EATON PRODUCT SECURE CONFIGURATION GUIDELINES

Documentation to securely deploy and configure Eaton products

Intelligent Power Protector 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 and competitive for customers.

The following whitepapers are available for more information on general cybersecurity best practices and guidelines:

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

Cybersecurity Best Practices Checklist Reminder (WP910003EN):
http://www.cooperindustries.com/content/dam/public/powersystems/resources/library/1100_EAS/WP910003EN.pdf

Category	Description
Intended Use & Deployment Context	Intelligent Power Protector is protection software offered from Eaton Corporation at 'no charge'. It enables users to avoid data loss by gracefully shutting down computers and servers powered by an Eaton UPS in the event of an extended power outage. This software provides a clear, easy-to-use, multilingual interface from any PC with an Internet browser. Intelligent Power Protector acquires UPS information through local or network communication and can be easily deployed on many computers. Intelligent Power Protector can be remotely managed, configured and updated with our Intelligent Power Manager supervisory software.
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, **Intelligent Power Protector** supports the following identifying information: Name, Target Operating System, Version. Once deployed, **Intelligent Power Protector** asset information are available in the "System" panel. This information includes Software name and version details.
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.

Category	Description
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. **Intelligent Power Protector** 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 **Intelligent Power Protector** and the associated system. Monitor and log the access at all times. • 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. • **Intelligent Power Protector** supports of physical access ports will depends of the computer hosting it. 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.

Category	Description
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.

Category	Description
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: • Ensure default credentials are changed upon first login. **Intelligent Power Protector** 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 "Admin" or "User" 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. **Intelligent Power Protector** allows to manage several local user accounts with two profiles "Admin" (view and configuration) and "User" (view only). The admin account is preconfigured. It is built in the deployment package and will be asked to change its default password at first connection prior any other action. Administrators can manage users, including adding new users or change their roles. The default password shall have at least 8 characters and one digit and one special character. Sessions expire after 15 minutes of inactivity.

Category	Description
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). Please refers to the host operating system manual to manage the system clock properly.

Network Security	**Intelligent Power Protector** 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 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: **Intelligent Power Protector** 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: • Replace the Self Signed Web Server SSL Certificate by a Certificate signed by a Certificate Authority. The private and public certificates have to be placed in <IPP folder>/bin. The private key file name is "key.pem" and the public key is "cert.pem". • **Intelligent Power Protector** uses encrypted communication when possible. All incoming communications (HTTPS) are secured. Incoming HTTP connection stay open to redirect to HTTPS. Only TLS 1.2 and upper with secured recent ciphers are allowed. • Outcoming communications are secured by default when possible. **Intelligent Power Protector** always try to establish the most secure channel with external devices but could lower security constraints to fit to device capabilities or configuration. • Eaton recommends referring to device specific secured configuration guidance to allow IPM to connect the safest way. • When many protocols are supported by external devices, Eaton recommends using the strongest available, with strongest configuration. For example, When SNMPv1 and SNMPv3 are both available, prefer using SNMPv3 with most secured hash and encryption methods like SHA over MD5 and AES over DES. • **Intelligent Power Protector** web server generates and uses a self-generated RSA-2048 bit key and SHA-512 self-signed certificate. 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. By default, **Intelligent Power Protector** is configured to operate smoothly with the host operating system and the device protocols it has to operate with.

Category	Description
	List of network services protocols, port and direction used by **Intelligent Power Protector:** • *SMTP TCP/25 OUT* • *TFTP UDP/69 OUT* • *HTTP TCP/80 OUT* • *SNMP UDP/161 OUT* • *UNMP UDP/200 IN/OUT* • *HTTPS TCP/443 OUT* • ***Eaton Supervision TCP/4679 IN/OUT*** • *Eaton Notification Broadcast UDP/4679 IN/OUT* • ***Eaton SSL Supervision TCP/4680 IN/OUT*** • *Eaton Alarms Broadcast UDP/4680 IN* • *Eaton Connected Alarms TCP/5000 OUT* • *Eaton Connected Alarms TCP/5001 OUT* • *MQTTS TCP/8883 OUT* Protocols in bold are mandatory. Other protocols will depends on the network interface used to communicate with the device or on the additional required services (i.e. emails, shutdown controller, etc…).
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. **Intelligent Power Protector** can only be accessed through HTTP/HTTPS web server. The HTTP access is only allowed to redirect Web navigation to HTTPS and to provide remote discovery for remote supervision. The Web navigation and remote configuration are secured by HMAC-SHA password based authentication. All remote sessions and user system activities are logged in the application system log. The user session lifetime is 15 minutes by default.

Category	Description
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. System events logged in system logs are: • User login • System configuration change • Scan of new device • Test of action • Purge of system or event logs • Application execution detected errors The system logs can be exported and downloaded through a CSV file.
Vulnerability Scanning	It is possible to install and use third-party software with **Intelligent Power Protector**. 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), 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.*

Category	Description
Malware Defenses	Eaton recommends deploying adequate malware defenses to protect the product or the platforms used to run the Eaton product.
Secure Maintenance	**Best Practices** 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. Please check Eaton's cybersecurity website for information bulletins about available firmware and software updates. System panel provides "Automatic Update Settings" allowing to check and upgrade to new version in an easy way. Upgrade could also be triggered from Intelligent Power Manager.
Business Continuity / Cybersecurity Disaster Recovery	**Plan for Business Continuity / Cybersecurity Disaster Recovery** Eaton recommends incorporating **Intelligent Power Protector** 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: • Updated software for **Intelligent Power Protector**. 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 section describes the details of failures states and backup functions: • Software configuration is saved in "<application path>/configs/config.js" file. • Device list and events are stored in "<application path>/db/mc2.db"

Category	Description
Customer Application Security	**Intelligent Power Protector** 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. • 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.

Category	Description
Sensitive Information Disclosure	Eaton recommends that sensitive information (i.e. connectivity, log data, personal information) that may be stored by **Intelligent Power Protector** be adequately protected through the deployment of organizational security practices. **Intelligent Power Protector** stores sensitive information like connectivity credentials including passwords, logs or user details like contact information and emails.
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.

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):
http://www.cooperindustries.com/content/dam/public/powersystems/resources/library/1100_EAS/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