SIEMENS

SIMATIC IT

SIMATIC IT R&D Suite V7.5

Electronic Records / Electronic Signatures (ERES)

Compliance Response

Edition 08/2019

Answers for industry.

SIEMENS

SIMATIC IT

R&D SUITE V7.5
ERES Compliance Response

Product Information

Electronic Records /
Electronic Signatures (ERES)

08/2019
A5E47751024-AA

Legal information

Warning notice system

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.

⚠ DANGER
indicates that death or severe personal injury **will** result if proper precautions are not taken.

⚠ WARNING
indicates that death or severe personal injury **may** result if proper precautions are not taken.

⚠ CAUTION
indicates that minor personal injury can result if proper precautions are not taken.

NOTICE
indicates that property damage can result if proper precautions are not taken.

If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

Qualified Personnel

The product/system described in this documentation may be operated only by **personnel qualified** for the specific task in accordance with the relevant documentation, in particular its warning notices and safety instructions. Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products/systems.

Proper use of Siemens products

Note the following:

⚠ WARNING
Siemens products may only be used for the applications described in the catalog and in the relevant technical documentation. If products and components from other manufacturers are used, these must be recommended or approved by Siemens. Proper transport, storage, installation, assembly, commissioning, operation and maintenance are required to ensure that the products operate safely and without any problems. The permissible ambient conditions must be complied with. The information in the relevant documentation must be observed.

Trademarks

All names identified by ® are registered trademarks of Siemens AG. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Disclaimer of Liability

We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.

Siemens AG
Digital Industries
Postfach 48 48
90026 NÜRNBERG
GERMANY

A5E47751024-AA
℗ 08/2019 Subject to change

Table of contents

Introduction 1

Life science industry is basing key decisions on regulated records that are increasingly generated, processed and kept electronically. Reviews and approval of such data are also being provided electronically. Thus the appropriate management of electronic records and electronic signatures has become an important topic for the life science industry.

Accordingly, regulatory bodies defined criteria under which electronic records and electronic signatures will be considered as reliable and trustworthy as paper records and handwritten signatures executed on paper. These requirements have been set forth by the US FDA in 21 CFR Part 11 (21 CFR Part 11 Electronic Records; Electronic Signatures, US FDA, 1997; in short: *Part 11*) and by the European Commission in Annex 11 of the EU GMP Guideline (EU Guidelines to Good Manufacturing Practice, Volume 4, Annex 11: Computerised Systems, European Commission, 2011; in short: *Annex 11*).
Since requirements on electronic records and electronic signatures are always tied to a computerized system being in a validated state, both regulations also include stipulations on validation and lifecycle of the computerized system.

Application of *Part 11* and *Annex 11* (or their corresponding implementation in national legislation) is mandatory for the use of electronic records and electronic signatures. However, these regulations are only valid within their defined scope.
The scope of both regulations is defined by the regional market to which the finished pharmaceutical product is distributed and by whether or not the computerized systems and electronic records are used as part of GMP-regulated activities (see Part 11.1 and Annex 11 Principle).

Supplemental to the regulations, a number of guidance documents, good practice guides and interpretations have been published in recent years to support the implementation of the regulations. Some of them are referred to within this document.

To help its clients, Siemens as supplier of SIMATIC IT R&D Suite has evaluated version 7.5 of the system with regard to these requirements and published its results in this Compliance Response.

SIMATIC IT R&D Suite V7.5 fully meets the functional requirements for the use of electronic records and electronic signatures.

Operation in conformity with the regulations is ensured in conjunction with organizational measures and procedural controls to be established by the client (the regulated user). Such measures and controls are mentioned in chapter "Evaluation List for SIMATIC IT R&D Suite (Page 17)" of this document.

This document is divided into three parts:

1. Chapter "The Requirements in Short (Page 7)" provides a brief description of the requirement clusters,
2. Chapter "Meeting the Requirements with SIMATIC IT R&D Suite (Page 9)" introduces the functionality of SIMATIC IT R&D Suite as means to meet those requirements.
3. Chapter "Evaluation List for SIMATIC IT R&D Suite (Page 17)" contains a detailed system assessment on the basis of the individual requirements of the relevant regulations.

The Requirements in Short

2

Annex 11 and Part 11 take into account that the risk of manipulation, misinterpretation and changes without leaving a visible trace is higher with electronic records and electronic signatures than with conventional paper records and handwritten signatures. Furthermore the means to restrict access to electronic records to authorized individuals are very different to those required to restrict access to paper records. Additional measures are required for such reasons.

The terms "electronic record" / "electronic document" mean 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.

The term "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. Since electronic signatures are also considered as being electronic records by themselves, all requirements for electronic records are applied to electronic signatures too.

The following table provides an overview of the requirements from both regulations.

Requirement	Description
Lifecycle and Validation of Computerized Systems	Computerized systems used as a part of GMP-related activities must be validated. The validation process should be defined using a risk-based approach. It should cover all relevant steps of the lifecycle and must provide appropriate documented evidence. The system's functionality should be traceable throughout the lifecycle by being documented in specifications or a system description. A formal change control procedure as well as an incident management should be established. Periodic evaluation should confirm that the validated state of the system is being maintained.
Suppliers and Service Providers	Since competency and reliability of suppliers and service providers are considered key factors, the supplier assessment should be decided on a risk-based approach. Formal agreements should exist between the regulated user and these third parties, including clear responsibilities of the third party.
Data Integrity	Under the requirements of both regulations, electronic records and electronic signatures must be as reliable and trustworthy as paper records. The system must provide the ability to discern altered records. Built-in checks for the correct and secure handling of data should be provided for manually entered data as well as for data being electronically exchanged with other systems. The system's ability to generate accurate and complete copies is essential for the use of the electronic records for regulated purposes, as well as the accessibility, readability, and integrity of archived data throughout the retention period.

Requirement	Description
Audit Trail, Change Control Support	Besides recording changes to the system as defined in the lifecycle, both regulations require that changes on GMP-relevant data are being recorded. Such an audit trail should include information on the change (before / after data), the identity of the operator, a time stamp, as well as the reason for the change.
System Access, Identification Codes and Passwords	Access to the system must be limited to authorized individuals. Attention should be paid to password security. Changes on the configuration of user access management should be recorded. Periodic reviews should ensure the validity of identification codes. Procedures should exist for recalling access rights if a person leaves and for loss management. Special consideration should be given to the use of devices that bear or generate identification code or password information.
Electronic Signature	Regulations consider electronic signatures being legally binding and generally equivalent to handwritten signatures executed on paper. Beyond requirements on identification codes and passwords as stated above, electronic signatures must be unique to an individual. They must be linked to their respective electronic record and not be copied or otherwise being altered.
Open Systems	Open systems might require additional controls or measures to ensure data integrity and confidentiality.

Meeting the Requirements with SIMATIC IT R&D Suite 3

The Siemens recommendations for the system architecture, conception, and configuration will assist system users in achieving compliance. For additional information and assistance see "SIMATIC IT R&D Suite Manual" from Siemens.

The requirements explained in chapter "The Requirements in Short (Page 7)" can be supported by the system as follows.

3.1 Lifecycle and Validation of Computerized Systems

In Annex 11 from 1992 and in Part 11 from 1997, the law already required that computerized systems need to be validated. Criteria for the validation of the system and its lifecycle were added in the edited revision of Annex 11 from 2011.

Nonetheless the requirements to validate a computerized system and to keep it in a validated state had long been a part of regulations other than *Part 11* and *Annex 11*. This was the motivation for the ISPE (International Society of Pharmaceutical Engineers, http://www.ispe.org) to publish practical guidance like the Baseline Guides (Baseline® Pharmaceutical Engineering Guides for New and Renovated Facilities, Volume 1-7, ISPE), the GAMP 5 guide (GAMP 5 – A Risk-Based Approach to Compliant GxP Computerized Systems, ISPE, 2008) as well as the GAMP Good Practice Guides.

Thus the system lifecycle as well as the approach to validation should be defined considering the guidance from the GAMP 5 guide. The guide also includes a number of appendices for lifecycle management, system development and operation of computerized systems.
Since most pharmaceutical companies already have a validation methodology for computerized systems as a part of their process landscape, it is preferable to set up the systems lifecycle and validation according to these.

3.2 Suppliers and Service Providers

Suppliers of systems, solutions and services must be evaluated accordingly, see GAMP 5 Appendix M2. Siemens as a manufacturer of hardware and software components follows internal procedures of Product Lifecycle Management and works according to a Quality Management System, which is regularly reviewed and certified by an external certification company.

3.3 Data Integrity

Data integrity is assured in the system by measures like access protection, audit trail, data type checks, checksums, backup/restore, and archiving/retrieval, completed by system validation, appropriate procedures and training for personnel.

Data storage

All data is stored in a secure database, it is also possible to link external data like pdf files containing material certificates to a data set. All linked documents will be individually identified and a checksum will be generated in order to detect any alteration to these documents. If an alteration is detected, SIMATIC IT R&D Suite will display an error message and prevent to open this affected document.

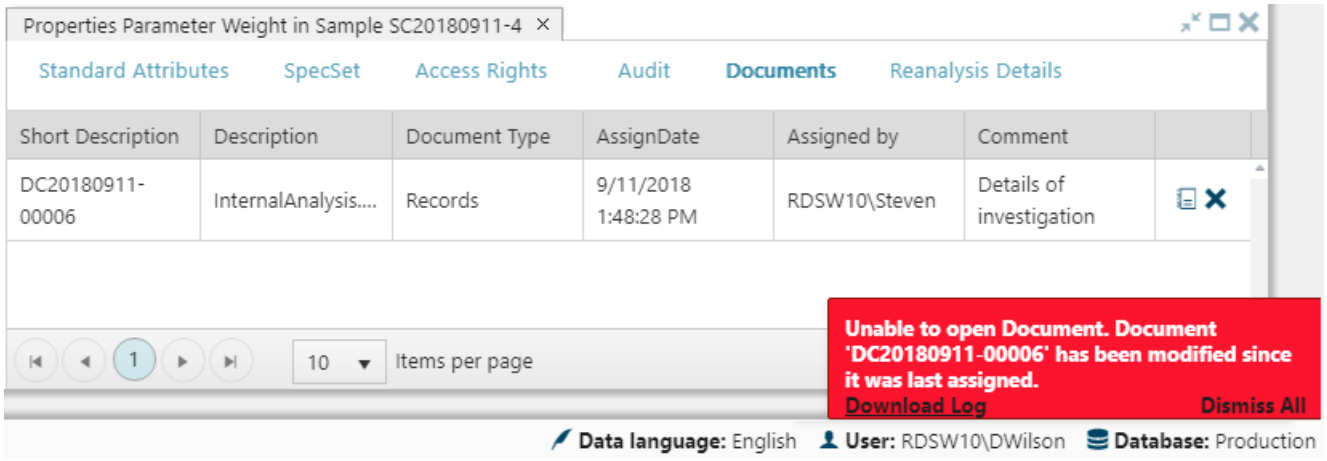

Figure 3-1 SIMATIC IT R&D Suite - Unilab prevents opening of documents which were altered after assignment. An error message informs the user.

Changes to GMP relevant data

All changes to GMP relevant data is required to be tracked and needs to be reasoned. In the configuration of SIMATIC IT R&D Suite it needs to be determined which fields are GMP relevant and which are not GMP relevant based on the requirements by the Regulated Company. In the operation of SIMATIC IT R&D Suite a comment is mandatory for the changes of GMP relevant fields. Subsequently, the change and the reasoning will be shown in the audit trail.

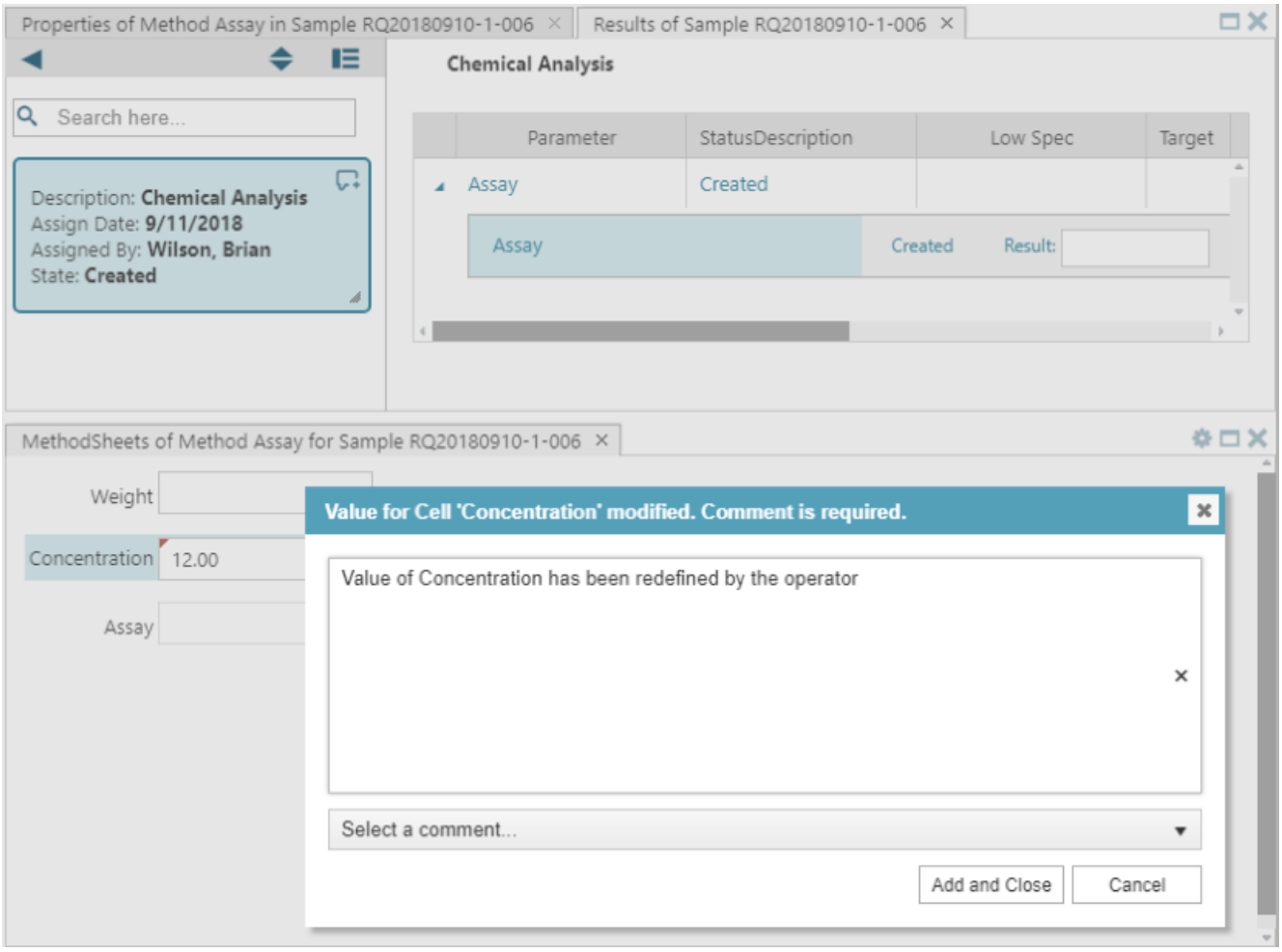

Figure 3-2 The GMP relevant field "Concentration" is edited. A confirmation including a comment is required.

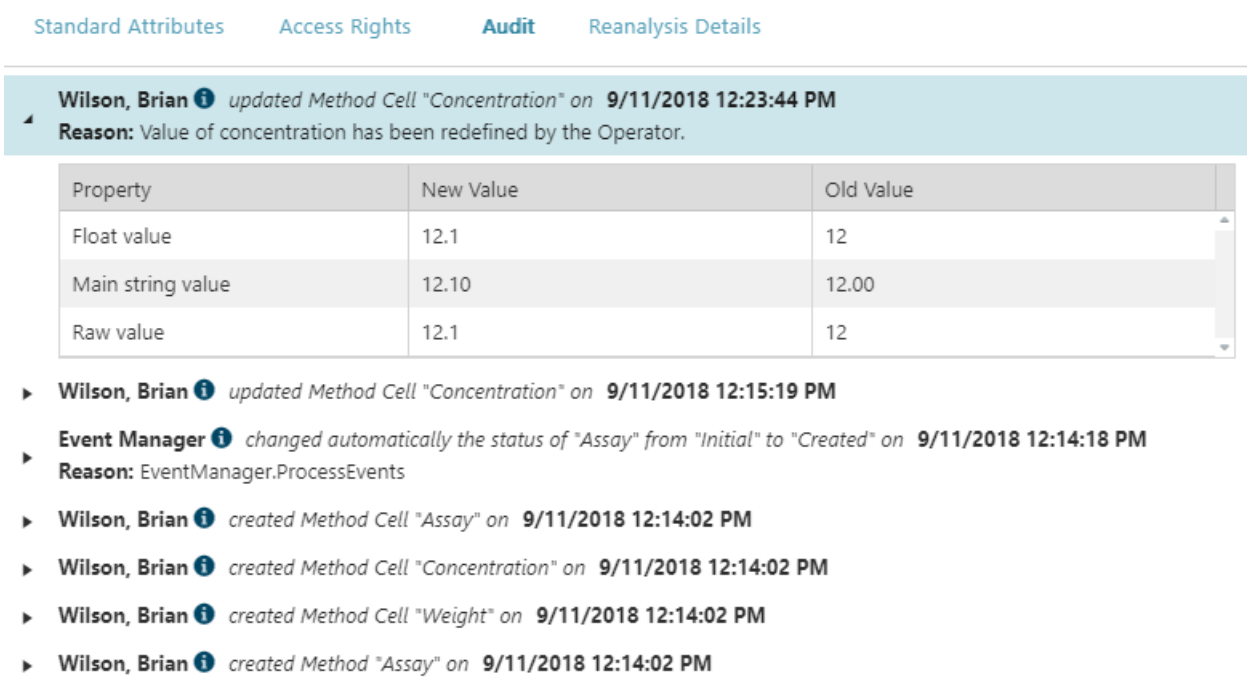

Figure 3-3 The audit trail contains the change including the reason.

3.4 Audit Trail, Change Control Support

"Audit trails are of particular importance in areas where operator actions generate, modify, or delete data in the course of normal operation." (Guidance for Industry Part 11 – Scope and Application, FDA, 2003)

An audit trail is not required for automatically generated electronic records which can neither be modified nor deleted by the operator. SIMATIC IT R&D Suite provides adequate system security mechanisms for such electronic records (e.g. access protection).

The following section describes how the SIMATIC IT R&D Suite system supports the implementation of requirements with regard to the audit trails during runtime operation. Moreover, it also informs about the system support for tracing changes made of the Configuration Objects.

Audit trail

SIMATIC IT R&D Suite supports the requirement for audit trail of GMP relevant operations by recording such actions appropriately (who, what, when, and optionally why). And it provides adequate system security for such electronic records (e.g. access control). The GMP relevant data is defined by the regulated company based on the applicable regulatory requirements.

Operator actions

All changes and inputs of relevant data entered by the operator during operation must be recorded in an audit trail.

Therefore Operator actions performed in SIMATIC IT R&D Suite can be recorded in an audit trail containing information like old value, new value, user ID, date and time stamp, operation, etc.

Recording Laboratory data

Laboratory data (e.g. material values or test results) are stored in the system without any option for the operator to change this data. No audit trail is required for these data since the data cannot be altered once the data is entered.

The audit trail is stored in the database. The audit trail can be printed, exported, and archived. Data access right prevents the user from changing the audit.

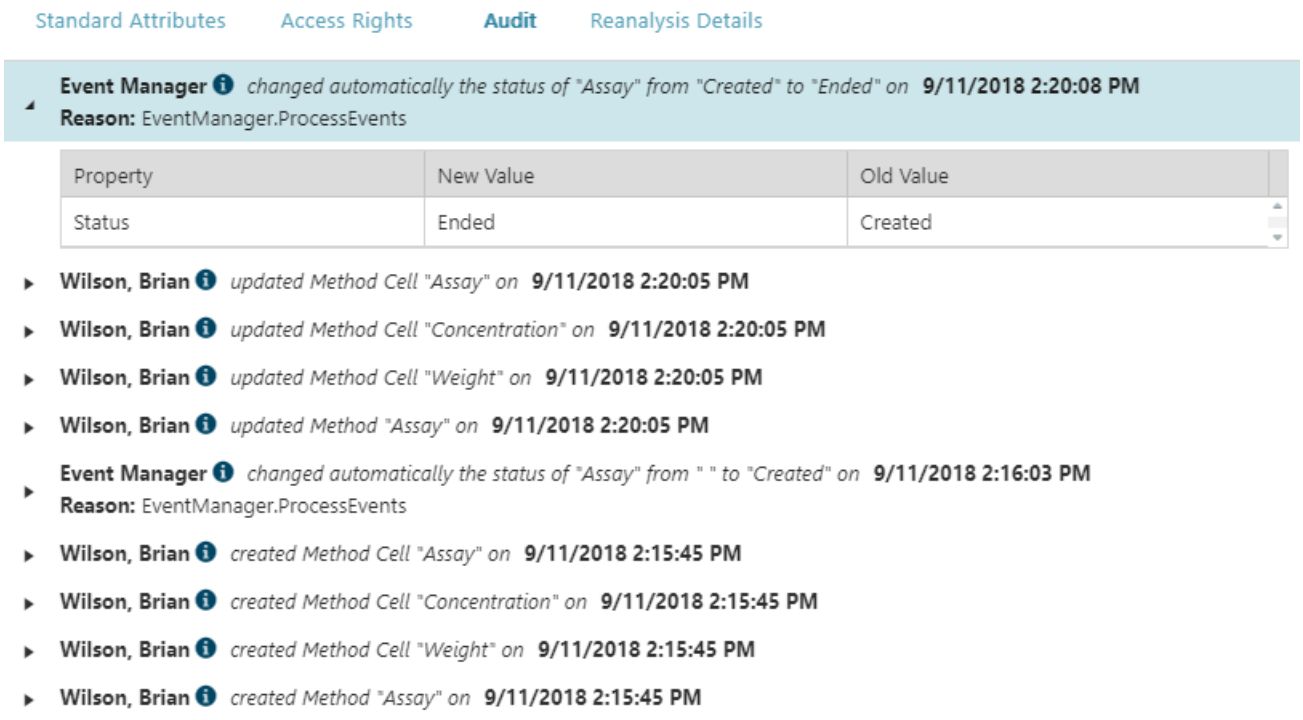

Figure 3-4 Example of the audit trail

Versioning of Configuration Objects

All configurable objects are stored as so called Glossary data. Any change to the Glossary data succumb a versioning of the individual configuration objects. This functionality supports the change control procedure in place of the regulated industry.

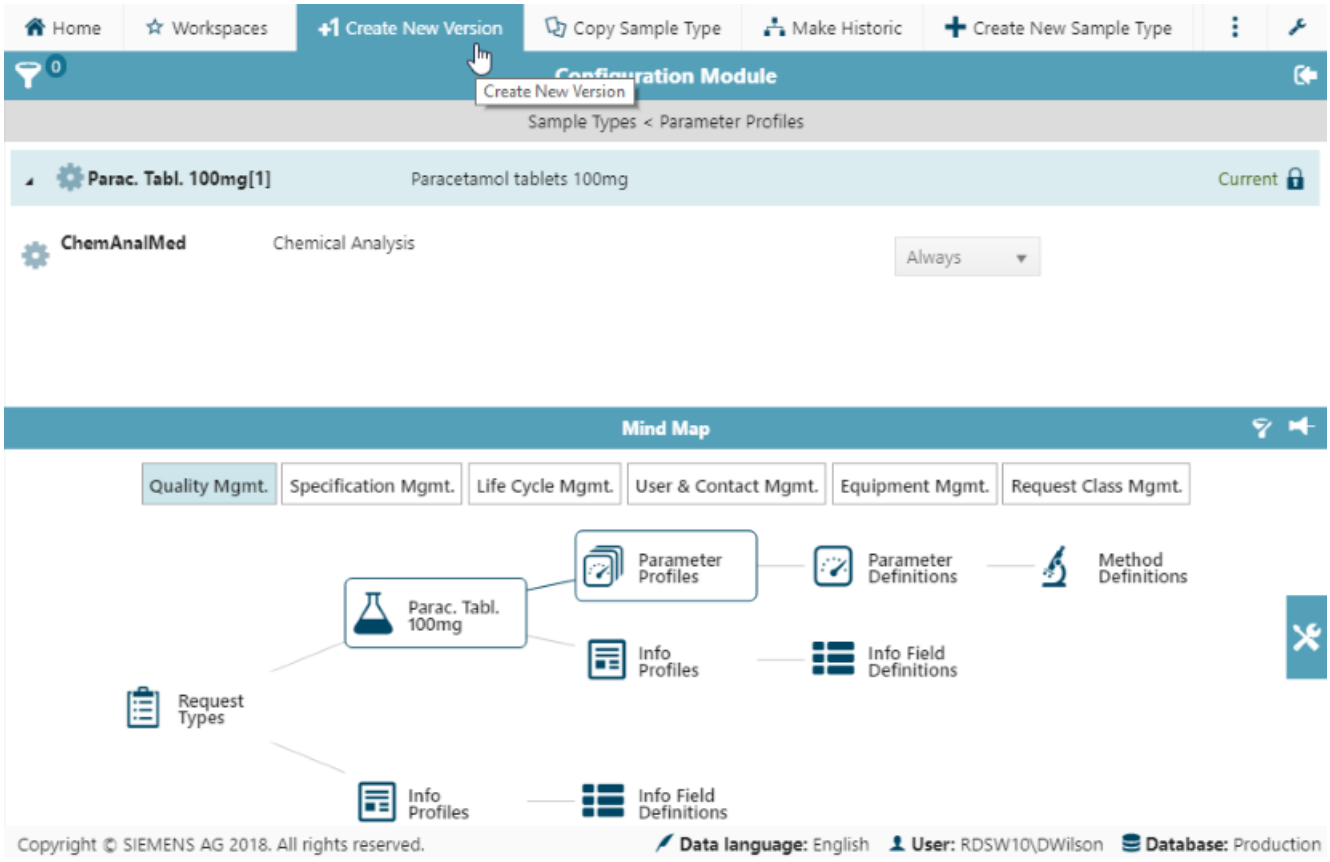

Figure 3-5 Creation of a new version of a configurable object

3.5 System Access, Identification Codes and Passwords

Users must be assigned the required access rights only, in order to prevent unauthorized access to and unintended manipulation of the file system, directory structures, and system data.

The requirements regarding access security are fully met in combination with procedural controls, such as those for "specifying the responsibility and access authorization of the system users".

Additional security mechanisms need to be set up for any "open paths" which might exist. For more information on the basic policies of the security concept and configuration recommendations, refer to the SIMATIC IT R&D Suite Security Guide.

A SIMATIC IT R&D Suite user connects via a browser using the network connection to the SIMATIC IT R&D Suite WebServer. The authentication of the user is passed though from Microsoft Windows to the application (Single Sign on). Therefore the user management relies

on the Microsoft Windows user administration. SIMATIC IT R&D Suite is then used to set up the user profiles.

The SIMATIC IT R&D Suite user profile application is used to set up user management by assigning functional acces rights (FAR) to different user profiles and assigning users to the different user profiles. The basic functionalities of this application are listed below:

- Management of the system functionalities
- Management of user profiles
- Management of user accounts

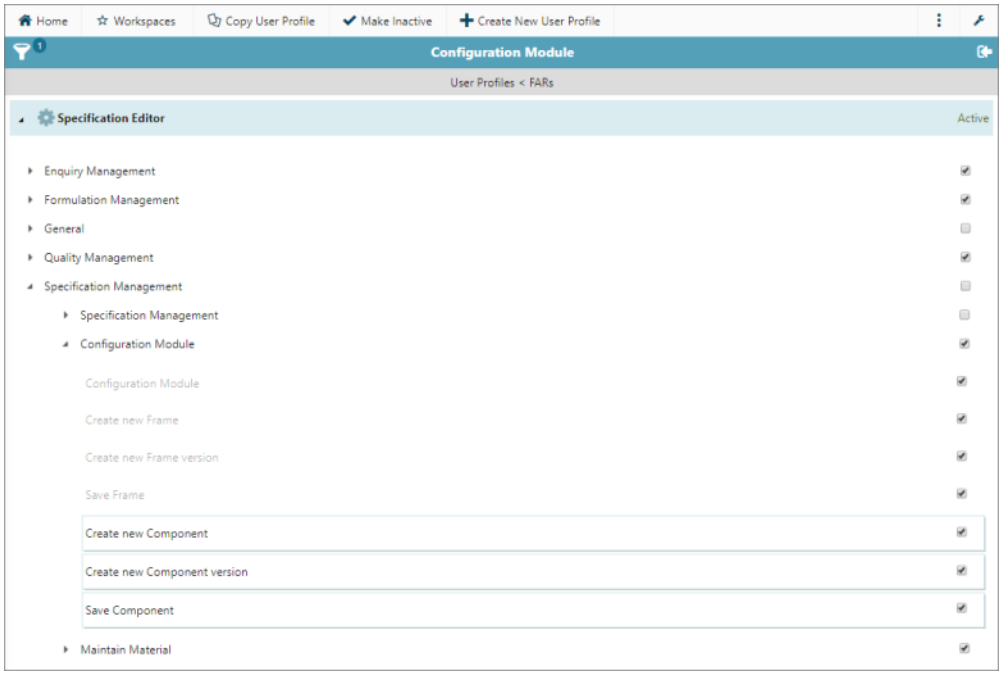

Figure 3-6 Assigning functional access rights to the user profile "Specification Management"

Thereby the following requirements for access protection are fulfilled using the Microsoft User management:

- Central user management (setup, deactivation, blocking, unblocking, assignment to user groups) by the administrator
- Use of a unique user identification (user ID) in combination with a password
- Definition of access rights for user groups
- Password settings and password aging: The user is forced to change his/her password on expiration of a configurable time; the password can be reused only after "n" generations.
- Prompt the user to define a new password at initial logon (initial password).
- A user which is not active on Windows is unable to connect to the application.
- Automatic logoff (auto-logout) after a configurable idle time of the keyboard and mouse.
- Log functions for actions related to access protection, such as logon, manual and automatic logoff, input of incorrect user ID or password, user blocked after several attempts to enter an incorrect password, and password change by user. This functionality is covered by Windows authentication.

3.6 Electronic Signature

SIMATIC IT R&D Suite provides functions for configuring an electronic signature. The actions which require an electronic signature upon modifications are specified during the configuration phase.

The electronic signature is being executed in a seperate dialog in which the user has to sign electronically by confirming the intended action with entering his password. Subsequently the electronic signature is saved in the audit trail along with the user name, time stamp, and the action performed.

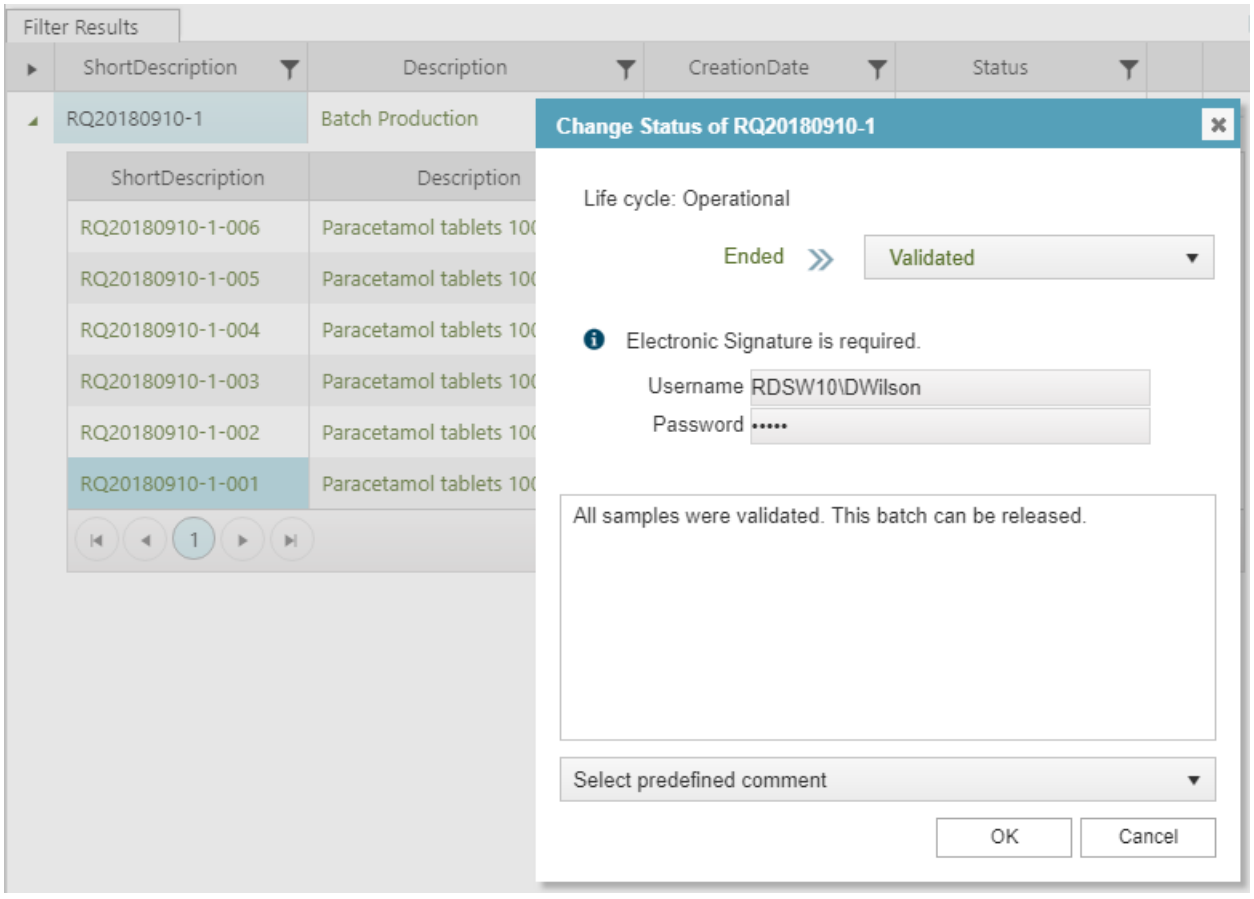

Figure 3-7 Electronic Signature for the modification of the status of *"Medicine"* from *"Ended"* to *"Validated"* including a mandatory comment.

SIMATIC IT R&D Suite also supports the Security Assertion Markup Language (SAML) 2.0 protocol. This functionalty is being enabled by the Siemens User Management Component (UMC) and it allows different users to single sign-on during one operator session.

Evaluation List for SIMATIC IT R&D Suite 4

The following list of requirements includes all regulatory requirements from 21 CFR Part 11 as well as from Annex 11 of the EU-GMP Guidelines. All requirements are structured in the same topics as those introduced in the chapter "The Requirements in Short (Page 7)" of this Compliance Response.

The *requirements* listed fully consider both regulations, regardless of whether technological or procedural controls or a combination of both are needed to fully comply with Part 11 and Annex 11.

The *answers* include, among other things, information about how the requirement is handled during the development of the product and which measures should be implemented during configuration and operation of the system. Furthermore, the answers include references to the product documentation for technical topics and to the GAMP 5 guide for procedural controls that are already considered in the guide.

4.1 Lifecycle and Validation of Computerized Systems

The fundamental requirement that a computerized system, used as a part of GMP related activities, must be validated is extended in the revision of Annex 11 from 2011 by requirements detailing expectations on a system's lifecycle.

	Requirement	Reference	Answer
4.1.1	Risk management should be applied throughout the lifecycle of the computerized system.	Annex 11, 1	The R&D process for Siemens software products incorporates risk management accordingly. During the validation of a customer-specific application, risk management should be ensured by the regulated user.
4.1.2	Validation of a system ensures its accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	21 CFR 11.10 (a)	Yes. The development of the software product (COTS, see Annex 11, glossary) is subject to the control of the Siemens QMS and the Product Lifecycle Management process. The regulated user should take appropriate measures to validate the application (see Annex 11, glossary), as well as maintaining its validated state.
4.1.3	Validation documentation covers relevant steps of the lifecycle.	Annex 11, 4.1	Yes. The R&D process for the software product covers all relevant documents. The responsibility for the validation of the application (see Annex 11, glossary) is with the regulated user.

	Requirement	Reference	Answer
4.1.4	A process for the validation of bespoke or customized systems should be in place.	Annex 11, 4.6	The validation process for customer-specific applications is the responsibility of the regulated user. Nonetheless, Siemens is able to offer support regarding validation activities.
4.1.5	Change management and deviation management are applied during the validation process.	Annex 11, 4.2	Yes. The R&D process for the software product includes change management, deviation management and fault corrections. The regulated user should ensure appropriate change management and deviation management (see GAMP 5, appendices M8 and D5).
4.1.6	An up-to-date inventory of all relevant systems and their GMP functionality is available. For critical systems an up-to-date system description […] should be available.	Annex 11, 4.3	The regulated user should establish appropriate reporting, a system inventory as well as system descriptions (see GAMP 5, appendix D6).
4.1.7	User requirements should describe required functions, be risk-based and be traceable throughout the lifecycle.	Annex 11, 4.4	Specification of requirements is part of the development process during product development. For the project-specific configuration, the regulated user should take into account the user requirements appropriately in the system's lifecycle (see GAMP 5, appendix D1).
4.1.8	Evidence of appropriate test methods and test scenarios should be demonstrated.	Annex 11, 4.7	Ensuring the suitability of test methods and scenarios is an integral part of the SIMATIC IT product's R&D process and test planning. The regulated user should be involved to agree upon testing practice (see GAMP 5, appendix D5) for the application.
4.1.9	Appropriate controls should be used over system documentation. Such controls include the distribution of, access to, and use of system operation and maintenance documentation.	21 CFR 11.10 (k)	During the development of the product the product's documentation is treated as being part of the product. Thus the documentation itself is under the control of the development process. The regulated user should establish appropriate procedural controls during development and operation of the production system (see GAMP 5, appendices M9 and D6).
4.1.10	A formal change control procedure for system documentation maintains a time sequenced record of changes.	21 CFR 11.10 (k) Annex 11.10	During the development of the product changes are handled according to the development process. The regulated user should establish appropriate procedural controls during development and operation of the system (see GAMP 5, appendices M8 and O6)
4.1.11	Persons who develop, maintain, or use electronic record/electronic signature systems should have the education, training and experience to perform their assigned task.	21 CFR 11.10 (i)	Siemens' processes do ensure that employees have appropriate training for their tasks and that such training is properly documented. Furthermore, Siemens offers a variety of training courses for users, administrators and support staff.
4.1.12	Computerized systems should be periodically evaluated to confirm that they remain in a valid state and are compliant with GMP.	Annex 11, 11	The regulated user should establish appropriate procedural controls (see GAMP 5, appendices O3 and O8).

	Requirement	Reference	Answer
4.1.13	All incidents should be reported and assessed.	Annex 11, 13	SIMATIC IT R&D Suite logs all incidents in logfiles on the webserver. The logfiles can be retrieved by users with adminstrotor rights. The regulated user should establish appropriate procedural controls (see GAMP 5, appendix O5).
4.1.14	For the availability of computerized systems supporting critical processes, provisions should be made to ensure continuity of support for those processes in the event of a system breakdown.	Annex 11, 16	The regulated user should appropriately consider the system in its business continuity planning (see GAMP 5, appendix O10).

4.2 Suppliers and Service Providers

If the regulated user is partnering with third parties for planning, development, validation, operation and maintenance of a computerized system, then the competence and reliability of this partner should be considered utilizing a risk-based approach.

	Requirement	Reference	Answer
4.2.1	When third parties are used, formal agreements must exist between the manufacturer and any third parties.	Annex 11, 3.1	The regulated user is responsible to establish formal agreements with suppliers and third parties.
4.2.2	The competency and reliability of a supplier are key factors when selecting a product or service provider. The need for an audit should be based on a risk assessment.	Annex 11, 3.2 Annex 11, 4.5	The regulated user should assess its suppliers accordingly (see GAMP 5, appendix M2).
4.2.3	The regulated user should ensure that the system has been developed in accordance with an appropriate Quality Management System.	Annex 11, 4.5	The development of SIMATIC IT products follows the R&D process stipulated in the Siemens Quality Management System.
4.2.4	Documentation supplied with commercial off-the-shelf products should be reviewed by regulated users to check that user requirements are fulfilled.	Annex 11, 3.3	The regulated user is responsible for the performance of such reviews.
4.2.5	Quality system and audit information relating to suppliers or developers of software and implemented systems should be made available to inspectors on request.	Annex 11, 3.4	The content and extent of the documentation affected by this requirement should be agreed upon by the regulated user and Siemens. The joint non-disclosure agreement should reflect this requirement accordingly.

4.3 Data Integrity

The main goal of both regulations is to define criteria under which electronic records and electronic signatures are as reliable and trustworthy as paper records. This requires a high degree of data integrity throughout the whole data retention period, including archiving and retrieval of relevant data.

	Requirement	Reference	Answer
4.3.1	The system should provide the ability to discern invalid or altered records.	21 CFR 11.10 (a)	Yes. An entry can be generated in the audit trail for any operator action (if, for example, the operator changes values or attach additional information). All relevant changes are recorded including time stamp, user ID, old value and new value and comment. Unauthorized changes are prevented by the system through access control. Attached external documents, which might be added to records, are individually identified. Any alteration will be detected by the system.
4.3.2	For records supporting batch release, it should be possible to generate printouts indicating if any of the data has been changed since the original entry.	Annex 11, 8.2	Operational modification of data is recorded in the general audit trail and can be printed out in a report with internal or external functionality.
4.3.3	The system should provide the ability to generate accurate and complete copies of electronic records in both human readable and electronic form.	21 CFR 11.10 (b) Annex 11, 8.1	Yes. Accurate and complete copies can be generated in electronic portable document formats or on paper.
4.3.4	Computerized systems exchanging data electronically with other systems should include appropriate built-in checks for the correct and secure entry and processing of data.	Annex 11, 5	Yes. Depending on the type of data, such built-in checks include value ranges, data type check, access authorizations, checksums, etc. and finally the validation process including interface testing.
4.3.5	For critical data entered manually, there should be an additional check on the accuracy of the data.	Annex 11, 6	The system has built-in plausibility checks for data entry. In addition, a multiple signature or operator dialog can be implemented as an additional check.
4.3.6	Data should be secured by both physical and electronic means against damage.	Annex 11, 7.1	In addition to the system's access security mechanisms, the regulated user should establish appropriate security means like physical access control, backup strategy, limited user access authorizations, regular checks on data readability, etc. Furthermore, the data retention period should be determined by the regulated user and appropriately considered in the user's processes (see GAMP 5, appendices O3, O4, O8, O9, O11 and O13). The SIMATIC IT R&D Suite security concept provides additional information which should be considered.
4.3.7	Regular backups of all relevant data should be done.	Annex 11, 7.2	The regulated user should establish appropriate processes for backup and restore (see GAMP 5, appendix O9). SIMATIC IT R&D Suite supports automated backups.

	Requirement	Reference	Answer
4.3.8	Electronic records must be readily retrievable throughout the records retention period.	21 CFR 11.10 (c) Annex 11, 17	Yes. As stated above, procedural controls for Backup/ Restore and Archiving/Retrieval should be established. Any data is generally stored in the database but can also be written in a user definable format to (single) files. SIMATIC IT R&D Suite provides automatic online back-up, automatic external history storage and is, if desired, also capable of hot standby redundancy.
4.3.9	If the sequence of system steps or events is important, then appropriate operational system checks should be enforced.	21 CFR 11.10 (f)	Yes. For example, allowances can be made for a specific sequence of operator actions by configuring the application accordingly.

4.4 Audit Trail, Change Control Support

During operation, regulations require the recording of operator actions that may result in the generation of new relevant records or the alteration or deletion of existing records.

	Requirement	Reference	Answer
4.4.1	The system should create a record of all GMP-relevant changes and deletions (a system generated "audit trail"). For change or deletion of GMP-relevant data, the reason should be documented.	21 CFR 11.10 (e) Annex 11, 9	Yes. Changes during operation can be traced back by the system itself via audit trail and contain information with time stamp, user ID, old and new value and comment. The audit trail is secure within the system and cannot be changed by a user. It can be made available and also be exported in electronic portable document formats.
4.4.2	Management systems for data and documents should be designed to record the identity of operators entering, changing, confirming or deleting data including date and time.	Annex 11, 12.4	Yes, see also requirement 4.4.1.
4.4.3	Changes to electronic records shall not obscure previously recorded information.	21 CFR 11.10 (e)	Yes. Recorded information is not overwritten and is always available in the database.
4.4.4	The audit trail shall be retained for a period at least as long as that required for the subject electronic records.	21 CFR 11.10 (e) Annex 11, 9	Yes. This is technically feasible and must be considered in the application specific backup and restore process (see GAMP 5, appendices O9 and O13).
4.4.5	The audit trail should be available for review and copying by regulatory agencies.	21 CFR 11.10 (e)	Yes, see also requirement 4.4.1.

4.5 System Access, Identification Codes and Passwords

Since access to a system must be restricted to authorized individuals and the uniqueness of electronic signatures also depends on the authenticity of user credentials, user access management is a vital set of requirements regarding the acceptance of electronic records and electronic signatures.

	Requirement	Reference	Answer
4.5.1	System access should be limited to authorized individuals.	21 CFR 11.10 (d) 21 CFR 11.10 (g) Annex 11, 12.1	Yes. System access is based on the operating system's user administration, and user rights are to be defined in the system. Nonetheless also procedural controls should be established by the regulated user, as described in GAMP 5, appendix O11.
4.5.2	The extent of security controls depends on the criticality of the computerized system.	Annex 11, 12.2	System security is a key factor during design and development of SIMATIC IT products. SIMATIC IT R&D Suite complies with the International Standard IEC 61508. Nonetheless, since system security strongly depends on the operating environment of each IT system, these aspects should be considered in security management (see GAMP 5, appendix O11). Recommendations and support is given by SIMATIC IT R&D Suite security concept.
4.5.3	Creation, change, and cancellation of access authorizations should be recorded.	Annex 11, 12.3	Changes in user access management are recorded and should be subject to change control procedures of the regulated user.
4.5.4	If it is a requirement of the system that input data or instructions can only come from certain input devices (e.g. terminals), does the system check the validity of the source of any data or instructions received? (Note: This applies where data or instructions can come from more than one device, and therefore the system must verify the integrity of its source, such as a network of weigh scales, or remote, radio controlled terminals).	21 CFR 11.10 (h)	Yes. The SIMATIC IT R&D Suite workstations can be configured so that special input data / commands can only be performed from a dedicated workstation, or from a group of dedicated workstations. All other workstations then have read only access rights.
4.5.5	Controls should be in place to maintain the uniqueness of each combined identification code and password, so that no individual can have the same combination of identification code and password as any other.	21 CFR 11.300 (a)	Yes. The user administration of the operating system is used as a platform for access management. It is not possible to define more than one user with the same user ID within a workgroup / domain. Thus each combination of user ID and password is unique.
4.5.6	Procedures are in place to ensure that the validity of identification codes is checked periodically.	21 CFR 11.300 (b)	The regulated user should establish appropriate procedural controls (see "Good Practice and Compliance for Electronic Records and Signatures, Part 2").

	Requirement	Reference	Answer
4.5.7	Passwords should periodically expire and have to be revised.	21 CFR 11.300 (b)	Yes. Password aging is based on the operating system's user administration.
4.5.8	A procedure should be established for recalling identification codes and passwords if a person leaves or is transferred.	21 CFR 11.300 (b)	The regulated user should establish appropriate procedural controls (see "Good Practice and Compliance for Electronic Records and Signatures, Part 2"). The Microsoft Windows security system can be used to deactivate user accounts.
4.5.9	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.	21 CFR 11.300 (c)	The regulated user should establish appropriate procedural controls (see "Good Practice and Compliance for Electronic Records and Signatures, Part 2").
4.5.10	Measures for detecting attempts of unauthorized use and for informing security and management should be in place.	21 CFR 11.300 (d)	Yes. Non existing users are unable to connect to the webserver. These attempts can be logged by Windows Logon Auditing functionality. Failed attempts of existing users to use the system or to perform electronic signatures are recognized and can be logged. The regulated user should establish appropriate procedural controls to ensure a periodic review of security and access control information logs (see GAMP 5, appendix O8).
4.5.11	Initial and periodic testing of devices, such as tokens and 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.	21 CFR 11.300 (e)	Such devices are not part of SIMATIC IT R&D Suite portfolio, but might be integrated in the system with third party tools. The regulated user should establish appropriate procedural controls (see "Good Practice and Compliance for Electronic Records and Signatures, Part 2").

4.6 Electronic Signature

To ensure that electronic signatures are generally accepted as equivalent to handwritten signatures executed on paper, requirements are not only limited to the act of electronically signing records. They also include requirements on record keeping as well as on the manifestation of the electronic signature.

	Requirement	Reference	Answer
4.6.1	Written policies should be established that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.	21 CFR 11.10 (j) Annex 11, 14.a	The regulated user should establish appropriate procedural controls.
4.6.2	Signed electronic records should contain the following related information: • The printed name of the signer • The date and time of signing • The meaning of the signing (such as approval, review, responsibility)	21 CFR 11.50 (a) Annex 11, 14.c	Yes. The username of the signer, date and time, and the meaning associated with the signature are stored in a database which is maintained by SIMATIC IT R&D Suite.
4.6.3	The above-listed information is shown on displayed and printed copies of the electronic record.	21 CFR 11.50 (b)	Yes.
4.6.4	Electronic signatures 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.	21 CFR 11.70 Annex 11, 14.b	Yes.
4.6.5	Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	21 CFR 11.100 (a) 21 CFR 11.200 (a) (2)	Yes. The electronic signature uses the unique identifiers for user accounts in the Microsoft Windows user administration. The re-use or re-assignment of electronic signatures is effectively prevented.
4.6.6	When a system is used for recording certification and batch release, the system should allow only Qualified Persons to certify the release of the batches and it should clearly identify and record the person releasing or certifying the batch.	Annex 11, 15	Electronic signatures are linked to an individual. The system allows strict determinations about which role and/or individual is allowed to perform a signature.
4.6.7	The identity of an individual should be verified before electronic signature components are allocated.	21 CFR 11.100 (b)	The regulated user should establish appropriate procedural controls for the verification of an individual's identity before allocating a user account and/or electronic signatures.
4.6.8	When an individual executes one or more signings not performed during a single session, each signing shall be executed using all of the electronic signature components.	21 CFR 11.200 (a) (1) (ii)	Yes. Performing an electronic signature requires the user ID as well as the user password.

	Requirement	Reference	Answer
4.6.9	When an individual executes a series of signings during a single session, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one private electronic signature component.	21 CFR 11.200 (a) (1) (i)	Yes. Each signature consists of two components (user ID and password). In order to enhance to signature process multiple records may be signed in one signature procedure.
4.6.10	The use of an individual's electronic signature by anyone other than the genuine owner would require the collaboration of two or more individuals.	21 CFR 11.200 (a) (3)	Yes. It is not possible to falsify an electronic signature during signing or after recording of the signature. In addition, the regulated user needs proccedures that prevent the disclosure of passwords.
4.6.11	Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owner.	21 CFR 11.200 (b)	Standard tools of third-party manufacturers can be used to create biometric electronic signatures. The integrity of such solutions should be assessed separately.

4.7 Open Systems

The operation of an open system may require additional controls to ensure data integrity as well as the possible confidentiality of electronic records.

	Requirement	Reference	Answer
4.7.1	To ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records additional measures such as data encryption are used.	21 CFR 11.30	SSL encryption for communication of managers to each other and to all clients is used consistently. Also the use of Kerberos is supported to allow secure communication over a non-secure network.
4.7.2	To ensure the authenticity and integrity of electronic signatures, additional measures such as the use of digital signature standards are used.	21 CFR 11.30	SIMATIC IT R&D Suite does not provide functionality for digital (encrypted) signatures.

Further information

E-Mail:
pharma@siemens.com

Internet:
www.siemens.com/pharma

Siemens AG
Process Industries and Drives
Pharmaceutical and Life
Science Industry
76181 Karlsruhe
GERMANY

Subject to change without prior notice.
A5E47751024-AA

Siemens
Pharma Industry

www.siemens.com/automation