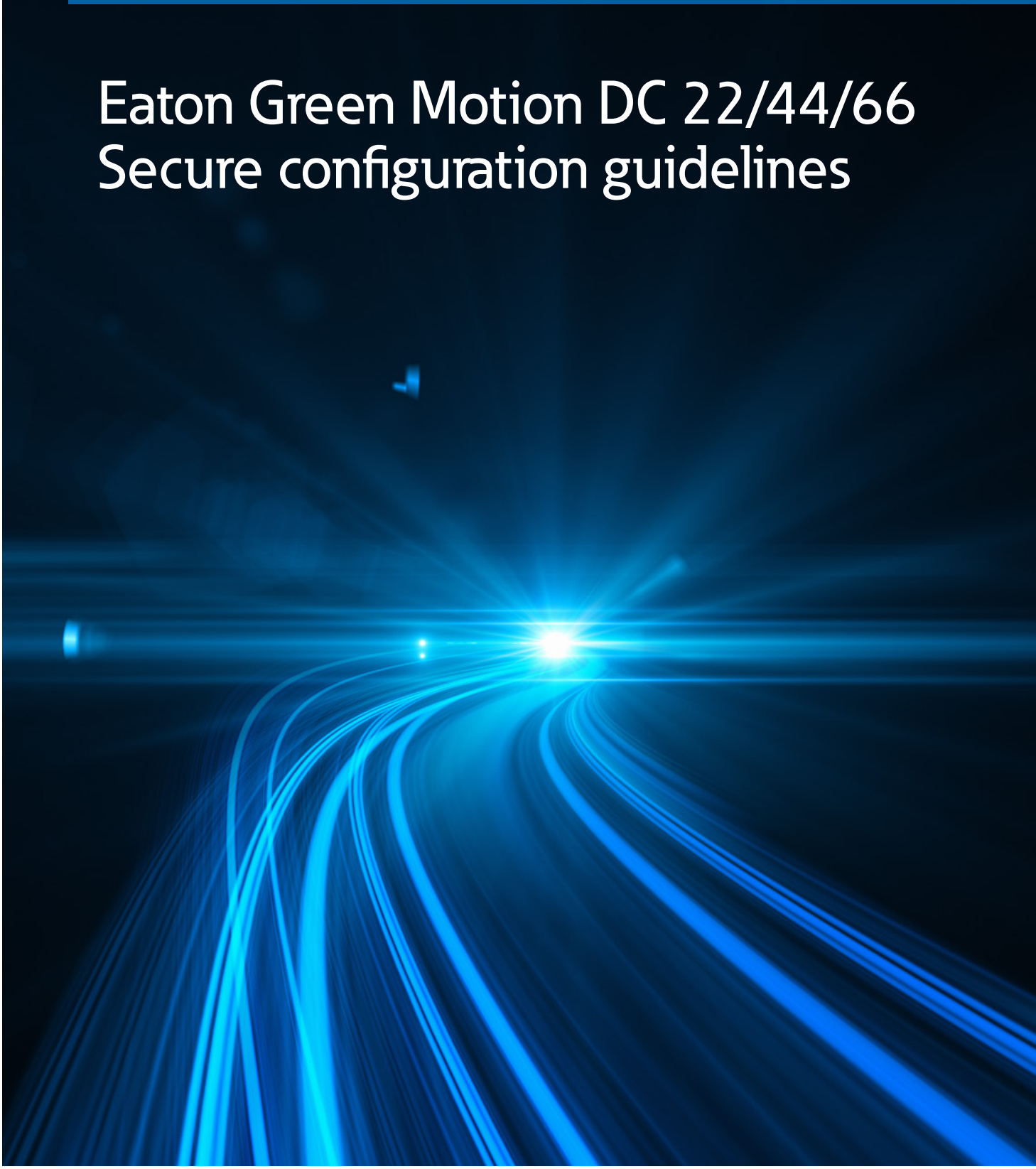
Eaton Cybersecurity Center of Excellence
Cybersecurity Recommendations

Eaton Green Motion DC 22/44/66 Secure configuration guidelines



Powering Business Worldwide

Documentation to securely deploy and configure Eaton products

Eaton Green Motion DC 22/44/66 EV chargers have 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):

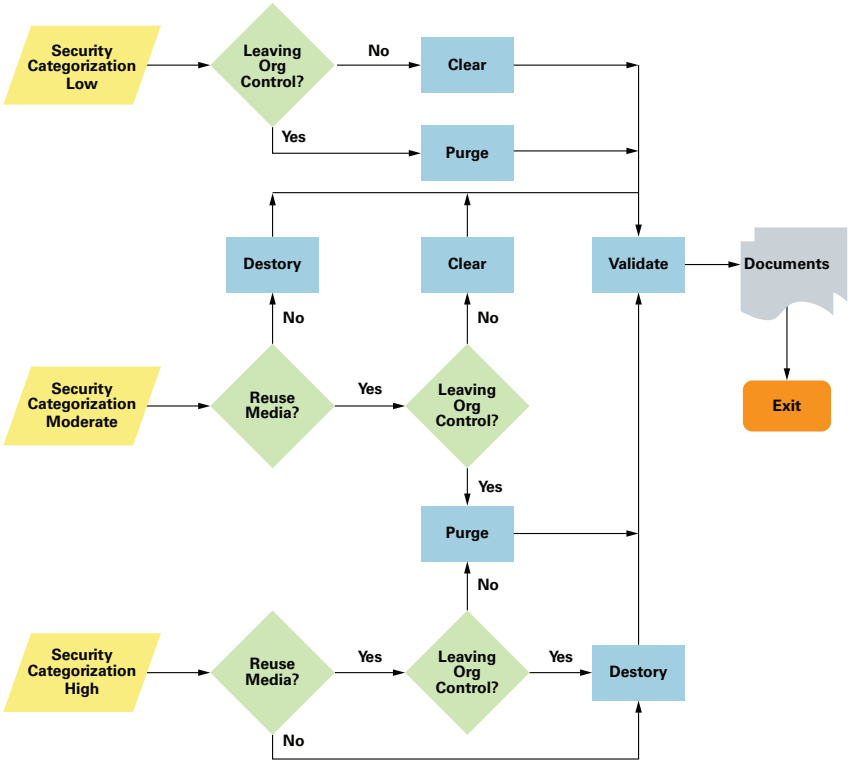
http://www.eaton.com/ecm/groups/public/@pub/@eaton/@corp/documents/content/pct_1603172.pdf

Cybersecurity Best Practices Checklist Reminder (WP910003EN):

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

Category	Description
Intended Use & Deployment Context	Deployed at customer premises in parking places, private or publicly accessible, to allow charging of EVs, authentication, billing, etc. For chargers installed in public locations, users are authenticated uniquely using RFID cards. The end user can use the HMI to set/retrieve information regarding type of charge, type of plug, usage statistics, etc. Please refer to the product user manual for more details.
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 DC 22/44/66** supports the following identifying information: Product catalogue number, serial number, (available on product). Refer installation manual for more information.
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 **Eaton Green Motion DC 22/44/66** and their 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. Physical security is an important layer of defense in such cases. **Eaton Green Motion DC 22/44/66** is designed to be deployed and operated in a physically secure location. Following are some of the best practices 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 is best practice to use metal conduits for the network cabling running between equipment cabinets. • **Eaton Green Motion DC 22/44/66** supports the following physical access ports: Ethernet, Serial Port, USB Port. Access to these ports should be restricted for un-authorized users. • 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). Serial and SSH accounts 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). The time synchronization will occur automatically once the device is connected online and gets access to OCPP Boot Notification and Heartbeat. All timestamps are with UTC time zone reference.
Network Security	**Eaton Green Motion DC 22/44/66** 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.

Category	Description
	Communication Protection: **Eaton Green Motion DC 22/44/66** provides encryption of its network communications. This encryption is enabled by default. Eaton recommends enabling 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, the charger connects with the backend using OCPP protocol via 4G connection or ethernet. It is recommended to use a sim card provided by Eaton. If the customer chooses to procure their own sim card, it is recommended to use 4G IoT sim cards from a Telecom service provider (TSP) which supports below "Recommended Security features". Recommended Security features To use a sim card which offers private Access Point Name (APN) while installing Green Motion DC 22/44/66 and commissioning the Charging Network Manager. It is strongly recommended to not use sim cards operating on public APN as they are not considered secure from cybersecurity risks. To Choose a utilize 4G SIM service providers that provide an option to encrypt the data communications using either a Virtual private network (VPN) or IPSec protection for 4G communication. Use a sim card which provides a feature to enable Universal integrated circuit card (UICC) pin to prevent unauthorized access to network. Use a sim card which provides security measures against theft and sim cloning. Do not use sim cards available over- the-counter which operate on public APN as those are not meant for IoT commercial products. **Note:** It is strongly recommended to not use sim cards operating on public APNs as they are not considered secure from cybersecurity risks.
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	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 engineers. Customer is not supposed to use this functionality. **Note:** 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 through Eaton Charging Network Manager, which ensures that you are using trusted firmware files, or through known third parties CNM (that will get trusted firmware files from Eaton) • For chargers in online mode (connected to Internet), EV charger will update automatically when an update is available. EV charger will not be available for usage during the time device is upgrading the firmware.

Category	Description
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. Flash memory can be erased by using factory reset functionality. Refer installation manual for more information.  **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 to destroy 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

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

Publication No. MZ192001EN
March 2023

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