

Paxton Solo – Security Overview

Overview

Paxton Solo has been designed to make access control simple to use while maintaining strong security throughout the system. Security is built into each stage of communication and administration from the user's phone to the door controller, and into the cloud services that support the system.

This document provides an overview of the key security measures included in Paxton Solo.

Phone to Controller communications

Paxton Solo uses Bluetooth Low Energy (BLE) for communication directly between the user's phone and the Solo Controller.

To protect this connection, both the controller and the mobile device use secure hardware and secure processes designed to prevent credentials being copied or intercepted.

A secure element within the controller provides a protected environment for storing sensitive security information. On supported mobile devices, security features built into the phone provide similar protection for digital credentials.

This means access information is not openly stored or exchanged in a way that could easily be extracted, cloned, or reused by unauthorized users. As communication takes place directly between the phone and the Solo Controller, the Solo hardware does not require connection to the customer's on-site network for normal operation.

Asymmetric Cryptography

Communication between the Paxton Solo mobile app and the Solo Controller is protected using asymmetric cryptography.

In simple terms, this means the system uses a pair of digital keys, one public and one private. These keys work together to confirm identity and protect information during communication.

Because the private key is never shared, the system can verify that both devices are genuine without exposing sensitive information. This approach reduces the risk of credential copying, replay attacks, and unauthorized devices attempting to gain access.

Each interaction is designed to confirm that the phone and Solo Controller are trusted before access is granted, without requiring the Solo Controller to communicate across the customer's local network.

Phone to Cloud communications

Paxton Solo hardware does not connect directly to the customer's network or the internet. Where cloud communication is required, the user's mobile app acts as the communication path to Paxton cloud services.

Communication between the app and cloud services takes place over standard HTTPS connections using port 443 and is protected using SSL/TLS encryption.

This approach reduces network complexity on site, avoids opening inbound connections into customer infrastructure, and keeps communication within standard secure internet traffic. Data transmitted between the app and cloud services is protected while in transit and supports secure management of users and permissions.

Secure Login with Passkeys (Optional)

User login can be protected using passkeys, which are widely recognized as one of the strongest and most user-friendly approaches to multi-factor authentication.

Unlike traditional passwords, passkeys use cryptographic credentials stored securely on a user's device and can be combined with device authentication methods such as biometrics or device PINs.

This reduces the risks associated with weak passwords, password reuse, and phishing attacks. Passkeys are optional, allowing organizations to choose the approach that best fits their security policies and user requirements.

Controlled Administration Through Permission Levels

Administrative access within Paxton Solo is controlled through app permission levels. This allows organizations to assign users only the access they need for their role.

For example, some users may only manage day-to-day administration, while others can configure system settings or device settings.

By limiting access based on responsibility, organizations can reduce the risk of accidental changes and maintain clearer control over system administration.

Door Access Managed Through Customizable Access Levels

Paxton Solo allows organizations to control who can access specific doors and when.

Customizable access levels make it possible to define permissions based on users, teams, locations, time schedules, or operational requirements. This gives organizations flexibility to support different working patterns while maintaining secure control of entry points.

Changes to access permissions can be managed centrally, helping ensure access rights remain aligned with business needs.

Security That Supports Everyday Use

Paxton Solo combines modern security practices with straightforward day-to-day operation.

By securing phone-to-controller communication, protecting credentials, separating hardware from on-site networks, controlling administration, and enabling flexible access management, the system is designed to help organizations manage access with confidence.

Security Credentials

Paxton Solo security controls are supported by recognized independent cybersecurity assessments.

IASME IoT Cyber Assurance Level 2

Paxton Solo has achieved IASME IoT Cyber Assurance Level 2 accreditation.

This certification is designed specifically for connected products and assesses whether security controls have been implemented and independently verified. It covers areas such as secure development practices, device protection, vulnerability management, data handling, and ongoing security processes.

Level 2 includes independent technical assessment to provide additional confidence that security measures are operating as intended.

For end-users, this offers reassurance that security has been considered as part of both product design and ongoing product management.

UL Cybersecurity Diamond Rating

Paxton Solo has also achieved the UL Cybersecurity Diamond rating.

This rating recognizes products that demonstrate a broad and mature approach to cybersecurity across multiple areas, including product security controls, software processes, vulnerability handling, and lifecycle management.

The Diamond level represents the highest tier within the program and reflects a commitment to building and maintaining secure connected products.

For organizations selecting an access control solution, independent accreditation provides additional assurance that security measures have been reviewed against recognized industry standards.

Secured by Design

Paxton Solo is also accredited under the Secured by Design scheme, the official police security initiative owned by the UK's College of Policing.

Secured by Design (SBD) accreditation recognizes products that meet recognized security standards and requirements designed to help reduce crime and improve security. For organizations selecting an access control solution, this provides additional assurance that security has been independently assessed against established industry and policing standards.