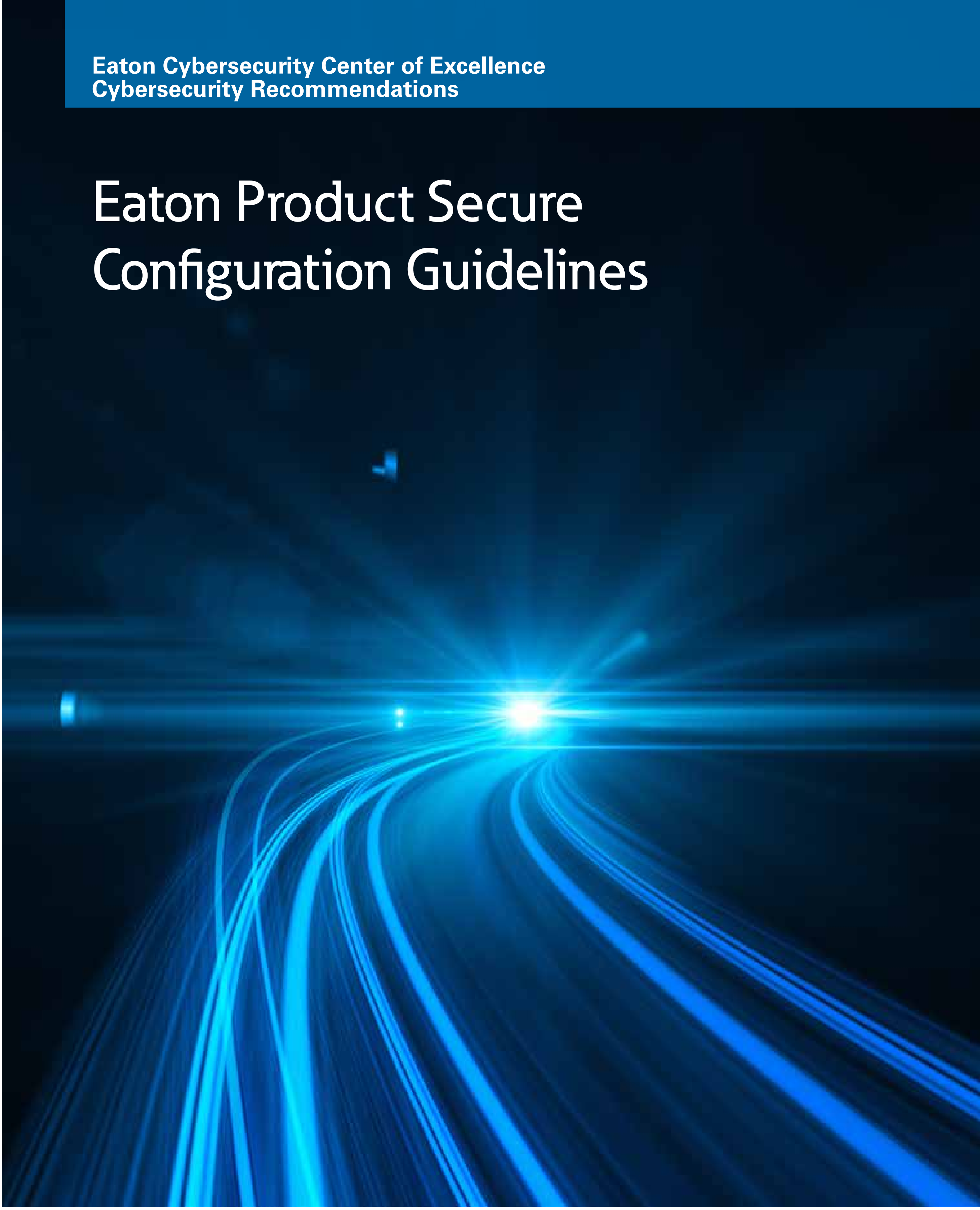
Eaton Cybersecurity Center of Excellence
Cybersecurity Recommendations

Eaton Product Secure Configuration Guidelines



Powering Business Worldwide

Documentation to securely deploy and configure Eaton products

Eaton Green Motion AC Home 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):

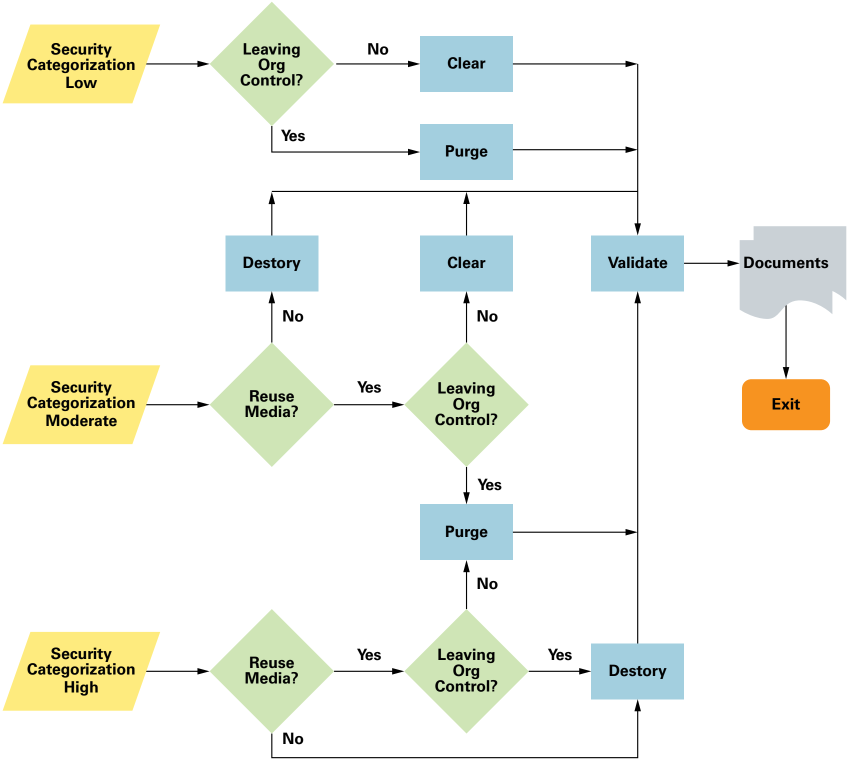
https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/white-papers/WP910003EN.pdf

Cybersecurity Best Practices for Modern Vehicles - NHTSA

https://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf

Category	Description
Intended Use & Deployment Context	This product shall be used to charge electric vehicles for private home users. Product is installed at customer premise and can be used in 1. Offline mode (no connection to internet) 2. Online mode (connected to internet / backend) More information on safe usage and installation of product is available at link: www.eaton.com/greenmotionhome
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, **Eaton Green Motion AC Home** supports the following identifying information: Product catalogue number, serial number, (available on product) Factory hotspot details, Unique device ID (leaflets provided with product, to be kept safe for future need). Refer installation manual for more information.
Physical Security	An attacker with unauthorized physical access can cause serious disruption to system/device functionality. Physical security is an important layer of defense in such cases. **Eaton Green Motion AC Home** 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. • 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. • **Eaton Green Motion AC Home** supports the following physical access ports: Ethernet, Serial Port, USB Port. Access to these ports should be restricted for un-authorized user. • Do not connect removable media (e.g., USB devices, SD cards, etc.)
Account Management	Logical access to the system | device should be restricted to legitimate users. Some of the following best practices may need to be implemented, 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: • Ensure default credentials are changed upon first login 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. • 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). - Password and account policies supported: - Hotspot, 16 characters, A-F and 0-9 and special characters Only accessible withing Wi-Fi range, timeout 30minutes, lockout system delay User should set a complex password on their home router Serial and SSH account are meant to be used only by Eaton technical support for debugging / troubleshooting purposes.
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). In online mode the time synchronization will occur automatically once the device gets access to OCPP Boot Notification and Heartbeat. In offline mode the time synchronization occurs when connected to the mobile app. All timestamps are with UTC time zone reference.

Category	Description
Network Security	**Eaton Green Motion AC Home** 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: **Eaton Green Motion AC Home** provides encryption of its network communications. This encryption is enabled by default. 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. In online mode charger connects with backend using OCPP protocol. In offline mode charger connects to mobile application via Wi-Fi.
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. • The remote access capabilities are provided by the Secure protocol OCPP over TLS 1.2. • The device pushes the activities logged under system logs to the backend via OCPP protocol. • Firmware updates are pushed to the devices from the backend via OCPP if the device is connected online. • For more information, please consult the Eaton Cybersecurity best practices [R2]
Logging and Event Management	• Charge statistics are available on mobile app for user to review. • Review the logs regularly. • For online charger's logs are available from Eaton Charging Network Manager (backend), for further details, please see product technical documentation or contact your local support team.
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 SSH local connection to allow a service engineer with help from site administrator to troubleshoot the device functionality. SSH port is disabled by default. This connection is only meant for service engineer. Customer is not supposed to use this functionality. **Note:** Enabling of TCP port 22 is provided for diagnostic purposes only and shall not be left enabled. **Best Practices** Update device firmware prior to deploying 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. Firmware updates shall be managed and installed exclusively through the Eaton Charging Network Manager, which ensures that you are using trusted firmware files. • For chargers in online mode (connected to Internet), EV charger will update automatically when an update is available. • For chargers in offline mode (not connected to Internet), mobile application will notify on availability and process to update. EV charger will not be available for usage during the time device is downloading and upgrading the firmware.

Category	Description
Decommissioning or Zeroization	It is a best practice to purge data before disposing of any device containing data. This includes sensitive information like credentials, logs, RFID information, etc. Flash memory can be erased by using factory reset functionality. Refer installation manual for more information.  Security Categorization Low Leaving Org Control? No Clear Yes Purge Destory Clear Validate Documents No No Exit Security Categorization Moderate Reuse Media? Yes Leaving Org Control? Yes Purge No Security Categorization High Reuse Media? Yes Leaving Org Control? Yes Destory No **Figure 1:** Sanitization and disposition decision flow * Figure and data from NIST SP800-88 The charging station will be recycled following process ISO9001. **Embedded Flash Memory on Boards and Devices** 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:** Reset the state to original factory settings by pressing and maintaining the reset button for at least 5 seconds. Refer to technical documentation for more details. **Purge:** The flash memory cannot be easily identified and removed from the board. For this reason, Eaton recommends destroying the whole computing board. **Destroy:** Shred, disintegrate, pulverize, or incinerate by burning the device in a licensed incinerator.

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

[R7] A Summary of Cybersecurity Best Practices - Homeland Security
https://www.hsdl.org/?view&did=806518

[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

Powering Business Worldwide

Eaton Industries Manufacturing GmbH
Place de la Gare 2
1345 Le Lieu, Switzerland

Publication No. MZ191002EN
September 2022

Follow us on social media to get the
latest product and support information.