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 requirements, 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.
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

2) Segment your network using VLANs/Subnets to separate different types of network traffic and improve security

   Virtual Local Area Networks (VLANs) segment a physical layer 2 network consisting of a single switch or a network of switches into multiple logical layer 2 networks. Since each VLAN is also its own sub-network, a proper VLAN strategy that makes the most sense in terms of grouping devices is needed.

   From a security standpoint, it’s best to place similar devices onto the same subnet. For example, put the Paxton10 server and Paxton10 controllers in the first VLAN, all printers in the second VLAN, all wireless users in the third VLAN, all IP phones in the fourth VLAN, etc. We can then easily apply layer 3 filters or firewall rules that target specific devices in separate VLANs in how traffic in and out of that VLAN is treated.

   Create separate VLANs for management and user traffic. Also, security can be further improved by configuring all the ports on all switches to be associated with a custom VLAN rather than leaving them on default VLAN 1.

3) Decrease congestion by limiting number of devices in a VLAN/Subnet

   Due to broadcast overhead and noise, it’s best not to place more than 500 devices in a single subnet.

4) Place the Paxton10 server and Paxton10 controllers in the same subnet/VLAN wherever possible for improved monitoring/troubleshooting of Paxton10 traffic

   Wherever possible, create a dedicated subnet/VLAN for the Paxton10 server and all Paxton10 controllers so that Paxton10 traffic gets separated from other business traffic, thus providing security and less congestion. This will also make sure that the Paxton10 server and Paxton10 controllers are in the same broadcast domain enabling them to easily detect each other without having to traverse a Layer 3 VLAN Gateway/Router. However, once the number of devices in a VLAN reaches about 500, it is recommended to add additional devices into a different VLAN and use our ‘Manual add’ feature to keep them connected.

5) Avoid assigning overlapping IP address spaces to your subnets/sites/WAN

   Address overlap causes duplicate address assignment, resulting in loss of communication between devices.

6) Keep your network routing simple and minimize the number of routers between the Paxton10 server and Paxton10 controllers
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. IEEE 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

Paxton 10 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.
<table>
<thead>
<tr>
<th>Feature</th>
<th>Standard</th>
<th>Hardware</th>
<th>Direction</th>
<th>Outbound port</th>
<th>Destination Host</th>
<th>Inbound port</th>
<th>Socket Type</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Video Server</td>
<td>Yes</td>
<td>Video Controller, Controller MK1, Paxton10 Server</td>
<td>Outbound</td>
<td>3478</td>
<td>twilio.com</td>
<td>3478</td>
<td>UDP</td>
<td>STUN/TURN</td>
</tr>
<tr>
<td>Video Server</td>
<td>Yes</td>
<td>Video Controller, Controller MK1, Paxton10 Server</td>
<td>Inbound</td>
<td>3478</td>
<td>twilio.com</td>
<td>3478</td>
<td>UDP</td>
<td>STUN/TURN</td>
</tr>
<tr>
<td>Video Server</td>
<td>Yes</td>
<td>Video Controller, Controller MK1</td>
<td>Inbound</td>
<td>8090</td>
<td>IP of controller</td>
<td>8090</td>
<td>TCP</td>
<td>HTTP</td>
</tr>
<tr>
<td>Video Server</td>
<td>Yes</td>
<td>Video Controller, Controller MK1</td>
<td>Inbound</td>
<td>8091</td>
<td>IP of controller</td>
<td>8091</td>
<td>TCP</td>
<td>HTTPS</td>
</tr>
<tr>
<td>MQTT Broker discovery multi-cast</td>
<td>Yes</td>
<td>Paxton10 Server</td>
<td>Outbound</td>
<td>N/A</td>
<td>UDP Group Address</td>
<td>8070</td>
<td>UDP</td>
<td>Proprietary</td>
</tr>
<tr>
<td>MQTT Broker discovery multi-cast</td>
<td>Yes</td>
<td>Paxton10 Server</td>
<td>Inbound</td>
<td>8070</td>
<td>UDP Group Address</td>
<td>N/A</td>
<td>UDP</td>
<td>Proprietary</td>
</tr>
<tr>
<td>Paxton10 Updates</td>
<td>Yes</td>
<td>Paxton10 Server</td>
<td>Outbound</td>
<td>ANY</td>
<td><a href="https://updates.paxton-access.com">https://updates.paxton-access.com</a></td>
<td>443</td>
<td>TCP</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Windows Updates</td>
<td>Yes</td>
<td>Paxton10 Server</td>
<td>Outbound</td>
<td>ANY</td>
<td><a href="http://go.microsoft.com">http://go.microsoft.com</a></td>
<td>80</td>
<td>TCP</td>
<td>HTTP/HTTPS</td>
</tr>
<tr>
<td>Paxton10 Remote (Web access)</td>
<td>Yes</td>
<td>Paxton10 Server</td>
<td>Outbound</td>
<td>443</td>
<td>paxton10 remote.com</td>
<td>443</td>
<td>TCP</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Password Resets</td>
<td>Yes</td>
<td>Paxton10 Server</td>
<td>Outbound</td>
<td>ANY</td>
<td>paxton10 portal.com</td>
<td>443</td>
<td>TCP</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Smart Credential Email</td>
<td>Yes</td>
<td>Paxton10 Server</td>
<td>Outbound</td>
<td>ANY</td>
<td>paxton10 portal.com</td>
<td>443</td>
<td>TCP</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Legacy Upgrades</td>
<td>Yes</td>
<td>Controllers</td>
<td>Inbound</td>
<td>ANY</td>
<td>IP of Controller</td>
<td>ANY</td>
<td>UDP</td>
<td>Proprietary</td>
</tr>
<tr>
<td>Peer to Peer Comms</td>
<td>Yes</td>
<td>Controllers</td>
<td>Outbound</td>
<td>ANY</td>
<td>IP of other Controller</td>
<td>8031</td>
<td>UDP</td>
<td>Proprietary</td>
</tr>
<tr>
<td>Feature</td>
<td>Allowance</td>
<td>Type</td>
<td>Port</td>
<td>Direction</td>
<td>Remote IP</td>
<td>Protocol</td>
<td>Protocol Type</td>
<td></td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------</td>
<td>--------</td>
<td>-------</td>
<td>-----------</td>
<td>-----------</td>
<td>----------</td>
<td>--------------</td>
<td></td>
</tr>
<tr>
<td>Peer to Peer Comms</td>
<td>Yes</td>
<td>Controllers</td>
<td>Inbound</td>
<td>8031</td>
<td>IP of other Controller</td>
<td>UDP</td>
<td>Proprietary</td>
<td></td>
</tr>
<tr>
<td>Web Remoting Support</td>
<td>Yes</td>
<td>Controller</td>
<td>Inbound</td>
<td>8034</td>
<td>Paxton10 Server</td>
<td>TCP</td>
<td>Proprietary</td>
<td></td>
</tr>
<tr>
<td>Web Remoting Support</td>
<td>Yes</td>
<td>Controller</td>
<td>Outbound</td>
<td>ANY</td>
<td>Paxton10 Server</td>
<td>8034</td>
<td>TCP</td>
<td>Proprietary</td>
</tr>
</tbody>
</table>