EcoStruxure™ Machine SCADA Expert FDA 21 CFR Part 11 Features Technical Note

12/2018

EIO0000002720_01

www.schneider-electric.com

Schneider Electric™

FDA 21 CFR Part 11 Features

Introduction

The 21 CFR Part 11 regulations from the Food and Drug Administration (FDA) sets forth the criteria under which the agency considers electronic records and electronic signatures to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper.

This document describes features available in EcoStruxure™ Machine SCADA Expert, allowing application engineers to easily design HMI/SCADA applications in conformance with the 21 CFR Part 11 regulations. Comprehensive information about such features is available in the product's Technical Reference (Help) manual. The goal of this document is just to provide general guidelines about the interfaces in the product typically used in applications compliant with the 21 CFR Part 11 regulations.

Remarks

General

- The software (SCADA) cannot state that it complies with FDA Part 11. The software shall provide the necessary tools to allow a user to create a system (application) that is compliant with FDA Part 11.
- The SCADA system does not "force" the user to build an application compliant with FDA Part 11. FDA Part 11 compliance is optional during application development.
- An *Electronic Record* is any data that can be saved as electronic media and retrieved later.
  An *Electronic Signature* is a specific type of Electronic Record that contains the following information:
    - Timestamp
    - User name
    - Meaning of the signature

  A *Digital Signature* is a specific type of Electronic Signature, in which the data is encrypted.
- An *Open System* (such as the World Wide Web or Web) requires encryption for electronic reports and for the Electronic Signature (Digital Signature).
- Electronic records are associated with events (such as tag changes, load recipes, and so forth), whether the user triggered the event or not. Electronic signatures are associated with actions triggered by the user (such as pressing a button, changing a slider, entering a set-point manually, and so forth).

Electronic Records (Event Logger, Alarms, Reports)

- The Part 11 rule does not mention whether the electronic records must be stored in a standard database (such as Oracle, SQL Server, etc.) or in a proprietary format. When you use a standard database, the responsibility for guaranteeing the confidentiality of the database relies on the database features for data protection (such as password protected databases). EcoStruxure™ Machine SCADA Expert v6.0 + SP3 or higher has direct interfaces to databases for Alarms, Events, Trend and Grid objects through ADO.NET, ADO, OLE DB or ODBC.

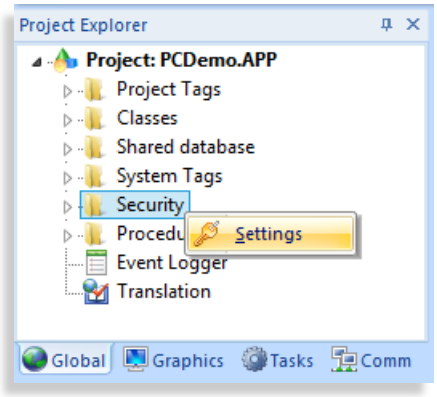
Electronic Signatures (Security System)

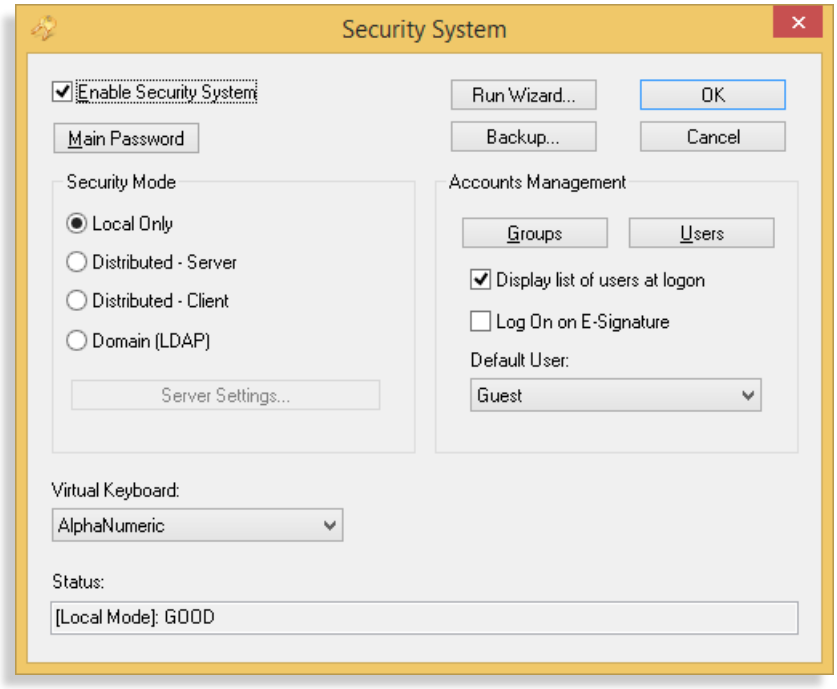
- The system administrator must be able to access the user account settings to create new accounts, lockout users, and de-authorize them. These changes can be logged, even if the runtime is not running.
- Nobody (not even the System Administrator) has access to the password of any user.

Security System

EcoStruxure™ Machine SCADA Expert provides a sophisticated and comprehensive security system, which allows application engineers to configure access and control policies for the project based on authentication.

The main Security System settings can be configured through “Project Explorer > Global > Security”:





You can easily enable (check) or disable (uncheck) the Security System for the whole application through the “Enable Security System” check-box. For real-world applications that must comply with the FDA 21 CFR Part 11 regulations, the security system must be enabled.

Moreover, clicking on the “Main Password”, you can assign a single password (user agnostic), which will be required to view/edit the Security System settings in the future. Only people with rights to modify the security system configuration for the project should have access to this password.

Security System Modes

The Security System from EcoStruxure™ Machine SCADA Expert supports the following modes:

Local Only: The Security System settings (groups, users, rules) are configured with EcoStruxure™ Machine SCADA Expert and the settings are stored (encrypted) within the application's directory. Therefore, if you move the application to a different location (another directory or even another station), the settings are copied along with the application. This configuration is recommended for a single, stand-alone HMI/SCADA station, which is isolated from other HMI/SCADA stations.

Distributed (Server and Client): This mode allows two or more HMI/SCADA stations running EcoStruxure™ Machine SCADA Expert to share the Security System settings. Even if you update the settings from one station during the runtime (e.g.: create new users, remove existing users, changing passwords, etc.), all stations will be automatically updated with the new settings, so you do not have to update the settings manually in each one of them. In this mode, one of the stations must be set with "Distributed - Server" mode (Security System Server station) and the remaining stations configured with "Distributed – Client" mode (Security System Client stations). As long as the Security System Server station is running, you can modify the security system settings from any other station and the new settings will be automatically updated in any other station. If the Security System Server station is unavailable for any reason, all remaining stations will keep running with the most current version of the Security System settings, but they will not allow you to change the settings until the Security System Server station becomes available again.

Domain (LDAP): This mode allows you to configure EcoStruxure™ Machine SCADA Expert to share the settings (users and groups) from a system domain and authenticate users in the application through the Active Directory. The main advantage of this method is the ability to centralize the maintenance of users and groups in a single repository (Active Directory). In other words, when new users are created, or existing users are removed/blocked, or user passwords are modified in the Active Directory, these changes are automatically (dynamically) reflected in the EcoStruxure™ Machine SCADA Expert application. In many cases, this is the most suitable mode for projects that require compliance with the FDA CFR Part 11 regulation.

Security System Groups

The “Account Management > Groups” interface allows you to configure the policies (rights and restrictions) for each group available for the project.

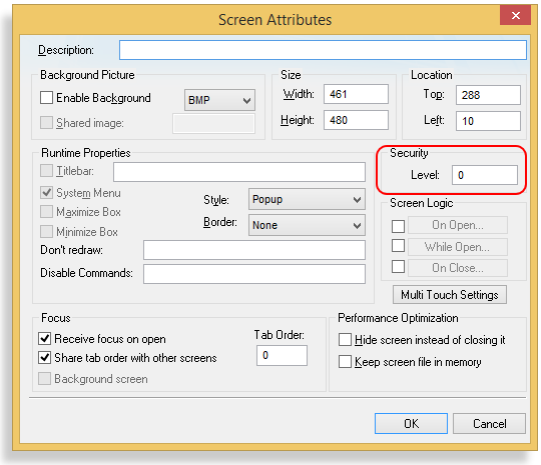
Security Rights - Development: Allows you to define the rights and restrictions for each user on the development environment (IDE) of EcoStruxure™ Machine SCADA Expert. This feature is important to prevent unauthorized users from modifying the configuration of the project, even if they have access to a development license for EcoStruxure™ Machine SCADA Expert.

Note: In addition to the “Security Rights - Development” settings, EcoStruxure™ Machine SCADA Expert also offers the **Password Protection** feature to encrypt configuration files with a user defined password. You can apply the password to the whole project (Home > Tools > Verity > Set password for all files) or at least for the configuration documents (screens, worksheets, etc) that must be protected from unauthorized users from viewing or modifying their configuration (right-click on the document from the Project Explorer and select the option Password Protection). The Password Protection is independent from the Security System (it is not associated with any particular group or user from the security system). The main goal of the Password Protection feature is to protect the Intellectual Property of the application configuration with a master password.

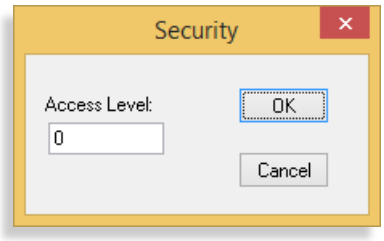
Security Rights - Runtime: Allows you to define the rights and restrictions for each user during the runtime (local graphical interface – Viewer – or remote graphical interface – Thin Clients). This feature is important to prevent unauthorized users from visualizing screens or interaction with objects through animations configured in the project (commands, text input, sliders, etc.).

You can assign a **Security Level** range for each group. When configuring the documents (screens, worksheets) and the objects on the graphical screens, you can assign a security level to each one of them, as follows:

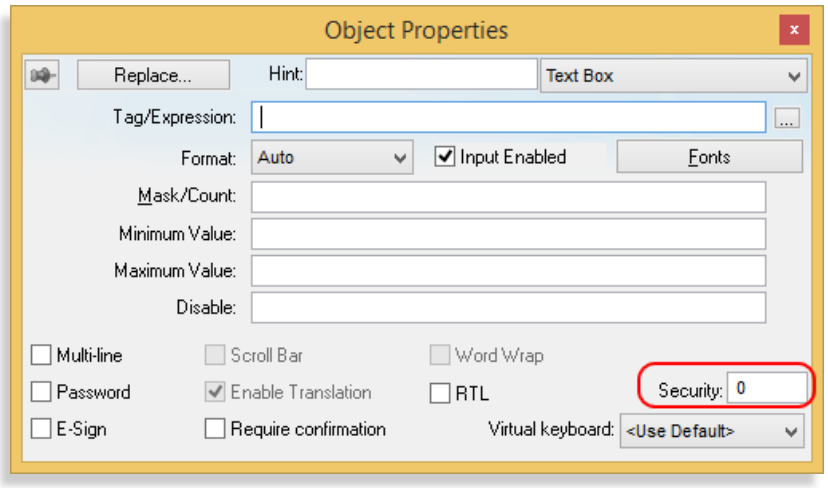
- **Screens**: From the ribbon, select “Graphics > Screen > Attributes > Security Level”. Only users associated with at least one group that have this security access level within its range (Security Rights – Development) will be able to open the screen on the development environment. Only users associated with at least one group that have this security access level within its range (Security Rights – Runtime) will be able to open the screen during the runtime.



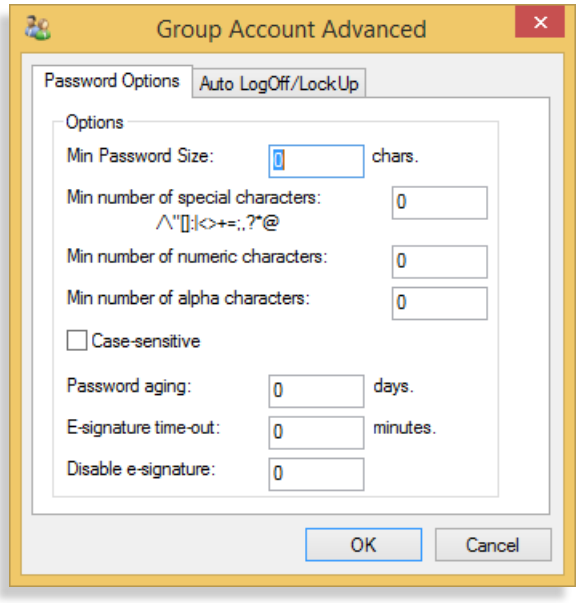
- **Worksheets** (Alarms, Trends, Recipes, Reports, etc.): From the ribbon, select “Project > Security System > Access Level” (you need to click on the body of the worksheet to enable this option). Only users associated with at least one group that have this security access level within its range (Security Rights – Development) will be able to open the worksheet on the development environment.

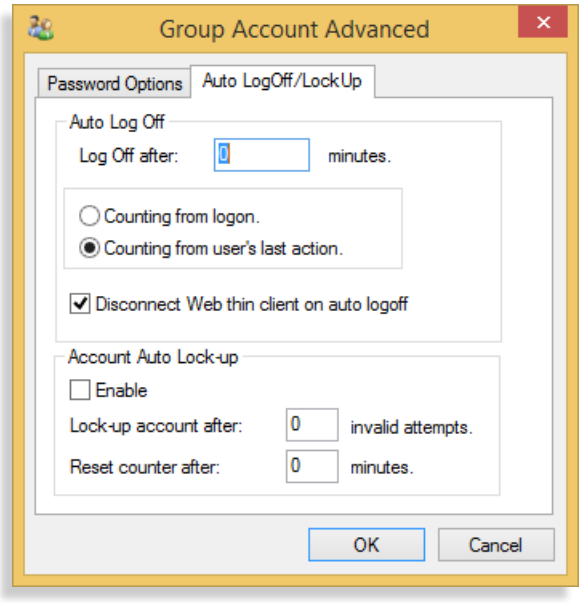


- **Objects and animations from the graphical screens**: Set the Security property through the Object Properties dialog for the Text Box, Pushbutton, Check Box, Radio Button, Combo Box, List Box, Smart Message, Alarm/Event (Advanced > Delete Message, Advanced > Acknowledgment),Grid, Command (Config), Hyperlink, Text Data Link (Input Enabled), Visibility/Position (Slider/Gestures), Resize (Gesture), Rotation (Gesture). Only users associated with at least one group that have this security access level within its range (Security Rights – Runtime) will be able to interact with this object or animation during the runtime.



When configuring the Groups, you can also configure Advanced Settings that will apply for the users associated with this specific group:



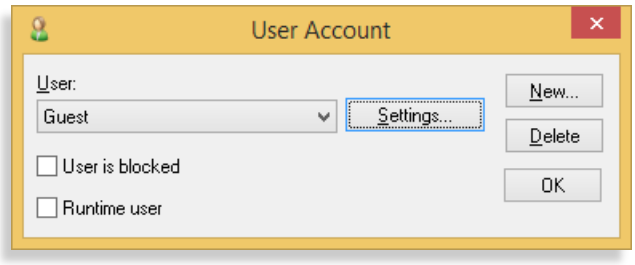


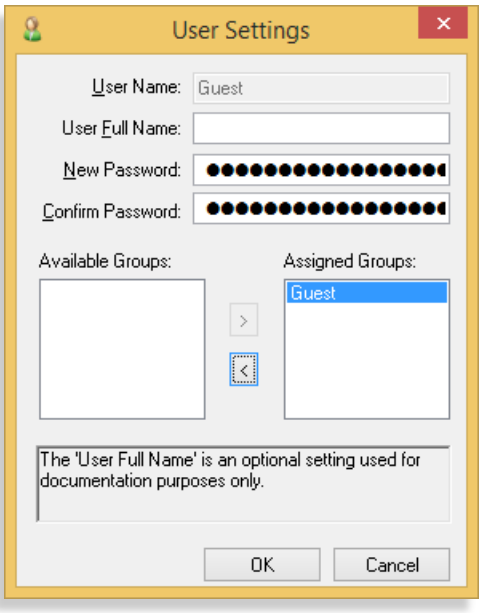
- **Password Options**: Allows you to define the password rules, including the Password again, which will force users from this group to change their password in a user defined interval (number of days).

- **Auto Logoff/Lockup**: Allows you to automatically log off users for inactivity during a period of time or block users after a number of consecutive attempts to log on with an invalid password.

Note: Some settings are configured and enforced by the Active Directory (not by EcoStruxure™ Machine SCADA Expert) when using the Domain (LDAP) mode.

Security System Users

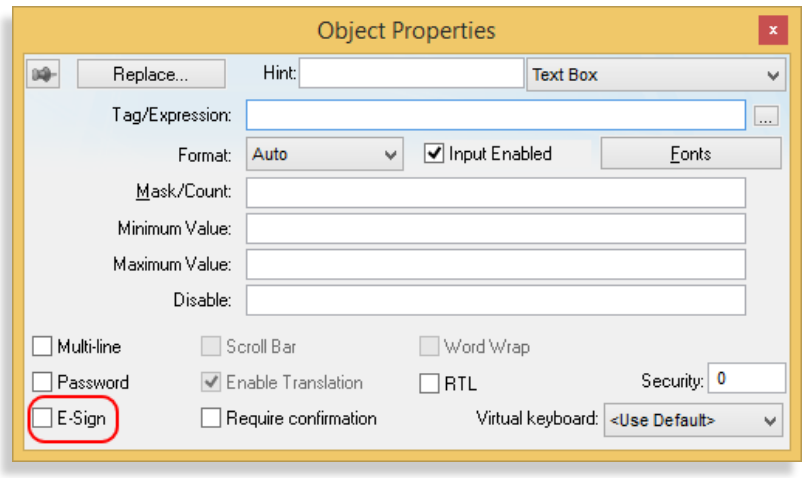




You can define user name, user full name (saved in built-in Alarm/Event logs), password and group(s) assigned to each user. Each user will inherit the rights (priviledges) from the Group(s) assigned to him/her.

Electronic Signature (E-Sign)

Objects and animation that allow the user to perform an action during the runtime allow you to enforce an Electronic Signature (E-sign) in order to execute the respective task.



When this option (check-box) is enabled (checked), the user is prompted with a dialog to enter his/her user name and password before executing the action, regardless of the user currently logged on the application. Electronic Signature is important to avoid “impersonification” of the user logged on the system when executing a particular action. If an E-sign has been executed within the E-signature time-out period (Security System Groups > Advanced > Password options), a subsequent request for Electronic Signature will automatically show the name of the user name who executed the last E-sign and ask him/her only for the password. This feature allows you to improve the productivity of the application during the runtime, since E-sign demands an extra step for the operator. Moreover, this feature must be used critereously in interfaces that require a higher level of control over the user who is executing the task.

Eletronic Signature are usually configured in conjunction with the Event Logger, which records the name of the user who executed the action (along with other parameters, such as the timestamp of the action execution and a message describing the action). The Event Logger will be described in details in another chapter from this document.

Log-On and Log-Off

There is always one user logged at any given time on the runtime station (where EcoStruxure™ Machine SCADA Expert is installed and the process “Studio Manager.exe” is running). Moreover, there is also one user logged at any given time on each Thin Client connected to the runtime station (Server). The user logged on the server and on each Thin Clients can be different at any given time.

The log-on and log-off actions can be peformed from:

The development environment: From the ribbon, select “Project > Security System > Log-On”.

The runtime (local Viewer or Thin Clients): Configure an object/animation to execute the built-in fucntions LogOn() or LogOff(). You can also log on a user during the runtime executing an Eletronic Signagure (as long as the property (chek-box) “Log On on E-Signature” from the Security System dialog is enabled (checked).

Whe logging off, the “Default User” is automatically logged on. In other words, logging off means logging on the “Default User”. You can set the “Default User” from the Security System dialog (Guest, by default). Since the log off action does not require the knowledge of any password, it is strongly recommended to assign a user associated to a group that has no rights or minimum rights and privileges.

Security System Built-in Functions

EcoStruxure™ Machine SCADA Expert provides a set of built-in functions that can be executed during the runtime to manage the security system:

Function	Description
BlockUser	Blocks an existing user from logging onto a project. This allows you to disable a user account without deleting it.
CheckESign	Prompts the run-time user to electronically sign an event by entering their username and password. You can call this function to secure scripts and expressions, just as you can select the E-Sign option in object properties to secure screen objects and animations.
CheckSecurityLevel	Checks whether the current user has access to the specified security level.
CreateUser	Creates a new user in your project's security system.
ExportSecuritySystem	Exports the security system configuration to an encrypted file.
GetLastESignUser	Gets the last user who electronically signed an event during run time.
GetSecuritySystemStatus	Gets the status of the security system and its connection to the authentication server, when the security mode is either Distributed–Client or Domain (LDAP).
GetUserFullName	Gets the full name (if any) of a specified user in the project security system.
GetUserNames	Gets the list of user names available in the project.
GetUserPwdAging	Gets the age of the password for a specified user — that is, the time remaining until the password expires, or if it has expired, the time since it expired.
GetUserState	Gets the current status of a selected user.
ImportSecuritySystem	Imports a security system configuration from an external file.
RemoveUser	Removes a specified user from your project's security system.
SetPassword	Sets a new password for a specified user in your project's security system.
UnblockUser	Unblocks a blocked user in the security system.

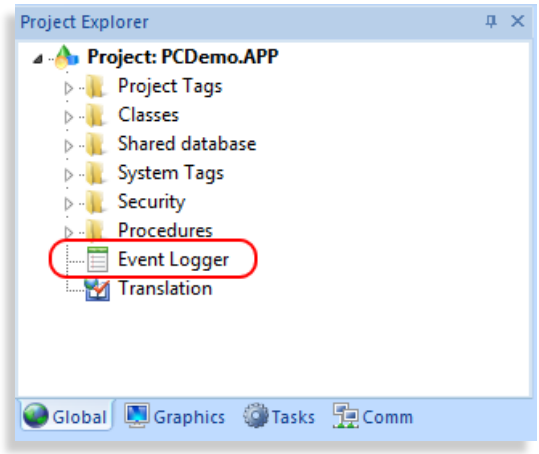
Detailed description about each built-in function is available in the product’s Technical Reference (Help) manual.

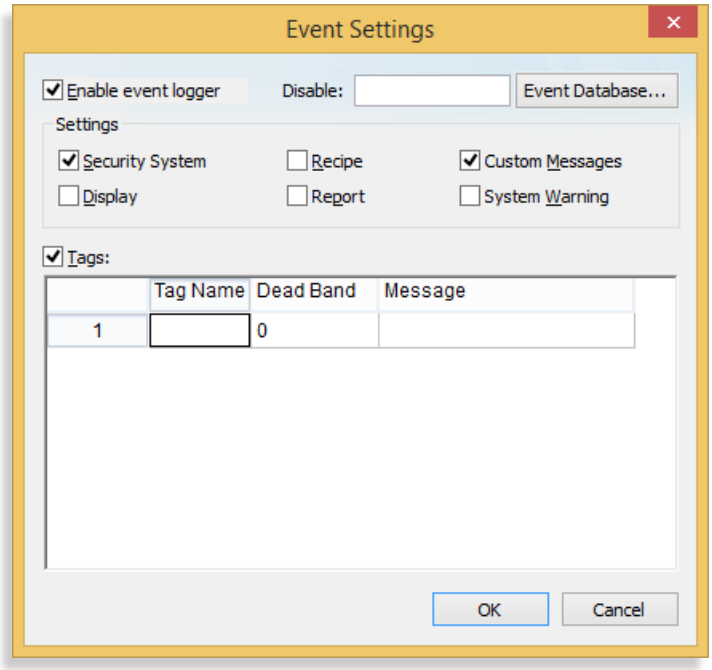
Events

EcoStruxure™ Machine SCADA Expert allows you to keep a record of events, providing traceability through future audits. The Event Logger module saves the events into the history repositoty and the Alarm/Event control allows you to view the events in a graphical screen.

Event Logger

You can configure what events should be saved into the Event History (log of events) by double-clicking on the "Event Logger" icon from "Project Explorer > Global":





After enabling the event logger (checking the "Enable event logger" check-box), you can define what type of events will be saved.

- **Security System**: All actions directly associated with the security system, such as user log on, user log off, invalid attempt to log on (invalid user or password), user blocked, user unblocked, user created, user removed, password changed, etc.

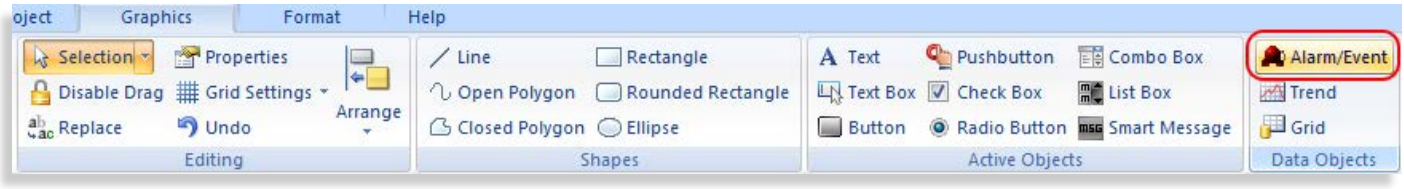
- **Display**: Creates a record whenever a screen is open or closed during the runtime. This option is usually enabled for troubleshooting for a limited period of time to avoid a high number of records saved into the Event History. If you want to log only when specific screens are open or closed, you can use the Custom Messages option (with the SendEvent() built-in function).

- **Recipe**: Creates a record whenever a recipe is loaded, saved, deleted, or initialized (using the built-in Recipe() function).

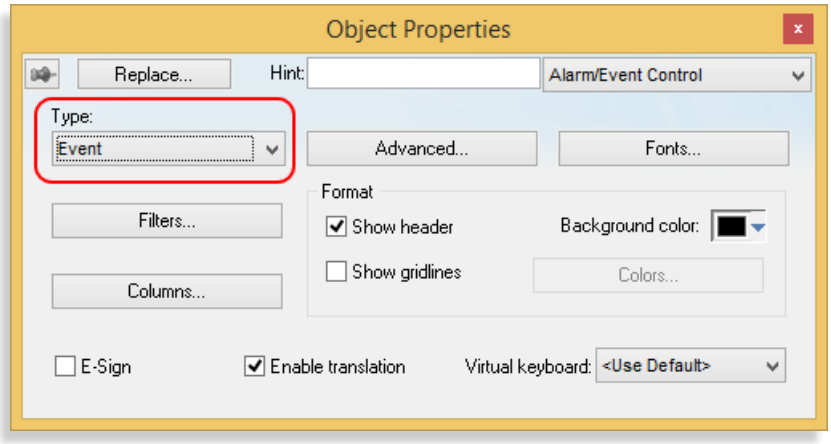
- **Report**: Creates a record whenever a report is saved, or printed (using the built-in Report() function).
- **Custom Messages**: Allows you to create custom messages to be recorded by the Event Logger. When this option is enabled, you can send custom messages to the event logger through the built-in function SendEvent(). For example, when the user clicks on a button to execute the Command animation, you can add a line in the script to execute the SendEvent() built-in function and send a custom message to the Event History (e.g.: SendEvent("Start Process button pressed")).
- **System Warnings**: Creates a record whenever a script error occurs (e.g.: division by zero). This option is usually enabled for troubleshooting for a limited period of time to avoid a high number of records saved into the Event History.
- **Tags**: Creates a record with a customized message (Message column) whenever the respective tag changes of value (regardless of how the tag value was changed – e.g.: communication driver, script, user interface, etc.). You can assign a dead-band to avoid generating too many records for analog values and you can also concatenate tags or expressions in the Message column by configuring them between curly braces (e.g.: The new state of the Motor ABC is {If(TagMotorABC=0,"OFF","ON")}).

Alarm/Event Control (Event Viewer)

The Alarm/Event control allows you to view the events saved by the Event Logger module.



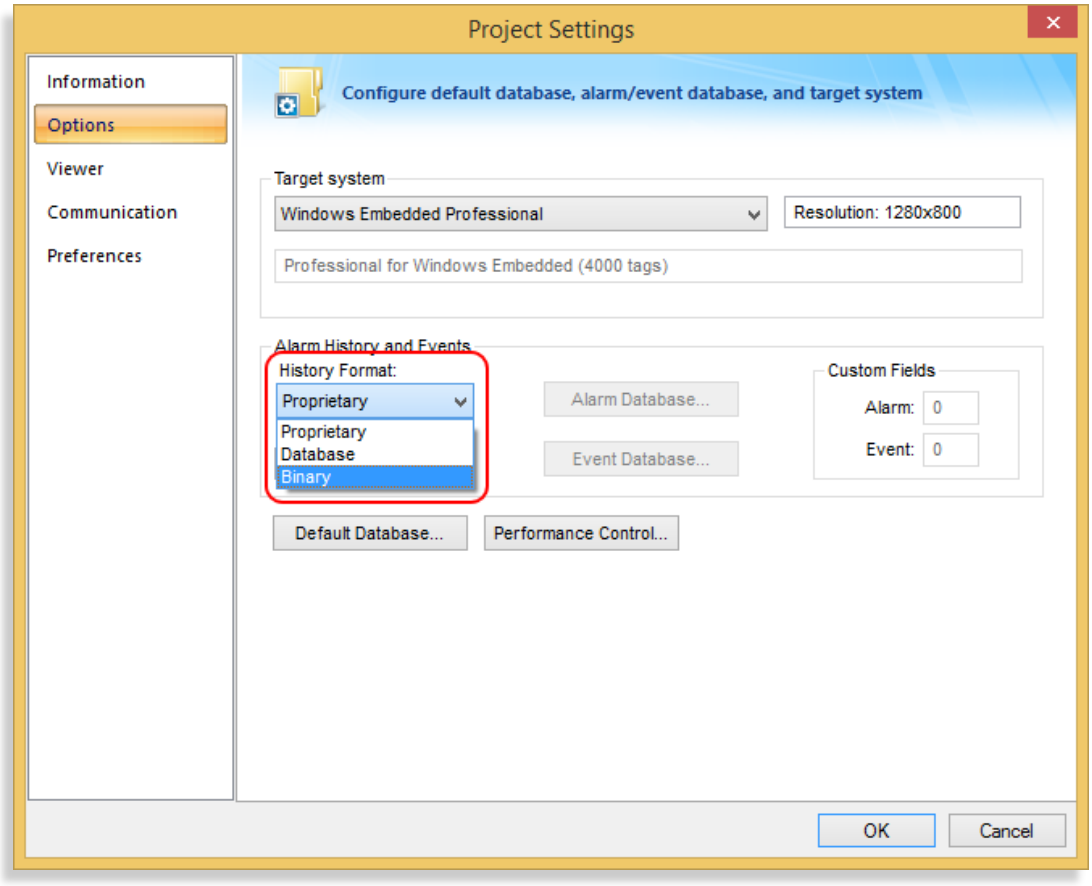
After adding the Alarm/Event object into a screen, just set its "Type" to "Event" (or to Alarm History + Event if you want to combine the visualization of both logs).



Detailed description about the Alarm/Event control is available in the product's Technical Reference (Help) manual.

Event History Format

EcoStruxure™ Machine SCADA Expert allows you to save the Event History data in three different formats: Proprietary, Database, or Binary. You can set the format for the Alarm and Event history data through the ribbon "Project > Options" interface:



- **Proprietary**: Saves the Event history files in the \Alarm sub-folder of the application with the file name syntax EVYYMMDD.EVT (YY=Year, MM=Month, DD=Day) – one file per day. This format is NOT recommended for applications that must be compliant with the FDA 21 CFR Part 11. We recommend either Database or Binary for these cases.

- **Binary**: Saves the Event history files in the \Alarm sub-folder of the application with the file name syntax EVYYMMDD.EVT (YY=Year, MM=Month, DD=Day) – one file per day. The information is saved in binary format to prevent it from being easily edited.

- **Database**: Saves the Event history data into an external SQL Relational Database. In this case, the third-part database engine tools must be used to prevent unauthorized access to the history data (e.g.: password protection).

Regardless of the format, the Event Logger will save not only the Timestamp, message, and user name associated with the event, but also additional information, such as User Full Name (if any), Station, among others.

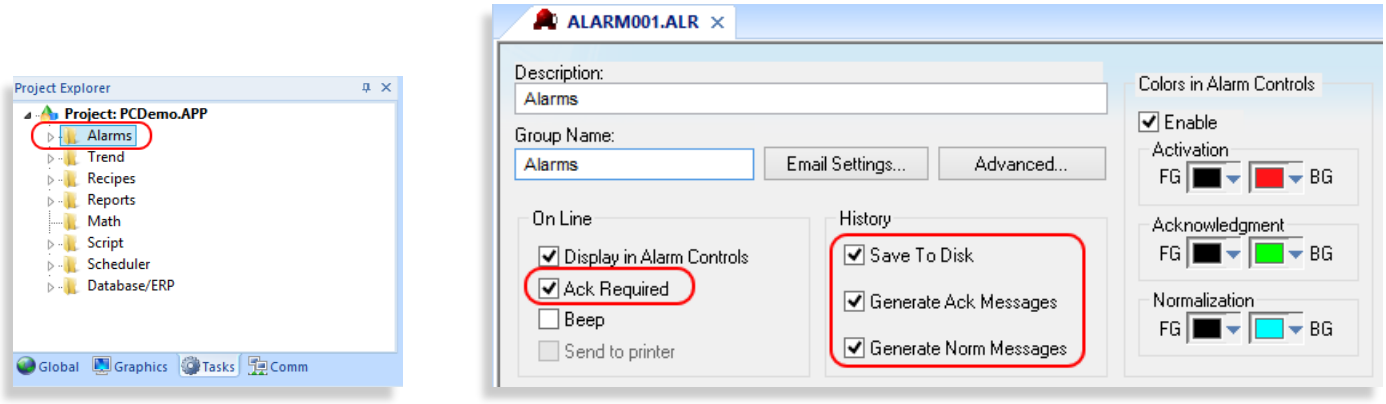
Detailed description about the Event History format and data saved by the event logger is available in the product's Technical Reference (Help) manual.

Alarms

EcoStruxure™ Machine SCADA Expert provides a sophisticated module for Alarm management (both online and history). The Alarm (background) task can be configured to generate alarms and save their events (activation, acknowledgement, and or normalization) into the history repository, providing traceability through future audits. Moreover, the Alarm/Event control (graphical object) allows the users to visualize and/or acknowledge the alarms during the runtime.

Alarm (background) task

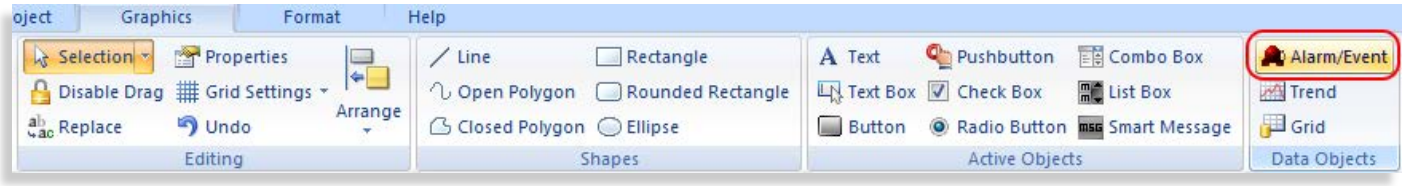
You can configure the alarms conditions and respective messages through Alarm groups (worksheets) that can be created under "Project Explorer > Tasks > Alarms"



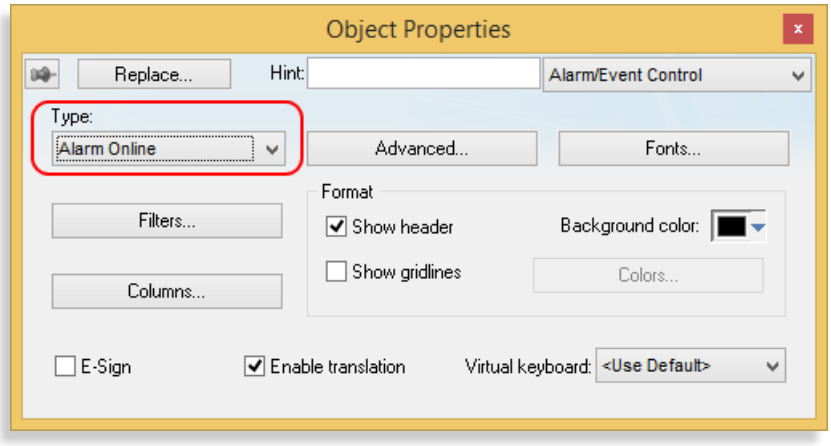
After creating an Alarm group (worksheet), all alarms configured in this group will require acknowledgment, as long as the "Ack Required" property (check-box) is enabled (checked). Moreover, you can configure the Alarm (background) task to save alarm records into the history repository by enabling (checking) the options (check-boxes) "Save to disk" (save a record when the alarm becomes active), "Generator Ack Messages" (save a record when the alarm is acknowledged), and/or "Generate Norm Messages" (save a record when the alarm is normalized).

Alarm/Event Control (Alarm Viewer)

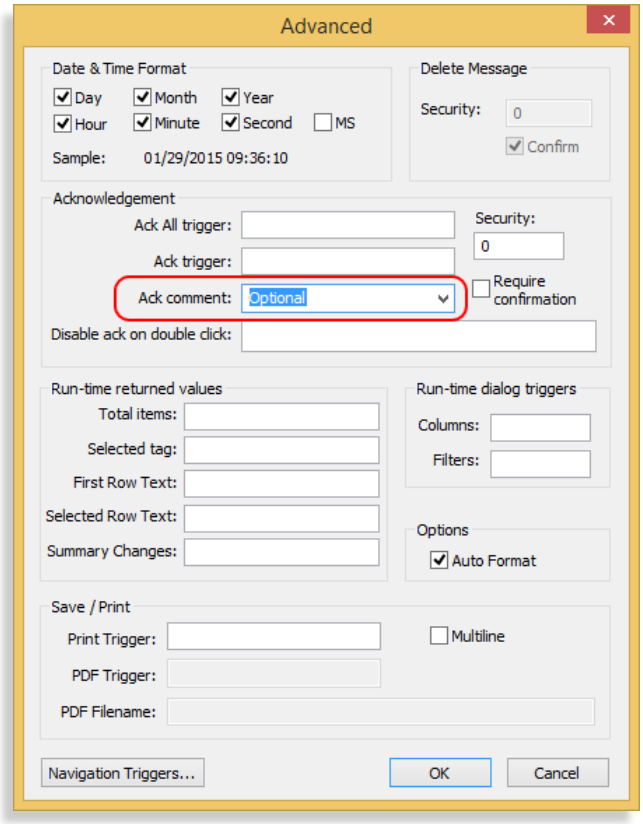
The Alarm/Event control allows you to view the events saved by the Alarm background task.



After adding the Alarm/Event object into a screen, just set its “Type” to “Alarm Online” to visualize the online alarms only, or “Alarm History” to visualize the History of Alarms (or even to “Alarm History + Event if you want to combine the visualization of both logs).



When setting the Alarm/Event control with the Type “Alarm Online”, the user may have the option to acknowledge any online alarm by double-clicking on the respective alarm record displayed by the object, during the runtime. You can configure the Alarm/Event control to allow the user to enter a comment when acknowledging an alarm during the runtime (or even enforce it).

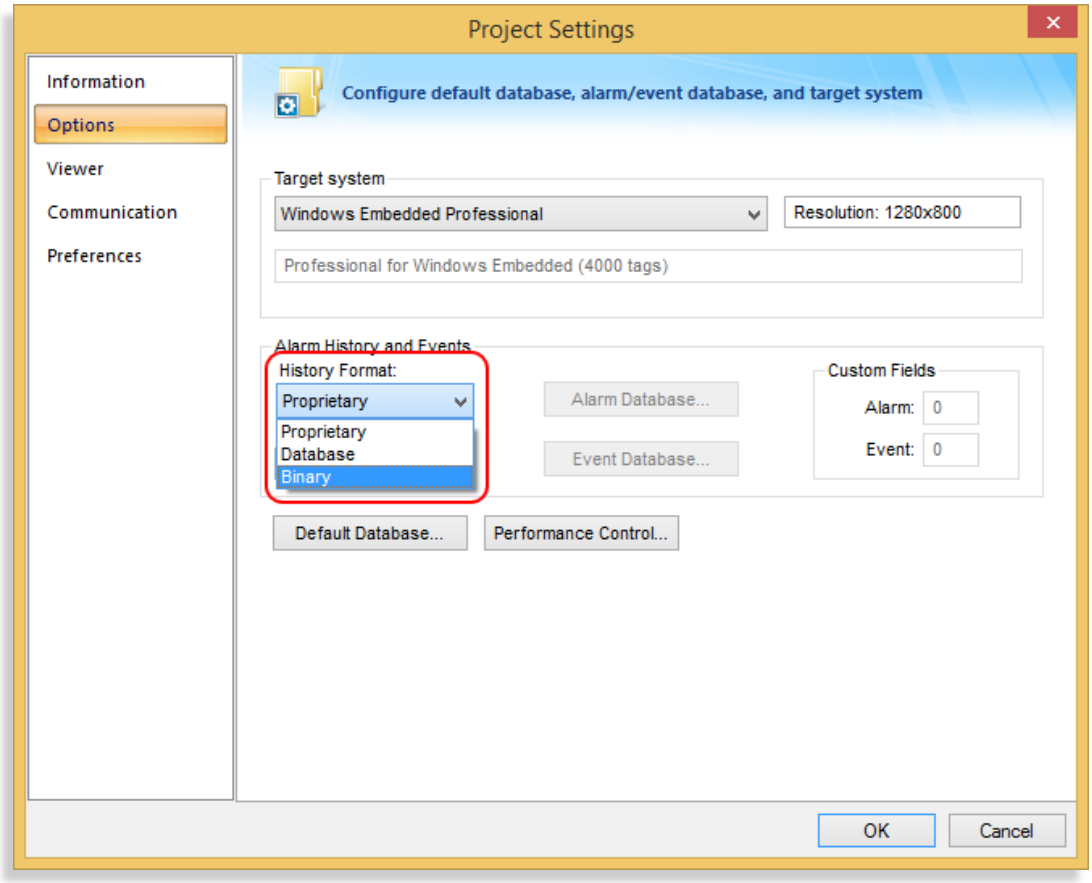


Just set the “Advanced > Ack comment” property to “Optional” (or even to “Mandatory”, if you want to enforce the comment). After double-clicking on the alarm record to acknowledge it, the user will be prompted with a dialog to enter his/her comments. The comments written by the user during the runtime will be saved along with the alarm record into the History repository (if any).

Detailed description about the Alarm/Event control is available in the product’s Technical Reference (Help) manual.

Alarm History Format

EcoStruxure™ Machine SCADA Expert allows you to save the Alarm History data in three different formats: Proprietary, Database, or Binary. You can set the format for the Alarm and Event history data through the ribbon “Project > Options” interface:



- **Proprietary**: Saves the Alarm history files in the \Alarm sub-folder of the application with the file name syntax ALYYMMDD.ALH (YY=Year, MM=Month, DD=Day) – one file per day. This format is NOT recommended for applications that must be compliant with the FDA 21 CFR Part 11. We recommend either Database or Binary for these cases.

- **Binary**: Saves the Alarm history files in the \Alarm sub-folder of the application with the file name syntax ALYYMMDD.ALH (YY=Year, MM=Month, DD=Day) – one file per day. The information is saved in binary format to prevent it from being easily edited.

- **Database**: Saves the Alarm history data into an external SQL Relational Database. In this case, the third-part database engine tools must be used to prevent unauthorized access to the history data (e.g.: password protection).

Regardless of the format, the Alarm (background) task will save not only the Timestamp, message, and user name associated with the alarm, but also additional information, such as User Full Name (if any), Station, among others.

Detailed description about the Alarm History format and data saved by the Alarm (background) task is available in the product's Technical Reference (Help) manual.