

Paxton10 Sichere Gerätekommunikation

Übersicht

Paxton10 Version 4.11 SR1 führte eine wichtige Sicherheitsverbesserung für die Kommunikation zwischen dem Paxton10-Server und seinen Geräten ein

Dieses Update verwendet verschlüsselte, zertifikatsbasierte Kommunikation, um das System vor unbefugtem Zutritt oder Abhören im lokalen Netzwerk zu schützen

Das Update ist einfach gestaltet. Ein Systemingenieur startet den Prozess in der Paxton10-Weboberfläche, bestätigt, dass die vorhandenen Geräte vertrauenswürdig sind, und Paxton10 führt das Update automatisch im Hintergrund aus.

Dies ist ein einmaliger Prozess beim Aktualisieren eines bestehenden Systems auf Version 4.11 SR1 oder höher. Neue mit dieser Version oder später ausgelieferte Paxton10-Server werden die Sicherheitsverbesserung bereits aktiviert haben.

Wichtig: Netzwerk-Anforderung

Paxton10 erfordert, dass Port 8884 im lokalen Netzwerk verfügbar ist, damit Paxton10-Geräte sicher mit dem Paxton10-Server kommunizieren können

Dies ist nur eine Anforderung für das interne LAN. Port 8884 sollte nicht dem öffentlichen Internet ausgesetzt sein.

Wenn Sie mit dem Update der sicheren Gerätekommunikation fortfahren, während Port 8884 nicht verfügbar ist, werden Paxton10 Geräte als offline angezeigt und erhalten keine Datenbank-Aktualisierungen vom Server. Sie werden weiterhin mit der zuletzt empfangenen Datenbank arbeiten.

Wichtig: Firmware-Anforderung für Entry Panels

Bevor Sie das Update für die sichere Gerätekommunikation auf Ihrem System aktivieren, müssen alle Entry-Türstationen im System die erforderliche Mindestversion der Firmware (v4.02.16916.801) oder höher aufweisen und online sein. Falls Ihre Entry-Türstationen ein Firmware-Upgrade benötigen, müssen Sie v4.3 oder höher des Entry-Konfigurationsdienstprogramms verwenden, das die erforderliche Firmware-Version enthält.

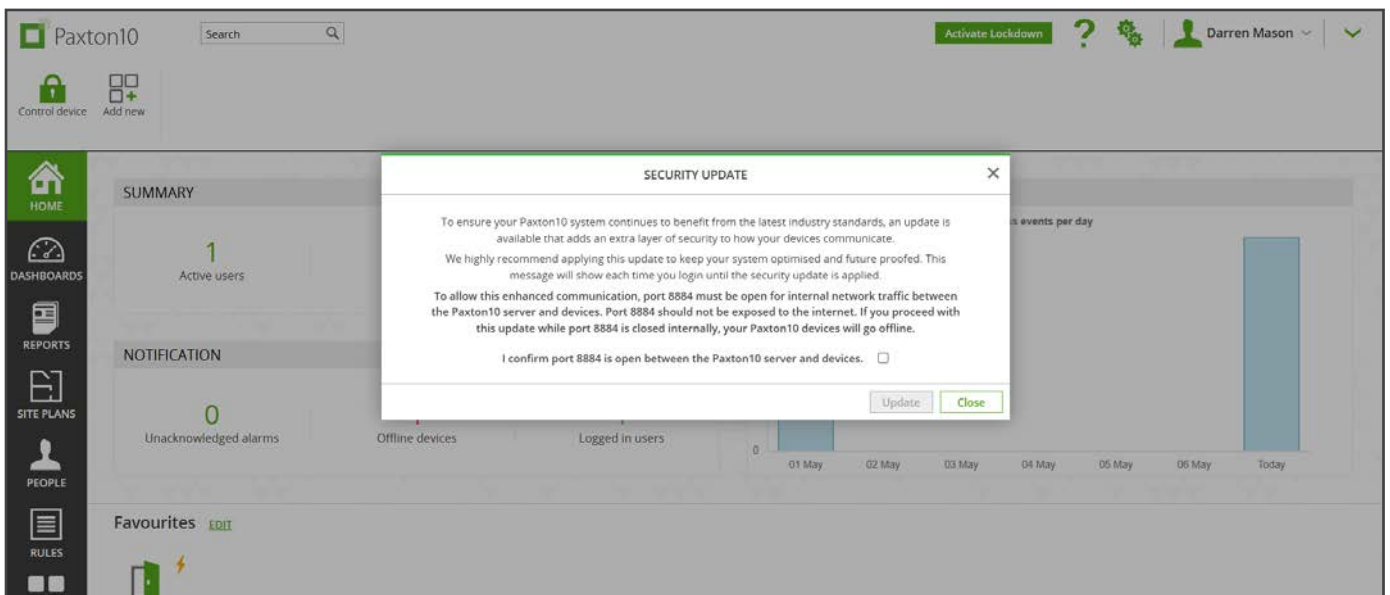
Beim Start des Sicherheitsupdates überprüft Paxton10 automatisch die Firmware-Versionen aller Entry-Türstationen im System. Wenn Entry-Türstationen unterhalb der erforderlichen Mindestversion (weniger als v4.02.16916.801) sind, werden Sie zum Upgrade aufgefordert, bevor Sie fortfahren können. Sie können die Firmware-Versionen auch selbst prüfen, indem Sie die Entry-Türstation-Details in der Hardware-Verwaltung ansehen.

Die Firmware für Entry Panels wird mit dem Entry Configuration Utility aktualisiert, das hier heruntergeladen werden kann: <https://paxton.info/1907>

Im Gegensatz zu anderen Paxton10 Geräten erhalten Entry Panels keine automatischen Firmware-Updates über den Paxton10 Server.

Starten des Sicherheitsupdates

Nachdem die Paxton10-Software auf Version 4.11 SR1 oder höher aktualisiert wurde, sehen Systemingenieure beim Einloggen eine Benachrichtigung. Diese Benachrichtigung weist darauf hin, dass ein Sicherheitsupdate für die Gerätekommunikation verfügbar ist.



Wenn Sie noch nicht bereit sind, können Sie die Nachricht schließen. Die Update-Nachricht wird bei jedem Einloggen der Systemingenieure angezeigt, bis sie angewendet wird.

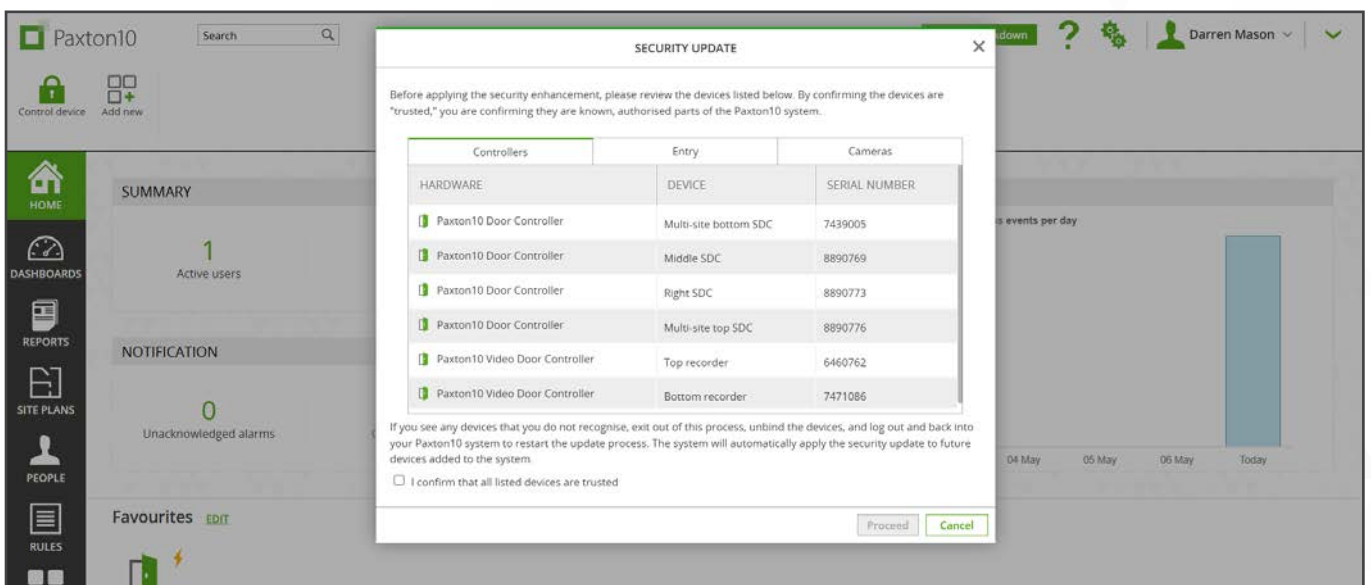
Bestätigung vertrauenswürdiger Geräte

Bevor das Update startet, zeigt Paxton10 eine Liste der derzeit mit dem System verbundenen Geräte an. Überprüfen Sie diese Liste sorgfältig.

Indem Sie die Geräte als ‚vertrauenswürdig‘ bestätigen, bestätigen Sie, dass sie bekannte und autorisierte Teile des Paxton10 Systems sind

Wenn Sie ein Gerät sehen, das Sie nicht erkennen, fahren Sie nicht fort. Beenden Sie den Prozess, untersuchen Sie das Gerät und entfernen oder lösen Sie es gegebenenfalls. Melden Sie sich ab und wieder bei Paxton10 an, um das Sicherheitsupdate neu zu starten, sobald die Geräteliste korrekt ist.

Sobald die vertrauenswürdigen Geräte bestätigt sind, wird Paxton10 mit der Anwendung des Sicherheitsupdates beginnen.



Was während der Einführung passiert

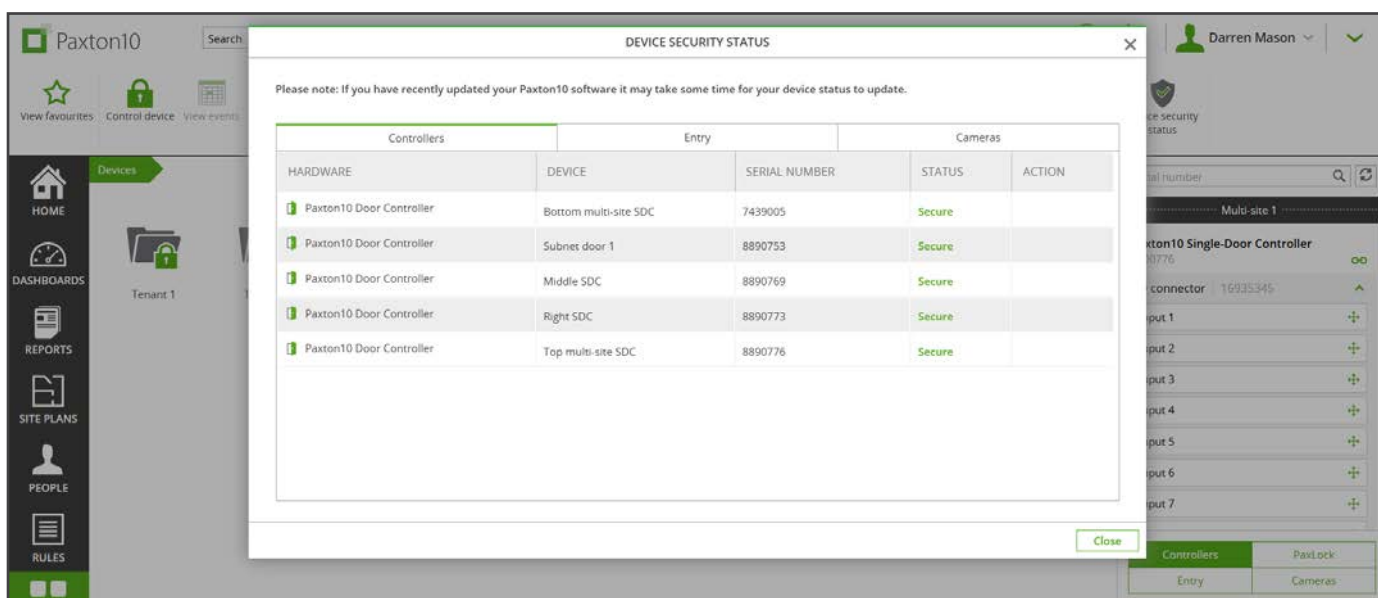
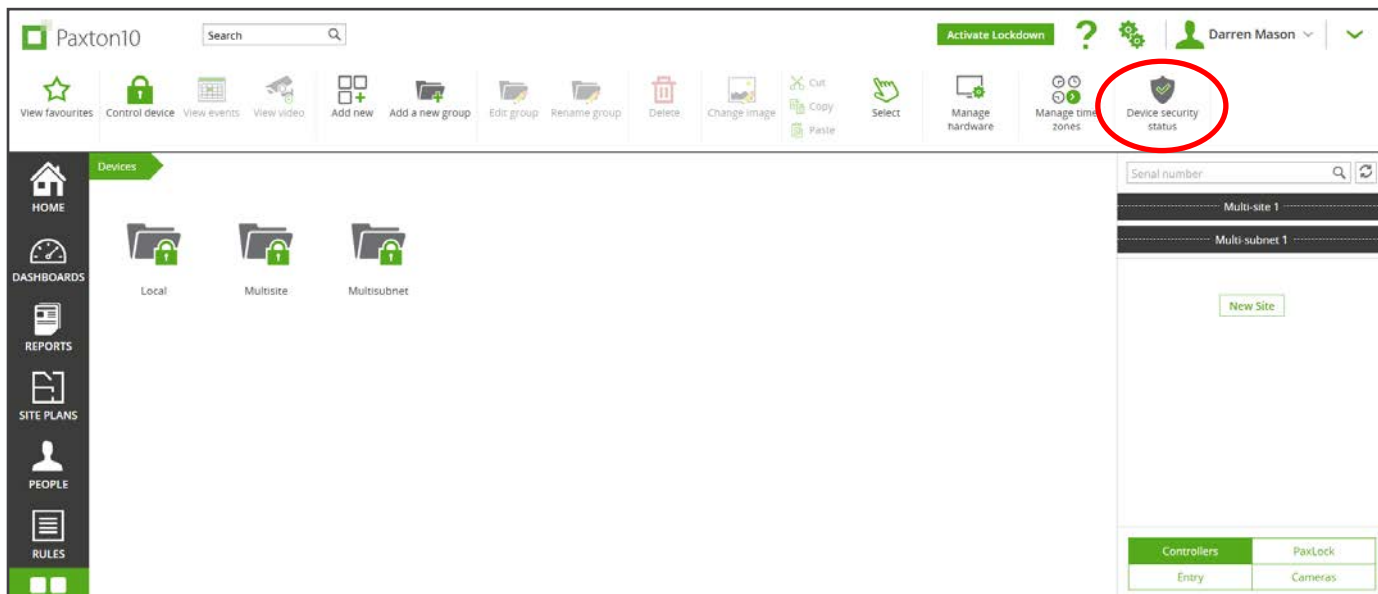
Paxton10 verwaltet die Einführung des Sicherheitsupdates für Geräte automatisch, um Unterbrechungen zu minimieren. Nach Abschluss der Grundeinrichtung werden die Geräte im Hintergrund aktualisiert. Das System ist so konzipiert, dass es während der Aktualisierung betriebsbereit bleibt, und nach Abschluss des Updates kommunizieren die Geräte mit der neuen Methode.

Sicherheitsstatus der Geräte überwachen

Sie können den Sicherheitsstatus der Geräte des Systems jederzeit in der Paxton10-Software überprüfen

Wählen Sie auf dem Bildschirm Geräte die Schaltfläche ‚Sicherheitsstatus der Geräte‘, um zu sehen, welche Geräte konform sind und welche Geräte noch Aufmerksamkeit benötigen

Kann ein Gerät im Hintergrund nicht aktualisiert werden, zeigt Paxton10 dies im Sicherheitsstatus-Dashboard für Geräte an und schlägt Maßnahmen zur Lösung vor.



Wenn ein Gerät im Hintergrund nicht aktualisiert werden kann

Wenn Paxton10 meldet, dass ein Gerät das Sicherheitsupdate nicht abschließen konnte, sind die häufigsten Ursachen

- Das Gerät ist offline
- Das Gerät hat noch nicht die erforderliche Firmware aktualisiert
- In einem Multi-Site- oder Multi-Subnetz-System hat der Master Controller das Update noch nicht abgeschlossen (der Master Controller muss das Sicherheitsupdate abschließen, bevor die sekundären Controller das Sicherheitsupdate abschließen können)

Führen Sie die normalen Fehlerbehebungsschritte durch

- Überprüfen Sie die Netzwerkverbindung zum Gerät
- Wenn das Gerät offline ist, bringen Sie es wieder online und lassen Sie Paxton10 Zeit, das Update fortzusetzen
- Starten Sie das Gerät neu und setzen Sie es aus der Paxton10-Software zurück
- Schalten Sie das Gerät bei Bedarf aus und wieder ein
- Löschen Sie das Gerät aus der Hardware-Verwalten und binden Sie es bei Bedarf erneut an das System. Vor einer erneuten Bindung kann ein physikalischer Reset erforderlich sein.

Wenn das Gerät das Sicherheitsupdate immer noch nicht empfangen kann, wenden Sie sich an den Paxton-Support, um Hilfe zu erhalten

Neue Geräte nach dem Update hinzufügen

Sobald die sichere Gerätekommunikation im System aktiviert wurde, werden alle neu hinzugefügten Geräte das Sicherheitsupdate automatisch im Hintergrund erhalten

Sie können weiterhin das Sicherheitsstatus-Dashboard für Geräte verwenden, um zu bestätigen, dass neu hinzugefügte Geräte konform werden.