Paxton10 Data Protection

Overview

To accommodate EU regulations that came into effect in May 2018, it is important to understand how Paxton10 stores and uses data, and what can be done to protect and restrict the use of this data.

Events

Events keep track of system activity, providing a log of everything that has happened on your Paxton10 site. Events can be viewed by users that have been given the 'Events' permission within their software permission.

Aside from keeping track of system activity, events are required for many system functions to work, including:

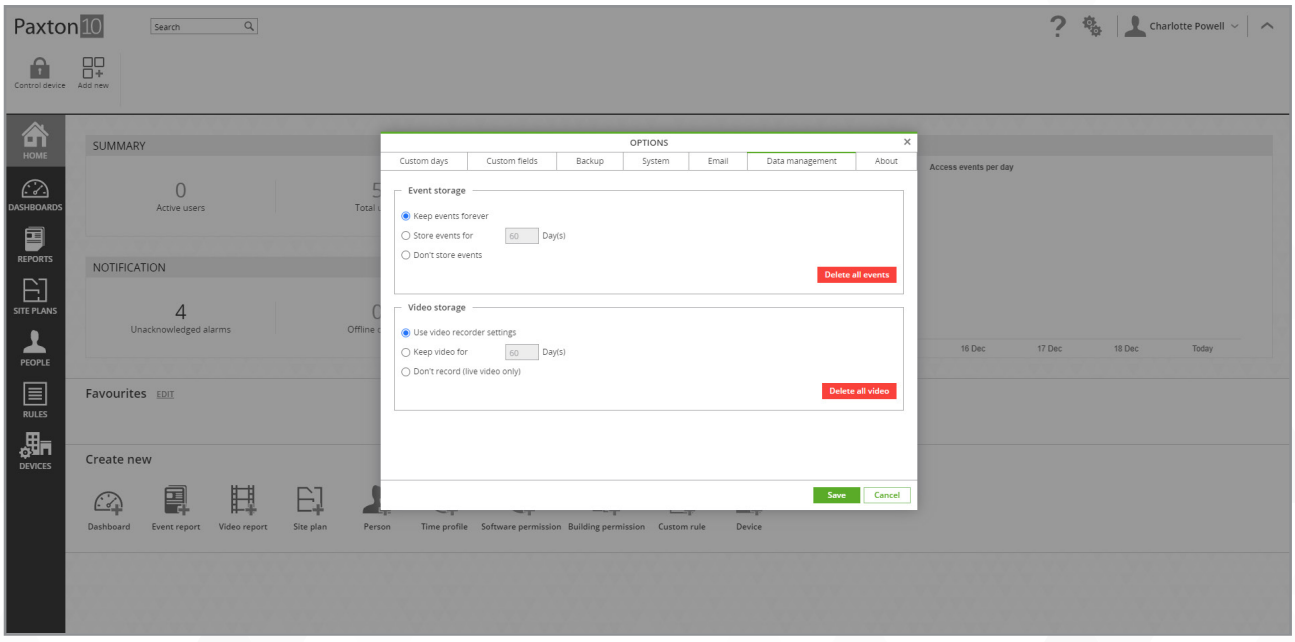
- Site plans
- Roll call and muster
- Anti-passback

Deleting events

Events can be deleted after a specified number of days, or not stored at all. These settings are available in the '**Data management**' tab within '**Options**'.

In addition, events can be deleted as a one-time action by using the '**Delete all events**' button. This will delete all events from the system, but new events may still be stored according to the event storage option.

Note: Some features may not function or may be unreliable without sufficient event storage. It is recommended to store events for a minimum of 3 days.



Video

Cameras added to the Paxton10 system can be viewed using video reports, event reports, dashboards and site plans. Video can be viewed by users that have events permission to an event with associated video, or read permission to a selected camera, video report, dashboard or site plan containing a camera.

APN-0041-AE

Deleting video

Old video is erased automatically when storage space is exceeded.

Video can be deleted after a specified number of days, or not stored at all. These settings are available in the '**Data management**' tab within '**Options**'. Alternatively, video storage can be managed on a per video recorder basis, where the settings can be found in the '**Storage location**' section of each video recorder device.

In addition, video can be deleted as a one-time action by using the '**Delete all video**' button. This will delete all video from all cameras, but new video may still be recorded depending to the video storage option.

Users

User records in Paxton10 represent the person and their activity on the system. User details can be viewed by anyone with '**Events**' permission to the user and '**Read**' permission to Reports, or '**Read**' permission to the user.

Reporting on a user

To view all information stored for a user, there are 2 reports that will help:

- List all users – This default report displays all user entered information for each user on the system. Select 'Field chooser' in the ribbon to enable all fields to ensure nothing is missed.
- All events – This default report displays all system recorded activity. Filter the report by an individual to view all their recorded activity.

Deleting a user

With a user's record open, use the '**Delete**' button within the ribbon to remove the selected user from the system.

For deleted users, their name in associated events will be substituted with '**Deleted user**'.

Software access

To prevent unauthorised use of the software, several measures are in place to permission and restrict the use of the software.

Software permissions

A user can only access the Paxton10 software if they have:

- A valid email address.
- A Software permission providing access to at least one part of the system.

Each user will only be able to view what they have been given software permission to see.

To remove a user's access to the software, any one of the following can be used:

- Bar the user.
- Set the user's expiry date.
- Remove the user's email address.
- Remove the user from software permission(s).
- Delete the user.

Automatic log out

Users will be logged out after 2 hours of inactivity.

For added security, a session may last a maximum of 8 hours before the user must re-login.

If the logged in user is barred or has their software permission removed or changed during their current session, they will be immediately logged out.

Strong Passwords

Paxton10 uses an email address and password to secure each login. When creating a password, users must meet the minimum requirements: at least seven characters and a mix of at least three character types, including uppercase letters, lowercase letters, numbers, and punctuation. The system also checks new passwords against a large open-source list of more than 100,000 common or previously compromised passwords. If a password appears on that list, Paxton10 will reject it to prevent weak or unsafe choices. A built-in strength indicator helps users see how secure their password is as they type.

If needed, administrators can raise the minimum password length and can also enable a policy that forces users to change their passwords every 60 days. Both options are available in the Options menu.

To protect against repeated guessing, Paxton10 allows six failed login attempts. After the sixth incorrect attempt, the user is blocked from logging in for 15 minutes before they can try again.

Passwords are stored securely in the server database using salted hash.

Backup and restore

Paxton10 backs up data and events each day. The system can be restored with this information at a later date by a software user with System Engineer permissions.

Deleted users and events may still be available on these backups. Backups are overwritten automatically when space requires. Depending on the size of the system, a backup may remain available for a few weeks.

Please call Paxton support if you would like to know how to remove your backups safely at a given time.

Frequently asked questions

How do I import credentials?

Currently, it is not possible to import credentials from another system.

Can I update details of existing users?

To update details of existing users, ensure the user records contain an email address, then include the email address in the import file, along with the user's name and updated information. If the email addresses are found to match existing users, the import will update these users with any new or changed information.

Can I import users directly from the export of a Net2 or Paxton BLU system?

A CSV export from Net2 or Paxton BLU can be utilized by copying the relevant information into the correct columns within the template provided.

Note: Not all data exported by Net2 or Paxton BLU can be imported into Paxton10. For example, access levels are not imported meaning new building permissions must be created.

Can I import users directly from the export of a third party system?

The import can identify data from a number of headings and can extract data where custom delimiters are used. Providing a name field can be detected, Paxton10 will do its best at importing what it can.
For best results, use the template provided.

Always do a system backup prior to importing if you are unsure of the results.

© Paxton Ltd Rev C