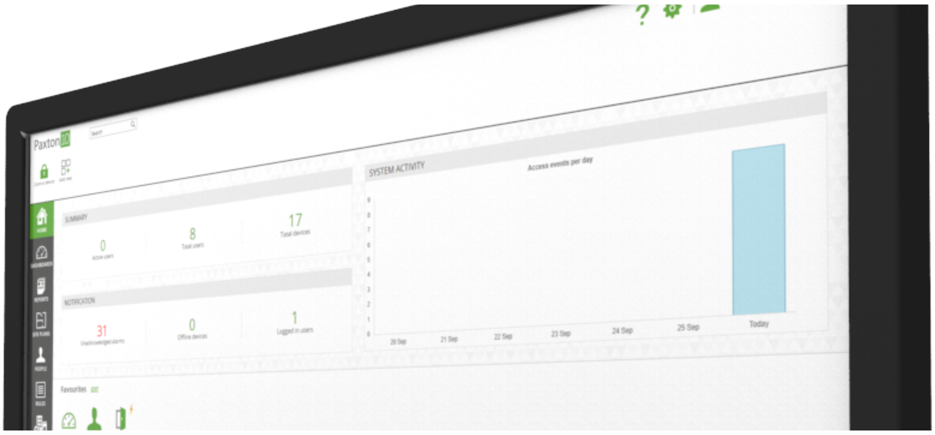

Using Keypads with Paxton10

Overview

Keypad readers can be a great way of enhancing security and safeguarding against lost and stolen credential use. Keypad readers add additional reader operating modes to an access point or controllable device.

Reader operating mode	User action required	User identified
Token only	Present a valid proximity token.	Y
PIN only	Enter the user's PIN at the keypad.	Y
Code only	Enter one of the device's codes at the keypad.	N
Token + PIN	Present a valid proximity token, then enter the user's PIN. The token holder and PIN must belong to the same user.	Y
Token + Code	Present a valid proximity token, then enter one of the device's codes.	Y
Token or PIN	Present a valid proximity token, OR enter the user's PIN.	Y
Token or Code	Present a valid proximity token, OR enter one of the device's codes.	Y/N
Token or PIN or Code	Present a valid proximity token, OR enter user's PIN, OR enter one of the device's codes.	Y/N

A code is specific to a device whereas a PIN is specific to a user

When to use a Paxton10 Keypad

A Paxton10 keypad reader can be installed in place of any existing Paxton10 reader.

Security

Keypad readers can be used to add a second level of authentication by requiring token holders to provide a secondary confirmation.

When used in '**Token + PIN**' or '**Token + Code**' operating modes, a lost token or overheard code on its own would not allow access to the building; to gain entry an intruder would need to possess both a valid token AND its associated PIN or door code.

Convenience

It is common for users to forget their token, or leave their token on their desk at work, giving opportunity to being locked out. Using a '**Token or PIN**' or '**Token or Code**' operating mode allows users to gain access without their token, which can be ideal for low security doors.

Permissions

Where a PIN or token is used, access is permissioned by the user's building permissions. Where only a code is used, the user is not known, and therefore will be granted access providing the code is valid at the device.

Mapping a keypad reader

Keypad readers are mapped to a device in the same way as proximity readers.
See: AN0006 - How to add a reader <paxton.info/4966>

Configuring a reader's operating mode

1. Navigate to the device which has a reader mapped to it

2. In the '**Configuration**' tab, expand the 'Readers' section

3. Check the box next to Authentication options to enable the operating mode selection

4. Select the operating mode required

For access points, Entry and Exit readers can have different operating modes (For example, require a Token + PIN to enter the building, but only require a Token to exit the building).

5. If Bluetooth credentials (Smart devices or Paxton10 Hands free keyfob) are in use, select the read range of these credentials, and check 'Verification' if smart device users are required to have a PIN or Biometrics setup on their device for them to be valid

See: AN0006 - How to add a reader <paxton.info/4966> for more information on Bluetooth credentials.

If a different operating mode is required at a specified time, 'Timed authentication' may be used.

6. Complete the above steps for '**Authentication options**'

7. Check the box next to '**Timed authentication**' to enable the additional operating modes

8. Click '**Select**' and choose the time profile required for different operation

9. Configure the reader operating mode, Bluetooth mode, and Verification settings to apply during the selected time profile

(For example, authentication options may be set to a secure Token + code mode, but during working hours when there are always people in the building, a more convenient Token or code option may be appropriate)

When Authentication options is not checked, the readers will operate in Token only mode.

Managing codes

Codes are managed per device, and can be used by any user.

When a code operating mode has been set, click '**Manage codes**' in the device's '**Readers**' section to create a code for that device. Enter a code, then click 'Add', or select an existing code and click 'Remove' to delete it.

Each device can have multiple codes.

Managing PINs

PINs are unique to each user, and are treated as a credential within the user record.

To give a user a PIN credential:

1. Open the user's record, and click on their '**Credentials**' tab
2. Click '**Add a credential**'
3. Select '**PIN**' from the drop-down
4. Enter a new PIN number, or accept the randomly generated one
5. Click '**OK**'

PIN length can be changed in system options.

Frequently asked questions

What is the difference between a PIN and a code?

A personal identification number (PIN) is unique to each user. Each user will have their own PIN, and their PIN will only give access at devices they have Building permission for.

In comparison, a code is set at each device, and can be used by multiple users. A code cannot be used to identify a user, and therefore are not constrained by Building permissions.

What is the length of a PIN?

The PIN length must be between 4 and 8 digits; this is configured in system options. All PINs on a system must be the same length.

I have run out of unique PIN numbers, what do I do?

The PIN length can be changed in system options. Increasing the PIN length will increase the possible number of PIN combinations, also increasing system security.

Note: Increasing the system PIN length will add '0's to the end of all existing PIN's to meet the new length requirement. Warning! Decreasing the system PIN length will delete all PIN credentials.

What is the length of a code?

Codes must be between 4 and 8 digits. Codes of different lengths can exist.
Why can a device have multiple codes?

There are many scenarios where multiple codes may be given to a device, for example:

- A code for the car park barrier to be given to visitors, which changes on a weekly basis. While the code used by employees remains constant.
- Different codes to represent different levels of access, such as higher management using one code which works at every device, and cleaners using a different code which only works at some devices.

Does using a code operating mode affect anti-passback or roll call?

When using 'Code only' operating mode, the user is not known and therefore user position cannot be determined. For roll call reporting and anti-passback restriction, an operating mode that includes a user credential (Token or PIN) is required.