PX4 User Guide

Copyright © 2025 Legrand
PDU_G4_UG_G1_4.3.11
October 2025
Release 4.3.11

Contents

Introduction to Xerus Technology Platform **13**

Safety Instructions. . . . 13
Safety Warnings. . . . 14
Safety Warnings. . . . 16
Package Contents. . . . 19
Zero U Products. . . . 19
1U Products. . . . 19
2U Products. . . . 20
Before You Begin. . . . 20
Unpacking the Product and Components. . . . 20
Preparing the Installation Site. . . . 20
Checking the Branch Circuit Rating. . . . 20
Filling Out the Equipment Setup Worksheet. . . . 20
APIPA and Link-Local Addressing. . . . 21

Rackmounts **22**

Circuit Breaker Orientation Limitation. . . . 22
Rackmount Safety Guidelines. . . . 22
0U Button Mount. . . . 22

Initial Installation and Configuration **24**

Connecting the PDU to a Power Source. . . . 24
Connecting to Your Network. . . . 24
USB Wireless LAN Adapter - DX2-WIFI-KIT. . . . 25
Supported Wireless LAN Configuration. . . . 25
Dual Ethernet Connection. . . . 25
Configuring the PX4. . . . 26
Connecting a Mobile Device. . . . 26
Saving User Credentials for PDView's Automatic Login. . . . 30
Connecting to a Computer. . . . 32
Bulk Configuration Methods. . . . 33
Cascading for Shared Ethernet Connectivity. . . . 34
Best Practices for Cascading. . . . 35
Power-Sharing Restrictions and Connection. . . . 36
Power Sharing Port on iX9 Controllers. . . . 37
Power-Sharing Configurations and Restrictions. . . . 37
Smart Sensor Configurations for Power Sharing. . . . 38
Power Sharing Limitations on Mobile Devices. . . . 39

Linking Units **40**

FAQs. 41
Linking in the Web Interface. 44
Viewing the Primary Unit. 44
Options for Adding Link Units. 45
TLS Certificates for PDU Linking. 45
Adding a Link Unit. 45
Linking Cascaded Units. 47
Primary Units Manage Link Units. 52
Releasing a Link Unit. 52
Switching to a Different Unit. 53
Re-linking a Link Unit. 54
Viewing Link Unit Information. 54
Pairwise Outlet Groups. 58
OCPs Page. 60
Peripherals Page. 60
Device Information Page. 60
Outlet Groups. 62
Controlling Outlets in Groups. 64
PDU Linking at the Rack. 65
Displays for Primary and Link Units. 67
Linking in the CLI. 68
Linking CLI Commands. 69

Using the Hardware Features **71**

Inlet. 71
Outlets and Outlet LEDs. 71
PX4 Series Outlets and LEDs. 71
Connection Ports. 72
PX4 Series Connection Ports. 72
Connection Port Functions. 73
Front Panel Display. 73
Automatic and Manual Modes. 74
Control Buttons. 75
Operating the Front Panel Display. 75
Alerts Notice in a Yellow or Red Screen. 106
Port Overload - Reset Fuse. 109
Showing the Firmware Upgrade Progress. 110
Manually Changing Zero U LCD Orientation. 110
Reset Button. 111

Circuit Breakers. 111
Resetting the Button-Type Circuit Breaker. 111
Resetting the Handle-Type Circuit Breaker. 112
Fuse. 113
Fuse Replacement on Zero U Models. 114
Fuse Replacement on 1U Models. 115
Beeper. 117
Replaceable Controller. 117
Threaded Grounding Point. 118
Universal Input Cord. 118

Using the Web Interface **120**

Supported Web Browsers and Mobile Devices. 120
Login, Logout and Password Change. 120
Login and Logout. 120
Changing Your Password. 121
Web Interface Overview. 122
Menu. 124
Quick Access to a Specific Page. 125
Sorting a List. 125
Minimum and Maximum Values for Numeric Sensors. 125
Dashboard - PDUs. 129
Dashboard - Inlet I1. 130
Dashboard - OCP. 132
Dashboard - Alerted Sensors. 134
Dashboard - Inlet History. 135
Dashboard - Alarms. 136
PDU. 138
Latching Relay Behavior. 142
Options for Outlet State on Power Up. 143
Initialization Delay Use Cases. 144
Inrush Current and Inrush Guard Delay. 144
Trip Cause Outlet Handling. 144
Time Units. 144
Setting Thresholds for Total Active Energy or Power. 145
Power Supply Sensor. 146
Inlet. 147
Configuring a Multi-Inlet Model. 153
Outlets. 155
Available Data of the Outlets Overview Page. 158
Threshold Bulk Setup. 159
Sequence Setup. 162

Load Shedding Setup: Setting Non-Critical Outlets. 164
Load Shedding Mode: Activate or Deactivate. 165
Individual Outlet Pages. 168
Outlet Groups. 175
Creating an Outlet Group. 176
Outlet Group Power Control. 177
Resetting a Group's Energy Counter and Minimum/Maximum Values. 178
Modifying an Outlet Group. 179
Deleting an Outlet Group. 180
OCPs. 180
Individual OCP Pages. 182
OCP Trip-Cause Detection. 185
OCP Trip-Cause Waveform. 187
Peripherals. 188
Yellow- or Red-Highlighted Sensors. 193
Managed vs Unmanaged Sensors/Actuators. 194
Sensor/Actuator States. 194
Finding the Sensor's Serial Number. 196
Group Peripheral Sensors. 196
Identifying the Sensor Position and Channel. 197
Automatic Management of Sensors. 198
Managing One Sensor or Actuator. 198
Individual Sensor/Actuator Pages. 200
Z Coordinate Format. 205
Asset Strips. 206
Asset Strip Automatic Firmware Upgrade. 214
Serial Access With Dominion Serial Access Module. 215
DSAM Connection. 216
DSAM LED Operation. 216
View DSAM Serial Ports 217
Configure DSAM Serial Ports. 217
Connect to DSAM Serial Targets in the Web Interface. 219
DSAM CLI Commands. 219
Connect to DSAM Serial Targets via SSH. 221
User Management. 221
Creating Users. 222
Editing or Deleting Users. 226
Creating Roles. 227
Editing or Deleting Roles. 229
Setting Your Preferred Measurement Units. 230
Setting Default Measurement Units. 231
Device Settings. 232

Network Settings. 232
Configuring Network Services. 255
Configuring Security Settings. 265
Setting the Date and Time. 286
Door Access. 289
Event Rules and Actions. 291
Setting Data Logging. 343
Configuring Data Push Settings. 346
Monitoring Server Accessibility. 351
Front Panel Settings. 357
Configuring the Serial Port. 358
Lua Scripts. 359
Miscellaneous. 363
Using Prometheus and Grafana. 364
Requirements for Prometheus and Grafana. 365
Collected Data 365
Maintenance. 366
Device Information. 366
Viewing Connected Users. 367
Viewing, Pausing, Resuming or Clearing the Local Event Log. 368
Updating the Firmware. 370
Viewing Firmware Update History. 372
Bulk Configuration. 372
Backup and Restore of Device Settings. 377
Network Diagnostics. 378
Downloading Diagnostic Information. 378
Hardware Issue Detection. 379
Rebooting. 380
Resetting All Settings to Factory Defaults. 381
Webcam Management. 382
Configuring Webcams and Viewing Live Images. 383
Sending Links to Snapshots or Videos. 386
Viewing, Downloading, Deleting Locally-Saved Snapshots. 387
Changing Storage Settings. 388
SmartLock. 391
Door Status and Control. 394
Card Readers. 396

Using SNMP **398**

Enabling and Configuring SNMP. 398
SNMPv3 Notifications. 399
SNMPv2c Notifications. 401
Downloading SNMP MIB. 401
SNMP Gets and Sets. 402
The MIB File. 402
SNMP Sets and Thresholds. 403
Configuring NTP Server Settings. 403
Retrieving Energy Usage. 404

Using the Command Line Interface **405**

Logging in to CLI. 405
With HyperTerminal. 405
With SSH or Telnet. 406
Different CLI Modes and Prompts. 407
Closing a Local Connection. 407
Logging out of CLI. 407
Tips for Using the CLI. 408
The ? Command for Showing Available Commands. 408
Querying Available Parameters for a Command. 408
Retrieving Previous Commands. 409
Automatically Completing a Command. 409
Multi-Command Syntax. 410
Showing Information. 411
Actuator Information. 412
Asset Strip Settings. 412
Authentication Settings. 413
Blade Slot. 414
Command History. 415
Clearing Information. 415
Date and Time Settings. 416
Default Measurement Units. 416
Device Configuration. 416
Environmental Sensor Threshold Information. 417
Event Log. 418
Existing Roles. 419
Existing User Profiles. 419
Environmental Sensor Information. 420
Environmental Sensor Default Thresholds. 421
Front Panel Permissions. 422
Inlet Information. 423
Inlet Sensor Threshold Information. 423

Inlet Pole Sensor Threshold Information. 425
Linking. 427
Load Shedding Settings. 427
Network Configuration. 427
Network Connections Diagnostic Log. 431
Outlet Group Information. 431
Outlet Information. 432
Overcurrent Protector Information. 433
Outlet Pole Sensor Threshold Information. 434
Outlet Group Threshold Information. 435
Outlet Sensor Threshold Information. 435
Overcurrent Protector Sensor Threshold Information. 436
Peripheral Devices Settings. 437
Environmental Sensor Package Information. 437
Rack Unit Settings of an Asset Strip. 438
Reliability Data. 438
Reliability Error Log. 438
Reliability Hardware Failures. 439
Security Settings. 439
Server Reachability Information. 439
Configuring the Device and Network. 440
Actuator Configuration Commands. 441
Actuator Control Operations. 442
Authentication Commands. 443
Configuring Environmental Sensors' Default Thresholds. 457
Device Configuration Commands. 459
Environmental Sensor Configuration Commands. 463
Inlet Configuration Commands. 466
Load Shedding Configuration Commands. 468
Network Configuration Commands. 469
Outlet Configuration Commands. 498
Outlet Group Configuration Commands. 499
Overcurrent Protector Configuration Commands. 502
Peripheral Devices Configuration Commands. 502
Power Control Operations. 504
Resetting Energy Readings. 507
Resetting to Factory Defaults. 509
Resetting the PX4. 510
Restarting the PX4. 510
Role Configuration Commands. 510
Security Configuration Commands. 515
Serial Port Configuration Commands. 534

Server Reachability Configuration Commands. 535
Sensor Threshold Configuration Commands. 538
Time Configuration Commands. 552
User Configuration Commands. 555
Unblocking a User. 564
Network Troubleshooting in Diagnostic Mode. 565
Querying DNS Servers. 565
Showing Network Connections. 565
Testing the Network Connectivity. 566
Tracing the Route. 566
Example - Ping Command. 567
Example: Ping Monitoring and SNMP Notifications. 567

Appendices **568**

Specifications. 569
PX4-Series Specifications. 569
Equipment Setup Worksheet Sample. 570
Outlets detail. 571
Special Configuration and Upgrade Methods. 573
Configuration or Firmware Upgrade with a USB Drive. 573
Bulk Configuration or Firmware Upgrade via DHCP (TFTP/HTTPS). 585
Raw Configuration Upload and Download. 602
Bulk Configuration, Firmware Upgrade, or Backup/Restore via SCP. 607
Cascading Solutions for Xerus. 616
Cascading Solution Overview. 616
Cascading Procedure Overview. 621
Cascading Modes Overview. 621
Setting the Cascading Mode. 623
Device-Cascading Methods. 626
Adding, Removing or Swapping Cascaded Devices. 635
Accessing Cascaded Devices. 637
Identifying Cascaded Devices. 641
Firmware Upgrade for Cascading Chains. 650
Cascade Troubleshooting. 651
Resetting to Factory Defaults. 654
Factory Default Settings. 654
Factory Default Login. 655
Using the Front Panel Display. 655
Using the CLI Command. 656
iX9 Controller Reset Button. 656
Models with Residual Current Monitoring. 657

RCM Current Sensor. 657
RCM State Sensor. 657
Compliance with IEC 62020. 658
RCM Self-Test. 659
Web Interface Operations for RCM. 660
Front Panel Operations for RCM. 665
RCM SNMP Operations. 668
CLI Operations for RCM. 668
Remote Authentication Examples. 670
LDAP Configuration Illustration. 670
RADIUS Configuration Illustration. 675
Cisco ISE Xerus TACACS+ Authentication. 689
Updating the LDAP Schema. 696
Returning User Group Information. 696
Setting the Registry to Permit Write Operations to the Schema. 696
Creating a New Attribute. 698
Adding Attributes to the Class. 699
Updating the Schema Cache. 700
Editing rciusergroup Attributes for User Members. 700
Additional Xerus Information - Assorted Products. 702
Reserving IP Addresses in DHCP Servers. 702
Sensor Threshold Settings. 705
Default Voltage and Current Thresholds. 711
Altitude Correction Factors. 712
Unbalanced Current Calculation. 713
Ways to Probe Existing User Profiles. 714
Role of a DNS Server. 714
Installing the USB-to-Serial Driver (Optional). 714
Device-Specific Settings. 715
TLS Certificate Chain. 716
Xerus Product Integration. 722
Connecting a PDU to a Dominion KVM or Serial Device. 722
Power IQ Configuration. 724
Connecting a Modbus RTU Device or Bus. 724
dcTrack. 725
Third Party Licenses. 727
Licenses - Angular. 727
Licenses - Bind9. 736
Licenses - Clish. 742
Licenses - Dropbear. 747
Licenses - FreeType. 749
Licenses - IW. 751

Licenses - JSON-C. 751
Licenses - LIBTIRPC. 752
Licenses - LIBXML2. 752
Licenses - Mbus. 752
Licenses - Net-SNMP. 753
Licenses - Open LDAP. 758
Licenses - OpenSSL. 760
Licenses - Wireless-RegDB. 761
Licenses - WPA Supplicant and Hostapd. 761

Index **763**

Copyright Notice

This document contains proprietary information that is protected by copyright. All rights reserved. No part of this document may be photocopied, reproduced, or translated into another language without express prior written consent of Legrand.

© Copyright 2025 Legrand. All third-party software and hardware mentioned in this document are registered trademarks or trademarks of and are the property of their respective holders.

FreeType Project Copyright Notice

Portions of this software are copyright © 2015 The FreeType Project (www.freetype.org). All rights reserved.

FCC Information

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 in a commercial installation. This equipment generates, uses, and can radiate radio frequency energy and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. Operation of this equipment in a residential environment may cause harmful interference.

VCCI Information (Japan)

この装置は，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。 VCCI－A

Legrand is not responsible for damage to this product resulting from accident, disaster, misuse, abuse, modification of the product, or other events outside of Legrand's reasonable control or not arising under normal operating conditions.

If a power cable is included with this product, it must be used exclusively for this product.

c UL us
LISTED
1F61
I.T.E.

Introduction to Xerus Technology Platform

The Xerus Technology Platform combines hardware and software technologies embedded in our power solutions. It drives data center efficiency by delivering security, high compute power, advanced alerting, and complete visibility into your power chain. With Xerus cyber-resilient intelligence, your team receives actionable data to aid in decisions that help safeguard assets and maximize your data center continuity and performance.

In This Chapter

Safety Instructions. 13
Safety Warnings. 14
Safety Warnings. 16
Package Contents. 19
Before You Begin. 20
APIPA and Link-Local Addressing. 21

Safety Instructions

1. Installation of this product should only be performed by a person who has knowledge and experience with electric power.
2. Make sure the line cord is disconnected from power before physically mounting or moving the location of this product.
3. This product is designed to be used within an electronic equipment rack. The metal case of this product is electrically bonded to the line cord ground wire. A threaded grounding point on the case may be used as an additional means of protectively grounding this product and the rack.
4. Examine the branch circuit receptacle that will supply electric power to this product. Make sure the receptacle's power lines, neutral and protective earth ground pins are wired correctly and are the correct voltage and phase. Make sure the branch circuit receptacle is protected by a suitably rated fuse or circuit breaker.
5. If the product is a model that contains receptacles that can be switched on/off, electric power may still be present at a receptacle even when it is switched off.
6. The outlet (socket) shall be installed near the equipment and shall be easily accessible.

For detailed information on any PDU's overcurrent protectors' design, refer to that model's product specification.

Safety Warnings

WARNING! Before installing or operating this product, read and understand all sections in this guide.

WARNING! Connect this product to an AC power source with a voltage that is within the range specified on the product's nameplate. Operating this product outside the nameplate voltage range may result in electric shock, fire, personal injury and death.

WARNING! Connect this product to an AC power source that is current limited by a suitably rated fuse or circuit breaker in accordance with national and local electrical codes. Operating this product without proper current limiting may result in electric shock, fire, personal injury and death.

WARNING! Connect this product to a protective earth ground. Never use a "ground lift adapter" between the product's plug and the wall receptacle. Failure to connect to a protective earth ground may result in electric shock, fire, personal injury and death.

WARNING! This product contains no user serviceable parts. Do not open, alter or disassemble this product. All servicing must be performed by qualified personnel. Disconnect power before servicing this product. Failure to comply with this warning may result in electric shock, personal injury and death.

WARNING! Use this product in a dry location. Failure to use this product in a dry location may result in electric shock, personal injury and death.

WARNING! Do not rely on this product's receptacle lamps, receptacle relay switches or any other receptacle power on/off indicator to determine whether power is being supplied to a receptacle. Unplug a device connected to this product before performing repair, maintenance or service on the device. Failure to unplug a device before servicing it may result in electric shock, fire, personal injury and death.

WARNING! Only use this product to power information technology equipment that has a UL/IEC 62368-1 or equivalent rating. Attempting to power non-rated devices may result in electric shock, fire, personal injury and death.

WARNING! Do not use a product containing outlet relays to power large inductive loads such as motors or compressors. Attempting to power a large inductive load may result in damage to the relay.

WARNING! Do not use this product to power critical patient care equipment, fire or smoke alarm systems. Use of this product to power such equipment may result in personal injury and death.

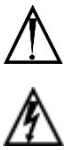
WARNING! If this product is a model that requires the assembly of the line cord or plug, the assembly must be performed by a licensed electrician, and the line cord or plugs used must be rated based on the product's nameplate ratings, as well as national and local electrical codes. Assembly by unlicensed electricians or failure to use suitably rated line cords or plugs may result in electric shock, fire, personal injury or death.

WARNING! This product contains a chemical known to the State of California to cause cancer, birth defects, or other reproductive harm.

Safety Warnings

	WARNING: ELECTRIC SHOCK HAZARD. To reduce the risk of electric shock, disconnect all power cords at the safety disconnect to completely remove power.	AVERTISSEMENT : RISQUE D'ÉLECTROCUTION. Afin de réduire le risque de choc électrique, débranchez tous les cordons d'alimentation sur le dispositif de sûreté afin de couper complètement le courant.	WARNUNG: STROMSCHLAGGEFAHR! Um Stromschläge zu vermeiden, trennen Sie alle Netzkabel vom Stromnetz, um das System stromlos zu machen.
	WARNING: ELECTRIC SHOCK HAZARD. The mains inlet and interconnecting cable plug are not rated for current interruption or disconnection under load. Always disconnect the power supply cord before servicing to avoid electrical shock.	AVERTISSEMENT : RISQUE D'ÉLECTROCUTION. La fiche secteur et la fiche du câble de raccordement ne sont pas prévues pour sectionner ou interrompre le courant lorsque le produit est sous tension. Débranchez toujours le cordon d'alimentation avant de réaliser toute opération d'entretien afin d'éviter une électrocution.	WARNUNG: STROMSCHLAGGEFAHR! Die Stromeingangsbuchse und der Verbindungsstecker sind nicht für eine Stromunterbrechung beziehungsweise eine Netztrennung unter Last geeignet. Trennen Sie vor der Durchführung von Reparatur- und Wartungsarbeiten stets das Netzkabel vom Stromnetz, um Stromschläge zu vermeiden.
	Installation of this product should only be performed by a person who has knowledge and experience with electric power.	L'installation de ce produit ne doit être réalisée que par une personne qui possède des compétences et de l'expérience dans le domaine de l'électricité.	Dieses Produkt darf nur von Personen aufgestellt und installiert werden, die ausreichende Kenntnisse und Erfahrung mit elektrischem Strom haben.
	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.
	WARNING: Only use this product to power information technology equipment that has a UL/ IEC 62368-1 or equivalent rating. Attempting to power non-rated devices may result in electric shock, fire, personal injury, and death.	AVERTISSEMENT : n'utilisez ce produit que pour alimenter des appareils informatiques conformes à la norme UL/CEI 62368-1 ou une norme équivalente. En essayant d'alimenter des appareils non conformes à cette norme, vous vous exposez à des risques d'électrocution et de blessures corporelles pouvant être mortelles.	WARNUNG: Sie dürfen dieses Produkt nur zur Stromversorgung von Geräten benutzen, die gemäß UL/IEC 62368-1 oder einem äquivalenten Prüfsiegel zertifiziert sind. Wenn Sie nicht zertifizierte Geräte anschließen, können Stromschläge, Verletzungen oder Tod die Folge sein.

	WARNING: Connect this product to an AC power source that is current limited by a suitably rated fuse or circuit breaker in accordance with national and local electrical codes. Operating this product without proper current limiting may result in electric shock, fire, personal injury, and death.	AVERTISSEMENT : branchez ce produit sur une source d'alimentation secteur dont le courant est limité par un fusible ou un disjoncteur dont le courant d'emploi assigné est adapté conformément aux normes électriques locales et nationales. L'utilisation de ce produit sans dispositif de limitation du courant peut provoquer une électrocution, un incendie ou des blessures corporelles pouvant entraîner la mort.	WARNUNG: Das Gerät darf nur an einen elektrischen Stromkreis angeschlossen werden, der mit einer Schmelzsicherung oder einem Sicherungsautomaten gemäß der geltenden elektrotechnischen Sicherheitsbestimmungen ausgestattet ist. Wenn Sie das Produkt an einem nicht abgesicherten Stromkreis betreiben, besteht die Gefahr von Stromschlägen, Brand und Verletzungen sowie Lebensgefahr.
	WARNING: Connect this product to an AC power source whose voltage is within the range specified on the product's nameplate. Operating this product outside the nameplate voltage range may result in electric shock, fire, personal injury, and death.	AVERTISSEMENT : branchez ce produit sur une source d'alimentation secteur dont la tension est située dans la plage indiquée sur la plaque signalétique du produit. L'utilisation de ce produit en dehors de la plage de tension indiquée sur la plaque signalétique peut provoquer une électrocution, un incendie ou des blessures corporelles pouvant entraîner la mort.	WARNUNG: Schließen Sie das Produkt nur an eine Wechselstromsteckdose an, die eine Spannung gemäß der Angaben auf dem Typenschild des Gerätes liefert. Wenn Sie das Produkt außerhalb des auf dem Typenschild angegebenen Spannungsbereichs betreiben, besteht die Gefahr von Stromschlägen, Brand und Verletzungen sowie Lebensgefahr.
	WARNING: Always disconnect the power supply cord before servicing to avoid electrical shock.	ATTENTION! Toujours débrancher le cordon d'alimentation avant de l'ouverture pour éviter un choc électrique.	ACHTUNG! Trennen Sie das Netzkabel vom Stromnetz, bevor Sie Wartungsarbeiten durchführen, um Stromschläge zu vermeiden.
	WARNING: Connect this product to a protective earth ground. Never use a "ground lift adapter" between the product's plug and the receptacle. Failure to connect to a protective earth ground may result in electric shock, fire, personal injury, and death.	AVERTISSEMENT : veuillez raccorder ce produit à la terre. N'utilisez jamais une barrette de coupure de terre entre la fiche du produit et la prise de courant. Si vous omettez de relier le produit à la terre, vous vous exposez à un risque d'électrocution, d'incendie et de blessures corporelles pouvant entraîner la mort.	WARNUNG: Dieses Gerät darf nur an eine Steckdose mit Erdleiter angeschlossen werden. Verwenden Sie keine Adapterstecker ohne Erdleiter, wenn Sie das Produkt mit dem Stromnetz verbinden. Wenn Sie das Gerät nicht ordnungsgemäß mit einer Steckdose mit Erdleiter verbinden, besteht die Gefahr von Stromschlägen, Brand und Verletzungen sowie Lebensgefahr.
	WARNING: Use this product in a dry location. Failure to use this product in a dry location may result in electric shock, personal injury, and death.	AVERTISSEMENT : veuillez utiliser ce produit dans un endroit sec. La non-prise en compte de cet avertissement peut entraîner un risque d'électrocution et de blessures corporelles pouvant être mortelles.	WARNUNG: Dieses Produkt darf nur an trockenen Standorten betrieben werden. Anderenfalls können Stromschläge, Verletzungen oder Tod die Folge sein.

	WARNING: With the exception of the controller module, this product contains no user serviceable parts. Do not open, alter, or disassemble this product. All servicing must be performed by qualified personnel. Disconnect power before servicing this product. Failure to comply with this warning may result in electric shock, personal injury, and death.	AVERTISSEMENT : à l'exception du module du contrôleur, le produit ne comprend aucune pièce réparable par l'utilisateur. Évitez d'ouvrir, de modifier ou de désassembler le produit. Toutes les opérations d'entretien doivent être effectuées par des personnes qualifiées. Débranchez le courant avant de procéder à l'entretien de ce produit. La non-prise en compte de cet avertissement peut entraîner un risque d'électrocution et de blessures corporelles pouvant être mortelles.	WARNUNG: Mit Ausnahme des Steuermoduls enthält dieses Produkt keine durch den Benutzer zu wartenden Bauteile. Versuchen Sie nicht, das Produkt zu öffnen, umzubauen oder auseinander zu bauen. Wartungsarbeiten dürfen nur durch qualifizierte Techniker durchgeführt werden. Trennen Sie das Gerät vor der Durchführung von Wartungsarbeiten vom Stromnetz. Anderenfalls können Stromschläge, Verletzungen oder Tod die Folge sein.
	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. Bei Verwendung eines Verlängerungskabels darf die zulässige Gesamtlänge ebenfalls nicht überschritten werden. Der Stecker dient zur Trennung vom Netz und muss einfach erreichbar sein.
	Products rated for 240/415VAC may be fitted with a plug that is rated for a higher voltage. Caution must be taken to assure that the rating of the unit and the supply voltage match.	Les produits prévus pour 240/415VAC peut être équipé d'un bouchon qui est conçu pour une tension plus élevée. Des précautions doivent être prises pour assurer que la cote de l'unité et la tension d'alimentation correspond.	Produkte, die für 240/415V Wechselstrom zugelassen sind, können mit einem Stecker, der für eine höhere Spannung zugelassen ist, ausgestattet sein. Vorsicht ist geboten, um sicherzustellen, dass die erlaubten Betriebswerte des Gerätes und der Versorgungsspannung zueinander passen.
	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" Geräte sind zur vertikalen Installation vorgesehen.
	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 bei der Installation dieses Produkts keine Belüftungslöcher blockiert werden. Stellen Sie zu jeder Zeit eine maximale Luftzirkulation sicher.

	This product is designed to be used within an electronic equipment rack. The metal case of this product is electrically bonded to the line cord ground wire. A threaded grounding point on the case may be used as an additional means of protectively grounding this product and the rack.	Ce produit est conçu pour être utilisé dans une baie pour appareils électroniques. Le boîtier métallique de ce produit est raccordé électriquement au fil de terre du cordon d'alimentation. Il est possible d'utiliser en plus un point de mise à la terre fileté placé sur le boîtier pour relier ce produit et la baie à la terre.	Dieses Produkt muss in einem Einbauschrank für elektronische Geräte installiert werden. Das Metallgehäuse dieses Produkts ist elektrisch mit dem Erdleiter des Netzkabels verbunden. Als zusätzliche Sicherheitsmaßnahme empfehlen wir die weitere Erdung über einen Erdungsanschluss am Gehäuse des Produktes und des Einbauschranks.
	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 unfertigem Netzkabel: Der Eingangsstecker darf nur von qualifiziertem Wartungspersonal installiert werden. Der Eingangsstecker muss für alle geltenden und verbindlichen Normen und Vorschriften zugelassen sein.
	WARNING: CHINA NOTIFICATION: For use at altitude 2,000 meters or lower.	AVERTISSEMENT : AVIS CONCERNANT LA CHINE : conçu pour être utilisé à une altitude maximale de 2 000 mètres.	WARNUNG: EINSATZLAND CHINA: nur für den Betrieb auf Höhen bis maximal 2000 m.
	The manufacturer is not responsible for damage to this product resulting from accident, disaster, misuse, abuse, modification of the product, or other events outside of the manufacturer's reasonable control or not arising under normal operating conditions.	Le fabricant décline toute responsabilité concernant les dommages subis par ce produit qui résulteraient d'un accident, d'une catastrophe naturelle, d'une mauvaise utilisation, d'une utilisation abusive, de la modification du produit ou d'autres événements indépendants de la volonté raisonnable du fabricant ou qui ne se seraient pas produits dans des conditions normales d'utilisation.	Der Hersteller haftet nicht für Produktschäden, die durch Unfälle, Naturkatastrophen, falsche Bedienung, mutwillige Beschädigung, Änderungen am Produkt oder andere Umstände außerhalb des Verantwortungsbereichs des Herstellers entstanden sind beziehungsweise durch Betrieb außerhalb der normalen Arbeitsbedingungen verursacht wurden.

Package Contents

The following sub-topics describe the equipment and other material included in a typical product package.

Zero U Products

- One PX4
- Screws, brackets and/or buttons for Zero U

1U Products

- One PX4
- 1U bracket pack and screws
- Cable retention clips for the inlet (for some models only)

2U Products

- One PX4
- 2U bracket pack and screws
- Cable retention clips for the inlet (for some models only)

Before You Begin

Before beginning the installation, perform the following activities:

- Unpack the product and components
- Prepare the installation site
- Check the branch circuit rating
- Fill out the equipment setup worksheet

Unpacking the Product and Components

1. Remove the product and other equipment from the box in which they were shipped.
2. Compare the serial number of the equipment with the number on the packing slip located on the outside of the box and make sure they match.
3. Inspect the equipment carefully. If any of the equipment is damaged or missing, contact Technical Support for assistance.
4. Verify that all circuit breakers on the product are set to ON. If not, turn them ON.

Or make sure that all fuses are inserted and seated properly. If there are any fuse covers, ensure that they are closed.

Note: Not all models have overcurrent protectors.

Preparing the Installation Site

1. Make sure the installation area is clean and free of extreme temperatures and humidity.

Note: Check the product specification sheet for the maximum operating temperature for your model.

---

2. Allow sufficient space around the product for cabling and outlet connections.
3. Review Safety Instructions listed in this guide.

Checking the Branch Circuit Rating

The rating of the branch circuit supplying power to the product shall be in accordance with national and local electrical codes.

Filling Out the Equipment Setup Worksheet

An Equipment Setup Worksheet is provided in this guide. Use this worksheet to record the model, serial number, and use of each IT device connected.

As you add and remove devices, keep the worksheet up-to-date.

APIPA and Link-Local Addressing

PX4 supports Automatic Private Internet Protocol Addressing (APIPA).

With APIPA, your PX4 automatically configures a link-local IP address and a link-local host name when it cannot obtain a valid IP address from any DHCP server in the TCP/IP network. Only IT devices connected to *the same subnet* can access the PX4 using the link-local address/host name. Those in a different subnet cannot access it.

Exception: Port Forwarding mode does not support APIPA.

Once the PX4 can get a DHCP-assigned IP address, it stops using APIPA and the link-local address is replaced by the DHCP-assigned address.

► *Scenarios where APIPA applies:*

- DHCP is enabled on the PX4, but no IP address is assigned to the PX4. This may be caused by the absence or malfunction of DHCP servers in the network. For example, connecting the PX4 to a computer using a network cable.
- The PX4 previously obtained an IP address from the DHCP server, but the lease of this IP address has expired, and the lease cannot be renewed, or no new IP address is available.

► *Link-local addressing:*

- *IPv4 address*:

  Factory default is to enable IPv4 only. The link-local IPv4 address is *169.254.x.x/16*, which ranges between 169.254.1.0 and 169.254.254.255.
- *IPv6 address*:

  A link-local IPv6 address is available only after IPv6 is enabled on the PX4. See Configuring Network Settings.
- *Host name* - pdu.local:

  You can type *https://pdu.local* to access the PX4 instead of typing the link-local IP address.

► *Retrieval of the link-local address:*

- See Device Info.

Rackmounts

In This Chapter

Circuit Breaker Orientation Limitation. 22
Rackmount Safety Guidelines. 22
0U Button Mount. 22

Circuit Breaker Orientation Limitation

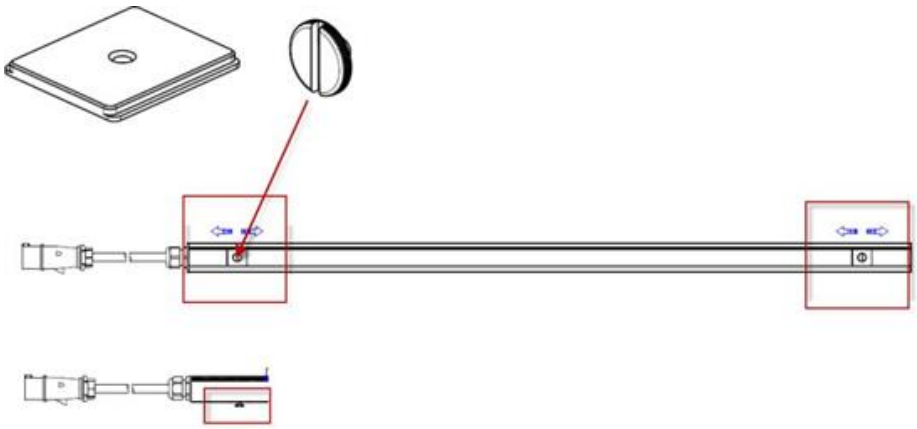
Usually a PDU can be mounted in any orientation. However, when mounting a PDU with circuit breakers, you must follow these rules:

- Circuit breakers CANNOT face down. For example, do not horizontally mount a Zero U PDU with circuit breakers facing up or down.

Rackmount Safety Guidelines

- Operating temperature in a closed rack environment may be greater than room temperature. Do not exceed the rated maximum ambient temperature of the Power Distribution Units. See Specifications (on page 569) in the User Guide.
- Ensure sufficient airflow through the rack environment.
- Mount equipment in the rack carefully to avoid uneven mechanical loading.
- Connect equipment to the supply circuit carefully to avoid overloading circuits.
- Ground all equipment properly, especially supply connections, to the branch circuit.

0U Button Mount



Part Numbers: • G4-M4-RACK: button (2) • G4-M4-RACK: bracket (2)	• Slide flat brackets onto rear of 0U model and align over holes at each end. • Press button into bracket hole and turn with finger. • Mount by positioning the PDU at the rack, then pressing the buttons through the holes in the cabinet and letting the PDU drop down slightly.

Initial Installation and Configuration

This chapter explains how to install your device and configure network connectivity.

In This Chapter

Connecting the PDU to a Power Source. 24
Connecting to Your Network. 24
Configuring the PX4. 26
Bulk Configuration Methods. 33
Cascading for Shared Ethernet Connectivity. 34
Power-Sharing Restrictions and Connection. 36

Connecting the PDU to a Power Source

1. Verify that all circuit breakers on the PDU are set to ON. If not, turn them ON.

Or make sure that all fuses are inserted and seated properly. If there are any fuse covers, ensure that they are closed.

Note: Not all models have overcurrent protectors.

---

2. Connect each PDU to an appropriately rated branch circuit. Refer to the label or nameplate for appropriate input ratings or range of ratings.

Connecting to Your Network

To remotely administer the PX4, you must connect it to your local area network (LAN). Wired or wireless networks are supported.

Ethernet port is enabled by default. Port layouts and number of Ethernet ports vary by model.

► *To make a wired connection:*

1. Connect a standard network patch cable to one or both Ethernet ports on the PDU.
   - If one Ethernet port is higher speed, use the higher speed port for network connection.
2. Connect the other end of the cable to your LAN.

Sample iX9 controller. Port locations may vary by model.

Warning: Accidentally plugging an RS-232 RJ-45 connector into the Ethernet port can cause permanent damage(s) to the Ethernet hardware.

► *To make a wireless connection:*

Do one of the following:

- Plug a supported USB wireless LAN adapter into the USB-A port on your PDU.
- Connect a USB hub to the USB-A port on the PDU. Then plug the supported USB wireless LAN adapter into the appropriate USB port on the hub.

USB Wireless LAN Adapter - DX2-WIFI-KIT

The Legrand DX2-WIFI-KIT is the supported wireless LAN adapter.

Wi-Fi LAN adapter	Supported 802.11 protocols	Supported Xerus releases	Supported controllers
Legrand DX2-WIFI-KIT	AC/A/B/G/N	Release 4.1.0 and later	iX7 and later

Supported Wireless LAN Configuration

If wireless networking is preferred, ensure that the wireless LAN configuration of your PX4 matches the access point. The following wireless LAN configuration supports the PX4.

- Supported 802.11 protocols: AC/A/B/G/N
- Protocol: WPA2 (RSN)
- Key management: WPA-PSK, or WPA-EAP with PEAP and MSCHAPv2 authentication
- Encryption: CCMP (AES)

Tips: Supported 802.11 network protocols vary according to the wireless LAN adapter being used.

Dual Ethernet Connection

Models with two Ethernet ports may support different speeds. Note the speed marking on your Ethernet port. Port layouts and labels may vary by model.

- ETH1 or ETH2 marked 10/100/1000: supports up to 1000 Mbps.

Exception: USB-cascading chains have different requirements.

► *Check list when connecting both ports to the networks:*

- Both Ethernet interfaces are connected to different subnets.
- Ethernet interfaces are enabled. (default setting).
- Ethernet interfaces are configured with proper IPv4 and/or IPv6 settings.

It is NOT required that the two Ethernet interfaces share similar network settings.

For example:

- Enable IPv4 settings on one interface and IPv6 settings on the other.
- Apply static IP to one interface and DHCP IP to the other.
- Ensure the cascading mode is disabled (default settings).
- Navigate to Device Settings > Network to verify.

Configuring the PX4

You can initially configure via one of the following:

- A TCP/IP network that supports DHCP
- A mobile device with PDView installed
- A computer physically connected to the PDU

Basic configuration process overviews:

► *Configuration via a DHCP-enabled network:*

1. Connect the PX4 to a DHCP IPv4 network.
2. Use the front panel LCD display to retrieve the IP address.
3. Launch a web browser to configure the PX4.

► *Configuration via a connected mobile device:*

1. Download the PDView app to your mobile device.
2. Connect the mobile device to PX4 via USB.
3. Launch PDView to configure the PX4.

► *Configuration via a connected computer:*

1. Connect the PX4 to a computer.
2. Use the connected computer to configure via the command line or web interface.
   - Command line interface: See Initial Network Configuration via CLI.
   - Web interface: Launch a web browser on the computer, and enter the link-local IP address or *pdu.local*.

Connecting a Mobile Device

Raritan's PDView is a free app that turns your iOS or Android mobile device into a local display for PX4. It is especially helpful when your PX4 is not connected to the network but you need to check status, retrieve information, or change settings.

► *Requirements for using PDView:*

- If using an Android device, it must support USB "On-The-Go" (OTG).
- An appropriate USB cable is required.

► *Step A: Download and install PDView*

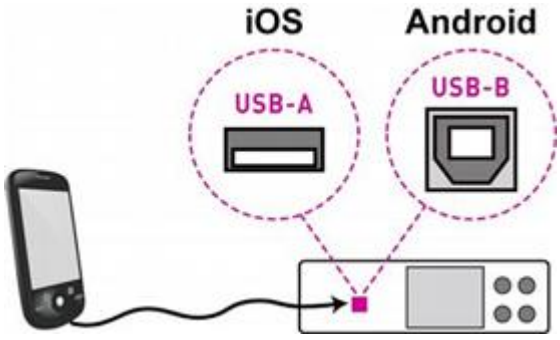
1. Visit either Apple App or Google Play Store.
   - *https://itunes.apple.com/app/raritan-pdview/id780382738*

   - *https://play.google.com/store/apps/details?id=com.raritan.android.pdview*

2. Install PDView.

► *Step B: Connect the mobile device to PX4*

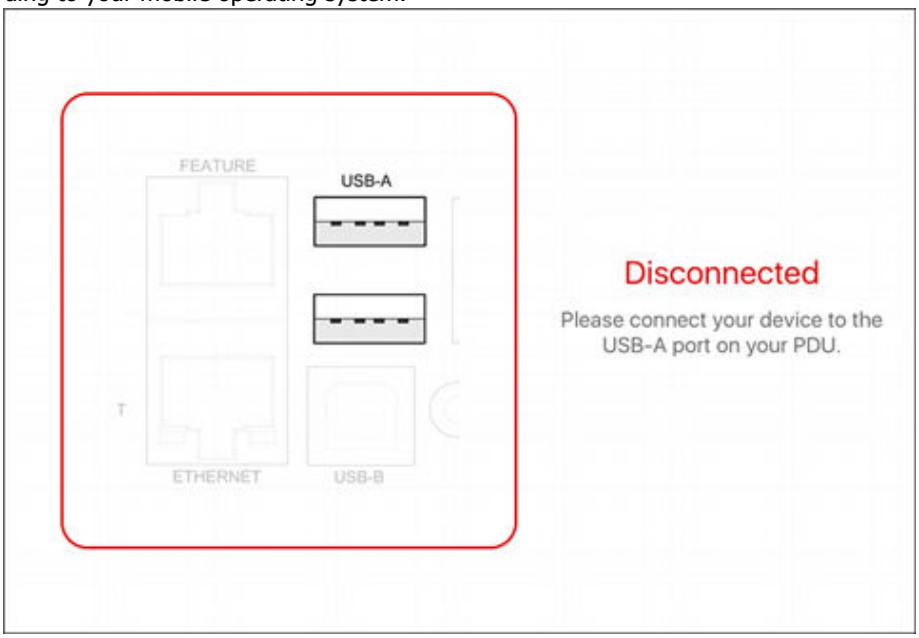
1. Get an appropriate USB cable for your mobile device.
   - *iOS*: Use the regular USB cable shipped with your iOS mobile device.
   - *Android*: Use a USB OTG adapter cable.
2. Connect the mobile device to the appropriate USB port on the PX4.
   - *iOS*: USB-A port.
   - *Android*: USB-B port



► *Step C: Launch PDView*

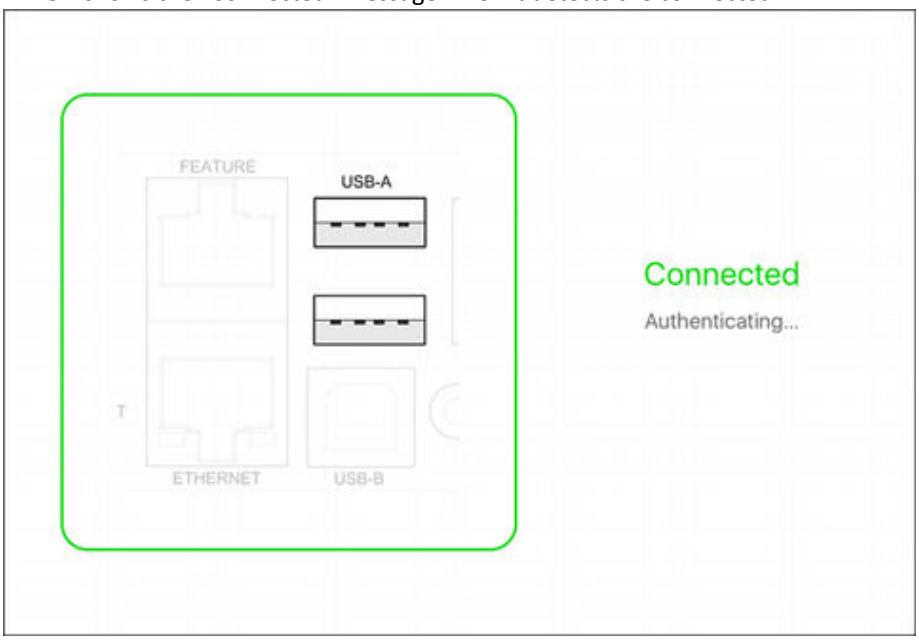
1. Launch the PDView app from your mobile device. The following illustrates iPad's PDView screens.
   a. The "Disconnected" message displays first when PDView has not detected the PX4 yet.

A diagram in PDView indicates the appropriate USB port your mobile device should connect according to your mobile operating system.



Note: PDView also shows the 'Disconnected' status during the firmware upgrade. If so, wait until the firmware upgrade finishes.

b. The PDView shows the "Connected" message when it detects the connected PX4.



2. If the factory-default login credentials remain unchanged, or if PDView has been configured with accurate login credentials, PDView will automatically log in to the web interface.
   - If PDView can not log in automatically, the login screen will display and you must enter the appropriate user credentials.
   - Upon first-time login, the web interface will prompt you to change the password.

Tip: You can store the updated "admin" or other user credentials in PDView to ensure automatic login functions properly upon detection of the PX4.

Saving User Credentials for PDView's Automatic Login

When PDView detects PX4 for the first time, it automatically attempts to log in with the factory-default user credentials. If you have modified the factory-default user credentials, PDView's automatic login will fail, and the login screen will display for you to manually enter user credentials.

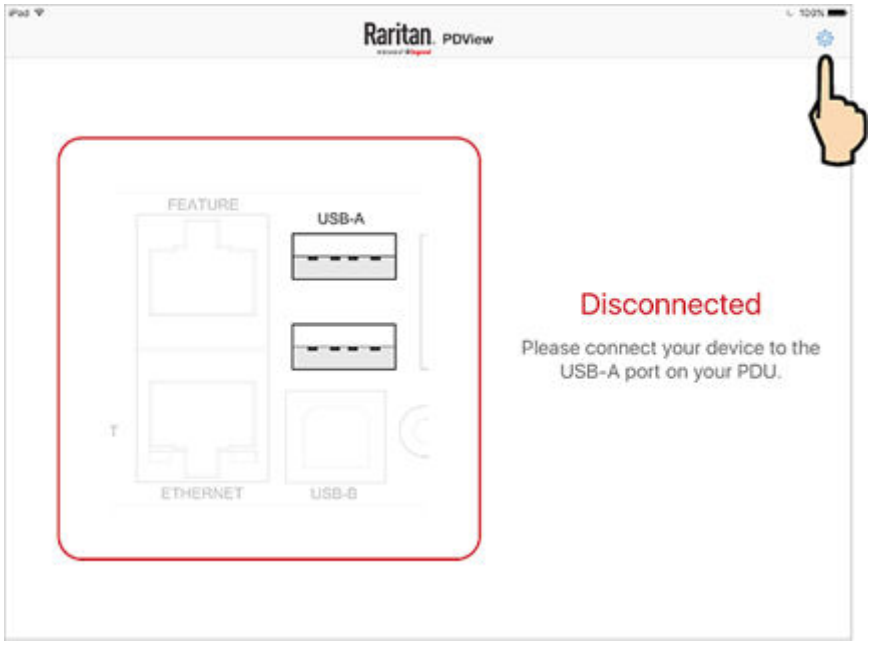
To make automatic login work again, you can save the modified admin credentials or any custom user credentials in PDView. A maximum of 5 user credentials can be saved, and PDView will try these credentials one by one until the login succeeds.

The following procedure illustrates iPad only, but the procedure applies to any iOS or Android mobile device.

► *To save user credentials in PDView:*

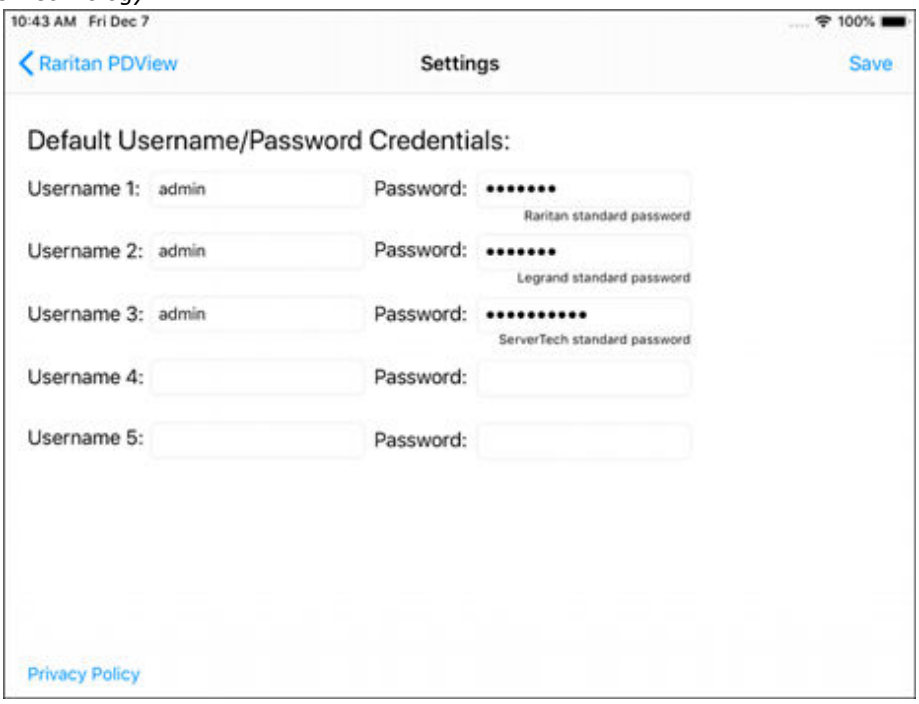
1. Make sure your mobile device is NOT connected to the PX4 so that PDView does NOT perform the automatic login feature after it is launched.
2. Launch PDView on your mobile device.

3. Tap the top-right Settings icon (iOS) or (Android).



4. The user credentials setup page opens.
   - Per default, three administrator user credentials are pre-configured for three Legrand brands:

- *Raritan*
- *Legrand*
- *Server Technology*



5. Modify existing user credentials or type new ones, and tap Save. The pre-configured admin credentials can be removed or overwritten to meet your needs.

Connecting to a Computer

The PX4 can be connected to a computer for configuration via one of the following ports.

- Ethernet ports
- USB-B port

To use the command line interface (CLI) for configuration, establish a USB connection.

To use a web browser for configuration, make a network connection to the computer. The following link-local addressing is available in any network without DHCP available:

- *https://169.254.x.x* Use the front panel display to find the address.
- *https://pdu.local*

Establish one of the following connections to a computer.

► *Direct network connection:*

1. Connect one end of a standard network patch cable to an Ethernet port of the PDU.
2. Connect the other end to a computer's Ethernet port.
3. On the connected computer, launch a web browser to access using either link-local addressing: *pdu.local* or *169.254.x.x*.

► *USB connection:*

1. A USB-to-serial driver is required in Windows®. Install this driver before connecting the USB cable.
2. Connect a USB cable between a computer's USB-A port and the USB-B port of PX4.
3. Perform initial network configuration via CLI.

► *Initial network configuration via CLI sample:*

These sample commands set up the ETH1 interface with static IP address, gateway, and DNS server settings.

```
#config
config:# network bridge enabled false
config:# network ipv4 interface ETH1 enabled true
config:# network ipv4 interface ETH1 configMethod static
config:# network ipv4 interface ETH1 address 192.168.56.80/24
config:# network ipv4 interface ETH1 gateway 192.168.56.128
config:# network dns firstServer 1.1.1.1 secondServer 1.0.0.1
config:# network ethernet Eth1 speed 100Mbps duplexMode full
config:# apply
```

Bulk Configuration Methods

If you have to set up multiple devices, you can use one of the following configuration methods to save time.

► *A bulk configuration file downloaded from PX4:*

- *Requirement*: All devices to configure are of the same model and firmware.
- *Procedure*:
  1. First finish configuring one PX4.
  2. Download the bulk configuration file from it.
  3. Copy this file to all of the other PX4 devices. See: Bulk Configuration (on page 372).

For the remaining methods, see Special Configuration and Upgrade Methods (on page 573).

► *A TFTP server:*

- *Requirement*: DHCP is enabled in your network and a TFTP server is available.
- *Procedure*:
  1. Prepare special configuration files, which must include *fwupdate.cfg.*
  2. Copy them to the root directory of the TFTP server.
  3. Reboot all PX4 devices after connecting them to the network.

► *Curl command:*

- *Requirement*: Two files are required -- one is a configuration file in TXT and the other is a devices list file in CSV. See: config.txt and devices.csv.
- *Procedure*:
  1. Upload both files to all PX4 devices one by one, using the appropriate curl command.

► *SCP or PSCP command:*

- *Requirement*: Two files are required -- one configuration file in TXT and a devices list file in CSV format.
- *Procedure*:
  1. Upload both files to all PX4 devices one by one, using the appropriate SCP or PSCP command.

► *A USB flash drive:*

- *Requirement*: A FAT32- or superfloppy-formatted USB flash drive containing two special configuration files and one device list file is required.
- *Procedure*:
  1. Plug this USB drive into the PX4.
  2. When a happy smiley is shown on the front panel display, press and hold one of the control buttons on the front panel until the display turns blank.

Cascading for Shared Ethernet Connectivity

For full details on network setup, physical setup, and supported configurations for all cascades across products, see the Cascading Solution Guide. The sections documented here are a brief overview. See: Cascading Solutions for Xerus (on page 616).

You can have multiple devices share one Ethernet connection by cascading them using either the USB interface or Ethernet interface

The first one in the cascade is the primary device and all the other devices follow it in the cascade. Only the primary device is physically connected to the LAN -- wired or wireless.

Raritan
A brand of legrand

Each device in the cascade is accessible over the network, with Bridging or Port-Forwarding cascading mode activated on each device.

- Bridging: Each device in the cascading chain is accessed with a different IP address.
- Port Forwarding: Each device in the cascading chain is accessed with the same IP address(es) but with a different port number assigned.

► *Basic cascading restrictions:*

- All devices in the chain must run compatible firmware versions of 3.3.10 or later.
- The cascading mode of all devices in the chain must be the same.
- In the Bridging mode, the primary device can have only one connection to the network. DO NOT connect both Ethernet ports to the network(s) unless your network has the R/STP protocol enabled.

Note: The Port Forwarding mode does NOT have this restriction. In this mode, you can enable two wired and one wireless network connections.

- Do NOT connect cascaded devices other than primary to the LAN or WLAN.
- (WIFI only) You must use Raritan's USB WIFI wireless LAN adapter instead of other WIFI adapters for wireless network connection.

Best Practices for Cascading

► *One Ethernet connection per cabinet is better:*

One Ethernet connection per cabinet is better than one Ethernet connection across cabinets because of these advantages:

- More reliable connectivity.
- Easier to manage or maintain one cabinet when all of the cabling and connections are located in the same cabinet.
- Reduces the cross-cabinet cabling.

► *When to establish a chain comprising 32 devices:*

A chain consisting of 32 devices saves the most Ethernet connections and costs, and it is recommended only when:

- External Ethernet ports are expensive or limited.
- Available IP addresses are limited.

► *Ethernet cascading is recommended for supported devices with Dual Ethernet ports:*

If all the devices in the intended cascade have dual Ethernet ports, cascading them via Ethernet is better than via USB. The Ethernet interface offers the following benefits:

- Longer cabling distance
- Lower latency
- Connection more reliable with RJ-45 connectors

Power-Sharing Restrictions and Connection

Two devices can share power supply to their controllers via a designated port, so that when either controller fails to receive adequate power from its inlet(s), it continues to receive backup power from another device which functions properly and therefore remains accessible to users.

For documentation purposes, the term "power-sharing mode" is used to describe the status when the PDU controller is receiving power from another device.

Before making a power-sharing connection, first read Power-Sharing Configurations and Restrictions (on page 37), and remove unsupported equipment from BOTH PDUs.

After a PDU enters power-sharing mode, some data/operations are no longer available.

► *Unavailable data or operations in power-sharing mode:*

- All outlets lose power, and enter the "disabled" state.
- No outlet switching can be performed.
- All internal sensors become "unavailable", including sensors of inlets, outlets, and OCPs.

  Exception: Only energy data remains available.

- Communications with relay/meter boards are lost. Therefore, firmware upgrade may fail.

► *Available data or operations in power-sharing mode:*

- Change software settings, such as customizing names, modifying network settings, configuring thresholds, and so on.
- Monitor the status of connected environmental sensor packages, or configure/control their settings.
- Operate the front panel display.

► *Events that occur when entering power-sharing mode:*

- The power supply sensor enters the fault state.

Tip: You can set an event rule for sending a notification when this sensor enters the fault state.

- The above event is logged in the internal event log.

► *To check status of power-sharing mode:*

- Check the state of the power supply sensor. For SNMP, the sensor type is i1smpsStatus (46).

Power Sharing Port on iX9 Controllers

Two PDUs with iX9 controllers can be connected at the "PDU LINK" port using a cat5 network cable for power sharing.

See PDU Linking at the Rack (on page 65).

Power-Sharing Configurations and Restrictions

When either PDU enters power-sharing mode, BOTH PDUs support "less" external equipment than usual. It is strongly recommended to remove specific equipment from both PDUs when making a power-sharing connection.

► *Configuration limitations on "both" PDUs:*

- Connect the two PDUs with a standard network patch cable (Cat5e/6) that is up to 2 meters long, using the "PDU LINK" port for power sharing.

- NO USB wireless LAN adapter is connected.

  That is, you have to connect both PDUs to a "wired" network if LAN access is wanted.
- For models that support asset strips: No asset management strips can be connected while power sharing.
- The maximum number of DX2 environmental sensor packages or door handles that can be connected decreases. See Smart Sensor Configurations for Power Sharing (on page 38).
- After either PDU enters the power-sharing mode, you must NOT physically remove or add any environmental sensor packages to either PDU.

Smart Sensor Configurations for Power Sharing

All information and restrictions described in this section apply to BOTH PDUs involved in the power-sharing configuration, unless otherwise specified.

- NO changes to usual support for DX2 sensors in power sharing configurations.

► *Door handle connection restrictions (via DX2-DH2C2):*

- (Restriction only for DX2-DH2C2 manufactured before 2019) DO NOT connect any "SouthCo H3-EM series" door handle(s) because of insufficient power supply in the power-sharing mode.

Note: The latest generation of DX2-DH2C2 does NOT have this restriction and can have SouthCo H3-EM series connected in the power-sharing mode.

- A maximum of 2 door handles connected to a maximum of one DX2-DH2C2 are supported.
- Both of the 2 door handles must be controlled by the same PDU so that you can have "only one" handle opened at a time to avoid critical power consumption. That is, ALL door handles must be connected to only one PDU in the power-sharing connection, NOT both PDUs.

Note: It is strongly suggested to check and make sure the upper limit of "powered cry contact actuators" is set to 1 when making a power-sharing connection.

► *Other sensor restrictions when door handles are present:*

First make sure the connection of door handles complies with the above restrictions.

The following restrictions apply only to the PDU that has all the door handles connected.

- When there are 2 door handles connected to the PDU, up to 10 sensor packages of DX2. Raritan's sensor hubs must NOT be used.
- When there is only 1 handle connected, up to 12 sensor packages of DX2. Sensor hubs must NOT be used.

► *NO physical changes made to the number of connected sensor packages:*

- After either PDU enters the power-sharing mode, you must NOT physically remove or add any environmental sensor packages to BOTH PDUs.

Warning: The inrush current of a newly added sensor package may cause both PDUs to reboot.

Raritan
A brand of legrand

Power Sharing Limitations on Mobile Devices

You can connect to Android devices in Power sharing mode. As USB-A port is not supported during power sharing mode, the iOS devices will not work.

You can use PDView on the connected mobile devices to download diagnostic data without additional restrictions, aside from the existing power sharing limitations.

Linking Units

The Linking feature makes it easy to connect one Primary unit with multiple Link units, so you can keep track of everything in one place. The Primary unit knows all about the location, power status, and environmental details of the Link units. You can manage both the Primary and Link units effortlessly through the GUI, SNMP, or CLI.

To set up linking through the link port:

- Make sure the Link units are reset to factory defaults.
- If the Link unit's password doesn't match, the connection won’t work.
- For linking through other interfaces, you'll need to specify the Link unit's password.

Communication between the Primary and Link units happens over HTTPS, and you'll need HTTPS enabled on the default port (443). For added security, certificates are checked during the setup.

- Certificates: Each Link unit needs either the demo certificate or custom certificates installed. If you're using custom certificates, the CA certificate has to be installed on the Primary unit. To configure certificates, just go to PDU > Link Units and click the "TLS Certificate" button

You can use all network modes, but make sure network and physical configurations are set before starting. Administrator privileges are required for tasks like adding, configuring, or removing units. Once everything is set up, you can monitor and manage each unit remotely using these protocols:

- HTTP(S)
- SNMP
- SSH
- Telnet

Keep in mind that all units in the linked chain need to be the same model and run the same firmware version. If needed, you can upgrade the firmware for each unit individually.

In This Chapter

FAQs. 41
Linking in the Web Interface. 44
Outlet Groups. 62
PDU Linking at the Rack. 65
Displays for Primary and Link Units. 67
Linking in the CLI. 68

FAQs

► *What's the difference between a "primary unit" and a "link unit"?*

Primary and link units are the same model PX4 and are equal to each other, and each has its own IP address. You designate a PX4 as the primary unit by logging into it and then adding a link unit.

- The first unit becomes the primary.
- When the first link unit is added, the primary unit is automatically assigned ID "1", which is reserved to identify a primary unit only, and the ID "1" cannot be edited.
- A connection between the primary and the link unit has now occurred and the chain is formed.

As you continue to add link units to the chain (up to seven link units), you select Link ID "2" through "8" for the Link ID numbers. Note that the Link ID "2-8" is the sequential number of each link unit that you select as you add the unit to the chain. Once selected, the Link ID cannot be edited.

When the chain is established with a single primary unit, and one or more link units, communication occurs with the primary unit through its IP address. The primary unit, in turn, communicates to the other link units in the chain through their individual IP addresses, which optimizes monitoring and management.

► *Which models can be linked?*

Linking is supported on various products, but all devices in the chain should be the same models, running the same firmware version. The main controller must have 128 MiB RAM or more to support this feature. Following table lists the supported controllers and its board revision. See: Device Information (on page 366) of your PX4.

Main Controller	Board Revision
iX7	0x10, 0x15, 0x23, (iX7-G1), 0x1F (iX7-G2), 0x1E (iX7-G3)
iX9	0x1A, 0x1D
iX12	0x25

Note: Only PDUs with iX7/iX7-G2 and later can be a Primary PDU in a Linked configuration. You can link the PDU with a V6 controller but can not set it as a Primary PDU.

► *Which network setup modes are supported?*

For the underlying network, the Linking feature can use the typical network setup modes:

Independent Setup: All units have their own regular IP address. They don't need to be in a physical chain to be logically chained. You communicate only to the primary using its normal IP address. Configure networking of the units, and then add link units using the Web GUI, CLI, or USB.

Bridged Setup: Same as Independent Setup, but the units are physically connected as a chain, either by ethernet or USB. The configuration steps are the same as with Independent Setup.

Port Forwarding Cascade: The units are physically connected as a chain (either by Ethernet or USB). Only the first primary unit is connected to your network with the IP address you assigned. The other units will get automatically-assigned private IP addresses. When a Cascading in Port Forwarding mode configuration is detected, you can automatically convert the cascaded units into Link Units using the GUI in the primary unit, or add link units with the other methods in the Web GUI, CLI, or USB.

See Cascading Solutions for Xerus (on page 616).

- *Can primary units be linked together?*

No. Once a unit is designated as the primary unit in a chain, it cannot be linked to a primary unit in another chain. A primary unit can only be linked to one or more link units in a chain.

- *How many units can be linked?*

Including the primary, a full chain can include a total of eight units. The first unit added is designated as the primary unit with the ID "1". Each unit you then add to the chain is designated as a link unit, beginning with ID "2" and ending with ID "8".

- *What user credentials are used for my Primary and Linked Units?*

When Linking is used, the primary unit's admin password will be synced to the link units.

- *What is re-linking?*

Re-linking is a required function when a link unit no longer recognizes or responds to the primary unit, most likely caused by the link unit being reset to factory defaults. The status of the disassociated link unit will be displayed as "Access Denied". Selecting the link unit when in this status displays the Re-link button that allows reconnection of the link unit in the chain for regaining device control.

Note: Re-linking uses the same Link Unit ID and hostname, but you will need to reauthenticate with your login credentials.

- *What user privileges are required for managing the Linking configuration?*

Administrative privileges are required for both the primary unit and link unit. To add a link, your administrative login account is required, but after that you only log in to the primary to manage the chain, as all link units in the chain are visible in the user interface from the primary unit view.

Raritan
A brand of legrand

► *What happens if the connection is lost between the primary and link units?*

The primary unit's dashboard displays information about unreachable link units in the Link Unit Failures section.

If the network connection is lost, these link unit functions will still work:

1. Front panel display
2. Energy accumulation and outlet states (not applicable to SRC)

and these link unit functions will stop working:

1. Event log entries are lost
2. Event rules, actions and alarms
3. Remote access to the link unit
4. Synchronization of primary settings and time when not using NTP

► *Which system areas of the primary and link units are automatically synchronized?*

The primary unit periodically checks link unit reachability. You can define rules to be alerted when communication with a link unit fails, such as a system alarm. Some link unit settings are automatically synchronized with the primary:

1. Peripheral device settings
2. Front panel privileges and default view
3. USB host port lockdown
4. Time and date settings
5. General data logging settings

► *How are firmware updates handled?*

Uploaded firmware images in the GUI are automatically distributed to all link units at the same time. Starting a firmware update requires the automatic image upload on the link units to be finished first.

Firmware version must match between primary units and link units to function normally. If the primary unit is updated before the link units, for example, you will see a "Firmware version mismatch" message in the Link Units section. When this occurs, link unit data will not display. You will not be able to switch to the mismatched link unit. Upon update of the linked unit to the matching firmware version, normal data displays will resume.

► *Does Linking support mass deployment?*

Yes, mass deployment has been extended to support a setup for the Linking feature (multi-IP or single-IP) via the Mass Deployment Utility, which provides the Excel spreadsheet process used for bulk configuration. For information about using the utility, see Configuration or Firmware Upgrade with a USB Drive.

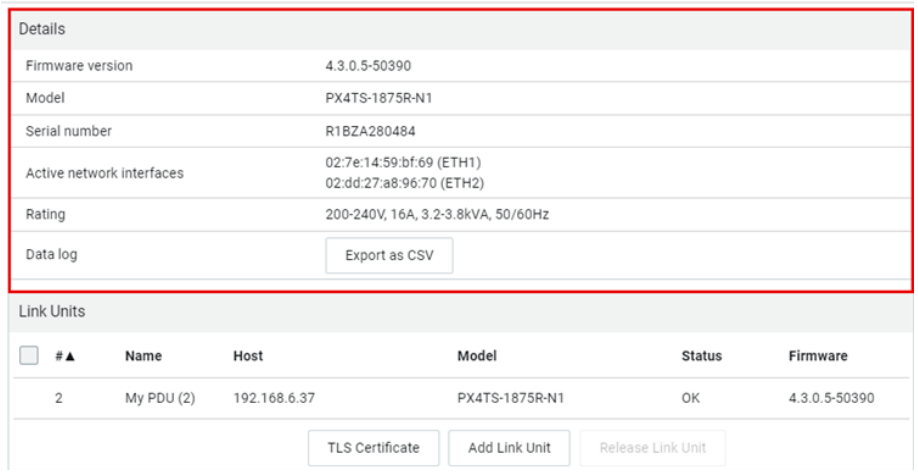
Linking in the Web Interface

The following topics describe how to configure and use Linking in the web interface.

Viewing the Primary Unit

To view and manage Linking, log in to the unit designated as the primary unit, and go to the PDU page.

When you add a link unit, a chain is established between the primary and the new link, and the primary becomes ID "1".



The PDU page displays the following information about the primary PDU:

1. Firmware version
2. Model
3. Serial number
4. MAC address
5. Rating
6. Link to Data Log

The ID of the primary unit is automatically assigned the ID "1", as shown in the example as "My PDU (1)". The ID cannot be edited.

Options for Adding Link Units

To start configuring the Primary Unit with Link Units, your options in the web interface depend on the network and physical configuration of units.

- If you configured units in Independent or Bridging Mode, where they may or may not be physically cascaded, and each one is assigned its own IP address, you can manually add each link unit. You can use this manual function anytime to add link units. See Adding a Link Unit (on page 45).
- If you configured units in a Port-Forwarding Cascade Mode configuration, in which they are physically cascaded and only the first unit is connected to the network, you can automatically link the cascaded units. See Linking Cascaded Units (on page 47)

TLS Certificates for PDU Linking

To enhance security, you can upload a TLS certificate to your primary unit to be verified for communication with the link units. The built-in demo CA certificate is used to verify link units until you upload your own. You will need a CA certificate for the primary unit, and certificates for each link unit that have been signed by the same CA. Before creating the cascade, CA-signed TLS certificates must be installed to designated link units. See Setting Up a TLS Certificate (on page 270).

If you are using the Link Port for setup at the rack, or if you are in Port Forwarding mode, certificates for link-local addresses and/or internal wildcard domain (*.pf-cascade) are required. Note that Link Port is not available on all models.

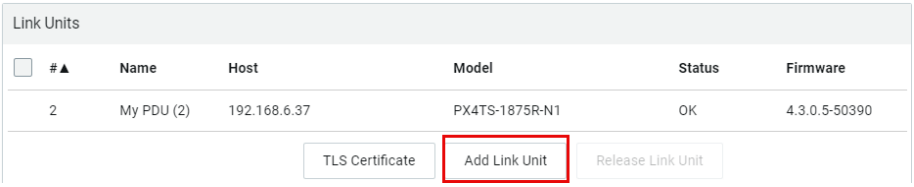
► *To add the CA Certificate to the Primary Unit:*

1. Login to the designated primary unit.
2. On the PDU page, click TLS Certificates.
3. Click Browse, then select the CA certificate file and click OK to upload it.
4. Select the "Allow Expired and Not Yet Valid certificates" checkbox to skip time verification when certificates are validated.
5. Click Save.

Adding a Link Unit

A link unit (up to seven units) can be added to a single primary unit.

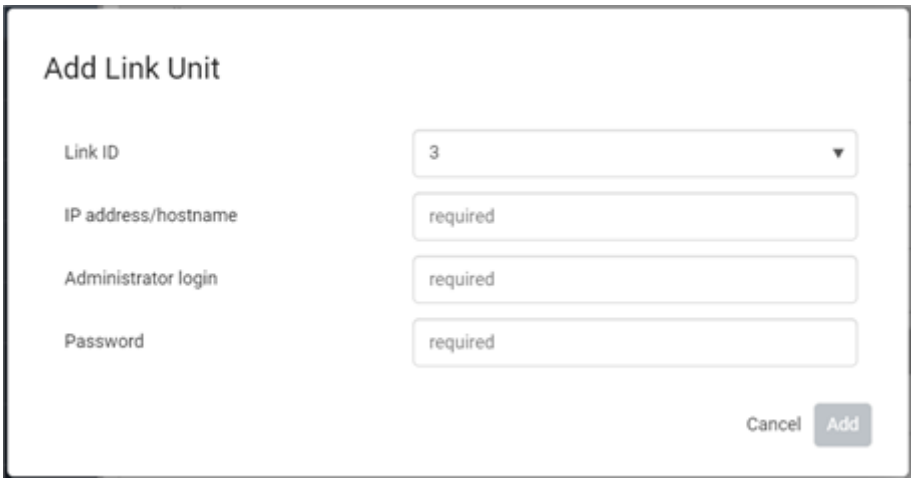
On the PDU page, the Link Units section will contain all link units. The Add Link Unit button, highlighted in green in the screen example, also displays in the Link Units section.



► *To add a link unit:*

- Primary and link units must be the same model, running the same firmware versions.

1. Log in to the primary unit and go to the PDU page.
2. Click Add Link Unit. The following add box displays:



3. The Link ID is populated as the next available ID number (2-8), assigned sequentially as each link unit is added to the chain to identify the link unit in the user interfaces. Note: From the drop-down, you can manually select the desired Link ID to order the link units in the chain as desired. Once associated with a link unit, the Link ID cannot be edited.
4. Provide the IP address of the link unit.
5. Provide the login credentials for the link unit. Note: If the link unit has factory settings, you will be prompted to set the new password.
6. Click Add.
   - The link unit's firmware version is checked to ensure it matches the primary unit. If a mismatch is found, a message appears and the link unit is not added.
7. When the firmware matches, the new link unit is added in a list in the Link Units section. All link units added to the chain are now managed by the single primary unit.

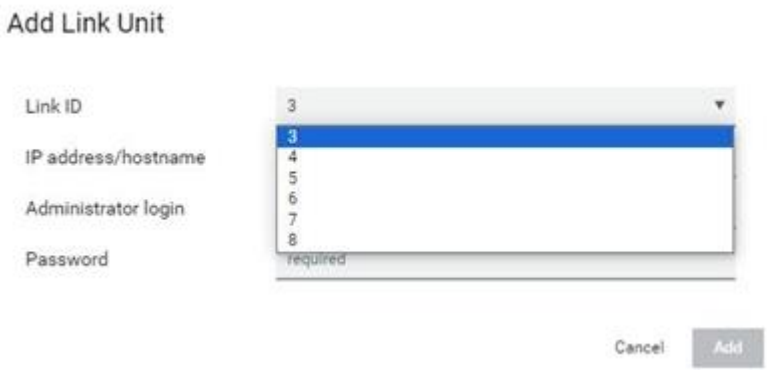
The PDU page displays the following information about the link unit:

- Link ID
- Host/IP address
- Communication status
- Firmware version

About the Link ID

The Link ID "1" is automated and reserved internally for the primary unit. The primary unit’s ID "1" cannot be edited.

The Link ID "2-8" is available for you to select as the ID for each of the link units you add to the chain. From the Link ID drop-down, you can select the desired Link ID to manage the link units in the chain. Once selected, the Link ID cannot be edited.



Linking Cascaded Units

When units are physically connected in a cascade and set to Port Forwarding mode, PX4 can automatically detect expansion units through the primary unit and link the cascaded units.

While a cascaded chain can support up to 32 units and may include various products and models, the Linking feature is limited to a maximum of 8 linked units. Additionally, all linked units must be the same model and run the same firmware version.

Link units can be added using various methods, but keep in mind that the total number of linked units cannot exceed 8.

You can link cascaded units in two ways:

- Link All Cascaded Units (Automatic Method): This method is ideal when your cascade includes 1 to 8 expansion units of the same product, model, and firmware. It allows you to seamlessly and efficiently convert this configuration into a Linked setup.

The automatic linking option simplifies the process by assigning each cascaded unit either a link-local IPv6 address or a node-index-dependent URL as it is discovered and linked. The process starts with the first expansion unit connected to the Primary unit and continues sequentially through the cascade. The linking process concludes either when all 8 Link unit IDs are assigned or when a link attempt fails.

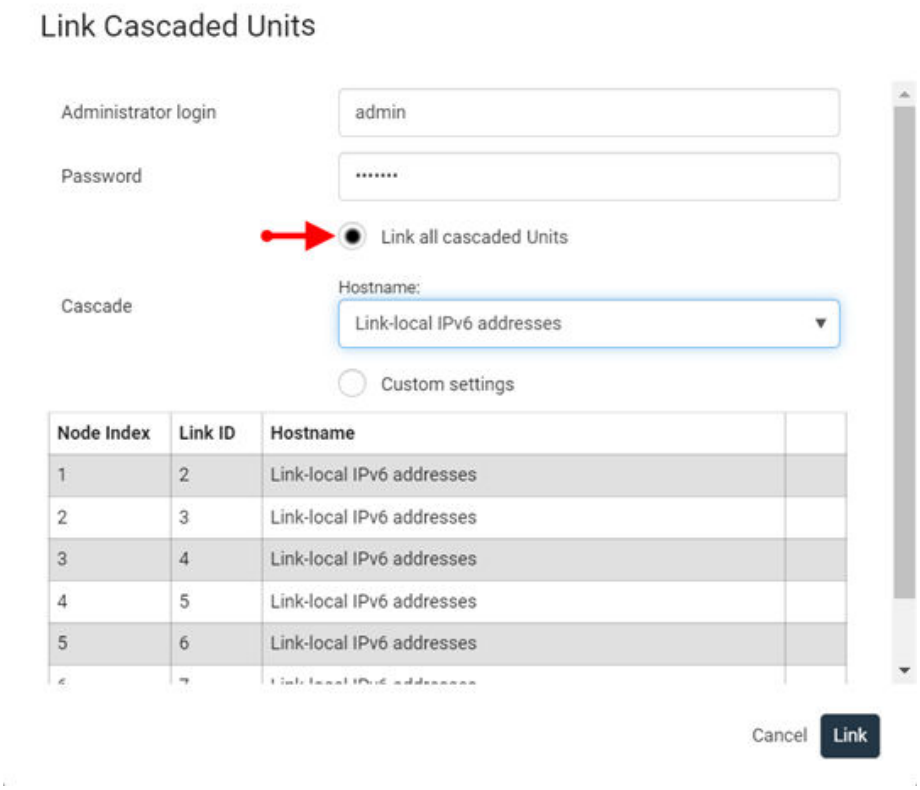
- Custom Method: Choose this method if you want to selectively add specific expansion units from the cascade or customize the linking process, including the order in which the units are linked.

With this option, you manually select each cascaded unit by its node number and assign it to a Link ID. Additionally, you'll need to choose a hostname type for each link. The linking process follows your customized list and attempts to add all the selected expansion units accordingly.

► *To link all cascaded units (Automatic method):*

1. On the PDU page, click the Link Cascaded Units button. The Link Cascaded Units dialog opens.
2. Enter the administrator user name and password assigned to all designated link units. Must be the same credentials for all units.
3. Select "Link all Cascaded Units" for automatic linking.

4. Select the Hostname type to be assigned to all link units:
   - Link-local IPv6 address: Units are assigned IPv6 addresses that are accessible from the primary unit.
   - Dependent on node index: Units are assigned a URL that includes their node index number, for example "expansion-1.pf-cascade", "expansion-2.pf-cascade", "expansion-3.pf-cascade", where the node number indicates the expansion unit's position in the chain related to the primary unit.
5. The table shows the process that will run: Node Index indicates the expansion unit number to be linked, Link ID shows the link ID to be assigned, and Hostname shows the hostname type for all, as specified.



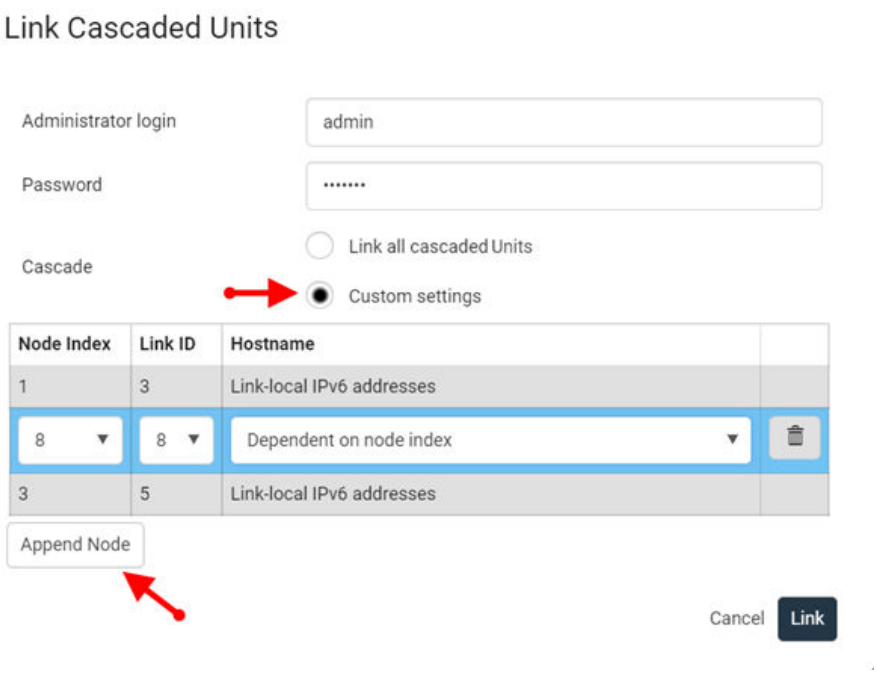
6. Click Link to start the linking process. The table shows progress and then final results. In the example below, expansion unit 1 was linked successfully. Expansion unit 2 failed--the connection may have failed, or this result may also indicate there was no unit at that position. Expansion units 3-7 were skipped because the process stops upon first failure.

Node Index	Link ID	Hostname	Link State
1	2	Link-local IPv6 addresses	✔ Linked
2	3	Link-local IPv6 addresses	✖ Connection to the link unit failed.
3	4	Link-local IPv6 addresses	✖ Skipped
4	5	Link-local IPv6 addresses	✖ Skipped
5	6	Link-local IPv6 addresses	✖ Skipped
6	7	Link-local IPv6 addresses	✖ Skipped
7	8	Link-local IPv6 addresses	✖ Skipped

► *To link cascaded units (Custom method):*

1. On the PDU page, click the Link Cascaded Units button. The Link Cascaded Units dialog opens.
2. Enter the Primary Unit's administrator user name and password.
3. Select Custom Settings.
4. Click Append Node to add a row to the table, then complete each field in the row to describe how the expansion unit should be linked. Repeat this step as needed to create a table of all nodes to link.

- Node Index: Select the node index for the expansion unit you want to add. Node index 1 indicates the first expansion unit connected to the primary unit, then expansion units are numbers sequentially as you go down the cascaded chain.
- Link ID: Select the Link ID that this expansion unit will be mapped to once linked.
- Hostname: Select the hostname type to be assigned to this link unit.
  - Link-local IPv6 address: Units are assigned IPv6 addresses that are accessible from the primary unit.
  - Dependent on node index: Units are assigned a URL that includes their node index number, for example "expansion-1.pf-cascade", "expansion-2.pf-cascade", "expansion-3.pf-cascade", where the node number indicates the expansion unit's position in the chain related to the primary unit.



5. The completed table you create shows the process that will run.
6. Click Link to start the linking process. The table shows progress and then final results.

Note: If a unit is removed from a linked cascade, a reset to defaults is necessary to access the unit.

Primary Units Manage Link Units

The primary unit manages the following functions for the entire chain of linked units:

- User management and authentication – configured only on the primary.
- Date and time – the primary synchronizes its date and time settings to link units. If NTP is not used, then the synchronization interval is every 10 minutes.
- Device settings – only the primary device settings are configurable, except for Network Settings. Some settings will be synced to link units. The serial port is configurable for the primary only; link units use the console.
- Data model settings – such as outlet names, thresholds, peripherals, etc., are configured on the primary and stored on link units. Features vary by model.
- Lua scripts – Communication with link units in a Lua script is possible.

Releasing a Link Unit

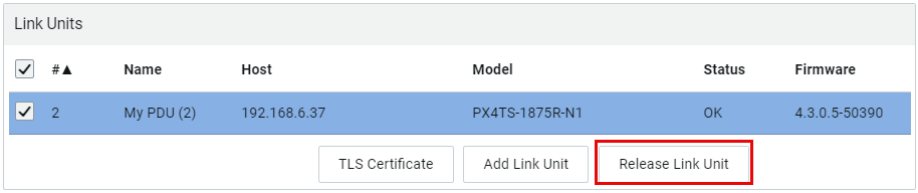
Releasing a link unit means the unit is separated from the chain and the unit then becomes standalone. The primary unit no longer has access to the released link unit.

► *To release a link unit from the Primary Unit's web interface:*

Note: If a release action is attempted on a link unit when the unit is an unreachable state, a warning message displays, and the primary will not recognize the link unit.

1. From the PDU page, in the Link Units section, click a link unit to select it.
2. Click Release Link Unit.
3. A confirmation prompts to cancel or release.

If released, the link unit is removed from the page.

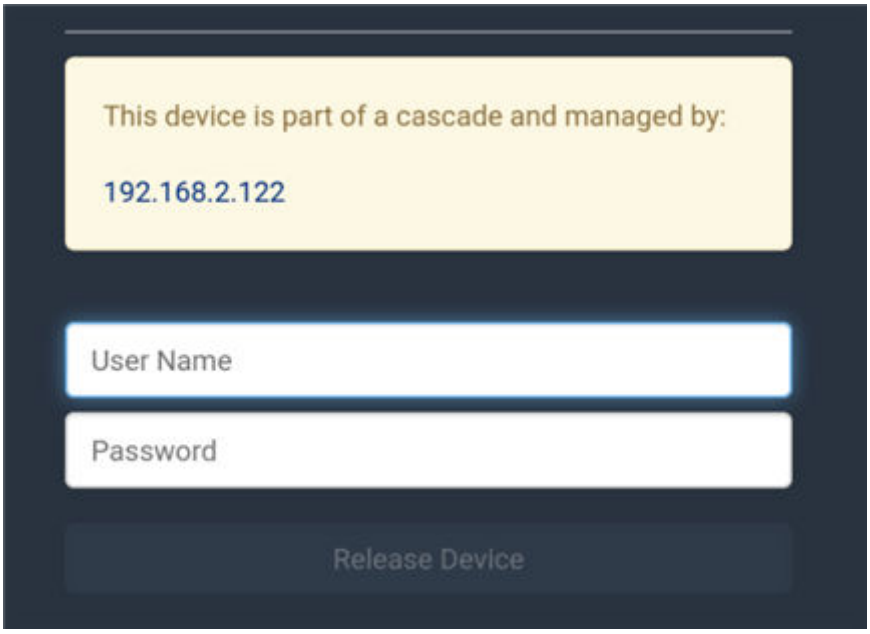


► *To release a link unit directly:*

Caution: Should be used only in a emergency situation.

If you navigate to a link unit directly, in a web browser, a Release Link option is available instead of a login option.

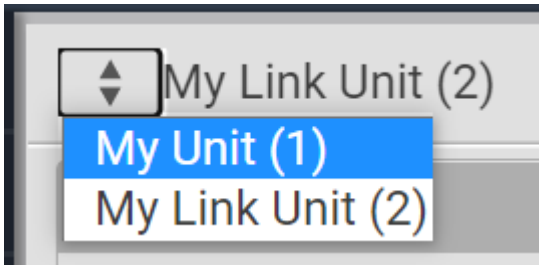
- Enter the username and password, then click Release Device.



Switching to a Different Unit

Switching your view to a different unit is a control function noted by the Switch control in the upper left corner of the pages that display primary and link unit information.

Displayed data in the GUI defaults to the primary unit. The Switch control allows you to switch from a primary page to a link unit page, and back again to the primary.



► *To switch to a different unit:*

1. Click the Switch control.
2. Select one of the link units from the drop-down list. Link number "2-8" appears in parentheses.
3. The page displays data for the selected link unit.
4. To return to the page for the primary, select the primary unit. Primary number "1" appears in parentheses.

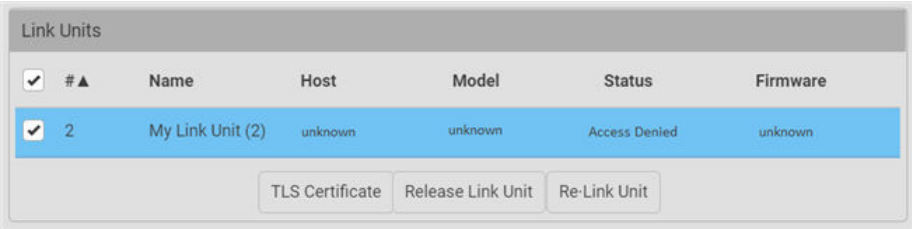
► *Configure load shedding on linked units*

You can switch between units in the GUI and setup / activate load shedding separately for every link unit. Activating load shedding on the primary unit will not activate load shedding for the whole cascade.

Re-linking a Link Unit

Re-link function is necessary when a Link unit stops recognizing or responding to the Primary unit, which often happens if the Link unit has been reset to factory defaults. Resetting to factory defaults renders the Link unit in the chain unreachable, requiring its removal from the chain manually before re-establishing the link.

If reset to factory defaults, the status of the disassociated link unit will be displayed as "Access Denied", shown below.



► *To re-link a link unit:*

1. When you select the link unit in the "Access Denied" status, the Re-link button displays, as noted above.
2. To reconnect the link unit in the chain, and to regain full control of the unit, click Re-Link Unit.
3. Although re-linking uses the same Link Unit ID and hostname of the unreachable unit, you will need to reauthenticate with your login credentials.
4. Click the Re-link button.
5. The status of the link unit changes to "OK".

Viewing Link Unit Information

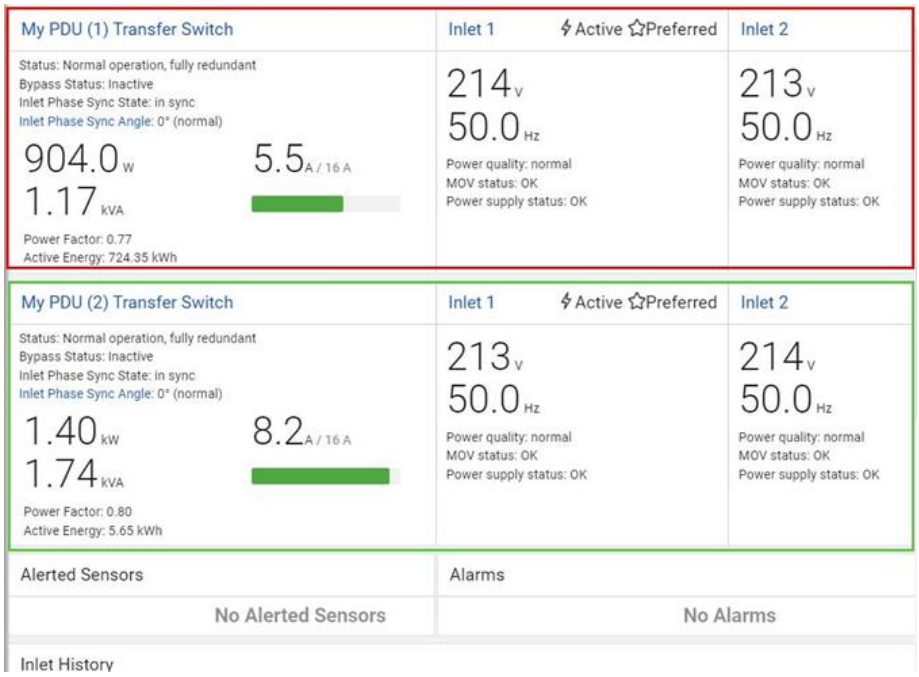
When a link unit is added to the chain, the primary unit view (through the GUI) allows full access to the operational data of the link unit. For example, using the navigation tabs of the GUI, link unit data is displayed in several pages: the Dashboard, PDUs, Inlets, Outlets, Outlet Groups, Peripherals, and Feature Ports.

► *Dashboard*

The Dashboard shows inlets, OCPs, alerted sensors, and inlet history for the entire linked chain.

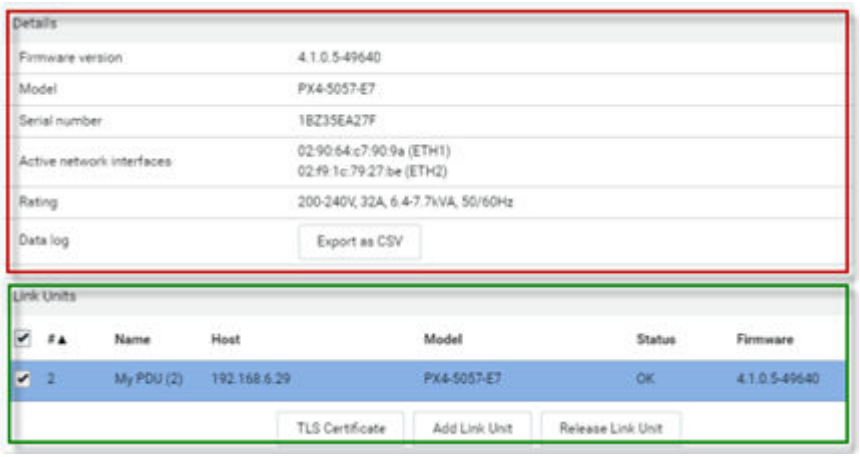
In this example, data for the single inlet of the primary "My PDU (1)" Inlet I1, and the inlet of the link unit "My PDU (2)" Inlet I1, are displayed together. The OCPs for the units are also available together on the Dashboard page.

Peripheral sensors are not shown on the dashboard by default. Only sensors (both PDU or peripheral) in warned or critical state are displayed in the Alerted Sensors section.



► *PDU Page*

The PDU page displays the details and settings for the selected unit (primary or link). The Link PDUs section is only shown when the primary unit is selected.



► *Inlets Page*

On the Inlets page, the primary unit and link units are displayed together on the same page.

In this example, data for the single inlet of the primary "My PDU (1)" Inlet I1, and the inlet of the link unit "My PDU (2)" Inlet I1, are shown together on the Inlets page.

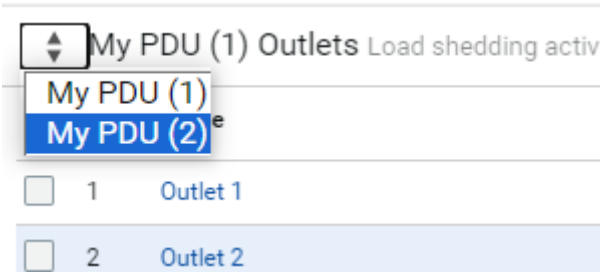
► *Outlets Page*

The Outlets page defaults to display only the outlets of the primary unit, in this example 30 outlets.

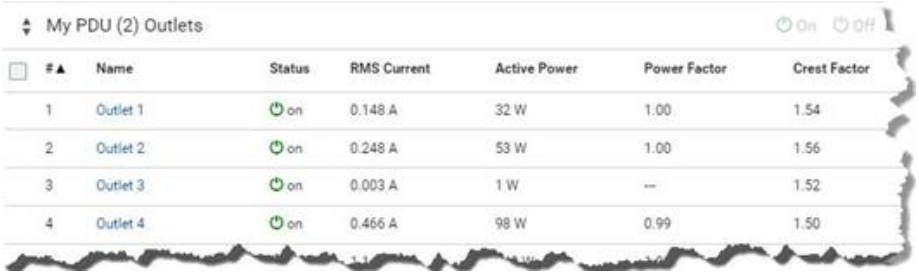
► *Viewing Outlets for Link Units*

On the Outlets page, you can switch from the primary to the link.

1. From the Outlets page drop-down, select the link unit "My PDU (2)". Note: To view outlets for a specific link unit, the link unit must be selected by name.



All outlets of the link unit display for viewing and access exactly like the outlets of the primary unit.



2. You can switch back to the primary unit by selecting "My PDU (1)".

Note: The Switch control is only available when there is at least one link unit in the chain; otherwise, the page defaults to displaying only the outlets of the primary.

3. From the Outlets page (either primary or link), select an outlet in the list to view operational details for the specific outlet and to configure outlet settings.

Pairwise Outlet Groups

The PDU Linking feature includes a "pairwise" outlet grouping functionality. This feature automatically creates pairs of outlet groups with matching outlet labels, spanning multiple PDUs (both primary and link units). Each pair is auto-named and forms an outlet group, enabling centralized control of paired outlets across linked PDUs.

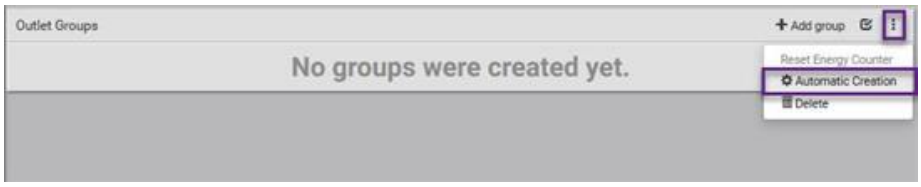
Example: Chain with primary and a single link unit

PDU 1 (Primary Unit)	**Server Load**	**PDU 2 (Link Unit)**
Outlet 1	Server 1	Outlet 1
Outlet 2	Server 2	Outlet 2
Outlet 3	Server 3	Outlet 3
…	…	…
Outlet 20	Server 20	Outlet 20

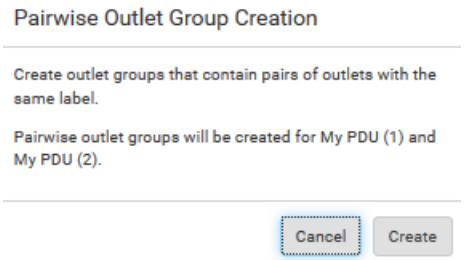
In the given scenario, controlling power to a server usually involves switching one outlet on PDU 1 and another on PDU 2. With the pairwise feature, you can streamline this by auto-creating an outlet group named "Outlet Pair 3." This group will automatically include Outlet 3 from PDU 1 (primary) and Outlet 3 from PDU 2 (link), allowing you to manage them as a single unit.

Automatically Create Pairwise Outlet Groups

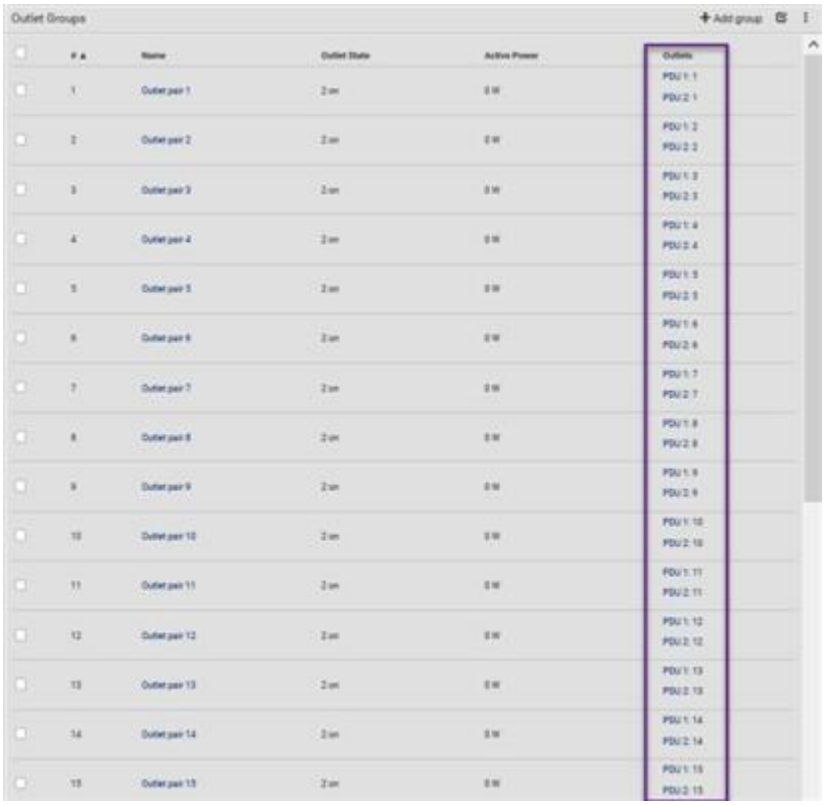
1. From the Outlet Groups page, from the drop-down menu ⋮ select Automatic Creation.



2. Confirm the pairwise creation.



3. Pairwise outlet groups are created and named automatically for all outlets on the primary and link unit, such as "Outlet pair 1", "Outlet pair 2", "Outlet pair 3", etc.

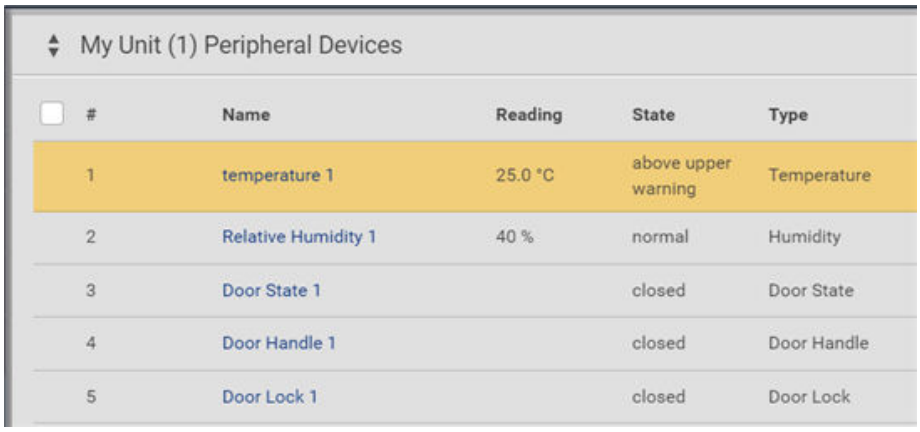


OCPs Page

Overcurrent protectors from both primary and link PDUs are displayed together on the same OCPs page. If sensors are present on the units, sensor data for both primary and link units will also appear on the page.

Peripherals Page

The Peripherals Page shows peripheral devices connected to the primary or link unit.

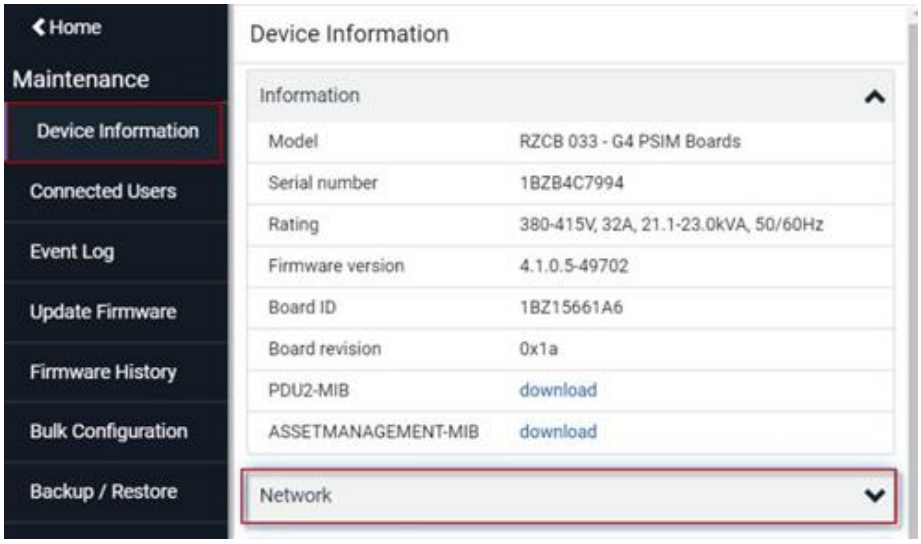


Device Information Page

The Device Information page shows the information about connected devices on the Link port. You can see the primary and link units, link port information, and the link port status.

► *To display link port information:*

1. Log in to the primary link unit.
2. Click Maintenance > Device Information.
3. Expand Network section.



Outlet Groups

An outlet group is a named collection of selected outlets that can be user-defined. These groups can include outlets from multiple PDUs, such as both primary and link units. Outlet groups enable fast and efficient control actions (On, Off, Power Cycle) across multiple PDUs.

With PDU Linking, outlets from both the primary unit and its link units can be grouped together into the same outlet group. These groups are managed by the primary unit, allowing simultaneous control of multiple outlet groups. Additionally, summary and power energy readings are available for each outlet group, offering centralized and streamlined management.

The Outlet Groups page provides a comprehensive overview of user-defined outlet groups. It displays information such as the group name, outlet state, active power readings, and the outlet labels selected for the group. In the Outlets column, you'll notice that outlets from both primary and link units appear together within a single named group. This demonstrates the "pairwise" functionality, which is explained in greater detail in the following section.

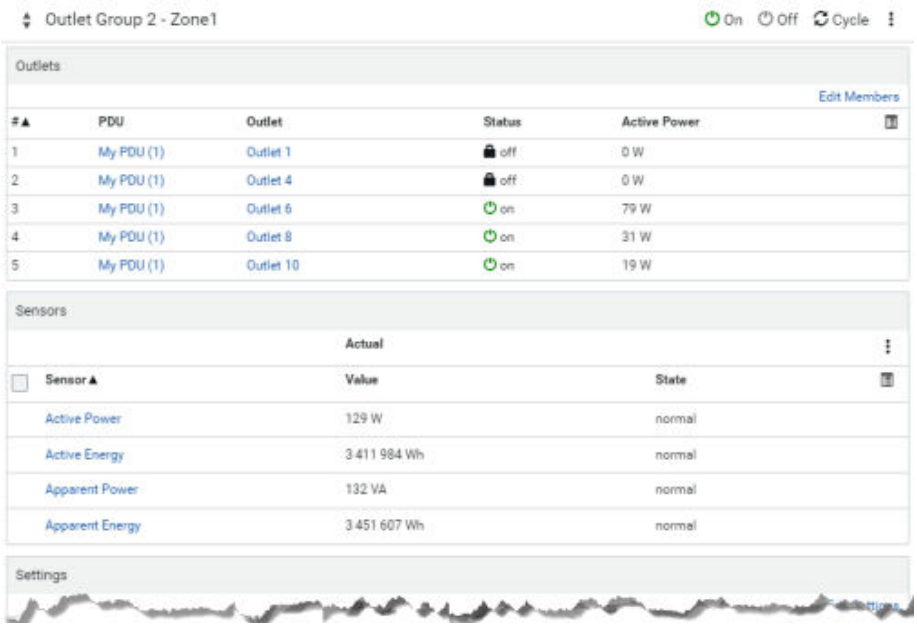
Note: Outlet groups can contain multiple pairs of outlets; the next screen example shows only two outlet pairs in the sample groups.

Click the control arrow to toggle the outlet group list in ascending or descending order by group number.

Raritan
A brand of legrand

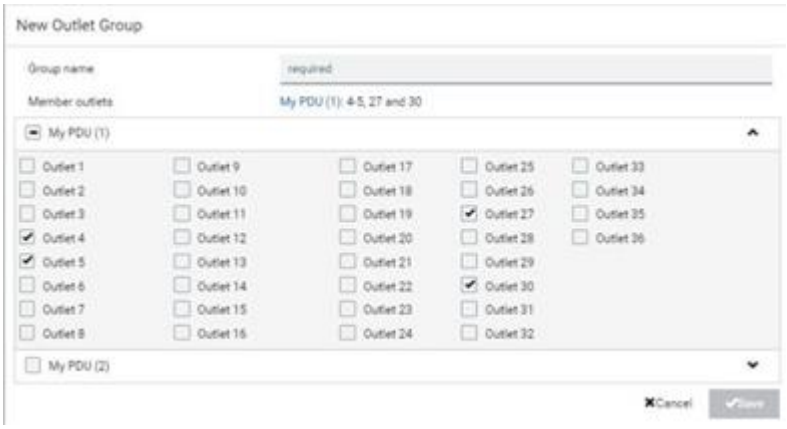
► *Viewing Outlet Group Details*

Click an outlet group name in the list to display operations details for the outlet group. From this page, you can issue the outlet control actions On, Off, and Cycle (power cycling to restore the outlet) for all member outlets in the outlet group. The page also allows editing of the outlet group members and its outlet settings.



► *To add an outlet group:*

1. On the Outlet Groups page, click Add Group. The New Outlet Group page displays, defaulting to the outlets in the primary unit.



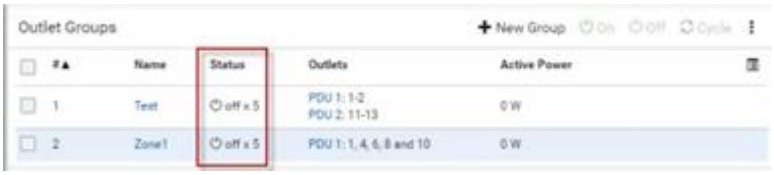
2. Type a name for the new outlet group.
3. Select individual member outlets for the primary as shown in the default page, or to select all outlets for the primary, select My PDU (1).
4. To select individual member outlets for the link unit My PDU (2), click Add Outlets. To select all outlets for the link unit, select My PDU (2). Note: Link units have to be selected by name to display their outlets.
5. Click Save.

The following example shows the outlet group named "TEST 1" with all outlet members selected for the primary unit and outlet members 1-6 selected for the link unit.

Controlling Outlets in Groups

1. From the Outlet Groups page, select an outlet group by name.
2. Click the desired control: On, Off, or Cycle. This example shows three outlets in status On. When Off is clicked, a prompt appears to confirm applying the action to all outlets in the group.
3. Click the Switch button.

4. The status of the outlets in the group appears on the Outlets Group page as Off.



PDU Linking at the Rack

PDUs with the iX9 or iX12 controller have a PDU Link port that supports directly connecting two same model, same firmware version PDUs in a primary-link configuration. This connection also allows for power-sharing between the two PDUs. If you're working at the rack, to allow PDU linking of the wired PDUs, complete the configuration using the PDU front panel display of the Primary unit. You do not have to say Yes to PDU Linking to use power sharing. OR, to complete the configuration remotely, you can use CLI commands. See Linking in the CLI (on page 68).

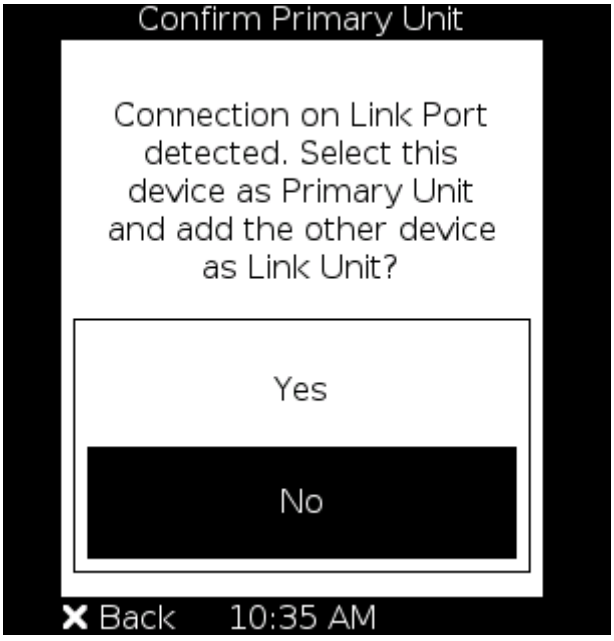
► *Requirements*

- 2 PDUs with iX9 or iX12 controllers
- Units are set to default password
- Ethernet cable

► *To configure PDU Linking at the rack:*

1. Connect the PDU Link port of the first iX9 controller to the PDU Link Port of the second iX9 controller using a standard network patch cable.

2. The units will detect the connection and display messages on the front panels.
3. On the front panel display of the PDU you want to designate as Primary, select Yes to confirm the Primary Unit setting. OR: Use the CLI command "linkport link" now to complete the configuration with CLI.



- Select No to deny PDU Linking for these 2 PDUs. The message will not appear again.

Note: For units without display: Use JSON-RPC function "addLinkPortLinkUnit" to acknowledge the connection on the link port.

---

4. Upon selecting Yes, the units will be linked as Primary and Link units, and will operate as other PDU Linking configurations.

Displays for Primary and Link Units

Each unit in a PDU Linking chain displays its own PDU data (inlets, outlets, sensors, alerts, etc.)

► *Primary unit:*

From the following example of the primary unit display, navigate the options for displaying Link PDU identification and status, and to confirm the primary unit that is controlling the link unit in the chain.

1. Can show alarms, which may be triggered by link units.
2. PDU information shows a list of link units with host name/IP address, model, device name, serial number, firmware version, and communication status.

► *Link units:*

1. No display of alarms/events.
2. PDU information shows the primary IP address

Raritan
A brand of legrand

CLI. If any link units are configured, the CLI prompt includes the currently selected unit and Link ID, such as My Unit (1) or My Unit (2).

Some commands are not available for link units:

- Authentication settings
- Security settings (login, role-based access control, user blocking, and strong passwords.)
- Server monitor
- User management
- Data logging

Linking CLI Commands

Commands for Linking begin with *pdu.*

► *List the Units in the Linked Chain*

Displays the following information for each unit:

- Link ID
- Communication status (for link unit only)
- Device name
- Model name
- Serial number
- Firmware version

```
# pdu list
```

► *Switch Unit*

Switch between the primary and link units. The Link ID must be 1 (primary) or 2-8 (link units).

```
# pdu [id]
```

► *Add a New Link Unit*

Add a link unit to a primary unit. Only available when ID 1 (primary) is selected. The command can be used to re-establish a connection to an existing link unit if the Link ID and host match exactly. The command requires admin privileges and prompts for the user's password.

```
# pdu link [id] [host] [login]
```

- id: New link ID (IDs 2-8)
- host: Host name or IP address
- login: Name of user with admin privileges

► *Release a Link Unit*

Release a link unit from a chain until the unit becomes standalone. The primary unit does not have access to a released link unit. The command is only available when ID 1 (primary) is selected. The command requires admin privileges, and prompts for confirmation unless the "/y" is specified.

```
# pdu release [id] {/y}
```

- id: Link ID of the unit to be released (IDs 2-8).

► *Setup Linking with a Connected Link Port Neighbor:*

Supported only on models with Link Port.

After physically connecting a Primary and Expansion Units at the Link Port, use this command to automatically create a linked configuration. This command can be used instead of the front panel display when connecting supported PDUs at the Link Port.

```
# linkport link
```

► *Show Link Port Status*

Supported only on models with Link Port.

Show the status of the link port. This command shows whether or not the link port is up, and if so, shows the neighbor address and whether it's linked.

```
# show linkport
```

► *Reset to Factory Defaults:*

You can reset the primary and all expansion units to factory default settings with a CLI command.

```
# reset factorydefaults all
```


Raritan
A brand of legrand

Using the Hardware Features

Xerus firmware runs on various hardware designs, including different sizes and controllers.

In This Chapter

Inlet. 71
Outlets and Outlet LEDs. 71
Connection Ports. 72
Front Panel Display. 73
Reset Button. 111
Circuit Breakers. 111
Fuse. 113
Beeper. 117
Replaceable Controller. 117
Threaded Grounding Point. 118
Universal Input Cord. 118

Inlet

PX4 has a 45 degree inlet that is factory-installed on most vertical PDUs.

Connect to an appropriately rated branch circuit. Refer to the label or nameplate affixed to your PDU for appropriate input ratings or range of ratings.

There is no power switch. To power cycle the unit, unplug it from the branch circuit, wait 10 seconds and then plug it back in.

Some models have an inlet that accepts the Universal Input Cord, which is detachable. See Universal Input Cord (on page 118).

Outlets and Outlet LEDs

The total number and type of outlets varies from model to model.

Outlets that are metered and/or switched have an LED that indicates their state.

PX4 Series Outlets and LEDs

Both metered and un-metered models have outlet LEDs that change color as per the outlet state.

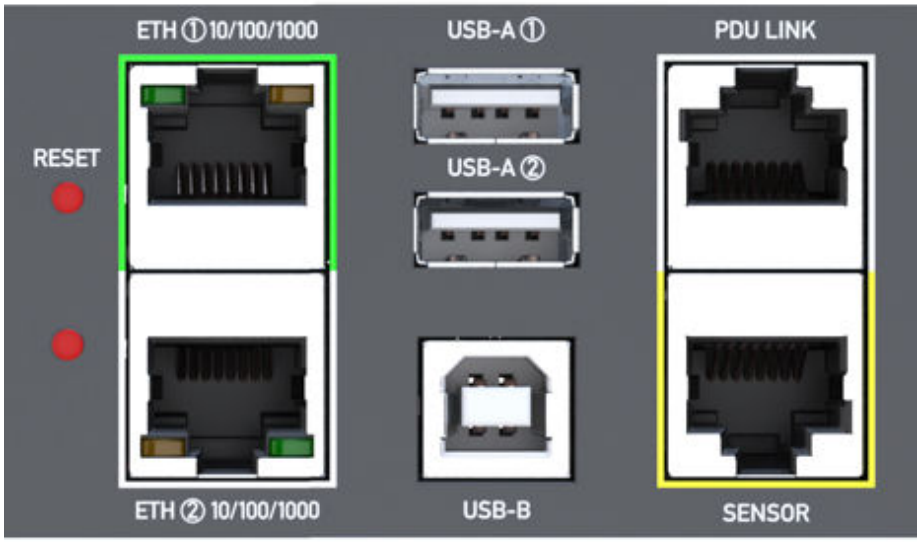
Color	**What it means...**
Green	Outlet powered ON
Unlit	Outlet powered OFF

Amber blinking	Any outlet sensor above or below warning threshold
White/Green blinking	Outlet service mode: Outlet ON
White blinking	Outlet service mode: Outlet OFF
Red	Outlet OFF and suspended after OCP trip
Red blinking	OCP tripped: Outlet OFF
Red/Green blinking	OCP tripped: Outlet ON
Red/Yellow/Green blinking	Boot Up Sequence: Firmware is loading

Connection Ports

Connection ports vary by model.

PX4 Series Connection Ports



PX4 Series models have the following ports:

- USB-A x2
- USB-B x1
- ETH1/ETH2 10/100/1000
- PDU LINK x1
- SENSOR x1

Connection Port Functions

Port	Used for...

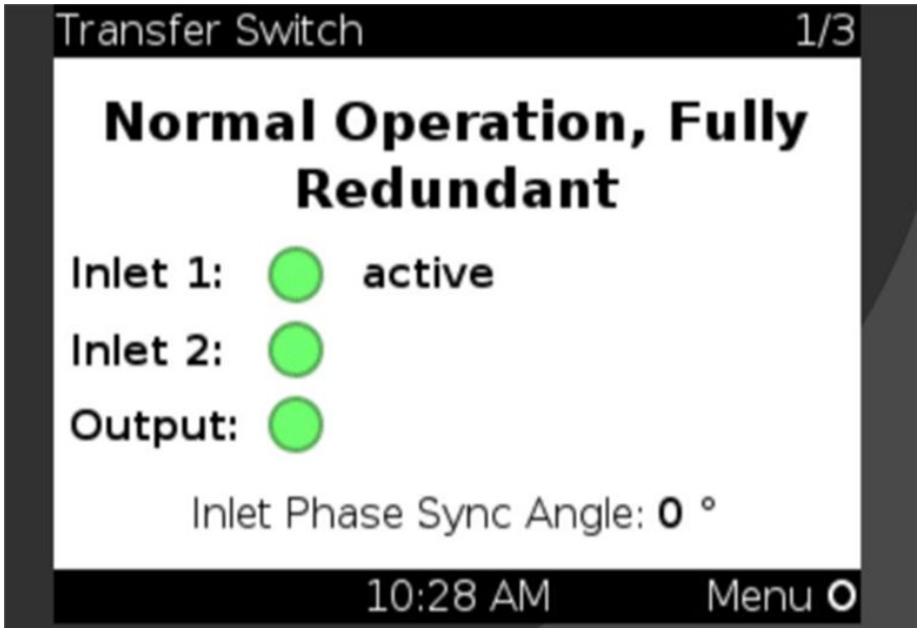
USB-B	• Cascading devices for sharing a network connection.
	• Establishing a USB connection with a computer for:
	  • Using the command line interface.
	  • Performing disaster recovery with Technical Support.
	• Connecting to an Android mobile device.

USB-A	**This is a powered "host" port.** • Connecting to an iOS mobile device. • Connecting a USB device, such as a Logitech® webcam or wireless LAN adapter. • Cascading devices for sharing a network connection. • Connecting to a Raritan KVM device using a supported Power CIM.
SENSOR (RJ-45)	Connection to one of the following devices: • Environmental and security sensor package(s). • Sensor hub. • AMS2-series asset management strip
ETH1/ETH2	Connecting to your company's network via a standard network patch cable (Cat5e/6).
PDU LINK	Connection between two compatible PDUs: • PDU Linking • Power sharing

Front Panel Display

The front panel display will vary by model.

The following diagram shows a sample 0U front panel display. 1U/2U displays are horizontal.



Use the front panel display to view information and even administer features on supported models. It consists of:

- LCD display
- Four control buttons

Zero U models automatically adjust the orientation of the content shown after detecting the direction of installation. You can also manually change the orientation. 1U and 2U models do NOT adjust the content's orientation.

Note: All front panel display images in the User Guide are for Zero U models with the LCD front panel display. Displays may differ slightly by model and on 1U and 2U models.

Automatic and Manual Modes

After powering on or resetting, the front panel display first shows some dots, then logo and finally enters the automatic mode.

► *Automatic mode without alerts available:*

In this mode, the display cycles through information as long as there are no alerts.

► *Manual mode:*

To view more information or control outlets, enter manual mode.

Press or to enter the manual mode, where the Main Menu is first displayed.

To return to the automatic mode, press until you return to the main display.

► *Alerts:*

- In the automatic mode, when an alert occurs, the display stops cycling through information, and warns you by showing the alerts notice in a yellow or red background.

  To enter the manual mode, press .
- In the manual mode, both the top and bottom bars will turn yellow or red to indicate the presence of any alert.

Control Buttons

Use the control buttons to navigate to the menu in the manual mode.

Button	Function
	Up
	Down
	OK
	Back -- OR -- Switch between automatic and manual modes

Operating the Front Panel Display

Enter manual mode when you want to operate the front panel display.

► *Color changes of the display's top and bottom bars:*

- In manual mode, both the top and bottom bars will turn yellow or red to indicate the presence of any alert.
- These examples are generic model samples. Information categories vary by model.

Screen with yellow bars	Screen with red bars
All alerts enter the warning level only. 	Partial or all alerts enter the critical level.

- Both bars turn black when there are NO alerts.

Screen with black bars

Main Menu

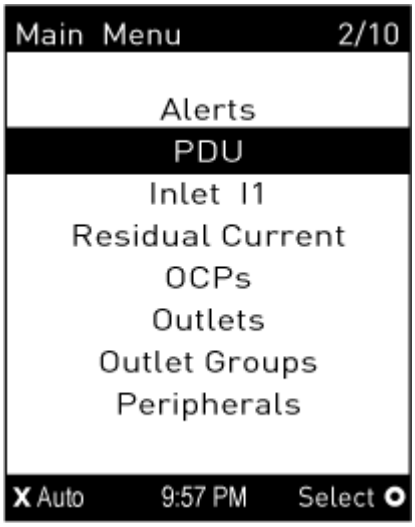
Main Menu

The Main Menu commands depend on the model.

The system time and the X and O buttons and their action on each page are shown at the bottom of the display.

For example, "X Auto" means you can press the X button to enter automatic mode. "Select O" means you can press O to select an option. Always use the arrow buttons to navigate lists and options.

The currently-selected item's number and total of menu items are indicated in the top-right corner of the display.



Alerts

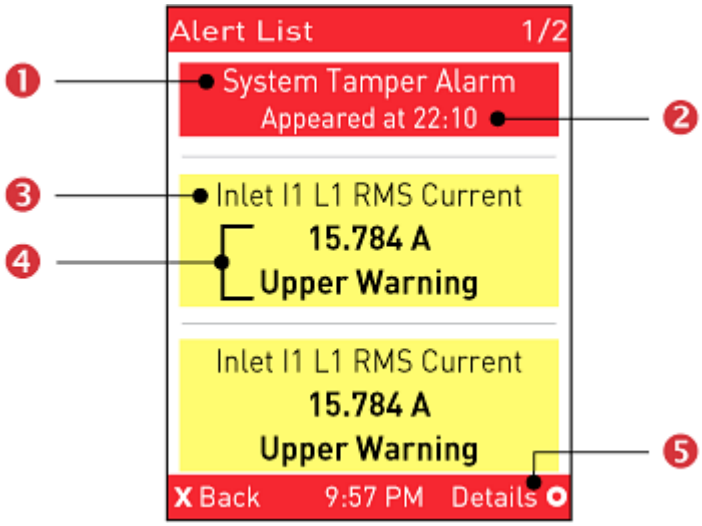
Select Alerts in the Main Menu to view a list of alerted sensors, including both internal and external sensors.

- Numeric sensors in the warning or critical range of an enabled threshold.
- Alarmed state sensors
- Tripped circuit breakers or blown fuses

If there are no alerted sensors, the display shows the message "No Alerts."

► *Alerted sensors:*

- The top and bottom bars on the LCD display may be yellow or red, depending on the type(s) of available alerts.



Number	Description
❶	Alarm names.
❷	The time the alarm occurred. If the alarm occurred at least two times, then more information is shown. • Number of alarms • The first occurrence time • The last occurrence time
❸	Alerted sensor names.
❹	Sensor readings and/or states. A numeric sensor shows both the reading and state. A state sensor or actuator shows the state only. Available states: • Alarmed • Lower Critical = below lower critical • Lower Warning = below lower warning • Upper Warning = above upper warning • Upper Critical = above upper critical • Open (only available for overcurrent protectors)

Number	Description
❺	The 'Details' command appears for alarms only.

1. Press or to view additional pages. When there are multiple pages, page numbers appear in the top-right corner of the display.
2. (Optional) If there are alarms in the Alert List, you can perform the following operations.
   a. Press to view detailed information of the alarm.

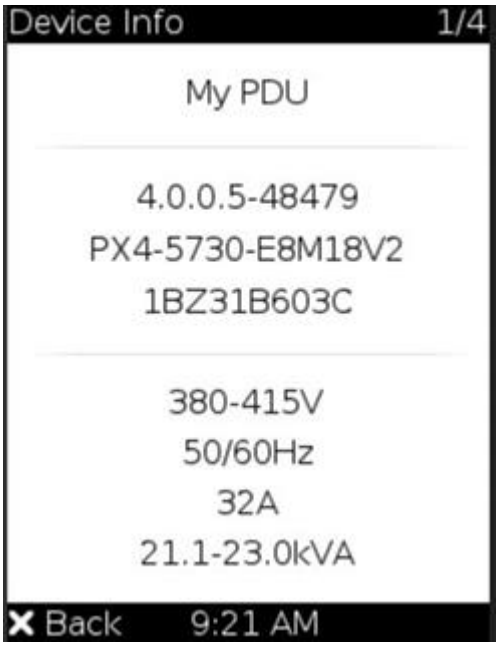
   b. (Optional) If the alarm occurred more than one time, the numbers of current page and total pages are shown in the top-right corner, similar to the above diagram. Press or to view the information of other occurrences.
   c. To acknowledge all alarms now, press .

PDU

Depending on model, the PDU menu includes internal beeper states, unit-level power and energy readings (for models with multiple inlets), Energy pulse output settings, and power supply status.

► *To view or configure PDU information:*

1. Select "PDU" in the Main Menu, and press .
   - PDU name, firmware version, model, serial number, and ratings are displayed.



2. Use the arrow buttons to view additional pages of details:

► *PDU Link Status:*

If Link PDUs are connected, a Link PDUs page appears with details.

Raritan
A brand of legrand

► *Internal beeper state:*

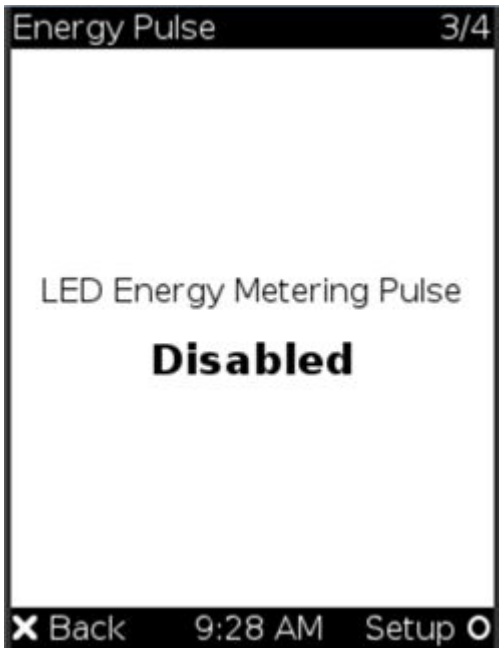
- Active or Off.
  - In the Active state, the reason of turning on the beeper is indicated, and the top/bottom bars turn red. To mute the beep sound immediately, press .

► *Energy pulse output*

Models that support Energy Pulse have an LED Energy Pulse Status page.

By default the energy pulsing is turned off. DO NOT enable this feature unless you have to use it.

Note: This feature, once enabled, blinks all outlet LEDs proportional to the energy consumption. It can be used as a simple interface in certification labs where an optical sensor counts the number of pulses and compares it to the energy reading of a reference meter.



a. To change the energy pulse settings, press for Setup, then select to enable or disable the feature.

Note: All outlet LEDs turn OFF after enabling the energy pulsing. You still can turn on or off outlets during the pulsing period though outlet LEDs do not change their status.

► *Power Supply Status:*

- Power Supply Status shows the status of the controller's power supply.

► *Muting the Internal Beeper*

After enabling the internal beeper's mute control function, you can choose to mute the beeper via the front panel whenever the beeper sounds for an alarm.

By default, the beeper's mute control feature via front panel is enabled.

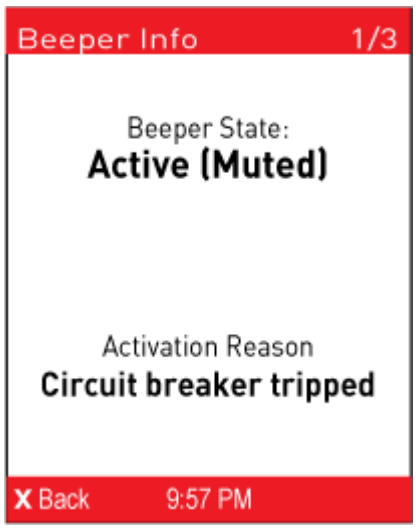
► *To mute the internal beeper during an alarm:*

Note that muting the beeper does not change the alarmed state.

1. Select "PDU" in the Main Menu, and press . The Beeper Info displays

2. Press for Mute, then confirm the operation by selecting Yes.

3. The beeper stops, and the Beeper State shows "Active (Muted)".



Inlet

Inlet details display over multiple pages.

► *To show the inlet information:*

1. Select "Inlet I1" in the Main Menu, and press .
   - Models with one inlet, the first page of details shows immediately.
   - Models with more than one inlet, use the arrow buttons to select the inlet you want to view, then press Select.

► *Single Phase Inlet Details:*

A single phase inlets shows the following readings over multiple pages. Use the arrow keys to go to each page.

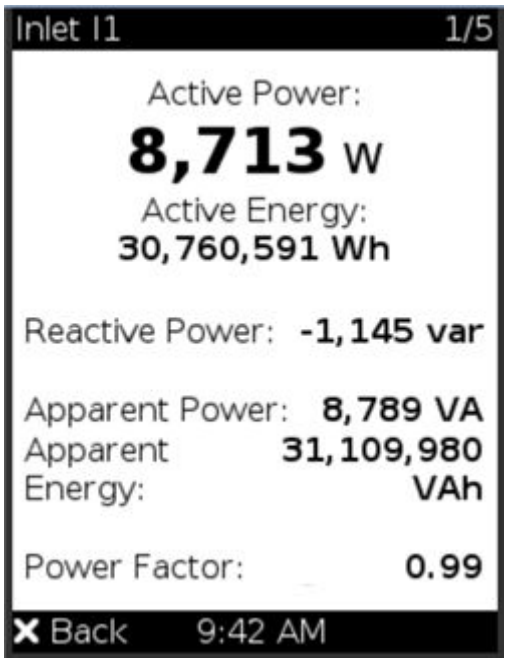
- RMS voltage
- Line frequency
- RMS current
- Active power
- Reactive power
- Apparent power
- Power factor
- Active energy
- Apparent energy
- Phase angle
- Crest factor
- Voltage/current total harmonic distortion

► *Three Phase Inlet Details:*

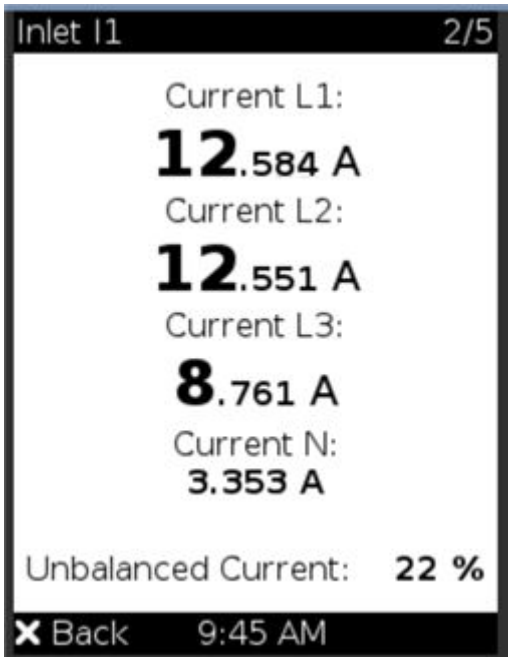
A three phase inlets shows the following readings over multiple pages. Use the arrow keys to go to each page. Use the arrow buttons to scroll between the pages.

- Active Power
- Active Energy
- Reactive Power
- Apparent Power
- Apparent Energy

- Power Factor



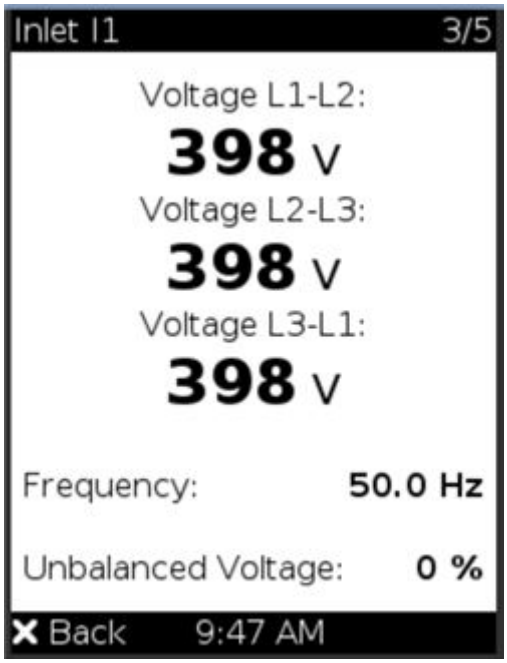
- Current L1
- Current L2
- Current L3
- Current N
- Unbalanced Current



- Voltage L1-L2

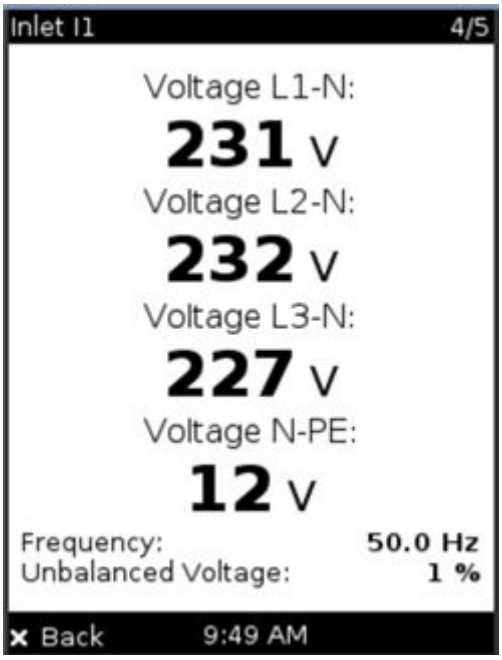
Raritan
A brand of legrand

- Voltage L2-L3
- Voltage L3-L1
- Frequency
- Unbalanced Voltage

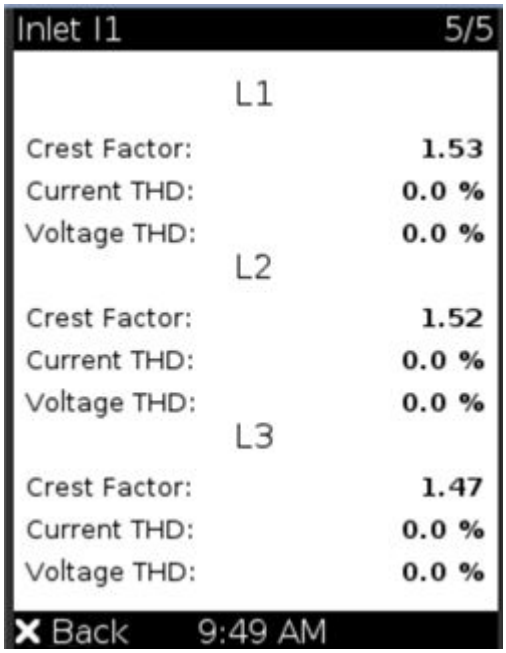


- Voltage L1-N
- Voltage L2-N
- Voltage L3-N

- Frequency
- Unbalanced Voltage



- L1, L2, and L3:
  - Crest Factor
  - Current THD (total harmonic distortion)
  - Voltage THD (total harmonic distortion)



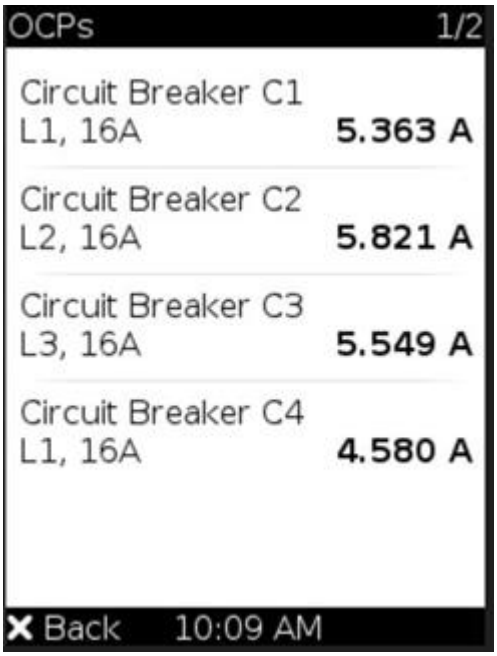
OCPs

If your model has more overcurrent protectors (OCPs) than the display can show at a time, a page number appears in the top right corner of the display. Use the arrow buttons to scroll through the pages.

► *To show the overcurrent protector information:*

1. Select "OCPs" in the Main Menu, and press .
2. The display shows a list of overcurrent protectors with the details:
   - OCP name, such as Circuit Breaker C1
   - Associated lines and rated current for each OCP
   - Current reading (A)

Note: Tripped breakers will show "open" instead of a current reading.



Outlets

With the front panel display, you can:

- Show each outlet's information.
- Turn on, off or power cycle an individual outlet on models that support switching. Front panel outlet control must be enabled in the Front Panel Settings.

Multiple outlet information can be shown on the display. Check the bottom of the display for control buttons and their actions.

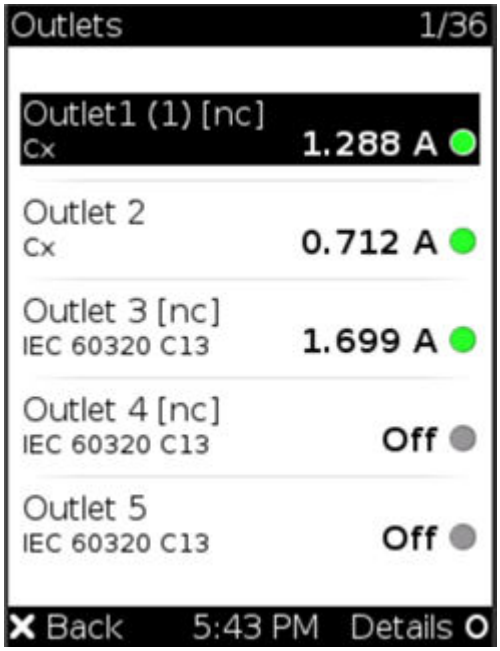
► *To show an outlet's information:*

1. Select "Outlets" in the Main Menu, and press .
2. The list of outlets is shown with their receptacle types, current values (A), and power states which are indicated by the colors of circles.

The currently-selected outlet number and total of outlets are indicated in the top-right corner of the display.

- A green circle indicates that this outlet is powered on.
- A gray circle indicates that this outlet is powered off.

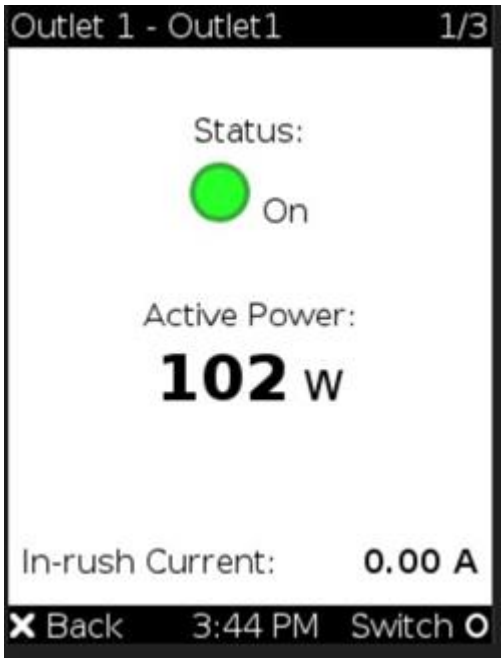
  If so, the word "Off" replaces the current value.



3. Press or to select an outlet, and press .
4. Each outlet has several pages of details. Use the arrow buttons to scroll between the pages.

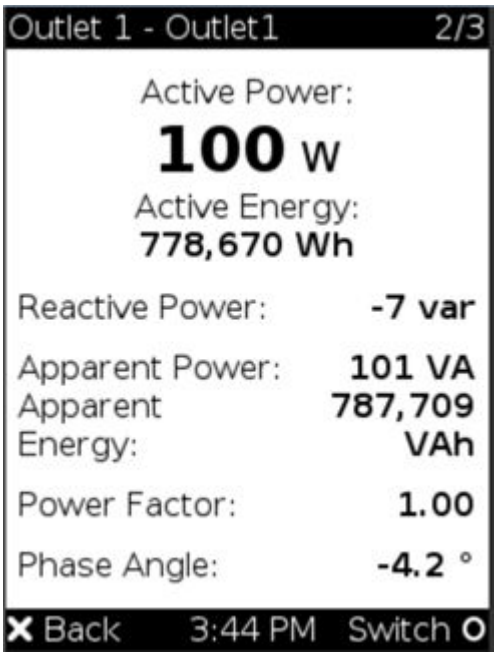
Raritan
A brand of legrand

- outlet power state,
- active power (W)
- inrush current

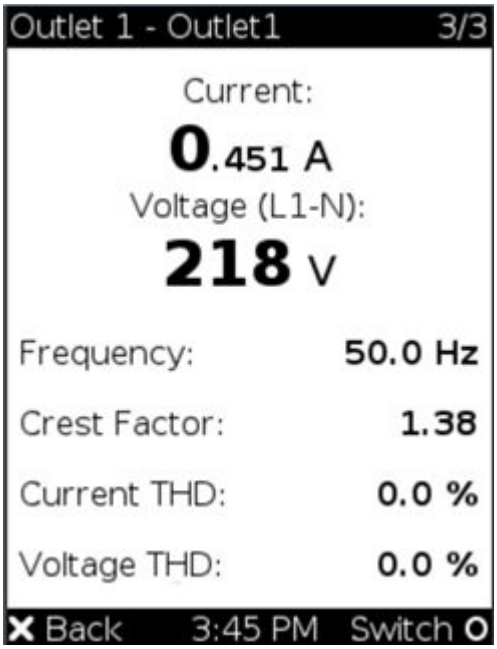


- Active Power
- Active Energy
- Reactive Power
- Apparent Power
- Apparent Energy
- Power Factor

- Phase Angle



- Current
- Voltage
- Frequency
- Crest Factor
- Current THD (total harmonic distortion)
- Voltage THD (total harmonic distortion)



Raritan
A brand of legrand

► *Power Control*

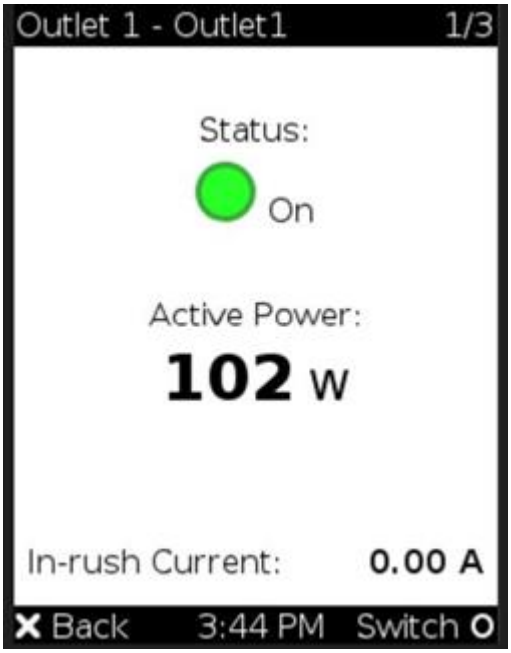
This section applies to outlet-switching capable models only.

The front panel outlet control must be enabled for performing this power control function. The default is to disable this function.

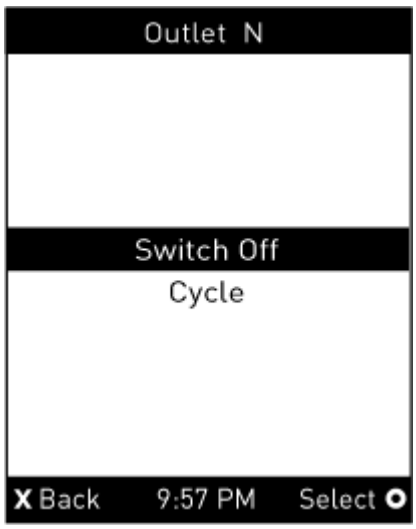
Available options for power control vary, based on the power state of the selected outlet.

► *To power on, off or cycle an outlet:*

1. Select "Outlets" in the Main Menu, and press .
2. Use the arrow buttons to select an outlet, and press .



- In the individual page for the outlet, press for Switch to go to the power control page. In this example, the outlet is On, so the available options are 'Switch Off' and Cycle.



3. Use the arrow buttons to select the desired option, and press .

- Switch Off: Turn off the outlet.
- Switch On: Turn on the outlet.
- Cycle: Power cycle the outlet. The outlet is turned off and then on.

4. A confirmation message appears. Select Yes or No, and then press .
5. Verify that the selected outlet is switched on or off.
   - Check the outlet state shown on the LCD display.
   - Check the outlet LED for the correct Off or On color. Not all models have outlet LEDs.

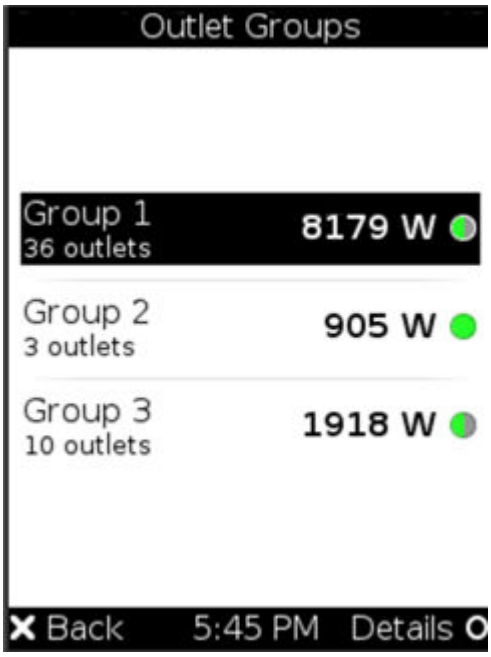
► *Outlet Groups*

Only PDUs with outlet-switching and/or outlet-metering feature show this menu item.

If any outlet group has been created, the front panel then shows a list of these groups and their status.

► *To show an outlet group's information:*

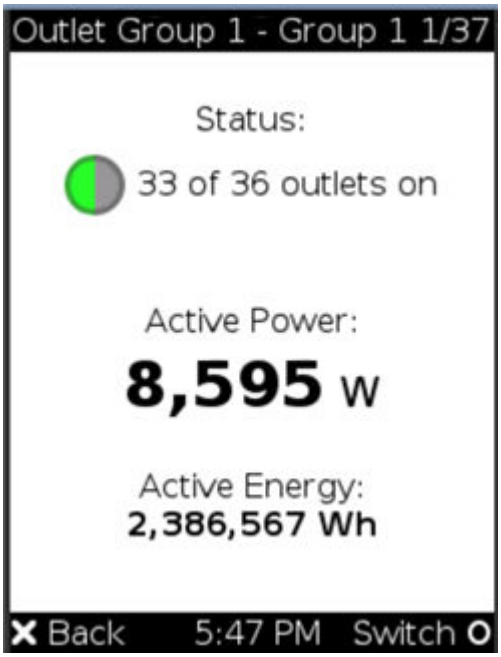
1. Select "Outlet Groups" in the Main Menu, and press .
2. The LCD display shows a list of outlet groups with the information below:
   - The total number of outlets in the group
   - Power states which are indicated by the colors of circles
   - Each group's active power value



The currently-selected outlet group's number and total of outlet groups are indicated in the top-right corner of the display.

- Gray circle: All outlets are OFF
- Green circle: All outlets are ON
- Half Green/Half Gray circle: Some outlets are ON, and some outlets are OFF.

3. Select an outlet group, and press .
4. Outlet Group details display:
   - group power state
   - active power (W)
   - active energy (Wh).



5. To check the status of each member outlet of the group, use the arrow buttons to scroll through the outlet pages.

► *Outlet Group Power Control:*

This section applies to outlet-switching capable models only.

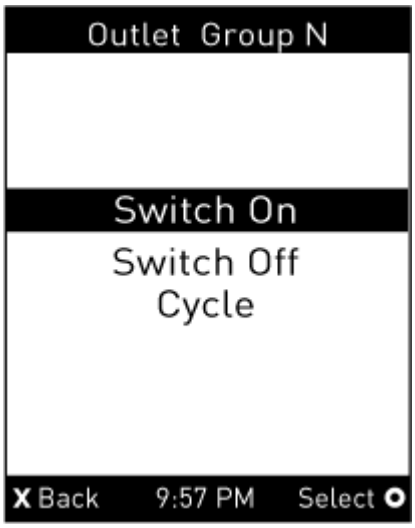
The front panel outlet control must be enabled for performing this power control function. The default is to disable this function.

Check the bottom of the display for control buttons and their actions.

► *To power on, off or cycle an outlet group:*

1. Select "Outlet Groups" in the Main Menu, and press .
   - The LCD display shows a list of outlet groups.
2. Select an outlet group, and press to go to the Outlet Group's details page.

- Press for the Switch command. The power control page opens.



1. Select the desired option, and press .
   - Switch On: Turn on the outlet group.
   - Switch Off: Turn off the outlet group.
   - Cycle: Power cycle the outlet group.
2. A confirmation message appears. Select Yes or No, and then press .
3. Verify that the selected outlet group is switched:
   - Check the outlet group state shown on the LCD display.
   - Check each member outlet's LED of the group.

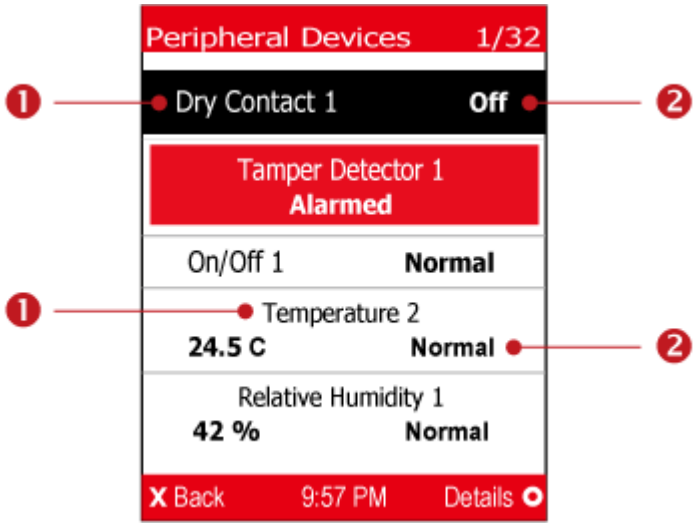
Peripherals

If there are no environmental sensor packages connected, the display shows the message "*No managed devices*" for the "Peripherals" menu command.

► *To show environmental sensor or actuator information:*

1. Select "Peripherals" in the Main Menu, and press .
2. The display shows a list of environmental sensors/actuators.
   - When the list exceeds one page, the currently-selected sensor/actuator's ID number and total of managed sensors/actuators are indicated in the top-right corner of the display.
   - If any sensor enters warning, critical, or alarmed state, like 'Tamper Detector 1' shown below, it is highlighted in yellow or red.

     The top and bottom bars also turn yellow or red.

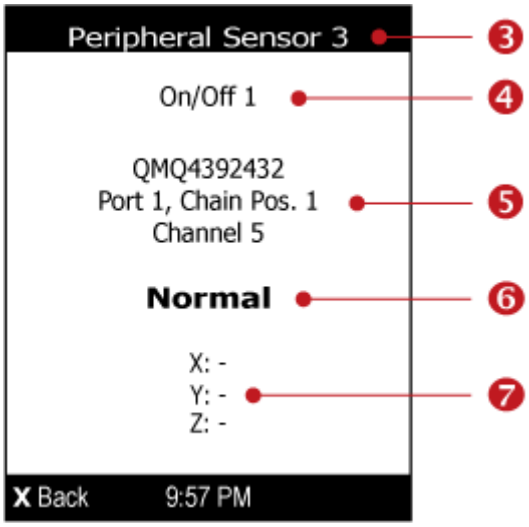


Number	Description
1	Sensor or actuator names.

Raritan
A brand of legrand

Number	Description
❷	Sensor or actuator states: • *n/a* = unavailable • *Normal* • *Alarmed* • *Lower Critical* = below lower critical • *Lower Warning* = below lower warning • *Upper Warning* = above upper warning • *Upper Critical* = above upper critical • *On* • *Off* • *Open* • *Closed* A numeric sensor shows both the reading and state. A state sensor or actuator shows the state only.

3. To view an environmental sensor or actuator's detailed information, select it, and press . A screen similar to the following is shown.



Number	Description
❸	The ID number assigned to this sensor or actuator. • A sensor shows "Peripheral Sensor x" (x is the ID number) • An actuator shows "Peripheral Actuator x"
❹	Sensor or actuator name.

Number	Description

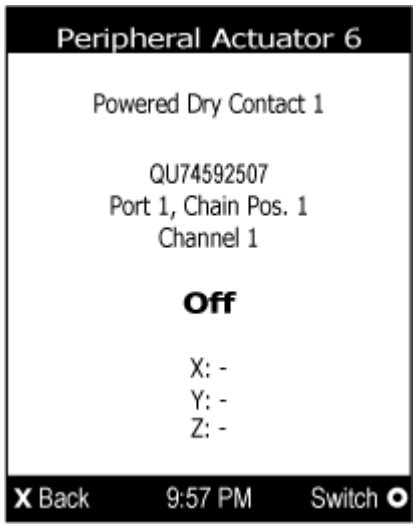
❺	The following information is listed.
	• Serial number
	• Chain position, which involves the following information:
	  • *Port <N>*: <N> is the number of the sensor port where this sensor or actuator is connected.
	  • *Chain Pos. <n>*: <n> is the sensor or actuator's position in a sensor daisy chain.
	• If this sensor or actuator is on a sensor package with multiple channels, its channel number is indicated.

❻	Depending on the sensor type, any of the following information is displayed: • State of a state sensor: *Normal*, *Alarmed*, *Open* or *Closed*. • State of an actuator: *On* or *Off*. • Reading of a numeric sensor.
❼	X, Y, and Z coordinates which you specify for this sensor or actuator.

► *To switch on or off an actuator:*

By default peripheral actuator control is disabled. You have to enable it in the web interface.
See:Peripherals (on page 188)

1. Select "Peripherals" in the Main Menu, and press . Select an actuator to switch and press .



2. Press to turn on or off the actuator. A confirmation message similar to the following is shown.

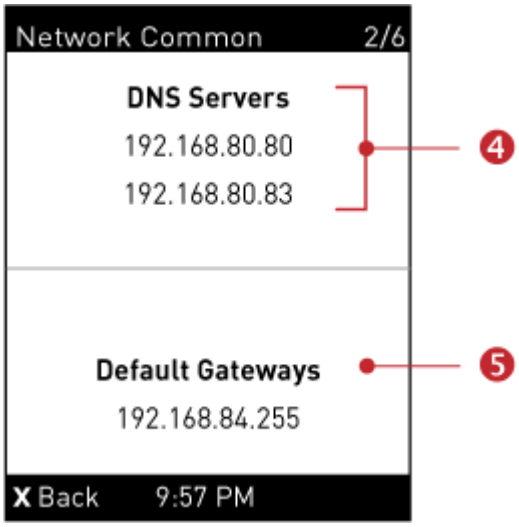
3. Use the arrow buttons to select Yes or No, and then press .
4. Verify that the actuator status shown has been changed.

Device Info

The display shows the device's information, network and IPv4/IPv6 settings through various pages. Page numbers are indicated in the top-right corner of the LCD display.

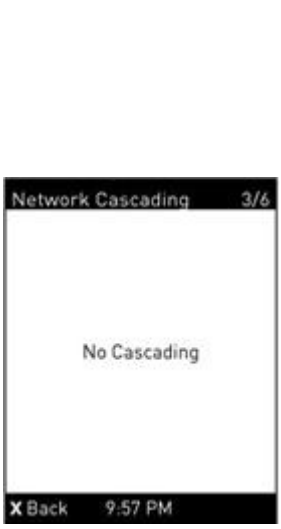
► *To show the device information:*

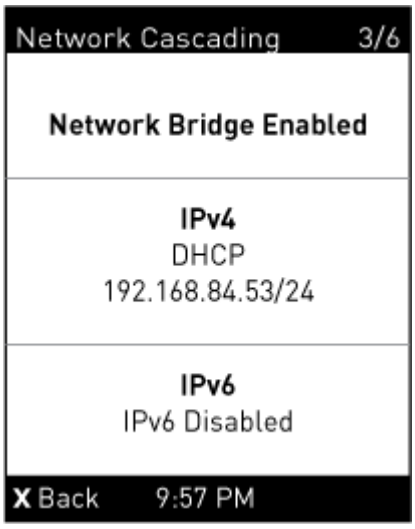
1. Use the arrow buttons to select "Device Info" in the Main Menu, and press .
2. Device information for your model displays.
   - Device name.
   - Firmware version, model name and serial number.
   - Device ratings, including rated voltage, frequency, current and power.
3. Press to show the Network Common page.



Number	Description
4	DNS servers.
5	Default gateways.

4. Press to show the Network Cascading page. Display shows details on your cascading mode, as shown in these examples.



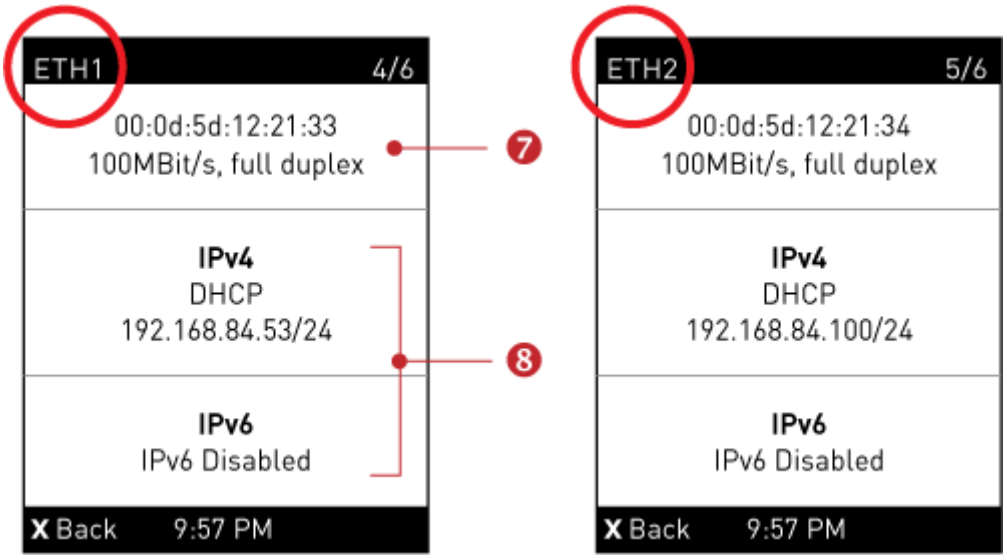


Description

Cascading status, which can be one of the following:
• No Cascading: This device's cascading mode is set to None.
• Network Bridge Enabled: This device's cascading mode is set to Bridging. Its IP address is also displayed on this page.
• Port Forwarding Primary: This device's cascading mode is set to Port Forwarding, and it is a primary device.
  • Expansion unit Connected: Indicates whether the presence of a expansion unit device is detected - *yes* or *no*.
• Port Forwarding Expansion unit: This device's cascading mode is set to Port Forwarding, and it is a expansion unit device.
  • Expansion unit Connected: Indicates whether the presence of a expansion unit device is detected - *yes* or *no*.
  • Cascade Position: Indicates the position of a expansion unit device in the Port Forwarding mode. 1 represents Expansion unit 1, 2 represents Expansion unit 2, and so on.
  • A port forwarding expansion unit device will also display the primary device's IP address on this page.

5. Press to show the Ethernet pages.

There can be one or two pages: ETH1 and ETH2.



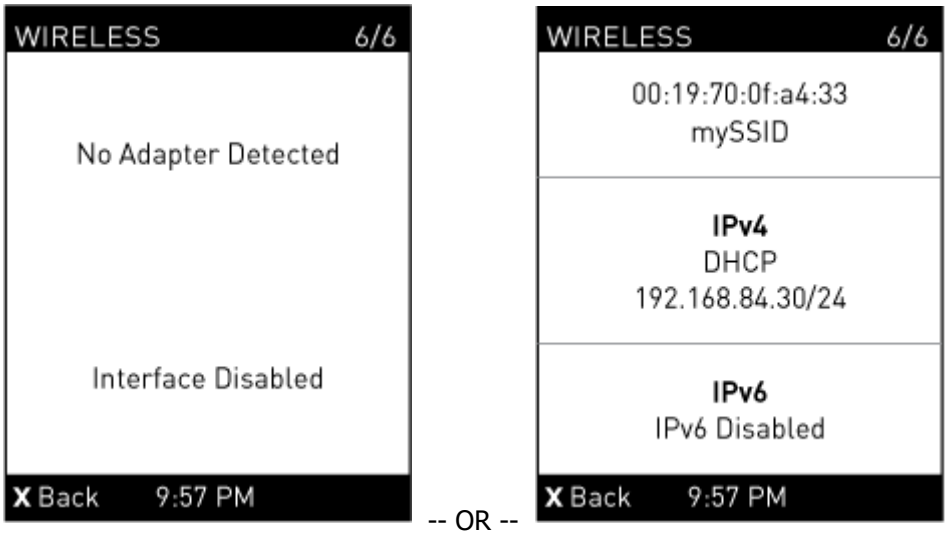
Number	Description
7	Ethernet interface information, including: • MAC address. • Speed. • Full or half duplex.

Number	Description
8	IPv4/IPv6 network information, including: • Network configuration: DHCP (or Automatic), or Static. Static represents Static IP. • IP address. • Prefix length, such as "/24". *Note: If you disable any Ethernet interface, a message 'Interface Disabled' is shown. See Ethernet Interface Settings.*

If you do not enable IPv4/IPv6 settings, an 'IPv4 (or IPv6) Disabled' message is displayed.

6. Press to show the WIRELESS page.
   - If NO supported WLAN adapter is plugged or detected, the message "No Adapter Detected" is shown.
   - If a supported WLAN adapter is detected and configured properly, wireless network information is shown instead, including:

- MAC address
- SSID
- IPv4/IPv6 network information



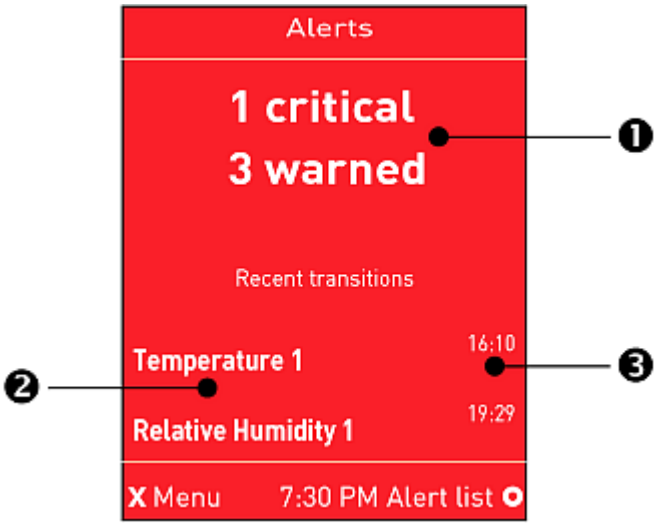
Alerts Notice in a Yellow or Red Screen

In automatic mode, if an alert occurs, the LCD display automatically switches to either a yellow or red screen. This screen displays the total number of alerted sensors along with information about the latest transitions.

- When all alerted sensors are at warning levels, the screen's background turns yellow.
- When at least one alerted sensor reaches a critical level or if there is any "alarm," the background turns red.

The following illustrates the alerts notices in red.

► *When there are only alerted sensors -- NO ALARMS are present:*

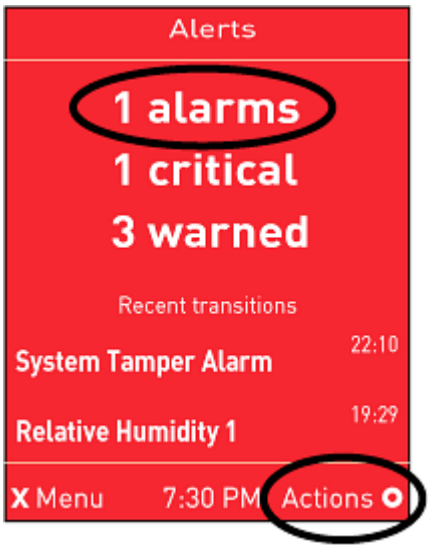


Number	***Description***
❶	***The total of alerted sensors in critical and warning levels.***
❷	***A list of alerted sensors.***

Number	*Description*
❸	***The latest reading/status time related to each alerted sensor.***

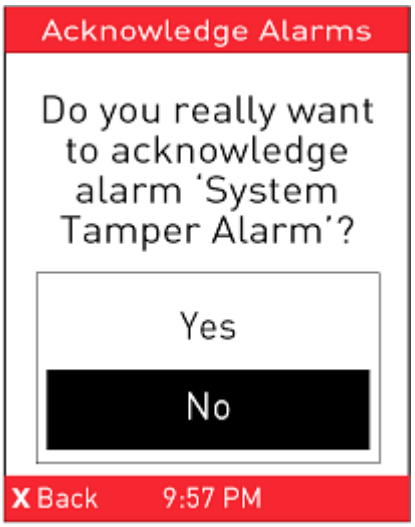
► *When there is any alarm present:*

The display shows the alarm(s) and the available command in the bottom-right corner is 'Actions'.



► *Available operations:*

- For alerted sensors only, press to view a list of all alerted sensors. You do not have to acknowledge alerted sensors.
- When an alarm is present, press to view the options. Use the arrow buttons to select an option, and press .
  - Show alert list: View a list of alerted sensors and alarms. You still can choose to acknowledge alarms after viewing the list.
  - Acknowledge all alarms: This option immediately acknowledges all existing alarms, without showing the list of alarms. When you select this option, you must next select Yes to confirm.



Port Overload - Reset Fuse

If an overload condition is detected on an external port, the front panel displays an alert notification. This notification includes a detailed list of ports that might have contributed to the overload.

The alert cannot be dismissed until the overload condition is resolved and the fuse has been reset.

► *To resolve a Port Overload condition:*

1. Remove all attached devices from the ports listed in the alert.
2. Press the Select button on the front panel to reset the fuse.

Showing the Firmware Upgrade Progress

When upgrading the PX4, the firmware upgrade progress will be displayed as a percentage on the LCD display, similar to the following diagram.

In the end, a message appears, indicating whether the firmware upgrade succeeds or fails.

Manually Changing Zero U LCD Orientation

A Zero U model has a tilt sensor that can detect the orientation of its physical device to automatically adjust ts LCD content's orientation.

If the LCD's orientation does not meet your need, you can manually configure it.

The factory default is automatic orientation.

► *To set up the LCD orientation:*

1. Press and simultaneously until you see the LCD shows "Fixed Orientation".
2. If the current LCD orientation does not meet your need, repeat the above step until the orientation you preferred is displayed.

Reset Button

The reset button is located inside the small hole labeled RESET near the display panel.

Pressing this reset button restarts the Xerus software without any loss of power to outlets.

Circuit Breakers

PX4 models rated over 20A (North American) or 16A (international) contain overcurrent protectors for outlets, which are usually branch circuit breakers. These circuit breakers automatically trip (disconnect power) when the current flowing through the circuit breaker exceeds its rating.

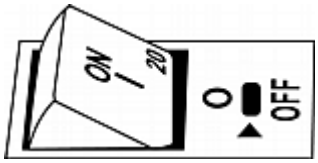
If a circuit breaker switches off power, the front panel display shows `open`. To find which circuit breaker is open (trips), select Alerts or OCPs in the front panel display menu. When a circuit breaker trips, power flow ceases to all outlets connected to it. You must manually reset the circuit breaker so that affected outlets can resume normal operation.

Resetting the Button-Type Circuit Breaker

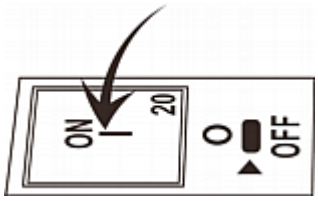
Your button-type circuit breakers may look slightly different from the images shown in this section, but the reset procedure remains the same.

► *To reset the button-type breakers:*

1. Locate the breaker whose ON button is up, indicating that the breaker has tripped.



2. Examine your PX4 and the connected equipment to remove or resolve the cause that results in the overload or short circuit. This step is required, or you cannot proceed with the next step.
3. Press the ON button until it is completely down.

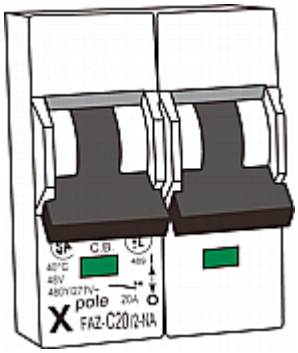


Resetting the Handle-Type Circuit Breaker

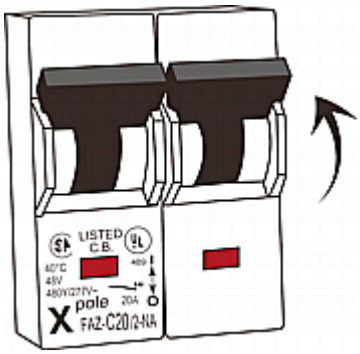
Your handle-type circuit breakers may look slightly different from the images shown in this section, but the reset procedure remains the same.

► *To reset the handle-type breakers:*

1. Lift the hinged cover over the breaker.
2. Check if the colorful rectangle or triangle below the operating handle is GREEN, indicating that the breaker has tripped.



3. Examine your PX4 and the connected equipment to remove or resolve the cause that results in the overload or short circuit. This step is required, or you cannot proceed with the next step.
4. Pull up the operating handle until the colorful rectangle or triangle turns RED.



Fuse

Some devices may be implemented with fuses instead of circuit breakers. A fuse blows to protect associated outlets if it detects overload.

If your PDU uses fuses, you must replace it with a new one when it blows or malfunctions. The rating and type of the new fuse must be the same as the original one.

Use of inappropriately rated fuse results in damage to the PDU and connected equipment, electric shock, fire, personal injury or death.

Depending on the design of your PDU, the fuse replacement methods differ.

Fuse Replacement on Zero U Models

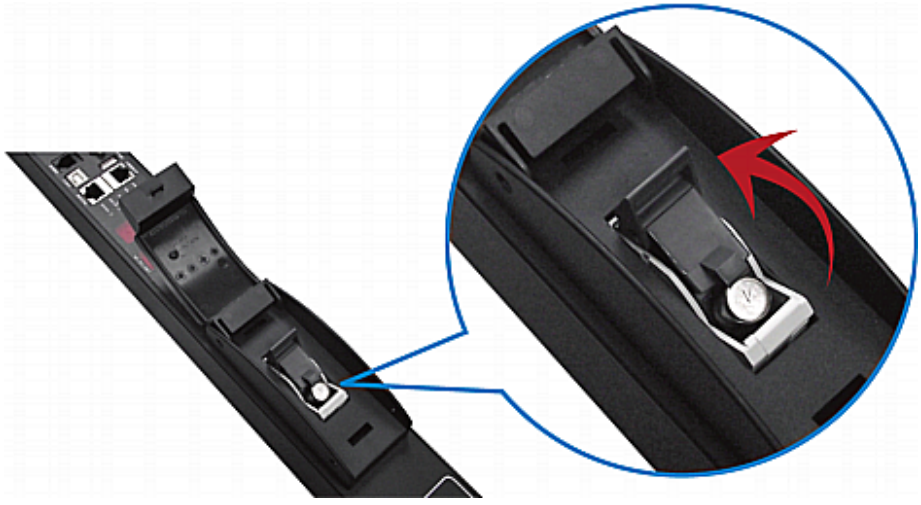
This section only applies to a Zero U PDU with "replaceable" fuses.

► *To replace a fuse on Zero U models:*

1. Lift the hinged cover over the fuse.

2. Verify the new fuse's rating against the rating specified in the fuse holder's cover.

3. Push the cover of the fuse holder to expose the fuse.

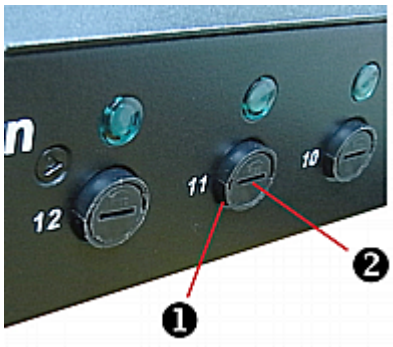


4. Take the fuse out of the holder.

5. Insert a new fuse into the holder. There is no orientation limit for fuse insertion.
6. Close the fuse holder and the hinged cover in a reverse order.

Fuse Replacement on 1U Models

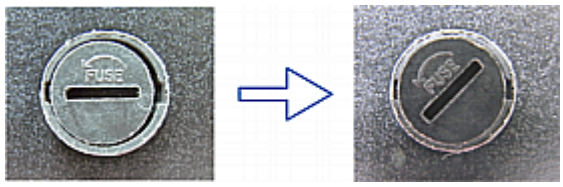
On the 1U model, a fuse is installed in a fuse knob, which fits into the PDU's fuse carrier.



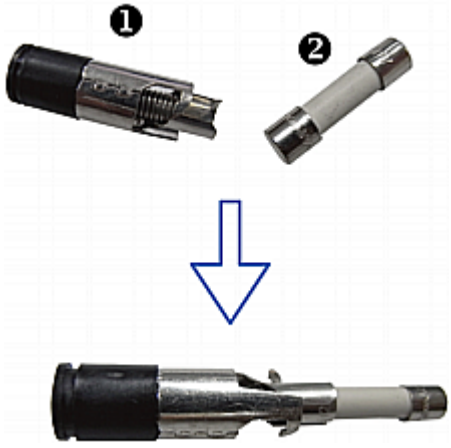
Number	Description
❶	Fuse carrier
❷	Fuse knob where a fuse is installed

► *To replace a fuse on 1U PDUs:*

1. Disconnect the PDU's power cord from the power source.
2. Remove the desired fuse from the PDU's fuse carrier using a flat screwdriver.
   a. Rotate the fuse knob counterclockwise until its slot is inclined to 45 degrees.



   b. Take this knob out of the fuse carrier.
3. Remove the original fuse from this knob, and insert either end of a new one into the knob. Make sure the new fuse's rating is the same as the original one.

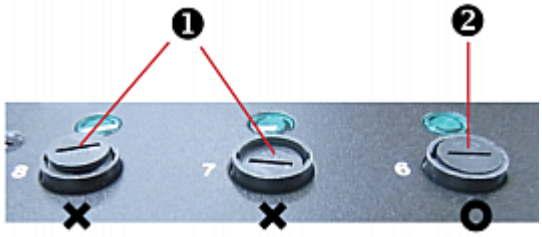


Number	Description
❶	Fuse knob
❷	Fuse

Raritan
A brand of legrand

4. Install this knob along with the new fuse into the fuse carrier using a flat screwdriver.
   a. Have this knob's slot inclined 45 degrees when inserting the knob into the fuse carrier.

   b. Gently push this knob into the fuse carrier and then rotate it clockwise until its slot is horizontal.
5. Verify whether this knob's head is aligned with the fuse carrier. If its head is higher or lower than the fuse carrier, re-install it.



Number	Description
❶	INAPPROPRIATE installations
❷	Appropriate installation

6. Connect the PDU's power cord to the power source and verify that the corresponding fuse LED is lit, indicating that the fuse works properly.

Beeper

The PX4 includes an internal beeper to issue an audible alarm for an overcurrent protector which is open.

- The beeper sounds an alarm within 3 seconds of a circuit breaker trip.
- The beeper stops as soon as all circuit breakers have been reset.

You can also set the internal beeper to sound for specific events.

Tip: You can remotely check this beeper's state in the web interface on the PDU page.

Replaceable Controller

The PX4 is designed for flexibility, and utilizes a hot-swappable, replaceable controller.

If the controller is broken, you can send the controller only back for repair, or purchase a new controller.

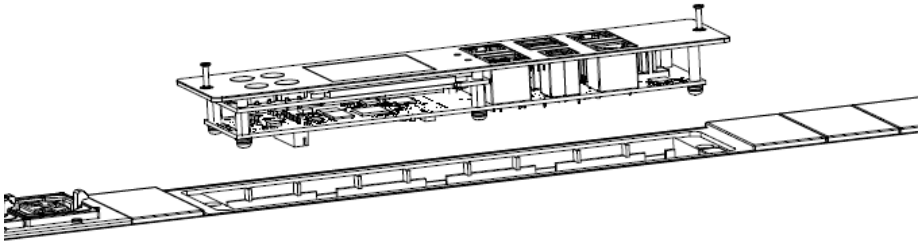
► *To request a new controller:*

Contact Technical Support to request a new controller.

► *To replace a controller:*

1. PDU is NOT required to be powered off.
2. Loosen the screws at two sides of the controller, and lift it up.

Note: Loosen the screws instead of removing them.



3. Get a new controller and install it back into the PDU in the reverse order.

Threaded Grounding Point

Some models have a threaded grounding point. Identify it via the grounding symbol:

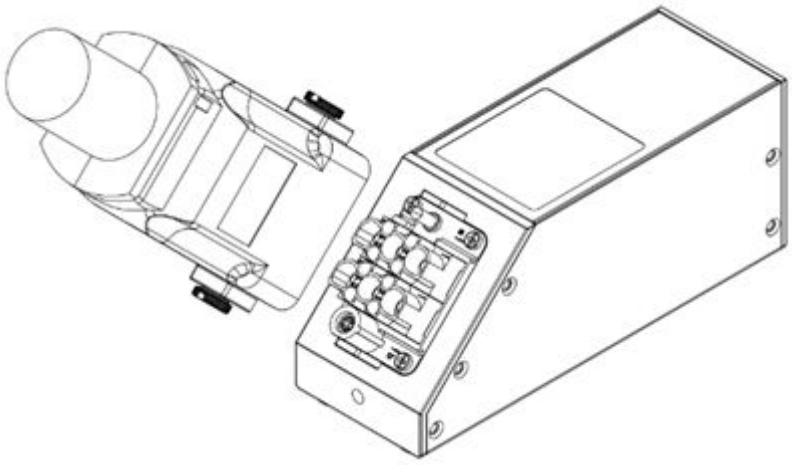
Wire this point to an electrical system to protectively ground the PX4.

Universal Input Cord

PX4 is available with a detachable cord, the Legrand Universal Input Cord. The input cord is detachable as either a low-voltage (LV) version or a high-voltage (HV) version. Once installed, the user interfaces will automatically detect the wiring and display the correct details.

Use the inlet to connect the input cord to the PDU.

Check Safety Warnings (on page 14), Safety Warnings (on page 16) before proceeding.



► *To connect the detachable input cord:*

1. Connect the input cord to the PDU.
2. Secure the input cord to the PDU, maneuvering the cord so that the plug is fully seated against the PDU.
3. Torque the screws on the plug to 15 in-lbs (1.7 Nm).
4. Connect the other end of the input cord to an appropriately rated branch circuit.
   - To power cycle the PDU, unplug it from the branch circuit, wait 10 seconds, and plug it back in. Do not power cycle this PDU by detaching/reattaching the Universal Input Cord at the inlet.
   - If your PDU has been installed in a new configuration with a new DTCORD, a review of threshold settings is recommended. See Inlet.

Using the Web Interface

This chapter explains how to use the product web interface for administration.

In This Chapter

Supported Web Browsers and Mobile Devices. 120
Login, Logout and Password Change. 120
Web Interface Overview. 122
Dashboard - PDUs. 129
PDU. 138
Inlet. 147
Outlets. 155
Outlet Groups. 175
OCPs. 180
Peripherals. 188
Asset Strips. 206
Serial Access With Dominion Serial Access Module. 215
User Management. 221
Device Settings. 232
Using Prometheus and Grafana. 364
Maintenance. 366
Webcam Management. 382
SmartLock. 391
Card Readers. 396

Supported Web Browsers and Mobile Devices

- Firefox® 100 and later
- Safari® (Mac)
- Google® Chrome® 100 and later
- Android 8.1 and later
- iOS 12.5 and later
- Edge (Windows 10, 11 (chrome-based versions))

Login, Logout and Password Change

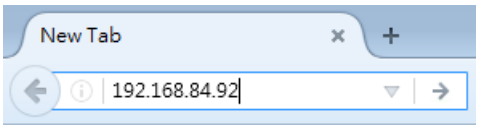
The first time you log in, use the factory default user credentials. For details, refer to the Quick Setup Guide accompanying the product. Password change is forced upon first login.

Login and Logout

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

► *To log in to the web interface:*

1. In a supported browser go to the IP address of your PX4
   - If the link-local addressing has been enabled, you can type *pdu.local* instead of an IP address.



2. If any security alert message appears, accept it.
3. You can set contrast polarity by clicking on Dark and Light icon

or

on bottom left of the login screen.
4. Enter your user name and password, accept any security agreement displayed, and click Login.

Note: To configure the security agreement, go to Device Settings > Security > Service Agreement.

---

5. The web interface opens.

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

- Click Logout in the top right corner, or close the tab or browser.

Changing Your Password

You need appropriate permissions to change your password or others' passwords.

► *Password requirements:*

- Case sensitive.
- 4 to 64 characters.

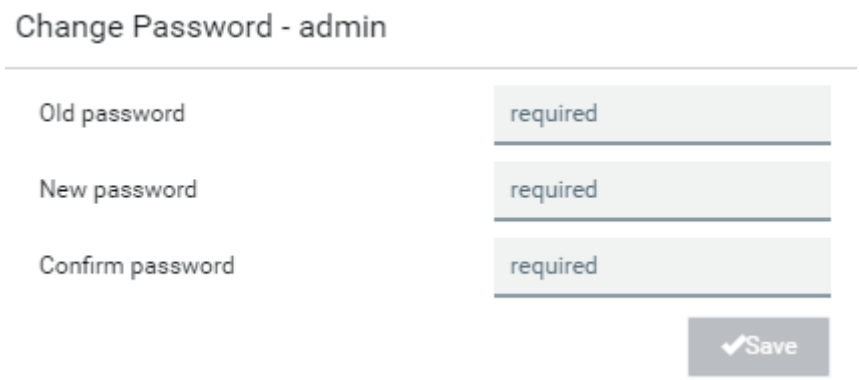
► *Password change required on first login:*

- On *first login*, password change is forced and strong passwords are enabled by default. The new password must be at least 8 characters and contain at least one upper case letter, one lower case letter, and one digit.
- Change the default password and click OK.

► *To change your password via the Change Password command:*

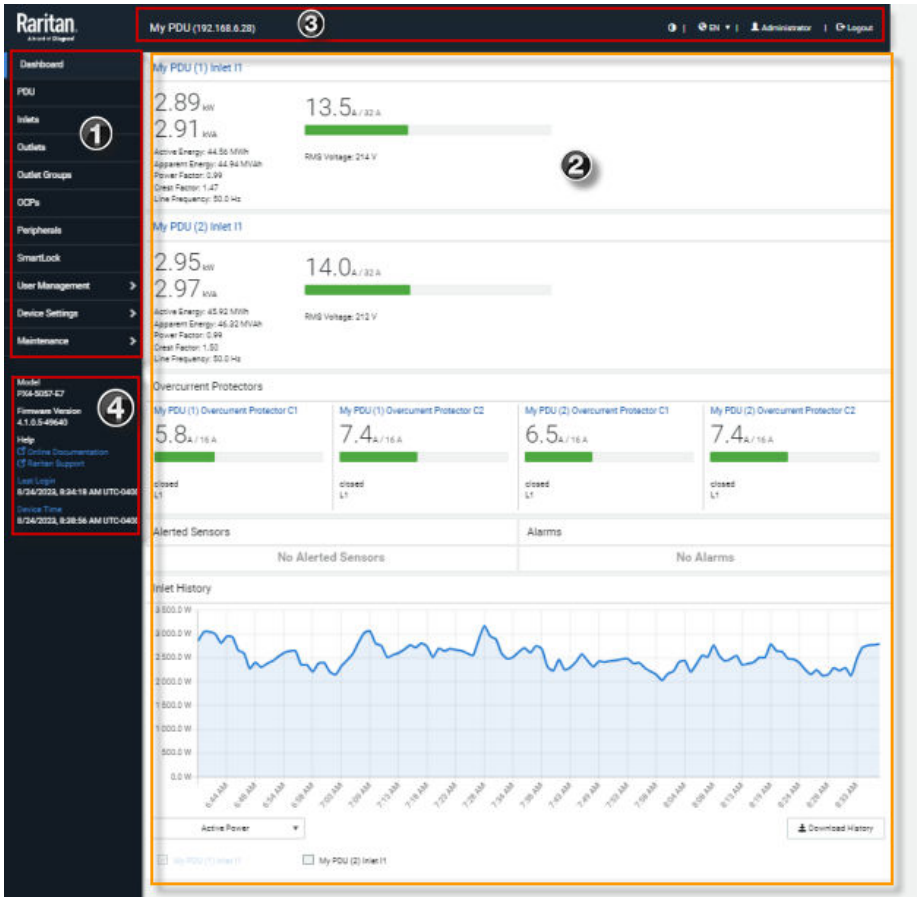
You must have the Change Own Password permission to change your own password.

- Choose User Management > Change Password. Change the password and click Save.



Web Interface Overview

The web interface consists of four areas as shown below.



Number	Web interface element
1	*Menu* - Not all models support all menu options.
2	Data/setup page of the selected menu item.
3	• Left side: - PX4 device name. • Right side: - Displayed language, which is English (EN) by default. You can change it. - Your login name, which you can click to view your user account settings. - Logout button.
4	From top to bottom -- • Your PX4 model. • Current firmware version. • Online Documentation: link to the online help.

Number	Web interface element
	• Support: link to Technical Support. • Date and time of your user account's last login. - Click Last Login to view your login history. • PX4 system time, which is converted to the time zone of your computer or mobile device. - Click Device Time to open the Date/Time setup page.

Menu

Depending on your model and hardware configuration, your PX4 may show all or some menu items shown below.

Menu	Information shown
Dashboard	Summary of the PX4 status, including a list of alerted sensors and alarms, if any.
PDU	Device data and settings, such as the device name and MAC address.
Inlet	Inlet status and settings, such as inlet thresholds.
Outlets	Outlet status, settings and outlet control if your model is outlet-switching capable.
Outlet Groups	Only PDUs with outlet-switching and/or outlet-metering feature show this menu item. You can create groups of outlets. Functions that you can perform on an outlet group vary depending on the model you purchased.
OCPs	The OCPs menu item displays only if your model is equipped with overcurrent protectors. OCP status and settings, such as OCP thresholds.
Peripherals	Status and settings of environmental sensor packages, if connected.
Asset Strip	Status and settings of an Asset Strip, if connected.
Webcams	The Webcams menu is available when a webcam is detected or webcam images have been saved locally. Webcam live snapshots/video and webcam settings.

Menu	Information shown
SmartLock *-- and/or --* Card Readers	The SmartLock and Card Readers menus are available when SmartLock kit is detected. • SmartLock: Configures and controls the door connected to this product via DX2-DH2C2. This page is not available with other door controllers. • Card Readers: Lists the card readers connected directly or indirectly.
User Management	Data and settings of user accounts and groups, such as password change.
Device Settings	Device-related settings, including network, security, system time, event rules and more.
Maintenance	Device information and maintenance commands, such as firmware upgrade, device backup and reset.

Quick Access to a Specific Page

If you often visit a specific page in the PX4 web interface, you can bookmark or share the URL. This allows you to log in directly to the desired page.

Sorting a List

Hover on a column header to see if it is sortable. Click headers that appear as a blue link to sort the list in ascending or descending order based on the selected column.

The arrow is displayed adjacent to the header currently sorted.

ID	Timestamp	Event Class ▲	Event
100	2/26/2022, 4:59:51 AM UTC-0500	Device	The ETH2 network interface link is now up.
101	2/26/2022, 4:59:52 AM UTC-0500	Device	System started.
169	2/26/2022, 5:00:01 AM UTC-0500	Device	[Link Unit 2] System started.
269	3/11/2022, 2:43:34 PM UTC-0500	Device	The ETH2 network interface link is now up.
270	3/11/2022, 2:43:35 PM UTC-0500	Device	System started.
338	3/11/2022, 2:43:44 PM UTC-0500	Device	[Link Unit 2] System started.

Minimum and Maximum Values for Numeric Sensors

You can manually view the minimum and maximum values for each sensor or group of measurements. These values show the last changes before a reset and stay the same after reboots. However, a factory reset will erase them and return settings to default.

Sections where min/max values are available:

Page	Section
PDU	Sensors (if numeric sensors in list)
PDU Sensor Details	Sensor

Page	Section
Inlet Single Phase	Single-phase sensor table
Inlet Multi Phase	Multi phase sensor table
Inlet Detail	Detailed sensor table
Inlet Sensor Details	Sensor
Inlet Residual Current	Detailed sensor table (for multi-phase)
Inlet Residual Current Sensor Details	Sensor
Outlets	List
Outlet	Sensors table
Outlet Sensor Details (numeric sensors only)	Sensor
Inlet/Outlet (single phase)	Single-phase sensor table
Inlet/Outlet (multi phase)	Multi-phase sensor table
Inlet/Outlet (detailed)	Detailed sensor table
Inlet/Outlet Sensor Details (numeric sensors only)	Sensor
Inlet/Outlet Residual Current Sensor Details (numeric sensors only)	Sensor
Outlet Groups	List
Outlet Group	Outlets list and Sensor table
Outlet Group Sensor Details (numeric sensors only)	Sensor
Overcurrent Protectors	List
Overcurrent Protector	Sensors table
Overcurrent Protector Sensor Details (numeric sensors only)	Sensor
Peripheral Devices	List
Peripheral Device Details (numeric sensors only)	Sensor

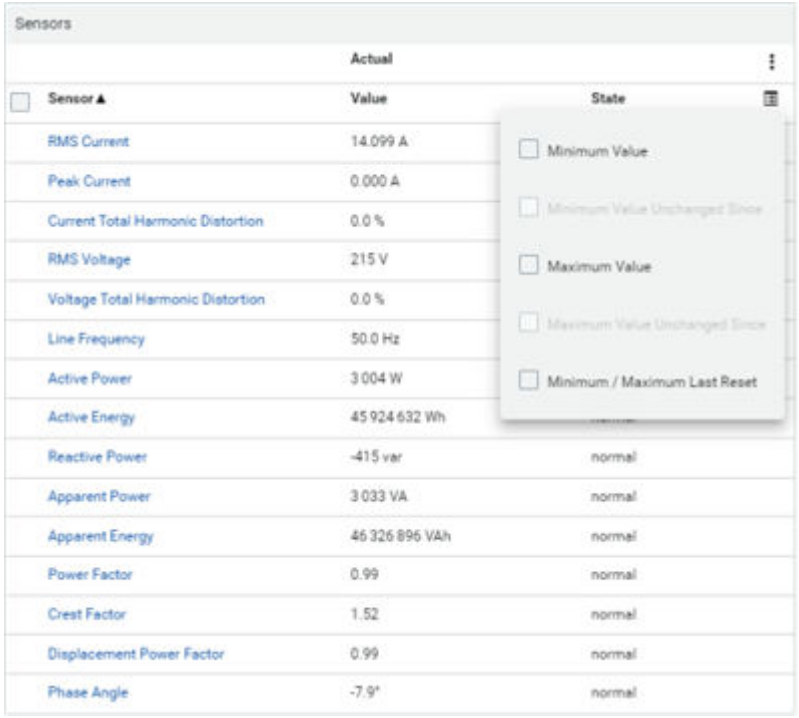
Show and Hide Min/Max Values

You can reset the minimum/maximum values using Web UI.

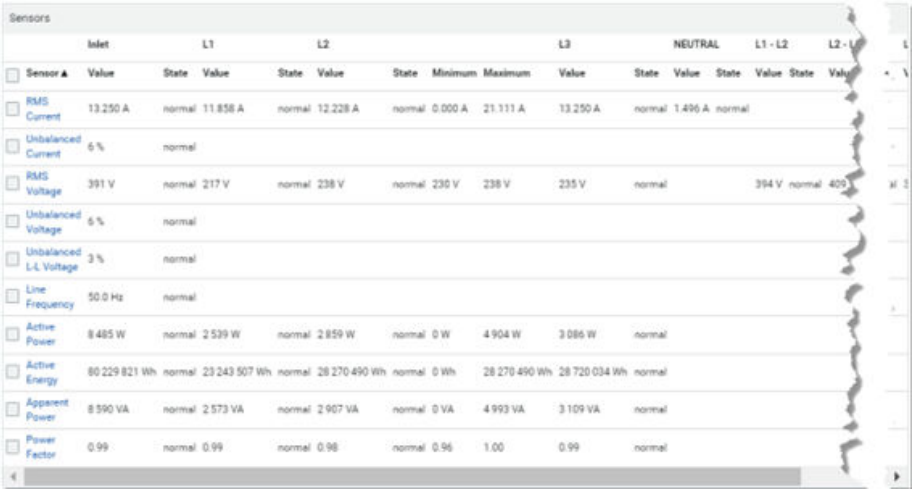
► *To configure the min/max functionality:*

1. Go to the sections of the pages listed in the table of Minimum and Maximum Values for Numeric Sensors (on page 125).
2. Click . Minimum/maximum columns are only selectable if at least one row provides min/max values.
3. Select the check boxes of Minimum and Maximum values.

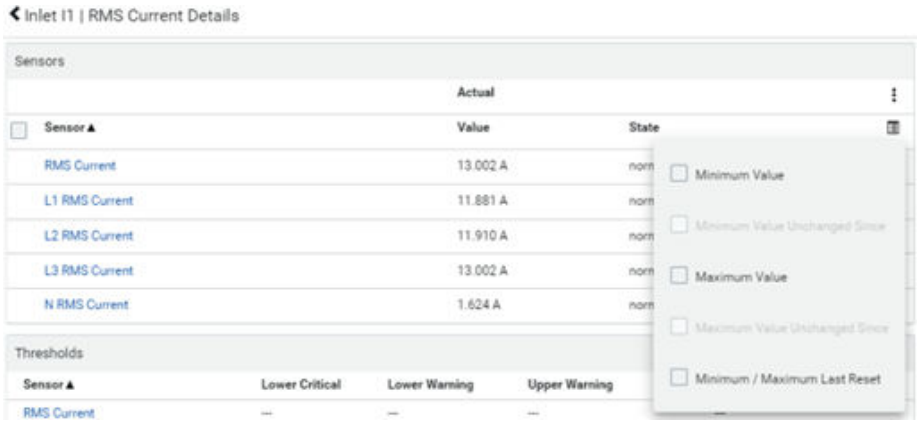
Sensor table single-phase:



Sensor table Multi-phase:



- By default overviews/tables where multiple numeric sensors are listed, min/max values are not displayed.
- You can configure the displayed values, and make min/max values visible. Your configuration is saved and will be available when GUI is reloaded.
- You can configure visible columns of sensor tables including min/max values and on sensor details pages show min/max values.



Raritan
A brand of legrand

► *To reset the min/max values:*

1. Go to the sections of the pages listed in the table of Minimum and Maximum Values for Numeric Sensors (on page 125).
2. Click ⋮. The menu item "Reset Minimum / Maximum" is only visible (active or inactive) if at least one row of the table has min/max values.

Dashboard - PDUs

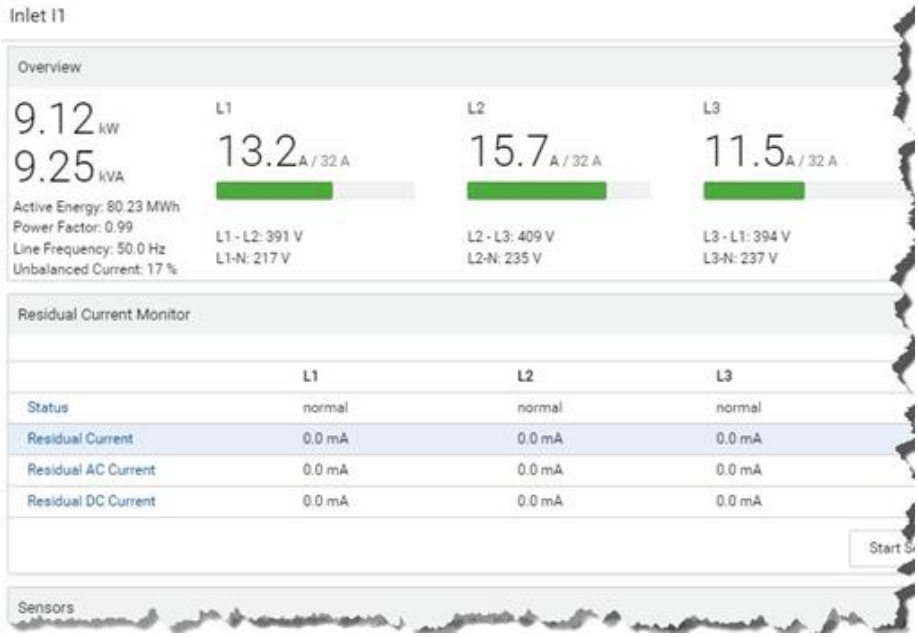
- The Dashboard page gives you an overview of your PX4 in various sections, depending on your model.
- Click any blue hyperlink to go to the main page for that information.
- Not all models have overcurrent protectors.

► *What to look for:*

- All green status bars indicate performance in normal ranges.
- Red or yellow status bars indicate alerts or alarms.
- Check the Alerted Sensors and Alarms sections for any issues that need attention.
- Alarms are listed if there are events that must be acknowledged according to your configurations.
- Alerts are listed when sensor thresholds are entered according to your configurations.

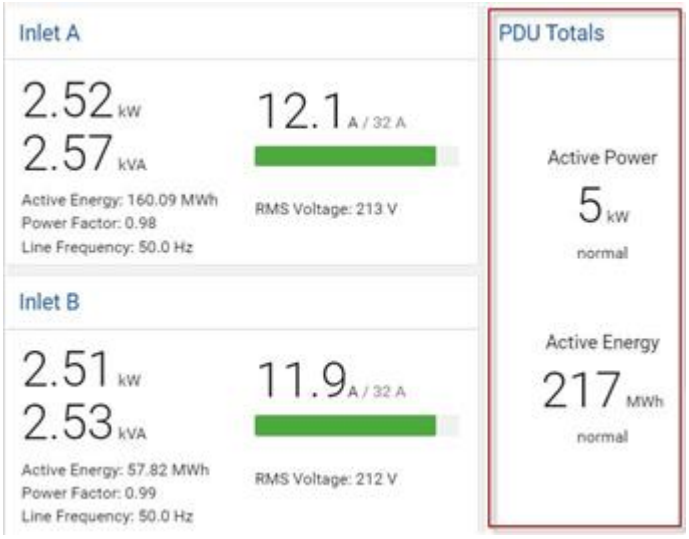
► *What can be customized on the Dashboard?*

- The Inlet History chart at the bottom of the Dashboard shows active power by default.
- Select a different data type to change the chart view temporarily.



► *PDU Totals*

- For multi-inlet models or inline monitors PDU Totals sum up the total active power and active energy.

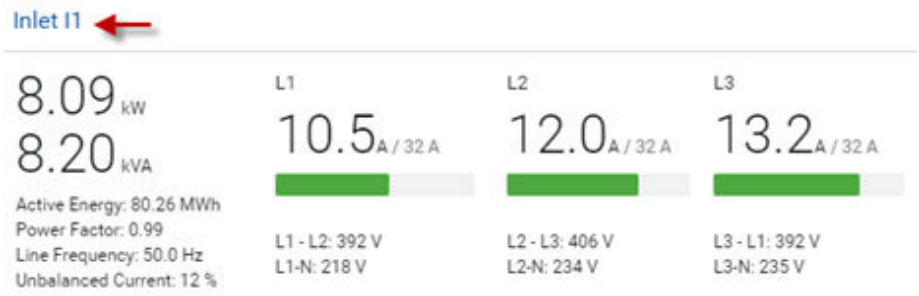


Dashboard - Inlet I1

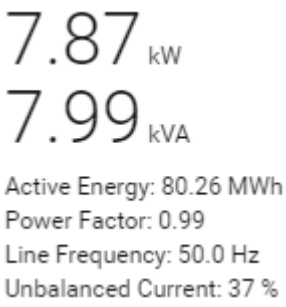
The number of phases shown in the Inlet section is model dependent.

► *Link to the Inlet page:*

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



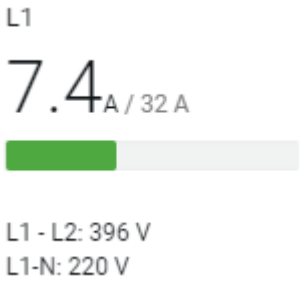
► *Left side - generic inlet power data:*



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

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

► *Right side - inlet's current and voltage:*



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

Inlet data from top to bottom includes:

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

The RMS current bars automatically change colors to indicate the current status according to your configured thresholds. To configure thresholds, see Inlet.

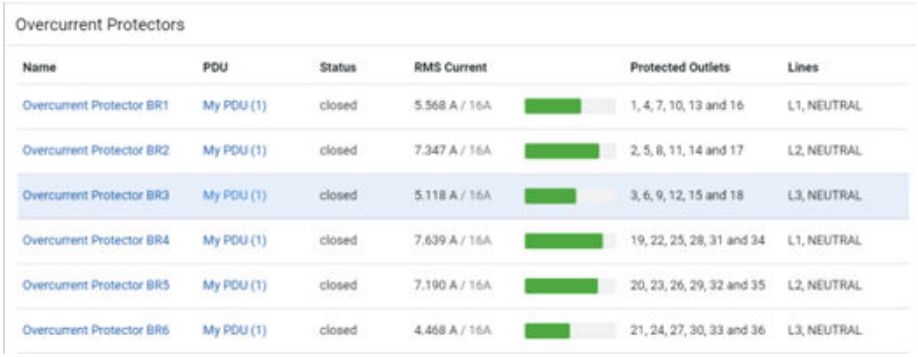
Status	Bar colors
normal	
above upper warning	
above upper critical	

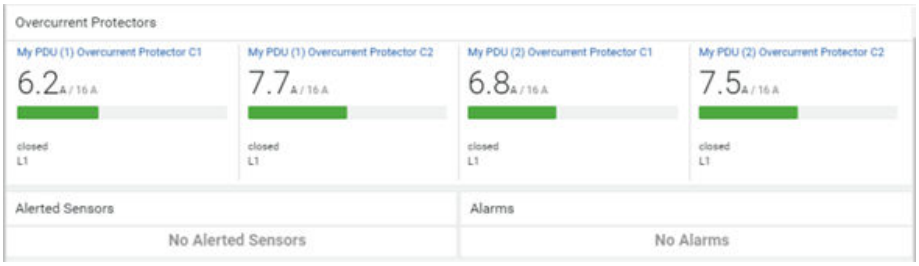
Dashboard - OCP

Availability and total number of OCPs depend on the models.

► *Each OCP's link:*

To view more information or configure individual OCPs, click the desired OCP's index number, which is either BR1, BR2, and so on; or C1, C2 and so on, to go to its setup page.





► *Each OCP's power data:*

OCP data from top to bottom includes:

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

The RMS current bars automatically change colors to indicate the current status according to your configured thresholds. To configure thresholds, see OCPs (on page 180).

Status	Bar colors
normal	
above upper warning	
above upper critical	

Dashboard - Alerted Sensors

When any internal sensors or environmental sensor packages connected to the PX4 enter an abnormal state, the Alerted Sensors section in the Dashboard shows them for alerting users. This section also lists tripped circuit breakers or blown fuses, if available.

To view detailed information or configure each alerted sensor, click each sensor's name to go to individual sensor pages. See Individual Sensor/Actuator Pages (on page 200).

► *Summary in the section title:*

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

For example:

- 1 Critical: 1 sensor enters the critical or alarmed state. 1 Warned: 1 'numeric' sensor enters the warning state.
  - Numeric sensors enter warning or critical states, as their values enter the threshold ranges.
  - State sensors enter an alarmed state.

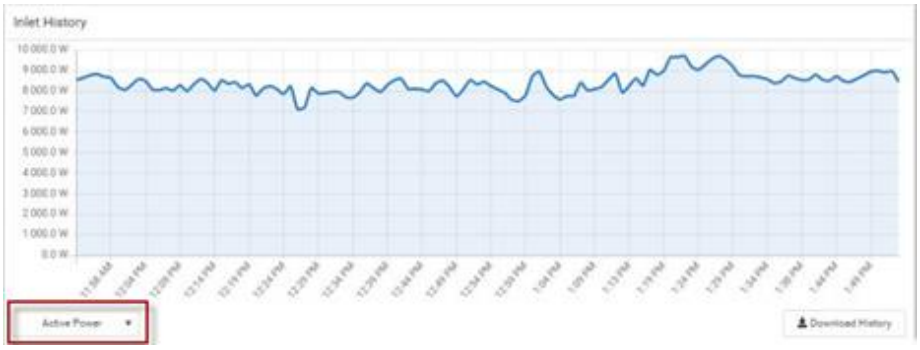
See Sensor/Actuator States (on page 194) for more details.

	Numeric sensors: • Warning
	Numeric sensors: • Critical
	State sensors: • Alarmed state

Raritan
A brand of legrand

Dashboard - Inlet History

- The Inlet History graph displays the history of the sensor values. Select a different data type by clicking the selector below the diagram.



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

ection on multi-inlet models:

If your PDU is a multi-inlet model, you can have one or multiple inlets show their power charts by

selecting the checkbox(es) of the desired inlet(s).

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

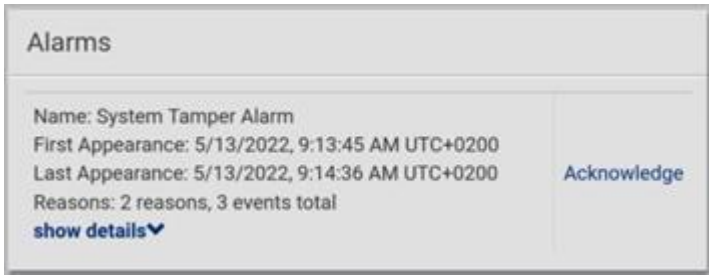
- When both inlets are shown in the chart, simply hover your mouse over either inlet's data line. Both inlets' values display simultaneously, marked with corresponding colors.

Dashboard - Alarms

If configuring any event rules which create or emit device alarms, the Alarms section will list any event that hasn't been acknowledged yet.

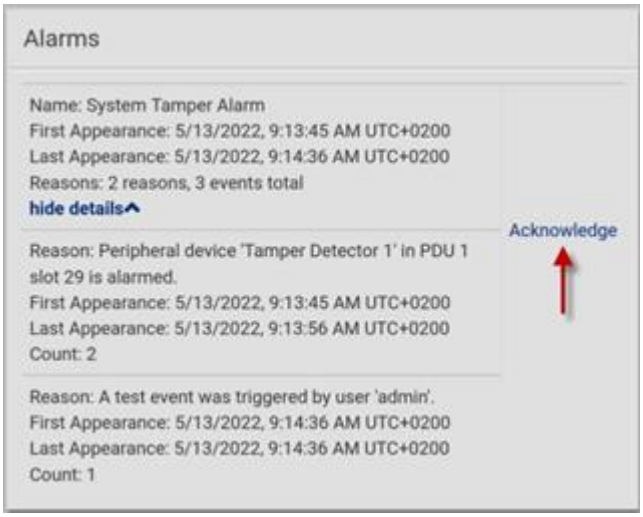
Note: For information on event rules, see Event Rules and Actions (on page 291).

You must have the 'Acknowledge Alarms' permission to manually acknowledge an alarm.



► *To acknowledge an alarm:*

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



This table explains each field of the alarms list.

Field	Description
Name	Custom name of the Alarm action.
Reason	Shows the log message if the alarm was only triggered by one specific event.
Reasons	Short summary if there were multiple different events.
First Appearance	Date and time when the event indicated in the Reason column occurred for the first time.
Last Appearance	Date and time when the event indicated in the Reason column occurred for the last time.

Field	Description
Count	Number of times the event indicated in the Reason column has occurred.
Show details	This field appears only when there are multiple types of events triggering the same alert. If there are other types of events (that is, other reasons) triggering the same alert, the total number of additional reasons is displayed. You can click it to view a list of all events.

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

Tip: You can also acknowledge all alarms in the front panel display.

PDU

Generic information and PDU settings are available on the PDU page.

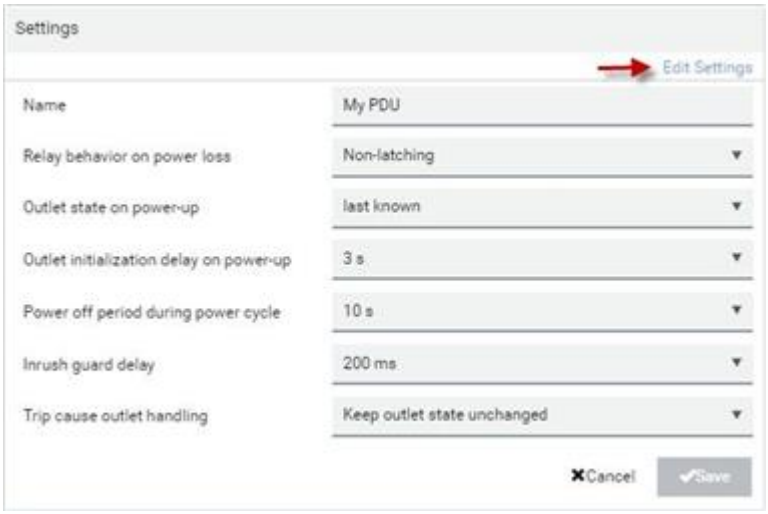
To open the PDU page, click 'PDU' in the Menu.

► *Device information shown:*

- Firmware version
- Serial number
- MAC address
- Rating
- Internal Beeper State
- Status of Power Supply Sensor

► *To configure global settings:*

1. Click Edit Settings.



2. Now you can configure the fields.
   - For time-related fields, you can also type a value manually, making sure to type in a time unit as shown in the drop-down list of values. For example, 30 s for seconds, 30 min for minutes, and so on.

*In the following table, those fields marked with * are available on an outlet-switching capable model only.*

Field	Function	Note
Name	Customizes the device name.	
*Relay behavior on power loss	Selects an operating mode to determine the latching relay behavior when PDU power is lost. • *Options: Non-latching and Latching* • *Non-latching has all relays open at the power loss while latching has all relays remain unchanged at the power loss.*	See Latching Relay Behavior (on page 142). • PXO, PXC and Legrand PDU do not support Latching Relays.
*Outlet state on power up (for non-latching mode only)	Determines the initial power state of ALL outlets after the PX4 powers up. • *Options: on, off, and last known* See Options for Outlet State on Power Up (on page 143)	• After removing power from the PDU, you must wait for a minimum of 10 seconds before powering it up again. Otherwise, the default outlet state settings may not work properly. • You can override the global outlet state setting on a per-outlet basis so specific outlets behave differently on power up. Configure this on the individual outlet page. • This setting works only when 'Relay behavior on power loss' is set to *Non-latching*. This is because all relays keep their states unchanged in the latching mode regardless of the power supply status.

Field	Function	Note
*Outlet initialization delay on power up (for non-latching mode only)	Determines how long the PX4 waits before providing power to all outlets after recovering from a temporary power loss. • *Range: 1 second to 1 hour*	See Initialization Delay Use Cases (on page 144). • This setting works only when 'Relay behavior on power loss' is set to *Non-latching*. This is because all relays keep their states unchanged in the latching mode regardless of the power supply status.
*Power off period during power cycle	Determines the power-off period after the outlet is switched OFF during a power cycle. • *Range: 1 second to 1 hour*	• Power cycling the outlet(s) turns the outlet(s) off and then back on. • You can override this global power cycle setting on a per-outlet basis so specific outlets' power-off period is different.
*Inrush guard delay	Prevents a circuit breaker trip due to inrush current when many devices connected to the PDU are turned on. • *Range: 100 milliseconds to 10 seconds*	See Inrush Current and Inrush Guard Delay (on page 144).
*Trip cause outlet handling	If an outlet is suspected to have caused an OCP trip event, it can optionally be marked as "Suspended" and handled differently. • *Options: Keep outlet state unchanged, or Suspend Outlet*	Suspended outlets are not turned back on when the OCP is closed. See Trip Cause Outlet Handling (on page 144). Not supported on PX2, PXE, and PXO.

1. Click Save.

► *To reset ALL energy counters:*

An energy reading is a value of total accumulated energy, which is never reset, even if the power fails or the PX4 is rebooted. However, you can manually reset this reading to restart the energy accumulation process. Only users with the "Admin" role assigned can reset energy readings.

Note: This reset button does not reset the energy values of outlet groups. Go to the Outlet Groups page to reset that value.

---

1. On the PDU page, in the Settings section, make sure Edit Settings is not clicked, or cancel out of editing settings.
2. On the Reset all energy counters option, click Reset, then click on the confirmation message.
   - All energy readings are reset to zero.

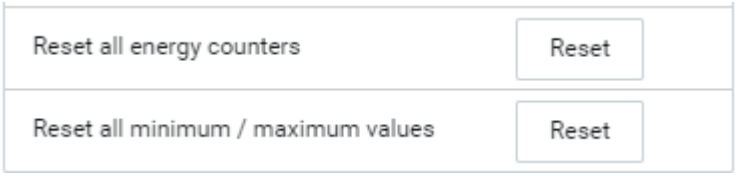
Tip: You can also reset the energy reading of an individual inlet or outlet on those pages.

Raritan
A brand of legrand

► *To reset all minimum/maximum values:*

For readings that record a maximum and minimum numeric value, you can reset these values as needed to clear the previous highs and lows.

1. On the PDU page, in the Settings section, make sure Edit Settings is not clicked, or cancel out of editing settings.
2. On the Reset all minimum/maximum values option, click Reset, then click on the confirmation message.
   - All previously recorded maximum and minimum values are reset.



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

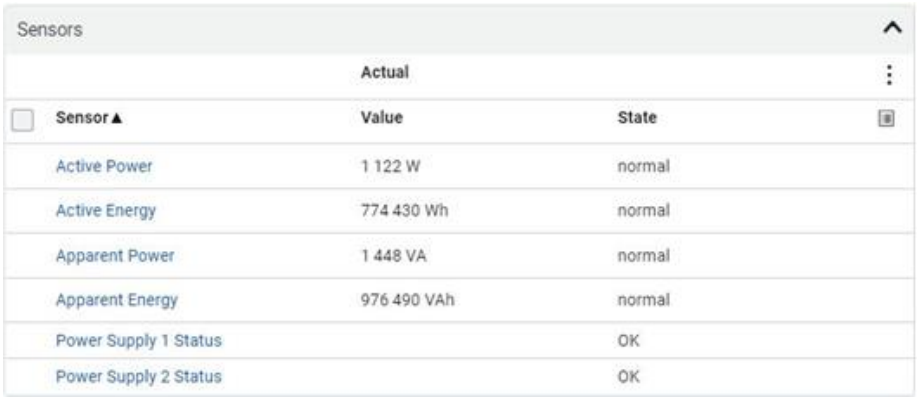
For multi-inlet models or inline monitors, a "Sensors" section show the data of total active energy and total active power."PDU Total" also gives the sum of active power and active energy and it is displayed on the Dashboard.Dashboard - PDUs (on page 129)

For a regular model with multiple inlets:

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

For an inline monitor with multiple inlets/outlets:

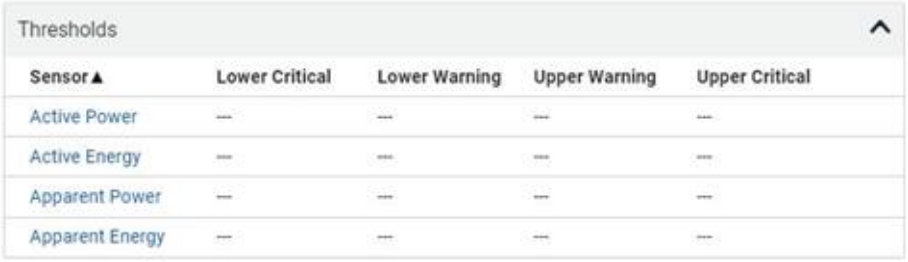
- Total active energy = sum of all outlets' energy values
- Total active power = sum of all outlets' active power values



► *To configure the thresholds of total energy and power:*

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

See Setting Thresholds for Total Active Energy or Power (on page 145)



Latching Relay Behavior

Unlike non-latching relays, latching relays retain their last position (open or closed) without requiring continuous power. In latching mode, they preserve their status during power outages, allowing the load to be instantly powered when power is restored.

Supported models allow outlet switching to be configured as either a true latching relay or a simulated non-latching relay. The selected operating mode defines how the latching relay behaves during a power outage. Regardless of the mode, relays do not require power to maintain their state.

► *Non-Latching Mode:*

- Relay always opens when power is lost. This insures all relays are open when power is applied to the PDU.
- Always select this mode if the combined inrush current of the devices connected to the PDU trip circuit breakers when power is applied to the PDU.
- This is the factory default operating mode.

► *Latching Mode:*

- Preserve the relay state when power is lost.
- This is the preferred operating mode ONLY if you are sure inrush current does not trip circuit breakers when power is applied to the PDU.
- Power to the outlet is not disrupted if a PDU internal failure occurs.

In latching mode, the following features are disabled.

On PDU page in Settings section:

- Outlet state on startup = last known
- Outlet initialization delay on device startup = 1sec

On Individual outlet page:

- State on device startup = PDU defined (last known)

► *Non-Latching Relay Behavior on Power-Up*

When outlets start receiving power (be it on PDU power up after power cycle, when turning on an inlet in a multi-inlet PDU or when a transfer switch switches back on after being off for some time), relays are initialized to a state configurable per outlet:

- Leave outlet switched off after power-up
- Switch outlet on after power-up
- Restore outlet to last known state (default)

Note: PDU reboot, firmware update, and factory reset does not affect relay states.

Options for Outlet State on Power Up

The following are available options for initial power states of outlets after powering up the PX4 device. This setting is used in three scenarios:

- powering up the whole PDU
- powering up a single inlet in a multi-inlet PDU (on most, but not all, multi-inlet units the outlet boards are powered through the respective inlet)
- transfer switch switches on again after being off due to e.g. internal failure

Option	Function
on	Turns on the outlet(s).
off	Turns off the outlet(s).
last known	Restores the outlet(s) to the previous power state(s) before the PX4 was powered off.

When configuring an individual outlet, there is one more outlet state option.

Additional option	Function
PDU defined (on/off/last-known)	Follows the global outlet state setting, which is set on the PDU page. The value in parentheses is the currently-selected global option.

Initialization Delay Use Cases

Apply the initialization delay in either of the following scenarios.

- When power may not initially be stable after being restored
- When UPS batteries may be charging

Tip: When there are a large number of outlets, set the value to a smaller number to avoid a long wait before all outlets are available.

Inrush Current and Inrush Guard Delay

► *Inrush current:*

When electrical devices are turned on, they can initially draw a very large current known as inrush current. Inrush current typically lasts for 20-40 milliseconds.

► *Inrush guard delay:*

The inrush guard delay prevents circuit breaker trips caused by the high inrush current when multiple devices are turned on together.

For example, with a 100-millisecond delay, the PDU turns outlets on one by one, with a 100-millisecond gap between each.

Trip Cause Outlet Handling

When an outlet has been suspected as the cause of a trip, the Trip Cause Outlet Handling setting allows you to mark the outlet as Suspended.

A Suspended outlet is handled differently than usual:

- once the respective OCP is closed, the outlet is not turned on again
- outlet state shows as 'suspended' in the web interface and the CLI
- warnings are shown when you attempt to turn on a suspended outlet
- for supported models, a different outlet LED color is shown

Time Units

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

Note that different fields have different range of valid values.

► *Time units:*

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

Setting Thresholds for Total Active Energy or Power

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

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

For a regular PX4 model with multiple inlets:

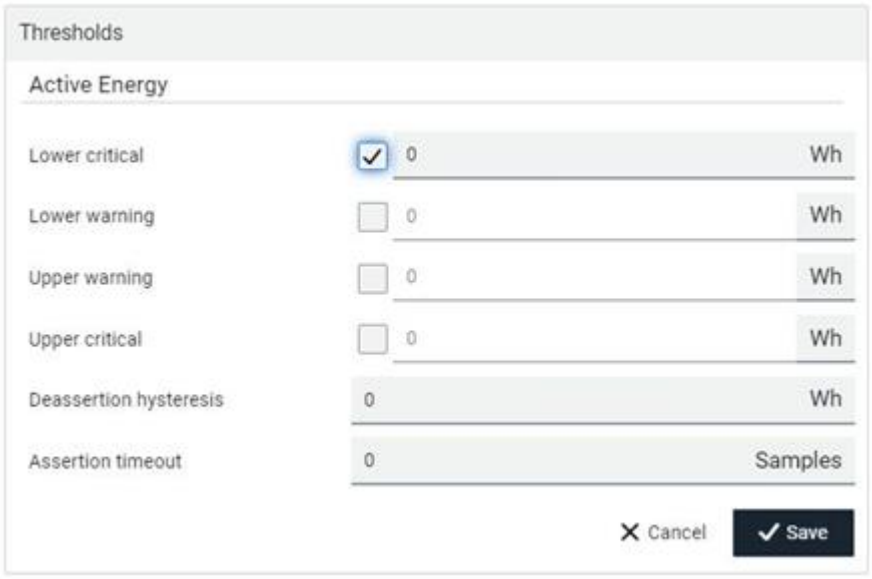
- Total active energy = sum of all inlets' active energy values
- Total active power = sum of all inlets' active power values

For an inline monitor with multiple inlets/outlets:

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

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

1. Click PDU.
2. Click the Thresholds title bar at the bottom of the page to display thresholds.
3. Click a sensor to edit the thresholds.
4. Make changes as needed.
   - To enable any threshold, select the corresponding checkbox.
   - Type a new value in the accompanying text box.

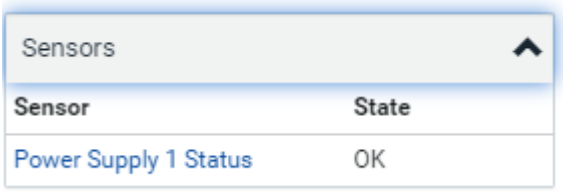


5. Click Save.

Power Supply Sensor

The PX4's controller receives power from its inlet. A sensor monitors the power supply status and indicates it on the PDU page.

This status is also available on the PDU's front panel display, or via the CLI with the command: `show pdu details`.



State	Description
OK	The controller is receiving power from its own inlet.
fault	The controller cannot receive power from its own inlet because of a power failure on the inlet or a broken power supply. Instead it is receiving power from another PX4 PDU. See Power-Sharing Restrictions and Connection (on page 36). After entering the fault state, this sensor is listed in the Alerted Sensors section of the Dashboard. .
unavailable	The communication with the power supply sensor is lost.

Inlet

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

Inlet thresholds help you identify when your inlet enters warning or critical level. In addition, you can automatically generate alert notifications for any warning or critical status. See Event Rules and Actions (on page 291).

Note: For multi-inlet models, see Configuring a Multi-Inlet Model (on page 153).

► *Overview:*

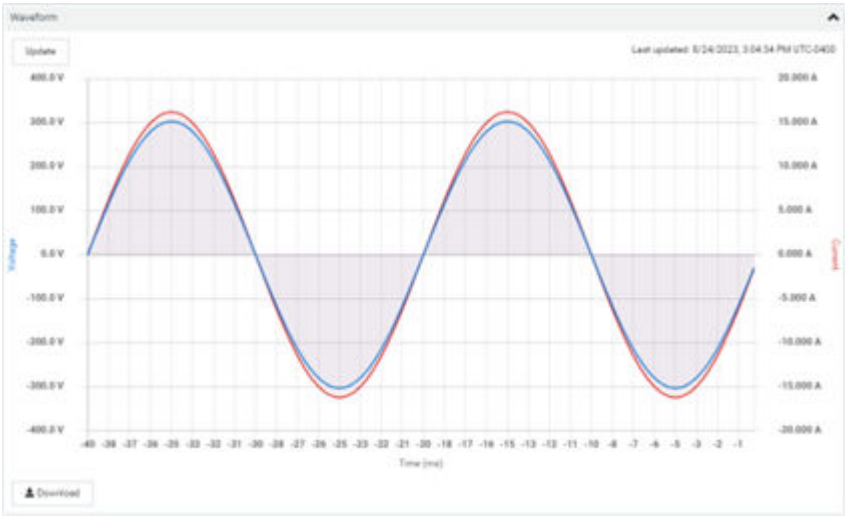
- Inlet power overview, which is the same as Dashboard - Inlet I1 (on page 130).

► *Dip/Swell Events:*

Dip/swell Events provides monitoring for short-term under-voltage events, also known as "Dips", and short-term over-voltage events, also known as "Swells".

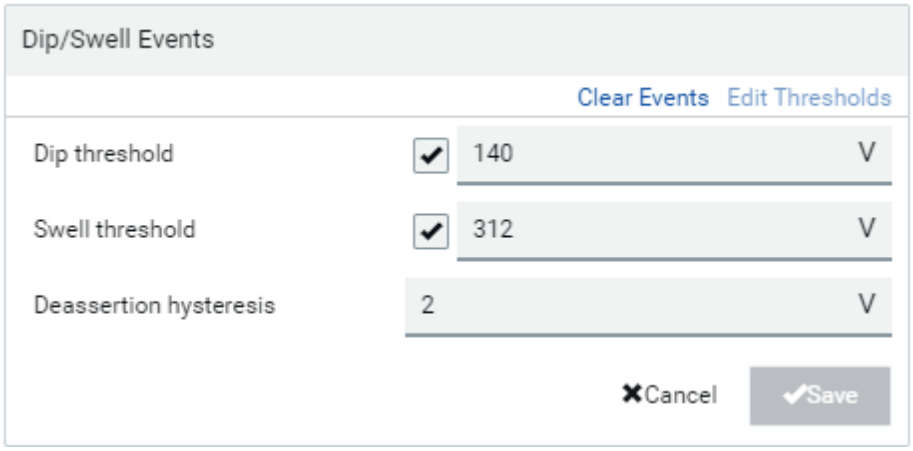
After configuring the thresholds for dips and swells, a waveform is captured when an event meets the thresholds.

► *Dip/Swell Event Waveform Example:*



► *To configure dip/swell thresholds:*

1. On the Inlet page, click Edit Thresholds in the Dip/Swell section to enable the form.
2. Dip threshold: Select the checkbox to enable the threshold. Enter a voltage value. The default is set to enabled, and the value is relative to the inlet's voltage rating.
3. Swell threshold: Select the checkbox to enable the threshold. Enter a voltage value. The default is set to enabled, and the value is relative to the inlet's voltage rating.
4. Deassertion hysteresis: Enter a value for deassertion hysteresis. The default is set to 2.
5. Click Save.



► *Sensors:*

The sensors section contains a list of inlet sensors with more details. Available inlet sensors depends on the model. Sensors show both readings and states. Sensors in warning or critical states are highlighted in yellow or red. PX4 includes total harmonic distortion (THD) monitoring for all three phases and line pairs, along with other enhanced power metrics. These features allow for real-time visibility, reporting, and alerting of power quality issues. The inlet power chart shows the selected sensor, and is the same information as found in the Dashboard - Inlet History.

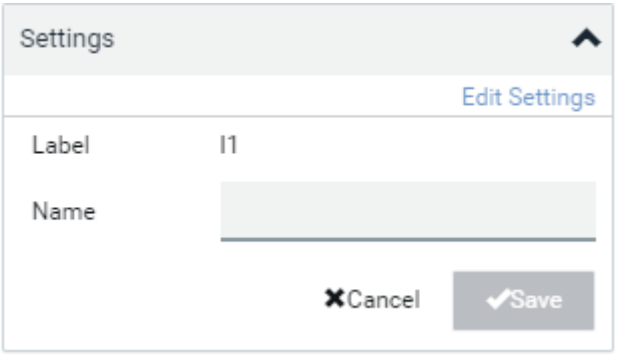
- Complete list of inlet power sensors:
  - RMS Current
  - Peak Current
  - Unbalanced Current
  - Current Total Harmonic Distortion
  - RMS Voltage
  - Unbalanced Voltage
  - Unbalanced L-L Voltage
  - Voltage Total Harmonic Distortion
  - Line Frequency
  - Active Power
  - Active Energy
  - Reactive Power
  - Apparent Power
  - Apparent Energy
  - Power Factor

- Crest Factor
- Displacement Power Factor
- Phase Angle

► *Settings--Name the inlet:*

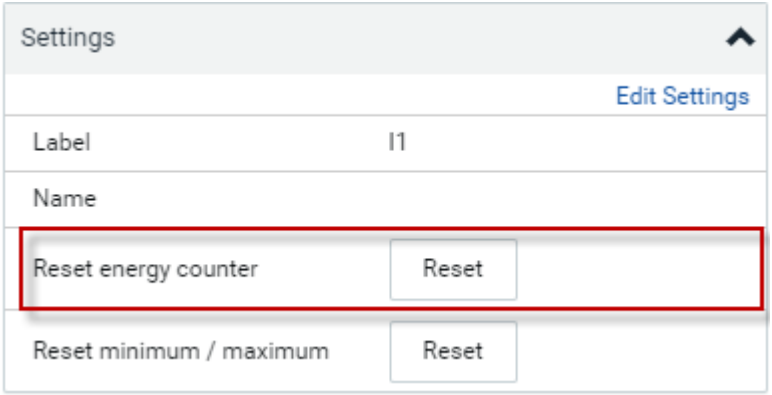
Scroll down past the Sensor list to the Settings.

- Click Edit Settings, enter a name for the inlet, then click Save. For example, name the inlet after the power source.
- The inlet's custom name is displayed on the Inlet or Dashboard page, followed by its label in parentheses.



► *Settings--Reset energy counter:*

The energy counter reset feature per inlet is especially useful when your PX4 has more than one inlet. Only users with the "Admin" role assigned can reset this value.



- Click Reset and then confirm in the message.
  This inlet's active energy reading is then reset to zero.

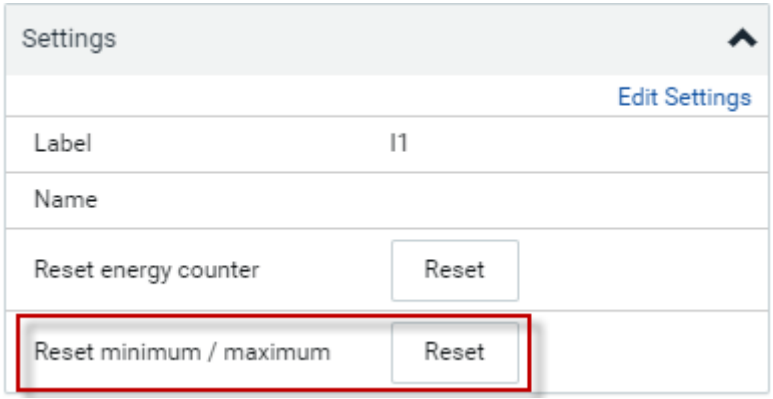
Tip: To reset ALL active energy counters on the PX4, go to the PDU page.

► *Settings: Reset minimum/maximum:*

All inlet sensors with numeric readings store their minimum and maximum recorded reading. You can reset these as desired. Only users with the "Admin" role assigned can reset this value.

Tip: To enable the display of minimum/maximum for any sensor, click the Options icon at the top right of the Sensors lists.

- Click Reset and then confirm in the message.
  This inlet's sensor's minimum and max values are reset.



► *Waveform:*

In addition to the waveforms captured automatically on OCP trip events, dip/swell events, and relay switch-on events, you can generate a waveform capture whenever you require on the inlet page. For three-phase inlets, you can select a phase to generate the waveform. Waveforms created manually represent only the moment in which they are created. Refreshing the browser removes the waveform image.

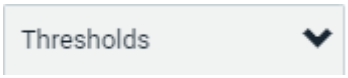
► *To manually capture a waveform:*

1. On the Inlet page, scroll down to the Waveform section.
2. Click Update to generate the waveform.
   - For three-phase inlets, you can also select a phase from the L1 - L2 - L3 drop-down list, then click Update to generate the waveform per line.
   - Hover your mouse over the waveform to view individual data points.

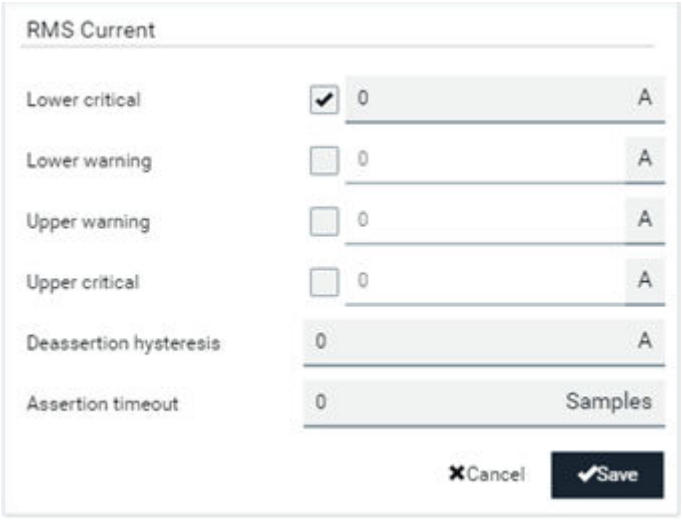
► *To configure inlet thresholds:*

By default, there are predefined RMS voltage and current threshold values in related fields. You can modify them to meet your needs.

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



2. Click the desired sensor to open the settings.
3. To enable a threshold, select the corresponding checkbox.
4. Type a new value in the accompanying text box.



► *Residual Current Monitor--Configure residual current thresholds:*

If your model supports residual current monitoring, a section titled "Residual Current Monitor" is displayed on the Inlet page. See Web Interface Operations for RCM.

Configuring a Multi-Inlet Model

If the PX4 has more than one inlet, the Inlets page lists all inlets.

► *To view or configure each inlet:*

1. Click the desired inlet.

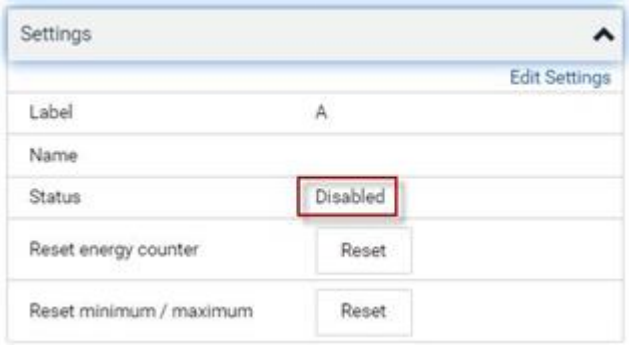
2. Now you can configure the selected inlet, such as enabling thresholds or resetting its energy.
   - To disable the inlet, see the following instructions.

► *To disable one or multiple inlets:*

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

2. Select the "Disable this inlet" checkbox.
3. Click Save.

4. The inlet status now shows "Disabled."



5. To disable additional inlets, repeat the above steps. If disabling one inlet causes all inlets to be disabled, a confirmation message will appear.
6. Click "Yes" to confirm or "No" to cancel the operation.

After disabling any inlet, several critical monitoring and control functions are affected:

- Electrical components powered by the disabled inlet will not report any events or alarms.
- Any remote switching capability for connected outlets will be deactivated.
- Power metering functions will also stop operating.
- Sensors continue accumulating data, even though control functions are disabled.
- Threshold-based alerts (for example, high power consumption) will not trigger warnings or notifications. The system does not flag abnormal conditions associated with the disabled inlet.

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

Outlets

The Outlets page shows a list of all outlets and the overview of outlet status and data. To open this page, click 'Outlets' in the *Menu*.

On this page, you can:

- View all outlets' status.

  Outlets above or below thresholds are highlighted in yellow or red.
- Perform actions on all or multiple outlets simultaneously with setup/power-control commands on the top-right corner.

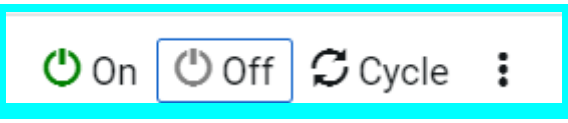
  Only outlet-switching capable models show the power-control buttons, and you must have the Switch Outlet permission to perform outlet-switching operations.

  Select an outlet checkbox to enable the power control commands.

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

► *To power control:*

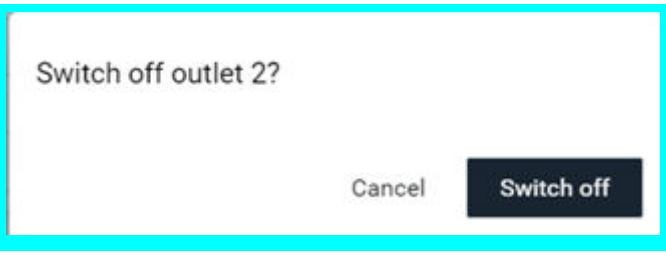
1. Select the checkboxes of the outlets you want to control.
2. Click the power control command.



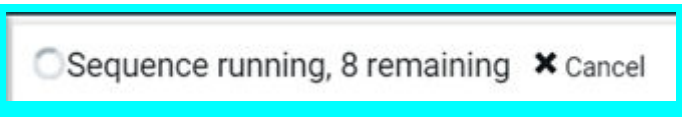
Raritan
A brand of legrand

- On: Power ON
- Off: Power OFF
- Cycle: Power cycle turns outlet OFF then back ON

3. A confirmation message appears. Click to confirm, or cancel

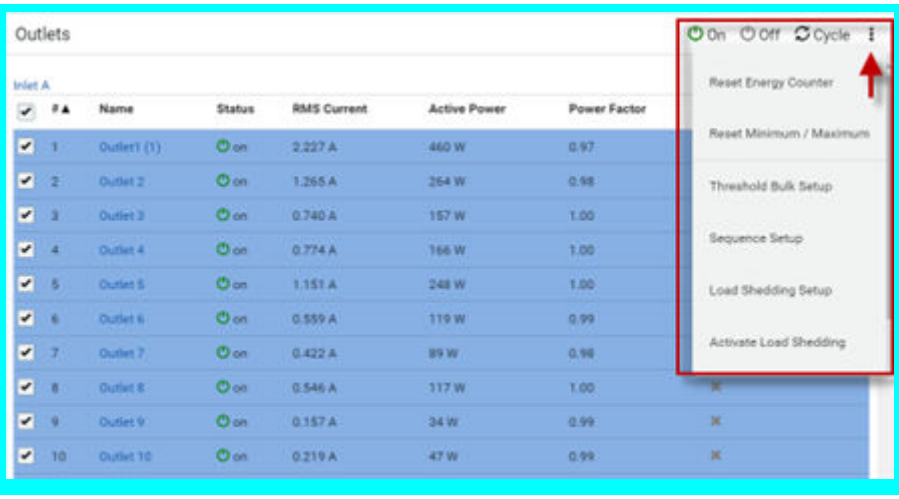


4. A 'Sequence running' message may appear while the outlet-switching process finishes. Click Cancel to interrupt the process if needed.



► *To reset Energy Counter or Minimum/Maximum Readings:*

- Available on models with outlet-metering



1. Select the checkboxes of the outlets you want to reset.
2. Click the Three Dots options icon, then select a reset option:
   - Reset Energy Counter: You must have the Admin role. Resets the active energy readings for the selected outlets.
   - Reset Minimum/Maximum: Resets the minimum and maximum recorded values for power sensors for the selected outlets.
3. Confirm the operation when prompted.

► *To configure global outlet settings or perform the load-shedding command:*

1. Click ⋮ to show a list of commands.
2. Select the desired command.

Only outlet-switching capable models have the commands marked with * in the table.

Command	Refer to
Threshold Bulk Setup	Threshold Bulk Setup (on page 159)
*Sequence Setup	Sequence Setup (on page 162)
*Load Shedding Setup	Load Shedding Setup: Setting Non-Critical Outlets (on page 164)
*Activate Load Shedding -- OR-- Deactivate Load Shedding	Load Shedding Mode: Activate or Deactivate (on page 165)

Important: In power control operations, even if the outlet is off, there may still be live voltage present. To avoid electrical shock, never touch the metal contacts of an outlet, regardless of whether it is on or off.

Delta models only cut off one of the two power phases. So there can still be a dangerous voltage present between the other phase and the protective earth (PE) connection.

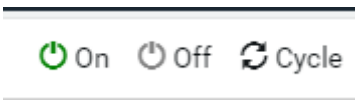
In Wye or single-phase PX3 models, switching off an outlet disconnects the neutral line. However, a live voltage can still exist between the phase and protective earth (PE) connections.

See Safety Instructions (on page 13) for miore details.

Available Data of the Outlets Overview Page

To show or hide outlet data columns, click the columns icon.

- Status: Outlet status, shown with color icon. Available on outlet-switching capable models only.



- RMS current (A)
- Active power (W)
- Power Factor

- Crest Factor
- Non-Critical: Outlet-switching capable models only. Non-Critical outlets display a green checkmark. Critical outlets display a gray X.

- Lines
- Outlet Groups: if the outlet is part of a group, the outlet group name appears as a link.

Threshold Bulk Setup

Enable outlet thresholds to monitor if an outlet reaches warning or critical levels. You can set up automatic alerts for these conditions. The Outlets page lets you configure thresholds for multiple or all outlets at once. By default, RMS voltage and current threshold values are already pre-set in the related fields. See Default Voltage and Current Thresholds (on page 160), Default Voltage and Current Thresholds (on page 711).

Available on models with outlet-metering.

► *To configure thresholds-related settings for multiple outlets:*

1. On the Outlets page, click ⋮ > Threshold Bulk Setup.
2. In the "Show Outlet Sensors of Type" field, select a sensor type.
3. In the "For Outlets of Receptacle Type" field, select an outlet type.
4. Select the checkboxes of the outlets you want to configure.

5. Click the Edit Thresholds link.
6. Make changes as needed.
   - To enable any threshold, select the corresponding checkbox.
   - Type a new value in the accompanying text box.

7. Click Save.

Default Voltage and Current Thresholds

The following are factory-default voltage and current thresholds. There are no default values set for *lower* current thresholds because lower thresholds are not useful.

Availability of diverse thresholds depends on the capability of the model you purchased.

► *Single-phase inlets or outlets:*

- RMS voltage:

Threshold	Default value
Lower critical	-6% of minimum rating
Lower warning	-3% of minimum rating
Upper warning	+3% of maximum rating
Upper critical	+6% of maximum rating
Hysteresis	2V

- RMS current:

Threshold	Default value
Upper warning	65% of rating

Threshold	Default value
Upper critical	80% of rating
Hysteresis	1A

► *Multi-phase inlets or outlets:*

- Line-Line RMS voltage:

Threshold	Default value
Lower critical	-6% of minimum rating
Lower warning	-3% of minimum rating
Upper warning	+3% of maximum rating
Upper critical	+6% of maximum rating
Hysteresis	2V

- Line RMS current:

Threshold	Default value
Upper warning	65% of rating
Upper critical	80% of rating
Hysteresis	1A

- Unbalanced current:

Threshold	Default value
Upper critical	10% -- disabled by default
Upper warning	5% -- disabled by default
Hysteresis	2%

► *Overcurrent protectors which aims to protect the PDU's outlets:*

- OCP RMS current:

Threshold	Default value
Upper critical	80% of OCP rating
Upper warning	65% of OCP rating

Threshold	Default value
Hysteresis	1A

► *Total residual current:*

Threshold	***Default value***
Upper critical	***30mA***
Hysteresis	***15mA***

Sequence Setup

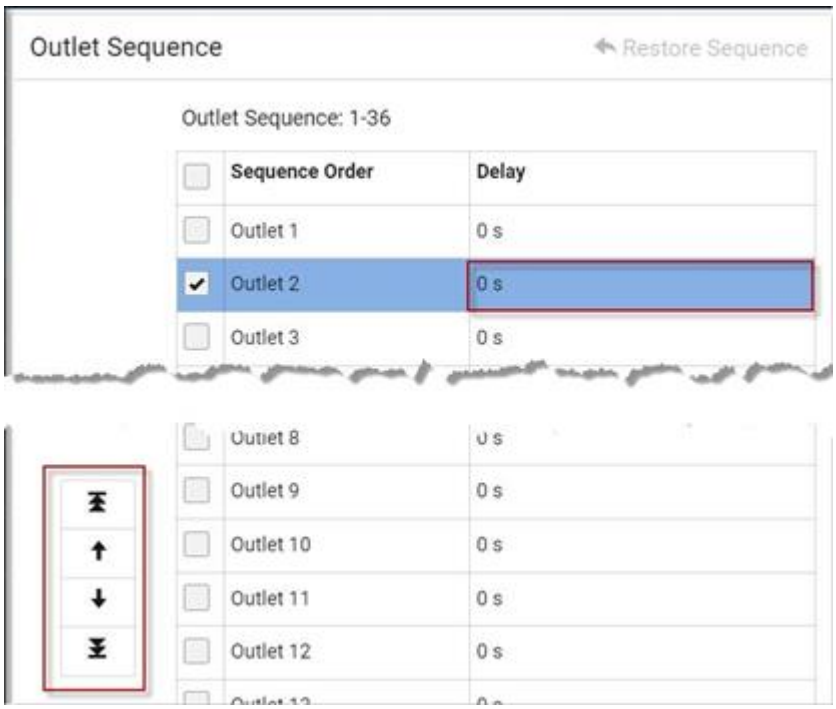
By default, outlets power on sequentially from outlet 1 to the last when turning on or cycling power for all outlets. You can customize the order to prioritize specific IT equipment that needs to start up first.

You can set a delay between outlets when they are turned on consecutively. For instance, if outlets power on from 1 to 8, and you want a 5-second pause before turning on Outlet 4 after Outlet 3, just assign a 5-second delay to Outlet 3.

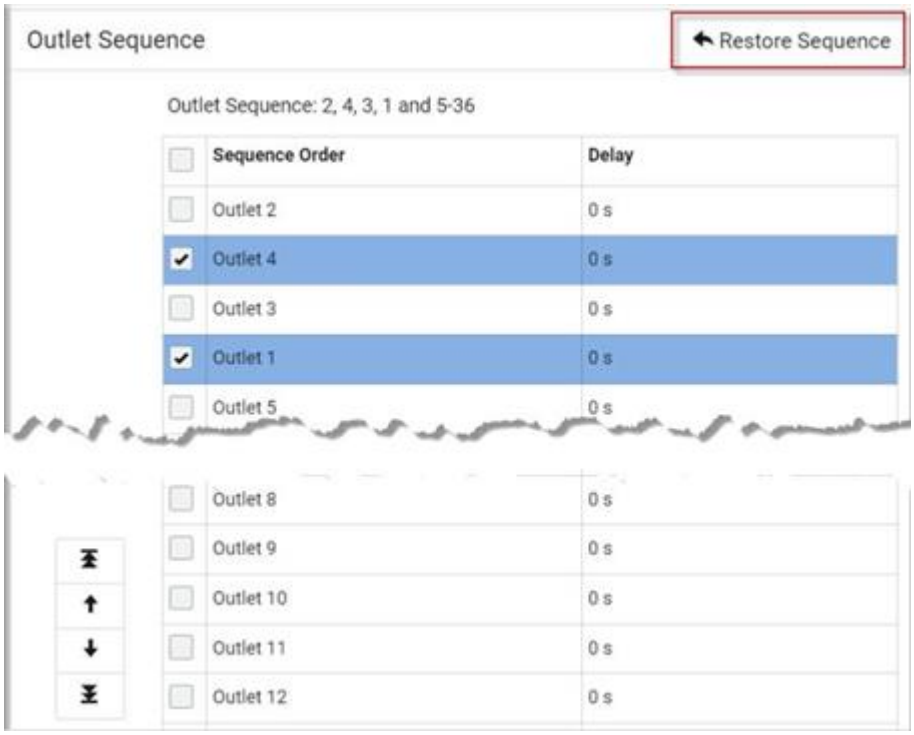
► *To set the outlet power-on sequence and delay:*

1. On the Outlets page, click ⋮ > Sequence Setup.
2. Select one or multiple outlets by clicking them one by one in the 'Outlet' column.
3. Click the arrow buttons to change the outlet positions.

4. Click the 'Delay' column of the outlet that requires a wait after it is turned on.
5. Type a new value in seconds.
6. Click Save.



To change the order of outlets in the sequence, select the outlet and then click the up or down arrow buttons to reorder them as needed. If you need to reset the order click on Restore sequence.



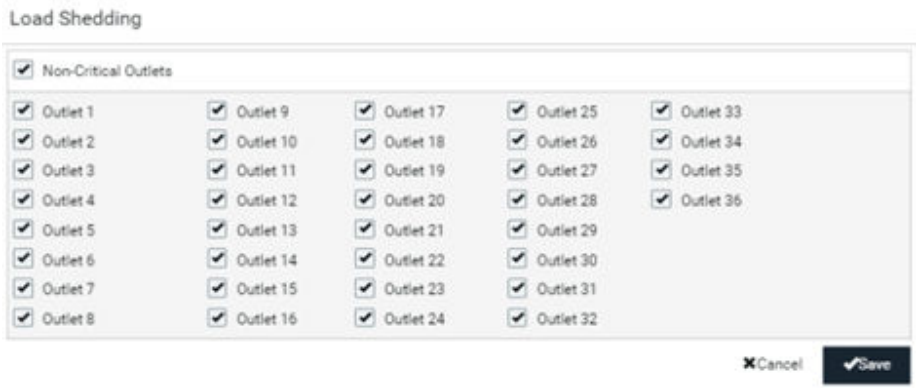
Load Shedding Setup: Setting Non-Critical Outlets

Outlets that are turned off when load shedding is activated are called non-critical outlets. Outlets that are not affected by load shedding are called critical outlets.

Per default, all outlets are configured as critical.

► *To determine critical and non-critical outlets:*

1. On the Outlets page, click ⋮ > Load Shedding Setup.
2. To set non-critical outlets, select the checkboxes of those you want. Or, select the Non-Critical Outlets checkbox to set all outlets as non-critical.
3. To turn non-critical outlets into critical ones, deselect their checkboxes.
4. Click Save.



Load Shedding Mode: Activate or Deactivate

Load shedding isn't available on all models. When a UPS supplying power to PX4 switches to battery backup, you can save battery life by turning off non-critical outlets. This process is called load shedding.

During load shedding, non-critical outlets are turned off while critical outlets remain unaffected. By default, all outlets are considered critical. When load shedding starts, PX4 switches off non-critical outlets, and when it stops, PX4 turns back on the non-critical outlets that were previously on.

Exception: If you once manually perform switch-off operation on any non-critical outlets during the load shedding mode, those outlets will NOT be turned back on when exiting the load shedding mode.

Activation of load shedding can be accomplished using the web interface, SNMP or CLI, or triggered by the contact closure sensors.

Tip: It is better to check non-critical outlets prior to manually entering the load shedding mode. The non-critical information can be retrieved from the Outlets page.

You must have one of the following permissions to perform the load shedding commands.

- 'Change Pdu, Inlet, Outlet & Overcurrent Protector Configuration'
- 'Switch Outlet' permission for all non-critical outlets
- Administrative privileges

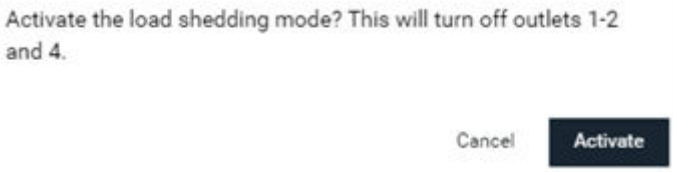
► *To activate load shedding mode:*

1. On the Outlets page, click ⋮ > Activate Load Shedding.

Note: If the command is not available, check your permissions, especially whether you have the Switch Outlet permission for ALL noncritical outlets.

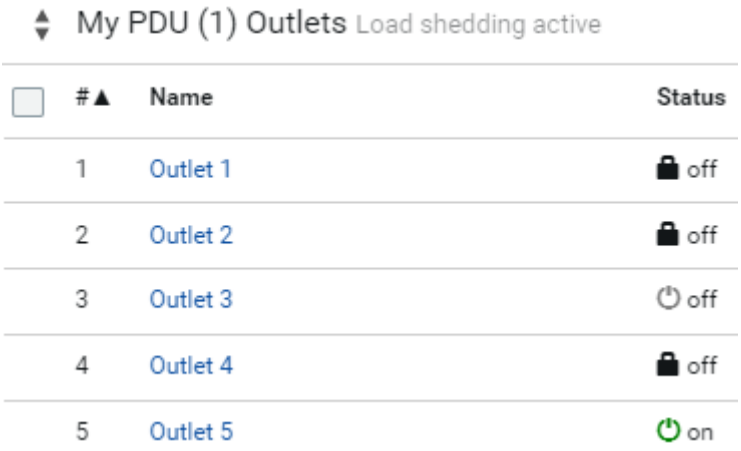
---

2. Click Activate on the confirmation message.



In the load shedding mode:

- You CANNOT power on any "non-critical" outlets. Note the Lock icon displays for these outlets.



- The lock icon appears for "non-critical" outlets that WILL be automatically powered on when deactivating the load shedding mode.
- The off icon appears for outlets, critical or non-critical, that WILL NOT be automatically powered on when deactivating the load shedding mode.

Tip: If you manually perform any power operations on non-critical outlets during the load shedding mode, the icons vary. See Off and Lock Icons for Outlets (on page 167).

- The message "Load shedding active" appears next to the 'Outlets' title.
- If the Non-Critical column was hidden, it automatically is shown when load shedding mode is activated.

► *To deactivate load shedding mode:*

1. On the Outlets page, click > Deactivate Load Shedding.
2. Click Deactivate on the confirmation message.

Now you can turn on/off any outlets.

► *TIP -- automatic load shedding via contact closure sensors:*

If you have connected a contact closure sensor, you can set up an event rule in a manner that this sensor's status change automatically activates or deactivates the load shedding mode. See Sample Environmental-Sensor-Level Event Rule (on page 341).

Off and Lock Icons for Outlets

This section further explains the following two icons for outlets, which display in the load shedding mode.

- Lock icon : It means the outlet WILL be automatically powered on after deactivating the load shedding mode.
- Off icon : It means the outlet will remain powered OFF when deactivating the load shedding mode.

► *Which outlets show the lock icon* *:*

- Non-critical outlets that were powered ON prior to the load shedding mode
- Non-critical outlets that you manually switch on during the load shedding mode

Note: The switching-on operation does not power on the selected non-critical outlets while the load shedding mode is active, but will cause those outlets to be automatically turned on after disabling the load shedding mode.

► *Which outlets show the Off icon* *:*

- Any outlets, critical or non-critical, that were powered OFF prior to the load shedding mode
- Any outlets, critical or non-critical, that you manually switch off during the load shedding mode

Individual Outlet Pages

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

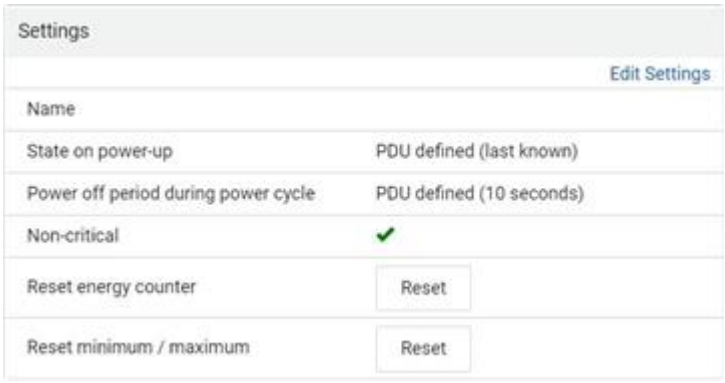
The individual outlet's page shows this outlet's detailed information. See Detailed Information on Outlet Pages.

► *To control power:*

On outlet-switching capable models, you can control power on the individual outlet page using power control buttons just like the main Outlets page. You must have the Switch Outlet permission to perform outlet-switching operations.

► *To configure this outlet:*

1. Click Edit Settings.



2. Configure available fields. Note that the fields marked with * are only available on outlet-switching capable models.

Field	Description
Name	Type an outlet name up to 64 characters long.
*State on device startup	Click this field to select this outlet's initial power state. • Options: *on*, *off*, *last known* and *PDU defined*. • Note that any option other than "PDU defined" will override the global outlet state setting on this particular outlet.
*Power off period during power cycle	Select an option to determine how long this outlet is turned off before turning back on. • Options: *PDU defined* or customized time. See Power-Off Period Options for Individual Outlets (on page 174). • Note that any time setting other than "PDU defined" will override the global power-off period setting on this particular outlet.
*Non-critical	Select this checkbox only when you want this outlet to turn off in the load shedding mode. See Load Shedding Mode: Activate or Deactivate (on page 165).

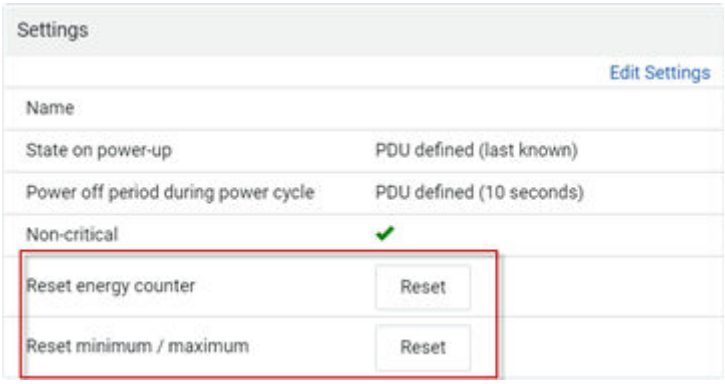
3. Click Save.
4. The outlet's custom name, if available, is displayed in the outlets list, following by its label in parentheses.

Note for 'State on device startup': This setting works only when 'Relay behavior on power loss' is set to *Non-latching*. This is because all relays keep their states unchanged in the latching mode regardless of the power supply status.

► *To reset this outlet's energy counter or minimum/maximum values:*

Energy counter is stored for each outlet. All outlet sensors with numeric readings store their minimum and maximum recorded reading. You can reset these values for an individual outlet as desired. Only users with the "Admin" role assigned can reset these readings.

1. On the individual outlet page, scroll down to Settings.
2. Click the Reset button to either "Reset energy counter" or Reset minimum/maximum.
3. Click to confirm the reset.

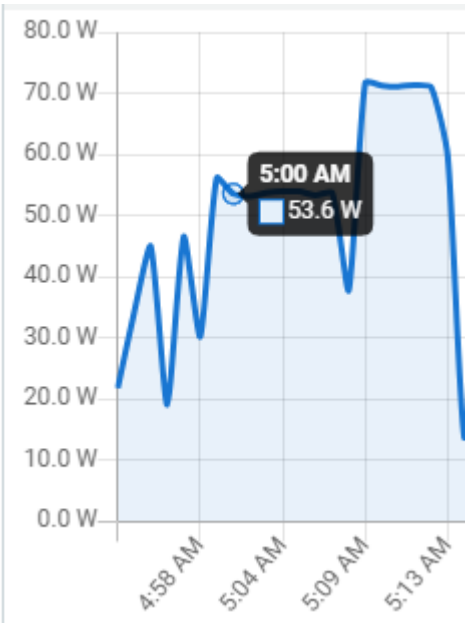


► *To view this outlet's Outlet History power chart:*

By default this outlet's active power data within the past two hours is shown in the power chart.

- Click the selector under the chart to view any other power sensor reading for this outlet.

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



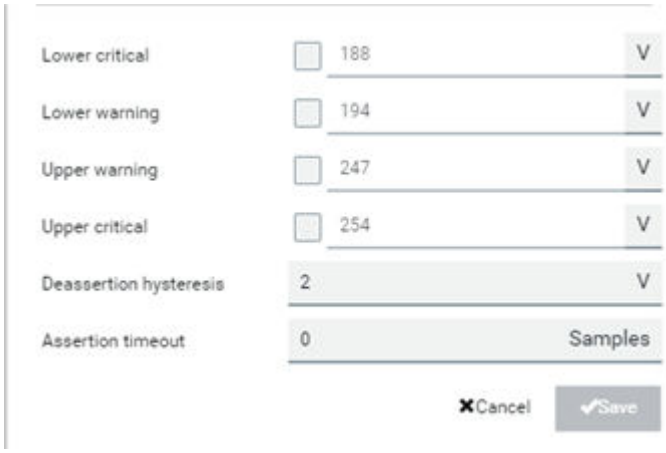
► *To configure this outlet's threshold settings:*

Per default, there are predefined RMS voltage and current threshold values in related fields. See Default Voltage and Current Thresholds. You can modify the defaults as needed.

These threshold settings apply to a single outlet. You can also configure thresholds for multiple outlets at once. See Threshold Bulk Setup (on page 159).

1. If the outlet's threshold data is invisible, click the Thresholds title bar to display it.

2. Click the desired sensor to edit.
3. Make changes as needed.
   - To enable any threshold, select the corresponding checkbox.
   - Type a new value in the accompanying text box.



4. Click Save.

Detailed Information on Outlet Pages

Each outlet's data page has the Details section for showing general outlet information and Sensors section for showing the outlet sensor status.

► *Details section:*

Field	Description
Label	The physical outlet number
Outlet status	Available on outlet-switching capable models. • On or Off • Inrush details: Click this link to view the inrush details waveform.
Receptacle type	This outlet's receptacle type
Lines	Lines associated with this outlet
Inlet	Inlet associated with this outlet
Overcurrent protector	Overcurrent protector associated with this outlet, if present.

Field	Description
Outlet Groups	Groups associated with this outlet.

► *Sensors section:*

- RMS current (A)
- Peak Current
- Inrush Current
- Current Total Harmonic Distortion
- RMS voltage (V)
- Voltage Total Harmonic Distortion
- Line Frequency (depends on model)
- Active Power (W)
- Active Energy (Wh)
- Reactive Power
- Apparent Power (VA)
- Apparent Energy
- Power Factor
- Crest Factor
- Displacement Power Factor
- Phase Angle

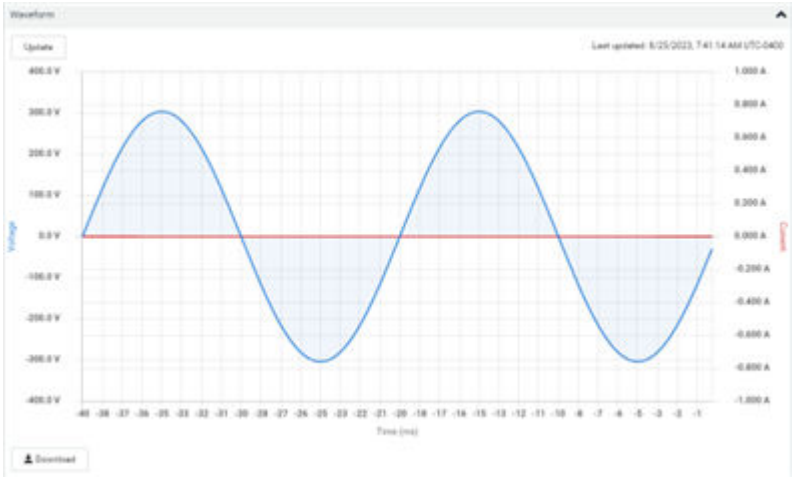
Waveforms for Outlets

► *Waveform:*

In addition to the waveforms captured automatically on OCP trip events, dip/swell events, and relay switch-on events, you can generate a waveform capture whenever you require for an individual outlet. Waveforms created manually represent only the moment in which they are created. Refreshing the browser removes the waveform image.

► *To manually capture a waveform:*

1. On the Outlets page, click an outlet to go to the details page.
2. Scroll down to the Waveform section.
3. Click Update to generate the waveform.
   - Hover your mouse over the waveform to view individual data points.



Power-Off Period Options for Individual Outlets

The 'Power off period during power cycle' setting determines how long an outlet stays off during a power cycle. By default, outlets remain off for 10 seconds before turning back on.

► *Power-Off Period Settings:*

The following items are settings that are present during the Power Cycle of a Power-Off Period:

- The value is between 1 second and 1 hour, or PDU-defined
- The default is to use the PDU-global setting (10 seconds)
- This is only applicable for switched outlets
- The longest power off period configured is used for all outlets when multiple outlets are power cycled. This setting (Cycle Delay) can be displayed as an optional column on the Outlets list page.

► *Power-Off Period Options*

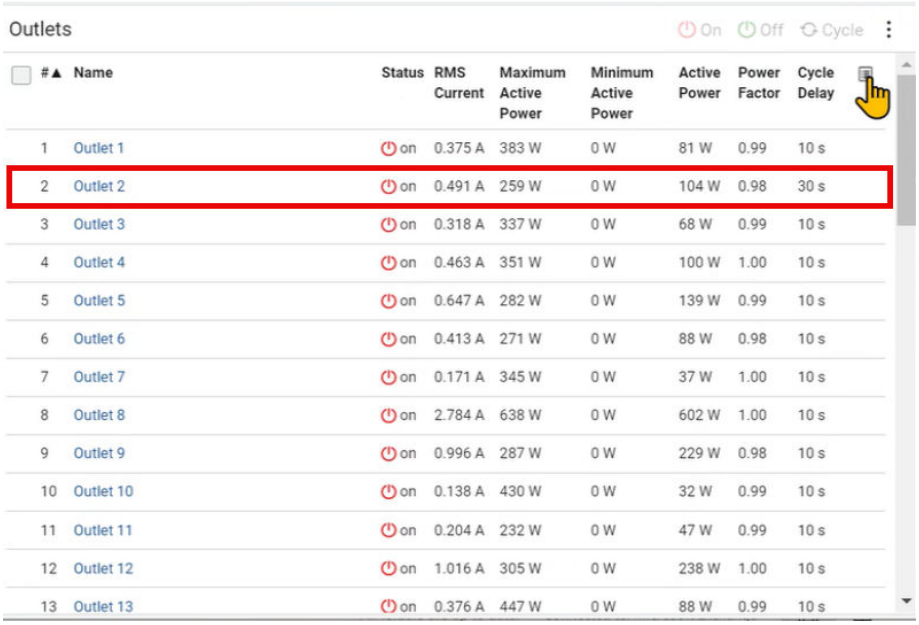
There are two options for setting the power-off period during the power cycle on each individual outlet's page.

Option	**Function**
PDU defined (configured value)	Follows the global power-off period setting, which is set on the *PDU page*. The value in parentheses is the current global value.

Option	Function
Customized time	• Select an existing time option, or type a new value *with an appropriate time unit added, such as s for seconds.*

► *View the Cycle Delay for All Outlets:*

When power cycling multiple outlets, view this column to check for the longest power off delay set. This setting is a Cycle Delay.



Outlet Groups

Only PDUs with outlet-switching and/or outlet-metering feature show this menu item.

Choose Outlet Groups in the *Menu*.

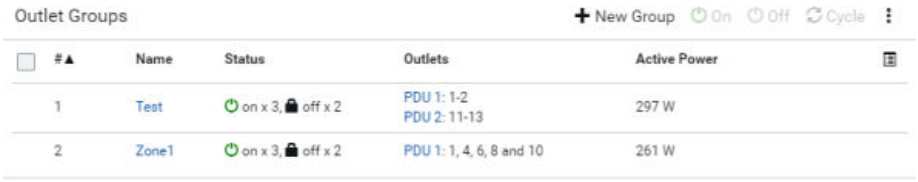
► *Required permissions:*

You must have one of the permissions below to be able to operate all or some of the outlet group features.

- Administrator Privileges -- *all operations*
- Change Pdu, Inlet, Outlet & Overcurrent Protector Configuration -- *creating, editing and deleting outlet groups*
- Switch Outlet Group -- *powering on, off or cycle outlet groups*

► *Outlet group data:*

The Outlet Groups page will list all outlet groups you create.



- For each group, you can view the following data on the Outlet Groups page:
  - Group number
  - Name: the outlet group name displays as a link. Click to go to the details page for the group.
  - Status: number of outlets with status ON, number of outlets with status OFF.
  - Active Power: The active power for the group. A sum of all member outlets' active power values.
  - Maximum Active Power: Hidden by default. Click the columns icon to add this data. The highest recorded active power for the group.
  - Outlets: A list of the outlet numbers who are members of the group. The PDU(s) of the outlets displays as links.

Creating an Outlet Group

You can create an outlet group if you often have to perform the same action on the same outlets at a regular interval.

For example, create an outlet group when you need to:

- Power cycle specific outlets every week.
- Sum up and track specific outlets' active power values every month.
- Sum up the increased values of specific outlet's active energy values every month.

Note that an outlet can be a member of one or multiple groups.

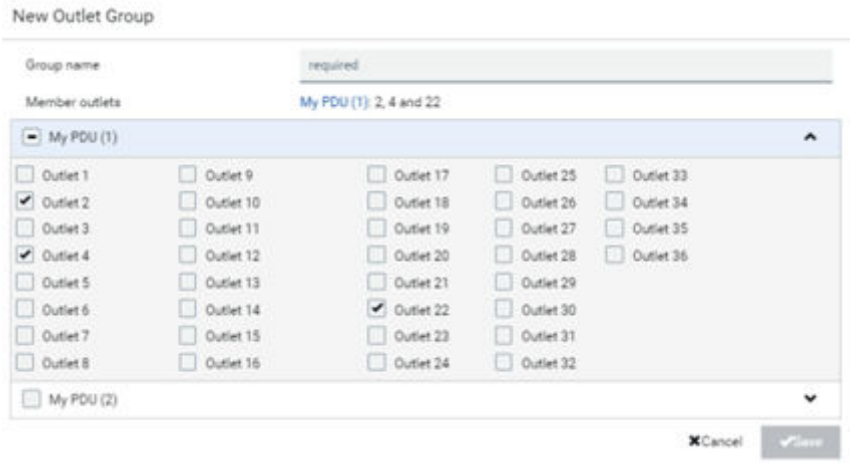
To create an outlet group, you must have either permission below.

- Administrator Privileges
- Change Pdu, Inlet, Outlet & Overcurrent Protector Configuration

► *To create an outlet group:*

1. In the Outlet Groups page, click Add Group.
2. Enter a Group name.

Tip: Outlet group names do not have to be unique. Different groups with the same group name can be identified through their unique index numbers.



3. Click Save.

Outlet Group Power Control

To control outlet groups, you need one of the following permissions

- Administrator Privileges
- Switch Outlet Group

Power control commands are accessible on the Outlet Groups main page, where you can manage multiple groups, or on individual outlet group pages, where you can control a single group while viewing its details.

► *To switch one or multiple groups on the Outlet Groups page:*

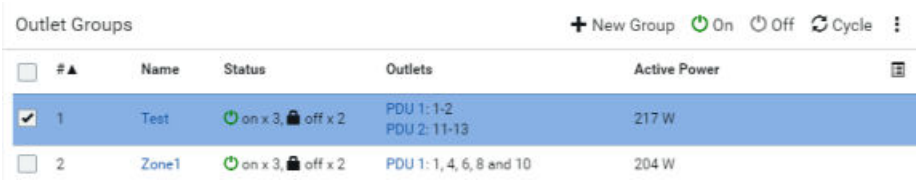
1. On the Outlet Groups page, select the group or groups you want to control.
2. The power control commands appear in the top right corner.
3. Click a power control command.

- On: Power ON
- Off: Power OFF
- Cycle: Power cycle turns outlet OFF then back ON

4. Confirm the operation when prompted.

► *To switch one group on a specific outlet group's page:*

1. In the Outlet Groups page, click a group name to go to its details page.
2. Click a power control command on the top-right corner.



3. Confirm the operation when prompted.

If Switchable Outlet Groups are Limited

If a user is assigned the 'Switch Outlet Group' permission for specific outlet groups rather than all groups, certain switching issues might occur.

► *Issue:*

- When an outlet group that the user originally can switch is deleted, and then re-created with the same group name, the user will not be able to switch the "new" outlet group with the same group name.

► *Solution:*

1. Edit the role assigned to the user. See Editing or Deleting Users (on page 226).
2. Find the Switch Outlet Group permission, and re-select that newly-created outlet group in its outlet group list.

Note: The above issue does not occur for any role which has "All Outlet Groups" selected for its Switch Outlet Group permission.

Resetting a Group's Energy Counter and Minimum/Maximum Values

An outlet group's active energy is calculated by adding up the energy increments from all its member outlets. The group's active energy starts at zero when outlets are grouped together. Subsequent energy changes are calculated based on the increments from the time they joined the group, not their absolute values.

For example:

- Take outlet 1 which has 200 kWh of active energy, and outlet 2 has 300 kWh.
- Add these two outlets in a group. After grouping, the group's energy starts at 0.
- If outlet 1's energy increases to 205 kWh and outlet 2's energy rises to 310 kWh: The increment for outlet1 is (205 - 200 = 5) kWh.- The increment for outlet2 is (310 - 300 = 10) kWh.- The group's total energy becomes (5 + 10 = 15) kWh.

The focus is on the energy changes (increments) rather than the absolute energy values.

Note: A group's active energy is calculated differently; it is NOT simply the total of the active energy values of all its member outlets.

You must have the Administrator Privileges to reset these values and it is available on models with outlet-metering.

- You can reset the energy counter and minimum/maximum values of other readings for one or more outlet groups at a time on the Outlet Groups page.
- To reset these values for a single outlet group, there are two methods -- either Outlet Groups page or individual group page.
- Resetting an outlet group's energy counter has NO impact on any member outlet's energy counter.

► *To reset values on the Outlet Groups page:*

1. On the Outlet Groups page, select one or more outlet groups to reset.
2. Click > Reset Energy Counter, or Reset Minimum/Maximum, then confirm the operation when prompted.

► *To reset values on a specific outlet group's page:*

1. On the Outlet Groups page, click a group name to open its page.
2. Scroll down to the Settings section.
3. Click the Reset button to either "Reset energy counter" or Reset minimum/maximum.
4. Click to confirm the reset.

Modifying an Outlet Group

To modify an outlet group, you must have either permission below.

- Administrator Privileges
- Change Pdu, Inlet, Outlet & Overcurrent Protector Configuration

► *To modify the member outlets:*

1. On the Outlet Groups page, click a group name to go to its details page.
2. Click Edit Members.
3. Add or remove outlets of this group by selecting or clearing checkboxes.
4. Click Save.

► *To change the group name:*

1. Scroll down to the Settings section, then click Edit Settings.
2. Type a new name.
3. Click Save.

► *To configure the thresholds of group sensors:*

1. Click the Thresholds title bar at the bottom of the page to display thresholds.
2. Click the desired sensor (required), and then click Edit Thresholds.
3. Make changes as needed.
   - To enable any threshold, select the corresponding checkbox.
   - Type a new value in the accompanying text box.
4. Click Save.

Deleting an Outlet Group

To delete an outlet group, you must have either permission below.

- Administrator Privileges
- Change Pdu, Inlet, Outlet & Overcurrent Protector Configuration

You can delete one or multiple outlet groups at a time.

To delete a single outlet group only, there are two methods -- either Outlet Groups page or individual group page.

► *To delete one or multiple groups on the Outlet Groups page:*

1. On the Outlet Groups page, select one or more outlet groups.
2. Click > Delete, then confirm the operation when prompted.

► *To delete a group on a specific outlet group's page:*

1. Open a specific outlet group's page by clicking on its name.
2. Click > Delete, then confirm the operation when prompted.

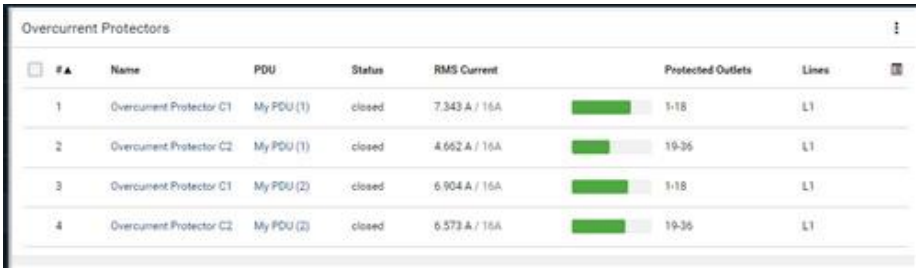
OCPs

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

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

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

You can go to each OCP's data/setup page by clicking its name on this page. OCPs may be numbered C1, C2, and so on, or BR1, BR2 and so on.



► *Overcurrent protector overview:*

- OCP status - open (tripped) or closed
- Current drawn, rated current and current bar
  - The smaller, gray text adjacent to "current drawn" is the rated current of each OCP.
  - The RMS current bars change colors to indicate the status if the OCP thresholds have been configured and enabled.

Status	Bar colors
normal	
above upper warning	
above upper critical	

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

- Protected outlets, which are indicated with outlet numbers
- Associated lines

► *To configure current thresholds for multiple overcurrent protectors:*

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

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

1. Click ⋮ > Threshold Bulk Setup.
2. Select one or multiple OCPs.
3. Click Edit Thresholds.
4. Make changes as needed.
   - To enable any threshold, select the corresponding checkbox.
   - Type a new value in the accompanying text box.

5. Click Save.

Individual OCP Pages

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

► *General OCP information:*

Field	Description
Label	This OCP's physical number. • C1, C2, C3... • BR1, BR2, BR3...
Status	open or closed. If a trip cause has been detected, the details are linked here with the Open status.
Type	This OCP's type.
Rating	This OCP's rated current.
Lines	Lines associated with this OCP.
Protected outlets	Outlets associated with this OCP.

Field	Description
Inlet	Inlet associated with this OCP. Useful when your PDU has multiple inlets.
RMS current	This OCP's current state and readings, including current drawn and current remaining.

► *To customize this OCP's name:*

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

► *To view this OCP's RMS current chart:*

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

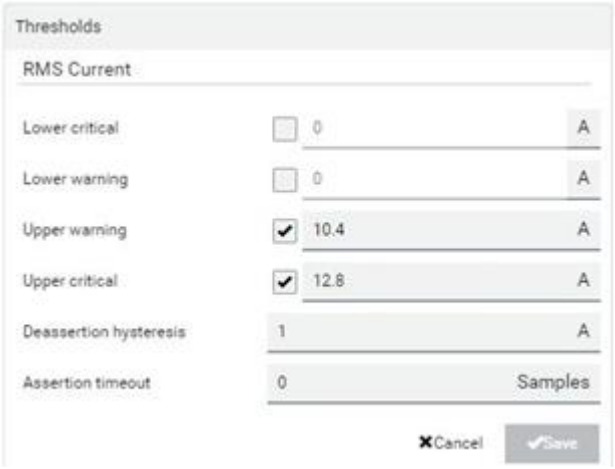
- To retrieve the exact data at a particular time, hover your mouse over the data line in the chart. Both the time and data are displayed as illustrated below.

► *To configure this OCP's threshold settings:*

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

1. Click the Thresholds title bar at the bottom of the page to display the threshold data.

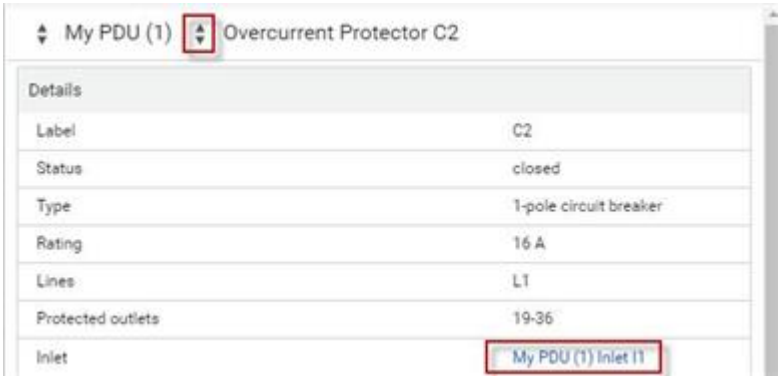
2. Click the RMS current sensor, then make changes as needed.
   - To enable any threshold, select the corresponding checkbox.
   - Type a new value in the accompanying text box.



3. Click Save.

► *Other operations:*

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



OCP Trip-Cause Detection

Not supported on all models.

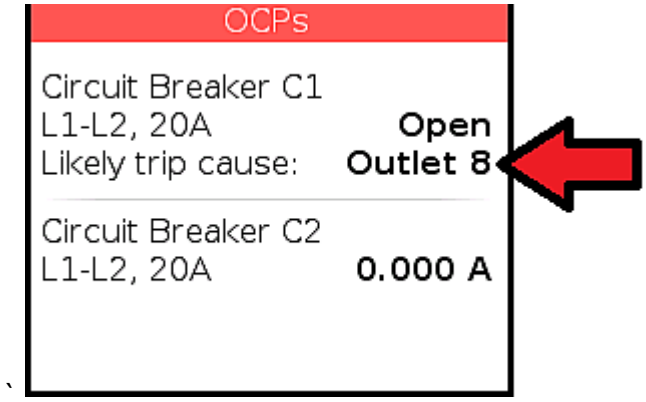
When the outlet that most likely caused a trip can be detected, this information displays in the web interface, front panel display, and command line interface (CLI).

► *Web interface:*

- On the page of a tripped OCP, the Status field indicates the outlet number that may cause the OCP-tripped event.

► *Front panel display:*

The 'Likely trip cause' message will be displayed for an "open" OCP, indicating which outlet may cause the OCP-tripped event.



► *CLI:*

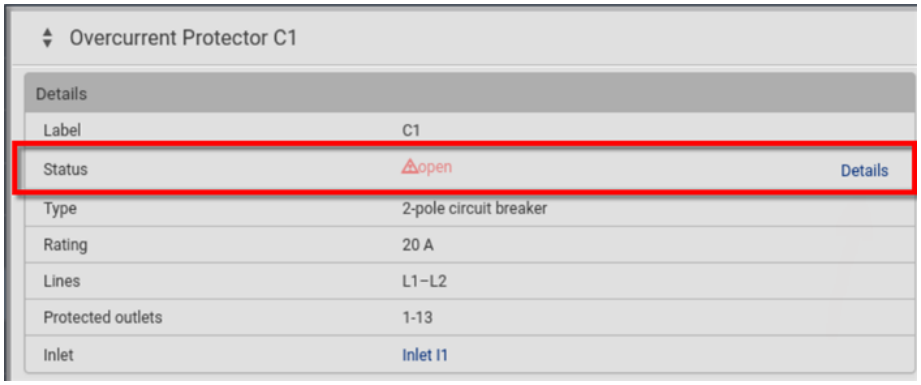
- Perform the `show ocp` command in the CLI. If any OCP has tripped, then the outlet that may cause this event is shown in parentheses in the State field of the tripped OCP.

OCP Trip-Cause Waveform

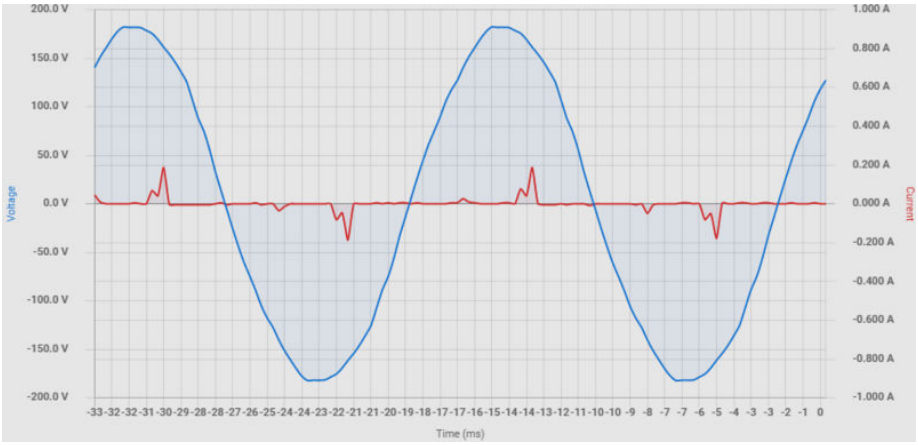
A waveform is captured for the outlet that showed the highest peak current value when the trip is detected. The data captured at the time of the trip event is stored persistently and kept until next trip event.

► *To view the waveform:*

1. In the OCP page, click the OCP with Open status.
   - The individual OCP page opens. A Details link is available if a trip-cause has been detected.



2. Click the Details link to view the waveform.



Peripherals

If there are environmental sensor packages connected, they are listed on the Peripherals page.

An environmental sensor package may contain:

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

PX4 communicates with *managed* sensors/actuators only and retrieves their data. One PX4 can manage a maximum of 64 sensors/actuators.

Open the Peripheral Devices page by clicking Peripherals in the *Menu.* Then you can:

- Perform actions on multiple sensors/actuators by using the control/action icons on the top-right corner.
- Go to an individual sensor's or actuator's data/setup page by clicking its name.

► *Sensor/actuator overview on this page:*

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

Column	Description
Name	By default, the name assigned contains: • Sensor/actuator type, such as "Temperature" or "Dry Contact." • Sequential number of the same sensor/actuator type, like 1, 2, 3 and so on. You can customize the name. Customize names on the individual sensor page.
Reading	Numeric sensors, such as temperature and humidity, show the reading.
Maximum	Maximum reading of all previously seen values since last reset.
Minimum	Minimum reading of all previously seen values since last reset.
State	Available for all sensors and actuators. Sensor/Actuator States (on page 194)
Type	Sensor or actuator type.
Serial Number	This is the serial number printed on the sensor package's label.
Position	Position indicates where this sensor or actuator is located in the sensor chain. Identifying the Sensor Position and Channel (on page 197)
Actuator	Indicates whether this sensor package is an actuator or not. If yes, the checkmark symbol ✔ is shown.

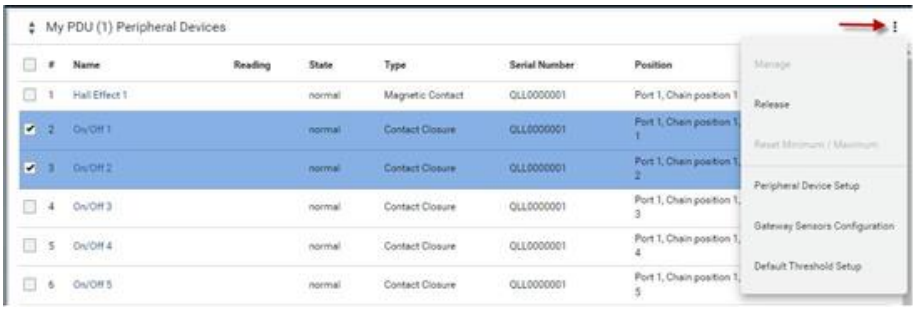
► *To release or manage sensors/actuators:*

You can multi-select sensors to release or manage them. Releasing is necessary when the maximum number of managed sensors are in use, and you need to make a change, such as replacing old sensors with new ones, or making space by removing an unneeded type and adding a different type. When you manage sensors individually, you can manually select ID numbers--this allows you to simultaneously

release an old sensor if you select to reuse its assigned ID: Managing One Sensor or Actuator (on page 198). When you manage multiple sensors at once, ID numbers are automatically assigned, and nothing else is changed or released.

1. Select the sensors/actuators that you want to manage/release from management.

2. Click ⋮ to view options and select Manage or Release.
   - Release: The items are automatically released, and you return to the list. Newly released sensors show at the end of the list as "Manage Device" if they are still physically connected, otherwise they disappear.
   - Manage: "Manage Peripheral Device" dialog opens. Click Manage to accept automatic sensor numbers. If a single item was selected, you can choose the ID number by selecting "Manually select a sensor number." Click Manage and you return to the list. Newly managed sensors appear and will show a status in the State column. They can now be renamed and configured.



► *To configure sensor/actuator-related settings:*

1. Click ⋮ > Peripheral Device Setup.

Raritan
A brand of legrand

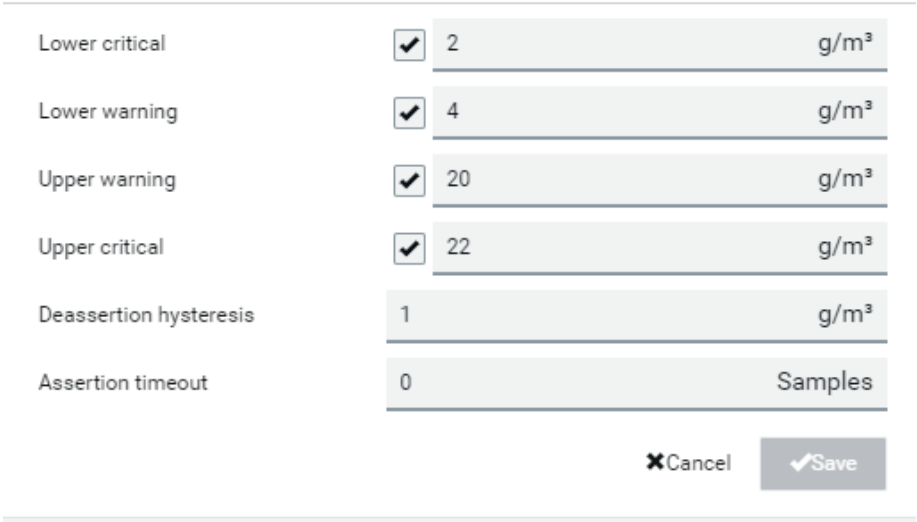
Field	Function	Note
Peripheral device Z coordinate format	Options to describe the vertical locations (Z coordinates) of environmental sensor packages. • *Rack units or Free-form* See Z Coordinate Format (on page 205).	Every sensor has a Z Coordinate field. The format setting specifies whether those coordinates are required to be rack unit numbers or can contain arbitrary text.
Peripheral device auto management	Enables or disables the automatic management feature for Raritan environmental sensor packages. • *Default is Enabled.*	Automatic Management of Sensors (on page 198)
Mute other door handle	• If selected, one door handle will be completely powered down (including any attached card reader or keypad) before opening the other lock of the same DX2-DH2C2.	• This option helps to avoid overload in power-limited setups with two door handles.
Altitude	Specify the altitude of PX4 above sea level when a differential air pressure sensor is attached. • *Range: -425 to 3000 meters (-1394 to 9842 feet)* • *Negative numbers indicate locations below sea level.*	• The device's altitude is associated with the altitude correction factor. • The default altitude measurement unit is meter. • Your user preference for measurements will take effect here.
Active powered dry contact limit	Determines the maximum number of "active" powered dry contact actuators that is permitted concurrently. • *Range: 0 to 24* • *Default:* 1	• An "active" actuator is turned ON, or, for a door handle, door is OPENED. • This setting only applies to "powered dry contact" (PD) actuators rather than normal "dry contact" actuators. • You need either 'Change Peripheral Device Configuration' privilege or 'Administrator Privileges' to change the setting.

2. Click Save.

► *To configure default threshold settings:*

Note that default threshold settings affect all sensors already being managed, and establish the initial settings for any sensor added from now on. To customize the threshold settings on a per-sensor basis, go to Individual Sensor/Actuator Pages (on page 200).

1. Click ⋮ > Default Threshold Setup.
2. Click a sensor to open the threshold settings.
3. Make changes as needed.
   - To enable any threshold, select the corresponding checkbox.
   - Type a new value in the accompanying text box.



4. Deassertion hysteresis: An alarm is cleared when the sensor reading normalizes the specified amount away from the threshold. In the screenshot example above, if temperature normalizes by more than 1 degree of the threshold, the alarm is cleared. When the reading is within 1°C from the threshold, the alarm will remain active. For example: A warning is raised when the temperature exceeds 30°C. It has to drop to 29°C to clear the warning.
5. Assertion timeout: An alarm is raised when the sensor reading exceeds a threshold for more than the specified number of samples. In the screenshot example above, timeout is set to Zero. An alarm would be raised immediately when the reading exceeds the threshold. If the timeout were set for 20, the sensor reading would have to persist in exceeding a threshold for 20 data samples before an alarm would be raised.
6. Click Save.

► *To turn on or off any actuator:*

1. Select one or multiple actuators . This activates the power buttons at the top right corner in the web interface.
2. Click On or Off. For Door Handles, click Open or Close.

Note: Per default you can turn on as many dry contact actuators as you want, but only one "powered dry contact" actuator can be turned on at the same time. Change this setting in ⋮ > Peripheral Device Setup.

---

3. Confirm the operation when prompted.

Yellow- or Red-Highlighted Sensors

The PX4 highlights those sensors that enter the abnormal state with a yellow or red color. Note that numeric sensors can change colors when thresholds are enabled.

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

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

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

Managed vs Unmanaged Sensors/Actuators

► *Managed sensors/actuators:*

- PX4 communicates with managed sensors/actuators and retrieves their data.
- Managed sensors/actuators are always listed on the Peripheral Devices page whether they are physically connected or not.

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

► *Unmanaged sensors/actuators:*

- PX4 does NOT communicate with unmanaged sensors/actuators.
- Unmanaged sensors/actuators are listed only when they are physically connected to PX4. They disappear from the web interface when they are no longer connected.
- They do *not* have an ID number.
- They show the "unmanaged" state.

Sensor/Actuator States

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

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

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

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

► *Managed sensor states:*

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

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

Note that for a contact closure sensor, the normal state depends on the normal setting you have configured.

► *Managed actuator states:*

State	Description
on	***The actuator is turned on.***
off	***The actuator is turned off.***
unavailable	• ***Communication with the managed actuator is lost.*** ***-- OR --*** • ***Sensor packages are upgrading their sensor firmware.***

► *Unmanaged sensor/actuator states:*

State	Description
unmanaged	***Sensors or actuators are physically connected to the PX4 but not managed yet.***

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

Finding the Sensor's Serial Number

A sensor package has a serial number tag attached to its rear side.

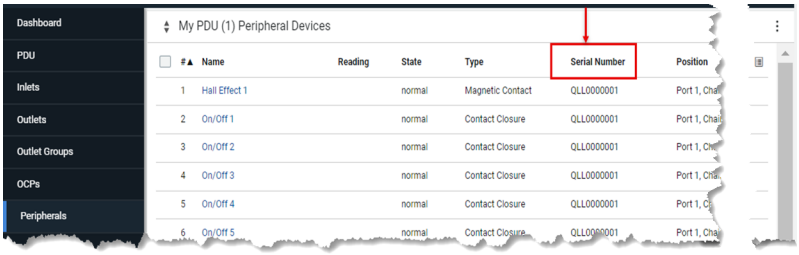
The serial number for each sensor or actuator appears listed in the web interface when it is detected. Match the serial number from the tag to those listed in the sensor table.

Group Peripheral Sensors

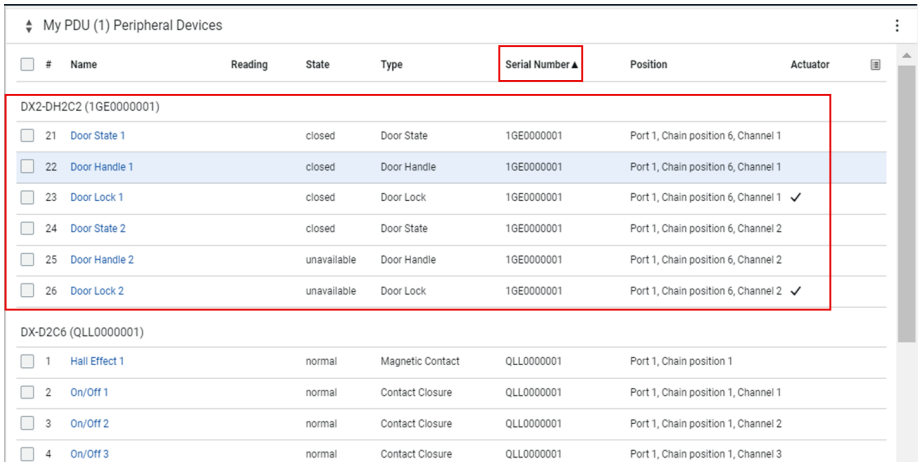
You can group peripheral sensors by their physical packages. Each physical package can contain many logical sensors.

► *To group peripheral sensors:*

1. On menu page of Peripheral Devices click on Serial number.

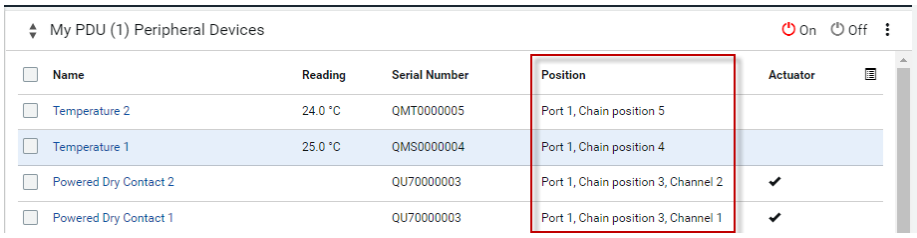


2. Sensors are grouped by the physical package.



Identifying the Sensor Position and Channel

The Peripheral Devices page shows where each sensor or actuator is connected.



- The position information includes the port name and the sensor's position in a sensor chain.
  For example: *Port 'Sensor', Chain Position 3*
- If a sensor hub is involved, the hub port information is also indicated for most sensors.
  For example: *Port 'Sensor', Hub port 2, Chain Position 3*
- If a sensor/actuator contains channels, such as a contact closure sensor or dry contact actuator, the channel information is included.
  For example, *Port 'Sensor', Hub port 2, Chain Position 3, Channel 1*

Automatic Management of Sensors

To configure automatic management, go to Peripherals > > Peripheral Device Setup.

► *After enabling the automatic management function:*

When the maximum number of sensors are not yet managed, newly-connected environmental sensors and actuators are automatically managed upon detection.

► *After disabling the automatic management function:*

You must manually manage all sensors to start communications. Until you do this, they will not have ID numbers or show sensor readings or states.

Managing One Sensor or Actuator

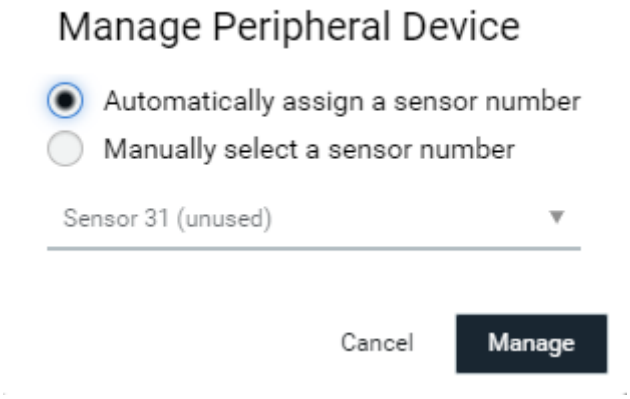
If you are managing only one sensor or actuator, you can assign the desired ID number to it. When managing multiple sensors/actuators at a time, the IDs are automatically assigned.

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

► *To manage only one sensor/actuator:*

1. Click Peripherals in the Menu.
2. Unmanaged sensors/actuators appear at the end of the list as "Manage Device". You can identify the sensor/actuator by the Type, Serial Number, and Position columns.

3. Click the Manage Device link, and the Manage Peripheral Device dialog appears.



- Select "Automatically assign a sensor number" to assign an unused ID number. This method does not release any managed sensor or actuator.
- Select "Manually select a sensor number" to select a desired ID number from the list. Selecting an ID already in use will release the sensor currently managed with that ID. IDs already in use show the sensor package's serial number. Available IDs show "unused."

4. Click Manage.

► *Special note for Legrand humidity sensors:*

A Legrand humidity sensor is able to provide three measurements - relative and absolute, and humidity values.

- A relative humidity value is measured in percentage (%).
- An absolute humidity value is measured in grams per cubic meter (g/m^3).
- A dew point is measured in degree celsius (°c).

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

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

Individual Sensor/Actuator Pages

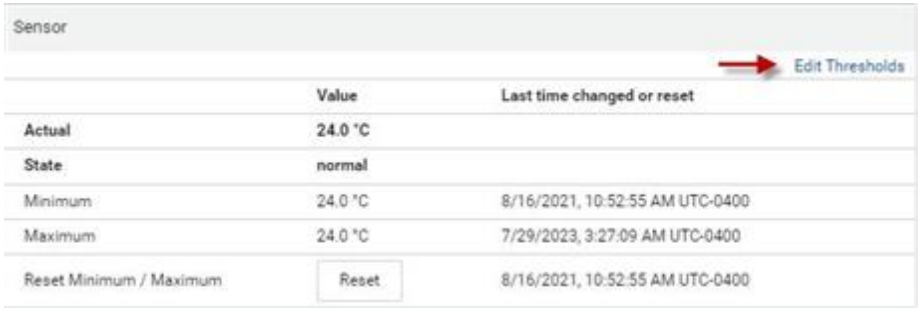
A sensor's or actuator's data/setup page is opened after clicking any sensor or actuator name on the Peripheral Devices page.

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

Threshold settings, if enabled, help you identify whether any numeric sensor enters the warning or critical level. In addition, you can have PX4 automatically generate alert notifications for any warning or critical status.

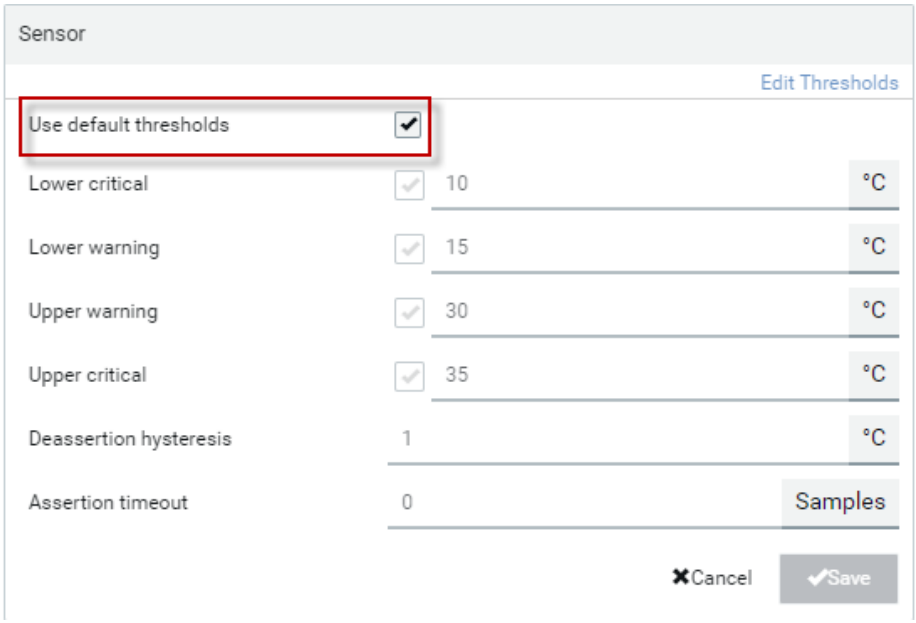
► *To configure a numeric sensor's threshold settings:*

1. Click Edit Thresholds.



Tip: The date and time shown on the PX4 web interface are automatically converted to your computer's time zone. To avoid time confusion, it is suggested to apply the same time zone to your computer or mobile device.

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



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

  The default threshold settings are configured on the page of *Peripherals.*
- To customize the threshold settings for this particular sensor, deselect the 'Use default thresholds' checkbox, and then modify the threshold fields below it.

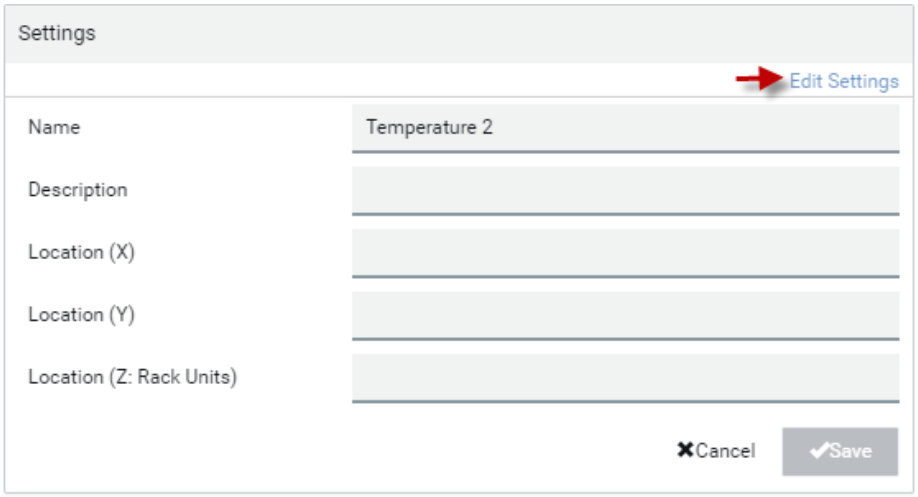
Note: For concepts of thresholds, deassertion hysteresis and assertion timeout, see Sensor Threshold Settings (on page 705).

---

3. Click Save.

► *To set up a sensor's or actuator's physical location and additional settings:*

1. Click Edit Settings.



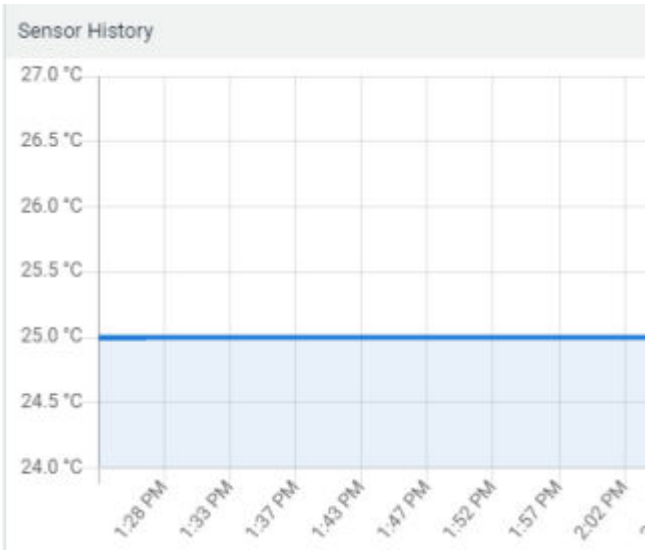
2. Make changes to available fields, and then click Save.

Fields	Description
Name	A name for the sensor or actuator.
Description	Any descriptive text you want.
Location (X, Y and Z)	Describe the sensor's or actuator's location in the data center by typing alphanumeric values for the X, Y and Z coordinates. See Sensor/Actuator Location Example: X, Y, Z Coordinates (on page 205) If the term "Rack Units" appears in parentheses in the Z location, you must type an integer number. The Z coordinate's format is determined on the page of *Peripherals.*
Alarmed to Normal Delay	This field is available for the DX2-PIR presence detector only. It determines the wait time before the PX4 announces that the presence detector is back to normal after it already returns to normal. Adjust the value in seconds.
Binary Sensor Subtype	This field is available for any Legrand contact closure sensor except for DX2-DH2C2's contact closure sensors. Determine the sensor type of your contact closure detector. • *Contact Closure* detects the door lock or door open/closed status. • *Smoke Detection* detects the appearance of smoke. • *Water Detection* detects the appearance of water on the floor. • *Vibration* detects the vibration of the floor.

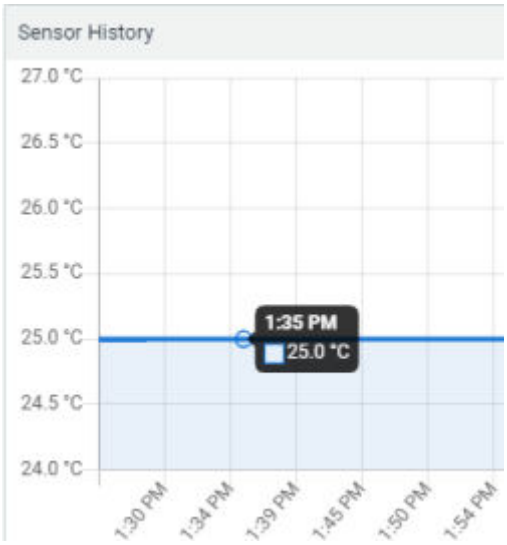
Fields	Description
Sensor Polarity	This field is available for DX2-CC2 contact closure sensors only. Determine the normal state of your DX2-CC2. • *Normal Open:* The open status of the connected detector/switch is considered normal. An alarm is triggered when the detector/switch turns closed. • *Normal Closed:* The closed status of the connected detector/switch is considered normal. An alarm is triggered when the detector/switch turns opened.

► *To view a numeric sensor's chart*

This sensor's data within the past tens of minutes is shown in the chart. Note that only a numeric sensor has this diagram. State sensors and actuators do not have such data.

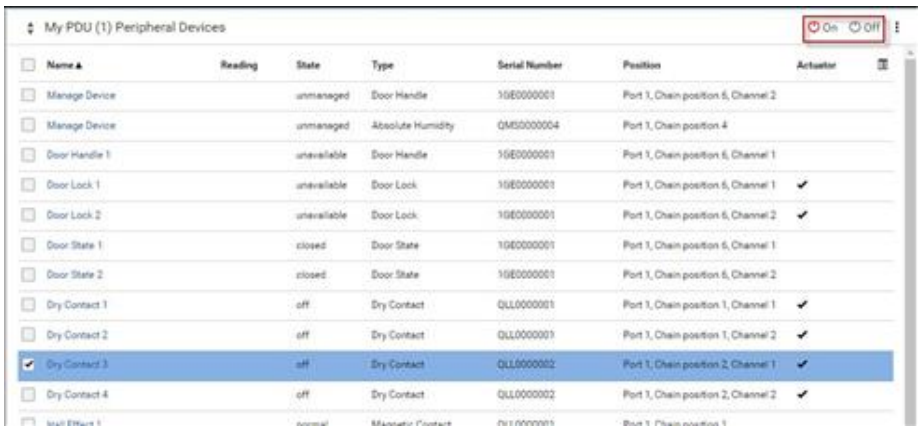


- To retrieve the exact data at a particular time, hover your mouse over the data line in the chart. Both the time and data are displayed as illustrated below.



► *To turn on or off an actuator:*

1. Click the desired control button.



Raritan
A brand of legrand

: Turn ON.

: Turn OFF.

2. Confirm the operation on the confirmation message.

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

► *Other operations:*

You can go to another sensor's or actuator's data/setup page by clicking the selector on the top-left corner.

Z Coordinate Format

Z coordinates refer to vertical locations of environmental sensor packages. You can use either the number of rack units or a descriptive text to describe Z coordinates.

► *To configure Z coordinates:*

1. Determine the Z coordinate format in the main Peripheral Device Setup page. Available Z coordinate formats include:
   - Rack Units: Measurement of the height is in standard rack units. Number from 0-60.
   - Free-form: Enter any alphanumeric string to describe the Z coordinate. Up to 24 characters. Example, "Top of Rack", "Bottom of Rack".
2. Enter the Z coordinates in the individual sensor settings.

Sensor/Actuator Location Example: X, Y, Z Coordinates

Use the X, Y and Z coordinates to describe each sensor's or actuator's physical location in the data center.

The X, Y and Z values act as additional attributes and are not tied to any specific measurement scheme. Therefore, you can use non-measurement values.

► *Example:*

X = ***`Brown Cabinet Row`***
Y = ***`Third Rack`***
Z = ***`Top of Cabinet`***

► *Values of the X, Y and Z coordinates:*

- X and Y: They can be any alphanumeric values comprising 0 to 24 characters.
- Z: When the Z coordinate format is set to *Rack units*, it can be any number ranging from 0 to 60. When its format is set to *Free-form*, it can be any alphanumeric value comprising 0 to 24 characters.

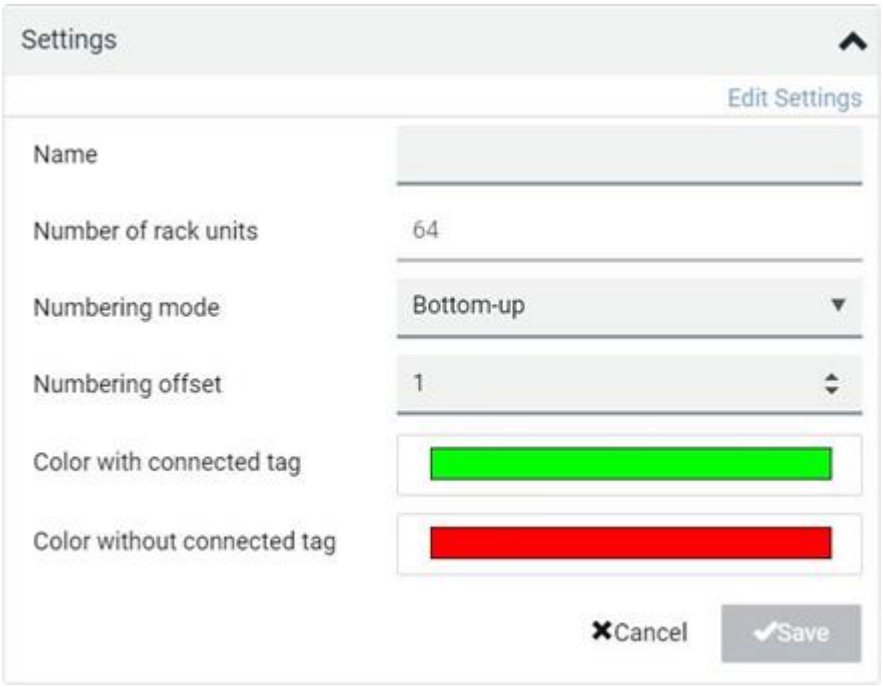
Asset Strips

After connecting and detecting asset management strips (asset strips), the PX4 shows 'Asset Strip' in the menu.

On this page, you can configure the rack units of asset strips and asset tags. A rack unit refers to a tag port on the asset strips. The "Change Asset Strip Configuration" permission is required.

► *To configure asset strip and rack unit settings:*

1. Click Asset Strips in the menu, then click the Asset Strip you want to configure.
2. Click Edit Settings.



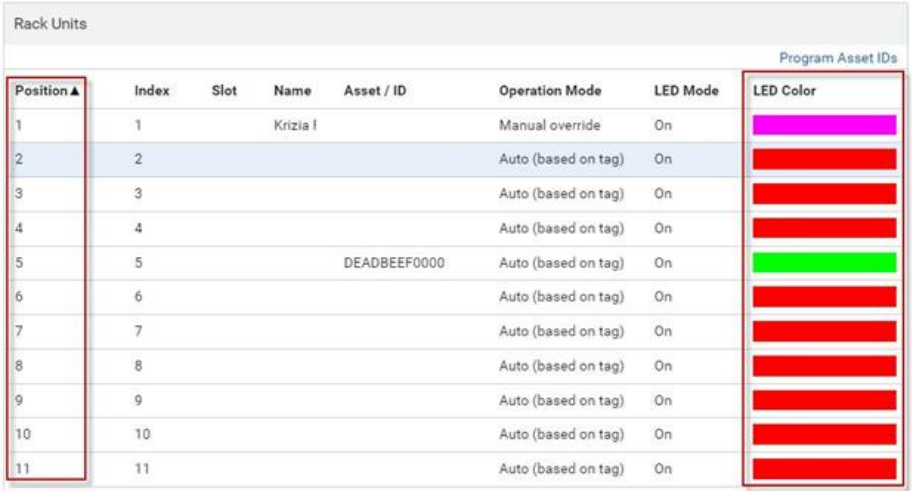
3. Make changes to the settings by directly typing a new value, or clicking that field to select a different option.

Field	Description
Name	Name for this asset strip assembly.
Number of rack units	The number of rack units is auto-detected for all supported AMS, the input field is always disabled.
Numbering mode	The rack unit numbering method in a rack/cabinet. • *Top-Down*: The numbering starts from the highest rack unit of a rack/cabinet. • *Bottom-Up*: The numbering starts from the lowest rack unit of a rack/cabinet.
Numbering offset	The start number in the rack unit numbering. For example, if this value is set to 3, then the first number is 3, the second number is 4, and so on.
Color with connected tag	Click this field to determine the LED color denoting the presence of an asset tag. • Default is green.
Color without connected tag	Click this field to determine the LED color denoting the absence of an asset tag. • Default is red.

For color settings, there are two ways to set the color.

- Click a color in the color palette.
- Type the hexadecimal RGB value of the color, such as #00FF00.

4. Click Ok. The rack unit numbering and LED color settings are immediately updated on the Rack Units list illustrated below.
   - The 'Index' number is the physical tag port number printed on the asset strip, which is not configurable. However, its order will change to reflect the latest rack unit position.



Position ▲	Index	Slot	Name	Asset / ID	Operation Mode	LED Mode	LED Color
1	1		Krizia I		Manual override	On	
2	2				Auto (based on tag)	On	
3	3				Auto (based on tag)	On	
4	4				Auto (based on tag)	On	
5	5			DEADBEEF0000	Auto (based on tag)	On	
6	6				Auto (based on tag)	On	
7	7				Auto (based on tag)	On	
8	8				Auto (based on tag)	On	
9	9				Auto (based on tag)	On	
10	10				Auto (based on tag)	On	
11	11				Auto (based on tag)	On	

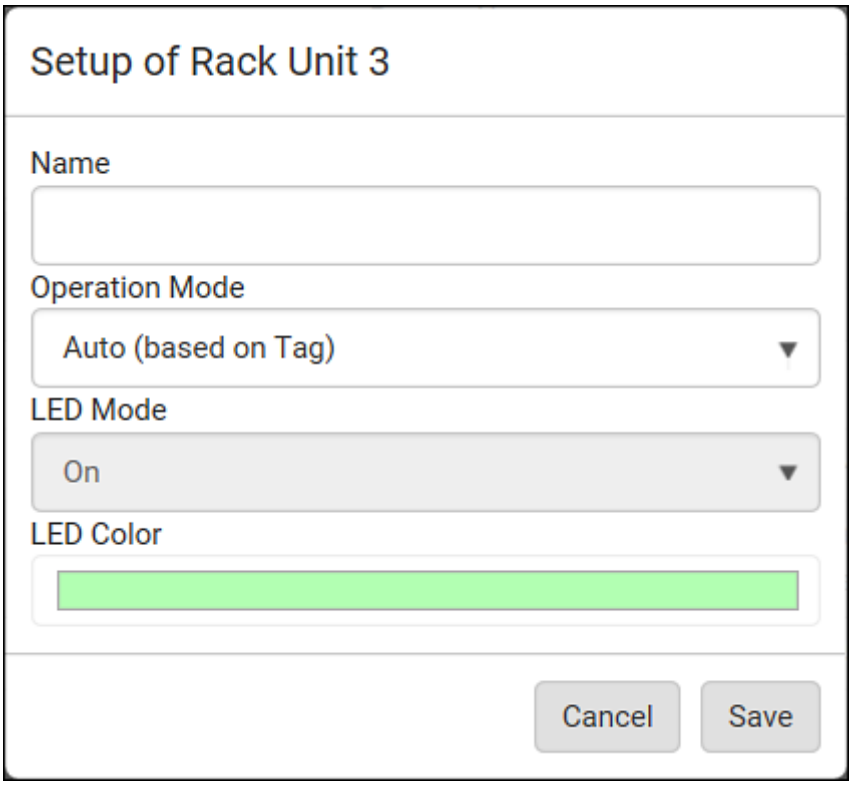
   - A blade extension strip and a *programmable* tag are marked with the word 'programmable' in the Asset/ID column. You can customize their Asset IDs.

► *To customize a single rack unit's settings:*

You can make a specific rack unit's LED behave differently from the others on the asset strip, including

the LED light and color.

1. Click the desired rack unit position on the Rack Units list. The setup dialog for the selected one appears.



2. Make changes to the information by typing a new value or clicking that field to select a different option.

Field	Description
Name	Name for this rack unit. For example, you can name it based on the associated IT device.
Operation Mode	Determine whether this rack unit's LED behavior automatically changes according to the presence and absence of the asset tag. • *Auto*: The LED behavior varies, based on the asset tag's presence. • *Manual Override*: This option differentiates this rack unit's LED behavior.

Field	Description
LED Mode	This field is configurable only after the Operation Mode is set to Manual Override. Determine how the LED light behaves for this particular rack unit. • *On*: The LED stays lit. • *Off*: The LED stays off. • *Slow blinking*: The LED blinks slowly. • *Fast blinking*: The LED blinks quickly.
LED Color	This field is configurable only after the Operation Mode is set to Manual Override. Determine what LED color is shown for this rack unit if the LED is lit.

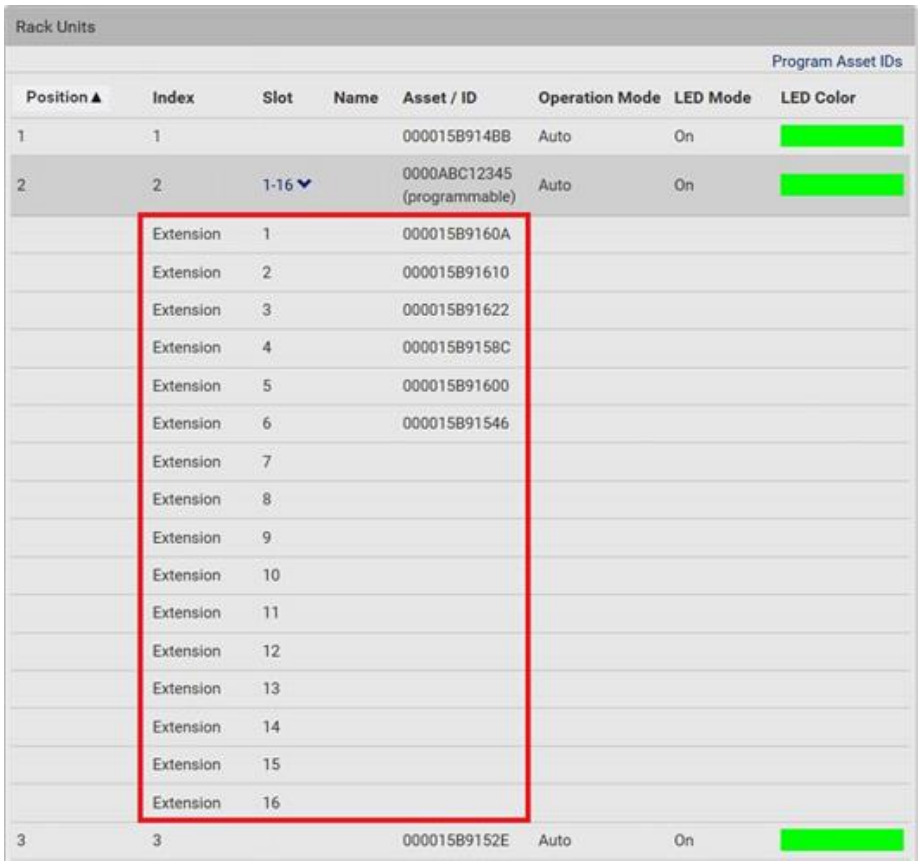
► *To expand a blade extension strip:*

A blade extension strip, like an asset strip, has multiple tag ports. An extension strip is marked with a grayer color on the Asset Strip page, and its tag ports list is collapsed by default.

Note: If you need to temporarily disconnect the blade extension strip from the asset strip, wait at least 1 second before re-connecting it back, or the PX4 device may not detect it.

1. Locate the rack unit (tag port) where the blade extension strip is connected. Click its slot number, whose format is similar to 1-N ^ , where N is the total number of its tag ports.

2. All tag ports of the blade extension strip are listed below it. Their port numbers are displayed in the Slot column.



- To hide the blade extension slots list, click 1-N v .

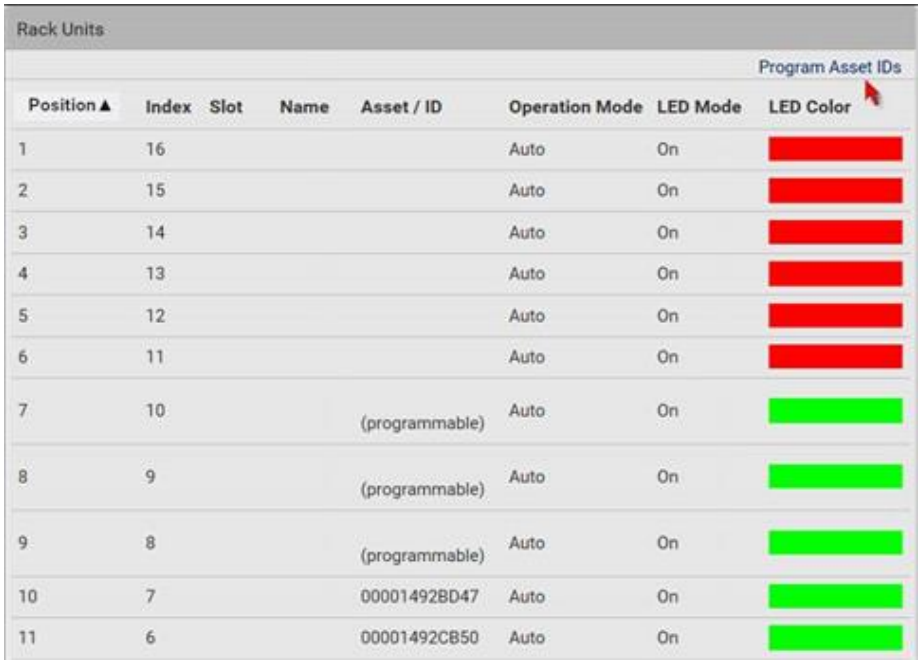
► *To customize asset IDs on programmable asset tags:*

You can customize asset IDs only when the asset tags are "programmable" ones. Non-programmable

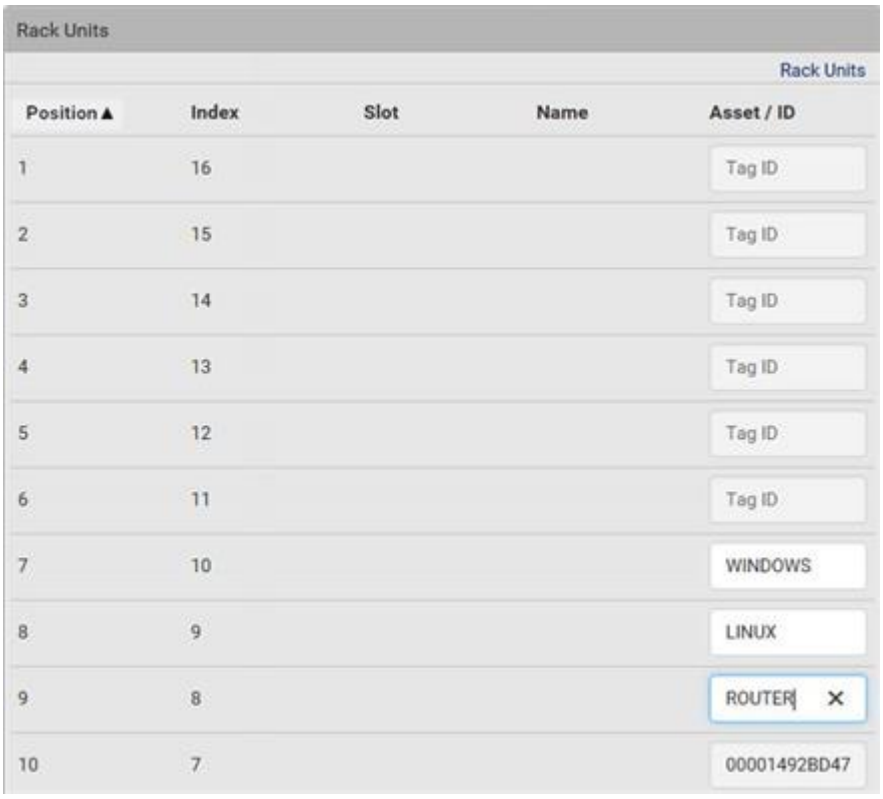
tags do not support this feature. In addition, you can also customize the ID of a blade extension strip.

If a barcode reader is intended, connect it to the computer you use to access the PX4.

1. Click Program Asset IDs.



2. In the Asset/ID column, enter the customized asset IDs by typing values or scanning the barcode.
   - When using a barcode reader, first click the desired rack unit, and then scan the asset tag. Repeat this step for all desired rack units.
   - An asset ID contains up to 12 characters that comprise only numbers and/or UPPER CASE letters. Lower case letters are NOT accepted.



3. Verify the correctness of customized asset IDs and modify as needed.
4. Click Apply at the bottom of the page to save changes.

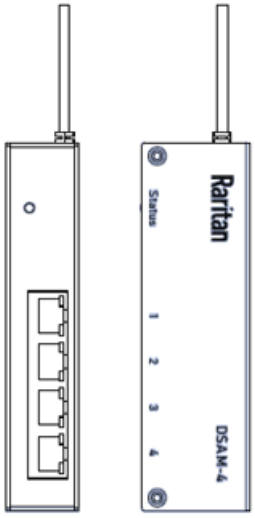
Asset Strip Automatic Firmware Upgrade

Upon connection, the asset strip automatically verifies its firmware version against the version stored in PX4. If a discrepancy is detected, the asset strip initiates a download of the latest firmware from PX4 to perform an upgrade.

During the firmware upgrade, the following events take place:

- The asset strip is completely lit up, with the blinking LEDs cycling through diverse colors.
- A firmware upgrade process is indicated in the web interface.
- An SNMP trap is sent to indicate the firmware upgrade event.ProductName

Serial Access With Dominion Serial Access Module



Connecting a PX4 and a Dominion Serial Access Module (DSAM) provides access to devices such as LAN switches and routers that have a RS-232 serial port.

The DSAM is a 2- or 4 port serial module that derives power from the PX4.

Connect a maximum of 2 DSAM modules to the PX4 using USB cables. DSAM can be mounted in a 0U configuration.

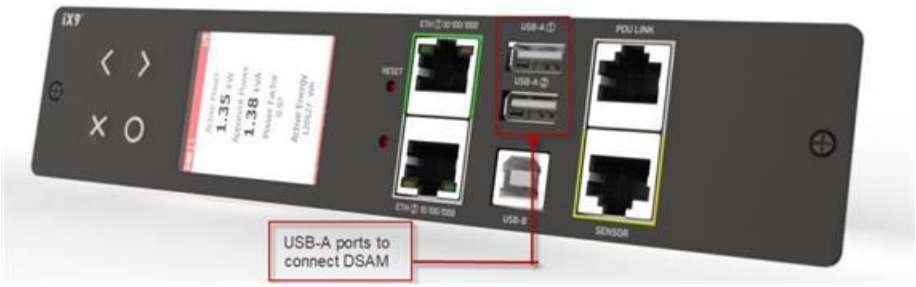
In This Chapter

DSAM Connection. 216
DSAM LED Operation. 216
View DSAM Serial Ports 217
Configure DSAM Serial Ports. 217
Connect to DSAM Serial Targets in the Web Interface. 219
DSAM CLI Commands. 219
Connect to DSAM Serial Targets via SSH. 221

DSAM Connection

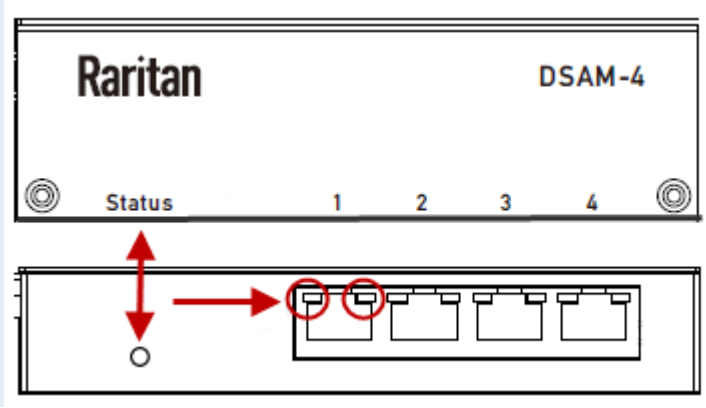
► *To connect DSAM to PX4:*

- Connect the DSAM unit's USB cable to the PX4 USB-A ports. No USB Hubs are supported
- Connect the serial devices to the serial ports on the DSAM unit.
- The serial access ports of DSAM can operate in DTE (Data Terminal Equipment) or DCE (Data Circuit Terminating Equipment) mode



DSAM LED Operation

The DSAM unit has one LED for status, and 2 LEDs on each port.



► *Status LED:*

The Status LED is labeled on the unit front. Light is on back. The Status LED gives information at bootup and upgrade.

- Green LED - Slow blink: DSAM booting up but not controlled by PX4.
- Blue LED - Slow blink: DSAM controlled by PX4.
- Blue LED - Fast blink: Firmware upgrade in progress.

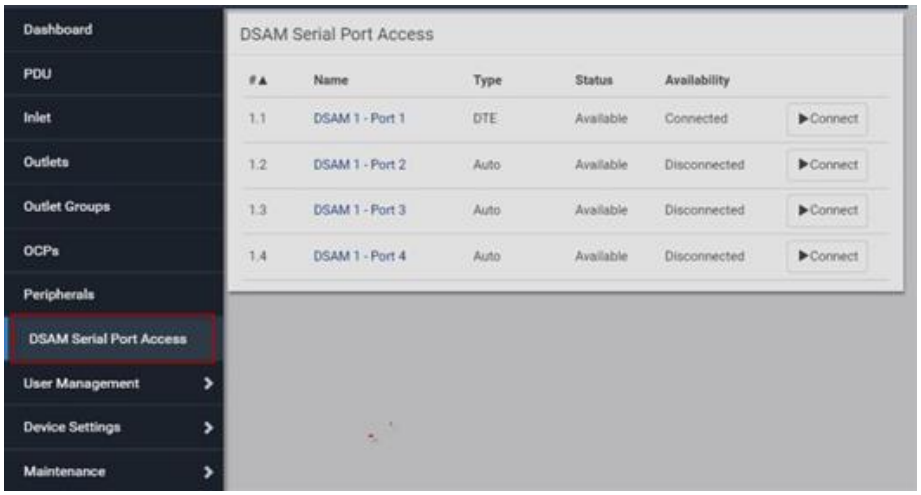
► *Port LEDs:*

Each port has a left Green LED and a right Yellow LED.

- Green LED: Port is set as DCE
- Yellow LED: Port is set as DTE
- LEDs off: Port is set as AUTO and no target is connected

View DSAM Serial Ports

When a DSAM unit is connected to the PX4, a DSAM Serial Ports page is available.



► *To view DSAM serial ports:*

Click DSAM Serial Port Access. You can access and configure serial ports from this page.

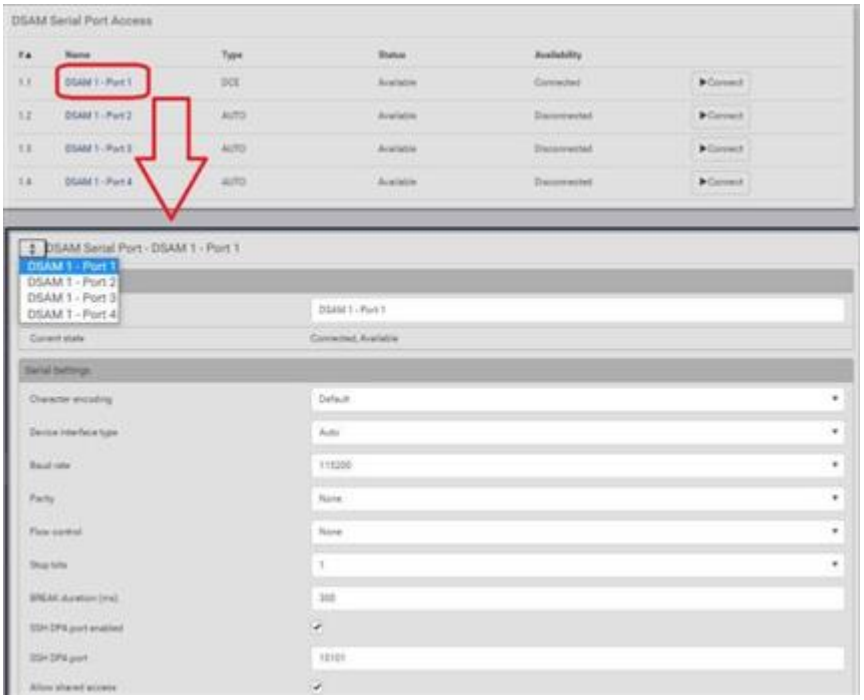
- Ports are listed by physical USB position on the DSAM unit.
- # column indicates which PX4 USB port DSAM is plugged into.
- Type column indicates port's DTE/DCE setting.
- Status and Availability columns show current activity.

Configure DSAM Serial Ports

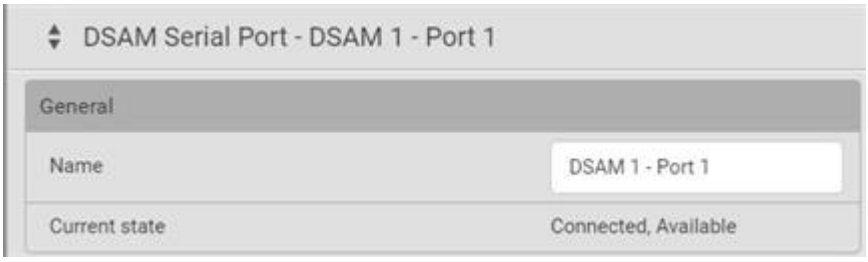
You can rename serial ports and configure their settings.

► *To configure DSAM serial ports:*

1. Click DSAM Serial Port Access, then click the name of the port for the port you want to configure.



2. In the General section:

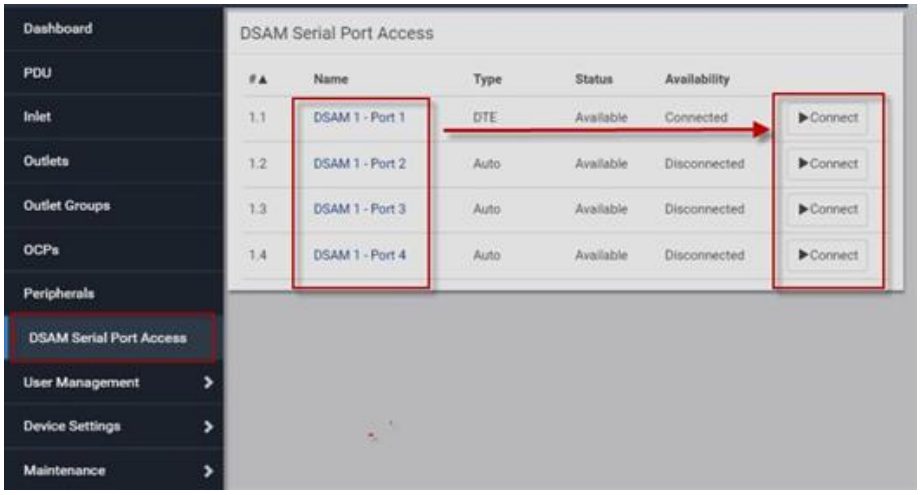


- Enter a Name for the port.
- Check the Current State of the port. Status and Availability are listed.

3. In the Serial Settings section, check or change the following settings:

Raritan
A brand of legrand

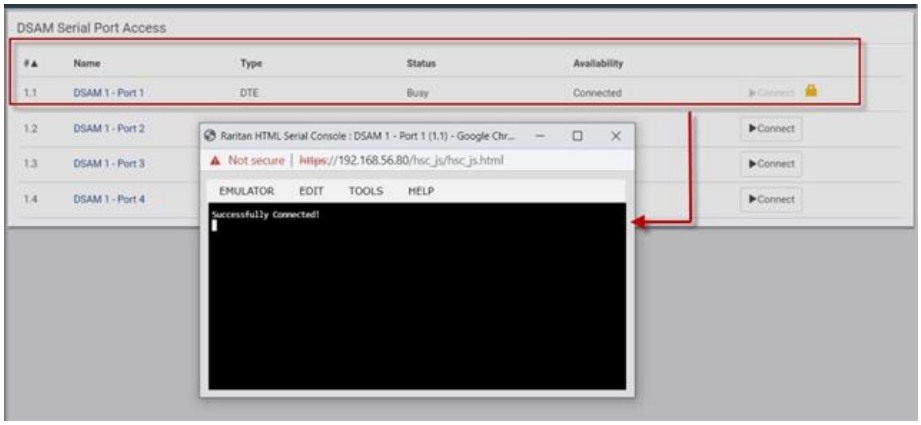
Connect to DSAM Serial Targets in the Web Interface



► *To connect to DSAM serial targets in the web interface:*

1. Click DSAM Serial Port Access to view the list of ports.
2. Click Connect button of the port you want to connect to.

HSC launches in a new window.



DSAM CLI Commands

- show
  - show sxport [<sxportid>]
    Shows serial access port parameters
  - sxportid Serial access port id (or 'all') (1.1/1.2/all) [all]
    Shows DSAM serial port parameters

Example:

```
# show sxport 1.1
```

Port ID: 1.1
Name: DSAM 1 - Port 1
Device connected: No
Device interface type: Automatic
Baud rate: 9600
Parity: None
Data bits: 8
Stop bits: 1
Flow control: None
BREAK duration: 300 ms
SSH DPA port enabled: No
SSH DPA port: 10101
Allow shared access: No
Status: Available

- connect:
  Connect to a DSAM serial port
  - `connect` [<sxportid>]

Note: You have write access to this port

During connecting to target, Pressing the escape sequence (CONTROL-]) the following target port CLI command can be reached:

clientlist Display all users on the port
close Close this target connection
getwrite Get write access for the port
resetport Reset port
return Return to the target session
sendbreak Send a break to the connected target
writelock Lock write access to this port
writeunlock Unlock write access to this port
Pressing ? will provide help

- config
  You can configure only connected DSAMs ports
  - config:# sxport
    sxport <sxportid> [name <name>] [devinterfacetype <deviftype>] [baudrate <baudrate>] [parity <parity>] [stopbits <stopbits>] [flowcontrol <flowcontrol>] [breakduration <breakduration>] [sshdpaportenabled <sshdpaportenabled>] [sshdpaport <sshdpaport>] [allowsharedaccess <allowsharedaccess>]
    Configure serial access port settings:
    sxportid Serial access port id (1.1/1.2)
    name Port name
    devinterfacetype Device interface type (AUTO/DTE/DCE)
    baudrate Serial port speed (baud rate) in bits-per-second (1200/1800/2400/4800/9600/19200/38400/57600/115200/230400)

parity Parity type (none/odd/even)
stopbits Number of stop bits (1..2)
flowcontrol Flow control type (none/hw/sw)
breakduration Duration of BREAK signal in ms (0..1000)
sshdpaportenabled Enable direct port access via Secure Shell (SSH) (true/false)
sshdpaport TCP port for direct port access via Secure Shell (SSH) (1024..49999)
allowsharedaccess Allow shared (r/o) access (true/false)

Connect to DSAM Serial Targets via SSH

► *To connect to DSAM serial targets via SSH:*

1. Make sure that SSH Access is enabled in Device Settings > Network Services > SSH.
2. Connect to the port in two ways:

- Via configured SSH DPA port:
  1. Type command ssh -p <SSH DPA port> user@device

Note: Make sure SSH DPA port enabled is selected in DSAM Serial Port Access >DSAM Port #.

- Via regular TCP port:
  1. Type command ssh user:1.2@device

1. After login, user will enter CLI interface.
2. Press Escape Sequence ^]
3. Type commands See: DSAM CLI Commands (on page 219)

Example: show sxport 1.1

---

4. To exit serial target, type escape-key-sequence, default is Ctrl-], then enter port sub-menu CLI interface.
5. Type "close", then enter main CLI interface.

User Management

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

PX4 includes a built-in administrator account by default. While this account's roles cannot be changed or deleted, it can be renamed. In addition to the default administrator account, you can create an extra administrative user, which can be disabled, renamed, or removed.

The Admin role is a system-defined role with full privileges. You also have the flexibility to create additional users and roles. These roles define the tasks and actions each user is authorized to perform, so assigning one or more roles to every user is essential.

If you are using remote authentication, you do not have to create users accounts locally. Settings are in Device Settings > Security > Authentication. See Setting Up External Authentication (on page 275).

Creating Users

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

To add users, choose User Management > Users > then click the Add User icon + New User .

Raritan.
A brand of legrand

► *User information:*

Field/setting	***Description***
User name	***The name the user enters to log in.*** • 1 to 32 characters • Case sensitive • Colon character :, forward slash /, and spaces are NOT permitted.
Full name	***The user's first and last names.***
Password, ***Confirm password***	• 4 to 64 characters • Case sensitive • Spaces are permitted.
Telephone number	***The user's telephone number***
Email address	***The user's email address*** • Up to 128 characters • Case sensitive
Enable	***When selected, the user can log in.***
Force password change on next login	***When selected, a password change request automatically appears the next time the user logs in.***

► *SSH:*

You need to enter the SSH public key only if public key authentication for SSH is enabled.

1. Open the SSH public key with a text editor.
2. Copy and paste all content in the text editor into the SSH Public Key field.

► *SNMPv3:*

The SNMPv3 access permission is disabled by default.

Field/ setting	**Description**
Enable SNMPv3	Select this checkbox when intending to permit the SNMPv3 access by this user. Note: The SNMPv3 protocol must be enabled for SNMPv3 access.

Field/ setting	Description
Security level	Click the field to select a preferred security level from the list: • None • Authentication: Authentication and no privacy. • Authentication & Privacy: Authentication protocol SHA-1, privacy protocol AES-128. Default.

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

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

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

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

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

Field/setting	Description
Authentication	Click this field to select the desired authentication protocol. Two protocols are available: • MD5 • SHA-1 (default) • SHA-224 • SHA-256 • SHA-384 • SHA-512

Field/setting	Description
Privacy	Click this field to select the desired privacy protocol. Two protocols are available: • DES • AES-128 (default) • AES-192 • AES-256 • AES-192 (3DES key extension) • AES-256 (3DES key extension)

► *Preferences:*

This section determines the measurement units displayed in the web interface and CLI for this user. The user can also change these in the User Management > User Preferences page. SNMP uses the defaults set in User Management > Default Preferences.

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

► *Roles:*

Select one or multiple roles to determine the user's permissions. A user can have a maximum of 32 roles. Note: With multiple roles selected, a user has the union of all roles' permissions.

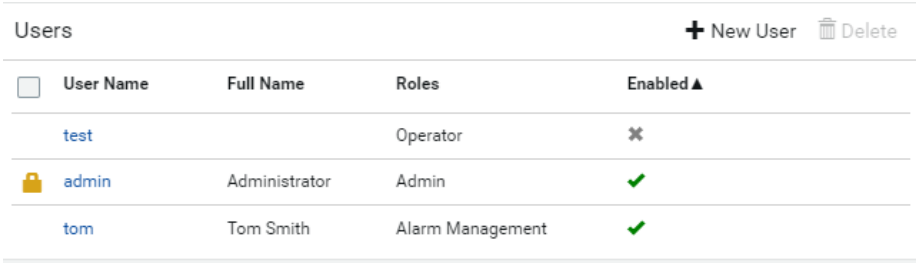
If the built-in roles do not satisfy your needs, add new roles by clicking New Role. This newly-created role will be then automatically assigned to the user account currently being created.

Built-in role	Description
Admin	Provide full permissions.

Built-in role	Description
Operator	Provide frequently-used permissions, including: • Acknowledge Alarms • Change Own Password • Change Pdu, Inlet, Outlet & Overcurrent Protector Configuration (if your model is a PDU) • Switch Outlet (if your model supports it) • Switch Outlet Group (if your model supports it) • Change PMC, PMB, & PMM Configuration (if your model is a branch circuit monitor) • View Event Settings • View Local Event Log

Editing or Deleting Users

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



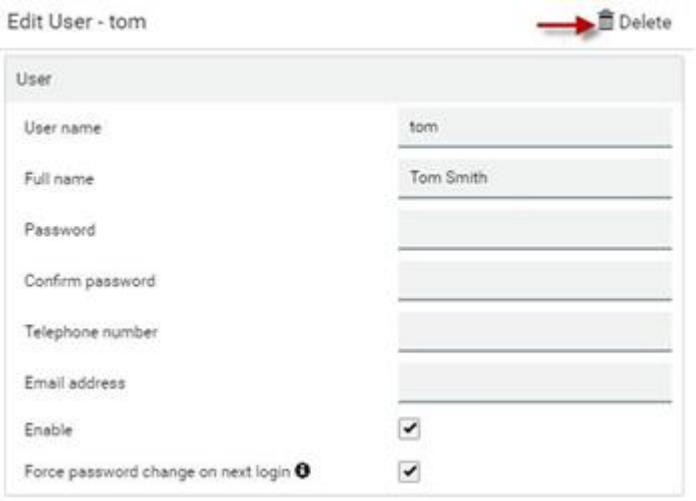
In the Enabled column:

- ✔ : The user is enabled.
- ✖ : The user is disabled.
- Sort the list by clicking the header.

► *To edit or delete a user account:*

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

- You can rename the user. This action is logged.
- To change the password, type a new password in the Password and Confirm Password fields. If the password field is left blank, the password remains unchanged.
- To delete this user, click Delete , and confirm the operation.

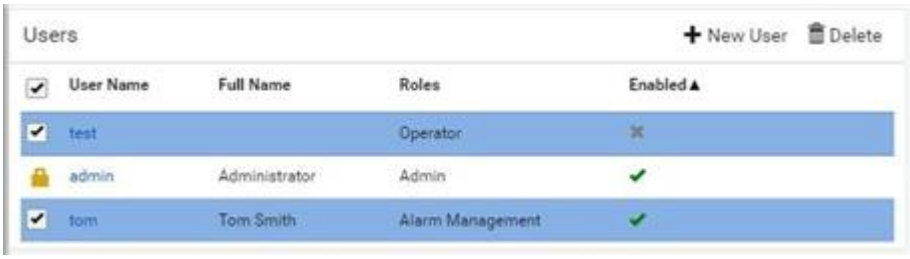


2. Click Save for changes.

► *To delete multiple user accounts:*

1. On the Users page, select users by clicking the checkboxes.
2. Click the Delete icon Delete then click to confirm.

Note: You cannot delete the original factory-default Administrator account, but you can disable it.



Creating Roles

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

The PX4 provides two built-in roles.

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

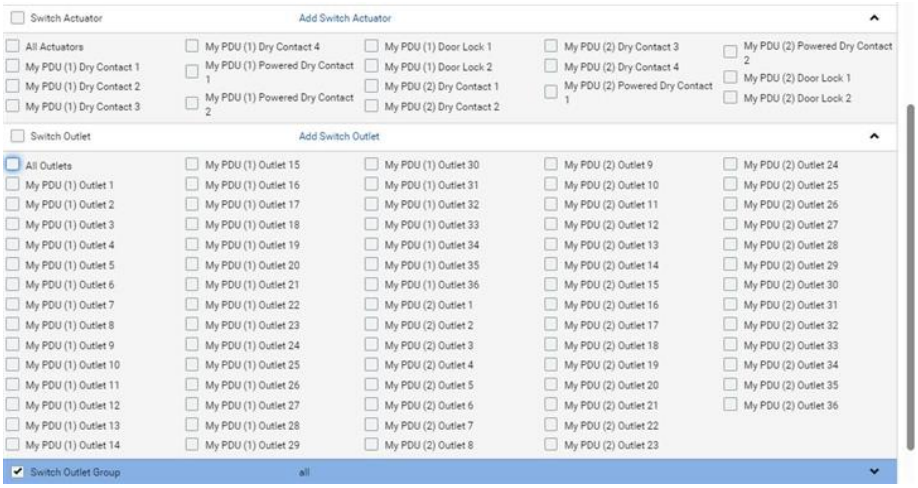
If the two roles do not satisfy your needs, add new roles. Up to 64 roles are supported.

► *To create a role:*

1. Choose User Management > Roles > New icon + New Role .

2. Assign a role name.
   - 1 to 32 characters long
   - Case sensitive
   - Spaces are permitted
3. Type a description for the role in the Description field.

4. Select the desired privilege(s).
   - The 'Administrator Privileges' includes all privileges.
   - The 'Unrestricted View Privileges' includes all 'View' privileges.
5. Some privileges have additional selections. These rows contain a blue hyperlink and expand arrow. Click either to view options.
   - For example, in the Switch Actuator and Switch Outlet privileges, you can specify the actuators and outlets that users can switch on/off.



6. Click Save. The role is created and you can assign it to any user.

Editing or Deleting Roles

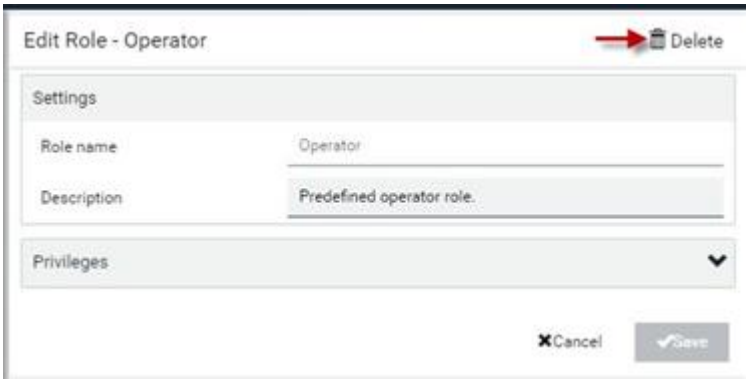
Roles cannot be renamed, but you can delete them or change their included privileges.

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

The built-in Admin role displays the lock icon . You cannot delete it or change it.

► *To edit a role:*

1. On the Roles page, click the desired role. The Edit Role page opens.
   - You can edit the description or change the privileges.
   - To delete this role, click Delete, and confirm the operation.



2. Click Save.

► *To delete any roles:*

1. On the Roles page, select the checkboxes for roles you want to delete.
2. Click the Delete icon Delete then click Delete in the confirmation message.

Setting Your Preferred Measurement Units

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

Measurement unit changes apply to the web interface and CLI. SNMP uses the default measurement units. See Setting Default Measurement Units (on page 231).

Setting your own preferences does not change the default measurement units.

► *To set user preferences:*

1. Choose User Management > User Preferences.
2. Make changes as needed.

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

3. Click Save.

Raritan
A brand of legrand

Setting Default Measurement Units

User preferences apply to displays in the GUI and CLI for locally authenticated users. Default preferences apply to the front panel and SNMP, and to remote-authenticated users.

► *To set up default user preferences:*

1. Click User Management > Default Preferences.
2. Make changes as needed.

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

3. Click Save.

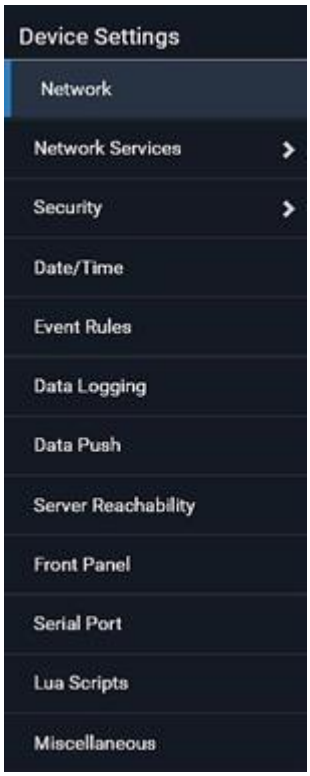
User Interfaces Showing Default Units

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

- Web interface for "newly-created" local users when they have not configured their own preferred measurement units.
- Web interface for users who are remotely authenticated.
- The sensor report triggered by the "Send Sensor Report" action.
- Front panel LCD display.

Device Settings

Click 'Device Settings' in the *Menu.*



Network Settings

Configure wired, wireless, and Internet protocol-related settings on the Network page after connecting the PX4 to your network.

You can enable both wired and wireless networking to assign multiple IP addresses—one for wired and one for wireless connections. For example, enabling an Ethernet interface allows you to obtain an IPv4 and/or IPv6 address, while configuring the wireless interface provides an additional IPv4 and/or IPv6 address. This setup also supports port forwarding mode, enabling PX4 to handle more than one IPv4 or IPv6 address simultaneously.

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

Default gateways are configured per interface.

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

Raritan
A brand of legrand

► *After enabling either or both Internet protocols:*

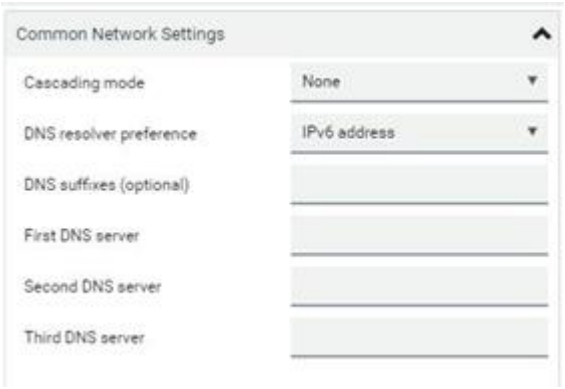
After enabling IPv4 and/or IPv6, all but not limited to the following protocols will be compliant with the selected Internet protocol(s):

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

Note: PX4 disables TLS *1.0* and *1.1* by default. It enables only TLS *1.2* and *1.3.*

Common Network Settings

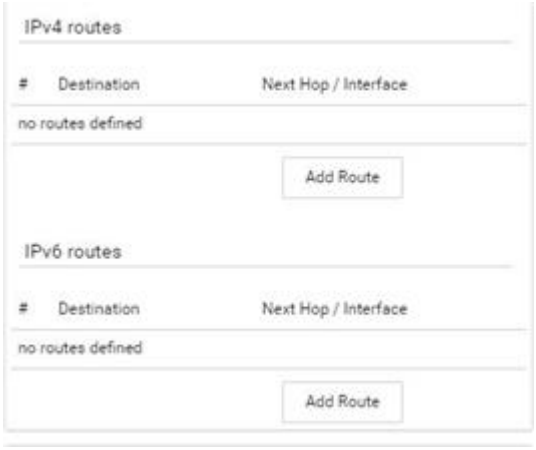
Common Network Settings are OPTIONAL, not required. Therefore, leave them unchanged if there are no specific local networking requirements.



Field	Description
Cascading mode	Leave it to the default "None" unless you are establishing a cascading chain. • Setting the Cascading Mode (on page 247)
DNS resolver preference	Determine which IP address is used when the DNS resolver returns both IPv4 and IPv6 addresses. • IPv4 address: Use the IPv4 addresses. • IPv6 address: Use the IPv6 addresses.

Field	Description
DNS suffixes (optional)	Specify a DNS suffix name if needed.
First/Second/ Third DNS server	Manually specify static DNS server(s). • If any static DNS server is specified in these fields, it will override the DHCP-assigned DNS server. • If DHCP (or Automatic) is selected for IPv4/IPv6 settings, and there are NO static DNS servers specified, DHCP-assigned DNS servers are used.

You can manually configure or the route information using IPv4 and IPv6 static routes. See Static Route Examples (on page 244) and Static Route Interface Names (on page 246).



802.1x Security Overview

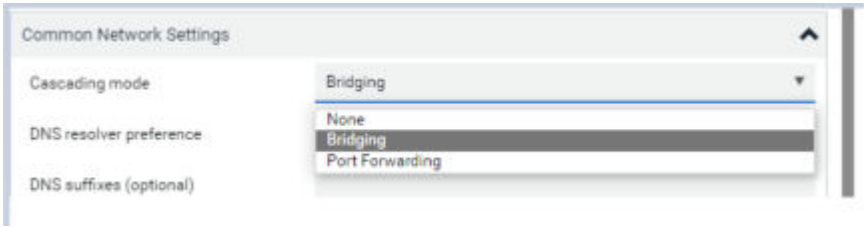
You can configure IEEE 802.1X authentication individually on each LAN port to ensure secure access for PX4 on both LAN and WLAN networks. This authentication protocol verifies a user's identity using their credentials or a certificate, which is validated by a RADIUS authentication server. IEEE 802.1X relies on the uploaded certificate from the Certificate Repository to perform identity verification. PX4 supports EAP_TLS and EAP_PEAP as authentication methods to securely exchange information. See Setting Up a TLS Certificate (on page 270) to configure and upload the proper certificate.

Ethernet (Wired) Interface Settings

On the Network page, click the ETHERNET section if the PX4 has one port or click ETH1 and ETH2 sections respectively to configure each port. By default, both ETH1 and ETH2 interfaces are enabled.

► *Bridging Cascading mode:*

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



► *IPv4 settings:*

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

- DHCP settings: Optionally specify the preferred hostname, which must meet the following requirements:
  - Consists of alphanumeric characters and/or hyphens
  - Cannot begin or end with a hyphen
  - Cannot contain more than 63 characters
  - Cannot contain punctuation marks, spaces, and other symbols
- Static settings:
  - Assign a static IPv4 address, which follows this syntax "IP address/prefix length". Example: *192.168.84.99/24*
  - Assign a Default Gateway.

► *IPv6 settings:*

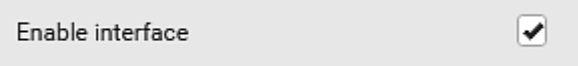
Field/setting	***Description***
Enable IPv6	***Enable or disable the IPv6 protocol.***
IP auto configuration	***Select the method to configure IPv6 settings.*** ● ***Automatic: Auto-configure IPv6 settings via DHCPv6.*** ● ***Static: Manually configure the IPv6 settings.***

Field/setting	*Description*
Preferred hostname	• *Enter the hostname you prefer for IPv6 connectivity*

- Automatic settings: Optionally specify the preferred hostname, which must meet the above requirements.
- Static settings:
  - Assign a static IPv6 address, which follows this syntax "IP address/prefix length".
    Example: *fd07:2fa:6cff:1111::0/128*
  - Assign a Default Gateway.

► *Enable Interface:*

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



► *Other Ethernet settings:*

Field	**Description**
Speed	Select a LAN speed. • *Auto:* System determines the optimum LAN speed through auto-negotiation. • *10 MBit/s:* Speed is always 10 Mbps. • *100 MBit/s:* Speed is always 100 Mbps. • *1 GBit/s:* Speed is always 1 Gbps (1000 Mbps).
Duplex	Select a duplex mode. • *Auto:* Selects the optimum transmission mode through auto-negotiation. • *Full:* Data is transmitted in both directions simultaneously. • *Half:* Data is transmitted in one direction at a time.
Current state	Show the LAN's current status, including the current speed and duplex mode.
MTU	• Set the MTU from 1280 to 1500.

Field	Description
Enable LLDP	• Default is enabled. When LLDP is enabled, device discovery is possible with LLDP management software that is often present in network switches.
Authentication	Select an authentication method. • *No Authentication:* No authentication data is required. • *EAP: PX4 supports 802.1X (EAP) Network Authentication. You must have a client-side certificate to communicate with the authentication server. Enter required authentication data in the fields that appear.*
Outer authentication	This field appears when 'EAP' is selected. There are two authentication methods for EAP. • *PEAP:* A TLS tunnel is established, and an inner authentication method can be specified for this tunnel. • *TLS:* Authentication between the client and authentication server is performed using TLS certificates.
Inner authentication	This field appears when both 'EAP' and 'PEAP' are selected. • *MS-CHAPv2:* Authentication based on the given password using MS-CHAPv2 protocol. • *TLS:* Authentication between the client and authentication server is performed using TLS certificates.
Identity	This field appears when 'EAP' is selected. Type your user name.
Password	This field appears only when 'EAP', 'PEAP' and 'MS-CHAPv2' are all selected. Type your password.

Field	Description
Client certificate, Client private key, Client private key password	A client certificate is required for two scenarios: (1) EAP+TLS, (2) EAP+PEAP+TLS . PEM encoded X.509 certificate and PEM encoded private key are required for certification-based authentication methods. Private key password is optional. • Private keys in PKCS#1 and PKCS#8 formats are supported. • Client Private Key Password should be entered only when your private key is encrypted with a password. • To view the uploaded certificate, click Show Client Certificate. • To remove the uploaded certificate and private key, click 'Clear Key/Certificate selection'.
CA certificate	This field appears when 'EAP' is selected. CA certificate is required when "Enable verification of TLS certificate chain" is selected by default; and strongly recommended
RADIUS authentication server name	This field appears when 'EAP' is selected. Type the name of the RADIUS server if it is present in the TLS certificate. • The name must match the fully qualified domain name (FQDN) of the host shown in the certificate Do not leave this field blank as it reduces security.

Note: Auto-negotiation is disabled after setting both the speed and duplex settings to NON-Auto values, which may result in a duplex mismatch.

- Available settings for the CA Certificate:

If the required certificate file is a chain of certificates, and you are not sure about the requirements of a certificate chain, see TLS Certificate Chain.

Field/setting	Description
Enable verification of TLS certificate chain	Select this checkbox to verify the certificate of the EAP authentication server. Then you must upload the certificate of the issuing CA in the next field.

Field/setting	Description
Browse button	Click this button to import the certificate of the issuing CA. Then you can: • Click Show to view the certificate's content. • Click Remove to delete the installed certificate if it is inappropriate.
Allow expired and not yet valid certificates	• Select this checkbox to make the authentication succeed regardless of the certificate's validity period. • After deselecting this checkbox, the authentication fails whenever any certificate in the selected certificate chain is outdated or not valid yet.
Allow connection if system clock is incorrect	If powered off for a long time, the system time may be incorrect. When this checkbox is deselected, and if the system time is incorrect, the installed TLS certificate is considered not valid yet and will cause the network connection to fail. When this checkbox is selected, it will make the network connection successful when the system time is earlier than the firmware build before synchronizing with any NTP server.

Wireless Network Settings

Wireless network is not supported for Bridging mode or for Expansion units in port forwarding mode.

Wireless interface is disabled by default. Enable it to use wireless networking.

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

► *Interface Settings:*

Field/setting	Description
Enable interface	Enable or disable the wireless interface. When disabled, the wireless networking fails.
Hardware state	Check this field to ensure that a wireless USB LAN adapter is detected. If not, verify that the USB LAN adapter is firmly connected or that it is supported.
SSID	Type the name of the wireless access point (AP).
Force AP BSSID	If the BSSID is available, select this checkbox.
BSSID	Type the MAC address of an access point.

Field/setting	Description
MTU	Set the Maximum Transmission Unit from 1280 to 1500.
Enable High Throughput (802.11n)	Enable or disable 802.11n protocol.
Authentication	Select an authentication method. • *No Authentication:* No authentication data is required. • *PSK*: A Pre-Shared Key is required. • *EAP:* PX4 supports 802.1X (EAP) Network Authentication. Enter required authentication data in the fields that appear.
Pre-Shared Key	This field appears only when PSK is selected. Type the PSK string.
Outer authentication	This field appears when 'EAP' is selected. There are two authentication methods for EAP. • *PEAP:* A TLS tunnel is established, and an inner authentication method can be specified for this tunnel. • *TLS:* Authentication between the client and authentication server is performed using TLS certificates.
Inner authentication	This field appears when both 'EAP' and 'PEAP' are selected. • *MS-CHAPv2:* Authentication based on the given password using MS-CHAPv2 protocol. • *TLS:* Authentication between the client and authentication server is performed using TLS certificates.
Identity	This field appears when 'EAP' is selected. Type your user name.
Password	This field appears only when 'EAP', 'PEAP' and 'MS-CHAPv2' are all selected. Type your password.

Field/setting	Description
Client certificate, Client private key, Client private key password	This field appears when 'EAP', 'PEAP' and 'TLS' are all selected. PEM encoded X.509 certificate and PEM encoded private key are required for certification-based authentication methods. Private key password is optional. • Private keys of PKCS#1 and PKCS#8 formats are supported. • Client Private Key Password should be entered only when your private key is encrypted with a password. • To view the uploaded certificate, click Show Client Certificate. • To remove the uploaded certificate and private key, click 'Clear Key/Certificate selection'.
CA certificate	This field appears when 'EAP' is selected. A third-party CA certificate may or may not be needed. If needed, follow the steps below.
RADIUS authentication server name	This field appears when 'EAP' is selected. Type the name of the RADIUS server if it is present in the TLS certificate. • The name must match the fully qualified domain name (FQDN) of the host shown in the certificate.

- Available settings for the CA Certificate:

If the required certificate file is a chain of certificates, and you are not sure about the requirements of a certificate chain, see TLS Certificate Chain.

Field/setting	Description
Enable verification of TLS certificate chain	Select this checkbox for the PX4 to verify the validity of the TLS certificate that will be installed. • For example, the certificate's validity period against the system time is checked.
Browse button	Click Browse to import a certificate file. Then you can: • Click Show to view the certificate's content. • Click Remove to delete the installed certificate if it is inappropriate.

Field/setting	Description
Allow expired and not yet valid certificates	• Select this checkbox to make the authentication succeed regardless of the certificate's validity period. • After deselecting this checkbox, the authentication fails whenever any certificate in the selected certificate chain is outdated or not valid yet.
Allow connection if system clock is incorrect	When this checkbox is deselected, and if the system time is incorrect, the installed TLS certificate is considered not valid yet and will cause the wireless network connection to fail. When this checkbox is selected, it will make the wireless network connection successful when the PX4 system time is earlier than the firmware build before synchronizing with any NTP server.

► *IPv4 settings:*

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

- DHCP settings: Optionally specify the preferred hostname, which must meet the following requirements:
  - Consists of alphanumeric characters and/or hyphens
  - Cannot begin or end with a hyphen
  - Cannot contain more than 63 characters
  - Cannot contain punctuation marks, spaces, and other symbols
- Static settings: Assign a static IPv4 address, which follows this syntax "IP address/prefix length".
  Example: *192.168.84.99/24*

► *IPv6 settings:*

Field/setting	***Description***
Enable IPv6	***Enable or disable the IPv6 protocol.***
IP auto configuration	***Select the method to configure IPv6 settings.*** • ***Automatic: Auto-configure IPv6 settings via DHCPv6.*** • ***Static: Manually configure the IPv6 settings.***

Field/setting	*Description*
Preferred hostname	• *Enter the hostname you prefer for IPv6 connectivity*

- Automatic settings: Optionally specify the preferred hostname, which must meet the above requirements.
- Static settings: Assign a static IPv6 address, which follows this syntax "IP address/prefix length". Example: *fd07:2fa:6cff:1111::0/128*

► *(Optional) To view the wireless LAN diagnostic log:*

- Click Show WLAN Diagnostic Log. See Diagnostic Log for Network Connections (on page 243)

Diagnostic Log for Network Connections

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

The diagnostic log shows data only after connection errors are detected.

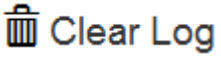
Each entry in the log consists of:

- ID number
- Date and time
- Description

► *To view the log:*

1. Access the diagnostic log with either method below.
   - Choose Device Settings > Network > ETH1/ETH2 > Show EAP Authentication Log.
   - Choose Device Settings > Network > WIRELESS > Show WLAN Diagnostic Log.
2. The log is refreshed automatically at a regular interval of five seconds.
   - To avoid any new events' interruption during data browsing, you can suspend the automatic update by clicking Pause.
   - To restore automatic update, click Resume. Those new events that have not been listed yet due to suspension will be displayed in the log now.

► *To clear the diagnostic log:*

1. On the top-right corner of the log, click > 

.
2. Click Clear Log on the confirmation message.

Static Route Examples

This section describes two static route examples: IPv4 and IPv6. Both examples assume that two network interface controllers (NIC) have been installed in one network server, leading to two available subnets, and IP forwarding has been enabled. All of the NICs and PX4 devices in the examples use static IP addresses.

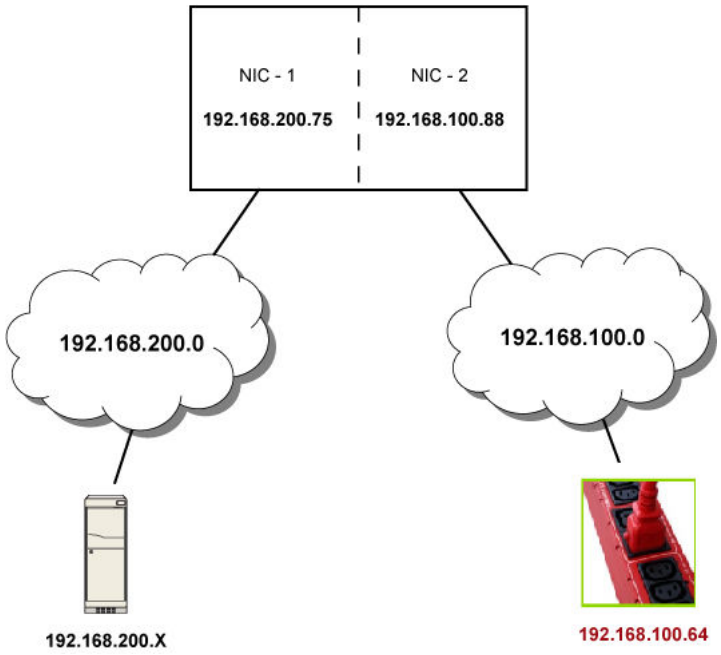
Most of local multiple networks are not directly reachable and require the use of a gateway. Therefore, we will select Gateway in the following examples. If your local multiple networks are directly reachable, you should select Interface rather than Gateway.

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

► *IPv4 example:*

- Your PX4: *192.168.100.64*
- Two NICs: *192.168.200.75* and *192.168.100.88*
- Two networks: *192.168.200.0* and *192.168.100.0*
- Prefix length: *24*

Raritan
A brand of legrand



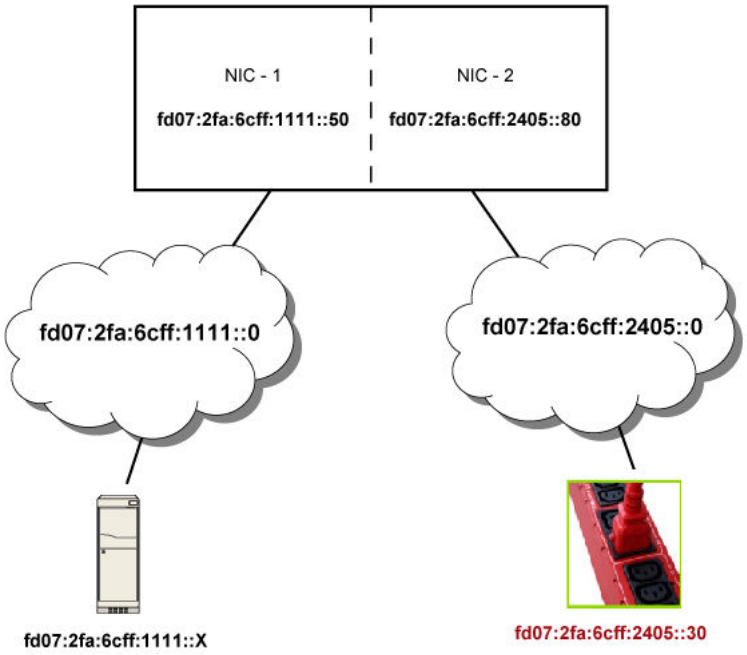
In this example, NIC-2 (192.168.100.88) is the next hop router for your PX4 to communicate with any device in the other subnet 192.168.200.0.

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

Tip: If you have configured multiple static routes, you can click on any route and then make changes, use or to re-sort the priority, or click to delete it.

► *IPv6 example:*

- Your PX4: *fd07:2fa:6cff:2405::30*
- Two NICs: *fd07:2fa:6cff:1111::50* and *fd07:2fa:6cff:2405::80*
- Two networks: *fd07:2fa:6cff:1111::0* and *fd07:2fa:6cff:2405::0*
- Prefix length: *64*



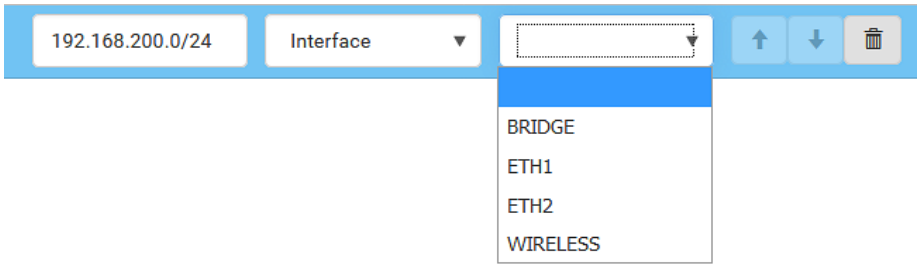
In this example, NIC-2 (fd07:2fa:6cff:2405::80) is the next hop router for your PX4 to communicate with any device in the other subnet fd07:2fa:6cff:1111::0.

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

Tip: If you have configured multiple static routes, use the arrow buttons to sort the priority, or click to delete it.

Static Route Interface Names

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



► *Interface list:*

Interface name	***Description***
BRIDGE	***When another wired network is connected to the Ethernet port of your PX4, and your PX4 has been set to the bridging mode, select this interface name instead of the Ethernet interface.***
ETH1	***When another wired network is connected to the ETH1 port of your PX4, select this interface name.***
ETH2	***When another wired network is connected to the ETH2 port of your PX4, select this interface name.***
WIRELESS	***When another wireless network is connected to your PX4, select this interface name.***

Setting the Cascading Mode

See the Cascading Solution Guide for full details on network setup, physical setup, and supported configurations for all cascades across products. The sections documented here are a brief overview.

The cascading mode configured on the primary device determines the Ethernet sharing method, which is either network bridging or port forwarding. The cascading mode of all devices in the chain must be the same.

You must have the Change Network Settings permission to configure the cascading mode.

Note: Port Forwarding mode does not support APIPA.

► *To configure the cascading mode:*

1. Choose Device Settings > Network > Common Network Settings section.
2. Select the preferred mode in the Cascading Mode field.

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

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

1. For the Port Forwarding mode, you must also configure the following settings.

Note that if either setting below is incorrectly configured, a networking issue occurs.

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

2. (Optional) Configure the network settings by clicking the BRIDGE, ETH1/ETH2, or WIRELESS section on the same page.
   - In the Bridging mode, each cascaded device can have different network settings. You may need to configure each device's network settings in the BRIDGE section.
   - In the Port Forwarding mode, all cascaded devices share the primary device's network settings. You only need to configure the primary device's network settings in the ETH1/ETH2 and/or WIRELESS section.

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

3. Click Save.

► *Recommendations for cascade loops:*

You can connect both the first and the last PDU to your network (cascade loop) under the following conditions:

- Bridging mode only.
- The remaining network MUST use R/STP to avoid network loops.

  AND
- Both the first and the last PDUs MUST either attach to the same switch or, if they are attached to two separate switches, you must configure both ports of these switches so that the STP costs are high. This prevents the STP protocol from sending unrelated traffic through the PDU cascade, which can cause bottlenecks that lead to connectivity issues in the whole network.

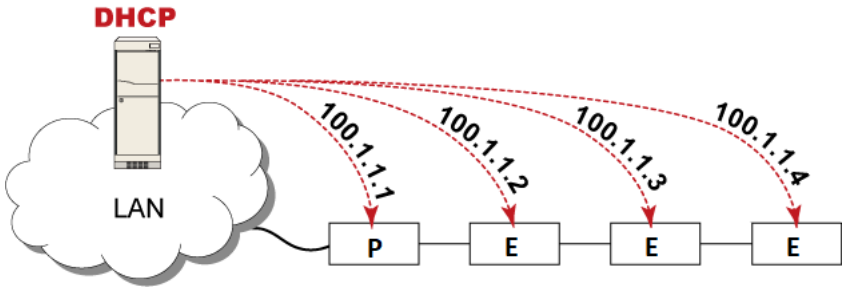
Cascading Modes Overview

The cascading mode is a network configuration setting that determines how each device in the chain is accessed.

There are two cascading modes: Bridging and Port Forwarding.

In the following illustration, it is assumed that users enable the DHCP networking for the cascading chain comprising four devices. In the diagrams, "P" is the primary device and "E" is an expansion device.

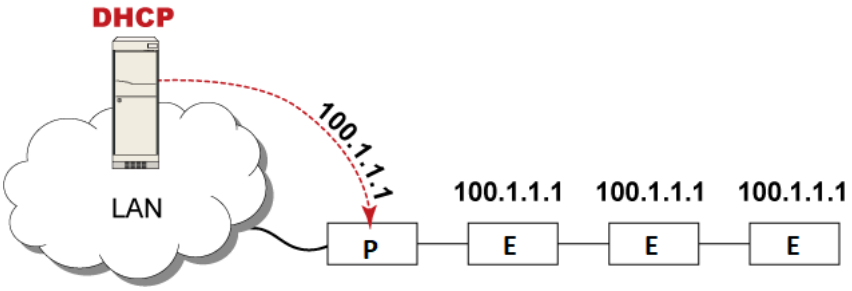
► *"Bridging" mode:*



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

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

► *"Port Forwarding" mode:*



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

You must specify a 5XXXX port number (where X is a number) when remotely accessing any expansion device with the shared IP address. See Port Number Syntax (on page 250), Port Number Syntax (on page 637).

► *Comparison between cascading modes:*

- The Bridging mode supports the wired network only, while the Port Forwarding mode supports both wired and wireless networks.
- Both cascading modes support a maximum of 32 devices in a chain.
- Both cascading modes support both DHCP and static IP addressing.
- In the Bridging mode, each cascaded device has a unique IP address.

  In the Port Forwarding mode, all cascaded devices share the same IP address(es) as the primary device.
- In the Bridging mode, each cascaded device has only one IP address.

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

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

Port Number Syntax

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

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

► *5NNXX port number syntax:*

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

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

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

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

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

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

► *Standard TCP/UDP ports:*

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

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

Protocols	Port Numbers
MODBUS	502

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

Port Forwarding Examples

In this example, Port Forwarding mode is applied to a cascading chain comprising three devices. The IP address is 192.168.84.77.

► *Primary device:*

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

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

Examples using "5NN00" ports:

- To access the primary device via HTTPS, the IP address is: *https://192.168.84.77:50000/*
- To access the primary device via HTTP, the IP address is: *http://192.168.84.77:50100/*
- To access the primary device via SSH, the command is: *ssh -p 50200 192.168.84.77*

Examples using standard TCP/UDP ports:

- To access the primary device via HTTPS, the IP address is: *https://192.168.84.77:443/*
- To access the primary device via HTTP, the IP address is: *http://192.168.84.77:80/*
- To access the primary device via SSH, the command is: *ssh -p 22 192.168.84.77*

► *Expansion 1 device:*

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

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

Examples:

- To access Expansion 1 via HTTPS, the IP address is: *https://192.168.84.77:50001/*
- To access Expansion 1 via HTTP, the IP address is: *http://192.168.84.77:50101/*
- To access Expansion 1 via SSH, the command is: *ssh -p 50201 192.168.84.77*

► *Expansion 2 device:*

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

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

Examples:

- To access Expansion 2 via HTTPS, the IP address is: *https://192.168.84.77:50002/*
- To access Expansion 2 via HTTP, the IP address is: *http://192.168.84.77:50102/*
- To access Expansion 2 via SSH, the command is: *ssh -p 50202 192.168.84.77*

Adding, Removing or Swapping Cascaded Devices

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

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

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

► *To add a device to an existing chain:*

1. Connect the device you will cascade to the LAN and find its IP address, or connect it to a computer.
2. Log in to this device and set its cascading mode to be the same as the existing chain's cascading mode.
3. (Optional) If this device will function as an expansion device, disconnect it from the LAN after configuring the cascading mode.
4. Connect this device to the chain, using either a USB or Ethernet cable.

► *To remove a device from the chain:*

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

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

---

2. Now disconnect it from the cascading chain.

► *To swap the primary and expansion device:*

- In the Bridging mode, you can swap the primary and expansion devices by disconnecting ALL cascading cables from them, and then reconnecting cascading cables. No changes to software settings are required.
- In the Port Forwarding mode, you must follow the procedure below:

Raritan
A brand of legrand

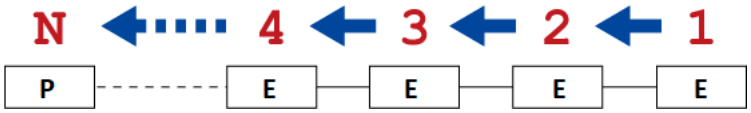
a. Access the expansion device that will replace the primary device, and set its role to 'Primary', and correctly set the downstream interface.
b. Access the primary device, set its role to 'Expansion'.
c. Swap the primary and expansion device now.
   - You must disconnect the LAN cable and ALL cascading cables connected to the two devices first before swapping them, and then reconnecting all cables.

► *To change the cascading mode applied to a chain:*

1. Access the last expansion device, and change its cascading mode.
   - If the new cascading mode is 'Port Forwarding', you must also set its role to 'Expansion'.
2. Access the second to last, third to last and so on until the first expansion device to change their cascading modes one by one.
3. Access the primary device, and change its cascading mode.
   - If the new cascading mode is 'Port Forwarding', you must also set its role to 'Primary', and correctly select the downstream interface.

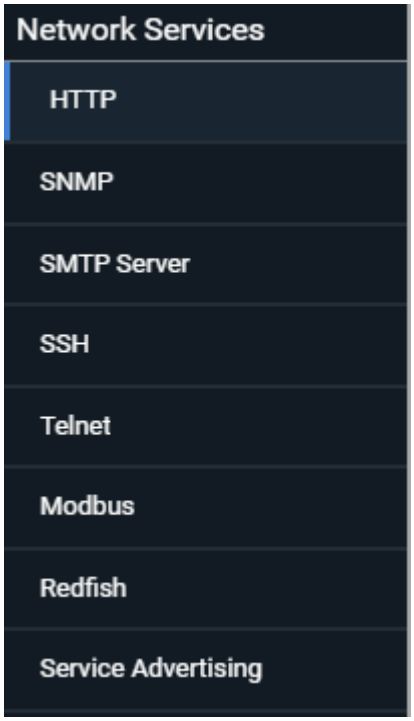
The following diagram indicates the correct sequence. 'N' is the final one.

- P = Primary device
- E = Expansion device



Configuring Network Services

PX4 supports the following network communication services.



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

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

Important: PX4 uses TLS rather than SSL.

Changing HTTP(S) Settings

HTTPS uses Transport Layer Security (TLS) technology to encrypt all traffic to and from the PX4 so it is a more secure protocol than HTTP. PX4 disables TLS *1.0* and *1.1* by default. It enables only TLS *1.2* and *1.3.*

By default, any access to the PX4 via HTTP is automatically redirected to HTTPS. You can disable this redirection if needed.

► *HTTP and HTTPS settings:*

1. Choose Device Settings > Network Services > HTTP.
2. HTTP settings:
   - Enable or disable HTTP access.
   - Default port is 80. You can enter a custom port.
   - Enforce use of HTTPS: Select the checkbox to Redirect HTTP connections to HTTPS.
3. HTTPS settings:
   - Enable or disable HTTPS access.
   - Enable HSTS: Default is enabled.
   - Default port is 443. You can enter a custom port.

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

► *Special note for AES ciphers:*

The PX4 device's TLS-based protocols support AES 128- and 256-bit ciphers. The exact cipher to use is negotiated between PX4 and the client (such as a web browser), which is impacted by the cipher priority of PX4 and the client's cipher availability/settings.

Tip: To force PX4 to use a specific AES cipher, refer to your client's user documentation for information on configuring AES settings. For example, you can enable a cipher and disable the other in the browser via the "about:config" command.

Regaining Access with HSTS and Expired Certificate

HSTS is enabled by default in the Device Settings > Security > HTTP settings. When HSTS is enabled, you can only access PX4 via web browser when a valid, unexpired certificate is installed. HSTS removes the ability for users to click through warnings about invalid certificates.

If access is lost due to HSTS restrictions, there are 2 methods to regain access.

► *Replace the certificate locally on the PX4:*

1. Save the new key and certificate to a USB drive.
2. Use one of the USB configuration methods to upload the new certificate to the device.

► *Replace the certificate over an insecure connection:*

1. Disable the client web browser HSTS security, and then access the PX4 "insecurely."
2. Replace the certificate in Device Settings > Security > TLS Certificates, then enable the HSTS security.

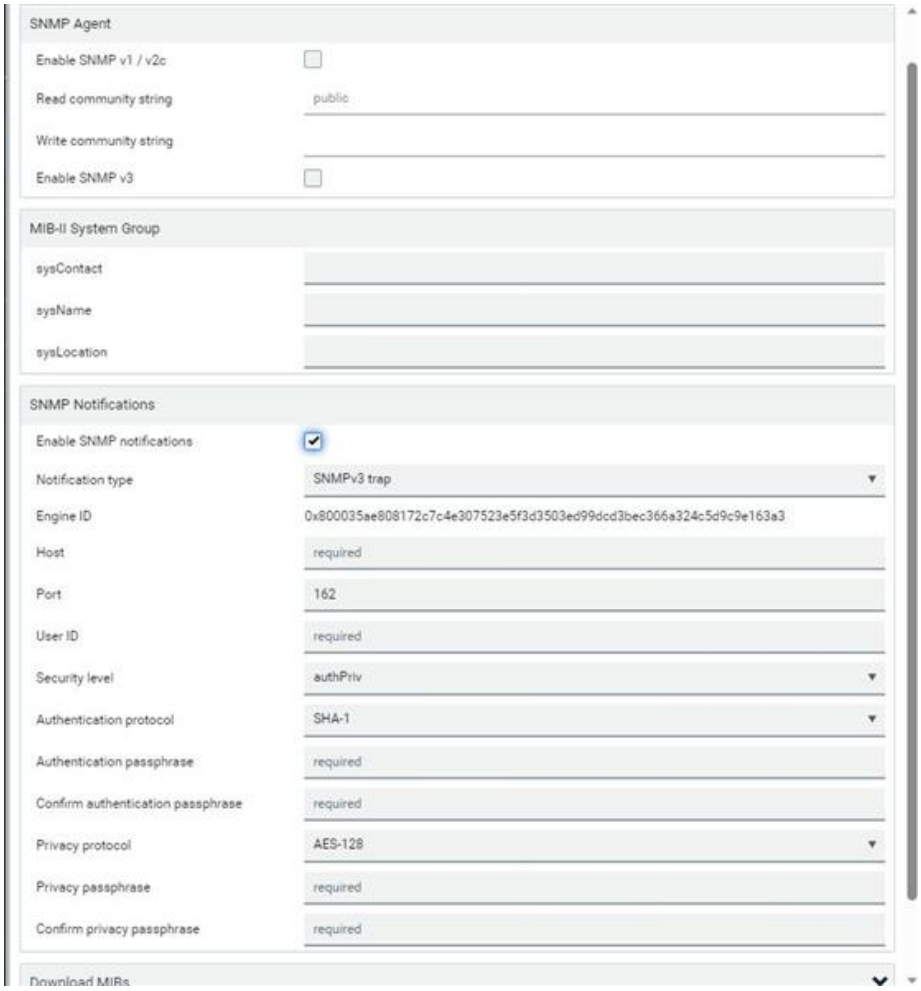
Configuring SNMP Settings

You can enable or disable SNMP communication between an SNMP manager and the PX4. Enabling SNMP communication allows the manager to retrieve and even control the power status of each outlet.

You may also need to configure the SNMP destination(s) if the built-in "System SNMP Notification Rule" is enabled and the SNMP destination has not been set yet. See Event Rules and Actions (on page 291).

► *To configure SNMP communication:*

1. Choose Device Settings > Network Services > SNMP.



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

a. Select the 'Enable SNMP notifications' checkbox.
b. Select a notification type -- SNMPv2c trap, SNMPv2c inform, SNMPv3 trap, and SNMPv3 inform.
c. Specify the SNMP notification destinations and enter necessary information. For details, refer to:
   - SNMPv2c Notifications
   - SNMPv3 Notifications

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

5. You must download the SNMP MIB for your PX4 to use with your SNMP manager.
   a. Click the Download MIBs title bar to show the download links.

   b. Click the PDU2-MIB download link. See Downloading SNMP MIB.
6. Click Save.

Configuring SMTP Settings

The PX4 can be configured to send alerts or event messages to a specific administrator by email. To send emails, you have to configure the SMTP settings and enter an IP address for your SMTP server and a sender's email address.

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

► *To set SMTP server settings:*

1. Choose Device Settings > Network Services > SMTP Server.
2. Enter the information needed.

Field	Description
IP address/host name	Type the name or IP address of the mail server.
Port	Type the port number. • Default is 25
Sender email address	Type an email address for the sender.
Number of sending retries	Type the number of email retries. • Default is 2 retries
Time between sending retries	Type the interval between email retries in minutes. • Default is 2 minutes.

Field	Description
Server requires authentication	Select this checkbox if your SMTP server requires password authentication.
User name, Password	Type a user name and password for authentication after selecting the above checkbox. • The length of user name and password ranges between 4 and 64. Case sensitive. • Spaces are not allowed for the user name, but allowed for the password.
Enable SMTP over TLS (StartTLS)	If your SMTP server supports the Transport Layer Security (TLS), select this checkbox.

- Settings for the CA Certificate:

If the required certificate file is a chain of certificates, and you are not sure about the requirements of a certificate chain, see TLS Certificate Chain.

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

3. Now that you have set the SMTP settings, you can test it to ensure it works properly.
   a. Type the recipient's email address in the 'Recipient email addresses' field. Use a comma to separate multiple email addresses.
   b. Click Send Test Email.
   c. Check if the recipient(s) receives the email successfully.
4. Click Save.

► *Special note for AES ciphers:*

The PX4 device's TLS-based protocols support AES 128- and 256-bit ciphers. The exact cipher to use is negotiated between PX4 and the client (such as a web browser), which is impacted by the cipher priority of PX4 and the client's cipher availability/settings.

Tip: To force PX4 to use a specific AES cipher, refer to your client's user documentation for information on configuring AES settings.

Changing SSH Settings

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

► *To change SSH settings:*

1. Choose Device Settings > Network Services > SSH.
2. To enable or disable the SSH access, select or deselect the checkbox.
3. To use a different port, type a port number.
4. Select one of the authentication methods.
   - *Password authentication only:* Enables the password-based login only.
   - *Public key authentication only:* Enables the public key-based login only. You must enter a valid SSH public key for each user profile to log in over the SSH connection.
   - *Password and public key authentication:* Enables both the password- and public key-based login. This is the default.
5. Click Save.

Changing Telnet Settings

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

► *To change Telnet settings:*

1. Choose Device Settings > Network Services > Telnet.
2. To enable the Telnet access, select the checkbox.
3. To use a different port, type a new port number.
4. Click Save.

Changing Modbus Settings

The PX4 supports both the Modbus/TCP and Modbus Gateway features. Enable either or both Modbus features according to your needs.

► *Modbus/TCP Access:*

You can enable or disable the Modbus/TCP access to PX4, set it to the read-only mode, or change the TCP port.

1. Choose Device Settings > Network Services > Modbus.
2. To enable the Modbus/TCP access, select the Enable Modbus/TCP access checkbox.
3. To use a different port, type a new port number.
4. To enable the Modbus read-only mode, select the "Enable read-only mode" checkbox. To enable the read-write mode, deselect it.

► *Modbus Gateway:*

You can connect Raritan's USB-MOD-DONGLE to the USB-A Port of the PX4 and the green connector to an external third-party device terminal. The gateway service runs on a dedicated TCP port and forwards incoming requests to the Modbus/RTU bus. Enable the Modbus Gateway feature and configure the Modbus gateway service independent of the Modbus/TCP service. The Modbus TCP clients on your network will be able to communicate with the Modbus RTU devices connected to PX4.

Once configured, connected devices appear in the Peripherals page.

1. To allow the Modbus TCP clients on the network to communicate with the Modbus RTU devices connected to the PX4, select the 'Enable Modbus gateway' checkbox.

2. Now configure the fields shown.

Field	Description
TCP port	Use the default port 503, or assign a different port. Valid range is 1 to 65535. Note: Port 502 is the default Modbus/TCP port for PX4, so you cannot use that port for the Modbus Gateway.
Parity, Line speed	Use the default values, or update if the Modbus RTU devices are using different communication parameters.

Field	Description
Default address	If the Modbus TCP client does not support Modbus RTU unit identifier addressing, enter a Default Address. If you must provide a unit identifier address: • Only one Modbus RTU device is supported. • The unit identifier address you provide is applied to the Modbus RTU device connected to PX4. Note that each Modbus RTU device's unit identifier address must be unique. Warning: If the connected Modbus RTU device's address does not match the address entered in this field, communications between the Modbus TCP clients and Modbus RTU device fail.

Enabling Redfish Services

You can enable or disable the Redfish services to manage the device through the Redfish API. By default, this service is enabled.

Enabling Redfish services allows you to retrieve the following details.

- configuration details, such as thresholds, names, etc.
- metric readings
- event polling

It also allows you to do the following actions

- power actions
- unit control, such as restart

Note: Go to the online Support page for your product to find full documentation of the Redfish API.

► *To enable or disable Redfish:*

Choose Device Settings > Network Services > Redfish.

Enabling Service Advertising

The PX4 advertises all enabled services that are reachable using the IP network. This feature uses DNS-SD (Domain Name System-Service Discovery) and MDNS (Multicast DNS). The advertised services are discovered by clients that have implemented DNS-SD and MDNS.

The advertised services include the following:

- HTTP
- HTTPS
- Telnet
- SSH
- Modbus
- JSON-RPC
- SNMP

By default, this feature is enabled.

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

The service advertisement feature supports both IPv4 and IPv6 protocols.

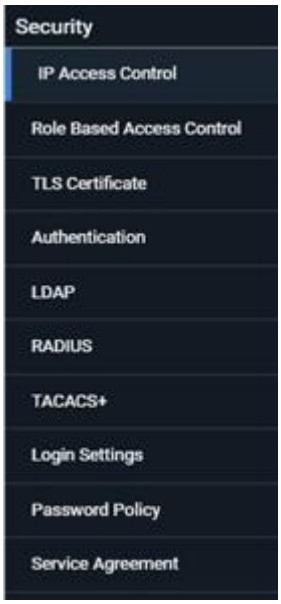
If you have set a preferred host name for IPv4 and/or IPv6, that host name can be used as the zero configuration .local host name, that is, *<preferred_host_name>.local*, where <preferred_host_name> is the preferred host name you have specified for PX4. The IPv4 host name is the first priority. If an IPv4 host name is not available, then use the IPv6 host name.

► *To enable or disable service advertising:*

1. Choose Device Settings > Network Services > Service Advertising.
2. To enable the service advertising, select either or both checkboxes.
   - To advertise via MDNS, select the Multicast DNS checkbox.
   - To advertise via LLMNR, select the Link-Local Multicast Name Resolution checkbox.
3. Click Save.

Configuring Security Settings

The PX4 provides tools to control access. You can enable the internal firewall, create firewall rules, and set login limitations. In addition, you can create and install the certificate or set up external authentication servers for access control. This product supports SHA-2 TLS certificates.



Creating IP Access Control Rules

IP access control rules (firewall rules) determine whether to accept or discard traffic to/from the PX4, based on the IP address of the host sending or receiving the traffic. When creating rules, keep these principles in mind:

- Rule order is important.

  When traffic reaches or is sent from the PX4, the rules are executed in numerical order. Only the first rule that matches the IP address determines whether the traffic is accepted or discarded. Any subsequent rules matching the IP address are ignored.
- Prefix length is required.

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

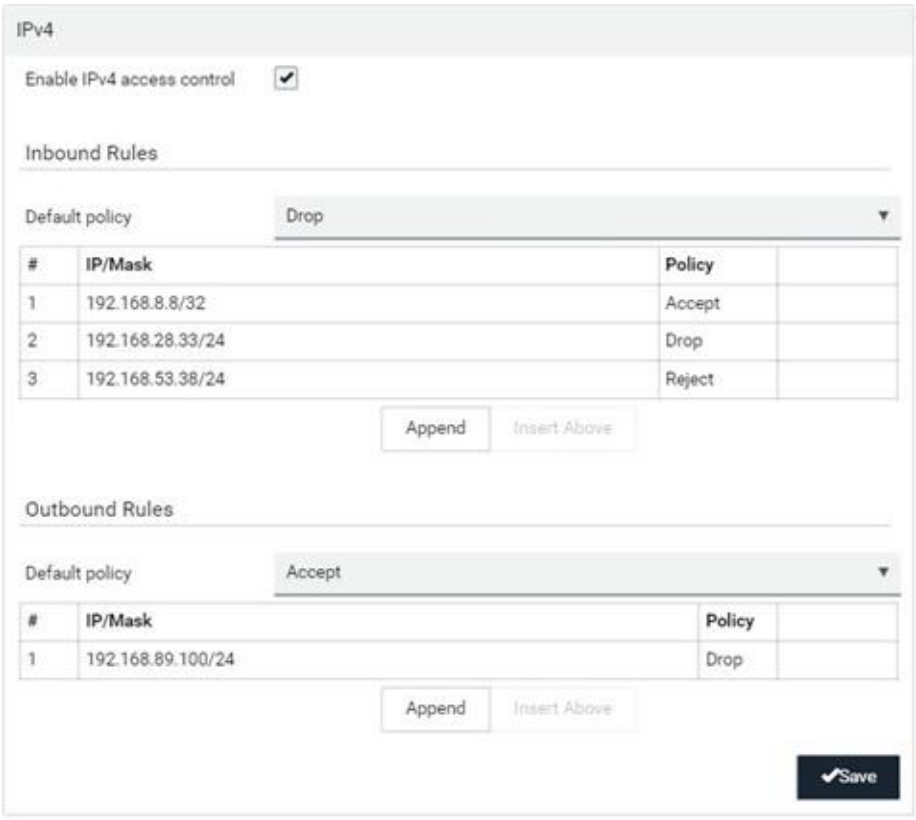
  x.x.x.x/24

  /24 = the prefix length.

Note: Valid IPv4 addresses range from 0.0.0.0 through 255.255.255.255.

► *To configure IPv4 or IPv6 access control rules:*

1. Choose Device Settings > Security > IP Access Control.
2. Select the 'Enable IPv4 access control' or "Enable IPv6 access control" checkboxes to enable the access control rules.
3. For either type, determine the default policy.
   - *Accept:* Accepts traffic from all IPv4 OR IPv6 addresses.
   - *Drop:* Discards traffic from all IPv4 OR IPv6 addresses, without sending any failure notification to the source host.
   - *Reject:* Discards traffic from all IPv4 OR IPv6 addresses, and an ICMP message is sent to the source host for failure notification.
4. Go to the Inbound Rules section or the Outbound Rules section according to your needs.
   - Inbound rules control the data sent to the PX4.
   - Outbound rules control the data sent from the PX4.
5. Create rules.
   - Click Append to add a row, then add the IP address and subnet mask. Select Policy. For each rule, the policy affects only the specified IP address.
   - Click Insert Above to add a rule above another rule.
   - The system automatically numbers the rules.
   - Use the arrow buttons to sort the priority order.
6. Click Save. The rules are applied. Make sure to click Save in each section if changes are made.



Editing or Deleting IP Access Control Rules

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

► *To modify or delete a rule:*

1. Choose Device Settings > Security > IP Access Control.
2. Go to the IPv4 or IPv6 section.
3. Select the desired rule in the list.
   - Ensure the IPv4 or IPv6 checkbox has been selected, or you may not edit or delete any rule.
4. Perform the desired action.

- Make changes to the selected rule, and then click Save.
- Click to remove it.
- To re-sort its order, click or .

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

Creating Role Based Access Control Rules

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

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

► *To create IPv4 role-based access control rules:*

1. Choose Device Settings > Security > Role Based Access Control.
2. Select the 'Enable role based access control for IPv4' checkbox to enable IPv4 access control rules.
3. Determine the IPv4 default policy.
   - *Accept:* Accepts traffic when no matching rules are present.
   - *Deny:* Rejects any user's login attempt when no matching rules are present.
4. Create rules. Refer to the tables below for different operations.

ADD a rule to the end of the list

• Click Append.
• Type a starting IP address in the Start IP field.
• Type an ending IP address in the End IP field.
• Select a role in the Role field. This rule applies to members of this role only.
• Select an option in the Policy field.
  • *Accept:* Accepts traffic from the specified IP address range when the user is a member of the specified role.
  • *Deny:* Rejects the login attempt of a user from the specified IP address range when that user is a member of the specified role.

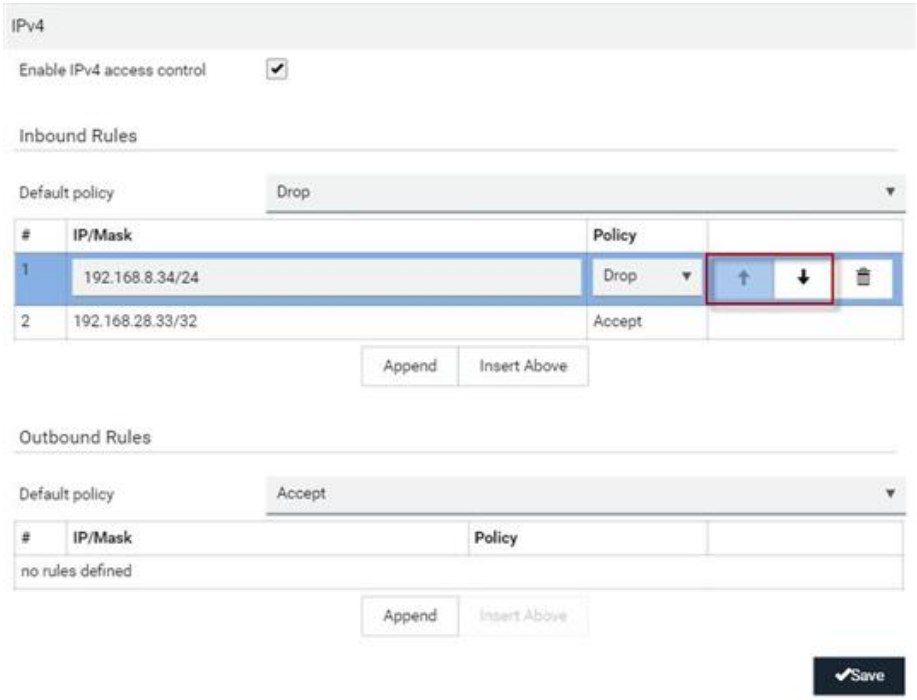
INSERT a rule between two rules

- Select the rule above which you want to insert a new rule. For example, to insert a rule between rules #3 and #4, select #4.
- Click Insert Above.
- Type a starting IP address in the Start IP field.
- Type an ending IP address in the End IP field.
- Select a role in the Role field. This rule applies to members of this role only.
- Select *Accept* or *Deny* in the Policy field. Refer to the above table for details.

The system automatically numbers the rule.

5. When finished, the rules are listed on this page.

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



6. Click Save. The rules are applied.

► *To configure IPv6 access control rules:*

1. On the same page, select the 'Enable role based access control for IPv6' checkbox to enable IPv6 access control rules.
2. Follow the same procedure as the above IPv4 rule setup to create IPv6 rules.
3. Make sure you click the Save button in the IPv6 section, or the changes made to IPv6 rules are not saved.

Editing or Deleting Role Based Access Control Rules

You can modify existing rules to update their roles/IP addresses, or delete them when they are no longer needed.

► *To modify a role-based access control rule:*

1. Choose Device Settings > Security > Role Based Access Control.
2. Go to the IPv4 or IPv6 section.
3. Select the desired rule in the list.
   - Ensure the IPv4 or IPv6 checkbox has been selected, or you may not edit or delete any rule.
4. Perform the desired action.
   - Make changes to the selected rule, and then click Save.
   - Click to remove it.
   - To resort its order, click or .
5. Click Save.
   - IPv4 rules: Make sure you click the Save button in the IPv4 section, or the changes made to IPv4 rules are not saved.
   - IPv6 rules: Make sure you click the Save button in the IPv6 section, or the changes made to IPv6 rules are not saved.

Setting Up a TLS Certificate

► *To obtain a CA-signed certificate:*

1. Create a Certificate Signing Request (CSR) in Device Settings > TLS Certificates.
2. Submit it to a certificate authority (CA). After the CA processes the information in the CSR, it provides you with a certificate.
3. Install the CA-signed certificate onto the PX4.

Note: If you are using a certificate that is part of a chain of certificates, each part of the chain is signed during the validation process. You can upload active and pending certificates and private keys saved in PEM format on a flash drive.

► *A CSR is not required in either scenario below:*

- Make the PX4 create a *self-signed* certificate.
- Appropriate, valid certificate and key files are already available, and you only need to import them.

Creating a TLS Certificate or CSR

Follow this procedure to create the CSR.

Raritan
A brand of legrand

► *To create a CSR:*

1. Choose Device Settings > Security > TLS Certificate.
2. In the New CSR section, provide the information requested.
   - Subject:

Field	Description
Country	The country where your company is located. Use the standard ISO country code, which comprises two uppercase letters. For a list of ISO codes, google ISO 3166 country codes.
State or province	The full name of the state or province where your company is located.
Locality	The city where your company is located.
Organization	The registered name of your company.
Organizational unit	The name of your department.
Common name	The fully qualified domain name (FQDN) of your PX4.
Email address	An email address where you or another administrative user can be reached.

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

   - Subject Alternative Names:

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

     Click Add Name when there are more than one additional hosts to add.

     - Examples of subject alternative names: *support.raritan.com*, *help.raritan.com*, *help.raritan.net*, and *192.168.77.50*.
   - Key Creation Parameters:

Field	Description
Key Type/Key Length	Key type RSA requires you to select Key Length: • 2048 bits • 3072 bits
Key Type/Elliptic Curve	Key type ECDSA requires you to select the elliptic curve: • NIST-P-256 • NIST P-384 • NIST P-521
Self-sign	For requesting a certificate signed by the CA, ensure this checkbox is NOT selected.

Field	Description
Challenge, Confirm challenge	Type a password. The password is used to protect the certificate or CSR. The value should be 4 to 64 characters long. Case sensitive.

1. Click Create CSR to create both the CSR and private key. This may take several minutes to complete.
2. Click Download Certificate Signing Request to download the CSR to your computer.
   a. You are prompted to open or save the file. Click Save to save it onto your computer.
   b. Submit it to a CA to obtain the digital certificate.
   c. If the CSR contains incorrect data, click Delete Certificate Signing Request to remove it, and then repeat the above steps to re-create it.
1. To store the newly-created private key on your computer, click Download Key in the New TLS Certificate or CSR section.

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

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

Installing a CA-Signed Certificate

To get a certificate from a certificate authority (CA), first create a CSR and send it to the CA. See Creating a TLS Certificate or CSR (on page 270).

After receiving the CA-signed certificate, install it onto the PX4.

► *To install the CA-signed certificate:*

1. Choose Device Settings > Security > TLS Certificate.
2. Click Browse to navigate to the CA-signed certificate file in the New TLS Certificate or CSR section.
3. Click Upload to upload the certificate.
4. Once complete, do the following:
   a. Double check the data shown in the New TLS Certificate or CSR section.
   b. If correct, click "Install Key and Certificate" to install the CA-signed certificate and private key.

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

      If incorrect, click "Delete Key and Certificate" to remove the CA-signed certificate and private key, and then repeat the above steps to re-create them.
5. (Optional) To download the CA-signed certificate and/or private key, click Download Certificate or Download Key in the New TLS Certificate section.
   - You are prompted to open or save the file. Click Save to save it onto your computer.

Raritan
A brand of legrand

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

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

Creating a Self-Signed Certificate

When appropriate certificate and key files for PX4 are unavailable, the alternative, other than submitting a CSR to the CA, is to generate a self-signed certificate.

► *To create and install a self-signed certificate:*

1. Choose Device Settings > Security > TLS Certificate.
2. Enter information.

Field	Description
Country	The country where your company is located. Use the standard ISO country code, which comprises two uppercase letters. For a list of ISO codes, google ISO 3166 country codes.
State or province	The full name of the state or province where your company is located.
Locality	The city where your company is located.
Organization	The registered name of your company.
Organizational unit	The name of your department.
Common name	The fully qualified domain name (FQDN) of your PX4.
Email address	An email address where you or another administrative user can be reached.
Generate Key in Secure Element	• This field appears for supported hardware only. Select this checkbox to allow the key to be generated within the Secure Element of the controller.
Key Type/Key Length	Key type RSA requires you to select Key Length: • 2048 bits • 3072 bits
Key Type/Elliptic Curve	Key type ECDSA requires you to select the elliptic curve: • NIST-P-256 • NIST P-384 • NIST P-521
Self-sign	Ensure this checkbox is selected, which indicates that you are creating a self-signed certificate.
Validity in days	This field appears after the Self-sign checkbox is selected. Type the number of days for which the self-signed certificate will be valid.

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

3. Click Create Self-Signed Certificate to create both the self-signed certificate and private key. This may take several minutes to complete and saved.
4. Once complete, do the following:
   a. Double check the data shown in the New TLS Certificate or CSR section.
   b. If correct, click "Install Key and Certificate" to install the self-signed certificate and private key.

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

   If incorrect, click "Delete Key and Certificate" to remove the self-signed certificate and private key, and then repeat the above steps to re-create them.
5. (Optional) To download the self-signed certificate and/or private key, click Download Certificate or Download Key in the New TLS Certificate section.
   - You are prompted to open or save the file. Click Save to save it onto your computer.

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

Installing or Downloading Existing Certificate and Key

You can download the already-installed certificate and private key from any PX4 for backup or file transfer. For example, you can install the files onto a replacement PX4, add the certificate to your browser and so on.

If valid certificate and private key files are already available, you can install them on the PX4 without going through the process of creating a CSR or a self-signed certificate.

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

► *To download active key and certificate files from PX4:*

1. Choose Device Settings > Security > TLS Certificate.
2. In the *Active TLS Certificate* section, click Download Key and Download Certificate respectively.

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

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

► *To install available key and certificate files onto PX4:*

1. Choose Device Settings > Security > TLS Certificate.
2. Select the "Upload key and certificate" checkbox at the bottom of the page.
3. The 'Key File' and 'Certificate file' buttons appear. Click each button to select the key and/or certificate file.
4. Click Upload. The selected files are installed.
5. To verify whether the certificate has been installed successfully, check the data shown in the Active TLS Certificate section.

SCEP

The PX4 supports automated certificate enrollment using the Simple Certificate Enrollment Protocol (SCEP). During initial enrollment, the device authenticates to the SCEP CA server using a shared secret. Subsequent renewals utilize the initially received client certificate for authentication.

More specifically:

1. Authentication: The SCEP Certificate Authority (CA) is authenticated to the device using a fingerprint of the Root CA certificate.
2. Connection and Request: The device connects to the SCEP CA and requests a certificate by sending a Certificate Signing Request (CSR).
3. Initial Enrollment: A shared secret is used on the CSR to authenticate the device to the SCEP CA during the initial enrollment process.
4. Renewal: For certificate renewals, the device authenticates using the client certificate it received during the initial enrollment.

https://xwiki.raritan.com/bin/view/Product_Sites/Dominion_PX/PX2/User_Stories/SCEP_User_Story/

Setting Up External Authentication

Important: Make sure your network infrastructure uses TLS rather than SSL.

PX4 supports the following authentication mechanisms:

- Local user database
- LDAP
- RADIUS
- TACACS+

Local authentication is the default method. If you use this method, you only need to create user accounts. See User Management (on page 221).

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

If both local and external authentication is needed, create user accounts on the PX4 in addition to providing the external AA server data.

When configured for external authentication, all users must have an account on the external AA server. Local-authentication-only users will have no access to the PX4 except for the admin, who always can access.

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

You must have the "Change Authentication Settings" permission to configure or modify the authentication settings.

Adding LDAP/LDAPS Servers

To use LDAP authentication, enable it in the Device Settings > Authentication page, and enter the information about the LDAP server in the LDAP page.

Note: If the PX4 clock and the LDAP server clock are out of sync, the installed TLS certificates, if any, may be considered expired. To ensure proper synchronization, administrators should configure the PX4 and the LDAP server to use the same NTP server(s).

► *To add LDAP/LDAPS servers:*

1. Choose Device Settings > Security > LDAP.
2. Click New.
3. Enter information.

Field/setting	Description
IP address / hostname	The IP address or hostname of your LDAP/LDAPS server. • Without the encryption enabled, you can type either the domain name or IP address in this field, but you must type the fully qualified domain name if the encryption is enabled.
Copy settings from existing LDAP server	This checkbox appears only when there are existing AA server settings on the PX4. To duplicate any existing AA server's settings, refer to the duplicating procedure below.
Type of LDAP server	Choose one of the following options: • OpenLDAP • Microsoft Active Directory.
Security	Determine whether you would like to use Transport Layer Security (TLS) encryption, which allows the PX4 to communicate securely with the LDAPS server. Three options are available: • StartTLS • TLS • None
Port (None/ StartTLS)	• The default Port is 389. Either use the standard LDAP TCP port or specify another port.

Field/setting	Description
Port (TLS)	Configurable only when "TLS" is selected in the Security field. The default is 636. Either use the default port or specify another one.
Enable verification of LDAP server certificate	Select this checkbox if it is required to validate the LDAP server's certificate by the PX4 prior to the connection. If the certificate validation fails, the connection is refused.
CA certificate	Consult your AA server administrator to get the CA certificate file for the LDAPS server. Click Browse to select and install the certificate file. • Click Show to view the installed certificate's content. • Click Remove to delete the installed certificate if it is inappropriate. *Note: If the required certificate file is a chain of certificates, and you are not sure about the requirements of a certificate chain, see TLS Certificate Chain.*
Allow expired and not yet valid certificates	• Select this checkbox to make the authentication succeed regardless of the certificate's validity period. • After deselecting this checkbox, the authentication fails whenever any certificate in the selected certificate chain is outdated or not valid yet.
Anonymous bind	Use this checkbox to enable or disable anonymous bind. • To use anonymous bind, select this checkbox. • When a Bind DN and password are required to bind to the external LDAP/LDAPS server, deselect this checkbox.
Bind DN	Required after deselecting the Anonymous Bind checkbox. Distinguished Name (DN) of the user who is permitted to search the LDAP directory in the defined search base.
Bind password, Confirm bind password	Required after deselecting the Anonymous Bind checkbox. Enter the Bind password.
Base DN for search	Distinguished Name (DN) of the search base, which is the starting point of the LDAP search. • Example: `ou=dev,dc=example,dc=com`
Login Name Attribute	The attribute of the LDAP user class which denotes the login name. • Usually it is the `uid`.
User entry object class	The object class for user entries. • Usually it is `inetOrgPerson`.

Field/setting	Description
User search subfilter	Search criteria for finding LDAP user objects within the directory tree.
Group lookup using memberOf attribute	• Select this checkbox to determine group membership by consulting the user's memberOf attribute(s). • Deselect this checkbox to determine group membership by doing a non-recursive search for groups containing the user's DN as member.
Group member attribute	• Required only when "Group lookup using memberOf attribute" is not selected. • Required for OpenLDAP only.
Support nested groups	• Select this checkbox to support the Active Directory LDAP nested groups. • Deselect this checkbox means no support.
Group entry object class	• Required only when "Group lookup using memberOf attribute" is not selected. • Required for OpenLDAP only.
Group search subfilter	• Required only when "Group lookup using memberOf attribute" is not selected. • Required for OpenLDAP only.
Active Directory domain	The name of the Active Directory Domain. • Example: `testradius.com`

4. Click Add Server. The new LDAP server is listed. To verify, click Test Connection to check whether the PX4 can connect to the new server successfully.
5. To add more servers, repeat the same steps.
6. In the LDAP page, use the arrow buttons to arrange the servers in the order they should be accessed, then click Save.
7. Make sure LDAP is enabled: Go to Device Settings > Security > Authentication, and select LDAP as the Authentication Type.

► *To duplicate LDAP/LDAPS server settings:*

If you have added any LDAP/LDAPS server to the PX4, and the server you will add shares identical settings with an existing one, the most convenient way is to duplicate that LDAP/LDAPS server's data and then revise the IP address/host name.

1. Choose Device Settings > Security > LDAP, then click New.
2. Select the "Copy settings from existing LDAP server" checkbox.
3. Select the LDAP/LDAPS server whose settings you want to copy.
4. Modify the IP Address/Hostname field.
5. Click Add Server.

Adding Radius Servers

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

Note: The RADIUS NAS Identifier is "DPC PDU SN:<device serial number>".

► *To add Radius servers:*

1. Choose Device Settings > Security > RADIUS.
2. Click New.
3. Enter information.

Field/setting	Description
IP address / hostname	The IP address or hostname of your Radius server.
Type of RADIUS authentication	Select an authentication protocol. • PAP (Password Authentication Protocol) • CHAP (Challenge Handshake Authentication Protocol) • MS-CHAPv2 (Microsoft Challenge Handshake Authentication Protocol) CHAP is generally considered more secure because the user name and password are encrypted, while in PAP they are transmitted in the clear. MS-CHAPv2 provides stronger security than the above two. Selecting this option will support both MS-CHAPv1 and MS-CHAPv2. *Note: All authentication methods are insecure. It is strongly recommended to use RADIUS only in a secure networking environment. A warning displays for all methods.*
Authentication port, Accounting port	The defaults are standard ports -- 1812 and 1813. To use non-standard ports, type a new port number.
Accounting Enabled?	Default is enabled. Accounting allows you to log activity executed on the RADIUS server. When RADIUS accounting is enabled and the RADIUS server does not support accounting, then authentication will fail.

Field/setting	Description
Timeout	This sets the maximum amount of time to establish contact with the Radius server before timing out. Type the timeout period in seconds.
Retries	Type the number of retries.
Shared secret, Confirm shared secret	The shared secret is necessary to protect communication with the Radius server.

4. To verify settings, click Test Connection to check if you can connect to the new server successfully.
5. Click Add Server. The new Radius server is listed on the RADIUS page.
6. To add more servers, repeat the same steps.
7. In the RADIUS page, use the arrow buttons to arrange the servers in the order they should be accessed, then click Save.
8. Make sure RADIUS is enabled: Go to Device Settings > Security > Authentication, and select RADIUS as the Authentication Type.

Adding TACACS+ Servers

To use TACACS+ authentication, add the server information and enable TACACS+.

Note: You need to create a new custom service attribute called Xerus on the TACACS+ server. This attribute value will match the role name (case sensitive) on the PX4. In the authorization request to the TACACS+ server, the PX4 will send a request for Xerus as a custom service attribute. TACACS+ server then returns the roles of the authenticated user in the Xerus: roles attribute. Returning multiple roles separated by a slash, for example, role1/role2, is supported. See Cisco ISE Xerus TACACS+ Authentication (on page 689) for configuration.

► *To add TACACS+ servers:*

1. Choose Device Settings > Security > TACACS+.
2. Click New.
3. Enter information.

Field/setting	Description
IP address / hostname	The IP address or hostname of your TACACS+ server.

Field/setting	Description
Type of TACACS+ authentication	Select an authentication protocol. • ASCII • PAP (Password Authentication Protocol) • CHAP (Challenge Handshake Authentication Protocol) • MS-CHAP (Microsoft Challenge Handshake Authentication Protocol) CHAP is generally considered more secure because the user name and password are encrypted, while in PAP they are transmitted in the clear. MS-CHAP provides stronger security than the other options. *Note: All authentication methods are insecure. It is strongly recommended to use TACACS+ only in a secure networking environment. A warning displays for all methods.*
Port	The default port is 49 To use non-standard port, type a new port number.
Enable Accounting?	Default is enabled. Accounting allows you to log activity executed on the TACACS+ server.
Timeout	Default is 10 seconds. Maximum amount of time to establish contact with the server before timing out. Enter the timeout period in seconds.
Retries	Default is 3. Enter the number of retries.
Shared secret, Confirm shared secret	The shared secret is necessary to protect communication with the server.

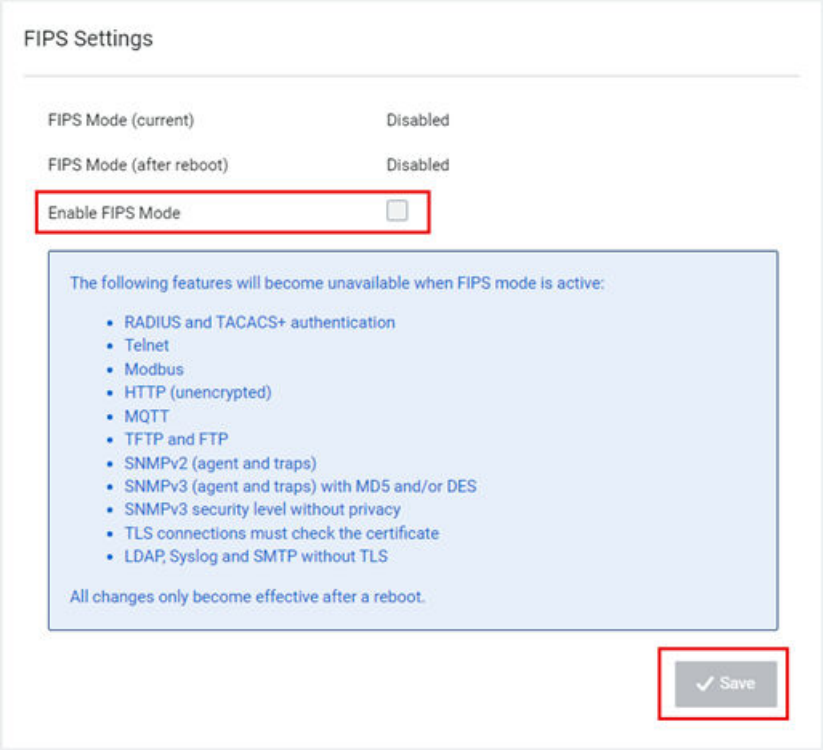
1. Click Add Server or Test Connection to verify the settings.
2. To add more servers, repeat the same steps.
3. In the TACACS+ page, use the arrow buttons to arrange the servers in the order they should be accessed, then click Save.
4. To begin using the configuration, make sure TACACS+ is enabled: Go to Device Settings > Security > Authentication, and select TACACS+ as the Authentication Type.

Enabling the FIPS Mode

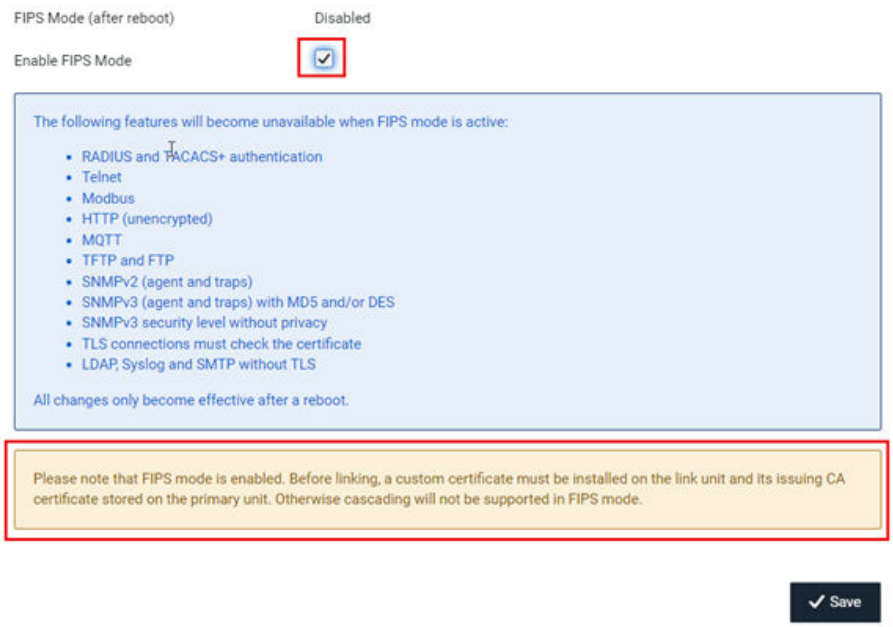
The PX4 optionally uses a FIPS 140-2 encryption module that supports the Security Requirements for Cryptographic Modules of the Federal Information Processing Standards (FIPS), which is defined in the *FIPS PUB 140-2, Annex A: Approved Security Functions*. These standards are used to protect the Federal government's sensitive information with the cryptographic-based security systems in the U.S. and Canada.

► *To enable the FIPS mode:*

1. Click Device Settings > Security > FIPS.
2. Select the 'Enable FIPS Mode' checkbox.

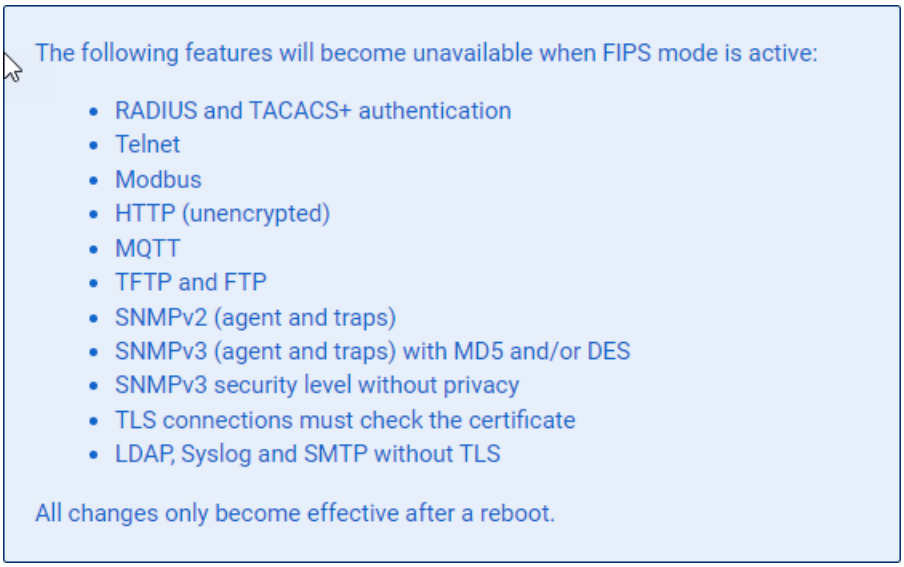


3. Once FIPS is enabled, message appears to install the CA certificate on the link unit.



4. Click Save.
5. Reboot the PX4

When FIPS mode is enabled, you will find following features will not be available.



Configuring Login Settings

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

- Configure the user blocking feature.

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

- Determine the timeout period for any inactive user.
- Prevent simultaneous logins using the same login name.

► *To configure user blocking:*

1. To enable the user blocking feature, select the 'Block user on login failure' checkbox.
2. In the 'Block timeout' field, select a time option. This setting determines how long the user is blocked.
   - If you type a value, the value must be followed by a time unit, such as '4 min.'
3. In the 'Maximum number of failed logins' field, type a number. This is the maximum number of login failures the user is permitted before the user is blocked from accessing the PX4.
4. Timeout for Failed Login Attempts: select a time option after which a failed attempt no longer counts against the user. For example, if "Maximum number of failed logins" is 3, but the "Timeout for Failed Login Attempts" has passed since the last failed attempt, the counter of failed logins restarts.
5. Click Save.

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

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

1. In the "Idle timeout period" field, type a value or click to select a time option. This setting determines how long users are permitted to stay idle before being forced to log out.
   - If you type a value, the value must be followed by a time unit, such as '4 min.' See Time Units (on page 144).
   - Keep the idle timeout to 20 minutes or less if possible. This reduces the number of idle sessions connected, and the number of simultaneous commands sent to the PX4.
2. Select the 'Prevent concurrent login with same username' checkbox to prevent multiple users from using the same login name simultaneously.
3. Click Save.

Configuring Password Policy

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

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

► *To configure password aging:*

1. Select the 'Enabled' checkbox of Password Aging.
2. In the 'Password aging interval' field, type a value or select a time option. This setting determines how often users are requested to change their passwords.
   - If you type a value, the value must be followed by a time unit, such as '10 d.'
3. Click Save.

► *To force users to create strong passwords:*

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

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

2. Make changes to the default settings as needed.
3. Click Save.

Enabling the Restricted Service Agreement

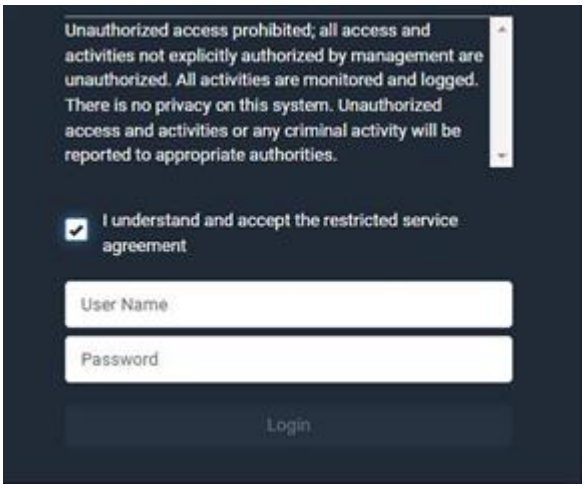
The restricted service agreement feature, if enabled, forces users to read a security agreement when they log in to the PX4. Users must accept the agreement, or they cannot log in. You can configure an event notifying you if a user has accepted or declined the agreement.

► *To enable the service agreement:*

1. Click Device Settings > Security > Service Agreement.
2. Select the 'Enforce restricted service agreement' checkbox.
3. Edit or paste the content as needed.
   - A maximum of 10,000 characters can be entered.
4. Click Save.

► *Login manner after enabling the service agreement:*

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



To log in when a restricted service agreement appears:

- In the web interface, select the checkbox labeled "I understand and accept the restricted service agreement."
- In the CLI, type `y` when the confirmation message "I understand and accept the restricted service agreement" is displayed.

Setting the Date and Time

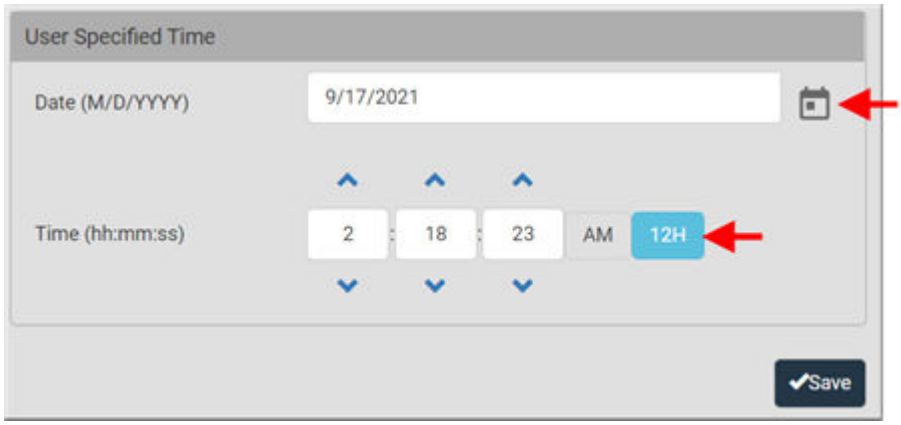
Set the internal clock manually, or link to a Network Time Protocol (NTP) server.

PX4 follows the NTP server sanity check per the IETF RFC.

Note: If you are using Sunbird's® Power IQ®, you must configure Power IQ and the PX4 to have the same date/time or NTP settings.

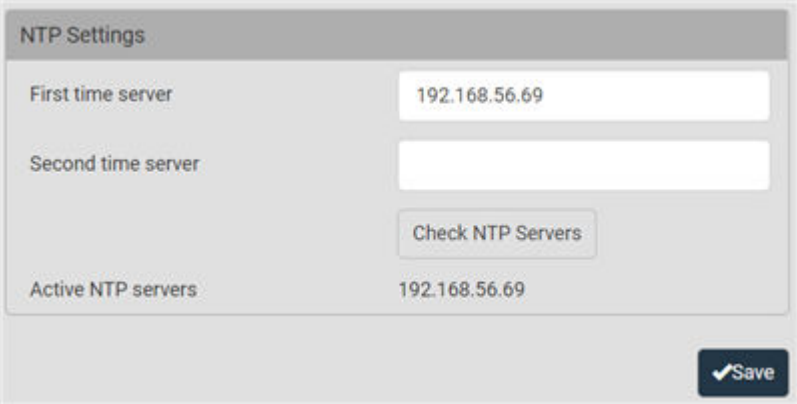
► *To set the date and time:*

1. Choose Device Settings > Date/Time.
2. Click the 'Time zone' field to select your time zone from the list.
3. If the daylight saving time applies to your time zone, verify the 'Automatic daylight saving time adjustment' checkbox is selected.
4. Select the method for setting the date and time. Choose settings and click Save.

Customize the date and time
• Select 'User specified time'. • Enter the date or click the calendar icon to select a date. • Click 12H/24H button to toggle time formats. • Click the AM/PM button to toggle. • Enter the time or click the arrows to set it. 
Use the NTP server

- Select "Synchronize with NTP server."
  - The DHCP-assigned NTP servers are available when DHCP is enabled. The IP address appears as Active NTP Server. To use this server, leave the primary and secondary server fields blank.
  - To specify NTP servers, enter the primary NTP server in the "First time server" field. A secondary NTP server is optional.

    Click Check NTP Servers to verify accessibility.



Windows NTP Server Synchronization Solution

The NTP client on the PX4 follows the NTP RFC so the PX4 rejects any NTP servers whose root dispersion is more than one second. An NTP server with a dispersion of more than one second is considered an inaccurate NTP server by the PX4.

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

Windows NTP servers may have a root dispersion of more than one second, and therefore cannot synchronize with the PX4. When the NTP synchronization issue occurs, change the dispersion settings to resolve it.

► *To change the Windows NTP's root dispersion settings:*

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

HKEY_LOCAL_MACHINE|SYSTEM|CurrentControlSet|Services|W32Time|Config

2. *AnnounceFlags* must be set to 0x05 or 0x06.
   - 0x05 = 0x01 (Always time server) and 0x04 (Always reliable time server)
   - 0x06 = 0x02 (Automatic time server) and 0x04 (Always reliable time server)

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

   ---

3. *LocalClockDispersion* must be set to 0.

Door Access

SmartLock enabled cabinets integrated with PowerIQ or other third party systems authorize door access remotely. In the event that the remote authorization is not accessible, local rules can be configured as an alternative or in addition to PIQ rules.

A door access rule can contain the following components:

- Selected door locks: must be configured in advance.
- Authorization via card: specify which card ID and card reader must be used
- Authorization via keypad: specify the PIN and keypad that must be used
- Two-factor authorization: a timeout that requires both card and keypad conditions to be met. For example: when a certain card is inserted, the correct PIN must be entered in the next 10 seconds.
- Absolute time conditions: grant access for a specific date and time
- Periodic time conditions: grant access on certain days of the week and certain times

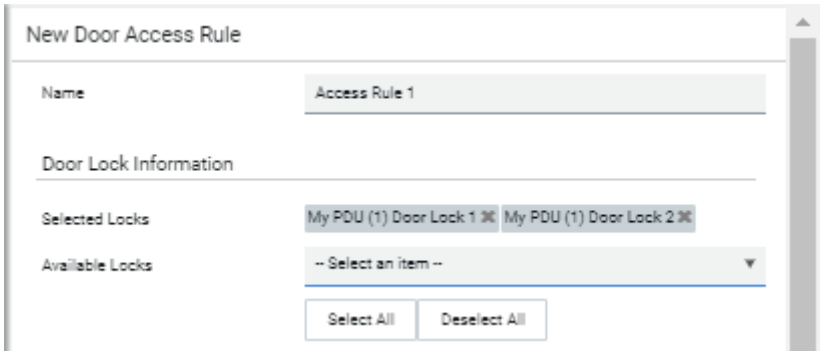
---

Note: In one access rule you can set 2 card IDs as 2-factor authorization.

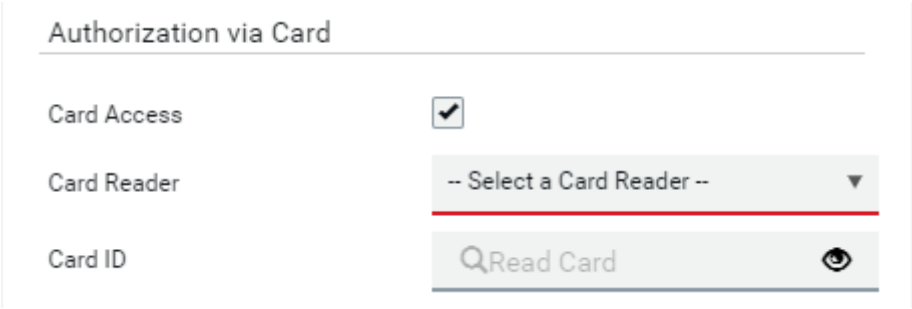
► *To create a door access rule:*

1. Choose Device Settings > Door Access.
2. Click New Access Rule.

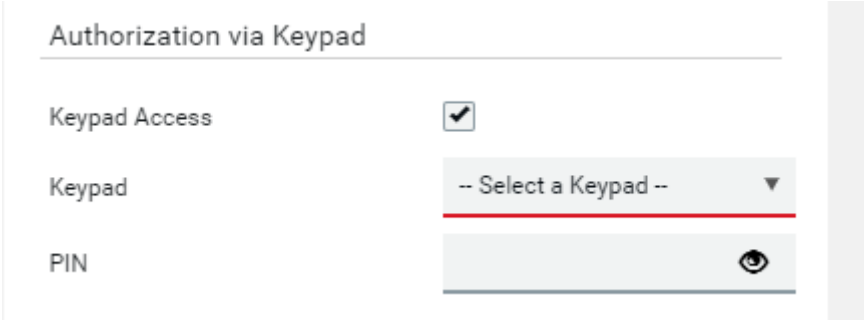
3. The New Door Access Rule page opens. Enter a name for the rule. 128 characters maximum.
4. Select the door locks this rule applies to in the Available Door Handle Locks list. Each selected door lock appears in the Selected Locks section.



5. To allow authorization via card reader, select the Card Access checkbox, then select the correct Card Reader and click Read Card to retrieve the Card ID. Card IDs are hidden for security. Click the eyeball icon to reveal and verify the Card ID.

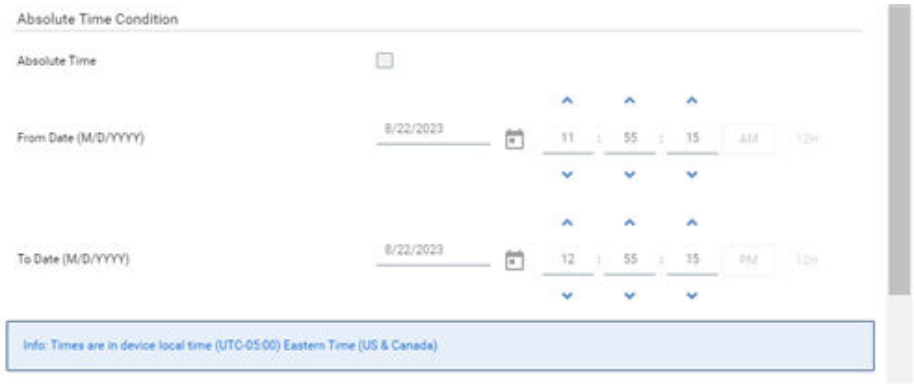


6. To allow Authorization via Keypad, select the Keypad Access checkbox, then select the correct keypad and enter the PIN. PINs are hidden for security. Click the eyeball icon to reveal and verify the PIN. PIN length varies by keypad, and a minimum PIN length of 4 is required.



7. When both Card and Keypad authorization are required, the Two-Factor Configuration controls are required. Enter a Timeout in seconds during which both Card and Keypad authorization must occur.

8. To allow authorization with an Absolute Time Condition, select the Absolute Time checkbox, then use the calendar tool to set the start and end dates, and the clock tools to set the start and end times during which access is granted. Note: Click the 12H/24H icon to toggle between clock styles.



9. To allow authorization with a Periodic Time Condition, select the Periodic Time checkbox, then select the Days of Week and range of hours on which access is granted. Note: Click the 12H/24H icon to toggle between clock styles.

10. Click Create to save the rule. All rules appear on the main Door Access Rule page.

Event Rules and Actions

Create event rules and actions to notify you of or react to a change in conditions.

An event rule consists of two parts:

- Event: This is the situation where the PX4 or a device connected to it meets a certain condition. For example, the inlet's voltage reaches the warning level.
- Action: This is the response to the event. For example, the system administrator is notified of the event via email.

Some actions can be scheduled at regular intervals instead of occurring in reaction to an event. For example, you can schedule the emailing of the temperature report every hour.

You must have the Administrator Privileges to configure event rules.

► *To create an event rule:*

1. Choose Device Settings > Event Rules.
2. If the needed action is not available yet, click New Action to create it.
   a. Assign a name to this action.
   b. Select the desired action and configure it as needed.
   c. Click Create.
3. Click New Rule to create a new rule.
   a. Assign a name to this rule.
   b. Make sure the Enabled checkbox is selected, to make the new rule active.
   c. In the Event field, select the event to react to.
   d. In the 'Available actions' field, select the desired action(s) to respond to the selected event.
   e. Click Create.

► *To create a scheduled action:*

1. Click New Scheduled Action to schedule the desired action.
   a. Assign a name to this scheduled action.
   b. Make sure the Enabled checkbox is selected to make the scheduled action active.
   c. Set the interval time, which ranges from every minute to yearly.
   d. In the 'Available actions' field, select the desired action(s).
   e. Click Create.

Built-in Rules and Rule Configuration

There are several built-in event rules, which cannot be deleted. If the built-in event rules do not satisfy your needs, create new rules.

► *Built-in rules:*

- *System Event Log Rule:*
  This causes ANY event occurred to the PX4 to be recorded in the internal log. It is enabled by default.

Note: Default log messages are generated for each event.

- *System SNMP Notification Rule:*

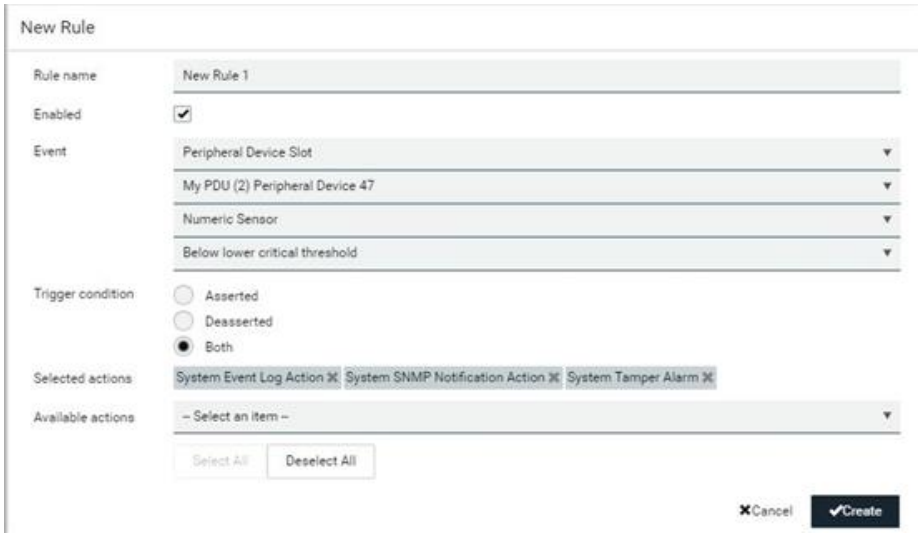
  This causes SNMP traps or informs to be sent to specified IP addresses or hosts when ANY event occurs to the PX4. It is disabled by default.
- *System Tamper Detection Alarmed:*

  This causes alarm notifications if a connected tamper sensor is detected to be in an alarmed state. It is enabled by default.
- *System Tamper Detection Unavailable:*

  This causes alarm notifications if a previously available tamper sensor is not detected. It is enabled by default.

► *Event rule configuration illustration:*

1. Choose Device Settings > Event Rules > New Rule.
2. Click the Event field to select an event type.
   - <Any sub-event> means all events shown on the list.
   - <Any Numeric Sensor> means all numeric sensors, including internal and environmental sensors. <Any Numeric Sensor> is especially useful if you want to receive the notifications when any numeric sensor's readings pass through a specific threshold.
3. In this example, the Peripheral Device Slot is selected, which is related to the environmental sensor packages. Then a sensor ID field for this event type appears. Click this additional field to specify which sensor should be the subject of this event.
4. In this example, sensor ID 3 (Slot 3) is selected, which is a temperature sensor. Then a new field for this sensor appears. Click this field to specify the type of event(s) you want.
5. In this example, Numeric Sensor is selected because we want to select numeric-sensor-related event(s). Then a field for numeric-sensor-related events appears. Click this field to select one of the numeric-sensor-related events from the list.
6. In this example, 'Above upper critical threshold' is selected because we want the PX4 to react only when the selected temperature sensor's reading enters the upper critical range. A "Trigger condition" field appears, requiring you to define the "exact" condition related to the "upper critical" event.
7. Select the desired radio button to finish the event configuration. Refer to the following table for different types of radio buttons.
   - *See* Sample Event Rules (on page 338).
8. Add and/or remove actions to configure the rule. Select actions from the 'Available actions' list to create the Select actions list.



► *Radio buttons for different events:*

Some events require you to configure the "Trigger condition".

Event types	Radio buttons
Numeric sensor threshold-crossing events, or the occurrence of the selected event -- true or false	• Asserted: action occurs only when the selected event occurs. That is, the status of the event transits from FALSE to TRUE. • Deasserted: action occurs only when the selected event disappears or stops. That is, the status of the selected event transits from TRUE to FALSE. • Both: action occurs both when the event occurs (asserts) and when the event stops/disappears (deasserts).
State sensor state change	• Alarmed/Open/On: action occurs only when the chosen sensor enters the alarmed, open or on state. • No longer alarmed/Closed/Off: action occurs only when the chosen sensor returns to the normal, closed, or off state. • Both: action occurs whenever the chosen sensor switches its state.
Sensor availability	• Unavailable: action occurs only when the chosen sensor is NOT detected and becomes unavailable. • Available: action occurs only when the chosen sensor is detected and becomes available. • Both: action occurs both when the chosen sensor becomes unavailable or available.

Event types	Radio buttons
Network interface link state	• Link state is up: action occurs only when the network link state changes from down to up. • Link state is down: action occurs only when the network link state changes from up to down. • Both: action occurs whenever the network link state changes.
Function enabled or disabled	• Enabled: action occurs only when the chosen function is enabled. • Disabled: action occurs only when the chosen function is disabled. • Both: action occurs when the chosen function is either enabled or disabled.
Restricted service agreement	• Accepted: action occurs only when the specified user accepts the restricted service agreement. • Declined: action occurs only when the specified user rejects the restricted service agreement. • Both: action occurs both when the specified user accepts or rejects the restricted service agreement.
Server monitoring event	• Monitoring started: action occurs only when the monitoring of any specified server starts. • Monitoring stopped: action occurs only when the monitoring of any specified server stops. • Both: action occurs when the monitoring of any specified server starts or stops.
Server reachability	• Unreachable: action occurs only when any specified server becomes inaccessible. • Reachable: action occurs only when any specified server becomes accessible. • Both: action occurs when any specified server becomes either inaccessible or accessible.
Device connection or disconnection, such as a USB-cascaded device	• Connected: action occurs only when the selected device is physically connected to it. • Disconnected: action occurs only when the selected device is physically disconnected from it. • Both: action occurs both when the selected device is physically connected to it and when it is disconnected.

Event types	Radio buttons
+12V Supply 1 Status	Available radio buttons include "Fault," "OK" and "Both." • Fault: action occurs only when the selected 12V power supply to the controller enters the fault state. • OK: action occurs only when the selected 12V power supply to the controller enters the OK state. • Both: action occurs whenever the selected 12 power supply's status changes.

Xerus Default Log Messages for All Products

Listed here are all default messages for all Xerus events, including all supported products. Not all products support all events, and events are marked here with the supported model type.

Event/context	Default message on event assertion	Default message on event deassetion	Model Type
Asset Management > Blade Extension Overflow	Blade extension overflow occurred on strip [AMSNUMBER] ('[AMSNAME]').	Blade extension overflow cleared for strip [AMSNUMBER] ('[AMSNAME]').	
Asset Management > Composite Asset Strip Composition Changed	Composition changed on composite asset strip [AMSNUMBER] ('[AMSNAME]').		
Asset Management > Device Config Changed	Config parameter '[CONFIGPARAM]' of asset strip [AMSNUMBER] ('[AMSNAME]') changed to '[CONFIGVALUE]' by user '[USERNAME]'.		
Asset Management > Firmware Update	Firmware update for asset strip [AMSNUMBER] ('[AMSNAME]'): status changed to '[AMSSTATE]'.		
Asset Management > Rack Unit > Blade Extension Connected	Blade extension with ID '[AMSTAGID]' connected at rack unit [AMSRACKUNITPOSITION] of asset strip [AMSNUMBER] ('[AMSNAME]').	Blade extension with ID '[AMSTAGID]' disconnected at rack unit [AMSRACKUNITPOSITION] of asset strip [AMSNUMBER] ('[AMSNAME]').	
Asset Management > Rack Unit > Tag Connected	Asset tag with ID '[AMSTAGID]' connected at rack unit [AMSRACKUNITPOSITION], slot [AMSBLADESLOTPOSITION] of asset strip [AMSNUMBER] ('[AMSNAME]').	Asset tag with ID '[AMSTAGID]' disconnected at rack unit [AMSRACKUNITPOSITION], slot [AMSBLADESLOTPOSITION] of asset strip [AMSNUMBER] ('[AMSNAME]').	
Asset Management > Rack Unit Config Changed	Config of rack unit [AMSRACKUNITPOSITION] of asset strip [AMSNUMBER] ('[AMSNAME]') changed by user '[USERNAME]' to: Name '[AMSRACKUNITNAME]', LED Operation Mode '[AMSLEDOPMODE]', LED Color '[AMSLEDCOLOR]', LED Mode '[AMSLEDMODE]'		

Asset Management > State	State of asset strip [AMSNUMBER] ('[AMSNAME]') changed to '[AMSSTATE]'.		
Card Reader Management > Card Reader > Card inserted	Card of type '[SMARTCARDTYPE]' inserted at Card Reader '[FORMATTEDCARDREADERPATH]'.		
Card Reader Management > Card Reader > Card removed	Card of type '[SMARTCARDTYPE]' removed at Card Reader '[FORMATTEDCARDREADERPATH]'.		
Card Reader Management > Card Reader attached	Card Reader '[FORMATTEDCARDREADERPATH]' connected.		
Card Reader Management > Card Reader detached	Card Reader '[FORMATTEDCARDREADERPATH]' disconnected.		
Card Reader Management > Card Reader settings changed	Settings with name '[CARDREADERNAME]' and description '[CARDREADERDESCRIPTION]' set at Card Reader '[FORMATTEDCARDREADERPATH]' by user '[USERNAME]' from host '[USERIP]'.		
Device > Event log cleared	Event log cleared by user '[USERNAME]' from host '[USERIP]'.		
Device > Bulk configuration copied	[LINKIDTAG]Bulk configuration copied by user '[USERNAME]' from host '[USERIP]'.		
Device > Bulk configuration saved	[LINKIDTAG]Bulk configuration saved by user '[USERNAME]' from host '[USERIP]'.		
Device > Device clock changed	The device clock was changed from [OLDDATETIME] to [DATETIME].		
Device > Data push failed	Data push to URL [DATAPUSHURL] failed. [ERRORDESC]		
Device > Device settings restored	[LINKIDTAG]Device settings restored by user '[USERNAME]' from host '[USERIP]'.		
Device > Device settings saved	[LINKIDTAG]Device settings saved by user '[USERNAME]' from host '[USERIP]'.		
Device > Firmware update completed	[LINKIDTAG]Firmware upgraded successfully from version '[OLDVERSION]' to version '[VERSION]' by user '[USERNAME]' from host '[USERIP]'.		
Device > Firmware update failed	[LINKIDTAG]Firmware upgrade failed from version '[OLDVERSION]' to version '[VERSION]' by user '[USERNAME]' from host '[USERIP]'.		

Device > Firmware update started	[LINKIDTAG]Firmware upgrade started from version '[OLDVERSION]' to version '[VERSION]' by user '[USERNAME]' from host '[USERIP]'.		
Device > Firmware validation failed	[LINKIDTAG]Firmware validation failed by user '[USERNAME]' from host '[USERIP]'.		
Device > Hardware failure present	[LINKIDTAG]Failure '[FAILURETYPESTR]' asserted for component '[COMPONENTID]'.	[LINKIDTAG]Failure '[FAILURETYPESTR]' deasserted for component '[COMPONENTID]'.	
Device > Device identification changed	Config parameter '[CONFIGPARAM]' changed to '[CONFIGVALUE]' by user '[USERNAME]' from host '[USERIP]'.		
Device > An LDAP error occurred	An LDAP error occurred: [ERRORDESC].		
Device > Network interface link state is up	The [IFNAME] network interface link is now up.	The [IFNAME] network interface link is now down.	
Device > Peripheral Device Firmware Update	Firmware update for peripheral device [EXTSENSORSERIAL] from [OLDVERSION] to [VERSION] [SENSORSTATENAME].		
Device > A Radius error occurred	A Radius error occurred: [ERRORDESC].		
Device > Raw configuration downloaded	[LINKIDTAG]Raw configuration downloaded by user '[USERNAME]' from host '[USERIP]'.		
Device > Raw configuration updated	[LINKIDTAG]Raw configuration updated by user '[USERNAME]' from host '[USERIP]'.		
Device > Sending SMS message failed	Sending SMS message to '[PHONENUMBER]' failed. [ERRORDESC]		
Device > Sending SMTP message failed	Sending SMTP message to '[SMTPRECIPIENTS]' using server '[SMTPSERVER]' failed. [ERRORDESC]		
Device > Sending SNMP inform failed or no response	Sending SNMP inform to manager [SNMPMANAGER]:[SNMPMANAGERPORT] failed or no response. [ERRORDESC]		
Device > Sending Syslog message failed	Sending Syslog message to server [SYSLOGSERVER]:[SYSLOGPORT] ([SYSLOGTRANSPORTPROTO]) failed. [ERRORDESC]		
Device > System reset	[LINKIDTAG]System reset performed by user '[USERNAME]' from host '[USERIP]'.		
Device > System started	[LINKIDTAG]System started.		

Raritan
A brand of legrand

Device > A TACACS+ error occurred	A TACACS+ error occurred: [ERRORDESC].		
Device > Unknown peripheral device attached	An unknown peripheral device with rom code '[ROMCODE]' was attached at position '[PERIPHDEVPOSITION]'.		
Device > Expansion unit connected	Expansion unit connected.	Expansion unit disconnected.	
Device > Wired network authentication result	The network authentication on interface [IFNAME] [NETAUTHRESULTSTR].		
Door Access Control > Door access denied	Door access was denied: [DOORACCESSDENIALREASON]		
Door Access Control > Door access granted	Door access was granted, rule '[DOORACCESSRULENAME]' ([DOORACCESSRULEID])		
Door Access Control > Door access rule added	Door access rule '[DOORACCESSRULENAME]' ([DOORACCESSRULEID]) was added by user '[USERNAME]' from host '[USERIP]'		
Door Access Control > Door access rule changed	Door access rule '[DOORACCESSRULENAME]' ([DOORACCESSRULEID]) was changed by user '[USERNAME]' from host '[USERIP]'		
Door Access Control > Door access deleted	Door access rule '[DOORACCESSRULENAME]' ([DOORACCESSRULEID]) was deleted by user '[USERNAME]' from host '[USERIP]'		
Door Access Control > Door Handle > (handle name) > Door Forced Open	[LINKIDTAG]Door '[DOORSTATENAME]' was opened without unlocking the door handle.		
Door Access Control > Door Handle > (handle name) > Mechanically Unlocked	[LINKIDTAG]Door handle '[DOORHANDLENAME]' was opened without being electronically unlocked.		
Peripheral Device Slot > Numeric Sensor > Above upper critical threshold	Peripheral device '[EXTSENSORNAME]' in [FORMATTEDEXTSENSORSLOT] asserted 'above upper critical' at [SENSORREADING] [SENSORREADINGUNIT].	Peripheral device '[EXTSENSORNAME]' in [FORMATTEDEXTSENSORSLOT] deasserted 'above upper critical' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	
Peripheral Device Slot > Numeric Sensor > Above upper warning threshold	Peripheral device '[EXTSENSORNAME]' in [FORMATTEDEXTSENSORSLOT] asserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT].	Peripheral device '[EXTSENSORNAME]' in [FORMATTEDEXTSENSORSLOT] deasserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	

Peripheral Device Slot > Numeric Sensor > Below lower critical threshold	Peripheral device '[EXTSENSORNAME]' in [FORMATTEDEXTSENSORSLOT] asserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT].	Peripheral device '[EXTSENSORNAME]' in [FORMATTEDEXTSENSORSLOT] deasserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	
Peripheral Device Slot > Numeric Sensor > Below lower warning threshold	Peripheral device '[EXTSENSORNAME]' in [FORMATTEDEXTSENSORSLOT] asserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT].	Peripheral device '[EXTSENSORNAME]' in [FORMATTEDEXTSENSORSLOT] deasserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	
Peripheral Device Slot > Numeric Sensor > Unavailable	Peripheral device '[EXTSENSORNAME]' in [FORMATTEDEXTSENSORSLOT] has become unavailable.	Peripheral device '[EXTSENSORNAME]' in [FORMATTEDEXTSENSORSLOT] is no longer unavailable; it is now [SENSORSTATENAME].	
Peripheral Device Slot > State Sensor / Actuator > Alarmed	Peripheral device '[EXTSENSORNAME]' in [FORMATTEDEXTSENSORSLOT] is [SENSORSTATENAME].	Peripheral device '[EXTSENSORNAME]' in [FORMATTEDEXTSENSORSLOT] is [SENSORSTATENAME].	
Peripheral Device Slot > State Sensor / Actuator > Switched by user	Peripheral device '[EXTSENSORNAME]' in [FORMATTEDEXTSENSORSLOT] has been switched to [SENSORSTATENAME] by user '[USERNAME]' from host '[USERIP]'.		
Peripheral Device Slot > State Sensor / Actuator > Unavailable	Peripheral device '[EXTSENSORNAME]' in [FORMATTEDEXTSENSORSLOT] has become unavailable.	Peripheral device '[EXTSENSORNAME]' in [FORMATTEDEXTSENSORSLOT] is no longer unavailable; it is now [SENSORSTATENAME].	
Keypad Management > Keypad > PIN entered	PIN entered at Keypad '[FORMATTEDKEYPADPATH]'.		
Keypad Management > Keypad attached	Keypad '[FORMATTEDKEYPADPATH]' connected.		
Keypad Management > Keypad detached	Keypad '[FORMATTEDKEYPADPATH]' disconnected.		
Keypad Management > Keypad settings changed	Settings with name '[KEYPADNAME]' and description '[KEYPADDESCRIPTION]' set at Keypad '[FORMATTEDKEYPADPATH]' by user '[USERNAME]' from host '[USERIP]'.		
Linking > Link unit added	Link unit [LINKID] ([LINKUNITHOST]) has been added by user '[USERNAME]' from '[USERIP]'.		
Linking > Link unit communication failed	Communication with link unit [LINKID] ([LINKUNITHOST]) failed.	Communication with link unit [LINKID] ([LINKUNITHOST]) is OK.	

Raritan
A brand of legrand

Linking > Link unit released	Link unit [LINKID] ([LINKUNITHOST]) has been released by user '[USERNAME]' from '[USERIP]'.		
Outlet Grouping > Outlet Group > Outlet Group Modified	Outlet group '[OUTLETGROUPID]' was modified.		
Outlet Grouping > Outlet Group > Power control > Power cycled	Outlet group '[OUTLETGROUPID]' power cycle initiated by user '[USERNAME]' from host '[USERIP]'.		
Outlet Grouping > Outlet Group > Power control > Powered off	Outlet group '[OUTLETGROUPID]' has been powered off by user '[USERNAME]' from host '[USERIP]'.		
Outlet Grouping > Outlet Group > Power control > Powered on	Outlet group '[OUTLETGROUPID]' has been powered on by user '[USERNAME]' from host '[USERIP]'.		
Outlet Grouping > Outlet Group > Sensor > Above upper critical threshold	Sensor '[OUTLETGROUPSENSOR]' on outlet group '[OUTLETGROUPID]' asserted 'above upper critical' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[OUTLETGROUPSENSOR]' on outlet group '[OUTLETGROUPID]' deasserted 'above upper critical' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	
Outlet Grouping > Outlet Group > Sensor > Above upper warning threshold	Sensor '[OUTLETGROUPSENSOR]' on outlet group '[OUTLETGROUPID]' asserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[OUTLETGROUPSENSOR]' on outlet group '[OUTLETGROUPID]' deasserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	
Outlet Grouping > Outlet Group > Sensor > Below lower critical threshold	Sensor '[OUTLETGROUPSENSOR]' on outlet group '[OUTLETGROUPID]' asserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[OUTLETGROUPSENSOR]' on outlet group '[OUTLETGROUPID]' deasserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	
Outlet Grouping > Outlet Group > Sensor > Below lower warning threshold	Sensor '[OUTLETGROUPSENSOR]' on outlet group '[OUTLETGROUPID]' asserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[OUTLETGROUPSENSOR]' on outlet group '[OUTLETGROUPID]' deasserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	
Outlet Grouping > Outlet Group > Sensor > Reset	Sensor '[OUTLETGROUPSENSOR]' on outlet group '[OUTLETGROUPID]' has been reset by user '[USERNAME]' from host '[USERIP]'.		
Outlet Grouping > Outlet Group > Sensor > Unavailable	Sensor '[OUTLETGROUPSENSOR]' of outlet group '[OUTLETGROUPID]' has become unavailable.	Sensor '[OUTLETGROUPSENSOR]' on outlet group '[OUTLETGROUPID]' is no longer unavailable; it is now [SENSORSTATENAME].	

Outlet Grouping > Outlet Group Created	Outlet group '[OUTLETGROUPID]' was created.		
Outlet Grouping > Outlet Group Deleted	Outlet group '[OUTLETGROUPID]' was deleted.		
PDU > Controller > Communication failed	Communication with PDU [PDUNUMBER] controller '[CONTROLLER]' (board ID [BOARDID]) failed	Communication with PDU [PDUNUMBER] controller '[CONTROLLER]' (board ID [BOARDID]) restored	
PDU > Controller > Firmware update	PDU [PDUNUMBER] controller '[CONTROLLER]' with board ID [BOARDID] has started firmware update	PDU [PDUNUMBER] controller '[CONTROLLER]' with board ID [BOARDID] has completed firmware update	
PDU > Controller > Incompatible	PDU [PDUNUMBER] controller '[CONTROLLER]' with board ID [BOARDID] is incompatible	PDU [PDUNUMBER] controller '[CONTROLLER]' with board ID [BOARDID] is no longer incompatible	
PDU > Controller > OK	PDU [PDUNUMBER] controller '[CONTROLLER]' with board ID [BOARDID] is OK	PDU [PDUNUMBER] controller '[CONTROLLER]' with board ID [BOARDID] is no longer OK	
PDU > Inlet > Dip	A dip event occurred on PDU [PDUNUMBER] inlet '[INLET]' for [DIPSWELLDURATION] s with a minimum voltage of [DIPSWELLVOLTAGE] V.		PX4 or PRO4X
PDU > Inlet > Dip/swell event list cleared	The dip/swell event list for PDU [PDUNUMBER] inlet '[INLET]' was cleared by user '[USERNAME]' from host '[USERIP]'.		PX4 or PRO4X
PDU > Inlet > Enabled	PDU [PDUNUMBER] inlet '[INLET]' has been enabled by user '[USERNAME]' from host '[USERIP]'.	PDU [PDUNUMBER] inlet '[INLET]' has been disabled by user '[USERNAME]' from host '[USERIP]'.	
PDU > Inlet > Line Pair > Sensor > Above upper critical threshold	Sensor '[PDULINEPAIRSENSOR]' on line '[INLETLINEPAIR]' of PDU [PDUNUMBER] inlet '[INLET]' asserted 'above upper critical' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[PDULINEPAIRSENSOR]' on line '[INLETLINEPAIR]' of PDU [PDUNUMBER] inlet '[INLET]' deasserted 'above upper critical' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	
PDU > Inlet > Line Pair > Sensor > Above upper warning threshold	Sensor '[PDULINEPAIRSENSOR]' on line '[INLETLINEPAIR]' of PDU [PDUNUMBER] inlet '[INLET]' asserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[PDULINEPAIRSENSOR]' on line '[INLETLINEPAIR]' of PDU [PDUNUMBER] inlet '[INLET]' deasserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	

PDU > Inlet > Line Pair > Sensor > Below lower critical threshold	Sensor '[PDULINEPAIRSENSOR]' on line '[INLETLINEPAIR]' of PDU [PDUNUMBER] inlet '[INLET]' asserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[PDULINEPAIRSENSOR]' on line '[INLETLINEPAIR]' of PDU [PDUNUMBER] inlet '[INLET]' deasserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	
PDU > Inlet > Line Pair > Sensor > Below lower warning threshold	Sensor '[PDULINEPAIRSENSOR]' on line '[INLETLINEPAIR]' of PDU [PDUNUMBER] inlet '[INLET]' asserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[PDULINEPAIRSENSOR]' on line '[INLETLINEPAIR]' of PDU [PDUNUMBER] inlet '[INLET]' deasserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	
PDU > Inlet > Line Pair > Sensor > Unavailable	Sensor '[PDULINEPAIRSENSOR]' on line '[INLETLINEPAIR]' of PDU [PDUNUMBER] inlet '[INLET]' has become unavailable.	Sensor '[PDULINEPAIRSENSOR]' on line '[INLETLINEPAIR]' of PDU [PDUNUMBER] inlet '[INLET]' is no longer unavailable; it is now [SENSORSTATENAME].	
PDU > Inlet > Pole > Dip	A dip event occurred on pole '[INLETPOLE]' of PDU [PDUNUMBER] inlet '[INLET]' for [DIPSWELLDURATION] s with a minimum voltage of [DIPSWELLVOLTAGE] V.		PX4 or PRO4X
PDU > Inlet > Pole > Dip/swell event list cleared	The dip/swell event list for pole '[INLETPOLE]' of PDU [PDUNUMBER] inlet '[INLET]' was cleared by user '[USERNAME]' from host '[USERIP]'.		PX4 or PRO4X
PDU > Inlet > Pole > Sensor > Above upper critical threshold	Sensor '[PDUPOLESENSOR]' on pole '[INLETPOLE]' of PDU [PDUNUMBER] inlet '[INLET]' asserted 'above upper critical' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[PDUPOLESENSOR]' on pole '[INLETPOLE]' of PDU [PDUNUMBER] inlet '[INLET]' deasserted 'above upper critical' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	
PDU > Inlet > Pole > Sensor > Above upper warning threshold	Sensor '[PDUPOLESENSOR]' on pole '[INLETPOLE]' of PDU [PDUNUMBER] inlet '[INLET]' asserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[PDUPOLESENSOR]' on pole '[INLETPOLE]' of PDU [PDUNUMBER] inlet '[INLET]' deasserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	
PDU > Inlet > Pole > Sensor > Below lower critical threshold	Sensor '[PDUPOLESENSOR]' on pole '[INLETPOLE]' of PDU [PDUNUMBER] inlet '[INLET]' asserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[PDUPOLESENSOR]' on pole '[INLETPOLE]' of PDU [PDUNUMBER] inlet '[INLET]' deasserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	

PDU > Inlet > Pole > Sensor > Below lower warning threshold	Sensor '[PDUPOLESENSOR]' on pole '[INLETPOLE]' of PDU [PDUNUMBER] inlet '[INLET]' asserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[PDUPOLESENSOR]' on pole '[INLETPOLE]' of PDU [PDUNUMBER] inlet '[INLET]' deasserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	
PDU > Inlet > Pole > Sensor > Critical	Sensor '[PDUPOLESENSOR]' on pole '[INLETPOLE]' of PDU [PDUNUMBER] inlet '[INLET]' entered critical state.	Sensor '[PDUPOLESENSOR]' on pole '[INLETPOLE]' of PDU [PDUNUMBER] inlet '[INLET]' exited critical state; it is now [SENSORSTATENAME].	
PDU > Inlet > Pole > Sensor > Failed	Sensor '[PDUPOLESENSOR]' on pole '[INLETPOLE]' of PDU [PDUNUMBER] inlet '[INLET]' entered failed state.	Sensor '[PDUPOLESENSOR]' on pole '[INLETPOLE]' of PDU [PDUNUMBER] inlet '[INLET]' exited failed state; it is now [SENSORSTATENAME].	
PDU > Inlet > Pole > Sensor > Normal	Sensor '[PDUPOLESENSOR]' on pole '[INLETPOLE]' of PDU [PDUNUMBER] inlet '[INLET]' entered normal state.	Sensor '[PDUPOLESENSOR]' on pole '[INLETPOLE]' of PDU [PDUNUMBER] inlet '[INLET]' exited normal state; it is now [SENSORSTATENAME].	
PDU > Inlet > Pole > Sensor > Self-Test	Sensor '[PDUPOLESENSOR]' on pole '[INLETPOLE]' of PDU [PDUNUMBER] inlet '[INLET]' started self test.	Sensor '[PDUPOLESENSOR]' on pole '[INLETPOLE]' of PDU [PDUNUMBER] inlet '[INLET]' finished self test; it is now [SENSORSTATENAME].	
PDU > Inlet > Pole > Sensor > Unavailable	Sensor '[PDUPOLESENSOR]' on pole '[INLETPOLE]' of PDU [PDUNUMBER] inlet '[INLET]' has become unavailable.	Sensor '[PDUPOLESENSOR]' on pole '[INLETPOLE]' of PDU [PDUNUMBER] inlet '[INLET]' is no longer unavailable; it is now [SENSORSTATENAME].	
PDU > Inlet > Pole > Sensor > Warning	Sensor '[PDUPOLESENSOR]' on pole '[INLETPOLE]' of PDU [PDUNUMBER] inlet '[INLET]' entered warning state.	Sensor '[PDUPOLESENSOR]' on pole '[INLETPOLE]' of PDU [PDUNUMBER] inlet '[INLET]' exited warning state; it is now [SENSORSTATENAME].	
PDU > Inlet > Pole > Swell	A swell event occurred on pole '[INLETPOLE]' of PDU [PDUNUMBER] inlet '[INLET]' for [DIPSWELLDURATION] s with a maximum voltage of [DIPSWELLVOLTAGE] V.		PX4 or PRO4X
PDU > Inlet > Sensor > Above upper critical threshold	Sensor '[INLETSENSOR]' on PDU [PDUNUMBER] inlet '[INLET]' asserted 'above upper critical' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[INLETSENSOR]' on PDU [PDUNUMBER] inlet '[INLET]' deasserted 'above upper critical' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	
PDU > Inlet > Sensor > Above upper warning threshold	Sensor '[INLETSENSOR]' on PDU [PDUNUMBER] inlet '[INLET]' asserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[INLETSENSOR]' on PDU [PDUNUMBER] inlet '[INLET]' deasserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	

PDU > Inlet > Sensor > Below lower critical threshold	Sensor '[INLETSENSOR]' on PDU [PDUNUMBER] inlet '[INLET]' asserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[INLETSENSOR]' on PDU [PDUNUMBER] inlet '[INLET]' deasserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	
PDU > Inlet > Sensor > Below lower warning threshold	Sensor '[INLETSENSOR]' on PDU [PDUNUMBER] inlet '[INLET]' asserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[INLETSENSOR]' on PDU [PDUNUMBER] inlet '[INLET]' deasserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	
PDU > Inlet > Sensor > Critical	Sensor '[INLETSENSOR]' on PDU [PDUNUMBER] inlet '[INLET]' entered critical state.	Sensor '[INLETSENSOR]' on PDU [PDUNUMBER] inlet '[INLET]' exited critical state; it is now [SENSORSTATENAME].	
PDU > Inlet > Sensor > Failed	Sensor '[INLETSENSOR]' on PDU [PDUNUMBER] inlet '[INLET]' entered failed state.	Sensor '[INLETSENSOR]' on PDU [PDUNUMBER] inlet '[INLET]' exited failed state; it is now [SENSORSTATENAME].	
PDU > Inlet > Sensor > Fault	Sensor '[INLETSENSOR]' on PDU [PDUNUMBER] inlet '[INLET]' entered fault state.	Sensor '[INLETSENSOR]' on PDU [PDUNUMBER] inlet '[INLET]' exited fault state; it is now [SENSORSTATENAME].	
PDU > Inlet > Sensor > Normal	Sensor '[INLETSENSOR]' on PDU [PDUNUMBER] inlet '[INLET]' entered normal state.	Sensor '[INLETSENSOR]' on PDU [PDUNUMBER] inlet '[INLET]' exited normal state; it is now [SENSORSTATENAME].	
PDU > Inlet > Sensor > OK	Sensor '[INLETSENSOR]' on PDU [PDUNUMBER] inlet '[INLET]' entered OK state.	Sensor '[INLETSENSOR]' on PDU [PDUNUMBER] inlet '[INLET]' exited OK state; it is now [SENSORSTATENAME].	
PDU > Inlet > Sensor > Reset	Sensor '[INLETSENSOR]' on PDU [PDUNUMBER] inlet '[INLET]' has been reset by user '[USERNAME]' from host '[USERIP]'.		
PDU > Inlet > Sensor > Self-Test	Sensor '[INLETSENSOR]' on PDU [PDUNUMBER] inlet '[INLET]' started self test.	Sensor '[INLETSENSOR]' on PDU [PDUNUMBER] inlet '[INLET]' finished self test; it is now [SENSORSTATENAME].	
PDU > Inlet > Sensor > Unavailable	Sensor '[INLETSENSOR]' on PDU [PDUNUMBER] inlet '[INLET]' has become unavailable.	Sensor '[INLETSENSOR]' on PDU [PDUNUMBER] inlet '[INLET]' is no longer unavailable; it is now [SENSORSTATENAME].	
PDU > Inlet > Sensor > Warning	Sensor '[INLETSENSOR]' on PDU [PDUNUMBER] inlet '[INLET]' entered warning state.	Sensor '[INLETSENSOR]' on PDU [PDUNUMBER] inlet '[INLET]' exited warning state; it is now [SENSORSTATENAME].	

PDU > Inlet > Swell	A swell event occurred on PDU [PDUNUMBER] inlet '[INLET]' for [DIPSWELLDURATION] s with a maximum voltage of [DIPSWELLVOLTAGE] V.		PX4 or PRO4X
PDU > Load Shedding > Started	PDU [PDUNUMBER] placed in Load Shedding Mode by user '[USERNAME]' from host '[USERIP]'.	PDU [PDUNUMBER] removed from Load Shedding Mode by user '[USERNAME]' from host '[USERIP]'.	
PDU > Outlet > Pole > Sensor > Above upper critical threshold	Sensor '[PDUPOLESENSOR]' on pole '[OUTLETPOLE]' of PDU [PDUNUMBER] outlet '[OUTLET]' asserted 'above upper critical' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[PDUPOLESENSOR]' on pole '[OUTLETPOLE]' of PDU [PDUNUMBER] outlet '[OUTLET]' deasserted 'above upper critical' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	
PDU > Outlet > Pole > Sensor > Above upper warning threshold	Sensor '[PDUPOLESENSOR]' on pole '[OUTLETPOLE]' of PDU [PDUNUMBER] outlet '[OUTLET]' asserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[PDUPOLESENSOR]' on pole '[OUTLETPOLE]' of PDU [PDUNUMBER] outlet '[OUTLET]' deasserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	
PDU > Outlet > Pole > Sensor > Below lower critical threshold	Sensor '[PDUPOLESENSOR]' on pole '[OUTLETPOLE]' of PDU [PDUNUMBER] outlet '[OUTLET]' asserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[PDUPOLESENSOR]' on pole '[OUTLETPOLE]' of PDU [PDUNUMBER] outlet '[OUTLET]' deasserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	
PDU > Outlet > Pole > Sensor > Below lower warning threshold	Sensor '[PDUPOLESENSOR]' on pole '[OUTLETPOLE]' of PDU [PDUNUMBER] outlet '[OUTLET]' asserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[PDUPOLESENSOR]' on pole '[OUTLETPOLE]' of PDU [PDUNUMBER] outlet '[OUTLET]' deasserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	
PDU > Outlet > Pole > Sensor > Unavailable	Sensor '[PDUPOLESENSOR]' on pole '[OUTLETPOLE]' of PDU [PDUNUMBER] outlet '[OUTLET]' has become unavailable.	Sensor '[PDUPOLESENSOR]' on pole '[OUTLETPOLE]' of PDU [PDUNUMBER] outlet '[OUTLET]' is no longer unavailable; it is now [SENSORSTATENAME].	
PDU > Outlet > Power control > Power cycled	PDU [PDUNUMBER] outlet '[OUTLET]' power cycle initiated by user '[USERNAME]' from host '[USERIP]'.		
PDU > Outlet > Power control > Powered off	PDU [PDUNUMBER] outlet '[OUTLET]' has been powered off by user '[USERNAME]' from host '[USERIP]'.		
PDU > Outlet > Power control > Powered on	PDU [PDUNUMBER] outlet '[OUTLET]' has been powered on by user '[USERNAME]' from host '[USERIP]'.		

Raritan
A brand of legrand

PDU > Outlet > Sensor > Above upper critical threshold	Sensor '[OUTLETSENSOR]' on PDU [PDUNUMBER] outlet '[OUTLET]' asserted 'above upper critical' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[OUTLETSENSOR]' on PDU [PDUNUMBER] outlet '[OUTLET]' deasserted 'above upper critical' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	
PDU > Outlet > Sensor > Above upper warning threshold	Sensor '[OUTLETSENSOR]' on PDU [PDUNUMBER] outlet '[OUTLET]' asserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[OUTLETSENSOR]' on PDU [PDUNUMBER] outlet '[OUTLET]' deasserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	
PDU > Outlet > Sensor > Below lower critical threshold	Sensor '[OUTLETSENSOR]' on PDU [PDUNUMBER] outlet '[OUTLET]' asserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[OUTLETSENSOR]' on PDU [PDUNUMBER] outlet '[OUTLET]' deasserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	
PDU > Outlet > Sensor > Below lower warning threshold	Sensor '[OUTLETSENSOR]' on PDU [PDUNUMBER] outlet '[OUTLET]' asserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[OUTLETSENSOR]' on PDU [PDUNUMBER] outlet '[OUTLET]' deasserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	
PDU > Outlet > Sensor > On	PDU [PDUNUMBER] outlet '[OUTLET]' state sensor changed to on.	PDU [PDUNUMBER] outlet '[OUTLET]' state sensor is no longer on; it is now [SENSORSTATENAME].	
PDU > Outlet > Sensor > Reset	Sensor '[OUTLETSENSOR]' on outlet '[OUTLET]' has been reset by user '[USERNAME]' from host '[USERIP]'.		
PDU > Outlet > Sensor > Unavailable	Sensor '[OUTLETSENSOR]' on PDU [PDUNUMBER] outlet '[OUTLET]' has become unavailable.	Sensor '[OUTLETSENSOR]' on PDU [PDUNUMBER] outlet '[OUTLET]' is no longer unavailable; it is now [SENSORSTATENAME].	
PDU > Outlet > Suspended	PDU [PDUNUMBER] outlet '[OUTLET]' was suspended after being suspected of having caused an OCP trip event.		
PDU > Overcurrent Protector > Sensor > Above upper critical threshold	Sensor '[OCPSENSOR]' on PDU [PDUNUMBER] overcurrent protector '[OCP]' asserted 'above upper critical' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[OCPSENSOR]' on PDU [PDUNUMBER] overcurrent protector '[OCP]' deasserted 'above upper critical' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	

PDU > Overcurrent Protector > Sensor > Above upper warning threshold	Sensor '[OCPSENSOR]' on PDU [PDUNUMBER] overcurrent protector '[OCP]' asserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[OCPSENSOR]' on PDU [PDUNUMBER] overcurrent protector '[OCP]' deasserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	
PDU > Overcurrent Protector > Sensor > Below lower critical threshold	Sensor '[OCPSENSOR]' on PDU [PDUNUMBER] overcurrent protector '[OCP]' asserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[OCPSENSOR]' on PDU [PDUNUMBER] overcurrent protector '[OCP]' deasserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	
PDU > Overcurrent Protector > Sensor > Below lower warning threshold	Sensor '[OCPSENSOR]' on PDU [PDUNUMBER] overcurrent protector '[OCP]' asserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[OCPSENSOR]' on PDU [PDUNUMBER] overcurrent protector '[OCP]' deasserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	
PDU > Overcurrent Protector > Sensor > Critical	Sensor '[OCPSENSOR]' on PDU [PDUNUMBER] overcurrent protector '[OCP]' entered critical state.	Sensor '[OCPSENSOR]' on PDU [PDUNUMBER] overcurrent protector '[OCP]' exited critical state; it is now [SENSORSTATENAME].	
PDU > Overcurrent Protector > Sensor > Failed	Sensor '[OCPSENSOR]' on PDU [PDUNUMBER] overcurrent protector '[OCP]' entered failed state.	Sensor '[OCPSENSOR]' on PDU [PDUNUMBER] overcurrent protector '[OCP]' exited failed state; it is now [SENSORSTATENAME].	
PDU > Overcurrent Protector > Sensor > Normal	Sensor '[OCPSENSOR]' on PDU [PDUNUMBER] overcurrent protector '[OCP]' entered normal state.	Sensor '[OCPSENSOR]' on PDU [PDUNUMBER] overcurrent protector '[OCP]' exited normal state; it is now [SENSORSTATENAME].	
PDU > Overcurrent Protector > Sensor > Open	Sensor '[OCPSENSOR]' on PDU [PDUNUMBER] overcurrent protector '[OCP]' is open. [OCPTRIPCAUSEINFO]	Sensor '[OCPSENSOR]' on PDU [PDUNUMBER] overcurrent protector '[OCP]' is no longer open; it is now [SENSORSTATENAME].	
PDU > Overcurrent Protector > Sensor > Self-Test	Sensor '[OCPSENSOR]' on PDU [PDUNUMBER] overcurrent protector '[OCP]' started self test.	Sensor '[OCPSENSOR]' on PDU [PDUNUMBER] overcurrent protector '[OCP]' finished self test; it is now [SENSORSTATENAME].	
PDU > Overcurrent Protector > Sensor > Unavailable	Sensor '[OCPSENSOR]' on PDU [PDUNUMBER] overcurrent protector '[OCP]' has become unavailable.	Sensor '[OCPSENSOR]' on PDU [PDUNUMBER] overcurrent protector '[OCP]' is no longer unavailable; it is now [SENSORSTATENAME].	

PDU > Overcurrent Protector > Sensor > Warning	Sensor '[OCPSENSOR]' on PDU [PDUNUMBER] overcurrent protector '[OCP]' entered warning state.	Sensor '[OCPSENSOR]' on PDU [PDUNUMBER] overcurrent protector '[OCP]' exited warning state; it is now [SENSORSTATENAME].	
PDU > Sensor > Above upper critical threshold	PDU [PDUNUMBER] sensor '[PDUSENSOR]' asserted 'above upper critical' at [SENSORREADING] [SENSORREADINGUNIT].	PDU [PDUNUMBER] sensor '[PDUSENSOR]' deasserted 'above upper critical' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	
PDU > Sensor > Above upper warning threshold	PDU [PDUNUMBER] sensor '[PDUSENSOR]' asserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT].	PDU [PDUNUMBER] sensor '[PDUSENSOR]' deasserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	
PDU > Sensor > Below lower critical threshold	PDU [PDUNUMBER] sensor '[PDUSENSOR]' asserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT].	PDU [PDUNUMBER] sensor '[PDUSENSOR]' deasserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	
PDU > Sensor > Below lower warning threshold	PDU [PDUNUMBER] sensor '[PDUSENSOR]' asserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT].	PDU [PDUNUMBER] sensor '[PDUSENSOR]' deasserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	
PDU > Sensor > Fault	PDU [PDUNUMBER] sensor '[PDUSENSOR]' entered fault state.	PDU [PDUNUMBER] sensor '[PDUSENSOR]' exited fault state; it is now [SENSORSTATENAME].	
PDU > Sensor > Reset	PDU [PDUNUMBER] sensor '[PDUSENSOR]' has been reset by user '[USERNAME]' from host '[USERIP]'.		
PDU > Sensor > Unavailable	PDU [PDUNUMBER] sensor '[PDUSENSOR]' has become unavailable.	PDU [PDUNUMBER] sensor '[PDUSENSOR]' is no longer unavailable; it is now [SENSORSTATENAME].	
PDU > Transfer Switch > Active inlet changed	Active inlet on PDU [PDUNUMBER] transfer switch '[TRANSFERSWITCH]' changed to '[ACTIVEINLET]' due to [TRANSFERSWITCHREASON].		Transfer switch
PDU > Transfer Switch > Sensor > Above upper critical threshold	Sensor '[TRANSFERSWITCHSENSOR]' on PDU [PDUNUMBER] transfer switch '[TRANSFERSWITCH]' asserted 'above upper critical' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[TRANSFERSWITCHSENSOR]' on PDU [PDUNUMBER] transfer switch '[TRANSFERSWITCH]' deasserted 'above upper critical' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	Transfer switch

PDU > Transfer Switch > Sensor > Above upper warning threshold	Sensor '[TRANSFERSWITCHSENSOR]' on PDU [PDUNUMBER] transfer switch '[TRANSFERSWITCH]' asserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[TRANSFERSWITCHSENSOR]' on PDU [PDUNUMBER] transfer switch '[TRANSFERSWITCH]' deasserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	Transfer switch
PDU > Transfer Switch > Sensor > Below lower critical threshold	Sensor '[TRANSFERSWITCHSENSOR]' on PDU [PDUNUMBER] transfer switch '[TRANSFERSWITCH]' asserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[TRANSFERSWITCHSENSOR]' on PDU [PDUNUMBER] transfer switch '[TRANSFERSWITCH]' deasserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	Transfer switch
PDU > Transfer Switch > Sensor > Below lower warning threshold	Sensor '[TRANSFERSWITCHSENSOR]' on PDU [PDUNUMBER] transfer switch '[TRANSFERSWITCH]' asserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[TRANSFERSWITCHSENSOR]' on PDU [PDUNUMBER] transfer switch '[TRANSFERSWITCH]' deasserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	Transfer switch
PDU > Transfer Switch > Sensor > Fault	Sensor '[TRANSFERSWITCHSENSOR]' on PDU [PDUNUMBER] transfer switch '[TRANSFERSWITCH]' is [SENSORSTATENAME].	Sensor '[TRANSFERSWITCHSENSOR]' on PDU [PDUNUMBER] transfer switch '[TRANSFERSWITCH]' is [SENSORSTATENAME].	Transfer switch
PDU > Transfer Switch > Sensor > Non-redundant	Operational state of PDU [PDUNUMBER] transfer switch '[TRANSFERSWITCH]' is now non-redundant.	Operational state of PDU [PDUNUMBER] transfer switch '[TRANSFERSWITCH]' is no longer non-redundant; it is now [SENSORSTATENAME].	Transfer switch
PDU > Transfer Switch > Sensor > Normal	Operational state of PDU [PDUNUMBER] transfer switch '[TRANSFERSWITCH]' is now normal.	Operational state of PDU [PDUNUMBER] transfer switch '[TRANSFERSWITCH]' is no longer normal; it is now [SENSORSTATENAME].	Transfer switch
PDU > Transfer Switch > Sensor > Off	Operational state of PDU [PDUNUMBER] transfer switch '[TRANSFERSWITCH]' is now off.	Operational state of PDU [PDUNUMBER] transfer switch '[TRANSFERSWITCH]' is no longer off; it is now [SENSORSTATENAME].	Transfer switch
PDU > Transfer Switch > Sensor > Out of sync	Sensor '[TRANSFERSWITCHSENSOR]' on PDU [PDUNUMBER] transfer switch '[TRANSFERSWITCH]' is out of sync.	Sensor '[TRANSFERSWITCHSENSOR]' on PDU [PDUNUMBER] transfer switch '[TRANSFERSWITCH]' is no longer out of sync; it is now [SENSORSTATENAME].	Transfer switch
PDU > Transfer Switch > Sensor > Standby	Operational state of PDU [PDUNUMBER] transfer switch '[TRANSFERSWITCH]' is now standby.	Operational state of PDU [PDUNUMBER] transfer switch '[TRANSFERSWITCH]' is no longer standby; it is now [SENSORSTATENAME].	Transfer switch

Raritan
A brand of legrand

PDU > Transfer Switch > Sensor > Unavailable	Sensor '[TRANSFERSWITCHSENSOR]' on PDU [PDUNUMBER] transfer switch '[TRANSFERSWITCH]' has become unavailable.	Sensor '[TRANSFERSWITCHSENSOR]' on PDU [PDUNUMBER] transfer switch '[TRANSFERSWITCH]' is no longer unavailable; it is now [SENSORSTATENAME].	Transfer switch
Port Fuse > Tripped	Fuse of [FORMATTEDEXTPORT] is [FUSESTATENAME].	Fuse of [FORMATTEDEXTPORT] is [FUSESTATENAME].	
Power Metering Controller > Power Meter > Circuit > Pole > Sensor > Above upper critical threshold	Sensor '[PDUPOLESENSOR]' on pole '[CIRCUITPOLE]' of panel '[POWERMETER]' circuit '[CIRCUIT]' asserted 'above upper critical' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[PDUPOLESENSOR]' on pole '[CIRCUITPOLE]' of panel '[POWERMETER]' circuit '[CIRCUIT]' deasserted 'above upper critical' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	BCM2 / PMC
Power Metering Controller > Power Meter > Circuit > Pole > Sensor > Above upper warning threshold	Sensor '[PDUPOLESENSOR]' on pole '[CIRCUITPOLE]' of panel '[POWERMETER]' circuit '[CIRCUIT]' asserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[PDUPOLESENSOR]' on pole '[CIRCUITPOLE]' of panel '[POWERMETER]' circuit '[CIRCUIT]' deasserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	BCM2 / PMC
Power Metering Controller > Power Meter > Circuit > Pole > Sensor > Below lower critical threshold	Sensor '[PDUPOLESENSOR]' on pole '[CIRCUITPOLE]' of panel '[POWERMETER]' circuit '[CIRCUIT]' asserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[PDUPOLESENSOR]' on pole '[CIRCUITPOLE]' of panel '[POWERMETER]' circuit '[CIRCUIT]' deasserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	BCM2 / PMC
Power Metering Controller > Power Meter > Circuit > Pole > Sensor > Below lower warning threshold	Sensor '[PDUPOLESENSOR]' on pole '[CIRCUITPOLE]' of panel '[POWERMETER]' circuit '[CIRCUIT]' asserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[PDUPOLESENSOR]' on pole '[CIRCUITPOLE]' of panel '[POWERMETER]' circuit '[CIRCUIT]' deasserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	BCM2 / PMC
Power Metering Controller > Power Meter > Circuit > Pole > Sensor > Unavailable	Sensor '[PDUPOLESENSOR]' on pole '[CIRCUITPOLE]' of panel '[POWERMETER]' circuit '[CIRCUIT]' has become unavailable.	Sensor '[PDUPOLESENSOR]' on pole '[CIRCUITPOLE]' of panel '[POWERMETER]' circuit '[CIRCUIT]' is no longer unavailable; it is now [SENSORSTATENAME].	BCM2 / PMC
Power Metering Controller > Power Meter > Circuit > Sensor > Above upper critical threshold	Sensor '[CIRCUITSENSOR]' on panel '[POWERMETER]' circuit '[CIRCUIT]' asserted 'above upper critical' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[CIRCUITSENSOR]' on panel '[POWERMETER]' circuit '[CIRCUIT]' deasserted 'above upper critical' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	BCM2 / PMC

Power Metering Controller > Power Meter > Circuit > Sensor > Above upper warning threshold	Sensor '[CIRCUITSENSOR]' on panel '[POWERMETER]' circuit '[CIRCUIT]' asserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[CIRCUITSENSOR]' on panel '[POWERMETER]' circuit '[CIRCUIT]' deasserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	BCM2 / PMC
Power Metering Controller > Power Meter > Circuit > Sensor > Below lower critical threshold	Sensor '[CIRCUITSENSOR]' on panel '[POWERMETER]' circuit '[CIRCUIT]' asserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[CIRCUITSENSOR]' on panel '[POWERMETER]' circuit '[CIRCUIT]' deasserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	BCM2 / PMC
Power Metering Controller > Power Meter > Circuit > Sensor > Below lower warning threshold	Sensor '[CIRCUITSENSOR]' on panel '[POWERMETER]' circuit '[CIRCUIT]' asserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[CIRCUITSENSOR]' on panel '[POWERMETER]' circuit '[CIRCUIT]' deasserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	BCM2 / PMC
Power Metering Controller > Power Meter > Circuit > Sensor > Reset	Sensor '[CIRCUITSENSOR]' on panel '[POWERMETER]' circuit '[CIRCUIT]' has been reset by user '[USERNAME]' from host '[USERIP]'.		BCM2 / PMC
Power Metering Controller > Power Meter > Circuit > Sensor > Unavailable	Sensor '[CIRCUITSENSOR]' on panel '[POWERMETER]' circuit '[CIRCUIT]' has become unavailable.	Sensor '[CIRCUITSENSOR]' on panel '[POWERMETER]' circuit '[CIRCUIT]' is no longer unavailable; it is now [SENSORSTATENAME].	BCM2 / PMC
Power Metering Controller > Power Meter > Circuit Created	Circuit '[CIRCUIT]' on panel '[POWERMETER]' was created.		BCM2 / PMC
Power Metering Controller > Power Meter > Circuit Deleted	Circuit '[CIRCUIT]' on panel '[POWERMETER]' was deleted.		BCM2 / PMC
Power Metering Controller > Power Meter > Circuit Modified	Circuit '[CIRCUIT]' on panel '[POWERMETER]' was modified.		BCM2 / PMC
Power Metering Controller > Power Meter > Pole > Sensor > Above upper critical threshold	Sensor '[PDUPOLESENSOR]' on pole '[POWERMETERPOLE]' of power meter '[POWERMETER]' asserted 'above upper critical' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[PDUPOLESENSOR]' on pole '[POWERMETERPOLE]' of power meter '[POWERMETER]' deasserted 'above upper critical' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	BCM2 / PMC

Power Metering Controller > Power Meter > Pole > Sensor > Above upper warning threshold	Sensor '[PDUPOLESENSOR]' on pole '[POWERMETERPOLE]' of power meter '[POWERMETER]' asserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[PDUPOLESENSOR]' on pole '[POWERMETERPOLE]' of power meter '[POWERMETER]' deasserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	BCM2 / PMC
Power Metering Controller > Power Meter > Pole > Sensor > Below lower critical threshold	Sensor '[PDUPOLESENSOR]' on pole '[POWERMETERPOLE]' of power meter '[POWERMETER]' asserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[PDUPOLESENSOR]' on pole '[POWERMETERPOLE]' of power meter '[POWERMETER]' deasserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	BCM2 / PMC
Power Metering Controller > Power Meter > Pole > Sensor > Below lower warning threshold	Sensor '[PDUPOLESENSOR]' on pole '[POWERMETERPOLE]' of power meter '[POWERMETER]' asserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[PDUPOLESENSOR]' on pole '[POWERMETERPOLE]' of power meter '[POWERMETER]' deasserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	BCM2 / PMC
Power Metering Controller > Power Meter > Pole > Sensor > Unavailable	Sensor '[PDUPOLESENSOR]' on pole '[POWERMETERPOLE]' of power meter '[POWERMETER]' has become unavailable.	Sensor '[PDUPOLESENSOR]' on pole '[POWERMETERPOLE]' of power meter '[POWERMETER]' is no longer unavailable; it is now [SENSORSTATENAME].	BCM2 / PMC
Power Metering Controller > Power Meter > Sensor > Above upper critical threshold	Sensor '[POWERMETERSENSOR]' on power meter '[POWERMETER]' asserted 'above upper critical' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[POWERMETERSENSOR]' on power meter '[POWERMETER]' deasserted 'above upper critical' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	BCM2 / PMC
Power Metering Controller > Power Meter > Sensor > Above upper warning threshold	Sensor '[POWERMETERSENSOR]' on power meter '[POWERMETER]' asserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[POWERMETERSENSOR]' on power meter '[POWERMETER]' deasserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	BCM2 / PMC
Power Metering Controller > Power Meter > Sensor > Below lower critical threshold	Sensor '[POWERMETERSENSOR]' on power meter '[POWERMETER]' asserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[POWERMETERSENSOR]' on power meter '[POWERMETER]' deasserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	BCM2 / PMC
Power Metering Controller > Power Meter > Sensor > Below lower warning threshold	Sensor '[POWERMETERSENSOR]' on power meter '[POWERMETER]' asserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[POWERMETERSENSOR]' on power meter '[POWERMETER]' deasserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	BCM2 / PMC

Power Metering Controller > Power Meter > Sensor > Reset	Sensor '[POWERMETERSENSOR]' on power meter '[POWERMETER]' has been reset by user '[USERNAME]' from host '[USERIP]'.		BCM2 / PMC
Power Metering Controller > Power Meter > Sensor > Unavailable	Sensor '[POWERMETERSENSOR]' on power meter '[POWERMETER]' has become unavailable.	Sensor '[POWERMETERSENSOR]' on power meter '[POWERMETER]' is no longer unavailable; it is now [SENSORSTATENAME].	BCM2 / PMC
Power Metering Controller > Power Meter Created	Power meter '[POWERMETER]' was created.		BCM2 / PMC
Power Metering Controller > Power Meter Deleted	Power meter '[POWERMETER]' was deleted.		BCM2 / PMC
Power Metering Controller > Power Meter Modified	Power meter '[POWERMETER]' was modified.		BCM2 / PMC
Server Monitoring > Error	Error monitoring server '[MONITOREDHOST]': [ERRORDESC]		BCM2 / PMC
Server Monitoring > Monitored	Server '[MONITOREDHOST]' is now being monitored.	Server '[MONITOREDHOST]' is no longer being monitored.	BCM2 / PMC
Server Monitoring > Power control completed	Power control operation for '[MONITOREDHOST]' finished with result: [SERVERPOWERRESULT]		BCM2 / PMC
Server Monitoring > Power control initiated	User '[USERNAME]' initiated a power control operation for '[MONITOREDHOST]': [SERVERPOWEROPERATION]		BCM2 / PMC
Server Monitoring > Unreachable	Server '[MONITOREDHOST]' is unreachable.	Server '[MONITOREDHOST]' is reachable.	BCM2 / PMC
Server Monitoring > Unrecoverable	Connection to server '[MONITOREDHOST]' could not be restored.		BCM2 / PMC
Test > Test Event	A test event was triggered by user '[USERNAME]'.		
Timer Event > Occurred	Timer event '[EVENTRULENAME]' occurred.		
User Activity > User accepted the Restricted Service Agreement	User '[USERNAME]' from host '[USERIP]' accepted the Restricted Service Agreement.	User '[USERNAME]' from host '[USERIP]' declined the Restricted Service Agreement.	
User Activity > Authentication failure	Authentication failed for user '[USERNAME]' from host '[USERIP]'.		
User Activity > User logon state	User '[USERNAME]' from host '[USERIP]' logged in.	User '[USERNAME]' from host '[USERIP]' logged out.	

Raritan
A brand of legrand

User Activity > Session timeout	Session of user '[USERNAME]' from host '[USERIP]' timed out.		
User Activity > User blocked	User '[USERNAME]' from host '[USERIP]' was blocked.		
User Administration > Password changed	Password of user '[UMTARGETUSER]' changed by user '[USERNAME]' from host '[USERIP]'.		
User Administration > Password settings changed	Password settings changed by user '[USERNAME]' from host '[USERIP]'.		
User Administration > Role added	Role '[UMTARGETROLE]' added by user '[USERNAME]' from host '[USERIP]'.		
User Administration > Role deleted	Role '[UMTARGETROLE]' deleted by user '[USERNAME]' from host '[USERIP]'.		
User Administration > Role modified	Role '[UMTARGETROLE]' modified by user '[USERNAME]' from host '[USERIP]'.		
User Administration > User added	User '[UMTARGETUSER]' added by user '[USERNAME]' from host '[USERIP]'.		
User Administration > User deleted	User '[UMTARGETUSER]' deleted by user '[USERNAME]' from host '[USERIP]'.		
User Administration > User modified	User '[UMTARGETUSER]' modified by user '[USERNAME]' from host '[USERIP]'.		
User Administration > User renamed	User '[UMTARGETUSER]' renamed to '[NEWUMTARGETUSER]' by user '[USERNAME]' from host '[USERIP]'.		
Webcam Management > Image upload started	A snapshot upload of webcam '[WEBCAMNAME]' to folder [WEBCAMSNAPSHOTFOLDERURL] was started.		
Webcam Management > Webcam attached	Webcam '[WEBCAMNAME]' ('[WEBCAMMODEL]') added to port '[WEBCAMUSBPORT]'.		
Webcam Management > Webcam detached	Webcam '[WEBCAMNAME]' ('[WEBCAMMODEL]') removed from port '[WEBCAMUSBPORT]'.		
Webcam Management > Webcam settings changed	Webcam '[WEBCAMNAME]' settings changed by user '[USERNAME]'		

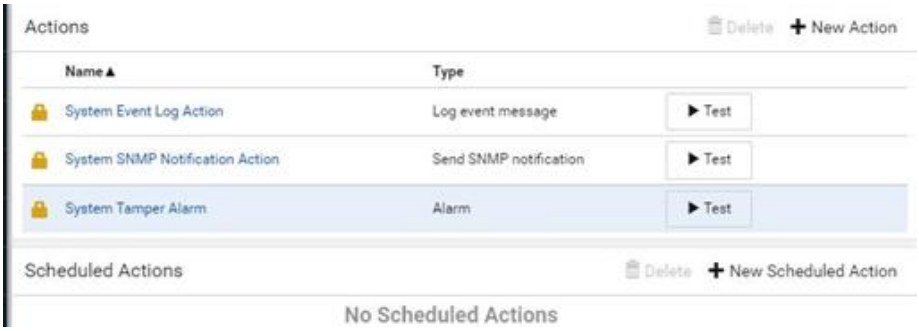
Available Actions

There are several built-in actions, which cannot be deleted. You can create additional actions for responding to different events.

Some actions have messages that you can customize using placeholders that will populate with specific information when the message is generated. Custom messages with placeholders can be used in these actions: Log event message, Send SMS, Send email (subject+body), Send webcam image (subject+body).

► *To test an action:*

- Click the Test button next to the Action. The action is triggered and you can verify it.



► *Built-in actions:*

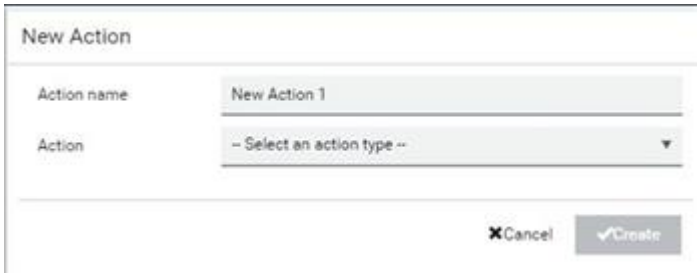
- *System Event Log Action:*
  This action records the selected event in the internal log when the event occurs.
- *System SNMP Notification Action:*
  This action sends SNMP notifications to one or multiple IP addresses after the selected event occurs.

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

- *System Tamper Alarm:*
  This action causes the PX4 to show the alarm for the tamper sensor, if any, on the Dashboard page until a person acknowledges it. By default, this action has been assigned to the built-in tamper detection event rules.

► *Actions you can create:*

1. Choose Device Settings > Event Rules > New Action.
2. Click the Action field to select an action type from the list.



3. Available actions depend on your model. See next sections for details on each action you can configure.
4. Click Create to save an action, then you can include it in an event rule.

Alarm

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

If the Alarm action has been included in a specific event rule and no one acknowledges that alert after it occurs, the PX4 resends or regenerates an alert notification regularly until the alert is acknowledged or the maximum number of alert notifications is sent. You can acknowledge an alert in the Dashboard.

► *Operation:*

1. Choose Device Settings > Event Rules > ✚ New Action .
2. Select Alarm from the Action list.
3. In the Alarm Notifications list box, specify one or multiple ways to issue the alert notifications. Available methods vary, depending on how many notification-based actions have been created. Notification-based action types include:

- External beeper
- Syslog message
- Send email
- Send SMS message
- Internal beeper

If no appropriate actions are available, create them first.

a. To select any methods, select them one by one in the Available field.
To add all available methods, simply click Select All.

b. To delete any methods, click a method's ✖ in the Selected field.
To remove all methods, simply click Deselect All.

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

5. In the 'Re-scheduling period' field, specify the time interval (in minutes) at which the alert notification is resent or regenerated regularly.
6. In the 'Re-scheduling limit' field, specify the maximum number of times the alert notification is resent. Values range from 1 to infinite.
7. (Optional) You can instruct the PX4 to send the acknowledgment notification after the alarm is acknowledged in the 'Acknowledgment notifications' field. Available methods are identical to those for generating alarm notifications.
   a. In the Available field, select desired methods, or click Select All.
   b. In the Selected field, click any method's ✖ to remove unnecessary ones, or click Deselect All.

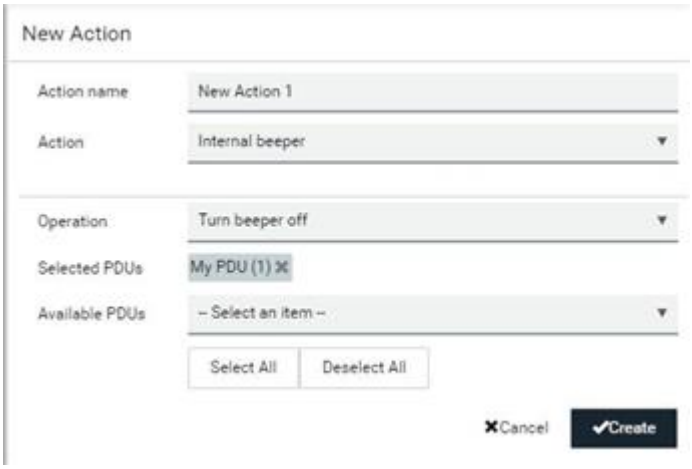
Action Group

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

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

► *Operation:*

1. Choose Device Settings > Event Rules > ✚ New Action .
2. Select 'Execute an action group' from the Action list.
3. Select the actions to include in group from the 'Available actions' list, or click Select All.
4. To remove any action(s) from the 'Selected actions' field, click it's X.
5. Click Create to save the action.



Change Load Shedding State

The "Change load shedding state" action is available only when your PX4 is able to control outlet power. Use this action to activate or deactivate the load shedding mode for responding to a specific event.

► *Operation:*

1. Choose Device Settings > Event Rules >

.
2. Select 'Change load shedding state' from the Action list.
3. In the Operation field, select either one below:
   - Start load shedding: Enters the load shedding mode when the specified event occurs.
   - Stop load shedding: Quits the load shedding mode when the specified event occurs.

External Beeper

If an external beeper is connected, you can change the beeper's behavior or status to respond to a certain event.

► *To control the connected external beeper:*

1. Choose Device Settings > Event Rules >

.
2. Select 'External beeper' from the Action list.
3. In the 'Beeper port' field, select the port where the external beeper is connected.
4. In the 'Beeper action' field, select an action for the external beeper to carry out.
   - Alarm: Causes the external beeper to sound an alarm cycle every 20 seconds - stays on for 0.7 seconds and then off for 19.3 seconds.
   - On: Turns on the external beeper so that it buzzes continuously.
   - Off: Turns off the external beeper so that it stops buzzing.

Warning: If you create an event rule for the external beeper but disconnect it when an event causes it to beep, the beeper no longer beeps after it is re-connected even though the event triggering the beeping action remains asserted.

Internal Beeper

You can have the built-in beeper of the PX4 turned on or off when a certain event occurs.

► *Operation:*

1. Choose Device Settings > Event Rules >

.
2. Select 'Internal beeper' from the Action list.
3. Select an option from the Operation field.
   - Turn beeper on: Turns on the internal beeper to make it buzz.
   - Turn beeper off: Turns off the internal beeper to make it stop buzzing.

Log an Event Message

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

A default log message will be generated for each type of event, or you can create a custom log message.

► *Operation:*

1. Choose Device Settings > Event Rules > New Action.
2. Select 'Log an event message' from the Action list.
3. Select the 'Use custom log message' checkbox, and then create a custom message in the provided text box.
   - To automatically insert message placeholders, open the Custom Log Message Help section. Search for placeholders and click to include them in your message.
4. Click Create.

Shut down a Server and Control its Power

The "Power control server" action is available only when your PX4 is outlet-switching capable.

You can configure the PX4 to shut down a specific server and then turn off its outlet(s), or turn on that server's outlet(s) after a certain event occurs.

The server must be one of the servers being monitored by your PX4 and the same PX4 supplies power to it. See Monitoring Server Accessibility (on page 351) .

Tip: If the server has multiple power cords, make sure all of its power cords are connected to the same PX4 and you have created an outlet group for controlling all outlets simultaneously.

► *Operation:*

1. Choose Device Settings > Event Rules >

.
2. Select 'Power control server' from the Action list.
3. In the Operation field, select an action for the server.
   - Power up: Turns on the outlet or outlet group associated with the selected server.
   - Graceful shutdown: Shuts down the selected server first and then turn off its associated outlet or outlet group.
4. Select the server you want in the Server field.
   - If PX4 cannot power control any server, a message 'Power control not configured' is shown in the end of the server's host name or IP address.

Push Out Sensor Readings

You can configure the PX4 to push sensor log to a remote server after a certain event occurs, including logs of internal sensors, environmental sensors and actuators.

If you have connected asset strips, you can also configure the PX4 to push the data to a server.

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

Tip: To send the data at a regular interval, schedule this action. Note that the "Asset management log" is generated only when there are changes made to any asset strips or asset tags, such as connection or disconnection events.

► *Operation:*

1. Choose Device Settings > Event Rules >

.
2. Select 'Push out sensor readings' from the Action list.
3. Select a server or host which receives the data in the Destination field.
   - If the desired destination is not available yet, go to the Data Push page to specify it.

Record Snapshots to Webcam Storage

This option allows you to define an action that starts or stops a specific webcam from taking snapshots.

Per default the snapshots are stored on the PX4. It is recommended to specify a remote server to store as many snapshots as possible.

► *Operation:*

1. Choose Device Settings > Event Rules >

.
2. Select 'Record snapshots to webcam storage' from the Action list.
3. Select a webcam in the Webcam field.
4. Select the action to perform - 'Start recording' or 'Stop recording.'

If 'Start recording' is selected, adjust the values of the following:

- Number of snapshots - the number of snapshots to be taken when the event occurs.

  The maximum amount of snapshots that can be stored on the PX4 is 10. If you set it for a number greater than 10 and the storage location is on the PX4, after the 10th snapshot is taken and stored, the oldest snapshots are overwritten. Storing snapshots on a remote server does not have such a limitation.
- Time before first snapshot - the amount of time in seconds between when the event is triggered and the webcam begins taking snapshots.
- Time between snapshots - the amount of time in seconds between when each snapshot is taken.
- Folder - names of the folders that will be automatically created to store webcam snapshots after the recording action is triggered by the rule you will configure.

  Note that the Folder field is available only when the selected webcam has been configured to store its snapshots on an "FTP" server.

Folder name options	**Definition**
Serial number / Webcam name	Two folders will be created. • The parent folder's name is the serial number of PX4. • The subfolder's name is the selected webcam's name.
Serial number / Webcam name / Rule name	Three folders will be created. • Definitions of the parent folder and first subfolder are the same as the first row. • The final subfolder's name is the name of event rule that triggers this recording action.

Folder name options	Definition
Serial number / Webcam name / Timestamp	Three folders will be created. • Definitions of the parent folder and first subfolder are the same as the first row. • The final subfolder's name is the time when the recording event occurs, which is the accumulated time in seconds since 1970/1/1.
Serial number / Webcam name / Rule name / Timestamp	Four folders will be created. • Definitions of the parent folder and first subfolder are the same as the first row. • The second subfolder's name is the name of event rule that triggers this recording action. • The final subfolder's name is the time when the recording event occurs, which is the accumulated time in seconds since 1970/1/1.
Serial number / Webcam name / Formatted timestamp	Three folders will be created. • Definitions of the parent folder and first subfolder are the same as the first row. • The final subfolder's name is the time when the recording event occurs, which is a format comprising year, month, date, hour, minute, second and timezone.
Serial number / Webcam name / Rule name / Formatted timestamp	Four folders will be created. • Definitions of the parent folder and first subfolder are the same as the first row. • The second subfolder's name is the name of event rule that triggers this recording action. • The final subfolder's name is the time when the recording event occurs, which is a format comprising year, month, date, hour, minute, second and timezone.

The timestamp is based on the time you have configured on the PX4.

To find the serial number of your PX4, go to Maintenance > *Device Information*.

Send Email

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

Messages consist of a combination of free text and placeholders. The placeholders represent information which is pulled from the PX4 and inserted into the message.

For example:

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

translates to

```
Mary logged into the device on 2022-January-30 21:00
```

► *Operation:*

1. Choose Device Settings > Event Rules >

.
2. Select 'Send email' from the Action list.
3. In the 'Recipient email addresses' field, specify the email address(es) of the recipient(s). Use a comma to separate multiple email addresses.

4. By default, the SMTP server specified on the SMTP Server page will be the SMTP server for performing this action.

To use a different SMTP server, select the 'Use custom settings' radio button.

Default messages are sent based on the event.

5. If needed, you can customize the subject and messages sent via this email.
   - Select the 'Custom subject' checkbox, and enter the text you prefer as this email's subject.
   - Select the 'Use custom log message' checkbox, and then create a custom message up to 1024 characters in the provided field.
   - To automatically insert message placeholders, open the Custom Log Message Help section. Search for placeholders and click to include them in your message.
6. Click Create.

Send Sensor Report

You may set the PX4 so that it automatically reports the latest readings or states of one or multiple sensors by sending a message or email or simply recording the report in a log. These sensors can be either internal or environmental sensors listed below.

- Inlet sensors, including RMS current, RMS voltage, active power, apparent power, power factor and active energy.
- Outlet sensors, including RMS current, RMS voltage, active power, apparent power, power factor, active energy and outlet state (for outlet-switching capable PDUs only).
- Overcurrent protector sensors, including RMS current and tripping state.
- Peripheral device sensors, which can be any environmental sensor packages connected to the PX4, such as temperature or humidity sensors.

SeeSend Sensor Report Example (on page 330).

► *Operation:*

1. Choose Device Settings > Event Rules >

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

The messaging action types include:

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

4. If no messaging actions are available, create them now.
5. In the 'Available sensors' field, select the desired target's sensor.

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

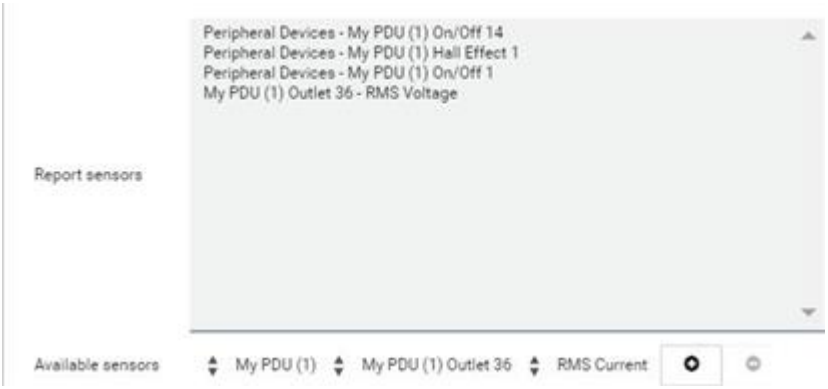
b. Click the second to select the specific sensor for the target from the list.

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

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

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

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



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

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

Send SMS Message

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

A supported modem, such as the Cinterion® GSM MC52i modem, must be plugged into the PX4 in order to send SMS messages.

Raritan
A brand of legrand

Note: The PX4 cannot receive SMS messages.

Only the 7-bit ASCII charset is supported for SMS messages. Messages consist of a combination of free text and placeholders. The placeholders represent information retrieved from the device and inserted into the message. For example:

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

translates to

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

► *Operation:*

1. Choose Device Settings > Event Rules >

.
2. Select 'Send SMS message' from the Action list.
3. In the 'Recipient phone number' field, specify the phone number of the recipient.
4. Select the 'Use custom log message' checkbox, and then create a custom message in the provided text box.
   - To automatically insert message placeholders, open the Custom Log Message Help section. Search for placeholders and click to include them in your message.
5. Click Create.

Send Snapshots via Email

This option notifies one or multiple persons for the selected events by emailing snapshots or videos captured by a connected Logitech® webcam.

► *Operation:*

1. Choose Device Settings > Event Rules >

.
2. Select 'Send snapshots via email' from the Action list.
3. In the 'Recipient email addresses' field, specify the email address(es) of the recipient(s). Use a comma to separate multiple email addresses.
4. By default, the SMTP server specified on the SMTP Server page will be the SMTP server for performing this action.

To use a different SMTP server, select the 'Use custom SMTP server' checkbox. The fields for customized SMTP settings appear.

5. Select the webcam that is capturing the images you want sent in the email.
6. Adjust the values of the following:

- Number of snapshots - the number of snapshots to be taken when the event occurs. For example, you can specify 10 images be taken once the event triggers the action.
- Snapshots per mail - the number of snapshots to be sent at one time in the email.
- Time before first snapshot - the amount of time in seconds between when the event is triggered and the webcam begins taking snapshots.
- Time between snapshots - the amount of time in seconds between when each snapshot is taken.

7. If needed, you can customize the subject and messages sent via this email.
   - Select the 'Custom subject' checkbox, and enter the text you prefer as this email's subject.
   - Select the 'Use custom log message' checkbox, and then create a custom message up to 1024 characters in the provided field.
   - To automatically insert message placeholders, open the Custom Log Message Help section. Search for placeholders and click to include them in your message.
8. Click Create.

Send an SNMP Notification

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

► *Operation:*

1. Choose Device Settings > Event Rules >

.
2. Select 'Send SNMP notification' from the Action list.
3. Select the type of SNMP notification. See either procedure below according to your selection.

► *To send SNMP v2c notifications:*

1. In the 'Notification type' field, select 'SNMPv2c trap' or 'SNMPv2c inform.'
2. For SNMP INFORM communications, leave the resend settings at their default or do the following:
   a. In the Timeout field, specify the interval of time, in seconds, after which a new inform communication is resent if the first is not received. For example, resend a new inform communication once every 3 seconds.
   b. In the 'Number of retries' field, specify the number of times you want to re-send the inform communication if it fails. For example, inform communications are re-sent up to 5 times when the initial communication fails.
3. In the Host fields, enter the IP address of the device(s) you want to access. This is the address to which notifications are sent by the SNMP system agent.
4. In the Port fields, enter the port number used to access the device(s).
5. In the Community fields, enter the SNMP community string to access the device(s). The community is the group representing the PX4 and all SNMP management stations.

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

► *To send SNMP v3 notifications:*

1. In the 'Notification type' field, select 'SNMPv3 trap' or 'SNMPv3 inform.'
2. For SNMP TRAPs, the engine ID is prepopulated.
3. For SNMP INFORM communications, leave the resend settings at their default or do the following:
   a. In the Timeout field, specify the interval of time, in seconds, after which a new inform communication is resent if the first is not received. For example, resend a new inform communication once every 3 seconds.
   b. In the 'Number of retries' field, specify the number of times you want to re-send the inform communication if it fails. For example, inform communications are re-sent up to 5 times when the initial communication fails.
4. For both SNMP TRAPS and INFORMS, enter the following as needed and then click OK to apply the settings:
   a. Host name
   b. Port number
   c. User ID for accessing the host -- make sure the User ID has the SNMPv3 permission.
   d. Select the host security level

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

Start or Stop a Lua Script

If you have created or loaded a Lua script file into the PX4, you can have that script automatically run or stop in response to a specific event.

See Lua Scripts (on page 359).

► *To automatically start or stop a Lua script:*

1. Choose Device Settings > Event Rules > ➕ New Action .
2. Select 'Start/stop Lua script' from the Action list.
3. In the Operation field, select 'Start script' or 'Stop script.'
4. In the Script field, select the script that you want it to be started or stopped when an event occurs. Scripts must be pre-loaded.
5. To apply different arguments than the default, do the following. Note that the newly-added arguments will override this script's default arguments.
   a. Click Add Argument.
   b. Type the key and value.
      - To remove any existing argument, click ➖ adjacent to it.

Switch Outlet Group

The "Switch outlet group" action is available only when your PX4 is outlet-switching capable. This action turns on, off or power cycles a specific outlet group.

► *Operation:*

1. Choose Device Settings > Event Rules > ➕ New Action .
2. Select 'Switch outlet group' from the Action list.
3. To specify the outlet group where this action will be applied, select it from the 'Group to switch' list.
4. In the Operation field, select an operation for the selected outlet group.
   - Turn on all outlets in group: Turns on the selected outlet group.
   - Turn off all outlets in group: Turns off the selected outlet group.
   - Cycle all outlets in group: Cycles power to the selected outlet group.

Switch Outlets

The "Switch outlets" action is available only when your PX4 is outlet-switching capable. This action turns on, off or power cycles a specific outlet.

► *Operation:*

1. Choose Device Settings > Event Rules > ➕ New Action .
2. Select 'Switch outlets' from the Action list.
3. In the Operation field, select an operation for the selected outlet(s).
   - Turn outlet on: Turns on the selected outlet(s).
   - Turn outlet off: Turns off the selected outlet(s).
   - Cycle outlet: Cycles power to the selected outlet(s).

4. To specify the outlet(s) where this action will be applied, select them one by one from the 'Available outlets' list.
   - To add all outlets, click Select All.
5. To remove any outlets from the 'Selected outlets' field, click that outlet's ✖.
6. If 'Turn outlet on' or 'Cycle outlet' is selected, choose to select the 'Use sequence order and delays' checkbox so that all selected outlets will follow the power-on sequence defined on the Outlets page.

Switch Peripheral Actuator

If you have any actuator connected to the PX4, you can set up the PX4 so it automatically turns on or off the system controlled by the actuator when a specific event occurs.

► *Operation:*

1. Choose Device Settings > Event Rules > ✚ New Action.
2. Select 'Switch peripheral actuator' from the Action list.
3. In the Operation field, select an operation for the selected actuator(s).
   - Turn on: Turns on the selected actuator(s).
   - Turn off: Turns off the selected actuator(s).
4. To select the actuator(s) where this action will be applied, select them one by one from the 'Available actuators' list.
   - To add all actuators, click Select All.
5. To remove any selected actuator from the 'Selected actuators' field, click that actuator's ✖.

Syslog Message

Use this action to automatically forward event messages to the specified syslog server. Determine the syslog transmission mechanism you prefer when setting it up - UDP, TCP or TLS over TCP.

PX4 may or may not detect the syslog message transmission failure. If yes, it will log this syslog failure as well as the failure reason in the event log.

► *Operation:*

1. Choose Device Settings > Event Rules > New Action.
2. Select 'Syslog message' from the Action list.
3. In the 'Syslog server' field, specify the IP address to which the syslog is forwarded.
4. In the 'Transport protocol' field, select one of the syslog protocols: TCP, UDP or TCP+TLS. The default is UDP.

Transport protocols	**Next steps**
UDP	• In the 'UDP port' field, type an appropriate port number. Default is 514. • Select the 'Legacy BSD syslog protocol' checkbox if applicable.
TCP	NO TLS certificate is required. Type an appropriate port number in the 'TCP port' field.

Transport protocols	Next steps
TCP+TLS	A TLS certificate is required. Do the following: a. Type an appropriate port number in the 'TCP port' field. Default is 6514. b. In the 'CA certificate' field, click Browse to select a TLS certificate. After importing the certificate, you may: • Click Show to view its contents. • Click Remove to delete it if it is inappropriate. c. Determine whether to select the 'Allow expired and not yet valid certificates' checkbox. • To always send the event message to the specified syslog server as long as a TLS certificate is available, select this checkbox. • To prevent the event message from being sent to the specified syslog server when any TLS certificate in the selected certificate chain is outdated or not valid yet, deselect this checkbox.

Scheduling an Action

An action can be regularly performed at a preset time interval instead of being triggered by a specific event. For example, you can make the PX4 report the reading or state of a specific sensor regularly by scheduling the "Send sensor report" action.

When scheduling an action, make sure you have a minimum of 1-minute buffer between this action's creation and first execution time. Otherwise, the scheduled action will NOT be performed at the specified time when the buffer time is too short. For example, if you want an action to be performed at 11:00 am, you should finish scheduling it at 10:59 am or earlier.

► *Operation:*

1. Choose Device Settings > Event Rules >

.
2. To select any action(s), select them one by one from the 'Available actions' list.
   - To select all available actions, click Select All.
3. To remove any action(s) from the 'Selected actions' field, click that action's .
   - To remove all actions, click Deselect All.
4. Select the desired frequency in the 'Execution time' field, and then specify the time interval or a specific date and time in the field(s) that appear. Use the clock and calendar tools to choose the schedule. Use the AM/PM button to toggle time settings.

Send Sensor Report Example

To create a scheduled action for emailing a temperature sensor report hourly, it requires:

- A 'Send email' action
- A 'Send sensor report' action
- A timer - that is, the scheduled action

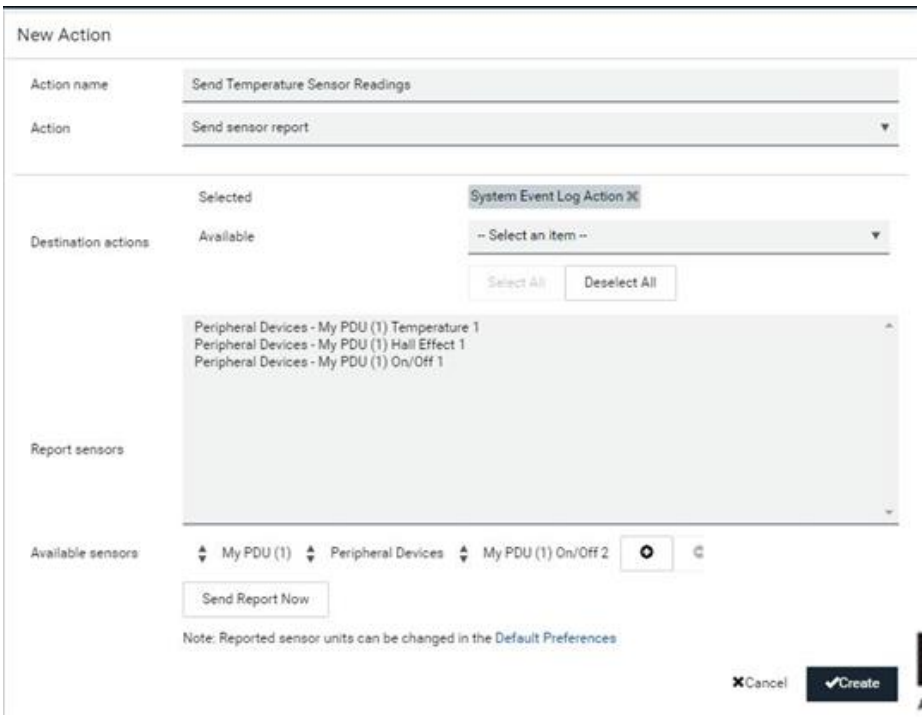
► *Steps:*

1. Click

to create a 'Send email' action that sends an email to the desired recipient(s).
   - In this example, this action is named *Email a Sensor Report*.
   - The subject and content of this email can be customized.

Click ➕ New Action to create a 'Send sensor report' action that includes the 'Email a Sensor Report' action as its destination action.

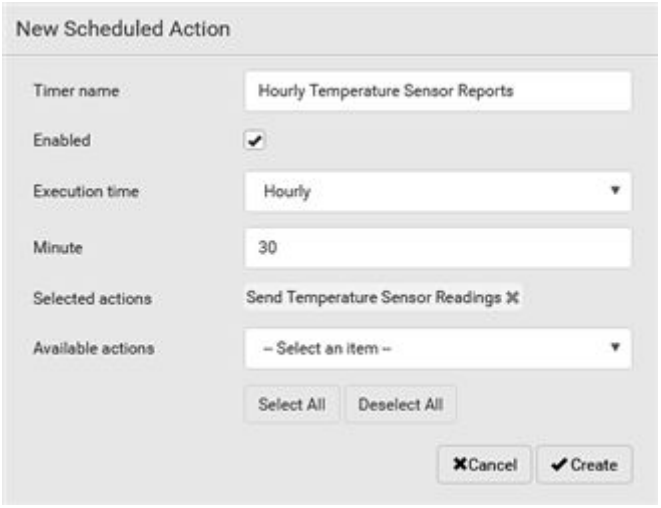
- In this example, this action is named *Send Temperature Sensor Readings*.
- You can specify more than one temperature sensor as needed in this action.



1. Click ➕ New Scheduled Action to create a timer for performing the 'Send Temperature

Sensor Readings' action hourly.

- In this example, the timer is named *Hourly Temperature Sensor Reports*.
- To perform the specified action at 12:30 pm, 01:30 pm, 02:30 pm, and so on, select Hourly, and set the Minute to 30.



- An email containing the specified temperature sensor readings will be sent hourly every day. If you no longer need the report, you can disable the timer by clearing the Enabled checkbox.

Placeholders for Custom Messages

Actions that include messages allow you to customize text and include placeholders that retrieve system information and include it in the message.

Supported actions:

- Send email
- Send snapshots via email
- Send SMS
- Log event message

The following are placeholders that can be used in custom messages. Because the placeholders employ square brackets, you must precede with a backslash any other square brackets that must be included in your message. For example, \[\].

If a placeholder is used in a situation where the information cannot be retrieved, it will be shown as "unknown" in the message.

Placeholder	**Definition**
[AMSBLADESLOTPOSITION]	The (horizontal) slot position inside a blade extension
[AMSLEDCOLOR]	The RGB LED color
[AMSLEDMODE]	The LED indication mode
[AMSLEDOPMODE]	The LED operating mode

Placeholder	Definition
[AMSNAME]	The name of an asset strip
[AMSNUMBER]	The numeric ID of an asset strip
[AMSRACKUNITPOSITION]	The (vertical) rack unit position
[AMSSTATE]	The human-readable state of an asset strip
[AMSTAGID]	The asset tag ID
[CARDREADERCHANNEL]	The channel number of a card reader
[CARDREADERDESCRIPTION]	The custom description of a card reader
[CARDREADERID]	The id of a card reader
[CARDREADERMANUFACTURER]	The manufacturer of a card reader
[CARDREADERNAME]	The custom name of a card reader
[CARDREADERPRODUCT]	The product name of a card reader
[CARDREADERSERIALNUMBER]	The serial number of a card reader
[COMPONENTID]	The ID of a hardware component
[CONFIGPARAM]	The name of a configuration parameter
[CONFIGVALUE]	The new value of a parameter
[DATETIME]	The human readable timestamp of the event occurrence
[DEVICEIP]	The IP address of the device the event occurred on
[DEVICENAME]	The name of the device the event occurred on
[DEVICESERIAL]	The unit serial number of the device the event occurred on
[DIPSWELLDURATION]	The formatted duration of the dip/swell event in seconds
[DIPSWELLVOLTAGE]	The formatted minimum/maximum voltage during the dip/swell event in volts
[DOORACCESSDENIALREASON]	The reason for the door access being denied
[DOORACCESSRULEID]	The id of a door access rule
[DOORACCESSRULENAME]	The name of a door access rule
[ERRORDESC]	The error message
[EVENTRULENAME]	The name of the matching event rule
[EXTPORTNAME]	The name of an external port
[EXTSENSOR]	The peripheral device identifier

Placeholder	Definition
[EXTSENSORNAME]	The name of a peripheral device
[EXTSENSORSLOT]	The ID of a peripheral device slot
[FAILURETYPE]	The numeric hardware failure type
[FAILURETYPESTR]	The textual hardware failure type
[FUSESTATENAME]	The human readable state of a fuse
[IFNAME]	The human readable name of a network interface
[INLET]	The inlet label
[INLETLINEPAIR]	The inlet line pair identifier
[INLETPOLE]	The inlet power line identifier
[INLETSENSOR]	The inlet sensor name
[ISASSERTED]	Boolean flag whether an event condition became true (1) or false (0)
[KEYPADCHANNEL]	The channel number of a keypad
[KEYPADDESCRIPTION]	The custom description of a keypad
[KEYPADID]	The id of a keypad
[KEYPADMANUFACTURER]	The manufacturer of a keypad
[KEYPADNAME]	The custom name of a keypad
[KEYPADPIN]	The PIN entered at a keypad
[KEYPADPRODUCT]	The product name of a keypad
[KEYPADSERIALNUMBER]	The serial number of a keypad
[LINKIDTAG]	Link ID prefix for link unit events, empty otherwise
[LINKID]	The link ID of a link unit
[LINKUNITHOST]	The host name or IP address of a link unit
[LOGMESSAGE]	The original log message
[MONITOREDHOST]	The name or IP address of a monitored host
[NETAUTHRESULTSTR]	The network authentication result string ('succeeded' or 'failed')
[NEWUMTARGETUSER]	The new target user of a user rename operation
[OCP]	The overcurrent protector label
[OCPSENSOR]	The overcurrent protector sensor name

Placeholder	Definition
[OCPTRIPCAUSELABEL]	The label of the outlet that likely caused the OCP trip
[OCPTRIPCURRENT]	The current flow before the trip event
[OLDDATETIME]	The device date and time before a clock change
[OLDVERSION]	The firmware version the device is being upgraded from
[OUTLET]	The outlet label
[OUTLETGROUPID]	The outlet group ID
[OUTLETGROUPNAME]	The outlet group name
[OUTLETGROUPSENSOR]	The outlet group sensor name
[OUTLETNAME]	The outlet name Note: If any outlet does not have a name, neither an outlet name nor an outlet number will be shown in the custom message for it. Therefore, it is recommended to check the availability of all outlet names if intending to use this placeholder.
[OUTLETPOLE]	The outlet power line identifier
[OUTLETSENSOR]	The outlet sensor name
[PDULINEPAIRSENSOR]	The sensor name for a certain line pair
[PDUNUMBER]	The PDU number in a cascade
[PDUPOLESENSOR]	The sensor name for a certain power line
[PDUSENSOR]	The PDU sensor name
[PERIPHDEVPOSITION]	The position of an attached peripheral device
[PHONENUMBER]	The destination phone number of an outgoing SMS message
[PORTID]	The label of the external port the event-triggering device is connected to
[PORTTYPE]	The type of the external port (e.g. 'feature' or 'auxiliary') the event-triggering device is connected to
[RADIUSERRORDESC]	The Radius error message
[ROMCODE]	The romcode of an attached peripheral device
[SENSORREADING]	The value of a sensor reading
[SENSORREADINGUNIT]	The unit of a sensor reading
[SENSORREPORT]	The formatted sensor report contents

Placeholder	Definition
[SENSORSTATENAME]	The human readable state of a sensor
[SENSORTHRESHOLDNAME]	The name of the threshold being crossed
[SENSORTHRESHOLDVALUE]	The value of the threshold being crossed
[SERVERPOWEROPERATION]	The power control operation that was initiated on a server (on/off)
[SERVERPOWERRESULT]	The result of a power control operation
[SMARTCARDID]	The id of a smart card
[SMARTCARDTYPE]	The type of a smart card
[SMTPRECIPIENTS]	The list of recipients of an outgoing mail
[SMTPSERVER]	The name or IP address of an SMTP server
[SYSCONTACT]	SNMP MIB-II sysContact field
[SYSLOCATION]	SNMP MIB-II sysLocation field
[SYSNAME]	SNMP MIB-II sysName field
[TIMEREVENTID]	The id of a timer event
[TIMESTAMP]	The timestamp of the event occurrence
[UMTARGETROLE]	The target role of a user management operation
[UMTARGETUSER]	The target user of a user management operation
[USERIP]	The IP address a user connected from
[USERNAME]	The user who performed an operation
[VERSION]	The firmware version the device is upgrading to

Editing or Deleting a Rule/Action

You can change the settings of an event rule, action or scheduled action, or delete them.

Exception: Some settings of the built-in event rules or actions are not user-configurable. You cannot delete built-in rules and actions.

► *To edit or delete an event rule, action or scheduled action:*

1. Choose Device Settings > Event Rules.
2. Click an item in the list of rules, actions or scheduled actions to open its page.
   - To modify settings, make changes and then click Save.
   - To delete it, click the Delete icon then confirm.

Sample Event Rules

Sample PDU-Level Event Rule

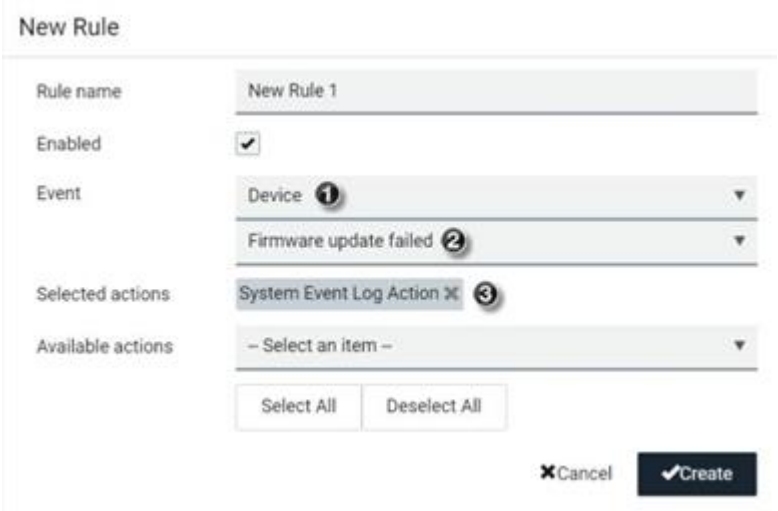
In this example, we want the PX4 to record the firmware upgrade failure in the internal log when it happens.

The event rule involves:

- Event: Device > Firmware update failed
- Action: System Event Log Action

► *To create this PDU-level event rule:*

1. For an event at the PDU level, select "Device" in the Event field.
2. Select "Firmware update failed" so that the PX4 responds to the event related to firmware upgrade failure.
3. To make PX4 record the firmware update failure event in the internal log, select "System Event Log Action" in the 'Available actions' field.



Sample Outlet-Level Event Rule

In this example, we want the PX4 to send SNMP notifications to the SNMP manager for any sensor change event of outlet 3.

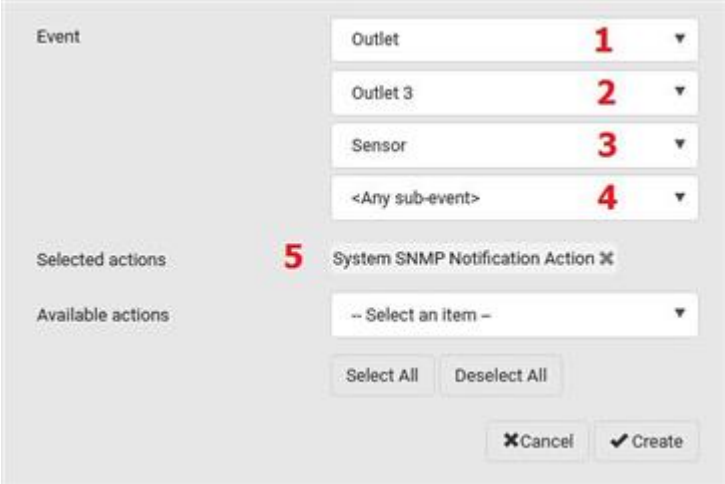
The event rule involves:

- Event: Outlet > Outlet 3 > Sensor > Any sub-event
- Action: System SNMP Notification Action

► *To create this outlet-level event rule:*

1. For an event at the outlet level, select "Outlet" in the Event field.
2. Select "Outlet 3" because that is the desired outlet.
3. Select "Sensor" to refer to sensor-related events.
4. Select "Any sub-event" to include all events related to all sensors of this outlet and all thresholds, such as current, voltage, upper critical threshold, upper warning threshold, lower critical threshold, lower warning threshold, and so on.
5. To make PX4 send SNMP notifications, select "System SNMP Notification Action" in the 'Available actions' field.

Note: The SNMP notifications may be SNMP v2c or SNMP v3 traps/informs, depending on the settings for the System SNMP Notification Action. See Enabling and Configuring SNMP.



Then the SNMP notifications are sent when:

- Any numeric sensor's reading enters the warning or critical range.
- Any sensor reading or state returns to normal.
- Any sensor becomes unavailable.
- The active energy sensor is reset.
- Any state sensor changes its state.

For example, when the outlet 3's voltage exceeds the upper warning threshold, the SNMP notifications are sent, and when the voltage drops below the upper warning threshold, the SNMP notifications are sent again.

Sample Inlet-Level Event Rule

In this example, we want the PX4 to send SNMP notifications to the SNMP manager for any sensor change event of the Inlet I1.

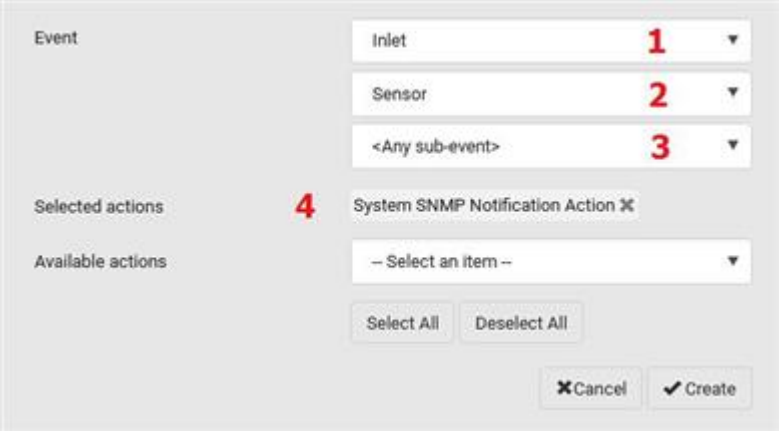
The event rule involves:

- Event: Inlet > Sensor > Any sub-event
- Action: System SNMP Notification Action

► *To create the above event rule:*

1. For an event at the inlet level, select "Inlet" in the Event field.
2. Select "Sensor" to refer to sensor-related events.
3. Select "Any sub-event" to include all events related to all sensors of this inlet and all thresholds, such as current, voltage, upper critical threshold, upper warning threshold, lower critical threshold, lower warning threshold, and so on.
4. To make the PX4 send SNMP notifications, select "System SNMP Notification Action" in the 'Available actions' box.

Note: The SNMP notifications may be SNMP v2c or SNMP v3 traps/informs, depending on the settings for the System SNMP Notification Action. See Enabling and Configuring SNMP.



Then the SNMP notifications are sent when:

- Any numeric sensor's reading enters the warning or critical range.
- Any sensor reading or state returns to normal.
- Any sensor becomes unavailable.
- The active energy sensor is reset.

For example, when the Inlet I1's voltage exceeds the upper warning threshold, the SNMP notifications are sent, and when the voltage drops below the upper warning threshold, the SNMP notifications are sent again.

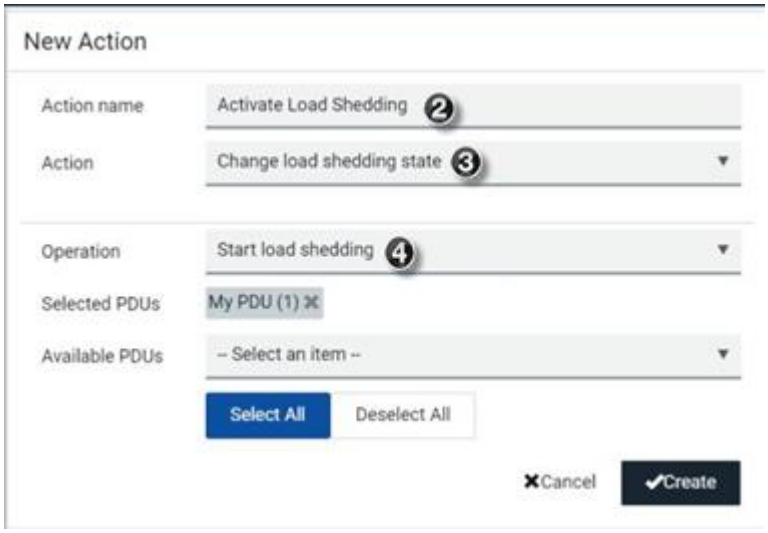
Sample Environmental-Sensor-Level Event Rule

This section applies to outlet-switching capable models only.

In this example, we want PX4 to activate the load shedding function when a contact closure sensor enters the alarmed state. This event rule requires creating a new action before creating the rule.

► *Step 1: create a new action for activating the load shedding*

1. Choose Device Settings > Event Rules > ➕ New Action .
2. In this illustration, assign the name "Activate Load Shedding" to the new action.
3. In the Action field, select "Change load shedding state."
4. In the Operation field, select "Start load shedding."



5. Click Create.

After the new action is created, follow the procedure below to create an event rule that triggers the load shedding mode when the contact closure sensor enters the alarmed state. This event rule involves the following:

- Event: Peripheral Device Slot > Slot 1 > State Sensor/Actuator > Alarmed/Open/On
- Trigger condition: Alarmed
- Action: Activate Load Shedding

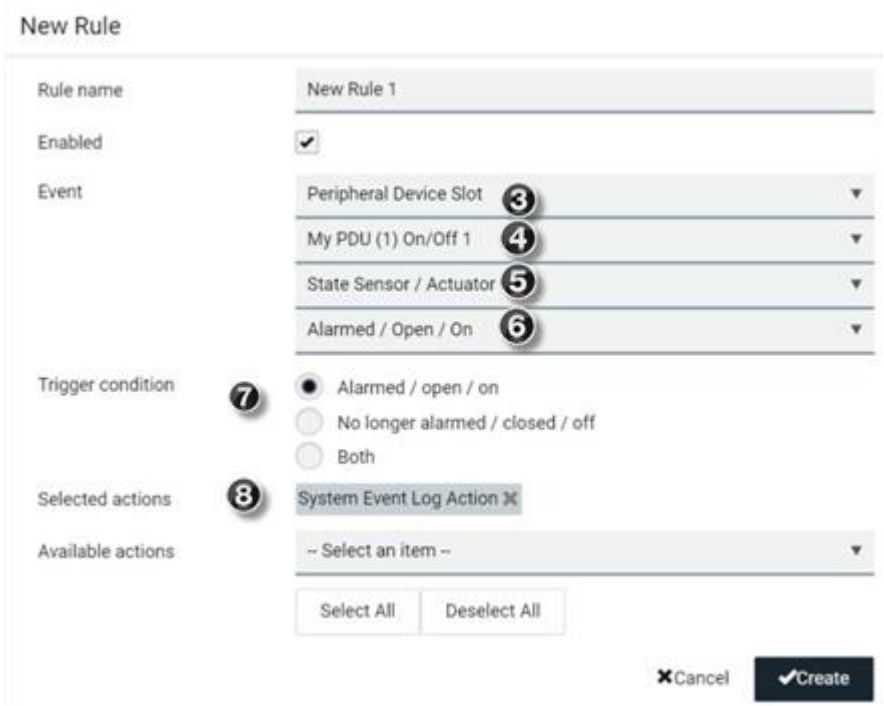
► *Step 2: create the contact closure-triggered load shedding event rule*

1. Click ➕ New Rule on the Event Rules page.
2. In this illustration, assign the name "Contact Closure Triggered Load Shedding" to the new rule.
3. In the Event field, select "Peripheral Device Slot" to indicate we are specifying an event related to the environmental sensor package.
4. Select the ID number of the desired contact closure sensor. In this illustration, the ID number of the desired contact closure sensor is 1, so select Slot 1.

Note: ID numbers of all sensors/actuators are available on the Peripherals page.

---

5. Select "State Sensor/Actuator" because the contact closure sensor is a state sensor.
6. Select "Alarmed" since we want the PX4 to respond when the selected contact closure sensor changes its state related to the "alarmed" state.
7. In the 'Trigger condition' field, select the Alarmed/Open/On radio button so that the action is taken only when the contact closure sensor enters the alarmed state.
8. Select "System Event log Action" from the 'Available actions' list.



A Note about Infinite Loop

You should avoid building an infinite loop when creating event rules.

The infinite loop refers to a condition where the PX4 keeps busy because the action or one of the actions taken for a certain event triggers an identical or similar event which will result in an action triggering one more event.

► *Example 1*

This example illustrates an event rule which continuously causes the PX4 to send out email messages.

Event selected	Action included
Device > Sending SMTP message failed	Send email

► *Example 2*

This example illustrates an event rule which continuously causes the PX4 to send out SMTP messages when one of the selected events listed on the Device menu occurs. Note that <Any sub-event> under the Device menu includes the event "Sending SMTP message failed."

Event selected	Action included
Device > Any sub-event	Send email

► *Example 3*

This example illustrates a situation where two event rules combined regarding the outlet state changes causes the PX4 to continuously power cycle outlets 1 and 2 in turn.

Event selected	Action included
Outlet > Outlet 1 > Sensor > Outlet State > On/Off > Both (trigger condition)	Cycle Outlet 2 (Switch outlets --> Cycle Outlet --> Outlet 2)
Outlet > Outlet 2 > Sensor > Outlet State > On/Off > Both (trigger condition)	Cycle Outlet 1 (Switch outlets --> Cycle Outlet --> Outlet 1)

A Note about Untriggered Rules

In some cases, a measurement exceeds a threshold causing an alert. The measurement then returns to a value within the threshold, but the PX4 does not generate an alert message for the Deassertion event. Such scenarios can occur due to the hysteresis tracking the PX4 uses. See "To De-assert" and Deassertion Hysteresis.

Setting Data Logging

The data log stores records of each internal sensor's readings. You can configure the log capacity and the frequency that measurements are taken and stored. The total size of the data log is limited due to memory constraints. For example, for a PDU with 500 sensors, the effective log size cannot be more than 200 records. A log capacity warning appears if the desired log capacity is higher than the effective log capacity.

You can configure how often measurements are written into the data log using the Measurements Per Log Entry field. Since the internal sensors are measured every second, specifying a value of 60, for example, would cause measurements to be written to the data log once every minute. Whenever measurements are written to the log, three values for each sensor are written: the average, minimum

and maximum values. For example, if measurements are written every minute, the average of all measurements that occurred during the preceding 60 seconds along with the minimum and maximum measurement values are written to the log.

The device's SNMP agent must be enabled. In addition, using an NTP time server ensures accurately time-stamped measurements.

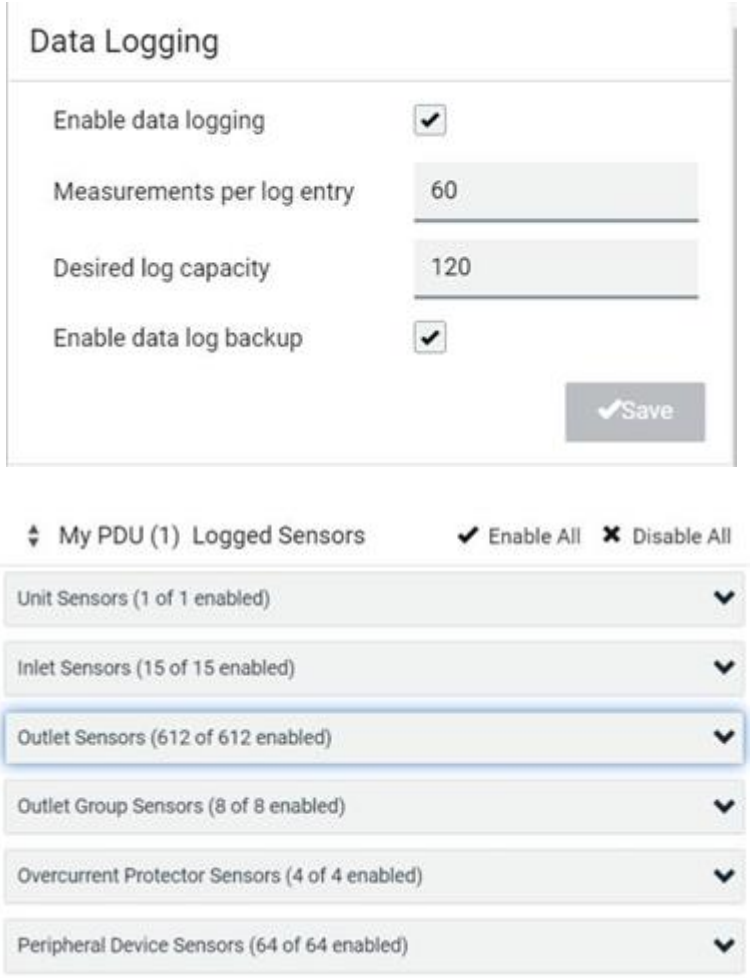
By default, data logging is enabled. You must have the "Administrator Privileges" or "Change Pdu, Inlet, Outlet & Overcurrent Protector Configuration" permissions to change the setting.

Important: The third-party management solutions like PowerIQ rely on the data logging feature, and the settings should be changed only in accordance with those systems' requirements.

► *To configure the data logging feature:*

1. Choose Device Settings > Data Logging.
2. To enable the data logging feature, select the "Enable" checkbox in the General Settings section.
3. Measurements Per Log Entry: Valid range is from 1 to 600. The default is 60.
4. Log capacity: Valid range varies, from 60 to 20,000.

5. Enable data log backup: Select this checkbox to enable an automatic USB backup of your data log. USB stick with specially configured file required, see procedure below.
6. Verify that all sensor logging is enabled. If not, click Enable All at the bottom of the page to have all sensors selected.
7. Click Save.



► *Enable Data Log Backup:*

This feature allows backup of the data log on a USB drive. When the PX4 reboots, e.g because of a power outage, it will repopulate the data log from the backup on the USB Stick.

To Prepare USB:

Before connecting a USB drive to the PX4, configure a file with these details:

1. Create a text file containing:

- user=<admin_username>
- password=<admin_user_password>
- destroy_and_format_for_storage=true

2. Save the file as "fwupdate.cfg" on the USB drive.
3. Make sure the Enable Data log backup checkbox is selected in Device Settings > Data Logging.
4. Connect the USB drive to the device.

On the console of the PX4, you will see the USB drive is reformatted and existing contents are removed. Once formatting is done, data is started to be backed up on the USB.

Note: Backed up data on the USB is in encrypted form.

Configuring Data Push Settings

You can push the sensor or asset strip data to a remote server for data synchronization. The destination and authentication for data push have to be configured properly on the PX4.

HTTP/HTTPS Destinations: The data will be sent in JSON format using HTTP POST when you select HTTP or HTTPS as the destination URL. Each push message contains exactly one JSON object. The data format is formally defined in IDL files, sharing several definitions from the JSON-RPC data model. IDL files are available by launching *JSON-RPC online help,* which is available on the Support site for your product.

MQTT Destinations: If MQTT is selected as the protocol, only data of the latest log row will be sent. The records of this log row are published under multiple topic names, one for each logged sensor.

After configuring the destination and authentication settings, do either or both of the following:

- To perform the data push after the occurrence of a certain event, create the data push action and assign it to an event rule.
- To push the data at a regular interval, schedule the data push action.

► *To configure data push settings:*

1. Choose Device Settings > Data Push.
2. To specify a destination, click New Destination.
3. Set up the URL field.
   a. Select *http , https, or MQTT*.
   b. Type the URL or host name in the accompanying text box.
4. If selecting https, a CA certificate is required for making the connection. Click Browse to install it. Then you can:
   - Click Show to view the certificate's content.
   - Click Remove to delete the installed certificate if it is inappropriate.
5. If the destination server requires authentication, select the 'Use authentication' checkbox, and enter the following data.
   - User name comprising up to 64 characters
   - Password comprising up to 128 characters
6. In the 'Entry type' field, determine the data that will be transmitted.

- *Asset management tag list:* Transmit the information of the specified asset strip(s), including the general status of the specified strip(s) and a list of asset tags. The asset tags list also includes the tags on blade extension strips, if any.
- *Asset management tag log:* Transmit the log of all asset strips, which is generated when there are changes made to asset tags and asset strips, including asset tag connection or disconnection events.
- *Sensor log:* Transmit the record of all logged sensors, including their sensor readings and/or status. Logged sensors refer to all internal and/or environmental sensors/actuators that you have selected on the Data Logging page.

7. If 'Asset management tag list' is selected in the above step, specify the asset strip(s) whose information to send. Depending on your PDU model, only one strip may be available.
   - To specify the asset strip(s), select them one by one from the Available AMS Ports list. Or click Select All to add all.
   - To remove the asset strip(s), click that asset strip's in the Selected AMS Ports field. Or click Deselect All to remove all.
8. Click Create.
9. Repeat the same steps for additional destinations. Up to 64 destinations are supported.

► *To immediately push out the data:*

1. On the Data Push page, choose the data source you want to push out.
2. Click the Push Now button.

► *To cancel a data push:*

- You can cancel the push in progress: Click Cancel.

► *To modify or delete data push settings:*

1. On the Data Push page, click the one you want in the list.
2. Perform either action below.
   - To modify settings, make necessary changes and then click Save.
   - To delete it, click Delete, and then confirm it on the confirmation message.

Data Push Format Examples

Sensor Log

The root object of the message is a `SensorLogPushMessage` structure. It comprises a list of sensor descriptors and a list of log rows.

► *Sensor descriptors:*

The sensor descriptor vector contains static information of all logged sensors, including:

- The electrical component a sensor is associated with. For example, an inlet pole or an overcurrent protector.
- The sensor's type. For example, RMS current or active energy.
- Unit and range of the sensor's readings.

► *Log rows:*

Each log row consists of a time stamp (accumulated seconds since 1/1/1970) and a list of log records -- one for each logged sensor.

The length and order of the record list is the same as the sensor descriptor vector.

Sensor Descriptors for Inlet Active Power

The following illustrates a descriptor for an inlet active power sensor.

The `metadata` field is relevant only to numeric sensors so the `readingtype` field is displayed twice in the illustration.

The comment beginning with // in each line, is added to the following illustration to help explain it.

```
{
    "device": {
        "type": 0,              // Inlet sensor (see DeviceType enumeration)
        "label": "I1",          // Inlet label: I1
        "line": 0               // Power line; not applicable for inlet sensors
    },
    "id": "activePower",        // Sensor identification
    "readingtype": 0,           // Reading type: numeric
    "metadata": {
        "type": {
            "readingtype": 0,   // Reading type: numeric
            "type": 5,          // Sensor type: Active power
            "unit": 3           // Reading unit: Watt
        },
        "decdigits": 0,         // No decimal digits
        "accuracy": 1.0,        // Accuracy: 1 percent
        "resolution": 1.0,      // Reading resolution: 1 W
        "tolerance": 1.5,       // Reading tolerance: +/- 1.5 W
        "range": {
            "lower": 0.0,       // Minimum reading: 0 W
            "upper": 30000.0    // Maximum reading: 30 kW
        }
    }
}
```

Log Rows

The following illustrates log rows with only one sensor record shown.

The actual length and order of log rows will be the same as those of sensors descriptors.

The comment beginning with // in each line, is added to the following illustration to help explain it.

```
{
    "timestamp": 1334052852,            // Time stamp (seconds since 1/1/1970)
    "records": [
        {
            "available": true,          // This record is available
            "takenValidSamples": 60,    // Number of valid samples in this log period
            "state": 5,                 // Sensor was in normal range
            "minValue": 5800.0,         // Minimum sensor value: 5.8 kW
            "avgValue": 5900.0,         // Average sensor value: 5.9 kW
            "maxValue": 6100.0          // Maximum sensor value: 6.1 kW
        },
        {
            // [...] record for next sensor
        }
    ]
}
```

Asset Management Tag List

The root object of the asset management tag list message is an `AssetStripsMessage` structure. It contains current data about all connected asset management strips and tags, which is similar to the illustration below.


```
{
    "assetStrips": [
        {
            "stripInfo": {
                "bladeOverflow": false,
                "bladeTagCount": 0,
                "cascadeState": 0,
                "componentCount": 1,
                "mainTagCount": 2,
                "maxBladeTagCount": 128,
                "maxMainTagCount": 64,
                "rackUnitCount": 48
            },
            "deviceInfo": {
                "appVersion": 24,
                "bootVersion": 6,
                "deviceId": 48,
                "hardwareId": 2,
                "isCascadable": false,
                "orientationSensAvailable": true,
                "protocolVersion": 257,
                "rackUnitCountConfigurable": true
            },
            "settings: {
                "rackUnitCount": 48,
                "name": "Asset Strip 1",
                "scanMode": 0,
                "defaultColorConnected": { "r": 0, "g": 255, "b": 0 },
                "defaultColorDisconnected": { "r": 255, "g": 0, "b": 0 },
                "numberingMode": 1,
                "numberingOffset": 1,
                "orientation": 0
            },
```


(Continued)


```
            "tags": [
                {
                    "rackUnitNumber": 4,
                    "slotNumber": 0,
                    "familyDesc": "Unknown",
                    "rawId": "DEADBEEF0000",
                    "programmable": 0
                },
                {
                    "rackUnitNumber": 5,
                    "slotNumber": 0,
                    "familyDesc": "Unknown",
                    "rawId": "DEADBEEF0500",
                    "programmable": 0
                }
            ]
        }
    ]
}
```


Raritan
A brand of legrand

Asset Management Tag Log

The root object of the asset management log message is an `AssetLogPushMessage` structure. It contains a list of tag or strip events since the last successful push.

The comment beginning with // in each line, is added to the following illustration to help explain it.

```
{
    "records": [
        {
            "timestamp": 1334052852,    // Time stamp (seconds since 1/1/1970)
            "type": 1,                  // 0: empty, 1: tag connected, 2: tag disconnected,
                                        // 3: asset strip state changed
            "assetStripNumber": 0,      // Asset strip number
            "rackUnitNumber" : 10,      // Rack unit number
            "rackUnitPosition" : 12,    // Rack unit position
            "slotNumber",               // Blade extension slot number
            "tagId",                    // The ID of the asset management tag
            "state": 5,                 // Sensor was in normal range
            "parentBladeId",            // ID of the parent blade extension tag
            "state": 0                  // 0: disconnected, 1: firmware update,
                                        // 2: unsupported, 3: available
        },
        {
            // [...] next record
        }
    ]
}
```

Monitoring Server Accessibility

You can monitor whether specific IT devices are alive by having the PX4 continuously ping them. An IT device's successful response to the ping commands indicates that the IT device is still alive and can be remotely accessed.

This function is especially useful when you are not located in an area with Internet connectivity.

PX4 can monitor any IT device, such as database servers, remote authentication servers, power distribution units (PDUs), and so on. It supports monitoring a maximum of 64 IT devices.

To perform this feature, you need the Administrator Privileges.

The default ping settings may not be suitable for monitoring devices that require high connection reliability so it is strongly recommended that you should adjust the ping settings for optimal results.

In addition, if your PX4 is outlet switching capable, you can even connect a monitored IT device to one or multiple outlets of PX4 and then have PX4 perform the following two actions as needed, in addition to monitoring its status:

- First shut down the monitored IT device.
- After the IT device is shut down, power off the outlet(s) where that device is connected.

Important: Not every IT device can be shut down by PX4 so it is suggested to verify whether the device can be shut down using a shutdown command. For example, PX4 cannot shut down a PDU with a shutdown command.

► *To add IT equipment for ping monitoring:*

1. Choose Device Settings > Server Reachability.
2. Click

.
3. By default, the "Enable ping monitoring for this server" checkbox is selected. If not, select it to enable this feature.
4. Configure the following.

Field	Description
IP address/hostname	IP address or host name of the IT equipment which you want to monitor.
Number of successful pings to enable feature	The number of successful pings required to declare that the monitored equipment is "Reachable." Valid range is 0 to 200.
Wait time after successful ping	The wait time before sending the next ping if the previous ping was successfully responded. Valid range is 5 to 600 (seconds).
Wait time after unsuccessful ping	The wait time before sending the next ping if the previous ping was not responded. Valid range is 3 to 600 (seconds).
Number of consecutive unsuccessful pings for failure	The number of consecutive pings without any response before the monitored equipment is declared "Unreachable." Valid range is 1 to 100.
Wait time before resuming pinging after failure	The wait time before the PX4 resumes pinging after the monitored equipment is declared "Unreachable." Valid range is 1 to 1200 (seconds).
Number of consecutive failures before disabling feature (0 = unlimited)	The number of times the monitored equipment is declared "Unreachable" consecutively before the PX4 disables the ping monitoring feature for it and shows "Waiting for reliable connection." Valid range is 0 to 100.

5. On a PDU with outlet switching capability, there is one more checkbox available -- *Power control enabled*.

To be able to shut down and power control the monitored IT device via the Server Reachability page, enable this checkbox and configure related settings, which are explained in the following table.

6. Click Create.
7. To add more IT devices, repeat the same steps.

► *To configure the shutdown and power control settings:*

Restriction: To make the power control feature work properly, the power cord(s) of the monitored IT device must be connected to the same PDU which is monitoring the IT device.

Raritan
A brand of legrand

Field	Description
Shutdown command	This is the command which is sent to the monitored IT device via SSH for shutting it down after you press the Shutdown button on PX4. • *GNU/Linux*: This option sends the GNU/Linux shutdown command. • *Windows*: This option sends the Windows shutdown command. • *Custom*: If the monitored device's system is neither GNU/Linux nor Windows, choose this option to specify a proper shutdown command, which can comprise a maximum of 1024 ASCII characters.
User name, Password	Specify user credentials for logging in to the monitored device via SSH. • *User name*: The name comprises up to 128 non-empty ASCII characters. • *Password*: The password comprises up to 128 ASCII characters.
SSH port	The monitored device's SSH port. • Default is 22.
Power target to switch	Select the outlet or outlet group that is powering the monitored device.
Method of checking successful shutdown	This field determines when PX4 will power off the outlet(s) that supplies power to the monitored device, after PX4 issues the shutdown command to that device. • *Timer*: • PX4 will power off the selected outlet or outlet group after the time specified in the 'Timer delay' field expires.*Active power drop*: PX4 will power off the selected outlet(s) after the active power value of the selected outlet or outlet group drops below the value specified in the 'Active power threshold' field. Note: Number of available methods is model dependent. The 'Active power drop' method is available only on models with outlet metering capability.
Timer delay	This field appears for the 'Timer' method. Valid values range between 5 and 10,000 seconds.

Field	Description
Active power threshold	The field appears for the 'Active power drop' method. Valid values range between 0 and 21,000 W.
Timeout for shutdown check	This field appears for the 'Active power drop' method. Valid values range between 5 and 10,000 seconds. The power-off operation is performed only when the active power value of the selected outlet or outlet group drops below the 'Active power threshold' within the period of time specified in this field. If the active power value drops below the 'Active power threshold' after the specified time expires, the power-off operation will NOT be performed.

Server Status Checking or Power Control

Not all models supports the shutdown and power control features via the Server Reachability page.

After adding IT equipment for monitoring, all IT devices are listed on the Server Reachability page.

In the beginning, the status of the added IT equipment shows "Waiting for reliable connection," which means the requested number of consecutive successful or unsuccessful pings has not reached before PX4 can declare that the monitored device is reachable or unreachable.

► *To check the server monitoring states and results:*

1. The column labeled "Ping Enabled" indicates whether the monitoring for the corresponding IT device is activated or not.
2. The column labeled "Status" indicates the accessibility of monitored equipment.

Status	Description
Reachable	The monitored equipment is accessible.
Unreachable	The monitored equipment is inaccessible.

Status	Description
Waiting for reliable connection	The connection between the device and the monitored equipment is not reliably established yet.

3. If your model supports outlet switching, one more column displays -- *Power Control*.

Power control status	Description
(disabled)	Power control is not enabled for the monitored equipment.
Server power is on	The outlet or outlet group associated with the monitored equipment is being powered on. • In the scenario where an 'outlet group' is associated with the equipment, the message 'Server power is on' is shown as long as one of the outlets in the outlet group remains powered on.
Server power is off	The outlet or all outlets of the outlet group associated with the monitored equipment are being powered off.
Server is shutting down	The shutdown command was sent to the monitored equipment, but the shutdown operation has not completed or succeeded yet.
Power state unknown	Cannot determine the power state of the outlet(s) associated with the monitored device. For example, maybe the outlet group associated with the monitored device has been deleted.

► *To shut down a monitored device:*

1. Select the IT device that you want to shut down.
2. Click Shutdown.
3. Confirm the operation when prompted.
4. Observe the Power Control status of the monitored device to make sure the shutdown operation succeeds.

► *To power on a monitored device:*

1. Select the IT device that you want to turn on.
2. Click Power Up.
3. Confirm the operation when prompted.
4. Observe the Power Control status of the monitored device to make sure the power-on operation succeeds.

Editing or Deleting Ping Monitoring Settings

You can edit the ping monitoring settings of any IT device or simply delete it if no longer needed.

► *To modify or delete any monitored IT device:*

1. Choose Device Settings > Server Reachability.
2. Click the desired one in the list.
3. Perform the desired action.
   - To modify settings, make necessary changes and then click Save. To delete it, click on the top-right corner.

Example: Ping Monitoring and SNMP Notifications

In this illustration, it is assumed that a significant PDU (IP address: 192.168.84.95) shall be monitored by your PX4 to make sure that PDU is properly operating all the time, and the PX4 must send out SNMP notifications (trap or inform) if that PDU is declared unreachable due to power or network failure. The prerequisite for this example is that the power sources are different between your PX4 and the monitored PDU.

This requires the following two steps.

► *Step 1: Set up the ping monitoring for the target PDU*

1. Choose Device Settings > Server Reachability.
2. Click .
3. Ensure the "Enable ping monitoring for this server" checkbox is selected.
4. Enter the data shown below.
   - Enter the server's data.

Field	Data entered
IP address/hostname	192.168.84.95

   - To make the PX4 declare the accessibility of the monitored PDU every 15 seconds (3 pings * 5 seconds) when that PDU is accessible, enter the following data.

Field	Data entered
Number of successful pings to enable feature	3
Wait time after successful ping	5

   - To make the PX4 declare the inaccessibility of the monitored PDU when that PDU becomes inaccessible for around 12 seconds (4 seconds * 3 pings), enter the following data.

Field	Data entered
Wait time after unsuccessful ping	4
Number of consecutive unsuccessful pings for failure	3

   - To make the PX4 stop pinging the target PDU for 60 seconds (1 minute) after the PDU inaccessibility is declared, enter the following data. After 60 seconds, the PX4 will re-ping the target PDU,

Field	Data entered
Wait time before resuming pinging after failure	60

- The "Number of consecutive failures before disabling feature (0 = unlimited)" can be set to any value you want.

5. Click Create.

► *Step 2: Create an event rule to send SNMP notifications for the target PDU*

1. Choose Device Settings > Event Rules.
2. Click

.
3. Select the Enabled checkbox to enable this new rule.
4. Configure the following.

Field/setting	Data specified
Rule name	Send SNMP notifications for PDU (192.168.84.95) inaccessibility
Event	Choose Server Monitoring > 192.168.84.95 > Unreachable
Trigger condition	Select the Unreachable radio button

This will make the PX4 react only when the target PDU becomes inaccessible.

5. Select the System SNMP Notification Action.

Front Panel Settings

You can set up the default mode of the front panel display, and front panel functions for outlet switching, actuator control, beeper mute or RCM self-test.

Note that available front panel settings are model dependent.

- Outlet switching -- available on outlet-switching capable models only.
- Actuator control -- available on all models.
- Internal beeper's mute function -- available on all models
- Default front panel mode setup -- available on all models, except for the PX3-3000 series, which does NOT provide inlet sensor information.
- RCM self-test -- available on those models which support residual current monitoring.

► *To configure the front panel settings:*

1. Choose Device Settings > Front Panel.
2. Configure the following:
   - To configure the default view of the LCD display, select one mode below.

Note: The default view is shown in the automatic mode.

Mode	Data entered
Automatic mode	The LCD display cycles through both the inlet and overcurrent protector information. This is the default. Overcurrent protector information is available only when your PX4 has overcurrent protectors.
Transfer switch overview	Shows the "Transfer Switch" page.
Inlet overview	The LCD display cycles through the inlet information only.

- To enable the front panel outlet-switching function, select the 'Outlet switching' checkbox.
- To enable the front panel actuator-control function, select the 'Peripheral actuator control' checkbox.
- The built-in beeper's mute control function is enabled per default. To disable it, deselect the 'Mute beeper' checkbox.
- By default the front panel RCM self-test function, if available, is enabled.

3. Click Save.

If the 'Mute beeper' feature is enabled, you can operate the front panel to mute it whenever it beeps. Or you can turn on or off outlets/actuators by operating the front panel.

Configuring the Serial Port

You can change the bit rate of the serial port labeled CONSOLE / MODEM that is present on some models. The default bit rate for console and modem operation is 115200 bps.

The following devices are supported via the serial interface:

- A computer for console management.
- A Raritan KVM product.
- An analog modem for remote dial-in and access to the CLI.
- A GSM modem for sending out SMS messages to a cellular phone.

Bit-rate adjustment may be necessary. Change the bit rate before connecting the supported device to the PX4 through the serial port, or there are communication problems.

You can set diverse bit-rate settings for console and modem operations. Usually the PX4 can detect the device type, and automatically apply the preset bit rate.

The PX4 will indicate the detected device in the Port State section of the Serial Port page.

To configure serial port and modem settings, choose Device Settings > Serial Port.

► *To change the serial port's baud rate settings:*

1. Click the 'Connected device' field to make the serial port enter an appropriate state.

Options	Description
Automatic detection	The PX4 automatically detects the type of the device connected to the serial port. Select this option unless your PX4 cannot correctly detect the device type.
Force console	The PX4 attempts to recognize that the connected device is set for the console mode.
Force analog modem	The PX4 attempts to recognize that the connected device is an analog modem.
Force GSM modem	The PX4 attempts to recognize that the connected device is a GSM modem.

2. Click the 'Console baud rate' field to select the baud rate intended for console management.

Note: For a serial RS-232 or USB connection between a computer and the PX4, leave it at the default (115200 bps).

---

3. Click the 'Modem baud rate' field to select the baud rate for the modem connected to the PX4.

The following modem settings/fields appear in the web interface after the PX4 detects the connection of an analog or GSM modem.

► *To configure the analog modem:*

1. Select the 'Answer incoming calls' checkbox to enable the remote access via a modem. Otherwise, deselect it.
2. Type a value in the 'Number of rings before answering' field to determine the number of rings the PX4 must wait before answering the call.

► *To configure the GSM modem:*

1. Enter the SIM PIN code.
2. Select the 'Use custom SMS center number' checkbox if a custom SMS center will be used.
   - Enter the SMS center number in the 'SMS center' field.
3. If needed, click Advanced Information to view detailed information about the modem, SIM and mobile network.
4. To test whether the PX4 can successfully send out SMS messages with the modem settings:
   a. Enter the number of the recipient's phone in the Recipient Phone field.
   b. Click Send SMS Test to send a test SMS message.

Lua Scripts

If you can write or obtain any Lua scripts, you can create or load them into the PX4 to control its behaviors.

Some Lua scripts examples are provided, which you can load as needed.

Note: Not all Lua script examples can apply to your PX4 model. You should read each example's introduction before applying them.

You must have the Administrator Privileges to manage Lua scripts.

Writing or Loading a Lua Script

You can enter or load up to 4 scripts.

► *To write or load a Lua script:*

1. Choose Device Settings > Lua Scripts >

.
2. Type a name for this script. Its length ranges between 1 to 63 characters.

The name must contain the following characters only.

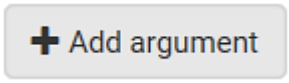
- Alphanumeric characters
- Underscore (_)
- Minus (-)

Note: Spaces are NOT permitted.

3. Determine whether and when to automatically execute the loaded script.

Checkbox	Behavior when selected
Start automatically at system boot	Whenever the PX4 reboots, the script is automatically executed.
Restart after termination	The script is automatically executed each time after 10 seconds since the script execution finishes.

4. (Optional) Determine the arguments that will be executed by default.

   a. Click 

.

   b. Type the key and value.

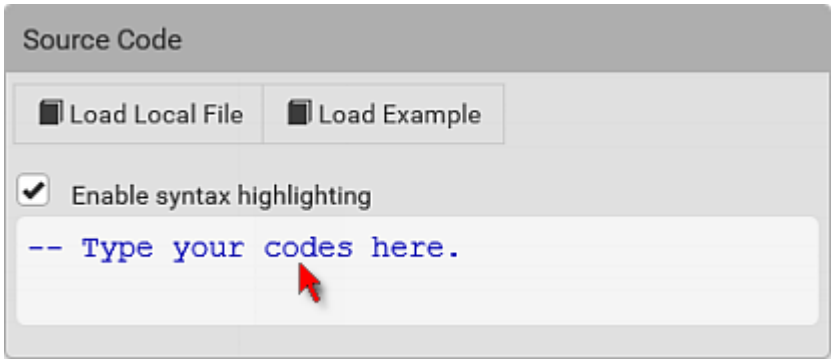
   c. Repeat the same steps to enter more arguments as needed.

   - To remove any existing argument, click adjacent to it.

   Note: The above default arguments will be overridden by new arguments specified with the "Start with Arguments" command or with any Lua-script-related event rule.

5. In the Source Code section, do one of the following. It is recommended to leave the Enable Syntax Highlighting checkbox selected unless you do not need different text colors to identify diverse code syntaxes.

- To write a Lua script, type the codes in the Source Code section.



- To load an existing Lua script file, click Load Local File.
- To use one of the default Lua script examples, click Load Example.

Warning: The newly-loaded script will overwrite all existing codes in the Source Code section. Therefore, do not load a new script if the current script meets your needs.

---

6. If you chose to load a script or the example in the previous step, its codes are then displayed in the Source Code section. Double check the codes. If needed, modify the codes to meet your needs.
7. Click Create.

Manually Starting or Stopping a Script

You can manually start or stop an existing Lua script at any time.

When starting a script, you can choose to start it either with its default arguments or with new arguments.

Tip: To have the PX4 automatically start or stop a script in response to an event, create an event rule.

► *To manually start a script:*

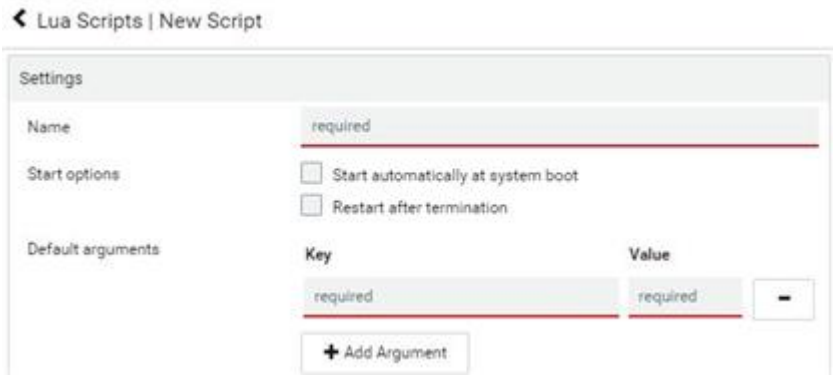
1. Choose Device Settings > Lua Scripts. The Lua scripts list displays.

2. Click the desired script whose state is either 'Terminated' or 'New.'
3. To start with default arguments, click

.

To start with new arguments, click ⋮ > Start With Arguments. Newly-assigned arguments will override default ones.

4. If you chose "Start With Arguments" in the above step, enter the key and value in the Start Lua Script dialog.
   - Click ✚ Add argument if needing additional arguments.



5. Click Start.
6. The script output will be shown in the Script Output section.
   - If needed, click Clear to delete the existing output data.

► *To manually stop a script:*

1. Choose Device Settings > Lua Scripts.
2. Click the desired script whose state is either 'Running' or 'Restarting.'
3. Click ■ Stop on the top-right corner.
4. Click Stop on the confirmation message.

Checking Lua Scripts States

Choose Device Settings > Lua Scripts to show the scripts list, which indicates the current state and settings of each script.

► *State:*

State	Description
New	The script is never executed since the device boot.
Running	The script is currently being executed.
Terminated	The script was once executed, but stops now.
Restarting	The script will be executed. Only the scripts with the "Restart" column set to "yes" will show this state.

► *Autostart:*

This column indicates whether the checkbox labeled "Start automatically at system boot" is enabled. .

► *Restart:*

This column indicates whether the checkbox labeled "Restart after termination" is enabled.

Modifying or Deleting a Script

► *To modify or replace a script:*

1. Choose Device Settings > Lua Scripts.
2. Click the desired one in the scripts list.
3. Click ⋮ > Edit Script.
4. Make changes to the information shown, except for the script's name, which cannot be revised.
   - To replace the current script, click Load Local File or Load Example to select a new script.

► *To delete a script:*

1. Choose Device Settings > Lua Scripts.
2. Click the desired one in the scripts list.
3. Click ⋮ > Delete.
4. Click Delete on the confirmation message.

Miscellaneous

The Miscellaneous page contains some assorted settings.

► *Enable USB Host Ports:*

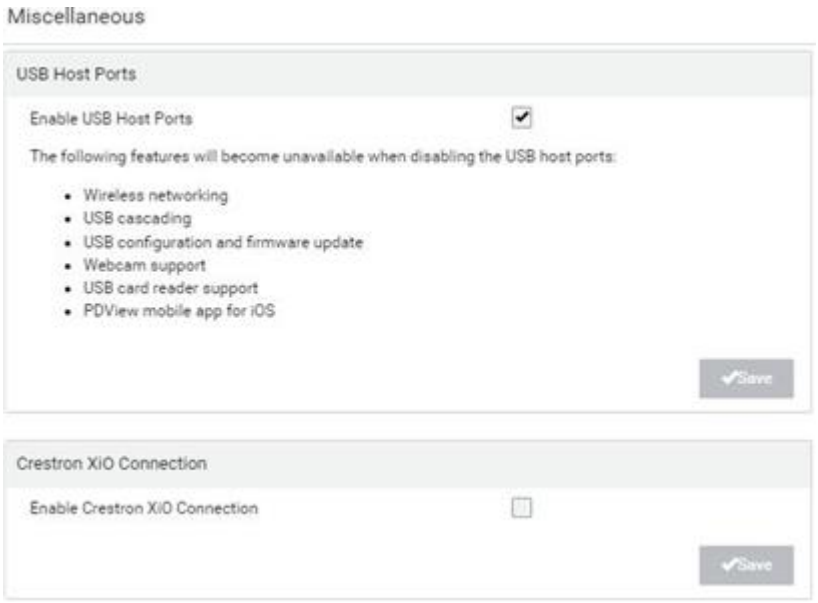
- If you want to enable/disable your PX4 USB host ports, use this checkbox.

When disabled, the following features are unavailable:

- Wireless networking
- USB cascading
- USB configuration and firmware update
- Webcam support
- USB card reader support
- PDView mobile app for iOS

► *Enable Crestron XiO Connection:*

- If the Crestron XiO connection is part of your configuration, you can enable/disable it here.



Using Prometheus and Grafana

You can use the open-source tools Prometheus and Grafana to collect sensor data and visualize it. In Prometheus, the sensor readings are stored locally as time series data, which can be visualized in graphs created by Grafana or similar tools This information is displayed on dashboards, and you can create multiple dashboards as needed.

Requirements for Prometheus and Grafana

► *Prometheus Requirements:*

- Prometheus v2.0 or higher
- Install on a computer in the PX4 network.
- Reference: https://prometheus.io/docs/introduction/first_steps/

► *Grafana requirements:*

- Grafana v8.1.5 or higher
- Install on a computer in the network of the Prometheus instance.
- Reference: https://grafana.com/grafana/download?pg=get&plcmt=selfmanaged-box1-cta1

Collected Data

For integration into a Prometheus system, the PDU can output all measurements in a Prometheus-compatible format that can be queried from the URL: 'https://<PDU_IP>/cgi-bin/dump_prometheus.cgi'. The URL has one optional parameter, "include_names=1", to include PDU, names for Inlet, Outlet, OCP, TransferSwitch,and Sensors as metric labels.

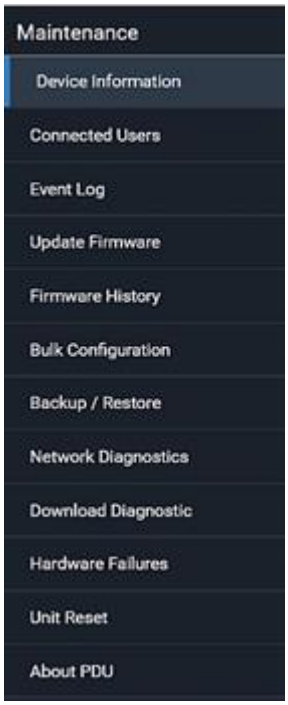
You can use cURL as follows to retrieve the data:

1. curl -k https://username:password@[PDU_IP]/cgi-bin/dump_prometheus.cgi

2. curl -k https://username:password@[PDU_IP]/cgi-bin/dump_prometheus.cgi?include_names=1

Maintenance

Click 'Maintenance' in the *Menu* to view the options.



Device Information

The Device Information page displays hardware and software information of components or connected peripheral devices.

Tip: If the information shown on this page does not match the latest status, press F5 to reload it.

► *To display device information:*

1. Choose Maintenance > Device Information. Click any header to expand the information. Available sections depend on your model.

Section title	Information shown
Information	General device information, such as model name, serial number, firmware version, board ID and revision, MIB download link(s) and so on. iX7-G1 hardware or newer shows both Board ID and revision.
Network	The network information, such as the current networking mode, IPv4 and/or IPv6 addresses and so on. Information on cascading configurations also shows here.

Section title	Information shown
Port Forwarding	If the port forwarding mode is activated, this section shows a list of port numbers for all cascaded devices.
Outlets	Each outlet's receptacle type, operating voltage and rated current.
Overcurrent Protectors	Each overcurrent protector's type, rated current and the outlets that it protects.
Controllers	Each inlet or outlet controller's serial number, Device ID,Hardware ID, Firmware Version and Status.
Peripheral Devices	Serial numbers, model names, position and firmware-related information of connected environmental sensor packages. *Note: Serial number when clicked provides the detail information of the peripheral device.*
Asset Management	Each asset strip's ID, boot version, application version and protocol version.
Security	SSH host keys.

Viewing Connected Users

You can check which users are logged in and their status. If you have administrator privileges, you can terminate any user's connection.

► *To view and manage connected users:*

1. Choose Maintenance > Connected Users. A list of logged-in users displays.

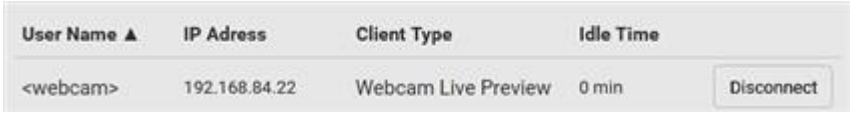
Column	Description
User Name	The login name of each connected user.
IP Address	The IP address of each user's host. For the login via a local connection (serial RS-232 or USB), <local> is displayed instead of an IP address.

Column	Description
Client Type	The interface through which the user is being connected to the PX4. • Web GUI: Refers to the web interface. • CLI: Refers to the command line interface (CLI). The information in parentheses following "CLI" indicates how this user is connected to the CLI. - Serial: The local connection, such as the serial RS-232 or USB connection. - SSH: The SSH connection. - Telnet: The Telnet connection. • Webcam Live Preview: Refers to the live webcam image sessions. See below.
Idle Time	The length of time for which a user remains idle.

2. To disconnect any user, click the corresponding Disconnect.
   a. Click Disconnect on the confirmation message.
   b. The disconnected user is forced to log out.

► *If there are live webcam sessions:*

All Live Preview window sessions sharing the same URL, including one Primary Standalone Live Preview window and multiple Secondary Standalone Live Preview windows, are identified as one single "<webcam>" user in the Connected Users list. You can disconnect a "<webcam>" user to terminate all sessions sharing the same URL.



The IP address refers to the IP address of the host where the Primary Standalone Live Preview window exists, NOT the IP address of the other two associated sessions.

Viewing, Pausing, Resuming or Clearing the Local Event Log

By default, certain system events are captured and saved in a local event log.

You can view over 2000 historical events in the local event log. When the log size exceeds 256KB, each new entry overwrites the oldest one.

► *To display the local event log:*

1. Choose Maintenance > Event Log.

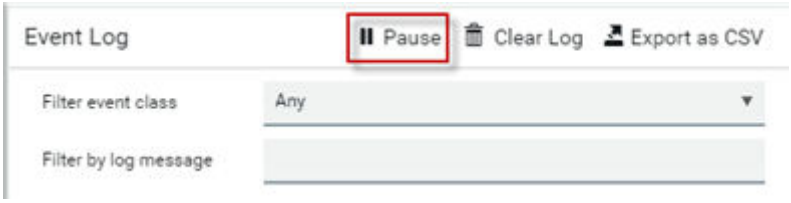
Each event entry consists of:

- ID number of the event
- Date and time of the event
- Event type
- A description of the event

2. To filter the list, select the desired event type in the 'Filter event class' field, or enter keywords in the 'Filter by log message' field.
3. The log is refreshed automatically at a regular interval of five seconds. To avoid any new events' interruption during data browsing, you can suspend the automatic update by clicking Pause.
   - To restore automatic update, click Resume. Those new events that have not been listed yet due to suspension will be displayed in the log now.

► *To Pause & Resume the local log:*

1. Click Pause on the top right corner.



GUI temporarily stops displaying Event Log updates and button label shows 'Resume'.

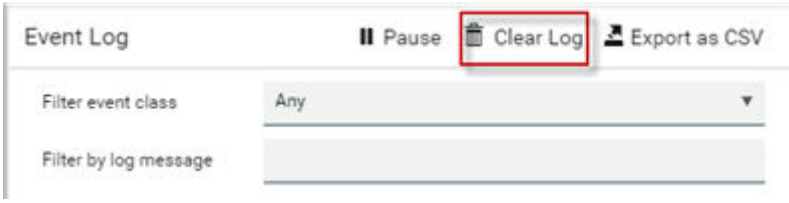
2. Click Resume on the top right corner.

GUI continues displaying Event Log updates and shows also messages which were skipped when paused. The Button label shows 'Pause'.

Note: After page change, Event Log list is automatically in 'Resumed' state again.

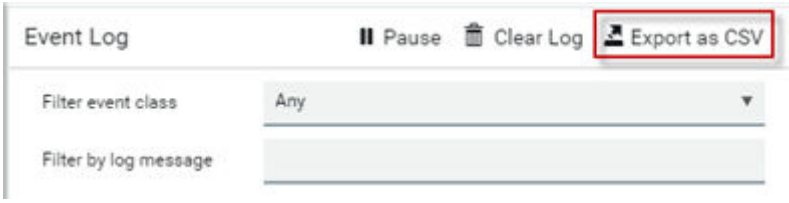
► *To clear the local log:*

1. Click Clear Log on the top-right corner.
2. Click Clear Log on the confirmation message.



► *To export the log:*

1. Click Export as CSV on top right corner.
2. CSV file gets downloaded to local machine.



Updating the Firmware

When performing the firmware update, the PX4 keeps each outlet's power status unchanged so no server operation is interrupted. During and after the firmware update, outlets that have been powered on prior to the update remain powered ON and outlets that have been powered off remain powered OFF.

You must be the administrator or a user with the Firmware Update permission to update the firmware.

Before starting, read the release notes. If you have any questions or concerns, contact Technical Support BEFORE updating.

On a multi-inlet PDU, all inlets must be connected to power for the PDU to successfully update its firmware.

Note that firmware update via iOS mobile devices, such as iPad, requires the use of iCloud Drive or a file manager app.

Firmware update can also be completed using methods other than the web interface. See Special Configuration and Upgrade Methods (on page 573).

Warning: Do NOT perform the firmware update over a wireless network connection.

Raritan
A brand of legrand

► *To update the firmware:*

1. Choose Maintenance > Update Firmware.
2. Click Browse to select an appropriate firmware file.
3. Click Upload. A progress bar appears to indicate the upload process.
4. Select Free memory before upload to clear up the memory.
5. Once complete, information of both installed and uploaded firmware versions as well as compatibility and signature-checking results are displayed.
   - The expected firmware platform and product category is displayed in case the uploaded file is incorrect.
   - If anything is incorrect, click Discard Upload.
6. To proceed with the update, click Update Firmware.

Warning: Do NOT power off the PX4 during the update.

---

7. During the firmware update:
   - A progress bar appears on the web interface, indicating the update status.
   - The front panel display shows the firmware upgrade message.
   - The outlet LEDs flash if the relay boards are being updated. If the firmware update does not include the update of the relay board firmware, outlet LEDs do NOT flash.
   - No users can log in.
   - Other users' operation, if any, is forced to suspend.
8. When the update is complete, the unit resets, and the Login page re-appears.

Important: If you are using the PX4 with an SNMP manager, download its MIB again after the firmware update to ensure your SNMP manager has the correct MIB for the latest release you are using.

Upgrade Matrix

In Xerus 4.0.x, the following upgrade paths must be followed:

Firmware Version	Upgrade Steps
4.0.x (x<40)	⇒ 4.2.11 (cannot use combo image)
4.0.x (x≥40)	⇒4.2.11
4.1.x	⇒ 4.2.11
4.2.x	⇒4.3.x

Note: Due to file system changes in Xerus 4.0.x, the upgrade paths must be followed, or the Xerus-based device may become inoperable and require manual recovery.

Upgrade Guidelines for Existing Cascading Chains

There are additional concerns when upgrading devices in a cascading chain. See Firmware Upgrade for Cascading Chains (on page 650)

A Note about Firmware Upgrade Time

The PDU firmware upgrade time varies from unit to unit, depending on various external and internal factors.

External factors include, but are not limited to: network throughput, firmware file size, and speed at which the firmware is retrieved from the storage location. Internal factors include: the necessity of upgrading the firmware on the microcontroller and the number of microcontrollers that require upgrade (which depends on the number of outlets). The microcontroller is upgraded only when required. Therefore, the length of firmware upgrade time ranges from approximately 3 minutes (without any microcontroller updated) to almost 7 minutes (with all microcontrollers for 48 outlets updated). Take the above factors into account when estimating the PDU's firmware upgrade time.

The time indicated in this note is for PX4 web-interface-based upgrades. Upgrades through other management systems, such as Sunbird's Power IQ, may take additional time beyond the control of the PDU itself. This note does not address the upgrades using other management systems.

Full Disaster Recovery

If the firmware upgrade fails, causing the PX4 to stop working, you can recover it by using a special utility rather than returning the device.

Contact Raritan Technical Support for the recovery utility. You will also need an appropriate firmware file in the recovery procedure.

Viewing Firmware Update History

The firmware upgrade history is permanently stored. It remains available even though you perform a device reboot or any firmware update.

► *To view the firmware update history:*

1. Choose Maintenance > Firmware History.

Each firmware update event consists of:

- Update date and time
- Previous firmware version
- Update firmware version
- Update result

Bulk Configuration

The Bulk Configuration feature lets you save generic settings of a configured PX4 device to your computer. You can use this configuration file to copy settings to other devices of the same model and firmware version.

A source device is the PX4 device where the configuration file is downloaded/saved. A target device is the PX4 device that loads the configuration file.

By default the configuration file downloaded from the source device contains settings based on the built-in bulk profile. The built-in bulk profile defines that all settings should be saved except for device-specific settings, such as IP address or environmental sensor settings. If you need to load these device-specific settings, you should use the Backup/Restore feature instead.

You can decide which settings are downloaded by creating your own bulk configuration profile.

When the date and time settings are included in the bulk configuration file, exercise caution when distributing that file to target devices located in a different time zone than the source device.

This bulk configuration method can be employed through the web interface, USB, or SCP. See Special Configuration and Upgrade Methods (on page 573).

► *Bulk configuration overview:*

1. A built-in configuration profile is available, or you can customize your own bulk configuration profile.
2. Select and download the file from the source device.
3. Upload the file to perform the configuration on the target device.

Bulk Configuration Restrictions

Before performing bulk configuration, make sure your source and target devices are compatible devices for sharing general settings.

► *Restrictions for bulk configuration:*

- The target device must be running the same firmware version as the source device.
- The target device must be of the same model type as the source device.
- Bulk configuration is permitted if the differences between the target and source devices are only "mechanical" designs which are indicated in the model name's suffix.

  For example, you can perform bulk configuration between PX3-4724-E2N1K2 and PX3-4724-E2N1K9 since the only difference between the two models is their chassis colors represented by K2 (blue) and K9 (gray).

► *Mechanical design codes in model numbers:*

These mechanical designs are represented by suffixes added to the model name. In the table, *x* represents a number. For example, A*x* can be A1, A2, A3, and so on.

Suffix	Mechanical design	Example
A*x*	The line cord's length in meters Note: For an inline monitor, it is likely two Ax's are added to the model name for indicating the lengths of its inlets' and outlets' line cords.	A20 = 3.3 meters
B*x*	The line cord's color	B501 = bright red orange
C*x*	Cord types or options	C4 = power cord with the standard gauge
D*x*	Plug types or options	D1 = IP67 watertight plug
E*x*	Outlet types or options	E2 = *Locking* C13 or *Locking* C19
G*x*	Controller options	G0 = no controller
K*x*	Chassis colors	K6 = yellow
L*x*	The line cord's length in centimeters	
N*x*	Chassis dimensions or other mechanical changes	
O*x*	OCP brand options	
P*x*	Special requests for device painting or printing	
Q*x*	Special requests for physical placement arrangements	
R*x*	Custom logo	
U*x*	Different power plug brands	

Customizing Bulk Configuration Profiles

A bulk profile defines which settings are downloaded/saved from the source device and which are not. The default is to apply the built-in bulk profile, which downloads all settings from the source device except for device-specific data.

If the built-in profile does not meet your needs, you can create your own profiles.

► *To create new bulk configurations profiles:*

1. Log in to the source device whose settings you want to download.
2. Choose Maintenance > Bulk Configuration.
3. Click New Profile, then enter a Profile name and Description.

4. To make this new profile the default one for future bulk configuration operations, select the 'Select as default profile' checkbox.
5. Now decide which settings to include or exclude.
   a. Click of the setting which you want to configure.
   b. When the pop-up menu appears, select one of the options.
      Note that the two options 'Inherited' and 'Built-in' are mutually exclusive.

Option	Description
Excluded	The setting will *not* be downloaded.
Included	The setting will be downloaded.
Inherited	The setting will follow its parent setting (that is, the upper-level setting). • If you select 'Excluded' for its upper-level setting, this setting will be also excluded. • If you select 'Included' for its upper-level setting, this setting will be also included. The option inherited from its parent setting will be enclosed in parentheses.
Built-in	The setting will follow the same setting of Raritan's built-in profile. • If 'Excluded' is selected in the built-in profile, this setting will be also excluded. • If 'Included' is selected in the built-in profile, this setting will be also included. The option inherited from the built-in profile will be enclosed in parentheses. *Note: The option 'Built-in' is available in those settings whose corresponding settings in the built in profile have been set to a non-inherited option -- Excluded or Included.*

6. Click Save.

Performing Bulk Configuration

To perform the bulk configuration using the web interface, first select and download the bulk configuration file, then upload it to the target device to configure it.

► *Step 1: Save a bulk configuration file*

You must have the Administrator Privileges or "Unrestricted View Privileges" to download the configuration.

1. Log in to the source device.
2. Choose Maintenance > Bulk Configuration.
3. Select the profile of the configuration you want to use in the Bulk Profile field.
4. In the 'Bulk format' field select Encrypted or Cleartext, to specify the security of the file.

Option	Description

Encrypted	• Partial content is base64 encoded. • Its content is encrypted using the AES-128 encryption algorithm. • The file is saved to the TXT format
Cleartext	• Content is displayed in clear text. • The file is saved to the TXT format.

5. In Encrypted mode, you can password protect the file. Select the Use Password checkbox, then enter a password. A password will be required when the file is uploaded on the target device.
6. Click Download Bulk Configuration. The file is named "bulk_config" with the source device serial number and a creation date/time stamp, such as "bulk_config_1BZ31B603C_20210927". Your browser's file download method determines download location. Save the file so that it's available to be uploaded to the target device.

► *Step 2: Upload the file to configure the target*

You must have the Administrator Privileges to upload the configuration.

1. Log in to the target device, which is of the same model and runs the same firmware as the source device.
2. Choose Maintenance > Bulk Configuration.
3. In the Restore Bulk Configuration section, click Browse to select the configuration file.
4. Click 'Upload & Restore Bulk Configuration'.
5. Confirm the operation and enter the administrator password, then click Restore.
6. Wait until the login page reappears.

Modifying or Deleting Bulk Configuration Profiles

You can modify or delete any bulk profile except for the built-in one.

Note that a profile that has been set as the default cannot be deleted. To remove it, you have to remove its default setting first.

Choose Maintenance > Bulk Configuration. A list of profiles displays and then do one of the following.

► *To modify an existing profile:*

1. Click on the row of the wanted profile in the list.
2. Change the settings you want.
3. Click Save.

► *To delete profiles*

1. Select one or multiple profiles, then click the Delete icon .
2. Click Delete in the confirmation message.

Backup and Restore of Device Settings

Unlike the bulk configuration file, the backup file contains ALL device settings, including device-specific data like device names and all network settings. To back up or restore the device settings, you should use the Backup/Restore feature. To perform bulk configuration among multiple PX4 devices, use the Bulk Configuration feature instead.

All PX4 information is captured in the plain-TEXT-formatted backup file except for the device logs and TLS certificate.

Backup/Restore can also be completed using other methods. See Special Configuration and Upgrade Methods (on page 573).

► *To download a backup file:*

You must have the Administrator Privileges or "Unrestricted View Privileges" to download a backup file.

1. Choose Maintenance > Backup/Restore.
2. Check the 'Backup format' field. If the chosen value does not match your need, change it.

Option	Description
Encrypted	• Partial content is base64 encoded. • Its content is encrypted using the AES-128 encryption algorithm. • The file is saved to the TXT format
Cleartext	• Content is displayed in clear text. • The file is saved to the TXT format.

3. Click Download Device Settings. Save the file onto your computer.

► *To restore using a backup file:*

You must have the Administrator Privileges to restore the device settings.

1. Choose Maintenance > Backup/Restore.
2. Click Browse to select the backup file.
3. Click 'Upload & Restore Device Settings' to upload the file.
   - A message appears, prompting you to confirm the operation and enter an administrator password.
4. Enter the password, then click Restore.
5. Wait until the PX4 resets and the Login page re-appears, indicating that the restore is complete.

Network Diagnostics

PX4 provides the following tools in the web interface for diagnosing potential networking issues.

- Ping: The tool is useful for checking whether a host is accessible through the network or Internet.
- Trace Route: The tool lets you find out the route over the network between two hosts or systems.
- List TCP Connections: You can use this function to display a list of TCP connections.

Tip: These network diagnostic tools are also available through the CLI.

Choose Maintenance > Network Diagnostics, and then perform any function below.

► *Ping:*

1. Type values in the following fields.

Field	Description
Network host	The name or IP address of the host that you want to check.
Number of requests	A number up to 20. This determines how many packets are sent for pinging the host.

2. Click Run Ping to ping the host. The Ping results are then displayed.

► *Trace Route:*

1. Type values in the following fields.

Field/setting	Description
Hostname	The IP address or name of the host whose route you want to check.
Timeout(s)	A timeout value in seconds to end the trace route operation.
Use ICMP packets	To use the Internet Control Message Protocol (ICMP) packets to perform the trace route command, select this checkbox.

2. Click Run. The Trace Route results are then displayed.

► *List TCP Connections:*

1. Click the List TCP Connections title bar to show the list.

Downloading Diagnostic Information

Important: Use this function only when you are directed by Technical Support.

You can download the diagnostic file to a client machine. The file is compressed into a .tgz file and should be sent to Technical Support.

This feature is accessible only by users with Administrative Privileges or Unrestricted View Privileges.

► *To retrieve a diagnostic file:*

1. Choose Maintenance > Download Diagnostic > Download Diagnostic.
2. The system prompts you to save or open the file. Save the file.

Hardware Issue Detection

This page lists any internal hardware issues PX4 has detected, including current events and historical records.

Choose Maintenance > Hardware Failures, and the page similar to either of the following diagrams opens.

Current hardware failure events, if any, will also display on the Dashboard.

► *NO hardware failures detected:*

► *Hardware failure(s) detected:*

► *Hardware failure types:*

Hardware issues	Description
Network device not detected	A specific networking interface is NOT detected.
I2C Bus stuck	A specific I2C bus is stuck, which affects the communication with sensors.
Sub controller not reachable	Communication with a specific sub unit controller fails.
Sub controller malfunction	A specific sub unit controller does not work properly.
Outlet power state inconsistent	The physical power state of a specific outlet is different from the chosen power state set by the software.
Sub controller incompatible	A specific sub unit controller is incompatible with the firmware.

Rebooting

You can remotely reboot the PX4 via the web interface.

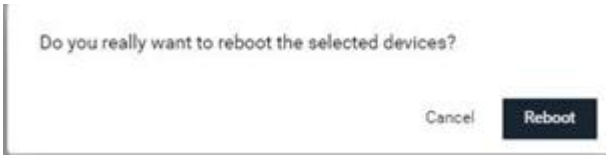
Resetting/rebooting does not interrupt the operation of connected servers because there is no loss of power to outlets. During and after the reboot, outlets that have been powered on prior to the reboot remain powered on, and outlets that have been powered off remain powered off.

Warning: Rebooting deletes all webcam snapshots that are saved locally. If needed, download important snapshots before rebooting the device.

Raritan
A brand of legrand

► *To reboot the device:*

1. Choose Maintenance > Unit Reset > Reboot Unit.



2. Click Reboot.
3. A message appears, with a countdown timer showing the remaining time of the operation. It takes about one minute to complete.
4. When the restart is complete, the login page opens.

Tip: If you are not redirected to the login page after the restart is complete, click the text "this link" in the countdown message.

Note: Device reset will cause CLI communications over an "USB" connection to be lost. Therefore, re-connect the USB cable after the reset is complete.

Resetting All Settings to Factory Defaults

You must have the Administrator Privileges to reset all settings to factory defaults.

Resetting to factory default can also be completed in the CLI or with a Reset button on the unit. See Resetting to Factory Defaults (on page 654)

Important: Exercise caution before resetting to factory defaults. This erases existing information and customized settings, such as user profiles, threshold values, and so on. Only active energy data and firmware upgrade history are retained.

If your PDU is in a Linking configuration, you can reset expansion units through the primary unit.

► *To reset the device to factory defaults:*

1. Choose Maintenance > Unit Reset
   - If your PDU is in a cascaded configuration, select the units you want to reset. If you do not have cascaded devices listed, move to step 2.

2. Click Reset to Factory Defaults.

3. Type your password and then click Factory Reset.
4. A message appears, with a countdown timer showing the remaining time of the operation. It takes about two minutes to complete.
5. When the reset is complete, the login page opens.

Tip: If you are not redirected to the login page after the reset is complete, click the text "this link" in the countdown message.

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.

Webcam Management

With a Logitech® webcam connected, you can visually monitor the environment around the PX4 via snapshots or videos captured by the webcam.

The 'Webcams' menu item appears when there is any webcam connected to the PX4, or when there are snapshots saved onto already.

► *Permissions required:*

To do...	Permission(s) required
View snapshots and videos	Either permission below: • Change Webcam Configuration • View Webcam Snapshots and Configuration
Configure webcam settings	Change Webcam Configuration

Configuring Webcams and Viewing Live Images

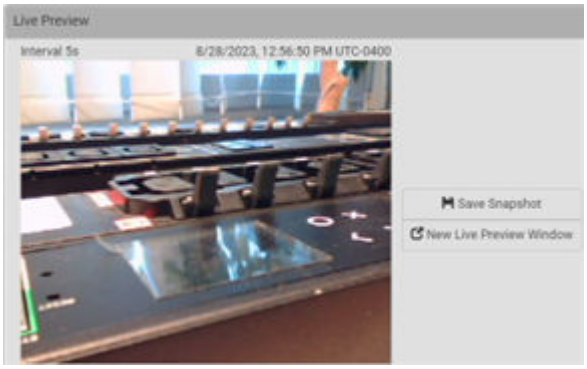
To configure a webcam or view live snapshot/video sessions, choose Webcams in the *Menu*. Then click the desired webcam to open that webcam's page.

Note that default webcam names are determined by the detection order. The one that is detected first is named *Webcam*, and a second webcam detected later is named *Webcam 2*.

The Webcam page consists of three sections -- *Live Preview*, *Image Controls* and *Settings*.

► *Live Preview:*

1. By default the Live Preview section is opened, displaying the live snapshot/video session captured by the webcam.
   - The default is to show live snapshots. Interval time and capture date/time of the image are displayed on the top of the image. In video mode, the number of frames per second (fps) and the video capture date/time are displayed.



Tip: The date and time shown on the PX4 web interface are automatically converted to your computer's time zone.

---

2. To save the current image onto PX4 or a remote server, click Save Snapshot.
   - The default storage location for snapshots is the PX4 device. To save them onto a remote server, you can change the storage settings.
   - To download an image onto your computer, you can right-click it and save.
3. To have the same live session displayed in a separate window, click New Live Preview Window.
   - A separate window appears, which is called the Primary Standalone Live Preview window in this User Guide.
   - You can send out this window's URL to share the live image with others.
   - Note that your browser may block the pop-up window

► *Image Controls:*

1. Adjust the brightness, contrast, saturation and gain by modifying their values or adjusting the corresponding slide bar.
   - To customize the gain value, you must deselect the Auto Gain checkbox first.
   - To restore all settings to this webcam's factory defaults, click Set to Webcam Defaults.

► *Settings:*

1. Click Edit Settings.
2. Enter a name for the webcam. Up to 64 ASCII printable characters are supported.
   - If configured to store snapshots on a *remote* server, the webcam's name determines the name of the folder where snapshots are stored.
   - It is suggested to customize a webcam's name before saving snapshots on the remote server. In case you change the webcam's name after saving any snapshots, PX4 will create a new folder with the new webcam name while keeping the old folder with the old name.
3. Type the location information in each location field as needed. Up to 63 ASCII printable characters are supported.
   - Note that the location data you enter is not available in those snapshots stored on remote servers.

   Tip: If the webcam's location is important, you can customize the webcam's name based on its location.

   ---

4. Select a resolution for the webcam.
   - If you connect two webcams to one USB-A port using a powered USB hub, set the resolution to 352x288 or lower for optimal performance.
5. Select the webcam mode.

Mode	Description
Video	The webcam enters the video mode. • Set the 'Framerate' (frames per second) as needed.
Snapshot	The webcam shows static images captured by the webcam at a regular interval. • To determine the interval, set the 'Time Between Snapshots' (seconds).

6. Click Save. The changes made to the settings are applied to the live session in the above *Live Preview* section immediately.

Sending Links to Snapshots or Videos

When opening a Primary Standalone Live Preview window, a unique URL is generated for this window session. You can email or instant message this URL to as many people as possible as long as your system resources permit. Recipients can then click on the provided link and view live snapshots or videos simultaneously in the Secondary Standalone Live Preview window(s).

Tip: All Live Preview window sessions sharing the same URL, including one Primary Standalone Live Preview window and multiple Secondary Standalone Live Preview windows, are identified as one single "<webcam>" user in the Connected Users list. You can disconnect a "<webcam>" user to terminate all sessions sharing the same URL.

► *Best practice:*

1. The sender opens the Primary Standalone Live Preview window, and sends the link to one or multiple recipients.
2. The sender must wait until at least one recipient opens the Secondary Standalone Live Preview window.
3. The recipient(s) should inform the sender that the link has been opened.
4. Now the sender can close the Primary Standalone Live Preview window.

► *To send a snapshot or video link via email or instant message:*

1. Choose Webcams in the *Menu*.
2. Click the desired webcam to open the Webcam page.
3. Click New Live Preview Window in the Live Preview section. The live snapshot or video in a standalone window opens.

4. Copy the URL from that live preview window.
   a. Select the URL shown on the top of the image.

   b. Right click to copy the URL, or press CTRL+ C.
5. Send the URL link through an email or instant message application to one or multiple persons.
6. Leave the live preview window open until the recipient(s) opens the snapshot or video via the link.

How Long a Link Remains Accessible

For documentation purposes, the one who opens and sends the URL of the Primary Standalone Live Preview window is called *User A* and the two recipients of the same URL link are called *User B* and *C*.

User C is able to access the snapshot or video image via the link when the URL link remains valid, which can be one of these scenarios:

- The Primary Standalone Live Preview window remains open on User A's computer. If so, even though User A logs out of the PX4 or the login session times out, the link remains accessible.
- User B's Secondary Standalone Live Preview window remains open. If so, even though User A already closes the Primary Standalone Live Preview window, the link remains accessible.
- Neither User A's Primary Standalone Live Preview window nor User B's Secondary Standalone Live Preview window remains open, but it has not exceeded two minutes yet after the final live preview window session was closed.

Note: The link is no longer valid after two minutes since the final live preview window is closed.

Viewing, Downloading, Deleting Locally-Saved Snapshots

This section describes the operation for snapshots saved onto the PX4 device only.

When saving a snapshot, it is stored locally on the PX4 device by default. Up to 10 snapshots can be stored locally. The oldest snapshot is automatically overridden by the newest one when the total of snapshots exceeds 10, if no snapshots are deleted manually.

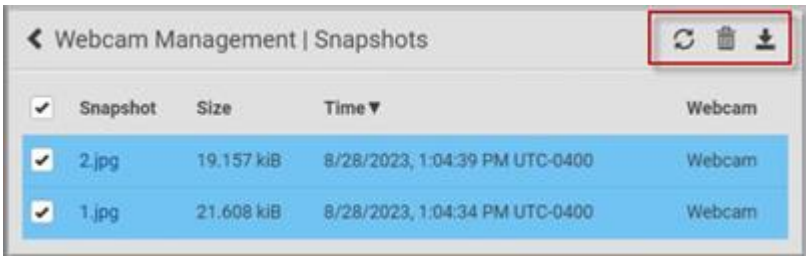
When there is more than one webcam connected, then the oldest snapshot of the webcam with the most snapshots is overwritten.

Snapshots are saved as JPG files, and named with sequential numbers, such as *1.jpg*, *2.jpg*, *3.jpg*.

Warning: Rebooting the PX4 deletes all webcam snapshots that are saved locally. If needed, download important snapshots before rebooting the device.

► *To view, refresh, download or delete saved snapshots:*

1. Choose Webcams > Browse Snapshots. The Snapshots page opens.
   - To view a snapshot, click the link in the list. The image, capture time and resolution is displayed on the same page.
   - To refresh the list, click the Refresh icon.
   - To download an image file, click the Download icon.
   - To delete an image, select the checkbox of the image and click the Delete icon.



Changing Storage Settings

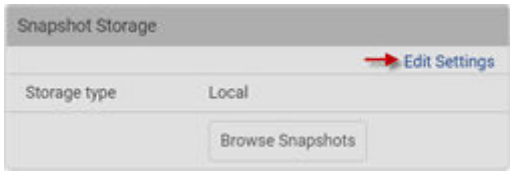
Important: The PX4 web interface only lists the snapshots stored locally on the PX4 device, but does NOT list those saved onto remote servers. You must launch appropriate third-party applications, such as an FTP client, to access and manage the snapshots stored on remote servers.

The default is to store snapshots locally on the device, which has a limitation of 10 snapshots. Note that any operation involving device reboot, such as firmware upgrade, will remove the locally saved snapshots.

If you need to keep more than 10 images or need to keep them permanently, configure the settings to move images onto a remote FTP server.

► *To configure the storage settings:*

1. Choose Webcams > Edit Settings.



2. Click the Storage Type field to select the desired storage location and configure as needed.

Note: When entering user credentials for remote servers, make sure the user credentials you enter have the write permission, or NO snapshots can be successfully saved onto remote servers.

Storage location	Description
Local	'Local' means the PX4. This is the default. • It can store a maximum of 10 snapshots only. • The web interface can list and display all snapshots stored on the PX4. • All snapshots are CLEARED when the PX4 is rebooted.
FTP	Snapshots are saved onto a FTP server. • Total number of saved snapshots depends on the server's capacity. • Saved snapshots are not affected by reboots of the PX4. • Configure the following fields: * *Server URL* - the FTP server's path * *Username* - for server access * *Password* - for server access

1. Click Save.

Warning: Before disconnecting or powering off any remote server where the webcam snapshots are being stored, you must first change the storage settings, or the connectivity issue of the remote server may degrade the performance of the PX4 web interface. If this issue occurs, first restore the connectivity of the remote server and then change the storage settings of the webcam snapshots.

► *Tip for notifications showing the snapshots path on FTP:*

If you are using SNMP to retrieve data, you can make PX4 automatically send a notification containing the full path or URL to the snapshots saved onto FTP with this SNMP code: `webcamStorageUploadStarted`.

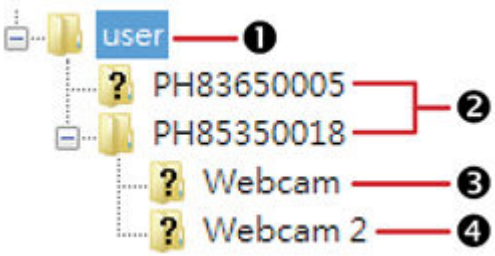
Identifying Snapshots Folders on Remote Servers

If saving snapshots onto a remote server, you can access those snapshots via an appropriate third-party application, such as an FTP client.

All snapshots are saved as JPEG and named according to the date and time when saving the snapshots. Note that the date and time of the filename are based on the time zone of the PX4 rather than that of the computer or mobile device you are operating.

Tip: To check the time zone, choose Device Settings > Date/Time.

The structure of a snapshots folder looks similar to the diagram below.



Number	Folder name description
❶	User-defined parent directory, whose name depends your server settings, such as your FTP configuration.
❷	Serial number of your PX4 device where the webcam is connected. For example, *PH85350018*. • View your serial number in Device Information.
❸	The name of the webcam that your PX4 detects first. This is the folder where the snapshots captured by the first webcam are stored. • The first webcam's default name is "Webcam". • You can customize the webcam's name, which will change the snapshots folder's name. • If the webcam's location is important, you can customize the webcam's name based on its location when configuring PX4 to save snapshots onto a remote server.
❹	The name of the webcam that your PX4 detects later, if an additional webcam is connected. This is the folder where the snapshots captured by the second webcam are stored. • The second webcam's default name is "Webcam 2". • Changing this webcam's name also changes the second snapshots folder's name. • If the webcam's location is important, you can customize the webcam's name based on its location when configuring PX4 to save snapshots onto a remote server.

Note: It is suggested to customize a webcam's name "prior to" saving snapshots on the remote server. In case you change the webcam's name after saving any snapshots, PX4 will create a new folder with the new webcam name while keeping the old folder with the old name.

SmartLock and Card Reader

Raritan's SmartLock kits provide several cabinet access control solutions.

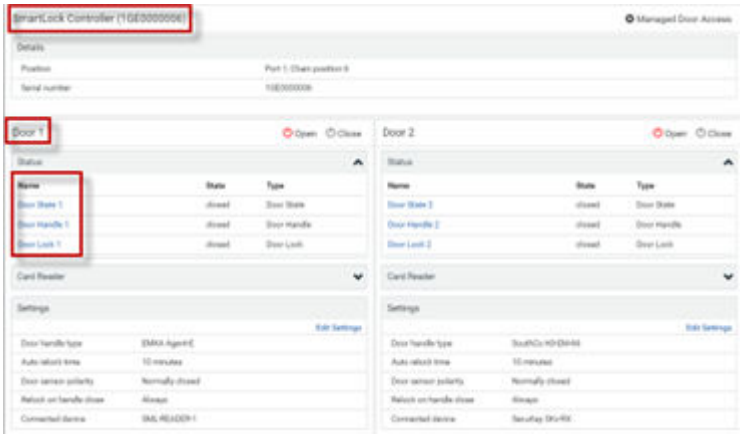
If you have purchased a SmartLock kit with the door handle controller "DX2-DH2C2", both menu items "SmartLock" and "Card Readers" will appear in the menu after connecting and configuring properly DX2-DH2C2 and the door handles included in the kit.

Note that "SmartLock" appears only when your door handles are connected via DX2-DH2C2, but "Card Readers" appears as long as any card reader is detected, whether standalone USB card reader or a card reader integrated with the door handles.

SmartLock

To open the SmartLock page, choose SmartLock in the *Menu*.

The page shows information of all DX2-DH2C2 modules connected, including its serial number, position and its door configuration. When primary units and/or link units have SmartLock controllers connected, this page includes all door information for both.



On this page you can:

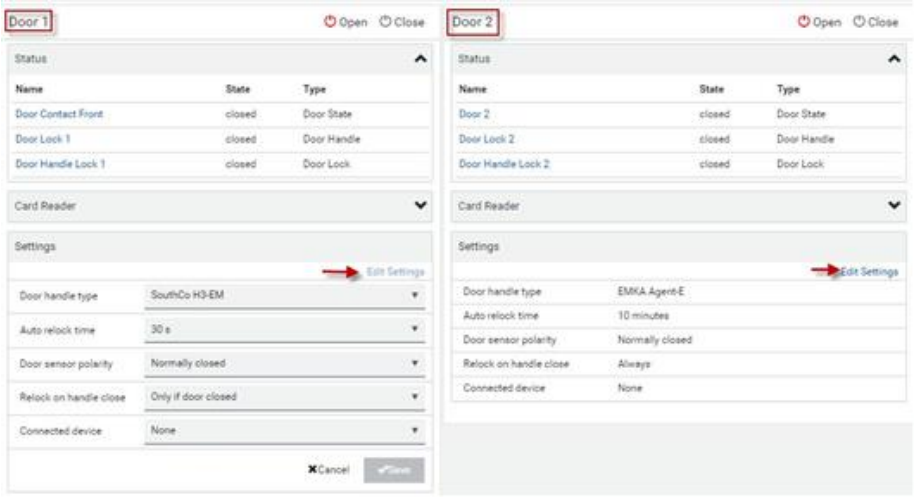
- View the status of the cabinet door and card reader.

  Note: Data of "external" USB card readers is shown on the Card Readers page.

- Configure the doors connected to DX2-DH2C2. You must set this because the types of connected door handles are not automatically detected.
- Control the doors connected to DX2-DH2C2.
- Manage the door access.

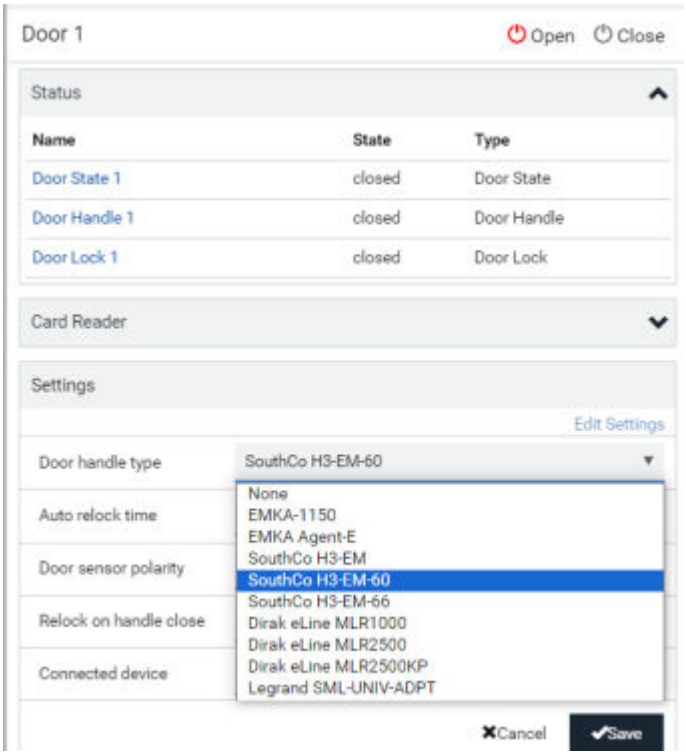
► *To configure the doors:*

There are two door sections per DX2-DH2C2 because a DX2-DH2C2 has two door handle ports.



Raritan
A brand of legrand

1. Click Edit Settings in the Settings section.
2. In the 'Door handle type' field, select the door handle type you are using.
   - If your specific Southco H3-EM model is listed, select it. For all other supported Southco H3-EM models, select "Southco H3-EM".



3. Make changes to the remaining fields as needed, then click Save.

Section	Description
Auto Relock Time	• Specify how long the lock can remain open after someone opens the door handle lock via smart card or remote control without the handle being opened during that period. When the timeout expires, the lock will be automatically closed. Default is 600 seconds (that is, 10 minutes).
Door sensor polarity	• Choose the correct setting based on the type of contact closure sensors used to monitor the door: • Normally closed: The contact is closed (conducting) when the door is closed and open (not conducting) when the door is open. Default. • Normally open: The contact is not conducting when the door is closed and is conducting when the door is open. • Note: For both normally closed and normally open sensors, the reported state is "open" when the door is open and "closed" when the door is closed.
Relock on Handle Close	• This setting controls auto-locking. Select "Only if door closed" to delay auto-locking until "Door State" and "Door Handle State" are both verified as "Closed". Select "Always" to relock automatically.

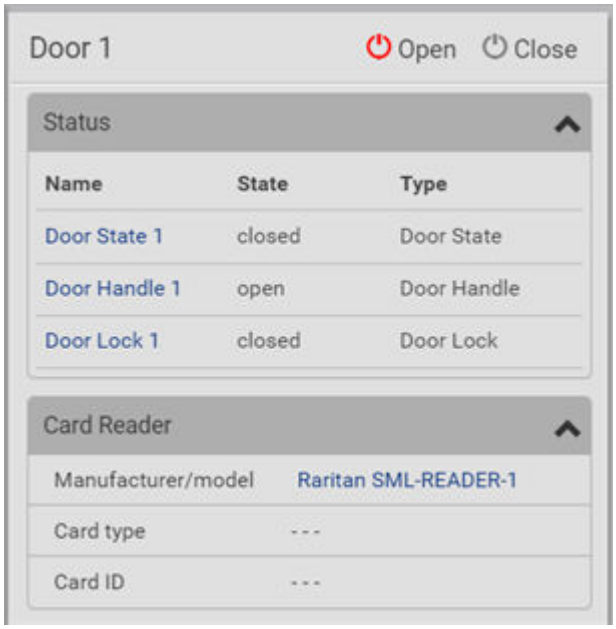
Section	Description
Connected Device	• If your door handle has a connected device, such as a keypad, select it from the list.

► *To manage the door access:*

"Managed Door Access" link provides access to "Door Access Rules" where you can create new rules. Door Access (on page 289)

Door Status and Control

After configuring the door handle type properly, you can see the Status and Card Reader sections.



► *To view the status of the door and card reader:*

Section	Description
Status	Shows all sensor states detected by DX2-DH2C2, including: • *Door State*: States of contact closure sensors connected to DX2-DH2C2. Contact closure sensors detect whether the door is physically opened or closed. • *Door Handle*: States of door locks integrated with the door handles. • *Door Lock*: States of the door handle locks. Door locks and door handle locks are interrelated so their states are changed one after another. The door handle lock is opened first and then the door lock. Exception: If you manually open the door lock with the key shipped with your door handle, the Door Lock state will enter the open state while the Door Handle Lock state remains closed.
Card Reader	Shows the data of the smart card scanned by the internal or external card reader accompanying each door handle connected to DX2-DH2C2.

Tip: All sensors of the connected door handles are also listed on the Peripherals page. The same Card Reader information is also available on the Card Reader page.

► *To control the door:*

Per default, only one door handle can be opened at the same time so you must close one door before opening another. To increase the upper limit of concurrently opened doors, go to the Peripherals page.

1. Go to the proper door section, and click Open or Close.

2. Confirm the operation when prompted.
3. Now you can physically open or close the door.

► *Door Terms:*

The following terms and definitions are helpful when discussing doors, door handles, and locks. Note that all door sensors also display in the Peripherals page.

- SmartLock Controllers: DX2-DH2C2
- Door Handle Assembly: Door Handle and Door Lock which are connected to the SmartLock controller 8 pin connector, for example "door handle 1".
- Door: Door is the same as "Door Handle Assembly", but with optional contact closure sensor that is connected to the SmartLock controller connector. The contact closure sensor status describes whether the cabinet door is open or closed.
- Door Handle: The small grip on the front of the Door Handle Assembly, which is used to mechanically open the door by hand if it's unlocked. Sensor status describes if the Door Handle is pulled out (open) or closed.
- Door Lock: The small lock actuator inside of the Door Handle Assembly which locks or unlock the Door Handle. Sensor status describes if the Door Handle is unlocked or locked.

Card Readers

To open the Card Readers page, choose Card Readers in the *Menu*.

This page lists all card readers connected, including:

- Standalone USB card readers
- Card readers integrated with door handles

When a user scans a smart card with the card reader, the card's type and ID are retrieved and shown in the corresponding Card Type and Card ID column. If no data is shown in the two columns, it means the scanned card may not be supported by the card reader.

Tip: You can use a third-party application, such as Power IQ, to retrieve the card's data to perform security features like cabinet access control. Refer to that application's user documentation for more information.

► *Door handle-integrated card readers:*

- This type of card reader is integrated in the door handle, which is any series below:
  - Emka Agent E
  - SouthCo H3-EM
  - Dirak eLine MLR 2500

Note: Not every SouthCo H3-EM door handle has a card reader integrated.

- It is connected via the DX2-DH2C2 module.
- The Channel column indicates which door handle port (channel) it is connected to.
- Note that the serial number displayed for this card reader is the same as DX2-DH2C2's serial number.

  Each DX2-DH2C2 module can show two card readers because they have two ports for connecting two door handles with card readers integrated.

► *Standalone USB card readers:*

- It is directly connected to PX4.
- The Channel column does not show any data.

Using SNMP

This SNMP section guides you in configuring PX4 for integration with an SNMP manager. PX4 can be set up to send traps or informs to the SNMP manager, enabling real-time notifications. Additionally, it can receive GET and SET commands to retrieve status updates and adjust basic settings efficiently.

In This Chapter

Enabling and Configuring SNMP. 398
SNMPv3 Notifications. 399
SNMPv2c Notifications. 401
Downloading SNMP MIB. 401
SNMP Gets and Sets. 402

Enabling and Configuring SNMP

To enable communication with an SNMP manager, you must activate SNMP protocols on PX4. By default, SNMP functionality is disabled.

SNMP v3 protocol supports encrypted communication to enhance security. To utilize this feature, configure users with SNMP v3 access permissions and specify both an Authentication Pass Phrase and a Privacy Pass Phrase. These pass phrases serve as shared secrets between SNMP and PX4, ensuring secure communication.

Important: You must download the SNMP MIB for your PX4 to use with your SNMP manager.

► *To enable SNMP v1/v2c and/or v3 protocols:*

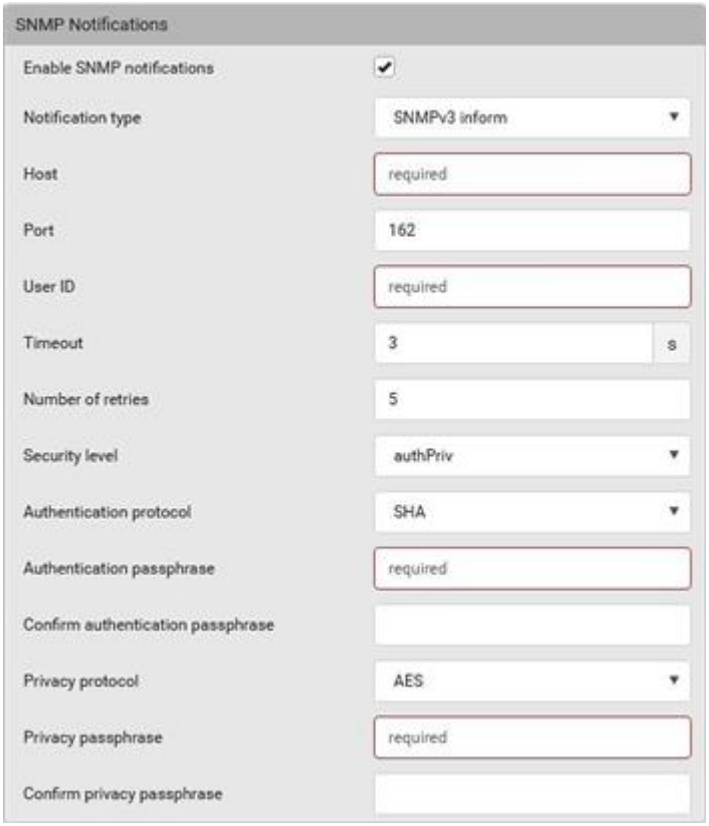
1. Choose Device Settings > Network Services > SNMP.
2. In the SNMP Agent section, enable SNMP v1/v2c or SNMP v3, and configure related fields, such as the community strings.
   - If SNMP v3 is enabled, you must determine which users shall have the SNMP v3 access permission.

► *To configure users for SNMP v3 access:*

1. Choose User Management > Users.
2. Create or modify users to enable their SNMP v3 access permission.
   - If authentication and privacy is enabled, configure the SNMP password(s) in the user settings.

SNMPv3 Notifications

1. Choose Device Settings > Network Services > SNMP.
2. In the SNMP Agent, make sure the Enable SNMP v1/v2c checkbox is selected.
3. In the SNMP Notifications section, make sure the 'Enable SNMP notifications' checkbox is selected.



4. Select 'SNMPv3 trap' or 'SNMPv3 inform' as the notification type.
5. For SNMP TRAPs, the engine ID is prepopulated.
6. Type values in the following fields.

Field	Description
Host	The IP address of the device(s) you want to access. This is the address to which notifications are sent by the SNMP agent.
Port	The port number used to access the device(s).
User ID	User name for accessing the device. • Make sure the user has the SNMP v3 access permission.
Timeout	The interval of time, in seconds, after which a new inform communication is resent if the first is not received. • For example, resend a new inform communication once every 3 seconds.
Number of retries	Specify the number of times you want to resend the inform communication if it fails. • For example, inform communications are resent up to 5 times when the initial communication fails.
Security level	Three types are available. • noAuthNoPriv - neither authentication nor privacy protocols are needed. • authNoPriv - only authentication is required. • authPriv - both authentication and privacy protocols are required.
Authentication protocol, Authentication passphrase, Confirm authentication passphrase	The three fields are available when the security level is set to AuthNoPriv or authPriv. • Select the authentication protocol - MD5 or SHA • Enter the authentication passphrase
Privacy protocol, Privacy passphrase, Confirm privacy passphrase	The three fields are available when the security level is set to authPriv. • Select the Privacy Protocol - DES or AES • Enter the privacy passphrase and then confirm the privacy passphrase

7. Click Save.

SNMPv2c Notifications

1. Choose Device Settings > Network Services > SNMP.
2. In the SNMP Agent, make sure the Enable SNMP v1/v2c checkbox is selected.
3. In the SNMP Notifications section, make sure the 'Enable SNMP notifications' checkbox is selected.

4. Select 'SNMPv2c trap' or 'SNMPv2c inform' as the notification type.
5. Type values in the following fields.

Field	Description
Timeout	The interval of time, in seconds, after which a new inform communication is resent if the first is not received. • For example, resend a new inform communication once every 3 seconds.
Number of retries	The number of times you want to resend the inform communication if it fails. • For example, inform communications are resent up to 5 times when the initial communication fails.
Host	The IP address of the device(s) you want to access. This is the address to which notifications are sent by the SNMP agent. You can specify up to 3 SNMP destinations.
Port	The port number used to access the device(s).
Community	The SNMP community string to access the device(s). The community is the group representing the PX4 and all SNMP management stations.

6. Click Save.

Downloading SNMP MIB

You must download an appropriate SNMP MIB file for successful SNMP communications. Always use the latest SNMP MIB downloaded from the current firmware of your PX4.

You can download the MIBs from two different pages of the web interface.

► *MIB download via the SNMP page:*

1. Choose Device Settings > Network Services > SNMP.
2. Click the Download MIBs title bar.

3. Select the desired MIB file to download.
   - PDU2-MIB: The SNMP MIB file for PX4 management.
   - ASSETMANAGEMENT-MIB: The SNMP MIB file for asset management.
4. Click Save to save the file onto your computer.

► *MIB download via the Device Information page:*

1. Choose Maintenance > Device Information.
2. In the Information section, click the desired download link:
   - PDU2-MIB
   - ASSETMANAGEMENT-MIB
3. Click Save to save the file onto your computer.

SNMP Gets and Sets

In addition to sending notifications, the PX4 is able to receive SNMP get and set requests from third-party SNMP managers.

- Get requests are used to retrieve information about the PX4, such as the system location, and the current on a specific outlet.
- Set requests are used to configure a subset of the information, such as the SNMP system name.

Note: The SNMP system name is the PX4 device name. When you change the SNMP system name, the device name shown in the web interface is also changed.

The PX4 does NOT support configuring IPv6-related parameters using the SNMP set requests.

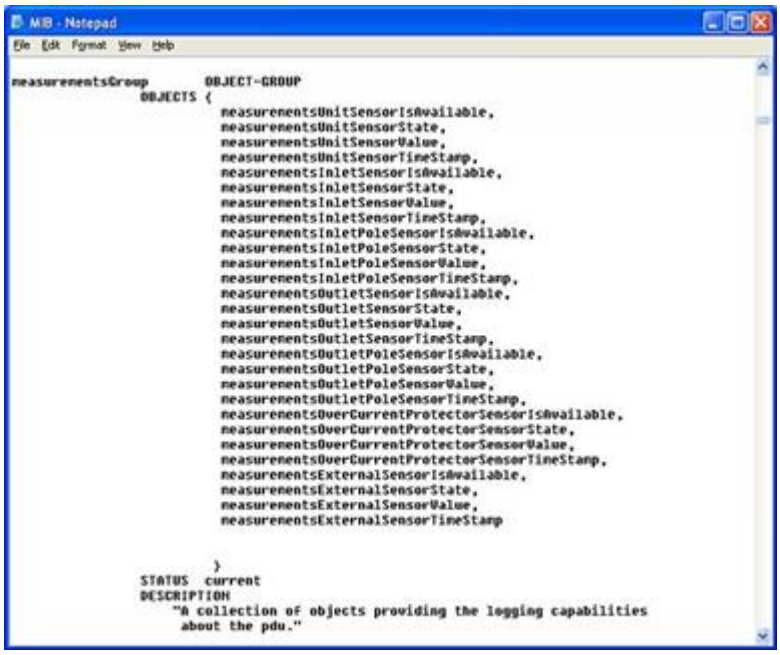
Valid objects for these requests are limited to those found in the SNMP MIB-II System Group and the custom PX4 MIB.

The MIB File

An SNMP MIB file describes the SNMP functions.

Opening the MIB reveals the custom objects that describe the PX4 system at the unit level as well as at the individual-outlet level.

As standard, these objects are first presented at the beginning of the file, listed under their parent group. The objects then appear again individually, defined and described in detail.



For example, the measurementsGroup group contains objects for sensor readings of PX4 as a whole. One object listed under this group, measurementsUnitSensorValue, is described later in the MIB as "The sensor value". pduRatedCurrent, part of the configGroup group, describes the PDU current rating.

SNMP Sets and Thresholds

Some objects can be configured from the SNMP manager using SNMP set commands. Objects that can be configured have a MAX-ACCESS level of "read-write" in the MIB.

These objects include threshold objects, which cause the PX4 to generate a warning and send an SNMP notification when certain parameters are exceeded. See Sensor Threshold Settings for a description of how thresholds work.

Note: When configuring the thresholds via SNMP set commands, ensure the value of upper critical threshold is higher than that of upper warning threshold.

Configuring NTP Server Settings

Using SNMP, you can change the following NTP server-related settings in the unitConfigurationTable:

- Enable or disable synchronization of the device's date and time with NTP servers (synchronizeWithNTPServer)
- Enable or disable the use of DHCP-assigned NTP servers if synchronization with NTP servers is enabled (useDHCPProvidedNTPServer)
- Manually assign the primary NTP server if the use of DHCP-assigned NTP servers is disabled (firstNTPServerAddressType and firstNTPServerAddress)
- Manually assign the secondary NTP server (optional) (secondNTPServerAddressType and secondNTPServerAddress)

Tip: To specify the time zone, use the CLI or web interface instead.

When using the SNMP SET command to specify or change NTP servers, it is required that both the NTP server's address type and address be set in the command line simultaneously.

For example, the SNMP command to change the primary NTP server's address from IPv4 (192.168.84.84) to host name looks similar to the following:

```
snmpset -v2c -c private 192.168.84.84 firstNTPServerAddressType = dns
firstNTPServerAddress = "angu.pep.com"
```

Retrieving Energy Usage

You can discover how much energy an IT device consumes by retrieving the Active Energy for the outlet this IT device is plugged into. The Active Energy values are included in the outletSensorMeasurementsTable, along with other outlet sensor readings.

Using the Command Line Interface

This section explains how to use the command line interface (CLI) to administer the PX4.

Note that available CLI commands are model dependent.

CLI commands are case sensitive.

The CLI can be used to:

- Reset
- Display the device and network information, such as the device name, firmware version, IP address, and so on
- Configure the device 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. To enable Telnet, go to Device Settings > Network Services > Telnet.

In This Chapter

Logging in to CLI. 405
Tips for Using the CLI. 408
Showing Information. 411
Configuring the Device and Network. 440
Network Troubleshooting in Diagnostic Mode. 565

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 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

Tip: For a USB connection, you can determine the COM port by choosing Control Panel > System > Hardware > Device Manager, and locating the "Device Serial Console" under the Ports group.

3. In the communications program, press Enter to send a carriage return to the PX4. The Username prompt appears.
4. Type a name and press Enter. The name is case sensitive. Then you are prompted to enter a password.
5. Type a password and press Enter. The password is case sensitive.

After properly entering the password, the PX4 name appears at the prompt.

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 using commands.

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.

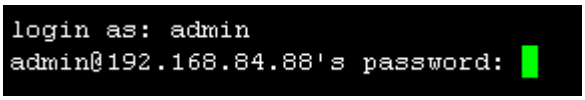
► *To log in using SSH or Telnet:*

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

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.



4. Type a password and press Enter. The password is case sensitive.
5. After properly entering the password, the PX4 name appears at the prompt.

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.

Different CLI Modes and Prompts

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

- User Mode: When you log in as a normal user, who may not have full permissions to configure the PX4, the > prompt appears.
- Administrator Mode: When you log in as an administrator, who has full permissions to configure the PX4, 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 PX4 device and network configurations. See Configuring the Device and Network (on page 440).
- 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. See Network Troubleshooting in Diagnostic Mode (on page 565).

Closing a Local Connection

Close the window or terminal emulation program when you finish accessing the PX4 over the local connection.

When accessing or upgrading multiple PX4 devices, do not transfer the local connection cable from one device to another without closing the local connection window first.

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.

Tips for Using the CLI

The ? Command for Showing Available Commands

When you are not familiar with CLI commands, you can press the ? key at anytime 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 ?
```


Raritan
A brand of legrand

► *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 ?
```

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:*

1. 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.
2. Press Tab or Ctrl+i until the complete command appears.
3. 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.
- 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.

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.

```
config:# 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.

```
config:#  sensor ocp 2 current upperCritical disable upperWarning 15
```


Raritan
A brand of legrand

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.

```
config:# 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.

Showing Information

You can use the show commands to view current settings or the status of the PX4 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.

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. Tip: You can also type the command without adding this option "all" to get the same data.
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 PX4 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.

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. Tip: You can also type the command without adding this option "all" to get the same data.
A specific asset strip number	Displays the settings of the asset strip connected to the specified FEATURE port number. For the PX4 device with only one FEATURE port, the valid number is always 1.

Authentication Settings

► *General authentication settings:*

This command displays the authentication settings of the PX4, including LDAP, Radius,and TACACS+ 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> details
```

► *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
```

► *One TACACS+ server's settings:*

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

```
#  show authentication tacplusServer <server_num>
```

-- OR--

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

Variables:

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

Displayed information:

- Without specifying any server, PX4 shows the authentication type and a list of LDAP, Radius, and TACACS+ servers that have been configured.
- When specifying a server, only that server's configuration is displayed. For LDAP server IP address/ hostname, server type, security, and port number are displayed, whereas Radius or TACCS+ servers show their IP address/host name Authentication type and Port/s.

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. Whereas Radius and Tacacs+ servers show accounting, timeout, retries, and shared secret values.

Blade Slot

This command shows the blade extension information,such as number of blade extensions connected to the rack unit on the asset strip.

```
# show bladeSlot [<assetstrip>] [<rackunit>]
  [<bladeslot>]
```

- assetstrip Asset strip index (1..99) [1]
- rackunit Rack unit index (1..99) [1]
- bladeslot Blade slot index (1..99 or all) [all]

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.

Clearing Information

You can use the clear commands to remove unnecessary data.

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.

Date and Time Settings

This command shows the current date and time settings on the PX4.

```
#         show time
```

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

```
#      show time details
```

Note: If details is not specified, only the deviceTime, timeZone and setupMethod will be displayed.

Default Measurement Units

This command shows the default measurement units applied to the PX4 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. See Existing User Profiles (on page 419) for the preferred measurement units for a specific user.

Device Configuration

This command shows the device configuration, such as the device name, firmware version, model type and upper limit of active powered dry contact actuators. The CLI is supported by various Xerus products.

```
#           show pdu
```

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

```
#      show pdu details
```

Variables:

- pdu is one of the options: pdu, src, pmc or ts.

Note: Your Xerus product may not support all commands.

Raritan
A brand of legrand

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 PX4 web interface.

Displayed information:

- Without the parameter "details," only the reading, threshold, deassertion 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.

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.

Event type	Description
sensor	Internal or external sensor events, such as state changes of any sensors.
serverMonitor	Server-monitoring records, such as a server being declared reachable or unreachable.
assetManagement	Raritan asset management events, such as asset tag connections or disconnections.
modem	Modem-related events.
timerEvent	Scheduled action events.
webcam	Events for webcam management, if available.
cardReader	Events for card reader management, if available.

Existing Roles

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

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

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. Tip: You can also type the command without adding this option "all" to get the same data.
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.

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. Tip: You can also type the command without adding this option "all" to get the same data.
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.

Environmental Sensor Information

This command syntax shows the external 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. Tip: You can also type the command without adding this option "all" to get the same data.
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 PX4 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.

- 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 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 Tip: You can also type the command without adding this option "all" to get the same data.

Displayed information:

- Without the parameter "details," only the default upper and lower thresholds, deassertion 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.

Front Panel Permissions

This command shows the front panel permissions applied to the PX4.

```
#   show frontPanelPermission
```

Switch Peripheral Actuator: no

Acknowledge Alarm: no

Factory Reset: no

Mute Beeper: yes

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, or a label.

Option	Description
all	Displays the information for all inlets. Tip: You can also type the command without adding this option "all" to get the same data.
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.

Inlet Sensor Threshold Information

This command is NOT available for an in-line monitor (PX3-3000 series).

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, deassertion 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 PX4 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	Supported on PXC and Legrand PDU only • three-phase models also support pole-level peak current • models with metered breakers also support breaker-level peak current
reactivePower	Reactive power sensor	
displacementPowerFactor	Displacement power factor sensor	

Sensor type	Description	
residualCurrent	RCM current sensor • 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.	

Note: For information on RCM Type A and B sensors, see RCM Current Sensor.

Inlet Pole Sensor Threshold Information

This command is only available for a three-phase PDU except for an in-line monitor (PX3-3000 series).

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

Sensor type	Description
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, deassertion 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 PX4 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	Supported on PXC and Legrand PDU only • three-phase models also support pole-level peak current • models with metered breakers also support breaker-level peak current
reactivePower	Reactive power sensor	
displacementPowerFactor	Displacement power factor sensor	
residualCurrent	RCM current sensor • 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.	

Note: For information on RCM Type A and B sensors, see RCM Current Sensor.

Linking

This command syntax shows the PDU linking settings

```
#       show linking
```

Load Shedding Settings

This section applies to outlet-switching capable models only.

This command shows the load shedding settings.

```
#     show loadshedding
```

Displayed information:

- The load shedding state is displayed along with non-critical outlets.

Note: The load shedding mode is associated with critical and non-critical outlets. To specify critical and non-critical outlets through CLI, see Specifying Non-Critical Outlets (on page 462).

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
```

Network Diagnostics

This command shows the network diagnostics (Wi-Fi/802.1x) log.

```
#     show network diagLog limit <limit>
```

Variable:

- <limit> Number of log lines to display (1..10000 or all)

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 PX4 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. Tip: You can also type the command without adding this option "all" to get the same data. That is, *show network ip interface*.

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
```


Raritan
A brand of legrand

► *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 PX4 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.
all	Show the IPv4 or IPv6 configuration of all interfaces. Tip: You can also type the command without adding this option "all" to get the same data. That is, *show network ipv4 interface*.

Network Diagnostics

► *Show network diagnostics log:*

This command shows the network diagnostics (Wi-Fi/802.1x) log.

```
#    show network diagLog
```

► *Clear network diagnostics log:*

This command clear the network diagnostics log.

```
#    clear networkDiagLog
```

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 PX4 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. Tip: You can also type the command without adding this option "all" to get the same data. That is, *show network interface*.

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. Tip: You can also type the command without adding this option "all" to get the same data.
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.
redfish	Only displays the redfish service settings.
zeroconfig	Only displays the settings of the zero configuration advertising.

Network Connections Diagnostic Log

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

```
#    show network diagLog
```

Outlet Group Information

This command syntax shows the outlet group information.

```
#    show outletgroups <n>
```

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

```
#   show outletgroups <n> details
```

Variables:

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

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

Displayed information:

- Without the parameter "details," only the group's name, the group's index number, member outlets and the group's power state (if it is a switched PDU) are displayed.
- With the parameter "details," more inlet information is displayed in addition to the above outlet group information, such as each member outlet's power state and the group's active energy.

Tip: PX4 allows you to assign the same name to diverse outlet groups. If this really occurs, you still can identify different groups through their unique index numbers.

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

Displayed information:

- Without the parameter "details," only the outlet name and state are displayed.
- With the parameter "details," more outlet information is displayed in addition to the state, such as rated current, voltage, active power, active energy, and outlet settings.

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
```

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

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

Variables:

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

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

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.
- For Raritan's outlet-metered models that support "outlet peak current" sensors, information indicating which outlet MAY cause the OCP-tripped event is available with this command. See Possible OCP-Tripped Root Cause.

Outlet Pole Sensor Threshold Information

This command is available for an in-line monitor only, including PX2-3000 and PX3-3000 series.

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

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

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

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

Variables:

- <n> is the number of the outlet whose pole sensors you want to query.
- <p> is the label of the outlet 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, deassertion hysteresis and assertion delay settings of the specified outlet 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.

Outlet Group Threshold Information

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

```
#  show sensor outletgroup <ID> <sensor type>
```

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

```
#  show sensor outletgroup <ID> <sensor type> details
```

Variables:

- <ID> is an outlet group's index number.
- <sensor type> is one of the following sensor types:

Sensor type	Description
activePower	An outlet group's active power sensor
activeEnergy	An outlet group's active energy sensor

For definitions on an outlet group's sensors, see Outlet Groups.

Displayed information:

- Without the parameter "details," only the sensor reading, state, threshold, deassertion hysteresis and assertion timeout settings of the specified group sensor are displayed.
- With the parameter "details," more sensor information is displayed, including resolution and range.

Outlet Sensor Threshold Information

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

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

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

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

Variables:

- <n> is the number of the outlet whose sensors you want to query.
- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor

Sensor type	Description
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor
lineFrequency	Line frequency sensor

Displayed information:

- Without the parameter "details," only the sensor reading, state, threshold, deassertion hysteresis and assertion timeout settings of the specified outlet 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.

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, deassertion 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.

Peripheral Devices Settings

This command shows peripheral devices settings, including Z coordinate format of external sensors, device altitude, peripheral device auto management, maximum number of concurrently active powered dry contacts, and muting of other door handle.

```
#   show peripheralDevicesSetup
```

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
```

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 PX4 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. Tip: You can also type the command without adding this option "all" to get the same data.
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.

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. Tip: You can also type the command without adding this option "0" to get all data.
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
```

For details, see Hardware Issue Detection.

Security Settings

This command shows the security settings of the PX4.

```
#      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, HTTPS encryption is displayed and current FIPs mode status.
- 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) and FIPs Mode status.

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.

Configuring the Device and Network

To configure the device or network settings through the CLI, it is highly recommended to log in as the administrator so that you have full permissions. If you enter configuration mode from user mode, you may have limited permissions to make configuration changes.

To configure any settings, enter the configuration mode. Configuration commands are case sensitive.

► *To enter configuration mode:*

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

► *To quit the configuration mode, use either "apply" or "cancel" command:*

```
config:#                    apply
```

-- OR --

```
config:#                    cancel
```

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

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 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"
```

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 PX4 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 PX4 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
```

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:*

```
config:# 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 only.
radius	Enable Radius authentication only.
tacplus	Enable TACACS+ authentication only.

- <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.

► *Add a new LDAP server:*

```
config:# 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*. 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: *anonymouseBind*, 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:*

```
config:# 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:*

```
config:# 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 • 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 • 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:*

```
config:# authentication ldap add op-ldap.raritan.com 389 openldap none
         anonymousBind dc=raritan,dc=com uid inetOrgPerson
```

► *A Microsoft Active Directory server:*

```
config:# 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."*

```
config:# 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: Select and copy the content including the starting line containing "BEGIN CERTIFICATE" and the ending 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.

```
config:# 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 Authentication 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.

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:

```
config:#   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.

▶ *Parameters:*

Parameters	Description
host <host>	Change the IP address or host name. • <host> is the new IP address or host name.
port <port>	Change the TCP port number. • <port> is the new TCP port number.
serverType <ldap_type>	Change the server type. • <ldap_type> is the new type of the LDAP server. • <ldap_type> values include: `openldap` and `activeDirectory`.
securityType <security>	Change the security type. • <security> is the new security type. • <security> values include: `none`, `startTls`, and `ssl`
bindType <bind_type>	Change the bind type. • <bind_type> is the new bind type. • <bind_type> values include: `anonymousBind` and `authenticatedBind`.
searchBaseDN <base_DN>	Change the base DN for search. • <base_DN> is the new base DN for search.
loginNameAttribute <login_name_att>	Change the login name attribute. • <login_name_att> is the new login name attribute.
userEntryObjectClass <user_entry_class>	Change the user entry object class. • <user_entry_class> is the new user entry class.
userSearchSubfilter <user_search_filter>	Change the user search subfilter. • <user_search_filter> is the new user search subfilter.

Parameters	Description
adDomain <AD_domain>	Change the Active Directory Domain name. • <AD_domain> is the new domain name of the Active Directory.
verifyServerCertificate <verify_cert>	Enable or disable the certificate verification. • <verify_cert> enables or disables the certificate verification feature. • Available values include: `true`, `false`
certificate	Re-upload a different certificate. a. First add the "certificate" parameter to the command, and press Enter. b. The system prompts you for the input of the certificate. c. 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. • <allow_exp_cert> determines whether to accept an expired or not valid yet certificate • <allow_exp_cert> values include: `true`, and `false`
bindDN <bind_DN>	Change the bind DN. • <bind_DN> is the new bind DN.
bindPassword	Change the bind DN password. a. First add the "bindPassword" parameter to the command, and press Enter. b. The system prompts you for the input of the password. c. Type the password and press Enter.
sortPosition <position>	Change the priority of the server (that is, resorting). • <position> is the new sequential number of the server in the LDAP server list.

► *Examples:*

- Change the IP address of the 1st LDAP server

```
config:#    authentication ldap modify 1 host 192.168.3.3
```

- Change both the IP address and TCP port of the 1st LDAP server

```
config:#  authentication ldap modify 1 host 192.168.3.3 port 633
```

- Change the IP address, TCP port and the type of the L1st DAP server

```
config:# authentication ldap modify 1 host 192.168.3.3 port 633
         serverType activeDirectory
```


Raritan
A brand of legrand

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:*

```
config:# 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:*

1. After executing the above Radius command, the system automatically prompts you to enter the shared secret.
2. Type the secret and press Enter.
3. Re-type the same secret and press Enter.

► *Example:*

```
config:#  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:*

```
config:#   authentication radius modify <server_num> host <host>
```

► *Change the Radius authentication type:*

```
config:#  authentication radius modify <server_num> authType <rds_type>
```

► *Change the authentication port:*

```
config:#  authentication radius modify <server_num> authPort <auth_port>
```

► *Change the accounting port:*

```
config:# authentication radius modify <server_num> accountPort <acct_port>
```

► *Change the timeout value:*

```
config:#  authentication radius modify <server_num> timeout <timeout>
```

► *Change the number of retries:*

```
config:#  authentication radius modify <server_num> retries <retries>
```

► *Change the shared secret:*

```
config:#    authentication radius modify <server_num> secret
```

► *Change the priority of the specified server:*

```
config:# authentication radius modify <server_num> sortPositon <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:*

1. After executing the above Radius command, the system automatically prompts you to enter the shared secret.
2. Type the secret and press Enter.
3. Re-type the same secret and press Enter.

► *Example:*

```
config:#  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.

TACACS+ Settings

All TACACS+ related commands begin with *authentication tacplus*.

If you enable TACACS+ authentication, you must add at least one TACACS+ server. Later you can modify or delete any existing TACACS+ server as needed.

Adding TACACS+ Server

You can repeat the following commands to add TACACs+ server one by one.

► *Command syntax:*

```
config:# authentication tacplus add <host> [port <port>] [type ] [timeout
         <timeout>] [retries <retries>] [disableAcct <disableacct>]
```

Variables:

- <host> is the IP address or host name of the TACACS+ server.
- <port> is the port number (Default: 49) (1..65535).
- is one of the authentication type (Default: msChap) (ascii/pap/chap/msChap).

Type	Description
ascii	ASCII
`chap`	CHAP
`pap`	PAP
`msChap`	MSCHAP

- <timeout> is the timeout value in seconds. It ranges between 1 to 60 seconds.
- <retries> is the number of retries. It ranges between 0 to 5.
- <disableAcct> is disable Accounting (true/false).

► *To enter the shared secret:*

1. After executing the above TACCS+ command, the system automatically prompts you to enter the shared secret.
2. Type the secret and press Enter.
3. Re-type the same secret and press Enter.

- *Example:*

```
config:# authentication tacplus add 192.168.7.99 port 49 type chap timeout
         5 retries 3 disableAcct false
```

Modifying an Existing TACACS+ Server

You can modify one or multiple parameters of an existing TACACS+ server, or change the priority or sequence of existing servers in the server list.

- *Change the IP address or host name:*

```
config:#    authentication tacplus modify <index> host <host>
```

- *Change the authentication type:*

```
config:#     authentication tacplus modify <index> type
```

- *Change the authentication port:*

```
config:#    authentication tacplus modify <index> port <port>
```

- *Change the timeout value:*

```
config:#   authentication tacplus modify <index> timeout <timeout>
```

- *Change the number of retries:*

```
config:#   authentication tacplus modify <index> retries <retries>
```

- *Disable or Enable the account:*

```
config:# authentication tacplus modify <index> disableAcct <disableacct>
```

- *Change the shared secret:*

```
config:#     authentication tacplus modify <index> secret
```

► *Change the priority of the specified server:*

```
config:#  authentication tacplus modify <index> sortPositon <position>
```

Tip: You can add more than one parameters to the command. For example, "`authentication tacplus modify <index>` host <host> `type` port <port> `disableAcct <disableacct> …`".

Variables:

- <index> is the sequential number of the specified server in the TACACS+ server list.
- <host> is the new IP address or host name of the TACACS+ server.
- <port> is the new authentication port number.
- is one of the TACACS+ authentication types: *pap, chap, msChapV2*.
- <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.
- <disableacct> is to disable or enable the account.

► *To enter the shared secret:*

1. After executing the above TACACS+ command, the system automatically prompts you to enter the shared secret.
2. Type the secret and press Enter.
3. Re-type the same secret and press Enter.

► *Example:*

```
config:# authentication tacplus modify 1 host 192.168.25.1 port 49 type
         pap timeout 5 retries 3 disableAcct False
```

Removing an Existing TACACS+ Server

This command removes an existing TACACS+ server from the server list.

```
config:#   authentication tacplus delete <index>
```


Raritan
A brand of legrand

Variables:

- <index> is the sequential number of the specified server in the TACACS+ server list.

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:*

```
config:#  defaultThresholds <sensor type> upperCritical <value>
```

▶ *Set the Default Upper Warning Threshold for a specific sensor type:*

```
config:#  defaultThresholds <sensor type> upperWarning <value>
```

▶ *Set the Default Lower Critical Threshold for a specific sensor type:*

```
config:#  defaultThresholds <sensor type> lowerCritical <value>
```

▶ *Set the Default Lower Warning Threshold for a specific sensor type:*

```
config:#  defaultThresholds <sensor type> lowerWarning <value>
```

▶ *Set the Default Deassertion Hysteresis for a specific sensor type:*

```
config:#  defaultThresholds <sensor type> hysteresis <hy_value>
```

▶ *Set the Default Assertion Timeout for a specific sensor type:*

```
config:#  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

- <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 °C and Upper Critical threshold to 24 °C for all temperature sensors.

```
config:# defaultThresholds temperature upperWarning 20
         upperCritical 24
```

Device Configuration Commands

Device configuration command begins with pdu. You can use the pdu configuration commands to change the settings that apply to the whole device.

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

Changing the Device Name

```
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.

Setting the Outlet Relay Behavior

This section applies to outlet-switching capable models only.

This command syntax determines the relay behavior of all outlets on a PX4 model.

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

Variables:

- <option> is one of the options: *latching* or *nonLatching*

Setting the Outlet Power-On Sequence

This section applies to outlet-switching capable models only.

This command sets the outlet power-on sequence when the PDU powers up.

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

Variables:

- <option> is one of the options: *default*, or a comma-separated list of outlet numbers.

Option	Description
default	All outlets are switched ON in the ASCENDING order (from outlet 1 to the final outlet) when the PX4 powers up.

Option	Description
A comma-separated list of outlet numbers	All outlets are switched ON in the order you specify using the comma-separated list. The list must include all outlets on the PDU.

Note: Power-on sequencing is disabled in the latching mode.

Setting the Outlet Power-On Sequence Delay

This section applies to outlet-switching capable models only.

This command sets the delays (in seconds) for outlets when turning on all outlets in sequence.

```
config:# pdu outletSequenceDelay <outlet1>:<delay1>;<outlet2>:<delay2>;
          <outlet3>:<delay3>;...
```

Separate outlet numbers and their delay settings with a colon. Outlets followed by delays are separated with a semicolon.

Variables:

- <outlet1>, <outlet2>, <outlet3> and the like are individual outlet numbers or a range of outlets using a dash. For example, *3-8* represents outlets 3 to 8.
- <delay1>, <delay2>, <delay3> and the like are the delay time in seconds.

Note: Power-on sequencing is disabled in the latching mode.

Setting the PDU-Defined Default Outlet State

This section applies to outlet-switching capable models only.

This command determines the initial power condition of all outlets after powering up the PDU. This setting is used in three scenarios:

- powering up the whole PDU
- powering up a single inlet in a multi-inlet PDU (on most, but not all, multi-inlet units the outlet boards are powered through the respective inlet)
- transfer switch switches on again after being off due to e.g. internal failure

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

Variables:

- <option> is one of the options: *off*, *on* or *lastKnownState*.

Option	Description
off	Switches OFF all outlets when the PX4 powers up.
on	Switches ON all outlets when the PX4 powers up.
lastKnownState	Restores all outlets to the previous status before powering down the PX4 when the PDU powers up again.

Note: This feature does NOT take effect and cannot be configured on a PX4 device after the outlet relay is set to the "Latching" mode.

Setting the PDU-Defined Cycling Power-Off Period

This section applies to outlet-switching capable models only.

This command sets the power-off period of the power cycling operation for all outlets.

```
config:#   pdu cyclingPowerOffPeriod <timing>
```

Variables:

- <timing> is the time of the cycling power-off period in seconds, which is an integer between 0 and 3600, or *pduDefined* for following the PDU-defined timing.

Setting the Inrush Guard Delay Time

This section applies to outlet-switching capable models only.

This command sets the inrush guard delay.

```
config:#    pdu inrushGuardDelay <timing>
```

Variables:

- <timing> is a delay time between 100 and 100000 milliseconds.

Setting the Outlet Initialization Delay

This section applies to outlet-switching capable models only.

This command determines the outlet initialization delay timing on device startup. See PDU for information on outlet initialization delay.

```
config:#   pdu outletInitializationDelayOnPowerUp <timing>
```

Variables:

- <timing> is a delay time between 1 and 3600 seconds.

Note: This feature does NOT take effect and cannot be configured on a PX4 device after the outlet relay is set to the "Latching" mode.

Specifying Non-Critical Outlets

This section applies to outlet-switching capable models only.

This command determines critical and non-critical outlets. It is associated with the load shedding mode. See Load Shedding Mode.

```
config:#  pdu nonCriticalOutlets <outlets1>:false;<outlets2>:true
```

Separate outlet numbers and their settings with a colon. Separate each "false" and "true" setting with a semicolon.

Variables:

- <outlets1> is one or multiple outlet numbers to be set as critical outlets. Use commas to separate outlet numbers.

  Use a dash for a range of consecutive outlets. For example, *3-8* represents outlets 3 to 8.
- <outlets2> is one or multiple outlet numbers to be set as NON-critical outlets. Use commas to separate outlet numbers.

  Use a dash for a range of consecutive outlets. For example, *3-8* represents outlets 3 to 8.

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.

Raritan
A brand of legrand

Option	Description
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.

Setting Log Capacity

This command defines the size of data log (records per sensor).

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

Variables:

- <number> is an integer between 60 and 20,000. Desired default log capacity is 120.

Enabling or Disabling data backup

This command enables or disables the data backup feature.

```
config:#       pdu dataBackup <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.

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. Actuators are configured with their own commands.

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 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

Raritan's contact closure sensor supports 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 PX4 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 PX4 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 PX4 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 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 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 PX4 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 DX2-passive infrared sensor

This command determines the value of the Alarmed to Normal Delay setting for a Legrand 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 PX4 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.

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 PX4 contains multiple inlets, this command names the 1st inlet.

```
config:#       inlet 1 name "AC source"
```

Load Shedding Configuration Commands

This section applies to outlet-switching capable models only.

A load shedding configuration command begins with *loadshedding*.

Unlike other CLI configuration commands, the load shedding configuration command is performed in the *administrator mode* rather than the configuration mode.

Enabling or Disabling Load Shedding

This section applies to outlet-switching capable models only.

This command determines whether to enter or exit from the load shedding mode.

```
#    loadshedding <option>
```

After performing the above command, PX4 prompts you to confirm the operation. Press `y` to confirm or `n` to abort the operation.

To skip the confirmation step, you can add the "/y" parameter to the end of the command so that the operation is executed immediately.

```
#    loadshedding <option> /y
```

Variables:

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

Option	Description
start	Enter the load shedding mode.
stop	Quit the load shedding mode.

► *Example*

The following command has the PX4 enter the load shedding mode.

```
config:#          loadshedding start
```


Raritan
A brand of legrand

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 PX4 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 PX4 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

Setting the IPv4 Address

After selecting the static IP configuration mode, you can use this command to assign a permanent IP address to the PX4.

```
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 PX4 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.

Raritan
A brand of legrand

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 PX4. 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 interface eth1 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.

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).

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 PX4 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. For further information, see Static Route Examples.

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

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

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

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

► *Delete an existing static route:*

```
config:#   network ipv4 staticRoutes delete <route_ID>
```

► *Modify an existing static route:*

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

-- OR --

```
config:# 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 PX4 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 PX4 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.

---

*You can configure the PX4 to either "Manual" or "Automatic" IPv6 settings. In manual mode, you must specify the device's IP address, the default router, the DNS server etc. But when Automatic mode is selected, the behavior of the PX4 depends on the configuration of the Router Advertisement (RA) in the network's router. If the RA contains a Prefix Information that has the "Autonomous address-configuration flag" set, the PX4 will use SLAAC and use an IPv6 address based on that Prefix. The PX4 will create a stable privacy address according to RFC 7217. If the RA has the "otherconf" flag set, the PX4 will also use Stateless DHCP to retrieve information like a DNS server. If the "managed" flag is set in the RA, Stateful Address Auto configuration is used via DHCPv6. Both modes (SLAAC and DHCPv6) can be used at the same time.

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>
```

Variables:

- <ETH> is one of the network interfaces: *ETH1/ETH2*, *WIRELESS*, or *BRIDGE*. Note that you must choose/configure the bridge interface if your PX4 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 PX4.

```
config:# network ipv6 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 PX4 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.

Raritan
A brand of legrand

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 PX4. 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 interface gateway eth1 <ip
         address>
```

Variables:

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

Interface	Description
eth1	Determine the IPv6 address of the ETH1 interface (that is, wired networking).
eth2	Determine the IPv6 address of the ETH2 interface (that is, 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).

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 PX4 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. For further information, see Static Route Examples.

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

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

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

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

► *Delete an existing static route:*

```
config:#   network ipv6 staticRoutes delete <route_ID>
```

► *Modify an existing static route:*

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

-- OR --

```
config:# 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 PX4 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 PX4 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>
```


Raritan
A brand of legrand

► *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 --

```
config:# 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 PX4. For example, <suffix1> can be *raritan.com*, and <suffix2> can be *legrand.com*. 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.

Option	Description
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 PX4 selects the optimum transmission mode through auto-negotiation.
half	Half duplex: Data is transmitted in one direction (to or from the PX4) at a time.
full	Full duplex: Data is transmitted in both directions simultaneously.

Setting the LAN MTU

This command sets the MTU for the ethernet interface.

config:# *network ethernet <ETH> mtu <mtu>*

Variables:

- <ETH> is one of the options -- eth1 or eth2.
- <mtu> is the Maximum Transfer Unit. Enter a value from 1280-1500.

Setting the Ethernet Authentication Method

PX4 supports 802.1X (EAP) Network Authentication. Enable the ethernet interface, and then set the authentication method.

```
config:# network ethernet <interface> [enabled
         <enabled>]
```

The following 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. For more information, see Ethernet Interface Settings.

► *Determine the outer authentication protocol:*

```
config:#  network ethernet <ETH> eapOuterAuthentication <outer_auth>
```

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

```
config:#  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 PX4 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. For an example with detailed procedure, see EAP CA Certificate Example (on page 483).

- *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
```

- *Eable or disable verification of the TLS certificate chain:*

```
config:#  network ethernet <ETH> enableCertVerification <option1>
```

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

```
config:#  network ethernet <ETH> allowOffTimeRangeCerts <option2>
```

► *Allow network connection with incorrect system time:*

```
config:# 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 PX4 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 PX4 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.

```
--- BEGIN CERTIFICATE ---
MIICjTCCAfigAwIBAgIEMaYgRzALBgkqhkiG9w0BAQQwRTELMAkGA1UEBhMCVVMx
NjA0BgNVBAoTLU5hdGlvbmFsIEFlcm9uYXV0aWNzIGFuZCBTcGFjZSBBZG1pbmlz
dHJhdGlvbjAmFxE5NjA1MjgxMzQ5MDUrMDgwMBcROTgwNTI4MTM0OTA1KzA4MDAw
ZzELMAkGA1UEBhMCVVMxNjA0BgNVBAoTLU5hdGlvbmFsIEFlcm9uYXV0aWNzIGFu
ZCBTcGFjZSBBZG1pbmlzdHJhdGlvbjEgMAkGA1UEBRMCMTYwEwYDVQQDEwxTdGV2
ZSBTY2hvY2gwWDALBgkqhkiG9w0BAQEDSQAwRgJBALrAwyYdgxmzNP/ts0Uyf6Bp
miJYktU/w4NG67ULaN4B5CnEz7k57s9o3YY3LecETgQ5iQHmkwlYDTL2fTgVfw0C
AQOjgaswgagwZAYDVR0ZAQH/BFowWDBWMFQxCzAJBgNVBAYTAlVTMTYwNAYDVQQK
Ey1OYXRpb25hbCBBZXJvbmF1dGljcyBhbmQgU3BhY2UgQWRtaW5pc3RyYXRpb24x
DTALBgNVBAMTBENSTDEwFwYDVR0BAQH/BA0wC4AJODMyOTcwODEwMBgGA1UdAgQR
MA8ECTgzMjk3MDgyM4ACBSAwDQYDVR0KBAYwBAMCBkAwCwYJKoZIhvcNAQEEA4GB
AH2y1VCEw/A4zaXzSYZJTTUi3uawbbFiS2yxHvgf28+8Js0OHXk1H1w2d6qOHH21
X82tZXd/0JtG0g1T9usFFBDvYK8O0ebgz/P5ELJnBL2+atObEuJy1ZZ0pBDWINR3
WkDNLCGiTkCKp0F5EWIrVDwh54NNevkCQRZita+z4IBO
--- END CERTIFICATE ---
```

5. Select and copy the contents as illustrated below, including the starting line containing "BEGIN CERTIFICATE" and the ending line containing "END CERTIFICATE."
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:#
```


Raritan
A brand of legrand

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 None, 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.
None	The authentication method is set to None.

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. For more information, see Wireless Network Settings.

► *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 PX4 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. For an example with detailed procedure, see EAP CA Certificate Example (on page 483).

- *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
```

- *Eable 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:*

```
config:# 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.
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 PX4 system time is earlier than the firmware build before synchronizing with the NTP server, causing the TLS certificate to become invalid.

Option	Description
false	The network connection is NOT successfully established when the PX4 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.

Setting the Wireless MTU

This command sets the MTU for the wireless interface.

config:# *network wireless mtu<mtu>*

Variables:

- <mtu> is the Maximum Transfer Unit. Enter a value from 1280-1500.

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.

Mode	Description
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 primary device, you must configure the 'downstream interface' setting.

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

Variables:

- <option2> is one of the following cascading roles:

Role	Description
primary	The device is a primary device.
expansion	The device is an expansion device.

- <option3> is one of the following options:

Option	Description
ETH1/ETH2	ETH1/ETH2 port is the port where the 1st expansion device is connected.
Usb	USB port is the port where the 1st expansion 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	• The HTTP port is enabled. - OR - • HTTP redirection to HTTPS is enabled.
false	• 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 PX4 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.

Option	Description
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.

Option	Description
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.

Setting Redfish Service

You can enable or disable the redfish service.

► *Enabling or Disabling Redfish service:*

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

Variables:

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

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

Enabling or Disabling Service Advertising

This command enables or disables the zero configuration protocol, which enables advertising or auto discovery of network services. See Enabling Service Advertising for details.

```
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 LLMNR 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.

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.

Changing an Outlet's Default State

This section applies to outlet-switching capable models only.

This command determines the initial power condition of an outlet after the PX4 powers up.

```
config:#    outlet <n> stateOnPowerUp <option>
```

Variables:

- <n> is the number of the outlet that you want to configure.
- <option> is one of the options: *off*, *on, lastKnownState* and *pduDefined.*

Raritan
A brand of legrand

Option	Description
off	Turn off the outlet.
on	Turn on the outlet.
lastKnownState	Restore the outlet to the state prior to last PDU power down.
pduDefined	PDU-defined setting.

Note: Setting the outlet's default state to an option other than *pduDefined* overrides the PDU-defined default state on that outlet.

Setting an Outlet's Cycling Power-Off Period

This section applies to outlet-switching capable models only.

This command determines the power-off period of the power cycling operation for a specific outlet.

```
config:#   outlet <n> cyclingPowerOffPeriod <timing>
```

Variables:

- <n> is the number of the outlet that you want to configure.
- <timing> is the time of the cycling power-off period in seconds, which is an integer between 0 and 3600, or *pduDefined* for following the PDU-defined timing.

Note: This setting overrides the PDU-defined cycling power-off period on a particular outlet.

Example - Outlet Naming

The following command assigns the name "Win XP" to outlet 8.

```
config:#        outlet 8 name "Win XP"
```

Outlet Group Configuration Commands

An outlet group configuration command begins with *outletgroup*. Such a command allows you to configure or operate an outlet group.

Creating an Outlet Group

This command creates a new outlet group.

```
config:#   outletgroup add "<name>" <members>
```

Variables:

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

  Tip: PX4 allows you to assign the same name to diverse outlet groups. If this really occurs, you still can identify different groups through their unique index numbers.

- <members> is one or multiple member outlets' index numbers separated with commas. If the member outlets are consecutive outlets, you can type a hyphen between the initial and the final index number instead of using commas.

  For example, to assign outlets 3, 4, 5, 8 and 10 to the outlet group named "servers", you have two choices -- either use a hyphen for consecutive outlets 3 to 5, or use commas for all of member outlets:

  - `outletgroup add servers 3-5,8,10`

    -- OR --

  - `outletgroup add servers 3,4,5,8,10`

Managing an Outlet Group

You can modify an outlet group's name and member outlets, or simply remove any existing outlet group.

You can modify both the name and members of an outlet group at a time by combining multiple commands.

► *Modify an outlet group's name:*

```
config:#      outletgroup modify <ID> name "<name>"
```

► *Modify an outlet group's member outlets:*

```
config:#     outletgroup modify <ID> members <members>
```

► *Delete an outlet group:*

```
config:#            outletgroup delete <ID>
```

Variables:

Raritan
A brand of legrand

- <ID> is an outlet group's index number.
- <name> is a string comprising up to 64 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.
- <members> is one or multiple member outlets' index numbers separated with commas. If the member outlets are consecutive outlets, you can type a hyphen between the initial and the final index number instead of using commas.

  For example, to assign outlets 3, 4, 5, 8 and 10 to the outlet group named "servers", you have two choices -- either use a hyphen for consecutive outlets 3 to 5, or use commas for all of member outlets:

  In the following examples, it is assumed that the "servers" outlet group's index number is 2.

  - `outletgroup modify 2 members 3-5,8,10`

    -- OR --

  - `outletgroup modify 2 members 3,4,5,8,10`

Powering On/Off/Cycle Outlet Groups

This section applies to outlet-switching capable models only.

You must perform this operation in the *administrator mode*.

► *Power on one outlet group:*

```
#   power outletgroup <ID> on
```

► *Power off one outlet group:*

```
#   power outletgroup <ID> off
```

► *Power cycle one outlet group:*

```
#   power outletgroup <ID> cycle
```

To quicken the operation, you can add the parameter "/y" to the end of the command, which confirms the operation.

For example:

```
#   power outletgroup <ID> off /y
```

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

Variables:

- <ID> is an outlet group's index number.

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 PX4.

```
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"
```

Peripheral Devices Configuration Commands

You can use the CLI to set the Z Coordinate format for external sensors, set the device altitude, enable/disable device auto management, set the active powered dry contact limit, and enable/disable the "mute other door handle" setting.

Peripheral device configuration commands begin with:

config:# peripheralDevicesSetup

Field	Description	More Information
externalSensorsZCoordinateFormat	Keyword	Z coordinate refers to the height of sensors.

rackUnits / freeForm	Enter one of these values	rackUnits: The height of the Z coordinate is measured in standard rack units. Type a numeric value in the rack unit to describe the Z coordinate. freeForm: Any alphanumeric string can be used for specifying the Z coordinate.
deviceAltitude	Keyword	Specifies the altitude of your PDU above sea level (in meters). Must be set if a differential air pressure sensor is attached because the device's altitude is associated with the altitude correction factor.
number1	Enter an integer number from -425 up to 3000 when using Meters.	Negative numbers indicate altitude below sea level.
peripheralDeviceAutoManagement	Keyword	Enable or disable the automatic management feature for sensors.
enable / disable	Enter one of these values	
activePoweredDryContactLimit	Keyword	You need either 'Change Peripheral Device Configuration' privilege or 'Administrator Privileges'.
number2	Enter an integer number from 0 - 24.	An "active" actuator is turned ON, or, if with a door handle connected, is OPENED.
muteOtherDoorHandle	Keyword	
enable / disable	Enter one of these values	

► *Examples:*

```
config:# peripheralDevicesSetup

externalSensorsZCoordinateFormat freeForm
```

```
deviceAltitude 3

peripheralDeviceAutoManagement enable

activePoweredDryContactLimit 2

muteOtherDoorHandle disable
```

Power Control Operations

This section applies to outlet-switching capable models only.

Outlets can be turned on or off, or power cycled through the CLI.

You can also cancel the power-on process while the system is powering on ALL outlets.

You must perform this operation in the *administrator mode*.

Turning On the Outlet(s)

This section applies to outlet-switching capable models only.

This command turns on one or multiple outlets.

```
#   power outlets <numbers> on
```

To quicken the operation, you can add the parameter "/y" to the end of the command, which confirms the operation.

```
#   power outlets <numbers> on /y
```

Variables:

- <numbers> is one of the options: *all*, an outlet number, a list or a range of outlets.

Option	Description
all	Switches ON all outlets.
A specific outlet number	Switches ON the specified outlet.
A comma- separated list of outlets	Switches ON multiple, inconsecutive or consecutive outlets. For example, to specify 7 outlets -- 2, 4, 9, 11, 12, 13 and 15, type: `outlets 2,4,9,11-13,15.`

Option	Description
A range of outlets with a hyphen in between	Switches ON multiple, consecutive outlets. For example, to specify 6 consecutive outlets -- 3, 4, 5, 6, 7, 8, type: `outlets 3-8.`

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

If you have configured outlet switching sequence and/or delay, PX4 will prompt you with one more question:

```
Should outlet sequence order and delays be used during switching?
```

- Type `y` to apply the current outlet sequence and delay settings when switching on outlets. See Setting Outlet Power-On Sequence and Delay.
- Type `n` to apply the default sequence and delays.

Turning Off the Outlet(s)

This section applies to outlet-switching capable models only.

This command turns off one or multiple outlets.

```
#   power outlets <numbers> off
```

To quicken the operation, you can add the parameter "/y" to the end of the command, which confirms the operation.

```
#   power outlets <numbers> off /y
```

Variables:

- <numbers> is one of the options: *all*, an outlet number, a list or a range of outlets.

Option	Description
all	Switches OFF all outlets.
A specific outlet number	Switches OFF the specified outlet.

Option	Description
A comma- separated list of outlets	Switches OFF multiple, inconsecutive or consecutive outlets. For example, to specify 7 outlets -- 2, 4, 9, 11, 12, 13 and 15, type: `outlets 2,4,9,11-13,15.`
A range of outlets with a hyphen in between	Switches OFF multiple, consecutive outlets. For example, to specify 6 consecutive outlets -- 3, 4, 5, 6, 7, 8, type: `outlets 3-8.`

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

Power Cycling the Outlet(s)

This section applies to outlet-switching capable models only.

This command power cycles one or multiple outlets.

```
# power outlets <numbers> cycle
```

To quicken the operation, you can add the parameter "/y" to the end of the command, which confirms the operation.

```
# power outlets <numbers> cycle /y
```

Variables:

- <numbers> is one of the options: *all*, an outlet number, a list or a range of outlets.

Option	Description
all	Power cycles all outlets.
A specific outlet number	Power cycles the specified outlet.
A comma- separated list of outlets	Power cycles multiple, inconsecutive or consecutive outlets. For example, to specify 7 outlets -- 2, 4, 9, 11, 12, 13 and 15, type: `outlets 2,4,9,11-13,15.`

Option	Description
A range of outlets with a hyphen in between	Power cycles multiple, consecutive outlets. For example, to specify 6 consecutive outlets -- 3, 4, 5, 6, 7, 8, type: `outlets 3-8`.

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

If you have configured outlet switching sequence and/or delay, PX4 will prompt you with one more question:

```
Should outlet sequence order and delays be used during switching?
```

- Type `y` to apply the current outlet sequence and delay settings when switching on outlets. See Setting Outlet Power-On Sequence and Delay.
- Type `n` to apply the default sequence and delays.

Canceling the Power-On Process

This section applies to outlet-switching capable models only.

After issuing the command to power on ALL outlets, you can use the following command to stop the power-on process.

```
#    power cancelSequence
```

To quicken the operation, you can add the parameter "/y" to the end of the command, which confirms the operation.

```
#   power cancelSequence /y
```

Example - Power Cycling Specific Outlets

The following command power cycles these outlets: 2, 6, 7, 8, 10, 13, 14, 15 and 16.

```
#  power outlets 2,6-8,10,13-16 cycle
```

Resetting Energy Readings

You can reset either one energy sensor or all energy sensors at a time to restart the energy accumulation process.

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

► *To reset all energy counters:*

All counters includes inlets, outlets, and PDU (for multi-inlet models).

```
#     reset energy pdu
```

-- OR --

```
#     reset energy pdu /y
```

► *To reset one inlet's energy readings:*

```
#    reset energy inlet <n>
```

-- OR --

```
#    reset energy inlet <n> /y
```


Raritan
A brand of legrand

► *To reset one outlet's energy readings:*

```
#  reset energy outlet <outlet_n>
```

-- OR --

```
#  reset energy outlet <outlet_n> /y
```

► *To reset one outlet group's energy readings:*

```
#  reset energy outletgroup <ID>
```

-- OR --

```
#  reset energy outletgroup <ID> /y
```

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

Variables:

- <n> is the inlet number.
- <outlet_n> is an outlet number.
- <ID> is an outlet group's index number.

Resetting to Factory Defaults

The following commands restore all settings of the PX4 to factory defaults.

► *To reset PX4 settings after login, use either command:*

```
#    reset factorydefaults
```

-- OR --

```
#    reset factorydefaults /y
```

► *To reset PX4 settings before login:*

```
Username:              factorydefaults
```

See Using the CLI Command for details.

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 the PX4

You can reset the PX4 to factory defaults or simply restart it using the CLI commands.

Restarting the PX4

This command restarts the PX4. It is not a factory default reset.

► *To restart the PX4:*

1. Ensure you have entered administrator mode and the # prompt is displayed.
2. Type either of the following commands to restart the PX4.

```
#       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.

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.

Raritan
A brand of legrand

```
config:#  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).

```
config:#  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. For example, a PDU without the outlet switching function does not have the privilege "switchOutlet."

Privilege	**Description**
acknowledgeAlarms	Acknowledge Alarms
adminPrivilege	Administrator Privileges
changeAssetStripConfiguration	Change Asset Strip Configuration
changeAuthSettings	Change Authentication Settings
changeDataTimeSettings	Change Date/Time Settings
changeExternalSensorsConfiguration	Change Peripheral Device Configuration
changeModemConfiguration	Change Modem Configuration
changeNetworkSettings	Change Network Settings
changePassword	Change Own Password
changePduConfiguration	Change Pdu, Inlet, Outlet & Overcurrent Protector Configuration
changeSecuritySettings	Change Security Settings
changeSnmpSettings	Change SNMP Settings

Privilege	Description
changeUserSettings	Change Local User Management
changeWebcamSettings	Change Webcam Configuration
clearLog	Clear Local Event Log
firmwareUpdate	Firmware Update
performReset	Reset (Warm Start)
switchActuator*	Switch Actuator
switchOutlet**	Switch Outlet
switchOutletGroup***	Switch Outlet Group
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 PX4 web interface. It is an integer.

** The "switchOutlet" privilege requires an argument that is separated with a colon. The argument could be:

- All outlets, that is,

Raritan
A brand of legrand

```
switchOutlet:all
```

- An outlet number. For example:

```
switchOutlet:1
switchOutlet:2
switchOutlet:3
```

- A list of comma-separated outlets. For example:

```
switchOutlet:1,3,5,7,8,9
```

*** The "switchOutletGroup" privilege requires an argument that is separated with a colon. The argument could be:

- All outlet groups, that is,

```
switchOutletGroup:all
```

- An outlet group number. For example:

```
switchOutletGroup:1
switchOutletGroup:2
switchOutletGroup:3
```

- A list of comma-separated outlet groups. For example:

```
switchOutletGroup:1,3,5,7,8,9
```

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. See *All Privileges* (on page).
- <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. For arguments syntax, see *All Privileges* (on page).

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
```


Raritan
A brand of legrand

Results:

- A new role "tester" is created.
- Two privileges are assigned to the role: firmwareUpdate (Firmware Update) and viewEventSetup (View Event Settings).

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 PX4 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:*

```
config:#  security ipAccessControl ipv4 enabled <option>
```

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

```
config:#  security ipAccessControl ipv4 defaultPolicyIn <policy>
```

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

```
config:#  security ipAccessControl ipv4 defaultPolicyOut <policy>
```

- *IPv6 commands*

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

```
config:#  security ipAccessControl ipv6 enabled <option>
```

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

```
config:#  security ipAccessControl ipv6 defaultPolicyIn <policy>
```

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

```
config:#  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.

Option	Description
reject	Discards traffic from all IP addresses, and an ICMP message is sent to the source host for failure notification.

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:*

```
config:# security ipAccessControl ipv4 rule add <direction> <ip_mask>
         <policy>
```

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

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

-- OR --

```
config:# 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:*

```
config:# security ipAccessControl ipv6 rule add <direction> <ip_mask>
         <policy>
```

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

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

-- OR --

```
config:# 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: *new rule's number = the specified rule number*
insertBelow	Inserts the new rule below the specified rule number. Then: *new rule's number = the specified rule number + 1*

- <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:*

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

► *Modify an IPv4 rule's policy:*

```
config:# security ipAccessControl ipv4 rule modify <direction>
         <rule_number> policy <policy>
```

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

```
config:# 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:*

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

► *Modify an IPv6 rule's policy:*

```
config:# security ipAccessControl ipv6 rule modify <direction>
         <rule_number> policy <policy>
```

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

```
config:# 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*

```
config:# security ipAccessControl ipv4 rule delete <direction>
         <rule_number>
```

► *IPv6 commands*

```
config:# security ipAccessControl ipv6 rule delete <direction>
         <rule_number>
```

Variables:

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

Direction	Description
in	Inbound traffic.

Direction	Description
out	Outbound traffic.

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

FIPS

You can configure FIPS mode through the CLI. This command begins with security fips [enabled <enabled> and set the mofr for the next reboot.

▶ *Configure FIPS mode:*

```
config:#        security fips <option> <option1>
```

Variables:

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

Option	Description
enable	Enables the FIPS.
disable	Disables the FIPS.

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

Option	Description
true	Enables the FIPS mode on next reboot
false	Disables the FIPS mode on next reboot

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.

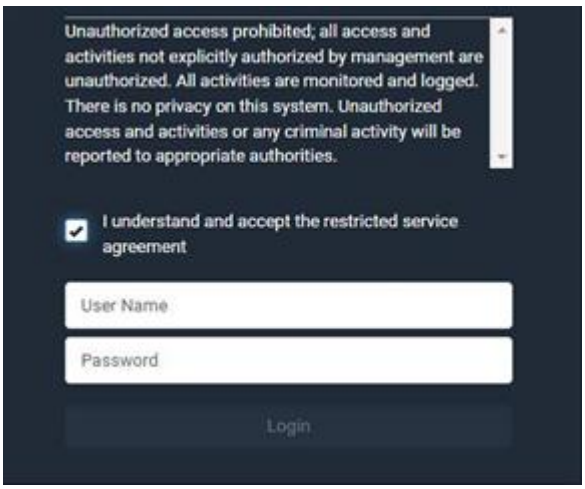
```
config:#  security restrictedServiceAgreement enabled <option>
```

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.



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.

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*.

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.

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.

Option	Description
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 PX4 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`.

► *Determine the maximum number of failed logins before blocking a user:*

```
config:#  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`.

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 minimumLength <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 maximumLength <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.

```
config:# 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.

```
config:# 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.

```
config:# 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.

```
config:# 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:*

```
config:#  security roleBasedAccessControl ipv4 enabled <option>
```

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

```
config:#  security roleBasedAccessControl ipv4 defaultPolicy <policy>
```

- *IPv6 commands*

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

```
config:#  security roleBasedAccessControl ipv6 enabled <option>
```

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

```
config:#  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.

Option	Description
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:*

```
config:# 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:*

```
config:# 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:*

```
config:# 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:*

```
config:# 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: *new rule's number = the specified rule number*
insertBelow	Inserts the new rule below the specified rule number. Then: *new rule's number = the specified rule number + 1*

- <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:*

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

► *Modify an IPv4 rule's role:*

```
config:# security roleBasedAccessControl ipv4 rule modify <rule_number>
         role <role>
```

► *Modify an IPv4 rule's policy:*

```
config:# security roleBasedAccessControl ipv4 rule modify <rule_number>
         policy <policy>
```

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

```
config:# 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:*

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

► *Modify an IPv6 rule's role:*

```
config:# security roleBasedAccessControl ipv6 rule modify <rule_number>
         role <role>
```

► *Modify an IPv6 rule's policy:*

```
config:# security roleBasedAccessControl ipv6 rule modify <rule_number>
         policy <policy>
```

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

```
config:# 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*

```
config:# security roleBasedAccessControl ipv4 rule delete <rule_number>
```

► *IPv6 commands*

```
config:# 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 Outlet Switching

This section applies to outlet-switching capable models only.

The following CLI commands control whether you can turn on or off an outlet by operating the front panel display.

► *To enable the front panel outlet control feature:*

```
config:#    security frontPanelPermissions add switchOutlet
```

► *To disable the front panel outlet control feature:*

```
config:#   security frontPanelPermissions remove switchOutlet
```

Tip: If your PX4 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 outlet switching functions simultaneously.

```
security frontPanelPermissions add switchActuator;switchOutlet
```

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 PX4 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 PX4 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`

Serial Port Configuration Commands

A serial port configuration command begins with *serial*.

Forcing the Device Detection Mode

This command forces the serial port on the PX4 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 PX4 automatically detects the type of the device connected to the serial port. Select this option unless your PX4 cannot correctly detect the device type.
forceConsole	The PX4 attempts to recognize that the connected device is set for the console mode.
forceAnalogModem	The PX4 attempts to recognize that the connected device is an analog modem.

Option	Description
forceGsmModem	The PX4 attempts to recognize that the connected device is a GSM modem.

Example - Baud Rate

The following command sets the CONSOLE baud rate of the PX4 device's serial port to 9600 bps.

```
config:#   serial consoleBaudRate 9600
```

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.

```
config:# 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 an unsuccessful ping. Valid range is 3 to 600 (seconds).
- <resume> is the wait time before the PX4 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 PX4 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*.

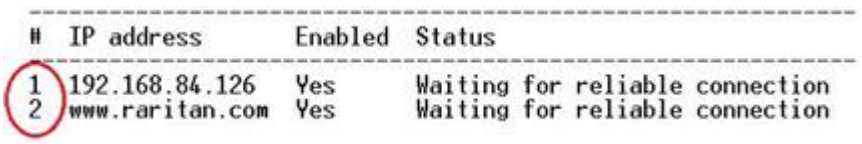
Deleting a Monitored Device

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  192.168.84.126   Yes      Waiting for reliable connection
2  www.raritan.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:*

```
config:#   serverReachability modify <n> ipAddress <IP_host>
```

► *Enable or disable the ping monitoring feature for the device:*

```
config:# serverReachability modify <n> pingMonitoringEnabled <option>
```

► *Modify the number of successful pings for declaring "Reachable":*

```
config:# serverReachability modify <n> numberOfSuccessfulPingsToEnable
         <succ_number>
```

► *Modify the number of unsuccessful pings for declaring "Unreachable":*

```
config:# serverReachability modify <n> numberOfUnsuccessfulPingsForFailure
         <fail_number>
```

► *Modify the wait time after a successful ping:*

```
config:# serverReachability modify <n> waitTimeAfterSuccessfulPing
         <succ_wait>
```

► *Modify the wait time after an unsuccessful ping:*

```
config:# serverReachability modify <n> waitTimeAfterUnsuccessfulPing
         <fail_wait>
```

► *Modify the wait time before resuming pinging after declaring "Unreachable":*

```
config:# serverReachability modify <n> waitTimeBeforeResumingPinging
         <resume>
```

► *Modify the number of consecutive "Unreachable" declarations before disabling the ping monitoring feature:*

```
config:# 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 an unsuccessful ping. Valid range is 3 to 600 (seconds).
- <resume> is the wait time before the system 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 disabling 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.

```
config:# serverReachability modify 2 numberOfSuccessfulPingsToEnable 10
         numberOfUnsuccessfulPingsForFailure 8
         waitTimeAfterSuccessfulPing 30
```

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:

- Outlets
- Outlet groups
- 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.

Note: Your Xerus product may not support all commands.

Commands for Outlet Sensors

A sensor configuration command for outlets begins with *sensor outlet*.

You can configure various outlet sensor threshold settings at a time by combining multiple commands.

Raritan
A brand of legrand

► *Set the Upper Critical threshold for an outlet sensor:*

```
config:#  sensor outlet <n> <sensor type> upperCritical <option>
```

► *Set the Upper Warning threshold for an outlet sensor:*

```
config:#  sensor outlet <n> <sensor type> upperWarning <option>
```

► *Set the Lower Critical threshold for an outlet sensor:*

```
config:#  sensor outlet <n> <sensor type> lowerCritical <option>
```

► *Set the Lower Warning threshold for an outlet sensor:*

```
config:#  sensor outlet <n> <sensor type> lowerWarning <option>
```

► *Set the deassertion hysteresis for an outlet sensor:*

```
config:#  sensor outlet <n> <sensor type> hysteresis <hy_value>
```

► *Set the assertion timeout for an outlet sensor:*

```
config:# sensor outlet <n> <sensor type> assertionTimeout <as_value>
```

Variables:

- <n> is the number of the outlet that you want to configure.
- <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

Sensor type	Description
lineFrequency	Line frequency 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 outlet sensor.
disable	Disables the specified threshold for a specific outlet sensor.
A numeric value	Sets a value for the specified threshold of a specific outlet sensor and enables this threshold at the same time.

- <hy_value> is a numeric value that is assigned to the hysteresis for the specified outlet sensor. See "To De-assert" and Deassertion Hysteresis.
- <as_value> is a number in samples that is assigned to the assertion timeout for the specified outlet sensor. See "To Assert" and Assertion Timeout.

Commands for Outlet Group Sensors

A sensor configuration command for outlets begins with *sensor outletgroup*.

You can configure various outlet group sensor threshold settings at a time by combining multiple commands.

► *Set the Upper Critical threshold for an outlet group sensor:*

```
config:#  sensor outletgroup <ID> <sensor type> upperCritical <option>
```

► *Set the Upper Warning threshold for an outlet group sensor:*

```
config:#  sensor outletgroup <ID> <sensor type> upperWarning <option>
```

► *Set the Lower Critical threshold for an outlet group sensor:*

```
config:#  sensor outletgroup <ID> <sensor type> lowerCritical <option>
```

► *Set the Lower Warning threshold for an outlet group sensor:*

```
config:#  sensor outletgroup <ID> <sensor type> lowerWarning <option>
```

► *Set the deassertion hysteresis for an outlet group sensor:*

```
config:#  sensor outletgroup <ID> <sensor type> hysteresis <hy_value>
```

► *Set the assertion timeout for an outlet group sensor:*

```
config:# sensor outletgroup <ID> <sensor type> assertionTimeout <as_value>
```

Variables:

- <ID> is an outlet group's index number.
- <sensor type> is one of the following sensor types:

Sensor type	Description
activePower	An outlet group's active power sensor
activeEnergy	An outlet group's active energy sensor

For definitions on an outlet group's sensors, see Outlet Groups.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the specified threshold for a specific group sensor of the chosen outlet group.
disable	Disables the specified threshold for a specific group sensor of the chosen outlet group.
A numeric value	Sets a value for the specified threshold of the chosen outlet group's specific group sensor, and enables this threshold at the same time.

- <hy_value> is a numeric value that is assigned to the hysteresis for the specified group sensor of the chosen outlet group.
- <as_value> is a number in samples that is assigned to the assertion timeout for the specified group sensor of the chosen outlet group.

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:*

```
config:# sensor inlet <n> <sensor type> upperCritical <option>
```

► *Set the Upper Warning threshold for an inlet sensor:*

```
config:# sensor inlet <n> <sensor type> upperWarning <option>
```

► *Set the Lower Critical threshold for an inlet sensor:*

```
config:# sensor inlet <n> <sensor type> lowerCritical <option>
```

► *Set the Lower Warning threshold for an inlet sensor:*

```
config:# sensor inlet <n> <sensor type> lowerWarning <option>
```

► *Set the deassertion hysteresis for an inlet sensor:*

```
config:# sensor inlet <n> <sensor type> hysteresis <hy_value>
```

► *Set the assertion timeout for an inlet sensor:*

```
config:# 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

Sensor type	Description
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 PX4

Specific 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	• three-phase models also support pole-level peak current • models with metered breakers also support breaker-level peak current
reactivePower	Reactive power sensor	
displacementPowerFactor	Displacement power factor sensor	

Sensor type	Description	
residualCurrent	RCM current sensor • 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.	
voltageThd	Voltage total harmonic distortion	
currentThd	Current total harmonic distortion	
unbalancedLineLineCurrent	Unbalanced Line-Line current	
unbalancedVoltage	Unbalanced voltage	
unbalancedLineLineVoltage	Unbalanced line-line voltage	
crestFactor	Crest Factor	
phaseAngle	Phase Angle	
residualACCurrent	RCM AC current sensor - detects residual AC current only. Available only on PDUs with RCM Type A	

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:*

```
config:# sensor inletpole <n> <p> <sensor type> upperCritical <option>
```

► *Set the Upper Warning Threshold for an Inlet Pole:*

```
config:# sensor inletpole <n> <p> <sensor type> upperWarning <option>
```

► *Set the Lower Critical Threshold for an Inlet Pole:*

```
config:# sensor inletpole <n> <p> <sensor type> lowerCritical <option>
```

► *Set the Lower Warning Threshold for an Inlet Pole:*

```
config:#  sensor inletpole <n> <p> <sensor type> lowerWarning <option>
```

► *Set the Inlet Pole's Deassertion Hysteresis:*

```
config:#  sensor inletpole <n> <p> <sensor type> hysteresis <hy_value>
```

► *Set the Inlet Pole's Assertion Timeout:*

```
config:# sensor inletpole <n> <p> <sensor type> assertionTimeout
         <as_value>
```

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
apparentEnergy	Apparent Energy sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor
L-L Voltage	Voltage is measured per line

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 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	Supported on PXC and Legrand PDU only • three-phase models also support pole-level peak current • models with metered breakers also support breaker-level peak current
reactivePower	Reactive power sensor	
displacementPowerFactor	Displacement power factor sensor	
residualCurrent	RCM current sensor • 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 Line Sensors

A sensor configuration command for inlet line begins with *sensor inletline*. This type of command is available on a three-phase PDU only.

You can configure various inlet line sensor threshold settings at a time by combining multiple commands.

► *Set the Upper Critical Threshold for an Inlet line:*

```
config:# sensor inletline <n> <p> <sensor type> upperCritical <option>
```

► *Set the Upper Warning Threshold for an Inlet line:*

```
config:# sensor inletline <n> <p> <sensor type> upperWarning <option>
```

► *Set the Lower Critical Threshold for an Inlet line:*

```
config:# sensor inletline <n> <p> <sensor type> lowerCritical <option>
```

► *Set the Lower Warning Threshold for an Inlet line:*

```
config:# sensor inletline <n> <p> <sensor type> lowerWarning <option>
```

► *Set the Inlet line's Deassertion Hysteresis:*

```
config:# sensor inletline <n> <p> <sensor type> hysteresis <hy_value>
```

► *Set the Inlet line's Assertion Timeout:*

```
config:# sensor inletline <n> <p> <sensor type> assertionTimeout
         <as_value>
```

Variables:

- <n> is the number of the inlet whose line sensors you want to configure. For a single-inlet PDU, <n> is always 1.
- <p> is the label of the inlet line that you want to configure.
- <sensor type> is voltage.

Label <n>	Line <p>
1	L1-L2

Label <n>	Line <p>
2	L2-L3
3	L3-L1

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the specified threshold for the specified inlet line sensor.
disable	Disables the specified threshold for the specified inlet line sensor.
A numeric value	Sets a value for the specified threshold of the specified inlet line sensor and enables this threshold at the same time.

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:*

```
config:#  sensor ocp <n> <sensor type> upperCritical <option>
```

► *Set the Upper Warning threshold for an overcurrent protector:*

```
config:#  sensor ocp <n> <sensor type> upperWarning <option>
```

► *Set the Lower Critical threshold for an overcurrent protector:*

```
config:#  sensor ocp <n> <sensor type> lowerCritical <option>
```

► *Set the Lower Warning threshold for an overcurrent protector:*

```
config:#  sensor ocp <n> <sensor type> lowerWarning <option>
```

► *Set the deassertion hysteresis for an overcurrent protector:*

```
config:#  sensor ocp <n> <sensor type> hysteresis <hy_value>
```

► *Set the assertion timeout for an overcurrent protector:*

```
config:#  sensor ocp <n> <sensor type> assertionTimeout <as_value>
```

► *Set the residual current sensor parameters*

```
config:# sensor ocp <n> residualCurrent|residualDCCurrent
         upperCritical|upperWarning|lowerWarning|lowerCritical|
         hysteresis|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.

► *Additional sensors supported by specific models:*

Specific models support OCP residual current sensors per input phase, and output branches. 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
residualCurrent	RCM current sensor • 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.
residualACCurrent	RCM AC current sensor - detects residual AC current only. Available only on PDUs with RCM Type A.

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:*

```
config:# sensor externalsensor <n> <sensor type> upperCritical <option>
```

► *Set the Upper Warning threshold for an environmental sensor:*

```
config:# sensor externalsensor <n> <sensor type> upperWarning <option>
```

► *Set the Lower Critical threshold for an environmental sensor:*

```
config:# sensor externalsensor <n> <sensor type> lowerCritical <option>
```

► *Set the Lower Warning threshold for an environmental sensor:*

```
config:# sensor externalsensor <n> <sensor type> lowerWarning <option>
```

► *Set the deassertion hysteresis for an environmental sensor:*

```
config:#  sensor externalsensor <n> <sensor type> hysteresis <hy_value>
```

► *Set the assertion timeout for an environmental sensor:*

```
config:# 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 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.

Option	Description
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.

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>
```


Raritan
A brand of legrand

► *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 *2015-11-30* 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 *13:50:20* for 1:50:20 pm.

Setting the Time Zone

The CLI has a list of time zones to configure the date and time for PX4.

```
config:#              time zone
```

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

► *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.

Checking the Accessibility of NTP Servers

This command verifies the accessibility of NTP servers specified manually 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
```

Example -Time Configuration

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
```

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 PX4 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.

Option	Description
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, you are prompted 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.
5. 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 PX4 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.

```
config:#  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 PX4 for the specified user:*

```
config:#     user modify <name> snmpV3Access <option1>
```

▶ *Determine the security level:*

```
config:#     user modify <name> securityLevel <option2>
```

▶ *Determine whether the authentication passphrase is identical to the password:*

```
config:# user modify <name> userPasswordAsAuthenticationPassphrase
         <option3>
```

▶ *Determine the authentication passphrase:*

```
config:#     user modify <name> authenticationPassPhrase
```

After performing the above command, the system prompts you to enter the authentication passphrase.

▶ *Determine whether the privacy passphrase is identical to the authentication passphrase:*

```
config:# user modify <name> useAuthenticationPassPhraseAsPrivacyPassPhrase
         <option4>
```


Raritan
A brand of legrand

► *Determine the privacy passphrase:*

```
config:#       user modify <name> privacyPassPhrase
```

After performing the above command, the system prompts you to enter the privacy passphrase.

► *Determine the authentication protocol:*

```
config:#   user modify <name> authenticationProtocol <option5>
```

► *Determine the privacy protocol:*

```
config:#    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 following options:

Option	Description
MD5	MD5 authentication protocol is applied.
SHA-1	SHA-1 authentication protocol is applied.
SHA-224	SHA-224 authentication protocol is applied.
SHA-256	SHA-256 authentication protocol is applied.
SHA-384	SHA-384 authentication protocol is applied.
SHA-512	SHA-512 authentication protocol is applied.

- <option6> is one of the following options:

Option	Description
DES	DES privacy protocol is applied.
AES-128	AES-128 privacy protocol is applied.
AES-192	AES-192 privacy protocol is applied.
AES-256	AES-256 privacy protocol is applied.
AES-192 (3DES key extension)	AES-192 privacy protocol is applied.
AES-256 (3DES key extension)	AES-256 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>
```


Raritan
A brand of legrand

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.
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>
```


Raritan
A brand of legrand

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 system prompts you to enter both current and new passwords respectively.

Important: After the password is changed successfully, the new password is effective immediately whether or not you type the command "apply" 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 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:*

```
config:#  user defaultpreferences preferredTemperatureUnit <option1>
```

► *Set the default length unit:*

```
config:#  user defaultpreferences preferredLengthUnit <option2>
```

► *Set the default pressure unit:*

```
config:#  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.

Unblocking a User

If any user is blocked from accessing, 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 `unblock` and press Enter.

```
Username: unblock
```

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.

Network Troubleshooting in Diagnostic Mode

The PX4 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.

The diagnostic command syntax varies from command to command.

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.

► *To quit the diagnostic mode:*

```
diag>                          exit
```

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

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:

```
diag> ping <host> count <number1> size <number2> timeout <number3>
```

Tracing the Route

This command syntax traces the network route between your PX4 and a network host.

```
diag>  traceroute <host> <useICMP> <timeout>
```

Variables:

Raritan
A brand of legrand

- <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.
- <timeout> is the maximum amount of time (in seconds) until traceroute will be terminated (1..900).

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. You can also use ipv6 address to check the connectivity.

```
diag> ping 192.168.84.222 count 5

      ping fd07:a47c:0000:823e:3b02:0000:982b:0463
      count 5
```

Example: Ping Monitoring and SNMP Notifications

In this illustration, it is assumed that a significant PDU (IP address: 192.168.84.95) shall be monitored by your PX4 to make sure that PDU is properly operating all the time, and the PX4 must send out SNMP notifications (trap or inform) if that PDU is declared unreachable due to power or network failure. The prerequisite for this example is that the power sources are different between your PX4 and the monitored PDU.

This requires the following two steps.

► *Step 1: Set up the ping monitoring for the target PDU*

1. Choose Device Settings > Server Reachability.
2. Click

.
3. Ensure the "Enable ping monitoring for this server" checkbox is selected.
4. Enter the data shown below.
   - Enter the server's data.

Field	Data entered
IP address/hostname	192.168.84.95

   - To make the PX4 declare the accessibility of the monitored PDU every 15 seconds (3 pings * 5 seconds) when that PDU is accessible, enter the following data.

Field	Data entered
Number of successful pings to enable feature	3
Wait time after successful ping	5

   - To make the PX4 declare the inaccessibility of the monitored PDU when that PDU becomes inaccessible for around 12 seconds (4 seconds * 3 pings), enter the following data.

Field	Data entered
Wait time after unsuccessful ping	4
Number of consecutive unsuccessful pings for failure	3

- To make the PX4 stop pinging the target PDU for 60 seconds (1 minute) after the PDU inaccessibility is declared, enter the following data. After 60 seconds, the PX4 will re-ping the target PDU,

Field	Data entered
Wait time before resuming pinging after failure	60

- The "Number of consecutive failures before disabling feature (0 = unlimited)" can be set to any value you want.

5. Click Create.

► *Step 2: Create an event rule to send SNMP notifications for the target PDU*

1. Choose Device Settings > Event Rules.
2. Click

.
3. Select the Enabled checkbox to enable this new rule.
4. Configure the following.

Field/setting	Data specified
Rule name	Send SNMP notifications for PDU (192.168.84.95) inaccessibility
Event	Choose Server Monitoring > 192.168.84.95 > Unreachable
Trigger condition	Select the Unreachable radio button

This will make the PX4 react only when the target PDU becomes inaccessible.

5. Select the System SNMP Notification Action.

Appendices

Specifications

In This Chapter

PX4-Series Specifications. 569

PX4-Series Specifications

► *Max Ambient Operating Temperature:*

- 60 degrees Celsius

► *Sensor Port Pinouts:*

Pin#	Signal	Direction	Description
1	+12V	—	Power (fuse protected)
2	+12V	—	Power (fuse protected)
3	GND	—	Signal Ground
4	RS485 DP	bi-directional	Data positive of the RS-485 bus
5	RS485 DN	bi-directional	Data negative of the RS-485 bus
6	GND	—	Signal Ground
7	1-Wire	—	1-wire signal for Legrand environmental sensor packages
8	GND	—	Signal Ground

► *PDU Link Port Pinouts:*

Pin#	Signal	Direction	Description
1	+12V	—	Power (fuse protected)
2	+12V	—	Power (fuse protected)
3	GND	—	Signal Ground
4	TxD+	Output	Transmit data (+)
5	TxD-	Output	Transmit data (-)
6	GND	—	Signal Ground
7	RxD+	Input	Receive data (+)
8	RxD-	Input	Receive data (-)

Equipment Setup Worksheet Sample

- *PX4 Model* _____
- *PX4 Serial Number* _____
- *Types of adapters* _____

- *Types of cables* _____
- *Name of software program* _____

In This Chapter

Outlets detail. 571

Outlets detail

OUTLET 1	OUTLET 2	OUTLET 3
MODEL	MODEL	MODEL
SERIAL NUMBER	SERIAL NUMBER	SERIAL NUMBER
USE	USE	USE
OUTLET 4	OUTLET 5	OUTLET 6
MODEL	MODEL	MODEL
SERIAL NUMBER	SERIAL NUMBER	SERIAL NUMBER
USE	USE	USE
OUTLET 7	OUTLET 8	OUTLET 9
MODEL	MODEL	MODEL
SERIAL NUMBER	SERIAL NUMBER	SERIAL NUMBER
USE	USE	USE
OUTLET 10	OUTLET 11	OUTLET 12
MODEL	MODEL	MODEL

SERIAL NUMBER	SERIAL NUMBER	SERIAL NUMBER
USE	USE	USE
OUTLET 13	OUTLET 14	OUTLET 15
MODEL	MODEL	MODEL
SERIAL NUMBER	SERIAL NUMBER	SERIAL NUMBER
USE	USE	USE
OUTLET 16	OUTLET 17	OUTLET 18
MODEL	MODEL	MODEL
SERIAL NUMBER	SERIAL NUMBER	SERIAL NUMBER
USE	USE	USE
OUTLET 19	OUTLET 20	OUTLET 21
MODEL	MODEL	MODEL
SERIAL NUMBER	SERIAL NUMBER	SERIAL NUMBER
USE	USE	USE
OUTLET 22	OUTLET 23	OUTLET 24
MODEL	MODEL	MODEL
SERIAL NUMBER	SERIAL NUMBER	SERIAL NUMBER
USE	USE	USE

Special Configuration and Upgrade Methods

In This Chapter

Configuration or Firmware Upgrade with a USB Drive. 573
Bulk Configuration or Firmware Upgrade via DHCP (TFTP/HTTPS). 585
Raw Configuration Upload and Download. 602
Bulk Configuration, Firmware Upgrade, or Backup/Restore via SCP. 607

Configuration or Firmware Upgrade with a USB Drive

You can accomplish the following tasks simultaneously by plugging a USB flash drive which contains special configuration files into the device.

- Configuration changes
- Firmware upgrade
- Diagnostic data download

Device Configuration/Upgrade Procedure

Firmware downgrade is NOT supported by default. Contact Technical Support.

You can use one USB drive to configure or upgrade multiple devices one by one as long as it contains valid configuration files.

► *To use a USB drive to configure or upgrade firmware:*

1. Check requirements. System and USB Requirements (on page 574).
2. Prepare required configuration files. See Configuration Files (on page 574).
3. Copy required configuration files to the root directory of the USB drive.
   - For firmware upgrade, an appropriate firmware binary file is also required.
4. Plug the USB drive into the USB-A port of the device.

5. The initial message shown on the front panel display depends on the first task performed.
   - If the USB contains a firmware upgrade, that task happens first. The front panel display shows an upgrade message. When the firmware upgrade completes successfully, then a happy smiley appears.
   - If no firmware upgrade task will be performed, a happy smiley is displayed after around 30 seconds.

6. If nothing is shown on the display and no task is performed after plugging the USB drive, check the log file in the USB drive.
7. After the happy smiley appears, press one of the control buttons next to the display for one second until the smiley disappears. Wait for several seconds until the device resumes normal operation, indicated by the normal message of the display.

Tip: Once the happy smiley displays, you can safely remove the USB drive and move it to the next device you are working on.

System and USB Requirements

You must satisfy ALL of the following requirements prior to using a USB flash drive to perform device configuration and/or firmware upgrade.

► *System requirements:*

- There is at least one USB-A port available on your Xerus device.
- Your Xerus device must run firmware version 2.2.13 or later.

► *USB drive requirements:*

- The drive contains either a single partition formatted as a Windows FAT32 filesystem, or NO partition tables (that is, a superfloppy-formatted drive).

Configuration Files

There are three types of configuration files. To generate these files, use the Mass Deployment Utility. See Creating Configuration Files via Mass Deployment Utility (on page 582).

- fwupdate.cfg:

  This file MUST always be present for performing configuration or firmware upgrade tasks. See fwupdate.cfg (on page 575).
- config.txt:

  This file is used for configuring device settings. See config.txt (on page 578).
- devices.csv:

Raritan
A brand of legrand

This file is required only when there are device-specific settings to configure for multiple devices. See devices.csv (on page 580).

fwupdate.cfg

The configuration file, *fwupdate.cfg*, is an ASCII text file containing key-value pairs, one per line.

Each value in the file must be separated by an equal sign (=), without any surrounding spaces. Keys are not case sensitive.

Illustration:

```
user=admin
password=admn
set_password=newpassword Or
set_encrypted_password=<cyphertext>
logfile=log.txt
config=config.txt
device_list=devices.csv
```

This section explains common options in the file.

► *user*

- A required option.
- Specify the name of a user account with Administrator Privileges.

► *password*

- A required option.
- Specify the password of the specified admin user.

Tip: You can add multiple user credentials to fwupdate.cfg. Each 'user' line must be immediately followed by its 'password' line. Each user will be authenticated until one of them succeeds, or until all user credentials fail.

► *set_password / set_encrypted_password*

- You are required to change the default password for all units. Access to units with factory default password settings will be denied unless this option is used.
- Changes the password of the given user before executing any commands.
- To get encrypted password use the hidden CLI command 'config encrypt <value>'.

► *logfile*

- Specify the name of a text file where the where log messages will be saved when interpreting the USB drive contents.
- If the specified file does not exist in the USB drive, it will be automatically created.
- If this option is not set, no log messages are recorded, and there will be no feedback if there is a problem with the USB drive contents.

► *firmware*

- Specify the name of a firmware file.
- The specified firmware file must be compatible with your device.
- The default is to NOT permit any firmware downgrade . To do this, the parameter "allow_downgrade" must be present and properly set in the *fwupdate.cfg* file.

► *config*

- Specify the name of the configuration file containing device settings.
- The default filename is *config.txt*.

► *device_list*

- Specify the name of the configuration file listing all devices to configure and their device-specific settings.
- This file is required if any macros are used in the device configuration file "config.txt."
- The default filename is *devices.csv*.

► *match*

- Specify a match condition for identifying a device in the device configuration file "devices.csv."
  The option's value comprises one word and one number as explained below:
  - The word prior to the colon is an identification property, which is either `serial` for serial number or `mac` for MAC address.
  - The number following the colon indicates a column in the *devices.csv* file.

  For example, `mac:7` will search for the MAC address in the 7th column of the "devices.csv" file.
- The default value is `serial:1`, to search for its serial number in the first column.
- This option is used only if the "device_list" option has been set.

► *factory_reset*

- If this option is set to `true`, the device will be reset to factory defaults.
- If the device configuration will be updated at the same time, the factory reset will be executed before updating the device configuration.

► *bulk_config_restore*

- Specify the name of the bulk configuration file used to configure or restore.

Note: See Bulk Configuration or Firmware Upgrade via DHCP (TFTP/HTTPS) (on page 585) for instructions on generating a bulk configuration file.

- Additional configuration keys set via the *config.txt* file will be applied after performing the bulk restore operation.
- This option CANNOT be used with the option "full_config_restore."
- If a firmware upgrade will be performed at the same time, you must generate the bulk configuration file based on the NEW firmware version instead of the current firmware version.

► *full_config_restore*

- Specify the name of the full configuration backup file used to restore the device.
- Additional configuration keys set via the *config.txt* file will be applied after performing the configuration restore operation.
- This option CANNOT be used with the option "bulk_config_restore."
- If a firmware upgrade will be performed at the same time, you must generate the full configuration backup file based on the NEW firmware version instead of the current firmware version.

► *collect_diag*

- If this option is set to `true`, the diagnostic data is transmitted to the USB drive.
- The filename of the diagnostic data written into the USB drive is:
  diag_<unit-serial>.zip
- The device beeps after it finishes writing the diagnostic data to the USB drive.

► *switch_outlets*

- This feature works on outlet-switching capable models only.
- Switch on or off specific outlets.
- The option's value comprises outlet numbers and the setting "on" or "off" as explained below:

- Each "on" or "off" setting consists of three parts: outlet numbers, a colon, and the word "on" or "off".
- Each "on" or "off" setting is separated with a semicolon.
- If all outlets will share the same "on" or "off" setting, replace the outlet numbers with the word "all".

- Examples:
  - Turn on outlets 1 to 3, and 10, and turn off outlets 4 to 9.

    ```
    switch_outlets=1,2,3:on;4-9:off;10:on
    ```
  - Turn on all outlets.

    ```
    switch_outlets=all:on
    ```

► *tls_cert_file*

- Specify the filename of the wanted TLS server certificate. The filename can contain a single placeholder ${SERIAL} that is replaced with the serial number of the device.
- This option should be used with tls_key_file listed below.
- *This option is NOT supported by bulk configuration or backup/restore via DHCP/TFTP.*

► *tls_key_file*

- Specify the filename of the wanted TLS server key. The filename can contain a single placeholder ${SERIAL} that is replaced with the serial number of the device.
- This option should be used with tls_cert_file listed above.
- *This option is NOT supported by bulk configuration or backup/restore via DHCP/TFTP.*

► *execute_lua_script*

- Specify a Lua script file. For example:

  ```
  execute_lua_script=my_script.lua
  ```
- Script output will be recorded to a log file -- <BASENAME_OF_SCRIPT>.<SERIAL_NUMBER>.log. Note this log file's size is limited on DHCP/TFTP.
- A DHCP/TFTP-located script has a timeout of 60 seconds. After that duration the script will be removed.
- This feature can be used to manage LuaService, such as upload, start, get output, and so on.
- If you unplug the USB drive while the Lua script is still running, the script will be removed.
- An exit handler can be used but the execution time is limited to three seconds. Note that this is not implemented on DHCP/TFTP yet.

config.txt

To perform device configuration using a USB drive, you must:

- Copy the device configuration file "config.txt" to the root directory of the USB drive.
- Reference the "config.txt" file in the *config* option of the "fwupdate.cfg" file.

The file, *config.txt*, is a text file containing a number of configuration keys and values to configure or update.

This section only introduces the device configuration file in brief, and does not document all configuration keys, which vary according to the firmware version and your model.

You can use the Mass Deployment Utility to create this file by yourself, or contact Technical Support to get a device configuration file specific to your model and firmware version.

Tip: You can choose to encrypt important data in the "config.txt" file so that people cannot easily recognize it, such as the SNMP write community string. See Data Encryption in 'config.txt' (on page 583) .

If you are using a password as auth/priv passphrases, you must set the password in the config file to ensure it generates the SNMPv3 hash.

► *Regular configuration key syntax:*

- Each configuration key and value pair is in a single line as shown below:

  ```
  key=value
  ```

  Note: Each value in the file must be separated by an equal sign (=), without any surrounding spaces.

- Multi-line values are supported by using the *Here Document Syntax* with a user-chosen delimiter.

  The following illustration declares a value in two lines. You can replace the delimiter `EOF` with other delimiter strings.

  ```
  key<<EOF
  value line 1
  value line 2
  EOF
  ```

  Note: The line break before the closing EOF is not part of the value. If a line break is required in the value, insert an additional empty line before the closing EOF.

► *Special configuration keys:*

There are 3 special configuration keys that are prefixed with `magic:`.

- A special key that sets a user account's password without knowing the firmware's internal encryption/hashing algorithms is implemented.

  Example:

  ```
  magic:users[1].cleartext_password=joshua
  ```

- Two special keys that set the SNMPv3 passphrases without knowing the firmware's internal encryption/hashing algorithms are implemented.

  Examples:

  ```
  magic:users[1].snmp_v3.auth_phrase=swordfish
  ```

```
magic:users[1].snmp_v3.priv_phrase=opensesame
```

► *To configure device-specific settings:*

1. Make sure the device list configuration file "devices.csv" is available in the USB drive.
2. In the "config.txt" file, refer each device-specific configuration key to a specific column in the "devices.csv" file. The syntax is: `${column}`, where "column" is a column number.

Examples:

```
net.interfaces[eth0].ipv4.static.addr_cidr.addr=${4}
pdu.name=${16}
```

► *To rename the admin user:*

You can rename the admin user by adding the following configuration key:

```
users[0].name=new admin name
```

Example:

```
users[0].name=May
```

► *To restore a specific setting to factory default:*

Add "delete:" to the beginning of the key whose setting you want to remove. The custom setting will be removed and then reset to factory default.

Example:

```
delete:net.port_forwarding
```

devices.csv

If there are device-specific settings to configure, you must create a device list configuration file - *devices.csv*, to store unique data of each device.

This file must be:

- A CSV (comma-separated values) format file exported from a spreadsheet application like Excel.
- Copied to the root directory of USB drive.
- Referenced in the *device_list* option of the "fwupdate.cfg" file. See fwupdate.cfg (on page 575).

Every device identifies its entry in the "devices.csv" file by comparing its serial number or MAC address to one of the columns in the file.

► *Determine the column to identify devices:*

- By default, each device searches for its serial number in the 1st column of "devices.csv".
- To override the default, set the *match* option in the "fwupdate.cfg" file to a different column.

► *Syntax:*

- Values containing commas, line breaks or double quotes are all supported.
- The commas and line breaks to be included in the values must be enclosed in double quotes.
- Every double quote to be included in the value must be escaped with another double quote.
  For example:

```
Value-1,"Value-2,with,three,commas",Value-3
Value-1,"Value-2,""with""three""double-quotes",Value-3
Value-1,"Value-2
with a line break", Value-3
```

Configuration Files for Linking

When Linking is enabled multiple versions of config.txt are required:

- config_link_unit.txt containing the configuration for all link units
- config_<serial>.txt for each primary unit containing its specific settings, including a list of link units.

► *Commands for device Linking:*

The following commands are used in the fwupdate.cfg file to configure Linking.

► *add_link_unit*

Add a new link unit. The option can be specified more than once to add multiple link units.

```
add_link_unit=<id>,<host>,<login>:<password>
```

- Parameters are: <id>: new link unit id (2..8), <host>: hostname or IP address, <login>:<password>: credentials for admin user

► *add_link_unit_new_password:*

Change the password when adding a new link unit. Required in case the link unit still uses the factory default password.

```
add_link_unit_new_password=<id>,<new_password>
```

► *add_cascade_link_units*

Add port-forwarding expansion units as link units. The option can be specified more than once to link multiple port-forwarding nodes with different parameters.

```
add_cascade_link_units=<link ids>:<nodes>:<position
dependent>:<login>:<password>
```

Parameters are:

<link ids>: comma-separated list of new link unit ids (2..8)

<nodes>: comma-separated list of port-forwarding node indices (1..31, needs to be same length as <link ids>), or the special word "all", which will link all port-forwarding nodes until an error occurs.

<position dependent>: "true" or "false": if true, use position-dependent host-names (i.e. expansion-<n>.pf-cascade) or, if false, use link-local IPv6 addresses.

<login>:<password>: credentials for admin user on the port-forwarding node

- Example: `add_cascade_link_units=2,3:1,2:false:admin:<password>`

Configuration Files for Linking: Port-Forwarding Cascade Example

In this example, you can configure a port-forwarding cascade containing a Primary PDU and supported Expansion Units. Complete physical, wired setup first, then use the USB drive method with a fwupdate.cfg file as described here.

- Prerequesite: Wired setup with primary units and connected expansion units

1. Prepare a USB drive with a fwupdate.cfg file with the following included details

```
port_forwarding_auto_setup=[downstreamInterface:<INTERFACE-LABEL>,]<number of
expansion units>,admin:<password>
```

2. Attach the USB drive to the primary units to automatically setup the port-forwarding cascade and linking.

Creating Configuration Files via Mass Deployment Utility

The Mass Deployment Utility is an Excel file that lets you fill in basic information required for the three configuration files, such as the admin account and password.

After entering required information, you can generate all configuration files with only one click, including *fwupdate.cfg*, *config.txt* and *devices.csv*.

Note: The firmware version of your device must match the version of the Mass Deployment Utility spreadsheet. Do not mix versions.

New commands that have been introduced in later versions of the spreadsheet will not be effective on devices with older firmware.

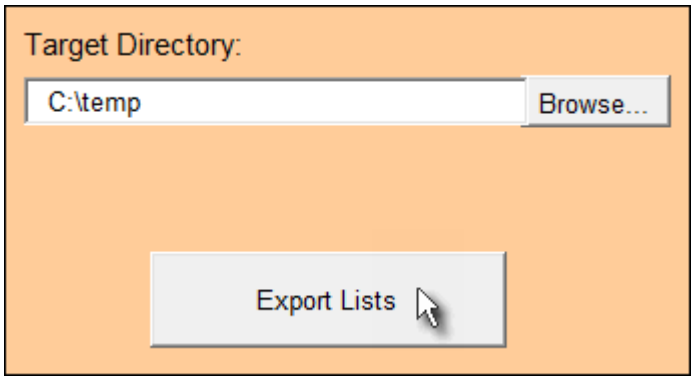
► *To use the Mass Deployment Utility:*

1. Download the Mass Deployment Utility from the support page.
   - The utility is named *mass_deployment-xxx* (where xxx is the firmware version number).
2. Launch Excel to open this utility.

Raritan
A brand of legrand

Note: Other programs, such as OpenOffice and LibreOffice, are not supported.

3. Read the instructions in the 1st worksheet of the utility, and make sure Microsoft Excel's security level has been set to Medium or the equivalent for executing unsigned macros of this utility.
4. Enter information in the 2nd and 3rd worksheets.
   - The 2nd worksheet contains information required for *fwupdate.cfg* and *config.txt*.
   - The 3rd worksheet contains device-specific information for *devices.csv*.
5. Return to the 2nd worksheet to execute the export macro.
   a. In the Target Directory field, specify the folder where to generate the configuration files. For example, you can specify the root directory of a connected USB drive.
   b. Click Export Lists to generate configuration files.



Verify that at least 3 configuration files are created - *fwupdate.cfg*, *config.txt* and *devices.csv*. You are ready to configure or upgrade with these files.

Data Encryption in 'config.txt'

When intending to prevent people from identifying the values of any settings, you can encrypt them. Encrypted data still can be properly interpreted and performed by any device running Xerus firmware version 3.2.20 or later.

When using the USB stick to perform an initial configuration, a user will receive an error message when the initial password change is not performed:Password change for user admin required, use set_password or set_encrypted_password. See:config.txt (on page 578)

► *Data encryption procedure:*

1. Open the "config.txt" file to determine which setting(s) to encrypt.
2. Launch a terminal to log in to the CLI of the device.
3. Type the encryption command and the value of the setting you want to encrypt.
   - The value *cannot* contain any double quotes (") or backslashes (\).
   - If the value contains spaces, it must be enclosed in double quotes.

```
# config encrypt <value>
```

```
-- OR --
```

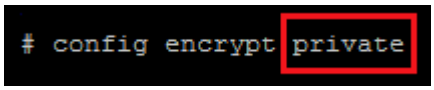
```
# config encrypt "<value with spaces>"
```

4. Press Enter. The CLI generates and displays the encrypted form of the typed value.
5. Go to the "config.txt" file and replace the chosen value with the encrypted one by typing or copying the encrypted value from the CLI.
6. Add the text "encrypted:" to the beginning of the encrypted setting.
7. Repeat steps for additional settings you intend to encrypt.
8. Save the changes made to the "config.txt" file. Now you can use this file to configure other devices.

► *Illustration:*

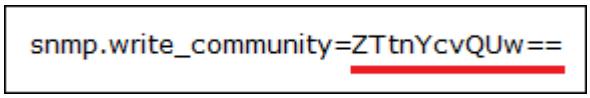
In this example, we will encrypt the word "private", which is the value of the SNMP write community in the "config.txt" file.

1. In the CLI, type the following command to encrypt "private."

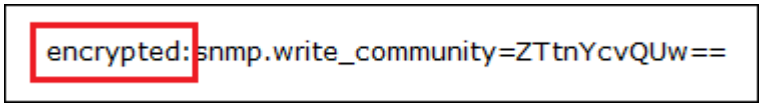


2. The CLI generates and shows the encrypted form of "private."

3. In the "config.txt" file, make the following changes to the SNMP write community setting.
   a. Replace the word "private" with the encrypted value that CLI shows.



   b. Add "encrypted:" to the beginning of that setting.



Firmware Upgrade via USB

Firmware files are available on the product support page.

Note that if the firmware file used for firmware upgrade is the same as the firmware version running on the PX4, no firmware upgrade will be performed unless you have set the *force_update* option to true in the "fwupdate.cfg" file.

► *To use a USB drive to upgrade the PX4:*

1. Copy the configuration file "fwupdate.cfg" and an appropriate firmware file to the root directory of the USB drive.
2. Reference the firmware file in the *firmware* option of the "fwupdate.cfg" file.
3. Plug the USB drive into the USB-A port on the PX4.
4. The front panel display shows the firmware upgrade progress.

Tip: You can remove the USB drive and plug it into another unit for firmware upgrade when the firmware upgrade message displays.

---

5. It may take one to five minutes to complete the firmware upgrade, depending on your product.
6. When the firmware upgrade finishes, the front panel display indicates the firmware upgrade result.
   - Happy smiley: Successful.

   - Sad smiley: Failed. Check the log file in the USB drive or contact Technical Support to look into the failure cause.

Note: If your unit does not have a front panel display, you should wait for few minutes, remove the USB drive, and reboot the unit.

---

1. Remove USB drive and push any front panel button to continue.

Bulk Configuration or Firmware Upgrade via DHCP (TFTP/HTTPS)

If a TFTP or HTTPS server is available, you can use it and appropriate configuration files to perform any or all of the following tasks for a large number of devices in the same network.

- Initial deployment
- Configuration changes
- Firmware upgrade
- Downloading diagnostic data

This feature is useful if you have hundreds or even thousands of devices to configure or upgrade.

Warning: The feature of bulk configuration or firmware upgrade via DHCP (TFTP/HTTPS)only works on standalone devices directly connected to the network. This feature does NOT work for expansion units in a cascading configuration.

Bulk Configuration/Upgrade Procedure

Firmware downgrade is NOT supported by default. Contact Technical Support.

► *Steps of using DHCP (TFTP/HTTPS) for bulk configuration/upgrade:*

1. Create configuration files specific to your PX4 models and firmware versions. Create your own or contact Technical Support to properly prepare some or all of the following files:
   - *fwupdate.cfg (always required)*
   - *config.txt*
   - *devices.csv*

   Note: Supported syntax of "fwupdate.cfg" and "config.txt" may vary based on different firmware versions. If you have existing configuration files, it is suggested to double check with Technical Support for the correctness of these files prior to using this feature.
2. Configure your TFTP or HTTPS server properly.
3. Copy ALL required configuration files into the TFTP or HTTPS root directory. If the tasks you will perform include firmware upgrade, an appropriate firmware binary file is also required.
4. Properly configure your DHCP server so that it refers to the file "fwupdate.cfg" on the TFTP/HTTPS server.
5. Make sure all of the desired devices use DHCP as the IP configuration method and have been *directly* connected to the network.
6. Reboot these devices. The DHCP server will execute the commands in the "fwupdate.cfg" file on the TFTP server to configure or upgrade those devices supporting DHCP in the same network.

DHCP will execute the "fwupdate.cfg" commands once for IPv4 and once for IPv6 respectively if both IPv4 and IPv6 settings are configured properly in DHCP.

Note: If both TFTP and HTTP server options are specified, HTTP takes precedence. For HTTP, both 'http' and 'https' schemes are supported, but when using https, the certificate is not checked.

TFTP/HTTPS Requirements

To perform bulk configuration or firmware upgrade successfully, your TFTP/HTTPS server must meet the following requirements:

- The server is able to work with both IPv4 and IPv6.
  In Linux, remove any IPv4 or IPv6 flags from */etc/xinetd.d/tftp*.

Note: DHCP will execute the "fwupdate.cfg" commands once for IPv4 and once for IPv6 respectively if both IPv4 and IPv6 settings are configured properly in DHCP.

- All required configuration files are available in the TFTP/HTTPS root directory. See *Bulk Configuration/Upgrade Procedure* (on page).

If you are going to upload any PX4 diagnostic file or create a log file in the TFTP server, the first of the following requirements is also required.

Note: The HTTPS server does not support file writes(diag data, log files etc.).

► *TFTP Server:*

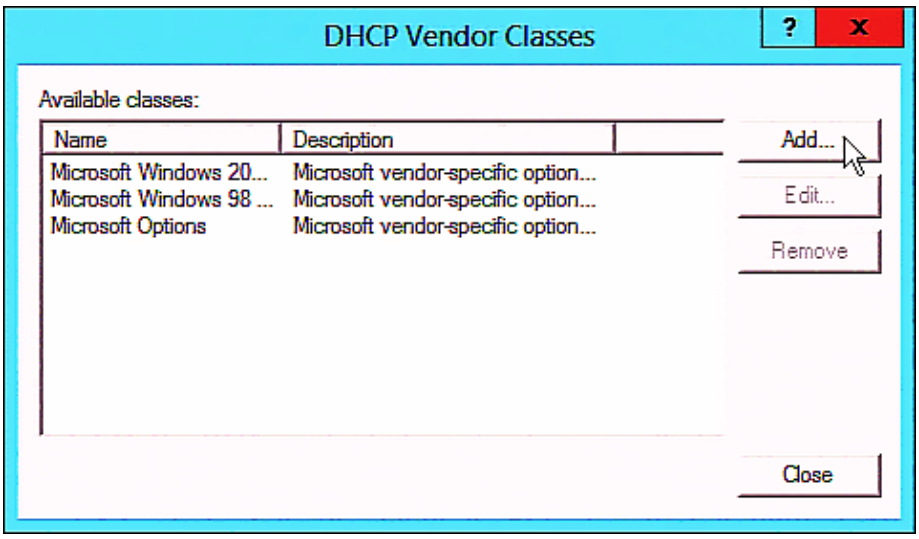
- The TFTP server supports the write operation, including file creation and upload.
  In Linux, provide the option "-c" for write support.
- Required for uploading the diagnostic file only - the timeout for file upload is set to one minute or longer.

DHCP IPv4 Configuration in Windows

For those PX4 devices using IPv4 addresses, follow this procedure to configure your DHCP server. The following illustration is based on Microsoft® Windows Server 2012 system.

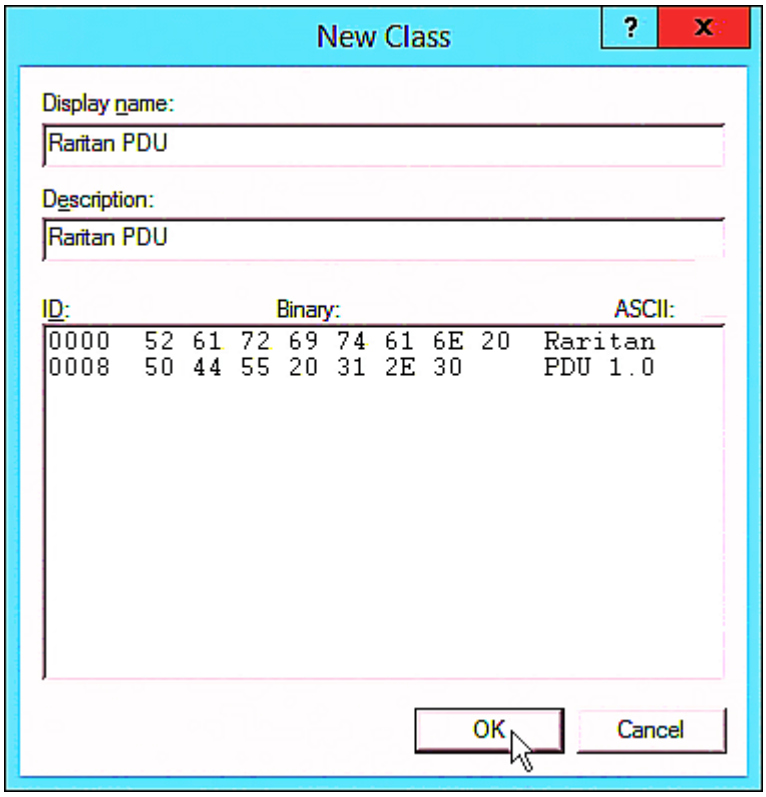
► *Required Windows IPv4 settings in DHCP:*

1. Add a new vendor class for PX4 under IPv4.
   a. Right-click the IPv4 node in DHCP to select Define Vendor Classes.
   b. Click Add to add a new vendor class.

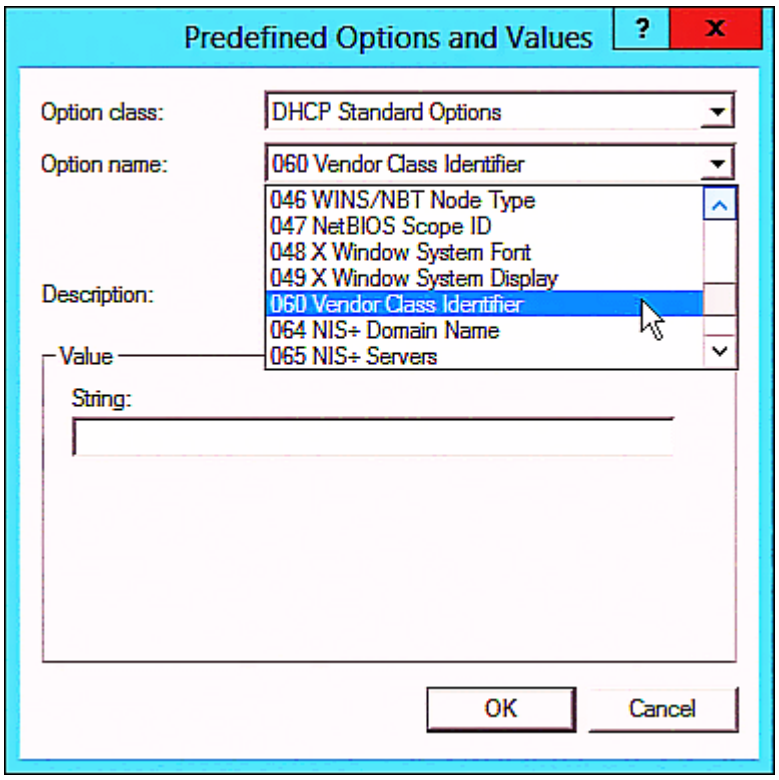


   c. Specify a unique name for this vendor class and type the binary codes of "Raritan PDU 1.0" in the New Class dialog.

The vendor class is named "Raritan PDU" in this illustration.

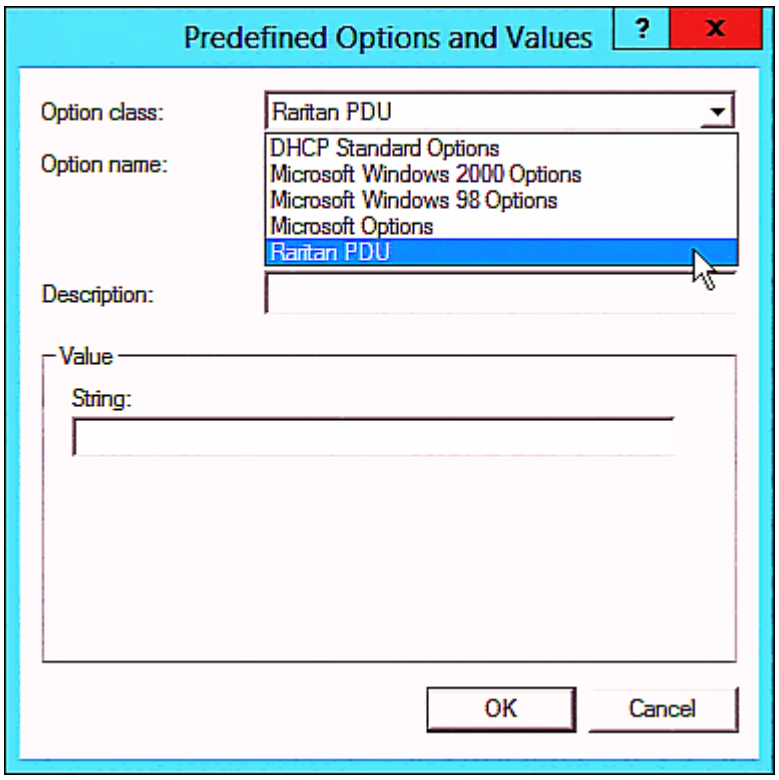


2. Define one DHCP standard option - Vendor Class Identifier.
   a. Right-click the IPv4 node in DHCP to select Set Predefined Options.
   b. Select DHCP Standard Options in the "Option class" field, and Vendor Class Identifier in the "Option name" field. Leave the String field blank.

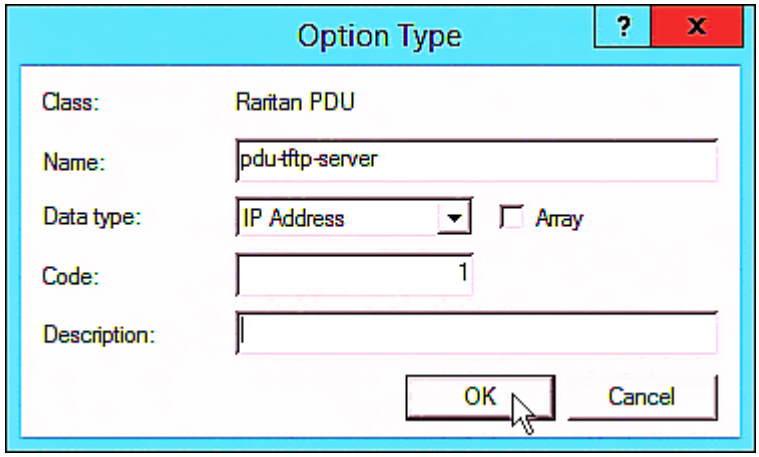


3. Add three options to the new vendor class "Raritan PDU" in the same dialog.

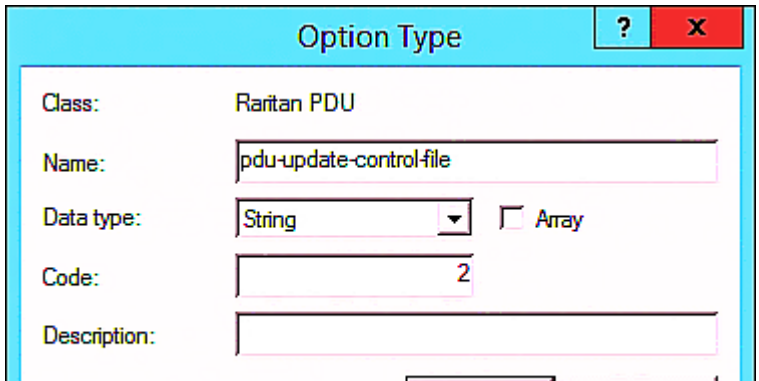
a. Select Raritan PDU in the "Option class" field.



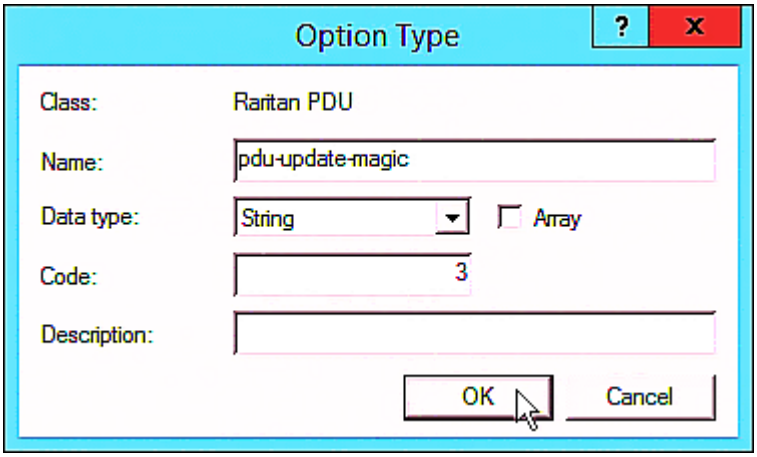
b. Click Add to add the first option. Type "pdu-tftp-server" or "pdu-https-server" in the Name field, select IP Address as the data type, and type 1 in the Code field for tftp server and type 7 in the Code field for https server.



c. Click Add to add the second option. Type "pdu-update-control-file" in the Name field, select String as the data type, and type 2 in the Code field.



data type, and type 3 in the Code field.



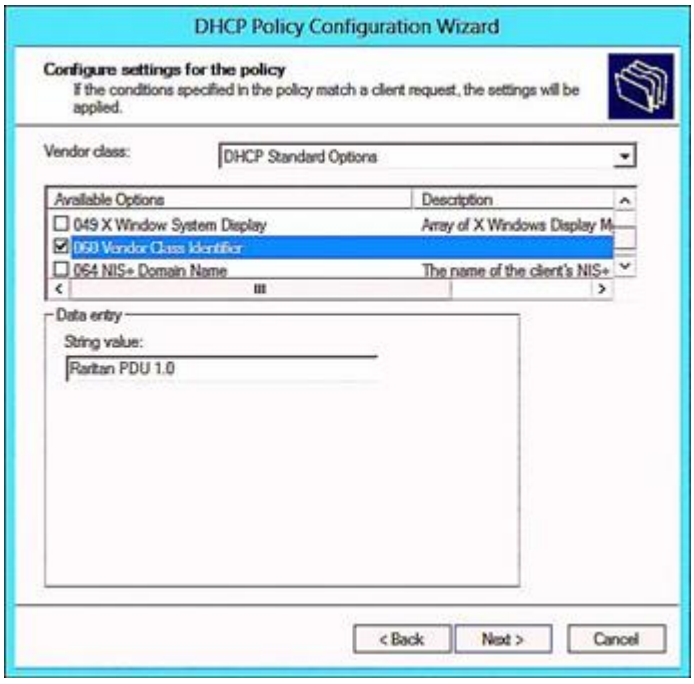
4. Create a new policy associated with the "Raritan PDU" vendor class.
   a. Right-click the Policies node under IPv4 to select New Policy.
   b. Specify a policy name, and click Next.
      The policy is named "PDU" in this illustration.

   c. Click Add to add a new condition.

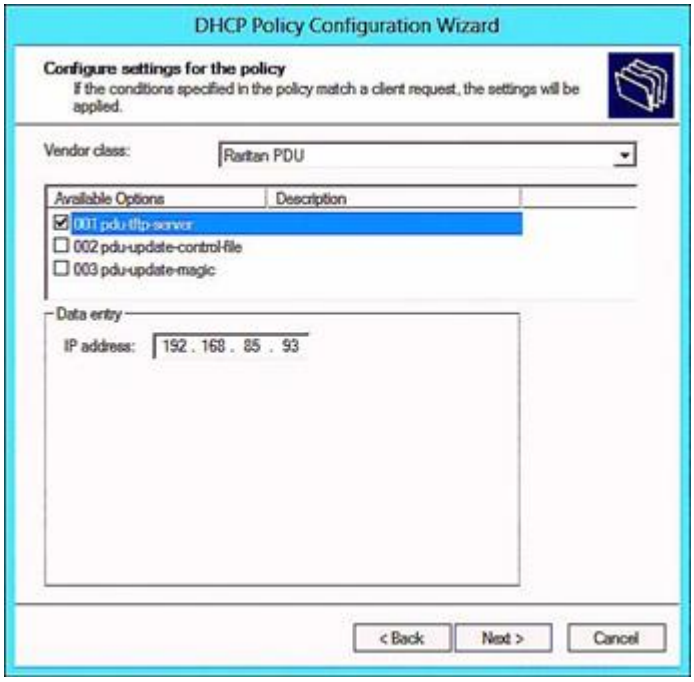
d. Select the vendor class "Raritan PDU" in the Value field, click Add and then Ok.

e. Click Next.

f. Select DHCP Standard Options in the "Vendor class" field, select "060 Vendor Class Identifier" from the Available Options list, and type "Raritan PDU 1.0" in the "String value" field.



g. Select the "Raritan PDU" in the "Vendor class" field, select "001 pdu-tftp-server" or "007 pdu-https-server" from the Available Options list, and type your TFTP/https server's IPv4 address in the "IP address" field.

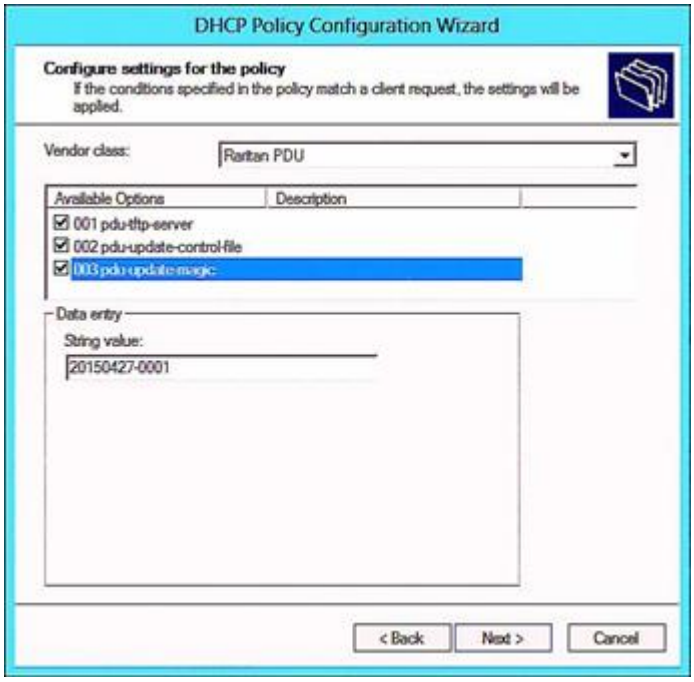


h. Select "002 pdu-update-control-file" from the Available Options list, and type the filename "fwupdate.cfg" in the "String value" field.

i. Select "003 pdu-update-magic" from the Available Options list, and type any string in the "String value" field. This third option/code is the magic cookie to prevent the *fwupdate.cfg* commands from being executed repeatedly. It does NOT matter whether the IPv4 magic cookie is identical to or different from the IPv6 magic cookie.

   The magic cookie is a string comprising numerical and/or alphabetical digits in any format. In the following illustration diagram, it is a combination of a date and a serial number.

Important: The magic cookie is transmitted to and stored in PX4 at the time of executing the "fwupdate.cfg" commands. The DHCP(TFTP/HTTPS) operation is triggered only when there is a mismatch between the magic cookie in DHCP and the one stored in PX4. Therefore, you must modify the magic cookie's value in DHCP when intending to execute the "fwupdate.cfg" commands next time.

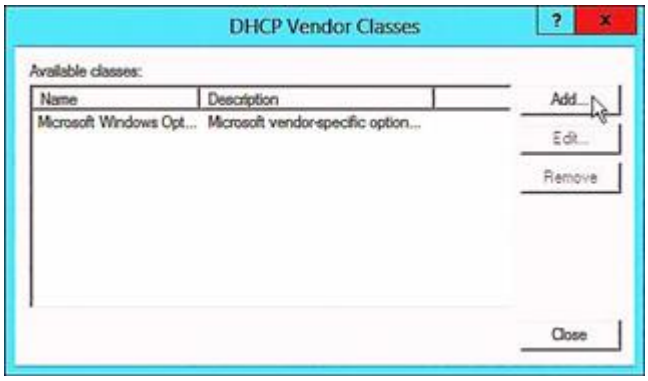


DHCP IPv6 Configuration in Windows

For those PX4 devices using IPv6 addresses, follow this procedure to configure your DHCP server. The following illustration is based on Microsoft® Windows Server 2012 system.

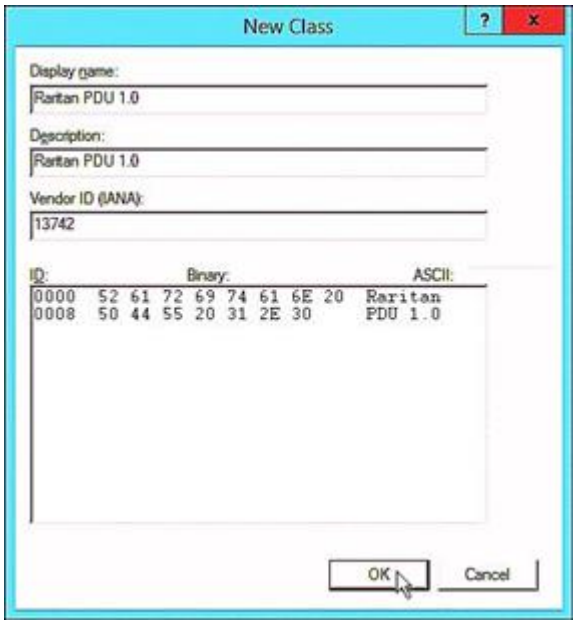
► *Required Windows IPv6 settings in DHCP:*

1. Add a new vendor class for Raritan's PX4 under IPv6.
   a. Right-click the IPv6 node in DHCP to select Define Vendor Classes.
   b. Click Add to add a new vendor class.



   c. Specify a unique name for the vendor class, type "13742" in the "Vendor ID (IANA)" field, and type the binary codes of "Raritan PDU 1.0" in the New Class dialog.

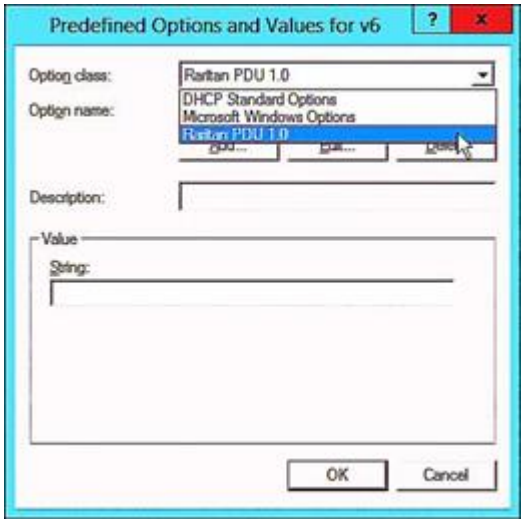
The vendor class is named "Raritan PDU 1.0" in this illustration.



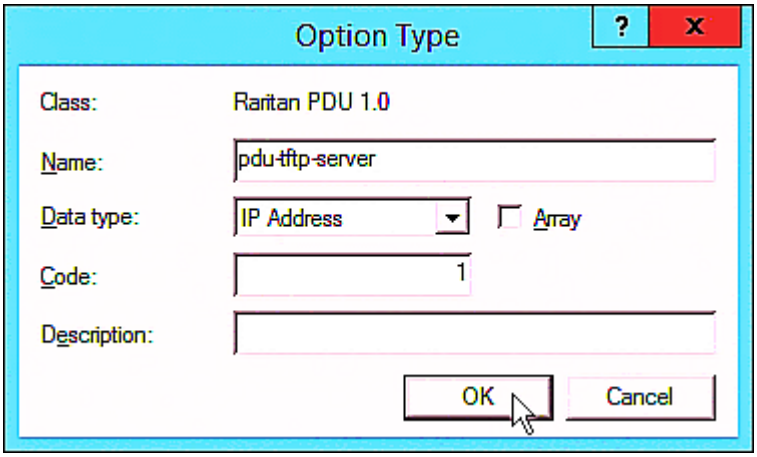
2. Add three options to the "Raritan PDU 1.0" vendor class.

a. Right-click the IPv6 node in DHCP to select Set Predefined Options.

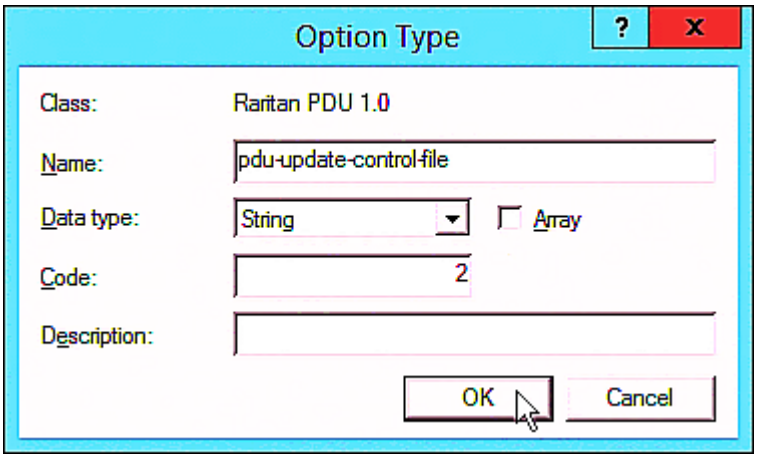
b. Select Raritan PDU 1.0 in the "Option class" field.



c. Click Add to add the first option. Type "pdu-tftp-server" or "pdu-https-server" in the Name field, select IP Address as the data type, and type 1 in the Code field and type 7 in the Code field for https server.

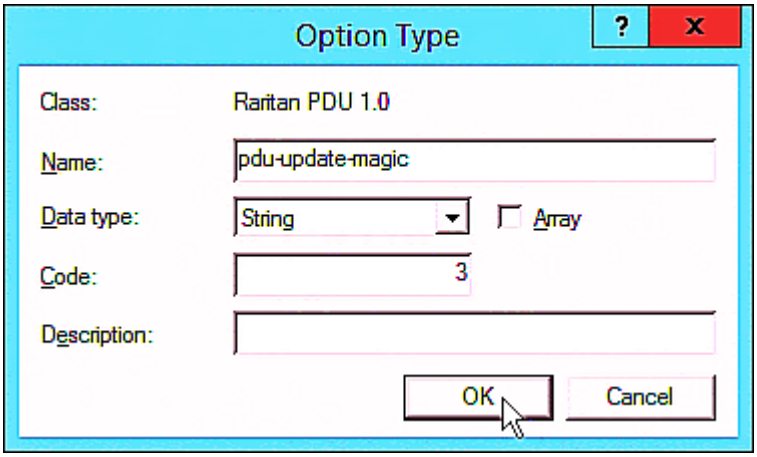


d. Click Add to add the second option. Type "pdu-update-control-file" in the Name field, select String as the data type, and type 2 in the Code field.



e. Click Add to add the third one. Type "pdu-update-magic" in the Name field, select String as the

data type, and type 3 in the Code field.

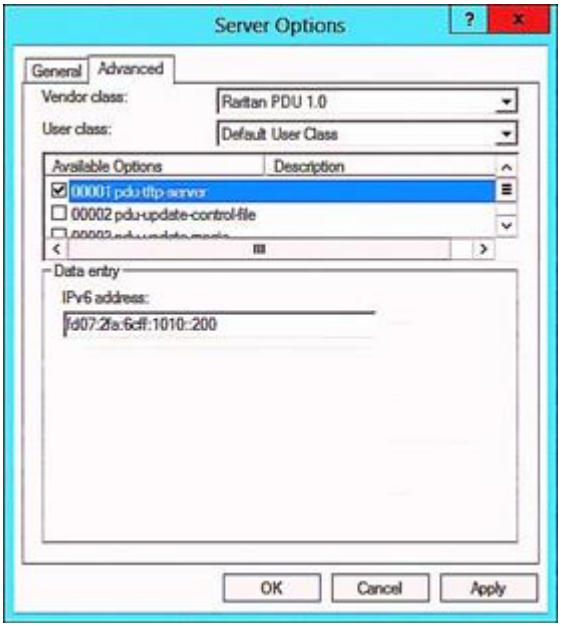


3. Configure server options associated with the "Raritan PDU 1.0" vendor class.

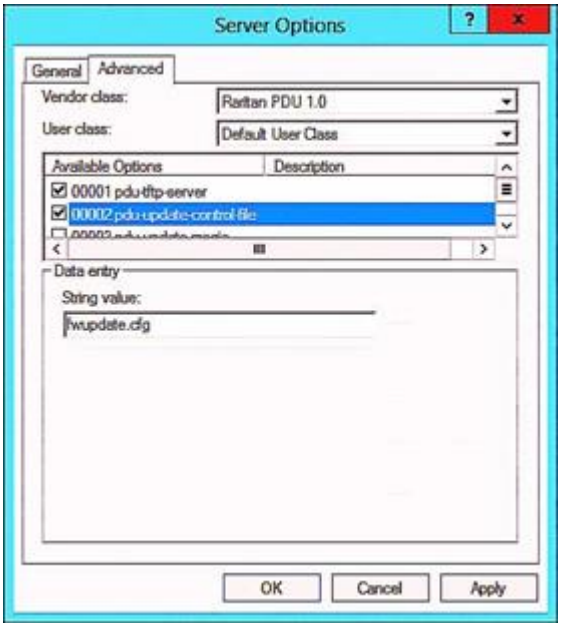
a. Right-click the Server Options node under IPv6 to select Configure Options.

b. Click the Advanced tab.

c. Select "Raritan PDU 1.0" in the "Vendor class" field, select "00001 pdu-tftp-server" or "00007 pdu-https-server" from the Available Options list, and type your TFTP/HTPPS server's IPv6 address in the "IPv6 address" field.



d. Select "00002 pdu-update-control-file" from the Available Options list, and type the filename "fwupdate.cfg" in the "String value" field.

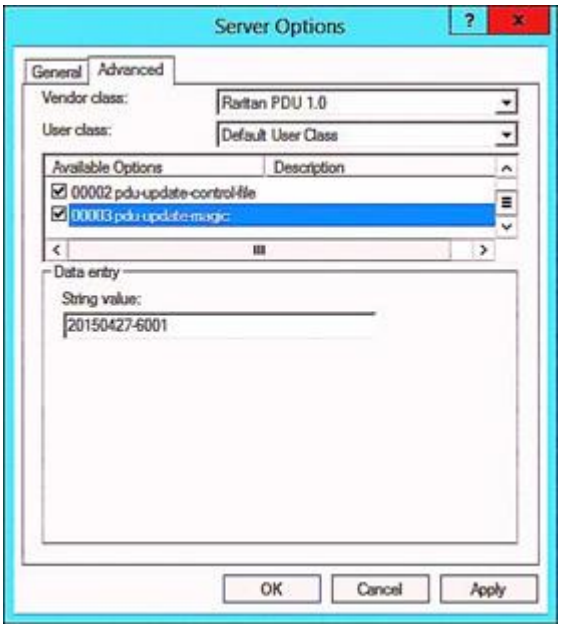


e. Select "00003 pdu-update-magic" from the Available Options list, and type any string in the "String value" field. This third option/code is the magic cookie to prevent the *fwupdate.cfg* commands from being executed repeatedly. It does NOT matter whether the IPv6 magic cookie

is identical to or different from the IPv4 magic cookie.

The magic cookie is a string comprising numerical and/or alphabetical digits in any format. In the following illustration diagram, it is a combination of a date and a serial number.

Important: The magic cookie is transmitted to and stored in PX4 at the time of executing the "fwupdate.cfg" commands. The DHCP(TFTP/HTTPS) operation is triggered only when there is a mismatch between the magic cookie in DHCP and the one stored in PX4. Therefore, you must modify the magic cookie's value in DHCP when intending to execute the "fwupdate.cfg" commands next time.



DHCP IPv4 Configuration in Linux

Modify the "dhcpd.conf" file for IPv4 settings when your DHCP server is running Linux.

► *Required Linux IPv4 settings in DHCP:*

1. Locate and open the "dhcpd.conf" file of the DHCP server.
2. The PX4 will provide the following value of the vendor-class-identifier option (option 60).
   - vendor-class-identifier = "Raritan PDU 1.0"

Configure the same option in DHCP accordingly. The PX4 accepts the configuration or firmware upgrade only when this value in DHCP matches.

3. Set the following three sub-options in the "vendor-encapsulated-options" (option 43).
   - code 1 (pdu-tftp-server) = the TFTP server's IPv4 address or
   - code 7 (pdu-https-server) = the HTTPS server's IPv4 address
   - code 2 (pdu-update-control-file) = the name of the control file "fwupdate.cfg"
   - code 3 (pdu-update-magic) = any string

This third option/code is the magic cookie to prevent the *fwupdate.cfg* commands from being executed repeatedly. It does NOT matter whether the IPv4 magic cookie is identical to or different from the IPv6 magic cookie.

The magic cookie is a string comprising numerical and/or alphabetical digits in any format. In the following illustration diagram, it is a combination of a date and a serial number.

Important: The magic cookie is transmitted to and stored in PX4 at the time of executing the "fwupdate.cfg" commands. The DHCP(TFTP/HTTPS) operation is triggered only when there is a mismatch between the magic cookie in DHCP and the one stored in PX4. Therefore, you must modify the magic cookie's value in DHCP when intending to execute the "fwupdate.cfg" commands next time.

► *IPv4 illustration example in dhcpd.conf:*

```
[...]

set vendor-string = option vendor-class-identifier;
option space RARITAN code width 1 length width 1 hash size 3;
option RARITAN.pdu-tftp-server code 1 = ip-address;
option RARITAN.pdu-update-control-file code 2 = text;
option RARITAN.pdu-update-magic code 3 = text;
option RARITAN.pdu-model code 4 = text;
option RARITAN.pdu-serial code 5 = text;
option RARITAN.pdu-cascading-info code 6 = text;
option RARITAN.pdu-http-uri-base code 7 = text;

option local-encapsulation code 43 = encapsulate RARITAN;

class "raritan" {
    match if option vendor-class-identifier = "Raritan PDU 1.0";
    vendor-option-space         RARITAN;
    option RARITAN.pdu-tftp-server 192.168.1.7;
    option RARITAN.pdu-http-uri-base "https://192.168.1.100/update";
    option RARITAN.pdu-updateupdate-control-file "fwupdate.cfg";
    option RARITAN.pdu-update-magic "20150123-0001";
    option vendor-class-identifier "Raritan PDU 1.0";

    # optional logging of the parameters sent by the PDU
    log(info, concat("PDU model: ", option RARITAN.pdu-model));
    log(info, concat("PDU serial: ", option RARITAN.pdu-serial));
    log(info, concat("PDU cascading info: ", option RARITAN.pdu-cascading-info));
}

[...]
```

DHCP IPv6 Configuration in Linux

Modify the "dhcpd6.conf" file for IPv6 settings when your DHCP server is running Linux.

► *Required Linux IPv6 settings in DHCP:*

1. Locate and open the "dhcpd6.conf" file of the DHCP server.
2. The PX4 will provide the following values to the "vendor-class" option (option 16). Configure related settings in DHCP accordingly.

- 13742 (Raritan's IANA number)
- Raritan PDU 1.0
- 15 (the length of the above string "Raritan PDU 1.0")

3. Set the following three sub-options in the "vendor-opts" (option 17).
   - code 1 (pdu-tftp-server) = the TFTP server's IPv6 address or
   - code 7 (pdu-https-server) = the HTTPs server's IPv6 address
   - code 2 (pdu-update-control-file) = the name of the control file "fwupdate.cfg"
   - code 3 (pdu-update-magic) = any string

     This third option/code is the magic cookie to prevent the *fwupdate.cfg* commands from being executed repeatedly. It does NOT matter whether the IPv6 magic cookie is identical to or different from the IPv4 magic cookie.

     The magic cookie is a string comprising numerical and/or alphabetical digits in any format. In the following illustration diagram, it is a combination of a date and a serial number.

Important: The magic cookie is transmitted to and stored in PX4 at the time of executing the "fwupdate.cfg" commands. The DHCP(TFTP/HTTPS) operation is triggered only when there is a mismatch between the magic cookie in DHCP and the one stored in PX4. Therefore, you must modify the magic cookie's value in DHCP when intending to execute the "fwupdate.cfg" commands next time.

► *IPv6 illustration example in dhcpd6.conf:*

```
[...]

option space RARITAN code width 2 length width 2 hash size 3;
option RARITAN.pdu-tftp-server code 1 = ip6-address;
option RARITAN.pdu-update-control-file code 2 = text;
option RARITAN.pdu-update-magic code 3 = text;
option RARITAN.pdu-model code 4 = text;
option RARITAN.pdu-serial code 5 = text;
option RARITAN.pdu-cascading-info code 6 = text;
option RARITAN.pdu-http-uri-base code 7 = text;
option vsio.RARITAN code 13742 = encapsulate RARITAN;

[...]

# optional logging of the parameters sent by the PDU
log(info, concat("PDU model: ", option RARITAN.pdu-model));
log(info, concat("PDU serial: ", option RARITAN.pdu-serial));
log(info, concat("PDU cascading info: ", option RARITAN.pdu-cascading-info));

subnet6 xxxx {

[...]
        option RARITAN.pdu-tftp-server 1::2;
        option RARITAN.pdu-http-uri-base "https://192.168.1.100/update";
        option RARITAN.pdu-update-control-file "fwupdate.cfg";
        option RARITAN.pdu-update-magic "20150123-0001";
[...]

}
```

Raw Configuration Upload and Download

You can modify any existing "config.txt", and then upload it to a specific device for modifying part or all of its settings. Both configuration download and upload operations require the Administrator Privileges.

There are two ways to get one "config.txt":

- You create this file by yourself. See Configuration Files (on page 574).
- You download the raw configuration data from the device.

The downloaded raw configuration contains almost all of current settings on your device.

Warning: When you download the raw configuration data, some configuration keys are commented out and must remain that way. See Keys that Cannot Be Uploaded (on page 614).

Download via Web Browsers

There are two scenarios by using web browsers.

► *URL containing login credentials:*

To log in immediately while issuing the download request, type an URL containing the login credentials in the web browser.

Raritan
A brand of legrand

```
http(s)://<user>:<password>@<device IP>/cgi-bin/raw_config_download.cgi
```

Parameter	Description
<user>	Any user name that has the Administrator Privileges.
<password>	The password of the specified user name.
<device IP>	Hostname or IP address of the device whose raw configuration you want to download.

- For example:

```
https://admin:admn@192.168.84.114/cgi-bin/raw_config_download.cgi
```

► *URL without login credentials contained:*

If you would like to log in after issuing the download request, type an URL without login credentials contained in the web browser. The system will then prompt you to enter the login credentials.

```
http(s)://<device IP>/cgi-bin/raw_config_download.cgi
```

- For example:

```
https://192.168.84.114/cgi-bin/raw_config_download.cgi
```

Download via Curl

If you have installed curl on your computer, you can download the raw configuration from your device by performing the curl command.

► *To download raw configuration via curl:*

1. Type the following curl command in the command line interface.

```
curl -k https://<user>:<password>@<device IP>/cgi-bin/raw_config_download.cgi > config.txt
```

Parameter	Description
<user>	Any user name that has the Administrator Privileges.
<password>	The password of the specified user name.

Parameter	Description
<device IP>	Hostname or IP address of the device whose raw configuration you want to download.

2. When the download is complete, a line indicates 100 in the first % column.

3. Go to the directory where you perform the curl command to find the "config.txt" file.

Tip: In the above curl command, you can replace the filename "config.txt" with any filename you prefer.

► *Example:*

```
curl -k https://admin:admn@192.168.84.114/cgi-bin/raw_config_download.cgi
> config.txt
```

Uploading Raw Configuration

There are two upload methods:

- *SCP or PSCP command:* SeeRaw Configuration Upload and Download (on page 602).
- *CURL command:* See Upload via Curl (on page 604).

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.

Authentication-related data or HTTP(S) port may be no longer the same after uploading raw configuration. Therefore, it is suggested to double check what configuration keys will be changed in the raw configuration file that you will upload.

Upload via Curl

If curl is available on your computer, you can upload the raw configuration to PX4 with the curl command.

There are two scenarios with the curl upload methods.

- When there are NO device-specific settings involved, you upload the configuration file only, regardless of the number of PX4 devices to update.
- When there are device-specific settings involved for updating more than one PX4 devices, you must upload two files. including one configuration file and one device list file.

► *To upload one configuration file only:*

1. Type the following curl command in the command line interface.

```
curl -k -F "config_file=@<config file>" https://<user>:<password>@<device IP>/cgi-bin/raw_config_update.cgi
```

Parameter	Description
<user>	Any user name that has the Administrator Privileges.
<password>	The password of the specified user name.
<device IP>	Hostname or IP address of the PX4 whose raw configuration you want to upload.
<config file>	Filename of the configuration file. • For the syntax, see *config.txt* (on page).

2. When the upload is completed successfully, the curl returns the code 0 (zero).

Note: If the upload fails and curl returns other codes, see Curl Upload Return Codes (on page).

---

3. After several seconds, PX4 reboots automatically. Changed settings take effect after the reboot process finishes.

► *To upload both configuration and device list files:*

1. Type the following curl command in the command line interface.

```
curl -k -F "config_file=@<config file>" -F "device_list_file=@<dev_list file>" https://<user>:<password>@<device IP>/cgi-bin/raw_config_update.cgi?match=<dev_col>
```

Parameter	Description
<user>, <password>, <device IP>, <config file>	Refer to the above table for explanation. • For device-specific settings in the <config file>, refer each device-specific configuration key to a specific column in the <dev_list file>. See *config.txt* (on page).
<dev_list file>	Filename of the device list file in CSV format. • For the content format, see *devices.csv* (on page).

Parameter	Description
<dev_col>	<dev_col> comprises "serial:" or "mac:" and the number of the column where the serial number or MAC address of each PX4 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.

2. PX4 will reboot after Curl shows the return code 0. For details, refer to above steps 2 to 3.

► *Examples:*

- Upload of the configuration file only:

```
curl -k -F "config_file=@config.txt" https://admin:admn@192.168.84.114/
cgi-bin/raw_config_download.cgi
```

- Upload of both configuration and device list files:

```
curl -k -F "config_file=@config.txt" -F "device_list_file=@devices.csv"
https://admin:admn@192.168.84.114/cgi-bin/raw_config_download.cgi
```

Curl Upload Return Codes

After performing raw configuration *Upload via Curl* (on page), curl will return a code to indicate the result of the file upload.

Code	Description
0	Operation was successful.
1	An internal error occurred.
2	A parameter error occurred.
3	A raw configuration update operation is already running.
4	The file is too large.
5	Invalid raw configuration file provided.
6	Invalid device list file or match provided.
7	Device list file required but missing.

Code	Description
8	No matching entry in device list found.
9	Macro substitution error.
10	Decrypting value failed.
11	Unknown magic line.
12	Processing magic line failed.

Bulk Configuration, Firmware Upgrade, or Backup/Restore via SCP

You can perform a SSH File Transfer Protocol (SFTP) or Secure Copy (SCP) command to update the firmware, do bulk configuration, or back up and restore the configuration.

Note: Because of security issues the SFTP (SSH File Transfer Protocol) should be used. SCP client in newer OpenSSH versions uses SFTP protocol by default. SCP is still supported and needs to be enabled.

Firmware Update via SCP

Same as any 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 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 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 device, and shows the transmission speed and percentage.
4. When the transmission is complete, it shows the following message, indicating that the PX4 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 device.

b. Copy the configuration file to one or multiple destination device.

Note: You can configure *device-specific* settings with the upload of raw configuration but not with the bulk configuration file.

► *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 any user profile with Administrator Privileges.
   - *<device ip>* is the IP address or hostname of the device whose configuration you want to save.
   - *<filename>* is the custom filename you assign to the "bulk_config.txt" of the source device.
2. Type the user password when prompted.
3. The system saves the configuration to a file named "bulk_config.txt."

► *To copy the configuration via SCP:*

1. Type the following SCP command and press Enter.

```
scp bulk_config.txt <user name>@<device ip>:/bulk_restore
```

   - *<user name>* any user profile with Administrator Privileges
   - *<device ip>* is the IP address of the device whose configuration you want to copy.
2. Type the user password when prompted.
3. The system copies the configuration included in the file "bulk_config.txt" to another device, and displays the following message.

```
Starting restore operation. The connection will be closed now.
```

► *SCP examples:*

- Save operation:

Raritan
A brand of legrand

```
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
```

For the linked units you can backup each unit by specifying the link id.

- Save operation:

```
scp admin@10.0.42.3:/backup_settings.txt/link_id=2 backup_settings.txt
```

- Copy operation:

```
scp backup_settings.txt admin@10.0.42.3:/settings_restore/link_id=2
```

► *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
```

Backup and Restore via SCP

To back up ALL settings of a PX4, 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 PX4 whose settings you want to back up.
2. Type the user password when prompted.
3. The system saves the settings from the PX4 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 PX4 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 PX4, 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.
   - *<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 PX4 whose data you want to download.
   - <port> is the current SSH/SCP port number, or the port number of a specific expansion device in the Port-Forwarding chain.
   - *<filename>* is the new filename of the downloaded file.

   Scenario 1: Use the default SCP port and default filename

   - SSH/SCP port is the default (22), and the accessed PX4 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 PX4 is a Port-Forwarding expansion 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 PX4 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 PX4 is a Port-Forwarding expansion device.
- Renaming the diagnostic file is wanted.

```
scp -P <port> <user name>@<device ip>:/diag-data.zip <filename>
```

2. Type the password when prompted.
3. The system downloads the specified data from the PX4 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 device for review, backup or modification.

After modifying or creating any raw configuration data, you can upload it to a specific device 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. See config.txt.

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 device. See Keys that Cannot Be Uploaded (on page 614).

► *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 device 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 device is a Port-Forwarding expansion 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 device is a standalone device.
- Renaming the raw configuration file is wanted.

```
scp <user name>@<device ip>:/raw_config.txt <filename>
```


Raritan
A brand of legrand

Scenario 4: Specify a different SCP port and a new filename

- SSH/SCP port is NOT the default (22), or the accessed device is a Port-Forwarding expansion 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 device whose data you want to download.
- <port> is the current SSH/SCP port number, or the port number of a specific link unit 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 device 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:*

1. Type one of the following SCP commands and press Enter.

Scenario 1: Only one device to configure, with the default SCP port

- SSH/SCP port is the default (22), and the accessed device 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 device to configure, with a non-default SCP port

- SSH/SCP port is NOT the default (22), or the accessed device is a Port-Forwarding expansion 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 device to configure, with the default SCP port

- SSH/SCP port is the default (22), and the accessed device 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 device to configure, with a non-default SCP port

- SSH/SCP port is NOT the default (22), or the accessed device is a Port-Forwarding expansion 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 device where you want to upload the specified file.
- <port> is the current SSH/SCP port number, or the port number of a specific expansion device in the Port-Forwarding chain.
- `<dev_list file>` is the name of the CSV file for configuring multiple device with device-specific settings. For this file's format, see devices.csv.
  - For device-specific settings in the `<config file>`, refer each device-specific configuration key to a specific column in the `<dev_list file>`. See config.txt.
- `<dev_col>` comprises "serial:" or "mac:" and the number of the column where the serial number or MAC address of each device 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.

Keys that Cannot Be Uploaded

The raw configuration downloaded from any PX4 contains a few configuration keys that are commented out with either syntax below.

These configuration keys cannot be part of the configuration that you will upload to any PX4. That is, they should be either not available or remain commented out in the configuration file you will upload.

Comment syntax	Description
#INTERNAL#	Internal use only. They are NOT user configurable settings.
#OLD/INVALID#	These keys are old or invalid ones.

Cascading Solutions for Xerus

In This Chapter

Cascading Solution Overview. 616
Cascading Procedure Overview. 621
Cascading Modes Overview. 621
Setting the Cascading Mode. 623
Device-Cascading Methods. 626
Adding, Removing or Swapping Cascaded Devices. 635
Accessing Cascaded Devices. 637
Identifying Cascaded Devices. 641
Firmware Upgrade for Cascading Chains. 650
Cascade Troubleshooting. 651

Cascading Solution Overview

Multiple power products can share network connectivity by cascading them through the USB or Ethernet interface. To reduce the number of Ethernet connections or save networking costs in your data center, you can apply this cascading solution.

You can access and administer each device in the cascading chain over the Internet from anywhere via various protocols -- HTTP(S), SNMP, SSH, Telnet and Modbus. Each device can be upgraded respectively.

Applicable Products

The Xerus Technology platform's cascading solution is supported on the following products.

► *Xerus requirements:*

- All devices must run Xerus firmware version 3.3.10 or later. Check firmware versions before cascading your devices and upgrade any device as needed.
- If your cascade includes "newer" devices, such as SRC, PX4, PRO4X, and PRO3X, note that newer devices are only supported as of their introductory firmware version. Avoid downgrading cascades.

► *Raritan products:*

- PX4 PDUs
- PX2 series PDUs
- PX3 series PDUs, including PX3-iX7
- PX3TS transfer switches, including PX3TS-iX7
- Branch Circuit Monitor 2 (BCM2), PMC and PMMC series, including:
- BCM2-iX7
- PMC-iX7

- PXC series PDUs
- PXO series PDUs
- Smart Rack Controller (SRC)

► *Server Technology products:*

- PRO4X PDUs
- PRO3X PDUs

► *Legrand products:*

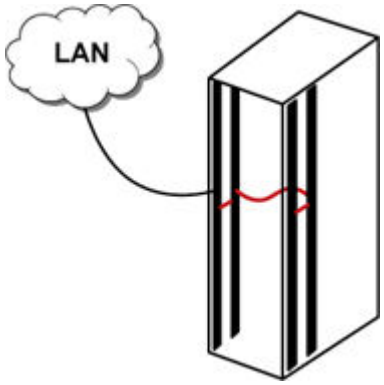
- Legrand PDUs

Illustration

In a cascading chain, all PDUs are cascaded via USB or Ethernet, and only the primary device is connected to the LAN.

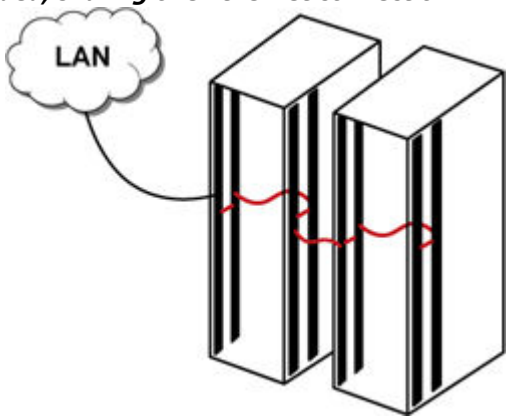
The following diagrams illustrate different cascading scenarios using Zero U PDUs. Red lines in the diagrams represent the cascading connections, which are either USB or standard network patch cables.

► *Scenario 1: Cabinet 1 has four PDUs cascaded, sharing one Ethernet connection.*



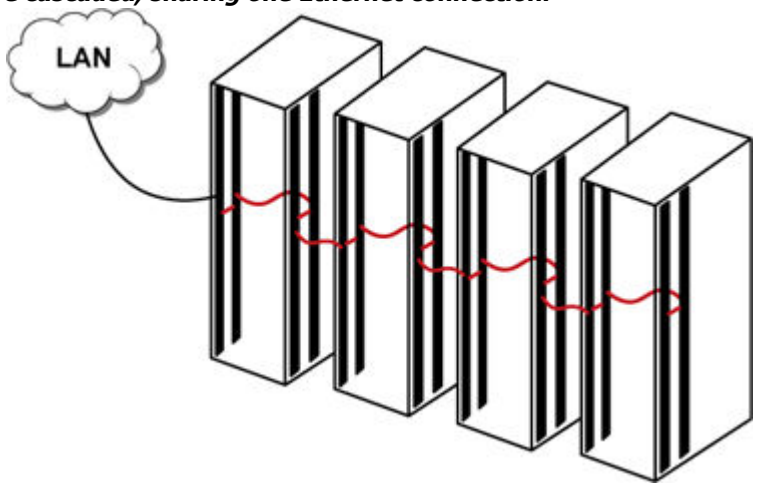
► *Scenario 2: Cabinet 1 and Cabinet 2 have four PDUs respectively.*

The eight PDUs are cascaded, sharing one Ethernet connection.



► *Scenario 3: Cabinet 1 through Cabinet 4 have four PDUs respectively.*

The 16 PDUs are cascaded, sharing one Ethernet connection.



Best Practices for Cascading

► *One Ethernet connection per cabinet is better:*

One Ethernet connection per cabinet is better than one Ethernet connection across cabinets because of these advantages:

- Easier to manage or maintain one cabinet when all of the cabling and connections are located in the same cabinet.
- Reduces cross-cabinet cabling.

► *When to establish a chain comprising 32 devices:*

A chain consisting of 32 devices saves the most Ethernet connections and costs, and it is recommended only when:

- External Ethernet ports are expensive or limited.
- Available IP addresses are limited.

► *Ethernet cascading is recommended for PDUs/Devices with Dual Ethernet ports:*

When cascading devices that have dual Ethernet ports, choose Ethernet cascading when possible instead of USB cascading. The Ethernet interface offers the following benefits over USB.

- Longer cabling distance
- Lower latency
- Connection more reliable with RJ-45 connectors

Supported products with dual Ethernet ports include: Raritan's PX3-iX7 PDUs, PX3TS-iX7 transfer switches, PXC PDUs, PXO PDUs, SRC, Legrand PDUs, Server Technology PRO3X and PRO4X PDUs.

When to Avoid Cascading Devices

There are two scenarios where the cascading solution is NOT recommended.

► *High network reliability is required:*

The cascading solution increases the number of network bridging points for cascaded devices, which may result in network unreliability. Therefore, when high network reliability is required, establish a separate network connection for each PDU to minimize the number of potential network failure points.

► *High bandwidth is required:*

The bandwidth among cascaded devices is limited by the USB or Ethernet interface where they are connected. When high bandwidth is required, such as transmission of webcam videos, it is strongly recommended to directly connect that PDU to the network to optimize the data transfer rate.

The maximum bandwidth supported by each interface:

- *USB*:
  - 12 Mbps (half duplex) when both or either side supports full-speed USB only.
  - 480 Mbps (half duplex) when both cascaded devices support high-speed USB.
- Ethernet:
  - 100 Mbps, full duplex

Note: Effective throughput may be lower than the rate listed due to protocol overhead.

Cascading Procedure Overview

You must follow the steps below to establish a cascading chain.

Warning: Networking issues occur if the following steps are reversed.

► *Main cascading procedure:*

1. Log in to each PDU and configure the cascading mode.
2. Cascade all devices.

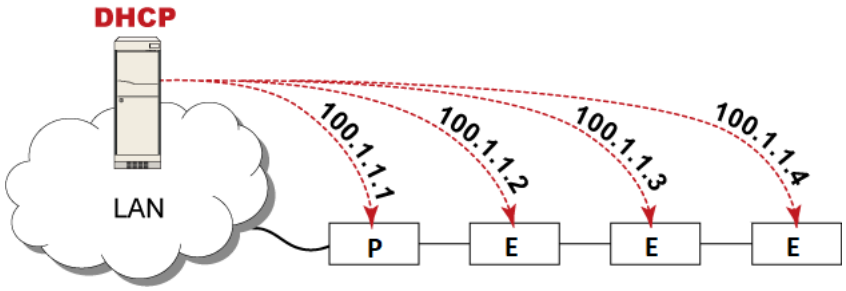
Cascading Modes Overview

The cascading mode is a network configuration setting that determines how each device in the chain is accessed.

There are two cascading modes: Bridging and Port Forwarding.

In the following illustration, it is assumed that users enable the DHCP networking for the cascading chain comprising four devices. In the diagrams, "P" is the primary device and "E" is an expansion device.

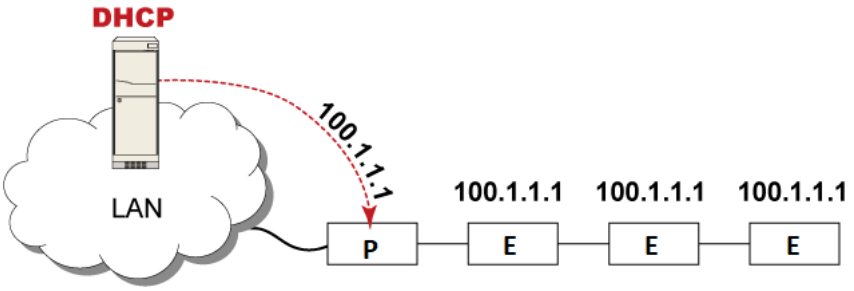
► *"Bridging" mode:*



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

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

► *"Port Forwarding" mode:*



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

You must specify a 5XXXX port number (where X is a number) when remotely accessing any expansion device with the shared IP address. See Port Number Syntax (on page 250), Port Number Syntax (on page 637).

► *Comparison between cascading modes:*

- The Bridging mode supports the wired network only, while the Port Forwarding mode supports both wired and wireless networks.
- Both cascading modes support a maximum of 32 devices in a chain.
- Both cascading modes support both DHCP and static IP addressing.
- In the Bridging mode, each cascaded device has a unique IP address.

  In the Port Forwarding mode, all cascaded devices share the same IP address(es) as the primary device.
- In the Bridging mode, each cascaded device has only one IP address.

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

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

Setting the Cascading Mode

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

Different cascading modes in a chain cause a networking failure in all subsequent expansion devices.

Repeat the following procedure for each device you want to cascade until all devices share the same cascading mode.

The cascading mode can be configured via the web interface or command line interface (CLI).

You must have the Change Network Settings permission to configure the cascading mode.

► *To set the cascade mode in the web interface:*

1. Log in to the web interface of each device you intend to cascade.
2. Choose Device Settings > Network.
3. Select the preferred mode in the Cascading Mode field.

Mode	Description
None	No cascading mode is enabled. This is the default.
Bridging	Each device in the cascading chain is accessed with a different IP address.
Port Forwarding	Each device in the cascading chain is accessed with the same IP address(es) but with a different port number assigned. See Port Number Syntax (on page 250), Port Number Syntax (on page 637).

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

1. For the Port Forwarding mode, one to two more fields have to be configured.

Note that if either setting below is incorrectly configured, a networking issue occurs.

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

2. (Optional) Configure the network settings by clicking the BRIDGE, ETH1/ETH2, or WIRELESS section on the same page.
   - In the Bridging mode, each cascaded device can have different network settings. You may need to configure each device's network settings in the BRIDGE section.
   - In the Port Forwarding mode, all cascaded devices share the primary device's network settings. You only need to configure the primary device's network settings in the ETH1/ETH2 and/or WIRELESS section.

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

3. Click Save.

► *To set the cascade mode in the CLI:*

1. Access each device you intend to cascade via CLI.
2. Type `config` and press Enter to enter the configuration mode.
3. Type the following command to set 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 primary device, you must configure the 'downstream interface' setting.

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

Variables:

- <option2> is one of the following cascading roles:

Role	Description
primary	The device is a primary device.
expansion	The device is a expansion device.

- <option3> is one of the following options:

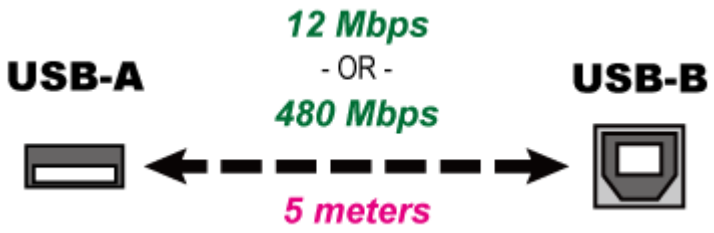
Option	Description
ETH1/ETH2	port is the port where the 1st expansion device is connected.
Usb	USB port is the port where the 1st expansion device is connected.

Device-Cascading Methods

There are two cascading methods.

- *USB cascading*: All devices in the chain are cascaded via USB ports. All products described in this guide support this cascading method.
- *Extended cascading*: Devices in the chain are cascaded via either USB or Ethernet ports, as needed. Only devices with dual Ethernet ports can be cascaded in this way. Supported products have iX7, iX9, or PRO3X NIM8G2 controllers with dual ethernet ports.

USB Cascading



Products with full-speed USB transfer data at a maximum rate of 12 Mbps.

Products with high-speed USB transfer data at a maximum rate of 480 Mbps. iX7, iX9 and Pro3X controllers support high-speed USB.

USB communication is always half duplex.

Note that the USB bandwidth between the primary and the first expansion device will limit the actual data transfer rate between all USB-cascaded expansion devices.

Tip: If two or more PDUs with high-speed USB are involved in a USB-cascading chain, you can set them as the primary and the first expansion units for optimal data transmission.

The distance between two USB-cascaded devices CANNOT exceed 5 meters (16 feet).

USB-Cascading Requirements

The USB-cascading chain comprises either identical or diverse supported products. For example, you can cascade PX3 PDUs only, or you can mix other supported models in a USB-cascading chain.

► *Hardware requirements:*

Raritan/Legrand/ServerTech products	*Number of USB-A ports*
PX4 series PDU	***2***
PX3 series PDUs, including PX3-iX7	***2***
PX2 series PDUs	***1***
PX3TS transfer switches, including PX3TS-iX7	***2***
BCM2	***2***
PMC	***2***
PMMC	***1***
PXC	***1***
PXO	***1***
Legrand PDUs	***1***
SRC	***2***
PRO4X PDU	***2***

Raritan/Legrand/ServerTech products	*Number of USB-A ports*
PRO3X PDU	***1***

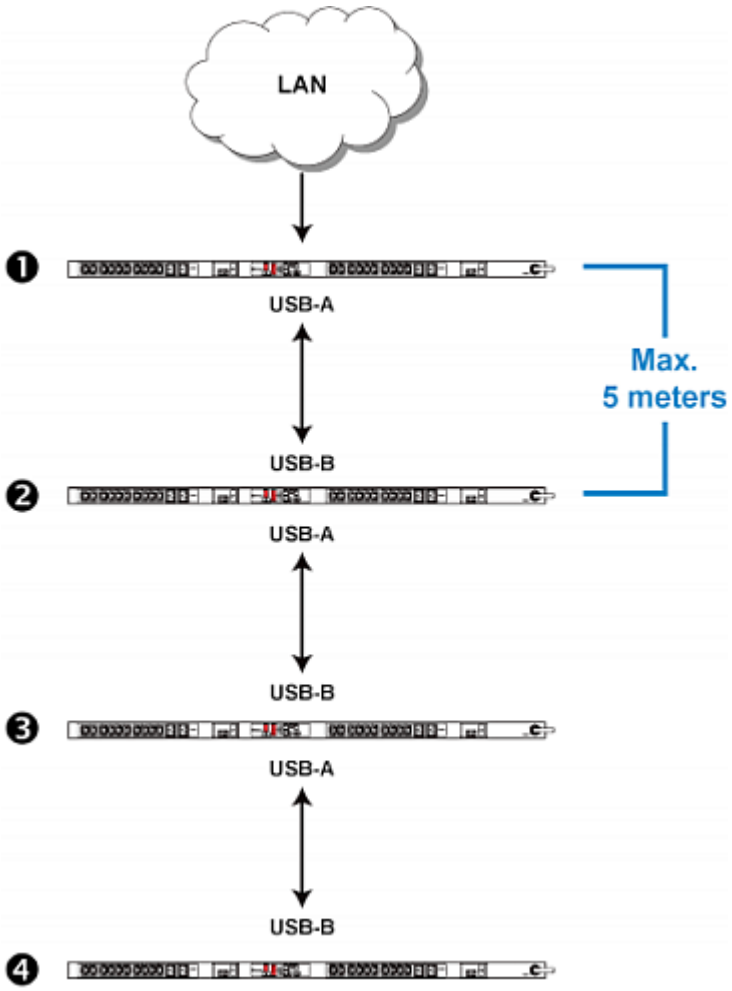
- If wireless networking is wanted, the primary device must be a product with "dual" USB-A ports.

Cascading All Devices via USB-Only

To avoid networking problems, make sure to configure each unit's Cascading Mode in the network settings before creating the cascade. All units in a cascade must be in the same cascading mode.

- Any certified USB 2.0 cable up to 5 meters (16 feet) long can be used.
- Up to 32 units in total can be cascaded. 1 Primary unit and 31 Expansion units.

The following illustrates a USB-cascading chain.



Number	Device role
❶	Primary unit
❷	Expansion 1
❸	Expansion 2
❹	Expansion 3

► *To cascade devices:*

1. Connect the Primary unit to the LAN, using a method below.
   - Bridging mode:
     Use a standard network patch cable (CAT5e or higher).
   - Port Forwarding mode:
     Use a standard network patch cable and/or a Raritan USB WIFI wireless LAN adapter.
2. Connect the USB-A port of the primary device to the USB-B port of the next product you want to cascade. This additional unit is Expansion 1.
3. Connect Expansion 1's USB-A port to the USB-B port of the next product via another USB cable. The second additional device is Expansion 2.
4. Repeat to connect all remaining expansion devices.

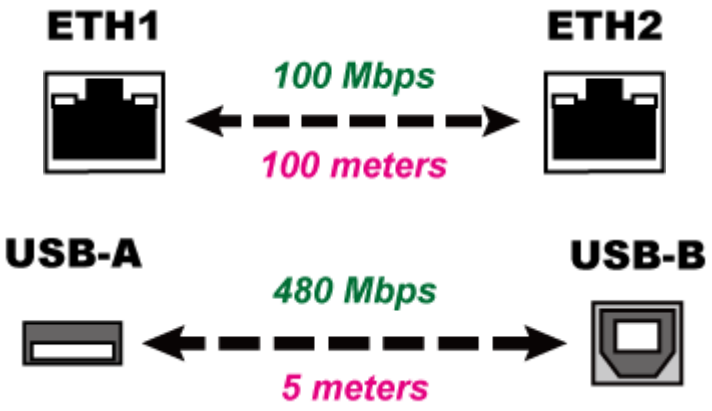
Extended Cascading for Dual Ethernet and USB

Extended cascading can be made via USB or Ethernet interfaces on devices with Dual Ethernet and high-speed USB. See Extended-Cascading Requirements (on page 630)

Data transfer speeds and cable restrictions vary:

Item	Maximum rate or distance
Data transfer rate	• *USB*: 480 Mbps (half duplex) • Ethernet: 100 Mbps (full duplex)

Cabling distance between two cascaded devices	• *USB*: 5 meters (16 feet) • *Ethernet*: 100 meters (328 feet)



Extended-Cascading Requirements

The extended-cascading chain must meet these requirements.

► *Hardware requirements:*

All cascaded devices must have dual Ethernet ports and at least one USB-A port. This includes Raritan/Legrand/Servertech supported devices with:

- iX7 controller
- iX9 controller
- Pro3X NIM8G controller

Note: There is one exception for iX7 controllers. Raritan's BCM2 series, including BCM2-iX7, PMC-iX7 and PMMC, are not supported because they have only one Ethernet port in their iX7 controller.

Cascading Devices via Dual Ethernet and USB

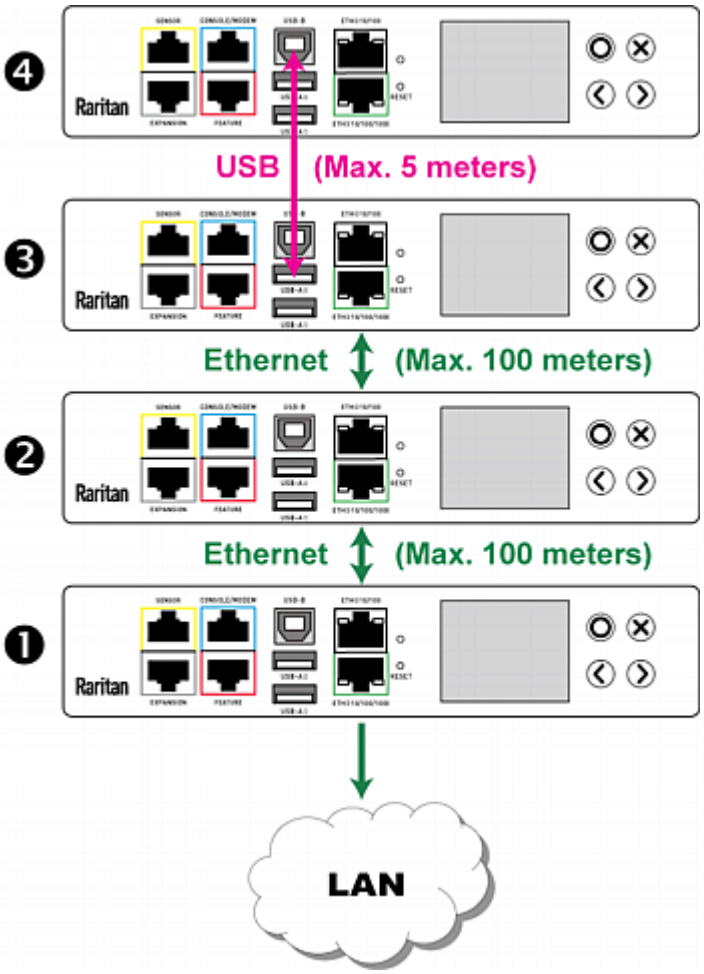
To avoid networking problems, make sure to configure each unit's Cascading Mode in the network settings before creating the cascade. All units in a cascade must be in the same cascading mode.

Make sure all devices in your intended cascade support Extended Cascading. See Extended-Cascading Requirements (on page 630).

When cascading devices in a port forwarding configuration, make sure to follow additional restrictions. See Restrictions of Port-Forwarding Connections (on page 633)

- You can use either Ethernet port for cascading.
- If the two Ethernet ports support different network speeds, use the faster one for the upstream connection.

Note: The following diagram illustrates PX3-iX7 Zero U PDUs, but the same procedure also applies to all supported devices.



Number	Device role
❶	Primary unit
❷	Expansion 1

Number	Device role
❸	Expansion 2
❹	Expansion 3

► *To cascade via Dual Ethernet ports:*

1. Choose an appropriate device as the primary unit.
2. Connect the Primary unit to the LAN, using a method below.
   - Bridging mode:
     Use a standard network patch cable (CAT5e or higher).
   - Port Forwarding mode:
     Use a standard network patch cable and/or a Raritan USB WIFI wireless LAN adapter.
3. Connect an available Ethernet port of the primary device to either Ethernet port of another supported device via a standard network patch cable. This additional unit is Expansion 1.
4. Connect Expansion 1's available Ethernet port to either Ethernet port of another supported device via a standard network patch cable. The second additional unit is Expansion 2.
5. In this "extended cascading" configuration, you can also choose to connect expansion units via USB. See Cascading All Devices via USB-Only (on page 628) for instructions.
6. Repeat to connect all remaining expansion devices.

► *Recommendations for cascade loops:*

You can connect both the first and the last PDU to your network (cascade loop) under the following conditions:

a. The remaining network MUST use R/STP to avoid network loops.

AND

b. Both the first and the last PDUs MUST either attach to the same switch or, if they are attached to two separate switches, you must configure both ports of these switches so that the STP costs are high. This prevents the STP protocol from sending unrelated traffic through the PDU cascade, which can cause bottlenecks that lead to connectivity issues in the whole network.

Cascading Restrictions

► *Xerus Version Requirements:*

- Mixing firmware versions is not supported. All cascaded devices must be on the same firmware version to ensure compatibility.

► *Network Requirements:*

- Only the primary device is connected to the LAN. Do NOT connect expansion units to the LAN or WLAN.
- Appropriate networking methods vary based on the cascading mode.
  - The Bridging mode supports the *wired* networking only.
  - The Port Forwarding mode supports both the *wired* and *wireless* networking.
- Your network switch's port security settings must support the cascading solution. Make sure that packets forwarding is enabled for the "external" Ethernet port where the primary device is connected.
- Plug-and-play is not supported. You CANNOT add, remove or swap cascaded devices in a chain randomly. For the appropriate procedure, see Adding, Removing or Swapping Cascaded Devices.

► *Bridging Mode Restrictions:*

- In the Bridging mode, the primary unit device can have only one connection to the network. If the primary device has two Ethernet ports, DO NOT connect both Ethernet ports to the network(s) unless your network has the R/STP protocol enabled.

Note: The Port Forwarding mode does NOT have this restriction. In this mode, you can enable one wired and one wireless network connections for devices with only one Ethernet port, or enable two wired and one wireless network connections for Dual Ethernet devices.

► *Wireless LAN Restrictions (Port Forwarding mode only):*

- You must use Raritan's USB WIFI wireless LAN adapter.
- No external USB hub is used with the primary device.
- To establish a USB-cascading chain, the primary unit must have two USB-A ports so that both the wireless LAN adapter and the expansion device can be connected.

Restrictions of Port-Forwarding Connections

The following guidelines must be obeyed for establishing a cascading chain in the Port Forwarding mode.

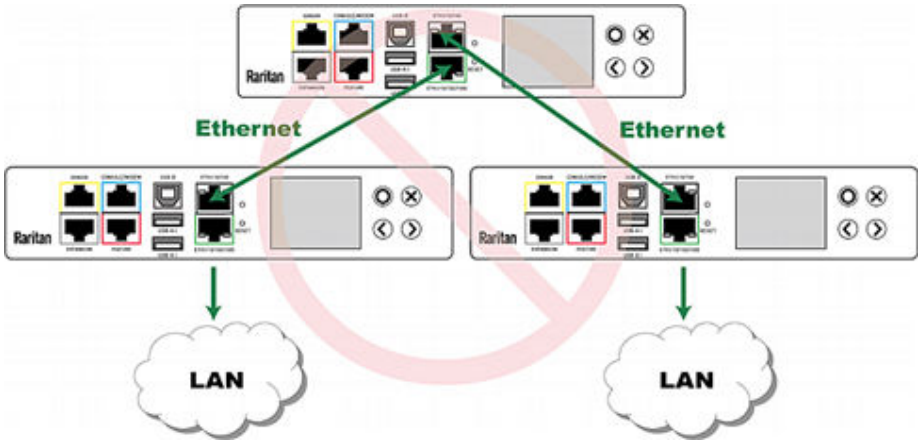
- Each cascaded device, except for the primary device, must have only one upstream device.
- Each cascaded device, except for the last expansion device, must have only one downstream device.
- Use only one cable to cascade two devices. That is, NO simultaneous connection of USB and Ethernet cables between two cascaded devices.

The following diagrams illustrate cascading connections that are NOT supported.

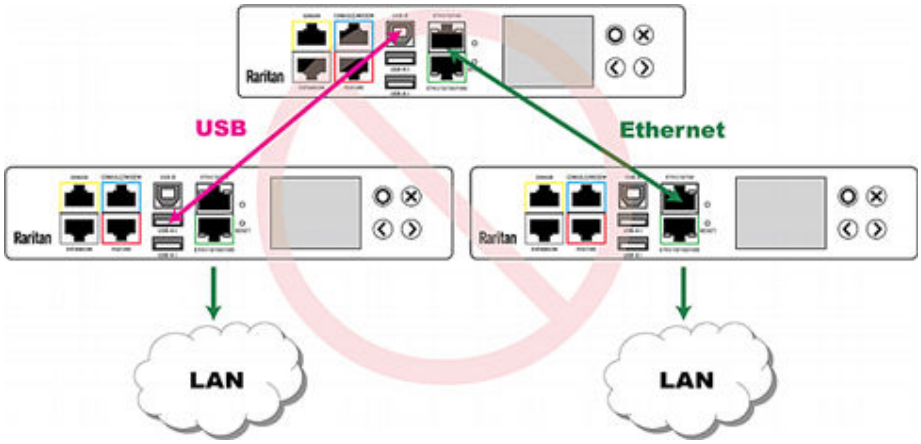
Note: Specific models and port layouts vary, but the same restricted configurations apply to all supported devices.

► *UNSUPPORTED connections:*

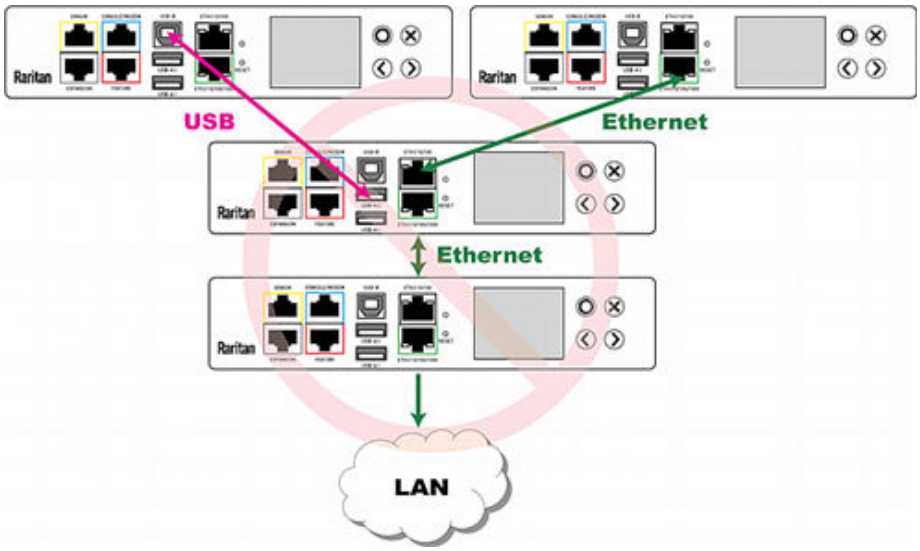
- One cascaded device has two upstream devices via Ethernet cables.



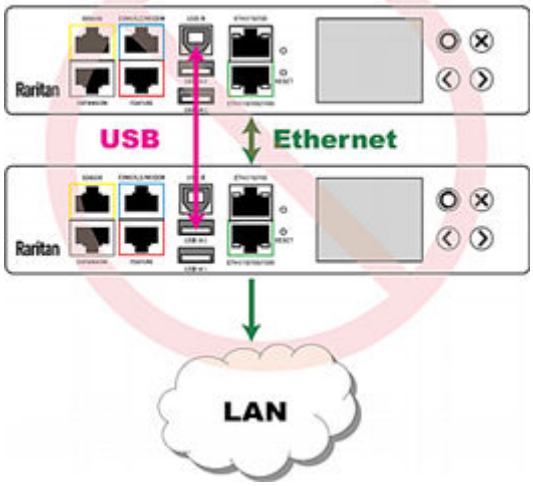
- One cascaded device has two upstream devices via Ethernet and USB cables.



- One cascaded device has two downstream devices.



- One device is connected to another device via two cascading cables - USB and Ethernet cables.



ɡ, Removing or Swapping Cascaded Devices

device's cascading mode first before adding that device to a cascading chain, or before

disconnecting that device from the chain.

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

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

► *To add a device to an existing chain:*

1. Connect the device you will cascade to the LAN and find its IP address, or connect it to a computer.
2. Log in to this device and set its cascading mode to be the same as the existing chain's cascading mode.
3. (Optional) If this device will function as an expansion device, disconnect it from the LAN after configuring the cascading mode.
4. Connect this device to the chain, using either a USB or Ethernet cable.

► *To remove a device from the chain:*

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

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

---

2. Now disconnect it from the cascading chain.

► *To swap the primary and expansion device:*

- In the Bridging mode, you can swap the primary and expansion devices by disconnecting ALL cascading cables from them, and then reconnecting cascading cables. No changes to software settings are required.
- In the Port Forwarding mode, you must follow the procedure below:

Raritan
A brand of legrand

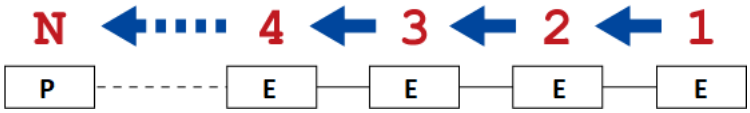
a. Access the expansion device that will replace the primary device, and set its role to 'Primary', and correctly set the downstream interface.
b. Access the primary device, set its role to 'Expansion'.
c. Swap the primary and expansion device now.
   - You must disconnect the LAN cable and ALL cascading cables connected to the two devices first before swapping them, and then reconnecting all cables.

► *To change the cascading mode applied to a chain:*

1. Access the last expansion device, and change its cascading mode.
   - If the new cascading mode is 'Port Forwarding', you must also set its role to 'Expansion'.
2. Access the second to last, third to last and so on until the first expansion device to change their cascading modes one by one.
3. Access the primary device, and change its cascading mode.
   - If the new cascading mode is 'Port Forwarding', you must also set its role to 'Primary', and correctly select the downstream interface.

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

- P = Primary device
- E = Expansion device



Accessing Cascaded Devices

The primary device functions as the network bridge and can transmit IP packets between the LAN and all expansion devices connected to it. Therefore, you can remotely access the primary and every expansion device via the Web (http or https), SNMP, SSH, or Telnet interface.

Port Numbers for Port-Forwarding Devices

All devices in a Port-Forwarding chain share the same IP address(es). Therefore, a TCP/UDP port number is required when accessing any cascaded device in the chain.

Port Number Syntax

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

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

► *5NNXX port number syntax:*

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

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

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

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

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

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

► *Standard TCP/UDP ports:*

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

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

Raritan
A brand of legrand

Protocols	Port Numbers
MODBUS	502

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

Port Forwarding Examples

In this example, Port Forwarding mode is applied to a cascading chain comprising three devices. The IP address is 192.168.84.77.

► *Primary device:*

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

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

Examples using "5NN00" ports:

- To access the primary device via HTTPS, the IP address is: *https://192.168.84.77:50000/*
- To access the primary device via HTTP, the IP address is: *http://192.168.84.77:50100/*
- To access the primary device via SSH, the command is: *ssh -p 50200 192.168.84.77*

Examples using standard TCP/UDP ports:

- To access the primary device via HTTPS, the IP address is: *https://192.168.84.77:443/*
- To access the primary device via HTTP, the IP address is: *http://192.168.84.77:80/*
- To access the primary device via SSH, the command is: *ssh -p 22 192.168.84.77*

► *Expansion 1 device:*

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

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

Examples:

- To access Expansion 1 via HTTPS, the IP address is:
  https://192.168.84.77:50001/
- To access Expansion 1 via HTTP, the IP address is:
  http://192.168.84.77:50101/
- To access Expansion 1 via SSH, the command is:
  ssh -p 50201 192.168.84.77

► *Expansion 2 device:*

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

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

Examples:

- To access Expansion 2 via HTTPS, the IP address is:
  https://192.168.84.77:50002/
- To access Expansion 2 via HTTP, the IP address is:
  http://192.168.84.77:50102/
- To access Expansion 2 via SSH, the command is:
  ssh -p 50202 192.168.84.77

Identifying Cascaded Devices

You can retrieve a device's cascading status from one of these interfaces:

- Web interface: Accessible via HTTP or HTTPS.
- Command line interface (CLI): Accessible via SSH, Telnet or the serial interface.
- SNMP: An SNMP manager is required.
- LCD display: Use the front panel LCD display if your device has it.

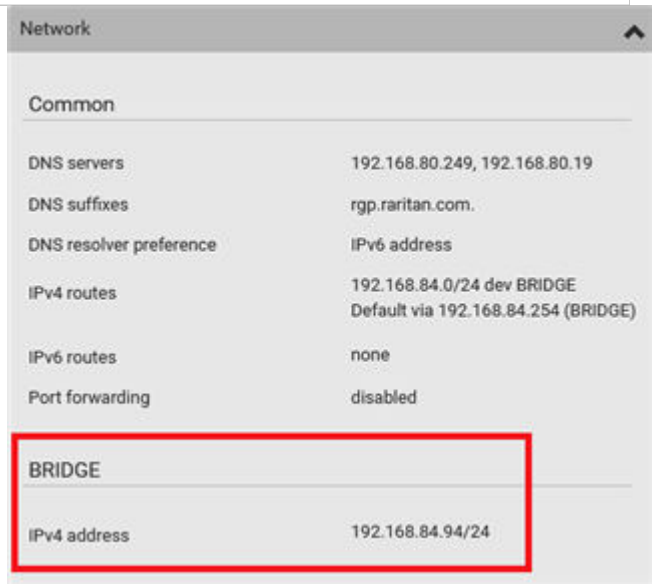
Using the Web Interface

1. Choose Maintenance > Device Information.
2. Check the Network section. Press F5 to reload it if needed.

► *Cascading information in the Bridging mode:*

- The Common section contains two read-only fields for indicating the cascading status. Note that the cascading position is NOT available in the Bridging mode.

Fields	Description
Port forwarding	Indicates the Port Forwarding is disabled. See Setting the Cascading Mode (on page 623).
BRIDGE section	Indicates the device is in the Bridging mode and its IP address.

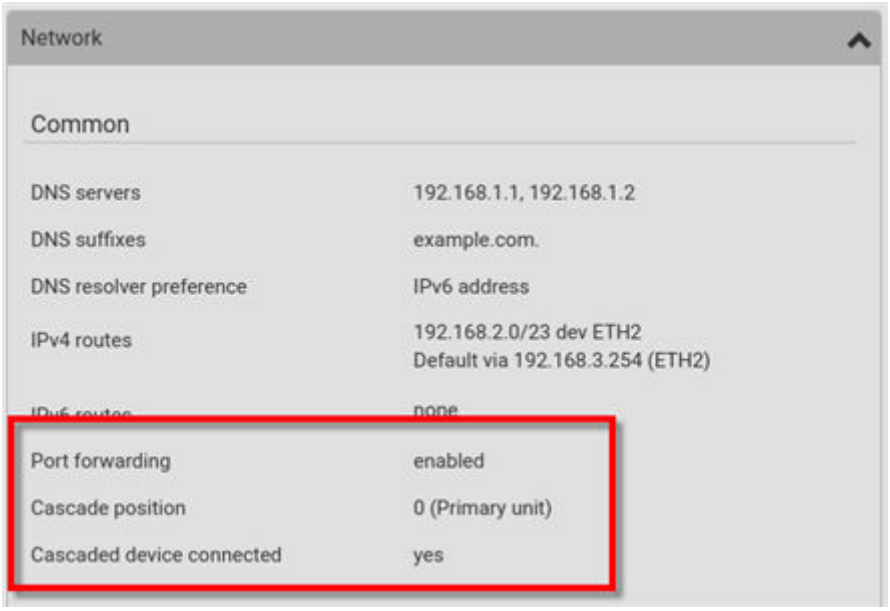


► *Cascading information in the Port Forwarding mode:*

- The Common section contains three read-only fields for indicating the cascading status.

Fields	Description
Port forwarding	Indicates the Port Forwarding is enabled. See Setting the Cascading Mode (on page 623).
Cascade position	Indicates the position of the PX4 in the cascading chain. • 0 (zero) represents the primary device. • A non-zero number represents a expansion device. 1 is Expansion 1, 2 is Expansion 2, 3 is Expansion 3 and so on.
Cascaded device connected	Indicates whether a expansion device is detected on the USB-A or Ethernet port. • yes: Connection to a expansion device is detected. • no: NO connection to a expansion device is detected.

- A primary device shows *0* (zero) in the 'Cascade position' field and *yes* in the 'Cascaded device connected' field.



- A expansion device in the middle position shows the number of its exact position in the 'Cascade position' field and *yes* in the 'Cascaded device connected' field.

The following diagram shows 1, indicating it is the first expansion device - Expansion 1.

- The final expansion device shows a non-zero number which indicates its position in the 'Cascade position' field and *no* in the 'Cascaded device connected' field.

  The following diagram shows 2, indicating it is the second expansion device - Expansion 2. The 'Cascaded device connected' field shows *no*, indicating that it is the final one in the chain.

- For a list of port numbers required for accessing each cascaded device in the Port Forwarding mode, click the Port Forwarding title bar on the same page.

Using the CLI

1. Log in to the CLI of the desired cascaded device. To use the SSH or Telnet service, see SSH/Telnet Access.
2. Type the following CLI commands and press Enter.

```
#        show network
```

► *In the Bridging mode:*

In the Bridging mode, IP-related information is shown under the 'BRIDGE' interface, similar to the following.

```
Interface 'BRIDGE'
  Link
    MAC address:         00:0d:5d:0e:e1:2d
  IPv4
    Config method:       DHCP
    Address:             None
    Preferred hostname: Not configured
    DHCP server:         Not available
  IPv6
    Disabled
```

► *In the Port Forwarding mode:*

In the Port Forwarding mode, the Port Forwarding status shows 'Enabled'.

```
Port forwarding
  Status:                Enabled
```

The 'Role' or 'Expansion number' field indicates the device's position.

- For a primary device, the Role field shows 'Primary'.

```
Port forwarding
  Status:                   Enabled
  Role:                     Primary unit
  Downstream interface:     USB
```

- For a expansion device, the Role field shows 'Expansion'. The 'Expansion number' field indicates its position: *1* is the first expansion device, 2 is the second, and so on.

```
Port forwarding
  Status:                       Enabled
  Role:                         Expansion unit
  Expansion unit number:        1
```

Using the SNMP

The *unitConfigurationTable* in MIB contains entries for cascading information. One SNMP MIB manager, such as a MIB browser, is required for retrieving the SNMP data.

As of release 3.3.10, cascading information other than the cascading mode is no longer available in the Bridging mode, but all cascading information remains available in the Port Forwarding mode.

► *In the Port Forwarding mode:*

1. Launch your SNMP MIB manager and connect to the desired PX4.
2. To find whether the PX4 is in a cascading chain, retrieve the value of either one below:
   - SNMP name - pduDaisychainMemberType
   - SNMP object identifier (OID) - 1.3.6.1.4.1.13742.6.3.2.2.1.41

One of the following values is returned.

SNMP value	Description
standalone (0)	The PX4 is not in the cascading chain. It is a standalone device.
primary (1)	The PX4 is the primary device.
expansion (2)	The PX4 is a expansion device.

3. To check which cascading mode is applied, retrieve the value of either one below:
   - SNMP name - deviceCascadeType
   - SNMP OID - 1.3.6.1.4.1.13742.6.3.2.2.1.70

One of the values in the following table is returned.

SNMP value	Cascading mode
0	Bridging mode
1	Port Forwarding mode

The value 1 is returned in the Port Forwarding mode.

4. To identify the device's position in the cascading chain, retrieve the value of either one below:
   - SNMP name - deviceCascadePosition
   - SNMP OID - 1.3.6.1.4.1.13742.6.3.2.2.1.71

One of the following values is returned.

SNMP value	Device position
0	Primary device
1 to 15	Expansion 1 to Expansion 15

5. To find whether the PX4 is the final expansion device, retrieve the value of either one below:
   - SNMP name - cascadedDeviceConnected
   - SNMP OID - 1.3.6.1.4.1.13742.6.3.2.2.1.58

Check which value is returned. A final expansion device has NO expansion device connected to its Ethernet (ETH1 or ETH2) or USB-A port.

SNMP value	Description
true (1)	A expansion device has been connected to either Ethernet or USB-A port of this PX4.
false (2)	No expansion device is connected to either Ethernet or USB-A port of this PX4.

► *In the Bridging mode:*

1. Launch your SNMP MIB manager and connect to the desired PX4.
2. To check which cascading mode is applied, retrieve the value of either one below:
   - SNMP name - deviceCascadeType
   - SNMP OID - 1.3.6.1.4.1.13742.6.3.2.2.1.70

One of the values in the following table is returned.

SNMP value	Cascading mode
0	Bridging mode
1	Port Forwarding mode

The value 0 is returned in the Bridging mode.

3. The following cascading information is NOT available in the Bridging mode so they always show a permanent value, which CANNOT correctly indicate the current cascading status.
   - `pduDaisychainMemberType (1.3.6.1.4.1.13742.6.3.2.2.1.41)` always shows 'standalone (0)'
   - `deviceCascadePosition (1.3.6.1.4.1.13742.6.3.2.2.1.71)` always shows 'Primary device (0)'
   - `cascadedDeviceConnected (1.3.6.1.4.1.13742.6.3.2.2.1.58)` always shows 'false (2)'

Using the LCD Display

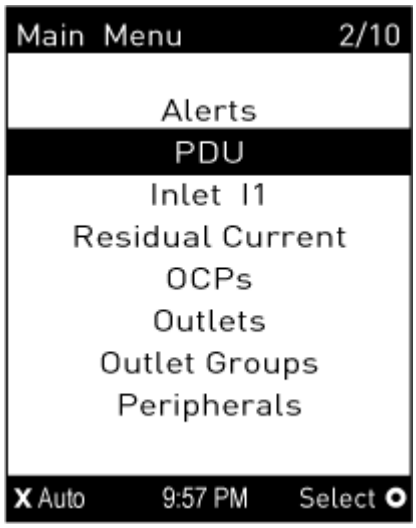
Some supported products have a front panel display which can show cascading information, such as the device position. In the event when the PX4 releases warning or critical message, LCD will turn on.

Dot-Matrix LCD Display

On the dot-matrix LCD display, available cascading information depends on the cascading mode.

Note that the diagrams illustrated in this section are for Zero U PDUs, and your dot-matrix LCD display may look slightly different if it is on a different product model.

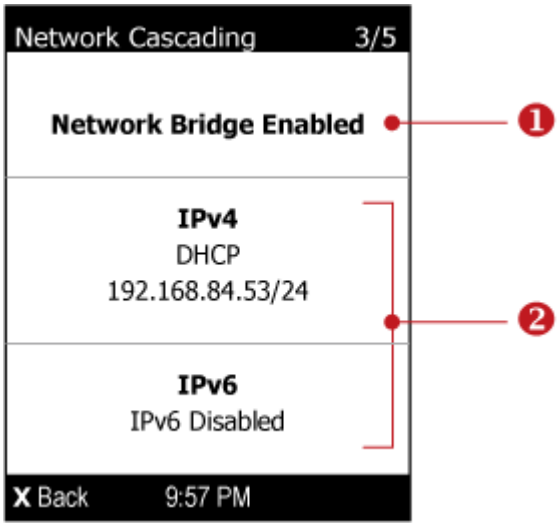
1. If the LCD display is in the Automatic mode, exit it by pressing or . The Main Menu similar to the following is displayed.



2. Press or to select "Device Info" in the Main Menu, and press .
3. Press until the Network Cascading page displays.

► *Bridging mode:*

In this mode, the LCD display only indicates the Bridging mode is enabled, but the device position information is NOT available.



Number	Description
❶	*Current cascading mode.* ● *In the above diagram, it shows the Bridging mode.*
❷	*IPv4/IPv6 network information, including:* ● *Network configuration: DHCP (or Automatic), or Static. Static represents Static IP.* ● *The device's IP address.* ● *IPv4 or IPv6 prefix length (such as "/24").*

If you do not enable IPv4 or IPv6 settings, a message is displayed to indicate IPv4 or IPv6 is disabled.

► *Port Forwarding mode:*

In this mode, the LCD display indicates the cascading mode, device position and the presence/ absence of a connected expansion device.

Description
Cascading mode-related information, including: • ***Port Forwarding mode*** • ***Primary or Expansion*** • ***Cascade position -- This information is available on expansion devices only.*** ***1 represents the first expansion, 2 represents the second expansion, and the like.*** • ***Expansion Connected: yes indicates a downstream expansion device is detected, and no indicates no downstream expansion devices are detected.***
The primary device's IPv4/IPv6 address.

Character LCD Display

Note: As of release 3.3.10, the following cascading information is no longer available in the Bridging mode, but remains available in the Port Forwarding mode.

A cascaded device's position is available by operating the LCD display.

Section	Example information
❶	"d" means the LCD display has entered the Device mode.

Section	Example information
❷	"CA" indicates that the cascading information is being displayed.
❸	"Expansion" indicates that this PX4 is an expansion device. Note: For a primary device, it shows the word "Primary" instead.
❹	The number 1 means the device position is Expansion 1.

► *To retrieve the device's cascading position information:*

1. Press the MODE button to enter the Device mode, indicated by a 'd' in at the top left of the display.
2. Press the FUNC button until "CA" is displayed at the top right of the display.
3. The device's position is represented by any number defined below:

Number	Device position	Number	Device position
0	Primary device	**8**	Expansion 8
1	Expansion 1	**9**	Expansion 9
2	Expansion 2	**10**	Expansion 10
3	Expansion 3	**11**	Expansion 11
4	Expansion 4	**12**	Expansion 12
5	Expansion 5	**13**	Expansion 13
6	Expansion 6	**14**	Expansion 14
7	Expansion 7	**15**	Expansion 15

Firmware Upgrade for Cascading Chains

You can upgrade each individual device in the cascading chain through the web interface. The upgrade procedure is completely identical to the procedure for a standalone device.

Do not mix devices running older releases in your cascading chain.

► *Firmware upgrade restrictions:*

- Intermediate firmware required for upgrades from "pre-3.3.0" to 3.5.0 or later:
  Follow the sequence below:
  a. Upgrade to an intermediate firmware first, which is either *3.3.x* or *3.4.x*.
  b. Then upgrade from the intermediate firmware to 3.5.0 or later.
- Start from the last expansion device for any upgrade from "pre-3.3.10":

To upgrade an existing USB-cascading chain from a firmware version older than 3.3.10, you must start from the last expansion device and so on until the primary device. Otherwise, a networking issue occurs. See Upgrade Sequence in an Existing Cascading Chain.

► *Warning for firmware DOWNGRADE:*

AVOID downgrading your cascading chain unless instructed by Technical Support.

Upgrade Sequence for Existing Cascading Chains

Depending on the firmware version(s) of your cascading chain, there may or may not be limitations for the firmware upgrade sequence in the chain.

► *Upgrade from 3.3.10 or later:*

There is no upgrade sequence limitation.

Firmware version 3.3.10 is compatible with later firmware versions so you can upgrade all devices of the chain in a random order.

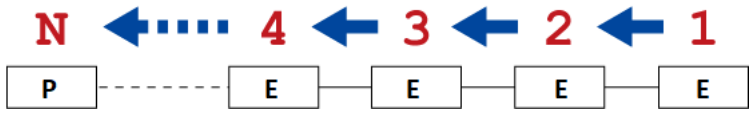
Important: It is not guaranteed that no upgrade sequence limitation will be required for all future firmware versions. It is highly suggested to check the latest revision of the Cascading Guide or your product's User Guide/Online Help before performing the firmware upgrade. The other alternative is to always stick to the same sequence as the above diagram.

► *Upgrade from "pre-3.3.10" to 3.3.10 and later:*

You must follow the firmware upgrade sequence below to upgrade a cascading chain from a firmware version older than 3.3.10 to version 3.3.10 or later. If you do not follow this upgrade sequence, you will not be able to access some cascaded devices over the Internet.

- The upgrade must start from the last expansion device (E), then the second to last, the third to last, and so on until the primary device (P).

  Red numbers below represent the appropriate upgrade sequence. 'N' is the final one to upgrade.



- You must upgrade ALL devices in the chain to 3.3.10 or later. If you upgrade only some devices in the chain, networking issues occur on some cascaded devices.

Cascade Troubleshooting

Any accessibility problem in one of the devices in the cascading chain may result in failure to access all downstream expansion devices that are connected to it.

You can troubleshoot the software settings by connecting the device whose connection has failed to a computer.

Tip: To determine which device may be the failure point, you may ping each device in the cascading chain, or check the expansion-related events in the event log of each device.

Symptom	Probable cause

Failure to access the primary device	• Primary device has a loose or lost network connection or power supply connection.
	• Primary device Ethernet or wireless interface is disabled.
	  • Primary device IPv4 or IPv6 settings are disabled.
	• In the Port Forwarding mode, related settings are incorrectly configured on the primary device.
	  • The primary device's role is incorrectly set to Expansion.
	  • The interface where the network is connected is incorrectly set as the downstream interface.
	• For the wireless networking, one of the following issues occurs:
	  • The USB wireless LAN adapter attached to the primary device is not the Raritan USB WIFI LAN adapter.
	  • The wireless LAN configuration is not supported.
	  • The installed CA certificate chain contains any certificate that has expired or is not valid yet.

Failure to access an expansion device	• One of the following issues occurs on the primary device:
	  • Network connection is lost.
	  • Power is lost.
	  • The Ethernet or wireless interface is disabled.
	• One of the following issues occurs on the expansion device in question or any upstream device (if available):
	  • Connection of the cascading cable is loose or lost.
	  • No power supply.
	  • The cascading mode is set incorrectly.
	  For example, the primary device is set to Bridging, but the expansion device in question or any upstream device is set to Port Forwarding.
	• In the Bridging mode, IPv4 (or IPv6) settings are disabled on the expansion device in question.
	• In the Port Forwarding mode, one of the following issues occurs:
	  • The primary device's role is incorrectly set to 'Expansion'.
	  • The primary device's downstream interface is incorrectly set. For example, you use a USB cable to connect the 1st expansion device, but select the Ethernet port as the downstream interface.
	  • The role of the expansion device in question or any upstream device is set to 'Primary' instead of 'Expansion'.
	  • The port number you added to the IP address is incorrect. See Port Number Syntax.
	  • IPv4 (or IPv6) settings are disabled on the primary device.
	• The expansion device in question or any upstream device is running a "pre-3.3.10" firmware version while the rest of the chain runs firmware version 3.3.10 or later.

► *For a cascading chain comprising only products with "dual" Ethernet ports, also check the following:*

- Whether the Ethernet interface (ETH1 or ETH2) where the network or cascading cable is connected is disabled on the cascaded device in question or any upstream device.
- Whether the connection complies with the cascading guidelines, when set to the Port Forwarding mode. See Restrictions of Port-Forwarding Connections.
- Whether a newer product model, if involved in the chain, runs the appropriate minimum firmware version or later.

Expansion Device Events in the Log

In the Bridging mode, events regarding connection/disconnection of a downstream expansion device via USB are NOT logged.

However, in the Port Forwarding mode, whenever the connection or disconnection of a downstream expansion device via USB is detected, the device at the USB-A end of the USB cable logs it in its internal log.

There are two expansion-related events in the Port Forwarding mode:

Event	Description
Expansion connected	Expansion device on its USB-A port is detected
Expansion disconnected	Disconnection of a expansion device from its USB-A port

Resetting to Factory Defaults

Important: Exercise caution before resetting the PX4 to its factory defaults.

This erases existing information and customized settings, such as user profiles, threshold values, and so on. Only energy data and firmware upgrade history are retained.

In This Chapter

Factory Default Settings. 654
Factory Default Login. 655
Using the Front Panel Display. 655
Using the CLI Command. 656
iX9 Controller Reset Button. 656

Factory Default Settings

Only secure access--physical or by secure network protocols--is enabled by default in Xerus.

During the first login, before any service can be used, you are forced to change the default password.

► *Default configuration:*

The factory default configuration disables these services:

- SNMP Agent (remains disabled even after default password is changed)
- SCP interface (disabled until default password is changed)

The factory default configuration enables these services:

- Both Ethernet ports are IPv4 enabled for DHCP with access to APIPA link local address
- HTTPS Server
- SSH Server
- Console (not applicable to PX4/PRO4X models)

► *Default password change requirement:*

The default password must be changed upon first use, before any other configuration changes or device access are allowed. In factory default configuration, the following protocols and tools, with the following restrictions, allow you to first update the default password:

- HTTPS Server Web User Interface: Restricted to a password change page/form only.
- HTTPS Server (JSON API Web Service): API limited to a password change for the default account.
- SSH Server: Prompts for a password change.
- Console: Prompts for a password change.

Note: Once the default password is changed, the restrictions are removed and the device resumes normal operations for the protocols and tools listed above. Upon any reset to factory defaults, the restrictions will again be enforced and a change to the default password will again be required.

Factory Default Login

username: admin

password: legrand

Using the Front Panel Display

The Front Panel Display provides a reset command for resetting to factory defaults. This option must be enabled in the Front Panel privileges: Device Settings > Front Panel, select the Factory Reset option in the Permissions section. By default, the function is disabled.

► *To reset to factory defaults using the front panel display:*

1. At the PDU, use the arrow buttons to navigate to the Device Info pages.
2. You will see several pages of information. Go to General Information. The list should show:
   - General information:
   - Device name
   - Firmware version
   - Model name
   - Serial number
   - Nameplate ratings
3. Press the Select button while on this page to open a Device Reset menu.
4. Use the arrow buttons to choose the Factory Reset option. (You can also reboot from this menu.)

5. You must confirm a Factory Reset by holding the Select button for five seconds.

Using the CLI Command

The Command Line Interface (CLI) provides a reset command for resetting to factory defaults.

► *To reset to factory defaults after logging in to the CLI:*

1. Log in to the CLI by typing the user name "admin" and its password.
2. After the # system prompt appears, type either of the following commands and press Enter.

```
#    reset factorydefaults
```

-- OR --

```
#    reset factorydefaults /y
```

3. If you entered the command without "`/y`" , a message appears prompting you to confirm the operation. Type y to confirm the reset.
4. Wait until the reset is complete.

► *To reset to factory defaults without logging in to the CLI:*

You can also reset the product to factory defaults in the CLI prior to login. This option requires physical access to the unit, either at the console (for older models) or using a USB configuration method.

1. Connect to the PX4 and launch a terminal emulation program.
2. At the Username prompt in the CLI, type "factorydefaults" and press Enter.

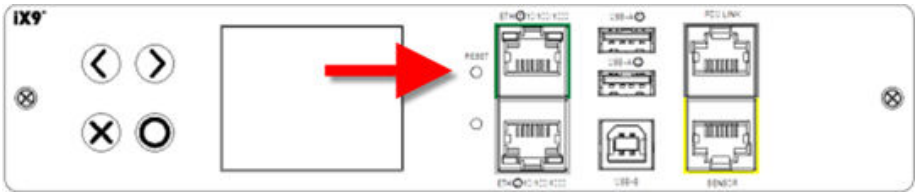
```
Username:            factorydefaults
```

3. Type `y` on a confirmation message to perform the reset.

iX9 Controller Reset Button

The iX9 controller reset button forces a restart and reboots the operating system, and can be used if the unit somehow becomes unresponsive.

It does NOT perform a Factory Reset.



Models with Residual Current Monitoring

Models with residual current monitoring (RCM) detect and report residual current, which is abnormal flow of current into the protective earth conductor.

Residual current is a safety issue since electrocution is possible if the rack or any device within it is touched.

Depending on the model you purchase, some models report residual current by inlet only, while some models report residual current by inlet pole. Some models are also able to report residual DC current in addition to the total residual current.

Warning: PX4 RCM cannot disconnect power to stop residual current flow. Devices like RCD and GFI disconnect power when residual current is detected, but the PX4 with RCM are NOT RCD or GFI protected devices.

In This Chapter

RCM Current Sensor. 657
RCM State Sensor. 657
Compliance with IEC 62020. 658
RCM Self-Test. 659
Web Interface Operations for RCM. 660
Front Panel Operations for RCM. 665
RCM SNMP Operations. 668
CLI Operations for RCM. 668

RCM Current Sensor

The RCM current sensor detects current imbalance which indicates current is flowing to ground. The sensor cannot determine the exact location. It just reports the sum of all residual current in the PDU and devices plugged into it, which is either per inlet or per inlet pole, depending on the model.

Most equipment leaks a small amount of current and the UL/IEC 60950-1 standard for IT equipment permits up to 3mA. For example, if a PDU has one RCM sensor on its inlet and twenty plugged-in devices -- each leaking 1mA, the RCM sensor then reports the sum - 20mA.

- All RCM models (M5, M11, M18 and M24) have a residual current sensor.
- Models with RCM type B (M11, M18 and M24) additionally have separate sensors for "Residual AC current" and "Residual DC current".

Important: The RCM sensor is 'unavailable' in power-sharing mode.

RCM State Sensor

The RCM state sensor reports events based on residual current thresholds or RCM self-test failure.

The RCM state is always determined by the magnitude of "total" residual current values per inlet or per inlet pole as explained below.

- For Type A, it is the sum of residual AC current.
- For Type B, it is the sum of residual AC and DC current.

  In other words, the RCM state is NOT determined by the residual DC current detected by the separate RCM "DC" sensor on Type B models.

RCM state	Description
normal	Residual current is within normal range.
warning	Residual current is above warning level.
critical	Residual current is above critical level. In addition to an event, the CRITICAL state causes the PX4 front panel to display a special error message.
self-test active	RCM diagnostics are running.
failure	RCM current sensor has malfunctioned. Contact Raritan Technical Support.

Note: The factory default is to disable the Warning state. To define and enable this state, see *Setting RCM Current Thresholds* (on page).

Important: When your PX4 enters the power-sharing mode, the RCM sensor enters the 'unavailable' state and will not work until the power-sharing mode ends. For information on power sharing, see Power-Sharing Restrictions and Connection.

Compliance with IEC 62020

IEC 62020 is an international standard for Residual Current Monitors. All PX4 with RCM are IEC 62020 compliant.

IEC 62020 uses the term *rated residual operating current* (IΔn) to specify residual current, equal to or above which causes an alarm. IEC 62020 recommends preferred values 6mA, 10mA, 30mA, 100mA, 300mA and 500mA. In the PX4 with RCM, IΔn is specified using the Critical Rated Residual Operating Current threshold.

IEC 62020 uses the term *residual non-operating current* (IΔno) to specify residual current, below which does not cause an alarm. IEC 62020 specifies IΔno be no higher than 0.5 IΔn. In PX4 with RCM, IΔno is set using the RCM Deassertion Hysteresis and this value must be no higher than 0.5 the RCM critical threshold.

PX4 with RCM allows you to establish an optional WARNING state, which is not part of the IEC 62020 specification. PX4 RCM remains IEC 62020 compliant when the RCM deassertion hysteresis is configured properly.

IEC 62020 specification	PX4 with RCM characteristics
Method of operation	Dependent on line voltage. RCM only functions if line voltage is present.

IEC 62020 specification	PX4 with RCM characteristics
Type of installation	PX4 with flexible line cords and plugs are for mobile installation and corded connection.
Current paths	1-phase PX4 are two current paths RCM. 3-phase 3W+PE are three current paths RCM. 3-phase 4W+PE are four current paths RCM.
Ability to adjust residual operating current	Adjustable. • Type A: 6mA-500mA. • Type B: 14mA-300mA.
Adjustable time delay	Non-adjustable time delay.
Protection against external influence	Enclosed-type RCM.
Method of mounting	Panel board type RCM.
Method of connection	Not associated with mechanical mounting.
Connection of load conductors	Monitored line is directly connected.
Fault indicating means	Visual, with other output signals.
Ability to directly discriminate	Directionally non-discriminating.
Rated residual operating current	0.5A (highest value).
Residual currents with direct current components	Model dependent. • Models ending in M5 are Type A. • Models ending in M11 or M18 are Type B.

RCM Self-Test

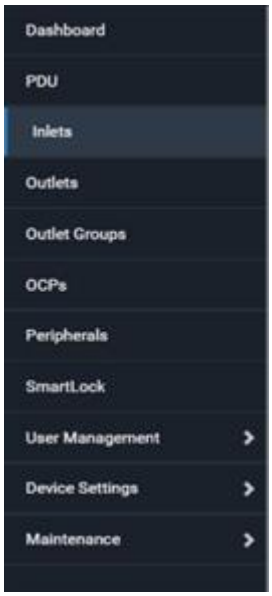
PX4 with RCM have a built-in self-test feature that performs these functions:

- When residual current is less than 3mA, 15mA is momentarily added to determine whether the low reading is due to a faulty sensor. The residual current added is done in a safe manner that does not run current into ground or pose operator risk.
- The RCM state sensor changes to SELF-TEST and then back to its original state if self-test passes, or to the FAILURE state if self-test fails. These state changes are useful to verify your monitoring systems (SNMP, syslog, or email) are correctly set up to receive PX4 event notifications.
- For Type B "M18" models, the self-test feature will perform tests on all poles of the selected inlet simultaneously.

Note: If self-test fails, the FAILURE state persists until another self-test runs and passes.

Web Interface Operations for RCM

The RCM on PX4 is either an inlet sensor or an inlet pole sensor. To view, configure or run self-test, click Inlet in the Menu.



Checking RCM State and Current

A section titled 'Residual Current Monitor' is available on the Inlet page, showing both the present RCM state and residual current.

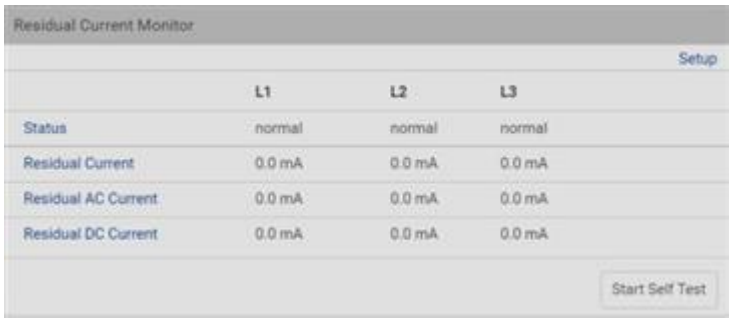
Important: When your PX4 enters the power-sharing mode, the RCM sensor enters the 'unavailable' state and will not work until the power-sharing mode ends. For information on power sharing, see Power-Sharing Restrictions and Connection.

► *To check RCM state and current on the Inlet page:*

1. Click Inlet.
2. Locate the Residual Current Monitor section on the Inlet page.
   - RCM State: There are five states - normal, warning, critical, self-test active and failure. For more information, see *RCM State Sensor* (on page).
   - Residual Current:
     For Type A, it is the sum of residual AC current.

For Type B, it is the sum of residual AC and DC current.

For Type B "M18" models, the listed fields are available per inlet pole as shown below. Besides, a Type B model, either "M11" or "M18", is able to display the residual DC current.



Note: To determine the RCM's normal, warning and critical levels, configure the RCM current thresholds. See *Setting RCM Current Thresholds* (on page). To configure the residual DC current thresholds, see *Setting RCM DC Current Thresholds* (on page).

RCM Critical State Alarm

When a RCM sensor enters the Critical state, the device beeps and this alarm is displayed in the Alerted Sensors section of the Dashboard page.

Note that only the RCM sensor will cause the beep while RCM "DC" sensor does not cause the beep regardless of its sensor state.

Warning: RCM sensors do not work in power-sharing mode.

Number	Description
1	The magnitude of residual current reported by the RCM current sensor.
2	Critical state reported by the RCM state sensor.

Tip: RCM critical state is also indicated on the Inlet page or the Internal Beeper section of the PDU page.

Setting RCM Current Thresholds

Warning Rated Residual Operating Current is the upper warning threshold of the PX4 RCM sensor, and Critical Rated Residual Operating Current is the upper critical threshold of the RCM sensor. These thresholds are set in the configuration mode. See Entering Configuration Mode.

Note: A residual current sensor's LOWER warning and LOWER critical thresholds do NOT affect the operations of the RCM state sensor so you can ignore them.

For Type B "M18" models, this command configures all RCM sensors of the same inlet simultaneously.

► *To configure the RCM's Critical level:*

```
config:# residualCurrentMonitor <n> criticalRatedResidualOperatingCurrent
         <value>
```

Note: The PX4 triggers events when residual current values are above (but not equal to) thresholds. For example, you would set the critical threshold to 29mA to specify the IEC 62020 IΔn of 30mA. See *Compliance with IEC 62020* (on page).

► *To configure the RCM's Warning level:*

```
config:# residualCurrentMonitor <n> warningRatedResidualOperatingCurrent
         <value>
```

► *To configure the RCM's deassertion hysteresis:*

```
config:#  residualCurrentMonitor <n> deassertionHysteresis <hy_value>
```

Variables:

- <n> is the number of the inlet where the desired RCM current sensor is mounted. For a single-inlet PDU, this number is always 1.
- <value> is one of the options: *enable*, *disable* or a numeric value measured in amperes.

Option	Description
enable	Enables the specified RCM current threshold for the specified inlet.
disable	Disables the specified RCM current threshold for the specified inlet.
A numeric value	Sets a value for the specified RCM current threshold of the specified inlet and enables this threshold simultaneously. Note that this value is measured in A, not mA. Therefore, to set the value to 6mA, type *0.006*.

- <hy_value> is a numeric value measured in amperes (A), not milliamperes (mA). For example, to set the value to 15mA, type *0.015*.

► *Tip -- other RCM-related "threshold-setting" commands:*

- For models detecting residual current per inlet, see Commands for Inlet Sensors
- For models detecting residual current per inlet pole, see Commands for Inlet Pole Sensors

Scheduling RCM Self-Test

You can have the PX4 run RCM self-test automatically at a regular time interval or on a specific date and time. See Scheduling an Action for the procedure and select "Start residual current monitor self test" to create the scheduled RCM self-test action.

Note: For Type B "M18" models, the self-test feature will perform tests on all poles of the selected inlet simultaneously.

Disabling or Enabling Front Panel RCM Self-Test

You can enable or disable the function of performing the RCM self-test by operating the front panel buttons. By default, this function is enabled.

► *To disable or enable the front panel RCM self-test:*

1. Choose Device Settings > Front Panel.
2. Do either below:
   - To disable this function, deselect the "Perform RCM self-test" checkbox.
   - To enable this function, select the "Perform RCM self-test" checkbox.
3. Click Save.

Setting RCM DC Current Thresholds

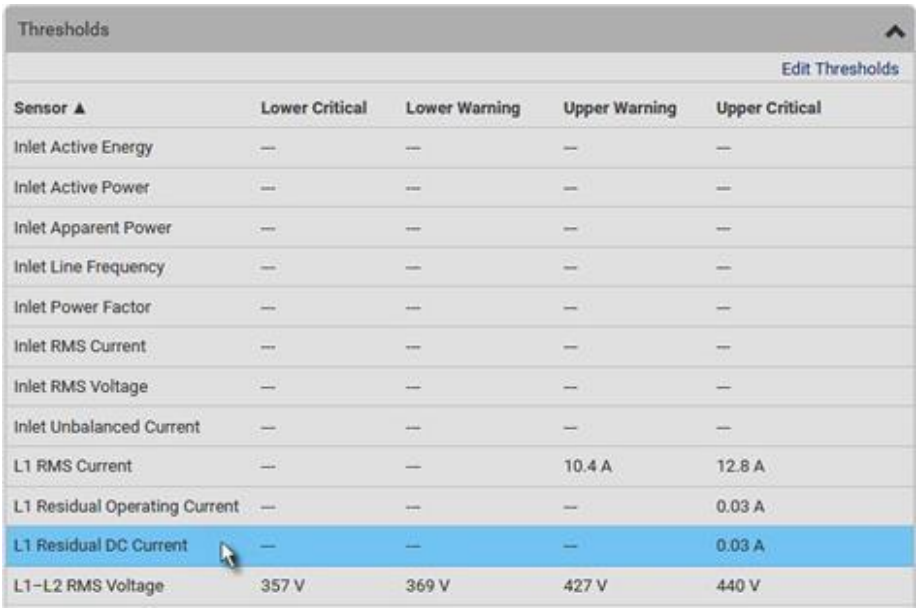
RCM DC current sensors are available on Type B models only.

You can also configure upper thresholds for RCM DC current sensors so that an alarm will be displayed on the page of Dashboard when RCM DC sensors enter an alerted state.

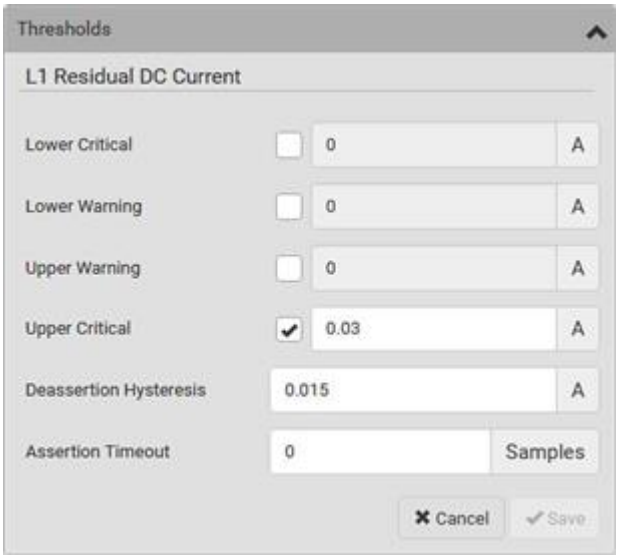
► *To configure RCM DC's upper thresholds:*

1. Click Inlet to open the Inlet page.
2. Click the Thresholds title bar at the bottom of the page to display inlet thresholds.

3. Click the desired sensor (required), and then click Edit Thresholds. For example, select "L1 Residual DC Current".



4. Make changes as needed.
   - To enable any threshold, select the corresponding checkbox.
   - Type a new value in the accompanying text box.



For concepts of thresholds, deassertion hysteresis and assertion timeout, see Sensor Threshold Settings.

5. Click Save.

Front Panel Operations for RCM

The front panel LCD display shows an alarm message when the RCM enters the critical state. Besides, you can operate the LCD display to check the RCM status.

This section introduces the RCM information shown on the dot-matrix LCD display.

Note: For RCM information shown on the character LCD display of an old PX4 model, see *RCM Information* (on page).

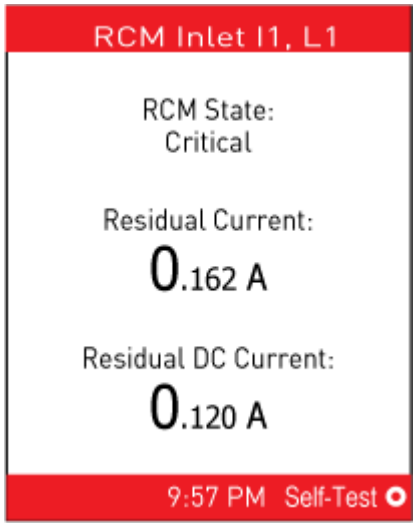
LCD Message for RCM Critical State

In the RCM critical state, the PDU beeps and the LCD display indicates the RCM critical state.

The RCM alarm information continues to display as long as RCM is in a critical state. The top and bottom bars on the display turn red at the same time.

► *RCM alarm information in the critical state:*

1. The LCD display shows two or three pieces of information for the inlet or inlet pole with the RCM alarm:
   - RCM State: Critical.
   - Residual Current: Residual current value in Amps.
     - For Type A, it is the sum of residual AC current.
     - For Type B, it is the sum of residual AC and DC current.
   - Residual DC Current: If your PDU is an RCM Type B model, an additional DC-only residual current value is also reported on the LCD.



If your PX4 has more than one inlet, only the inlet which has the RCM alarm enters the critical state.

2. If needed, you can press to perform RCM self-test for this inlet. For details, see steps 4 to 5 in the topic titled *Running RCM Self-Test* (on page).

Checking RCM States and Current

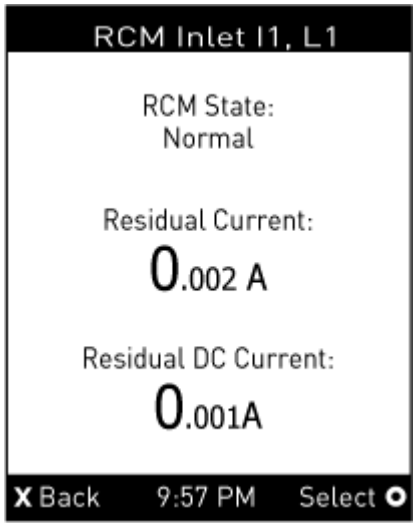
You can retrieve RCM information from the LCD display.

► *To check RCM information:*

1. Press or to access the Main Menu.
2. Press or to select "Residual Current", and press .
3. The LCD display shows two or three pieces of information for Inlet 1 as shown below, or a list of inlet poles.

If a list of inlet poles displays, press or , and then to select one inlet pole.

- RCM State: Normal or Warning.
- Residual Current: Residual current value in Amps.
  - For Type A, it is the sum of residual AC current.
  - For Type B, it is the sum of residual AC and DC current.
- Residual DC Current: If your PDU is an RCM Type B model, an additional DC-only residual current value is also reported on the LCD.



If your PX4 has more than one inlet, a list of inlets is displayed, along with each inlet's RCM state and reading(s).

4. To return to the Main Menu, press .

Running RCM Self-Test

You can perform RCM self-test for a specific inlet via CLI. After the self-test finishes, the test result is shown: pass or fail.

For Type B "M18" models, the self-test feature will perform tests on all poles of the selected inlet simultaneously.

► *To perform RCM self-test:*

```
#     rcm selfTest inlet <n>
```

Variables:

- <n> is the inlet's number. For a single-inlet PDU, <n> is always 1.

RCM SNMP Operations

Make sure you have the correct version of SNMP MIB. The PX4 supports the RCM feature as of firmware version 2.5.20. See Downloading SNMP MIB for details.

RCM Trap

An *InletSensorStateChange* trap is sent when the RCM state sensor changes. *InletSensorStateChange* is the generic trap sent for all inlet sensors. The specific trap for RCM has the object *typeOfSensor* set to 27. Included with the trap are *measurementsInletSensorValue* (the residual current value) and *measurementsInletSensorState* (the RCM state that caused the trap).

RCM Residual Current and State Objects

The *inletSensorMeasurementsTable* contains entries for RCM residual current and states.

Use index *sensorType* = 26 to retrieve the row for residual current. Column *measurementsInletSensorValue* contains the residual current.

Use index *sensorType* = 27 to retrieve the row for RCM state. Column *measurementsInletSensorState* contains the RCM state enumeration value.

Setting RCM Thresholds

The inletSensorConfigurationTable contains a row for configuring RCM thresholds. Use index *sensorType* = 26 to reference the row. Columns *inletSensorUpperWarningThreshold*, *inletSensorUpperCriticalThreshold* and *inletSensorHysteresis* set values for RCM warning, critical and deassertion hysteresis respectively.

CLI Operations for RCM

For information on entering and using the CLI, see Using the Command Line Interface.

Showing Residual Current Monitoring Information

This command syntax shows the residual current monitoring (RCM) information, which is only available on the models with RCM. The information displayed include the RCM current, state and thresholds.

For Type B "M18" models, this command shows the information of all RCM sensors of the same inlet at a time.

```
#  show residualCurrentMonitor <n>
```

Variables:

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

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

► *Tip -- other RCM-related "show" commands:*

- For models detecting residual current per inlet, see Inlet Sensor Threshold Information
- For models detecting residual current per inlet pole, see Inlet Pole Sensor Threshold Information

Setting Front Panel RCM Self-Test

You can enable or disable the front panel RCM self-test function via CLI in addition to the web interface.

► *To enable the front panel RCM self-test:*

```
#  security frontPanelPermissions add rcmSelfTest
```

► *To disable the front panel RCM self-test:*

```
#  security frontPanelPermissions remove rcmSelfTest
```

Degaussing RCM Type B Sensors

Only the models with RCM 'Type B' sensors support degaussing the RCM sensors. Those with RCM Type A sensors do NOT support this feature.

You can degauss the RCM sensor after a current surge, such as a short circuit.

For Type B "M18" models, this command will degauss all RCM sensors simultaneously.

► *To degauss RCM Type B sensors:*

```
#          rcm degauss
```

Remote Authentication Examples

In This Chapter

LDAP Configuration Illustration. 670
RADIUS Configuration Illustration. 675
Cisco ISE Xerus TACACS+ Authentication. 689

LDAP Configuration Illustration

This section provides an LDAP example for illustrating the configuration procedure using Microsoft Active Directory® (AD). To configure LDAP authentication, four main steps are required:

a. Determine user accounts and roles (groups) intended for the device
b. Create user groups for the device on the AD server
c. Configure LDAP authentication on the device
d. Configure roles on the device

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

Step A. Determine User Accounts and Roles

Determine the user accounts and roles (groups) that are authenticated for accessing the device. In this example, we will create two user roles with different permissions. Each role (group) will consist of two user accounts available on the AD server.

User roles	User accounts (members)
PX_User	usera
	pxuser2
PX_Admin	userb
	pxuser

Group permissions:

- The PX_User role will have neither system permissions nor outlet permissions.
- The PX_Admin role will have full system and outlet permissions.

Step B. Configure User Groups on the AD Server

You must create the groups (roles) for the PX4 on the AD server, and then make appropriate users members of these groups.

In this illustration, we assume:

- The groups (roles) for the PX4 are named *PX_Admin* and *PX_User*.
- User accounts *pxuser*, *pxuser2*, *usera* and *userb* already exist on the AD server.

► *To configure user groups on the AD server:*

1. On the AD server, create new groups -- *PX_Admin* and *PX_User*.

Note: Refer to the documentation or online help accompanying Microsoft AD for detailed instructions.

---

2. Add the *pxuser2* and *usera* accounts to the PX_User group.
3. Add the *pxuser* and *userb* accounts to the PX_Admin group.
4. Verify whether each group comprises correct users.

Step C. Configure LDAP Authentication on the PX4

You must enable and set up LDAP authentication properly on the PX4 to use external authentication.

In the illustration, we assume:

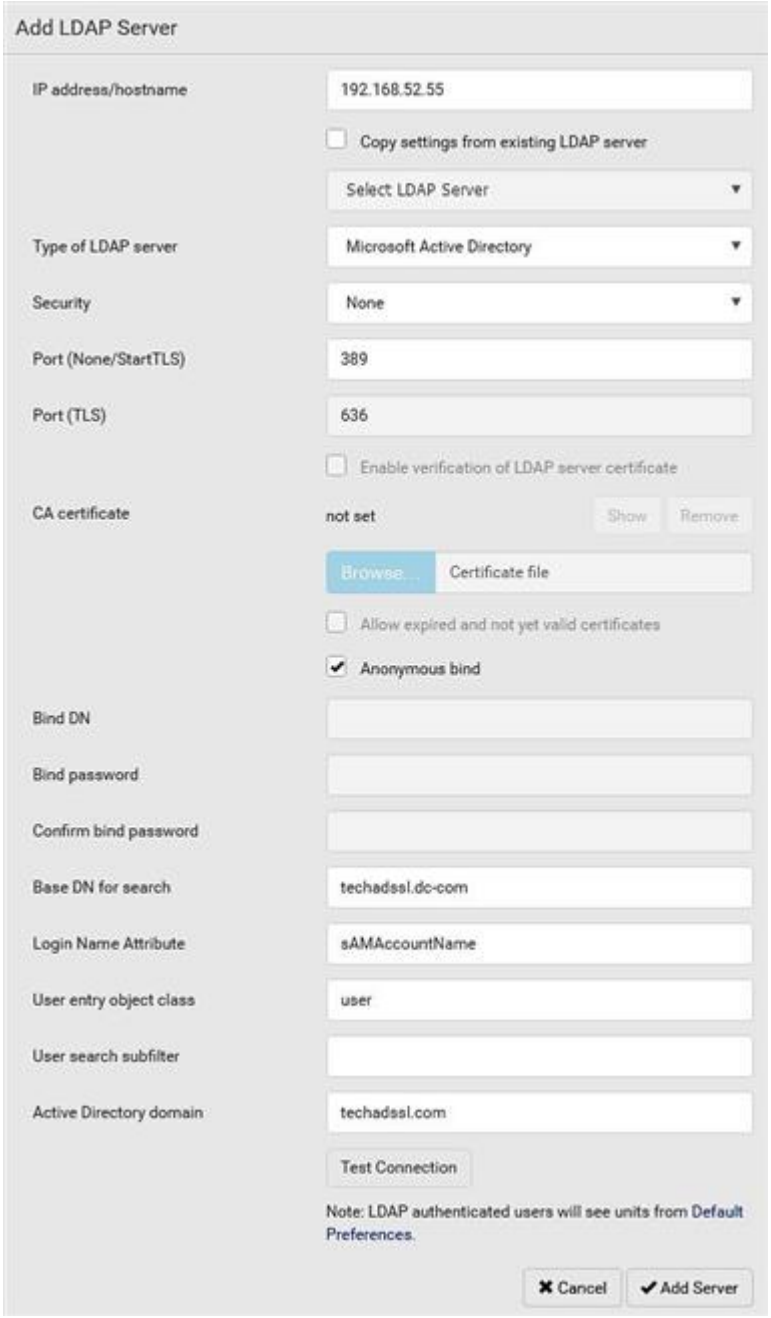
- The DNS server settings have been configured properly. See Wired Network Settings and Role of a DNS Server.
- The AD server's domain name is *techadssl.com*, and its IP address is *192.168.56.3*.
- The AD protocol is NOT encrypted over TLS.
- The AD server uses the default TCP port *389*.
- Anonymous bind is used.

► *To configure LDAP authentication:*

1. Choose Device Settings > Security > Authentication.
2. In the LDAP Servers section, click New to add an LDAP/LDAPS server.
3. Provide the PX4 with the information about the AD server.

Field/setting	Do this...
IP address / hostname	Type the domain name `techadssl.com` or IP address `192.168.56.3`. • Without the encryption enabled, you can type either the domain name or IP address in this field, but you must type the fully qualified domain name if the encryption is enabled.
Copy settings from existing LDAP server	Leave the checkbox deselected unless the new LDAP server's settings are similar to any existing LDAP settings.
Type of LDAP server	Select "Microsoft Active Directory."
Security	Select "None" since the TLS encryption is not applied in this example.
Port (None/StartTLS)	Ensure the field is set to `389`.
Port (TLS), CA certificate	Skip the two fields since the TLS encryption is not enabled.
Anonymous bind	Select this checkbox because anonymous bind is used.
Bind DN, Bind password, Confirm bind password	Skip the three fields because of anonymous bind.
Base DN for search	Type `dc=techadssl,dc=com` as the starting point where your search begins on the AD server.
Login Name Attribute	Ensure the field is set to `sAMAccountName` because the LDAP server is Microsoft Active Directory.
User entry object class	Ensure the field is set to `user` because the LDAP server is Microsoft Active Directory.
User search subfilter	The field is optional. The subfilter information is also useful for filtering out additional objects in a large directory structure. In this example, we leave it blank.

Field/setting	Do this...
Active Directory domain	Type `techadssl.com`.



1. Click Add Server.The LDAP server is saved.
2. In the Authentication Type field, select LDAP.
3. Click Save. The LDAP authentication is activated.

Note: If the PX4 clock and the LDAP server clock are out of sync, the installed TLS certificates, if any, may be considered expired. To ensure proper synchronization, administrators should configure the PX4 and the LDAP server to use the same NTP server(s).

Step D. Configure Roles on the PX4

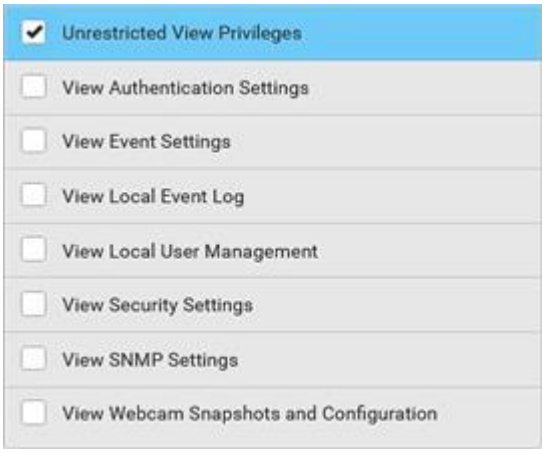
A role on the PX4 determines the system and outlet permissions. You must create the roles whose names are identical to the user groups created for the PX4 on the AD server or authorization will fail. Therefore, we will create the roles named *PX_User* and *PX_Admin* on the PDU.

In this illustration, we assume:

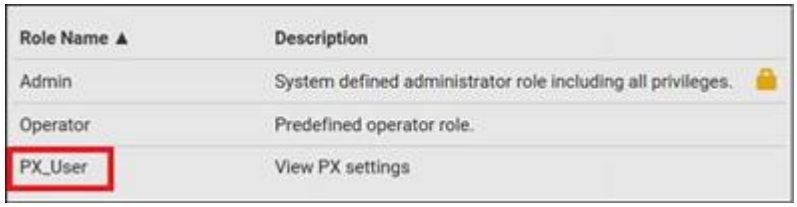
- Users assigned to the *PX_User* role can view settings only, but they can neither configure PX4 nor access the outlets.
- Users assigned to the *PX_Admin* role have the Administrator Privileges so they can both configure PX4 and access the outlets.

► *To create the PX_User role with appropriate permissions assigned:*

1. Choose User Management > Roles.
2. Click to add a new role.
   a. Type `PX_User` in the Role Name field.
   b. Type a description for the PX_User role in the Description field. In this example, we type "View PX settings" to describe the role.
   c. In the Privileges list, select Unrestricted View Privileges, which includes all View permissions. The Unrestricted View Privileges permission lets users view all settings without the capability to configure or change them.



   d. Click Save.
3. The PX_User role is created.

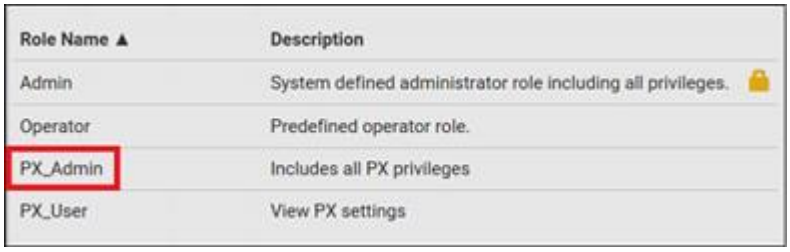


4. Keep the Roles page open to create the PX_Admin role.

► *To create the PX_Admin role with full permissions assigned:*

1. Click to add another role.
   a. Type `PX_Admin` in the Role Name field.
   b. Type a description for the PX_Admin role in the Description field. In this example, we type "Includes all PX privileges" to describe the role.
   c. In the Privileges list, select Administrator Privileges. The Administrator Privileges allows users to configure or change all PX4 settings.

   d. Click Save.
2. The PX_Admin role is created.



RADIUS Configuration Illustration

This section provides illustrations for configuring RADIUS authentication. One illustration is based on the Microsoft® Network Policy Server (NPS), and the other is based on a FreeRADIUS server.

The following steps are required for any RADIUS authentication:

1. Configure RADIUS authentication on the PX4. See Adding Radius Servers.
2. Configure roles on the PX4. See Creating Roles.
3. Configure PX4 user credentials and roles on your RADIUS server.
   - To configure using standard attributes, see *Standard Attributes* (on page).
   - To configure using vendor-specific attributes, see *Vendor-Specific Attributes* (on page).

Note that we assume that the NPS is running on a Windows 2008 system in the NPS illustrations.

Standard Attributes

The RADIUS standard attribute "Filter-ID" is used to convey the group membership, that is, roles.

- If a user has multiple roles, configure multiple standard attributes for this user.
- The syntax of a standard attribute is:
  `Raritan:G{role-name}`

FreeRADIUS Standard Attribute Illustration

With standard attributes, NO dictionary files are required. You simply add all user data, including user names, passwords, and roles, in the following FreeRADIUS path.

`/etc/raddb/users`

► *Presumptions in the illustration:*

- User name = `steve`
- Steve's password = `test123`
- Steve's roles = `Admin` and `SystemTester`

► *To create a user profile for "steve" in FreeRADIUS:*

1. Go to this location: `/etc/raddb/users`.
2. Add the data of the user "steve" by typing the following. Note that the values after the equal sign (=) must be enclosed in double quotes (").

```
steve Cleartext-Password := "test123"
Filter-ID = "Raritan:G{Admin}",
Filter-ID = "Raritan:G{SystemTester}"
```

Vendor-Specific Attributes

You must specify the following properties when using a RADIUS vendor-specific attribute (VSA).

- Vendor code = `13742`
- Vendor-assigned attribute number = `26`
- Attribute format = `String`

The syntax of the vendor-specific attribute for specifying one or multiple roles is:

`Raritan:G{role-name1 role-name2 role-name3}`

For configuration on NPS, see *NPS VSA Illustration* (on page).

For configuration on FreeRADIUS, see *FreeRADIUS VSA Illustration* (on page).

NPS VSA Illustration

To configure Windows 2008 NPS with the *vendor-specific attribute*, you must:

a. Add your PX4 to NPS. See *Step A: Add Your PX4 as a RADIUS Client* (on page).
b. On the NPS, configure connection request policies and the vendor-specific attribute. See *Step B: Configure Connection Policies and Vendor-Specific Attributes* (on page).

Some configuration associated with Microsoft Active Directory (AD) is also required for RADIUS authentication. See *AD-Related Configuration* (on page).

Step A: Add Your PX4 as a RADIUS Client

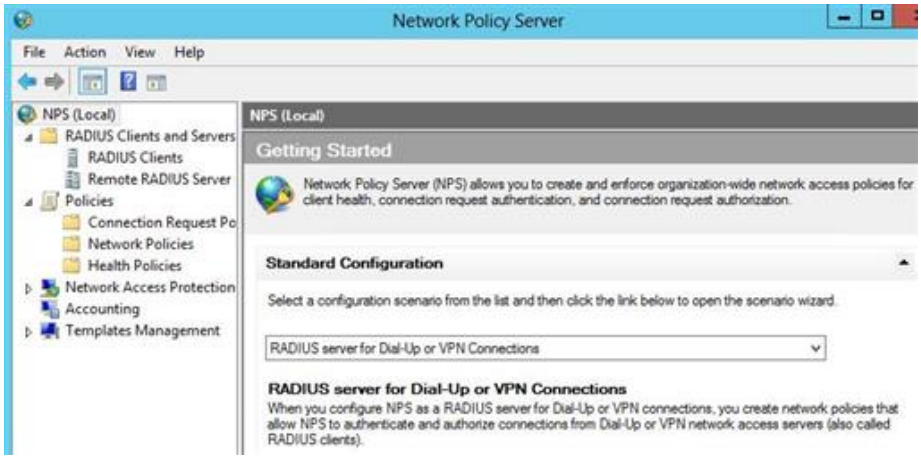
The RADIUS implementation on the PX4 follows the standard RADIUS Internet Engineering Task Force (IETF) specification so you must select "RADIUS Standard" as its vendor name when configuring the NPS server.

► *Presumptions in the illustration:*

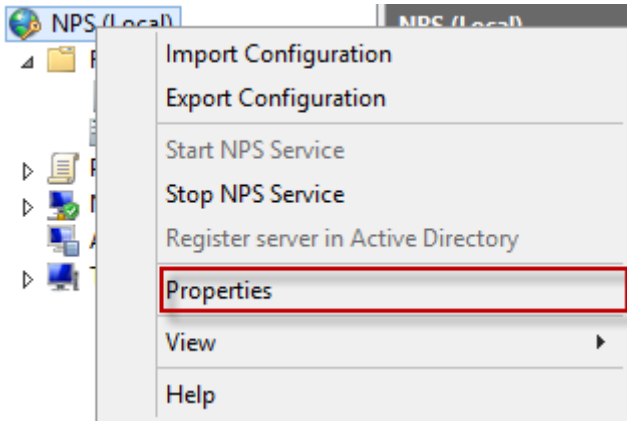
- IP address of your PX4 = `192.168.56.29`
- RADIUS authentication port specified for PX4: *1812*
- RADIUS accounting port specified for PX4: *1813*

► *To add your PX4 to the RADIUS NPS:*

1. Choose Start > Administrative Tools > Network Policy Server. The Network Policy Server console window opens.

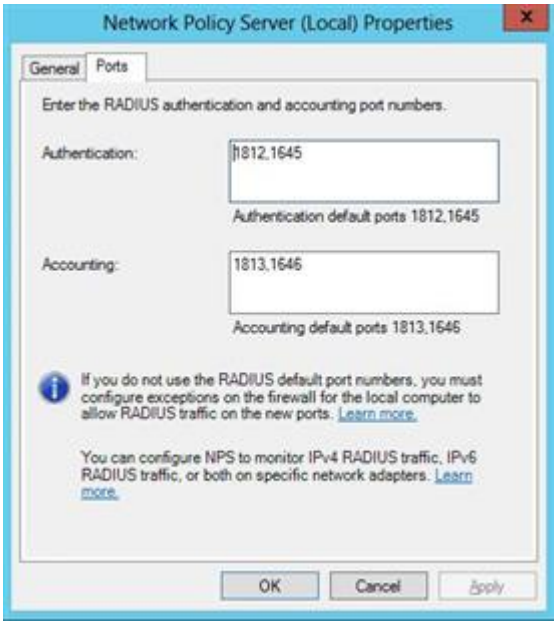


2. Right-click NPS (Local), and select Properties.

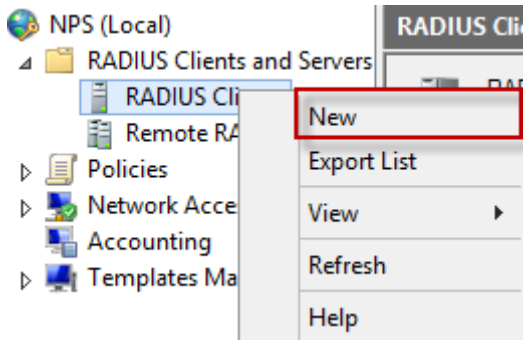


Raritan
A brand of legrand

Verify the authentication and accounting port numbers shown in the properties dialog are the same as those specified on your PX4. In this example, they are 1812 and 1813. Then close this dialog.



3. Under "RADIUS Clients and Servers," right-click RADIUS Client and select New RADIUS Client. The New RADIUS Client dialog appears.

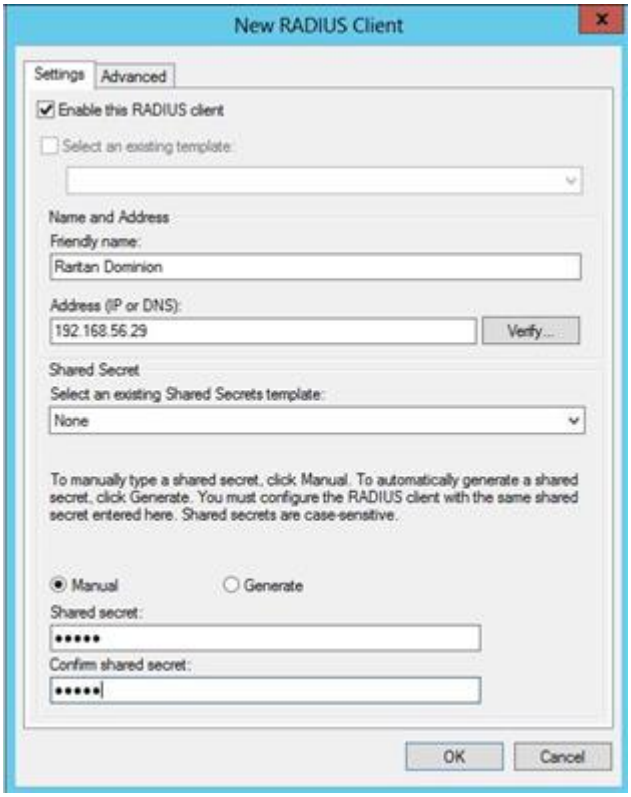


4. Do the following to add your PX4 to NPS:
   a. Verify the "Enable this RADIUS client" checkbox is selected.
   b. Type a name for identifying your PX4 in the "Friendly name" field.
   c. Type *192.168.56.29* in the "Address (IP or DNS)" field.

d. Select *RADIUS Standard* in the "Vendor name" field.

e. Select the *Manual* radio button.

f. Type the shared secret in the "Shared secret" and "Confirm shared secret" fields. The shared secret must be the same as the one specified on your PX4.



5. Click OK.

Step B: Configure Connection Policies and Vendor-Specific Attributes

You need to configure the following for connection request policies:

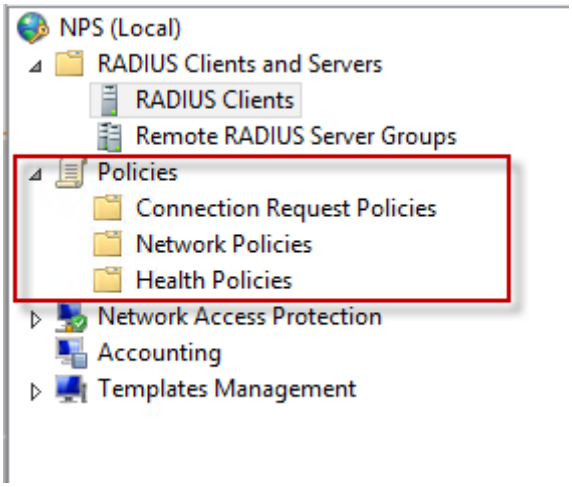
- IP address or host name of the PX4
- Connection request forwarding method
- Authentication method(s)
- Standard RADIUS attributes

► *Presumptions in the illustration:*

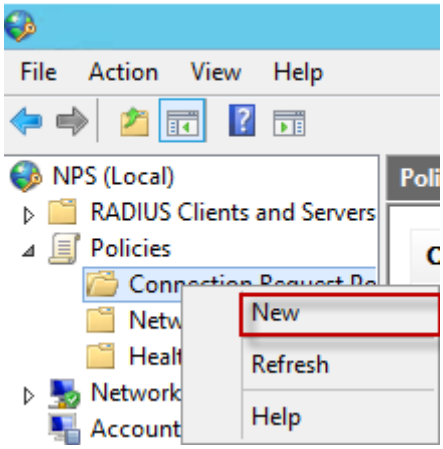
- IP address of your PX4 = `192.168.56.29`
- *Local* NPS server is used
- RADIUS protocol selected on your PX4 = `CHAP`
- Existing roles of your PX4 = `Admin`, `User` and `SystemTester`

► *Illustration:*

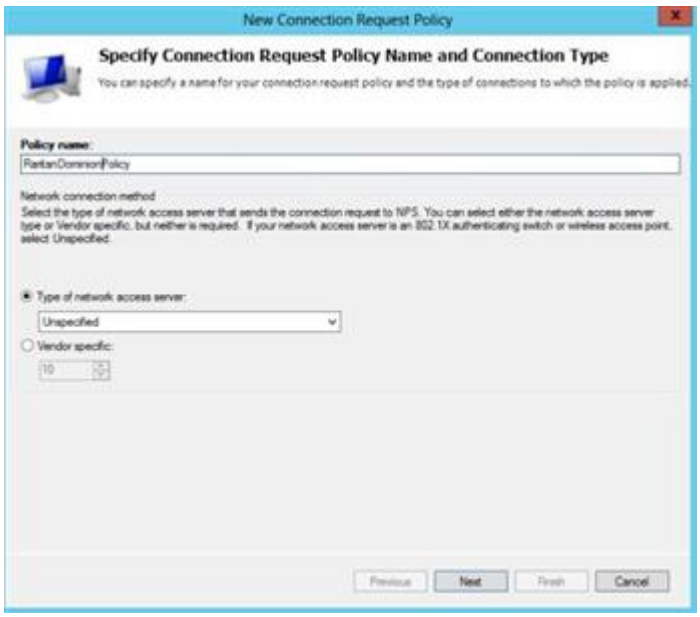
1. Open the NPS console, and expand the Policies folder.



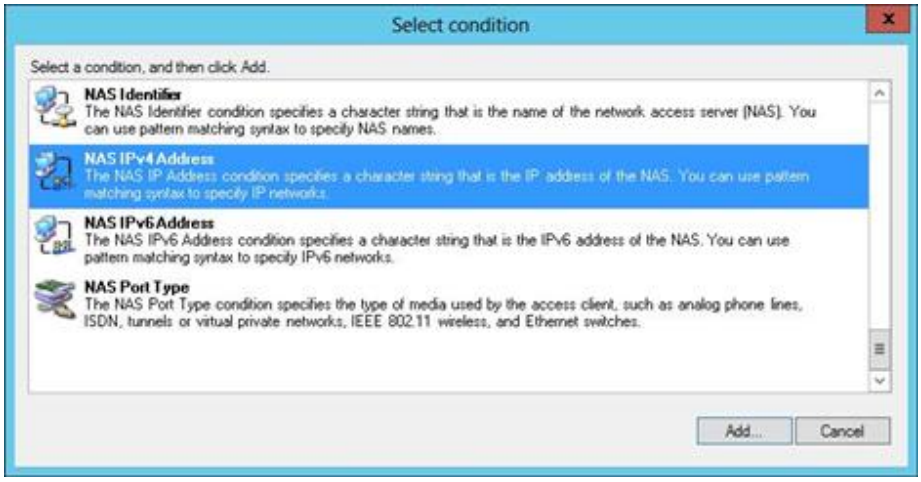
2. Right-click Connection Request Policies and select New. The New Connection Request Policy dialog appears.



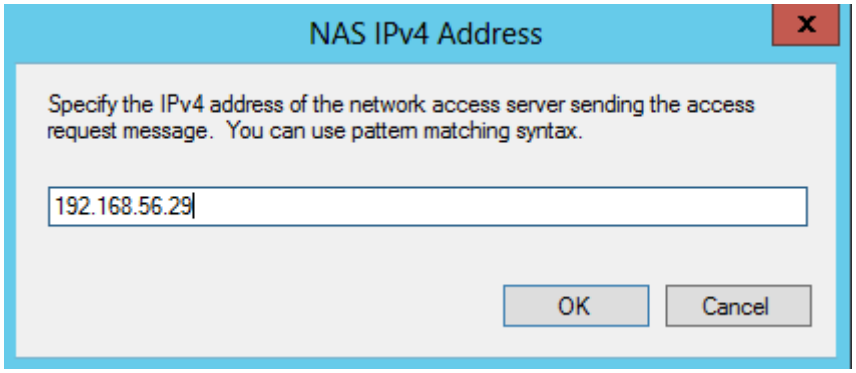
3. Type a descriptive name for identifying this policy in the "Policy name" field.
   - You can leave the "Type of network access server" field to the default -- Unspecified.



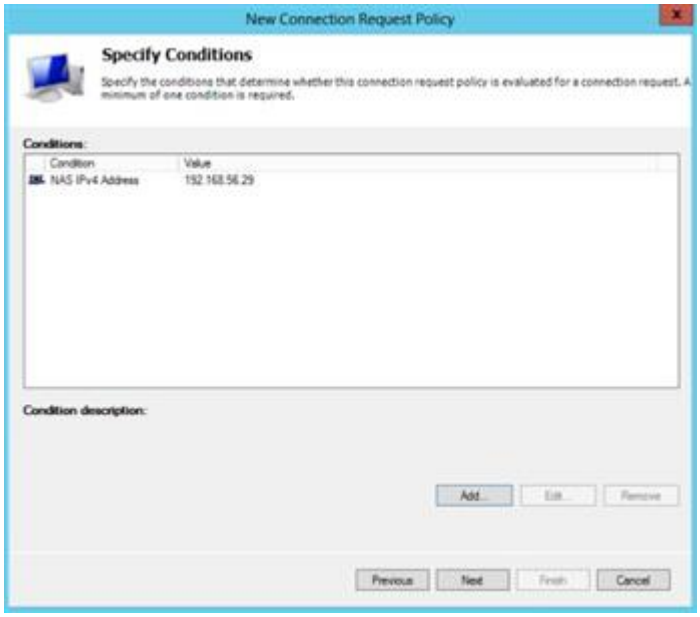
5. The "Select condition" dialog appears. Click Add.



6. The NAS IPv4 Address dialog appears. Type the PX4 IP address -- *192.168.56.29*, and click OK.

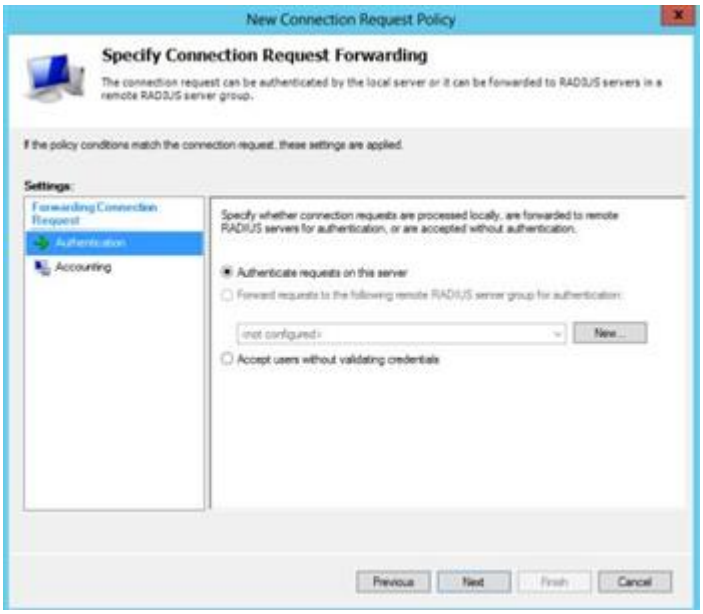


7. Click Next in the New Connection Request Policy dialog.



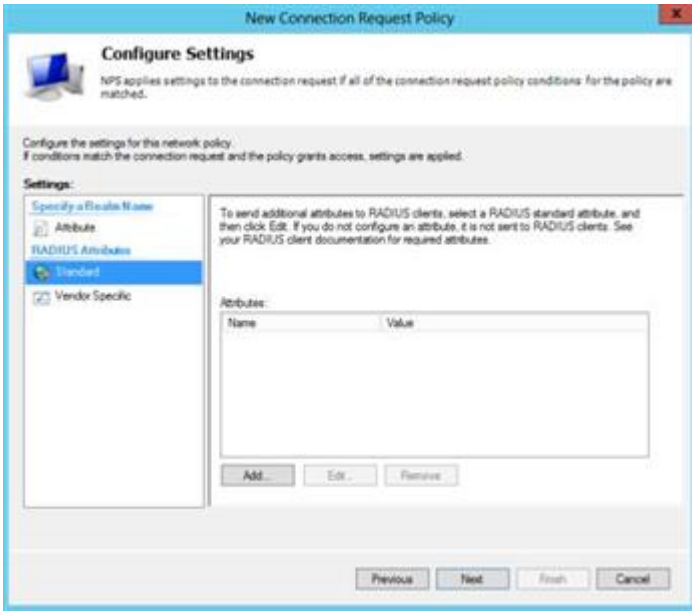
8. Select "Authenticate requests on this server" because a local NPS server is used in this example. Then click Next.

Note: Connection Request Forwarding options must match your environment.



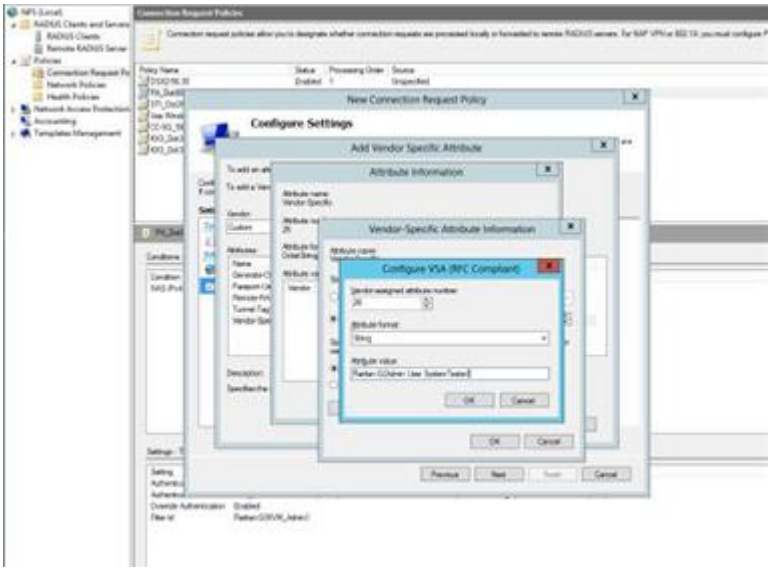
9. When the system prompts you to select the authentication method, select the following two options:
   - Override network policy authentication settings
   - CHAP -- the PX4 uses "CHAP" in this example

   Note: If your PX4 uses PAP, then select "PAP."



10. Select Vendor Specific to the left of the dialog, and click Add. The Add Vendor Specific Attribute dialog appears.
11. Select Custom in the Vendor field, and click Add. The Attribute Information dialog appears.
12. Click Add, and the Vendor-Specific Attribute Information dialog appears.
13. Click "Enter Vendor Code" and type *13742*.
14. Select "Yes, it conforms" to indicate that the custom attribute conforms to the RADIUS Request For Comment (RFC).
15. Click Configure Attribute, and then:
    a. Type *26* in the "Vendor-assigned attribute number" field.
    b. Select String in the "Attribute format" field.
    c. Type *Raritan:G{Admin User SystemTester}* in the "Attribute value" field. In this example, three roles 'Admin,' 'User' and 'SystemTester' are specified inside the curved brackets {}.

Note that multiple roles are separated with a space.



16. Click OK.

FreeRADIUS VSA Illustration

A vendor-specific dictionary file is required for the vendor-specific-attribute configuration on FreeRADIUS. Therefore, there are two major configuration steps.

a. Use a dictionary to define the Raritan vendor-specific attribute
b. Add all user data, including user names, passwords, and roles

► *Presumptions in the illustration:*

- Raritan attribute = `Raritan-User-Roles`
- User name = `steve`
- Steve's password = `test123`
- Steve's roles = `Admin`, `User` and `SystemTester`

► *Step A -- define the vendor-specific attribute in FreeRADIUS:*

1. Go to this location: `/etc/raddb/dictionary`.
2. Type the following in the Raritan dictionary file.

```
VENDOR Raritan 13742
BEGIN-VENDOR Raritan
ATTRIBUTE Raritan-User-Roles 26 string
END-VENDOR Raritan
```

► *Step B -- create a user profile for "steve" in FreeRADIUS:*

1. Go to this location: `/etc/raddb/users`.
2. Add the data of the user "steve" by typing the following. Note that the values after the equal sign (=) must be enclosed in double quotes (").

```
steve Cleartext-Password := "test123"
Raritan-PDU-User-Roles = "Raritan:G{Admin User SystemTester}"
```

AD-Related Configuration

When RADIUS authentication is intended, make sure you also configure the following settings related to Microsoft Active Directory (AD):

- Register the NPS server in AD
- Configure remote access permission for users in AD

The NPS server is registered in AD only when NPS is configured for the FIRST time and user accounts are created in AD.

If CHAP authentication is used, you must enable the following feature for user accounts created in AD:

- Store password using reversible encryption

Important: Reset the user password if the password is set before you enable the "Store password using reversible encryption" feature.

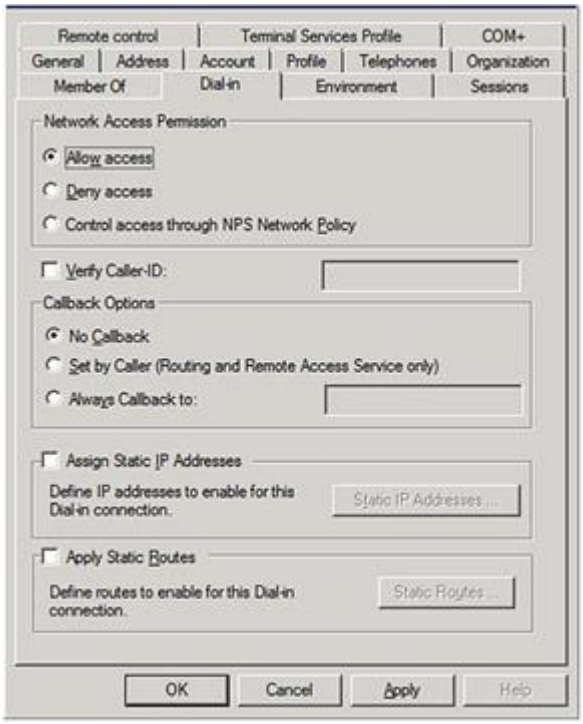
► *To register NPS:*

1. Open the NPS console.
2. Right-click NPS (Local) and select "Register server in Active Directory."

3. Click OK, and then OK again.

► *To grant PX4 users remote access permission:*

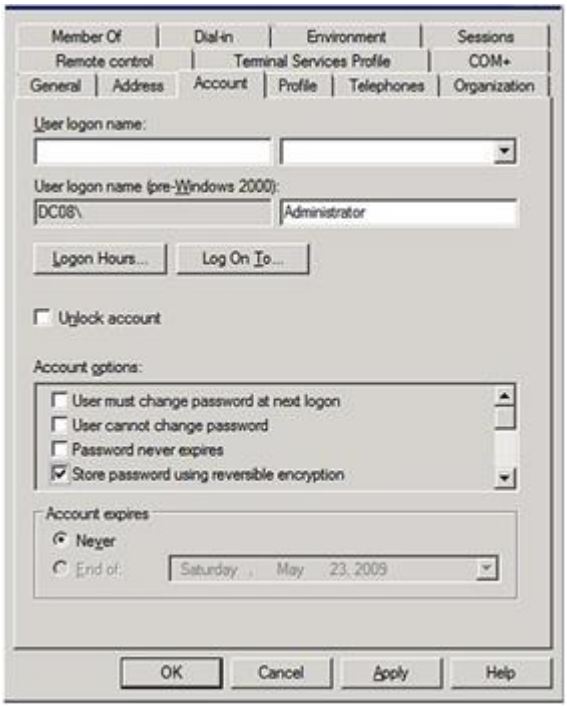
1. Open Active Directory Users and Computers.
2. Open the properties dialog of the user whom you want to grant the access permission.
3. Click the Dial-in tab and select the "Allow access" checkbox.



Raritan
A brand of legrand

► *To enable reversible encryption for CHAP authentication:*

1. Open Active Directory Users and Computers.
2. Open the properties dialog of the user that you want to configure.
3. Click the Account tab and select the "Store password using reversible encryption" checkbox.



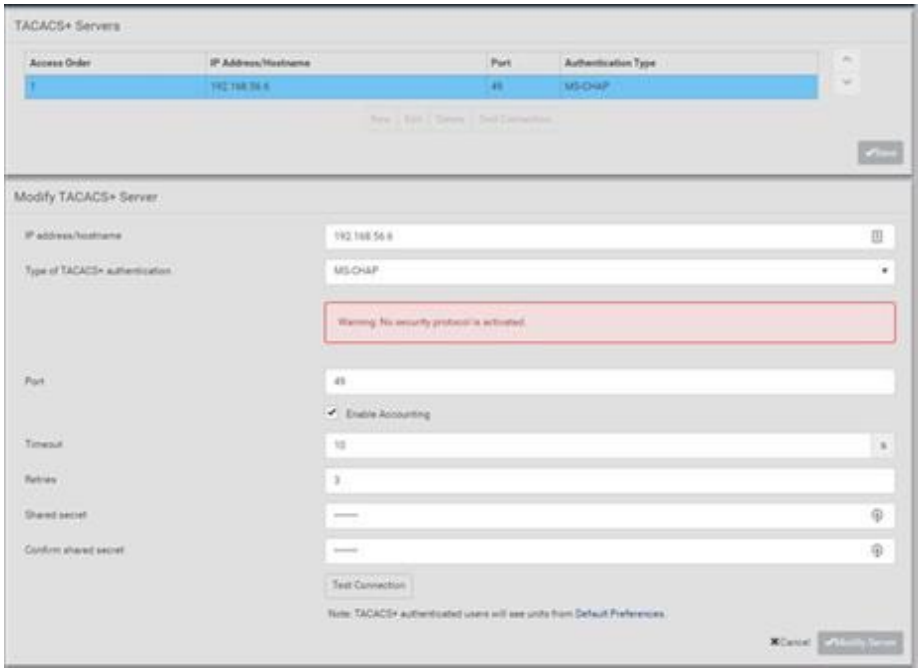
Cisco ISE Xerus TACACS+ Authentication

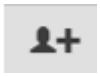
► *Configuring Cisco ISE 2.1.x for authenticating TACACS users on the Xerus Platform*

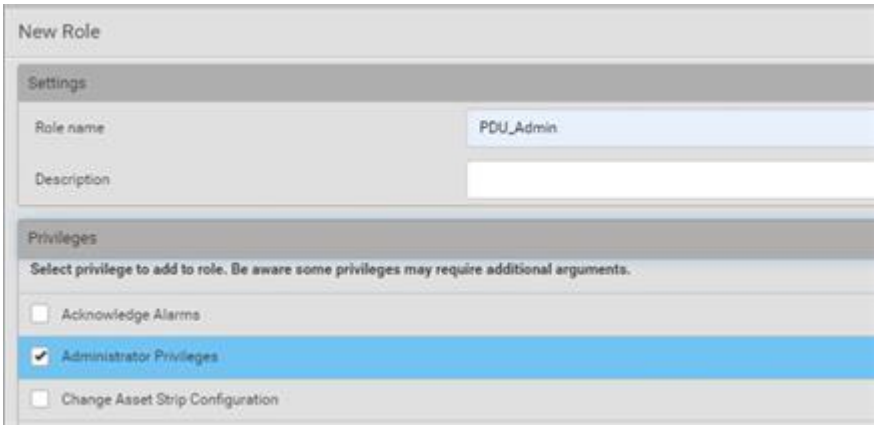
Xerus performs authorization through the user's membership in local roles. You must create a local role on Xerus and matching role (case sensitive) on Cisco ISE.

► *Configure TACACS+ on Xerus:*

1. Log in to PX4 with an administrative account.
2. Select Access Device Settings > Security > TACACS+ and add the Cisco ISE running the TACACS+ server. Select the Type of TACACS+ authentication types (ASCII/PAP/CHAP/MS-CHAP) as appropriate and match the TACACS+ server.



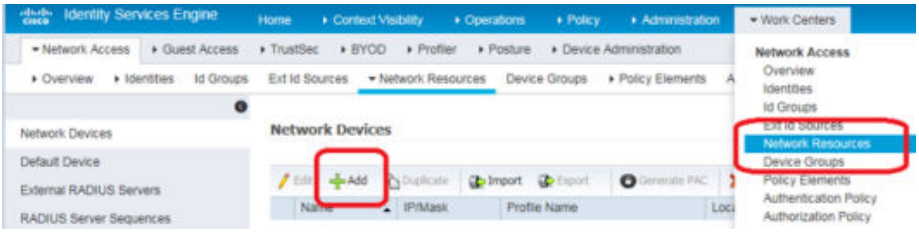
3. Create Roles with appropriate permissions by accessing User Management > Roles > and clicking on Add Role  .



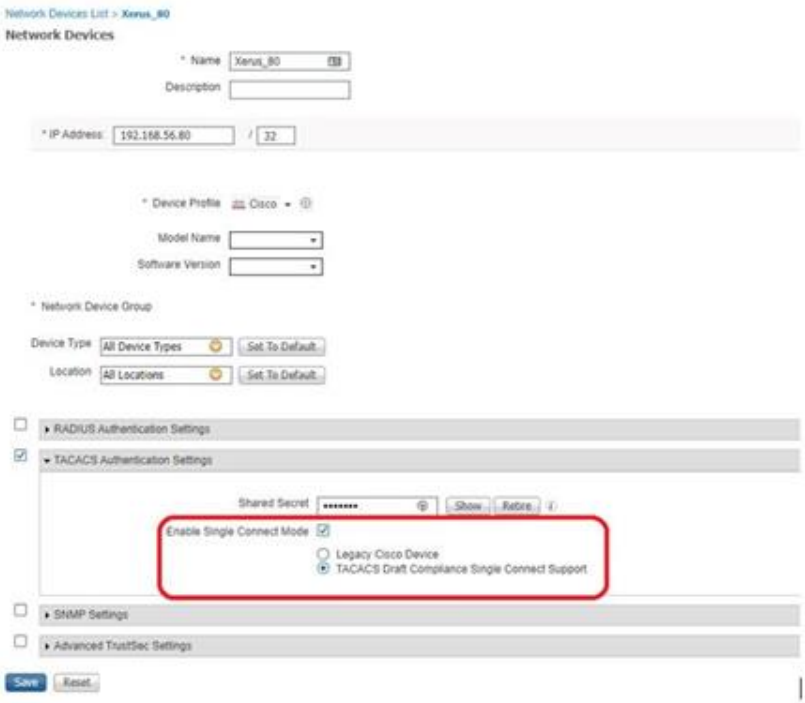
► *Configure Cisco ISE:*

Add the Xerus device to Cisco ISE server:

1. Access Cisco ISE Web URL https://x.x.x.x/admin and log in with administrative credentials.
2. Select Access Work Centers tab > Network Access > Network Resources. On Network Devices click Add.

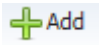


3. Configure Name, Description, IP Address/Range, enable the TACACS Authentication Settings option, set Shared secret, and click Submit to save changes. Be sure to enable Enable Single Connect Mode option and select the TACACS Draft Compliance Single Connect Support radio button.

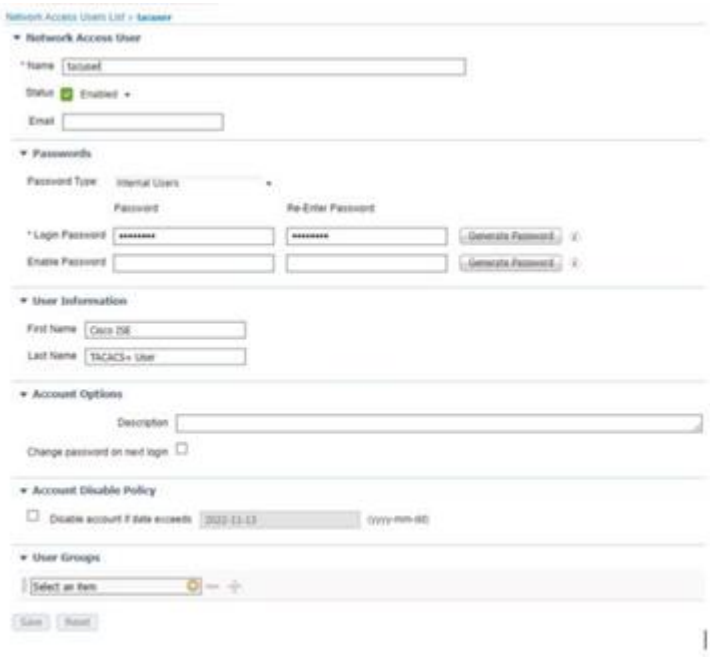


Create/Edit Users:

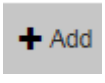
Note: If your environment already has user accounts or configured with external identity source (AD/ LDAP), you may skip this step.

1. Access Work Centers > Device Administration > Identities > and click 

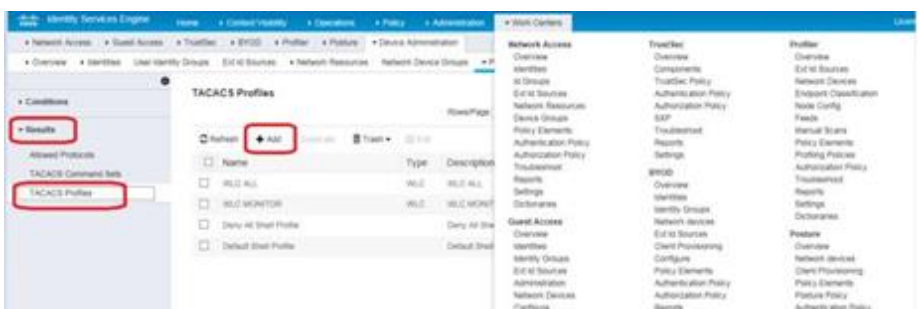
to add a user.



Create TACACS Profile Policy Element:

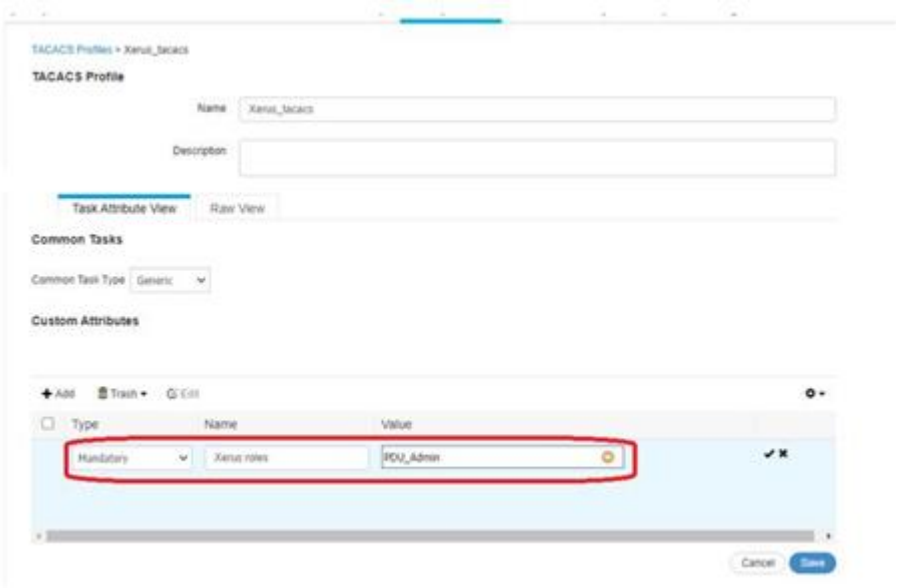
1. On Access Work Centers tab>select Device Administration > Policy Elements > Results >TACACS Profiles and click 

to add a profile.



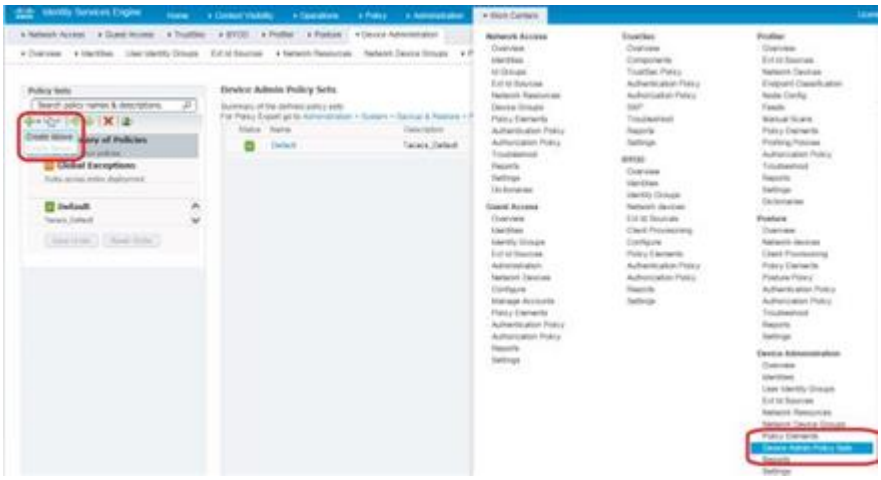
Raritan
A brand of legrand

down, select option Mandatory, Attribute Name as Xerus:roles and value PDU_Admin where PDU_Admin is the role name created locally on Xerus. (Case sensitive) then Click on ✔ to add attribute then click Submit to save changes.

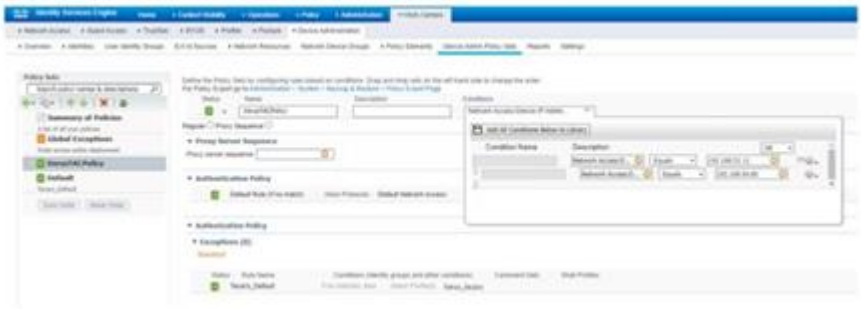


Configure/Create Device Admin Policy Set

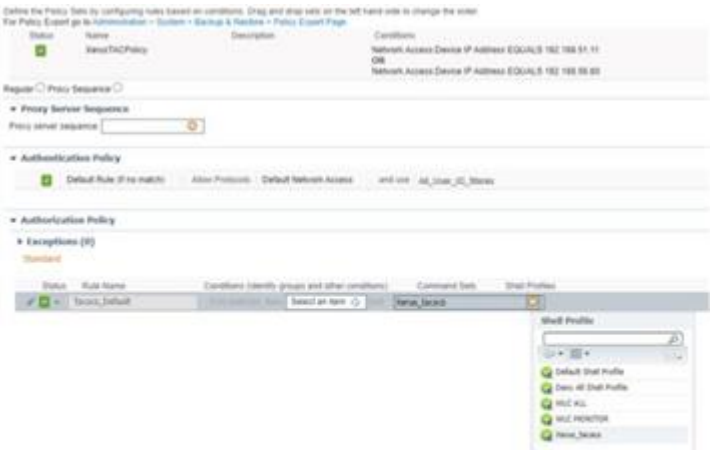
1. On the Work Centers tab, click Device Administration > Device Admin Policy Sets. Click to create a new policy set in left pane. New Policy Set 1 will be created



2. Click Edit, enter the Name, Description, and Condition (optional), and click Done. Authentication Policy is optional unless it is explicitly required for security guidelines.



3. Create the required Authorization Policy. Next, click Edit, specify a drop-down / under Command Sets, select the profile created earlier, and then click Done to save changes.



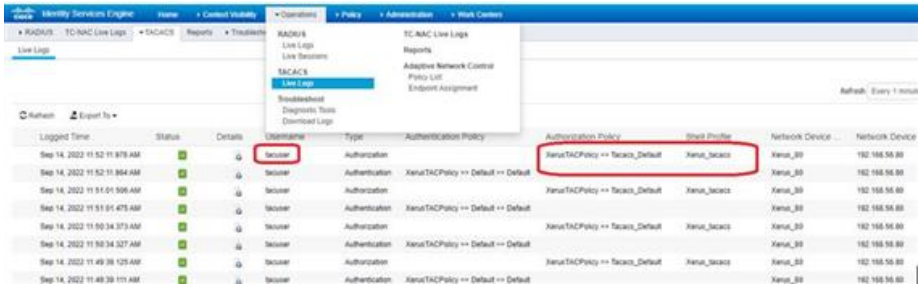
Raritan.
A brand of legrand

► *Troubleshooting Tips*

Logs, and ISE reports are great references to troubleshoot the issues with configuration.

1. Verify from Live Logs under Operations> TACACS that the correct Authorization Policy is applied.

   Click the Details icon to see more information. Alternatively Choose Work Centers > Device Administration > Reports > ISE Reports.



2. User authorization may fail on Xerus if an incorrect policy is applied, considering the following options.
   - Moving policy higher up in the order (in case of multiple policy sets).
   - More appropriate conditions in policy coupled with device type and location when adding Xerus as a network device in Cisco ISE.

Updating the LDAP Schema

In This Chapter

Returning User Group Information. 696
Setting the Registry to Permit Write Operations to the Schema. 696
Creating a New Attribute. 698
Adding Attributes to the Class. 699
Updating the Schema Cache. 700
Editing rciusergroup Attributes for User Members. 700

Returning User Group Information

Use the information in this section to return User Group information (and assist with authorization) once authentication is successful.

From LDAP/LDAPS

When an LDAP/LDAPS authentication is successful, the PX4 determines the permissions for a given user based on the permissions of the user's . Your remote LDAP server can provide these user names by returning an attribute named as follows:

rciusergroup	attribute type: string

This may require a schema extension on your LDAP/LDAPS server. Consult your authentication server administrator to enable this attribute.

In addition, for Microsoft® Active Directory®, the standard LDAP memberOf is used.

From Microsoft Active Directory

Note: This should be attempted only by an experienced Active Directory® administrator.

Returning user information from Microsoft's® Active Directory for Windows 2000® operating system server requires updating the LDAP/LDAPS schema. See your Microsoft documentation for details.

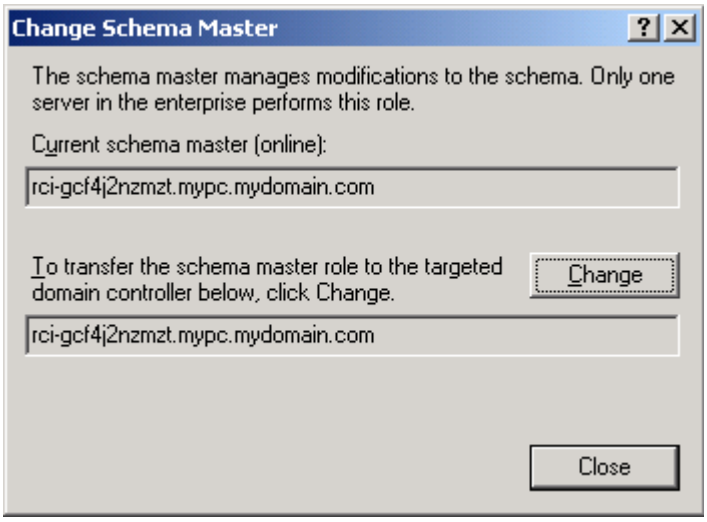
1. Install the schema plug-in for Active Directory. See Microsoft Active Directory documentation for instructions.
2. Run Active Directory Console and select Active Directory Schema.

Setting the Registry to Permit Write Operations to the Schema

To allow a domain controller to write to the schema, you must set a registry entry that permits schema updates.

► *To permit write operations to the schema:*

1. Right-click the Active Directory® Schema root node in the left pane of the window and then click Operations Master. The Change Schema Master dialog appears.

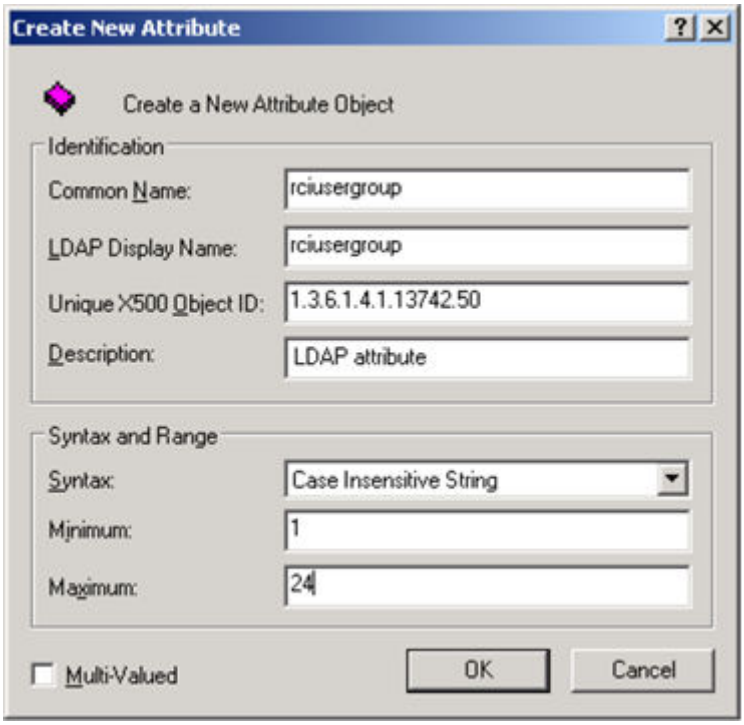


2. Select the "Schema can be modified on this Domain Controller" checkbox. Optional
3. Click OK.

Creating a New Attribute

► *To create new attributes for the rciusergroup class:*

1. Click the + symbol before Active Directory® Schema in the left pane of the window.
2. Right-click Attributes in the left pane.
3. Click New and then choose Attribute. When the warning message appears, click Continue and the Create New Attribute dialog appears.

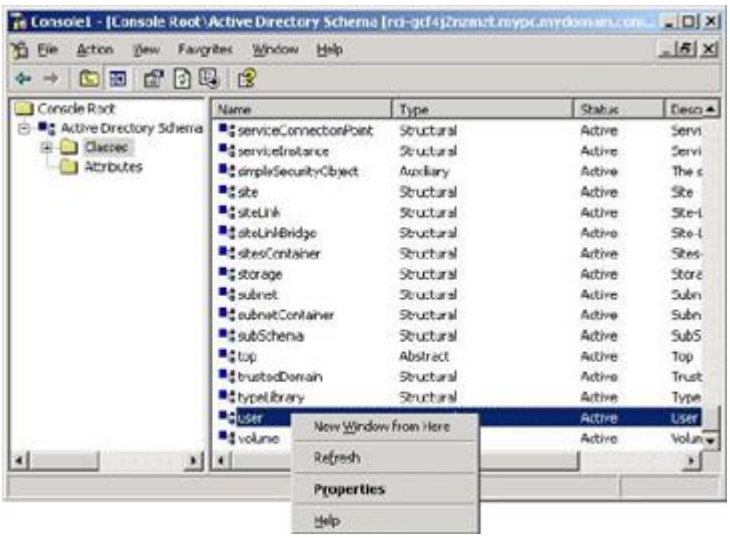


4. Type *rciusergroup* in the Common Name field.
5. Type *rciusergroup* in the LDAP Display Name field.
6. Type *1.3.6.1.4.1.13742.50* in the Unique x5000 Object ID field.
7. Type a meaningful description in the Description field.
8. Click the Syntax drop-down arrow and choose Case Insensitive String from the list.
9. Type *1* in the Minimum field.
10. Type *24* in the Maximum field.
11. Click OK to create the new attribute.

Adding Attributes to the Class

► *To add attributes to the class:*

1. Click Classes in the left pane of the window.
2. Scroll to the user class in the right pane and right-click it.



3. Choose Properties from the menu. The user Properties dialog appears.
4. Click the Attributes tab to open it.
5. Click Add.
6. Choose rciusergroup from the Select Schema Object list.

7. Click OK in the Select Schema Object dialog.
8. Click OK in the User Properties dialog.

Updating the Schema Cache

► *To update the schema cache:*

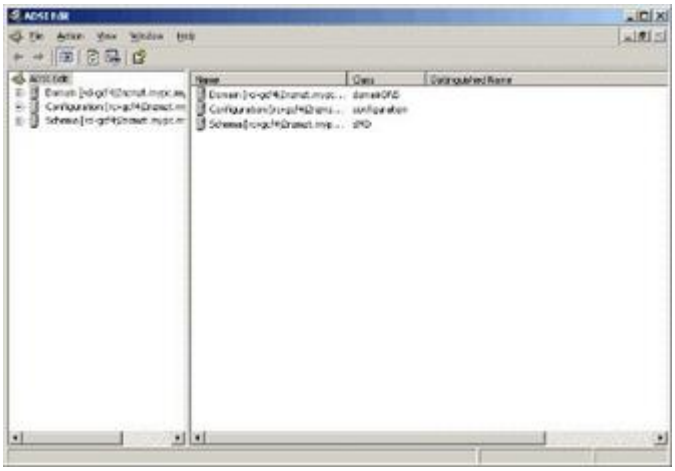
1. Right-click Active Directory® Schema in the left pane of the window and select Reload the Schema.
2. Minimize the Active Directory Schema MMC (Microsoft® Management Console) console.

Editing rciusergroup Attributes for User Members

To run the Active Directory® script on a Windows 2003® server, use the script provided by Microsoft® (available on the Windows 2003 server installation CD). These scripts are loaded onto your system with a Microsoft® Windows 2003 installation. ADSI (Active Directory Service Interface) acts as a low-level editor for Active Directory, allowing you to perform common administrative tasks such as adding, deleting, and moving objects with a directory service.

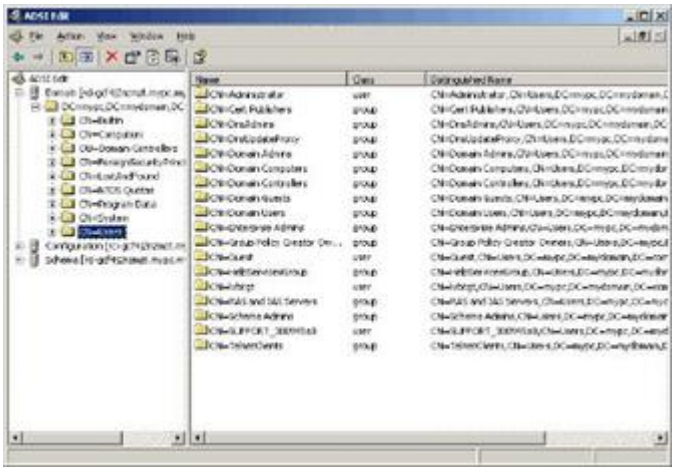
► *To edit the individual user attributes within the group rciusergroup:*

1. From the installation CD, choose Support > Tools.
2. Double-click SUPTOOLS.MSI to install the support tools.
3. Go to the directory where the support tools were installed. Run adsiedit.msc. The ADSI Edit window opens.

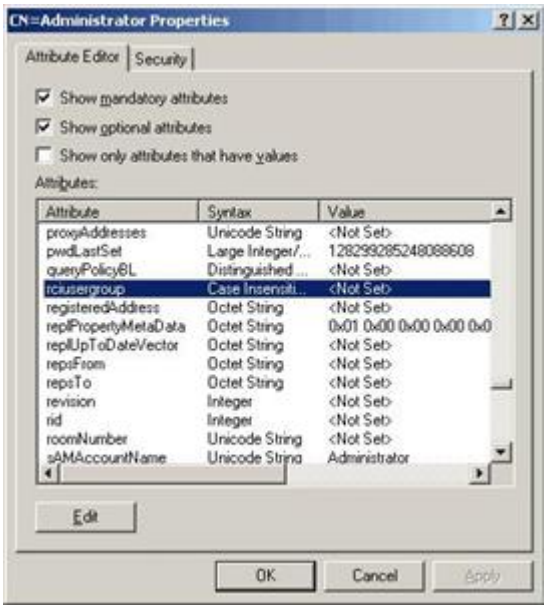


4. Open the Domain.

5. In the left pane of the window, select the CN=Users folder.



6. Locate the user name whose properties you want to adjust in the right pane. Right-click the user name and select Properties.
7. Click the Attribute Editor tab if it is not already open. Choose rciusergroup from the Attributes list.



8. Click Edit. The String Attribute Editor dialog appears.
9. Type the user (created in the PX4) in the Edit Attribute field. Click OK.

Additional Xerus Information - Assorted Products

In This Chapter

Reserving IP Addresses in DHCP Servers. 702
Sensor Threshold Settings. 705
Default Voltage and Current Thresholds. 711
Altitude Correction Factors. 712
Unbalanced Current Calculation. 713
Ways to Probe Existing User Profiles. 714
Role of a DNS Server. 714
Installing the USB-to-Serial Driver (Optional). 714
Device-Specific Settings. 715
TLS Certificate Chain. 716

Reserving IP Addresses in DHCP Servers

Xerus uses the product serial number as the client identifier in the DHCP request. To successfully reserve an IP address in a DHCP server, use the device's serial number as the unique ID instead of the MAC address.

Since all network interfaces can be simultaneously enabled and configured with diverse static IP addresses, the client identifier of each network interface is different. The main difference is the absence/presence of a suffix, which is the interface name added to the end of the serial number. The table below lists the client identifiers of all network interfaces.

Interface	Client identifier
ETH1	serial number
ETH2	serial number plus the uppercase suffix "-ETH2"
WIRELESS	serial number plus the uppercase suffix "-WIRELESS"
BRIDGE	serial number

You can reserve the IP addresses of more than one interfaces in the DHCP server if preferred. Note that you must choose/configure the bridge interface if your device is set to the bridging mode.

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

Reserving IP in Windows

To reserve the IP address of any network interface in the Windows DHCP server, you must convert that interface's client identifier into *hexadecimal* ASCII codes.

In the following illustration, it is assumed that the serial number is PEG1A00003.

► *Windows IP address reservation illustration:*

1. Convert the client identifier of the desired network interface into ASCII codes (*hexadecimal*).

Interface	Client identifier conversion
ETH1	PEG1A00003 = 50 45 47 31 41 30 30 30 30 33
ETH2	PEG1A00003-ETH2 = 50 45 47 31 41 30 30 30 30 33 2D 45 54 48 32 • The suffix comprising the dash symbol and the word "ETH2" is also converted.
WIRELESS	PEG1A00003-WIRELESS = 50 45 47 31 41 30 30 30 30 33 2D 57 49 52 45 4C 45 53 53 • The suffix comprising the dash symbol and the word "WIRELESS" is also converted.
BRIDGE	PEG1A00003 = 50 45 47 31 41 30 30 30 30 33

2. In your DHCP server, go to the New Reservation dialog, and enter the converted ASCII codes without spaces.

For example, to reserve the ETH1 interface's IP address, enter the following data in the dialog.

Field	Data entered
IP address	The IP address you want to reserve.
MAC address	The following ASCII codes. 5045473141303030303 3
Other fields	Configure as needed.

Reserving IP in Linux

There are two methods to reserve the IP address of any network interface in the standard Linux DHCP server (ISC DHCP server):

- Convert an interface's client identifier into *hexadecimal* ASCII codes.
- Use an interface's original client identifier without converting it into ASCII codes.

In the following illustrations, it is assumed that the PX4 serial number is PEG1A00003, and the IP address you want to reserve is 192.168.20.1.

► *Illustration with ASCII code conversion:*

1. Convert the client identifier of the desired network interface into ASCII codes (*hexadecimal*).

Interface	Client identifier conversion
ETH1	PEG1A00003 = 50 45 47 31 41 30 30 30 30 33
ETH2	PEG1A00003-ETH2 = 50 45 47 31 41 30 30 30 30 33 2D 45 54 48 32 • The suffix comprising the dash symbol and the word "ETH2" is also converted.

Interface	Client identifier conversion
WIRELESS	PEG1A00003-WIRELESS = 50 45 47 31 41 30 30 30 30 33 2D 57 49 52 45 4C 45 53 53 • The suffix comprising the dash symbol and the word "WIRELESS" is also converted.
BRIDGE	PEG1A00003 = 50 45 47 31 41 30 30 30 30 33

2. Separate the converted ASCII codes with a colon, and a prefix "00:" must be added to the beginning of the converted codes.

For example, the *converted* client identifier of the ETH1 interface looks like the following:

`00:50:45:47:31:41:30:30:30:30:33`

3. Now enter the converted client identifier with the following syntax.

```
host mypx {
option dhcp-client-identifier = 00:50:45:47:31:41:30:30:30:30:33;
fixed-address 192.168.20.1;
}
```

► *Illustration without ASCII code conversion:*

1. Use the original client identifier of the desired network interface. DO NOT convert them into ASCII codes.
2. A prefix "\000" must be added to the beginning of the client identifier.

For example, the client identifier of the ETH1 interface looks like the following:

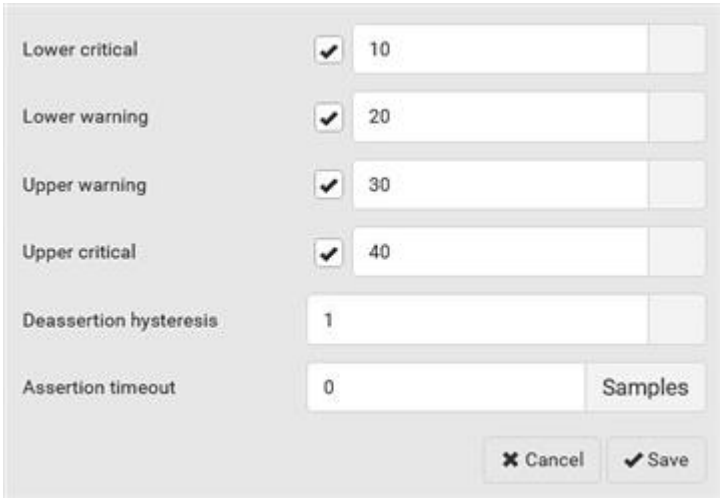
`\000`PEG1A00003

3. Now enter the original client identifier with the following syntax. The client identifier is enclosed in quotation marks.

```
host mypx {
option dhcp-client-identifier = "\000PEG1A00003";
fixed-address 192.168.20.1;
}
```

Sensor Threshold Settings

This section explains the thresholds settings for a numeric sensor.



Thresholds and Sensor States

A numeric sensor has four thresholds: Lower Critical, Lower Warning, Upper Warning and Upper Critical.

The threshold settings determine how many sensor states are available for a certain sensor and the range of each sensor state. The diagram below shows how each threshold relates to each state.

above upper critical
Upper Critical
above upper warning
Upper Warning

normal
Lower Warning
below lower warning
Lower Critical
below lower critical

► *Available sensor states:*

The more thresholds are enabled for a sensor, the more sensor states are available for it. The "normal' state is always available regardless of whether any threshold is enabled.

For example:

- When a sensor only has the Upper Critical threshold enabled, it has two sensor states: normal and above upper critical.
- When a sensor has both the Upper Critical and Upper Warning thresholds enabled, it has three sensor states: normal, above upper warning, and above upper critical.

States of "above upper warning" and "below lower warning" are warning states to call for your attention.

States of "above upper critical" and "below lower critical" are critical states that require you to immediately handle.

► *Range of each available sensor state:*

The value of each enabled threshold determines the reading range of each available sensor state.

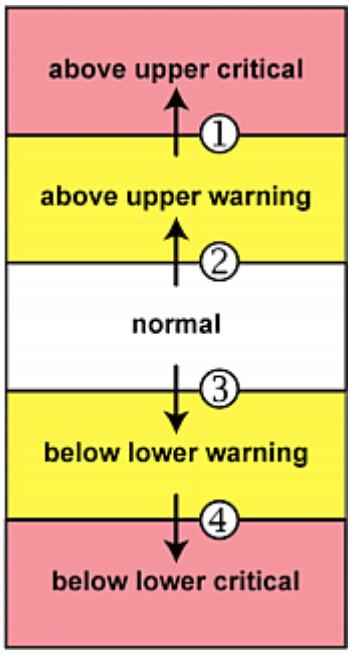
"To Assert" and Assertion Timeout

If multiple sensor states are available for a specific sensor, the PX4 asserts a state for it whenever a bad state change occurs.

► *To assert a state:*

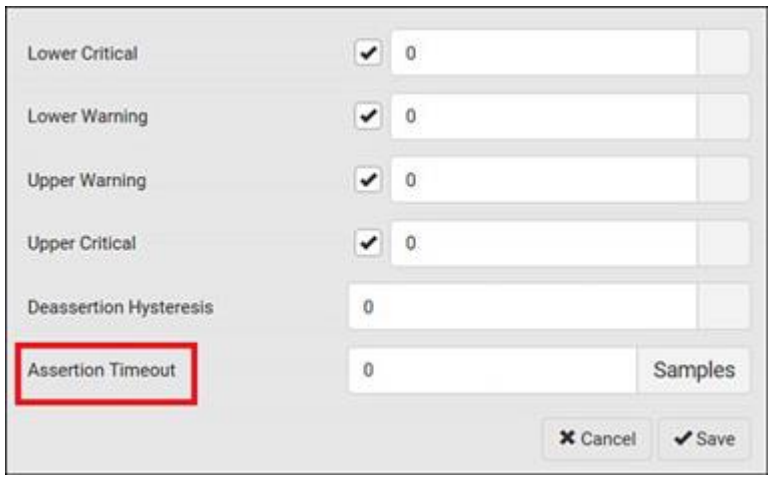
To assert a state is to announce a new, "worse" state.

Below are bad state changes that cause the PX4 to assert.



1. above upper warning --> above upper critical
2. normal --> above upper warning
3. normal --> below lower warning
4. below lower warning --> below lower critical

► *Assertion Timeout:*



In the threshold settings, the Assertion Timeout field postpones the "assertion" action. It determines how long a sensor must remain in the "worse" new state before the PX4 triggers the "assertion" action. If that sensor changes its state again within the specified wait time, the PX4 does NOT assert the worse state.

To disable the assertion timeout, set it to 0 (zero).

Note: For most sensors, the measurement unit in the "Assertion Timeout" field is sample. Sensors are measured every second, so the timing of a sample is equal to a second. Raritan's BCM2 is an exception to this, with a sample of 3 seconds.

► *How "Assertion Timeout" is helpful:*

If you have created an event rule that instructs the PX4 to send notifications for assertion events, setting the "Assertion Timeout" is helpful for eliminating a number of notifications that you may receive in case the sensor's readings fluctuate around a certain threshold.

Assertion Timeout Example for Temperature Sensors

Assumption:

```
Upper Warning threshold is enabled.
Upper Warning = 25 (degrees Celsius)
Assertion Timeout = 5 samples (that is, 5 seconds)
```

When a temperature sensor's reading exceeds 25 degrees Celsius, moving from the "normal" range to the "above upper warning" range, the PX4 does NOT immediately announce this warning state. Instead it waits for 5 seconds, and then does either of the following:

- If the temperature remains above 25 degrees Celsius in the "above upper warning" range for 5 seconds, the PX4 performs the "assertion" action to announce the "above upper warning" state.
- If the temperature drops below 25 degrees Celsius within 5 seconds, the PX4 does NOT perform the "assertion" action.

"To De-assert" and Deassertion Hysteresis

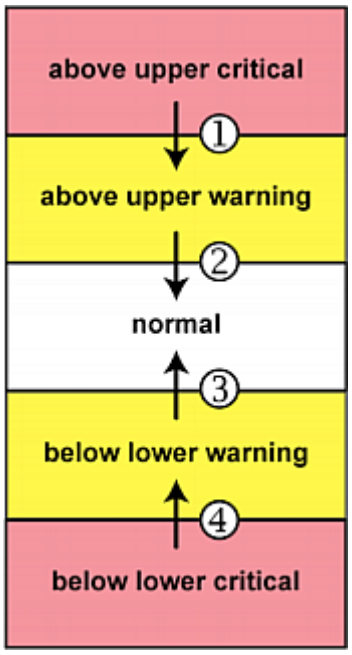
After the PX4 asserts a worse state for a sensor, it may de-assert that state later on if the readings improve.

► *To de-assert a state:*

To de-assert a state is to announce the end of the previously-asserted worse state.

Below are good state changes that cause the PX4 to de-assert the previous state.

Raritan
A brand of legrand



1. above upper critical --> above upper warning
2. above upper warning --> normal
3. below lower warning --> normal
4. below lower critical --> below lower warning

- *Deassertion Hysteresis:*

In the threshold settings, the Deassertion Hysteresis field determines a new level to trigger the "deassertion" action.

This function is similar to a thermostat, which instructs the air conditioner to turn on the cooling system when the temperature exceeds a pre-determined level. "Deassertion Hysteresis" instructs the PX4 to de-assert the worse state for a sensor only when that sensor's reading reaches the pre-determined "deassertion" level.

For upper thresholds, this "deassertion" level is a decrease against each threshold. For lower thresholds, this level is an increase to each threshold. The absolute value of the decrease/increase is exactly the hysteresis value.

For example, if Deassertion Hysteresis = 2, then the deassertion level of each threshold is either "+2" or "-2" as illustrated below.

Threshold value	**Deassertion value**
Upper Critical = 33	Deassertion level = 31 • 33 - 2 = 31
Upper Warning = 25	Deassertion level = 23 • 25 - 2 = 23
Lower Critical = 10	Deassertion level = 12 • 10 + 2 = 12
Lower Warning = 18	Deassertion level = 20 • 18 + 2 = 20

To use each threshold as the "deassertion" level instead of determining a new level, set the Deassertion Hysteresis to 0 (zero).

Note: The difference between Upper Warning and Lower Warning must be at least "two times" of the deassertion value.

► *How "Deassertion Hysteresis" is helpful:*

If you have created an event rule that instructs the PX4 to send notifications for deassertion events, setting the "Deassertion Hysteresis" is helpful for eliminating a number of notifications that you may receive in case a sensor's readings fluctuate around a certain threshold.

Deassertion Hysteresis Example for Temperature Sensors

Assumption:

```
Upper Warning threshold is enabled.
Upper Warning = 20 (degrees Celsius)
Deassertion Hysteresis = 3 (degrees Celsius)
"Deassertion" level = 20-3 = 17 (degrees Celsius)
```

When the PX4 detects that a temperature sensor's reading drops below 20 degrees Celsius, moving from the "above upper warning" range to the "normal" range, either of the following may occur:

- If the temperature falls between 20 and 17 degrees Celsius, the PX4 does NOT perform the "deassertion" action.
- If the temperature drops to 17 degrees Celsius or lower, the PX4 performs the "deassertion" action to announce the end of the "above upper warning" state.

Default Voltage and Current Thresholds

The following are factory-default voltage and current thresholds. There are no default values set for *lower* current thresholds because lower thresholds are not useful.

Availability of diverse thresholds depends on the capability of the model you purchased.

► *Single-phase inlets or outlets:*

- RMS voltage:

Threshold	Default value
Lower critical	-6% of minimum rating
Lower warning	-3% of minimum rating
Upper warning	+3% of maximum rating
Upper critical	+6% of maximum rating
Hysteresis	2V

- RMS current:

Threshold	Default value
Upper warning	65% of rating
Upper critical	80% of rating
Hysteresis	1A

► *Multi-phase inlets or outlets:*

- Line-Line RMS voltage:

Threshold	Default value
Lower critical	-6% of minimum rating
Lower warning	-3% of minimum rating
Upper warning	+3% of maximum rating

Threshold	Default value
Upper critical	+6% of maximum rating
Hysteresis	2V

- Line RMS current:

Threshold	Default value
Upper warning	65% of rating
Upper critical	80% of rating
Hysteresis	1A

- Unbalanced current:

Threshold	Default value
Upper critical	10% -- disabled by default
Upper warning	5% -- disabled by default
Hysteresis	2%

► *Overcurrent protectors which aims to protect the PDU's outlets:*

- OCP RMS current:

Threshold	Default value
Upper critical	80% of OCP rating
Upper warning	65% of OCP rating
Hysteresis	1A

► *Total residual current:*

Threshold	***Default value***
Upper critical	***30mA***
Hysteresis	***15mA***

Altitude Correction Factors

If a Raritan differential air pressure sensor is attached to your device, the altitude you enter for the device can serve as an altitude correction factor. That is, the reading of the differential air pressure sensor will be multiplied by the correction factor to get a correct reading.

This table shows the relationship between different altitudes and correction factors.

Altitude (meters)	Altitude (feet)	Correction factor
0	0	0.95
250	820	0.98
425	1394	1.00
500	1640	1.01
740	2428	1.04
1500	4921	1.15
2250	7382	1.26
3000	9842	1.38

Unbalanced Current Calculation

Information on unbalanced current is currently available for 3-phase models only and is not applicable to Branch Circuit Monitors.

This section explains how the product calculates the unbalanced current percentage.

► *Calculation:*

1. Calculate the average current of all 3 lines.

```
Average current = (L1+L2+L3) / 3
```

2. Calculate each line's current unbalance by having each line current subtracted and divided with the average current.

```
L1 current unbalance = (L1 - average current) / average current
L2 current unbalance = (L2 - average current) / average current
L3 current unbalance = (L3 - average current) / average current
```

3. Determine the maximum absolute value among three lines' current unbalance values.

```
Maximum (|L1 current unbalance|, |L2 current unbalance|, |L3 current
unbalance|)
```

4. Convert the maximum value to a percentage.

```
Unbalanced load percent = 100 * maximum current unbalance
```

► *Example:*

- Each line's current:
  L1 = 5.5 amps
  L2 = 5.2 amps

L3 = 4.0 amps

- Average current: (5.5+5.2+4.0) / 3 = 4.9 amps
- L1 current unbalance: (5.5 - 4.9) / 4.9 = 0.1224
- L2 current unbalance: (5.2 - 4.9) / 4.9 = 0.0612
- L3 current unbalance: (4.0 - 4.9) / 4.9 = -0.1837
- Maximum current unbalance:
  Maximum (|0.1224|, |0.0612|, |-0.1837|) = 0.1837
- Current unbalance converted to a percentage:
  100 * (0.1837) = 18%

Ways to Probe Existing User Profiles

This section indicates available ways to query existing user accounts on the PX4.

- With SNMP v3 activated, you get the "user unknown" error when the user name used to authenticate does not exist.
- Any user with the permission to view event rules can query all local existing users via JSON RPC.
- Any user with the permission to view the event log may get information about existing users from the log entries.
- Any authenticated users can query currently-existing connection sessions, including Webcam-Live-Preview sessions, which show a list of associated user names.

Role of a DNS Server

As Internet communications are carried out on the basis of IP addresses, appropriate DNS server settings are required for mapping domain names (host names) to corresponding IP addresses, or the PX4 may fail to connect to the given host.

Therefore, DNS server settings are important for external authentication. With appropriate DNS settings, the PX4 can resolve the external authentication server's name to an IP address for establishing a connection. If the *SSL/TLS encryption* is enabled, the DNS server settings become critical since only fully qualified domain name can be used for specifying the LDAP server.

For information on external authentication, see Setting Up External Authentication.

Installing the USB-to-Serial Driver (Optional)

The PX4 can emulate a USB-to-serial converter over a USB connection. A USB-to-serial driver named "Dominion PX2 Serial Console" is required for Microsoft® Windows® operating systems.

Download the Windows driver for USB serial console from the Raritan website's *Support page* (www.raritan.com/support). The downloaded driver's name is *dominion-serial-setup-<n>.exe*, where <n> represents the file's version number.

There are two ways to install this driver: automatic and manual installation. Automatic driver installation is highly recommended.

► *Automatic driver installation in Windows®:*

1. Make sure the PX4 is NOT connected to the computer via a USB cable.
2. Run dominion-serial-setup-<n>.exe on the computer and follow online instructions to install the driver.

Note: If any Windows security warning appears, accept it to continue the installation.

---

3. Connect the PX4 to the computer via a USB cable. The driver is automatically installed.

► *Manual driver installation in Windows®:*

1. Make sure the PX4 has been connected to the computer via a USB cable.
2. The computer detects the new device and the "Found New Hardware Wizard" dialog appears.
   - If this dialog does not appear, choose Control Panel > System > Hardware > Device Manager, right-click the *Dominion PX2 Serial Console*, and choose Update Driver.
3. Select the option of driver installation from a specific location, and then specify the location where both *dominion-serial.inf* and *dominion-serial.cat* are stored.

Note: If any Windows security warning appears, accept it to continue the installation.

---

4. Wait until the installation is complete.

Note: If the PX4 enters the disaster recovery mode when the USB serial driver is not installed yet, it may be shown as a 'GPS camera' in the Device Manager on the computer connected to it.

► *In Linux:*

No additional drivers are required, but you must provide the name of the tty device, which can be found in the output of the "dmesg" after connecting the PX4 to the computer. Usually the tty device is "/dev/ttyACM#" or "/dev/ttyUSB#," where # is an integer number.

For example, if you are using the kermit terminal program, and the tty device is "/dev/ttyACM0," perform the following commands:

> set line /dev/ttyACM0

> Connect

Device-Specific Settings

A bulk configuration file will NOT contain any device-specific information like the following list.

For further information, simply open the built-in bulk profile for a detailed list of 'excluded' settings.

- Device name
- SNMP system name, contact and location
- Part of network settings (IP address, gateway, netmask and so on)
- Device logs
- Names, states and values of environmental sensors and actuators
- TLS certificate
- Server monitoring entries
- Asset strip names and rack unit names
- Outlet names and states

TLS Certificate Chain

A TLS server sends out a certificate to any client attempting to connect to it. The receiver determines whether a TLS server can be trusted by verifying that server's certificate, using the certificate (chain) stored on the receiver.

Therefore, to successfully connect to a TLS server, you must upload a valid certificate or (partial) certificate chain to the receiver.

The uploaded certificate (chain) must contain all missing certificates "related to" that TLS server's certificate in some way. Otherwise, the connection made to that TLS server will fail.

- For information on how the uploaded certificate (chain) is related to a TLS server's certificate, see *What is a Certificate Chain* (on page).
- For an example of creating and uploading a TLS certificate to PX4, see *Illustration - GMAIL SMTP Certificate Chain* (on page).

What is a Certificate Chain

If you are familiar with a certificate chain, you can ignore this topic and refer to *Illustration - GMAIL SMTP Certificate Chain* (on page).

A certificate or a chain of certificates is used for trusting a TLS server that you want to connect.

The receiver, such as PX4, can trust a TLS server only after an appropriate certificate (chain) which is "related to" that TLS server's certificate is uploaded to the receiver.

► *How a certificate chain is generated:*

To explain how a TLS server's certificate is "related to" the certificate (chain) that is uploaded to the receiver, we assume that there are three "related" certificates.

- Certificate C. The certificate issued to the TLS server you want to connect.
  'Certificate C' is issued by the certificate authority (CA) entity called 'Issuer B'.
- Certificate B. The certificate issued to 'Issuer B'.
  'Certificate B' is issued by a CA entity called 'Issuer A', and it is an intermediate certificate.
- Certificate A. The self-signed certificate issued by Issuer A. Issuer A is a root CA.

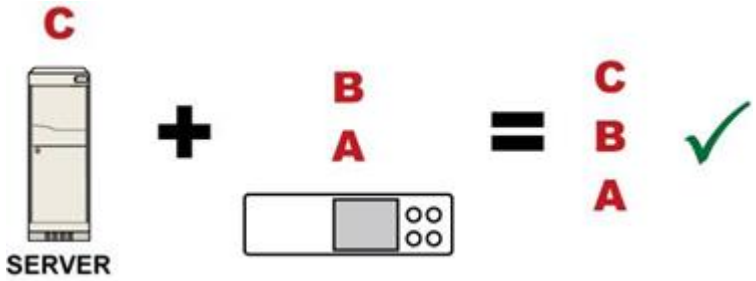
The above three certificates form a certificate path, which is called the "certificate chain".

Each certificate in the chain is the issuer certificate of the certificate that follows it. That is, A is the issuer certificate of B, and B is the issuer certificate of C.

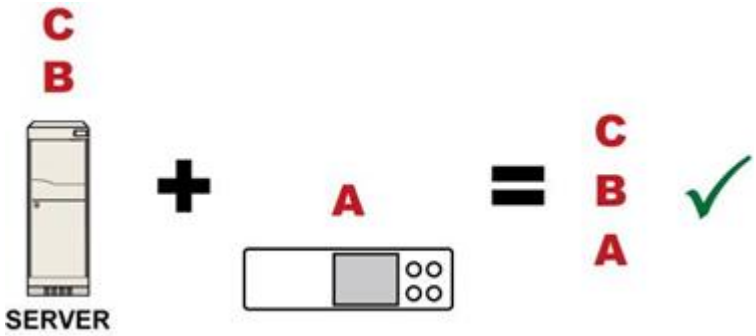
Note: In fact many certificate chains may comprise only the root certificate and a TLS server's certificate and do not have any intermediate certificate(s) like 'Certificate B' involved. Or some chains may contain more than one intermediate certificates.

► *Certificate (chain) that you must upload to the receiver, such as PX4:*

Because the TLS server provides only 'Certificate C', you need to upload a file containing the missing certificates of the chain (that is, 'Certificate A' and 'Certificate B') to the receiver.

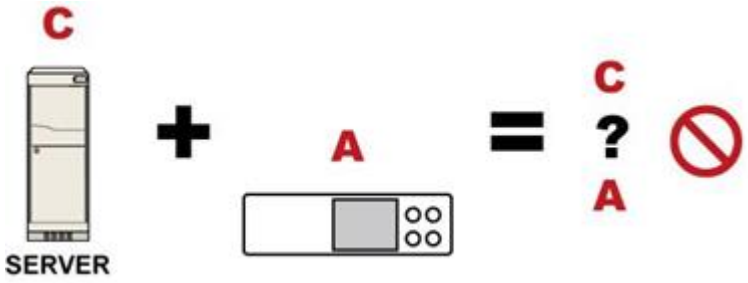


In reality some servers may provide a partial (or even a full) certificate chain instead of a single server certificate. If your server provides a partial certificate chain containing 'Certificate B' and 'Certificate C', then you only need to upload 'Certificate A" to the receiver. If the server has a full certificate chain containing Certificates 'A', 'B', and 'C', then you also need to upload the root certificate 'A".

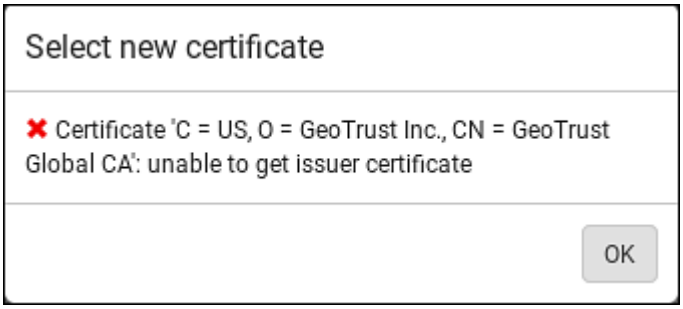


Warning: The certificate (chain) uploaded to the receiver must always contain the ROOT certificate even though the TLS server provides the root certificate. When uploading a (partial) chain onto the PX4, it means you trust each certificate in the chain to certify the authenticity of certificates a server sends to PX4. Therefore, at least the root certificate must be authentic, issued by a CA you trust, and downloaded from that CA over a secure channel. Never implicitly trust a root certificate that is sent by the server which you want to connect to. It could have been created by an attacker.

If either certificate 'A' or 'B' is missing in the certificate file uploaded to the receiver, the connection to the wanted TLS server will fail.



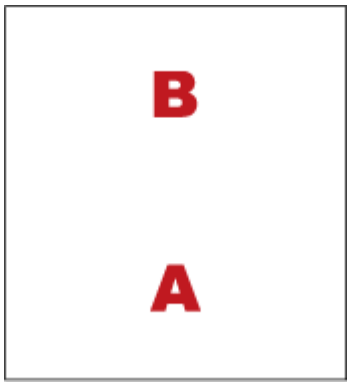
For PX4, if any required certificate is missing, a certificate error message similar to the following is shown on the PX4 web interface.



It is NOT recommended to upload the server certificate to the receiver except when it is a self-signed certificate. Using self-signed server certificates is also not recommended and may not even work in all cases.

► *Order of the chain in the certificate file:*

The order of a certificate chain's content in the certificate file uploaded to the receiver must look like the following.



- The top is the final intermediate certificate of the chain "B" if you have to upload a partial chain.
- The bottom is always the root certificate "A".
- When copying multiple certificates to a single file, make sure you also copy the lines of BEGIN CERTIFICATE and END CERTIFICATE from each certificate.

Illustration - GMAIL SMTP Certificate Chain

If you will apply your company's SMTP service to PX4, ignore this GMAIL illustration topic. Simply contact your IT department to retrieve the appropriate certificate (chain) file and upload it to the PX4.

This section illustrates the upload of a TLS "root" certificate for using the "gmail.com" SMTP service.

Unlike normal TLS websites, where you can easily find its server certificate by using a Web browser, the method to find an SMTP server's certificate is more difficult, which requires appropriate tools and sufficient technical knowledge. For example, you may have to use the openssl command as illustrated below to retrieve the certificate of the GMAIL SMTP server.

► *Step 1 -- Find the certificate(s) the SMTP server has:*

1. Issue the following command in the appropriate command line application.
   - In the following example command, we assume the server "smtp.gmail.com" provides the SMTP service. You can change the server name, port number, command or even the tool as needed.

```
openssl s_client -showcerts -connect smtp.gmail.com:465
```

Alternative: To view the certificate chain instead of all certificates, you can remove the "-showcerts" option from the above command.

---

1. Information that shows the certificates the SMTP server has is displayed.

```
.
.
.
Certificate chain
0 s:/C=US/ST=California/L=Mountain View/O=Google Inc/CN=smtp.gmail.com
i:/C=US/O=Google Inc/CN=Google Internet Authority G2
-----BEGIN CERTIFICATE-----
MIIEdjCCA16gAwIBAgIIbzO9vIL2OXcwDQYJKoZIhvcNAQELBQAwSTELMAkGA1UE
.
.
YHKKJH96sSNC+6dLpOOoRritL5z+jn2WFLcQkL2mRoWQi6pYTzPyXB4D
-----END CERTIFICATE-----
1 s:/C=US/O=Google Inc/CN=Google Internet Authority G2
i:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
-----BEGIN CERTIFICATE-----
MIIEKDCCAxCgAwIBAgIQAQAhJYiw+lmnd+8Fe2Yn3zANBgkqhkiG9w0BAQsFADBC
.
.
MqO5tzHpCvX2HzLc
-----END CERTIFICATE-----
2 s:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
i:/C=US/O=Equifax/OU=Equifax Secure Certificate Authority
-----BEGIN CERTIFICATE-----
MIIDfTCCAuagAwIBAgIDErvmMA0GCSqGSIb3DQEBBQUAME4xCzAJBgNVBAYTAlVT
.
.
b8ravHNjkOR/ez4iyz0H7V84dJzjA1BOoa+Y7mHyhD8S
-----END CERTIFICATE-----
---
Server certificate
subject=/C=US/ST=California/L=Mountain View/O=Google Inc/CN=smtp.gmail.com
issuer=/C=US/O=Google Inc/CN=Google Internet Authority G2
.
.
.
```

2. Onscreen information under the title 'Certificate chain' indicates that there are three issuers and three certificates on this server.
   - Each line beginning with the letter "i" indicates an issuer. They are:

Raritan
A brand of legrand

        - *Google Internet Authority G2*
        - *GeoTrust Global CA*
        - *Equifax Secure Certificate Authority*
    - Each certificate begins with the line "BEGIN CERTIFICATE" and ends with the line "END CERTIFICATE".
    - The topmost certificate is the server certificate.
3. The section titled "Server certificate" indicates that the issuer (CA) *Google Internet Authority G2* issues the server certificate.
4. As the server has the server certificate and two intermediate certificates, we conclude that this server sends a partial certificate chain to the receiver.
5. Check whether the issuer "Equifax Secure Certificate Authority" is the root CA.
    - If yes, you only need to upload the root certificate self-signed by *Equifax Secure Certificate Authority* to PX4.
    - If not, you need to find all missing issuer certificates, including the root certificate, and upload them to PX4.

► *Step 2 -- Find and download the content of missing issuer certificate(s):*

1. View the name of the issuer (CA) at the bottom. In this example, this issuer is 'Equifax Secure Certificate Authority'.
2. Use the issuer's name 'Equifax Secure Certificate Authority' to search for its certificate on the Internet, and then download or copy the content from an authentic source, which is usually its official website.

Important: To prevent the downloaded certificate from being modified or manipulated, you must secure the download with TLS via a trusted certificate.

---

3. As it is found the Equifax Secure Certificate Authority's certificate is self signed by 'Equifax Secure Certificate Authority', which indicates it is the root CA, there are no more missing certificates to search for.

► *Step 3 -- Upload the missing certificate(s) to PX4:*

1. Paste the root certificate's content into a plain text file that will be uploaded to PX4.
    - Content copying must include the lines of "BEGIN CERTIFICATE" and "END CERTIFICATE".
2. Save that file as a *.pem*, *.crt* or *.cer* file. In this example, it is named as "my-root.pem."
3. Upload the file "my-root.pem" to PX4 for using the GMAIL SMTP service.

Note: If your SMTP server requires the upload of a certificate file comprising multiple certificates, make sure the order of these certificates is correct in the file. See *What is a Certificate Chain* (on page).

► *IMPORTANT NOTE:*

If your SMTP server provides a full certificate chain, you should be suspicious whether any attacker fakes the certificate chain and doubt whether the root certificate on that server is authentic. It is STRONGLY recommended to download the root certificate from an authentic source, which is usually the root CA's website, rather than from the server you want to connect.

Xerus Product Integration

This section contains information about possible integrations of Xerus products with other Legrand, Raritan, Server Technology, or third-party products to provide diverse power solutions. Not all Xerus products support all integrations.

Connecting a PDU to a Dominion KVM or Serial Device

Some Xerus- firmware PDUs can be integrated with Raritan KVM or Serial devices.

► *PDU connection via Feature port (only for PX2, PX3 or PX3TS devices)*

Raritan PX series rack PDUs can be connected to the Dominion device using the D2CIM-PWR CIM.

► *To connect the rack PDU:*

1. Connect a Raritan KX3 KVM switch to the "FEATURE" port of the rack PDU using a D2CIM-PWR CIM and CAT5 cable. For example, set up as KX3 <-> CAT5 cable <-> D2CIM-PWR CIM <-> "FEATURE" port of the PX4 PDU. or set up as KX3 <-> CAT5 cable <-> D2CIM-PWR CIM <-> "FEATURE" port of the PRO4X PDU.

Note: PX2, PX3 or PX3TS series has RJ-45 "FEATURE" port.

---

1. Attach an AC power cord to the target server and an available rack PDU outlet.
2. Connect the rack PDU to an AC power source.
3. Power on the device.

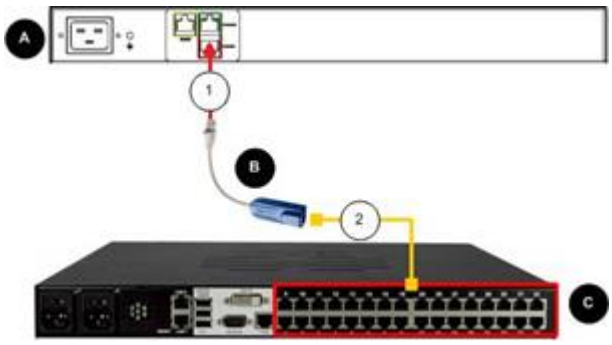


Diagram key

A	Rack PDU
B	D2CIM-PWR
C	KX III
1	D2CIM-PWR to rack PDU connection
2	D2CIM-PWR to KX III target device port via Cat5 cable

► *PDU connection via USB port (only for PRO4X and PX4 devices)*

PRO3X, PRO4X and PX4 devices do not have a feature port, so the connection to a Power CIM peer can be achieved through an USB dongle (DSER-PWR-USB-G4, DKX3-PWR-USB-G4 and DSER-CLI-USB-G4) and a USB-A port. You can use SNMP protocol to communicate to the Raritan KVM or serial devices.

Note: Power CIM peer stands for either a Raritan KVM switch (KX2, KX3 via D2CIM-PWR) or a Raritan serial switch (SX2, KSX2).

► *To connect PX4 or PRO4X*

1. You can connect a Raritan KX3 KVM Switch via Power CIM DKX3-PWR-USB-G4 or via Power CIM DSER-CLI-USB-G4 for a CLI connection or Power CIM DSER-PWR-USB for a serial device. Listed here are the several ways devices can be connected via power CIMs.
   - To connect a Raritan KX3 KVM Switch to one of the PDU's USB-A ports use a CAT5 cable and a Power CIM (DKX3-PWR-USB-G4 USB dongle). For example, set up as KX3 <-> CAT5 cable <-> DKX3-PWR-USB-G4 <-> PX4 PDU USB-A or set up as KX3 <-> CAT5 cable <-> DKX3-PWR-USB-G4 <-> PRO4X PDU USB-A.
   - To connect a Raritan KX3 KVM Switch and DSAM module to one of the PDU's USB-A ports use a CAT5 cable and a Power CIM (DSER-CLI-USB-G4 dongle) For example, set up as KX3 <-> DSAM <-> CAT5 <-> DSER-CLI-USB-G4 <-> PX4 PDU USB-A or set up as KX3 <-> DSAM <-> CAT5 <-> DSER-CLI-USB-G4 <-> PRO4X PDU USB-A.
   - To connect a PC using a USB port requires a DSER-CLI-USB-G4 dongle, a USB-to-Serial adapter, and a Cisco cable. For example, set up as PC <-> USB-to-serial adapter <-> Cisco cable <-> DSER-CLI-USB-G4 <-> PX4 PDU USB-A or set up as PC <-> USB-to-serial adapter <-> Cisco cable <-> DSER-CLI-USB-G4 <-> PRO4X PDU USB-A.

► *Only for PX4*

- To connect a PC with a Serial port requires a DSER-CLI-USB-G4 dongle and a Cisco cable. For example, set up as PC serial port <-> Cisco cable <-> DSER-CLI-USB-G4 <-> PX4 PDU USB-A.
- To connect a Serial Console Server, such as the Raritan SX2 to one of the PX4's USB-A ports use a CAT5 cable and a DSER-PWR-USB-G4 USB dongle. For example, set up as Serial Console Server (such as the SX2) <-> CAT5 cable <-> DSER-PWR-USB-G4 <-> PX4 PDU USB-A.

► *Only for PRO4X*

- To access a serial device you can connect a Raritan DSAM Serial Access Module (DSAM) directly to the PRO4X PDU's USB-A port, and the serial device would then connect directly to an available RJ45 port on the DSAM module. NOTE: This functionality requires Xerus Firmware 4.0.20 or later.

1. Attach an AC power cord to the target server and an available the PDU outlet.
2. Connect the PDU to an AC power source.
3. Power on the device.

Power IQ Configuration

Sunbird's Power IQ is a software application that collects and manages the data from different PDUs installed in your server room or data center. With this software, you can:

- Do bulk configuration for multiple PDUs
- Name outlets on different PDUs
- Switch on/off outlets on outlet-switching capable PDUs

For more information on Power IQ, refer to the Power IQ online help on the Sunbird website: *http://support.sunbirddcim.com.*

Connecting a Modbus RTU Device or Bus

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

► *To use the Modbus Gateway feature:*

1. Connect a Modbus RTU device, or a Modbus bus with multiple RTU devices, to the Xerus PDU via two adapters described below.

a. Connect an isolated RS485-to-RS232 adapter to the Modbus RTU device or Modbus bus.
b. Connect an RS232-to-USB adapter (using FTDI's FT232 chip) to the RS485-to-RS232 adapter.
c. Connect the RS232-to-USB adapter to the USB-A port on the Xerus PDU.

2. On the Xerus PDU, enable and properly configure the Modbus Gateway feature. See Changing Modbus Settings.

► *Communications between Modbus TCP and RTU devices:*

- The Xerus PDU acts only as a message gateway for the Modbus TCP client.

  Messages from the Modbus TCP client(s) are passed through the Xerus PDU to the connected Modbus RTU devices or Modbus bus.
- The Modbus RTU devices on the bus are identified with their Modbus RTU addresses using the Modbus unit identifier addresses in the Modbus TCP protocol.

  If the Modbus TCP client does not support unit identifier addressing, refer to Changing Modbus Settings.
- The Xerus PDU supports communications to multiple Modbus RTU devices. Note that the connected Modbus RTU devices are invisible to the Xerus PDU.

dcTrack

Sunbird's dcTrack® is a product that allows you to manage the data center. The PX4 is categorized as a power item in dcTrack.

You can use dcTrack to:

- Record and manage the data center infrastructure and assets
- Monitor the electrical consumption of the data center
- Track environmental factors in the data center, such as temperature and humidity
- Optimize the data center growth

For more information on dcTrack, refer to the online help accessible from the dcTrack application, or user documentation available on the Sunbird's website: *http://support.sunbirddcim.com*.

Asset Management Strips and dcTrack

If any asset strips are connected to the PX4, the PX4 can transmit their information to Sunbird's dcTrack. Add the PX4 to dcTrack, and also add each IT item where an asset tag is attached to dcTrack.

If SNMP is enabled, event information can be transmitted to dcTrack. Specifically, Sunbird's Power IQ detects when an asset tag is connected or disconnected from an asset strip. Power IQ then generates a connection or disconnection event. When dcTrack polls Power IQ, the connection/disconnection events are pulled into dcTrack, and displayed in the dcTrack Web Client.

► *To poll and display asset management events in dcTrack*

- The PX4 that the asset strip is connected to must exist in dcTrack.
- Each IT item connected to the asset strip via an asset tag must exist in dcTrack.

  You do not need to manually enter the asset tag IDs for IT items that already exist in dcTrack as long as these items are in the Installed status.

Plug the item's asset tag into an asset strip that is connected to the PX4 that exists in dcTrack. dcTrack automatically assigns the asset tag ID to the existing IT item.

Third Party Licenses

This appendix contains third party licenses for software used by Xerus that require including the license in documentation.

For information on open source software, see: https://www.raritan.com/about-us/legal/open-source-software-statement

In This Chapter

Licenses - Angular. 727
Licenses - Bind9. 736
Licenses - Clish. 742
Licenses - Dropbear. 747
Licenses - FreeType. 749
Licenses - IW. 751
Licenses - JSON-C. 751
Licenses - LIBTIRPC. 752
Licenses - LIBXML2. 752
Licenses - Mbus. 752
Licenses - Net-SNMP. 753
Licenses - Open LDAP. 758
Licenses - OpenSSL. 760
Licenses - Wireless-RegDB. 761
Licenses - WPA Supplicant and Hostapd. 761

Licenses - Angular

@angular-devkit/build-angular

MIT

The MIT License

Copyright (c) 2017 Google, Inc.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

@angular-devkit/core

MIT

The MIT License

Copyright (c) 2017 Google, Inc.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

@angular/animations

MIT

@angular/cdk

MIT

The MIT License

Copyright (c) 2021 Google LLC.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

@angular/common

MIT

@angular/core

MIT

@angular/forms

MIT

@angular/material

MIT

The MIT License

Copyright (c) 2021 Google LLC.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

@angular/platform-browser

MIT

@angular/router

MIT

@babel/runtime

MIT

MIT License

Copyright (c) 2014-present Sebastian McKenzie and other contributors Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

@ctrl/ngx-chartjs

MIT

MIT License

Copyright (c) Scott Cooper <scttcper@gmail.com>

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

@ngx-translate/core

MIT

chart.js

MIT

The MIT License (MIT)

Copyright (c) 2018 Chart.js Contributors

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

core-js

MIT

Copyright (c) 2014-2021 Denis Pushkarev

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

regenerator-runtime

MIT

MIT License

Copyright (c) 2014-present, Facebook, Inc.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

rxjs

Apache-2.0

Apache License

Version 2.0, January 2004

http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual,

worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made,

use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable

by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and

do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions.

Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other

Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright (c) 2015-2018 Google, Inc., Netflix, Inc., Microsoft Corp. and contributors

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License.

You may obtain a copy of the License at http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.

See the License for the specific language governing permissions and limitations under the License.

tslib

0BSD

Copyright (c) Microsoft Corporation.

Permission to use, copy, modify, and/or distribute this software for any purpose with or without fee is hereby granted.

THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

zone.js

MIT

The MIT License

Copyright (c) 2010-2020 Google LLC. https://angular.io/license

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Licenses - Bind9

Copyright (C) 2004-2016 Internet Systems Consortium, Inc. ("ISC")

Copyright (C) 1996-2003 Internet Software Consortium.

Permission to use, copy, modify, and/or distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Portions of this code release fall under one or more of the following Copyright notices. Please see individual source files for details.

For binary releases also see: OpenSSL-LICENSE.

Copyright (C) 1996-2001 Nominum, Inc.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND NOMINUM DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL NOMINUM BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Copyright (C) 1995-2000 by Network Associates, Inc.

Permission to use, copy, modify, and/or distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC AND NETWORK ASSOCIATES DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Copyright (C) 2002 Stichting NLnet, Netherlands, stichting@nlnet.nl.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND STICHTING NLNET DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL STICHTING NLNET BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

The development of Dynamically Loadable Zones (DLZ) for Bind 9 was conceived and contributed by Rob Butler.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ROB BUTLER DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL ROB BUTLER BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Copyright (c) 1987, 1990, 1993, 1994

The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (C) The Internet Society 2005. This version of this module is part of RFC 4178; see the RFC itself for full legal notices.

(The above copyright notice is per RFC 3978 5.6 (a), q.v.)

Copyright (c) 2004 Masarykova universita

(Masaryk University, Brno, Czech Republic)

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (c) 1997 - 2003 Kungliga Tekniska Hogskolan

(Royal Institute of Technology, Stockholm, Sweden).

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of the Institute nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE INSTITUTE AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE INSTITUTE OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (c) 1998 Doug Rabson

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright ((c)) 2002, Rice University

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of Rice University (RICE) nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

This software is provided by RICE and the contributors on an "as is" basis, without any representations or warranties of any kind, express or implied including, but not limited to, representations or warranties of non-infringement, merchantability or fitness for a particular purpose. In no event shall RICE or contributors be liable for any direct, indirect, incidental, special, exemplary, or consequential damages (including, but not limited to, procurement of substitute goods or services; loss of use, data, or profits; or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of this software, even if advised of the possibility of such damage.

Copyright (c) 1993 by Digital Equipment Corporation.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies, and that the name of Digital Equipment Corporation not be used in advertising or publicity pertaining to distribution of the document or software without specific, written prior permission.

THE SOFTWARE IS PROVIDED "AS IS" AND DIGITAL EQUIPMENT CORP. DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL DIGITAL EQUIPMENT CORPORATION BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Copyright 2000 Aaron D. Gifford. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of the copyright holder nor the names of contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR(S) AND CONTRIBUTOR(S) ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR(S) OR CONTRIBUTOR(S) BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (c) 1998 Doug Rabson.

Copyright (c) 2001 Jake Burkholder.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (C) 1995, 1996, 1997, and 1998 WIDE Project.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of the project nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE PROJECT AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE PROJECT OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (c) 1999-2000 by Nortel Networks Corporation

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND NORTEL NETWORKS DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL NORTEL NETWORKS BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Copyright (c) 2000-2002 Japan Network Information Center. All rights reserved.

By using this file, you agree to the terms and conditions set forth bellow.

LICENSE TERMS AND CONDITIONS

The following License Terms and Conditions apply, unless a different license is obtained from Japan Network Information Center ("JPNIC"), a Japanese association, Kokusai-Kougyou-Kanda Bldg 6F, 2-3-4 Uchi-Kanda, Chiyoda-ku, Tokyo 101-0047, Japan.

1. Use, Modification and Redistribution (including distribution of any modified or derived work) in source and/or binary forms is permitted under this License Terms and Conditions.

2. Redistribution of source code must retain the copyright notices as they appear in each source code file, this License Terms and Conditions.

3. Redistribution in binary form must reproduce the Copyright Notice, this License Terms and Conditions, in the documentation and/or other materials provided with the distribution. For the purposes of binary distribution the "Copyright Notice" refers to the following language:

"Copyright (c) 2000-2002 Japan Network Information Center. All rights reserved."

4. The name of JPNIC may not be used to endorse or promote products derived from this Software without specific prior written approval of JPNIC.

5. Disclaimer/Limitation of Liability: THIS SOFTWARE IS PROVIDED BY JPNIC "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL JPNIC BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Copyright (C) 2004 Nominet, Ltd.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND NOMINET DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Portions Copyright RSA Security Inc.

License to copy and use this software is granted provided that it is identified as "RSA Security Inc. PKCS #11 Cryptographic Token Interface (Cryptoki)" in all material mentioning or referencing this software.

License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Security Inc. PKCS #11 Cryptographic Token Interface (Cryptoki)" in all material mentioning or referencing the derived work.

RSA Security Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

Copyright (c) 1996, David Mazieres <dm@uun.org>

Copyright (c) 2008, Damien Miller <djm@openbsd.org>

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Copyright (c) 2000-2001 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.OpenSSL.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact licensing@OpenSSL.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.OpenSSL.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (c) 1995, 1997, 1998 The NetBSD Foundation, Inc.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE NETBSD FOUNDATION, INC. AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE FOUNDATION OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Licenses - Clish

This package contains code which is copyrighted to multiple sources. The initial public release of this software was developed by Graeme McKerrell whilst in the employment of 3Com Europe Ltd.

Copyright (c) 2005, 3Com Corporation

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of 3Com Corporation nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Newport Networks Ltd.

The 0.6-0.7 releases of this software was developed by Graeme McKerrell whilst in the employment of Newport Networks Ltd.

As well as enhancing the existing code the following new modules were developed.

Copyright (c) 2005,2006, Newport Networks Ltd

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of Newport Networks Ltd nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

tinyxml

Yves Berquin

As of release 0.6 the tinyxml library is included (unchanged) as part of the distribution.

tinyxml (v2.5.1)

http://www.sourceforge.net/projects/tinyxml

Original file by Yves Berquin.

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

GNU binutils

As of release 0.7.1 libbfd can be used to resolve symbols forstacktraces. This feature can be turned off if linking with GPL code is problematic, using "configure --without-gpl".

The Binary File Descriptor library is part of GNU binutils

http://www.gnu.org/software/binutils/

The following file is licensed under the GPLv2.

This file is part of the CLISH project http://clish.sourceforge.net/

The code in this file is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; version 2

This code is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA.

Derived from addr2line.c in the GNU binutils package by Ulrich.Lauther@mchp.siemens.de

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or, b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or, c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Licenses - Dropbear

Dropbear contains a number of components from different sources, hence there are a few licenses and authors involved. All licenses are fairly non-restrictive.

The majority of code is written by Matt Johnston, under the license below.

Portions of the client-mode work are (c) 2004 Mihnea Stoenescu, under the same license:

Copyright (c) 2002-2015 Matt Johnston

Portions copyright (c) 2004 Mihnea Stoenescu

All rights reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

=====

LibTomCrypt and LibTomMath are written by Tom St Denis, and are Public Domain.

=====

sshpty.c is taken from OpenSSH 3.5p1,

Copyright (c) 1995 Tatu Ylonen <ylo@cs.hut.fi>, Espoo, Finland

All rights reserved

"As far as I am concerned, the code I have written for this software can be used freely for any purpose. Any derived versions of this software must be clearly marked as such, and if the derived work is incompatible with the protocol description in the RFC file, it must be called by a name other than "ssh" or "Secure Shell". "

=====

loginrec.c

loginrec.h

atomicio.h

atomicio.c

and strlcat() (included in util.c) are from OpenSSH 3.6.1p2, and are licensed under the 2 point BSD license.

loginrec is written primarily by Andre Lucas, atomicio.c by Theo de Raadt.

strlcat() is (c) Todd C. Miller

=====

Import code in keyimport.c is modified from PuTTY's import.c, licensed as follows:

PuTTY is copyright 1997-2003 Simon Tatham.

Portions copyright Robert de Bath, Joris van Rantwijk, Delian Delchev, Andreas Schultz, Jeroen Massar, Wez Furlong, Nicolas Barry, Justin Bradford, and CORE SDI S.A.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

=====

curve25519-donna:

/* Copyright 2008, Google Inc.

* All rights reserved.

*

* Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

*

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of Google Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

* curve25519-donna: Curve25519 elliptic curve, public key function

* http://code.google.com/p/curve25519-donna/

* Adam Langley <agl@imperialviolet.org>

* Derived from public domain C code by Daniel J. Bernstein <djb@cr.yp.to>

* More information about curve25519 can be found here

* http://cr.yp.to/ecdh.html

* djb's sample implementation of curve25519 is written in a special assembly language called qhasm and uses the floating point registers.

* This is, almost, a clean room reimplementation from the curve25519 paper. It uses many of the tricks described therein. Only the crecip function is taken from the sample implementation.

Licenses - FreeType

The FreeType Project LICENSE

2006-Jan-27

Copyright 1996-2002, 2006 by

David Turner, Robert Wilhelm, and Werner Lemberg

Introduction

==========

The FreeType Project is distributed in several archive packages; some of them may contain, in addition to the FreeType font engine, various tools and contributions which rely on, or relate to, the FreeType Project.

This license applies to all files found in such packages, and which do not fall under their own explicit license. The license affects thus the FreeType font engine, the test programs, documentation and makefiles, at the very least.

This license was inspired by the BSD, Artistic, and IJG (Independent JPEG Group) licenses, which all encourage inclusion and use of free software in commercial and freeware products alike. As a consequence, its main points are that:

o We don't promise that this software works. However, we will be interested in any kind of bug reports. (`as is' distribution)

o You can use this software for whatever you want, in parts or full form, without having to pay us. (`royalty-free' usage)

o You may not pretend that you wrote this software. If you use it, or only parts of it, in a program, you must acknowledge somewhere in your documentation that you have used the FreeType code. (`credits')

We specifically permit and encourage the inclusion of this software, with or without modifications, in commercial products.

We disclaim all warranties covering The FreeType Project and assume no liability related to The FreeType Project.

Finally, many people asked us for a preferred form for a credit/disclaimer to use in compliance with this license. We thus encourage you to use the following text:

Portions of this software are copyright <year> The FreeType Project (www.freetype.org). All rights reserved.

Please replace <year> with the value from the FreeType version you actually use.

Legal Terms

==========

0. Definitions

Throughout this license, the terms `package', `FreeType Project', and `FreeType archive' refer to the set of files originally distributed by the authors (David Turner, Robert Wilhelm, and Werner Lemberg) as the `FreeType Project', be they named as alpha, beta or final release.

`You' refers to the licensee, or person using the project, where `using' is a generic term including compiling the project's source code as well as linking it to form a `program' or `executable'.

This program is referred to as `a program using the FreeType engine'.

This license applies to all files distributed in the original FreeType Project, including all source code, binaries and documentation, unless otherwise stated in the file in its original, unmodified form as distributed in the original archive.

If you are unsure whether or not a particular file is covered by this license, you must contact us to verify this.

The FreeType Project is copyright (C) 1996-2000 by David Turner, Robert Wilhelm, and Werner Lemberg. All rights reserved except as specified below.

1. No Warranty

THE FREETYPE PROJECT IS PROVIDED `AS IS' WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT WILL ANY OF THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY DAMAGES CAUSED BY THE USE OR THE INABILITY TO USE, OF THE FREETYPE PROJECT.

2. Redistribution

This license grants a worldwide, royalty-free, perpetual and irrevocable right and license to use, execute, perform, compile, display, copy, create derivative works of, distribute and sublicense the FreeType Project (in both source and object code forms) and derivative works thereof for any purpose; and to authorize others to exercise some or all of the rights granted herein, subject to the following conditions:

o Redistribution of source code must retain this license file (`FTL.TXT') unaltered; any additions, deletions or changes to the original files must be clearly indicated in accompanying documentation. The copyright notices of the unaltered, original files must be preserved in all copies of source files.

o Redistribution in binary form must provide a disclaimer that states that the software is based in part of the work of the FreeType Team, in the distribution documentation. We also encourage you to put an URL to the FreeType web page in your documentation, though this isn't mandatory.

These conditions apply to any software derived from or based on the FreeType Project, not just the unmodified files. If you use our work, you must acknowledge us. However, no fee need be paid to us.

3. Advertising

Neither the FreeType authors and contributors nor you shall use the name of the other for commercial, advertising, or promotional purposes without specific prior written permission.

We suggest, but do not require, that you use one or more of the following phrases to refer to this software in your documentation or advertising materials: `FreeType Project', `FreeType Engine', `FreeType library', or `FreeType Distribution'.

As you have not signed this license, you are not required to accept it. However, as the FreeType Project is copyrighted material, only this license, or another one contracted with the

authors, grants you the right to use, distribute, and modify it. Therefore, by using, distributing, or modifying the FreeType Project, you indicate that you understand and accept all the terms of this license.

4. Contacts

There are two mailing lists related to FreeType:

o freetype@nongnu.org

Discusses general use and applications of FreeType, as well as future and wanted additions to the library and distribution. If you are looking for support, start in this list if you haven't found anything to help you in the documentation.

o freetype-devel@nongnu.org

Discusses bugs, as well as engine internals, design issues, specific licenses, porting, etc.

Our home page can be found at http://www.freetype.org

Licenses - IW

Copyright (c) 2007, 2008 Johannes Berg

Copyright (c) 2007 Andy Lutomirski

Copyright (c) 2007 Mike Kershaw

Copyright (c) 2008-2009 Luis R. Rodriguez

Permission to use, copy, modify, and/or distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Licenses - JSON-C

Copyright (c) 2009-2012 Eric Haszlakiewicz

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Copyright (c) 2004, 2005 Metaparadigm Pte Ltd

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Licenses - LIBTIRPC

Copyright (c) Copyright (c) Bull S.A. 2005 All Rights Reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Licenses - LIBXML2

Except where otherwise noted in the source code (e.g. the files hash.c, list.c and the trio files, which are covered by a similar licence but with different Copyright notices) all the files are:

Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Licenses - Mbus

Copyright (c) 2002-2003, 2013-2019 Victor Antonovich (v.antonovich@gmail.com)

Copyright (c) 2011 Andrew Denysenko <nitr0@seti.kr.ua>

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of the copyright holder nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Licenses - Net-SNMP

Various copyrights apply to this package, listed in various separate parts below. Please make sure that you read all the parts.

Part 1: CMU/UCD copyright notice: (BSD like) -----

Copyright 1989, 1991, 1992 by Carnegie Mellon University

Derivative Work - 1996, 1998-2000

Copyright 1996, 1998-2000 The Regents of the University of California

All Rights Reserved

Permission to use, copy, modify and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU and The Regents of the University of California not be used in advertising or publicity pertaining to distribution of the software without specific written permission.

CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CMU OR THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM THE LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Part 2: Networks Associates Technology, Inc copyright notice (BSD) -----

Copyright (c) 2001-2003, Networks Associates Technology, Inc

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of the Networks Associates Technology, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 3: Cambridge Broadband Ltd. copyright notice (BSD) -----

Portions of this code are copyright (c) 2001-2003, Cambridge Broadband Ltd.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

The name of Cambridge Broadband Ltd. may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 4: Sun Microsystems, Inc. copyright notice (BSD) -----

Copyright (c) 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.

Use is subject to license terms below.

This distribution may include materials developed by third parties.

Sun, Sun Microsystems, the Sun logo and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of the Sun Microsystems, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 5: Sparta, Inc copyright notice (BSD) -----

Copyright (c) 2003-2013, Sparta, Inc

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of Sparta, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 6: Cisco/BUPTNIC copyright notice (BSD) -----

Copyright (c) 2004, Cisco, Inc and Information Network

Center of Beijing University of Posts and Telecommunications.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of Cisco, Inc, Beijing University of Posts and Telecommunications, nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS;OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 7: Fabasoft R&D Software GmbH & Co KG copyright notice (BSD) -----

Copyright (c) Fabasoft R&D Software GmbH & Co KG, 2003

oss@fabasoft.com

Author: Bernhard Penz <bernhard.penz@fabasoft.com>

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

The name of Fabasoft R&D Software GmbH & Co KG or any of its subsidiaries, brand or product names may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS

INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 8: Apple Inc. copyright notice (BSD) -----

Copyright (c) 2007 Apple Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of Apple Inc. ("Apple") nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY APPLE AND ITS CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL APPLE OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 9: ScienceLogic, LLC copyright notice (BSD) -----

Copyright (c) 2009, ScienceLogic, LLC

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of ScienceLogic, LLC nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 10: Lennart Poettering copyright notice (BSD-like) -----

Copyright 2010 Lennart Poettering

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Part 11: IETF copyright notice (BSD) -----

Copyright (c) 2013 IETF Trust and the persons identified as authors of the code. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. Neither the name of Internet Society, IETF or IETF Trust, nor the names of specific contributors, may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 12: Arista Networks copyright notice (BSD) ----

Copyright (c) 2013, Arista Networks, Inc.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of Arista Networks, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 13: VMware, Inc. copyright notice (BSD) -----

Copyright (c) 2016, VMware, Inc.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of VMware, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR

OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 14: USC/Information Sciences Institute copyright notice (BSD) -----

Copyright (c) 2017-2018, Information Sciences Institute

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of Information Sciences Institue nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Licenses - Open LDAP

Copyright 1998-2019 The OpenLDAP Foundation

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted only as authorized by the OpenLDAP Public License.

A copy of this license is available in the file LICENSE in the top-level directory of the distribution or, alternatively, at <http://www.OpenLDAP.org/license.html>.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

Individual files and/or contributed packages may be copyright by other parties and/or subject to additional restrictions.

This work is derived from the University of Michigan LDAP v3.3 distribution. Information concerning this software is available at <http://www.umich.edu/~dirsvcs/ldap/ldap.html>.

This work also contains materials derived from public sources. Additional information about OpenLDAP can be obtained at <http://www.openldap.org/>.

Portions Copyright 1998-2012 Kurt D. Zeilenga.

Portions Copyright 1998-2006 Net Boolean Incorporated.

Portions Copyright 2001-2006 IBM Corporation.

All rights reserved.

Redistribution and use in source and binary forms, with or without

modification, are permitted only as authorized by the OpenLDAP

Public License.

Portions Copyright 1999-2008 Howard Y.H. Chu.

Portions Copyright 1999-2008 Symas Corporation.

Portions Copyright 1998-2003 Hallvard B. Furuseth.

Portions Copyright 2007-2011 Gavin Henry.

Portions Copyright 2007-2011 Suretec Systems Ltd.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that this notice is preserved. The names of the copyright holders may not be used to endorse or promote products derived from this software without their specific prior written permission. This software is provided "as is'' without express or implied warranty.

Portions Copyright (c) 1992-1996 Regents of the University of Michigan.

All rights reserved.

Redistribution and use in source and binary forms are permitted provided that this notice is preserved and that due credit is given to the University of Michigan at Ann Arbor. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission. This software is provided ``as is'' without express or implied warranty.

The OpenLDAP Public License

Version 2.8, 17 August 2003

Redistribution and use of this software and associated documentation ("Software"), with or without modification, are permitted provided that the following conditions are met:

1. Redistributions in source form must retain copyright statements and notices,

2. Redistributions in binary form must reproduce applicable copyright statements and notices, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution, and

3. Redistributions must contain a verbatim copy of this document.

The OpenLDAP Foundation may revise this license from time to time. Each revision is distinguished by a version number. You may use this Software under terms of this license revision or under the terms of any subsequent revision of the license.

THIS SOFTWARE IS PROVIDED BY THE OPENLDAP FOUNDATION AND ITS CONTRIBUTORS ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OPENLDAP FOUNDATION, ITS CONTRIBUTORS, OR THE AUTHOR(S) OR OWNER(S) OF THE SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The names of the authors and copyright holders must not be used in advertising or otherwise to promote the sale, use or other dealing in this Software without specific, written prior permission. Title to copyright in this Software shall at all times remain with copyright holders.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

Copyright 1999-2003 The OpenLDAP Foundation, Redwood City, California, USA. All Rights Reserved. Permission to copy and distribute verbatim copies of this document is granted.

Licenses - OpenSSL

LICENSE ISSUES

The OpenSSL toolkit stays under a double license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts.

OpenSSL License

Copyright (c) 1998-2019 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

==========

This product includes cryptographic software written by Eric Young

(eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.

If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used.

This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public License.]

Licenses - Wireless-RegDB

Copyright (c) 2008, Luis R. Rodriguez <mcgrof@gmail.com>

Copyright (c) 2008, Johannes Berg <johannes@sipsolutions.net>

Copyright (c) 2008, Michael Green <Michael.Green@Atheros.com>

Permission to use, copy, modify, and/or distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Licenses - WPA Supplicant and Hostapd

Copyright (c) 2002-2019, Jouni Malinen <j@w1.fi> and contributors

All Rights Reserved.

These programs are licensed under the BSD license (the one with advertisement clause removed).

If you are submitting changes to the project, please see CONTRIBUTIONS file for more instructions.

This package may include either wpa_supplicant, hostapd, or both. See README file respective subdirectories (wpa_supplicant/README or hostapd/README) for more details.

Source code files were moved around in v0.6.x releases and compared to earlier releases, the programs are now built by first going to a subdirectory (wpa_supplicant or hostapd) and creating build configuration (.config) and running 'make' there (for Linux/BSD/cygwin builds).

License

This software may be distributed, used, and modified under the terms of BSD license:

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name(s) of the above-listed copyright holder(s) nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Index

"

"To Assert" and Assertion Timeout 706

"To De-assert" and Deassertion Hysteresis 708

0

0U Button Mount 22

1

1U Products 19

2

2U Products 20

8

802.1x Security Overview 234

A

A Note about Firmware Upgrade Time 372

A Note about Infinite Loop 342

A Note about Untriggered Rules 343

About the Link ID 46

Accessing Cascaded Devices 637

Action Group 318

Actuator Configuration Commands 441

Actuator Control Operations 442

Actuator Information 412

Adding a Firewall Rule 517

Adding a Link Unit 45

Adding a Monitored Device 535

Adding a Radius Server 451

Adding a Role-Based Access Control Rule 529

Adding an LDAP Server 445

Adding Attributes to the Class 699

Adding LDAP/LDAPS Servers 276

Adding Radius Servers 279

Adding TACACS+ Server 454

Adding TACACS+ Servers 280

Adding, Removing or Swapping Cascaded Devices 254, 635

Additional sensors supported by PX4 543

Additional Xerus Information - Assorted Products 702

AD-Related Configuration 686

Alarm 317

Alerts 77

Alerts Notice in a Yellow or Red Screen 106

All Privileges 511

Altitude Correction Factors 712

APIPA and Link-Local Addressing 21

Appendices 568

Applicable Products 616

Assertion Timeout Example for Temperature Sensors 708

Asset Management Strips and dcTrack 725

Asset Management Tag List 350

Asset Management Tag Log 351

Asset Strip Automatic Firmware Upgrade 214

Asset Strip Settings 412

Asset Strips 206

Authentication Commands 443

Authentication Settings 413

Automatic and Manual Modes 74

Automatic Management of Sensors 198

Automatically Completing a Command 409

Automatically Create Pairwise Outlet Groups 59

Available Actions 315

Available Data of the Outlets Overview Page 158

B

Backup and Restore of Device Settings 377

Backup and Restore via SCP 609

Beeper 117

Before You Begin 20

Best Practices for Cascading 35, 619

Blade Slot 414

Built-in Rules and Rule Configuration 292

Bulk Configuration 372

Bulk Configuration Methods 33
Bulk Configuration or Firmware Upgrade via DHCP (TFTP/HTTPS) 585
Bulk Configuration Restrictions 373
Bulk Configuration via SCP 608
Bulk Configuration, Firmware Upgrade, or Backup/Restore via SCP 607
Bulk Configuration/Upgrade Procedure 586

C

Canceling the Power-On Process 507
Card Readers 396
Cascade Troubleshooting 651
Cascading All Devices via USB-Only 628
Cascading Devices via Dual Ethernet and USB 630
Cascading for Shared Ethernet Connectivity 34
Cascading Modes Overview 248, 621
Cascading Procedure Overview 621
Cascading Restrictions 633
Cascading Solution Overview 616
Cascading Solutions for Xerus 616
Change Load Shedding State 318
Changing a User's Password 556
Changing an Outlet's Default State 498
Changing HTTP(S) Settings 256
Changing Measurement Units 561
Changing Modbus Settings 261
Changing SSH Settings 261
Changing Storage Settings 388
Changing Telnet Settings 261
Changing the Device Name 459
Changing the Inlet Name 467
Changing the LAN Duplex Mode 479
Changing the LAN Interface Speed 478
Changing the Modbus Configuration 496
Changing the Outlet Name 498
Changing the Overcurrent Protector Name 502
Changing the Role(s) 560
Changing the Sensor Description 465
Changing the Sensor Name 464
Changing the SSH Configuration 492
Changing the Telnet Configuration 492
Changing Your Own Password 563
Changing Your Password 121
Character LCD Display 649
Checking Lua Scripts States 362
Checking RCM State and Current 660
Checking RCM States and Current 666
Checking the Accessibility of NTP Servers 554
Checking the Branch Circuit Rating 20
Circuit Breaker Orientation Limitation 22
Circuit Breakers 111
Cisco ISE Xerus TACACS+ Authentication 689
Clearing Diagnostic Log for Network Connections 415
Clearing Event Log 415
Clearing Information 415
CLI Operations for RCM 668
Closing a Local Connection 407
Collected Data 365
Command History 415
Commands for Environmental Sensors 550
Commands for Inlet Line Sensors 546
Commands for Inlet Pole Sensors 544
Commands for Inlet Sensors 541
Commands for Outlet Group Sensors 540
Commands for Outlet Sensors 538
Commands for Overcurrent Protector Sensors 548
Common Network Settings 233
Compliance with IEC 62020 658
config.txt 578
Configuration Files 574
Configuration Files for Linking 581
Configuration Files for Linking: Port-Forwarding Cascade Example 582
Configuration or Firmware Upgrade with a USB Drive 573
Configure DSAM Serial Ports 217
Configuring a Multi-Inlet Model 153
Configuring Data Push Settings 346
Configuring DNS Parameters 476
Configuring Environmental Sensors' Default Thresholds 457
Configuring IPv4 Parameters 469

Configuring IPv6 Parameters 472
Configuring Login Settings 284
Configuring Network Services 255
Configuring NTP Server Settings 403
Configuring Password Policy 285
Configuring Security Settings 265
Configuring SMTP Settings 259
Configuring SNMP Settings 257
Configuring the Cascading Mode 489
Configuring the Device and Network 440
Configuring the PX4 26
Configuring the Serial Port 358
Configuring Webcams and Viewing Live Images 383
Connect to DSAM Serial Targets in the Web Interface 219
Connect to DSAM Serial Targets via SSH 221
Connecting a Mobile Device 26
Connecting a Modbus RTU Device or Bus 724
Connecting a PDU to a Dominion KVM or Serial Device 722
Connecting the PDU to a Power Source 24
Connecting to a Computer 32
Connecting to Your Network 24
Connection Port Functions 73
Connection Ports 72
Control Buttons 75
Controlling Outlets in Groups 64
Copying an Existing Authentication Server's Settings 448
Creating a New Attribute 698
Creating a Role 510
Creating a Self-Signed Certificate 273
Creating a TLS Certificate or CSR 270
Creating a User Profile 555
Creating an Outlet Group 176, 499
Creating Configuration Files via Mass Deployment Utility 582
Creating IP Access Control Rules 265
Creating Role Based Access Control Rules 268
Creating Roles 227
Creating Users 222
Curl Upload Return Codes 606
Customizing Bulk Configuration Profiles 374

D

Dashboard - Alarms 136
Dashboard - Alerted Sensors 134
Dashboard - Inlet History 135
Dashboard - Inlet I1 130
Dashboard - OCP 132
Dashboard - PDUs 129
Data Encryption in 'config.txt' 583
Data Push Format Examples 347
Date and Time Settings 416
dcTrack 725
Deassertion Hysteresis Example for Temperature Sensors 710
Default Measurement Units 416
Default Voltage and Current Thresholds 160, 711
Degaussing RCM Type B Sensors 669
Deleting a Firewall Rule 520
Deleting a Monitored Device 536
Deleting a Role 514
Deleting a Role-Based Access Control Rule 532
Deleting a User Profile 562
Deleting an Outlet Group 180
Detailed Information on Outlet Pages 172
Determining the Authentication Method 443
Device Configuration 416
Device Configuration Commands 459
Device Configuration/Upgrade Procedure 573
Device Info 102
Device Information 366
Device Information Page 60
Device Settings 232
Device-Cascading Methods 626
devices.csv 580
Device-Specific Settings 715
DHCP IPv4 Configuration in Linux 599
DHCP IPv4 Configuration in Windows 587
DHCP IPv6 Configuration in Linux 600
DHCP IPv6 Configuration in Windows 594
Diagnostic Log for Network Connections 243

Different CLI Modes and Prompts 407
Disabling or Enabling Front Panel RCM Self-Test 664
Displays for Primary and Link Units 67
Door Access 289
Door Status and Control 394
Dot-Matrix LCD Display 646
Download via Curl 603
Download via Web Browsers 602
Downloading Diagnostic Data via SCP 610
Downloading Diagnostic Information 378
Downloading SNMP MIB 401
DSAM CLI Commands 219
DSAM Connection 216
DSAM LED Operation 216
Dual Ethernet Connection 25

E

EAP CA Certificate Example 483
Editing or Deleting a Rule/Action 337
Editing or Deleting IP Access Control Rules 267
Editing or Deleting Ping Monitoring Settings 355
Editing or Deleting Role Based Access Control Rules 270
Editing or Deleting Roles 229
Editing or Deleting Users 226
Editing rciusergroup Attributes for User Members 700
Enabling and Configuring SNMP 398
Enabling or Disabling 802.11n High Throughput 485
Enabling or Disabling a User Profile 557
Enabling or Disabling an Inlet (for Multi-Inlet PDUs) 467
Enabling or Disabling data backup 463
Enabling or Disabling Data Logging 462
Enabling or Disabling Front Panel Actuator Control 533
Enabling or Disabling Front Panel Beeper-Sound Control 534
Enabling or Disabling Front Panel Outlet Switching 533
Enabling or Disabling Load Shedding 468
Enabling or Disabling Service Advertising 497
Enabling or Disabling Strong Passwords 525
Enabling or Disabling the LAN Interface 477
Enabling or Disabling the Restricted Service Agreement 521
Enabling Redfish Services 263
Enabling Service Advertising 264
Enabling the FIPS Mode 282
Enabling the Restricted Service Agreement 286
Environmental Sensor Configuration Commands 463
Environmental Sensor Default Thresholds 421
Environmental Sensor Information 420
Environmental Sensor Package Information 437
Environmental Sensor Threshold Information 417
Equipment Setup Worksheet Sample 570
Ethernet (Wired) Interface Settings 234
Event Log 418
Event Rules and Actions 291
Example - Actuator Naming 442
Example - Baud Rate 535
Example - Creating a Role 514
Example - Default Upper Thresholds for Temperature 458
Example - Inlet Naming 467
Example - OCP Naming 502
Example - Outlet Naming 499
Example - Ping Command 567
Example - Power Cycling Specific Outlets 507
Example - Server Settings Changed 538
Example - Turning On a Specific Actuator 443
Example -Time Configuration 555
Example: Ping Monitoring and SNMP Notifications 356, 567
Existing Roles 419
Existing User Profiles 419
Expansion Device Events in the Log 653
Extended Cascading for Dual Ethernet and USB 629
Extended-Cascading Requirements 630
External Beeper 319

F

Factory Default Login 655
Factory Default Settings 654
FAQs 41
Filling Out the Equipment Setup Worksheet 20
Finding the Sensor's Serial Number 196
FIPS 521
Firewall Control 515
Firmware Update via SCP 607
Firmware Upgrade for Cascading Chains 650
Firmware Upgrade via USB 584
Forcing a Password Change 557
Forcing the Device Detection Mode 534
FreeRADIUS Standard Attribute Illustration 676
FreeRADIUS VSA Illustration 685
From LDAP/LDAPS 696
From Microsoft Active Directory 696
Front Panel Display 73
Front Panel Operations for RCM 665
Front Panel Permissions 422
Front Panel Settings 357
Full Disaster Recovery 372
Fuse 113
Fuse Replacement on 1U Models 115
Fuse Replacement on Zero U Models 114
fwupdate.cfg 575

G

Group Peripheral Sensors 196

H

Hardware Issue Detection 379
How Long a Link Remains Accessible 387

I

Identifying Cascaded Devices 641
Identifying Snapshots Folders on Remote Servers 389
Identifying the Sensor Position and Channel 197
Idle Timeout 524
If Switchable Outlet Groups are Limited 178
Illustration 617
Illustration - GMAIL SMTP Certificate Chain 719
Illustrations of Adding LDAP Servers 447
Individual OCP Pages 182
Individual Outlet Pages 168
Individual Sensor/Actuator Pages 200
Initial Installation and Configuration 24
Initialization Delay Use Cases 144
Inlet 147, 71, 85
Inlet Configuration Commands 466
Inlet Information 423
Inlet Pole Sensor Threshold Information 425
Inlet Sensor Threshold Information 423
Inrush Current and Inrush Guard Delay 144
Installing a CA-Signed Certificate 272
Installing or Downloading Existing Certificate and Key 274
Installing the USB-to-Serial Driver (Optional) 714
Internal Beeper 319
Introduction to Xerus Technology Platform 13
IP Configuration 427
IPv4-Only or IPv6-Only Configuration 428
iX9 Controller Reset Button 656

K

Keys that Cannot Be Uploaded 614

L

Latching Relay Behavior 142
LCD Message for RCM Critical State 666
LDAP Configuration Illustration 670
LDAP Settings 444
Licenses - Angular 727
Licenses - Bind9 736
Licenses - Clish 742
Licenses - Dropbear 747
Licenses - FreeType 749
Licenses - IW 751
Licenses - JSON-C 751
Licenses - LIBTIRPC 752
Licenses - LIBXML2 752
Licenses - Mbus 752
Licenses - Net-SNMP 753

Licenses - Open LDAP 758
Licenses - OpenSSL 760
Licenses - Wireless-RegDB 761
Licenses - WPA Supplicant and Hostapd 761
Linking 427
Linking Cascaded Units 47
Linking CLI Commands 69
Linking in the CLI 68
Linking in the Web Interface 44
Linking Units 40
Load Shedding Configuration Commands 468
Load Shedding Mode: Activate or Deactivate 165
Load Shedding Settings 427
Load Shedding Setup: Setting Non-Critical Outlets 164
Log an Event Message 319
Log Rows 348
Logging in to CLI 405
Logging out of CLI 407
Login and Logout 120
Login Limitation 523
Login, Logout and Password Change 120
Lowercase Character Requirement 526
Lua Scripts 359

M

Main Menu 76
Maintenance 366
Managed vs Unmanaged Sensors/Actuators 194
Managing an Outlet Group 500
Managing Firewall Rules 517
Managing One Sensor or Actuator 198
Managing Role-Based Access Control Rules 529
Manually Changing Zero U LCD Orientation 110
Manually Starting or Stopping a Script 361
Maximum Password History 527
Maximum Password Length 525
Menu 124
Minimum and Maximum Values for Numeric Sensors 125
Minimum Password Length 525
Miscellaneous 363
Models with Residual Current Monitoring 657
Modifying a Firewall Rule 519
Modifying a Monitored Device's Settings 536
Modifying a Role 513
Modifying a Role-Based Access Control Rule 531
Modifying a User Profile 556
Modifying a User's Personal Data 556
Modifying an Existing LDAP Server 448
Modifying an Existing Radius Server 452
Modifying an Existing TACACS+ Server 455
Modifying an Outlet Group 179
Modifying Firewall Control Parameters 515
Modifying or Deleting a Script 363
Modifying or Deleting Bulk Configuration Profiles 376
Modifying Role-Based Access Control Parameters 528
Modifying SNMPv3 Settings 558
Monitoring Server Accessibility 351
Multi-Command Syntax 410

N

Network Configuration 427
Network Configuration Commands 469
Network Connections Diagnostic Log 431
Network Diagnostics 378, 427, 429
Network Interface Settings 430
Network Service Settings 430
Network Settings 232
Network Troubleshooting in Diagnostic Mode 565
NPS VSA Illustration 677
Numeric Character Requirement 526

O

OCP Trip-Cause Detection 185
OCP Trip-Cause Waveform 187
OCPs 180, 89
OCPs Page 60
Off and Lock Icons for Outlets 167
Operating the Front Panel Display 75
Optional Parameters 446
Options for Adding Link Units 45

Options for Outlet State on Power Up 143
Outlet Configuration Commands 498
Outlet Group Configuration Commands 499
Outlet Group Information 431
Outlet Group Power Control 177
Outlet Group Threshold Information 435
Outlet Groups 175, 62
Outlet Information 432
Outlet Pole Sensor Threshold Information 434
Outlet Sensor Threshold Information 435
Outlets 155, 89
Outlets and Outlet LEDs 71
Outlets detail 571
Overcurrent Protector Configuration Commands 502
Overcurrent Protector Information 433
Overcurrent Protector Sensor Threshold Information 436

P

Package Contents 19
Pairwise Outlet Groups 58
Password Aging 523
Password Aging Interval 524
PDU 138, 79
PDU Linking at the Rack 65
Performing Bulk Configuration 375
Peripheral Devices Configuration Commands 502
Peripheral Devices Settings 437
Peripherals 188, 97
Peripherals Page 60
Placeholders for Custom Messages 333
Port Forwarding Examples 252, 639
Port Number Syntax 250, 637
Port Numbers for Port-Forwarding Devices 637
Port Overload - Reset Fuse 109
Power Control Operations 504
Power Cycling the Outlet(s) 506
Power IQ Configuration 724
Power Sharing Limitations on Mobile Devices 39
Power Sharing Port on iX9 Controllers 37
Power Supply Sensor 146
Powering On/Off/Cycle Outlet Groups 501
Power-Off Period Options for Individual Outlets 174
Power-Sharing Configurations and Restrictions 37
Power-Sharing Restrictions and Connection 36
Preparing the Installation Site 20
Primary Units Manage Link Units 52
Push Out Sensor Readings 320
PX4 Series Connection Ports 72
PX4 Series Outlets and LEDs 71
PX4-Series Specifications 569

Q

Querying Available Parameters for a Command 408
Querying DNS Servers 565
Quick Access to a Specific Page 125

R

Rack Unit Settings of an Asset Strip 438
Rackmount Safety Guidelines 22
Rackmounts 22
RADIUS Configuration Illustration 675
Radius Settings 451
Raw Configuration Upload and Download 602
RCM Critical State Alarm 661
RCM Current Sensor 657
RCM Residual Current and State Objects 668
RCM Self-Test 659
RCM SNMP Operations 668
RCM State Sensor 657
RCM Trap 668
Rebooting 380
Record Snapshots to Webcam Storage 321
Regaining Access with HSTS and Expired Certificate 256
Releasing a Link Unit 52
Reliability Data 438
Reliability Error Log 438
Reliability Hardware Failures 439
Re-linking a Link Unit 54
Remote Authentication Examples 670

Removing an Existing LDAP Server 451
Removing an Existing Radius Server 453
Removing an Existing TACACS+ Server 456
Removing the Uploaded Certificate or Private Key 484
Replaceable Controller 117
Requirements for Prometheus and Grafana 365
Reserving IP Addresses in DHCP Servers 702
Reserving IP in Linux 703
Reserving IP in Windows 702
Reset Button 111
Resetting a Group's Energy Counter and Minimum/Maximum Values 178
Resetting All Settings to Factory Defaults 381
Resetting Energy Readings 507
Resetting the Button-Type Circuit Breaker 111
Resetting the Handle-Type Circuit Breaker 112
Resetting the PX4 510
Resetting to Factory Defaults 509, 654
Restarting the PX4 510
Restricted Service Agreement 521
Restrictions of Port-Forwarding Connections 633
Retrieving Energy Usage 404
Retrieving Previous Commands 409
Returning User Group Information 696
Role Configuration Commands 510
Role of a DNS Server 714
Role-Based Access Control 528
Running RCM Self-Test 667

S

Safety Instructions 13
Safety Warnings 14, 16
Sample Environmental-Sensor-Level Event Rule 341
Sample Event Rules 338
Sample Inlet-Level Event Rule 340
Sample Outlet-Level Event Rule 338
Sample PDU-Level Event Rule 338
Saving User Credentials for PDView's Automatic Login 30
SCEP 275
Scheduling an Action 330
Scheduling RCM Self-Test 663
Security Configuration Commands 515
Security Settings 439
Send an SNMP Notification 326
Send Email 322
Send Sensor Report 323
Send Sensor Report Example 330
Send SMS Message 324
Send Snapshots via Email 325
Sending Links to Snapshots or Videos 386
Sensor Descriptors for Inlet Active Power 348
Sensor Log 347
Sensor Threshold Configuration Commands 538
Sensor Threshold Settings 705
Sensor/Actuator Location Example: X, Y, Z Coordinates 205
Sensor/Actuator States 194
Sequence Setup 162
Serial Access With Dominion Serial Access Module 215
Serial Port Configuration Commands 534
Server Reachability Configuration Commands 535
Server Reachability Information 439
Server Reachability Information for a Specific Server 440
Server Status Checking or Power Control 354
Setting an Outlet's Cycling Power-Off Period 499
Setting Data Logging 343
Setting Data Logging Measurements Per Entry 463
Setting Default Measurement Units 231, 563
Setting Ethernet EAP Parameters 480
Setting Front Panel RCM Self-Test 669
Setting IPv4 Static Routes 471
Setting IPv6 Static Routes 475
Setting LAN Interface Parameters 477
Setting Log Capacity 463
Setting Network Service Parameters 490
Setting RCM Current Thresholds 662
Setting RCM DC Current Thresholds 664
Setting RCM Thresholds 668
Setting Redfish Service 497

Setting the Alarmed to Normal Delay for DX2-passive infrared sensor 466
Setting the Automatic Daylight Savings Time 554
Setting the BSSID 489
Setting the Cascading Mode 247, 623
Setting the Date and Time 286
Setting the Ethernet Authentication Method 479
Setting the HTTP Port 491
Setting the HTTPS Port 491
Setting the Inrush Guard Delay Time 461
Setting the IPv4 Address 470
Setting the IPv4 Configuration Mode 469
Setting the IPv4 Gateway 471
Setting the IPv4 Preferred Host Name 469
Setting the IPv6 Address 474
Setting the IPv6 Configuration Mode 472
Setting the IPv6 Gateway 475
Setting the IPv6 Preferred Host Name 473
Setting the LAN MTU 479
Setting the Outlet Initialization Delay 461
Setting the Outlet Power-On Sequence 459
Setting the Outlet Power-On Sequence Delay 460
Setting the Outlet Relay Behavior 459
Setting the PDU-Defined Cycling Power-Off Period 461
Setting the PDU-Defined Default Outlet State 460
Setting the PSK 486
Setting the Registry to Permit Write Operations to the Schema 696
Setting the SNMP Configuration 494
Setting the SSID 485
Setting the Time Zone 553
Setting the Wireless Authentication Method 485
Setting the Wireless MTU 489
Setting the X Coordinate 464
Setting the Y Coordinate 465
Setting the Z Coordinate 465
Setting Thresholds for Total Active Energy or Power 145
Setting Up a TLS Certificate 270
Setting Up External Authentication 275
Setting Wireless EAP Parameters 486
Setting Wireless Parameters 485
Setting Your Preferred Measurement Units 230
Show and Hide Min/Max Values 126
Showing Information 411
Showing Network Connections 565
Showing Residual Current Monitoring Information 668
Showing the Firmware Upgrade Progress 110
Shut down a Server and Control its Power 320
Single Login Limitation 523
Smart Sensor Configurations for Power Sharing 38
SmartLock 391
SmartLock and Card Reader 391
SNMP Gets and Sets 402
SNMP Sets and Thresholds 403
SNMPv2c Notifications 401
SNMPv3 Notifications 399
Sorting a List 125
Special Character Requirement 527
Special Configuration and Upgrade Methods 573
Specifications 569
Specifying Non-Critical Outlets 462
Specifying the Agreement Contents 522
Specifying the CC Sensor Type 464
Specifying the SSH Public Key 562
Standard Attributes 676
Start or Stop a Lua Script 327
Static Route Examples 244
Static Route Interface Names 246
Step A. Determine User Accounts and Roles 670
Step A: Add Your PX4 as a RADIUS Client 677
Step B. Configure User Groups on the AD Server 670
Step B: Configure Connection Policies and Vendor-Specific Attributes 680
Step C. Configure LDAP Authentication on the PX4 671
Step D. Configure Roles on the PX4 674
Strong Passwords 525
Supported Web Browsers and Mobile Devices 120
Supported Wireless LAN Configuration 25
Switch Outlet Group 328

Switch Outlets 328
Switch Peripheral Actuator 329
Switching Off an Actuator 443
Switching On an Actuator 442
Switching to a Different Unit 53
Syslog Message 329
System and USB Requirements 574

T

TACACS+ Settings 454
Testing the Network Connectivity 566
TFTP/HTTPS Requirements 586
The ? Command for Showing Available Commands 408
The MIB File 402
Third Party Licenses 727
Threaded Grounding Point 118
Threshold Bulk Setup 159
Thresholds and Sensor States 705
Time Configuration Commands 552
Time Units 144
Tips for Using the CLI 408
TLS Certificate Chain 716
TLS Certificates for PDU Linking 45
Tracing the Route 566
Trip Cause Outlet Handling 144
Turning Off the Outlet(s) 505
Turning On the Outlet(s) 504

U

Unbalanced Current Calculation 713
Unblocking a User 564
Universal Input Cord 118
Unpacking the Product and Components 20
Updating the Firmware 370
Updating the LDAP Schema 696
Updating the Schema Cache 700
Upgrade Guidelines for Existing Cascading Chains 372
Upgrade Matrix 371
Upgrade Sequence for Existing Cascading Chains 651
Upload via Curl 604
Uploading or Downloading Raw Configuration Data 612
Uploading Raw Configuration 604
Uppercase Character Requirement 526
USB Cascading 626
USB Wireless LAN Adapter - DX2-WIFI-KIT 25
USB-Cascading Requirements 627
User Blocking 524
User Configuration Commands 555
User Interfaces Showing Default Units 231
User Management 221
Using Default Thresholds 466
Using Prometheus and Grafana 364
Using SNMP 398
Using the CLI 643
Using the CLI Command 656
Using the Command Line Interface 405
Using the Front Panel Display 655
Using the Hardware Features 71
Using the LCD Display 646
Using the SNMP 644
Using the Web Interface 120, 641

V

Vendor-Specific Attributes 676
View DSAM Serial Ports 217
Viewing Connected Users 367
Viewing Firmware Update History 372
Viewing Link Unit Information 54
Viewing the Primary Unit 44
Viewing, Downloading, Deleting Locally-Saved Snapshots 387
Viewing, Pausing, Resuming or Clearing the Local Event Log 368

W

Waveforms for Outlets 173
Ways to Probe Existing User Profiles 714
Web Interface Operations for RCM 660
Web Interface Overview 122
Webcam Management 382

What is a Certificate Chain 716
When to Avoid Cascading Devices 620
Windows NTP Server Synchronization Solution 288
Wireless Network Settings 239
With HyperTerminal 405
With SSH or Telnet 406
Writing or Loading a Lua Script 360

X

Xerus Default Log Messages for All Products 296
Xerus Product Integration 722

Y

Yellow- or Red-Highlighted Sensors 193

Z

Z Coordinate Format 205
Zero U Products 19