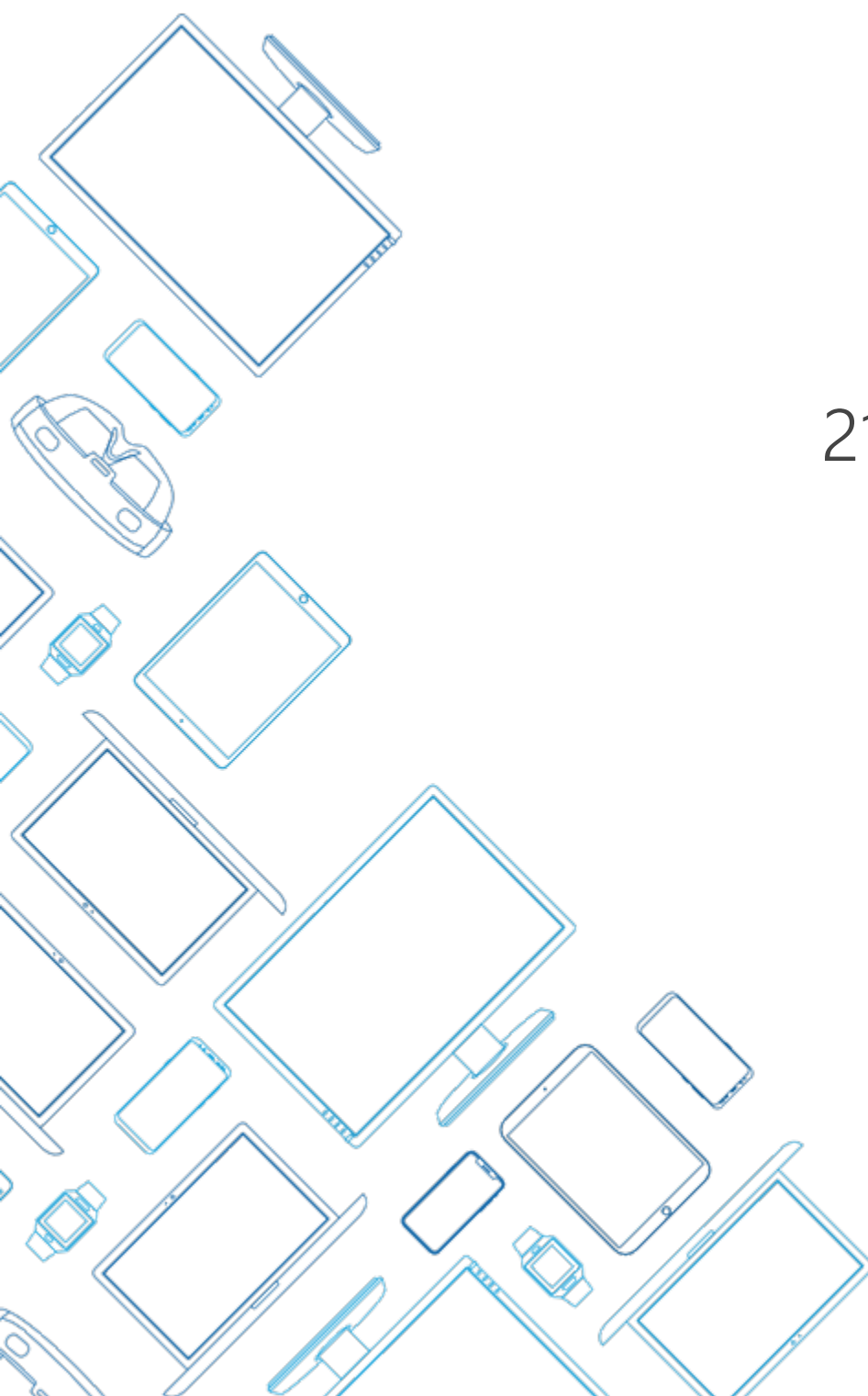




Make the Invisible Visible™



GENESIS64 FDA 21CFR11 Capabilities

An ICONICS Whitepaper
February 2023

CONTENTS

Table of Contents

1.1 Scope of the Document	2
1.2 Revision History	2
1.3 Definitions.....	2
2 Introductions.....	4
2.1 Definition	4
2.2 Quick Synopsis of Regulation	4
2.3 Industries Affected.....	4
2.4 Benefits	5
3 Requirements.....	6
3.1 Scope.....	6
3.2 Retention	7
3.3 Access.....	7
3.4 Audit Trails	9
3.5 Sequencing Checks.....	12
3.6 Revision Controls	14
3.7 Signature Manifestations.....	15
3.8 Alarm Acknowledgement.....	16
3.9 Electronic Signatures.....	18
3.10 Time-outs	20
3.11 Biometrics and Identity Assurance Management.....	21
3.11.1 Native Support for Biometric Devices.....	21
3.12 Password Revisions	21
3.13 Unauthorized Detection.....	22

1 About This Document

1.1 Scope of the Document

This document contains information on the features of several GENESIS64 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 GENESIS64 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 GENESIS64 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 GENESIS64 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 – DG – Prepared by Dharmesh Gohel, March 25, 2011 (ICONICS INDIA)

Version 2.0 – AB – Reviewed by Amit Bharadva, (ICONICS INDIA)

Version 3.0 – AP – Reviewed by Alexander Pinkham, (ICONICS)

Version 4.0 – TD – Reviewed and edited by Tim Donaldson (ICONICS) October 2011

Version 5.0 – AP – Reviewed and edited by Alexander Pinkham (ICONICS) October 2015

Version 6.0 – DO – Reviewed and edited by Dave Oravetz (ICONICS) February 2023

1.3 Definitions

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

- 21CFR11 – FDA Title 21 CFR Part 11
- A&E – Alarms and Events
- Ack – Acknowledge
- CFR – Code of Federal Regulations
- cGMPs – Current Good Manufacturing Practices
- FDA – Food and Drug Administration
- HMI – Human Machine Interface
- MFA – Multi-Factor Authentication

- OLEDB – OLE Database
- OPC – Open Platform Communications
- SAML – Security Assertion Markup Language
- SCADA - Supervisory Control and Data Acquisition
- PPT – Process Point Display Field in GraphWorX64

2 Introductions

2.1 Definition

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

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

CFR stands for Code of Federal Regulations and refers to an (extremely long) document listing United States Federal Regulations.

The number "21" 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, and Chapter I is the section related to FDA. 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:

"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 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 these 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 these are not necessary with respect to this white paper's coverage.

The many sub-sections that follow can be associated with the ICONICS solution GENESIS64. These can be summarized as dealing with Operator Event Tracking (operator set-point changes and 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.

GENESIS64 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:

- **GraphWorX64**
- **GenEvent Server**
- **Security Configurator**
- **Security Server**
- **Hyper Alarm Logger**
- **AlarmWorX64 Viewer**
- **AlarmWorX64 Historical Alarm Report**
- **AlarmWorX64 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 the 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 extremely important and have significant 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 Loggers do NOT use proprietary databases which would be subject to the above issues. Instead, these use standard databases that enjoy a history of conversion and compatibility. Users may elect to log to:

- AlarmWorX64 Logger – which uses Microsoft SQL Server, or
- Hyper Alarm Logger – which uses SQLite

By using such standard databases, GENESIS64 systems can be set up to log process alarms and events, operator set-point changes, and other events directly to secure corporate databases using the AlarmWorX64 Logger or indirectly (via its export capability) using the Hyper Alarm Logger and its exporting capabilities.

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

3.3 Access

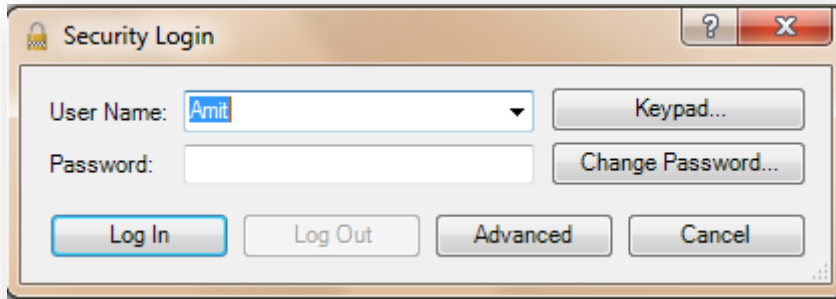
Part 11 mentions the following:

11.10 (d) Limiting system access to authorized individuals.

and

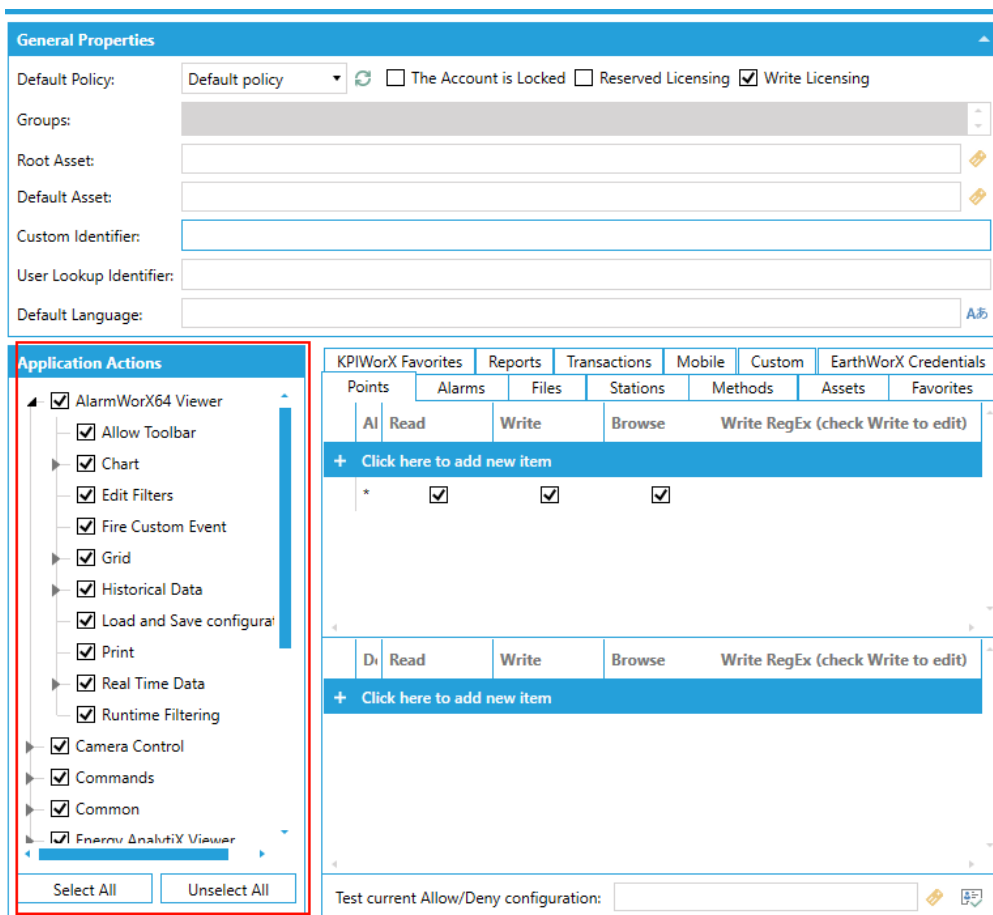
11.200 (a) (1) Employ at least two distinct identification components such as an identification code and password.

GENESIS64 has a component in its suite of applications called the Security Server. The various clients of GENESIS64 (e.g., GraphWorX64 for HMI visualizations, TrendWorX64 for data logging and trending, and AlarmWorX64 for alarm monitoring) tie into this security server. When users are asked to log in, they are prompted for a Username and Password, as shown in the following image.



Security Login Dialog Box

Actions and access are restricted based on configuration. Individual and/or group access to components, sub-components, and actions within the GENESIS64 system are defined via the ICONICS Security Configurator in the Workbench. The following image 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

3.4 Audit Trails

Part 11 mentions the following:

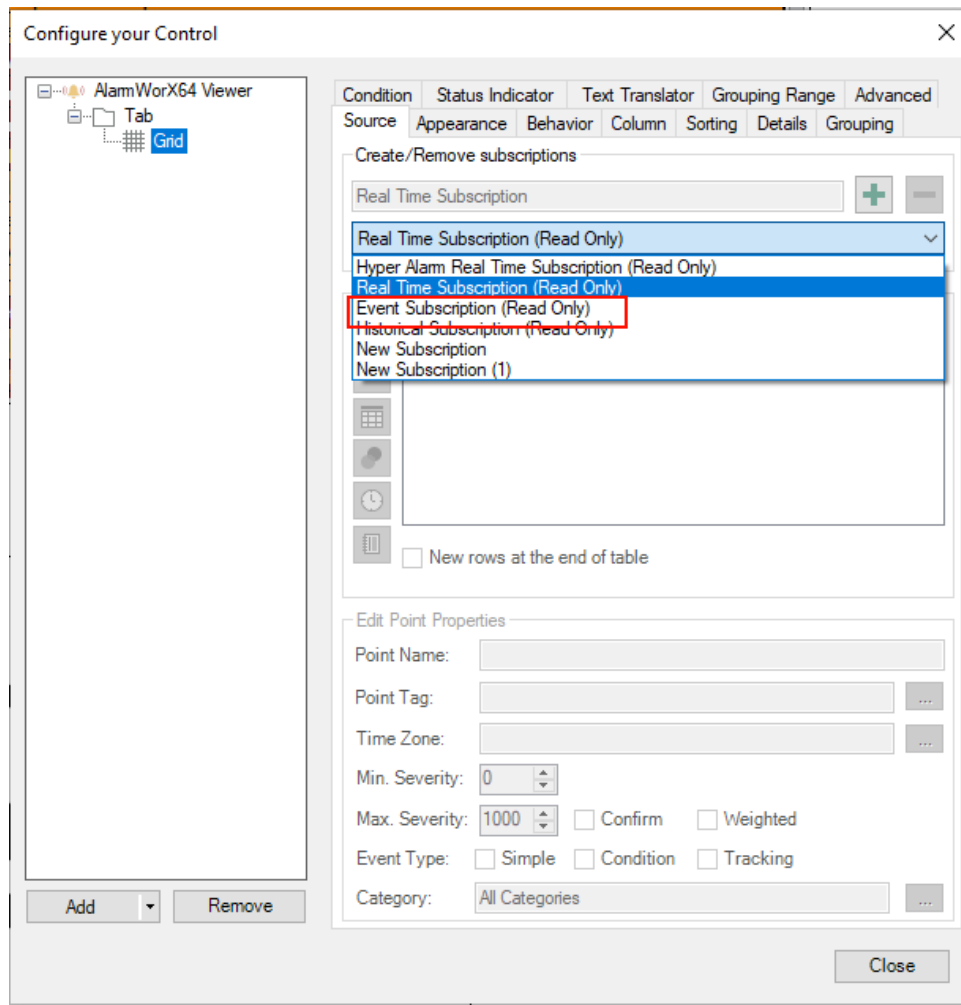
11.10 (e) Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be 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.

Two ICONICS product features that help address the requirement will be discussed now. GENESIS64 systems come with what is called the GenEvent Server. Its purpose is to post "events" to the alarm system. This feature captures items such as people logging into the system, log-out (and auto-log-out) actions, application start up messages and, more directly related to 11.10(e), operator set-point changes.

Whenever a user enters in a value in GraphWorX64 (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 whom, what, when and where.

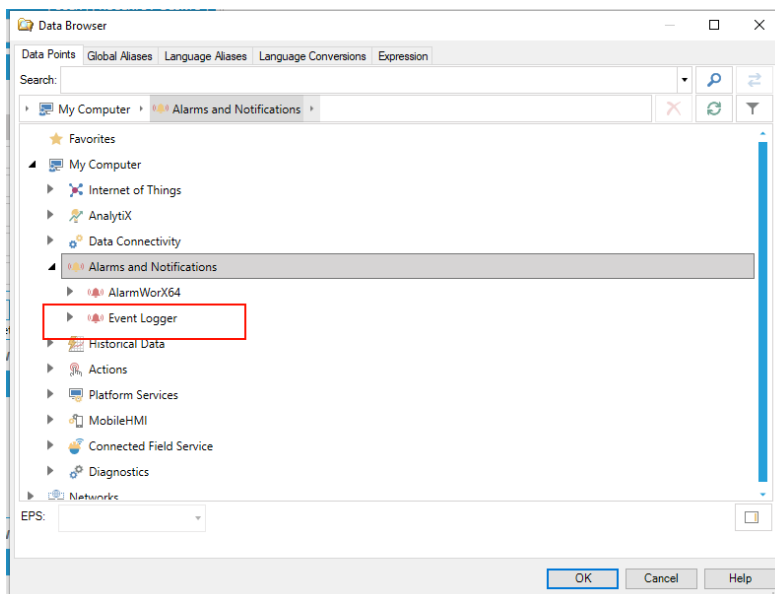
This information is presented as OPC Alarm and Event information to OPC A&E client applications.

For example, these records can be posted to the live AlarmWorX64 Viewer, so operators can view the events within an HMI screen. In GENESIS64, the AlarmWorX64 Viewer must add a Subscription to this GenEvent Server, as shown in the following image.



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 the Data Browser, as shown in the following image.



Data Browser Showing GenEvent Server

In GENESIS64, whenever a new AlarmWorX64 Viewer is first created, it is set up with default connections to the local Hyper Alarm Server, AlarmWorX64 Server, AlarmWorX64 Logger and GenEvent Server.

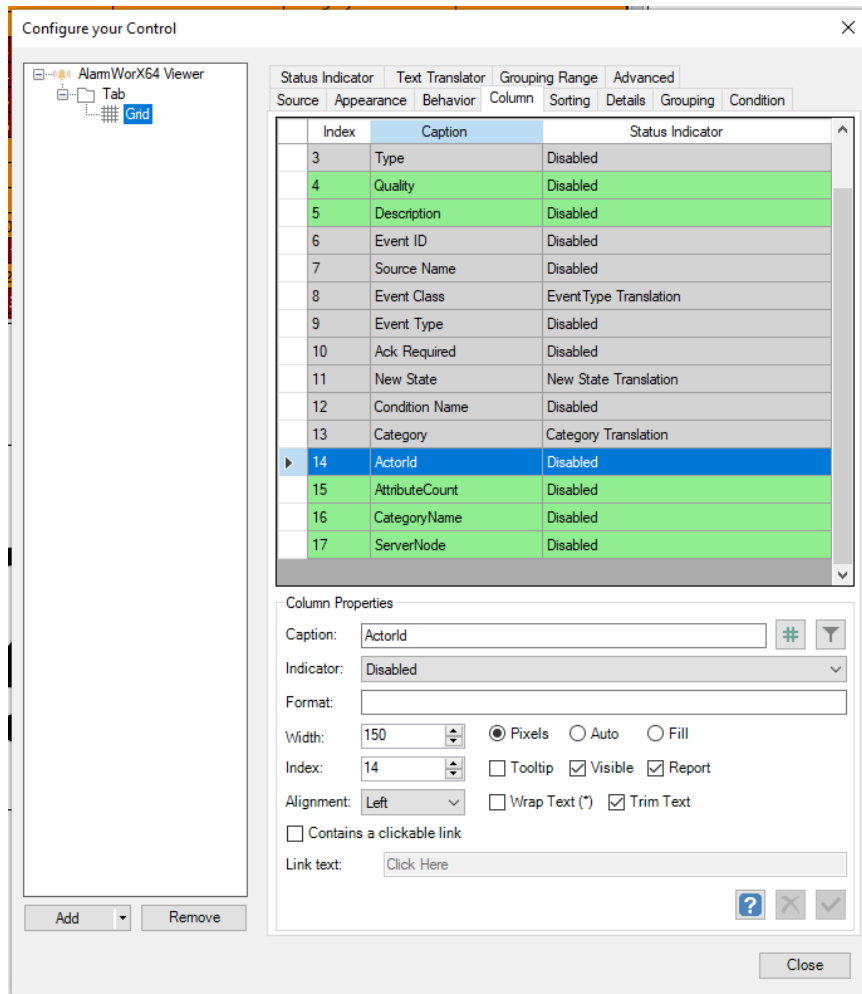
Below is an example of an AlarmWorX64 Viewer showing such tracking events. Notice how it shows the date and time of the event. Configurable options include a description of which tag was changed, the new value entered, and the application from which the change occurred.

Time / Date	Tag	Priority	Quality	Description
2/13/2023 6:46 PM	GraphWorX64	600	Good	Successfully wrote value 1 to @sim64:Double.Static("Static1").Value
2/13/2023 6:46 PM	GraphWorX64	600	Good	Successfully wrote value 5 to @sim64:Double.Static("Static1").Value
2/13/2023 6:46 PM	AWXLog64	500	Good	ICONICS AlarmWorX64 Logger Stopped.
2/13/2023 6:46 PM		600	Good	AWXLog64.exe connected to OPC AE server: ICONICS.GenEvent.1 on node:...
2/13/2023 6:46 PM		600	Good	AWXLog64.exe connected to OPC AE server: ICONICS.GenEvent.1 on node: Robertov-...
2/13/2023 6:46 PM		600	Good	AWXLog64.exe connected to OPC AE server: ICONICS.AlarmSvr.1 on node: 10.60.0.157,...
2/13/2023 6:46 PM		600	Good	AWXLog64.exe connected to OPC AE server: ICONICS.AlarmSvr.1 on node: Robertov-...
2/13/2023 6:46 PM	AWXLog64	500	Good	License Enabled
2/13/2023 6:46 PM	AWXLog64	500	Good	ICONICS AlarmWorX64 Logger Started.
2/13/2023 6:45 PM	GraphWorX64	600	Good	Successfully wrote value 2 to @sim64:Double.Static("Static1").Value
2/13/2023 6:45 PM	GraphWorX64	600	Good	Successfully wrote value 5 to @sim64:Double.Static("Static1").Value
2/13/2023 6:45 PM	FrameWorX64 Server	600	Good	User "John Doe" logged in

AlarmWorX64 Viewer Showing Operator Tracking Events

By default, the person's name is not pre-configured to be shown. In order to have this appear, be sure to show the field "Attribute1" which is the default 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.



AlarmWorX64 Viewer 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".

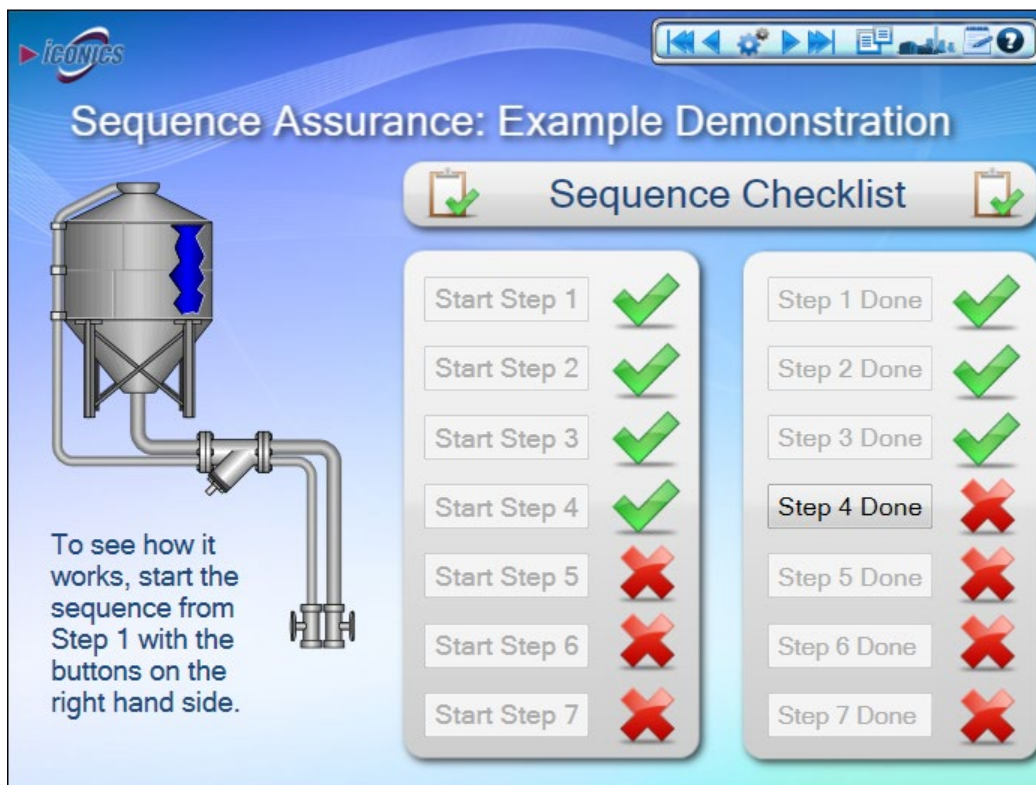
3.5 Sequencing Checks

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 kept as records.

Within GraphWorX64, one possibility for implementing a pre-defined sequence of events is to use Jscript.NET scripts. However, there is another direct and simpler approach for facilitating control over a sequence of "write" operations available in both GraphWorX64 and MobileHMI: use Disable Dynamics tied to Expressions. Disabling and enabling buttons allow control over the process. In the example below, only the next step is "allowed."



Sequencing Example in the Gen64Demo

This example shows how easy it is to disable functions, entry fields, and the like using the Disable/Hide Dynamic. This feature forces 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 your regional manager.

3.6 Revision Controls

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

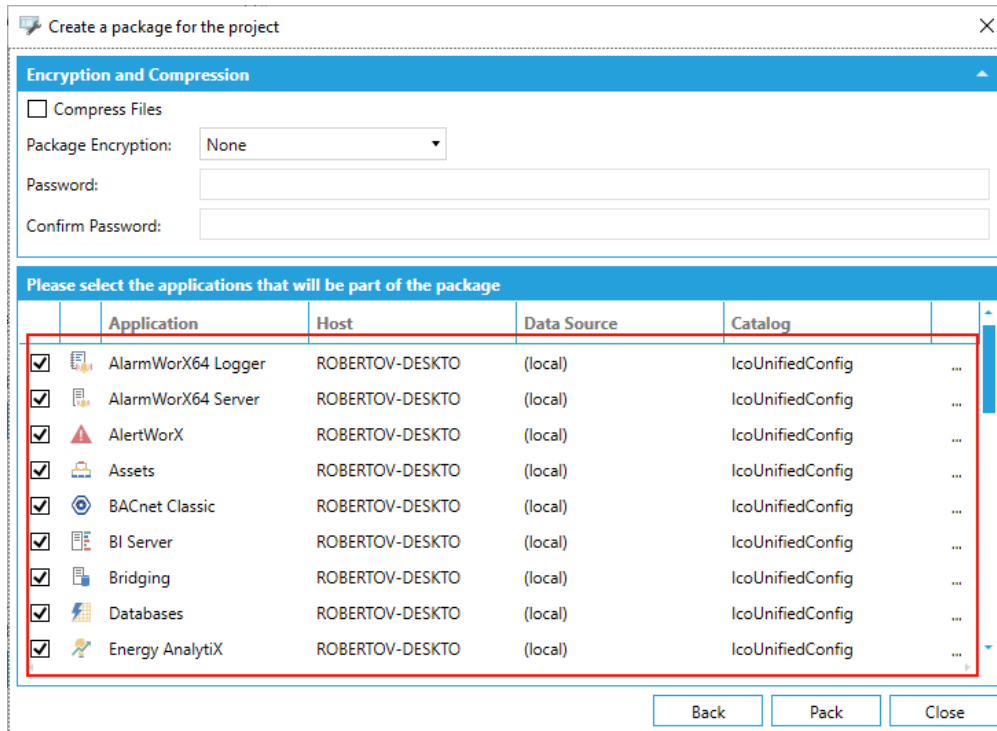
(1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.

(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 GENESIS64's direct control.

There are, however, several interesting features worth pointing out in GENESIS64. ICONICS incorporates the latest project tracking technology, taking maximum advantage of configuration management tools to create detailed reports of any engineering or configuration change. In Workbench there is the Audit Log. Audit Log allows tracking of all changes to the system (changes to configuration databases, changes to configuration files, and changes to the states of services). For each change, the following information is logged: the user who performed the change, a short human readable description of the change, and a JSON object that contains all the changes. It is possible to see the log in Workbench by opening the Audit Log Viewer. The Audit Log can be disabled (if the user is allowed via Security Settings) but by default is enabled after the installation. Each change is also sent as a classic OPC Event via GenEvent.

If the GraphWorX64 displays are considered part of the "system documentation" (e.g., a recipe entry screen with instructions), then these must somehow fit in with 11.10(k). All of the displays used by the HMI component, GraphWorX64, are stored as separate documents (each display corresponds to a *.gdfx file). This includes the graphics and dynamics as well as any scripts (JScript.NET) employed within the graphics. These 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 GENESIS64 ProjectWorX64

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.*

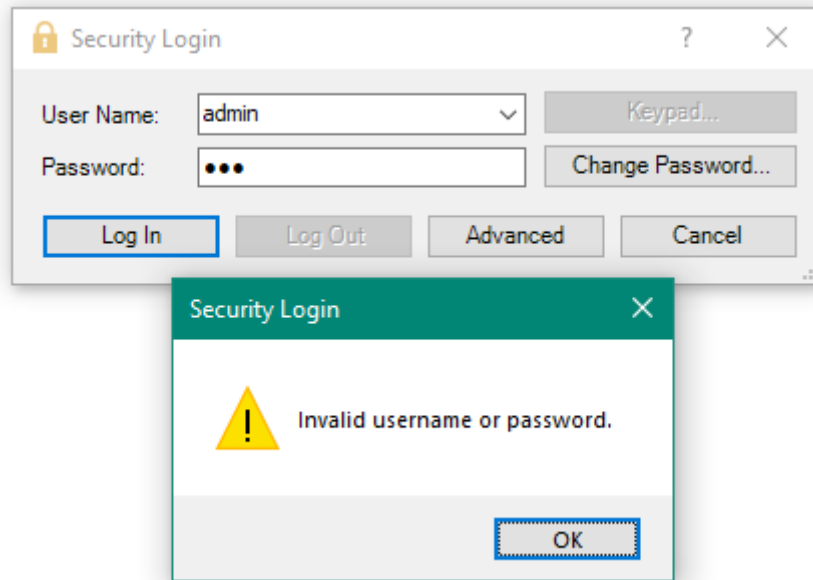
(b) The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).

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 is required to give a legal signature to a document. As

such, when setting up the usernames 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 AlarmWorX64 Viewer or the Alarm Reporting, be sure to include the appropriate columns. For example, it is the "Attribute1" field that contains the user's name.



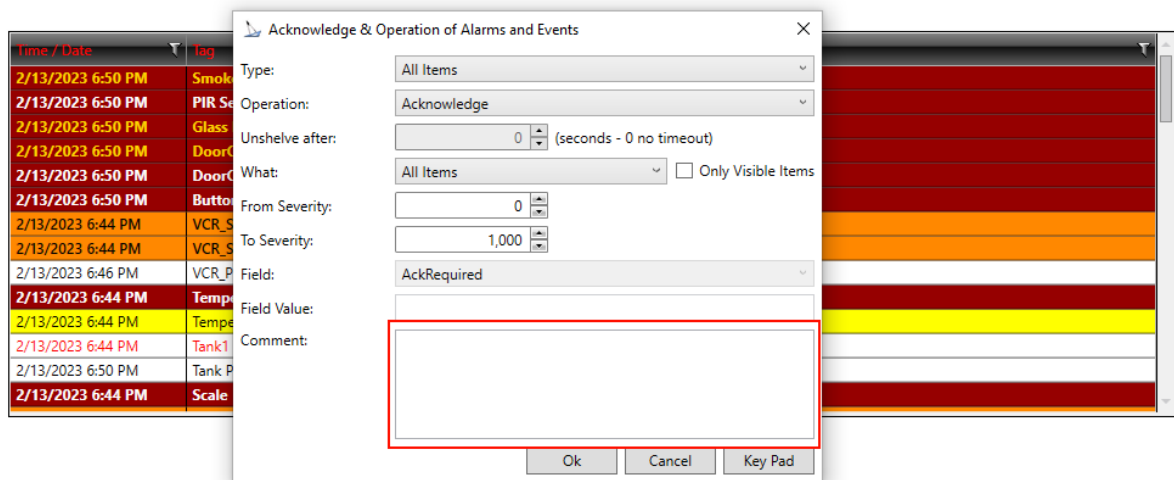
User Login Failure Message

3.8 Alarm Acknowledgement

One point concerning alarm acknowledgment: 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."

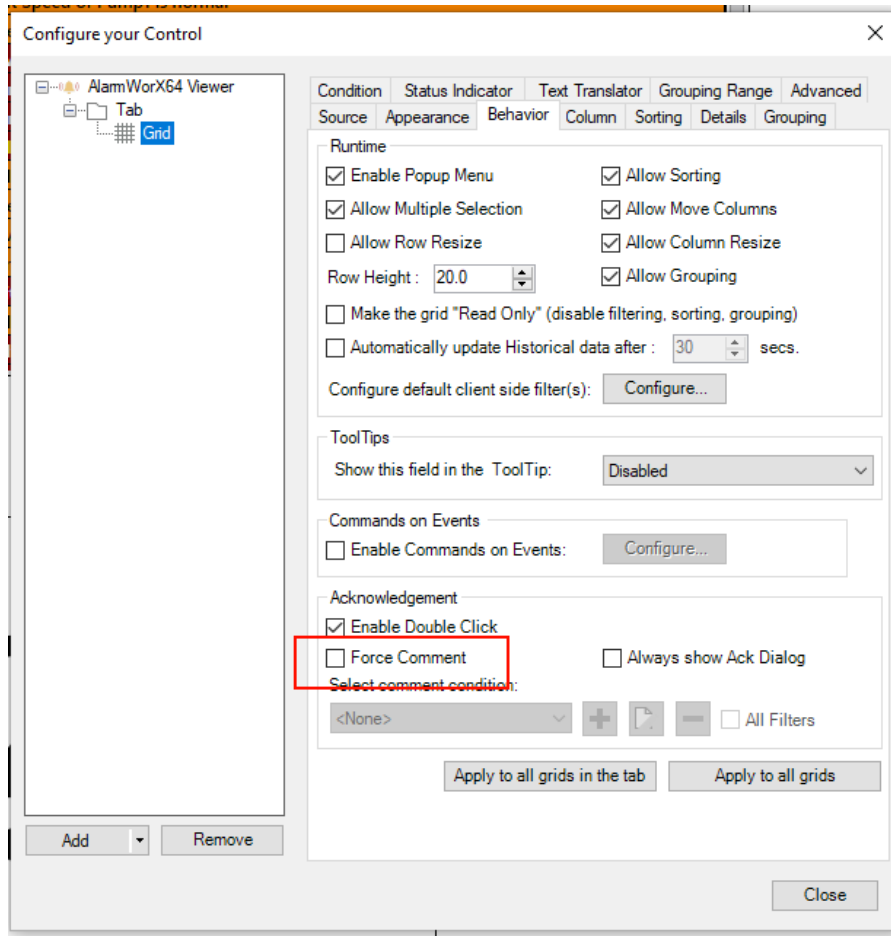
However, should operators wish to attach additional comments to an Alarm Acknowledgment event and provide such "lengthy explanations" to supplement the audit trail, the AlarmWorX64 Viewer does offer the chance to type in additional comments. These comments may be entered when the alarm/event is acknowledged 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 these to be viewed on other alarm stations in a networked environment so that these may be stored to a database by the alarm logger.

An additional optional feature in GENESIS64 may be used to FORCE operators to enter a comment with every Alarm Acknowledgment, should a company determine this is required for their operation.



FDA Force Comment Option

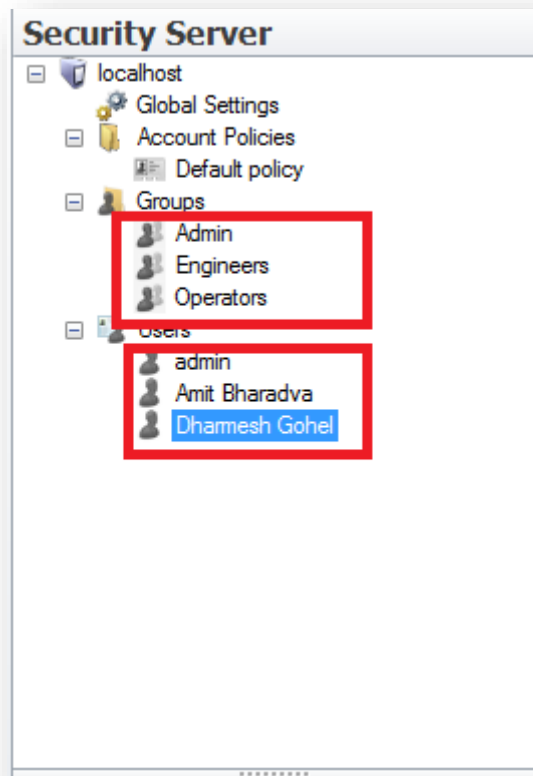
3.9 Electronic Signatures

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

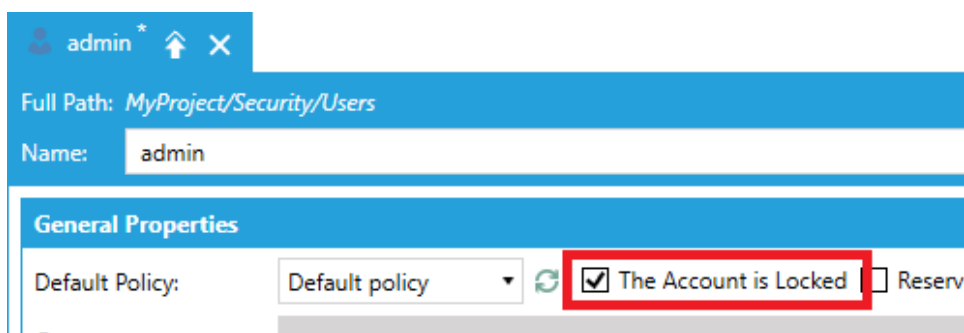
11.300 (a) Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.

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



Security Names Are Unique in GENESIS64

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 Locked**, as shown in the dialog box below. 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.



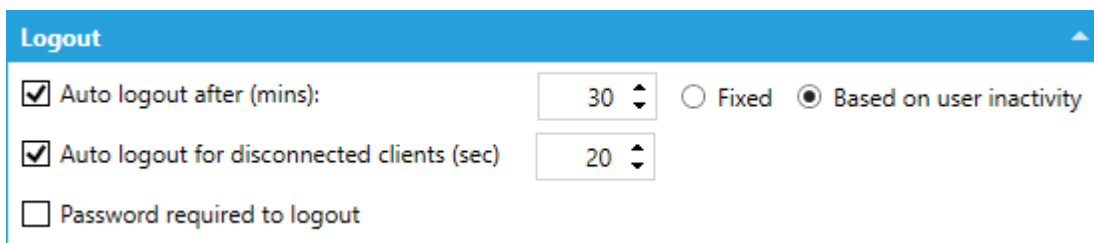
Account Locked So It Cannot Be Re-used or Re-assigned

3.10 Time-outs

Concerning 11.200, in its comments in the Federal Register the FDA 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 Logout 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 username and password can be entered via the Security Configurator, a section of which is shown below.



Auto Logout Feature in GENESIS64 Security Configurator

The amount of time entered to meet the relative term "fixed short-time frame" is up to each application. The Auto Logout feature is based on "idle time", and thus users will never be logged out during operations. If the machine is left for the configured time without any mouse movement or input, then the Auto Logout will log out the user.

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.

3.11 Biometrics and Identity Assurance Management

In various places in 21CFR11, there are mentions of using Biometrics in place of someone typing in a Username 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 (username and password suffice), we recognize that some companies may be interested in pursuing the use of these technologies.

3.11.1 Support for Biometric Devices

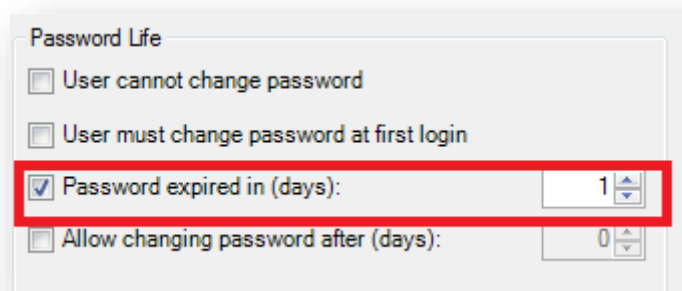
The integration of biometrics provides maximum security for user identification and provides added authentication for FDA regulated applications. In general, there are two ways to integrate Biometric authentication or Multi-Factor Authentication (MFA) into Genesis64.

1. The first option is to set up the login into Microsoft Windows to use Biometric authentication or MFA. Then, GENESIS64 can be set up to leverage the currently logged-in Windows user as the GENESIS64 login user.
2. The second option is to leverage external third-party web-based identity providers. GENESIS64 can be set up to integrate with SAML2.0 or OpenID Connect (OAuth based) identity providers. The means of user authentication is then only limited by the capabilities of the third party.

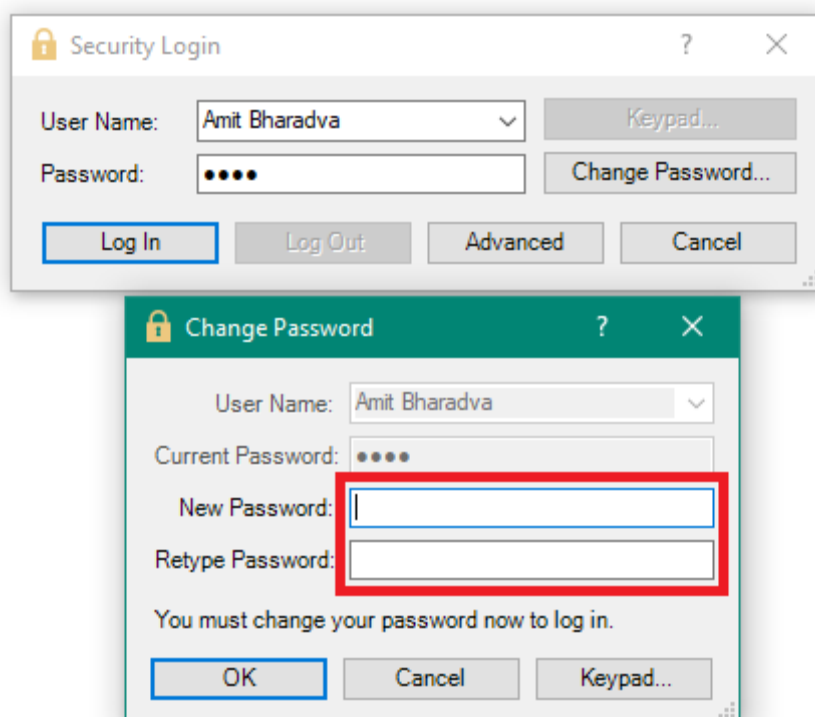
3.12 Password Revisions

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 screenshot is shown below:



Password Age in GENESIS64 Security Configurator



Re-Entering Aged Passwords Dialog from GENESIS64 Security Configurator

3.13 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 GENESIS64 Security Configurator offers an "Account Lockout" feature that addresses detection of attempting to "hack" into the system. On a per-individual basis, the number of attempts deemed sufficient to warrant a lockout may be configured, when the count should be reset, 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 in the following image.

Account Lock On Login Failure

Lock account after failed login (N attempts):

Reset login attempt count after (minutes):

Lock account forever (until admin unlocks)

Lock account for (mins):

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 AlarmWorX64 Logger or Hyper Alarm Logger as well as shown on a security or administrator station using the Alarm/Event Viewer.

Time / Date	Tag ▼	Priority	Type	Quality	Description
3/26/2011 2:48 PM	FrameWorX Server	500		Good	Refused login attempt of user "Dharmesh Gohel"
3/26/2011 2:48 PM	FrameWorX Server	500		Good	Refused login attempt of user "Dharmesh Gohel"
3/26/2011 2:48 PM	FrameWorX Server	500		Good	Refused login attempt of user "Dharmesh Gohel"
3/26/2011 2:48 PM	FrameWorX Server	500		Good	Locking user account "Dharmesh Gohel" because of too many failed login attempts
3/26/2011 2:47 PM	AlarmWorX64	500		Good	AlarmWorx64 Viewer is correctly connected to the subscription @M:Computer\As:ICONIC

Unauthorized Access Event Posted to Viewer



Founded in 1986, ICONICS, a group company of Mitsubishi Electric Corporation, is an award-winning global software provider offering real-time visualization, HMI/SCADA, energy management, fault detection, manufacturing intelligence, MES, and a suite of analytics solutions for operational excellence. ICONICS solutions are installed in 70 percent of the Global 500 companies around the world, helping customers to be more profitable, agile and efficient, to improve quality, and to be more sustainable.

ICONICS is leading the way in cloud-based solutions with its HMI/SCADA, analytics, mobile and data historian to help its customers embrace the Internet of Things (IoT). ICONICS products are used in manufacturing, building automation, oil and gas, renewable energy, utilities, water and wastewater, pharmaceuticals, automotive, and many other industries. ICONICS' advanced visualization, productivity, and sustainability solutions are built on its flagship products: GENESIS64™ HMI/SCADA, Hyper Historian™ plant historian, AnalytiX® solution suite, and MobileHMI™ mobile apps. Delivering information anytime, anywhere, ICONICS' solutions scale from the smallest standalone embedded projects to the largest enterprise applications.

ICONICS promotes an international culture of innovation, creativity, and excellence in product design, development, technical support, training, sales, and consulting services for end users, systems integrators, OEMs, and channel partners. ICONICS has over 375,000 applications installed in multiple industries worldwide.

ICONICS Sales Offices



World Headquarters

100 Foxborough Blvd.
Foxborough, MA, USA, 02035

+1 508 543 8600
us@iconics.com



European Headquarters

Netherlands
+31 252 228 588
holland@iconics.com

Australia

+61 2 9605 1333
australia@iconics.com

China

+86 10 8494 2570
china@iconics.com

Czech Republic

+420 377 183 420
czech@iconics.com

France

+33 4 50 19 11 80
france@iconics.com

Germany

+49 2241 16 508 0
germany@iconics.com

India

+65 6473 2308
india@iconics.com

Italy

+39 010 46 0626
italy@iconics.com

Singapore

+65 6470 2420
singapore@iconics.com

UK

+44 1384 246 700
uk@iconics.com



For more, visit iconics.com

© 2022 ICONICS, Inc. All rights reserved.
Specifications are subject to change without notice. AnalytiX and its respective modules are registered trademarks of ICONICS, Inc. GENESIS64, GENESIS32, Hyper Historian, IoTWorX, KPIWorX, CFSWorX, MobileHMI, WebHMI and their respective modules, OPC-to-the-Core, Make the Invisible Visible, and ICONICS company logo are trademarks of ICONICS, Inc. Other product and company names mentioned herein may be trademarks of their respective owners.

A Group Company of Mitsubishi Electric Corporation

Gold

Microsoft Partner

Eleven-time Microsoft Partner of the Year

