

Paxton Specification

Section One

Paxton10 Access Control & Video Management

Edit as required – this document can be edited and merged where appropriate with additional Paxton specifier documents for a complete/customised Access Control and Video solution.

Key - **[Square brackets]** – Options**.** Delete brackets and turn off bold to include.

**{Curly brackets}** – Comments. Delete before sharing document.

SECTION 1

ACCESS CONTROL – Paxton10 System

# GENERAL

## SUMMARY

### Section includes

#### Electronic Access Control and Video Management

### Related sections

#### 28 10 00 Electronic Access Control and Intrusion Detection

#### 28 13 00 Access Control

#### 28 23 00 Video Surveillance

### Products

### **{Choose to use either the Paxton product name or a general name for each}**

#### A **[server] [Paxton10 Server]** which shall contain the central database for the system, host the software, and provide storage for system events and user records.

#### A **[door controller] [Paxton10 Door Controller]**, which shall interface with access point peripherals and identity gathering devices, providing logic and decision making to manage an access point.

#### A **[video controller] [Paxton10 Video Controller]**, which in addition to interfacing with access point peripherals, shall also process and record video footage from network video cameras.

#### An **[alarm board] [Paxton10 Alarm Connector]**, which shall contain input and output peripherals to monitor and control the state of Intruder and Fire alarms.

#### A **[wireless interface board] [Paxton10 Wireless Connector]**, which shall communicate over Z-Wave wireless technology to communicate with and control Z-Wave devices.

#### A **[video surveillance camera] [Paxton10 Camera]**, which shall be capable of recording video up to either 1520p or 4K resolution and contain in-built memory for Edge storage.

#### A Power Supply Unit (PSU), which shall provide the power necessary to power the controllers.

#### A **[proximity reader] [Paxton10 Reader]** which shall read a variety of proximity credentials to verify and validate users.

#### A **[vandal resistant proximity reader] [Paxton10 VR Reader]** which shall read a variety of proximity credentials to verify and validate users, contained in a vandal resistant housing.

#### A **[keypad proximity reader] [Paxton10 Keypad Reader]** which shall read a variety of proximity credentials, in addition to providing code and PIN credentials, to verify and validate users.

#### A **[desktop reader] [Paxton10 Desktop Reader]** which shall provide the method of enrolling proximity tokens to the system to be associated with users.

#### The **[management software] [Paxton10 software]** that allows the interaction and configuration of system hardware, as well as the management of users and the system.

### System

#### The products above shall form a complete Access Control System (ACS), providing control and monitoring of access points at the installed site.

#### The products above shall form a complete Video Management System (VMS), providing video recording and video surveillance at the installed site.

#### The system shall be scalable, allowing for additional hardware from the same manufacturer.

#### All hardware provided by the manufacturer shall be plug-and-play.

#### The system shall contain multiple access points.

#### The system shall contain multiple controllable devices.

#### The system shall contain multiple monitorable devices.

#### The system shall contain intruder and fire alarm(s).

#### The system shall contain video surveillance cameras.

## PROJECT REQUIREMENTS

### The system shall monitor and control facility access via electronic access controllers utilising card readers, keypad devices, and smartphones. It shall be implemented through TCP/IP architecture using the electronic single door controller approach via PoE infrastructure.

### The system shall be capable of monitoring alarm points, controlling output devices, and managing lift control floors. The system shall maintain an audit trail of operator activity and all access control and alarm activity.

### The system shall be capable of starting with a single door, and expanding one door at a time, to up to a minimum of 1000 doors.

### Each controller shall be able to manage the hardware necessary to secure one door. If entry and exit is required, only one controller shall be required.

### Each controller shall maintain a full database of information to provide distributed and offline decision making, with no single point of failure.

### The controllers shall utilize IPv6 technology, supporting plug-n-play and automatic detection and addressing.

### The system shall allow unlimited workstations for programming and administration of the system including database management, report generation, and real-time monitoring of activity.

### No license keys or fees shall be required to access the administration software, and no installation shall be required on the server or any workstation.

### The system shall support at minimum 50,000 unique credentials.

### The system shall provide the following as a minimum:

#### Access Control

#### Door state monitoring (Door forced, Door left open)

#### Video Surveillance

#### Video Management

#### Event reporting

#### Site plans / Graphical maps

#### Triggers and actions

#### Anti-passback

#### Intruder alarm integration

#### Fire alarm monitoring

#### Roll call and Muster reports

#### Remote access

#### Smartphone application for system control

#### Smartphone application for user administration

#### Credential enrolment reader

#### Various proximity reader technologies, including Bluetooth

#### License free software and lifetime updates at no charge

#### Intercom / Video Entry Station

#### Wireless door locks

## DEFINITIONS

### Anti-passback: A term for preventing the sharing or ‘passing back’ of a token in aim to let unauthorised users into a site.

### AWG (American Wire Gauge): A unit of measurement for the diameter of wires.

### Browser: A computer program used to view and interact with data at a location on the connected network in a graphical manner.

### Client: A PC that can view and manage the system database.

### COM (Common): A contact on an I/O connector relay.

### Controller: An intelligent peripheral control unit that provides the interface between the Management and Monitoring Subsystem and the devices installed, for the purpose of restricting access, controlling, and monitoring user and device activity.

### DDR3 (Double Data Rate type 3): A type of RAM with a high bandwidth interface.

### Device: A video camera, light, alarm, access point or any other item that can be interacted with, either by controlling the action or outcome of, or by monitoring its output or state.

### Edge storage: The recording of video footage directly onto the camera.

### EMC: Electromagnetic Compatibility.

### Entry system (audio/video entry system): A system, either stand alone or integrated, comprised of Panels and Monitors to authorise access via video and audio communication.

### FCC: Federal Communications Commission.

### I/O: Input / Output, relating to peripherals where an input is used to monitor the high/low state of a signal, and an output consists of a relay capable of switching a device on/off.

### IC: Industry Canada.

### IP: Internet Protocol incorporated into Microsoft Windows.

### LAN: Local area network.

### Mbps: Megabits per second

### Monitor: A piece of hardware that allows an occupant to validate entry to a user via audio or video confirmation.

### N.C. (Normally Closed): A contact on an I/O connector relay.

### N.O. (Normally Open): A contact on an I/O connector relay.

### Occupant/Resident: The user of a Monitor or the user of a reader.

### Open air: Without obstruction or interference.

### Panel: A piece of hardware used to determine whether a known user is allowed access, and as a method of communication for unknown users to contact a building’s occupants.

### PC: Personal computer, used as a workstation, to access system software.

### PoE: Power over Ethernet.

### RAM (Random Access Memory): A type of storage used for software to store temporary date, required for the smooth running and use of software.

### Reader: A proximity, keypad, or biometric reader that captures credential information used to identify a user.

### RoHS: Restriction of Hazardous Substances.

### Roll call: An attendance check-list of users known to have been within a specified area.

### RS-485: A TIA/EIA standard for multipoint communications.

### RSS-210: IC standard for Licence-exempt Radio Apparatus.

### RSS-GEN: IC standard for General Requirements and Information for the Certification of Radio Apparatus.

### Server: A PC that contains the database of users and system configuration, which runs the system software.

### SIP: Session Initiation Protocol.

### Solid State Drive (SSD): A storage device that uses flash memory and has no moving parts.

### System: The hardware and software to be installed, combined with any existing hardware and software, to meet the requirements of the project.

### TCP: Transport Control Protocol incorporated into Microsoft Windows.

### Token: The credential issued to a person. This can be a PIN, or a device containing an encoded number, used to determine if access will be granted or denied.

### Triggers and Actions: A software component which provides the ability to create rules to perform custom/bespoke functionality.

### UDP: User Datagram Protocol incorporated into Microsoft Windows.

### UL: Underwriters Laboratories.

### Unicast: Communication where information is addressed to a single recipient.

### UPS: Uninterruptible power supply.

### USB: Universal Serial Bus. A communication port found on most computers.

### Vandal resistant (VR): A property of an item identifying the item as durable and attack resistant.

### Visitor: An unauthorised/unknown user. Or the user of a Panel.

### WAN: Wide area network.

### Wiegand: Patented magnetic principle that uses specially treated wires embedded in the credential card. Also known as reader data output format and Wiegand signal.

### Windows: Operating system by Microsoft Corporation.

### Workstation: A PC used to access the system software.

### Site: The location, or locations, in which the system is installed.

## SYSTEM DESCRIPTION

### General

#### The system shall monitor and restrict the movement of users through access points.

#### The system shall record, and manage the recordings of, video IP cameras located around the site

#### Users shall be identified and processed through any of these means:

##### Presenting a token to a reader

##### Presenting a smartphone or tablet to a reader

##### Entering a unique PIN to a keypad

##### Visual and/or audio confirmation from an occupant of the premises

##### Combination of the above

#### The system shall not require facility codes for card credentials. Each token/credential shall have a unique encryption for high security.

#### The system shall provide for unique card serial numbers, so the user will not need to determine the next sequence of cards to purchase.

#### A PC shall be used to administer the access control system.

##### A password shall be required to login and shall limit the activities an operator is permitted to perform.

#### Mobile applications shall be available for system control and user administration.

##### The mobile applications will be available for Android and iOS devices.

### Hardware

#### Hardware shall consist of:

##### A Server

##### Door controllers

##### Video controllers

##### Video cameras

##### Alarm peripheral boards

##### Wireless interface boards **{Required for PaxLock}**

##### Proximity readers

##### Keypad readers

##### Desktop readers

##### Power Supply Units

#### All hardware shall be plug-and-play.

#### All hardware peripherals shall be clearly labelled and identified for ease of installation.

#### Equipment used shall be provided with firmware upgrades from the manufacturer free of charge.

### Software

#### The system database containing all hardware and user information shall be held at the server.

#### The server shall host the system software and provide a web link for accessing and configuring the system.

##### The software shall be accessible to an unlimited number of workstations without installation.

##### The software shall be accessible using the latest version of the following browsers:

###### Google Chrome

###### Apple Safari

#### Software access shall be restricted using password-protected operator login.

#### Software access shall be permissioned to each administrator’s need and role.

#### The software shall feature:

##### A graphical user interface.

##### Tooltips on every control for user information.

##### Support for mobile, tablet and desktop devices.

##### Multi-user and multi-tasking to allow for independent activities and monitoring occurring simultaneously at different workstations.

#### System license shall be for the entire system and shall include capability for future additions that are within the indicated system size limits specified in this section. There shall be no license fee or yearly renewal fees.

### Feature set

#### The system and its associated software shall provide the following as a minimum:

##### Access Control

##### Video recording and management

##### Third party IP camera integration

##### PTZ camera support

##### Video wall

##### Export video

##### Export video snapshot

##### Video bookmarks

##### Smart search

##### Video scrubbing

##### Video playback speed control

##### Intruder Alarm Integration

##### Fire Alarm Integration

##### User Import

##### Graphical Maps

##### Custom Dashboards

##### User Favourites

##### Automatic User Image Display at PC on card use

##### Roll Call and Mustering

##### Roll Call Email Notifications

##### Smartphone Roll Call Reports

##### Triggers and actions to achieve custom/unique functionality

##### Anti-passback

##### Landlord Tenant

##### Support for multiple reader technologies, including Bluetooth

##### Remote site management

##### Android and iOS mobile application for site management

##### Android and iOS mobile application for user identification (Bluetooth token)

##### Secure software login using HTTPS

##### Data Management settings to manage data protection

##### Software available in multiple languages

#### These features shall be provided without additional cost or subscription

## PERFORMANCE REQUIREMENTS

### Any change made within the software shall automatically be communicated to all intelligent access control hardware, with appropriate changes taking immediate effect.

### Distributed Processing:

#### The system shall be a fully distributed processing system so that information (including time, date, valid codes, access levels, and similar data) is downloaded to Controllers in such manner that each Controller makes access-control decisions for that location.

#### If communications to the server are lost, all Controllers shall automatically buffer event transactions until communications are restored, at which time buffered events shall be uploaded to the server.

### System capacities:

#### The system shall support at minimum:

##### 1,000 access points.

##### 1,000 video cameras.

##### 50,000 users, each with a unique credential.

##### Unlimited access levels and rules.

##### Unlimited reporting

### System Network Requirements

#### Client PCs shall communicate with the server via HTTPS, using secure SSL encryption.

##### System events recorded by the server shall be communicated to clients.

##### Changes made to the database at a client shall be communicated to the server.

#### The server shall communicate with access control hardware via HTTPS.

##### Access control events shall be communicated to the server.

##### Changes to the database shall be communicated to the access control hardware.

#### The system shall utilise standard networking protocols to allow installation on corporate infrastructure.

#### No manual addressing shall be required.

## QUALITY ASSURANCE

### The software shall receive lifetime updates from the manufacturer free of charge.

### All equipment provided shall be covered by a manufacturer’s warranty for a minimum of 5 years, with the exception of the server, which shall be covered for a minimum of 3 years. The following aspects shall be covered:

#### Electrical

#### Electronic

#### Component

#### Mechanical

### All hardware provided shall receive firmware upgrades from the manufacturer free of charge.

## RELATED DOCUMENTS

### The system must interact with other physical parts of the facility and any construction either new or remodelled.

### When determining locations for placement of hardware, the installer shall follow all appropriate building codes and laws concerning life safety and construction.

## COMPLIANCE

### The system shall comply with:

#### The General Data Protection Regulation (GDPR) 2018

#### EN60839-11-1 Grade 1

#### EN60839-11-1 Grade 2

### Readers shall comply with the following standards:

#### EN 301 489-1 for EMC **{EU}**

#### EN 300 330 for Radio **{EU}**

#### EN 60950-1 for Safety **{EU}**

#### IEC/EN 60950-1 for Safety **{ROW}**

#### FCC Part 15C for Radio **{US}**

#### UL294 for Safety **{US}**

#### RSS-GEN, 210 for Radio **{Canada}**

#### CS C22.2 NO. 205-M1983 for Safety **{Canada}**

#### IP67 for Moisture resistance

### Vandal Resistant Readers shall comply with the following standards:

#### EN 301 489-1 for EMC **{EU}**

#### EN 300 330 for Radio **{EU}**

#### EN 60950-1 for Safety **{EU}**

#### IEC/EN 60950-1 for Safety **{ROW}**

#### FCC Part 15C for Radio **{US}**

#### UL294 for Safety **{US}**

#### RSS-GEN, 210 for Radio **{Canada}**

#### CS C22.2 NO. 205-M1983 for Safety **{Canada}**

#### IP67 for Moisture resistance

#### IK10 for Impact resistance

### Alarm connectors shall comply with the following standards:

#### EN 55032 for EMC **{EU}**

#### EN 50130-4 for EMC **{EU}**

#### EN 60950-1 for safety **{EU}**

#### FCC Part 15B for EMC **{US}**

#### UL 294 for safety **{US}**

#### ICES-003 for EMC **{Canada}**

#### CSA C22.2 NO. 205-M1983 for safety **{Canada}**

### Wireless connectors shall comply with the following standards:

#### EN 301 489-1 for EMC **{EU}**

#### EN 300 328 for Radio **{EU}**

#### EN 60950-1 for Safety **{EU}**

#### UL/CSA 60950-1 for Safety **{US/Canada}**

#### IEC 60950-1 for CB scheme

#### FCC Part 15C for Radio **{US}**

#### RSS-GEN, 210 for Radio **{Canada}**

### The server shall comply with the following standards:

#### EN 60950-1 for safety **{EU}**

#### EN 55022 for EMC **{EU}**

#### EN 55024 for EMC **{EU}**

#### EN 61000-3-2 for EMC **{EU}**

#### EN 61000-3-3 for EMC **{EU}**

#### Europe RoHS for Environmental compliance **{EU}**

#### FCC 47 CFR Part 15, Subpart B for EMC **{US}**

#### UL/CSA 60950-1 for safety **{US/Canada}**

#### ICES-003 for EMC **{Canada}**

#### IEC 60950-1 for safety

#### CISPR 22 for EMC

#### CIPSR 24 for EMC

#### IEC/EN 61000-4 Series for EMC

### Controllers shall comply with the following standards:

#### EN 55032 for EMC **{EU}**

#### EN 55024 for EMC **{EU}**

#### IEC/EN 62368-1 for Safety **{EU}**

#### FCC part 15B for EMC **{US}**

#### UL 294 for Safety **{US}**

#### CSA C22.2 NO. 205-M1983 for safety **{Canada}**

#### ICES-003 for EMC **{Canada}**

#### IEC 62368-1 for CB scheme

### Desktop readers shall comply with the following standards:

#### EN 301 489-1 for EMC **{EU}**

#### EN 300 330 for Radio **{EU}**

#### IEC/EN 60950-1 for Safety **{EU}**

#### FCC Part 15C for Radio **{US}**

#### RSS-GEN, 210 for Radio **{Canada}**

#### UL/CSA 62368-1 for Safety **{US/Canada}**

### Cameras shall comply with the following standards:

#### RoHS 2011/65/EU and Amd 2015/863/EU **{EU}**

#### EN 55032 for EMC Emissions **{EU}**

#### EN 50130-4 for EMC Immunity **{EU}**

#### EN 62368-1 for Safety **{EU}**

#### FCC part 15B for EMC **{US}**

#### ICES-003 for EMC **{Canada}**

#### UL/CSA 62368-1 for safety **{US/Canada}**

## GENERAL REQUIREMENTS FOR FUNCTIONALITY

### Through use of a controller, it shall be possible to:

#### Control the lock state of an access point.

#### Monitor the current open/close state of an access point.

#### Monitor door forced contacts.

#### Communicate events and configuration with the server.

#### Interface with hardware connectors to provide additional peripherals.

### Through use of a video controller, it shall be possible to:

#### Control the lock state of an access point.

#### Monitor the current open/close state of an access point.

#### Monitor door forced contacts.

#### Record video from 4 network IP cameras

#### Communicate events and configuration with the server.

#### Interface with hardware connectors to provide additional peripherals.

### It shall be possible to control and monitor additional devices using any spare Inputs/Outputs from a controller which are not used for securing an access point.

### Through use of an Alarm connector, it shall be possible to:

#### Interface with intruder and fire alarms:

##### Control the arm state of an intruder alarm.

##### Monitor the arm state of an intruder alarm.

##### Monitor the active state of an intruder alarm.

##### Monitor the active state of a fire alarm.

### It shall be possible to control and monitor additional devices using any spare Inputs/Outputs from an Alarm connector which are not used for monitoring or controlling an alarm.

### Through use of a proximity reader, it shall be possible to read a user’s credential.

#### A credential holder shall be able to present their token or Smart device to the reader to gain valid access to an access point.

##### Presentation of an invalid credential shall not allow access.

#### A credential holder shall be able to present their token to the reader to control a device.

##### Presentation of an invalid credential shall not action the device.

#### Visual feedback shall be provided to the user upon presentation of a credential.

##### Feedback shall indicate if the credential is valid or invalid for the intended action.

#### Audible feedback shall be provided to the user upon presentation of a credential.

##### Feedback shall indicate if the credential is valid or invalid for the intended action.

### Through use of a keypad reader, it shall be possible for a user to enter a PIN or code to identify themselves.

#### It shall be possible to use a PIN or code in conjunction with a proximity token or Smart device to further enhance security.

#### The system shall require a user authentication mode appropriate for the device or access point to be interacted with. The operating mode shall automatically change itself at various times of the day or days of the week according to its configuration.

### Through use of a server, it shall be possible to:

#### Access the software for configuration, maintenance and monitoring of the system.

#### Store the system database in a central location.

#### Record system events for displaying to a user live or at a later date.

### It shall be possible to mix-and-match hardware to fulfil the requirements of the project:

### The system shall utilise the existing network capabilities of the site. **{Remove if not true for project}**

### The system shall be versatile:

#### The system shall remain operational while the server is offline.

#### Each controller and its connectors shall remain operational while the network or other controllers are unavailable.

#### Each controller shall be fitted with a battery backup, to maintain operation to it and its connectors during power failure. **{Remove if no battery is fitted}**

##### The battery shall be monitored by the system, and provide the current battery state and charge in the user interface.

## GENERAL REQUIREMENTS FOR COMMUNICATIONS

### The server shall be connected to the local TCP/IP network.

#### A local URL shall be provided for which the software shall be accessible at on any computer on the same network.

#### A remote URL shall be generated if required for which the software shall be accessible at on any computer with an internet connection, provided the server also has internet access.

#### Communications to the server shall use secure HTTPS, encrypted using SSL.

#### The server shall be addressable by clients using a friendly DNS.

### Controllers shall be connected to the local TCP/IP network.

#### Controllers shall utilize IPv6 link-local.

#### Controllers shall communicate with the server.

#### Controllers shall communicate with other controllers (peer to peer).

#### Controllers shall be automatically detected by the server.

### Cameras shall be connected to the local TCP/IP network. **{If using Paxton10 cameras}**

#### Cameras shall utilise IPv6 link-local.

#### Cameras shall communicate with the server to provide information, user interaction and configuration.

#### Cameras shall communicate video directly to the client, reducing bandwidth requirements through the server.

#### Camera video and configuration shall be password protected.

##### The camera password shall be known only to the system and shall not require user entry.

### Cameras shall be connected to the local TCP/IP network. **{If using ONVIF cameras}**

#### Cameras shall be discovered automatically using ONVIF Profile S discovery.

#### Cameras shall communicate with a Video Controller.

### Cameras shall be connected to a TCP/IP network. **{If using RTSP cameras}**

#### Cameras shall be manually addressed using their RTSP address.

#### Cameras shall communicate with a Video Controller.

### Readers shall connect to a controller.

#### A single 22 AWG, 4 core twisted pair cable shall be used per reader.

##### 16' (5m) of cable shall be provided with each reader.

##### Cable type for extensions shall be 22 AWG, 4 core twisted pair.

##### Maximum length of cable shall be at minimum 328' (100m).

#### Readers shall be automatically detected by the system.

#### Each controller shall support at least 2 wired readers.

### Desktop reader shall connect to a client PC.

#### The desktop reader shall input data to the Paxton10 software via a client PC.

#### The desktop reader shall connect to a client PC via a mini USB to USB cable.

#### The desktop reader shall be plug-and-play, utilizing keyboard output.

### All network addressable controllers shall support IPv6 for auto detection and plug-and-play functionality.

### All cameras used shall output two video streams; a high resolution ‘main’ stream, and a low resolution ‘sub’ stream. The sub stream shall be used to save network bandwidth when streaming multiple video streams.

### The system shall utilise standard networking protocols to allow installation on corporate infrastructure.

# PRODUCTS

## MANUFACTURERS

### Acceptable manufacturer: Paxton **{Delete if necessary}**

#### Email address: **{Delete options which are not required}**

##### **{UK} [support@paxton.co.uk]**

##### **{FR} [support@paxtonaccess.fr]**

##### **{US} [supportUS@paxton-access.com]**

##### **{DE} [verkauf@paxton-gmbh.de]**

##### **{NL} [support@paxton-benelux.com]**

#### Telephone number:

##### **{UK} [01273 811011]**

##### **{FR} [01 57 32 93 56]**

##### **{US} [877.438.7298]**

##### **{DE} [0251 2080 6900]**

##### **{NL} [076 3333 999]**

#### Skype:

##### **{UK} [Paxton.support]**

##### **{FR} [Paxton.benelux.support]**

##### **{US} [usaPaxton.support]**

##### **{DE} [Paxton.gmbh.support]**

### Substitutions: Not permitted. **{Delete if necessary}**

### The components of the system shall be available from a single source manufacturer to assure compatibility of products.

### Components shall consist of:

#### System software. The manufacturer shall have in its employ the software engineering staff that write and manage the code for the system and shall maintain all licensing required.

#### Controllers. The manufacturer shall provide Door controllers and Video controllers for a plug-and-play solution to secure a building and control devices.

#### Readers. The manufacturer shall provide proximity readers, keypad readers, and vandal resistant variants, for identifying and validating a user.

#### Tokens/credentials. The manufacturer shall provide a range of proximity tokens to meet the requirements of the project.

#### Cameras. The manufacturer shall provide their own range of plug-and-play, 4K resolution, networked video surveillance cameras. The cameras shall be available in a range of form factors.

#### Door Entry Intercom. Should it be required now or at a later date, the manufacturer shall provide plug-and-play Entry Monitors and Entry Panels to allow occupants of a building to communicate with, and allow access to, visitors. The Door Entry Intercom shall add on to a new or existing system without redesign or re-architecture.

#### Wireless Door Handles. Should it be required now or at a later date, the manufacturer shall provide wireless door handles for access control solutions where a wired solution is not feasible. The wireless door handle shall be available to add any time, in any quantity, without system re-architecture.

### Substitution Limitations

#### No substitutions.

## SPECIFIC REQUIREMENTS FOR TOKENS

### The manufacturer of the system shall be able to supply Paxton HiTag2 125KHz tokens.

#### The supplied tokens shall contain an authentication method to deter the copying and unauthorised use of tokens.

## SPECIFIC REQUIREMENTS FOR [PAXTON10] SERVER

### Features

#### The server shall store and manage the central database for the system.

#### The server shall be embedded on a powerful computer provided by the manufacturer.

##### The hardware shall be a Next Unit of Computing (NUC) platform designed by Intel®.

#### The manufacturer shall provide a USB storage device for external backups of the database.

##### This shall be provided at no additional cost.

##### The USB storage device capacity shall be at minimum 32GB.

##### Database backups shall be automatic.

#### The server shall be plug-and-play.

#### The server shall update all system hardware on the network to changes in the database.

#### The software to manage the system shall be pre-installed on the server.

##### The software shall be accessible from any workstation on the same network.

### User Interaction

#### The computer shall be plug and play.

#### After installation, no further interaction with the hardware shall be required.

### The server shall maintain the system database, containing at minimum, but not limited to:

#### User records:

##### Name

##### Email address

##### Valid from / valid until date

##### Image

##### Group membership

##### Permissions

##### Custom fields

##### User preferences

#### Reports:

##### A log of all system and user events

#### Dashboards

#### Site plans

#### Devices:

##### Name

##### Hardware mapping

##### Configuration

##### Group membership

##### Permissions

#### Rules

##### Custom rules and behaviours

##### User permissions

##### Time profiles / schedules

##### Roll Call configuration

##### Anti-passback behaviour

### Server hardware specification:

#### The computer shall contain at minimum an Intel i3 processor.

#### The computer shall contain at minimum 8GB of RAM.

##### The RAM shall be DDR3.

#### The computer shall contain an internal hard drive for storing the system database:

##### The hard drive shall be a Solid State Drive (SSD).

##### The hard drive shall have a storage capacity of at least 60GB.

#### The computer shall contain at minimum an Intel® HD Graphics 4000 graphics card.

### Power supply

#### The computer shall be powered with a 19V, 65W AC-DC power adapter.

##### This shall be provided by the manufacturer at no additional cost.

#### The computer shall consume at maximum 25W.

#### The computer shall include a voltage sensor.

#### The computer shall contain ACPI-compliant power management control.

### Temperature

#### The computer shall meet the required temperature standards for an internal product.

##### The computer shall operate reliably within the temperature range of 32°F to +122°F (0°C to +50°C)

### Housing

#### The housing design shall be stylish and modern.

#### The housing shall be made out of aluminium and plastic.

#### There shall be no visible fixings on any displayed faces.

#### The item shall be available in black.

### Dimensions

#### The dimensions of the server shall not exceed:

##### A width of 4.6" (116 mm)

##### A height of 4.4" (112mm)

##### A depth of 1.7" (42mm)

## SPECIFIC REQUIREMENTS FOR [PAXTON10] DOOR CONTROLLER {Delete as required}

### Features

#### The controller shall allow the control and monitoring of a single access point.

#### The controller shall be able to automatically unlock access points during specified time periods.

#### The controller shall store locally the system database for faster and offline lookup.

#### The controller shall allow the connection of additional connectors to the system, increasing its available I/O connections.

#### The controller shall provide the decision making and logic to a system.

#### The controller shall be provided with an external battery backup.

##### The system shall remain functional for a period of time during a power failure.

##### The system shall report battery state and charge for user diagnosis and reporting.

#### All data shall be retained during a power loss.

#### The controller shall feature detachable terminals for quick and hassle-free maintenance.

### User Interaction

#### The controller shall be plug and play.

#### After installation, no further interaction with the hardware shall be required.

### Display

#### The controller shall have colour coding representation for reader, exit device, communications, and power connections to simplify installation, maintenance, and troubleshooting.

#### The unit shall include installation LED’s to indicate the output relay status’, input status, and TCP/IP communications status.

### Power supply

#### It shall be possible to power the controller by:

##### Power over Ethernet (PoE / PoE+)

##### A 12V, 2A Power Supply Unit (PSU)

#### Power consumption while idle shall not exceed 3.0W.

#### Maximum power consumption shall not exceed 5.6W.

#### The controller shall be supplied with a 12V lead acid battery back-up.

### Temperature

#### The Controller shall meet the required temperature standards for an internal product.

##### The Controller shall operate reliably within the temperature range of 32°F to +113°F (0°C to +45°C).

### Housing

#### Wall mountable housing shall be available.

#### The housing shall be available in white.

#### The controller shall include removable connectors to provide ease of installation and board exchange if necessary. The connection points shall not require any special tools to terminate.

### Dimensions

#### The dimensions of the Controller, when housed, shall not exceed:

##### A width of 9.3" (236 mm)

##### A height of 12.7" (322mm)

##### A depth of 3.1" (77mm)

### Peripherals

#### The controller shall provide the peripherals to control and secure a single access point. The following hardware connections shall be available:

##### 1 x powered lock output

###### The lock output shall provide the power to secure and control a single maglock

###### The lock output shall provide 1A @ 12V DC

###### The lock output shall be configurable as a fail-open or a fail-close lock

##### 1 x door contact

###### The door contact shall monitor the current open/close state of an access point

##### 1 x powered exit button

###### An exit button shall allow free movement of travel through the access point

###### The exit button peripheral shall provide 12V output to provide visual indication and feedback at the exit button.

###### The exit button peripheral may be disabled in the system software if not being used, to avoid access being made through hardware tamper.

##### 2 x relay

###### Each relay shall be provided with N.O. and N.C. contacts.

###### Relay contacts shall be voltage free.

###### Each relay shall be capable of switching a resistive load of at least 2A @ 30V DC.

###### A relay may be configured as an alarm output

###### A relay may be configured as a lock output

###### A relay may be used for devices other than the secured access point

##### 2 x reader ports

###### It shall be possible to use a combination of proximity readers, keypad proximity readers, and vandal resistant readers.

###### The reader peripherals shall provide data and power to any connected readers.

###### The reader peripheral shall not be limited to a fixed data input, and instead shall accept data read from a variety of token types of different lengths, including but not limited to the following:

###### PIN

###### Code

###### Token ID

###### Bluetooth credential ID

###### The reader peripheral shall output current states relevant to the device to control for supplying feedback to the token holder in the form of an LED and speaker.

###### The reader peripheral shall provide the power that the reader requires to operate.

###### A reader may be used for devices other than the secured access point

##### 1 x digital input

###### A digital input may be configured as an exit button

###### A digital input may be configured to monitor an external PSU

###### A digital input may be used for devices other than the secured access point

#### It shall be possible to assign any peripheral to different devices or give custom functionality.

#### The controller shall provide a connector port.

##### Connectors shall communicate with the system via the controller.

##### The controller shall provide PoE to the connectors.

#### The controller shall provide a voltage free tamper switch.

##### The system shall generate an alarm event when a tamper switch is triggered.

#### The controller shall provide battery terminals.

##### A 12V DC 7Ah battery shall be installed.

##### The controller shall monitor the state and charge of the battery.

## SPECIFIC REQUIREMENTS FOR [PAXTON10] VIDEO CONTROLLER {Delete as required}

### Features

#### The controller shall allow the control and monitoring of a single access point.

#### The controller shall be able to automatically unlock access points during specified time periods.

#### The controller shall provide the processing and storage handling for at least 4 network cameras.

#### The controller shall process and record at least 2 video streams from each camera, in addition to a regular periodic QCIF image. The controller shall provide the system with:

##### A high-resolution video stream, up to 4K resolution at 20 FPS

##### A low-resolution video stream, up to 640 x 480 resolution at 15 FPS

##### A low resolution QCIF image, recorded at 1 FPS

#### The controller shall provide interface and power to two storage drives for video storage.

#### The controller shall store locally the system database for faster and offline lookup.

#### The controller shall allow the connection of additional connectors to the system, increasing its available I/O connections.

#### The controller shall provide the decision making and logic to a system.

#### The controller shall be provided with an external battery backup.

##### The system shall remain functional for a period of time during a power failure.

##### The system shall report battery state and charge for user diagnosis and reporting.

#### All data shall be retained during a power loss.

#### The controller shall feature detachable terminals for quick and hassle-free maintenance.

### User Interaction

#### The controller shall be plug and play.

#### After installation, no further interaction with the hardware shall be required.

### Display

#### The controller shall have colour coding representation for reader, exit device, communications, and power connections to simplify installation, maintenance, and troubleshooting.

#### The unit shall include installation LED’s to indicate the output relay status’, input status, and TCP/IP communications status.

### Power supply

#### It shall be possible to power the controller by:

##### Power over Ethernet (PoE+)

##### A 12V, 4A Power Supply Unit (PSU)

#### Power consumption while idle shall not exceed 3.9W.

#### Maximum power consumption shall not exceed 8.3W.

#### The controller shall be supplied with a 12V lead acid battery back-up.

### Temperature

#### The Controller shall meet the required temperature standards for an internal product.

##### The Controller shall operate reliably within the temperature range of 32°F to +113°F (0°C to +45°C).

### Housing

#### Wall mountable housing shall be available.

#### The housing shall be available in white.

#### The controller shall include removable connectors to provide ease of installation and board exchange if necessary. The connection points shall not require any special tools to terminate.

### Dimensions

#### The dimensions of the Controller, when housed, shall not exceed:

##### A width of 10.8" (275 mm)

##### A height of 12.6" (320mm)

##### A depth of 2.8" (70mm)

### Peripherals

#### The controller shall provide the peripherals to control and secure a single access point. The following hardware connections shall be available:

##### 1 x powered lock output

###### The lock output shall provide the power to secure and control a single maglock

###### The lock output shall provide 1A @ 12V DC

###### The lock output shall be configurable as a fail-open or a fail-close lock

##### 1 x door contact

###### The door contact shall monitor the current open/close state of an access point

##### 1 x powered exit button

###### An exit button shall allow free movement of travel through the access point

###### The exit button peripheral shall provide 12V output to provide visual indication and feedback at the exit button.

###### The exit button peripheral may be disabled in the system software if not being used, to avoid access being made through hardware tamper.

##### 2 x relay

###### Each relay shall be provided with N.O. and N.C. contacts.

###### Relay contacts shall be voltage free.

###### Each relay shall be capable of switching a resistive load of at least 2A @ 30V DC.

###### A relay may be configured as an alarm output

###### A relay may be configured as a lock output

###### A relay may be used for devices other than the secured access point

##### 2 x reader ports

###### It shall be possible to use a combination of proximity readers, keypad proximity readers, and vandal resistant readers.

###### The reader peripherals shall provide data and power to any connected readers.

###### The reader peripheral shall not be limited to a fixed data input, and instead shall accept data read from a variety of token types of different lengths, including but not limited to the following:

###### PIN

###### Code

###### Token ID

###### Bluetooth credential ID

###### The reader peripheral shall output current states relevant to the device to control for supplying feedback to the token holder in the form of an LED and speaker.

###### The reader peripheral shall provide the power that the reader requires to operate.

###### A reader may be used for devices other than the secured access point

##### 1 x digital input

###### A digital input may be configured as an exit button

###### A digital input may be configured to monitor an external PSU

###### A digital input may be used for devices other than the secured access point

#### It shall be possible to assign any peripheral to different devices or give custom functionality.

#### The controller shall provide two SATA ports for connecting external hard drives.

##### The controller shall provide a powered MOLEX output

##### The controller shall provide 2 SATA ports

##### The controller shall record video to the drives using RAID 1 configuration.

#### The controller shall provide a connector port.

##### Connectors shall communicate with the system via the controller.

##### The controller shall provide PoE to the connectors.

#### The controller shall provide a voltage free tamper switch.

##### The system shall generate an alarm event when a tamper switch is triggered.

#### The controller shall provide battery terminals.

##### A 12V DC 7Ah battery shall be installed.

##### The controller shall monitor the state and charge of the battery.

## SPECIFIC REQUIREMENTS FOR [PAXTON10] ALARM CONNECTOR {Delete as required}

### Features

#### The connector shall allow the control and monitoring of an intruder alarm.

#### The connector shall allow the monitoring of a fire alarm.

#### The connector shall be small and compact, for installation within an existing alarm cabinet.

#### The connector shall feature fault finding LEDs.

#### The connector shall feature detachable terminals for quick and hassle-free maintenance.

### Communications

#### The connector shall include TCP/IP interface for network communications directly into the processing board (controller) via an RJ45 connector. Add-on modules are not approved.

### Power Supply

#### The item shall operate from DC power supplied by the controller.

##### No additional power source shall be required.

##### Data and power shall use the same cable, minimising installation and setup cost.

#### Operating voltage shall be 30V.

#### Power consumption while idle shall not exceed 0.6W.

### Display

#### Peripherals shall be labelled clearly and intuitively.

##### Labels shall be graphical.

#### The item shall house LEDs for fault finding.

#### The following peripheral states shall be indicated:

##### Relay status

##### Input status (for each input)

#### An LED shall indicate when the item is powered.

### Temperature

#### The item shall operate reliably within the temperature range of +32°F to +131°F (0°C to +55°C).

### Housing

#### The item shall be small and compact such that it can be installed into existing housing used for the relevant alarm.

### Dimensions

#### The dimensions of the I/O connector shall not exceed:

##### A width of 2" (51mm)

##### A height of 2.7" (68mm)

##### A depth of 1.3" (34mm)

### Peripherals

#### The Alarm connector shall house a single controllable relay.

##### Each relay shall be provided with COM, N.O. and N.C. contacts.

##### Relay contacts shall be voltage free.

##### Each relay shall be capable of switching a resistive load of at least:

###### 2A @ 24V DC

###### 0.5A @ 125V AC

##### Each relay shall retain its state when the Alarm connector losses power.

##### The relay functionality shall be configurable in the access control software provided with the system.

#### The Alarm connector shall house 2 digital inputs.

##### Each input shall be formed of 2 terminals.

##### Each input shall be capable of withstanding at minimum 14V.

##### The thresholds that the system shall associate with each state shall be:

###### Low: < 0.8V

###### High: > 3.0V

##### Each input shall be configurable to trigger a Trigger and Action rule to perform automated tasks and custom behaviour.

#### The Alarm connector shall not contain a tamper switch input.

##### The Alarm connector shall be installed within the housing of an alarm or another connector, of which shall contain its own tamper.

##### It shall be possible to use a spare input on the Alarm connector or another connector to generate alarm events within the system if a tamper input is required.

## SPECIFIC REQUIREMENTS FOR [PAXTON10] WIRELESS CONNECTOR {Delete as required – Wireless connector required for PaxLock}

### Features

#### The connector shall provide communication with wireless door handles.

#### The connector shall provide communication with Z-Wave devices.

#### The connector shall be cascadable, allowing additional wireless connectors to be connected through one another, extending their wireless coverage.

#### The connector shall feature fault finding LEDs.

### Communications

#### The connector shall include TCP/IP interface for network communications directly into the processing board (controller) via an RJ45 connector. Add-on modules are not approved.

#### The connector shall contain a Bluetooth interface for communicating with electronic door handles.

##### The connector shall communicate using Bluetooth Low Energy (BLE) 2.4 GHz

#### The connector shall contain a Z-Wave interface for communicating with Z-Wave certified devices.

##### The connector shall communicate using Z-Wave 868.40 MHz and 869.85 MHz.

### Power Supply

#### The item shall operate from DC power supplied by the controller.

##### No additional power source shall be required.

##### Data and power shall use the same cable, minimising installation and setup cost.

#### Operating voltage shall be 30V.

#### Power consumption while idle shall not exceed 0.7W.

#### Power consumption during Bluetooth activity shall not exceed 0.8W.

### Display

#### The item shall house LEDs for fault finding. The following states shall be indicated:

##### Health / Communication

##### Bluetooth activity

##### Z-Wave activity

### Temperature

#### The item shall operate reliably within the temperature range of +32°F to +113°F (0°C to +45°C).

### Housing

#### The item shall be visibly appealing for installation within sight of users, reducing obstructions between the connector and its communicating devices.

#### The item enclosure shall be white.

#### The item shall be suitable for mounting:

##### On a wall

##### On a ceiling

##### On plasterboard

##### On a backbox

### Dimensions

#### The dimensions of the connector shall not exceed:

##### A width of 6.5" (164mm)

##### A height of 6.4" (163mm)

##### A depth of 1.3" (34mm)

### Peripherals

#### The wireless connector shall contain an RS485 port for daisy chaining to additional connectors.

##### Up to 3 connectors shall be daisy-chained from one controller

##### Power and communication shall be daisy chained.

## SPECIFIC REQUIREMENTS FOR [PAXTON10] CAMERAS {Delete as required}

### Features

#### All Paxton10 Core series cameras shall be capable of providing 1520p resolution. All Paxton10 Pro series cameras shall be capable of providing 4k resolution.

#### All cameras shall contain ultra-low light sensors for low light recording.

##### IR range of cameras shall be at least 30 meters.

#### All cameras shall contain in-built storage for direct recording onto the camera (edge storage).

#### Each camera shall provide the system with multiple video streams of different qualities:

##### Paxton10 Core series cameras:

###### A high-resolution video stream, up to 4K resolution at 20 FPS

###### A low-resolution video stream, up to 640 x 480 resolution at 15 FPS

###### A low resolution QCIF image, recorded at 1 FPS

##### Paxton10 Pro series cameras:

###### A high-resolution video stream, up to 1520p resolution at 20 FPS

###### A low-resolution video stream, up to 640 x 480 resolution at 15 FPS

###### A low resolution QCIF image, recorded at 1 FPS

#### Video shall only be recorded when motion is detected, maximising storage efficiency and minimising video footage of uninvolved scenes.

#### The manufacturer shall provide 6 variants of camera:

##### Mini Bullet Camera - CORE Series

##### Mini Dome Camera - CORE Series

##### Turret Camera - CORE Series

##### Mini Bullet Camera - PRO Series

##### Turret Camera - PRO Series

##### Vari-Focal Bullet Camera - PRO Series

#### All cameras shall be plug-and-play.

#### All cameras shall communicate over an IP network.

#### All data shall be retained during a power loss.

### Communication

#### The camera shall process and record its own video, without requiring constant communication to an external video recorder.

#### The camera shall communicate with the server and clients over TCP/IP.

#### The maximum video bandwidth shall be configurable to meet the requirements of the network.

### User Interaction

#### All cameras shall be plug and play.

##### By default, cameras shall record 1080p at 20 FPS.

##### By default, cameras shall record video footage to their internal storage.

#### The following camera parameters shall be configurable:

##### Video rotation

##### Video standard (PAL / NTSC)

##### Video resolution

##### Frame rate (FPS)

##### Maximum bitrate (Kbps)

#### For vari-focal cameras, the following additional configuration shall be available:

##### Focal length

#### The following video recording settings shall be configurable:

##### Video storage location

###### Internal – save to camera

###### External – Save to network location

##### Video storage period / Auto delete video after a defined period of time

#### After installation, no further interaction with the hardware shall be required.

### Power supply

#### Each camera shall be powered using PoE.

#### Maximum power consumption from any camera shall not exceed 15W.

### Temperature

#### Each camera shall meet the required temperature standards for an external product.

##### The camera shall operate reliably within the temperature range of -22°F to +140°F (-30°C to +60°C).

### Housing

#### Each camera shall be suitable for mounting:

##### On a wall

##### On a ceiling

#### Each camera shall be weatherproof to IP66.

### Dimensions

#### The dimensions of the Mini Bullet camera – CORE series shall not exceed:

##### A width of 2.9" (73 mm)

##### A height of 2.9" (74 mm)

##### A depth of 7.5" (191 mm)

#### The dimensions of the Mini Dome camera – CORE series shall not exceed:

##### A diameter of 4.8" (121 mm)

##### A depth of 3.6" (92.2 mm)

#### The dimensions of the Turret camera – CORE series shall not exceed:

##### A diameter of 5.5" (139 mm)

##### A depth of 5.0" (127 mm)

#### The dimensions of the Mini Bullet camera – PRO series shall not exceed:

##### A width of 2.8" (70 mm)

##### A height of 2.7" (68 mm)

##### A depth of 6.7" (171 mm)

#### The dimensions of the Vari-Focal Bullet camera – PRO series shall not exceed:

##### A diameter of 5.7" (144 mm)

##### A depth of 13.1" (333 mm)

#### The dimensions of the Turret camera – PRO series shall not exceed:

##### A diameter of 5.5" (139 mm)

##### A depth of 5.0" (127 mm)

### Peripherals

#### Each camera shall contain a memory card slot for internal video storage.

##### The camera shall support the following memory cards:

###### Micro SD

###### Micro SDHC

###### Micro SDXC

##### The camera shall support memory cards up to the capacity of 256 GB.

##### Memory write speed shall be at most 24 MB/s.

##### Memory read speed shall be at most 95 MB/s.

## SPECIFIC REQUIRESMENTS FOR [PAXTON10] SOFTWARE

### Web user interface

#### The software shall be hosted at the server.

#### The software shall be accessible from any computer with network access.

#### No installation shall be required at any client workstation.

#### The software shall be free of charge.

#### The manufacturer of the software shall provide updates and upgrades free of charge.

#### The software shall offer all features required to manage an access control system.

#### The software shall offer all features required to manage a video management system.

### Remote access

#### It shall be possible to access the software from anywhere in the world with an internet connection.

#### This shall be permissionable in the software to restrict remote access to selected users.

### Client workstation requirements

#### It shall be possible to access the software from any computer or device running the latest version of:

##### Google Chrome.

##### Apple Safari

#### It shall be possible to access the software from any smartphone or tablet using a dedicated app.

##### The app shall be available on the following operating systems:

###### iOS

###### Android

##### The app shall be free of charge.

### View

#### The software shall provide a clean and simple user interface.

#### Navigation shall be visible on all screens, to allow for quick navigation to all areas of the software.

#### A top ribbon shall be provided offering further controls.

##### It shall be possible to minimise the ribbon, to provide increased working area.

##### To retain simplicity, the ribbon shall populate with the controls relevant to the currently viewed item.

#### It shall be possible to adjust how entities are presented:

##### Large icons, which shall be ideal for touch screen devices and also useful for graphical searching. User, and other entity images shall be displayed when viewing large icons.

##### Details, which shall provide additional information where relevant and allow the sorting of entities for more advanced use.

#### How the software is viewed shall be saved for each software user, such that their design and layout preference is remembered each time they log in.

### Interaction

#### The software shall support touch-screen interaction.

#### The software shall support mobile devices.

#### Tooltips shall be provided for every control to inform behaviour.

### Grouping

#### The software shall provide a simple yet effective method for organising software entities.

#### The software shall allow for segmentation and arrangement to suit department and building schemes.

### Data management

#### The software shall provide the capabilities to comply with data protection regulations.

#### All software users shall be enforced to create a strong password.

#### The software shall provide the ability to:

##### Delete users

##### Delete reports

##### Delete events

##### Delete events automatically after a specified period of time

##### Erase video

##### Erase video automatically after a specified period of time

### Language

#### The software shall be available in the following languages:

##### English (UK)

##### English (US)

##### French

##### German

##### Spanish

### Help and support

#### The software shall provide help to software users in the form of tooltips, wizards, videos and documentation.

##### Wizards shall guide users through specific tasks, giving the user the ability to complete their task as they learn the steps requires.

##### Videos shall provide instructions and supporting information to complete tasks and explore areas of the user interface.

##### Documentation shall consist of application notes, instructions, and datasheets.

##### Tooltips shall be available upon hovering a cursor over controls and options.

###### Where available, tooltips shall contain a link to direct the user to further information.

#### An inbuilt help tool shall allow the user to locate the support information they require.

##### The help tool shall be accessible from all locations of the software.

### Release notes

#### When a software update is available, release notes shall be presented to the user.

#### The release notes shall inform the user what the update will contain, and any important information relating to the update.

## SPECIFIC REQUIRESMENTS FOR [PAXTON10] SOFTWARE FEATURES

### People

#### Users shall be added to the system using the software.

##### It shall be possible to create at minimum 50,000 users.

##### It shall be possible to assign at minimum 50,000 unique credentials to users.

#### Users shall be assigned permissions to determine what each individual user can action, configure, or view.

##### Users shall only have access to access points and control of devices that are within the permissions that are assigned to them.

##### Users shall be able to log in to the software and view/modify areas that are within the permissions assigned to them.

#### Each user record shall contain input fields to store user data.

##### The following fields shall be available by default:

###### Email address

###### Valid from date

###### Expiry date

##### Further fields shall be available where required to capture additional information:

###### Mobile number

###### Car registration

###### Address 1

###### Address 2

###### Town

###### Country

###### Post code

##### It shall be possible to create custom input fields where the above do not cover the data required to be stored for each user. A label to display and the data type of the data to be input/stored shall be selectable. The following types of data shall be supported:

###### Boolean – checkbox

###### Date

###### Email

###### Number

###### Text

#### It shall be possible to upload an image of each user.

##### Each user record shall have a person silhouette as a default image.

##### It shall be possible to upload an image to replace the default image.

##### The software shall allow images of up to 4Mb to be uploaded.

##### At minimum, the following image formats shall be supported:

###### JPEG

###### JPG

###### GIF

###### PNG

##### It shall be possible to edit the uploaded image within the software. At minimum, it shall be possible to achieve the following:

###### Crop the uploaded image.

###### Place a border around the uploaded image.

###### Add a shadow to the uploaded image.

##### The image shall be used:

###### As a way of identifying a user

###### As a method of searching for users alongside their name

###### In site plans to associate a user with a credential being read

###### In video reports to associate a user with a credential being read

###### In dashboards for identifying a user

###### In roll call reports as visual confirmation

#### It shall be possible to assign credentials to a user.

##### The following credential types shall be supported:

###### Password

###### Token

###### Smart credential

###### PIN

##### Passwords shall be required for a user to access the software.

###### Users shall be restricted to having only a single password.

###### Passwords shall be created by the user when attempting to log-in for the first time.

###### The software shall enforce passwords to fit a criteria for security purposes.

###### Passwords shall:

###### Contain at least 7 characters.

###### Contain at least 3 different character types: Uppercase / Lowercase / Number / Punctuation

##### Tokens shall be required for a user to have access and control of access points and devices on a system.

###### It shall be possible to assign multiple tokens to each user.

###### Tokens shall be added to the system by means of:

###### A desktop reader provided by the manufacturer of the software.

###### An invalid access event

###### Multiple types of credential shall be supported. It shall be possible for users to select a type and give the credential a name for usability and reference purposes.

###### Each token type shall be distinguished with a unique image.

###### It shall be possible to mark a token as lost, which shall remove all access rights from that token while allowing the user to remain active with other tokens.

##### Smart credentials shall allow users to use their Smartphone or tablet to gain access and control of access points and devices on a system.

###### It shall be possible to assign multiple Smart credentials to each user.

###### Smart credentials shall exist as a registered application on a user’s Smart device.

###### The following mobile operating systems shall be supported:

###### Android

###### iOS

###### Smart credentials shall be free to issue and use.

###### Smart credentials shall be issued from the software via email.

###### The Smart credential email shall contain instructions, a download link, and a unique registration ID for the addressed user.

###### The registration ID shall only be valid for a single device.

###### It shall be possible to mark a Smart credential as lost, which shall remove all access rights from that token while allowing the user to remain active with other tokens.

###### It shall be possible to require verification when using Smart credentials. Where verification is required, a user shall authenticate themselves using:

###### Fingerprint, using their devices inbuilt biometric reader

###### Passcode or Pattern, using their devices inbuilt secure lock

###### It shall be possible to enter a time profile for when verification is required.

##### PINs provide a token-free way of validating and identifying a user.

###### Users shall be restricted to having only a single PIN.

###### The PIN length shall be configured in the software to meet the security requirements of the project.

###### The system shall generate a key hacker alarm event when multiple failed attempts are made at a keypad reader, protecting against hackers and unauthorised access attempts.

##### It shall be possible to require a combination of credentials from a user, such as Token + PIN, to ensure security of the site.

#### It shall be possible to bar a user.

##### Barring a user shall remove their access and control of all access points and devices.

##### Barring a user shall remove their access to the software.

##### It shall be possible to unbar a user to restore all of their previous permissions.

### Devices

#### Hardware shall be represented and configured as software entities, referred to as ‘devices’.

#### The software shall support the following types of device:

##### Access point

##### Controllable device

##### Digital input device

##### Intruder alarm

##### Fire alarm

##### Camera

##### Video recorder

#### It shall be possible to associate the created software device with the hardware it is to represent.

##### Configuration within the software device shall take affect at the hardware to perform the desired behaviour.

#### Access points shall provide the following configuration:

##### Operating mode:

##### Timed, which shall unlock the access point for a specified time upon each valid credential read.

##### Toggle, which shall invert the status of the lock upon each valid credential read.

##### Door open time, which shall determine how long the access point remains unlocked for when operating in timed mode.

##### Unlock schedule, allowing the access point to remain unlocked during specified periods.

##### Reader LED, allowing any mapped readers to have their LEDs toggled on or off.

##### Reader sound, allowing any mapped readers to have their sound muted or enabled

##### Always allow exit, which when enabled shall permit valid users to exit, even outside of their permissioned time.

##### Authentication options, configuring the credential type users must provide to access the area.

##### Bluetooth read range, configuring how Smart credentials and Bluetooth tokens operate.

##### Alarms to sound:

##### Door left open

##### Door forced

##### PSU fail

##### Cameras, which shall associate camera footage with events relating to the access point.

#### Controllable devices shall provide the following configuration:

##### Operating mode:

###### Timed, which shall turn on the device for a specified time upon each valid credential read.

###### Toggle, which shall invert the status of the device upon each valid credential read.

###### Momentary, which shall change the state of the output for a split second, before changing back.

##### On time, which shall determine how long the device remains on when operating in timed mode.

##### On schedule, allowing the device to remain on during specified periods.

##### Reader LED, allowing any mapped readers to have their LEDs toggled on or off.

##### Reader sound, allowing any mapped readers to have their sound muted or enabled

##### Always allow switch off, which when enabled shall permit valid users to turn off the device, even outside of their permissioned time.

##### Authentication options, configuring the credential type users must provide to control the device.

##### Bluetooth read range, configuring how Smart credentials and Bluetooth tokens operate.

##### Cameras, which shall associate camera footage with events relating to the device.

#### Digital input devices shall provide the following configuration:

##### Event, allowing the user to define an event that should be raised when the input changes state.

##### Cameras, which shall associate camera footage with events relating to the device.

#### Intruder alarms shall provide the following configuration:

##### Under what input condition the alarm is armed.

##### Under what input condition the alarm is active.

##### Pulse duration required to change the alarm state.

##### Exterior doors, allowing selected doors to remain locked while the intruder alarm is armed.

##### Disarm doors, allowing the intruder alarm to be disarmed at the selected doors.

##### Reader LED, allowing any mapped readers to have their LEDs toggled on or off.

##### Reader sound, allowing any mapped readers to have their sound muted or enabled

##### Authentication options, configuring the credential type users must provide to control the alarm.

##### Bluetooth read range, configuring how Smart credentials and Bluetooth tokens operate.

##### Cameras, which shall associate camera footage with events relating to the alarm.

#### Fire alarms shall provide the following configuration:

##### Under what input condition the alarm is active.

##### Fire doors, ensuring selected doors are unlocked when the fire alarm is active.

##### Cameras, which shall associate camera footage with events relating to the alarm.

#### Cameras and Video recorders shall provide the following configuration:

##### Record schedule, configuring during which periods of time the camera shall record.

##### Record location, providing the ability to save video to a network location or onto the camera or video recorder.

##### Video storage period, allowing video to be automatically erased after a defined number of days.

##### Video rotation, which shall allow the video footage to be rotated **{Paxton10 cameras only}**

##### Camera focal length, which shall allow the camera focal length to be adjusted **{Paxton10 veri-focal cameras only}**

##### Video quality, allowing the system to view, and for some cameras configure, the video resolution, frame rate, and maximum bitrate.

##### A video preview shall be provided within view of the camera’s configuration.

##### Devices, which shall associate video footage with events at the selected devices.

### Event reports

#### Event reports shall be used to display system activity.

#### Events shall be generated for, but not limited to:

##### Valid credential read

##### Invalid credential read (unknown credential, invalid permissions, credential marked as lost)

##### Access point unlocked/locked

##### Device turned on/off

##### Input change of state

##### Alarm at an access point (door forced, left open, tamper)

##### Intruder alarm armed/disarmed

##### Intruder alarm active

##### Fire alarm active

##### System events (hardware online/offline, server events)

##### Software events (person/device modified)

#### It shall be possible to filter events by the following criteria:

##### The user that the event relates to.

##### The device that the event relates to.

##### The time that the event occurred.

##### The type of event (credential read / alarm / system / software)

##### Contains video footage

#### A selection of default reports shall exist to display common areas of interest, including the following:

##### All events

##### All events last week

##### All events this week

##### All events today

##### All events yesterday

##### Expired tokens

##### First and last events

##### Last known position

##### List all users

##### Lost tokens

##### Permissions

##### Token last used

##### Unused tokens

##### Who’s been in today

#### The user shall be able to create custom reports to match their own requirements.

#### The following event interaction shall be available:

##### View video associated with an event.

##### View the person’s profile that an event relates to.

##### Acknowledge an alarm and leave a comment on the event.

##### Add a credential to the system from an access denied event.

##### Mark a user as safe or unsafe in a roll call report.

#### The events displayed in a report shall be filtered to only show those the viewer has permission to see.

### Video reports

#### Video reports shall be used to display live and archived video recorded by cameras in the system.

#### Video reports shall be scalable, providing view from 1 camera, up to a maximum of 20 cameras.

##### The display shall dynamically adjust to provide optimum viewing for the number of cameras in the report.

##### The video stream displayed shall adjust based on the number of cameras currently in display, optimising network bandwidth usage and client viewing area.

#### It shall be possible to view events within a video report.

##### The events shall be pre-filtered to show only the events that relate to the devices which can be seen by the cameras in the report.

##### It shall be possible to filter the events that are displayed.

##### Device related events and user details shall be overlaid onto the video where appropriate.

#### A selection of playback options shall be available, including:

##### Play/pause playback

##### Alter playback speed

##### Jump back 15 seconds

##### Go to live video

##### Timeline scrubber with QCIF preview

#### Camera view controls shall be available, including:

##### Show/hide camera name

##### Show/hide camera time

##### These settings shall not affect the camera itself or the video recording, they shall only affect the playback and view for the current client.

#### It shall be possible to export a clip of video to a network location.

##### The period to export shall be identified using a simple and graphical user interface.

##### By default, 5 minutes of video clip shall be selected.

###### Minimum clip duration shall be 1 minute.

###### Maximum clip duration shall be 30 minutes.

##### The clip shall be downloaded in MP4 format.

#### It shall be possible to export a still snapshot from video to a network location.

##### The system shall provide a selection of snapshots images surrounding the selected time.

##### The snapshot shall be downloaded in JPEG format.

#### It shall be possible to bookmark a moment in time for future reference.

##### It shall be possible to give a bookmark a name or description.

##### Bookmarks shall be clearly identified on the video timeline.

##### Bookmarks shall be automatically deleted when video is removed.

##### Controls shall be available to easily navigate through all bookmarks.

##### There shall be no limit to the number of bookmarks that can be created.

#### Smart search shall be available for searching for motion within recorded video.

##### Smart search shall allow users to easily locate when an item was moved, or when activity occurred.

##### A user shall be able to highlight areas over multiple video streams, which shall search the video streams for when motion occurred during the specified areas.

#### Digital zoom shall allow users to zoom in on a video stream to view additional detail.

##### When zooming in on a video stream, the system shall switch to the highest resolution stream it has available for the specified camera.

##### Digital zoom shall not affect the recording of the video, or the viewing for other users.

##### Digital zoom shall be available using on screen controls, mouse wheel, and touch screen.

#### Full screen and modal display for enlarged viewing.

##### It shall be possible to place each camera individually in full screen or in a modal.

##### When displayed full screen or in a modal, the system shall switch to the highest resolution stream it has available for the specified camera.

#### There shall be no limit to the number of video reports that can be created.

#### The viewing of a video report shall be permissionable such that each software user can only view the video they are permitted to see.

### Dashboards

#### Dashboards shall provide a customised view with user specific controls, setup to meet the requirements of each user.

#### Dashboards shall be made up of a combination of the following widgets:

##### Events

###### When added to a dashboard, an events widget shall display all system event and activity.

###### It shall be possible to filter the events widget to show only specific events.

##### System alerts

###### When added to a dashboard, a system alerts widget shall monitor system and access alarms.

###### It shall be possible to configure the widget to show alarms for specific devices or alarm types.

###### The widget shall provide information of the most recent alarm events.

###### It shall be possible to view video of an alarm event.

##### Alarm systems

###### When added to a dashboard, an alarm systems widget shall monitor the current state of selected fire alarms or intruder alarms.

##### Video

###### The video widget shall add video cameras to a dashboard, providing live and archived video viewing.

###### Each video widget shall provide view of a single camera’s video.

###### The following controls shall be supported when viewed in a dashboard:

##### Full screen / modal

##### Alter playback speed

##### Jump back 15 seconds

##### Go to live video

##### Timeline scrubber with QCIF preview

##### Digital zoom

##### Export clip

##### Export snapshot

##### Show/hide camera name

##### Show/hide camera time

##### Mute/unmute audio

##### Soft buttons

###### Soft buttons shall allow custom defined actions from a click of a button.

###### Soft button behaviour shall be configured and managed in a central location.

###### Soft buttons shall be graphical and indicate when they have been pressed.

###### A single widget shall contain any number of soft buttons.

##### Business card

###### When added to a dashboard, a business card widget shall display the image and details of each user as they interact with the system.

###### The business card widget shall display a user’s image as the user enters an area.

###### The business card widget shall display a user’s details as the user enters an area.

###### The widget shall be configurable to which device or access point to monitor, and the events to display.

###### It shall be possible to view the video of a user’s interaction.

##### Site plan

###### When added to a dashboard, a site plan widget shall provide a graphical interactive map of the site.

###### The widget shall display a site plan from the system.

###### The site plan shall be created and managed in a dedicated area in the software.

###### The widget shall allow navigation to other site plans.

###### The widget shall provide the following functionality and interaction:

##### Unlock door

##### Control device

##### Arm/disarm alarm

##### Acknowledge alarm

##### Navigate to device configuration

##### View device’s events

##### View device’s video

##### View camera video

##### Who’s in today

###### The widget shall provide a roll call of users that have been recorded on site on the current day.

###### The widget shall provide the following details:

##### Person name

##### Person group or department

##### Date and time they were recorded

##### Location (device) they were recorded at

##### Weather

###### A weather widget shall provide a weather forecast for a specified location.

###### The widget shall allow free text location lookup.

#### Dashboards shall be made up of between 1 and 16 widgets.

#### The widgets and their arrangement shall be defined by the client.

#### There shall be no limit to the number of dashboards that can be created.

#### Dashboards shall be permissionable such that each software user only views the dashboards appropriate for their tasks and role.

### Site plans

#### Site plans shall provide graphical viewing and interaction with the site.

#### It shall be possible to upload an image to use as a site plan.

###### The software shall allow images of up to 4 MB to be uploaded.

###### At minimum, the following image formats shall be supported:

###### JPEG

###### JPG

###### GIF

###### PNG

###### It shall be possible to crop the uploaded image within the software.

#### Devices shall be added to a site plan to represent the physical access point or device.

##### Device icons shall indicate the device’s current state by changing colour and flashing.

##### Device icons shall display events associated with the device as they occur.

##### It shall be possible to interact with the device icon to control the device or unlock the door.

##### It shall be possible to view a camera’s video from a site plan.

#### Navigation icons shall be added to a site plan to provide links to other site plans, allowing navigation between different sites or multiple floors of a building.

##### When clicked, navigation icons shall direct the user to a defined site plan.

##### Navigation icons shall display event icons to represent events occurring at devices on the linked site.

##### The transition used when switching site plans shall mimic the site’s perspective location.

#### Soft buttons shall be added to a site plan to provide custom defined actions from a click of a button.

##### Soft buttons shall be configurable by the user to perform a variety of actions when clicked.

##### Soft button behaviour shall be configured and managed in a central location.

##### Soft buttons shall be graphical and indicate when they have been pressed.

#### Alarm areas shall be added to a site plan to highlight important activity.

##### Alarm areas shall indicate alarm events for selected devices, such as intruder alarm sounding.

##### Alarm areas shall highlight part or all of a site plan to alert the user.

##### It shall be possible for a user to define the area that the alarm represents.

#### Labels shall be added to a site plan to provide user instructions and area titles.

##### Labels shall be simple text labels that can provide additional information and notes to the site plan.

#### A site plan shall be viewable in 2D and 3D.

##### While in 3D, it shall be possible to rotate the site plan.

### Building permissions

#### Building permissions shall be used to manage user access of devices.

#### There shall be no limit to the number of building permissions that can be created.

#### It shall be possible to assign users to multiple building permissions.

#### It shall be possible to assign devices to multiple building permissions.

#### It shall be possible to assign time profiles to multiple building permissions.

#### A user shall only have access to a device if they are combined in a building permission with an active time schedule.

### Software permissions

#### Software permissions shall be used to manage user access of the software.

#### There shall be no limit to the number of software permissions that can be created.

#### It shall be possible to assign users to multiple software permissions.

#### It shall be possible to select various levels of permissions to each software section. The following levels shall be possible:

##### Full – access to create/modify/delete

##### Read – access to view

##### Events – access to see events

#### A user shall only have access to the software if they are included in a software permission.

##### A user shall only have access to the areas of software specified in the software permission.

#### The following software areas shall be individually permissionable:

##### Dashboards, or specified groups of dashboards

##### Reports, or specified groups of reports

##### Site plans, or specified groups of site plans

##### People, or specified groups of people

##### Rules, or specified groups of rules

##### Devices, or specified groups of devices

##### Hardware management

##### Options

##### Software events

##### Hardware events

##### Remote access

### Time profiles

#### Time profiles shall be used to enable different functionality and behaviour for different times of the day or days of the week.

#### There shall be no limit to the number of time profiles that can be created.

#### It shall be possible to assign a different time schedule for at minimum 28 days in a single time profile.

#### Custom days shall be used to provide unique or abnormal functionality of specified days.

##### There shall be no limit to the number of custom days that can be created.

##### It shall be possible to assign a different time schedule for custom days.

##### Where custom days occur, time schedules shall be overwritten by those defined for the custom day.

#### The layout shall be graphical and easy to use, consisting of click-and-drag controls.

### Triggers and Actions

#### Trigger and action rules shall provide the system with bespoke functionality, defined by configuration.

#### The software shall allow trigger and action rules to be created to perform unique behaviour and to provide further functionality to the system.

#### There shall be no limit to the number of trigger and action rules that can be created.

#### It shall be possible to perform an action when a selected trigger occurs. The list of triggers shall include, but not be limited to:

##### Valid credential read

##### Invalid credential read

##### Input opened

##### Input closed

##### Input change of state

##### Exit request / exit button pressed

##### Door forced alarm

##### Door left open alarm

##### Intruder alarm armed

##### Intruder alarm disarmed

##### Intruder alarm activated

##### Fire alarm activated

##### Start of time profile

##### End of time profile

##### Soft button pressed

#### It shall be possible to constrain when a rule is run by the state of other devices on the system. The list of constraints shall include, but not be limited to:

##### Input high

##### Input low

##### Intruder alarm armed

##### Intruder alarm disarmed

##### Intruder alarm active

##### Intruder alarm inactive

##### Fire alarm active

##### Fire alarm inactive

##### Access point open

##### Access point closed

##### Output on

##### Output off

#### When a trigger occurs and all constraints are met, multiple actions can occur. The list of actions shall include, but not be limited to:

##### Unlock access point

##### Lock access point

##### Toggle access point

##### Switch on appliance

##### Switch off appliance

##### Toggle appliance

##### Arm intruder alarm

##### Disarm intruder alarm

##### Run roll call report

#### There shall be no limit to the number of triggers, constraints, and actions, that a rule can consist of.

### Anti-passback

#### Anti-passback rules shall provide the ability to monitor and restrict sequential access attempts.

#### There shall be 2 types of anti-passback available:

#### It shall be possible to specify the people that are enforced by an anti-passback rule.

#### It shall be possible to specify the access points that an anti-passback rule applies to.

##### Traditional

###### Once a user has entered through one of the defined access points, they cannot re-enter until they have been seen to exit.

###### Forgiveness shall be possible, resetting all in/out statuses at a defined time each day.

##### Timed

###### Once a user has entered through one of the defined access points, they cannot re-enter for a defined period of time.

###### It shall be possible to allow users to re-enter within this period if they have been seen to exit.

#### There shall be 2 types of access restriction:

##### Hard anti-passback – being non-compliant with the rule will restrict the user’s access.

##### Soft anti-passback – being non-compliant with the rule will allow access as per the user’s permissions, while raising an event to inform administrators of the violation.

#### There shall be no limit to the number of anti-passback rules that can be created.

### Roll call

#### The software shall provide roll call functionality.

#### Roll call rules shall be used to configure roll call functionality.

##### Each rule shall define the access points that make up an area.

##### Each rule shall define the muster readers located at each muster point for the area.

#### Roll call reports shall be used to list all users in an area at the point of report generation.

##### The report shall be generated following the configuration of an individual roll call rule.

##### It shall be possible to automate the generation of a roll call report in event of an emergency.

##### It shall be possible to automatically E-mail a roll call report upon generation.

#### The roll call report shall be viewable in the software.

#### The roll call report shall provide:

##### View of all users within an area.

##### User information, including name, email address, and any information stored for users.

##### User image.

##### Last known location of each user.

##### Missing / Safe status

###### Users can be marked as safe within the report.

###### Users can mark themselves as safe my presenting their token to a designated muster reader.

#### Only users that are known to be in an area will be included on the report when it is generated.

##### It shall be possible to clear the report at a defined time each day.

##### It shall be possible to remove users from the report after being inactive for a defined time.

### Hardware management

#### Hardware shall be mapped to the software using simple click and drag.

#### Hardware shall be managed in a central location.

#### The software shall report details of all bound hardware, including:

##### Hardware type

##### Serial number or unique ID

##### Subnet

##### IP address

##### Battery status

##### Firmware version

##### Online status

#### Hardware management shall be permissionable to selected software users.

#### Mapping hardware peripherals to deivces shall be flexible and versatile, allowing for devices to consist of multiple components from a number of hardware

##### It shall be possible to associate any output peripheral (relay) with a:

###### Lock for an access point

###### Alarm for an access point

###### Controlled output for a device

###### Arm control for an intruder alarm

##### It shall be possible to associate any digital input peripheral with a:

###### Exit button for an access point

###### Door contact for an access point

###### Digital input for a device

###### Alarm arm status for an intruder alarm

###### Alarm active status for an intruder alarm

###### Alarm active status for a fire alarm

##### It shall be possible to associate any reader with a:

###### Access point to monitor and restrict access

###### Controllable device to monitor and restrict use

###### Intruder alarm to monitor and restrict arming/disarming.

### Control device

#### The software shall allow for controlling system hardware remotely from the software.

#### At minimum, the following shall be possible from the software:

##### Unlock an access point

##### Turn on / turn off / toggle the state of a controllable device

##### Arm / disarm an intruder alarm.

#### Software users shall be restricted to only have access to control the devices remotely that they would be able to control if they had presented their token to a reader.

### Remote access

#### The software shall be accessible from anywhere with an internet connection.

##### It shall be possible to enable / disable this feature.

##### It shall be possible to restrict remote login to any group or individual.

#### When accessing remotely, no software installation or complex manual addressing shall be required.

#### When accessing remotely, the UI shall be identical to when accessing locally.

### Home page

#### A Home page shall provide users with a central place for viewing and managing their system.

#### The home page shall provide access to:

##### Creating new entities on the system

##### Favourites.

#### The home page shall provide a summary of the system and its activity, including:

##### Summary

###### Number of active users

###### Total number of users

###### Total number of devices

##### Notifications

###### Number of unacknowledged alarm events

###### Number of offline devices

###### Number of logged in users

##### System activity

###### Graph of access events per day, over the last 7 days

### Favourites

#### The software shall provide each software user with a customisable ribbon for control and navigational shortcuts.

#### It shall be possible for a user to add the following to the favourite’s ribbon:

##### Links – for quickly navigating to areas of the software.

##### Actions – for performing a device’s default action.

#### It shall be possible for a user to arrange shortcuts and actions on the favourite’s ribbon.

##### This shall be presented in a graphical, drag-and-drop interface.

#### Users shall have the option to open a specific area of software by default when they log in.

#### All favourites and options shall be stored per user, such that each software user can have their own personalised favourites and settings.

###  User import

#### It shall be possible to import user data into the system.

#### The following file formats shall be supported:

##### .xlsx

##### .xls

##### .csv

##### .text

##### .txt

#### The user shall be able to preview the data prior to the import taking place.

### Intercom / Access Entry Station

#### The software shall support an intercom station capable of allowing access entry from a remote monitor and/or an integrated access control reader.

##### The software shall report events from the intercom system.

##### The software shall provide the access point configuration used with the intercom system.

##### The entry panel shall be automatically detected by the system.

#### The intercom system shall meet the following criteria:

##### The reader will be built-in to the entry panel so that it is not visible accept by a label or graphical representation, so the user knows where to present their credential.

##### An LCD screen will be used to display and communicate verbally with the specified employee. Up to 1000 names can be displayed.

##### Once communications channel is open, the employee shall be able to view the visitor through the desktop station display monitor. An internal camera is included in the entry station.

##### All communications, audio, video and power shall be via a single cable using TCP/IP and Power-over-Ethernet, using IPV6 technology.

##### The remote display station shall include a monitor to view who is at the entrance.

##### The remote display station can initiate the communications to the entry station and make an announcement or to view video, as well as unlock the door.

##### Up to 100 stations can be on a single system and up to 1000 monitors.

##### A low-light colour camera will be included with the unit as default, and be housed internally to avoid damage due to vandalism.

##### A series of LED’s shall be included to illuminate the immediate area for night-time viewing.

##### If only one intercom station and one monitor are on the system – no configuration shall be required.

##### The unit shall not require an IP address to be configured. All units within the same LAN shall auto-detect each other on power up.

##### Where a keypad is present, the number five button shall have a unique design for touch reference.

##### The intercom station shall not require any external power, other than what is provided via POE to the main processor board. All power for the cameras, intercom and access panels shall be included.

##### A flush mount housing shall be available.

##### Any smart phone, computer, tablet can be used with the Entry system using SIP Compliance and an industry standard SIP (session initiation protocol) Server.

## SPECIFIC REQUIREMENTS FOR DESKTOP READER

### Features

#### The desktop reader shall facilitate assigning tokens to users.

#### The desktop reader shall read multiple types and formats of proximity tokens.

#### The desktop reader shall identify tokens/credentials that have already been assigned to users.

#### The desktop reader shall eliminate the need to know each token’s number.

#### In systems with several client PCs, the system shall be able to support multiple desktop readers.

#### The desktop reader shall output a unique ID from each token presented.

#### The desktop reader shall output a unique ID from a variety of formats and lengths.

### User interaction

#### The desktop reader shall operate in an intuitive mode:

##### When an unassigned token/credential is presented, the system software shall automatically create the user record and user screen for entering user information as well as other security settings.

##### When the operator is already in a user record, and an unassigned token/credential is presented, the software shall display the option to add the token/credential to the current record.

##### When an existing token/credential is presented to the desktop reader, the software shall automatically retrieve and display the user record associated with that user. If there are multiple tokens/credentials assigned to that user, the software shall highlight the specific one presented.

#### The reader shall be plug & play.

### Proximity reader

#### The item shall contain a proximity reader.

##### At a minimum, the following token technology shall be supported:

###### Paxton HiTag2 125KHz

###### HID 125KHz

###### EM4100/02

###### EM4200

###### Sony FeliCa Lite-S

###### MIFARE 1K

###### MIFARE 4K

###### MIFARE Ultralight / C

###### MIFARE DESFire / EV1

###### MIFARE Mini

##### All of the above token technology shall be supported concurrently.

##### The following formats of credential shall be supported:

###### ISO card

###### Clamshell

###### Minifob / keyfob

###### Proxidisc

###### Watchprox

###### Hands free token

### Power supply

#### The item shall be powered via USB.

### Communication

#### The desktop reader shall connect to a PC via a Mini USB to USB cable.

### Display

#### The item shall house a stylish LED display.

#### The LEDs shall indicate the following states:

##### Item powered / ready to use

##### Credential being read

### Temperature

#### The item shall meet the required temperature standards for an internal product

##### The item shall operate reliably within the temperature range of 0°C to +49°C (32°F to 120°F)

### Housing

#### The item shall be stylish and modern.

#### The product shall be available in black

### Dimensions

#### The desktop reader dimensions shall not exceed:

##### A width of 115mm (4.5")

##### A height of 19mm (0.7")

##### A depth of 75mm (3")

END OF SECTION

MIFARE®, MIFARE® Classic, DESFire®, MIFARE® Plus and MIFARE® Ultralight C are trademarks of NXP B.V.

FeliCa® is a registered trademark of Sony Corporation.

HID is a registered trademark of HID Global Corporation.

Intel® is a registered trademark of Intel Corporation.

Microsoft and Windows are registered trademarks of Microsoft Corportation.

Bluetooth is a registered trademark of Bluetooth SIG.