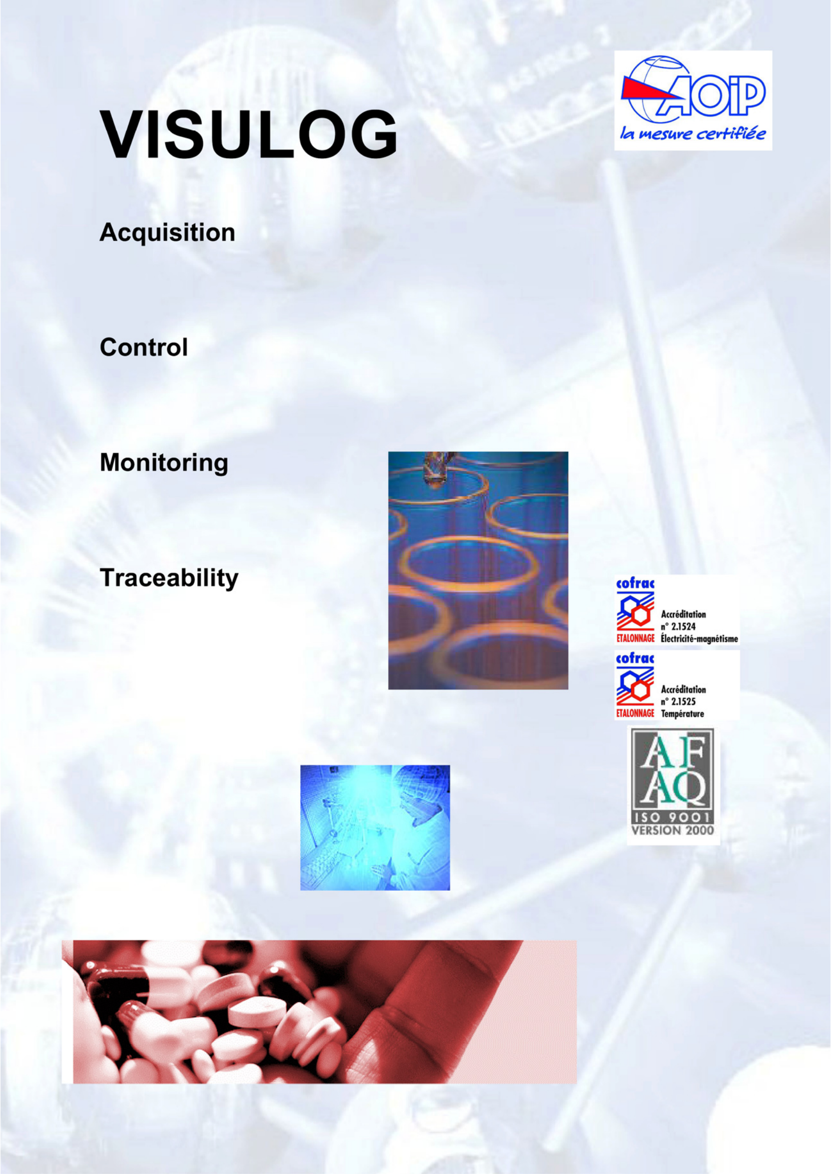
VISULOG

SUPERVISION AND MONITORING SOFTWARE

FDA 21 CFR PART 11 COMPLIANCE WHITE PAPER



VISULOG

Acquisition

Control

Monitoring

Traceability

la mesure certifiée
cofrac
ETALONNAGE
Accréditation n° 2.1524 Électricité-magnétisme
cofrac
ETALONNAGE
Accréditation n° 2.1525 Température
AFAQ
ISO 9001
VERSION 2000

Ed. September 08

Index

Purpose

This document describes the AOIP VISULOG compliance with the US Food and Drug Administration codes of federal regulations, chapter 21 , part 11(FDA 21CFR PART11)

All text in italic, in this documentation, is a copy of the paragraphs of the standard.

VISULOG is software providing a full set of tools to develop and deploy applications for Supervision, control and data acquisition data functionality.

The development of such applications from the tools offered by VISULOG, and its compliance with the FDA requirements remains the sole responsibility of the user.

FDA compliance embraces complete system including hardware, software, documentation, files &user management, user's rules of conduct, company security standards,…

Visulog is only one element in a system, and VISULOG cannot solely guarantee the compliance. This is also dependent of the environment in which VISULOG is deployed.

AOIP guarantees that, if the application is deployed and used according to our guidelines, it will not create any breaches in FDA compliance.

Subpart A—General Provisions

§ 11.1 Scope.

§11.2 implementation.

§11.3 Definitions

Subpart B- Electronic records

§11.10 Controls for closed system

§11.30 Controls for open systems

§11.50 Signature manifestations

§11.70 Signature/record linking

Subpart C- Electronic signatures

§11.100 General requirements

§11.200 Electronic signature components and controls

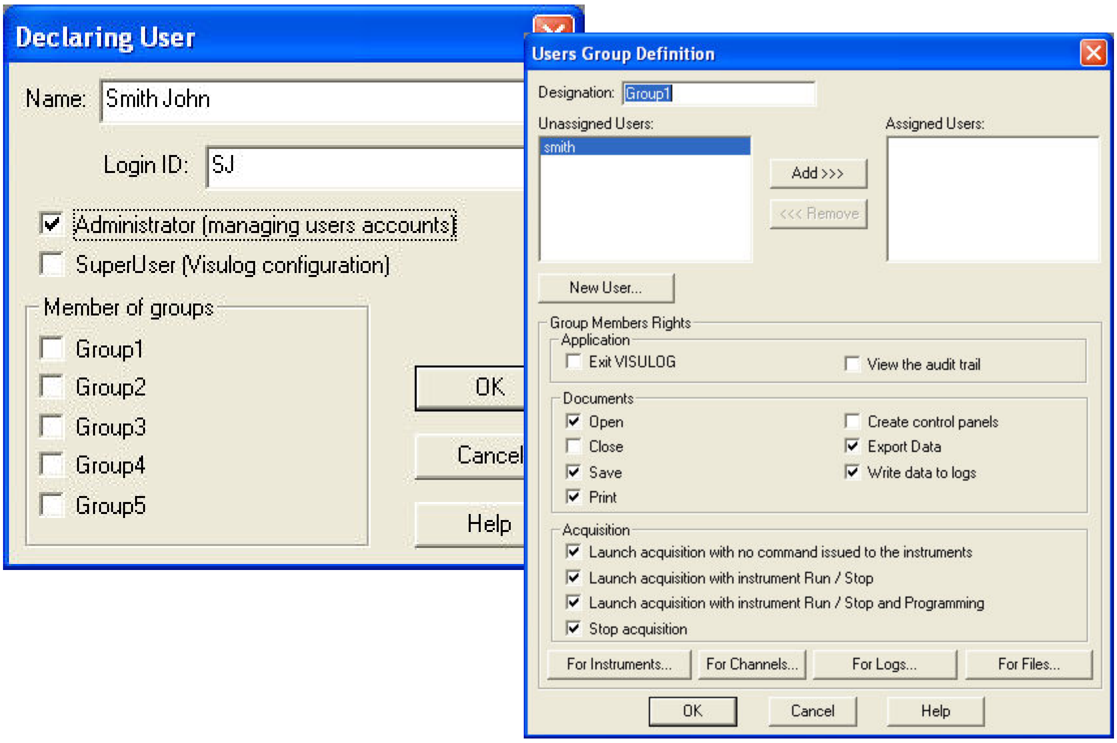
§11.300 Controls for identification codes/passwords.

VISULOG position and presentation

The following is a detailed list describing how VISULOG complies with each point of the regulation

Introduction to Visulog User right management

As required by FDA 21 CFR PART 11, §11.200, Visulog employs two distinct identification components such a s a unique combination of password and login.



Declaring User

Name: Smith John

Login ID: SJ

☑ Administrator (managing users accounts)
☐ SuperUser (Visulog configuration)

Member of groups
☐ Group1
☐ Group2
☐ Group3
☐ Group4
☐ Group5

Users Group Definition

Designation: Group1

Unassigned Users: smith

Assigned Users:

Group Members Rights

Application
☐ Exit VISULOG
☐ View the audit trail

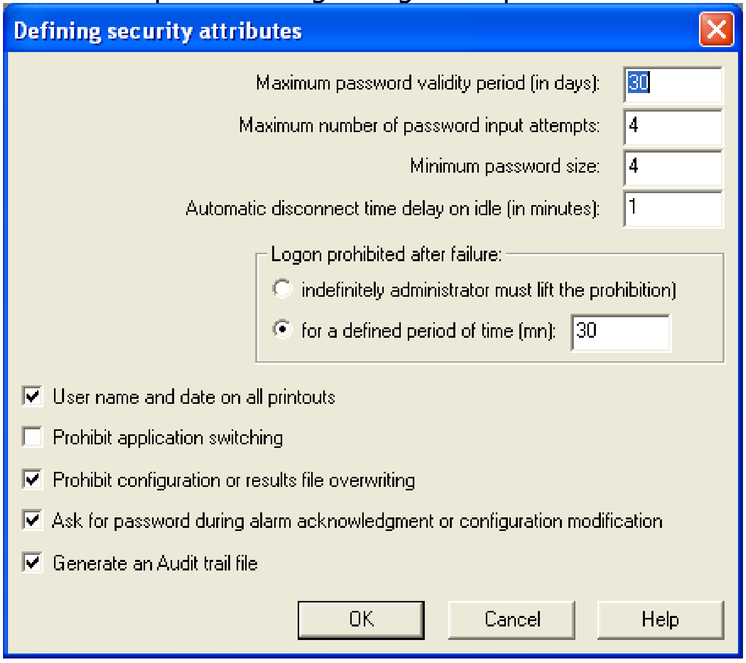
Documents
☑ Open
☐ Close
☑ Save
☑ Print
☐ Create control panels
☑ Export Data
☑ Write data to logs

Acquisition
☑ Launch acquisition with no command issued to the instruments
☑ Launch acquisition with instrument Run / Stop
☑ Launch acquisition with instrument Run / Stop and Programming
☑ Stop acquisition

Furthermore there are several levels of security access used to control access to VISULOG:

- Users must be created by an administrator
- Users are requested to enter their own password upon the first login
- Users can be forced to change their password after a specific time
- Rules on the content (length of passwords) can be applied
- Users are disallowed to use their old password once their current passwords have expired;
- Upon a specific amount of failed attempts to enter in VISULOG, the user is forbidden to access anymore, until the administrator authorizes it.

The system can be disabled after a specific time without any action during a session, and thus can request once again login and password.



Defining security attributes

Maximum password validity period (in days): 30

Maximum number of password input attempts: 4

Minimum password size: 4

Automatic disconnect time delay on idle (in minutes): 1

Logon prohibited after failure:

○ indefinitely administrator must lift the prohibition)

● for a defined period of time (mn): 30

☑ User name and date on all printouts

□ Prohibit application switching

☑ Prohibit configuration or results file overwriting

☑ Ask for password during alarm acknowledgment or configuration modification

☑ Generate an Audit trail file

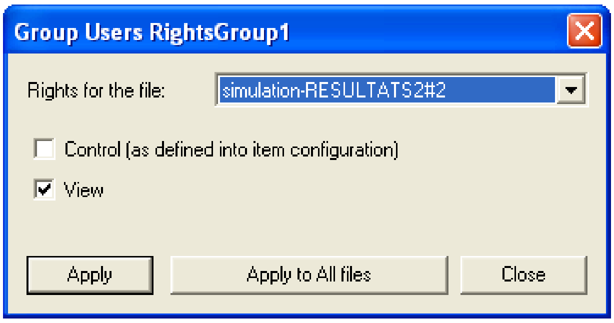
Access rights on a configuration

Access to all alarms, objects, files, and menus can be controlled via option only accessible when defining the application.

It is the responsibility of the application designer (also called in VISULOG, super user) to ensure that correct options are selected.

Access rights of a project can be defined for both users and users groups as described in the topics listed below

a/ Access rights for files

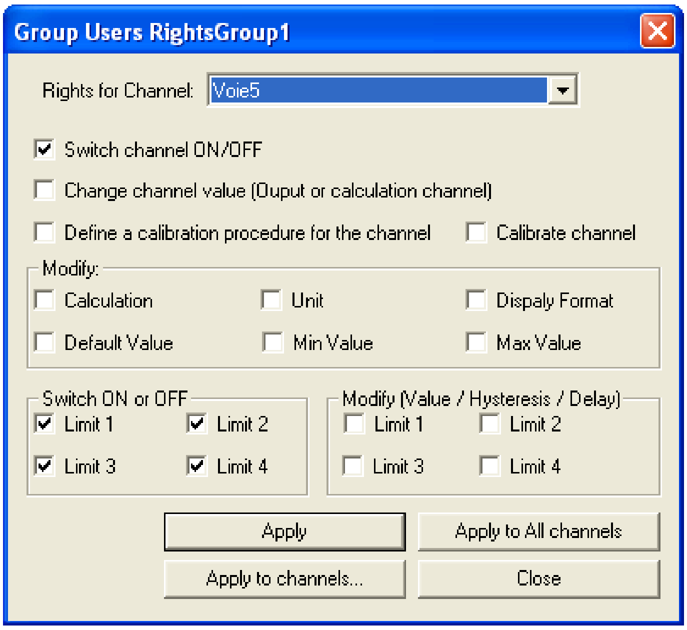


Rights for the file: simulation-RESULTATS2#2

☐ Control (as defined into item configuration)

☑ View

b/Access rights for channels



Rights for Channel: Voie5

☑ Switch channel ON/OFF

☐ Change channel value (Ouput or calculation channel)

☐ Define a calibration procedure for the channel ☐ Calibrate channel

Modify:

☐ Calculation ☐ Unit ☐ Dispaly Format

☐ Default Value ☐ Min Value ☐ Max Value

Switch ON or OFF

☑ Limit 1 ☑ Limit 2

☑ Limit 3 ☑ Limit 4

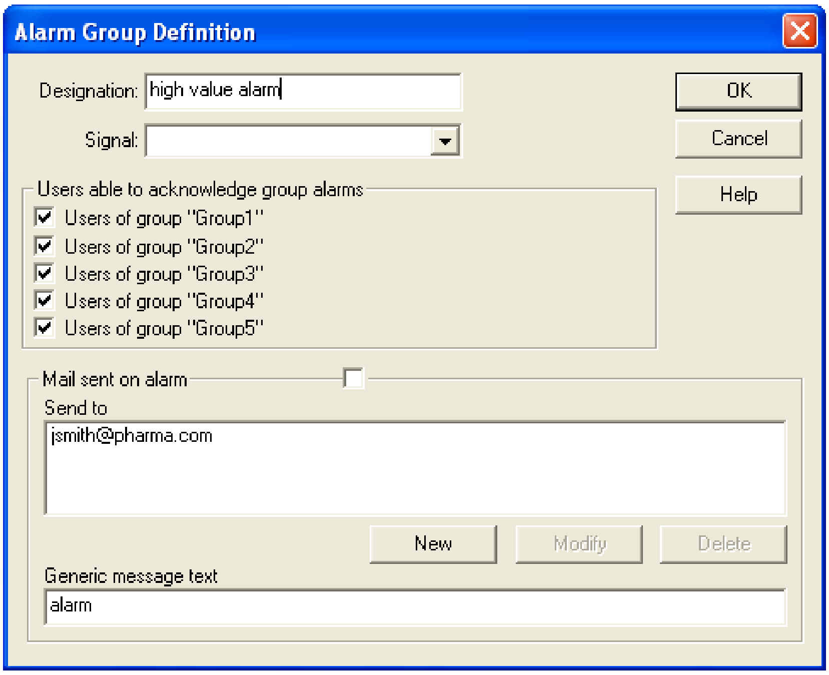
Modify (Value / Hysteresis / Delay)

☐ Limit 1 ☐ Limit 2

☐ Limit 3 ☐ Limit 4

c/ Access rights for alarms

It is possible to define for each alarm users and groups of users that can access to control or modify alarm values and settings or to acknowledge the alarm.



Alarm Group Definition

Designation: high value alarm

Signal:

Users able to acknowledge group alarms

☑ Users of group "Group1"

☑ Users of group "Group2"

☑ Users of group "Group3"

☑ Users of group "Group4"

☑ Users of group "Group5"

Mail sent on alarm ☐

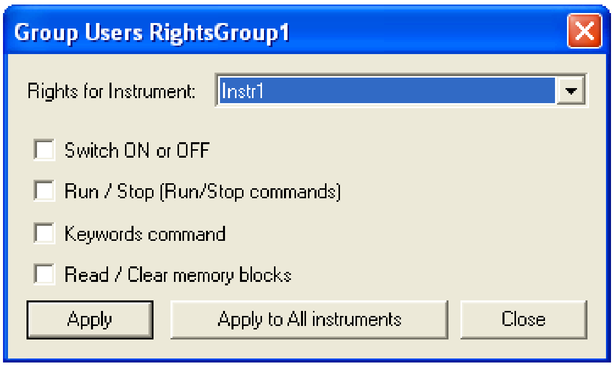
Send to

jsmith@pharma.com

Generic message text

alarm

d/ Access rights for menus and modules: here below the instruments



Group Users RightsGroup1

Rights for Instrument: Instr1

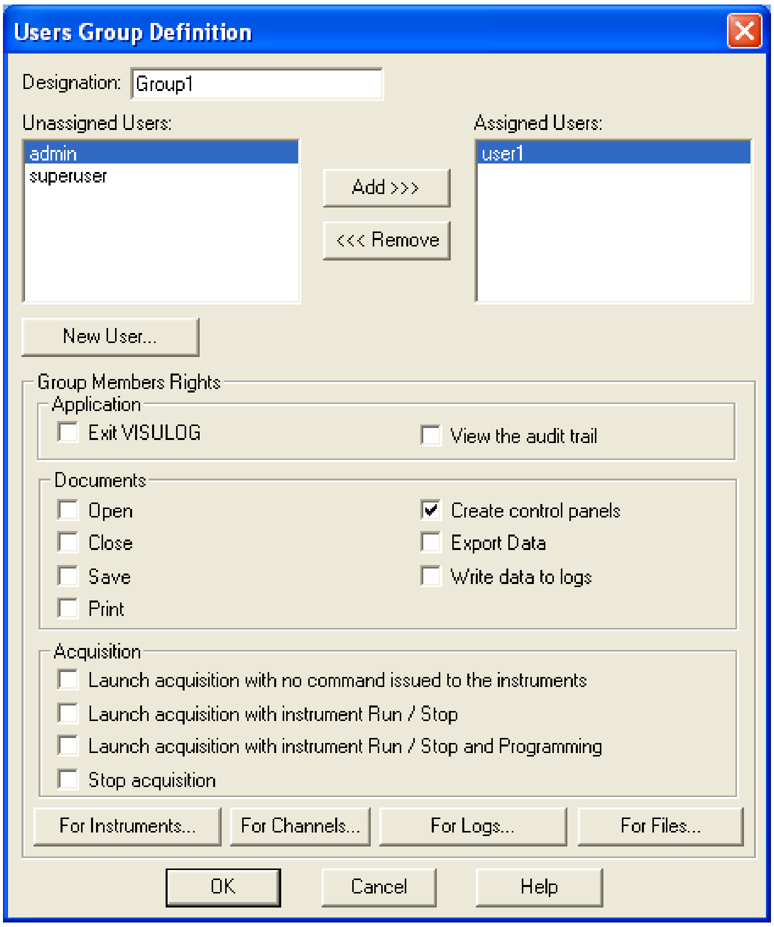
☐ Switch ON or OFF

☐ Run / Stop (Run/Stop commands)

☐ Keywords command

☐ Read / Clear memory blocks

VISULOG allows an extensive Access rights configuration of the different modules and menu items. Below is an example of such configuration where only user 1 can create to a layer.



Users Group Definition

Designation: Group1

Unassigned Users:
- admin
- superuser

Assigned Users:
- user1

Group Members Rights

Application
- □ Exit VISULOG
- □ View the audit trail

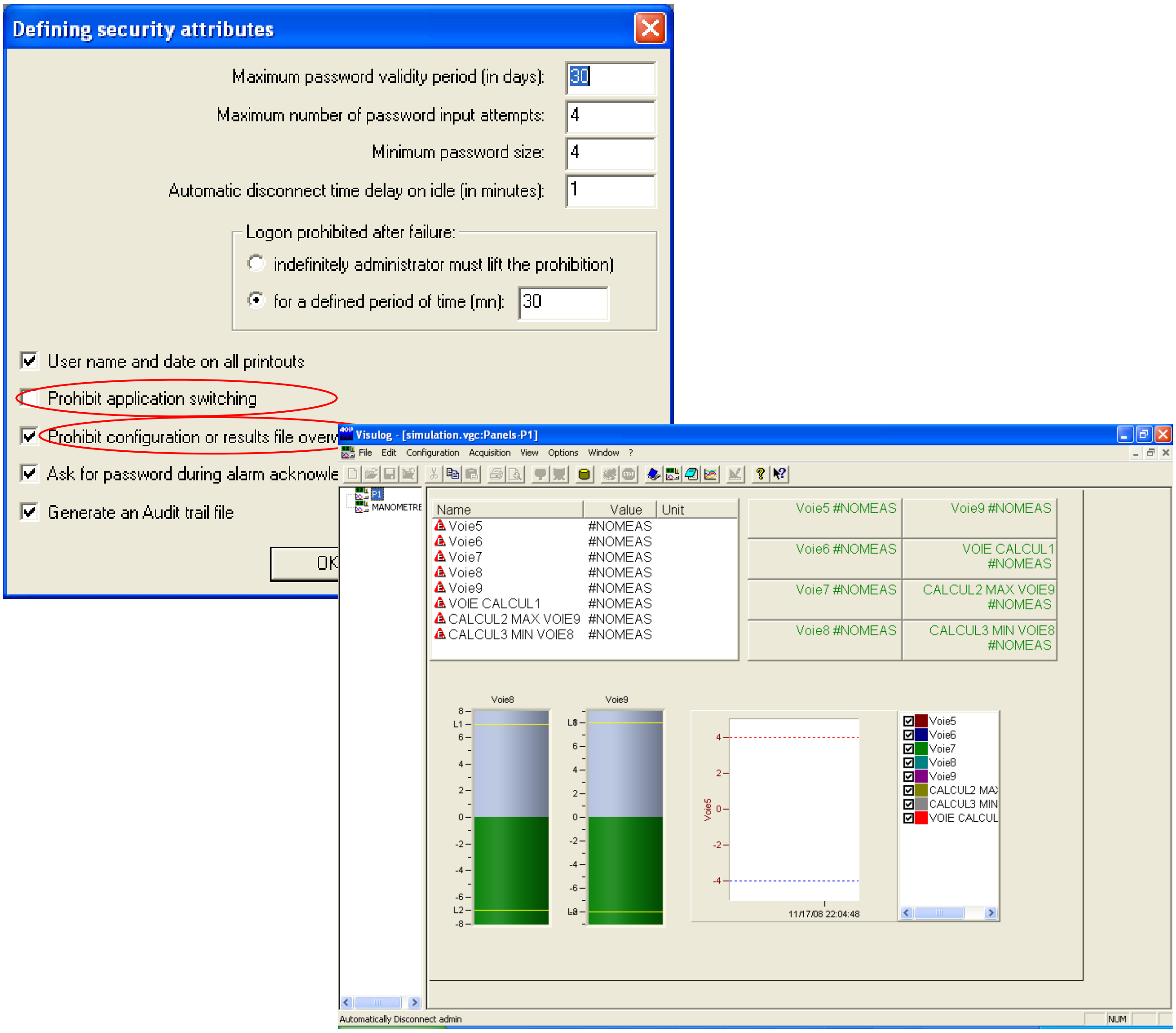
Documents
- □ Open
- □ Close
- □ Save
- □ Print
- ☑ Create control panels
- □ Export Data
- □ Write data to logs

Acquisition
- □ Launch acquisition with no command issued to the instruments
- □ Launch acquisition with instrument Run / Stop
- □ Launch acquisition with instrument Run / Stop and Programming
- □ Stop acquisition

Implementation of the access rights an Microsoft

Visulog internal user management system can be linked to directly interact with the Windows security system, thereby controlling the level of access for the user to the actual PC. This allows a user to have access only to VISULOG and no other programs that may be installed on the system.

The use of above feature is optional, general access limitation can also be achieved using Microsoft integrated User Management. If it is decide to implement the standard Microsoft user 's management mechanism for general access limitation, it remains the sole responsibility of the customer IT department to configure , manage and maintain these settings.



Defining security attributes

Maximum password validity period (in days): 30

Maximum number of password input attempts: 4

Minimum password size: 4

Automatic disconnect time delay on idle (in minutes): 1

Logon prohibited after failure:

○ indefinitely administrator must lift the prohibition)

● for a defined period of time (mn): 30

☑ User name and date on all printouts

☐ Prohibit application switching

☑ Prohibit configuration or results file overw

☑ Ask for password during alarm acknowle

☑ Generate an Audit trail file

Visulog - [simulation.vgc:Panels-P1]

Name	Value	Unit
Voie5	#NOMEAS	
Voie6	#NOMEAS	
Voie7	#NOMEAS	
Voie8	#NOMEAS	
Voie9	#NOMEAS	
VOIE CALCUL1	#NOMEAS	
CALCUL2 MAX VOIE9	#NOMEAS	
CALCUL3 MIN VOIE8	#NOMEAS	

Voie5 #NOMEAS

Voie9 #NOMEAS

Voie6 #NOMEAS

VOIE CALCUL1 #NOMEAS

Voie7 #NOMEAS

CALCUL2 MAX VOIE9 #NOMEAS

Voie8 #NOMEAS

CALCUL3 MIN VOIE8 #NOMEAS

Automatically Disconnect admin

FDA CFR PART 11 –Subpart A General Provisions

Sec §11;1 Scope

(a) The regulations in this part set forth the criteria under which the agency considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper.

(b) This part applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted, under any records requirements set forth in agency regulations. This part also applies to electronic records submitted to the agency under requirements of the Federal Food, Drug, and Cosmetic Act and the Public Health Service Act, even if such records are not specifically identified in agency regulations. However, this part does not apply to paper records that are, or have been, transmitted by electronic means.

(c) Where electronic signatures and their associated electronic records meet the requirements of this part, the agency will consider the electronic signatures to be equivalent to full handwritten signatures, initials, and other general signings as required by agency regulations, unless specifically excepted by regulation(s) effective on or after August 20 1997.

(d) Electronic records that meet the requirements of this part may be used in lieu of paper records, in accordance with § 11.2, unless paper records are specifically required.

(e) Computer systems (including hardware and software), controls, and attendant documentation maintained under this part shall be readily available for, and subject to, FDA inspection.

(f) This part does not apply to records required to be established or aminatanined by Sec. 1.326 through 1.68 of this chapter? Records that satisfy of part 1 subpart J of this chapter, but that also are required under either applicable statutory provisions or regulations, remain subject to this part.

Sec § 11.2 Implementation.

(a) For records required to be maintained but not submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that the requirements of this part are met.

(b) For records submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that:

(1) The requirements of this part are met; and

(2) The document or parts of a document to be submitted have been identified in public docket No. 92S– 0251 as being the type of submission the agency accepts in electronic form. This docket will identify specifically what types of documents or parts of documents are acceptable for submission in electronic form without paper records and the agency receiving unit(s) (e.g., specific center, office, division, branch) to which such submissions may be made. Documents to agency receiving unit(s) not specified in the public docket will not be considered as official if they are submitted in electronic form; paper forms of such documents will be considered as official and must accompany any electronic records. Persons are expected to consult with the intended agency receiving unit for details on how (e.g., method of transmission, media, file formats, and technical protocols) and whether to proceed with the electronic submission.

Sec § 11.3 Definitions.

(a) The definitions and interpretations of terms contained in section 201 of the act apply to those terms when used in this part.

(b) The following definitions of terms also apply to this part:
(1) Act means the Federal Food, Drug, and Cosmetic Act (secs. 201–903 (21 U.S.C. 321–393)).
(2) Agency means the Food and Drug Administration.
(3) Biometrics means a method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable.
(4) Closed system means an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.
(5) Digital signature means an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.
(6) Electronic record means 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.
(7) 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.
(8) Handwritten signature means the scripted name or legal mark of an individual handwritten by that individual and executed or adopted with the present intention to authenticate a writing in a permanent form. The act of signing with a writing or marking instrument such as a pen or stylus is preserved. The scripted name or legal mark, while conventionally applied to paper, may also be applied to other devices that capture the name or mark.
(9) Open system means an environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system.

FDA 21CFR PART11 Subpart B—Electronic Records

§ 11.10 Controls for closed systems.

Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:

(*a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.*

VISULOG COMPLIANCE: VISULOG provides all tools to generate, develop and maintain supervision and traceability projects.

The design and construction of any project by use of VISULOG, as well as the verification of its compliance with the FDA requirements and its final validation remain the sole responsibility of the project designer, system integrator and the customer.

(b) The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.
VISULOG COMPLIANCE:
VISULOG provides historical data points and historical alarms records in proprietary binary format.
VISULOG offers the ability to export data to a readable format such as any spreadsheet software. Using some virtual printing software, Visulog data reports can be printed out and stored in particular folders for an easy retrieval
VISULOG offers also the ability to print out data onto a virtual printer in order to create files under PDF format.

(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.
VISULOG COMPLIANCE: VISULOG historical data are stored in a binary proprietary format to avoid alteration and falsification.
However it remains the sole responsibility of the user to protect those files from being deleted, moved and renamed or from any other action which could harm the stored management to limit access right to these files.

(d) Limiting system access to authorized individuals.
VISULOG COMPLIANCE: VISULOG provides an advanced user management defining access rights to the project described in the chapter 1 of this document.
As required by FDA 21 CFR part 11 200.1, VISULOG employs two distinct identification components such as a unique combination of password and login.
Regarding general access limitations to the operating system, VISULOG provides an advanced user management which directly interacts with Microsoft Windows security mechanism this enabling the use of HMI project only.
The use of above features is optional, general access limitation can also be achieved using Microsoft's integrated user management. If it is decided to implement the standard Microsoft user management mechanism for general access limitation, it remains the sole responsibility of the customer's IT department to configure, manage and maintain these settings.

(e) Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.
VISULOG COMPLIANCE: When using VISULOG proprietary code format, there is no way to alter falsify, or delete a record of the historical data while VISULOG is running. However it remains the responsibility of the customer to protect those files from being corrupted, damaged , deleted, moved or renamed, or from any other action which harm the stored data.
In case of using, in parallel with proprietary files generated by Visulog,, an external ODBC compliant relational database, it is the sole responsibility of the customer

(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.
VISULOG COMPLIANCE: User and customer has to design its own using procedure. So it is the responsibility of the customer to use the desired system checks.

(g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.
VISULOG COMPLIANCE: Visulog provides an advanced user right management as described in chapter 1 of this document, defining access rights to the project. As required by FDA, Visulog employs two distinct identification components such as a unique combination of password and login.

(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.
VISULOG COMPLIANCE: No device can be used to determine the validity of the source of data input.

(i) Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.

VISULOG COMPLIANCE: Special training session can be performed BY AOIP technical staff to ensure education, of users.

Three steps training are delivered; Administrator stage, SUPER USER stage, and USER stage.

(j) The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.

VISULOG COMPLIANCE: Responsibility of the sole customer.

(k) Use of appropriate controls over systems documentation including:

(1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.

(2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.

VISULOG COMPLIANCE: Depending on the user level, the access to online documentation can be limited. Only the administrator can access to these documents. Audit trail is accessible according to the safety settings programmed by administrator.

Change control is the sole responsibility of the customer. However, last version of AOIP Visulog is always accessible by downloading from the website www.aoip.com.

§ 11.30 Controls for open systems.

Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in § 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.

VISULOG COMPLIANCE:

VISULOG is a closed system, and thus is not dealing with that chapter

§ 11.50 Signature manifestations.

(a) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:

(1) The printed name of the signer;

(2) The date and time when the signature was executed; and

(3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.

VISULOG COMPLIANCE: Signed electronic records such as events and alarms recorded in results files by Visulog are written with the name of the user who has acknowledged the event or alarm with the date and time stamp of the acknowledgment. In addition, VISULOG provides an Audit Trail to record time and date of the connection of the user who acknowledged the vent or alarm.

(b) The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).

VISULOG COMPLIANCE: The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of the section 11.50 A, a exportable to any software or can be printed to pdf files using virtual printer to give the ability to be human readable.

§ 11.70 Signature/record linking.

Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.

VISULOG COMPLIANCE:

All electronic signature are stored in proprietary format in a relational database. It is the sole responsibility of the user to forbid access to these database.

FDA 21 CFR PART 11 Subpart C—Electronic Signatures

§ 11.100 General requirements.

(a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.

VISULOG COMPLIANCE:All electronic signatures are composed by a combination of a unique set of login and password. It is the responsibility of the use not to give an existing set of login/password to other different operators

(b) Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.

VISULOG COMPLIANCE: The verification of the operator's identity before establishment or certification of an electronic signature is the responsibility of the customer.

(c) Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures.

VISULOG COMPLIANCE: this section remains the sole responsibility of the customer

(1) The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC–100), 5600 Fishers Lane, Rockville, MD 20857.

VISULOG COMPLIANCE: this section remains the sole responsibility of the customer

(2) Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.

VISULOG COMPLIANCE: this section remains the sole responsibility of the customer

§ 11.200 Electronic signature components and controls.

(a) Electronic signatures that are not based upon biometrics shall:

(1) Employ at least two distinct identification components such as an identification code and password.

VISULOG COMPLIANCE: All electronic signatures are composed by a combination of a unique set of login and password.

(i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual.

VISULOG COMPLIANCE: Visulog employs always a combination of a unique set of login and password.

(ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.

VISULOG COMPLIANCE: Visulog employs always a combination of a unique set of login and password

(2) Be used only by their genuine owners; and

VISULOG COMPLIANCE: verification and certification that a unique combination of identification components is not used by different individuals is the responsibility of the customer

(3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.

VISULOG COMPLIANCE: It is recommended that the customer shall prohibit the use of an individual's electronic signature by anyone either than its owner.

(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.

VISULOG COMPLIANCE: VISULOG does not use electronic signature based on biometrics.

§ 11.300 Controls for identification codes/ passwords.

Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:

(a) Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.
VISULOG COMPLIANCE: VISULOG user's management mechanism prohibits the coexistence of identical set of signature identification components

(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).
VISULOG COMPLIANCE: VISULOG user's management mechanism includes a configurable password ageing system to ensure the periodical checking, recalling and changing of the identification password.

(c) Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.
VISULOG COMPLIANCE: VISULOG user's management mechanism

(d) Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.
VISULOG COMPLIANCE: VISULOG user's management mechanism includes a system to prohibits any connexion after a certain number of attempts with invalid set of login/password

(e) Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.
VISULOG COMPLIANCE: VISULOG does not necessit any device such as token or card.