SIEMENS

# SIMATIC IT Unilab 6.7

# 21 CFR part 11

**User Guide**

**Edition 09/2014**

**A5E00428241-09**

## Guidelines

This manual contains notices intended to protect the products and connected equipment against damage. These notices are graded according to severity by the following texts:

**Caution**

Indicates that if the proper precautions are not taken, this can result into property damage.

**Notice**

Draws your attention to particularly important information on handling the product, the product itself or to a particular part of the documentation.

## Trademarks

All names identified by ® are registered trademarks of the 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
Industry Sector
Postfach 48 48
90026 NÜRNBERG
GERMANY

A5E00428241-09
09/2014

# Preface

## Where is this manual valid?

This manual is valid for release 6.7 of SIMATIC IT Unilab.

## Basic knowledge required

This guide is intended for SIMATIC IT Unilab users who are responsible for system configuration, such as application managers and system integrators (consultants). To be able to understand the concepts and examples discussed in this guide, the reader should at least have taken the SIMATIC IT Unilab Basic Training.

In order to understand this manual, a general knowledge of electronic records and signatures is required.

## Purpose

This User Guide explains how the US FDA rule 21CFR part 11 applies to Unilab.

## Related documentation

The technical note **Enabling 21 CFR part 11 support** contains more information related to the content of this User Guide.

## Conventions

The table below describes the specific typographic conventions that are used throughout this manual:

| **Symbol/Convention** | **Indicates...** |
|---|---|
| E.g. | Where examples are given. |
| **Text in bold** | The names of menus, commands, dialog boxes and toolbar buttons and, in general, all strings (e.g. **File** menu; **Save** command). |
| KEY1+KEY2 | Shortcut keys, which permit rapid access to commands (e.g. CTRL+C). |
| UPPERCASE | The names of keyboard keys (e.g. RETURN key). |
| *Italics* | Noun with special importance or significance for which emphasis is needed.<br>The names of parameters that must be replaced with a specific name or value. |
| **>** | A succession of commands in which the command preceding the symbol must be selected before the command following it. |

| Symbol/Convention | Indicates... |
|---|---|
| `Code example` | Code example. |

## SIMATIC IT Documentation Library

The SIMATIC IT Unilab Documentation Library provides you with a comprehensive and user-friendly interface to access the overall product documentation where manuals and helps online can be browsed by functionality or by component.

## Readme

The installation includes a readme file, which contains information on upgrade procedures and compatibility with previous releases. This file is supplied both in standard text (**Readme.wri**) and in Acrobat PDF (**Readme.pdf**) format.

This file is available in folder \ReleaseNotes of the setup DVD and is available from the SIMATIC IT Unilab Documentation Library.

## SIMATIC IT Training Center

Siemens IA AS MES offers a number of training courses to familiarize you with the SIMATIC IT product suite. To successfully achieve this goal, training consists of lessons in both theory and practice.

Courses are held year-round, according to a program that is published well in advance of the first scheduled session.

The material on the basis of which our courses are conducted reflects the result of years of experience in process, LIMS, quality control and production management.

All courses are held by expert personnel that are aware of the developments and innovations in the Siemens IA AS MES product suite.

Courses are held in English at the Siemens IA AS MES Training Centers.

Upon request, training courses can also be organized on the customer’s premises.

For more information on the training course calendar, please visit our technical web site (http://www.siemens.com/simatic-it/training).

## SIMATIC IT Service & Support

A comprehensive Software Maintenance program is available with SIMATIC IT products. Software Maintenance includes the following services:

- **Software Update Service** (SUS): automatic distribution of upgrades and service packs
- **Technical Support Service** (TSS): support on technical problems with SIMATIC IT software (standard support and other optional services)
- **Online Support**: a technical web site, providing information such as Frequently Asked Questions and technical documentation on SIMATIC IT products

## Software Update Service (SUS)

This service provides automatic shipment of new versions and service packs when released. When a new version / service pack is available for shipping, it is typically shipped within one month.

One copy of the installation DVD is shipped for each Server covered by Software Maintenance.

Hot fixes (officially tested and released) are not shipped and must be downloaded from the Technical Support Service web site.

## Technical Support Service (TSS)

Siemens provides a dedicated technical support team for SIMATIC IT products.

The following options are available:

Bronze support: 9 hours/day, 5 days/week

Silver support: 24 hours/day, 5 days/week

Gold support: 24 hours/day, 7 days/week

The principal language of the SIMATIC IT hotline is English.

SIMATIC IT partners and customers covered by the Software Maintenance program are entitled to direct access to the TSS.

## Access to TSS

To be able to access TSS, the customer needs to register as a user on the Technical Support web site. Connect to http://www.siemens.com/mes-simaticit/ and follow the **Technical Support Service** link.

The registration form must be completed with:

- Personal data
- The required company and plant information
- The Contract Number provided by Siemens Back Office when the contract is agreed.

## Online Support

A customer who is a registered TSS user, can access the Technical Support web site (http://www.siemens.com/mes-simaticit/tss), which contains technical information such as:

- Service conditions (Phone numbers, Working hours, Reaction times,…)
- SIMATIC IT knowledge base: a technical support database that includes practical service solutions from Technical Support or the SIMATIC IT community
- SIMATIC IT software (e.g. hot fixes, software examples) and release notes that can be downloaded
- SIMATIC IT cross-industry libraries that can be downloaded (limited access to SIMATIC IT certified partners)

- SIMATIC IT product documentation that can be downloaded
- Frequently Asked Questions and useful tips.

# Table of Contents

# 1 Introduction

The US FDA rule 21 CFR part 11 sets forth the criteria under which the FDA considers electronic records and electronic signatures – executed to electronic records – to be trustworthy, reliable and generally equivalent to paper records and handwritten signatures executed on paper.

21 CFR part 11 applies to all records required by predicate rules (GLP, GMP) maintained in electronic form, signatures in electronic format, and records submitted to the FDA under predicate rule in electronic format. Certain LIMS data is required to be maintained by predicate rules, mainly GLP, and so 21 CFR part 11 applies for LIMS systems.

In order for a LIMS to comply with 21 CFR part 11, a number of requirements must be met. These requirements generally concern the authenticity, integrity and confidentiality of the electronic records and signatures.

## 1.1 Control Types

The 21 CFR part 11 requirements can be met by applying the following types of controls on a computerized system:

- Technological controls: technical or functional features of the used software
- Procedural controls: standard operating procedures on the use of the application software or on the environment in which the software is used
- Administrative controls: procedures on system administration, such as system access, user management, password management, …

The procedural and administrative controls are the customer’s responsibility. The required technological controls include features contained in the standard Simatic IT Unilab software and features built in the custom software developed on standard Simatic IT Unilab (custom functions and add-on applications). Implementing these technological controls is the responsibility of the supplier (for standard features) or the shared responsibility of the system integrator and the customer (for custom software).

This document:

- Introduces the Simatic IT Unilab technological features in support of 21 CFR part 11
- Provides recommendations for architectural layout, configuration and system setup in order to become 21 CFR part 11 compliant
- Provides guidance on the development of custom software (custom functions and add-on applications) on the standard Simatic IT Unilab software for a 21 CFR part 11 compliant system
- Provides suggestions on the required procedural and administrative controls.

## 1.2 Customer's Responsibility

Sections of the 21 CFR part 11 rule that are solely the responsibility of the customer and on which the supplier or system integrator cannot provide any assistance, are not covered by this manual. These sections include:

- 11.10 (j): written policies on individual's accountability
- 11.100 (b): verification of individual's identity
- 11.100 (c): notification to the FDA on the use of electronic signatures.

## 1.3 Premises

The following general premises were made during the creation of this document:

- The regulation is open to interpretation, so the current document addresses the most commonly held interpretation. The most common interpretation is expected to modify over time and this document will be reissued to reflect the change. If the interpretation of the regulation implemented by an individual organization differs from the enclosed, please contact your Siemens representative for further information
- The user has the appropriate licenses for Simatic IT Unilab 21 CFR part 11 functionality (Advanced 21 CFR part 11 Pack)
- System installation and setup is only started if the Simatic IT Unilab pre-requisites are completely fulfilled
- Simatic IT Unilab is used as a system using password security. Biometric signatures are not covered by this manual.

## 1.4 Advanced 21 CFR part 11 Pack

Unilab functionality and behavior is controlled through object configuration, functional and data access rights, preferences and system settings.

The Unilab Advanced 21 CFR part 11 Pack:

- Enables specific functionality for 21 CFR part 11 compliant systems (version management and detailed audit trail)
- Disables functionality that would allow rendering a system non-21 CFR part 11 compliant (switch off audit trail, delete objects)
- Automatically sets the correct value for a number of preferences/system settings that control system behavior.

**Tip**

For details on upgrading a non-21 CFR part 11 Unilab database to a 21 CFR part 11 database, please refer to chapter Enabling 21CFR Part 11 Support in theUnilab Installation manual

## 1.5 Unilab Electronic Records

21 CFR part 11 applies only to records that are maintained to comply with FDA regulations (predicate rules) or for review by the FDA.

The table below lists the Unilab records that were defined as "Electronic records" according to the definition of the FDA:

| Location | Record | Description |
|---|---|---|
| Server | Configuration data | Configuration data (Oracle database) for all standard Unilab object types:<br>• Request types and Sample types<br>• Info profiles and info fields<br>• Parameter profiles<br>• Parameter definitions<br>• Methods<br>• Worksheet types<br>• Attributes |
| Server | Operational data | All operational data (Oracle database) |
| Client | Client event manager log files | |
| Client | Uniconnect files | Uniconnect templates, error files, log files |
| Server | Unilink files | Unilink input files, error files, log files |
| Server | Report templates, universes | Standard report templates and universes, stored in Unilab Reporting repository |

## 1.6 Closed versus Open Systems

By definition, a closed system is an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.

System access to Unilab is controlled on several levels by the persons responsible for the contents of the electronic records. The customer's IT department controls physical access to the used workstations and to the software installed on these workstations. The customer's IT department also controls PC and network security. It manages the user Ids, passwords and access rights for logging on to the network.

Unilab user management, user roles and privileges define the security profiles for each authorized user based upon responsibilities. The access to control individual configuration objects or operational data can be further restricted to certain users, user roles, tasks or physical workstations. For instance, it is considered good practices to install the Unilab configuration applications only on the system administrator's workstation.

Hence, Unilab C/S is considered a closed system. This assumption is withheld in this manual.

For the Unilab web version, the same security mechanisms apply. Additional controls, such as the use of a firewall, encryption techniques and digital signature standards, should be considered by the customer to ensure, as appropriate, record authenticity, integrity, and confidentiality.

# 2 Electronic Records

## 2.1 System Validation

Reference: 21 CFR part 11.10 (a)

Any computer system utilizing electronic records and signatures must be validated to ensure its accuracy, reliability, consistent intended performance, and ability to discern invalid or altered records.

The Unilab standard software is developed according to best practices set by the industry and by regulatory agencies. A formal life cycle approach is applied. Product requirements and testing address the issues of record accuracy, reliability, and consistent record performance. Requirements and testing also investigate the controlled mechanisms through which records can be altered. A validation file is available providing evidence on development life cycle in use during product development.

The validation of the configured system is the customer's responsibility. Validation of the custom software (custom functions and add-on applications) is the shared responsibility of the system integrator and the customer.

The customer must also provide that patches or upgrades to software are planned, applied and tested according to established procedures.

## 2.2 Record Reproducibility

Reference: 21 CFR part 11.10 (b)

According to 21 CFR part 11 § 11.10 (b), the systems must allow to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review and copying by the agency. The electronic format should be in a widely used industry standard.

All client-based records can be readily viewed and printed directly in ASCII format.

## 2.3 Record Protection and Retention

Reference: 21 CFR part 11.10 (c)

The records (and audit trails) must be accessible throughout the records retention period established by the customer. Backup, archival and retrieval procedures must support the retention of the records.

### Backup and recovery

Backup functionality for securing all the records is customer responsibility. Optional additional integrity can be achieved through the use of standard technologies such as RAID. Recovery testing is customer's responsibility.

### Archiving

All Unilab Database records can be archived through the Unilab Archiving module. This module allows determining which components of the electronic record will be archived and translates these records into an archivable format. The archiving of operational data includes all associated data, including audit trails.

Archiving to another DB is secure (the Unilab security mechanism described elsewhere in this document applies). In case of archiving to file, this file must be created on a secure medium (non-rewritable CD-ROM, …). The latter is procedural responsibility of the customer.

The Unilab Archiving module guarantees full backward compatibility: archive files from previous Unilab versions can always be imported in the current version. Users do not have to maintain older Unilab versions just for the purpose of being able to retrieve archived data.

**Important**

On archiving and restore of archived data, by default no update is done in the object’s audit trail. If required, this can be implemented through customization of the archiving scripts (refer to the Unilab Archiving manual for more information).

**Note**

It is highly recommended to restore the archived data in a test database, instead of in the operational database. This prevents accidental loss or corruption of operational data.

**Tip**

For more information on Unilab archiving, see the Unilab Archiving manual.

The customer is responsible for establishing the retention period and maintaining the records throughout this period. The customer is also responsible for providing maintenance of offsite backup copies of archive and/or backup files.

## 2.4 System Security and Authority Checks

Reference: 21 CFR part 11.10 (d), 11.10 (g), 11.10 (h)

The rule also requires that certain checks be placed on closed systems. These include the 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; and device checks to determine the validity of the source of data input or operational instruction.

### Application - Logging on and security

Only users with permission can gain access to the Unilab applications. The users working in a 21 CFR part 11 mode must log on to the application always with 2 components:

- User ID
- Password

Both the User ID and Password fields are empty in the logon screen. The User ID / password are never saved in the registry or elsewhere.

Invalid logon attempts are registered.

**Tip**

Refer to the paragraph on Tracking of unsuccessful attempts on page 3-6.

## Limiting system access

Operating system and platform security should be used to limit access to the different classes of computer (server, client). It is the customer's responsibility to implement security and access control to the different classes of computer (server, client).

Within Unilab, users are granted access to the functionality and data based on their responsibilities. Access to the individual applications, and the functionality within the application, is implemented through functional access rights on user profile or user level in the **User management** application.

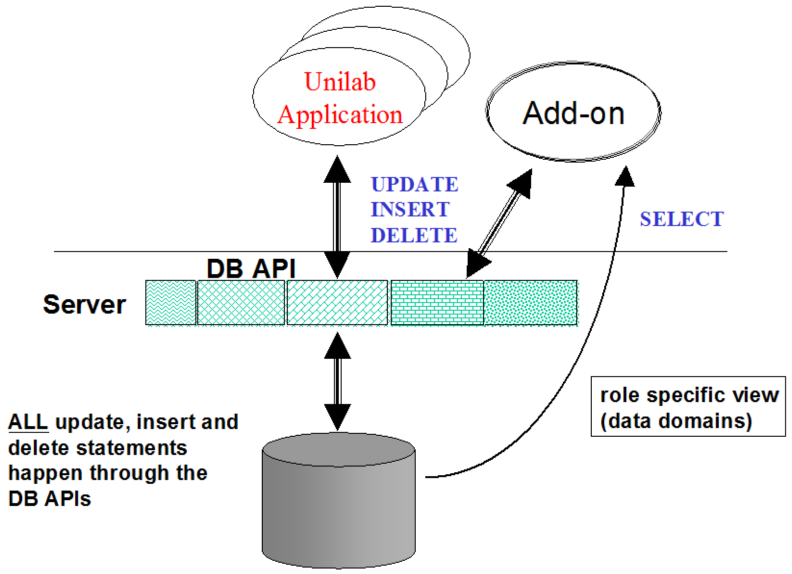
Additional security can be implemented by only installing specific applications on certain PCs. Typically, the configuration applications are only installed on the PC of users responsible for configuration.

## Data access

Standard Oracle database security limits access to the Oracle database. Security is configured in such a way that only the trained database administrator can access the tables! For all other users data domains implement the data access, based on their roles and responsibilities, by accessing the data through data domain specific views. These views exclude all rows for which the access rights of a specific data domain are set to **None**.

Access to database records can be further restricted for specific users / user profiles by means of the appropriate task definitions using hidden or protected fields.

The figure below shows the functional and data access rights to Unilab database records.


Unilab Application
Add-on
UPDATE
INSERT
DELETE
SELECT
DB API
Server
ALL update, insert and delete statements happen through the DB APIs
role specific view (data domains)

## Authority checks

Updates to database records are always performed by means of DB APIs. These APIs check the **Write** data access rights of the current user. This mechanism ensure that a user can for instance not update the analysis results of a sample for which his data access rights are set to **Read** – the user will get a message that he is not authorized to change the data.

Additional authority checks are available by approprioately modifying the Experience Levels table (utel - using the Edit table functionality in the Configuration application). This table allows you to manage the experience levels that can be assigned to the different Unilab users.

For operational actions, authority checks can be set on manual state transitions in the object’s life cycle. For each state transition, the list of users that are authorized to perform the manual transition, can be defined within the life cycle definition. These authority checks also apply to the electronic signatures.

## Security of client files

Security of client files should be guaranteed through controlling physical access to the files and through operating system and platform security. This is the customer’s responsibility.

Many client files are generated/stored on machines to which physical access is already restricted for other reasons. This is, for instance, the case for all Unilink data, error and log files. These files are stored on the database server. This server is installed in the server room, where physical access is restricted to the database administrator and/or other IT personnel only.

The same is valid for the client event manager log files. For security reasons, the client PC on which the Client Event Manager is running is not readily accessible for laboratory personnel (to prevent accidental shutdown of this PC). For practical reasons, it is recommended that this PC be installed in the server room as well.

Uniconnect configuration data is downloaded from the database on startup of Uniconnect and is stored in the registry. Access to the registry should be restricted to system administrators only.

Uniconnect input files are generated on client PCs that are readily accessible by the laboratory personnel. Special measure must be taken to protect these files (operating system security). Note however that the Uniconnect input files are in fact transient files, which are only available on the PC for a very short time before being processed by Uniconnect (as defined by the instrument polling frequency). As such, setting of a high polling frequency enhances file security. Also for the Uniconnect templates, security must be provided through operating system and platform security.

## Administrator privileges

System administrators are often granted full access to all applications and data contained within the system, or control the means to do so. A system administrator, logging on to Unilab as DBA, is granted full access on all Unilab tables, and hence on all Unilab data. Using the appropriate tools, the DBA can modify data without leaving a trace. Thus, special considerations are required for the DBA privileges.

The 21 CFR part 11 preamble makes a clear distinction between two roles: the responsibles for data content and the responsibles for data management. The first group are the normal business users (lab personnel), working with the application on a daily basis. They access the data through the application, so they are subject to all application functional, security and audit trail controls. This group includes the application manager, responsible for setting up and maintaining the Unilab configuration.

The second group is responsible for setup and management of the IT infrastructure, including system security, system backup and archiving, and database administration. This group consists of IT personnel, responsible for maintaining the system, not for its contents. They do not use the application on a daily basis. The DBA is part of this second group.

By making this distinction, falsification of the data, without leaving a trace, would then require the collaboration of at least two persons, for instance the system administrator and a lab user or the application manager.

Please consider the following recommendations for the DBA:

- Do not log on to Unilab as system administrator or as DBA for performing daily operations.
- Access to system administrator tools or applications, such as TOAD, should be limited to the system administrators only. Lab users should not get access to such tools.
- By extension, the previous rule could also be implemented for vital configuration applications, such as the **User management** application. The functionality for creating users could only be restricted to the DBA only.

Note that, when logging on to the system using any Unilab application, the same controls are available for the DBA as for all other Unilab users. For instance, an update performed by the DBA is logged in the object’s audit trail (with the user ID set to the DBA).

### Device checks

Device checks must be used to determine, as appropriate, the validity of the source of data input or operational instruction. During system setup authorized workstations are configured allowing the system devices to communicate to each other. Software loading and licensing further secures the system.

External devices are often used for collection or input of data into Unilab. This is the case for laboratory instruments connected to Unilab, barcode scanners or hand held devices. Information on the device connections is included in the associated electronic records.

## 2.5 Enforced Sequencing of Steps

Reference: 21 CFR part 11.10 (f)

The permitted sequencing of steps is implemented by means of the Unilab life cycles and preferences.

The life cycles implement the workflow to be followed. Life cycles also provide security protection to ensure only personnel authorized to perform an action (state transition) can do so. Others are prevented from performing the action. Through the allow_modify flag of the states, updating of data is controlled. All state transitions in the life cycle are logged in the object’s audit trail.

The customer and the system integrator are responsible for configuring the life cycles according to the required workflow and authorization.

Certain preferences also allow controlling the enforced sequencing of steps. Through the **scCreatePg** preference, for instance, it could be provided that the sample test plan be established only upon completion of the required administrative information (info card).

## 2.6 Audit Trail

Reference: 21 CFR part 11.10 (e)

An important requirement of systems complying with 21 CFR part 11 is their ability to generate an audit trail, defined as a record showing who has accessed a computer system and what operations he or she has performed during a given period of time. Any such audit trail must:

- Be secure, computer-generated and time-stamped.
- Not hide previously-changed data.
- Specify the person responsible for making the change.
- Contain original and changed data.
- Be available for review and copying by the FDA.

### Unilab audit trail

Audit trail functionality is provided on all database records. Audit trails keep track of any entries or changes to the objects. The audit trail information includes:

- What happened to the object (update, insert, …)?
- When did the modification occur (compute generated time stamp)?
- Who was responsible for the modification?
- Why the modification was made?

The audit trail is completely and exclusively handled through the DB API. Unilab users can neither update, nor delete audit trail entries from within the application.

The method-cell audit trail is part of the method audit trail, as this will be more user-friendly and method cells are properties of methods.The  audit trail for info fields is logged on the info-card level. Given that attributes and group keys are part of another object, changing an attribute/group-key value results in an entry of the master object’s audit trail.

In Simatic IT Unilab, the audit trail logs the audit-trail details. This means logging the old and new value of the property of the object that has been changed. These audit-trail details are not visualized on the client, but can be visualized via a report.

**Example**:

When updating a property of the object type, the database will log that “<object type> "<object id>" is updated: property <property description> changed value from "<old value>" to "<new value>".

Note that the <object type> is always a "readable description”.

The audit trail logging visualized on the client is composed of a “what” description, a “who” description, a “when” and a “why” column.

The data stored in these “what” and “who” description columns are meaningful and readable for an average user.

**Example**:

The details of a status change transaction are now stored in the “what” description column in the following form:

```
Status changed from <ssdescription> (<ss>) to
<ssdescription> (<ss>).
```

The “who” description always contains the name of the user who performed the transaction. This can also be an application. In this case, the “who” description holds a “readable” description of the job/application or additional details about the task that this application was performing.

Users working on a 21 CFR part 11 database can never switch off the audit trail and the audit trail detail loggings.

## Version control

Configuration data is considered a meta data on the corresponding operational data. Hence, configuration data is subject to the same 21 CFR part 11 requirements as the corresponding operational data.

This implies that changes to a configuration object:

- Are logged in the object’s audit trail.
- Do not obscure previously-recorded information.

The latter is implemented in Unilab by means of version control on the main configuration objects (attributes, info fields, info profiles, methods, parameters, parameter profiles, sample types, request types, etc.).

When a user wants to change the properties of a configuration object, a new version must be created. Older versions of an object can neither be altered nor deleted. For the new object version, the audit trail  specifies the version on which the current version is based.

**Tip**

The concept of version control is described in the Unilab Concepts Guide Part 3.

## Deleting configuration objects

For users working without a 21 CFR part 11 license, deleting configuration objects is managed through functional access rights on user (profile) level. However, on 21 CFR part 11 compliant systems, deleting objects is no longer allowed. Therefore the specific functional access right to delete configuration objects is not available on systems with 21 CFR part 11 license.

## Universes and standard report templates

Versioning of universes and standards report templates are to be managed procedural by the customer. Third-party tools, like Quality Manager from NOAD Business Intelligence, can be used for automating this task.

### Audit trail at operational level

Changes to operational objects are not managed through version control. An operational object is created by using the information of a specific version of the (corresponding) configuration object. Only individual properties of operational objects can be modified. These changes are traced in the audit trail.

For operational objects, audit trail details are logged.

Reanalysis results are not stored in the object audit trail. Instead, these results are logged in a separate table in the database.

### Audit trail retention and availability

The audit trail is retained, together with the corresponding electronic record, for a period at least as long as that required for the electronic record in question. The Unilab Archiving tool archives audit trail data together with the corresponding electronic records.

Audit trail is available for agency review and copying in the same way as the corresponding electronic records.

## 2.7 Education and Training

Reference: 21 CFR part 11.10 (i) )

The main responsibility on determining whether the person who develops, maintains or uses electronic records/electronic signature systems has the proper education, training and experience lies with the customer. However, both the supplier and the system integrator can assist the customer by organizing standard training sessions or training sessions on the implemented system.

## 2.8 System Documentation

Reference: 21 CFR part 11 .10 (k)

System documentation is found in manuals (PDF files on product CDs and on system) and online help files. Master copies of the system documentation are provided on the product CD. Documentation cannot be created, changed, or deleted from the product CD. End users can choose to install copies of this documentation on the system. Copied documentation cannot be modified. As a result, no audit trails are necessary on the documentation. Each document contains static version information.

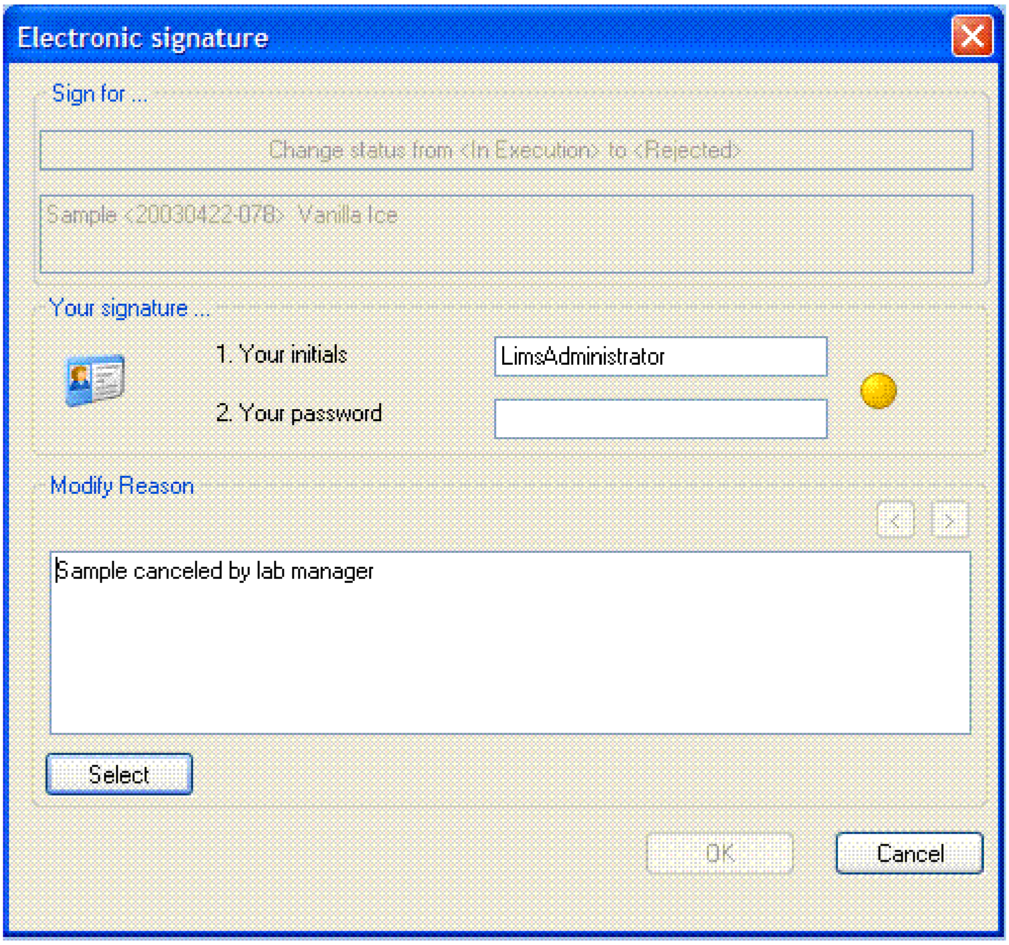
# 3 Electronic Signatures

## 3.1 Electronic Signatures in Simatic IT Unilab

In Unilab, electronic signatures can be configured on state transitions in the object’s life cycle. Each time an authorized user initiates a transition to such a state, he is prompted to enter his user ID, password and comment. The user ID and password are entered in the same window that describes the action the user is “signing off”.

### Configuration of electronic signatures

The figure below shows the **Electronic signature** window.



Electronic signature

Sign for ...

Change status from <In Execution> to <Rejected>

Sample <20030422-078> Vanilla Ice

Your signature ...

1. Your initials: LimsAdministrator

2. Your password:

Modify Reason

Sample canceled by lab manager

In Unilab, the list of states that require an electronic signature can be established. This is done through the system setting **STATES_TO_SIGN_OFF**. Each time an authorized user initiates a transition to such a state, the electronic signature dialog is displayed.

The **Electronic signature** dialog is also displayed when it succeeds a previous **Modify reason** dialog. When canceling an object, for instance (=state transition of status **cancelled @C**), the user first gets the dialog to account for the state transition to status **Cancelled**. When the status @**C** is included in the value list for the **States to sign off** system setting, this dialog is followed by the **Electronic signature** dialog.

The modify reason entered in a previous **Modify reason** dialog is not copied to the **Electronic signature** dialog. Both the modify reason and the modify reason in the **Electronic signature** dialog are saved in the object's audit trail!

Note that this mechanism is also influenced by a number of preferences on the user profile level (i.e. **ConfirmStatusChange**, **CancelwithoutComment**, **ReanalWithoutComment**).

## Signature manifestations

Reference: 21 CFR part 11 .50

Signature manifestations contain the following information.

- User ID/initials (unique) and Full user's name are recorded.
- Date and time are recorded.
- The product functionality records what action was taken by the signer (meaning). An additional field is provided for notes on the meaning of the action. In some situations, a comment is required.

The full name is part of the Why column. Example of the Why message: Signature by John Doe on 18 march 2002 10:00:00 for status change from "Created" (CR) to "In Execution" (IE). When the signature turns out to be valid, an entry will be saved in the audit trail logging of the corresponding object.

When the user fails to enter the correct password in the **Electronic signature** dialog, the state transition is reset and the entered comments are not saved. (This also counts for the comment entered in the **Modify reason** dialog).

## Uniqueness of user ID / password combination

Reference: 21 CFR part 11 .100 (a), 11.300 (a)

The electronic signature has two components: user ID/initials and password. In Unilab, each user ID is unique: therefore, no two individuals can have the same combination of user ID/password.

Furthermore, it is impossible to delete users. Unilab only allows to inactivate users. As a result, a user ID, (and, thus, an electronic signature) cannot be reused by, or reassigned to, anyone else.

### Signature / Record linking

Reference: 21 CFR part 11 .70

Signature manifestations are protected as electronic records and linked to the associated electronic record. The electronic signature information is displayed in the object’s audit trail.

Normal users cannot excise, copy or otherwise falsify a manifestation of an electronic signature.

The signature manifestations are protected in the same manner as the associated electronic record. The signature manifestations can be viewed and printed in the same manner as the associated record.

## 3.2 Components and Controls

Reference: 21 CFR part 11 .200

### Controlled access

According to 21 CFR part 11.200 electronic signatures that are not based upon biometrics shall employ at least two components. In Unilab, these components are the user ID and the password.

Users log on to Unilab, but this log-on name is not used for the creation of an electronic signature. Each time a user performs a series of actions, the two electronic signature components are required. This is the case within both a non-continuous period and a single, continuous period of controlled Unilab access.

### Application lock

When an application is not used for some time, it locks itself (to avoid unauthorized access to any data). A **LockApplication** preference is available to specify this “inactive” period. The **LockApplication** preference puts the application in a lock mode (= automatically minimize) when the specified time period has elapsed.

Only the same Unilab user can unlock the application session again.  To unlock the application, the user must fill out his user name and password.

**Important**

An alternative approach is to put the lock on OS level. In this manner, the entire workstation is locked after a set period of inactivity.

## 3.3 Controls for Identification Codes / Passwords

Reference: 21 CFR part 11 .300

According to 21 CFR part 11, organizations that use electronic signatures based on the use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Since this is the case for Unilab, a number of provisions must be taken. This paragraph describes these provisions.

The major part of password management in Unilab is controlled on the Oracle level. Password management is set on the user-profile level. DB users can be assigned to user profiles. User-profile and user settings can be managed by the Oracle Enterprise manager or using SQL statements. For more details, please refer to the Oracle documentation.

**Important**

- Note that when changing the DBA (Oracle) password, it may be necessary to change some settings in SIMATIC IT Report Manager.

## Password assignment

No one other than the user himself is allowed to know the password. Even the database administrator is not permitted to know the passwords of the users.

Upon user creation, the DBA assigns a password to the user. However, the first time the user accesses the application, he is forced to change this password. Application access is not permitted to the user as long as he does not change his password.

## Forgotten or lost passwords

When an application user has forgotten or lost his password, the user has no possibility to enter the application. The database administrator must reactivate the user’s access. Note that the DBA user cannot assign a new password to another user with the standard Unilab applications (User Management): this must be done using standard Oracle tools.

The first time the user accesses the application he must be forced to change this password as only he is allowed to know his password.

## Password complexity verification

The password complexity verification checks if the passwords satisfy certain rules (e.g. minimum length, number of special characters, etc.). It is possible to write your own password complexity verification function in PL/SQL. Please refer to the Oracle documentation on how to do this.

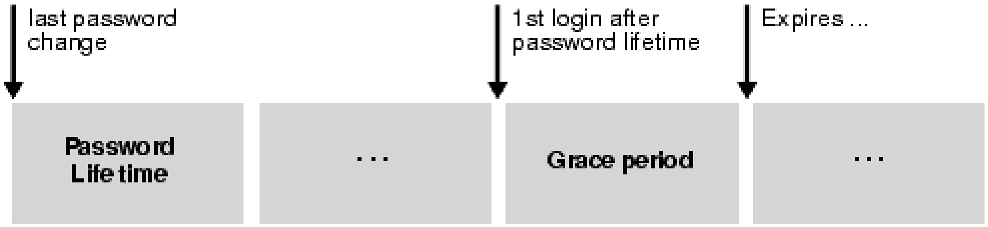
## Password expiration and aging

The DBA uses the **CREATE PROFILE** statement to specify a maximum lifetime for passwords. When the specified amount of time elapses and the password expires, the user or DBA must change the password. The following statement indicates that **ASHWINI** can use the same password for 90 days before it expires:

```
CREATE PROFILE prof LIMIT
     FAILED_LOGIN_ATTEMPTS 4
     PASSWORD_LOCK_TIME 30
     PASSWORD_LIFE_TIME 90;
ALTER USER ashwini PROFILE prof;
```

DBAs can also specify a grace period using the **CREATE PROFILE** statement. Users enter the grace period upon the first attempt to log on to a database account after their password has expired. During the grace period, a warning message appears each time users try to log on to their accounts, and continues to appear until the grace period expires. Users must change the password within the grace period. If the password is not changed within the grace period, the account expires and you cannot log on to that account anymore until the password is changed.

The figure below shows the chronology of the password lifetime and grace period.



For example, the lifetime of a password is 60 days, and the grace period is 3 days. If the user attempts to log on on *any* day after the 60th day (this could be the 70th day, 100th day, or another; the point here is that it is the first logon attempt after the password lifetime), that user receives a warning message indicating that the password is about to expire in 3 days. If the user does not change the password within three days from the first day of the grace period, the user's account expires. The following statement indicates that the user must change the password within 3 days of its expiration:

```
CREATE PROFILE prof LIMIT
     FAILED_LOGIN_ATTEMPTS 4
     PASSWORD_LOCK_TIME 30
     PASSWORD_GRACE_TIME 3;
ALTER USER ashwini PROFILE prof;
```

The messages returned by Oracle concerning password expiration and aging, are shown to the user when starting up the application. The following messages are available, and are visualized by the Simatic IT Unilab client applications:

- **Password is about to expire in <period>**
- **Password is expired**
- **Account is locked**

The following entry in the registry needs to be set in order to be able to see the SQL-error messages, raised by the Oracle database: **Sqlerror=yes**.

## Password history

The DBA uses the **CREATE PROFILE** statement to specify a time interval during which users cannot reuse a password.

In the following statement, the DBA indicates that the user cannot reuse his/her password for 60 days.

```
CREATE PROFILE prof LIMIT
     PASSWORD_REUSE_TIME 60
     PASSWORD_REUSE_MAX UNLIMITED;
```

The next statement shows that the number of times the user must change his/her password before he/she can re-use his/her  current password is 3.

```
CREATE PROFILE prof LIMIT
     PASSWORD_REUSE_MAX 3
     PASSWORD_REUSE_TIME UNLIMITED;
```

## Tracking of unsuccessful logon attempts

Tracking of successful and unsuccessful log on attempts is possible using the **audit session by session**  statement of Oracle. Any of the following commands can be used to view the audit info:

```
select * from dba_audit_session
select * from dba_audit_trail
select * from sys.aud$
```

**Important**

If the audit trail table becomes full, it is no longer possible to log on as a normal (Oracle) user. Only the system administrator can log on to purge the table. It is the DBA’s responsibility to control the growth and size of the audit trail.

After a number of unsuccessful log-on attempts, the user is blocked (can no longer log on). The database administrator must manually activate the user account. The first time the user accesses the application, he/she is forced to change this password as only he/she is allowed to know his/her own password. Oracle messages as e.g. password is expired, your account is locked, etc. are passed correctly to the Unilab application (see Password Expiration and Aging).

**Important**

Notification of management on unauthorized use of a password through for instance e-mail is not implemented by default. This can however be implemented through an Oracle trigger on the sys.dba_audit table.

The logon window automatically disappears after the third unsuccessful logon attempt. This is completely independent of any Oracle security settings!

## Password locking

When a particular user exceeds a specified number of unsuccessful logon attempts, the server automatically locks that user's account. The DBA specifies the maximum allowed number of unsuccessful logon attempts using the **CREATE PROFILE** statement. The DBA also specifies the duration for which the account remains locked.

In the following example, the maximum number of unsuccessful logon attempts for the user **ASHWINI** is 4, and the amount of time the account will remain locked is 30 days; the account will unlock automatically after 30 days have elapsed.

```
CREATE PROFILE prof LIMIT
     FAILED_LOGIN_ATTEMPTS 4
     PASSWORD_LOCK_TIME 30;
ALTER USER ashwini PROFILE prof;
```

If the DBA does not specify a time interval for unlocking the account, **PASSWORD_LOCK_TIME** assumes the value specified in a default. If the DBA specifies **PASSWORD_LOCK_TIME** as **UNLIMITED**, then the system security officer must explicitly unlock the account.

After a user successfully logs on to an account, the unsuccessful logon attempt count (if present) for that user is reset to 0.

The security officer can also explicitly lock user accounts. When this occurs, the account cannot be unlocked automatically; only the security officer can unlock the account.

# 4 Custom Functions / Add-ons

## Introduction

The standard Unilab software holds the necessary technical controls to obtain a 21 CFR part 11 compliant system. However, within the context of an implementation project, custom code or add-on applications are developed. This paragraph describes some considerations when developing custom code or add-on applications for a system that must be 21 CFR part 11 compliant.

The following considerations must be taken into account:

- Custom code and add-on must be validated
- DB APIs must be used as much as possible to connect to DB and perform updates
- User ID and password are blank at logon
- Privileges on Add-on tables must be set properly
- Evaluate the need for an audit trail on add-on records.

## Validation

The customer is responsible for validating configuration, custom code and add-on applications.

## Use of DB APIs

As described in the Unilab Concepts Guide, DB APIs implement the functional and data access rights on the database side. The APIs also implement version control for configuration objects.

For these reasons, it is strongly recommended that DB APIs be used to make any connections to the database and perform database updates. Freehand SQL to perform these actions must be avoided.

## User ID and PW during the logon procedure

For  security reasons, the user ID and password are blank in the logon screen of the standard applications. This good practice should be applied in add-on applications as well. Preferably use the Simatic IT Unilab objects to do so.

## Privileges on add-on tables

Access to the add-on tables is not controlled by the DB APIs. Hence, privileges on these tables must be considered during application development.

## Add-on records

21 CFR part 11 applies to all records that are required by the predicate rules. Hence, it must be considered whether records, created in the context of an add-on application, are required by the predicate rules. If so, 21 CFR part 11 applies and special provisions must be taken (such as audit trail, version control, …).