6 High Security features and enhancements

6.1 T20 and T21 cipher pad feature

Keep cardholder PINs safe from 'shoulder-surfing' through randomizing keypad numbers when a card is presented.

Background

For sites that require a higher level of security, a standard Card + PIN authentication may not be sufficient. This is due to the risk of a user's PIN number being read by a third party from a distance while it is entered into the keypad, or by tracing the keys used on the keypad. To reduce this risk, Gallagher is introducing a new feature that will allow you to configure T20 and T21 terminals to present a randomized key array on the screen each time PIN entry is required after presenting a card. This can be applied for both access control PIN entry and when logging on to perform alarm management functions.

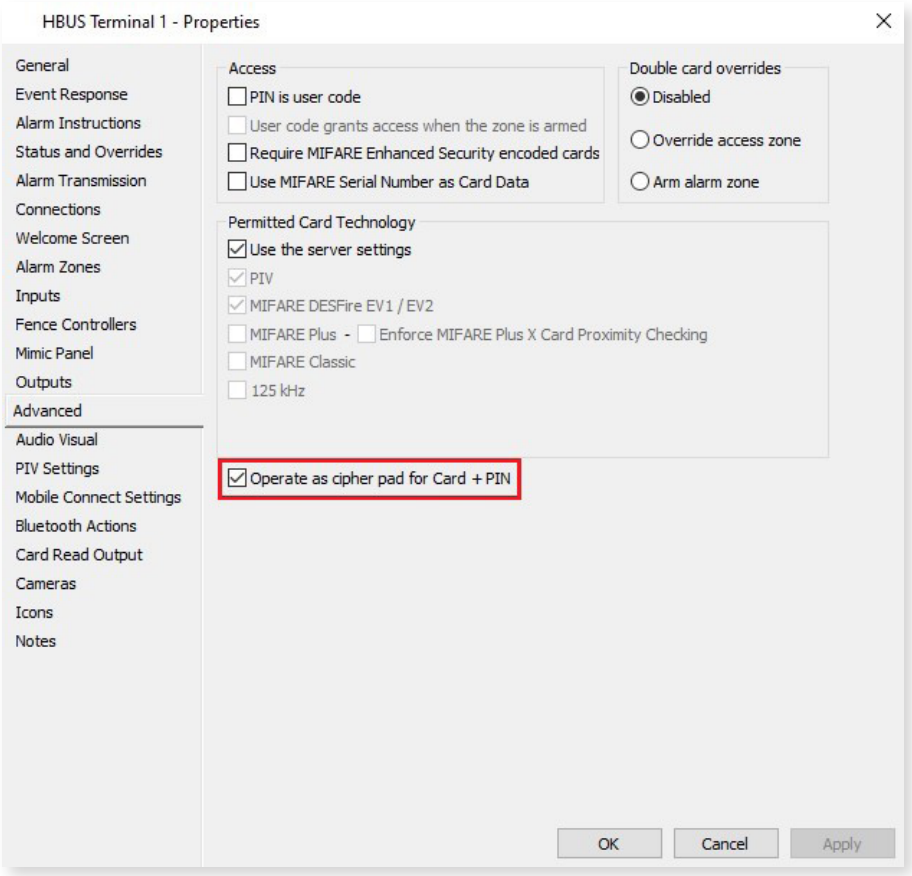
Figure 1

For visually impaired users, the cipher pad functionality can be bypassed when they present their cards at the terminal, reverting the T20 or T21 back to normal keypad operations. This ensures all users can gain access where the cipher pad functionality is enabled.

Configuration

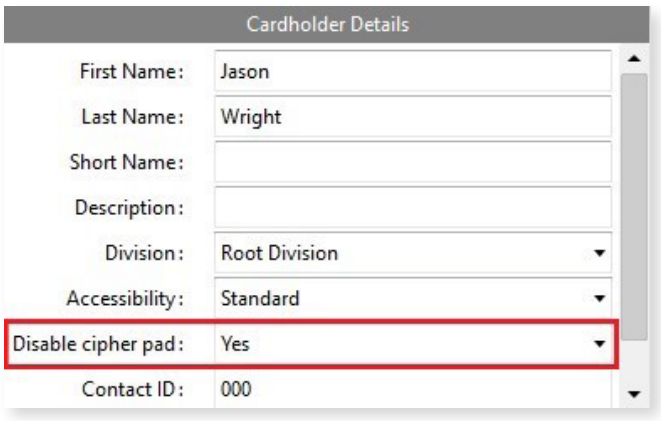
A new setting will be introduced against the terminal in v8.50 to allow it to operate as a cipher pad for the specific area requiring more secure PIN entry, when configured for Card + PIN authentication. With this setting selected, each time a user badges their card at that terminal, and the terminal is in PIN mode, a randomized set of numbers will appear on the screen.

Figure 2



To bypass the cipher pad operation for those with a visual impairment, a new accessibility option has been added against the cardholder. Cardholders with the 'Disable Cipher Pad' option enabled, will be able to operate the keypad without the numbers being randomized.

Figure 3



Licensing

This feature will be freely available to any site that is using T20 (excluding alarms only variant) or T21 terminals, with Command Centre v8.50 and beyond.