Planning a Paxton10 System

Overview

A system is comprised of a number of components:

Server

The server is where all information is stored. Each system must have one server. The server does not have a direct connection to any other component, instead it connects directly to the network.

Clients

Clients are the devices that will have access to the software. Once a user has been given permission, they can access the software with their e-mail address. This can be done using a web browser on a computer or a mobile device. This can be either locally on the network or from a remote location.

Paxton10 Door Controllers

Paxton10 Door Controllers are responsible for opening and closing doors on site. They communicate with the Paxton10 server via the network. Each controller acts independently of others, meaning if a single controller goes offline the rest of the system can continue normal operation.

Paxton10 Video Controllers

Paxton10 Video Controllers offer the same functionality of a Paxton10 Door Controller but add the ability to connect third party IP cameras and record footage locally onto connected hard drives.

Note: Video can be saved to a NAS drive. If using 2.5"HDD SATA drives they must be 24/7 surveillance grade, support RAID1 and provide 1TB of storage.

Alarms

Alarm connectors are connected using an expansion port on a Paxton10 Door Controller, or Paxton10 Video Controller. They enable integration with fire and intruder alarms.

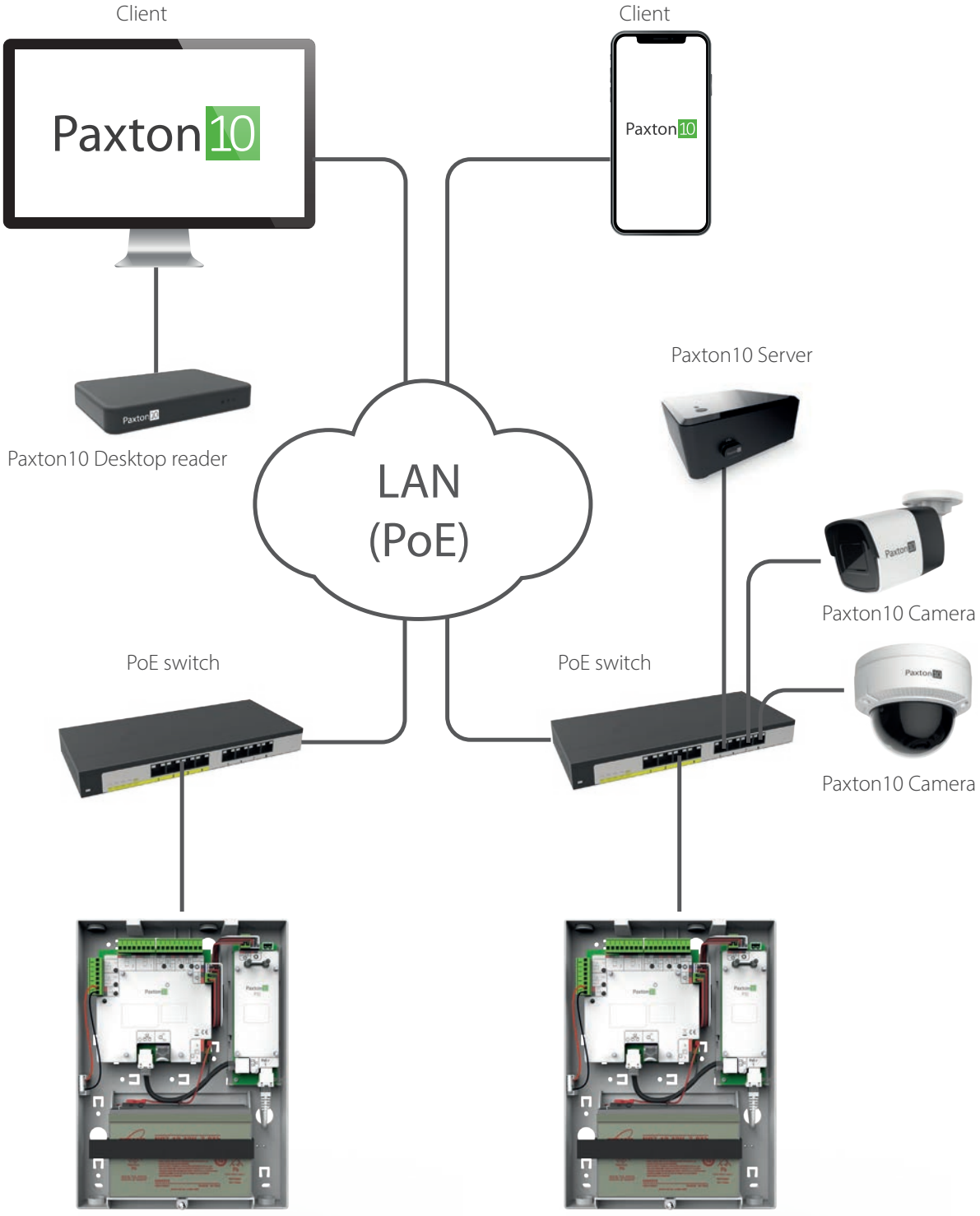
Readers

Readers read people's tokens to determin whether they are allowed access to a door or to action a device.

Paxton10 cameras

Paxton10 cameras record and store footage triggered by motion. The camera then provides this footage as requested to Paxton10 clients.

System diagram



Software Overview

The software is made up of 6 sections.

Dashboards

Dashboards are customisable screens which can be set up to display live information such as camera feeds, live user events and alarms.

Reports

Whenever something happens; a person presents their token, or updates a building permission, or a device goes offline, an event is created. Reports display all of these events in a way that makes it easy to see what is going on and what events have taken place. Video footage is also viewable within reports, either live or from recorded footage.

Site plans

Site plans pose as graphical representations of a site, they can be used as an overview to the layout of a site as well as provide an interactive graphics method of controlling and monitoring a system.

People

People are the users of the system. If a person requires access to a door, control of an device or access to the software they must first be created as a person in the software.

Rules

Rules determine who or what is allowed to action each device. The Rules section is made up of Building Permissions, Software Permissions, Custom Rules and Time Profiles.

Building Permissions:
Building Permissions control who is allowed access through each door and control of each device. Groups and individuals can be selected and assigned to a Building Permission, giving their credentials control of the doors and devices within the permission.

Software Permissions:
Software Permissions control who is allowed to access the Paxton10 software. People can be given access to edit, or just read, areas of the software.

Custom Rules:
Custom Rules are a way of defining unique behaviour and more complex tasks. This could include turning on the air conditioning when a thermostat input changes, locking all internal doors when the intruder alarm sounds, or defining anti-passback areas and roll call muster points.

Time Profiles:
Time Profiles are used to allow different behaviour and user permissions at different times/days. For instance, allowing a different selection of people access to a building at weekends, or keeping an office door unlocked during working hours.

Devices

Every device connected to the Paxton10 system will be located here. Once new devices are connected, they will appear in this area ready to be configured.

Note: Some switches will require specific configuration to provide POE+ (802.3at).

FAQ

What are the bandwidth requirements when using Paxton10 across multi-site or remote access?

- Any internet connection involved with Paxton10 is recommended to be 20Mbps Down and 10Mbps Up.
- For each primary stream of the camera being viewed, each network connection involved is recommended to have an additional 6Mbps Down and 2Mbps Up.

- For each secondary stream of the camera being viewed, each network is recommended to have an additional 3Mbps Down and 1Mbps Up.

If the recommended bandwidth requirements aren't met, you may experience performance issues when using Paxton10, this may include an increased buffering time when viewing live or archive video footage and increased load times when navigating the system.