The Impact of 21 CFR Part 11 on Software Development

by Allan McNaughton

Software has become a critical part of the highly regulated pharmaceutical industry. For those solutions that cannot be purchased off-the-shelf, many companies have developed custom software that closely meshes with their internal business and manufacturing processes. While this may result in significant cost savings by streamlining complex operations, it can also subject developers to the provisions of ruling 21 CFR Part 11 from the Food and Drug Administration (FDA).

FDA ruling 21 CFR Part 11 specifies how electronic records and electronic signatures can be used as a substitute for paper records and handwritten signatures. It is broadly applicable to any electronic records that are central to the process of developing and manufacturing drugs, including software. The goal of this paper is to educate software developers so they can understand the impact of this ruling and learn how to achieve compliance through the intelligent use of tools and process.

What are electronic records?

According to the FDA, an "electronic record means any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system." Not all electronic records are subject to 21 CFR Part 11, only those that are maintained in accordance with FDA published predicate rules.

These rulings, such as the Good Laboratory Practice (GLP) and Current Good Manufacturing Practice (CGMP), mandate what records must be maintained, what needs to be contained in the record, whether signatures are required and how long records must be maintained.

What is an electronic signature?

Electronic signatures are intended to be binding digital equivalents of handwritten signatures. The FDA states that an "electronic signature is a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature." It is important to note the FDA does not equate an electronic signature with a "digital" signature, such as those provided by commercial entities Verisign, Entrust, etc.

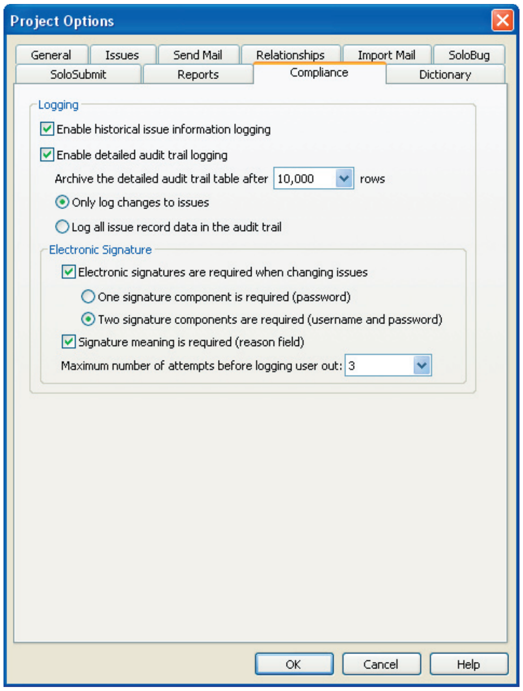
FDA predicate rules specify which electronic records require signatures, electronic or otherwise. If signatures are necessary, and they are collected electronically, then compliance with 21 CFR Part 11 is mandatory.

How does the ruling impact software development?

To meet the requirements of 21 CFR Part 11 a software project must follow rigorous change tracking and signoff procedures. The intent of this ruling is to ensure there is a clear and irrefutable record of each and every change made during the project lifecycle. This otherwise cumbersome task can be made simpler using change management tools that are built with compliance in mind. When selecting these tools one should look for the following qualities:

- Access is limited to authorized users.
- Records can only be updated by users with sufficient privileges.
- Timestamps are recorded for each change.
- Changes are authenticated using electronic signatures.
- Accurate change histories are maintained for all files.
- Meets audit trail requirements.

Fulfilling these requirements is straightforward with Seapine Software's issue management and change control tools, TestTrack Pro and Surround SCM. These tools are built for the task and offer an array of features that ease regulatory compliance. TestTrack Pro helps organizations meet FDA requirements with a capable issue tracking system that supports electronic signatures and audit trails (see Figures 1 and 2). Surround SCM furthers regulatory compliance by accurately tracking changes to any digital — source code, test plans, specifications, and other artifacts.



Logging

☑ Enable historical issue information logging

☑ Enable detailed audit trail logging

Archive the detailed audit trail table after 10,000 rows

● Only log changes to issues

○ Log all issue record data in the audit trail

Electronic Signature

☑ Electronic signatures are required when changing issues

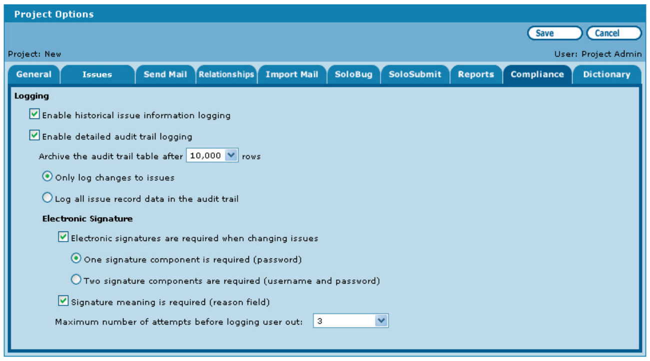
○ One signature component is required (password)

● Two signature components are required (username and password)

☑ Signature meaning is required (reason field)

Maximum number of attempts before logging user out: 3

Figure 1 Compliance Options Settings,
Windows Client View



Project: New

User: Project Admin

Logging

☑ Enable historical issue information logging

☑ Enable detailed audit trail logging

Archive the audit trail table after 10,000 rows

● Only log changes to issues

○ Log all issue record data in the audit trail

Electronic Signature

☑ Electronic signatures are required when changing issues

● One signature component is required (password)

○ Two signature components are required (username and password)

☑ Signature meaning is required (reason field)

Maximum number of attempts before logging user out: 3

Figure 2 Compliance Options Settings,
Web Client View

21 CFR Part 11 Compliance Matrix

The following matrix provides a detailed assessment of how TestTrack Pro and Surround SCM facilitate compliance with 21 CFR Part 11.

The term “acknowledged” is used to answer portions of the Scope where there is no notable action required on part of the software. This indicates the recommendation has been read and understood in the context presented.

Any software that is used to comply with 21 CFR Part 11 is only an element of the solution. Compliance cannot be achieved by the introduction of tools alone. It is how the tools are used that determines whether an organization reaches its compliance goals. A well defined process with strong rules for enforcing accountability greatly facilitates this end.

Subpart A — General Provisions

21CFR11.1 Scope	TestTrack Pro and Surround SCM Compliance
(a) The regulations in this part set forth the criteria under which the agency considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper.	TestTrack Pro and Surround SCM support electronic signatures by positively identifying the user through a unique username and password combination. This information is controlled and centrally managed via a license server. LDAP integration allows the administrator to use LDAP to replace/supplement the built-in user management.
(b) This part applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted, under any records requirements set forth in agency regulations. This part also applies to electronic records submitted to the agency under requirements of the Federal Food, Drug, and Cosmetic Act and the Public Health Service Act, even if such records are not specifically identified in agency regulations. However, this part does not apply to paper records that are, or have been, transmitted by electronic means.	acknowledged
(c) Where electronic signatures and their associated electronic records meet the requirements of this part, the agency will consider the electronic signatures to be equivalent to full handwritten signatures, initials, and other general signings as required by agency regulations, unless specifically excepted by regulation(s) effective on or after August 20, 1997.	TestTrack Pro and Surround SCM support electronic signatures by positively identifying the user through a unique username and password combination.
(d) Electronic records that meet the requirements of this part may be used in lieu of paper records, in accordance with Sec. 11.2, unless paper records are specifically required.	acknowledged
(e) Computer systems (including hardware and software), controls, and attendant documentation maintained under this part shall be readily available for, and subject to, FDA inspection.	acknowledged

21CFR11.2 Implementation	TestTrack Pro and Surround SCM Compliance
(a) For records required to be maintained, but not submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that the requirements of this part are met.	TestTrack Pro and Surround SCM maintain a history of the action completed, with timestamp and identification of the person who completed that action. A verbose log file can be enabled to capture the full detail and history of any changes to defect records.
(b) For records submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that:	acknowledged
(1) The requirements of this part are met; and	
(2) The document or parts of a document to be submitted have been identified in public docket No. 92S-0251 as being the type of submission the agency accepts in electronic form. This docket will identify specifically what types of documents or parts of documents are acceptable for submission in electronic form without paper records and the agency receiving unit(s) (e.g., specific center, office, division, branch) to which such submissions may be made. Documents to agency receiving unit(s) not specified in the public docket will not be considered as official if they are submitted in electronic form; paper forms of such documents will be considered as official and must accompany any electronic records. Persons are expected to consult with the intended agency receiving unit for details on how (e.g., method of transmission, media, file formats, and technical protocols) and whether to proceed with the electronic submission.	acknowledged

21CFR11.3 General Provisions	TestTrack Pro and Surround SCM Compliance
(a) The definitions and interpretations of terms contained in section 201 of the act apply to those terms when used in this part.	acknowledged
(b) The following definitions of terms also apply to this part:	acknowledged
(1) Act means the Federal Food, Drug, and Cosmetic Act (secs. 201-903 (21 U.S.C. 321-393)).	acknowledged
(2) Agency means the Food and Drug Administration.	acknowledged
(3) Biometrics means a method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable.	The use of biometrics is not currently supported by TestTrack Pro or Surround SCM.
(4) Closed system means an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.	TestTrack Pro and Surround SCM can be configured as either an open or closed system.
(5) Digital signature means an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified	TestTrack Pro and Surround SCM use a set of rules based on security group settings that uniquely identifies the user from their username and password combination. The internal security settings in these tools determine the access and privileges of the signed in user.
(6) Electronic record means any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.	acknowledged
(7) Electronic signature means a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.	TestTrack Pro and Surround SCM support electronic signatures by positively identifying the user through a unique username and password combination.
(8) Handwritten signature means the scripted name or legal mark of an individual handwritten by that individual and executed or adopted with the present intention to authenticate in writing in a permanent form. The act of signing with a writing or marking instrument such as a pen or stylus is preserved. The scripted name or legal mark, while conventionally applied to paper, may also be applied to other devices that capture the name or mark.	The use of biometrics is not currently supported by TestTrack Pro or Surround SCM.
(9) Open system means an environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system.	TestTrack Pro and Surround SCM can be configured as either an open or closed system.

Subpart B — Electronic Records

The FDA distinguishes between open and closed systems. Closed systems are those where access is controlled by persons who are responsible for the content of electronic records on the system. Open systems are accessible by those who are not directly responsible for the electronic records on the system.

21CFR11.10 Controls for Closed Systems	TestTrack Pro and Surround SCM Compliance
Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:	Since TestTrack Pro and Surround SCM are true client/server applications using an IP address and port to access the database and they require a unique username and password combination, the administrator can set up a closed system in which access is limited internally to the server.
(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	TestTrack Pro and Surround SCM can be configured as a closed system with an audit trail. The organization can use the audit trail to discern between valid and invalid records. The history of the actions completed within Surround SCM serves as an audit trail for validation purposes. TestTrack Pro maintains a distinct audit trail for this purpose.
(b) The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.	TestTrack Pro and Surround SCM reports include who made changes, when they made them, and the type of change. Changes are date/timestamped. Change comments are included. A verbose log file can be enabled to capture the full detail and history of any changes to records. The full record history can be tracked and reassembled from this log. These reports can be distributed in paper or electronic form.
(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.	The security within TestTrack Pro and Surround SCM gives complete control over which users can complete specified actions when using these tools. The organization is ultimately responsible for backing up and protecting the records.
(d) Limiting system access to authorized individuals.	TestTrack Pro and Surround SCM use a set of rules based on security group settings that uniquely identifies the user from their username and password combination. The internal security settings in these tools determine the access and privileges of the signed in user.
(e) Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.	The history of the actions completed within Surround SCM serves as an audit trail for validation purposes. TestTrack Pro maintains a distinct audit trail that can retained indefinitely. A verbose log file can be enabled to capture the full detail and history of any changes to records.
(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	The ability to complete any given action is controlled at the security group level and is under the control of the administrator(s) to set what permissions are allowed to what users to make what changes at any given point in the process. The configurable workflow allows administrators to set up a workflow that is appropriate for the process being managed. The history of actions completed within TestTrack Pro and Surround SCM contains timestamp information for when the action was completed and by what user, showing the sequence in which actions occurred. The organization is ultimately responsible for enforcing proper sequencing of steps and events.
(g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	TestTrack Pro and Surround SCM use a set of rules based on security group settings that uniquely identifies the user from their username and password combination. The internal security settings in these tools determine the access and privileges of the logged in user.
(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	Within TestTrack Pro no historical record is made until an action is completed, e.g. “Add file”, “Check in”, “Assign defect”, etc. Within Surround SCM administrators can restrict what actions can be done through the security group up and require association of code with a defect with TestTrack Pro enforcing a strong change management process.

21CFR11.10 Controls for Closed Systems cont.	TestTrack Pro and Surround SCM Compliance
(i) Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.	Access is controlled via security groups to those individuals deemed appropriate. The organization is ultimately responsible for this requirement.
(j) The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.	The organization is ultimately responsible for this requirement.
(k) Use of appropriate controls over systems documentation including:	
(1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.	There is online help and documentation. Printed copies of documents and guides are available. The organization is ultimately responsible for this requirement.
(2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	The history of the actions completed within Surround SCM serves as an audit trail for validation purposes. TestTrack Pro maintains a distinct audit trail for this purpose, including an optional verbose log.

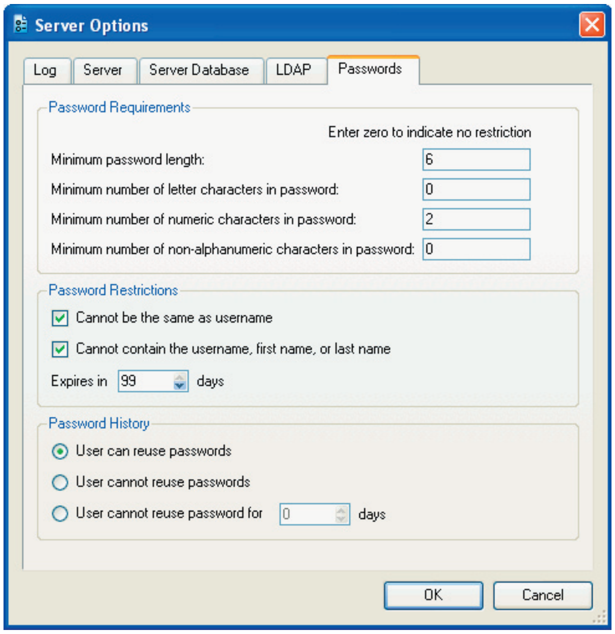
21CFR11.30 Controls for Open Systems	TestTrack Pro and Surround SCM Compliance
Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in Sec. 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.	TestTrack Pro and Surround SCM can be used as an open system or a closed system depending on the access to the server via an IP address and port. Through the use of the username and password combination and internal security groups the administrator has the ability to secure the system as required for compliance. Use of SoloSubmit, SoloBug, email import or any import method implicitly defines usage as an open system. This would mandate controls for open systems be applied.

21CFR11.50 Signature Manifestations	TestTrack Pro and Surround SCM Compliance
(a) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:	TestTrack Pro and Surround SCM use the username and password combination to uniquely identify the logged in user. LDAP support allows the use of an LDAP server to manage user compliance.
(1) The printed name of the signer;	The name of the signer is displayed.
(2) The date and time when the signature was executed; and	A date and timestamp are contained in the history.
(3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.	The completed action is logged. Information about the change, as entered by the signer, is also captured.
(b) The items identified in paragraphs (a)(1),	
(a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).	acknowledged

21CFR11.70 Signatures/Record Linking	TestTrack Pro and Surround SCM Compliance
Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.	The history of any action performed within TestTrack Pro and Surround SCM is not modifiable and contains the details of the action taken as well as a timestamp and the user who performed the action. A verbose log can be enabled to capture the full history of any committed changes.

Subpart C—Electronic Signatures

21CFR11.100 General Requirements	TestTrack Pro and Surround SCM Compliance
(a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	The unique username and password combination required by TestTrack Pro and Surround SCM ensures the user is authenticated when logging in. All records created by a user are permanently linked to the creators unique username. The administrator can configure the system so that passwords cannot be reused.
(b) Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.	The administrator is responsible for verifying that each user entered into the system is properly identified before entering a unique username and password combination for said user. Administrators can set strong passwords rules in the Seapine License Server that are applied universally, including the ability to enforce a minimum password length, minimum number of letter characters, numeric characters, and minimum number of non-alphanumeric characters in a password. Passwords can be restricted so they cannot be set to the user's username, first name, or last name. Passwords can optionally expire in "x" days. LDAP can be used instead of these features to centrally manage users. All records created by a user are permanently linked to the creators unique username (See Figures 3 and 4). The organization is ultimately responsible for this requirement.
(c) Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures.	The organization is ultimately responsible for this requirement.
(1) The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857.	The organization is ultimately responsible for this requirement.
(2) Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.	The organization is ultimately responsible for this requirement.



Password Requirements

Enter zero to indicate no restriction

Minimum password length: 6

Minimum number of letter characters in password: 0

Minimum number of numeric characters in password: 2

Minimum number of non-alphanumeric characters in password: 0

Password Restrictions

☑ Cannot be the same as username

☑ Cannot contain the username, first name, or last name

Expires in 99 days

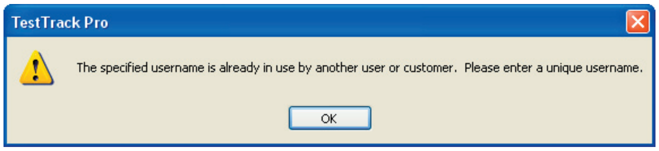
Password History

● User can reuse passwords

○ User cannot reuse passwords

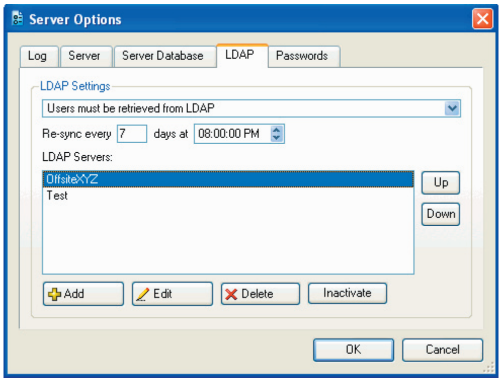
○ User cannot reuse password for 0 days

Figure 3
Passwords Options Settings, License Server Admin Client



The specified username is already in use by another user or customer. Please enter a unique username.

Figure 4
Existing Username Error Message

21CFR11.200 Electronic Signature Components and Controls	TestTrack Pro and Surround SCM Compliance
(a) Electronic signatures that are not based upon biometrics shall:	TestTrack Pro and Surround SMC use the user name and password combination to uniquely identify the user logging into the system. Privileges and access to actions is controlled by the security settings applied to the user. The security group settings to which the user belongs are determined by an administrator who has appropriate security access to manage such groups. Users can be members of multiple security groups in Surround SCM but only a single security group in TestTrack Pro. Security groups setting control the level of access for all users in the group.
(1) Employ at least two distinct identification components such as an identification code and password.	TestTrack Pro and Surround SCM use a username and password combination to identify the logged in User.
(i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual.	TestTrack Pro and Surround SCM require the user initiate a continuous period of controlled system access with a username and password combination. Each action that the individual executes within this period creates a historical record that contains information about the action and user. The username and password used at login positively identifies the user. The administrator can specify whether the password alone is sufficient for electronic signatures or that the username and password are both required.
(ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.	TestTrack Pro and Surround SCM require the user initiate a continuous period of controlled system access with a username and password combination. Each action that the individual executes within this period creates a historical record that contains information about the action and user.
(2) Be used only by their genuine owners; and	The organization is ultimately responsible for this requirement.
(3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.	This is a procedural issue since the "Administrator" user has the ability to manage and maintain all users and passwords. The "Administrator" user can change any user's password if necessary.
(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.	The use of biometrics is not currently supported by TestTrack Pro and Surround SCM. A unique username and password combination is required that identifies the individual logged in and completing actions. Administrators can set strong passwords rules in the Seapine License Server that are applied universally, including the ability enforce a minimum password length, minimum number of letter characters, numeric characters, and minimum number of non-alphanumeric characters in a password. Passwords can be restricted so they cannot be set to the user's username, first name or last name. Passwords can optionally expire in "x" days. LDAP can be used instead of these features to centrally manage users (see below). All records created by a user are permanently linked to the creators unique User Name.  Server Options LDAP Settings Users must be retrieved from LDAP Re-sync every 7 days at 08:00:00 PM LDAP Servers: OffsiteXYZ Test Log Server Server Database LDAP Passwords Up Down Add Edit Delete Inactivate OK Cancel

21CFR11.300 Controls for Identification Codes/Passwords	TestTrack Pro and Surround SCM Compliance
Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:	TestTrack Pro and Surround SCM require that a named user logs into the application. Administrators can set strong passwords rules in the Seapine License Server that are applied universally. LDAP can also be used to centrally manage users.
(a) Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.	TestTrack Pro and Surround SCM use a username and password to uniquely identify the person logged into the system. The password is not required by default but can be enforced. Usernames must be unique and are not case sensitive. All records created by a user are permanently linked to the user's unique username.
(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).	Administrators can set strong passwords rules in the Seapine License Server that are applied universally. LDAP can also be used to centrally manage users.
(c) Following loss management procedures to electronically de-authorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.	TestTrack Pro and Surround SCM do not use tokens, cards, or other devices at this time.
(d) Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.	TestTrack Pro and Surround SCM are true client/server applications that are accessed through an IP address and port. Intruders would first have to have access to the network then to the specific server, IP address, and port. Security is further enhanced as users are validated with a unique username and password combination. In addition before the user is logged in they must receive authorization from the license server. Failed login attempts are recorded. Administrators can set strong password rules in the Seapine License Server that are applied universally. LDAP can also be used to centrally manage users.
(e) Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.	TestTrack Pro and Surround SCM do not use tokens, cards, or other devices at this time.

About the Author

Allan McNaughton is a patent holding technologist and veteran writer with more than fifteen years of industry experience. He is the president of Technical Insight, LLC, a firm specializing in the composition of high-technology white papers. Mr. McNaughton is a frequent contributor to leading technology publications and can be reached at allan@technical-insight.com.

Seapine Software, Inc.

Headquarters
5412 Courseview Dr., Suite 200
Mason, OH 45040
Toll-free: (888) 683-6456

Seapine Software Europe
Canisiusgasse 6/39
1090 Vienna, Austria
Tel: +43 676 930 63 93

Seapine Software Asia Pacific
82/6 Moo5, T Nongplalai
A. Banglamung
Chon Buri, Thailand 20150
Tel: + 66 3 824 1784

Email: info@seapine.com
Web: www.seapine.com