Network requirements, optimisation and security in Paxton10

Overview

Paxton10 is a network-based access control and video management system, which is controlled and configured by the Paxton10 Server via its web User Interface. Paxton10 can work on almost any network but does require some network features in order to operate correctly.

This document discusses the network requirements and best practices for deploying Paxton10 devices into your IP network, to achieve optimal networking performance and network security.

The information and suggestions in this guide have been gathered through thorough testing of our products in a variety of networking topologies and environments.

By following this guide, sites can achieve the following benefits:

- Plug-and-play device discovery
- Improved responsiveness of Paxton devices by reducing latency in your IP network
- Reduced bandwidth consumption by Paxton devices
- Lower network latency/packet loss during communication between devices
- Ensured availability of Paxton10 devices
- Reduced upload/download times for firmware updates
- A secure network, preventing against hackers, sniffing tools, and data security breaches

Target audience

This document is intended for all Paxton10 installers and site IT professionals, including those with complex segmented networks using multiple subnets and/or physical locations.

Network requirements

Paxton10 does not require any specialist network hardware, however, to achieve full functionality and simplicity we recommend the below:

1) Internet connection: Paxton10 does not require the internet for day to day running. However, certain features are dependent on having an internet connection:

   - Remote Access: Remote access to the user interface, and use of the Paxton Connect mobile app, requires an internet connection to the Paxton10 server.

   - Multi-site: Paxton10's inbuilt multi-site feature requires an internet connection to the Paxton10 server and all Paxton10 controllers.

- System upgrade: Paxton10 offers free lifetime updates. Updates are detected and delivered via the internet connection to the Paxton10 server. Offline upgrades are currently not available.

- Smart credentials: The issuing of Paxton10 Smart credentials requires an internet connection to the Paxton10 server. Smart credentials can be barred and deleted while offline.

2) DHCP: The network should be running a DHCP server compatible with DNS, IPv4 and IPv6. A dedicated DHCP server may be used, alternatively many routers provide DHCP support without the need for additional hardware. Connect a router, or a DHCP server, to the network.

3) DNS: Paxton10 requires a DNS server to be running so that it can translate the Paxton10 server name (paxton10-xxxxxx) into its associated IP address. Without DNS, the Paxton10 server will need to be navigated to using its IP address.

4) Network Protocol: Paxton10 utilises both IPv4 and IPv6 to communicate. This means any network that Paxton10 uses must be compatible with both IPv4 and IPv6.

Network optimisation

Below are steps that can be carried out to aid network performance and reliability:

1) Evaluate and Test your network to understand your current network performance/capacity

- It is best to evaluate your existing network capacity and check if it can handle the expected network load from the number and type of Paxton10 devices that you are planning to deploy.

- If you are planning to deploy Paxton10 devices to different subnets spread across geographic regions, it is recommended to first perform tests between two devices in those subnets to gather statistics such as latency, packet loss, jitter and bandwidth.

- Test ICMP connectivity from all network locations/subnets to the Paxton10 server.

- Test UDP/TCP reliability metrics from all subnets to the Paxton10 server to ensure that all Paxton10 devices can establish and maintain a reliable connection to the server.

- Create an inventory of all physical locations, network locations, subnets and address spaces in which you are planning to deploy Paxton10 products.

Network security

We recommend that our customers implement security mechanisms at each of the 7 layers of the Network Open Systems Interconnection (OSI) model. Following are some approaches that should be followed to ensure the network is secure.

1) Implement strong physical security to the company premises by using token, PIN, or biometric-based authentication, so that an outsider can be stopped before he/she can enter company buildings.

2) Implement Network Access Control standards such as IEEE 802.1X authentication for securing LAN (Local Area Network) and WLAN (Wireless Local Area Network).

   This standard enforces security by granting only security policy–compliant devices access to network assets when those devices are plugged into a physical LAN port or are connected to a WLAN SSID. This standard not only handles access authentication and authorisation functions but also controls data accessed by those specific users by recognising users, their devices, and their network roles. IEE 802.1X is natively supported by all Windows, Mac and Linux machines.

3) Implement next generation Firewalls to prevent external and internal attacks.
   A next generation firewall, in addition to traditional packet based stateful inspection, should also perform functions such as application layer inspection, intrusion prevention and detection, securing web traffic, and more.

   Furthermore, stretch any potentially insecure internal layer 2 VLANs (Virtual Local Area Networks) to the firewall and protect access from those VLANs to other trusted/secure VLANs using security policies.

4) Implement VLANs for network security and segregation.
VLANs allow us to keep data packets from multiple networks (such as departmental networks, critical server networks, etc.) separated. Network segmentation with VLANs creates a collection of isolated networks within a corporate network and reduces the attack surfaces; even if an outsider gets access to a small logical network, he/she won't be able to view or directly attack devices on other VLANs.

5) Implement strong passwords for login to the Paxton10 application and any associated databases.

Paxton10 SSL certificates

Paxton10 uses HTTPS between clients, the server, and Paxton10 controllers. Each Paxton10 server is issued with a unique self-signed certificate, issued by Paxton10 Root Certificate Authority.

To avoid security warning messages from the browser, the Paxton10 certificate should be installed onto each client computer.

The certificate for a site can be found by suffixing your site URL with '/setup'. The setup page will also work over HTTP. For example, http://paxton10-xxxxxx/setup.

On the setup page, 2 options are available: 'Auto Install' will download an executable to automatically install the certificate on the current computer for the logged in user – a different executable is available for both Windows and Mac. 'Manual Install' will download the certificate to the default downloads folder – the certificate can be installed onto the current machine, or can be passed to an IT administrator to install onto all computers on the network.

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.

How does Paxton10 detect devices?

Paxton10 uses Multicast DNS over IPv6 to detect P10 door controllers on the network.

There is a known issue with a program that can be built into the network switches called MLD (Multicast listener discovery).

MLD is an efficient method to manage IPv6 communication on the network but it will prevent the P10 door controllers from being detected.

MLD needs to be disabled by a network engineer or IT for P10 to detect doors.

© Paxton Ltd 1.0.6