Change Log

Date	Prepared by	Description	Approval date
2019-03-27	Andreas Norén	Rebranded new template.	2019-03-27 /JA
2018-04-18	Andreas Norén	Updated with Sartorius template. Reviewed document.	2018-05-02 /JT
2014-10-09	Erik Renberg, Lisa Gabrielsson	Updated to include SIMCA-online recent features. Added references to help/UG concerning what is logged.	2014-10-09 /ÅN
2014-02-03	Lisa Gabrielsson	Added paragraph about electronic signatures in SIMCA-online. Other minor updates.	
2013-09-03	Lisa Gabrielsson	Updated for MODDE 10.	2013-09-04
2012-10-29	Erik Renberg	Updated for SIMCA-online 13	2012-10-30
2012-10-29	Joakim Sundström	Updated include MODDE 9 and SIMCA 13	
2009-03-20	Joakim Sundström	Updated 2.3 with registry details for 32 bit applications under 64 bit OS.	2009-03-20
2008-08-21	Lisa Gabrielsson	Updated to apply to and include the latest versions of the software. Updated to latest logo.	2008-08-21
2008-08-14	Lisa Gabrielsson	Updated header to display save date and time.	
2007-09-24	Lisa Gabrielsson	Added SBOL 3.0 info	2007-10-02
2006-05-30	Lisa Gabrielsson	Updated to include MODDE 8	2006-05-30
2006-01-11	Lisa Gabrielsson	Added audit trail info for SBOL	
2005-06-27	Lisa Gabrielsson	Added electronic records and electronic signatures in intro.	2005-08-15
2005-06-23	Lisa Gabrielsson	Added table of contents, updated with info on 11	
2005-02-25	Lisa Gabrielsson	Revised to include both software	
2005-01-25	Lisa Gabrielsson	First draft	

Contents

1 Introduction

This document describes the Audit Trail as implemented in SIMCA, MODDE and SIMCA-online, and how electronic records and electronic signatures (ERES) apply to these products.

1.1 Terminology

SIMCA when used in this document includes also SIMCA-P+ and SIMCA-P.

SBOL refers to SIMCA-Batch On-Line.

SIMCA-online is the online software that replaced SBOL in 2012 when SIMCA-online 13.0 was released. Unless separately noted below, SIMCA-online also refers to SBOL in this document.

A *project* (as in SIMCA and SIMCA-online project) when used in this document includes also *investigation* (as in MODDE investigation) and configurations in SIMCA-online.

A *session* starts when a project is opened, and ends when it is saved. For SIMCA-online the server audit trail is active as soon as the server is started. A *user session* starts when a user logs on to SIMCA-online and ends when the user logs out.

An *event* is a describing text about a change to the project, affecting the design, in addition to the date/time when the event occurred.

Extended User Information is an optional, additional text about a user, describing the user in greater detail. *Extended User Information* is unavailable in SIMCA-online.

DB is the abbreviation for Database.

2 CFR part 11 compliance – Audit Trail

See http://www.21cfrpart11.com/ for background information on 21 CFR Part 11.

In MODDE, SIMCA, and SIMCA-online, we have implemented this by adding the Audit Trail, which is a log where all changes to the project are logged. Each project has its own Audit Trail. In SIMCA and MODDE the audit trail is part of the project (saved in the same usp/mip-file) while it for SIMCA-online is saved in the global database of a SIMCA-online server. The audit trial is viewed in an output bar inside the software and can be printed if desired.

For a new installation of MODDE and SIMCA the Audit Trail is by default off but can be turned on by the user. By default, the user can control the audit trail and clear it, but administrators can block this if desired.

In SIMCA-online the audit trail is always on and cannot be turned off. From SIMCA-online version 13.2 electronic signatures are supported, see paragraph 2.7.

In addition to the Audit Trail, all plots will be marked with the project name, software version, date, and time. Thereby each plot can be tracked to what has happened with the project according to the log.

2.1 What the Audit Trail does

- When a file is imported, a new session is started. At the beginning of this first session the full path to the file imported and changes done during the import are added to the Audit Trail.
- When a project is opened, a new session is started. At the beginning of each session the full path to the usp/rusp/mip-file, the software version, information about the user and the date and time are added to the Audit Trail. The user name and domain are retrieved from Windows.
- When "prompt for extended user information is activated", a new user that has previously not run the software will be asked for Extended User Information, which allows the user to enter more information about him/herself. This information is stored in the beginning of each session started by that user (not applicable to SIMCA-online).
- When the user modifies the project an event is appended to the log, each event is also given a date and time stamp. See the help/user guide for a list of logged events.
- When saving the project a digital signature is computed on the latest session and appended to it. All data in the session is used for the checksum.
- For MODDE and SIMCA the audit trial is saved in the usp/mip-file (but only if the project is saved, the audit trail is not saved when a project is opened but not saved).

- For MODDE and SIMCA, when re-opening the project a new digital signature of the last session is computed and compared with the stored digital signature. If it doesn't match this is logged in the Audit Trail and the user is warned about the log being modified. This means that no tampering with the Audit trail is possible without discovery.

2.2 User Interface

2.2.1 Viewing the Audit Trail

The Audit Trail is a dockable window. To display the Audit trail window if hidden,

SIMCA 13; `View | Show/Hide | Audit Trail`

MODDE 10: `View | Show or hide | Audit Trail`.

SIMCA-online: `View | Audit Trail`.

The Audit Trail window displays the sessions and events of the open project. The newest events are found at the bottom.

By right clicking in the window you can copy and print the text in the Audit Trail.

In MODDE and SIMCA the content of the Audit Trail window is refreshed approximately every 3 seconds.

2.2.2 Control

The user can control the Audit Trail in the menu:

- `File | Project Options` in SIMCA.
- `File | Options | Investigation` (current investigation) or `MODDE Options` (for new investigations) in MODDE.

The Audit trail in SIMCA-online is always turned on and this cannot be changed by the user or the administrator.

MODDE

In the dialog pages in MODDE 10 Investigation Options the options apply to the currently open investigation:

- Turn on / off logging.
- Clear the Audit Trail for the open investigation.
- Save the audit trail to file.

In MODDE Options the option applies to new investigations:

- Turn on / off logging.

2.3 Storing the settings for the Audit Trail for SIMCA and MODDE

The settings for the Audit Trail page are stored in the registry of the computer running SIMCA in a registry key that is unique for each user. This means that each user logging in to a computer can have different settings. In SIMCA-online the audit trail is always turned on.

SIMCA stores the per-user information in the following registry key:

`HKEY_CURRENT_USER\Software\Umetrics\software\version\AuditTrail`
When running 32 bit application under 64 bit Vista the information is stored in

`HKEY_CURRENT_USER\Software\Wow6432Node\Umetrics\software\version\AuditTrail`
That key has the following values and allowed data

Keys	Data
`LogEvents`	1 for logging events to the Audit Trail, 0 for turning the logging off.
`PromptForExtendedUserInfo`	1 for prompting new users to edit extended user info, 0 for not prompting.

Keys	Data
ExtendedUserInfo\%username%	A string value with the extended user information for the user with username %username%.

2.3.1 Locking

The Audit trail behavior can be overridden by administrators if desired and in this case the entire Audit Trail page in File | Options | Project or File | Options | Investigation is disabled.

To lock the audit trail, create the following keys in the registry:

HKEY_LOCAL_MACHINE\Software\Umetrics\software\version\AuditTrail

There you should add the same keys as for the per-user settings (except for ExtendedUserInfo), but you can also add the following DWORD values:

LockedUI	1 for disabling all controls of the Audit Trail page (except editing the current user's Extended User Information). Recommended with Audit trail on. 0 for enabling all controls.

If this key exists in HKEY_LOCAL_MACHINE, ALL settings for the Audit Trail will be read from this key and shared between all users on that computer.

Unlike the HKEY_CURRENT_USER key, non-administrators cannot change a registry in HKEY_LOCAL_MACHINE. This means that the Audit Trail settings become impossible to change (= locked) for regular users.

2.4 Logged changes

Refer to the user guide or online help for each specific version of MODDE, SIMCA and SIMCA-online to learn about the specific events that are logged the audit trails.

For SIMCA-online, look for the topics about Server audit trail and Configuration audit trail.

2.5 SIMCA-online audit trails

In SIMCA-online there are two types of audit trails; Server audit trail and Configuration audit trail.

SIMCA-online uses one global Server audit trail. It logs events global to the entire server, such as events related to server starting or stopping, users, folders, permissions, workspaces and SIMCA projects.

In addition each project configuration has its own Configuration audit trail. In it events related to this particular configuration are logged, such as information about prediction, batches, alarms and notes.

2.6 Electronic signatures in SIMCA-online

Electronic signature is available in SIMCA-online 13.2 and later.

Electronic signatures, in combination with the built-in Audit trail, enable compliance with 21 CFR Part 11.

Electronic signatures can be enabled in the **Miscellaneous settings** page in SIMCA-online Server Options.

When enabled, the following actions in SIMCA-online require an electronic signature:

- Adding and changing a project configuration.
- Purge of projects and project configurations.
- Resetting alarms.
- Deleting predicted data.
- Repredict.