Paxton10 Secure Device Communications

Overview

Paxton10 version 4.11 SR1 introduced an important security enhancement for communication between the Paxton10 server and its devices.

This update uses encrypted, certificate based communication to help protect the system from unauthorised access or eavesdropping on the local network.

The update is designed to be simple. A System Engineer starts the process in the Paxton10 web interface, confirms that the existing devices are trusted, and Paxton10 applies the update automatically in the background.

This is a one-time process when updating an existing system to version 4.11 SR1 or higher. New Paxton10 servers shipped with this release or later will already have the security enhancement enabled.

Important: network requirement

Paxton10 requires port 8884 to be available on the local network so that Paxton10 devices can communicate securely with the Paxton10 server.

This is an internal LAN requirement only. Port 8884 should not need to be exposed to the public internet.

If you proceed with the secure device communications update when port 8884 is not available, Paxton10 devices will show as offline and will not receive any database updates from the server. They will still continue to operate with the last database they received.

Important: Entry Panel firmware requirement

Before enabling the secure device communications update on your system, all Entry Panels on the system must be on the required minimum firmware version (v4.02.16916.801) or higher and must be online. If your Entry Panels need their firmware upgraded, you must use v4.3 or higher of the Entry Configuration Utility, which contains the required firmware version.

When starting the security update, Paxton10 will automatically check the firmware versions of all Entry Panels on the system. If any Entry Panels are below the required minimum firmware version (less than v4.02.16916.801), you will be prompted to update them before continuing. You can also check firmware versions yourself by viewing Entry Panel details within Hardware Management.

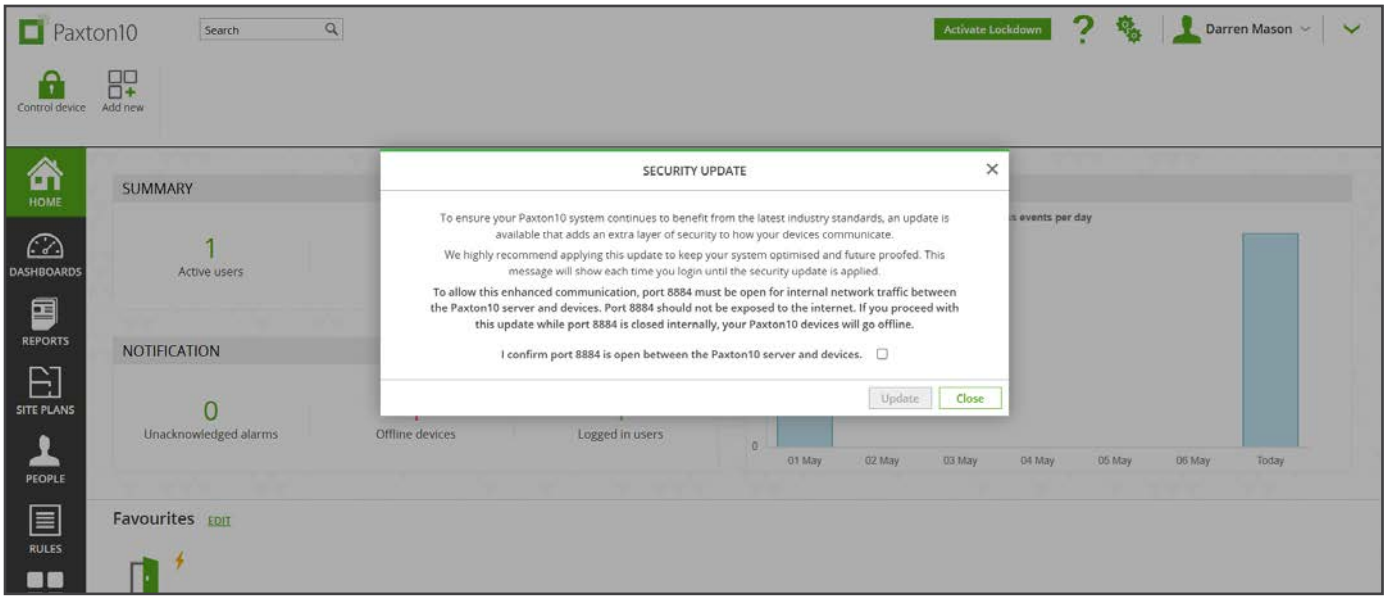
Entry Panel firmware is updated using the Entry Configuration Utility, which can be downloaded here:

https://paxton.info/1907

Unlike other Paxton10 devices, Entry Panels do not receive firmware updates automatically through the Paxton10 server.

Starting the security update

After the Paxton10 software has been updated to version 4.11 SR1 or higher, System Engineers will see an alert when they log in. This alert advises that a security update is available for device communication.



If you are not ready to proceed, you can close the message. The update message will show again each time System Engineers log in until it is applied.

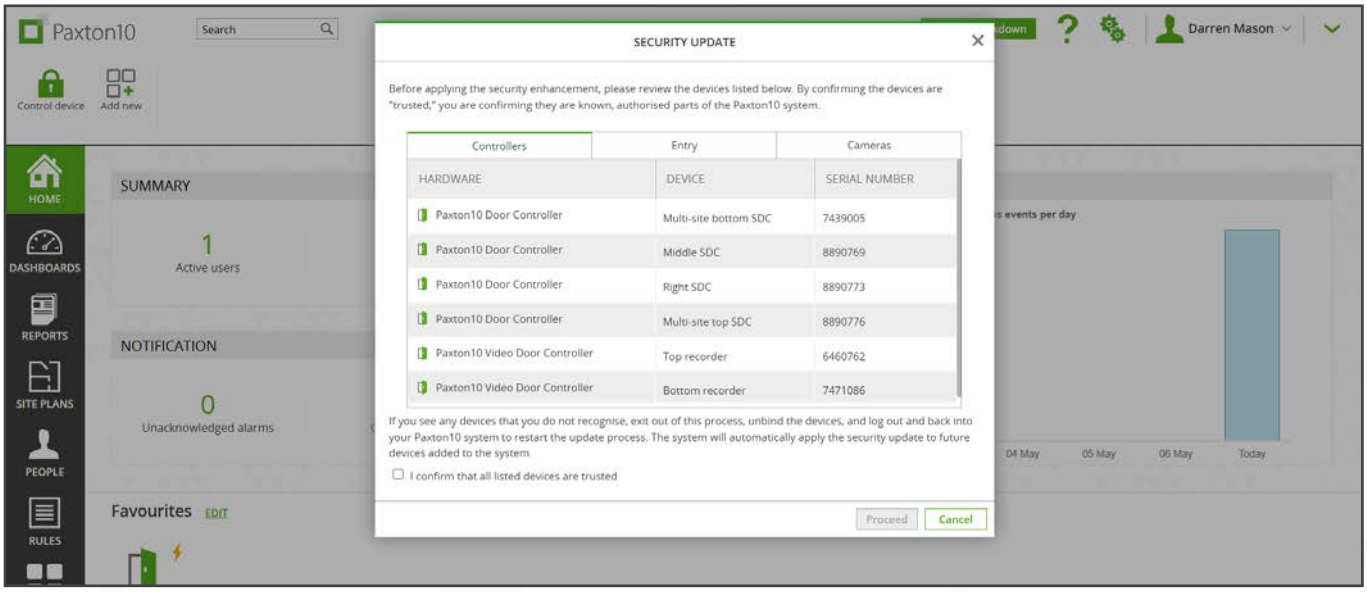
Confirming trusted devices

Before the update starts, Paxton10 will display a list of devices currently bound to the system. Review this list carefully.

By confirming the devices are 'trusted', you are confirming that they are known and authorised parts of the Paxton10 system.

If you see a device that you do not recognise, do not continue. Exit the process, investigate the device, and remove or unbind it if required. Log out and back into Paxton10 to restart the security update once the device list is correct.

Once the trusted devices are confirmed, Paxton10 will begin applying the security update.



What happens during the rollout

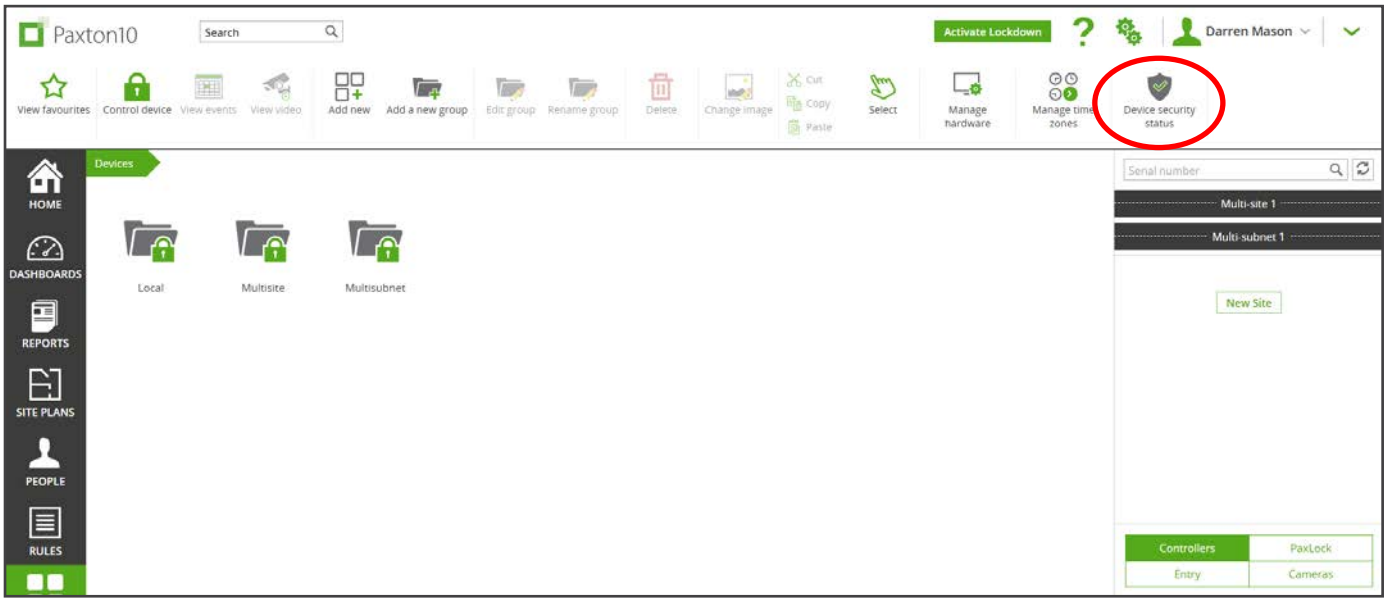
Paxton10 manages the security update rollout to devices automatically to minimise disruption. After the initial setup is complete, devices are updated in the background. The system is designed to remain operational while the update is applied and once complete, the devices will communicate using the new method.

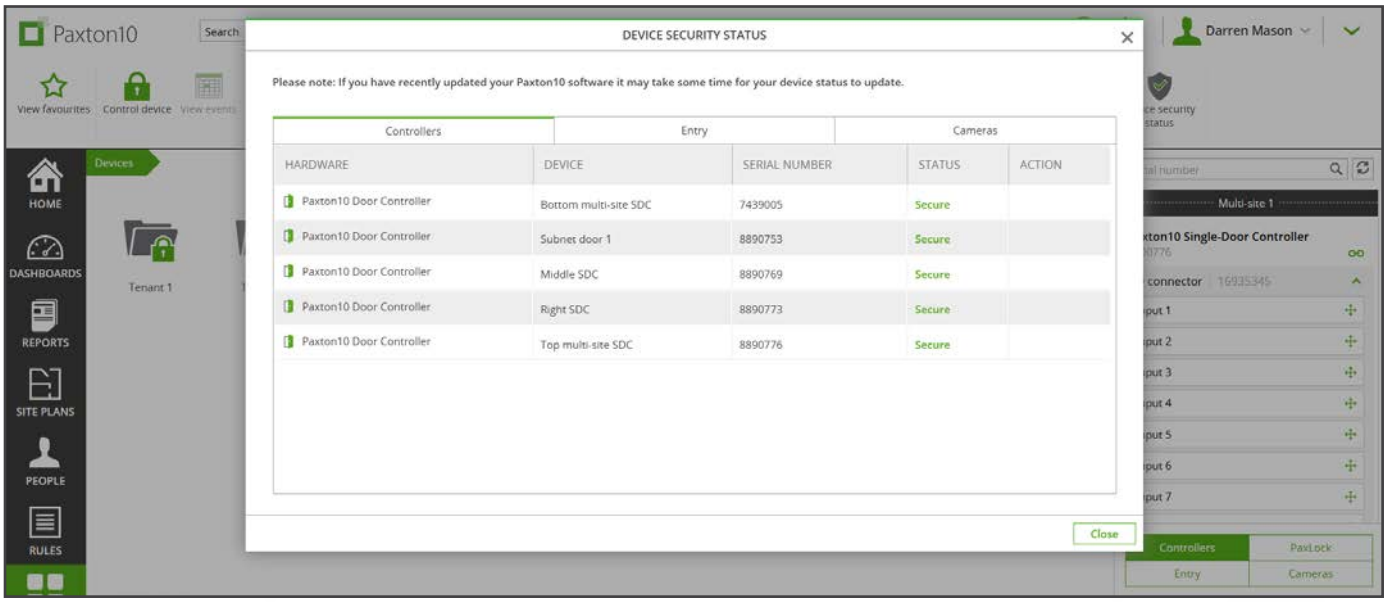
Monitoring device security status

You can check the device security status of the system at any time in the Paxton10 software.

From the Devices screen, select the '**Device security status'** button to view which devices are compliant and which devices still need attention.

If a device cannot be updated in the background, Paxton10 will show this in the Device security status dashboard and suggested actions to resolve it.





If a device cannot be updated in the background

If Paxton10 reports that a device could not complete the security update, the most common causes are:

- The device is offline.
- The device has not yet updated to the required firmware.
- In a multi-site or multi-subnet system, the Master Controller has not yet completed the update (the Master controller must complete the security update before secondary controllers can).

Carry out the normal troubleshooting steps:

- Check network connectivity to the device.
- If the device is offline, bring it back online and allow time for Paxton10 to continue the update.
- Reboot and reinstate the device from the Paxton10 software.
- Power cycle the device if required.
- Delete the device from Hardware Management and rebind it to the system if required. A physical reset may be needed before rebinding.

If the device still cannot receive the security update, contact Paxton Support for assistance.

Adding new devices after the update

Once Secure Device Communications has been enabled on the system, any new devices added afterwards will automatically receive the security update in the background.

You can continue to use the Device security status dashboard to confirm that newly added devices become compliant.