Eaton PDU Network module secure configuration guidelines

Documentation to securely deploy and configure the Eaton PDU Network module

Table of contents

PDU Network module

The Eaton PDU Network module was designed with cybersecurity as an important consideration and offers several features that address cybersecurity risks. These cybersecurity recommendations provide information to help users deploy and maintain the product in a manner that minimizes cybersecurity risks. The recommendations are not intended to provide a comprehensive guide to cybersecurity, but rather to complement customers' existing cybersecurity programs.

Eaton is committed to minimizing the cybersecurity risk in its products and deploying cybersecurity best practices in its products and solutions, making them more secure, reliable and competitive for customers.

Intended use and deployment context

The Eaton® Enclosure Power Distribution Unit (ePDU®) G3 is an intelligent PDU designed to distribute power within a standard 19-inch rack. A wide range of models let you connect and manage a variety of outlets from a single power connection. Most models have monitoring or switching capabilities, or both.

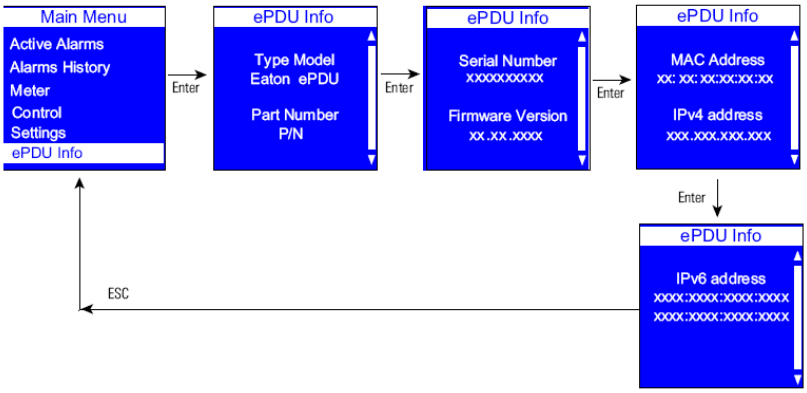
The Eaton rackmount PDU models support world-wide markets. These model types are defined primarily by the system management and monitoring capabilities, but the capabilities are also defined by the hardware configurations.

The rackmount PDU models support single-phase applications (or three-phase for American models) and can manage 6 to 54 outlets. Network-connected models feature an LCD display and LEDs to indicate status on communication connectors. Managed models contain LEDs to indicate outlet status. Most rackmount PDUs have attached power cords and circuit breakers.

Asset management

Keeping track of software and hardware assets in your environment is a pre-requisite for effectively managing cybersecurity. Eaton recommends that you maintain an asset inventory that uniquely identifies each important component. To facilitate this, the PDU Network module supports the following identifying information:

The previous information could be accessed through the LCD display:



This information is accessible through the next interfaces detailed in the indicated User Guide chapter of the product:

- Chapter 7: Serial interface
- Chapter 8: Web interface including SNMP agent

Risk assessment

Eaton recommends conducting a risk assessment to identify and assess reasonably foreseeable internal and external risks to the confidentiality, availability and integrity of the system device and its environment. This exercise should be conducted in accordance with applicable technical and regulatory frameworks such as IEC 62443 and NERC-CIP. The risk assessment should be repeated periodically.

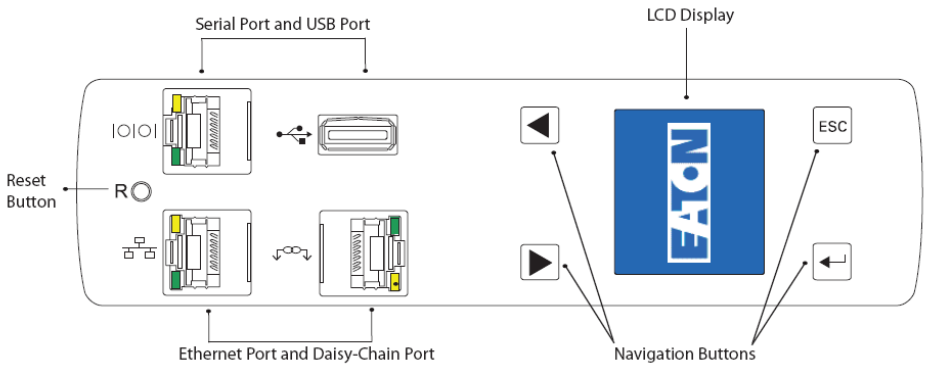
Physical security

An attacker with unauthorized physical access can cause serious disruption to system/device functionality. Additionally, Industrial Control Protocols don't offer cryptographic protections, making ICS and SCADA communications especially vulnerable to threats to their confidentiality. Physical security is an important layer of defense in such cases. The PDU Network module is designed to be deployed and operated in a physically secure location. The following are best practices that Eaton recommends to physically secure your system/device:

- Secure the facility and equipment rooms or closets with access control mechanisms such as locks, entry card readers, guards, man traps, CCTV, etc. as appropriate.
- Restrict physical access to cabinets and/or enclosures containing the PDU Network module and the associated system. Always monitor and log access.
- Physical access to the telecommunication lines and network cabling should be restricted to protect against attempts to intercept or sabotage communications. It's a best practice to use metal conduits for the network cabling running between equipment cabinets.

The PDU Network module supports the following physical access ports: Serial, Ethernet, Daisy-Chain and USB ports. Access to these ports should be restricted.

- Do not connect removable media (e.g., USB devices, SD cards, etc.) for any operation (e.g., firmware upgrade, configuration change or boot application change) unless the origin of the media is known and trusted.
- Before connecting any portable device through a USB port or SD card slot, scan the device for malware and viruses.



Account management

Logical access to the system device should be restricted to legitimate users, who should only be assigned the privileges necessary to complete their job roles/functions. Some of the following best practices may need to be implemented by incorporating them into the organization's written policies:

- Ensure default credentials are changed upon first login. The PDU Network module should not be deployed in production environments with default credentials, as default credentials are publicly known.
- No account sharing – Each user should be provisioned a unique account instead of sharing accounts and passwords. Security monitoring/logging features in the product are designed based on each user having a unique account. Allowing users to share credentials weakens security.
- Restrict administrative privileges - Attackers seek to gain control of legitimate credentials, especially those for highly privileged accounts. Administrative privileges should be assigned only to accounts specifically designated for administrative duties and not for regular use.
- Leverage the roles/access privileges to provide tiered access to users as per the business /operational need. Follow the principle of least privilege (allocate the minimum authority level and access to system resources required for the role).
- Perform periodic account maintenance (remove unused accounts).
- Ensure password length, complexity and expiration requirements are appropriately set, particularly for all administrative accounts (e.g., minimum 10 characters, mix of upper- and lower-case and special characters and expire every 90 days, or otherwise in accordance with your organization's policies).
- Enforce session time-out after a period of inactivity.

The level of access privilege determines what the user will see and what actions the user can perform. For example, the level of access privilege determines which menu items the user can access, or which fields display on individual setting and configuration dialogs. Any menu or dialog functions that are not included in the access privilege set for a user do not display, or are they are grayed-out.

These accounts can be configured not only for individuals, but also for groups. All remote users and administrators belong to a remote group and their access privileges are defined from this group. Remote accounts also provide a way to attach LDAP users.

Three user roles can be assigned these access privilege levels: SuperUser administrator, local or remote administrators and PDU-User.

SuperUser administrator

There can be one SuperUser and up to eight standard local or remote administrators. Only one user can be the SuperUser administrator. This defaults to the local user, but a SuperUser should be assigned at first connection. This account is not accessible or editable by the standard administrators or PDU-users/outlet users. The SuperUser always has read-write privileges to view and edit all data, plus the following privileges restricted only to the SuperUser:

- Exclusive access to modify the SuperUser account settings
- Exclusive access to XML Web services
- Upgrade firmware

Local or remote administrator

Up to eight standard administrators (local or remote) can be assigned. Only accessible menu items display for the user according to the assigned permissions.

A local or remote administrator who is assigned read-write access can perform the following:

- Access to up to date PDU data and measurements
- Create, modify or disable an administrator or user account except for the SuperUser
- Configure e-mail recipient addresses for e-mail notification to users
- Restart the communications module
- Access to both the Serial interface and the Web interface (some restrictions apply)
- Access to all menus on the Web interface
- Access to retrieved PDU up to date data and measurements
- Clear logs

A local or remote administrator with read-only access has limited privileges, including:

- Access to up to date PDU data and measurements
- Has the authority to change the password, but not the login (Remote PDU-users cannot change the login or password)
- Access to the Network and Date and Time Settings menu (some restrictions apply)
- Access to both the Serial interface and the Web interface
- Can access the log and notifications submenu, but cannot clear the logs data
- Cannot configure the TCP/IP, SNMP Global Security, and LDAP settings

An administrator with no access is not authorized to access to the Web page.

PDU-User

A local or remote PDU-User with read-write access has limited privileges, including:

- Cannot access the following menus: Devices, Syslog, Network (TCP/IP, SNMP, EnergyWise, Global security, LDAP, and RADIUS)
- Has the authority to change the password, e-mail address and login (Remote PDU-Users cannot change the login or password but can change their own e-mail address)
- Only accessible menu items display for the user according to the assigned permissions

A PDU-User with read-only access has limited privileges, including:

- Access to up to date PDU data and measurements
- Access to both the Serial interface and the Web interface (some restrictions apply)
- Access to the log and notifications submenu, but cannot clear the data from logs
- No access to the TCP/IP, SNMP, Global Security and LDAP settings
- Cannot upload the communication module configuration file or upgrade the firmware
- Cannot change his profile or another user's account

A PDU-User with read-only access has limited privileges, including:

- Access to up to date PDU data and measurements
- Access to both the Serial interface and the Web interface (some restrictions apply)
- Access to the log and notifications submenu, but cannot clear the data from logs
- No access to the TCP/IP, SNMP, Global Security and LDAP settings
- Cannot upload the communication module configuration file or upgrade the firmware
- Cannot change his profile or another user's account

A PDU-User with no access privileges is not authorized to access to the Web page.

Session management

The following session management restrictions apply:

- There can only be one SuperUser with read-write access rights and up to eight multi-users with configurable access rights.
- When the administrator connects, any existing read-write sessions are closed. The other user (or users) will be asked to authenticate and open a new read-only session.
- If a user with read-write access is logged in and another user with read-write access wants to log in, the following message displays: "Another user is logged in with R/W access. Continue as R/O?".

PDU sessions are also limited in the following ways:

- Only five standard sessions without SSL (Secure Sockets Layer) or SSH (Secure Shell) sockets are allowed.
- Only two secure sessions can be running at the same time.
- Only an administrator can have two simultaneous sessions open in HTTP/HTTPS (Hypertext Transfer Protocol / Hypertext Transfer Protocol Secure), Telnet/SSH.

During an HTTP/HTTPS or Telnet/SSH session, the session times out if there is no activity for five minutes. After a session times out, you must login again.

The Lightweight Directory Access Protocol (LDAP) allows the sharing of information about users over an Internet Protocol (IP) network. A password must be set to authenticate one user with a LDAP directory.

The eNMC card proposes two ways to encrypt LDAP connections with SSL/TLS:

- LDAPS encryption method
- Start TLS encryption method

Using a Simple Authentication and Security Layer (SASL) Digest MD5 mechanism to authenticate the user. A Certificate Authority can be uploaded by the Web interface of the eNMC card to validate the identity of the LDAP client.

The Remote Authentication Dial-In User Service (RADIUS) centralizes authentication, authorization and accounting management for users who connect to the eNMC card. The client and RADIUS server are authenticated through a shared secret string. The RADIUS server checks that the information is correct using authentication schemes such as Password Authentication Protocol (PAP) or Challenge-Handshake Authentication protocol (CHAP).

The Simple Network Management Protocol (SNMP) is an internet standard protocol for collecting and organizing information about devices over IP network. Use SNMPv3 to get security features:

- Confidentiality – Encryption of packets to prevent snooping by an unauthorized source
- Integrity – Message integrity to ensure that a packet has not been tampered while in transit including an optional packet replay protection mechanism
- Authentication – Verify that the message is from a valid source

For that, configure an authentication password and privacy key.

Time synchronization

Many operations in power grids and IT networks heavily depend on precise timing information. Ensure the system clock is synchronized with an authoritative time source (using manual configuration, NTP, SNTP, or IEEE 1588).

The Time Sync features and configuration is detailed in the Date & Time paragraph in Chapter 8 of the Product User Guide.

Network security

The PDU Network module supports network communication with other devices in the environment. This capability can present risks if it's not configured securely. The following are Eaton recommended best practices to help secure the network. Additional information about various network protection strategies is available in Eaton Cybersecurity Considerations for Electrical Distribution Systems [R1].

Eaton recommends segmentation of networks into logical enclaves, denying traffic between segments except that which is specifically allowed, and restricting communication to host-to-host paths (for example, using router ACLs and firewall rules). This helps to protect sensitive information and critical services and creates additional barriers in the event of a network perimeter breach. At a minimum, a utility Industrial Control Systems network should be segmented into a three-tiered architecture (as recommended by NIST SP 800-82 [R3]) for better security control.

Communication protection: the PDU Network module provides the option to encrypt its network communications. Please ensure that encryption options are enabled. You can secure the product's communication capabilities by taking the following steps:

Protocol	**Default state**	**Port number** (configurable)
FTP	Disable	21
FTPS	Enable	21
SSH	Enable	22
TELNET	Disable	23
HTTP (Basic and MD5 message-digest)	Enable	80
HTTPS (TLSv1.2)	Disable	443
Serial port – Command Line Interface	Enable	N/A
USB port	Enable	N/A
SNMPv1	Disable	161,162 (Trap)
SNMPv3	Disable	161,162 (Trap)

The following client protocol and features may be enabled or disabled:

Protocol	**Default state**	**Port number** (configurable)
DHCP	Enable	68
DNS	Enable	53
Email/SMTP	Disable	25
LDAP	Disable	389
RADIUS	Disable	1812 (UDP)
SNTP	Disable	123
Syslog	Disable	514 (UDP)
TFTP	Enable	69 (UDP)
EATON scan port	Enable	4679 (UDP)
EATON alarm port	Enable	4680 (UDP)

For secure Web communication with the PDU Network Module, the Secure Sockets Layer (SSL) must be enabled by selecting HTTPS as the protocol mode to use for access to the Web interface. The activation of the HTTPS limits the Daisy Chain capability and the simultaneous open sessions. The maximum number of Daisy Chain PDU is limited to 1 + 3 with 2 open HTTPS sessions. For more details about the configuration of the previous protocol, please refer to the User Guide.

The PDU Network module is currently hardcoded with a self-signed server certificate and its private key. The user can import their own SSL certificate and private key.

Certificate expiration will not be managed by the SCOB FW:

- No logs generated nor email alerts sent to warn about certificate expiration
- Even expired, the certificate will still be exposed by SCOB until the customer import a new certificate
- The content of the certificate is not checked, the user must ensure that its certificate is supported by SCOB firmware before importing it

Only 1024 and 2048 bit key length are supported and following ciphers:

- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256

Eaton recommends opening only those ports that are required for operations and protect the network communication using network protection systems like firewalls and intrusion detection systems/intrusion prevention systems. Use the information below to configure your firewall rules to allow access needed for the PDU Network module to operate smoothly.

Remote access

Remote access to devices/systems creates another entry point into the network. Strict management and validation of termination of such access is vital for maintaining control over overall ICS (Industrial Control System) security.

The remote access capabilities, permissions and secure configuration are described in the account management section. The remote access security recommendations are described in the security paragraph in Chapter 8 of the User Guide.

The session timeout settings are set to 5 minutes without activity and 15 minutes regardless of the activity. The remote sessions and all activities are logged for the following items: IP address, timestamp, user name and protocol.

Logging and event management

Eaton recommends logging all relevant system and application events, including all administrative and maintenance activities. Logs should be protected from tampering and other risks to their integrity (for example, by restricting permissions to access and modify logs, transmitting logs to a security information and event management system, etc.).

Review logs regularly and ensure that logs are retained for a reasonable and appropriate length of time. The frequency of review should be reasonable, considering the sensitivity and criticality of the system/device and any data it processes.

The logs/syslog management is described in the Logs and Syslog paragraph in Chapter 8 of the User Guide.

Vulnerability scanning

It is possible to install and use third-party software with the PDU Network module. Any known critical or high severity vulnerabilities on third-party component/libraries used to run software/applications should be remediated before putting the device/system into production.

Eaton recommends running a vulnerability scan to identify known vulnerabilities for software used with the product. For COTS components (e.g., applications running on Windows), vulnerabilities can be tracked on the **National Vulnerability Database (NVD).**

Keep software updated by monitoring security patches made available by COTS vendors and installing them as soon as possible. Many compliance frameworks and security best practices require a monthly vulnerability review. For many non-COTS products vulnerabilities will be communicated directly through the vendor site.

Malware defenses

Eaton recommends deploying adequate malware defenses to protect the product or the platforms used to run the Eaton product.

Secure maintenance

The device includes a RS232 and display to allow a service engineer, with help from the site administrator, to troubleshoot the device functionality. This interface allows service engineers to perform the following tasks:

- RS232
  - Restore the default password
  - Reset the default settings
  - Any configurations

- Display
  - Reset to default settings (exclude the Super Admin password)
  - Network settings (TCP/IP)
  - Daisy Chain settings

Enabling of the USB port is provided for commissioning purposes only and shall not be left enabled. If the USB port is left enabled on purpose, it is recommended to protect against unauthorized access by enabling the LCD pin code protection.

Update device firmware prior to putting the device into production. Thereafter, apply firmware updates and software patches regularly.

Eaton publishes patches and updates for its products to protect them against vulnerabilities that are discovered. Eaton encourages customers to maintain a consistent process to promptly monitor for and install new firmware updates. There is no process for acquiring, verifying and updating firmware, updates, patches and software. Eaton contact information is indicated in the Service and Support chapter in the User Guide. Please refer to Eaton's **Cybersecurity** website for information bulletins about available firmware and software updates.

Business continuity/Cybersecurity disaster recovery

Eaton recommends incorporating the PDU Network module into the organization's business continuity and disaster recovery plans. Organizations should establish business continuity and disaster recovery plans and periodically review, and where possible, exercise these plans. As part of the plan, important system/device data should be backed up and securely stored, including:

- Updated firmware for the PDU Network module. Make it a part of standard operating procedure to update the backup copy as soon as the latest firmware is updated
- The current configuration
- Documentation of the current permissions / access controls, if not backed up as part of the configuration

The following describes the details of failure states and backup functions:

- The failed states are detailed in the Ports, Operation Buttons and LED Status Indicators paragraph in the User guide
- Describe communication and power status indicators referred to "Serial Interface Operation" and "Web Interface Operation" detailed in chapter 7 of the User Guide
- The configuration of backup and recovery are described in the Maintenance and Alarms chapter in the User Guide and detail the following parts: UCF file (G3 PDU topology description file) and configuration files

Sensitive information disclosure

Eaton recommends that sensitive information (i.e., connectivity, log data and personal information) that may be stored by the PDU Network module be adequately protected through the deployment of organizational security practices. The following sensitive information can be stored by the PDU Network module: user name/password, email address and SNMP user name/password.

Decommissioning or zeroization

It is a best practice to purge data before disposing of any device containing data. Guidelines for decommissioning are provided in NIST SP 800-88. Eaton recommends that products containing embedded flash memory be securely destroyed to ensure data is unrecoverable.

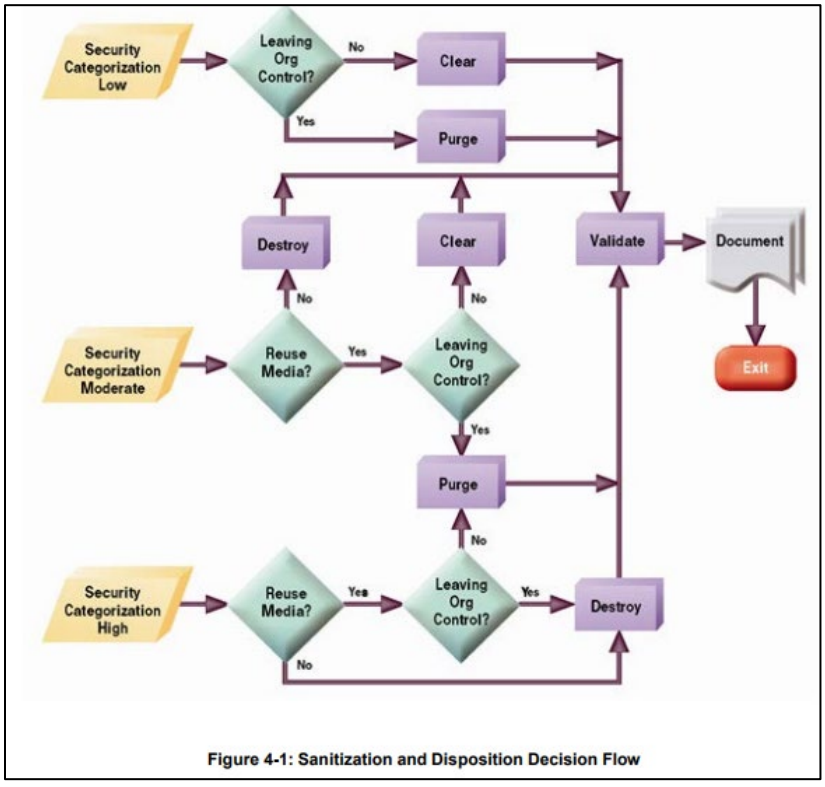


Figure 4-1: Sanitization and Disposition Decision Flow

* Figure and data from NIST SP800-88

Eaton recommends the following methods for disposing of motherboards, peripheral cards such as network adapters, or any other adapter containing non-volatile flash memory.

- Clear: If supported by the device, reset the state to original factory settings. The reset process is described in the Maintenance and Alarms Chapter in the User Guide.
- Purge: If the flash memory can be easily identified and removed from the board, the flash memory may be destroyed independently of the board that contained the flash memory. Otherwise, the whole board should be destroyed.
- Destroy: Shred, disintegrate, pulverize, or Incinerate by burning the device in a licensed incinerator.

References

- [R1] **Cybersecurity considerations for electrical distribution systems**
- [R2] **Cybersecurity best practices checklist reminder**
- [R3] **NIST SP 800-82 Rev 2, Guide to Industrial Control Systems (ICS) Security, May 2015**
- [R4] **National Institute of Technology (NIST) Interagency "Guidelines on Firewalls and Firewall Policy, NIST Special Publication 800-41", October 2009**
- [R5] **NIST SP 800-88, Guidelines for Media Sanitization, September 2006**
- [R6] **A Summary of Cybersecurity Best Practices - Homeland Security**

Powering Business Worldwide

1000 Eaton Boulevard
Cleveland, OH 44122
United States
Eaton.com

MN155001EN
August 2022