EcoStruxure Power CommissionMobile

Cybersecurity Guide

08/2023

DOCA0288EN-01

www.se.com

Legal Information

Table of Contents

Safety Information

Important Information

Read these instructions carefully, and look at the equipment to become familiar with the device before trying to install, operate, service, or maintain it. The following special messages may appear throughout this documentation or on the equipment to warn of potential hazards or to call attention to information that clarifies or simplifies a procedure.

The addition of this symbol to a “Danger” or “Warning” safety label indicates that an electrical hazard exists which will result in personal injury if the instructions are not followed.

This is the safety alert symbol. It is used to alert you to potential personal injury hazards. Obey all safety messages that follow this symbol to avoid possible injury or death.

⚠ DANGER

DANGER indicates a hazardous situation which, if not avoided, **will result in** death or serious injury.

⚠ WARNING

WARNING indicates a hazardous situation which, if not avoided, **could result in** death or serious injury.

⚠ CAUTION

CAUTION indicates a hazardous situation which, if not avoided, **could result** in minor or moderate injury.

NOTICE

NOTICE is used to address practices not related to physical injury.

Please Note

Electrical equipment should be installed, operated, serviced, and maintained only by qualified personnel. No responsibility is assumed by Schneider Electric for any consequences arising out of the use of this material.

A qualified personnel is one who has skills and knowledge related to the construction and operation of electrical equipment and its installation, and has received safety training to recognize and avoid the hazards involved.

About the Book

This document describes the secure guidelines to be followed by EcoStruxure Power Commission Mobile users.

EcoStruxure Power Commission Mobile Overview

Application Overview

EcoStruxure Power Commission application is used to setup and test wireless devices in Schneider Electric Panel Server gateways.

This free mobile application provides easy discovery, quick tests, and comprehensive reports to complete commissioning of Panel Server gateways and wireless devices within. It will make commissioning much simpler in certain use cases as carrying laptop may not be feasible.

Features Supported

- Connect to Panel Server over Bluetooth Low Energy (BLE)
- Discover and setup wireless devices
- Update firmware for devices
- Generate commissioning report

EcoStruxure Power Commission Mobile Application Installation

EcoStruxure Power Commission mobile application is available in Android and iOS versions. Scan the QR code below to download the app.

Download Application for iOS Devices

Download EcoStruxure Power Commission application from the EcoStruxure Power Commission iOS Application.

Download Application for Android Devices

Download EcoStruxure Power Commission application from the EcoStruxure Power Commission Android Application.

An Introduction to Cybersecurity

Introduction

Cybersecurity is intended to help protect your communication network and all equipment connected to it from attacks that could disrupt operations (availability), modify information (integrity), or give away confidential information (confidentiality). The objective of cybersecurity is to provide increased levels of protection for information and physical assets from theft, corruption, misuse, or accidents while maintaining access for their intended users. There are many aspects to cybersecurity including designing secure systems, restricting access using physical and digital methods, identifying users, as well as implementing security procedures and best practice policies.

Schneider Electric Guidelines

In addition to the recommendations provided in this guide that are specific to EcoStruxure Power Commission application, you should follow the Schneider Electric defense-in-depth approach to cybersecurity.

This approach is described in the system technical note How Can I Reduce Vulnerability to Cyber Attacks?

In addition, you will find many useful resources and up-to-date information on the Cybersecurity Support Portal on the Schneider Electric global website.

For more information on cybersecurity for EcoStruxure™, visit the website: https://www.se.com/ww/en/work/solutions/cybersecurity/

Schneider Electric Cybersecurity Policies and Rules

Schneider Electric uses a Secure Development Lifecycle (SDL) process, a key product development-based framework that helps ensure products follow secure design processes across all lifecycle stages. The Schneider Electric SDL process complies with IEC (International Electrotechnical Commission) 62443-4.1.

The SDL process includes the following:

- SDL practices applied to internal development actions, throughout the supply chain.
- Formal cybersecurity review required for project release.
- Security training for personnel involved in the product development.

Security Capabilities

Secure Communication

EcoStruxure Power Commission application uses secure channel to communicate with backend servers and connected devices, that means data is transmitted over a secure channel.

This security capability helps to protect the confidentiality of information through secure protocols that employ cryptographic algorithms, key sizes, and mechanisms used to help prevent unauthorized users from reading information in transit.

Wireless Communication Security with Panel Server

EcoStruxure Power Commission connects to the Wireless Panel Server using its BLE interface (Bluetooth Low Energy IEEE (Institute of Electrical and Electronics Engineers) 802.15.1). The IEEE 802.15.1 wireless communication is encrypted by AES-CCM-128 cryptographic mechanisms supporting the integrity and confidentiality of data exchanged between the mobile device and the Wireless Panel Server.

Communication Security with Cloud Backend

EcoStruxure Power Commission connects to its cloud backend using HTTPS (Hypertext Transfer Protocol Secure) protocol. The communication is encrypted using TLS (Transport Layer Security) and ensures integrity and confidentiality of data exchanged.

Application Signing

EcoStruxure Power Commission application is digitally signed with a certificate. The digital signature is used to verify the owner's identity for application updates. This process can help prevent an app from being tampered with or modified to include malicious code.

Compromised Device Detection (Root or Jailbreak Detection)

NOTICE

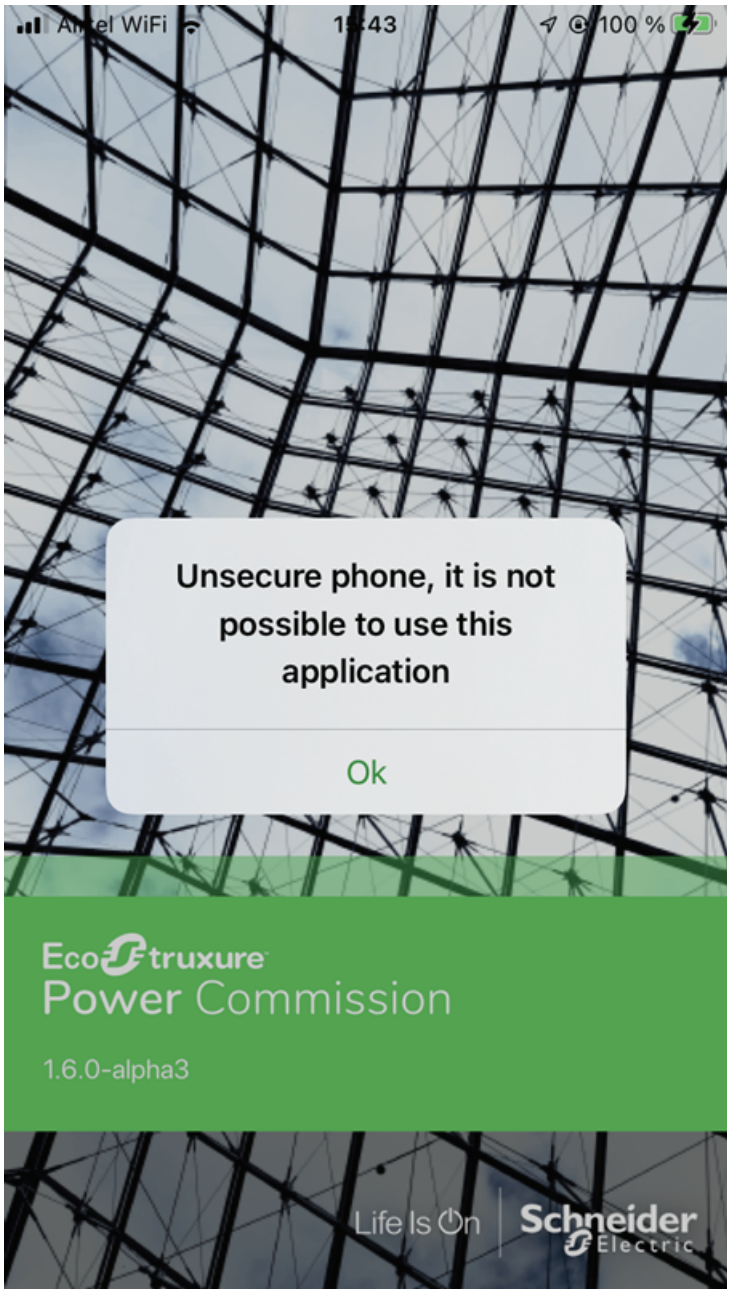
POTENTIAL COMPROMISE OF SYSTEM AVAILABILITY, INTEGRITY, AND CONFIDENTIALITY

- Do not use rooted or Jailbroken device for work purpose.
- Do not install EcoStruxure Power Commission application in rooted or Jailbroken device.
- Follow mobile device manufactures recommendations and cybersecurity best practices to help prevent unauthorized exposure, loss, modification of data and logs, or interruption of services.

Failure to follow these instructions can result compromise of mobile device.

EcoStruxure Power Commission application uses compromised device (Jailbroken or rooted device) detection method to detect if the mobile device is compromised.

If the application detects that the device is compromised, the application will not allow the user to proceed further. The application will exit with the message **Unsecure phone, it is not possible to use this application**.



Data Privacy and Protection

EcoStruxure Power Commission application is developed with privacy by design best practices. It collects, processes personal information in an open and transparent manner.

EcoStruxure Power Commission application provides details about the types of personally identifiable information processed, as well as security best practices followed in the app.

To check the details:

1. Search for EcoStruxure Power Commission application in the corresponding application marketplace (Google Play, App Store).
2. Go to the section **App Privacy** in App Store or **Data Safety** section in Google Play Store.

Read and understand how the app processes data and security practices followed in the app. Refer to Schneider Electric Data Privacy Policy.

Defense in Depth Measures Expected in User Environment

Schneider Electric recommends a Defense-in-Depth approach to cybersecurity for its customers. Defense-in-Depth is a hybrid, multi-layered security strategy that provides holistic security throughout an industrial enterprise.

Cybersecurity Policy

- Manage Security plan, policies and procedures that cover risk assessment, risk mitigation, mobile device management and methods to recover from disaster.
- Available and up-to-date guidance on governing the use of information and technology assets in your company.

Device Hardening

- Password management, user profile definition and deactivation of unused services to strengthen security on devices.
- Controls against malware – detection, prevention, and recovery controls to help protect against malware are implemented and combined with appropriate user awareness.
- Implement processes to reset the infected mobile devices to a known safe setting, such as factory settings.

Monitoring and Update

- Surveillance of user activity and network communications.
- Regular updates of mobile operating system and apps.
- Implement processes to manage the loss of a device to ensure remote deletion of the data held on the device.
- Implement solutions for the detection and protection against any malware in the mobile device.

Cybersecurity Training for Employees

- Provide cybersecurity training to your employees to help keep your organization secure.
- Train the users about phishing emails, infected attachments, malicious websites, and other methods that attack them directly.
- Training on the organization’s privacy policy and the personal information collected.
- Require any contractors or managed services vendors to complete the equivalent cybersecurity training.

Security Hardening Guidelines for Mobile Devices

General Security Recommendations

NOTICE

POTENTIAL COMPROMISE OF SYSTEM AVAILABILITY, INTEGRITY, AND CONFIDENTIALITY

- EcoStruxure Power Commission application does not require device administration permission. Review every device administration request carefully.
- Do not grant applications unexpected or unnecessary permissions.

Failure to follow these instructions can result compromise of mobile device and application.

- Use a password to protect the device to ensure it is locked.
- Protect your account credentials and enable multi-factor authentication options when available.
- Scrutinize every device administration permission request. Device Administrator permissions are extremely dangerous, and very few applications need it. If the request is not expected or the user does not recognize the application, the application should be uninstalled immediately.
- Be extra scrutinous of applications that request location or sensitive phone information permissions, and to deny any permissions requests for applications they do not recognize.
- Be cautious when granting applications dangerous or privacy-intrusive permissions, such as access to notifications, keyboard registration, send SMS (Short Message Service) or accessibility service access. EcoStruxure Power Commission application does not require any of these permissions.
- If a user sees a persistent notification they do not recognize, they should uninstall the source application and look for other unwanted applications or anomalies.
- Do not use rooted or jailbroken device. Rooting or Jailbreaking grants complete access to operating system and it allows unnecessary access to system services that presents critical security risks that could be taken advantage of without user's knowledge. EcoStruxure Power Commission application is not supported on rooted or jailbroken device.
- Do not connect the mobile devices to unknown wireless networks and devices.
- Have physical control over the mobile device and do not leave it unattended.
- Follow mobile device manufacturer recommendations to Protect against harmful apps
- Notify the organization if the mobile device used for work is lost or stolen and follow organizations recommendation to manage the incident.

Application Permissions

EcoStruxure Power Commission application requires permissions mentioned in the following table for normal operation. It does not require any other permissions to operate.

NOTE: EcoStruxure Power Commission application does not require device administrator permission.

For iOS Device

Permission	Purpose
CAMERA	Camera access is required to scan QR (Quick Response) Code from app.
BLUETOOTH	Bluetooth is used to communicate with BLE devices.

For Android Device

Permission	Purpose
CAMERA	Camera access is required to scan QR Code from app
INTERNET	Receive data from internet
ACCESS_NETWORK_STATE	View network connections
GET_ACCOUNTS	User account management
VIBRATE	Control vibration
BLUETOOTH	Bluetooth is used to communicate with BLE devices
BLUETOOTH_ADMIN	Bluetooth is used to communicate with BLE devices
ACCESS_COARSE_LOCATION **(1)**	Required for Bluetooth connection
ACCESS_FINE_LOCATION **(1)**	Required for Bluetooth connection
POST_NOTIFICATIONS **(2)**	Required to send notifications

NOTE: The EcoStruxure Power Commission mobile application requests:

1. Location (ACCESS_COARSE_LOCATION and ACCESS_FINE_ LOCATION) permission if the operating system (OS) is ≤ Android v11.0.

   Location permission is not required for OS ≥ Android v12.0.
2. POST_NOTIFICATIONS permission if the operating system (OS) is ≥ Android v13.0.

   Notification permission is not required for OS < Android v13.0.

QR Code Best Practices

QR Code may be tampered with untrusted content which could cause redirection to malicious sites and user credentials and user credentials can be stolen.

It is recommended that the users should verify that the QR code has not been tampered with (no rips, tears, punctures, or scratches) and check that the URL redirects you to a Schneider Electric website (domain).

Security Recommendation for Operation

General Security Recommendations

- EcoStruxure Power Commission application must be password protected and used for work only.
- Harden the mobile device that have the EcoStruxure Power Commission application by implementing all the security features recommended by the mobile device vendor or manufacturer.
- Use antivirus applications for mobile devices and keep it up-to-date.
- Do not disclose personal information such as mobile number, email address, and information about the mobile device (telephone number, Media Access Control (MAC) address) if it is not necessary.
- Do not store sensitive information on mobile devices that are used for work.
- Implement the device updates as soon as it is available. Mobile device user is responsible for updating the device.
- Change the password of the services that the user is allowed to connect to if the mobile device has been stolen or lost.
- Do not use public charging stations or computers to charge the devices. Instead, use a charger acquired from a trustworthy source.
- Do not click on device prompts to trust attached computers unless necessary.
- Do not grant consent for screen captures to occur unless expected.
- Avoid enabling USB (Universal Serial Bus) debugging (Android Debug Bridge) unless explicitly required.
- iOS device users should not download applications or updates from unofficial sources, as applications distributed via the Apple Application Store cannot list installed applications on a device.
- Do not open links or attachments in applications that are not recognized.
- Disable unused services or features on mobile device when you are not using them.
  - Disable Bluetooth when you are not using it.
  - Disable Wi-Fi when it is not needed. Delete unused Wi-Fi networks.
  - Disable location services when not needed.
- Install only verified CA certificates, iOS Configuration profiles after verifying the authenticity.

Application Update

NOTICE

POTENTIAL COMPROMISE OF SYSTEM AVAILABILITY, INTEGRITY, AND CONFIDENTIALITY

- Download and install EcoStruxure Power Commission Software updates from the official Google Play Store or Application Store.
- Do not install updates from unknown sources.

Failure to follow these instructions can result in compromise of mobile device and application.

EcoStruxure Power Commission application provides regular Software upgrades to include new features and security updates. It is recommended to keep the EcoStruxure Power Commission application up-to-date.

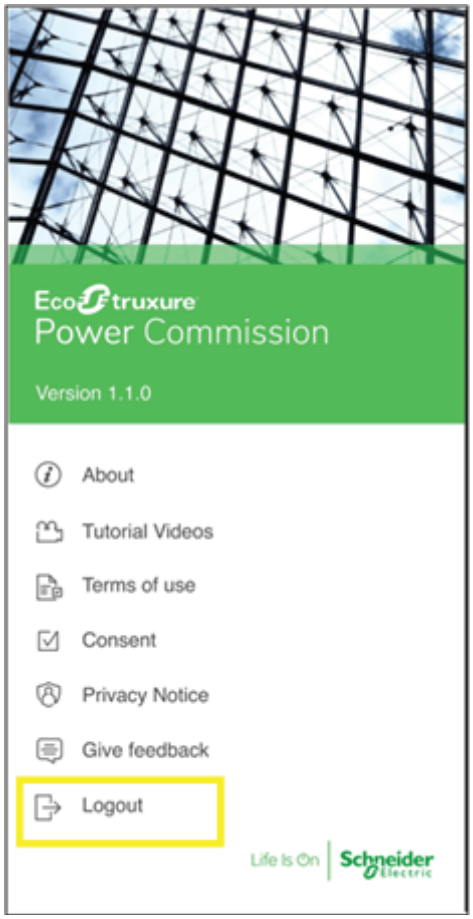
Upgrade EcoStruxure Power Commission application from official Google Play Store or Application Store.

Do not download updates from unknown sources.

EcoStruxure Power Commission mobile application supports push notification whenever a periodic or new update is available.

Logout

It is recommended to perform a logout before deleting the app or handing over the phone to another user. This is to ensure that no illegitimate user can access your phone and the EcoStruxure Power CommissionMobile application. Logout option is shown in the following figure:



It is recommended to perform a logout from the EcoStruxure Power Commission mobile application using the **Logout** option in hamburger menu. You can use this option if you want to use different credentials for other Schneider Electric mobile applications. Once you perform this action and navigate to any other Schneider Electric application, you will be provided with an option to enter the login credentials.

Security Recommendation for Decommissioning

Decommissioning removes EcoStruxure Power Commission application files to help prevent potential disclosure of sensitive, confidential, and proprietary data and software from your system. Your project data, system configuration, user information, and other sensitive information is at risk if you do not decommission. It is strongly recommended that you decommission your application at the end of its life.

NOTICE
UNINTENDED DATA LOSS OR LOSS OF SOFTWARE FUNCTION • Uninstall EcoStruxure Power Commission if it is no longer needed. • Backup project data before decommissioning. • Refer section Application Update, page 15 for updating the software. **Failure to follow these instructions can result in unintended data loss or loss of application function.**

Uninstall EcoStruxure Power Commission Application

Uninstallation of EcoStruxure Power Commission application removes project data associated with the application. It is recommended to log out from the application before uninstalling it.

If you uninstall the application, you will not be able to commission Wireless Panel Server and downstream devices.

Follow mobile device manufacturer guidelines to uninstall and delete the application.

Delete Schneider Electric User Account

EcoStruxure Power Commission application provides an option to delete Schneider Electric user account.

If the user, no longer wishes to use Schneider Electric account, they can delete their user account from EcoStruxure Power Commission application. If the account is deleted, users will not be able to use any of the Schneider Electric applications.

Deleting user account removes all the user related information provided during the registration.

Schneider Electric Cybersecurity Support

Overview

The Schneider Electric cybersecurity support portal outlines the Schneider Electric vulnerability management policy.

The aim of the Schneider Electric vulnerability management policy is to address vulnerabilities in cybersecurity affecting Schneider Electric products and systems, to protect installed solutions, customers, and the environment.

Schneider Electric works collaboratively with researchers, Cyber Emergency Response Teams (CERTs), and asset owners to ensure that accurate information is provided in a timely fashion to protect their installations.

Schneider Electric's Corporate Product CERT (CPCERT) is responsible for managing and issuing alerts on vulnerabilities and mitigations affecting products and solutions.

The CPCERT coordinates communications between relevant CERTs, independent researchers, product managers, and all affected customers.

Schneider Electric Cybersecurity Support Portal

The support portal provides the following information:

- Cybersecurity vulnerabilities of products.
- Cybersecurity incidents.
- An interface that enables users to declare cybersecurity incidents or vulnerabilities.

Security Notification

Product security notification posted can be viewed via Schneider Electric website: www.se.com

Vulnerability Reporting and Management

Cybersecurity incidents and potential vulnerabilities can be reported via the Schneider Electric website: Report a Vulnerability.

Definitions

Jailbreak

Jailbreaking is bypass of software restrictions imposed by device manufacturers on Apple devices. A jailbroken device permits root access within the operating system and provides the right to install software not available through the Application Store.

Rooting

Rooting (like modifying the Operating System (OS) so that you can run commands as the root user) is the process of obtaining privileged access to a device to have full control over the operating system.

Root Access

Root is a special user account with the highest privileges used for system administration.

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
France

+ 33 (0) 1 41 29 70 00

www.se.com

DOCA0288EN-01