EATON PRODUCT SECURE CONFIGURATION GUIDELINES

Documentation to securely deploy and configure Eaton products

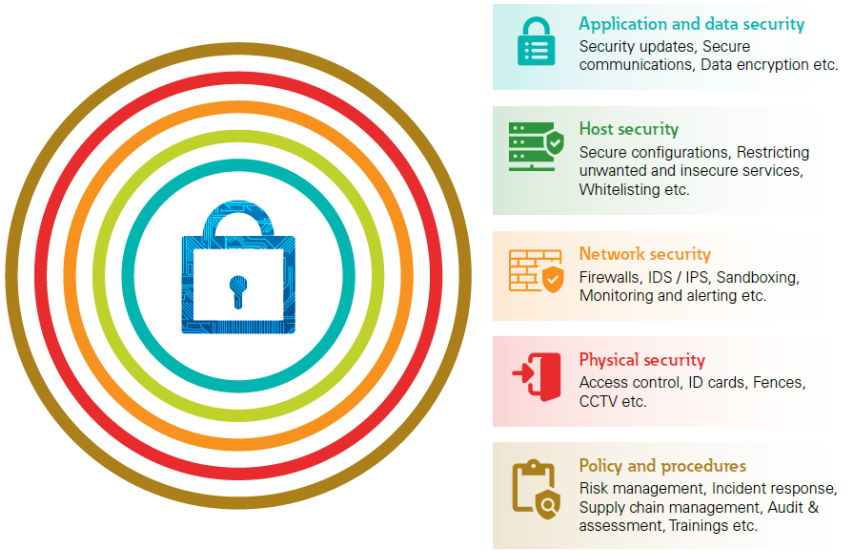
PXPM has been designed with cybersecurity as an important consideration. A number of features are offered in the product to address cybersecurity risks. These Cybersecurity Recommendations provide information to help users to deploy and maintain the product in a manner that minimizes the cybersecurity risks. These Cybersecurity 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, competitive for customers.

INSTRUCTIONS FOR FILLING THIS DOCUMENT –

- This document contains a master list of items that need to be part of a secure configuration document for a particular product.
- Please edit the content in RED to make the document product specific.
- Also, you can remove any sections/links/content that may not be applicable to your product.
- Finally this document needs to be part of your product manual that goes to your customers.

Category	Description
[1] Intended Use & Deployment Context	Power Xpert Protection Manager is a Microsoft Windows-based software that configures, controls and tests Eaton PXR trip units. For PXPM software, build is shared in form of installer which customer installs on their machine through either upgrade or fresh installation.
[2] 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, **PXPM** supports the following identifying information: • PXPM Software Current Release Information: Publisher: Eaton Corporation, Name: Power Xpert Protection Manager, Version: 22.09.1, Version date: 30th Sept, 2022. • For PXPM current version information, user can go to PXPM Homepage->Application Settings->About section. • Customer can get latest version information either from www.eaton.com/pxpm or at PXPM application launch itself new features added will be displayed on popup if any new version available. • Customer should maintain inventory details for PXPM versions, latest version information can be obtained from www.eaton.com/pxpm. • More information related to saving inventory can be obtained from PXPM quick start guide. • Information is maintained for all previous releases along with release notes and is shared. • The detailed information is available in the file 'PXPM Quick Start Guide – Eatonized' which can be accessed on the path below: "C:\Program Files (x86)\Eaton Corporation\Power Xpert Protection Manager" • The latest Quick start guide can be downloaded from www.eaton.com/pxpm
[3] Defense in Depth	Defense in Depth basically means applying multiple counter-measures for mitigating risks, in a layered or step wise manner. A layered approach to security as shown in the below diagram is what is recommended. Defense in Depth is the responsibility of both the manufacturer and the customer.

Category	Description
	 Application and data security: • Use of encryption to mask sensitive data (License key, settings file). • Password protection for updating device settings. • Application and device side data validation to prevent incorrect device configuration.
[4] 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.
[5] 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. **PXPM** is designed to be deployed and operated in a physically secure location. Following are some 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 **PXPM** and the associated system. Monitor and log the access at all times.

Category	Description
	• 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. • 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. • Assets should be secured from any unauthorized access and manipulation to the asset/devices that are used by PXPM.
[6] COTS Platform Security	Eaton recommends that customers harden third-party commercial off-the-shelf (COTS) operating systems or platforms that are used to run Eaton applications / products (e.g., third party hardware, operating systems and hypervisors, such as those made available by Dell, Microsoft, VMware, Cisco, etc.). • Eaton recommends that customers refer to the COTS vendor's documentation for guidance on how to harden these components. • Vendor-neutral guidance is made available by the Center for Internet Security https://www.cisecurity.org/ Irrespective of the platform, customers should consider the following best practices: • Install all security updates made available by the COTS manufacturer. • Change default credentials upon first login. • Disable or lock unused built-in accounts. • Limit use of privileged generic accounts (e.g., disable interactive login). • Change default SNMP community strings. • Restrict SNMP access using access control lists. • Disable unneeded ports & services. NA
[7] Account Management	Logical access to the system | device should be restricted to legitimate users, who should be assigned only 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:

Category	Description
	• Ensure default credentials are changed upon first login PXPMshould 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 the 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. NA
[8] 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). • PXPM shows date time data received from connected device through serial port communication. Through application, synchronizing device date time with system date time is possible. From PXPM homepage->Device Settings->Date and Time->Update Trip Unit Date time. For more information refer section '3.2' from PXPM Quick start guide • The detailed information is available in the file 'Power Xpert Protection Manager Quick Start Guide.pdf' which can be accessed from PXPM installed directory • The latest Quick start guide can also be downloaded from www.eaton.com/pxpm
[9] Network Security	Device_Name supports network communication with other devices in the environment. This capability can present risks if it's not configured securely. Following are Eaton recommended best practices to help secure the network. Additional information about various network protection strategies

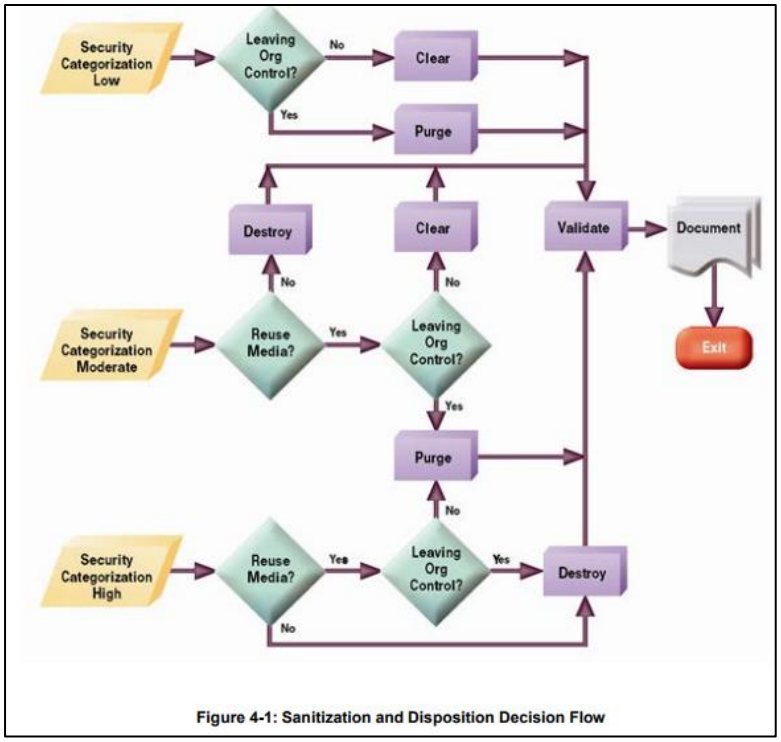
Category	Description
	is available in *Eaton Cybersecurity Considerations for Electrical Distribution Systems [R1]*. Eaton recommends segmentation of networks into logical enclaves, denying traffic between segments except that which is specifically allowed, and restricting communication to host-to-host 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. 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 Device Name to operate smoothly. NA
[10] 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 security. NA
[11] 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.). • Ensure that logs are retained for a reasonable and appropriate length of time. • Review the logs regularly. The frequency of review should be reasonable, taking into account the sensitivity and criticality of the system | device and any data it processes. • PXPM application Logs: Logs are generated for errors and events. • For errors additional information is added to the logs. • User can access error log file installed directory.
[12] Vulnerability Scanning	It is possible to install and use third-party software with **PXPM**. 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.

Category	Description
	• 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), available at https://nvd.nist.gov/. • Keep software updated by monitoring security patches made available by COTS vendors and installing them as soon as possible. *Note: 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.* NA
[13] Segmentation & Isolation	Privilege separation with boundary controls is important to improving security of systems. Logical and physical isolation techniques should be used to separate processors, vehicle networks, and external connections as appropriate to limit and control pathways from external threat vectors to cyber-physical features of vehicles. Strong boundary controls, such as strict whitelist-based filtering of message flows between different segments, should be used to secure interfaces. NA
[14] Critical Safety Communications	Critical safety messages are those that could directly or indirectly impact a safety-critical vehicle control system's operation. When possible, sending safety signals as messages on common data buses should be avoided. For example, providing an ECU with dedicated inputs from critical sensors eliminates the common data bus spoofing problem. If critical safety information must be passed across a communication bus, this information should reside on communication buses segmented from any vehicle ECUs with external network interfaces. A segmented communications bus may also mitigate the potential effects of interfacing insecure aftermarket devices to vehicle networks. Critical safety messages, particularly those passed across non-segmented communication buses, should employ a message authentication scheme to limit the possibility of message spoofing. NA
[15] Malware Defenses	Eaton recommends deploying adequate malware defenses to protect the product or the platforms used to run the Eaton product.

Category	Description
[16] Secure Maintenance	**Best Practices** Update PXPM software regularly and maintain latest version. 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 software updates. User can download latest version of PXPM software from www.eaton.com/pxpm website. Steps for installing/updating/verifying the PXPM software: • After downloading PXPM installer from above mentioned website, user can run the installer. If user upgrades to latest version, then user will get a popup stating it is an upgrade to existing software. For fresh installation no upgrade popup will appear. • Installation of drivers and required framework will happen automatically if required, after that, user needs to accept the agreement and then software will be installed. • For any PXPM support, please find below Eaton contact information: Americas: trc@eaton.com China: TechCareCPCD@eaton.com Other: trc@eaton.com Please check Eaton's cybersecurity website for information bulletins about available software updates, contact information Please visit: www.eaton.com/pxpm
[17] Business Continuity / Cybersecurity Disaster Recovery	**Plan for Business Continuity / Cybersecurity Disaster Recovery** Eaton recommends incorporating **PXPM** into the organization's business continuity and disaster recovery plans. Organizations should establish a Business Continuity Plan and a Disaster Recovery Plan and should 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: • Update to latest version for **PXPM**. Make it a part of standard operating procedure to update the backup copy as soon as the latest PXPM version is updated. • The current configuration. • Documentation of the current permissions / access controls, if not backed up as part of the configuration. • Customer to save device configuration file if required from PXPM application, in case customer goes for device firmware upgrade.

Category	Description
	• Configuration of backup and recovery: From PXPM application, User can save backup of device configuration settings before exporting/writing new setpoints from 'PXPM Setpoint screen' by choosing either 'Save As' or 'Export'->Save backup file. • A user can restore the trip unit to the settings from a previously saved backup file. Go to PXPM Homepage->Setpoint Configuration->Click Export to Unit and choose the desired file. This will export the setpoints from the selected file into the trip unit. For more information related to backup and restoring device setpoint configurations, refer section '2.4' from PXPM Quick start guide. • The detailed information is available in the file 'Power Xpert Protection Manager Quick Start Guide.pdf' which can be accessed from the installed directory. • The latest Quick start guide can be downloaded from www.eaton.com/pxpm
[18] Customer Application Security	**PXPM** provides a platform on which customers can customize and host applications according to their requirements. Security vulnerabilities in these applications may expose the underlying device to attack. Eaton recommends observing best practices for secure system development when customers develop and host an application on the device: • Privacy and Security by Design: The application should take security and privacy into consideration from the outset, including at the stage of defining requirements and assessing the associated risks. • Communication Protection: If the application communicates over the network, Eaton recommends encrypting the communications in accordance with the applicable level described by the FIPS 140-2 standard. • Access Enforcement: The application should provide the ability to enforce access controls to protect the application against unauthorized access and to protect accounts against unauthorized authentication attempts (for example, through account lockout). • Least Privilege: Any application developed by the customers should not run with root account privileges. The root account has full control over and access to the operating system. Therefore, if an application that requires root privileges has any security vulnerability, it endangers the entire system. • Input Checking: All input to the application should be sanitized before storing and processing by the application to protect against malicious code injection. • Output Handling: Data output by the application for user consumption, including error messages, should be appropriately handled to avoid revealing important information about the application and the underlying system.

Category	Description
	• Password Management: The application should securely store and transmit credentials (for example, encrypting authentication traffic, and salting and hashing passwords in transit and at rest). Password complexity should be implemented, and password should be masked when entered on-screen. • Secure Coding Practices: Follow secure coding practice while developing applications for the device (for example, implementing multiple security layers, verifying authorization for all requests, conducting code reviews, etc.). • Administration Interface: The interface for administering the application should be separated from the end-user interface. • Session Controls: All application sessions should be encrypted, logged and monitored. • Event Log Generation: The application should have the capability to log security related events at a minimum, including the time, date, and user. NA
[19] Sensitive Information Disclosure	Eaton recommends that sensitive information (i.e. connectivity, log data, personal information) that may be stored by **PXPM** be adequately protected through the deployment of organizational security practices. NA
[20] 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.

Category	Description
	 Figure 4-1: Sanitization and Disposition Decision Flow ** Figure and data from NIST SP800-88* • User is recommended to clear/delete all the PXPM software related data by uninstalling the application 'Power Xpert Protection Manager' from control panel. Also remove 'Power Xpert Protection Manager' folder from installed path.

References

[R1] Cybersecurity Considerations for Electrical Distribution Systems (WP152002EN):
http://www.eaton.com/ecm/groups/public/@pub/@eaton/@corp/documents/content/pct_1603172.pdf

[R2] Cybersecurity Best Practices Checklist Reminder (WP910003EN):
https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/white-papers/WP910003EN.pdf

[R3] NIST SP 800-82 Rev 2, Guide to Industrial Control Systems (ICS) Security, May 2015:
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

[R4] National Institute of Technology (NIST) Interagency "Guidelines on Firewalls and Firewall Policy, NIST Special Publication 800-41", October 2009: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf

[R5] NIST SP 800-88, Guidelines for Media Sanitization, September 2006:
http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=50819

[R6] A Summary of Cybersecurity Best Practices - Homeland Security
https://www.hsdl.org/?view&did=806518

[R7] Cybersecurity Best Practices for Modern Vehicles - NHTSA
https://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf

[R8] Characterization of Potential Security Threats in Modern Automobiles - NHTSA
https://www.nhtsa.gov/DOT/NHTSA/NVS/Crash%20Avoidance/Technical%20Publications/2014/812074_Characterization_PotentialThreatsAutos(1).pdf

[R9] Threat Modeling for Automotive Security Analysis
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf