Raritan
A brand of legrand

TECHNICAL NOTE: XERUS SECURITY
RARITAN PX3 & PX4 RACK PDUS

This Technical Note provides a reference for access paths to Raritan® PX3 and PX4 Rack Power Distribution Units (PDUs) built on the Xerus™ Technology Platform. The document covers security for access paths to these PDUs, but it does not cover the security of the data center.

THE XERUS TECHNOLOGY PLATFORM

The backbone of the PX3 and PX4 PDUs is the Xerus Technology Platform. It is a flexible and robust platform that combines robust hardware, software, and communication protocols. Xerus increases the lifecycle of your PDUs by facilitating power management and monitoring, environmental monitoring, capacity planning, asset governance, physical access control, and more.

Xerus helps maximize data center uptime and efficiency with security, advanced power monitoring, metrics and alerting, and complete visibility into your power chain. With Xerus, you receive actionable data to aid in decisions that help safeguard assets and maximize your data center's continuity and performance.

ABOUT CA SB-327 LOCK-DOWN

In September 2018, California Governor Jerry Brown signed a cybersecurity law, Senate Bill 327, covering Internet of Things (IoT) devices to incorporate minimum security features for every device, making California the first state with such a law. Starting January 1, 2020, the bill, SB-327, requires any manufacturer of a device that connects "directly or indirectly" to the internet to be more responsible for ensuring privacy and security for California residents by equipping devices with "reasonable" security features that are designed to prevent unauthorized access, modification, or information disclosure.

To comply with SB-327, Raritan's PX3 and PX4 PDUs and PDU firmware have been updated to ensure secure access (physical or by secure network protocols) by forcing all users to change the default administrator password upon first login. The new password must meet the default strong password requirements.

LOCKING FRONT PANEL CAPABILITIES

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

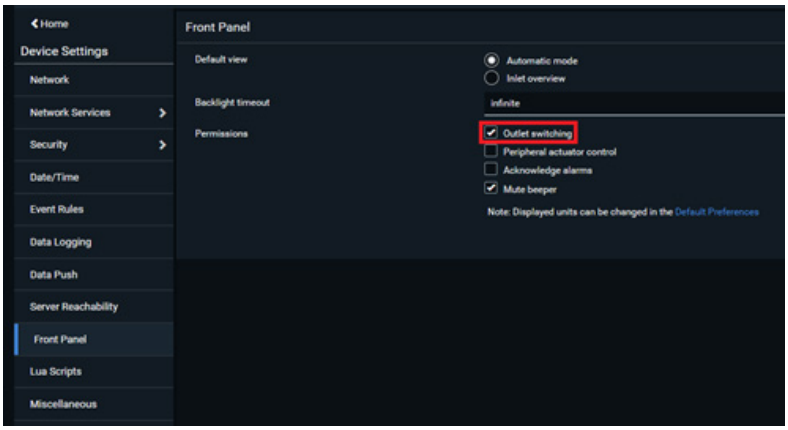
To enable the front panel actuator control feature:

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

To disable the front panel actuator control feature:

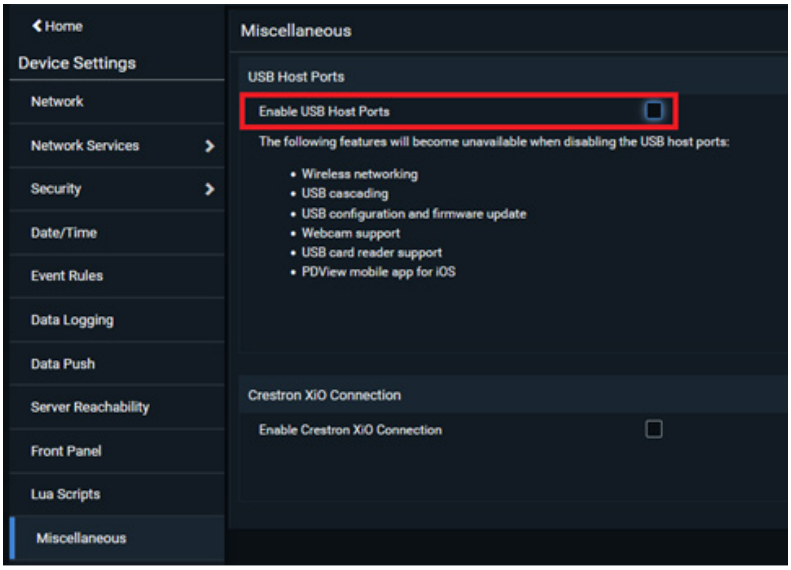
```
config:# security frontPanelPermissions remove switchOutlet
config:# apply
```

A Second option to disable the outlet switching from the front panel is accessing the GUI and going to Device Settings > Front Panel.



DISABLE USB TYPE A PORTS

In the web GUI, under Device Settings > Miscellaneous, you can disable the USB type A ports.



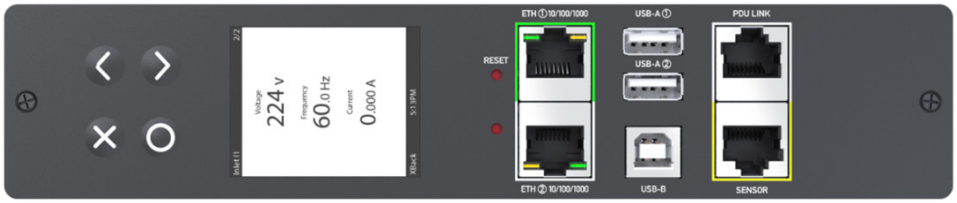
RESET AND REMOTE SHUTDOWN SECURITY

- You can 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 typing “factorydefaults” will reset the PDU with all default values.
- Disaster recovery button can be used in conjunction with a USB type B and computer executing the PDU recovery tool. You can find the tool on www.raritan.com/support after selecting the product (“PX2/PX3/PXC/PXO” or “PX4”). Under “Tools and Drivers”, you can find “PDU Recovery Tool”.

Examples of the controllers are below:

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, for example, HTTP/S, SSH, FTP, SFTP, SNMP, Telnet, etc. (as listed in Table A: Server Protocol Security below) – a secured login procedure with credentials (name and password), including strong password enabling. Some network protocols are secure, while others are not.
- 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.
- Using PDU link, you can connect 2 PDUs together (Only PX4).

SECURITY OF PDU ACCESS PATHS

By default, only secured protocols are enabled. If you enable an insecure protocol, you will get the following message: “Warning: An insecure protocol is activated”.

The only secure user-interface network protocols that are enabled by default are: HTTPS and SSH.

Access paths to the PDU and the related security methods for those paths are provided for reference in the two tables in this document: **Table A: Server Protocol Security and Table B: Client Feature Security**. Additional reference information specific to the server protocols and client features is also provided in this document, such as specifications, session-connection information, and cryptography ciphers.

TABLE A: SERVER PROTOCOL SECURITY

For the protocol access paths listed in the following table, the firmware actively listens on server ports to provide security for the PDU.

Access Path to PDU	Secure?	How Does it Work?
HTTPS (SSL/TLS)	Yes	Provides a secure connection on default port 443 or user-configured port (secure Web).
SNMPv3	Yes	Version 3 adds security to previous SNMP versions, such as security with a special key for both read-only and read-write username, authentication type/password, and privacy type/password; only the intended IP address can receive traps; and it is supported and implemented per IETF RFC standards.
SSH	Yes	Requires login credentials with password and keyboard interaction – two ways to collect credentials.
SFTP	Yes	Secure File Transport Protocol. Login credentials are required, and cross-transmission over the network is secure over an encrypted SSH transport.
Telnet	No	Login credentials are required, but cross-transmission over the network is not secure; the protocol can be disabled to remove security risks.
HTTP	No	Password is encoded, but username is not.
SNMPv1/v2c	No	SNMPv1 has well-known limited security; SNMPv1/v2c community strings are sent in clear text over the network; SNMPv2c offers protocol enhancements but no security enhancements over SNMPv1.
USB Port/ Serial Port – Command Line Interface (CLI)	Yes	Requires physical access to the PDU.

TABLE B: CLIENT FEATURE SECURITY

For the client access paths listed in the following table, the firmware gathers user credentials and transmits them to the server to provide validation and security for the PDU over the network.

Access Path to PDU	Secure?	How Does it Work?
Email	Yes	SMTP authentication is supported; if enabled, it authenticates with the server but does not encrypt the content.
LDAP	No	It supports anonymous binding with no required credentials. Some LDAP servers do not allow anonymous binding.
LDAPS	Yes	For LDAP over TLS, the encryption is enabled from the beginning. For LDAPS, encryption is enabled within the protocol. The LDAP server allows access to the PDU without having to create a local user per PDU.
RADIUS	Yes	Enables access using a RADIUS server for authentication, authorization, and accounting.
TACACS+	No	Enables authentication with a central TACACS+ server, per IETF RFC standards; secret phrase encodes all data packets between the PDU and the TACACS+ server.

SECURE SERVER PROTOCOLS

HTTPS

Specifications

- Secure HTTP over SSL Web Interface Protocol
- Transport Layer Security (TLS), version 1.3 (RFC 8446)
- Demo certificate SHA-256 with RSA encryption.
- Default HTTPS uses Asymmetric Cryptography: 3072-bit RSA Key Exchange
- Intermediate CA Certificate is supported.
- Support for Certificate Signing Request (CSR) using RSA or ECDSA.

Web Browsers Supported

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

Sessions and Connections

With HTTPS (SSL/TLS 1.3), SSL 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 firmware 4.0.0
- 0xC02B (ECDHE-ECDSA-AES128-GCM-SHA256)
  - added in firmware 4.0.0
- 0xC02C (ECDHE-ECDSA-AES256-GCM-SHA384)
  - added in 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

Specifications

SNMP allows network management systems to use SNMP requests to retrieve information and control power for individual outlets (Outlet Metered only). The PDU products include an SNMP v2c agent supporting 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 is allowed to 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 in clear text 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 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 firmware 4.0.0
- aes128-ctr
- aes256-ctr

MACs

- hmac-sha2-256
- hmac-sha2-512

Host Key Formats

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

Notes:

- Products that ship from the factory will have RSA 2048-bit keys with SHA256.
- User credentials (passwords) are generated with PBKDF2 using SHA256.
- The default password policy requires the user to set a new password before operating in a production environment.

Firewall

Rack PDUs are accessed over the network for various reasons ranging from simple data collection to critical alert notifications and even power control. With systems and users needing access from various segments of the corporate network, it is essential to keep unauthorized access entirely out 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 can be set to ACCEPT, DROP or REJECT.

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 for 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 key.
- TLS: The encryption and authentication method uses TLS or StartTLS. If the server is required, the proof of server identity and protection of data in transit is available.

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. We support RSA with 2048 or 3072 bits or ECDSA with the NIST P-256, P-384, or P-521 curves.

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 by either a custom service attribute or a shell privilege level.

SECURE BOOT (PX4)

Secure Boot is a technology traditionally used in servers, PCs, and mission-critical embedded devices that is designed to harden them against attacks by ensuring that only trusted and 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 cut short 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.

USERNAMES AND PASSWORDS

Default Administrative User Account

	PX3	PX4
Username	admin	admin
Password	raritan	legrand

Username Locked

By default, you have three attempts to log into 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.

Password Requirements

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

Password Expiration

The password won't expire by default, but you can modify the expiration to the following: 7,14,30,60,90,180 or 365 days.

Password History

Is user defined with 12 as maximum permitted.

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 LDAP user groups.

USER ROLES

In addition to security over the access paths to the PDU with user authentication, 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':

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

SECURITY CERTIFICATION

Legrand's Data, Power, and Control division achieved ISO/IEC 27001:2013 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 shows how Legrand's brands exceed standards and expectations for cybersecurity, data privacy, vulnerability testing, and penetration testing, from R&D to production.

In addition to achieving all 114 process controls required for ISO27001 certification in its engineering group, Legrand adheres to NIST and ISO standards and incorporates additional vulnerability and penetration testing for its 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.

TENABLE'S NESSUS SCAN

It's an industry standard for vulnerability assessment. It requires dynamic & automatic plugin updates to reduce the time to assess and remediate vulnerabilities.

Tenable Research works closely with the security community to discover new vulnerabilities and provide insights to help organizations mature their vulnerability assessment practices.

Raritan uses Tenable's Nessus scanner for the new Xerus platform to ensure that our firmware is free of vulnerabilities.

SYNOPSYS COVERITY TOOL

Legrand currently uses static code analysis tools from Synopsys to detect problematic parts in the source code for the products.

CVE CHECKS

We track the CVEs for all third-party components, assess whether they affect our products, and address them accordingly.

CONTACT TECHNICAL SUPPORT

Contact our support team by phone or email and we'll get you up and running in no time. If you want to open a ticket using our website, use this link.

Phone: (800) 724-8090 or 732-764-8886
For Technical Support: Press 6

Email: tech@raritan.com
For Global support, please find more information here.

NOTES

Raritan
A brand of legrand

Raritan Americas, Inc.
800.724.8090
raritan.com