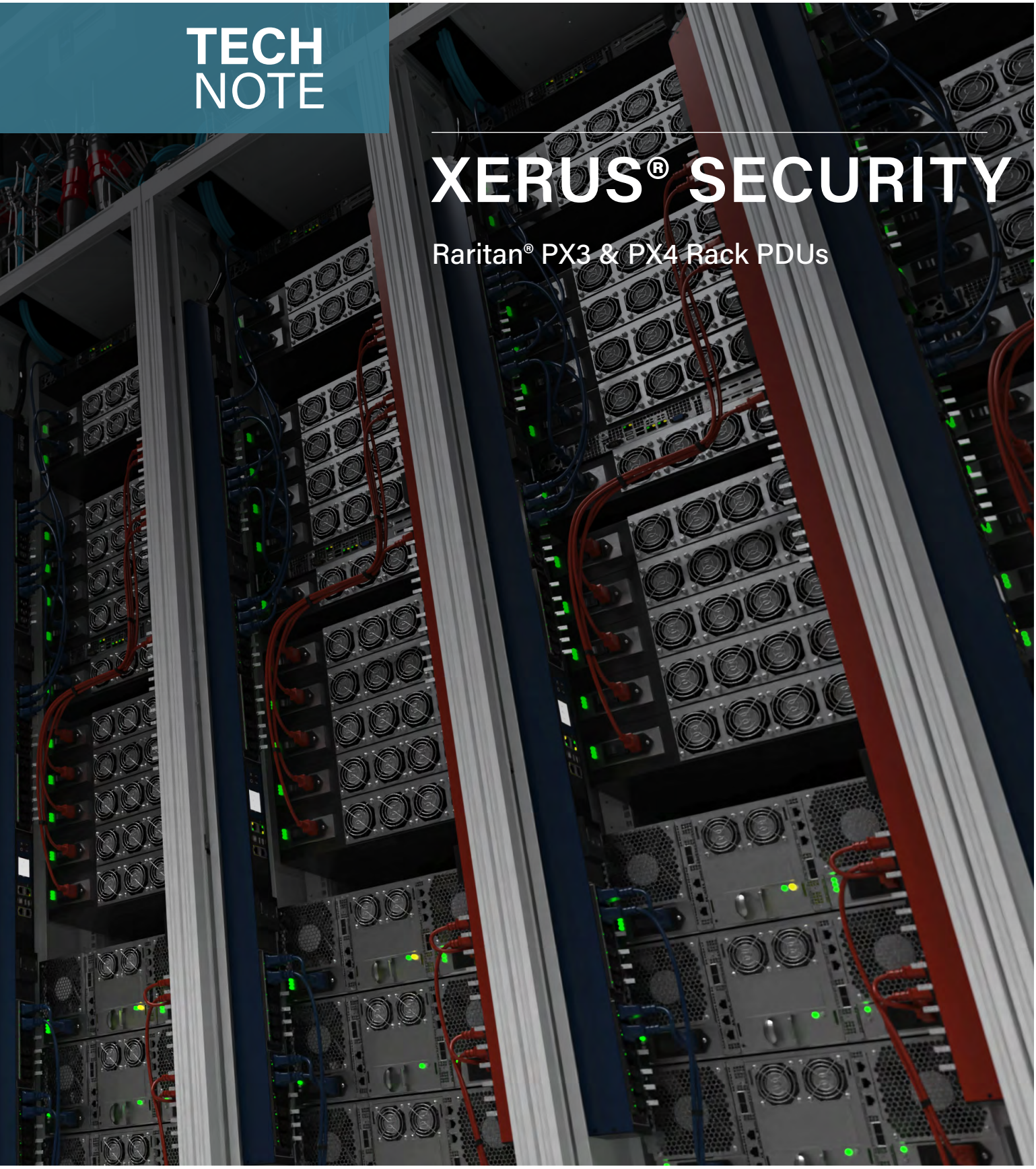
TECH
NOTE

XERUS® SECURITY

Raritan® PX3 & PX4 Rack PDUs



Raritan®
A brand of legrand®



Legrand's Raritan PX3 and PX4 Rack PDUs focus on digital security and access control at the rack level through the embedded Xerus Technology Platform. Xerus is a versatile, reliable platform that integrates hardware, software, and communication protocols directly into the device. Xerus' intelligence enables interoperability, power and environmental management, capacity planning, asset governance, physical access control, and more, enhancing data center continuity and performance.

To help understand the security and control features of the PX3 and PX4 PDUs, this Tech Note provides references to the following features of the embedded Xerus Technology Platform:

- **Encryption and Network Access**
- **Password Policies**
- **Firewall**
- **Certificate**
- **Defense-in-Depth**

ENCRYPTION AND NETWORK ACCESS FEATURES

SECURITY OF PDU NETWORK ACCESS PATHS

PX3 and PX4 PDUs, by default, only enable secure protocols such as HTTPS and SSH. Enabling an insecure protocol will result in the following message: "Warning: An insecure protocol is activated". Access paths to the PDU and the related security methods for those paths are provided for reference in the two tables below: Table A: Server Protocol Security and Table B: Client Feature Security. Additional reference information specific to server protocols and client features is also included in this document, such as specifications, session connection details, and cryptographic ciphers.

TABLE A: PX3/PX4 SERVER PROTOCOL SECURITY

This table summarizes the security and method of function for protocols and services that are run as server processes in the PDU's Xerus firmware.

Access Path to PDU	Secure?	How Does it Work?
HTTPS (TLS)	Yes	Provides a secure connection on default port 443 or user-configured port (secure Web access and JSON-RPC API).
SNMPv3	Yes	Adds security lacking in earlier versions. Users are configured with an authentication protocol and password as well as a privacy (encryption) protocol and password. Authentication confirms that messages come from a valid user and haven't been altered. Privacy encrypts message contents, including traps, so only the intended recipients can access them.
SSH	Yes	Requires login credentials with password and/or with public-key based login. Offers command line interface access to the PDU.
Secure File Transfer Protocol (SFTP)	Yes	Login credentials are required, and associated network traffic is secure over encrypted SSH transport.
Telnet	No	Login credentials are required, but associated network traffic is not secure.
HTTP	No	Login credentials are transmitted unencrypted.
SNMPv1/v2c	No	SNMPv1 has well-known limited security; SNMPv1/v2c community strings are sent unencrypted over the network; SNMPv2c offers protocol enhancements but no security enhancements over SNMPv1.
USB Port/Serial Port – Command Line Interface (CLI)	-	Physical ports that can facilitate remote connection to a PDU. One method of remote connection implements a B-SNMP protocol server to enable limited remote access to PDU power and outlet controls when connected to a compatible Raritan KVM or Serial Switch. Otherwise, PX3/PX4 supports out-of-band serial/CLI management from Raritan Serial Access Modules and third party devices. In either case, at minimum one set of device credentials is required, and connection security is dependent upon the configuration of the devices in the remote access chain. See "Secure Hardware Communications Paths" for more information.

TABLE B: PX3/PX4 CLIENT FEATURE SECURITY

This table summarizes the security and method of function for services and features run as client processes in the PDU's Xerus firmware that allow the PDU to communicate with remote authentication servers and other network services.

Access Path to PDU	Secure?	How Does it Work?
Email	Yes	SMTP authentication via TLS is supported (via StartTLS). Permits an initial unencrypted connection but then forces client/server negotiation to enable content encryption.
LDAP	No	Supports anonymous binding with no required credentials. Some LDAP servers do not allow anonymous binding. The LDAP server allows access to the PDU without having to create a local user(s) per PDU. Data is transmitted without encryption.
LDAP over TLS (LDAPS)	Yes	The TLS session is established before any LDAP data is exchanged, so all LDAP traffic, including user credentials, is encrypted. LDAP with StartTLS is also supported. This upgrades a standard LDAP connection to TLS, after which all LDAP traffic, including user credentials, is encrypted.
RADIUS	No	Enables access using a RADIUS server for authentication, authorization, and accounting.
TACACS+	No	Enables authentication with a central TACACS+ server, as defined in RFC standards; secret phrase obfuscates all data packets between the PDU and the TACACS+ server.

SECURE SERVER PROTOCOLS

HTTPS

Specifications

- Secure HTTP over Transport Layer Security (TLS) - version 1.3 (RFC 8446)
- Support for RSA Encryption (2048 and 3072-bit)
- Support for ECDSA Encryption (NIST curves P-256, P-384, P-521)
- Support for Certificate Signing Request (CSR) using RSA or ECDSA
- Intermediate CA Certificate is supported

Web Browsers Supported

A modern web browser with TLS 1.2 or 1.3 support is required. Current versions of Edge, Firefox, Chrome, and Safari have been tested and are supported.

Sessions and Connections

With HTTPS (TLS 1.3), TLS is enabled by default but can be disabled if desired. HTTP connections will be redirected to HTTPS by default.

Cryptography Ciphers

The following ciphers shall be enabled by default (based on Mozilla's Modern Security cipher list).

TLS 1.2

0xC030 (ECDHE-RSA-AES256-GCM-SHA384)
0xCCA8 (ECDHE-RSA-CHACHA20-POLY1305)
0xC02F (ECDHE-RSA-AES128-GCM-SHA256)
0xCCA9 (ECDHE-ECDSA-CHACHA20-POLY1305) added in Xerus firmware 4.0.0
0xC02B (ECDHE-ECDSA-AES128-GCM-SHA256) added in Xerus firmware 4.0.0
0xC02C (ECDHE-ECDSA-AES256-GCM-SHA384) added in Xerus firmware 4.0.0

TLS 1.3

0x1302 (TLS_AES_256_GCM_SHA384)
0x1303 (TLS_CHACHA20_POLY1305_SHA256)
0x1301 (TLS_AES_128_GCM_SHA256)

SNMPV1/V2C/V3

Specifications

SNMP allows network management systems to use SNMP requests to retrieve information and control power for individual outlets (on supported PDU models). The PDU includes an SNMP agent that supports standard MIB-1 and MIB-2 objects. A private enterprise MIB extension (PDU2-MIB) is also supported to provide remote power control, monitoring, and limited configuration.

A blank read/write community string can make all SNMP actions read-only.

SNMP can accept an indefinite number of SNMP requests in the queue. FIFO-style and traps can be sent to multiple trap destinations.

Notes for SNMPv1/v2c/v3:

- SNMPv1/v2c: no security; community strings are sent unencrypted over the network. SNMPv2c offers protocol enhancements but no security enhancements over SNMPv1.
- SNMPv1/v2c and SNMPv3 can be enabled or disabled independently; this means having SNMPv1/v2c and/or SNMPv3, or none.

SSH

Authentication

Username/Password: Entry is done using either the 'Password' or 'public key authentication', or 'password' and 'public key authentication' methods.

Key Exchange Methods

- curve25519-sha256
- curve25519-sha256@libssh.org
- ecdh-sha2-nistp521
- ecdh-sha2-nistp384
- ecdh-sha2-nistp256

Encryption Algorithms

- chacha20-poly1305@openssh.com
  - added in Xerus firmware 4.0.0
- aes128-ctr
- aes256-ctr

MACS

- hmac-sha2-256

Host Key Formats

- ssh-ed25519
  - added in Xerus firmware 4.0.0
- ecdsa-sha2-nistp384
- rsa-sha2-256
  - 2048-bit key length
  - added in Xerus firmware 4.0.0

Notes:

- User passwords are hashed via PBKDF2 with SHA256.
- The default password policy requires the user to set up a new password before operating in a production environment.

SECURE CLIENT FEATURES

EMAIL

The Email client in the PDU supports transmission of log entries and alerts. SMTP over TLS (STARTTLS) is supported if enabled.

LDAPS

Allows centralized username/password management on a networked directory server instead of locally on each PDU. Provides three security methods:

Specifications

- Transport Layer Security (TLS), version 1.2 and 1.3
- X.509 version 3 (RFC 2459) server certificates with RSA or ECDSA key.
- TLS: The encryption and authentication method uses TLS, requiring proof of server identity and protecting data in transit.

Server-Client Certificates

Server certificates are accepted and used dynamically. If a client certificate is requested, a NULL client certificate is sent to the server. RSA with 2048 or 3072 bits or ECDSA with the NIST P-256, P-384, or P-521 curves are supported.

RADIUS

Centralized Network Protocol

The RADIUS protocol is supported to provide a high-performance, centralized network protocol that enables remote authentication and authorization, such as usernames and passwords.

Vendor-Specific Attributes (VSA)

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

TACACS+

The TACACS+ protocol enables authentication and authorization with a central TACACS+ server.

User Accounts

User accounts do not need to be individually created locally on each PDU. Instead, one or more roles are made in the local PDU with the intended access rights for a TACACS+ user. A TACACS+ server response will then map a TACACS+ user to the local role(s) in the PDU. This occurs with either a custom service attribute or a shell privilege level.

SYSLOG WITH TLS

Specifications

A syslog target server can be specified in the PDU's Xerus firmware, and the following protocol and security options can be selected: UDP, TCP, or TCP + TLS. TCP + TLS is the default option. A valid CA certificate utilizing an X.509 certificate chain will then be required to finalize configuration.

FIPS FOR CRYPTOGRAPHIC MODULES (ONLY FOR PX4)

The PX4 offers a FIPS Mode that enables compliance with the Security Requirements for Cryptographic Modules of the Federal Information Processing Standards (FIPS), as defined in FIPS PUB 140-2, Annex A: Approved Security Functions. These standards are used to protect the Federal government's sensitive information with cryptography-based security systems in the US and Canada.

Separately, starting in Xerus firmware 4.4.0, the PX4 implements OpenSSL 3.1.2 which utilizes a FIPS 140-3-validated cryptographic module. This validation applies specifically to the cryptographic module, while the FIPS Mode governs system configuration and operation.

When FIPS mode is enabled, the following features will become unavailable:

- RADIUS and TACACS+ authentication
- Telnet
- Modbus
- HTTP (unencrypted)
- MQTT
- TFTP and FTP
- SNMPv2 (agent and traps)
- SNMPv3 (agent and traps) with MD5 and/or DES
- SNMPv3 security level without privacy
- TLS connections must check the certificate
- LDAP, Syslog, and SMTP without TLS

FIPS mode can be configured through:

- the PDU's GUI in the Device Settings > Security menu
- the CLI with a command that begins with security fips enabled <true/false> which sets the mode for the next reboot

PASSWORD POLICIES

Despite the many security measures in place, passwords remain among the most critical components of digital security. PX3 and PX4 PDUs offer several password security features, such as:

- strong passwords requiring a minimum of eight characters with lowercase, uppercase, numerals, and special characters
- customizable password expiration to ensure passwords are refreshed periodically and to prevent hackers from accessing the PDUs through known security breaches
- forced password changes to ensure that the default password gets changed after the first-time login, as default passwords are the easiest way for hackers to take control of connected devices

USERNAMES

Default Administrative User Account

	PX3	PX4
Username	admin	admin
Password	raritan	legrand

Username Locked

By default, users have three attempts to log in to the PDU. After the third attempt, the username will be locked for 10 minutes.

Username Restrictions

Usernames must be 1-32 characters in length; spaces are not allowed.

PASSWORDS

Password Requirements

By default, passwords must contain at least one digit, one lowercase character, and one uppercase character, be a minimum of 8 characters and a maximum of 64 characters. Strong password support can be disabled. The strong password requirements are configurable, so users can determine if they want one lowercase, one uppercase, one numeric, and one special character. A password change is enforced at first login.

Password Expiration

A password won't expire by default, but the expiration can be set to 7, 14, 30, 60, 90, 180 or 365 days.

Password History

A password is user-defined, with up to 12 as the maximum number of previous passwords that cannot be repeated when changing the password.

Why is a Password Change Forced Upon First Login?

California Senate Bill 327, also known as CA SB-327, primarily addresses California's landmark 2018 law on Internet of Things (IoT) device security, requiring manufacturers to implement "reasonable security" measures, such as unique passwords or mandatory password changes, for connected devices sold in the state, effective January 1, 2020, to prevent unauthorized access. To comply with CA SB-327, PX3 and PX4 PDUs and their Xerus firmware have been updated to ensure secure access (physical or via secure network protocols) by requiring all users to change the default administrator password upon first login.

FIREWALL FEATURES

PX3 and PX4 PDUs are accessed over the network for a range of uses, from simple data collection to critical alert notifications to power control. With systems and users needing such access from various segments of the corporate network, it is essential to keep out unauthorized access through the following means:

- IP-Based Access Control Lists (IP ACL) rules determine whether to accept or discard traffic to/from the PDUs based on the IP address of the host sending or receiving the traffic.
- Role-Based Access Control (RBAC) rules act like IP access control rules, which allow access to PDUs based on the roles of individual users.

The Default Policy in PX3 and PX4 PDUs can be set to Accept, Drop, or Reject.

CREATING IP ACCESS CONTROL RULES

IP access control rules (firewall rules) determine whether to accept or discard traffic to or from the PX3 or 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. Rules are executed in their defined order, with duplicate IP rules being ignored.
- Prefix length is required.
- When an existing IP access control rule requires updates to the IP address range and/or policy, modify them accordingly.
- Delete any unnecessary rules.

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 allows users to grant system permissions to a specific role based on their IP addresses. As with IP access control rules, the order of role-based access control rules matters because they are executed in numerical order.

Multiple user roles beyond the default 'Admin' and 'Operator' can be defined. Each user role can have differing levels of access to features, log data, settings, and more.

PDU Access with User Accounts

The maximum number of locally stored and active user accounts supported in the PDU is 32. These accounts are either local user accounts or local roles.

CERTIFICATE FEATURES

The digital certificates for the PX3 and PX4 PDUs ensure that both parties in a secure connection are authenticated. As rack PDUs are increasingly accessed over public networks, valid certificates protect against man-in-the-middle attacks. To make this process as efficient as possible, PX3 and PX4 PDUs support:

- CA certificates using either RSA or ECDSA keys, issued and signed by public certificate signing authorities after thorough verification of the user's business; the PDU interface even generates the certificate signing request for submission to signing authorities such as Verisign, DigiCert, and more.
- Self-signed certificates when a CA certificate is not deemed necessary; the PDU also provides an interface to generate a self-signed certificate.

SCEP SUPPORT

Starting with Xerus firmware 4.4.0, PX3 and PX4 PDUs support automated certificate enrollment via Simple Certificate Enrollment Protocol (SCEP) using RSA keys (both 2048 and 3072-bit). It uses encrypted communication for certificate requests, ensuring centralized control and authentication. During initial enrollment, the device authenticates to the SCEP CA server using a shared secret. To enable certificate issuance, you must configure the SCEP server and the associated gateway so the PDU can submit enrollment requests securely. Once SCEP is enabled, reconfiguration requires discarding of the existing configuration and proceeding with a fresh enrollment.

DEFENSE-IN-DEPTH FEATURES

Rack PDUs play a critical role in managing power infrastructure and servers, using their remote power control functionality. Therefore, it is essential to protect against network breaches. PX3 and PX4 PDUs have implemented several security measures that keep them one step ahead of these threats:

- Blocking access after repeated failed login attempts and logging the source of the attempts.
- Timing out inactive sessions to prevent unauthorized access.
- Limiting the use of the same login credentials from multiple clients.
- Enforcing restricted service agreement warnings and requiring that users accept them to log in.

USER ROLES

In addition to security over the access paths to the PDU with user authentication, the PX3 and PX4's Xerus firmware provides user roles to PDU features for further restriction over outlets, outlet groups, ports, LDAP, RADIUS, and more.

There are two predefined roles called 'Admin' and 'Operator'. The 'Admin' role is locked. These are the predefined roles for the 'Operator' (availability of some functions dependent upon PDU model):

- Acknowledge Alarms
- Change Own Password
- Change PDU, Inlet, Outlet & Overcurrent Protection Configuration
- Switch Outlet and Outlet Groups
- View Event Settings
- View Local Event Log

LOCKING FRONT PANEL CAPABILITIES

Using the steps below, enable or disable the capability of switching outlets using the Front panel:

To enable the front panel actuator control feature:

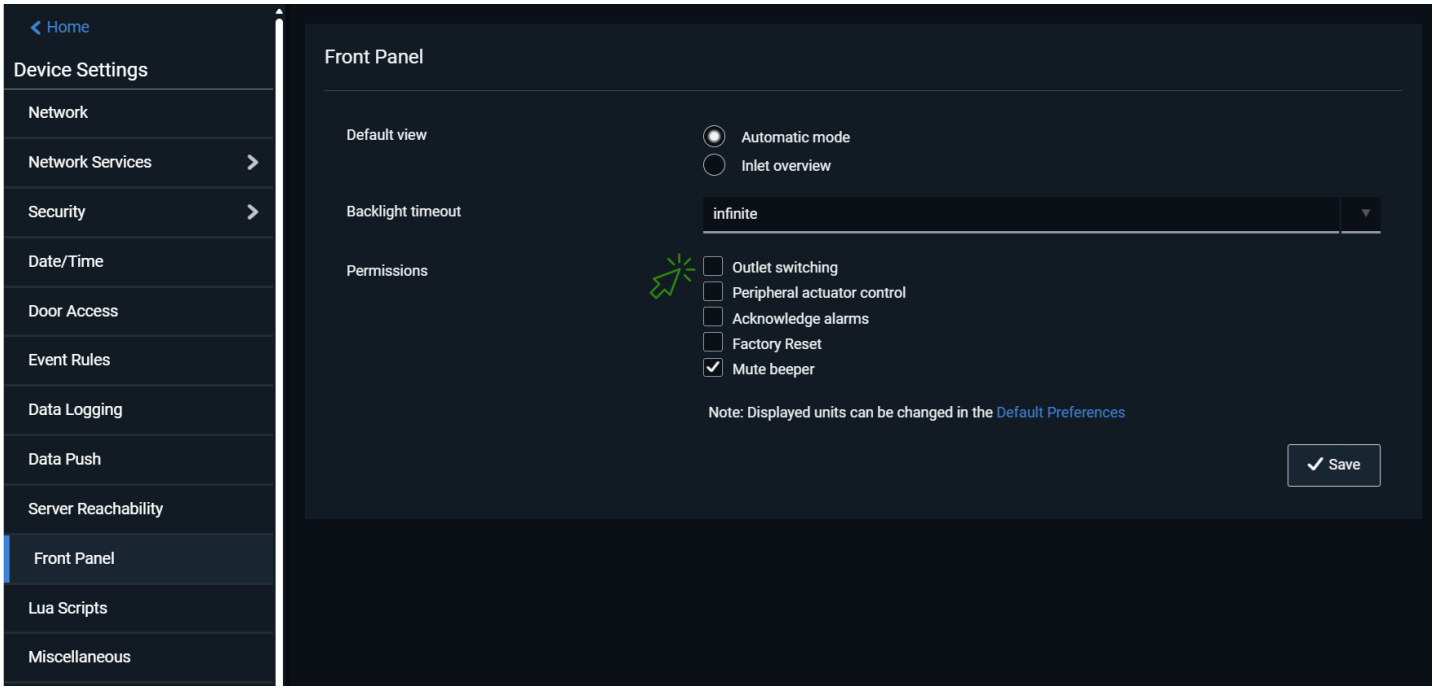
- config:# security frontPanelPermissions add switchOutlet
- config:# apply

To disable the front panel actuator control feature:

- config:# security frontPanelPermissions remove switchOutlet
- config:# apply

Use the PDU's GUI by going to Device Settings > Front Panel:

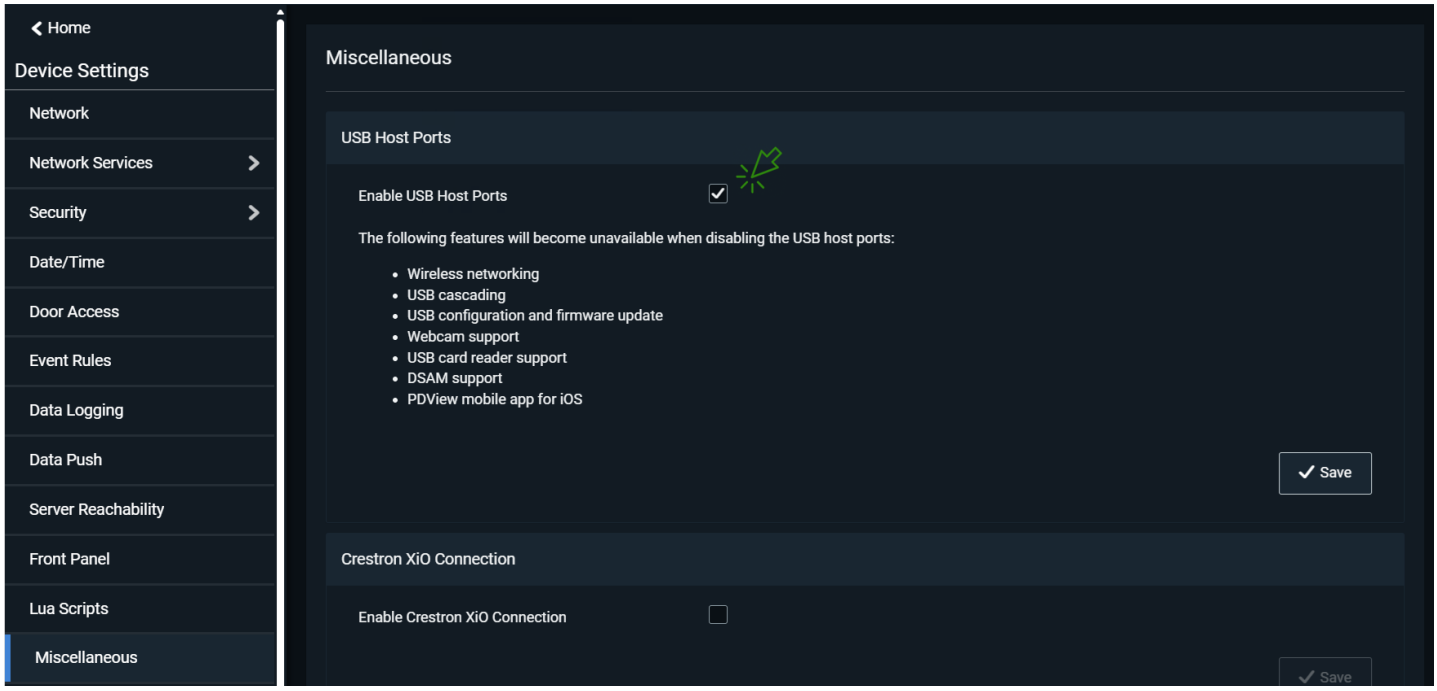
- Select the 'Outlet switching' checkbox to enable the outlet switching function
- Unselect the 'Outlet switching' checkbox to disable the outlet switching function



DISABLE USB TYPE A HOST PORT FUNCTIONALITY

In the PDU's GUI, under Device Settings > Miscellaneous, enable or disable USB Host ports:

- Select the 'Enable USB Host Ports' checkbox to enable the function
- Unselect the 'Enable USB Host Ports' checkbox to disable the function



RESET AND REMOTE SHUTDOWN SECURITY

- Restart the controller by pushing the reset button, but this will not affect the power status of the outlets.
- Console port/USB type B will be used to access using CLI, and entering "factorydefaults" will reset the PDU with all default values.
- The Disaster/PDU Recovery button can be used in conjunction with a USB type B and a computer executing the PDU recovery tool. The tool can be found on www.raritan.com/support after selecting the product ("PX2/PX3/PXC/PXO" or "PX4"). Under "Tools and Drivers", find "PDU Recovery Tool".

Examples of the controllers are below: (not all controller options are shown here)

PX3 CONTROLLER



PX4 CONTROLLER



SECURE HARDWARE COMMUNICATION PATHS

Physical connections allow access to the PDU via hardware communication paths:

PX3 only

- Console access using RJ45 connection and USB type B.

PX3 and PX4

- Ethernet (two per PDU) via various network protocols, such as HTTP/S, SSH, FTP, SFTP, SNMP, Telnet, etc. (as listed in Table A: Server Protocol Security below) – a secured login procedure with credentials (username and password), including strong password enabling. Insecure protocols are disabled by default. Each Ethernet port can be individually configured with 802.1x authentication to ensure secure access to the PDU on 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. EAP-TLS and EAP-PEAP are supported as authentication methods to securely exchange information.
- USB type B port – secured login procedure with credentials (name and password). Also using the PDView app on an Android device. For PX4, this port would be used for CLI.
- USB type A port (two in PX4) – secured login procedure with credentials (name and password). Also using the PDView app on an iPhone.

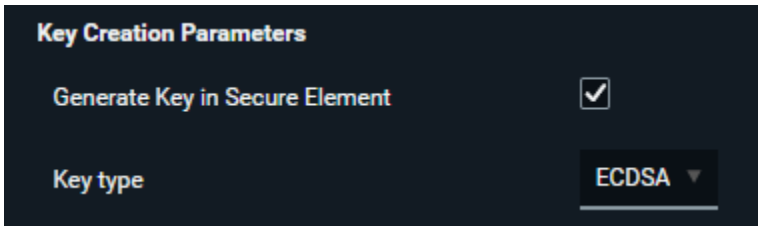
SECURE BOOT (ONLY FOR PX4)

Secure Boot is a technology traditionally used in servers, PCs, and mission-critical embedded devices, that hardens against attacks by ensuring that only trusted, properly signed software components are allowed to run during the device's boot process.

Secure Boot uses digital signatures, cryptographic protocols, and a robust chain of trust to verify the authenticity of each component involved in the boot sequence, from the firmware level to the root file system and system kernel, without requiring changes in firmware update procedures or additional administrative overhead. Should any of the multiple stages of software or file system validation fail, the Xerus-enabled product will immediately stop the boot process without compromising the stability of the critical load. Secure Boot offers customers adopting Xerus-enabled products the added peace of mind with one additional layer of security.

SECURE ELEMENT – CRYPTOGRAPHIC SECURITY MODULE (ONLY FOR PX4)

The PX4's Secure Element is a cryptographic coprocessor designed to provide hardware-based security for the PDU's embedded systems. It can be utilized to enhance communication security by generating and storing TLS Keys for Certificate Signing Requests (CSRs) or Self-Signed Certificates directly on the device. If such keys are generated and stored within the Secure Element, they cannot be extracted or duplicated, significantly strengthening the security of the PDU's encrypted communications. This level of protection is critical for data centers, where infrastructure security and compliance with stringent cybersecurity standards are paramount.



Feature within the PX4 Web GUI for enabling generation and storage of TLS Keys within the Secure Element

The flexible architecture of the Secure Element enables Legrand to continuously expand and enhance its security capabilities. For example, Xerus firmware version 4.4.10 and later introduces support for full encryption of Xerus device configuration data, along with Secure Element-protected storage of each device's unique cryptographic keys. This helps safeguard configuration and log data from unauthorized extraction, even through direct access to device flash storage. By providing a platform that can evolve alongside emerging cybersecurity threats and changing industry requirements, the PX4 PDU remains well positioned to adapt to future challenges and support the ongoing security of modern data centers.

*Availability of some features may be dependent on iX Controller version. Contact Technical Support to confirm availability.

IPV6 READY LOGO CERTIFIED & USGV6 REGISTRATION

PX3 and PX4 PDUs have qualified for an IPv6 Ready Logo certification, a global IPv6 Forum program that verifies networking products through rigorous conformance and interoperability testing to confirm correct implementation of IPv6 protocols. This certification confirms our rack power products correctly handle core IPv6 functions, such as addressing and configuration (e.g., DHCPv6), routing, and security (IPsec/IKEv2), as well as management to ensure compatibility, seamless connectivity and interoperability with other IPv6-enabled products in an IPv6 environment.

Our PDUs also meet the USGv6 requirements and capabilities for Core, SLAAC*, Address Architecture, and IPv6-Only. USGv6 is a testing program governed by the US Department of Commerce's National Institute of Standards and Technology (NIST) that executes a technical standards profile for the US Government and related agency acquisition of IPv6-enabled networked information technology and devices. This qualification ensures that our PDUs are IPv6 compliant and support future internet traffic demands.

*StateLess Address AutoConfiguration (SLAAC) is the native IPv6 facility for automatic IP address configuration for network devices.

Validate our certifications:

- IPv6 Ready Logo certification – go to https://www.ipv6ready.org/phase-2_approved_list and search for "Legrand" in the site's Vendor Name field
- USGv6 registration – go to https://www.iol.unh.edu/registry/usgv6?name=Legrand&test_lab=All and search for "Legrand" in the site's Company field

ISO SECURITY CERTIFICATION

Legrand's Power & Thermal Management division achieved ISO/IEC 27001 certification for its R&D centers in Somerset NJ, Zwickau Germany, Reno NV, and Canonsburg, PA, including the brands Raritan, Server Technology, and Starline. This certification demonstrates that Legrand's brands exceed standards and expectations for cybersecurity, data privacy, vulnerability testing, and penetration testing across R&D and production.

In addition to achieving all 114 process controls required for ISO 27001 certification in its engineering group, Legrand has also obtained ISO 9001, ISO 14001, and ISO 45001 certification. Our teams adhere to NIST and ISO standards and incorporate additional vulnerability and penetration testing for our network-connectable products. This additional testing puts products through cybersecurity testing to uncover areas of vulnerability or risk of unauthorized access to fix problems before they arise in real-world applications.

VULNERABILITY ASSESSMENT AND PENETRATION TESTING (VAPT)

Vulnerability Assessment and Penetration Testing (VAPT) is a crucial security testing approach in detecting and resolving cybersecurity vulnerabilities in our rack PDUs. Raritan engaged Pivot Point Security, a third-party consultant, to conduct an IoT security assessment and penetration test utilizing CREST-accredited testing methodology and prepare a vulnerability assessment. Pivot Point Security provided an unbiased and thorough evaluation of Raritan Rack PDU security measures and determined that the PDUs are secured consistent with industry best practices, CA SB 327, NISTIR 8259, and are on par with peer devices tested.

Raritan's quality and testing teams also utilize Tenable Nessus® scanners to reduce the time to discover, assess, and remediate vulnerabilities in Xerus Firmware.

SECURE SOFTWARE DEVELOPMENT AND VULNERABILITY MANAGEMENT

Legrand currently implements both manual testing procedures and automated static application security testing (SAST) and secure code analysis tools to identify potential issues in the PX3/PX4's source code. We actively monitor Common Vulnerabilities and Exposures (CVE) listings to detect potential weaknesses in our PDUs' software and hardware that cybercriminals could target. By closely tracking these vulnerabilities, we take preemptive action to address security gaps before they can be exploited. This involves our teams promptly releasing necessary patches and updates to users to fortify our systems and minimize the risk of security breaches. In today's rapidly changing cybersecurity landscape, vigilant CVE monitoring is essential for responding quickly to new threats, aiding in the protection of our PDUs, and maintaining the integrity of our infrastructure against potential attacks.

CVE.ORG AND US-CERT MONITORING

Raritan's technical teams monitor CVE.org as well as the US-CERT (now CISA) database and subscribe to vulnerability feeds to receive crucial, timely alerts on cyber threats, vulnerabilities and exposures, and incident information, enabling proactive defense, faster response, risk reduction, and compliance with mandates to protect critical systems and cyber infrastructure. This helps us understand threats, patch vulnerabilities, and align with best practices to improve situational awareness and resilience against attacks, and to stay ahead of potential exploits.

CONTACT TECHNICAL SUPPORT

Contact our support team by phone or email, and we'll get you up and running in no time.

Phone: (800) 724-8090 or 732-764-8886
For Technical Support: Press 6
Email: tech@raritan.com
Submit a Support Ticket: www.raritan.com/support/submit-a-ticket

To learn more visit

www.raritan.com

©2026, Legrand. All rights reserved. The industry-leading brands of Approved Networks, Kratos Industries, Ortronics, Raritan, Server Technology, Starline, and ZPE Systems empower Legrand's Power & Thermal Management division to produce innovative power, cooling, connectivity and management solutions for data center white space and gray space, building networks, and facility infrastructures. Our division designs, manufactures, and markets world-class products for a more efficient and sustainable future. The exceptional reliability of our technologies results from decades of proven performance and a dedication to research and development. Lit #V2470