Enhanced WinSPC security options ensure validity of collected data and uphold FDA 21 CFR Part 11 reg

Since Version 7.1 WinSPC has offered users a variety of password and audit trail settings to meet even the most stringent procedural requirements. Below are examples of controls in WinSPC to ensure system and data integrity.

Password and audit trail security options defined:

WinSPC centralizes the administration of password security on an "Audit/Security" tab. Here are ten ways to customize your password security options using the "Audit/Security" tab settings:

"Minimum password length": Specify the smallest number of characters that a password must contain. "Password mask": Use character-code specifications to define the acceptable format of passwords:

Spec	Defines
#	A numeric digit (0-9)
A	An uppercase letter (A-Z)
a	A lowercase letter (a-z)
&	An upper or lowercase letter (A-Z or a-z)
N	An uppercase letter or numeric digit (A-Z or 1-9)
n	A lowercase letter or numeric digit (a-z or 1-9)
?	Any character
\	Identical to the character that follows the slash

"Required password change every" Indicate a number of days after which a user is either reminded or required to change their password. "Password must be unique from previous" Stipulate that a password must be different from up to six previously used passwords. "Password changes allowed" Regulate the number of times a user can change their password within a specified number of days. "Maximum password failures allowed" Set the number of consecutive failed login attempts a station will tolerate before it locks. "Password required for administrative tasks" Require users to enter a password when attempting to perform an administrative task. "Password required to enter data collection" Require a password to go from the Navigator window into Data Collection. "Password required at beginning of each cycle in data collection" Require users to provide a password when beginning a data collection cycle. "Password required at end of each subgroup in data collection" Require password each time a user completes the collection of a subgroup of data.

The Audit/Security tab also contains audit trail option settings. When the system audit trail is enabled, actions taken within the software are recorded. These events can then be viewed and filtered within the event log. A new feature included in Version 7.1 offers a setting to require users to enter a reason for the modifications they perform, providing an extra level of detail when auditing your processes.

For added security, check the "Deleting events..." checkbox to require any record deleted from the Event Log be archived to preserve the complete audit trail history. Check the last checkbox in the "Audit Trail Options" pane to log Data Collection exceptions as well.

How to access the Audit/Security tab in WinSPC Versions 7.1 and Above:

On the "Administrator" window, from the menu bar, select "Tools" and then "System Settings". On the System Settings dialog box that appears, click the "Audit/Security" tab. This tab is divided into the two parts discussed above, "Password Options" at the top and "Audit Trail Options" on the bottom.

https://knowledgebase.winspc.com/questions/171/