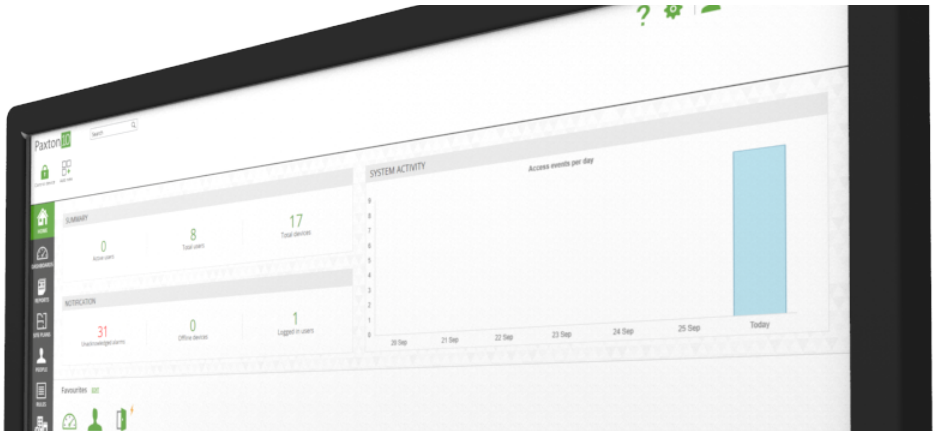

Paxton10 Security

Overview

Paxton10 is a network-based access control and video management system, which is controlled and configured by the Paxton10 Server via its web User Interface. This document discusses how Paxton10 remains secure and resilient to security attack and data breaches.

Paxton10 server

Operating system and BIOS

The Paxton10 Server runs Microsoft Windows 10 IoT (from February 2020). However, some earlier models (pre-2020) may be running Windows 7 Embedded – please contact support to find out more. < www.paxton.info/596 >

Remote desktop and file share are enabled at the server, secured with a 40-character Operating System password, unique to each system.

The server BIOS is similarly password protected.

Windows updates

Servers are provided with pre-selected security fixes and patches as part of Windows update. These are updated in the background where possible, and alongside service releases as part of the System Engineer controlled upgrade process where not. The server may need to be rebooted following a Windows update – the Paxton10 software will provide means of doing this when required. An internet connection is required to receive Paxton10 software and Windows updates.

Virus protection

Servers running Windows 10 IoT will include Windows Defender with automatic updates. An internet connection is required to receive updates.

USB ports

The Paxton10 Server is supplied with a USB memory stick for system backup. This memory stick can be inserted into any Paxton10 Server to restore/instate the system database onto that server. Database backup to USB occurs automatically every 24 hours. Backup to USB can be disabled simply by removing the USB memory stick.

APN-0053-ZA

The USB ports are not locked down, and as such may be used to access the server's data or execute commands. Security of the USB ports is achieved through securing the location of the server. Only the required installers and IT personnel should have access to the server's location.

Passwords and Client access

Login to the Paxton10 software is permissioned at a group/feature level. Each system user is given software access only to the data and control that they are allowed, if any.

Login is protected by email address and password. All passwords are enforced to contain at least 3 types of character: Lowercase, Uppercase, Number, Punctuation. Additionally, all passwords must contain at minimum 6 characters.

Passwords are stored securely in the server database using salted hash.

Network communication

Client software access

When accessing the Paxton10 software from the local network (via the server's local URL), communication is between the client and the server. Communication is secured using HTTPS, with a Paxton10 self-signed SSL certificate, in addition to any local network security measures in place.

When accessing the Paxton10 software from a remote location (via the server's remote access URL), the Paxton10 software is hosted using Microsoft Azure. Communication between the server, client, and Azure is secured using HTTPS with AES-256 encryption. An internet connection is required. No user or device data is stored within Azure.

Emails from Paxton10

Paxton10 uses email for resetting passwords and issuing Smart credentials. Emails will be sent from the following address: support@paxton10portal.com. Emails sent from Paxton10 utilize TLS encryption.

An additional email server may be configured in Paxton10 for use with Triggers and Actions. The security of this email server is determined by the host.

Controller communication and Firmware updates

Communication with Paxton10 controllers is over HTTPS/SSL.
We use TLS 1.2 for multi-site, which uses SHA-256 which is 256 bit encryption.

For more information on network security and the communication protocols used, see AN0051-AE Network requirements, optimisation, and security in Paxton10 < www.Paxton.Info/6393>.

Credentials and Smart devices

RFID tags and cards

Paxton10 cards and tokens store their serial number in a password protected sector, preventing unauthorised reading or copying. Additionally, Paxton10 reads the entire card or token, not just the card data; the credential is then created using a combination of the card's details (token data, serial number, date of manufacture etc.) making card cloning near impossible.

The Paxton10 software provides additional features and functionality which can be configured to further remove any risk of card cloning and stolen card access, such as anti-passback, user expiration dates, token baring, and dual authentication (Token + code, or Token + PIN).

Bluetooth communication

Smart credentials (smartphones, tablets and watches) and Bluetooth Fobs communicate with Paxton10 readers using Bluetooth Low Energy (BLE). A rolling code algorithm is used with encryption to prevent credential cloning and code grabbing.

Smart credentials

Smart credentials (smartphones, tablets and watches) are issued with a unique 32-character credential. Each credential can be registered to a single Android or iOS account, and once registered cannot be reissued. The credential is stored in the account's keychain or secure storage.

Where additional security is required, a Paxton10 system may enforce all smart devices to have a screen lock, preventing against unauthorised access from lost or stolen devices. Further security can be achieved using software features such as anti-passback and credential management, and additional authentication can be requested on top of the device and screen lock, such as PIN or Code at a keypad.