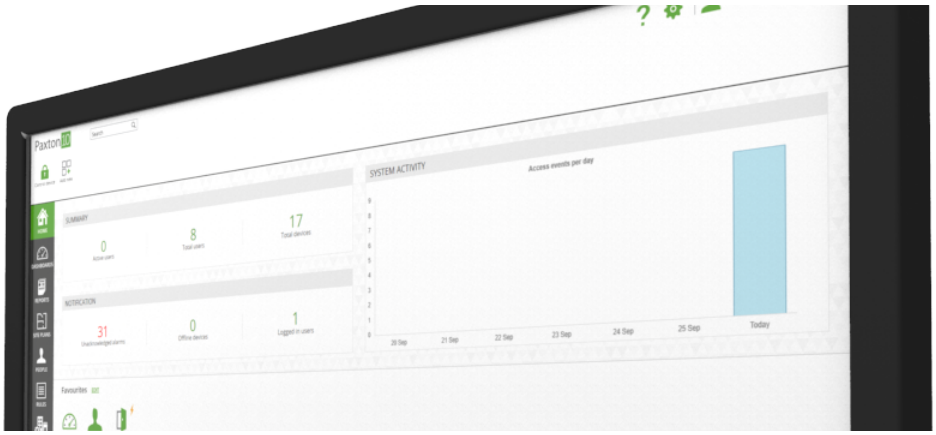

Netzwerkanforderungen, Optimierung und Sicherheit in Paxton10

Übersicht

Paxton10 ist ein netzwerkbasiertes Zugangskontroll- und Videoverwaltungssystem, das vom Paxton10-Server über seine Web-Benutzeroberfläche gesteuert und konfiguriert wird. Paxton10 kann in fast jedem Netzwerk eingesetzt werden, benötigt jedoch einige Netzwerkfunktionen, um korrekt zu funktionieren.

In diesem Dokument werden die Netzwerkanforderungen und bewährten Verfahren für den Einsatz von Paxton10-Geräten in Ihrem IP-Netzwerk erläutert, um eine optimale Netzwerkleistung und Netzwerksicherheit zu erreichen.

Die Informationen und Vorschläge in diesem Leitfaden wurden durch gründliche Tests unserer Produkte in einer Vielzahl von Netzwerktopologien und -umgebungen zusammengetragen.

Mit Hilfe dieses Leitfadens können Standorte die folgenden Vorteile erzielen:

- Einsatz von Plug-and-Play-Geräten
- Verbesserte Reaktionsfähigkeit von Paxton-Geräten durch Verringerung der Latenzzeit in Ihrem IP-Netzwerk
- Geringerer Bandbreitenverbrauch durch Paxton-Geräte
- Geringere Netzwerklatenz/Paketverluste bei der Kommunikation zwischen Geräten
- Garantierte Verfügbarkeit von Paxton10-Geräten
- Verkürzte Upload-/Download-Zeiten für Firmware-Updates
- Ein sicheres Netzwerk, das vor Hackern, Sniffing-Tools und Datensicherheitsverletzungen schützt

Zielgruppe

Dieses Dokument richtet sich an alle Paxton10-Installierer und IT-Fachleute, einschließlich solcher mit komplexen segmentierten Netzwerken mit mehreren Subnetzen und/oder physischen Standorten.

Netzwerkanforderungen

Paxton10 erfordert keine speziellen Netzwerkanforderungen, doch um die volle Funktionalität und Einfachheit zu erreichen, empfehlen wir Folgendes

1) Internetverbindung: Paxton10 benötigt für den täglichen Betrieb kein Internet. Bestimmte Funktionen sind jedoch von einer Internetverbindung abhängig:

- Fernzugriff: Der Fernzugriff auf die Benutzeroberfläche und die Verwendung der mobilen App Paxton Connect erfordert eine Internetverbindung zum Paxton10-Server.

- Mehrere Standorte: Die integrierte Funktion für mehrere Standorte von Paxton10 erfordert eine Internetverbindung zum Paxton10-Server und allen Paxton10-Steuereinheiten.

AN0051-D

- Systemaufrüstung: Paxton10 bietet kostenlose Updates auf Lebenszeit. Updates werden erkannt und über die Internetverbindung zum Paxton10-Server geliefert. Offline-Upgrades sind derzeit nicht verfügbar.

- Intelligente Identifikationsmedien: Die Ausstellung von Paxton10 intelligenten Identifikationsmedien erfordert eine Internetverbindung zum Paxton10-Server. Intelligente Identifikationsmedien können gesperrt und gelöscht werden, während sie offline sind.

2) DHCP: Im Netzwerk sollte ein DHCP-Server laufen, der mit DNS, IPv4 und IPv6 kompatibel ist. Ein dedizierter DHCP-Server kann verwendet werden, alternativ bieten viele Router DHCP-Unterstützung, ohne dass zusätzliche Hardware erforderlich ist. Schließen Sie einen Router oder einen DHCP-Server an das Netzwerk an.

3) DNS: Paxton10 erfordert die Ausführung eines DNS-Servers, damit dieser den Paxton10-Servernamen (Paxton10-xxxxxxxx) in seine zugehörige IP-Adresse übersetzen kann. Ohne DNS muss der Paxton10-Server zur Verwendung seiner IP-Adresse navigiert werden.

Netzwerkoptimierung

Nachfolgend sind Schritte aufgeführt, die durchgeführt werden können, um die Leistung und Zuverlässigkeit des Netzwerks zu verbessern:

1) Bewerten und testen Sie Ihr Netzwerk, um Ihre aktuelle Netzwerkleistung/-kapazität zu verstehen.

   - Am besten evaluieren Sie Ihre vorhandene Netzwerkkapazität und prüfen Sie, ob sie der erwarteten Netzwerkbelastung durch die Anzahl und den Typ der Paxton10-Geräte, die Sie einsetzen möchten, gewachsen ist.

   - Wenn Sie planen, Paxton10-Geräte in verschiedenen, über geografische Regionen verteilten Subnetzen einzusetzen, empfiehlt es sich, zunächst Tests zwischen zwei Geräten in diesen Subnetzen durchzuführen, um Statistiken wie Latenz, Paketverlust, Jitter und Bandbreite zu sammeln.

   - Testen Sie die ICMP-Konnektivität von allen Netzwerkstandorten/Subnetzen zum Paxton10-Server

   - Testen Sie UDP/TCP-Zuverlässigkeitsmetriken von allen Subnetzen zum Paxton10-Server, um sicherzustellen, dass alle Paxton10-Geräte eine zuverlässige Verbindung zum Server herstellen und aufrechterhalten können.

   - Erstellen Sie eine Bestandsaufnahme aller physischen Standorte, Netzwerkstandorte, Subnetze und Adressräume, in denen Sie planen, Paxton10-Produkte einzusetzen.

Netzwerksicherheit

Wir empfehlen unseren Kunden, Sicherheitsmechanismen auf jeder der 7 Schichten des OSI-Modells (Network Open Systems Interconnection) zu implementieren. Es folgen einige Ansätze, die befolgt werden sollten, um sicherzustellen, dass das Netzwerk sicher ist.

1) Implementieren Sie starke physische Sicherheit auf dem Firmengelände durch die Verwendung von Token, PIN oder biometrischer Authentifizierung, so dass ein Außenstehender aufgehalten werden kann, bevor er das Firmengebäude betreten kann.

2) Implementierung von Netzzugangskontrollstandards wie IEEE 802.1X-Authentifizierung zur Sicherung von LAN (Local Area Network) und WLAN (Wireless Local Area Network).

   Dieser Standard erzwingt Sicherheit, indem er nur sicherheitsrichtlinien-konformen Geräten Zugang zu Netzwerkressourcen gewährt, wenn diese Geräte an einen physischen LAN-Port angeschlossen oder mit einer WLAN-SSID verbunden sind. Dieser Standard behandelt nicht nur die Zugangsauthentifizierungs- und Autorisierungsfunktionen, sondern kontrolliert auch die Daten, auf die diese spezifischen Benutzer zugreifen, indem er die Benutzer, ihre Geräte und ihre Netzwerkrollen erkennt. IEE 802.1X wird von allen Windows-, Mac- und Linux-Rechnern nativ unterstützt.

3) Implementieren Sie Firewalls der nächsten Generation, um externe und interne Angriffe zu verhindern.

Eine Firewall der nächsten Generation sollte neben der traditionellen Zustandsorientierte Paketüberprüfung (SPI) auch Funktionen wie Inspektion der Anwendungsschicht, Verhütung und Erkennung von Eindringversuchen, Sicherung des Web-Verkehrs und mehr erfüllen.
Darüber hinaus sollten Sie alle potenziell unsicheren internen Layer-2-VLANs (Virtual Local Area Networks) auf die Firewall ausdehnen und den Zugriff von diesen VLANs auf andere vertrauenswürdige/sichere VLANs mithilfe von Sicherheitsrichtlinien schützen.

4) Implementierung von VLANs für Netzwerksicherheit und -trennung.

VLANs ermöglichen es uns, Datenpakete aus mehreren Netzwerken (wie Abteilungsnetzwerken, kritischen Servernetzwerken usw.) getrennt zu halten. Die Netzwerksegmentierung mit VLANs schafft eine Ansammlung isolierter Netzwerke innerhalb eines Unternehmensnetzwerks und verringert die Angriffsflächen; selbst wenn ein Außenstehender Zugang zu einem kleinen logischen Netzwerk erhält, kann er Geräte in anderen VLANs nicht einsehen oder direkt angreifen.

5) Implementieren Sie sichere Passwörter für die Anmeldung bei der Paxton10-Anwendung und allen zugehörigen Datenbanken.

Paxton10-SSL-Zertifikat

Paxton10 verwendet HTTPS zwischen Clients, dem Server und Paxton10-Controllern. Jeder Paxton10-Server verfügt über ein eindeutiges selbstsigniertes Zertifikat, das von der Paxton10 Root Certificate Authority ausgestellt wird.

Um Sicherheitswarnmeldungen des Browsers zu vermeiden, sollte das Paxton10-Zertifikat auf jedem Client-Computer installiert werden.

Das Zertifikat für eine Webseite finden Sie, indem Sie die URL Ihrer Webseite um ‚/setup' erweitern. Die Einrichtungsseite funktioniert auch über HTTP. Zum Beispiel http://Paxton10-xxxxxx/setup.

Auf der Setup-Seite stehen 2 Optionen zur Verfügung: ‚Auto Install' lädt eine ausführbare Datei herunter, um das Zertifikat automatisch auf dem aktuellen Computer für den angemeldeten Benutzer zu installieren - eine andere ausführbare Datei ist sowohl für Windows als auch für Mac verfügbar. ‚Manuelle Installation' lädt das Zertifikat in den Standard-Download-Ordner herunter - das Zertifikat kann auf dem aktuellen Rechner installiert werden oder an einen IT-Administrator zur Installation auf allen Computern im Netzwerk weitergegeben werden.

FAQ

<u>Was sind die Anforderungen an die Bandbreite bei der Nutzung über mehrere Standorte oder des Fernzugriffs?</u>

- Für jede Internetverbindung, die mit Paxton10 verbunden ist, wird eine Bandbreite von 20 Mbit/s (Downstream) und 10 Mbit/s (Upstream) empfohlen.
- Für jeden primären Stream der betrachteten Kamera wird für jede beteiligte Netzwerkverbindung eine zusätzliche Bandbreite von 6 Mbit/s (Downstream) und 2 Mbit/s (Upstream) empfohlen.
- Für jeden sekundären Stream der betrachteten Kamera wird für jedes Netzwerk eine zusätzliche Bandbreite von 3 Mbit/s (Downstream) und 1 Mbit/s (Upstream) empfohlen.

Wenn die empfohlenen Anforderungen an die Bandbreite nicht erfüllt werden, kann es bei der Nutzung von Paxton10 zu Leistungseinbußen kommen, z. B. durch längere Pufferzeiten beim Betrachten von Live- oder Archivvideos und längere Ladezeiten bei der Navigation im System.

Paxton10 Netzwerk- und Internet-Kommunikation

Externe Regeln (zu Zielen im Internet)

Quelladressen/ Objekte	Quell-Netzwerk/ Subnetz/Zone	Zieladressen/ Objekte	Zielnetz/Subnetz/ Zone	Anwendung	Zielport	IP-Protokoll (TCP/UDP)	Funktion
Client browser, P10 cameras, Video Servers - IP addresses	Client-Browser, P10 Kameras, Videoserver - Netzwerke	STUN/TURN server – twilio.com	STUN/TURN server – twilio.com	Sonder	3478	UDP	Kamera Video-Streaming
Client-Browser, P10 Server, P10 Kameras, Videoserver - IP-Adressen	Client-Browser, P10 Server, P10 Kameras, Videoserver - Netzwerke	STUN/TURN server – twilio.com	STUN/TURN server -twilio.com	HTTPS	443	TCP	Kamera Video-Streaming
Paxton 10 Server - IP-Adresse	Paxton 10 Server - Netzwerk	Windows Updates - go.microsoft. com	Paxton-Controller - Netzwerke	HTTP	80	TCP	Allgemeines System
Paxton 10 Server - IP-Adresse	Paxton 10 Server - Netzwerk	Paxton10 Updates - updates. paxtonaccess.com	Paxton10 Updates - updates. paxtonaccess.com	HTTPS	443	TCP	Allgemeines System
Paxton 10 Server - IP-Adresse	Paxton 10 Server - Netzwerk	Paxton Remote Access - paxton10remote. com	Paxton Remote Access - paxton10remote. com	Sonder	1234	TCP	Fernzugriff

Interne Regeln (falls Ihr Routing dies erfordert)

Quelladressen/ Objekte	Quell-Netzwerk/ Subnetz/Zone	Zieladressen/ Objekte	Zielnetz/Subnetz/ Zone	Anwendung	Zielport	IP-Protokoll (TCP/UDP)	Funktion
Client-Browser - IP-Adressen	Client-Browser - Netzwerke	Paxton10 Kamera, Videoserver - IP-Adressen	Paxton10 Kamera, Videoserver - Netzwerke	HTTP	8090	TCP	Kamera Video-Streaming
Client-Browser - IP-Adressen	Client-Browser - Netzwerke	Paxton10 Kamera, Videoserver - IP-Adressen	Paxton10 Kamera, Videoserver - Netzwerke	HTTPS	8091	TCP	Kamera Video-Streaming
Client-Browser - IP-Adressen	Client-Browser - Netzwerke	Paxton 10 Server - IP-Adresse	Paxton 10 Server - Netzwerk	HTTP	80	TCP	Allgemeines System
Client-Browser - IP-Adressen	Client-Browser - Netzwerke	Paxton 10 Server - IP-Adresse	Paxton 10 Server - Netzwerk	HTTPS	443	TCP	Allgemeines System
Paxton 10 Server - IP-Adresse	Paxton 10 Server - Netzwerk	Alle Paxton und zugehörige Hardware - IP-Adressen	Alle Paxton und zugehörige Hardware - Netzwerke	Sonder	8070	UDP	Allgemeine Systemerkennung
Paxton-Controller - IP-Adressen	Paxton-Controller - Netzwerke	Paxton-Controller - IP-Adressen	Paxton-Controller - Netzwerke	Sonder	8031	TCP	Allgemeines System

Interne Regeln (falls Ihr Routing dies erfordert)

Paxton-Controller - IP-Adressen	Paxton-Controller - Netzwerke	Paxton 10 Server - IP-Adresse	Paxton 10 Server - Netzwerk	Sonder	8034	TCP	Fernzugriff
Alle Geräte und Server von Paxton - IP-Adressen	Alle Geräte und Server von Paxton - Netzwerke	Alle Geräte und Server von Paxton - IP-Adressen	Alle Geräte und Server von Paxton - Netzwerke	Sonder	8883	MQTT	Allgemeines System
Paxton 10 Bereichscontroller - IP-Adressen	Alle Geräte und Server von Paxton - Netzwerke	ONVIF-Kameras von Drittanbietern - IP-Adressen	ONVIF-Kameras von Drittanbietern - Netzwerke	Sonder	3702	UDP	Kameraerkennung anderer Hersteller
Paxton 10 Bereichscontroller - IP-Adressen	Paxton 10 Bereichscontroller - Netzwerke	Paxton 10 Server - IP-Adresse	Paxton 10 Server - Netzwerk	HTTP	80	TCP	Allgemeines System
Paxton 10 Server - IP-Adresse	Paxton 10 Server - Netzwerk	Paxton 10 Bereichscontroller - IP-Adressen	Paxton 10 Bereichscontroller - Netzwerke	Sonder	5000	TCP	Mehrere Standorte/Mehrere Subnetz Support
Paxton 10 Server - IP-Adresse	Paxton 10 Server - Netzwerk	Paxton 10 Bereichscontroller - IP-Adressen	Paxton 10 Bereichscontroller - Netzwerke	Sonder	5001	TCP	Mehrere Standorte/Mehrere Subnetz Support
Paxton 10 Bereichscontroller - IP-Adressen	Paxton 10 Bereichscontroller - Netzwerke	BACnet-Steuergeräte - IP-Adressen	BACnet-Steuergeräte - Netzwerke	Sonder	47808	UDP	BACnet

Interne Regeln (falls Ihr Routing dies erfordert)

Paxton 10 Bereichscontroller - IP-Adressen	Paxton 10 Bereichscontroller - Netzwerke	RTSP-Kameras von Drittanbietern - IP-Adressen	RTSP-Kameras von Drittanbietern - IP-Adressen	Sonder	554	TCP	Kamera eines Drittanbieters Videostreams
Paxton 10 Bereichscontroller - IP-Adressen	Paxton 10 Bereichscontroller - Netzwerke	RTSP-Kameras von Drittanbietern - IP-Adressen	RTSP-Kameras von Drittanbietern - IP-Adressen	Sonder	554	UDP	Kamera eines Drittanbieters Videostreams