retries>
```

Variables:

<host> is the IP address or host name of the Radius server.

<rds_type> is one of the Radius authentication types: *pap*, *chap*, *msChapV2*.

Type	Description
chap	CHAP
pap	PAP
msChapV2	MSCHAP v2

<auth_port> is the authentication port number.

<acct_port> is the accounting port number.

<timeout> is the timeout value in seconds. It ranges between 1 to 10 seconds.

<retries> is the number of retries. It ranges between 0 to 5.

▶ **To enter the shared secret:**

6. After executing the above Radius command, the system automatically prompts you to enter the shared secret.
7. Type the secret and press Enter.
8. Re-type the same secret and press Enter.

▶ **Example:**

```
authentication radius add 192.168.7.99 chap 1812 1813 10 3
```

Modifying an Existing Radius Server

You can modify one or multiple parameters of an existing Radius server, or change the priority or sequence of existing servers in the server list.

▶ **Change the IP address or host name:**

```
authentication radius modify <server_num> host <host>
```

▶ **Change the Radius authentication type:**

```
authentication radius modify <server_num> authType <rds_type>
```

▶ **Change the authentication port:**

```
authentication radius modify <server_num> authPort <auth_port>
```

▶ **Change the accounting port:**

```
authentication radius modify <server_num> accountPort <acct_port>
```

▶ **Change the timeout value:**

```
authentication radius modify <server_num> timeout <timeout>
```

▶ **Change the number of retries:**

```
authentication radius modify <server_num> retries <retries>
```

▶ **Change the shared secret:**

```
authentication radius modify <server_num> secret
```

► Change the priority of the specified server:

```
authentication radius modify <server_num> sortPosition <position>
```

Tip: You can add more than one parameters to the command. For example, "authentication radius modify <server_num> host <host> authType <rds_type> authPort <auth_port> accountPort <acct_port> ...".

Variables:

<server_num> is the sequential number of the specified server in the Radius server list.

<host> is the new IP address or host name of the Radius server.

<rds_type> is one of the Radius authentication types: *pap*, *chap*, *msChapV2*.

<auth_port> is the new authentication port number.

<acct_port> is the new accounting port number.

<timeout> is the new timeout value in seconds. It ranges between 1 to 10 seconds.

<retries> is the new number of retries. It ranges between 0 to 5.

► To enter the shared secret:

9. After executing the above Radius command, the system automatically prompts you to enter the shared secret.
10. Type the secret and press Enter.
11. Re-type the same secret and press Enter.

► Example:

```
authentication radius add 192.168.7.99 chap 1812 1813 10 3
```

Removing an Existing Radius Server

This command removes an existing Radius server from the server list.

```
config:# authentication radius delete <server_num>
```

Variables:

<server_num> is the sequential number of the specified server in the Radius server list.

Environmental Sensor Configuration Commands

An environmental sensor configuration command begins with *externalsensor*. You can configure the name and location parameters of an individual environmental sensor.

Changing the Sensor Name

This command names an environmental sensor.

```
config:# externalsensor <n> name "<name>"
```

Variables:

<n> is the ID number of the environmental sensor that you want to configure. The ID number is available in the PRO3X web interface or using the command "show externalsensors <n>" in the CLI. It is an integer starting at 1.

<name> is a string comprising up to 64 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.

Specifying the CC Sensor Type

Contact closure sensors support the connection of diverse third-party. You must specify the type of connected detector/switch for proper operation. Use this command when you need to specify the sensor type.

```
config:# externalsensor <n> sensorSubType <sensor_type>
```

Variables:

<n> is the ID number of the environmental sensor that you want to configure. The ID number is available in the PRO3X web interface or using the command "show externalsensors <n>" in the CLI. It is an integer starting at 1.

<sensor_type> is one of these types: *contact*, *smokeDetection*, *waterDetection* or *vibration*.

Type	Description
contact	The connected detector/switch is for detection of door lock or door closed/open status.
smokeDetection	The connected detector/switch is for detection of the smoke presence.
waterDetection	The connected detector/switch is for detection of the water presence.
vibration	The connected detector/switch is for detection of the vibration.

Setting the X Coordinate

This command specifies the X coordinate of an environmental sensor.

```
config:#    externalsensor <n> xlabel "<coordinate>"
```

Variables:

<n> is the ID number of the environmental sensor that you want to configure. The ID number is available in the PRO3X web interface or using the command "show externalsensors <n>" in the CLI. It is an integer starting at 1.

<coordinate> is a string comprising up to 24 ASCII printable characters, and it must be enclosed in quotes.

Setting the Y Coordinate

This command specifies the Y coordinate of an environmental sensor.

```
config:#    externalsensor <n> ylabel "<coordinate>"
```

Variables:

<n> is the ID number of the environmental sensor that you want to configure. The ID number is available in the PRO3X web interface or using the command "show externalsensors <n>" in the CLI. It is an integer starting at 1.

<coordinate> is a string comprising up to 24 ASCII printable characters, and it must be enclosed in quotes.

Setting the Z Coordinate

This command specifies the Z coordinate of an environmental sensor.

```
config:#    externalsensor <n> zlabel "<coordinate>"
```

Variables:

<n> is the ID number of the environmental sensor that you want to configure. The ID number is available in the PRO3X web interface or using the command "show externalsensors <n>" in the CLI. It is an integer starting at 1.

Depending on the Z coordinate format you set, there are two types of values for the <coordinate> variable:

Type	Description
Free form	<coordinate> is a string comprising up to 24 ASCII printable characters, and it must be enclosed in quotes.
Rack units	<coordinate> is an integer number in rack units.

Changing the Sensor Description

This command provides a description for a specific environmental sensor.

```
config:#  externalsensor <n> description "<description>"
```

Variables:

<n> is the ID number of the environmental sensor that you want to configure. The ID number is available in the PRO3X web interface or using the command "show externalsensors <n>" in the CLI. It is an integer starting at 1.

<description> is a string comprising up to 64 ASCII printable characters, and it must be enclosed in quotes when it contains spaces.

Using Default Thresholds

This command determines whether default thresholds, including the deassertion hysteresis and assertion timeout, are applied to a specific environmental sensor.

```
config:#  externalsensor <n> useDefaultThresholds <option>
```

Variables:

<n> is the ID number of the environmental sensor that you want to configure. The ID number is available in the PRO3X web interface or using the command "show externalsensors <n>" in the CLI. It is an integer starting at 1.

<option> is one of the options: *true* or *false*.

Option	Description
true	Default thresholds are selected as the threshold option for the specified sensor.
false	Sensor-specific thresholds are selected as the threshold option for the specified sensor.

Setting the Alarmed to Normal Delay for DX-PIR

This command determines the value of the Alarmed to Normal Delay setting for a presence detector.

```
config:#    externalsensor <n> alarmedToNormalDelay <time>
```

Variables:

<n> is the ID number of the environmental sensor that you want to configure. The ID number is available in the PRO3X web interface or using the command "show externalsensors <n>" in the CLI. It is an integer starting at 1.

<time> is an integer number in seconds, ranging between 0 and 300.

Examples

This section illustrates several environmental sensor configuration examples.

Example 1 - Environmental Sensor Naming

The following command assigns the name "Cabinet humidity" to the environmental sensor with the ID number 4.

```
config:#    externalsensor 4 name "Cabinet humidity"
```

Example 2 - Sensor Threshold Selection

The following command sets the environmental sensor #1 to use the default thresholds, including the deassertion hysteresis and assertion timeout, as its threshold settings.

```
config:#    externalsensor 1 useDefaultThresholds true
```

Configuring Environmental Sensors' Default Thresholds

You can set the default values of upper and lower thresholds, deassertion hysteresis and assertion timeout on a sensor type basis, including temperature, humidity, air pressure and air flow sensors. The default thresholds automatically apply to all environmental sensors that are newly detected or added.

A default threshold configuration command begins with *defaultThresholds*.

You can configure various default threshold settings for the same sensor type at a time by combining multiple commands.

▶ **Set the Default Upper Critical Threshold for a specific sensor type:**

```
defaultThresholds <sensor type> upperCritical <value>
```

▶ **Set the Default Upper Warning Threshold for a specific sensor type:**

```
defaultThresholds <sensor type> upperWarning <value>
```

▶ **Set the Default Lower Critical Threshold for a specific sensor type:**

```
defaultThresholds <sensor type> lowerCritical <value>
```

▶ **Set the Default Lower Warning Threshold for a specific sensor type:**

```
defaultThresholds <sensor type> lowerWarning <value>
```

▶ **Set the Default Deassertion Hysteresis for a specific sensor type:**

```
defaultThresholds <sensor type> hysteresis <hy_value>
```

▶ **Set the Default Assertion Timeout for a specific sensor type:**

```
defaultThresholds <sensor type> assertionTimeout  
<as_value>
```

Variables:

<sensor type> is one of the following numeric sensor types:

Sensor types	Description
absoluteHumidity	Absolute humidity sensors
relativeHumidity	Relative humidity sensors
temperature	Temperature sensors
airPressure	Air pressure sensors
airFlow	Air flow sensors
vibration	Vibration sensors

Using the PRO3X Command Line Interface (CLI)

<value> is the value for the specified threshold of the specified sensor type. Note that diverse sensor types use different measurement units.

Sensor types	Measurement units
absoluteHumidity	g/m ³ (that is, g/m ³)
relativeHumidity	%
temperature	Degrees Celsius (°C) or Fahrenheit (°F), depending on your measurement unit settings.
airPressure	Pascal (Pa) or psi, depending on your measurement unit settings.
airFlow	m/s
vibration	g

<hy_value> is the deassertion hysteresis value applied to the specified sensor type.

<as_value> is the assertion timeout value applied to the specified sensor type. It ranges from 0 to 100 (samples).

Example - Default Upper Thresholds for Temperature

It is assumed that your preferred measurement unit for temperature is set to degrees Celsius. Then the following command sets the default Upper Warning threshold to 20 Celsius and Upper Critical threshold to 24 Celsius for all temperature sensors.

```
defaultThresholds temperature upperWarning 20 upperCritical 24
```

Sensor Threshold Configuration Commands

A sensor configuration command begins with *sensor*. You can use the commands to configure the threshold, hysteresis and assertion timeout values for any sensor associated with the following items:

- Inlets
- Inlet poles (for three-phase PDUs only)
- Overcurrent protectors
- Environmental sensors

It is permitted to assign a new value to the threshold at any time regardless of whether the threshold has been enabled.

Commands for Inlet Sensors

A sensor configuration command for inlets begins with *sensor inlet*.

You can configure various inlet sensor threshold settings at a time by combining multiple commands. Set the Upper Critical threshold for an inlet sensor:

```
sensor inlet <n> <sensor type> upperCritical <option>
```

► Set the Upper Warning threshold for an inlet sensor:

```
sensor inlet <n> <sensor type> upperWarning <option>
```

► Set the Lower Critical threshold for an inlet sensor:

```
sensor inlet <n> <sensor type> lowerCritical <option>
```

► **Set the Lower Warning threshold for an inlet sensor:**

```
sensor inlet <n> <sensor type> lowerWarning <option>
```

► **Set the deassertion hysteresis for an inlet sensor:**

```
sensor inlet <n> <sensor type> hysteresis <hy_value>
```

► **Set the assertion timeout for an inlet sensor:**

```
sensor inlet <n> <sensor type> assertionTimeout <as_value>
```

Variables:

<n> is the number of the inlet that you want to configure. For a single-inlet PDU, <n> is always 1.

<sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor
unbalancedCurrent	Unbalanced load sensor
lineFrequency	Line frequency sensor
phaseAngle	Inlet phase angle sensor

Note: If the requested sensor type is not supported, the "Sensor is not available" message is displayed.

<option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the specified threshold for a specific inlet sensor.
disable	Disables the specified threshold for a specific inlet sensor.
A numeric value	Sets a value for the specified threshold of a specific inlet sensor and enables this threshold at the same time.

<hy_value> is a numeric value that is assigned to the hysteresis for the specified inlet sensor.

<as_value> is a numeric value that is assigned to the assertion timeout for the specified inlet sensor.

► Additional sensors supported by specific models:

Specific PRO3X models support some or all of the following sensors. The CLI command(s) listed above can be also applied to the following sensors. Note that the measurement unit of current values in CLI is **A**, not mA.

Sensor type	Description
peakCurrent	Peak current sensor
reactivePower	Reactive power sensor
displacementPowerFactor	Displacement power factor sensor
residualCurrent	RCM current sensor <ul style="list-style-type: none"> ▪ For Type A, it is the sensor that detects residual AC current. ▪ For Type B, it is the sensor that detects both residual AC and DC current.
residualDCCurrent	RCM DC current sensor - detects residual DC current only. Available only on PDUs with RCM Type B.

Commands for Inlet Pole Sensors

A sensor configuration command for inlet poles begins with *sensor inletpole*. This type of command is available on a three-phase PDU only. You can configure various inlet pole sensor threshold settings at a time by combining multiple commands.

▶ **Set the Upper Critical Threshold for an Inlet Pole:**

```
sensor inletpole <n> <p> <sensor type> upperCritical <option>
```

▶ **Set the Upper Warning Threshold for an Inlet Pole:**

```
sensor inletpole <n> <p> <sensor type> upperWarning <option>
```

▶ **Set the Lower Critical Threshold for an Inlet Pole:**

```
sensor inletpole <n> <p> <sensor type> lowerCritical <option>
```

▶ **Set the Lower Warning Threshold for an Inlet Pole:**

```
sensor inletpole <n> <p> <sensor type> lowerWarning <option>
```

▶ **Set the Inlet Pole's De-assertion Hysteresis:**

```
sensor inletpole <n> <p> <sensor type> hysteresis <hy_value>
```

▶ **Set the Inlet Pole's Assertion Timeout:**

```
sensor inletpole <n> <p> <sensor type> assertionTimeout <as_value>
```

Using the PRO3X Command Line Interface (CLI)

Variables:

<n> is the number of the inlet whose pole sensors you want to configure. For a single-inlet PDU, <n> is always 1.

<p> is the label of the inlet pole that you want to configure.

Pole	Label <p>	Current sensor	Voltage sensor
1	L1	L1	L1 - L2
2	L2	L2	L2 - L3
3	L3	L3	L3 - L1

<sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor
unbalancedCurrent	Unbalanced load sensor

Note: If the requested sensor type is not supported, the "Sensor is not available" message is displayed.

<option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the specified threshold for the specified inlet pole sensor.
disable	Disables the specified threshold for the specified inlet pole sensor.
A numeric value	Sets a value for the specified threshold of the specified inlet pole sensor and enables this threshold at the same time.

<hy_value> is a numeric value that is assigned to the hysteresis for the specified inlet pole sensor.

<as_value> is a number in samples that is assigned to the assertion timeout for the specified inlet pole sensor.

► Additional sensors supported by specific models:

Specific PRO3X models support some or all of the following sensors. The CLI command(s) listed above can be also applied to the following sensors. Note that the measurement unit of current values in CLI is **A**, not mA.

Sensor type	Description
peakCurrent	Peak current sensor
reactivePower	Reactive power sensor
displacementPowerFactor or	Displacement power factor sensor
residualCurrent	RCM current sensor <ul style="list-style-type: none">For Type A, it is the sensor that detects residual AC current.For Type B, it is the sensor that detects both residual AC and DC current.
residualDCCurrent	RCM DC current sensor - detects residual DC current only. Available only on PDUs with RCM Type B.

Commands for Overcurrent Protector Sensors

A sensor configuration command for overcurrent protectors begins with *sensor ocp*.

You can configure various overcurrent protector threshold settings at a time by combining multiple commands.

► Set the Upper Critical threshold for an overcurrent protector:

```
sensor ocp <n> <sensor type> upperCritical <option>
```

► Set the Upper Warning threshold for an overcurrent protector:

```
sensor ocp <n> <sensor type> upperWarning <option>
```

► Set the Lower Critical threshold for an overcurrent protector:

```
sensor ocp <n> <sensor type> lowerCritical <option>
```


► **Set the Lower Warning threshold for an overcurrent protector:**

```
sensor ocp <n> <sensor type> lowerWarning <option>
```

► **Set the deassertion hysteresis for an overcurrent protector:**

```
sensor ocp <n> <sensor type> hysteresis <hy_value>
```

► **Set the assertion timeout for an overcurrent protector:**

```
sensor ocp <n> <sensor type> assertionTimeout <as_value>
```

Variables:

<n> is the number of the overcurrent protector that you want to configure.

<sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor

Note: If the requested sensor type is not supported, the "Sensor is not available" message is displayed.

<option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the specified threshold for the overcurrent protector sensor.
disable	Disables the specified threshold for the overcurrent protector sensor.
A numeric value	Sets a value for the specified threshold of the overcurrent protector sensor and enables this threshold at the same time.

<hy_value> is a numeric value that is assigned to the hysteresis for the specified overcurrent protector sensor.

<as_value> is a number in samples that is assigned to the assertion timeout for the specified overcurrent protector sensor.

Commands for Environmental Sensors

A sensor threshold configuration command for environmental sensors begins with *sensor externalsensor*.

You can configure various environmental sensor threshold settings at a time by combining multiple commands.

▶ **Set the Upper Critical threshold for an environmental sensor:**

```
sensor externalsensor <n> <sensor type> upperCritical <option>
```

▶ **Set the Upper Warning threshold for an environmental sensor:**

```
sensor externalsensor <n> <sensor type> upperWarning <option>
```

▶ **Set the Lower Critical threshold for an environmental sensor:**

```
sensor externalsensor <n> <sensor type> lowerCritical <option>
```

▶ **Set the Lower Warning threshold for an environmental sensor:**

```
sensor externalsensor <n> <sensor type> lowerWarning <option>
```

▶ **Set the de-assertion hysteresis for an environmental sensor:**

```
sensor externalsensor <n> <sensor type> hysteresis <hy_value>
```

► **Set the assertion timeout for an environmental sensor:**

```
sensor externalsensor <n> <sensor type> assertionTimeout <as_value>
```

Variables:

<n> is the ID number of the environmental sensor that you want to configure. The ID number is available in the PRO3X web interface or using the command "show externalsensors <n>" in the CLI. It is an integer starting at 1.

<sensor type> is one of the following numeric sensor types:

Sensor types	Description
absoluteHumidity	Absolute humidity sensors
relativeHumidity	Relative humidity sensors
temperature	Temperature sensors
airPressure	Air pressure sensors
airFlow	Air flow sensors
vibration	Vibration sensors

Note: If the specified sensor type does not match the type of the specified environmental sensor, this error message appears: "Specified sensor type 'XXX' does not match the sensor's type (<sensortype>)," where XXX is the specified sensor type, and <sensortype> is the correct sensor type.

<option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the specified threshold for a specific environmental sensor.
disable	Disables the specified threshold for a specific environmental sensor.
A numeric value	Sets a value for the specified threshold of a specific environmental sensor and enables this threshold at the same time.

<hy_value> is a numeric value that is assigned to the hysteresis for the specified environmental sensor.

<as_value> is a number in samples that is assigned to the assertion timeout for the specified environmental sensor. It ranges between 1 and 100.

Examples

This section illustrates several environmental sensor threshold configuration examples.

Example 1 - Upper Critical Threshold for a Temperature Sensor

The following command sets the Upper Critical threshold of the environmental "temperature" sensor with the ID number 2 to 40 degrees Celsius. It also enables the upper critical threshold if this threshold has not been enabled yet.

```
config:# sensor externalsensor 2 temperature upperCritical 40
```

Example 2 - Warning Thresholds for Inlet Sensors

The following command sets both the Upper Warning and Lower Warning thresholds for the inlet 1 RMS current.

```
sensor inlet 1 current upperWarning 20 lowerWarning 12
```

Results:

The Upper Warning threshold for the inlet 1 RMS current is set to 20A. It also enables the upper warning threshold if this threshold has not been enabled yet.

The Lower Warning threshold for the inlet 1 RMS current is set to 12A. It also enables the lower warning threshold if this threshold has not been enabled yet.

Example 3 - Upper Thresholds for Overcurrent Protector Sensors

The following command sets both the Upper Critical and Upper Warning thresholds for the 2nd overcurrent protector.

```
sensor ocp 2 current upperWarning enable upperCritical 16
```

Results:

The Upper Critical threshold for the 2nd overcurrent protector's RMS current is set to 16A. It also enables the upper critical threshold if this threshold has not been enabled yet.

The Upper Warning threshold for the 2nd overcurrent protector's RMS current is enabled.

Actuator Configuration Commands

An actuator configuration command begins with *actuator*. You can configure the name and location parameters of an individual actuator.

You can configure various parameters for one actuator at a time.

► **Change the name:**

```
config:# actuator <n> name "<name>"
```

► **Set the X coordinate:**

```
config:# actuator <n> xlabel "<coordinate>"
```

► **Set the Y coordinate:**

```
config:# actuator <n> ylabel "<coordinate>"
```

► **Set the Z coordinate:**

```
config:# actuator <n> zlabel "<z_label>"
```

► **Modify the actuator's description:**

```
config:# actuator <n> description "<description>"
```

Variables:

<n> is the ID number assigned to the actuator. The ID number can be found using the PRO3X web interface or CLI. It is an integer starting at 1.

<name> is a string comprising up to 64 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.

<coordinate> is a string comprising up to 24 ASCII printable characters, and it must be enclosed in quotes.

There are two types of values for the <z_label> variable, depending on the Z coordinate format you set:

Type	Description
Free form	<coordinate> is a string comprising up to 24 ASCII printable characters, and it must be enclosed in quotes.
Rack units	<coordinate> is an integer number in rack units.

<description> is a string comprising up to 64 ASCII printable characters, and it must be enclosed in quotes when it contains spaces.

Example - Actuator Naming

The following command assigns the name "Door lock of cabinet 3" to the actuator whose ID number is 9.

```
config:# actuator 9 name "Door lock of cabinet 3"
```

Server Reachability Configuration Commands

You can use the CLI to add or delete an IT device, such as a server, from the server reachability list, or modify the settings for a monitored IT device. A server reachability configuration command begins with *serverReachability*.

Adding a Monitored Device

This command adds a new IT device to the server reachability list.

```
serverReachability add <IP_host> <enable> <succ_ping> <fail_ping> <succ_wait>  
<fail_wait> <resume> <disable_count>
```

Variables:

<IP_host> is the IP address or host name of the IT device that you want to add.

<enable> is one of the options: *true* or *false*.

Option	Description
true	Enables the ping monitoring feature for the newly added device.
false	Disables the ping monitoring feature for the newly added device.

<succ_ping> is the number of successful pings for declaring the monitored device "Reachable." Valid range is 0 to 200.

<fail_ping> is the number of consecutive unsuccessful pings for declaring the monitored device "Unreachable." Valid range is 1 to 100.

<succ_wait> is the wait time to send the next ping after a successful ping. Valid range is 5 to 600 (seconds).

<fail_wait> is the wait time to send the next ping after a unsuccessful ping. Valid range is 3 to 600 (seconds).

<resume> is the wait time before the PRO3X resumes pinging after declaring the monitored device "Unreachable." Valid range is 5 to 120 (seconds).

<disable_count> is the number of consecutive "Unreachable" declarations before the PRO3X disables the ping monitoring feature for the monitored device and returns to the "Waiting for reliable connection" state. Valid range is 1 to 100 or *unlimited*.

Deleting Monitored Devices

This command removes a monitored IT device from the server reachability list.

```
config:# serverReachability delete <n>
```

Variables:

<n> is a number representing the sequence of the IT device in the monitored server list.

You can find each IT device's sequence number using the CLI command of `show serverReachability` as illustrated below.

#	IP address	Enabled	Status
1	10.1.2.58	Yes	Waiting for reliable connection
2	www.servertech.com	Yes	Waiting for reliable connection

Modifying a Monitored Device's Settings

The command to modify a monitored IT device's settings begins with `serverReachability modify`.

You can modify various settings for a monitored device at a time.

► **Modify a device's IP address or host name:**

```
serverReachability modify <n> ipAddress <IP_host>
```

► **Enable or disable the ping monitoring feature for the device:**

```
serverReachability modify <n> pingMonitoringEnabled <option>
```

► **Modify the number of successful pings for declaring "Reachable":**

```
serverReachability modify <n> numberOfSuccessfulPingsToEnable <succ_number>
```

► **Modify the number of unsuccessful pings for declaring "Unreachable":**

```
serverReachability modify <n> numberOfUnsuccessfulPingsForFailure <fail_number>
```

► **Modify the wait time after a successful ping:**

Using the PRO3X Command Line Interface (CLI)

```
serverReachability modify <n> waitTimeAfterSuccessfulPing <succ_wait>
```

► **Modify the wait time after a unsuccessful ping:**

```
serverReachability modify <n> waitTimeAfterUnsuccessfulPing <fail_wait>
```

► **Modify the number of consecutive "Unreachable" declarations before disabling the ping monitoring feature:**

```
serverReachability modify <n> numberOfFailuresToDisable <disable_count>
```

Variables:

<n> is a number representing the sequence of the IT device in the server monitoring list.

<IP_host> is the IP address or host name of the IT device whose settings you want to modify.

<option> is one of the options: *true* or *false*.

Option	Description
true	Enables the ping monitoring feature for the monitored device.
false	Disables the ping monitoring feature for the monitored device.

<succ_number> is the number of successful pings for declaring the monitored device "Reachable." Valid range is 0 to 200.
<fail_number> is the number of consecutive unsuccessful pings for declaring the monitored device "Unreachable." Valid range is 1 to 100.

<succ_wait> is the wait time to send the next ping after a successful ping. Valid range is 5 to 600 (seconds).

<fail_wait> is the wait time to send the next ping after a unsuccessful ping. Valid range is 3 to 600 (seconds).

<resume> is the wait time before the PRO3X resumes pinging after declaring the monitored device "Unreachable." Valid range is 5 to 120 (seconds).

<disable_count> is the number of consecutive "Unreachable" declarations before the PRO3X disables the ping monitoring feature for the monitored device and returns to the "Waiting for reliable connection" state. Valid range is 1 to 100 or *unlimited*.

Example - Server Settings Changed

The following command modifies several ping monitoring settings for the second server in the server reachability list.

```
serverReachability modify 2 numberOfSuccessfulPingsToEnable 10  
numberOfUnsuccessfulPingsForFailure 8 waitTimeAfterSuccessfulPing 30
```

EnergyWise Configuration Commands

An EnergyWise configuration command begins with *energywise*.

Enabling or Disabling EnergyWise

This command syntax determines whether the Cisco® EnergyWise endpoint implemented on the PRO3X is enabled.

```
config:# energywise enabled <option>
```

Variables:

<option> is one of the options: *true* or *false*.

Option	Description
true	The Cisco EnergyWise feature is enabled.
false	The Cisco EnergyWise feature is disabled.

Specifying the EnergyWise Domain

This command syntax specifies to which Cisco® EnergyWise domain the PRO3X belongs.

```
config:# energywise domain <name>
```

Variables:

<name> is a string comprising up to 127 ASCII printable characters. Spaces and asterisks are NOT acceptable.

Specifying the EnergyWise Secret

This command syntax specifies the password (secret) to enter the Cisco® EnergyWise domain.

```
config:# energywise secret <password>
```

Variables:

<password> is a string comprising up to 127 ASCII printable characters. Spaces and asterisks are NOT acceptable.

Changing the UDP Port

This command syntax specifies the UDP port for communications in the Cisco® EnergyWise domain.

```
config:# energywise port <port>
```

Variables:

<port> is the UDP port number ranging between 1 and 65535.

Setting the Polling Interval

This command syntax determines the polling interval at which the Cisco® EnergyWise domain queries the PRO3X.

```
config:# energywise polling <timing>
```

Variables:

<timing> is an integer number in seconds. It ranges between 30 and 600 seconds.

Example - Setting Up EnergyWise

The following command sets up two Cisco® EnergyWise-related features.

```
config:# energywise enabled true port 10288
```

Results:

The EnergyWise feature implemented on the PRO3X is enabled.

The UDP port is set to 10288.

Asset Management Commands

You can use the CLI commands to change the settings of the connected asset strip (if any) or the settings of LEDs on the asset strip.

Asset Strip Management

An asset strip management configuration command begins with `assetStrip`.

Naming an Asset Strip

This command syntax names or changes the name of an asset strip connected to the PRO3X device.

```
config:#  assetStrip <n> name "<name>"
```

Variables:

<n> is the number of the FEATURE port where the selected asset strip is physically connected. For the PRO3X device with only one FEATURE port, the number is always 1.

<name> is a string comprising up to 64 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.

Specifying the Number of Rack Units

This command syntax specifies the total number of rack units on an asset strip connected to the PRO3X device.

```
config:#  assetStrip <n> numberOfRackUnits <number>
```

Note: A rack unit refers to a tag port on the asset strips.

Variables:

<n> is the number of the FEATURE port where the selected asset strip is physically connected. For the PRO3X device with only one FEATURE port, the number is always 1.

<number> is the total number of rack units available on the connected asset strip. This value ranges from 8 to 64.

Specifying the Rack Unit Numbering Mode

This command syntax specifies the numbering mode of rack units on the asset strips connected to the PRO3X device. The numbering mode changes the rack unit numbers.

```
config:#  assetStrip <n> rackUnitNumberingMode <mode>
```

Variables:

<n> is the number of the FEATURE port where the selected asset strip is physically connected. For the PRO3X device with only one FEATURE port, the number is always 1.

<mode> is one of the numbering modes: *topDown* or *bottomUp*.

Mode	Description
topDown	The rack units are numbered in the ascending order from the highest to the lowest rack unit.
bottomUp	The rack units are numbered in the descending order from the highest to the lowest rack unit.

Specifying the Rack Unit Numbering Offset

This command syntax specifies the starting number of rack units on the asset strips connected to the PRO3X device.

```
config:#  assetStrip <n> rackUnitNumberingOffset <number>
```

Variables:

<n> is the number of the FEATURE port where the selected asset strip is physically connected. For the PRO3X device with only one FEATURE port, the number is always 1.

<number> is a starting number for numbering rack units on the connected asset strip. This value is an integer number.

Specifying the Asset Strip Orientation

This command syntax specifies the orientation of the asset strips connected to the PRO3X device. Usually you do not need to perform this command unless your asset strips do NOT come with the tilt sensor, causing the PRO3X unable to detect the asset strips' orientation.

```
config:#  assetStrip <n> assetStripOrientation <orientation>
```

Variables:

<n> is the number of the FEATURE port where the selected asset strip is physically connected. For the PRO3X device with only one FEATURE port, the number is always 1.

<orientation> is one of the options: *topConnector* or *bottomConnector*.

Orientation	Description
topConnector	This option indicates that the asset strip is mounted with the RJ-45 connector located on the top.
bottomConnector	This option indicates that the asset strip is mounted with the RJ-45 connector located at the bottom.

Setting LED Colors for Connected Tags

This command syntax sets the LED color for all rack units on the asset strip #1 to indicate the presence of a connected asset tag.

```
config:#  assetStrip <n> LEDColorForConnectedTags <color>
```

Variables:

<color> is the hexadecimal RGB value of a color in HTML format. The <color> variable ranges from #000000 to #FFFFFF.

Setting LED Colors for Disconnected Tags

This command syntax sets the LED color for all rack units on the connected asset strip(s) to indicate the absence of a connected asset tag.

```
config:#  assetStrip <n> LEDColorForDisconnectedTags <color>
```

Variables:

<color> is the hexadecimal RGB value of a color in HTML format. The <color> variable ranges from #000000 to #FFFFFF.

Rack Unit Configuration

A rack unit refers to a tag port on the asset strips. A rack unit configuration command begins with `rackUnit`.

Naming a Rack Unit

This command syntax assigns or changes the name of the specified rack unit on the specified asset strip.

```
config:#   rackUnit <n> <rack_unit> name "<name>"
```

Variables:

<n> is the number of the FEATURE port where the selected asset strip is physically connected. For the PRO3X device with only one FEATURE port, the number is always 1.

<rack_unit> is the index number of the desired rack unit. The index number is available on the asset strip or the Asset Strip page of the web interface.

<name> is a string comprising up to 64 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.

Setting the LED Operation Mode

This command syntax determines whether a specific rack unit on the specified asset strip follows the global LED color settings.

```
config:#   rackUnit <n> <rack_unit> LEDOperationMode <mode>
```

Variables:

<n> is the number of the FEATURE port where the selected asset strip is physically connected. For the PRO3X device with only one FEATURE port, the number is always 1.

<rack_unit> is the index number of the desired rack unit. The index number is available on the asset strip or the Asset Strip page of the web interface.

<mode> is one of the LED modes: *automatic* or *manual*.

Mode	Description
automatic	This option makes the LED of the specified rack unit follow the global LED color settings. This is the default.

Mode	Description
manual	This option enables selection of a different LED color and LED mode for the specified rack unit.

Setting an LED Color for a Rack Unit

This command syntax sets the LED color for a specific rack unit on the specified asset strip. You need to set a rack unit's LED color only when the LED operation mode of this rack unit has been set to "manual."

```
config:#    rackUnit <n> <rack_unit> LEDColor <color>
```

Variables:

<n> is the number of the FEATURE port where the selected asset strip is physically connected. For the PRO3X device with only one FEATURE port, the number is always 1.

<rack_unit> is the index number of the desired rack unit. The index number is available on the asset strip or the Asset Strip page of the web interface.

<color> is the hexadecimal RGB value of a color in HTML format. The <color> variable ranges from #000000 to #FFFFFF.

Note: A rack unit's LED color setting overrides the global LED color setting on it.

Setting an LED Mode for a Rack Unit

This command syntax sets the LED mode for a specific rack unit on the specified asset strip. You need to set a rack unit's LED mode only when the LED operation mode of this rack unit has been set to "manual."

```
config:#    rackUnit <n> <rack_unit> LEDMode <mode>
```

Variables:

<n> is the number of the FEATURE port where the selected asset strip is physically connected. For the PRO3X device with only one FEATURE port, the number is always 1.

<rack_unit> is the index number of the desired rack unit. The index number is available on the asset strip or the Asset Strip page of the web interface.

<mode> is one of the LED modes: *on*, *off*, *blinkSlow* or *blinkFast*.

Mode	Description
on	This mode has the LED stay lit permanently.

Using the PRO3X Command Line Interface (CLI)

Mode	Description
off	This mode has the LED stay off permanently.
blinkSlow	This mode has the LED blink slowly.
blinkFast	This mode has the LED blink quickly.

Examples

This section illustrates several asset management examples.

Example 1 - Asset Strip LED Colors for Disconnected Tags

This command syntax sets the LED color for all rack units on the asset sensor #1 to BLACK (that is, 000000) to indicate the absence of a connected asset tag.

```
config:#    assetStrip 1 LEDColorForDisconnectedTags #000000
```

Note: Black color causes the LEDs to stay off.

Example 2 - Rack Unit Naming

The following command assigns the name "Linux server" to the rack unit whose index number is 25 on the asset sensor#1.

```
config:#    rackUnit 1 25 name "Linux server"
```

Serial Port Configuration Commands

A serial port configuration command begins with *serial*.

Setting the Baud Rates

The following commands set the baud rate (bps) of the serial port labeled CONSOLE / MODEM on the PRO3X device. Change the baud rate before connecting it to the desired device, such as a computer, a Raritan's P2CIM-SER, or a modem, through the serial port, or there are communications errors. If you change the baud rate dynamically after the connection has been made, you must reset the PRO3X or power cycle the connected device for proper communications.

► **Determine the CONSOLE baud rate:**

```
config:# serial consoleBaudRate <baud_rate>
```

► **Determine the MODEM baud rate:**

```
config:# serial modemBaudRate <baud_rate>
```

Variables:

<baud_rate> is one of the baud rate options: *1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200*.

Forcing the Device Detection Mode

This command forces the serial port on the PRO3X to enter a specific device detection mode.

```
config:# serial deviceDetectionType <mode>
```

Variables:

<mode> is one of the detection modes: *automatic, forceConsole, forceAnalogModem, or forceGsmModem*.

Option	Description
automatic	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.
SforceConsole	The PRO3X attempts to recognize that the connected device is set for the console mode.
forceAnalogModem	The PRO3X attempts to recognize that the connected device is an analog modem.
forceGsmModem	The PRO3X attempts to recognize that the connected device is a GSM modem.

Example

The following command sets the CONSOLE baud rate of the PRO3X device's serial port to 9600 bps.

```
config:#    serial consoleBaudRate 9600
```

Multi-Command Syntax

To shorten the configuration time, you can combine various configuration commands in one command to perform all of them at a time. All combined commands must belong to the same configuration type, such as commands prefixed with *network*, *user modify*, *sensor externalsensor* and so on.

A multi-command syntax looks like this:

```
<configuration type> <setting 1> <value 1> <setting 2> <value 2> <setting 3> <value 3> ...
```

Example 1 - Combination of ETH1's Activation, Configuration Method and IP

The following multi-command syntax configures IPv4 address, configuration method and activation status for ETH1's network connectivity simultaneously.

```
network ipv4 interface eth1 enabled true configMethod static address 192.168.84.225/24
```

Results:

The ETH1 interface is enabled.

ETH1's configuration method is set to static IP address.

ETH1's IPv4 address is set to 192.168.84.225/24.

Example 2 - Combination of Upper Critical and Upper Warning Settings

The following multi-command syntax simultaneously configures Upper Critical and Upper Warning thresholds for the RMS current of the 2nd overcurrent protector.

```
sensor ocp 2 current upperCritical disable upperWarning 15
```

Results:

The Upper Critical threshold of the 2nd overcurrent protector's RMS current is disabled.

The Upper Warning threshold of the 2nd overcurrent protector's RMS current is set to 15A and enabled at the same time.

Example 3 - Combination of SSID and PSK Parameters

This multi-command syntax configures both SSID and PSK parameters simultaneously for the wireless feature.

```
config:# network wireless SSID myssid PSK encryp_key
```

Results:

The SSID value is set to myssid.

The PSK value is set to encryp_key.

Example 4 - Combination of Upper Critical, Upper Warning and Lower Warning Settings

The following multi-command syntax configures Upper Critical, Upper Warning and Lower Warning thresholds for the outlet 5 RMS current simultaneously.

```
sensor outlet 5 current upperCritical disable upperWarning enable lowerWarning 1.0
```

Results:

The Upper Critical threshold of outlet 5 RMS current is disabled.

The Upper Warning threshold of outlet 5 RMS current is enabled.

The Lower Warning threshold of outlet 5 RMS current is set to 1.0A and enabled at the same time.

Actuator Control Operations

An actuator, which is connected to a dry contact signal channel of a sensor package, can control a mechanism or system. You can switch on or off that mechanism or system through the actuator control command in the CLI.

Perform these commands in the administrator or user mode.

Switching On an Actuator

This command syntax turns on one actuator.

```
# control actuator <n> on
```

To quicken the operation, you can add the parameter `"/y"` to the end of the command, which confirms the operation.

```
# control actuator <n> on /y
```

Variables:

`<n>` is an actuator's ID number.

The ID number is available in the PRO3X web interface or using the show command in the CLI. It is an integer starting at 1.

If you entered the command without `"/y"`, a message appears, prompting you to confirm the operation. Then:

- Type `y` to confirm the operation, OR
- Type `n` to abort the operation

Switching Off an Actuator

This command syntax turns off one actuator.

```
# control actuator <n> off
```

To quicken the operation, you can add the parameter `"/y"` to the end of the command, which confirms the operation.

```
# control actuator <n> off /y
```

Variables:

`<n>` is an actuator's ID number.

The ID number is available in the PRO3X web interface or using the show command in the CLI. It is an integer starting at 1.

If you entered the command without `/y`, a message appears, prompting you to confirm the operation. Then:

- Type `y` to confirm the operation, OR
- Type `n` to abort the operation

Example - Turning on a Specific Actuator

The following command turns on the actuator whose ID number is 8.

```
# control actuator 8 on
```

Unblocking a User

If any user is blocked from accessing the PRO3X, you can unblock them at the local console.

► To unblock a user:

1. Access the CLI interface using any terminal program via a local connection.
2. When the Username prompt appears, type `unlock` and press Enter.

Username: `unlock`

3. When the "Username to unblock" prompt appears, type the name of the blocked user and press Enter.

Username to unblock:

4. A message appears, indicating that the specified user was unblocked successfully.

Resetting the PRO3X

You can reset the PRO3X to factory defaults or simply restart it using the CLI commands.

Restarting the PDU

This command restarts the PRO3X. It is not a factory default reset.

► To restart the PRO3X:

1. Ensure you have entered administrator mode and the `#` prompt is displayed.
2. Type either of the following commands to restart the PRO3X.

```
# reset unit
```

-- OR --

```
# reset unit /y
```

3. If you entered the command without `/y` in Step 2, a message appears prompting you to confirm the operation. Type `y` to confirm the reset.
4. Wait until the reset is complete.

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 to Factory Defaults

The following commands restore all settings of the PRO3X to factory defaults.

► **To reset PRO3X settings after login, use either command:**

```
#      reset factorydefaults
      -- OR --
#      reset factorydefaults /y
```

► **To reset PRO3X settings before login:**

```
Username:  factorydefaults
```

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.

Network Troubleshooting

The PRO3X provides 4 diagnostic commands for troubleshooting network problems: *nslookup*, *netstat*, *ping*, and *traceroute*. The diagnostic commands function as corresponding Linux commands and can get corresponding Linux outputs.

Entering Diagnostic Mode

Diagnostic commands function in the diagnostic mode only.

► **To enter the diagnostic mode:**

1. Enter either of the following modes:
 - Administrator mode: The # prompt is displayed.
 - User mode: The > prompt is displayed.
2. Type `diag` and press Enter. The `diag#` or `diag>` prompt appears, indicating that you have entered the diagnostic mode.
3. Now you can type any diagnostic commands for troubleshooting.

Quitting Diagnostic Mode

► **To quit the diagnostic mode, use this command:**

```
diag>      exit
```

The # or > prompt appears after pressing Enter, indicating that you have entered the administrator or user mode.

Diagnostic Commands

The diagnostic command syntax varies from command to command.

Querying DNS Servers

This command syntax queries Internet domain name server (DNS) information of a network host.

```
diag> nslookup <host>
```

Variables:

<host> is the name or IP address of the host whose DNS information you want to query.

Showing Network Connections

This command syntax displays network connections and/or status of ports.

```
diag> netstat <option>
```

Variables:

<option> is one of the options: *ports* or *connections*.

Option	Description
ports	Shows TCP/UDP ports.
connections	Shows network connections.

Testing the Network Connectivity

This ping command sends the ICMP ECHO_REQUEST message to a network host for checking its network connectivity. If the output shows the host is responding properly, the network connectivity is good. If not, either the host is shut down or it is not being properly connected to the network.

```
diag> ping <host>
```

Variables:

<host> is the host name or IP address whose networking connectivity you want to check.

Options:

You can include any or all of additional options listed below in the ping command.

Options	Description
count <number1>	Determines the number of messages to be sent. <number1> is an integer number between 1 and 100.
size <number2>	Determines the packet size. <number2> is an integer number in bytes between 1 and 65468.
timeout <number3>	Determines the waiting period before timeout. <number3> is an integer number in seconds ranging from 1 to 600.

The command looks like the following when it includes all options:

```
ping <host> count <number1> size <number2> timeout <number3>
```

Tracing the Route

This command syntax traces the network route between your PRO3X and a network host.

```
diag> traceroute <host> <useICMP>
```

Variables:

<host> is the name or IP address of the host you want to trace.

<useICMP> is optional. It has only one value -- useICMP. Type useICMP in the end of this command only when you want to use ICMP packets rather than UDP packets.

Example - Ping Command

The following command checks the network connectivity of the host 192.168.84.222 by sending the ICMP ECHO_REQUEST message to the host for 5 times.

```
diag> ping 192.168.84.222 count 5
```

Retrieving Previous Commands

If you would like to retrieve any command that was previously typed in the same connection session, press the Up arrow (↑) on the keyboard several times until the desired command is displayed.

Automatically Completing a Command

A CLI command always consists of several words. You can easily enter a command by typing first word(s) or letter(s) and then pressing Tab or Ctrl+i instead of typing the whole command word by word.

▶ **To have a command completed automatically:**

4. Type initial letters or words of the desired command. Make sure the letters or words you typed are unique so that the CLI can identify the command you want.
5. Press Tab or Ctrl+i until the complete command appears.
6. If there are more than one possible commands, a list of these commands is displayed. Then type the full command.

▶ **Examples:**

Example 1 (only one possible command):

- a. Type the first word and the first letter of the second word of the "reset factorydefaults" command -- that is, reset f.
- b. Then press Tab or Ctrl+i to complete the second word.

Using the PRO3X Command Line Interface (CLI)

Example 2 (only one possible command):

- a. Type the first word and initial letters of the second word of the "security strongPasswords" command -- that is, security str.
- b. Then press Tab or Ctrl+i to complete the second word.

Example 3 (more than one possible commands):

- a. Type only the first two words of the "network ipv4 gateway xxx.xxx.xxx.xxx" command -- that is, network ipv4.
- b. Then press Tab or Ctrl+i one or two times, a list of possible commands displays as shown below.

```
gateway          interface      staticRoutes
```

- c. Type the full command "network ipv4 gateway xxx.xxx.xxx.xxx", according to the onscreen command list.

Logging out of CLI

After completing your tasks using the CLI, always log out of the CLI to prevent others from accessing the CLI.

► To log out of the CLI:

1. Ensure you have entered administrator mode and the # prompt is displayed.
2. Type **exit** and press Enter.

Using SCP Commands

You can perform a Secure Copy (SCP) command to update the PRO3X firmware, do bulk configuration, or backup and restore the configuration.

Firmware Update via SCP

Same as any PRO3X firmware update, all user management operations are suspended and all login attempts fail during the SCP firmware update.

Warning: Do NOT perform the firmware upgrade over a wireless network connection.

► To update the firmware via SCP:

1. Type the following SCP command and press Enter.

```
scp <firmware file> <user name>@<device ip>:/fwupdate
```

- *<firmware file>* is the PRO3X firmware's filename. If the firmware file is not in the current directory, you must include the path in the filename.
- *<user name>* is the "admin" or any user profile with the Firmware Update permission.
- *<device ip>* is the IP address or hostname of the PRO3X where you want to upload the specified file.

2. Type the password when prompted, and press Enter.

3. The system transmits the specified firmware file to the PRO3X, and shows the transmission speed and percentage.

4. When the transmission is complete, it shows the following message, indicating that the PRO3X starts to update its firmware now. Wait until the upgrade completes.

Starting firmware update. The connection will be closed now.

► SCP example:

```
scp pdu-px2-030410-44599.bin admin@192.168.87.50:/fwupdate
```

► Windows PSCP command:

PSCP in Windows works in a similar way to the SCP.

- `pscp <firmware file> <user name>@<device ip>:/fwupdate`

Bulk Configuration via SCP

Like performing bulk configuration via the web interface, there are two steps with the bulk configuration using the SCP commands:

- a. Save a configuration from a source PRO3X.
- b. Copy the configuration file to one or multiple destination PRO3X.

► To save the configuration via SCP:

1. Type the following SCP command and press Enter.

```
scp <user name>@<device ip>:/bulk_config.txt <filename>
```

- *<user name>* is the "admin" or any user profile with Administrator Privileges.

- `<device ip>` is the IP address or hostname of the PRO3X whose configuration you want to save.
 - `<filename>` is the custom filename you assign to the "bulk_config.txt" of the source PRO3X.
2. Type the user password when prompted.
 3. The system saves the configuration from the PRO3X to a file named "bulk_config.txt."

► To copy the configuration via SCP:

4. Type the following SCP command and press Enter.

```
scp bulk_config.txt <user name>@<device ip>:/bulk_restore
```

- `<user name>` is the "admin" or any user profile with Administrator Privileges
- `<device ip>` is the IP address of the PRO3X whose configuration you want to copy.

5. Type the user password when prompted.
6. The system copies the configuration included in the file "bulk_config.txt" to another PRO3X, and displays the following message.

```
Starting restore operation. The connection will be closed now.
```

► SCP examples:

Save operation:

```
scp admin@192.168.87.50:/bulk_config.txt today_config.txt
```

Copy operation:

```
scp today_config.txt admin@192.168.87.47:/bulk_restore
```

► Windows PSCP commands:

PSCP in Windows works in a similar way to the SCP.

Save operation:

```
pscp <user name>@<device ip>:/bulk_config.txt today_config.txt
```

Copy operation:

```
pscp today_config.txt <user name>@<device ip>:/bulk_restore
```

► Alternative of bulk configuration via SCP:

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.

Backup and Restore via SCP

To back up ALL settings of a PRO3X, including device-specific settings, you should perform the backup operation instead of the bulk configuration.

You can restore all settings to previous ones after a backup file is available.

▶ To back up the settings via SCP:

1. Type the following SCP command and press Enter.

```
scp <user name>@<device ip>:/backup_settings.txt
```

- <user name> is the "admin" or any user profile with Administrator Privileges
 - <device ip> is the IP address or hostname of the PRO3X whose settings you want to back up.
2. Type the user password when prompted.
 3. The system saves the settings from the PRO3X to a file named "backup_settings.txt."

▶ To restore the settings via SCP:

1. Type the following SCP command and press Enter.

```
scp backup_settings.txt <user name>@<device ip>:/settings_restore
```

- <user name> is the "admin" or any user profile with Administrator Privileges
 - <device ip> is the IP address or hostname of the PRO3X whose settings you want to restore.
2. Type the user password when prompted.
 3. The system copies the configuration included in the file "backup_settings.txt" to the PRO3X, and displays the following message.

```
Starting restore operation. The connection will be closed now.
```

▶ SCP examples:

Backup operation:

```
scp admin@192.168.87.50:/backup_settings.txt
```

Restoration operation:

```
scp backup_settings.txt admin@192.168.87.50:/settings_restore
```

▶ Windows PSCP commands:

PSCP in Windows works in a similar way to the SCP.

Backup operation:

```
pscp <user name>@<device ip>:/backup_settings.txt
```

Restoration operation:

```
pscp backup_settings.txt <user name>@<device ip>:/settings_restore
```

Downloading Diagnostic Data via SCP

You can download the diagnostic data via SCP.

► To download the diagnostic data via SCP:

1. Type one of the following SCP commands and press Enter.

Scenario 1: Use the default SCP port and default filename

- SSH/SCP port is the default (22), and the accessed PRO3X is a standalone device.
- The diagnostic file's default filename "diag-data.zip" is wanted. Then add a dot (.) in the end of the SCP command as shown below.

```
scp <user name>@<device ip>:/diag-data.zip .
```

Scenario 2: Specify a different SCP port but use the default filename

- SSH/SCP port is NOT the default (22), or the accessed PRO3X is a Port-Forwarding link device.
- The diagnostic file's default filename "diag-data.zip" is wanted. Then add a dot in the end of the SCP command as shown below.

```
scp -P <port> <user name>@<device ip>:/diag-data.zip .
```

Scenario 3: Specify a new filename but use the default SCP port

- SSH/SCP port is the default (22), and the accessed PRO3X is a standalone device.
- Renaming the diagnostic file is wanted.

```
scp <user name>@<device ip>:/diag-data.zip <filename>
```

Scenario 4: Specify a different SCP port and a new filename

- SSH/SCP port is NOT the default (22), or the accessed PRO3X is a Port-Forwarding link device.
- Renaming the diagnostic file is wanted.

```
scp -P <port> <user name>@<device ip>:/diag-data.zip <filename>
```

- *<user name>* is the "admin" or any user profile with Administrator Privileges or "Unrestricted View Privileges" privileges.
 - *<device ip>* is the IP address or hostname of the PRO3X whose data you want to download.
 - *<port>* is the current SSH/SCP port number, or the port number of a specific link device in the Port-Forwarding chain.
 - *<filename>* is the new filename of the downloaded file.
2. Type the password when prompted.
 3. The system downloads the specified data from the PRO3X onto your computer.
 - If you do NOT specify a new filename in the command, such as Scenarios 1 or 2, the downloaded file's default name is "diag-data.zip."
 - If you specify a new filename in the command, such as Scenarios 3 or 4, the downloaded file is renamed accordingly.

► SCP example:

```
scp admin@192.168.87.50:/diag-data.zip .
```

► **Windows PSCP command:**

PSCP in Windows works in a similar way to the SCP.

- `pscp -P <port> <user name>@<device ip>:/diag-data.zip <filename>`

Uploading or Downloading Raw Configuration Data

You can download the raw configuration data of a specific PRO3X for review, backup or modification.

After modifying or creating any raw configuration data, you can upload it to a specific PRO3X for changing its configuration. The uploaded raw configuration file can contain only partial configuration keys that you want to modify. Other settings that are not contained in the uploaded file will remain unchanged.

Syntax of the raw configuration data is completely the same as the syntax in the config.txt file.

Warning: Some configuration keys in the downloaded raw configuration are commented out, and those must NOT be part of the configuration that will be uploaded to any PRO3X.

► **To download raw configuration data:**

1. Type one of the following SCP commands and press Enter.

Scenario 1: Use the default SCP port and default filename

- SSH/SCP port is the default (22), and the accessed PRO3X is a standalone device.
- The raw configuration file's default filename "raw_config.txt" is wanted. Then add a dot (.) in the end of the SCP command as shown below.

```
scp <user name>@<device ip>:/raw_config.txt .
```

Scenario 2: Specify a different SCP port but use the default filename

- SSH/SCP port is NOT the default (22), or the accessed PRO3X is a Port-Forwarding link device.
- The raw configuration file's default filename "raw_config.txt" is wanted. Then add a dot in the end of the SCP command as shown below.

```
scp -P <port> <user name>@<device ip>:/raw_config.txt .
```

Scenario 3: Specify a new filename but use the default SCP port

- SSH/SCP port is the default (22), and the accessed PRO3X is a standalone device.
- Renaming the raw configuration file is wanted.

```
scp <user name>@<device ip>:/raw_config.txt <filename>
```

Scenario 4: Specify a different SCP port and a new filename

- SSH/SCP port is NOT the default (22), or the accessed PRO3X is a Port-Forwarding link device.
- Renaming the raw configuration file is wanted.

```
scp -P <port> <user name>@<device ip>:/raw_config.txt <filename>
```

- `<user name>` is the "admin" or any user profile with Administrator Privileges.
- `<device ip>` is the IP address or hostname of the PRO3X whose data you want to download.

- <port> is the current SSH/SCP port number, or the port number of a specific link device in the Port-Forwarding chain.
 - <filename> is the new filename of the downloaded file.
2. Type the password when prompted.
 3. The system downloads the specified data from the PRO3X onto your computer.
- If you do NOT specify a new filename in the command, such as Scenarios 1 or 2, the downloaded file's default name is "raw_config.txt."
 - If you specify a new filename in the command, such as Scenarios 3 or 4, the downloaded file is renamed accordingly.

► To upload raw configuration data:

4. Type one of the following SCP commands and press Enter.

Scenario 1: Only one PRO3X to configure, with the default SCP port

- SSH/SCP port is the default (22), and the accessed PRO3X is a standalone device.
- There is only one device to configure so a CSV file for device-specific settings is NOT needed.

```
scp <config file> <user name>@<device ip>:/raw_config_update
```

Scenario 2: Only one PRO3X to configure, with a non-default SCP port

- SSH/SCP port is NOT the default (22), or the accessed PRO3X is a Port-Forwarding link device.
- There is only one device to configure so a CSV file for device-specific settings is NOT needed.

```
scp -P <port> <config file> <user name>@<device ip>:/raw_config_update
```

Scenario 3: Multiple PRO3X to configure, with the default SCP port

- SSH/SCP port is the default (22), and the accessed PRO3X is a standalone device.
- There are multiple devices to configure so a CSV file for device-specific settings is needed during the upload.

```
scp <dev_list file> <config file> <user name>@<device ip>:/raw_config_update /match=<col>
```

Scenario 4: Multiple PRO3X to configure, with a non-default SCP port

- SSH/SCP port is NOT the default (22), or the accessed PRO3X is a Port-Forwarding link device.
- There are multiple devices to configure so a CSV file for device-specific settings is needed during the upload.

```
scp -P <port> <dev_list file> <config file> <user name>@<device ip>:/raw_config_update /match=<dev_col>
```

- <config file> is the filename of the custom raw configuration that you want to upload.
- <user name> is the "admin" or any user profile with Administrator Privileges.
- <device ip> is the IP address or hostname of the PRO3X where you want to upload the specified file.
- <port> is the current SSH/SCP port number, or the port number of a specific link device in the Port-Forwarding chain.
- <dev_list file> is the name of the CSV file for configuring multiple PRO3X with device-specific settings. For device-specific settings in the <config file>, refer each device-specific configuration key to a specific column in the <dev_list file>.

- `<dev_col>` comprises "serial:" or "mac:" and the number of the column where the serial number or MAC address of each PRO3X is in the uploaded CSV file. This is the data based on which each device finds its device-specific settings.

For example:

- If the second column contains each device's serial number, the parameter is then `serial:2`.
- If the seventh column contains each device's MAC address, the parameter is then `mac:7`.

▶ SCP examples:

Raw configuration download example --

```
scp admin@192.168.87.50:/raw_config.txt config.txt
```

Raw configuration upload example with the configuration file only --

```
scp config.txt admin@192.168.87.50:/raw_config_update
```

Raw configuration upload example with both configuration and device list files --

```
scp devices.csv config.txt admin@192.168.87.50:/raw_config_update /match=serial:2
```

▶ Windows PSCP commands:

PSCP in Windows works in a similar way to the SCP.

```
pscp -P <port> <user name>@<device ip>:/raw_config.txt <filename>
```

```
pscp -P <port> <CSV file> <config file> <user name>@<device ip>:/raw_config_update  
/match=<col>
```

▶ Alternative of bulk configuration via SCP:

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 via SCP (on page 172)

Keys that Cannot Be Uploaded

The raw configuration downloaded from any PRO3X contains a few configuration keys that are commented out with either syntax below.

Comment syntax	Description
#INTERNAL#	These keys are internal ones. They are NOT user configurable settings.
#OLD/INVALID#	These keys are old or invalid ones.

Note that these configuration keys cannot be part of the configuration that you will upload to any PRO3X. That is, they should be either not available or they remain to be commented out in the configuration file you will upload.

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 exigences 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)	0	0	0	0	0	0
印刷板组件 (PCAs)	X	0	0	0	0	0
<p>0 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.</p> <p>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.</p>						

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



be supported.

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

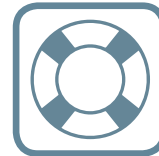
servertech.com/product-selector



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**