

Xerus Firmware Release Notes



Version: Xerus 4.2.0 / Build 50274 / Release Notes, Version 1

Release Status: General Availability (GA)

Date: March 08, 2024

Release Overview

Xerus 4.2.0 Firmware is a **General Availability (GA) Release** for applicable Xerus-based product groups. This release may include performance and productivity improvements, support for new products and accessories, new features and enhancements, bug fixes, and general fixes for specific model families.

Applicability

This firmware release applies to the following Xerus-based product brands and models.

<i>Product Group</i>	<i>Model</i>
Rack PDUs	PX3, PX2, PXC, PXO
Smart Rack Controller	SRC
Branch Circuit Monitors	BCM2
Transfer Switch	PX3TS
Access Control	SmartLock™
Sensors	DX2 SmartSensors™
Asset Management	AMS2

General Guidelines for this Release

This release may not support some custom-engineered models. Please check the **Support & Compatibility** section below. Or contact your regional Raritan Support team if you are unsure of the model number of your unit—it is typically viewable from the GUI's *Device Information* page and is also printed on a label located on the device.

Note: Do NOT upgrade ANY other Raritan model(s) to Xerus 4.2.0 Firmware (other than what is listed in the Applicability table above) because the unit may either not be compatible with Xerus Firmware or may have been built after this release entered our System Tests and installing it may result in the unit becoming non-functional.

Note: Do NOT downgrade your new Xerus-based product(s) to any prior Xerus Firmware release. Due to significant internal enhancements in Xerus 4.2.0, a downgrade from Release 4.2.0 Build 50274 to ANY prior firmware release is NOT SUPPORTED. Please contact your regional Raritan Support team with any questions.

Release Highlights

New Products & Accessories

<i>Issue ID</i>	<i>Description</i>
81227	New WIFI Adapter support (DX2-WIFI-KIT) for iX7 and newer controllers
81957	New Modbus interface module support (USB-MOD-DONGLE)

New Features & Enhancements

<i>Issue ID</i>	<i>Description</i>
82754	Updated Lua script engine to the latest release 5.4.6
81914	Added additional sensor state support for Prometheus
81182	Added support for Active Directory Nested Groups
77026	Added additional authorization support for TACACS+
80999	Added SNMP support for existing gateway sensor feature
81255	Removed CIFS/Samba support for storage of webcam snapshots (Snapshots can be saved locally or via FTP.)
82440	Improved USB devices view from the Device Information Page

Bug Fixes

<i>Issue ID</i>	<i>Description</i>
82827	Fixed Firefox browser issue not accepting keyboard input for the Lua script code editor
82839	Fixed issue with the Lua code editor crashing
82914	Fixed issue in the GUI with wrong Sensor value types being displayed
82950	Fixed Role names with uppercase letters not authenticating via LDAP
82834	Fixed default threshold error messaging not using preferred units of measure
82777	Fixed the user preferred unit of measure on a preference change from the CLI
81453	Fixed issue with CLI when linked PDU is added and not refreshing privilege options until the session is restarted
82653	Fixed inconsistent naming issue on Inlet page
82822	Fixed issue of default thresholds edit dialog disappearing
82746	Fixed issue of sensor selection combo box being hidden with lack of data

82744	Fixed empty sensor accordion on the PDU page
82297	Fixed line break issues with Lua output
82180	Fixed inconsistencies when language translation is changed in the GUI
74195	Fixed communication errors in GUI when changing firewall states
82836	Fixed issues when changing default temperature values from the CLI
82793	Fixed inconsistent CLI response on disconnected peripherals
82885	Fixed duplicate title bar issue in the PDView app
83061	SmartLock - Fixed inconsistent lock and handle status in GUI
83024	Fixed inconsistent port naming when connecting Asset Management strips

Security Fixes & Updates

<i>Issue ID</i>	<i>Description</i>
82840	Reject overflows of zip header fields addressed (CVE-2023-45853)
83164	Use-after-free vulnerability in Linux kernel addressed (CVE-2023-6932)
83143	SSH vulnerability (Terrapin Attack) addressed (CVE-2023-48795)
83268	A Null dereference vulnerability in the Linux Kernel was addressed (CVE-2023-6915)

Please consult the appropriate User Guide for more information on these firmware features at raritan.com/support.

Support & Compatibility with Xerus 4.2.0

Except for some recent Engineered to Order (ETO) models, applicable units/models that are Xerus-based can be upgraded to this firmware release (see Applicability table above).

If you are unsure that this Xerus Firmware release supports your unit/model or have any questions about supported or unsupported configurations, please contact your regional Raritan Support team.

Upgrade Matrix (Path for Upgrades)

This firmware release is intended for factory shipments and firmware upgrades on the units/models stated in the Applicability table above.

Note: Due to file system changes in Xerus 4.0.x, the following upgrade paths must be followed, or the Xerus-based device may become inoperable and require manual recovery.

<i>Firmware Version</i>	<i>Upgrade Steps</i>
3.0.x, 3.1.x, 3.2.x	» 3.4.0 » 3.5.0 » 4.2.0
3.3.x, 3.4.x	» 3.5.0 » 4.2.0
3.5.x, 3.6.x	» 4.2.0

Note: Due to an issue found in recently released Xerus 4.0.x firmware updates, we strongly recommend that you upgrade to release 4.2.0 Build 50274. If you need assistance, please contact your regional Raritan Support team.

Downloads

The following supplemental files can be downloaded at raritan.com/support:

- Product Documentation and User Guides
- SNMP MIBs
- Related Tools and Drivers
- JSON-RPC SDK
- Redfish[®] Documentation

Historical firmware version downloads can be found on raritan.com/support.

Release Package Details

The Xerus 4.2.0 Firmware is a General Availability release package and is posted on the Raritan support website at raritan.com/support.

Xerus 4.2.0 Package

- "Xerus_ReleaseNotes_4.2.0.pdf" (this file)
- A firmware release (binary): pdu-px2-040200-50274.bin

General Upgrade Instructions (*stand-alone upgrade from the browser-based user interface*)

- Enable JavaScript in your browser before logging into the unit to start the upgrade process.
- Follow the instructions in the proper device User Guide. Please read the entire upgrade instructions before starting an upgrade.

If you have any questions or cannot follow the instructions in the User Guide, please STOP and contact Raritan Support for further instructions.

Contact Us

Go to raritan.com/support for contact options.