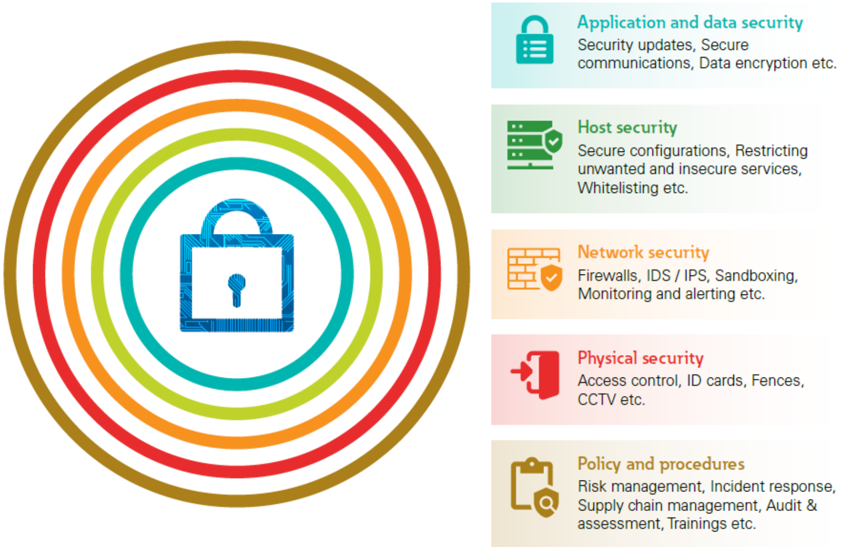
EN+ PRODUCT SECURE CONFIGURATION GUIDELINES

Documentation to securely deploy and configure EN+ products

AC Charger 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.

EN+ 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.

Category	Description
[1] Intended Use & Deployment Context	An EV charger is to keep the battery full for both electric vehicles and plug-in hybrid electric vehicles. AC chargers could usually be installed on places like residential buildings, malls, hotels, offices etc. DC chargers could be installed on places like fuel pumps, highways, restaurants where EV users come, stop for a while, charge their vehicles and go.
[2] Asset Management	Keeping track of software and hardware assets in your environment is a prerequisite for effectively managing cybersecurity. EN+ recommends that you maintain an asset inventory that uniquely identifies each important component. To facilitate this, AC Charger supports the following identifying information on product labels and manuals attached with products: Hardware - manufacturer, part name, serial number, f/w version number, and address. Software - publisher, name, version, and version date. (Firmware version information through serial port log)
[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.  Application and data security Security updates, Secure communications, Data encryption etc. Host security Secure configurations, Restricting unwanted and insecure services, Whitelisting etc. Network security Firewalls, IDS / IPS, Sandboxing, Monitoring and alerting etc. Physical security Access control, ID cards, Fences, CCTV etc. Policy and procedures Risk management, Incident response, Supply chain management, Audit & assessment, Trainings etc.

Category	Description
[4] Risk Assessment	EN+ conduct 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 IEC 62442. The risk assessment should be repeated periodically.

[5] 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. **AC Charger** is designed to be deployed and operated in a physically secure location. Following are some best practices that EN+ 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 **AC Charger** 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.

[6] COTS Platform Security

EN+ recommends that customers harden third-party commercial off-the-shelf (COTS) operating systems or platforms that are used to run EN+ applications / products (e.g., third party hardware, operating systems and hypervisors, such as those made available by Dell, Microsoft, VMware, Cisco, etc.).

Irrespective of the platform, customers should consider the following best practices:

CMS platform have authentication validation form low-level user accounts to high-level accounts on our platform. The server ID is attached to the Alibaba Cloud load balancing service we use. Used TLS1.2 & X.509 in authentication and authorization methods. Use a strong secure password to log in. Users are required to change their password for the first time. If the user has not changed the password for more than three months to force the user to change user password.

[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:

- 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:

- 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).

- No account sharing – Each user should be provisioned a unique account instead of sharing accounts and passwords. Security monitoring features in the product are designed based on each user having a unique account. Allowing users to share credentials weakens security.

	• Set remotely permissions-Our CMS Cloud Web could setting a account form low user accounts to high-level accounts, the setup process is as follows: 1. Set the management scope of the new account, including in the operations scope, station group scope and station scope) 2. Select the different permission roles for different accounts (e.g., the data) • HTTP tool permission setting, the user was prompted to change the AP mode password for the first time. And you should be entering the PIN code (CRC Algorithm) in AP web then Enforce session time-out after 15 minutes. • Ensure password length, complexity and expiration requirements are appropriately set, particularly for all administrative accounts (e.g., minimum 8 characters, including uppercase letters, lowercase letters, numbers, and characters and expire every 90 days, or otherwise in accordance with your organization's policies).
[8] Time Synchronization	Many operations in power grids and IT networks heavily depend on precise timing information. • OCPP recommended to use UTC (0 Time Zone) for all time values to improve interoperability between Central Systems and Charge Points • The backend time is sent to the charger device through the OCPP protocol of data transfer command of "0 UTC zone time"
[9] Network Security	**AC Charger** supports network communication with other devices in the environment. This capability can present risks if it's not configured securely. Following are EN+ recommended best practices to help secure the network. Additional information about various network protection strategies is available in EN+ Cybersecurity Considerations for Electrical Distribution Systems [R1]. EN+ 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: AC Charger 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: The charger communicates via 4G network, Wi-Fi or Ethernet, and there are mainly two parts of communication: 1.CMS Web App:

	CMS Web App running on the port 443(HTTPS): OCPP platform: using WebSocket + TLS method; TLS/SSL Configure TLS1.2 &X.509 is used for certificate management The security protocol uses in HTTPS 2. WIFI: Using WPA2 IEEE 802.11i encryption protocol by default. 3. 4G network: base on the LTE network service from Telecom operator 4. Ethernet: EN+ 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 **AC Charger** to operate smoothly.
[11] Logging and Event Management	• EN+ recommends logging all relevant system and application events, including all administrative and maintenance activities. The logs are uploaded to the server/platform in real time through OCPP protocol and can only be viewed by the operation account permission. • 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.). • Platform developers should review the sensitivity and criticality of the system/device and any data. The frequency of review should be reasonable, taking into account the sensitivity and criticality of the system | device and any data it processes. • Ensure that logs are retained for a reasonable and appropriate length of time. Logs are retained in server for one month by default that it will be clear regularly. The charger communicates through 4G network, Wi-Fi or Ethernet, and there are mainly two parts of communication: OCPP platform: using WebSocket + TLS method; Support the standard diagnostic information (equipment operation log) defined by OCPP, and can report the specified time period log to the OCPP server; The permission to view logs is only developed for background and maintenance personnel, and users and operation accounts do not have access.
[12] Vulnerability Scanning	It is possible to install and use third-party software with AC Charger. 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. • EN+ 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.*
[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.
[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.
[15] Malware Defenses	EN+ recommends deploying adequate malware defenses to protect the product or the platforms used to run the EN+ product.
[16] Secure Maintenance	The device includes an AP mode web to allow a service engineer with help from site administrator to trouble shoot the device functionality. Port used: HTTP Best Practices: Update device firmware prior to putting the device into production. Thereafter, apply firmware updates and software patches regularly.

	EN+ publishes patches and updates for its products to protect them against vulnerabilities that are discovered. EN+ encourages customers to maintain a consistent process to promptly monitor for and install new firmware updates. • For Wi-Fi module, Updating the firmware through our own platform or other platform at least every six months, the updated firmware package is EN+ signed, we will put EN+ signed firmware on the secure server, the OTA update will be initiated by the customer to download the firmware to the product, the product will authenticate the firmware and send to Wi-Fi module to start the update. • For Main MCU, Updating the firmware through our own platform or other platform at least every six months, the updated firmware package is EN+ signed, we will put EN+ signed firmware on the secure server, the OTA update will be initiated by the customer to download the firmware to the product, the product will authenticate the firmware and start the update.
[18] Customer Application Security	**AC Charger** 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. EN+ 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, EN+ 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.
[19] Sensitive Information Disclosure	EN+ recommends that sensitive information (i.e., connectivity, log data, personal information) that may be stored by **AC Charger** be adequately protected through the deployment of organizational security practices. 1.HTTP tool login username/password, debug port login password;(the original password is calculated by CRC to obtain the digest value, which is stored in the flash) 2.Basic device information: encrypted by AES256 stored in flash. 3.Device configuration information: encrypted by AES256 stored in flash; The following sensitive information is encrypted in the following scenarios: Sensitive information such as Wi-Fi、name、password、Bluetooth mac address, WIFI hotspots are encrypted during https transmission or using process. And this information was encrypted by AES256 stored in flash. In reset process, the WIFI name, Sensitive information such as Bluetooth address, and PIN code were hidden and could not be displayed in the local log.
[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. EN+ recommends that products containing embedded flash memory be securely destroyed to ensure data is unrecoverable.

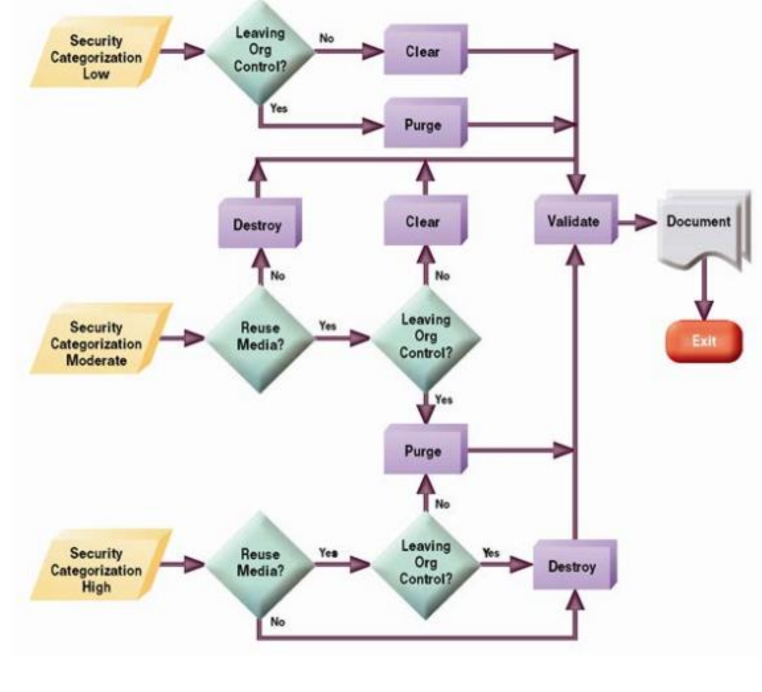


Figure 4-1: Sanitization and Disposition Decision Flow

* Figure and data from NIST SP800-88

Embedded Flash Memory on Boards and Devices
EN+ recommends the following methods for disposing of motherboards, peripheral cards such as network adapters, or any other adapter containing non-volatile flash memory.

- Clear: If supported by the device, reset the state to original factory settings.

Reset process:

1、 Set the charger into the AP Mode (Wi-Fi Hotspot) and then turn on the power supply and start the charger;

2、 Customer have to use the smart phone to connect to the charger's Wi-Fi hotspot;

3、 User need to access the web page designed for the Wi-Fi AP mode which includes functionalities such as “network configuration, server setting，plug mode and load balance mode";

4、 User will click on the “Factory reset” option to delete “Wi-Fi name, password, Hotspot password，plug setting，load balance setting parameters";

5、 The above steps will reset the EV charger to the original (0) state；

6、 After the charger was factory recovery, the Wi-Fi and server information

	Wi-Fi hotpot password, router information will be rolled back to default values. • Purge: If the flash memory can be easily identified and removed from the board, the flash memory may be destroyed independently of the board that contained the flash memory. Otherwise, the whole board should be destroyed. All data in flash is encrypted and stored and cannot be readable. • Destroy: Shred, disintegrate, pulverize, or incinerate by burning the device in a licensed incinerator.