

# EATON PRODUCT SECURE CONFIGURATION GUIDELINES





## Documentation to securely deploy and configure Eaton products

**ChargeLab site host dashboard and web-app (referred as ChargeLab dashboard and driver webapp in this document)** 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
<p><b>[1] Intended Use &amp; Deployment Context</b></p>	<p>The Eaton Charging Network Manager (“CNM”, operated by ChargeLab) site-host dashboard and user portal is a cloud-based interface through which site hosts (i.e., EV Charge Station owner/operators) can manage their EV charging infrastructure and the team members who have access to the system for the purpose of station access control, pricing management and vehicle management.</p> <p>Administrative users (<u>not</u> drivers) have password-controlled access to the portal.</p> <p>The CNM software is never deployed to a customer site.</p>
<p><b>[2] Asset Management</b></p>	<p>Keeping track of software and hardware assets in your environment is a prerequisite for effectively managing cybersecurity. Eaton recommends that you maintain an asset inventory that uniquely identifies each important component. To facilitate this, <b>CNM</b> supports the following identifying information:</p> <p>The CNM platform maintains connection to – and control over - EV charging stations deployed at customer sites. The EV charging stations are identified by their serial number and an internal identification number.</p> <p>Charge station information can be viewed by selecting the charge station through the portal.</p>
<p><b>[3] Defense in Depth</b></p>	<p>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.</p> <div data-bbox="625 1144 1096 1606" style="text-align: center;"> </div> <div data-bbox="1112 1102 1485 1648"> <ul style="list-style-type: none"> <li style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">  <b>Application and data security</b>              Security updates, Secure communications, Data encryption etc.         </li> <li style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">  <b>Host security</b>              Secure configurations, Restricting unwanted and insecure services, Whitelisting etc.         </li> <li style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">  <b>Network security</b>              Firewalls, IDS / IPS, Sandboxing, Monitoring and alerting etc.         </li> <li style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">  <b>Physical security</b>              Access control, ID cards, Fences, CCTV etc.         </li> <li style="border: 1px solid #ccc; padding: 5px;">  <b>Policy and procedures</b>              Risk management, Incident response, Supply chain management, Audit &amp; assessment, Trainings etc.         </li> </ul> </div>

<p><b>[4] Risk Assessment</b></p>	<p>Eaton and ChargeLab recommend that customers conduct a risk assessment to identify and assess reasonably foreseeable internal and external risks to the confidentiality, availability and integrity of the information contained in the customer account environment including checks on current named users and their access privileges. The risk assessment should be repeated periodically.</p>
<p><b>[7] Account Management</b></p>	<p>Logical access to the CNM 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:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• Perform periodic account maintenance (remove unused accounts).</li> </ul> <p>Access roles available to external dashboard users are Admin only. The CNM platform does not provide any type of role management which differentiates between functional access by user roles. Customers should exercise caution in the creation and management of user accounts.</p> <p>Users of the CNM platform are authenticated by the use of a One Time Password (OTP) delivered to the mobile phone number or email account of the named user. In this manner, shared access to accounts is discouraged but not eliminated entirely. It is the responsibility of customer administrator users to enable access only to named users with discrete (not shared) accounts.</p> <p>The CNM platform does not enforce an account expiration function whereby unused accounts are periodically removed. It is the responsibility of the customer to remove unused accounts.</p>
<p><b>[11] Logging and Event Management</b></p>	<p>The CNM platform logs all application events in a cloudtrail monitored via cloudwatch and SIEM. This information is not accessible to customers without assistance directly from ChargeLab.</p>
<p><b>[15] Malware Defenses</b></p>	<p>Eaton recommends deploying adequate malware defenses to protect the product or the platforms used to run the Eaton product.</p>

## References

[R1] Cybersecurity Considerations for Electrical Distribution Systems (WP152002EN):

[http://www.eaton.com/ecm/groups/public/@pub/@eaton/@corp/documents/content/pct\\_1603172.pdf](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](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](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](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>