Countess SAE Software for 21 CFR Part 11 support

The FDA issued the Electronic Records and Signatures Rule, known as 21 CFR Part 11, in August 1997 [1]. This rule defines the requirements for use of electronic documents in place of paper documents. The requirements apply to the system elements, controls, and procedures that are necessary to ensure the reliability of electronically stored records.

21 CFR Part 11 compliance encompasses both procedural and technical requirements. Procedural requirements apply to the standard operating procedures instituted by the end user. Technical requirements apply to the functional characteristics of the compliance management software used.

Invitrogen™ Countess™ SAE Software for 21 CFR Part 11 support includes three components that need to be to be installed, activated, and communicating with each other.

- **SAE software:** used to configure security, audit, and e-signature (SAE) settings for an Invitrogen™ Countess™ Automated Cell Counter; set up SAE application profiles (SAE administrator console is installed on a server with a static IP address)
- **SAE license:** used to activate SAE settings for the Countess Automated Cell Counter
- **SAE mode:** Countess Automated Cell Counter software is remotely connected to the SAE administrator console software

The combined functional characteristics of Countess SAE software do not by themselves guarantee 21 CFR Part 11 compliance. Compliance is a consequence of the work process and systems used by the end user.

The following details describe how the components of Countess SAE software work together to provide a technical basis for supporting 21 CFR Part 11 compliance throughout data acquisition and analysis within the workflow.

Section	Descriptor [1]	Summary	Features
11.10	**Controls for closed systems**		
11.10(a)	Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	System validation	Countess SAE Software for 21 CFR Part 11 compliance support (Countess SAE software) is validated for use with Invitrogen™ Countess™ 3 and Invitrogen™ Countess™ 3 FL Automated Cell Counters. When used with Countess 3 and Countess 3 FL cell counters, Countess SAE software creates an audit event for every dataset created. The audit events are stored on a server that is secure and blocked from external tampering. The integrity of the data files is secured through confirmation of an internal checksum. Any audit gaps can be detected and reported by comparing the checksum with audit records.
11.10(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.	Generation of records for inspection	Countess SAE software stores instrument settings, analysis parameters, results, and audit trails for analysis objects. Electronic signature histories are stored on a secure server to allow accurate and complete copies to be regenerated if necessary. Audit trail records for user actions can be viewed via the SAE administrator console and exported to a human-readable PDF file that can be printed.
11.10(c)	Protection of records to enable their accurate and ready retrieval throughout the records retention period.	Record protection	Countess SAE software manages the instrument settings, analysis parameters, and results in a server database. Record accuracy is ensured by calculating an internal checksum for all data files that are created and exported by the system. Experimental data files are stored on the server as audit objects. Countess SAE software has options for the user to set the archiving period.
11.10(d)	Limiting system access to authorized individuals.	System access limitation	Countess SAE software requires a user to log into the system using a username and password. The system administrator can define user roles to control access and workflows based on the assigned permissions.
11.10(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.	Audit trails	Countess SAE software generates audit records for operations performed by users. These include login, logout, slide imaging, image acquisition adjustment, cell count analysis, count adjustment, saving results settings, e-signatures, export/import of experimental protocols, and changes to the system settings. These records are maintained on the SAE administrator console. Audit records include the username; first and last name of the user; a date and time for the record; and the ID of the machine on which the record was generated. Audit records cannot be modified. All versions of data files are maintained together and can be viewed and compared.
11.10(f)	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	Operational checks	Countess SAE software restricts what users can do based on their roles and access privileges. A user must log into the software using a username and password, and access to features is based on their assigned role. Actions can be configured to require signatures to control workflows, ensuring data are reviewed prior to completing configured actions.

Section	Descriptor [1]	Summary	Features
11.10(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.	Authority checks	Countess SAE software ensures that only users with the proper authority can carry out particular functions based on their roles and access privileges. The software allows user role creation with differing levels of permissions.
11.10(h)	Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	Data and operation validity checks	Methods: Countess SAE software allows system validation, access control, and auditing of all actions resulting in deviation from the default or loaded protocol that would impact counting results. If specific protocols or instrument settings are required, local SOP control should be used. Data input: Countess instruments and software analyze only raw images to generate cell counts that cannot be altered. The user can alter the lighting, brightness, and focal plane for image capture but cannot alter the image once captured. Any change is access controlled, validated, and audited.
11.10(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.	Training and user accountability	Thermo Fisher Scientific will provide detailed user guides for setup and use of the instrument and SAE console. However, it is the client's responsibility to train employees and assign appropriate roles to users to control access to system features based on their training.
11.10(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.	User accountability	Countess SAE software requires the use of unique usernames. Once a result is generated, it cannot be changed. All events that generate results are audited. Modification of data is not allowed once e-signatures are initiated. Any change after the e-signatures are recorded creates a new version to which the signatures do not apply.
11.10(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, and (2) revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	System documentation control	Countess SAE software controls revision histories for system operation documents and follows the change control procedures when development and modification of system documents are required.
11.30	**Controls for open systems**		**Not applicable. Countess instruments in SAE mode and Countess Analysis Software in secure mode operate as a closed system.**
11.50	**Signature manifestations**		
11.50(a)	Signed electronic records shall contain information associated with the signing that clearly indicates all the following: (1) the printed name of the signer; (2) the date and time when the signature was executed; and (3) the meaning (such as review, approval, responsibility, or authorship) associated with the signature.	Signature manifestations	Countess SAE software generates an electronic signature for an image record that contains the full name of the user as defined in the SAE administrator console; the username; host ID; a date and time stamp; location; and signature meaning.

Section	Descriptor [1]	Summary	Features
11.50(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).	Signature manifestations	The electronic records generated by the SAE administrator console are time-, date-, and author-stamped. Any modifications to the user profile or password are audited. The user account ID cannot be changed or deleted. Accounts can only be inactivated.
11.70	**Signature/record linking**		
	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.	Signature/record linking	Electronic signatures are tied to the data record and the calculated checksum of the result file audit state at the time the signature is generated. Modifications to run results after electronic signing will invalidate any existing signatures and require the application of new signatures. Reports always contain signature information, version information, and page numbers in the header/footer of each page.
11.100	**Electronic signatures**		
11.100(a)	Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	General electronic signature requirements	Countess SAE software requires user authentication with a unique name and password when applying an electronic signature. All usernames are unique and cannot be reused, even if a user has been marked as inactive in the system.
11.100(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.	Verification of identity	The organization is responsible for verifying the identity of an individual. The organization is responsible for managing which users and which user roles are authorized to create and edit user accounts.
11.100(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.	General electronic signature requirements (certification)	The organization is responsible for the management and certification of electronic signatures.
11.200	**Electronic signature components and controls**		
11.200(a)	Electronic signatures shall employ 2 distinct IDs (ID and password) after first signing; subsequent signings only require a single ID during a continuous session.	Controls for electronic signatures	Countess SAE software and the console require both a unique username and password for all signature events.
11.200(b)	Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.	Controls for electronic signatures	Not applicable.

invitrogen

Section	Descriptor [1]	Summary	Features
11.300	**Controls for identification codes/passwords**		
11.300(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.	Uniqueness of ID code and password combination	All usernames must be unique and cannot be reused, even if a user has been marked as inactive in the system. The SAE administrator console prevents creation of duplicate usernames.
11.300(b)	Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).	Password aging	An administrator can set up password expiration policies and password criteria. The system can be configured to automatically suspend a user after a specified number of invalid login attempts.
11.300(c)	Following loss management procedures to electronically deauthorize 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.	Lost ID and password management	An administrator can reset passwords, configure account lockout policies, and manage user account status (active, inactive, or suspended). A user can reset their password. All changes are recorded in the audit history.
11.300(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.	Controls to prevent unauthorized credential use	Countess SAE software can be configured to automatically lock a user account after a specified number of login attempts and can also be configured to lock the screen after a period of inactivity to prevent unauthorized use. The SAE administrator console can be configured to notify the administrator of events, such as entry of an incorrect password, suspension of a user account, user session timeout, and role deletion.
11.300(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.	Periodic testing of ID and password information	An administrator can set up password expiration policies and password criteria. The organization is responsible for establishing periodic testing of ID and password information as required.

References

1. 21CFR11.10, Title 21 Part 11 (April 1, 2020) Electronic Records; Electronic Signatures.
2. Electronic Code of Federal Regulations (eCFR), ecfr.gov.

Find out more about our 21 CFR Part 11 compliance support package at **thermofisher.com/countesscfr**

ThermoFisher SCIENTIFIC