Net2 Security Settings - Data Protection and Strong Password Enforcement

Overview

In light of EU Regulations coming in effect in May 2018, Paxton have made some additions to their flagship Access Control software, Net2, to accommodate peoples right to be forgotten.

From v5.04 onwards, the options menu of Net2 now includes an additional security tab.

This tab will present you with two sections for enabling advanced security options; Password Strength and Automatic Logout & Event Retention settings.
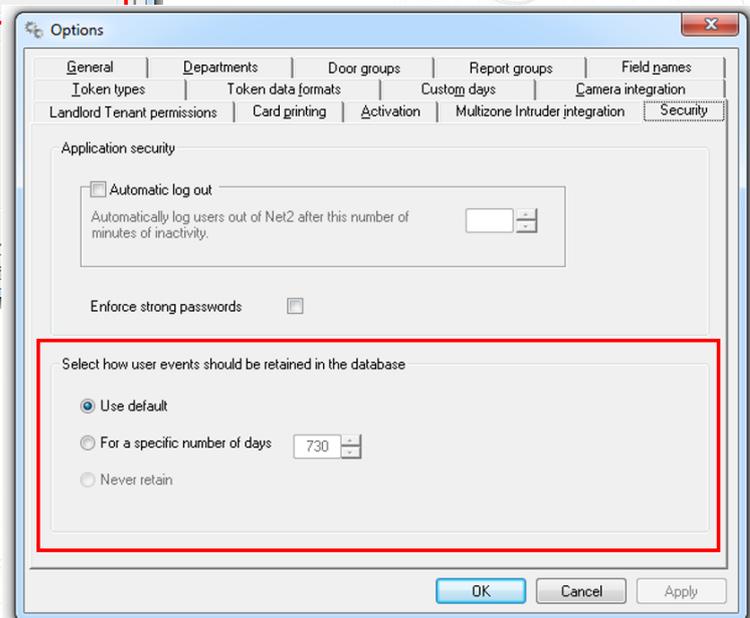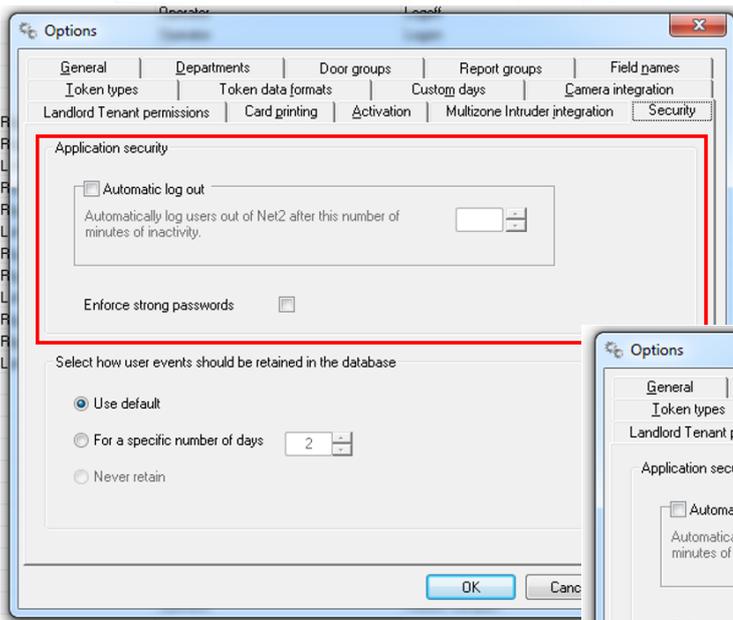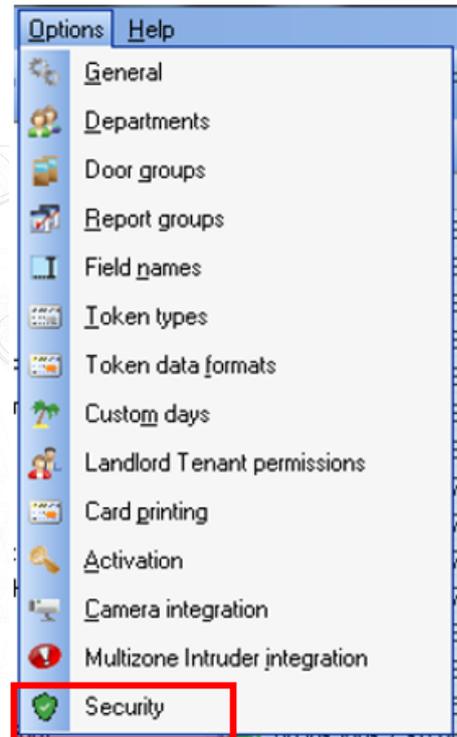
Password Strength and Automatic Logout

We have updated our software so as to comply with EN60839-11-1 Grade 1&2. In short, this provides a facility to allow stronger passwords to be used to access the Net2 system. When enabled by checking the 'Enable Strong Passwords' checkbox, a minimum of 5 Alphanumeric characters are required for any operator in the system.

Existing operators with passwords that do not meet the minimum requirement will be required to enter a new password for their operator account. To advise on this, operator passwords that do not meet the required character minimum will be advised on login and will need to speak to the system administrator to update their password.

NOTE: The default operator account, 'System Engineer' is unaffected by this rule so access to the system can still be achieved in the event that this service is enabled, but the default 'System Engineer' operator account has not been updated to meet the requirement.

When setting an operator password, you will be advised if the password meets the required number of characters with simple cross or tick advisories:
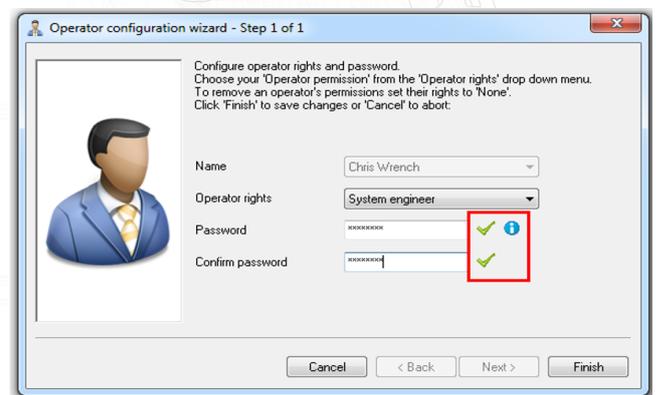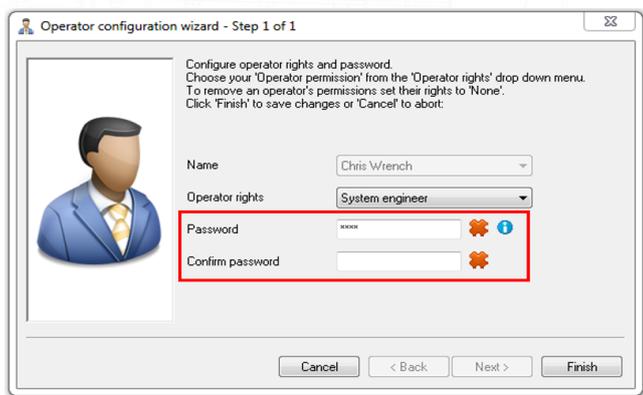

Automatic Logout

This facility will allow you to set a time by which the system can remain idle. Should the system remain idle or inactive beyond this time, the system will automatically log the user off and return to the login screen. This provides an added level of security and will help prevent systems left unattended from remaining open for extended periods and being at risk of access by unauthorised users.

The Automatic log out can be set from 1 - 500 minutes by adjusting the number using the arrow controls, or manually typing the required number of minutes.
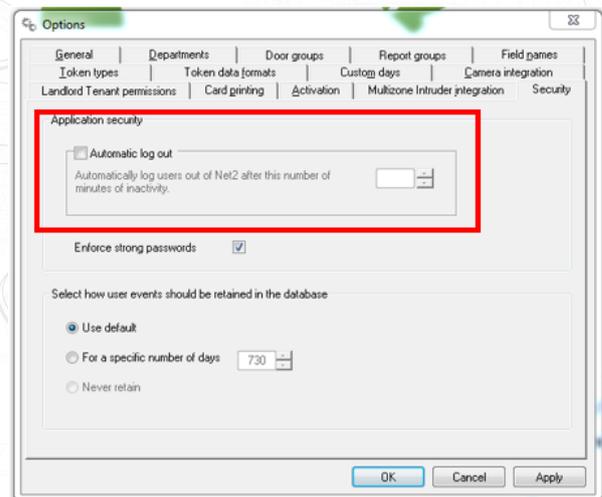
Event retention

It is now possible to specify how events should be retained within the database. The default setting remains in place, showing all events associated with the system, but also allows you to set the number of days the events will remain within the system or even the option not to retain events at all.

A warning will be issued when selecting either the specific number of days or the never retain option, advising you that the events will be deleted from the system:
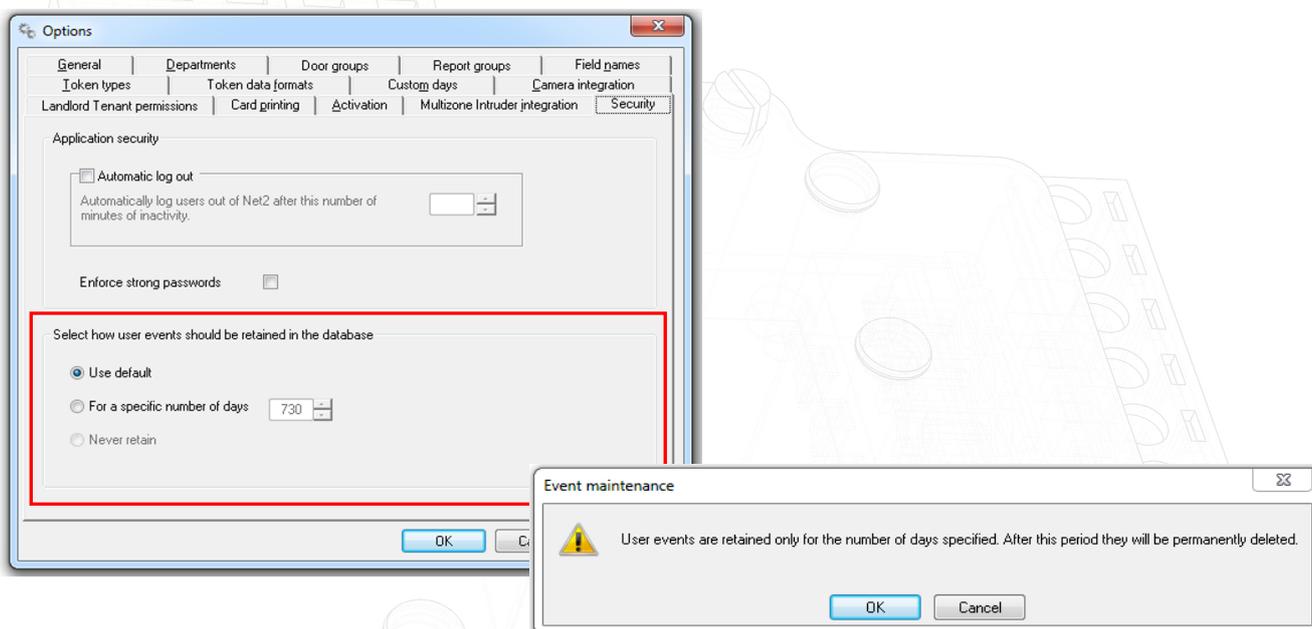
Choosing to never retain events will mean no events relating to a user's activity are stored within the system. Only System, Information and Alarm events will be displayed in the Events table.

Only System Engineers can make the changes to the data protection settings. To ensure that information is correctly recorded regarding data protection settings, events will be generated in Net2 to advise of changes made to these settings and by whom.

## User Deletion and removal from the system

As part of the 'right to be forgotten' policy, users who are removed from the system can also have events associated with their account removed from the system. When selecting to delete the user, the operator will be presented with additional confirmation screens. Once confirmed that the user is to be deleted you will be asked if you wish to retain or delete the events associated with that user.
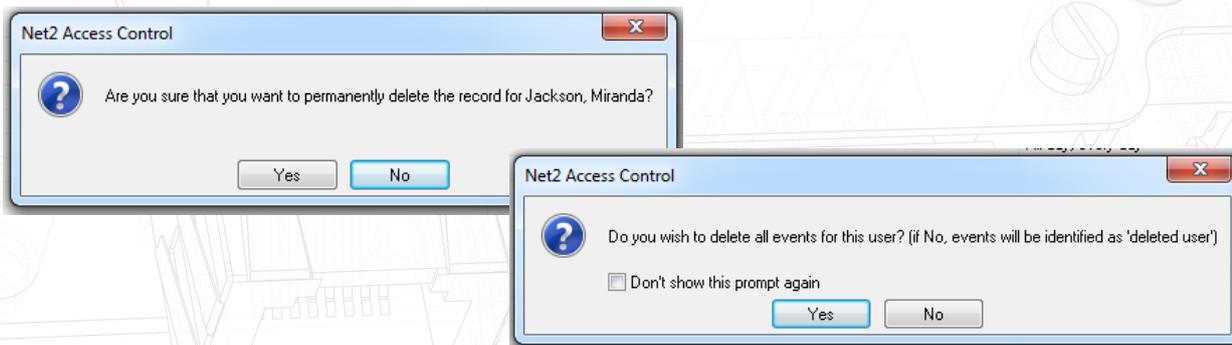
Selecting 'No' will retain the events within the system, but will label the events as 'Deleted' User' to prevent the user from being identified.

Because of this, you will be asked to confirm that you wish to retain the events as no user information will be associated with the event.

Net2 will also remove the video icon associated with a 'Deleted User' event to prevent a person being identified visually. This does NOT remove the video footage from the recording device. It is the responsibility of the video recording vendor to supply this functionality.

Depending on the size of the system, the length of time the user has been active in the system, the number of events associated with the user being deleted etc.., as users are deleted from the system, the system will search the database for events associated with that user and remove them from the database. This is performed in the background and depending on the amount of data held may take several minutes to complete. To advise you of the successful deletion of a user, an event will be generated to advise you the request has been completed. This will list the name of the deleted user but will not contain any other identifying information about that user. This is so confirmation can be made that the user was successfully deleted from the system.

Disclaimer: It is the responsibility of the System Administrator/ Owner to ensure that these settings are applied correctly and with the knowledge of their intended functionality. Paxton will not be held liable for any loss of data due to the incorrect or improper implementation of these services.