INFORS HT

**White Paper**

# 21 CFR Part 11 Compliance – Regulatory Conformity of eve®

*Franco Berz, Head of Quality Management INFORS HT*
*Dr. Britta Abellan, Computer System Validation Manager INFORS HT*

## 1. Introduction

More and more research and manufacturing processes in the life science industry use electronic devices, computerized systems and specific software. The United States Food and Drug Administration (FDA) has therefore defined regulations describing under which conditions computerized systems can be used in manufacturing and research processes. The **FDA 21 CFR Part 11** focuses on acceptance criteria of electronic records and electronic signatures as equivalent to paper records and handwritten signatures. It considers the risk of manipulation of electronic records and signatures, which could affect the manufactured product. The objective is to ensure that electronic records are always accurate, reliable, complete, and cannot be altered without trace. Where records must be authorized by a suitable person with a traceable signature, regulations on electronic signatures apply.

The regulations describe and require three types of control: administrative, technological, and procedural controls. In consequence, no instrument or software based system alone can be compliant. The technological controls are within the remit of the software system, whereas procedural and administrative controls are the concern of the customers. The responsibility for the implementation of all controls to achieve full compliance lies firmly with the customer.

The bioprocess software eve® is a record keeping system in terms of FDA 21 CFR Part 11. Moreover, several features are integrated to support the customer in achieving compliance in combination with a commercial solution for electronic signatures. Batch related eve® reports contain the required information and can be used for the creation of electronically signed electronic records.

The present document is divided into three subparts:

- Overview of the requirements of 21 CFR Part 11
- Functionalities implemented in eve® that are related to the requirements
- Detailed evaluation of the software eve®

The document refers to and is only valid for eve® installations including the User Management & Reporting functionalities (version 1.95 and higher). Infors AG offers professional support concerning system requirements and software configurations required to achieve compliance with 21 CFR Part 11.

## 2. Overview of the requirements

Replacing paper records and handwritten signatures by electronic records and signatures implies a higher risk of manipulation, misinterpretation, and non-traceable changes. Strict regulations addressing these challenges were defined by the FDA in 21 CFR Part 11 and apply to all GMP processes.

The following table presents the most important topics addressed.

| Requirement | Description |
|---|---|
| Validation | GMP-relevant computerized systems must be validated to ensure accuracy, reliability and consistent intended performance in data management. |
| Access Control | Access to electronic records must be limited to authorized and qualified users. Additional security procedures must be implemented for open systems. |
| Audit Trail | All user entries and actions that create, modify, or delete electronic records must be logged in a secure, computer-generated, time-stamped audit trail. |
| Training Measures | Persons who develop, maintain, or use electronic record/electronic signature systems must have the education, training, and experience to perform their assigned tasks. |
| Storage, Protection, Reproducibility and Availability | The system must allow the storage, protection, and availability of electronic records during the required retention period. Electronic records must be reproducible in both human readable and electronic form. |
| Electronic Signatures | The system must allow to control that electronic signatures are only used by their genuine owners, and that attempted use by anyone other than the genuine owner is immediately identified and recorded. Electronic signatures that are not based upon biometrics shall contain two distinct identification components (user ID, password).<br><br>All identification components must be entered for the first signing of a single, continuous period. Subsequent signings shall employ at least one signature component. Electronic signatures shall not be reused by, or reassigned to anyone else. The meaning must be associated with the electronic signature. Falsification of electronic signatures must be prevented by the system. Electronic signatures must be legally binding and equivalent of the signer´s handwritten signature. |
| System Documentation | Adequate controls must be in place over the distribution of, access to, and use of documentation for system operation and maintenance. |
| Certifcate for the FDA | Persons using electronic signatures must certify to the agency that the electronic signatures in the system are intended to be the legally binding equivalent of traditional handwritten signatures. |

# 3. eve® functionalities related to the requirements

## 3.1 Access control and security

Access to eve® is controlled by a combination of user ID and password which is unique for each user. The system does not allow the creation of an account with an existing user ID. Once an account has been created, it can only be deactivated, not completely deleted, thus preventing the reuse of user IDs.

Several security relevant features are configurable in eve® as shown in the graphic below.

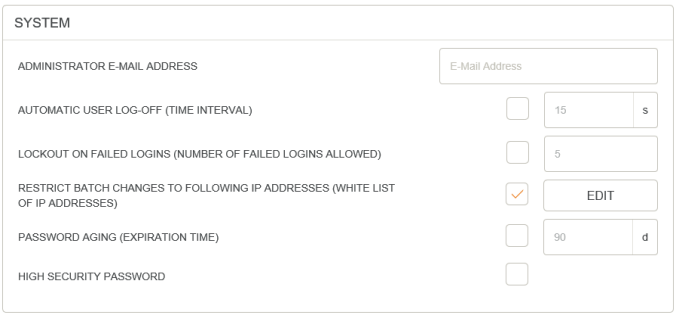


*Figure 1: Screenshot from eve® (v 1.95) showing the menu SETTINGS: GLOBAL: SYSTEM*

(1) Activation of automatic user log-off allows the automatic log-off of any user after a configurable period of inactivity. With this feature activated, every user is logged off from the software after a defined time of inactivity preventing a person other than the genuine owner from using a specific account.

(2) Activation of complete lockout from the software after a configurable number of failed logins (due to incorrect password) prevents unauthorized access.

(3) The restriction to specific IP addresses is used to control which who can execute changes within a batch.

(4) Password aging ensures that users are forced to change their passwords regularly after a configurable period (5 Password generations).

(5) High security password settings can be activated:

- at least 8 characters,
- at least one upper and one lower case character,
- at least one non-alpha numerical or numerical character.

## 3.2 User Management

Each user must be assigned one of the six roles with a distinct set of rights to use functionalities. The separation of operational and administrative/ security rights can be achieved with the different roles included (see table below).

| Role | Rights |
|---|---|
| System Administrator | • User administration<br>• Equipment management<br>• License management<br>• Configure software settings<br>• Backup and restore |
| Manager | • User administration<br>• Equipment management<br>• License management<br>• Configure software settings<br>• Plan and start atches<br>• Monitor and control batches<br>• Backup and restore |
| User | • Plan and start batches<br>• Monitor and control batches<br>• Extensive editing options |
| Technician | • Plan and start batches<br>• Monitor and control batches<br>• Restrictions concerning editing and deleting options |
| Operator | • Start batches<br>• Monitor and control batches |
| Guest | • Monitor batches<br>• Audit Trail access (e.g. for inspections) |

## 3.3 Audit Trail

The audit trail cannot be turned off and is always accessible within the software. The user interface does not allow any manipulations of the audit trail. All user management and batch related user actions are logged with date and time stamp. The time is synchronized with the windows server automatically and cannot be manipulated by the user within the software.

The audit trail comprises entries in the following categories:

- "EVENT TIME": the date and time of the logged action
- "USER": the user ID of the (logged) user responsible for this action
- "EVENT TYPE": what kind of action the user has executed (see details in table)
- "ACTION: detailed description of the action if required (old and new value),
- "PROJECT", EXPERIMENT", "BATCH": the project / experiment / batch associated to the action
- "DEVICE", "UNIT" : the device or unit concerned by the action
- "IP ADDRESS": the address of the device, the action was executed from

The categories "ACTION", "PROJECT", "EXPERIMENT","BATCH", "UNIT" and "DEVICE" can be empty according to the related user action. The audit trail report (after export) includes a table with the usernames, roles and statuses of all registered users current as of the date of the report.

## 3.4 Archive / Backup

For secure storage and for restoring, a backup function is implemented in eve®. Backups can be created at any time if no batch is running.

The system can be restored with previously created backup files at any time. This action will overwrite all data in the database at the moment of restoring.

Different warnings are appearing within the software during the backup process, but the customer has to install procedures to prevent loss of data, and electronic records associated with the restore process.

| EVENT TIME | USER | EVENT TYPE | ACTION | PROJECT | EXPERIMENT | BATCH | DEVICE | UNIT | IP ADDRESS |
|---|---|---|---|---|---|---|---|---|---|
| 07 Dec 2018 12:48:03 | service | LogOn | | | | | | | 127.0.0.1 |
| 06 Dec 2018 11:37:23 | System: Labfors / C | CommunicationLost | | | Test Culture Media | Test Culture Media | Labfors | C | 127.0.0.1 |
| 06 Dec 2018 11:37:23 | System: Labfors / D | CommunicationLost | | MyTestProject | Testbatch Technician | Testbatch Technician | Labfors | D | 127.0.0.1 |
| 06 Dec 2018 11:35:11 | EveSystem | OfflineParameterCreated | OD600 has been created | | | | | | 127.0.0.1 |
| 06 Dec 2018 11:35:11 | abellb | UserActivated | TestUser2 has been activated with role User | | | | | | 127.0.0.1 |
| 06 Dec 2018 10:45:58 | abellb | SettingsChanged | Whitelist for device control has been activated | | | | | | 127.0.0.1 |
| 06 Dec 2018 10:45:27 | abellb | SettingsChanged | Automatic user log off has been deactivated | | | | | | 127.0.0.1 |
| 06 Dec 2018 10:45:24 | abellb | SettingsChanged | Automatic user log off has been activated | | | | | | 127.0.0.1 |
| 06 Dec 2018 10:31:59 | abellb | LogOn | | | | | | | 127.0.0.1 |

*Figure 2: Screenshot from eve® (v 1.98) showing the audit trail.*

Filter: From date: 09 Oct 2018 00:00:00 To date: 10 Oct 2018 23:59:59 Created at: 10 Oct 2018 16:19:42

User Management Current as of 10 Oct 2018 16:19:42

| Username | Role | Is Active |
|---|---|---|
| TestUser1 | User | Yes |
| Operator | Operator | Yes |
| belaUser | User | Yes |
| Achema | Manager | No |
| User | User | No |
| Britta | User | Yes |
| Guest | Guest | Yes |
| Technician | Technician | Yes |
| Administrator | Administrator | Yes |
| abellb | Administrator | Yes |

*Figure 3: Screenshot of the "User Management" table from an audit trail report created with eve® (v 1.95)*

## 4. Detailed evaluation of the requirements for eve®

In the "Declaration of Regulatory Conformity" available as a part of software validation, the responses of eve® to the requirements of 21 CFR Part 11 are evaluated point by point. The evaluation is presented in the form of a questionnaire directly related to the original text of the Act (as published online by the FDA on Dec 20, 2016, www.ecfr.gov). The questions represent a generally accepted interpretation of the Act and help to describe relevant issues in a comprehensible, detailed form. The answers are divided into two parts.

The first part provides comments related to relevant features of the eve® software. The technical compatibility of eve® with the requirements is stated. Additionally, recommendations for the customer concerning procedural and administrative controls to achieve compliance are provided in the second part of the answer. An example can be found below for 21 CFR Part 11, Subpart B – Electronic records, 11.10 (E) – Audit trail:

**§ 11.10 Controls for closed systems (E)**

*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:*

| | |
|---|---|
| FDA requirement | 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. |
| Question 1 | Is there a secure, computer generated, time stamped audit trail that records the date and time of operator entries and actions that create, modify or delete electronic records? |
| Comments | Yes. A secure audit trail exists, in which all operator actions and entries (e.g. bioprocess data configurations) are automatically recorded with user ID, IP address, date and local time stamp. |
| Question 2 | Upon making a change to an electronic record, is previously recorded information still available (i.e. not obscured by the change)? |
| Comments | Yes. All user actions changing bioprocess parameters are recorded in the audit trail with the type of action, old and new value, user ID, IP address, date and local time stamp.<br>Changes to the system configuration are recorded in the same way. |
| Question 3 | Is an electronic record's audit trail retrievable throughout the record's retention period? |
| Comments | Yes. Audit trail data is stored within eve® and can be exported for storage. The data can be accessed at any time. |
| Question 4 | Is the audit trail available for review and copying by the FDA? |
| Comments | Yes. Audit trail data is accessible at any time with a read-only guest login, and available in versions suitable for electronic transfer and printing on paper like PDF.<br>Filter options exist for convenient review of specific topics of interest. |

*Figure 4: Extract of the "Declaration of Regulatory Conformity"*

## 5 Summary

The bioprocess platform software eve® is a record keeping system in terms of FDA 21 CFR Part 11.

eve® is technically compatible with the requirements of Subpart B – Electronic records. Validation documentation and services are offered by Infors AG to support the customer in regulation compliance.

Electronic signatures are not supported by eve® at the moment. However, achieving compliance with the regulations is supported by several features of the software. In combination with a commercial solution for electronic signatures, compliance can easily be achieved.

This White Paper refers to eve® versions 1.95 and 1.98



Infors AG
Rittergasse 27
CH-4103 Bottmingen
www.infors-ht.com
info@infors-ht.com