



FDA 21 CFR PART 11

An ICONICS Whitepaper

CONTENTS

1	ABOUT THIS DOCUMENT	1
1.1	SCOPE OF THE DOCUMENT	1
1.2	REVISION HISTORY	1
1.3	DEFINITIONS	1
2	INTRODUCTION	2
2.1	DEFINITION	2
2.2	QUICK SYNOPSIS OF REGULATION	2
2.3	INDUSTRIES AFFECTED	2
2.4	BENEFITS	3
3	REQUIREMENTS	4
3.1	SCOPE	4
3.2	RETENTION	5
3.3	ACCESS	6
3.4	AUDIT TRAILS	7
3.5	SEQUENCING CHECKS	10
3.6	REVISION CONTROLS	11
3.7	SIGNATURE MANIFESTATIONS	12
	ALARM ACKNOWLEDGEMENT	13
3.8	ELECTRONIC SIGNATURES	14
3.9	TIME-OUTS	15
3.10	BIOMETRICS AND IDENTITY ASSURANCE MANAGEMENT	16
3.10.1	<i>Native Support for Biometric Devices</i>	17
3.11	PASSWORD REVISIONS	18
3.12	UNAUTHORIZED DETECTION	19

1 About This Document

1.1 Scope of the Document

This document contains information on the features of several GENESIS32 components that may be of use to companies wishing to comply with FDA 21 CFR Part 11. An overview of this regulation and a summary of how it relates to the GENESIS32 product family are presented.

The intended audience includes engineers working on implementing solutions to meet this regulation; sales and marketing personnel desiring to gain an understanding of the issues and product features addressing those issues; and end users looking for information on using GENESIS32 in an FDA-regulated environment.

It should be noted that, as with many Federal Regulations, specific details and interpretation of scope and applicability of any given section or subsection is left to the individual companies. The FDA wishes to be flexible in meeting needs in the interest of public health. As such, there may be more than one view on a specific regulation, and/or the extent to which it applies to a specific operation.

This document does NOT pretend to provide direct interpretation and guidance on applying regulations for any specific purpose. Rather, this document points out various sections of the regulations and makes the reader aware of various features in the GENESIS32 product family that may be of interest in meeting the requirements of these regulations. This document serves as a guide to, not an absolute dictation of, deployment direction. With this in mind, it is hoped that this document will prove useful in understanding some of the benefits of the features offered by ICONICS.

1.2 Revision History

- Version 1.0 - BB, March 8, 2001 (initial release)
- Version 1.02 – BB, March 22, 2001 (added screen snapshots, edited)
- Version 1.03 - BB, Sept 6, 2001 (edited, updated to reflect GENESIS32 6.1 release)
- Version 8.0 - RLA, August 6, 2004 (edited, updated to reflect GENESIS32 8.0 release)
- Version 9.0 - RLA, July, 2006 (edited, updated to reflect GENESIS32 9 release)

1.3 Definitions

The following are acronyms used in this document, and are presented here for reference.

- FDA - Food and Drug Administration
- CFR - Code of Federal Regulations
- cGMPs - Current Good Manufacturing Practices
- HMI - Human Machine Interface
- SCADA - Supervisory Control and Data Acquisition
- OPC - OLE for Process Control
- ADO - ActiveX Data Object
- OleDb - OLE Database
- VBA - Visual Basic for Applications

2 Introduction

2.1 Definition

There has been a heightened awareness lately of what is called "21CFR11," or "FDA 21 CFR Part 11". First, let's define the two titles above.

FDA is the acronym for the Food and Drug Administration. Part of the US Department of Health and Human Services, FDA was established to serve and protect the interests of public health.

CFR stands for Code of Federal Regulations and refers to a (very large) document listing United States Federal Regulations.

The number "21" actually is short for "Title 21, Chapter I," and the number "11," for "Part 11". These are pointers to help reference the specific section of the CFR where this regulation can be found. More specifically, Title 21 concerns the area of Food and Drugs, Chapter I is the section related to FDA, and Part 11 is the sub-section of this chapter, which focuses on a specific area (i.e., Electronic Records; Electronic Signatures) which this document now covers.

So, the full title is truly:

"Code of Federal Regulations: Food and Drug Administration Title 21, Chapter I, Part 11 - Electronic Records; Electronic Signatures"

It is apparent why it is simply referred to as: "21 CFR 11".

2.2 Quick Synopsis of Regulation

Understand it is not possible to encapsulate the entire breadth of this regulation in a simple overview. However, a cursory understanding in the beginning is helpful for getting started in reviewing this document. So, a brief overview of this regulation is as follows:

Many FDA regulations, written well before the proliferation of computer systems, require handwritten signatures. In light of the new technologies available, there has been a demand to "go electronic". Part 11 covers the proper handling of recording FDA-regulated information electronically and applying "electronic signatures," such that they are considered by the FDA to be "equivalent" to that of handwritten signatures and documents.

2.3 Industries Affected

This Regulation affects companies that have their processes already regulated by the FDA. Examples include:

- Drug, Pharmaceutical Companies
- The Beverage Industry
- Blood Handling Processes
- Medical Device Manufacturing
- Food Processing Plants
- Cosmetic Manufacturers
- And more ...

It should be noted that any activities regulated by this ruling are entirely voluntary. As stated in the Federal Register: "No entity is required by this rule to maintain or submit records electronically if it does not wish to do so."

Although not mandated, many companies have elected to comply with this regulation because doing so offers significant benefits, as outlined in the next section.

2.4 Benefits

The costs of not switching over to electronic record-keeping and associated electronic signatures are too great for many in the affected industries to ignore. By switching to electronic solutions, companies expect to benefit in many ways. Section XVI, C.1. of the Federal Register discussing 21CFR11 lists the following, reproduced here for easy reference:

- Improved ability for the firm to analyze trends, problems, etc., enhancing internal evaluation and quality control
- Reduced data entry errors, due to automated checks
- Reduced costs of storage space
- Reduced shipping costs for data transmission to FDA
- More efficient FDA reviews and approvals of FDA-regulated products

Section III, A.1. also offers, as benefits:

- Manufacturing processing streamlining
- Increased speed of information exchange
- Product improvement
- Enabling of more advanced searches of information, thus obviating the need for manual paper searches
- Improved process control
- Multiple perspective views of information
- Avoidance of document misfiling from human error
- And more ...

These and other benefits greatly outweigh any associated costs of implementing 21CFR11 for many organizations. As such, there is now great interest in fulfilling the requirements outlined in this regulation.

ICONICS is here to help. For more information visit our WEB site at www.iconics.com or contact your local ICONICS representative.

3 Requirements

The following sections outline the requirements.

3.1 Scope

As of this writing (it is suggested that here, and throughout this document, references to 21CFR11 text be ultimately verified against any revisions to this regulation by reviewing the document available on the FDA's Web site, www.fda.gov), the opening section of Part 11 is as follows:

11.1 (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.

11.1 (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.

There are other sub-sections (c, d, e), but not necessary here with respect to this white paper's coverage.

The many sub-sections that follow relate to GENESIS32. They can be summarized as dealing with Operator Event Tracking (operator set-point changes & alarm acknowledgments), and its associated security tie-ins, to ensure the "electronic signature" of the responsible operator is used appropriately for acceptance by the FDA when such signatures are required.

GENESIS32 components are ready to assist in satisfying these FDA requirements. Presented here are "pointers" to features in our products that may be of interest. Products explored include:

- GraphWorX32**
- GenEvent Server**
- Security Configurator**
- Security Server**
- AlarmWorX32 Viewer ActiveX**
- AlarmWorX32 Historical Alarm Report ActiveX**
- AlarmWorX32 Logger**

The extent to which the items outlined in the remainder of this document apply to a given situation is ultimately up to each individual company.

3.2 Retention

Part 11 mentions the following:

11.10 (c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.

This requirement has raised several issues, including:

What about hardware and software upgrade issues?

Must companies keep antiquated systems operational throughout the period?

Are the costs of maintaining these old systems too great, and are they justified?

How can converting to newer systems in the future be handled?

These questions are very important and have great impact when using a data logging system that is designed around proprietary logging files and closed systems.

The good news is that the ICONICS Alarm and Event Logger does NOT use a proprietary database which would be subject to the above issues. Instead, it uses standard databases that enjoy a history of conversion and compatibility. Users may elect to log to:

Microsoft Access

Microsoft SQL Server

Oracle

MSDE (Microsoft Data Engine)

By using such standards as ADO and OLEDB, GENESIS32 systems can be set up to log process alarms and events, operator set-point changes and other events directly to secure corporate databases.

This facilitates an easy path for long-term maintenance as required by the FDA.

3.3 Access

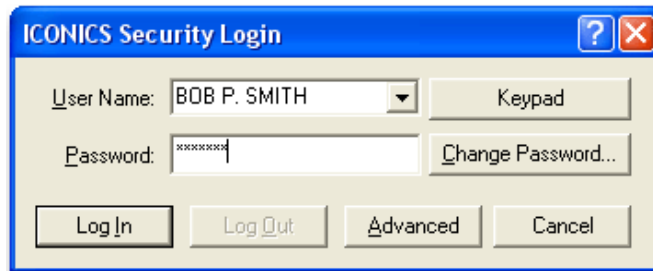
Part 11 mentions the following:

11.10 (d) Limiting system access to authorized individuals.

and

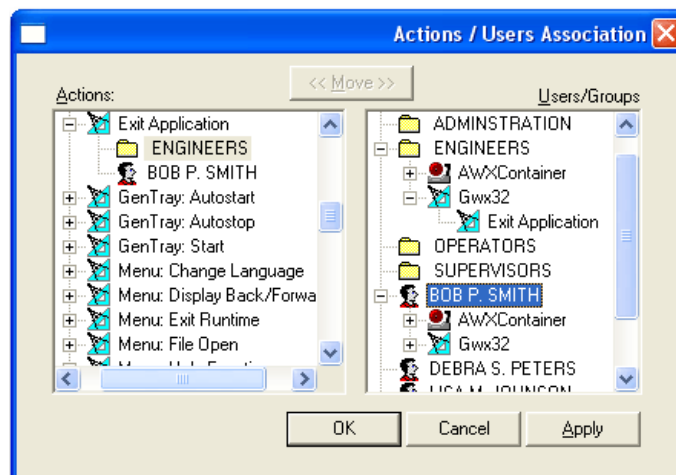
11.200 (a) (1) Employ at least two distinct identification components such as an identification code and password.

GENESIS32 has a component in its suite of applications called the Security Server. The various clients of GENESIS32 (e.g., GraphWorX32 for HMI visualizations, TrendWorX32 for data logging and trending, AlarmWorX32 for alarm monitoring) tie into this security server. When users are asked to log in, they are prompted for a User Name and Password, as shown below:



Security Log-in Dialog Box

Actions and access are restricted based on configuration. Individual and/or group access to components, sub-components, and actions within the GENESIS32 system are defined via the ICONICS Security Configurator. The following illustration shows a portion of this utility, whereby the system administrator can assign various actions. Further details on this utility are covered elsewhere in this document as it relates to other sections of Part 11. For now, be aware that 11.10(d) ties into the features of this powerful ICONICS component.



Security Server Configuration of Action Restrictions

One additional note: this Security Server is not limited just to NT, as may be discovered with other systems. Our component works on Windows, XP, XP Sp2, 2000, Windows 2003 Server, Windows 2003 Server R2, Windows SP 64, Windows 2003 Server 64. It also works on systems deployed across a local area network and/or the Internet. It offers system-wide security for ICONICS components.

3.4 Audit Trails

Part 11 mentions the following:

11.10 (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.

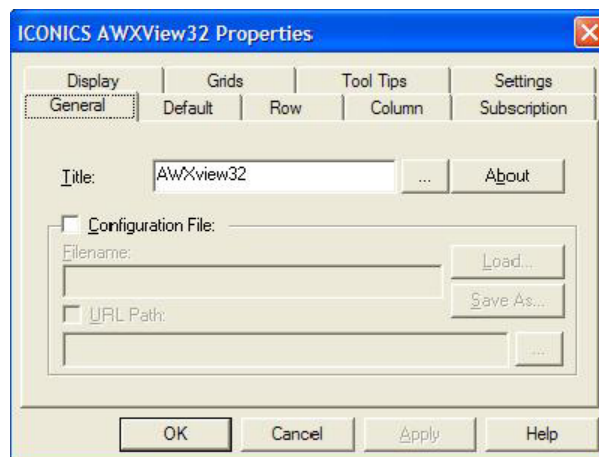
There are two product features ICONICS supplies to help address the requirement that we'll now discuss.

GENESIS32 systems come with what is called the GenEvent Server. Its purpose is to post "events" to the alarm system. This captures such items as people logging into the system, log-out (and auto-log-out) actions, application startup messages, and--more directly related to 11.10(e)--captures operator set-point changes.

Whenever a user enters in a value in GraphWorX32 (e.g., via a Data Entry PPT, slider action, dial, push button, etc.), the date & time stamp is captured along with the name of the person performing the action, as well as the value entered and the tag name being affected. GenEvent Server also captures the node name if it occurs on a networked set of systems, thus recording information pertaining to who, what, when and where.

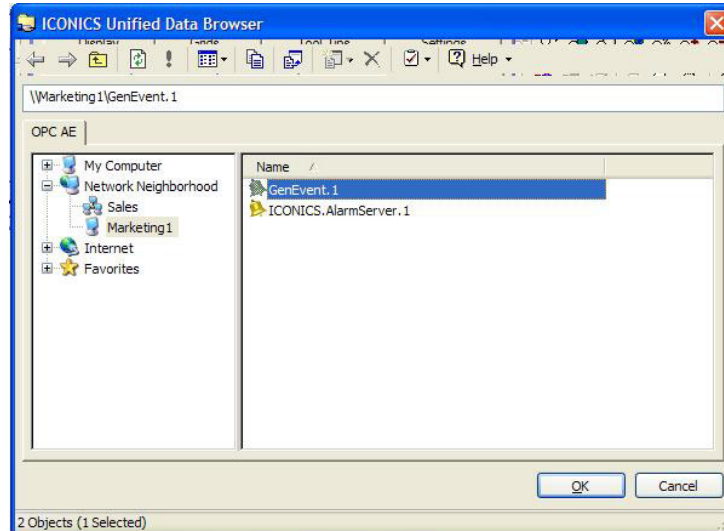
This information is presented as OPC Alarm and Event information to OPC A&E client applications.

For example, these records can be posted to the live Alarm Viewer ActiveX so operators can view the events within an HMI screen. In GENESIS32 6.0, the Alarm Viewer ActiveX must add a Subscription to this GenEvent Server, as shown below:



GenEvent Server Subscription

The link to the specific OPC Alarm and Event server is defined by pressing the Edit button and then pressing the Browse button, thereby bringing up our OPC Universal Tag Browser, as shown in the following illustration.



Unified Data Browser showing GenEvent Server

Beginning with GENESIS32 6.1, whenever a new Alarm Viewer ActiveX is first created, it reads in the "default.awv" file (located in the BIN directory) for initial setup parameters. The subscription to the GenEvent server, along with configurations for showing the Node and operator "Comments" field, is already pre-configured, making it plug-n-play for design engineers.

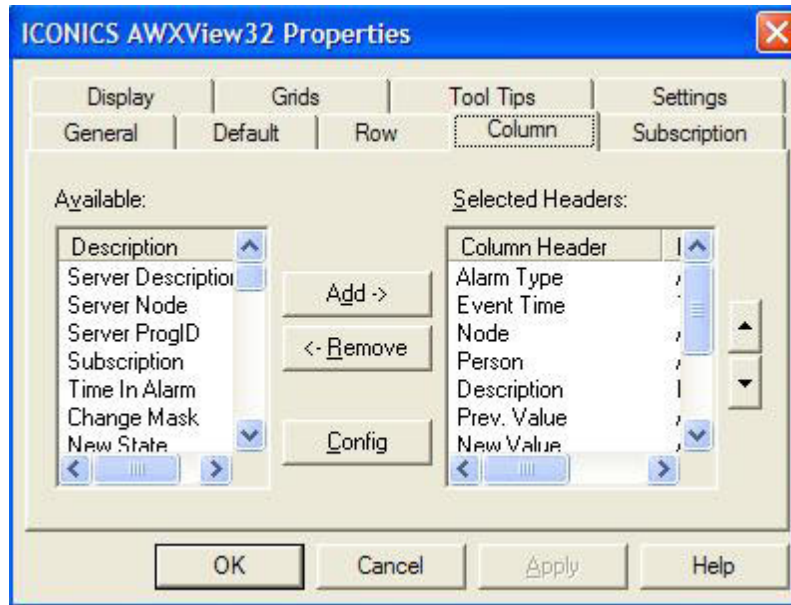
Below is an example of an Alarm Viewer ActiveX showing such tracking events. Notice how it shows the date and time of the event, the node from which the change was made, the person's name making the change (this should be wider to show both the first and last name of the operator), a description of which tag was change and the new value entered, and the application from which the change occurred.

Event Time	Node	Person	Description	Source
11:30:39:789 AM	9/6/2001 GATE20		User RUSS JONES has been automatically logged out from station GAT	Security Serv
11:25:48:199 AM	9/6/2001 GATE20	RUSS JONES	Wrote new value (1) to ICONICS.Simulator.1\SimulatePLC.OUTPUTS.BIT	GraphWorX32
11:25:36:863 AM	9/6/2001 GATE20		User BOB SMITH has logged out from station GATE2000	Security Serv
11:25:36:863 AM	9/6/2001 GATE20		User RUSS JONES has logged in from station GATE2000	Security Serv
11:25:23:544 AM	9/6/2001 GATE20	BOB SMITH	Wrote new value (0) to ICONICS.Simulator.1\SimulatePLC.OUTPUTS.BIT	GraphWorX32
11:25:22:933 AM	9/6/2001 GATE20	BOB SMITH	Wrote new value (1) to ICONICS.Simulator.1\SimulatePLC.OUTPUTS.BIT	GraphWorX32
11:25:20:770 AM	9/6/2001 GATE20	BOB SMITH	Wrote new value (36) to ICONICS.Simulator.1\SimulatePLC.OUTPUTS.FL	GraphWorX32
11:25:17:095 AM	9/6/2001 GATE20	BOB SMITH	Wrote new value (15) to ICONICS.Simulator.1\SimulatePLC.OUTPUTS.FL	GraphWorX32
11:25:13:930 AM	9/6/2001 GATE20	BOB SMITH	Wrote new value (0) to ICONICS.Simulator.1\SimulatePLC.OUTPUTS.BIT	GraphWorX32
11:25:12:718 AM	9/6/2001 GATE20	BOB SMITH	Wrote new value (69) to ICONICS.Simulator.1\SimulatePLC.OUTPUTS.FL	GraphWorX32
11:25:10:305 AM	9/6/2001 GATE20	BOB SMITH	Wrote new value (1) to ICONICS.Simulator.1\SimulatePLC.OUTPUTS.BIT	GraphWorX32
11:25:08:042 AM	9/6/2001 GATE20	BOB SMITH	Wrote new value (59) to ICONICS.Simulator.1\SimulatePLC.OUTPUTS.FL	GraphWorX32
11:25:04:677 AM	9/6/2001 GATE20	BOB SMITH	Wrote new value (0) to ICONICS.Simulator.1\SimulatePLC.OUTPUTS.BIT	GraphWorX32

Alarm Viewer ActiveX Showing Operator Tracking Events

By default, the person's name is not pre-configured to be shown. In order to have this appear, as shown in column three in the above example, be sure to show the field "ActorID", which is the internal OPC Alarm and Event field containing this information.

A snapshot of the column definitions used in the above viewer example is shown in the following illustration.



Alarm Viewer ActiveX Column Definitions

In addition to viewing these events live, the ICONICS Alarm Logger can be used to log the tracking information to a secure database. Be sure it has the same subscription to the GenEvent Server, and that the appropriate fields are configured to be logged and printed.

The other aspect of Audit Trails mentioned in the "discussion section" of the FDA document outlines Alarm Acknowledgment. ICONICS also records the time & date stamp and operator information for these events. Additional discussion on this topic is presented later in this document under the chapter "Alarm Acknowledgement".

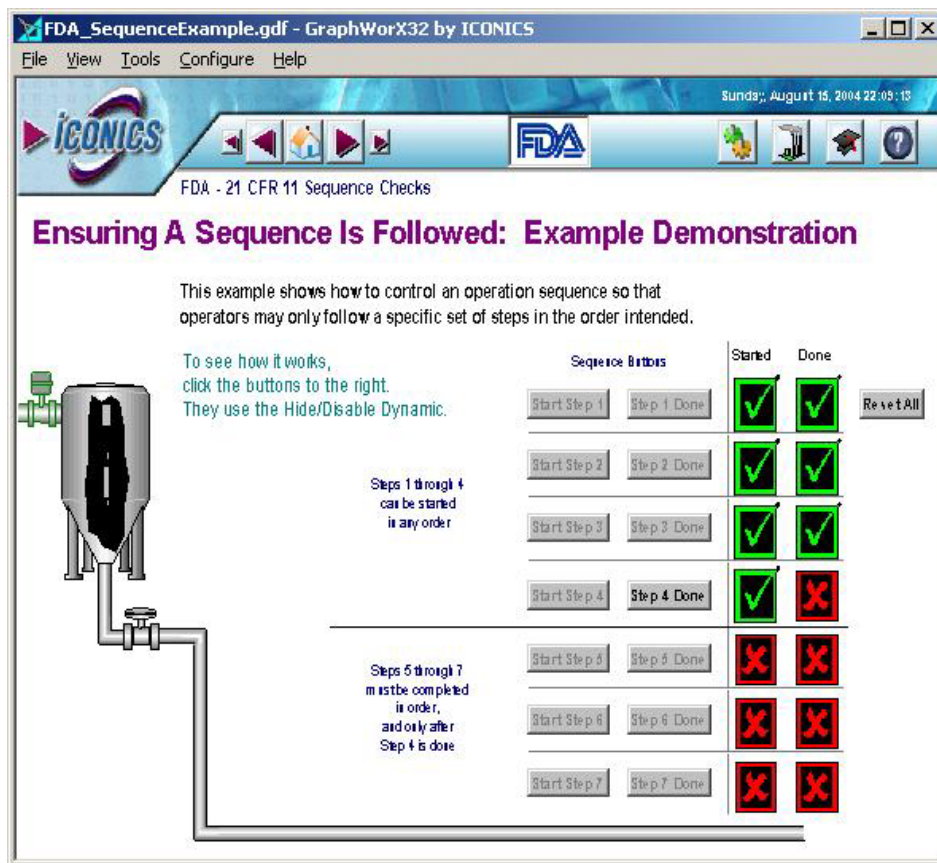
3.5 Sequencing Checks

11.10 (f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.

First, a note that the "as appropriate" phrase at the end of the sentence indicates this is not a requirement for ALL companies wishing to comply with 21CFR11, but rather only those having a pre-defined sequence of events which operators must follow in order to comply with an FDA regulation or other cGMPs, and which must be memorialized as records.

Within GraphWorX32, the HMI package in GENESIS32, there are several features that help facilitate such control over a sequence of "write" operations. Although using VBA scripts is one possibility, there is another direct and simpler approach: using Disable Dynamics tied to Expressions.

An example of this approach is included in our 6.1 Version of the Gen32Demo. The file is called GWX_EX_Sequence.gdf, a screen snapshot of which is shown below:



Sequencing Example in the Gen32Demo

Basically, this example shows how easy it is to disable functions, entry fields, and the like using the Disable/Hide Dynamic. This feature forces the operators to follow a predefined set of steps in the order originally intended.

For further details on this and other features that enable sequencing checks, please consult the Gen32Demo and/or talk to your regional manager.

3.6 Revision Controls

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

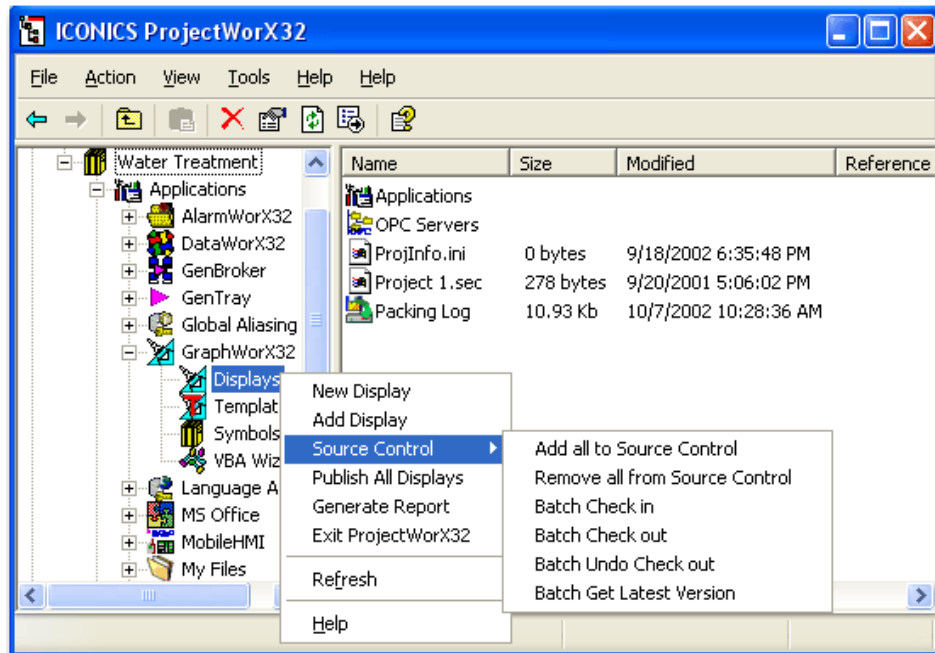
- (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.*
- (2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.*

These relate in many respects to controls and procedures put in place by the company and are outside the realm of GENESIS32 direct control.

There are, however, several interesting features worth pointing out in GENESIS32. ICONICS incorporates the latest Project tracking technology taking maximum advantage of Microsoft Source Safe and configuration management tools to create detailed reports of any engineering or configuration change.

If the GraphWorX32 displays are considered part of the "system documentation" (e.g., a recipe entry screen, with instructions), then they must somehow fit in with 11.10(k). All of the displays used by the HMI component GraphWorX32 are stored as separate documents (each display corresponds to a *.gdf file). This includes the graphics and dynamics as well as any VBA scripts employed within the graphic. They can, therefore, easily tie into "Revision Control" software employed by companies for the rest of the documents being tracked.

The same holds true for configuration files for Alarming, Trending, Reports, and so on.



Project tracking, Configuration Management in GENESIS32 ProjectWorX32

3.7 Signature Manifestations

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.*

(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).

As stated in Section 3.4 of this document, the ICONICS GenEvent server does take care of recording the name, date, time and meaning of the actions already discussed. Further points specific to this regulation are in order:

In (1) above, concerning the "printed name": it is important that it is not just "Joe," but rather "Joe K. Smith," the person's full name as required to give a legal signature to a document. As such, when setting up the user names in the ICONICS Security Configurator, make sure that users are defined using their full names.

When logging the events to a database, and when viewing the event information either via the Alarm Viewer ActiveX or the Alarm Report ActiveX, be sure to include the appropriate columns. For example, it is the "ActorID" field that contains the user's name.



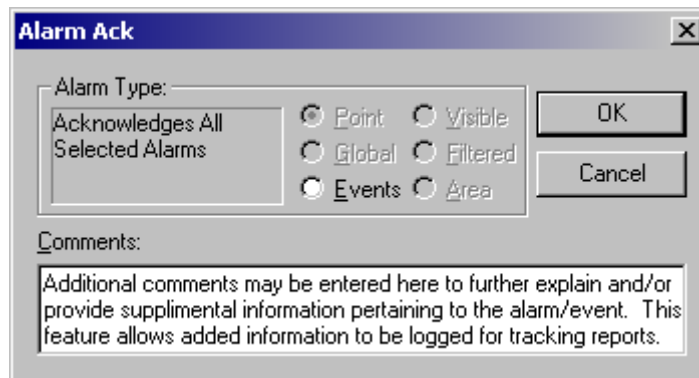
User Login Failure Message

Alarm Acknowledgement

One point concerning alarm acknowledgement: it has been concluded that since the system attaches the fact that it is an "Ack" event, the "meaning" is in fact logged and thus meets 11.50(a)(3) mentioned in the preceding section.

Indeed, the FDA states in its explanation area, "Recording the meaning of the signature does not infer that the signer's credentials or other lengthy explanations be part of that meaning."

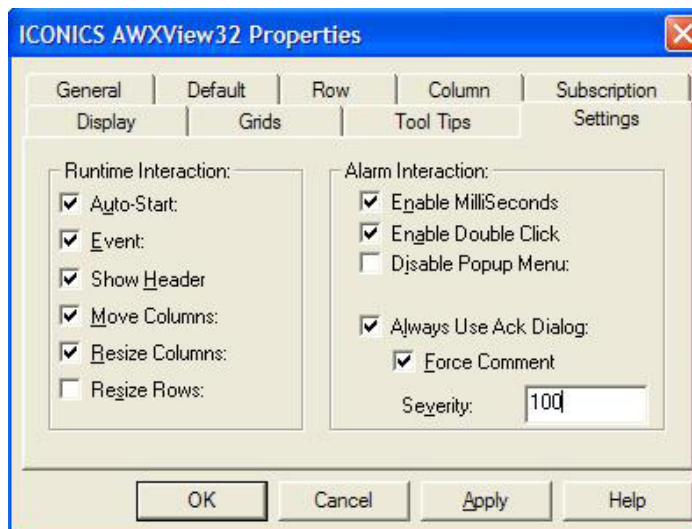
However, should operators wish to attach additional comments to an Alarm Acknowledgment event and provide such "lengthy explanations" to supplement the audit trail, the Alarm Viewer ActiveX does offer the chance to type in additional comments. These comments may be entered when the alarm/event is acknowledged for the first time. An example of this dialog is shown below:



Alarm/Event Acknowledgment Operator Comments

Operator comments are then propagated along with the Ack Event throughout the alarm system. This permits them to be viewed on other alarm stations in a networked environment, and so that they may be stored to a database by the alarm logger.

An additional feature has been added to GENESIS32 V6.1, which FORCES operators to enter a comment with each and every Alarm Acknowledgment, should a company determine this is required for their operation.



FDA Force Comment Option

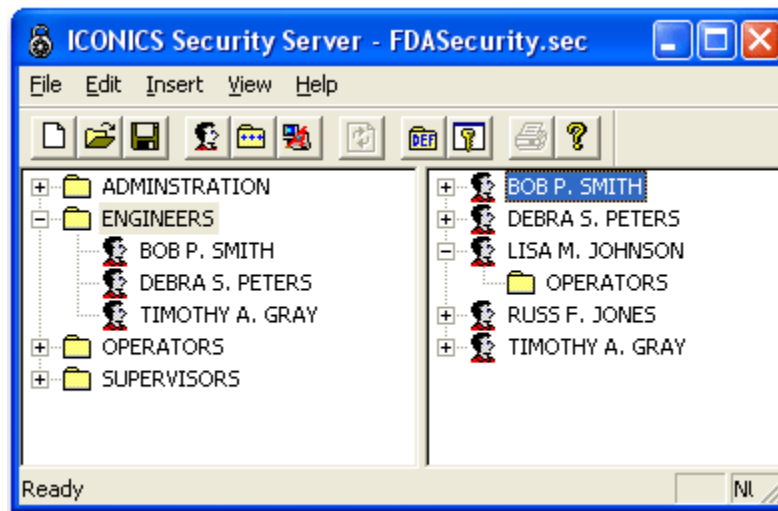
3.8 Electronic Signatures

11.100 (a) Each electronic signature shall be unique to one individual and shall not be re-used by, or re-assigned to, anyone else.

and

11.300 (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.

The ICONICS Security Server Configurator already enforces unique User Names, thereby ensuring a unique combination of User Name and Password (which the FDA then counts as an Electronic Signature). The screen snapshot below shows the configurator with full user names entered (as mentioned in the previous section).



Security Names are Unique in GENESIS32

This regulation also requires that names are not re-used by, or re-assigned to, anyone else. So, names created within the ICONICS Security Server can be left defined. If someone should leave the company or otherwise no longer be authorized to use the system, there is one other feature that comes in handy: **Account Disabled**, as shown in the dialog box at the top of page 16. Simply check the box and this account will no longer be active. Yet it will remain in the system for unique checking to prevent it from being used again.



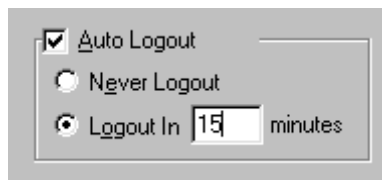
Account Disabled So It Cannot Be Re-used or Re-assigned

3.9 Time-outs

Concerning 11.200, the FDA in its comments in the Federal Register states (XII.124):

"The agency acknowledges that there are some situations involving repetitive signings in which it may not be necessary for an individual to execute each component of a non-biometric electronic signature for every signing." . . . "For example, an individual performs an initial system access or "log on," which is effectively the first signing, by executing all components of the electronic signature (typically both an identification code and a password)." . . . "... it is vital to have stringent controls in place to prevent the impersonation. Such controls include: (1) Requiring an individual to remain in close proximity to the workstation throughout the signing session; (2) use of automatic inactivity disconnect measures that would "de-log" the first individual if no entries or actions were taken within a fixed short timeframe; and (3) requiring that the single component needed for subsequent signings be known to, and usable only by, the authorized individual. "

Regarding (2) above, ICONICS has implemented an Auto Log-out feature that may be enabled on a per-individual basis. The amount of time during which each person may be logged in before being forced to re-enter his/her user name and password can be entered via the Security Configurator, a section of which is shown below.



Auto Log-out Feature in GENESIS32 Security Configurator

The amount of time entered to meet the relative term "fixed short-time frame" is up to each application. As an additional detail about this feature, whenever the user is close to being logged out, a Reminder Window appears, as shown below. This allows the user either to disregard this warning (by pressing the **Dismiss** button), postpone the warning for now (by pressing the **Postpone** button, which is similar to a Snooze button on an alarm clock), or re-logging in (by pressing the **Log-in Now** button).



Auto Log-out Reminder

Though not necessarily a requirement for any FDA regulation, this feature makes systems that must comply with the requirements a bit friendlier for users to work with.

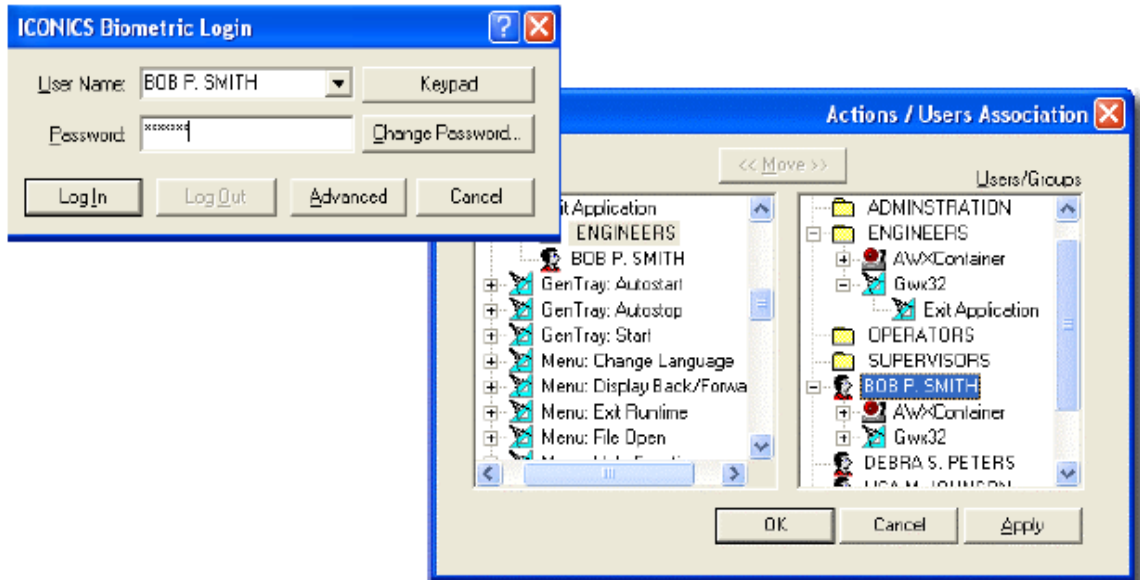
3.10 Biometrics and Identity Assurance Management

In various places in 21CFR11, there are mentions of using Biometrics in place of someone typing in a User Name and Password: for example, a "Retina Scan" or "Fingerprint Reader" to identify the individual. While use of these elaborate systems is not mandated by the Regulation (user name and password suffice), we recognize that some companies may be interested in pursuing the use of these technologies.

As such, ICONICS has made OLE Automation calls available for such product tie-ins to our Security Server. It is possible, for example, to make a function call (e.g., in C++, VBA, etc.) to log a person into the system. If you would like further information on linking into our system, please contact our Technical Support Department, or refer to the OLE Automation references provided with the product.

3.10.1 Native Support for Biometric Devices

ICONICS supports native biometric devices and interfaces, providing deep level support for greater identity assurance management. The ICONICS security servers now support biometric devices. The integration of biometrics provides maximum security for user identification and provides added authentication for FDA regulated applications.

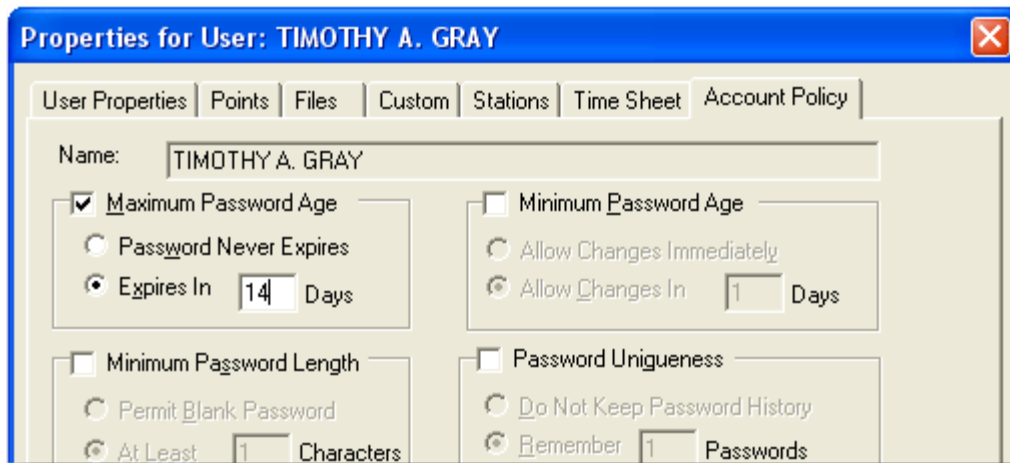


Biometric Login Dialogs for GENESIS32

3.11 Password Revisions

11.300 (b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).

ICONICS has implemented a "Maximum Password Age" feature in its Security Server. The number of days for recalling a password to be revised may be entered on a per-individual basis. A section of the screen snapshot is shown below:



Password Age in GENESIS32 Security Configurator

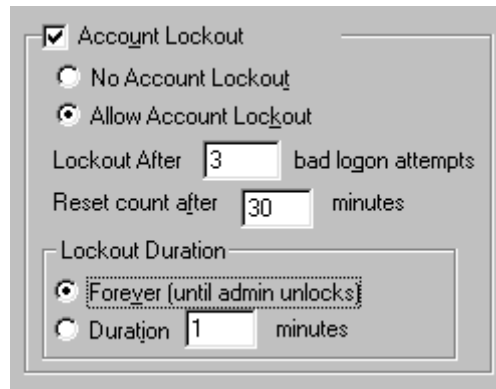


Re-entering Aged Passwords Dialog from GENESIS32 Security Configurator

3.12 Unauthorized Detection

11.300 (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.

The GENESIS32 Security Configurator offers an "Account Lockout" feature that addresses detection of attempting to "hack" into the system. On a per-individual basis, you may configure how many attempts is sufficient to warrant a lockout, when it should reset the count, and whether the lockout itself resets after a period of time or whether the Administrator of the security system must re-enable the account. A snapshot of this portion of the configuration screen is shown below.



Unauthorized Access Safeguard Parameters in GENESIS32 Security Configurator

In addition to locking out the account, the GenEvent Server captures this attempted breach in security and posts this event. This message, in turn, can be logged to disk by the Alarm Logger, as well as shown on a security or administrator station using the Alarm/Event ActiveX Viewer.

Event Time	Node	Description
11:54:52:327 AM 9/6/2001	GATE2	User BOB SMITH has been locked out the the Security System after 3 bad login attempts.

Unauthorized Access Event Posted to Viewe



VISIT US AT WWW.ICONICS.COM

Visualize Your Enterprise™

ICONICS World Headquarters

100 Foxborough Blvd.
Foxborough, MA 02035
Tel: 508 543 8600
Fax: 508 543 1503
Email: info@iconics.com

ICONICS Europe

Czech Republic

Tel: 420 37 718 3420
Fax: 420 37 718 3424
Email: czech@iconics.com

ICONICS Asia

Australia

Tel: 61 297 273 411
Fax: 61 297 273 422
Email: australia@iconics.com

ICONICS UK

United Kingdom

Tel: 44 1384 246 700
Fax: 44 1384 246 701
Email: info@iconics-uk.com

France

Tel: 33 45 019 1180
Fax: 33 45 001 0870
Email: france@iconics.com

China

Tel: 86 130 684 86069
Email: china@iconics.com

Germany

Tel: 49 2241 16 508 0
Fax: 49 2241 16 508 12
Email: germany@iconics.com

Italy

Tel: 39 010 46 0626
Fax: 39 010 65 22 187
Email: italy@iconics.com

Netherlands

Tel: 31 252 228 588
Fax: 31 252 226 240
Email: holland@iconics.com

India

Tel: 91 22 67291029
Fax: 91 22 67291001
Email: india@iconics.com



WHY CHOOSE ICONICS?

ICONICS, Inc. is a leading provider of award-winning enterprise Manufacturing intelligence and automation software solutions and implementation services. ICONICS solutions deliver real-time visibility into all enterprise operations and systems, helping companies to be more profitable, more agile and more efficient. ICONICS products have delivered value within over 250,000 installations worldwide and have been chosen by more than 70% of the Fortune 1000.

