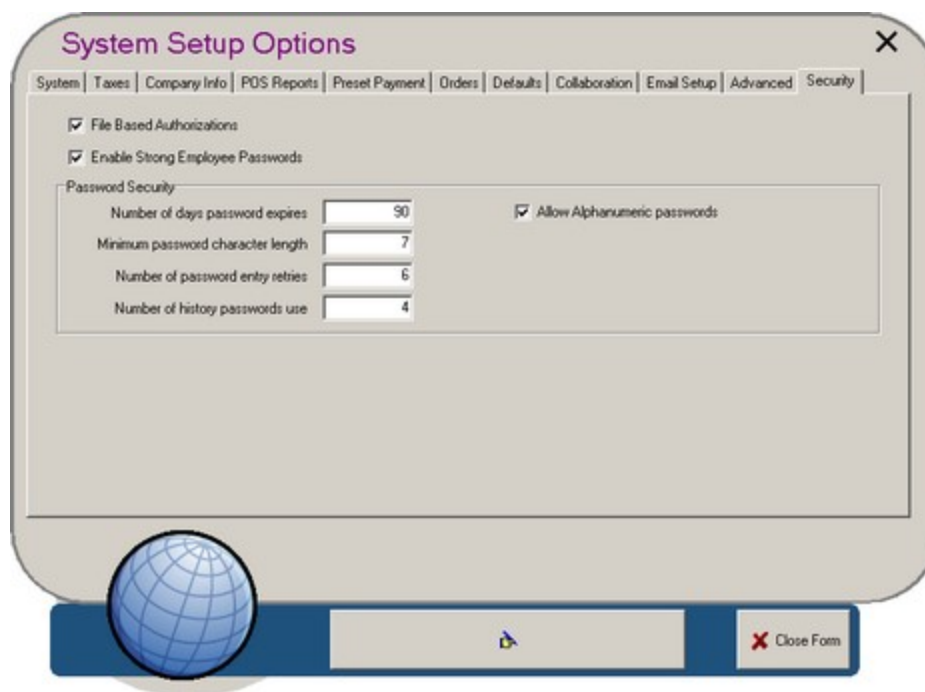


Advanced Tab

Administrator / System Setup / Security

This tab in System Setup provides options governing password security, and configures PixelPoint POS to store authorization data using file-based methods for PCI PA-DSS compliance.



The screenshot shows the 'System Setup Options' dialog box with the 'Security' tab selected. The dialog has a title bar with a close button (X) and a menu bar with options: System, Taxes, Company Info, POS Reports, Preset Payment, Orders, Defaults, Collaboration, Email Setup, Advanced, and Security. The 'Security' tab is active, showing two checked options: 'File Based Authorizations' and 'Enable Strong Employee Passwords'. Below these is a 'Password Security' section with four input fields: 'Number of days password expires' (90), 'Minimum password character length' (7), 'Number of password entry retries' (6), and 'Number of history passwords use' (4). There is also a checked option 'Allow Alphanumeric passwords'. At the bottom of the dialog is a blue bar with a globe icon, a small icon, and a 'Close Form' button with a red X.

File-Based Authorization

To temporarily store authorization data outside the PixelPoint database in order to adhere to PCI PA-DSS requirements, select the *File Based Authorizations* option.

Strong Employee Passwords

Several options are available to increase employee password security. They are:

Number of days password expires: Determines how many days the same password can be used for before a change is required.

Minimum password character length: Determines the minimum number of characters required within the password.

Number of password entry retries: The number of failed login attempts allowed before the employee is locked out and their password must be reset.

Number of history passwords use: The number of password changes before an old password may be reused.

Allow Alphanumeric passwords: Switches to an alphanumeric keyboard at login instead of numeric keypad. This is necessary if employee passwords contain alphanumeric characters and a physical keyboard is not available.

Select *Enable Strong Employee Passwords* to make these password options available. Doing so will enable additional password options in Employee Setup (see "[Employee Setup>Advanced Tab](#)") and also prompt employees to enter their password (instead of swipe #) at login.