

Configuring Keypads

The IEI eMerge™ supports the use of keypads requiring PIN entry. The keypads must send Wiegand formatted data and have a facility code that is not represented in the card population. This unique facility code is how the eMerge recognizes a PIN entry from a card read.

NOTE: PINS must be either 4 or 6 digit numbers.

As of version 3.0, the eMerge now also supports 8-bit burst keypads.

The example and procedures below assume that both a card reader and keypad are required.

Create a format for the keypad data:

1. Select **Setup : Access Control : Card/Keypad Formats**.

NOTE: The keypad must produce Wiegand formatted data and the facility code must differ from the facility codes used in the card population. This is how the eMerge will recognize the difference between the PIN entry and a card read.

2. Select **Setup : Access Control : Card/Keypad Formats** and create a separate format for the keypad. Check the keypad manufacturer's documentation for the correct bit length and facility code. We suggest naming this format so that it is clearly recognizable as the format for the keypad. This will help avoid confusion when setting up the reader/keypad.
3. Click **Save**.
4. If it is not already done select **Setup : Access Control : Card/Keypad Formats** and create a format for the access card.
5. Click **Save**.

Set up the reader/keypad:

1. Select **Setup : Access Control : Readers/Keypads**.
2. Complete the reader/keypad setup page and be sure to select **Wiegand Keypad and Card Reader** or **Bit-Burst Keypad and Wiegand Card Reader** from the **Reader/Keypad Type** drop-down.

NOTE: If you are setting up a keypad only then select **Wiegand Keypad** or **Bit-Burst Keypad**.

3. From the **Card/Keypad Format** drop-down that appears to the right select the keypad format.
4. Click **Save**.

Configure the reader and keypad as part of the portal:

1. Select **Setup : Access Control : Portals**.
2. Complete the portal setup page and in the **Card Readers/Keypads** section be sure to select both **Reader 1** and **Keypad 1** from the drop-downs. This configures the portal to require both a valid card read and a correct PIN entry. If the reader/keypad is a single device then the same name will be selected for both **Reader 1** and **Keypad 1**.

NOTE: A time spec and a threat level can be assigned to the keypad.

3. Click **Save**.

Set the keypad PIN entry timeout timer:

1. Select **Setup : Site Settings : Network Controller**.
2. Scroll down to the **Misc. Information** section.
3. In the **PIN entry timeout (secs)** field enter the number of seconds you wish to allow for the completion of PIN entry. If the PIN is not entered within this number of seconds access will be denied.
4. Click **Save**.

Enter a 4 or 6 digit PIN in the person's information page:

1. Select **Administration : People**.
2. Go to the user's information page.

NOTE: If it is not already done, issue a card to this person.

3. In the **Access Control** tab enter a 4 or 6 digit PIN in the **PIN** field.
4. Click **Save**.

Test your reader/keypad configuration:

1. Swipe the user badge across the reader.
2. Enter the PIN followed by the star (*) key.

NOTE: Bit-Burst Keypads do not require the star (*) key.

3. Check that the portal unlocks.
4. Check the **Activity Log** for an "Access granted" log entry.