# **Create Project With 21 CFR 11 Compliance**

Title 21 CFR Part 11 is the part of Title 21 of the Code of Federal Regulations that establishes the United States Food and Drug Administration (FDA) regulations on electronic records and electronic signatures (ERES).

# Overview

Part 11, as it is commonly called, defines the criteria under which electronic records and electronic signatures are considered trustworthy, reliable, and equivalent to paper records.

Listed below are described some security-related features available in the product:

- Access Control: Security technique that regulates who or what can view or use resources in a computing environment.
- Password Encryption: System administrator does not possess access to the user. They are encrypted before being stored.
- Maximum and Minimum Age for Password: A feature that imposes a minimum password age before allowing it to change and a maximum age before expiring.
- Required Password changing: Forces the user to alter his password after the first login has been made.
- User Name and Password Minimum Length: Defines username and the password's minimum length.
- Block on Invalid Login Attempt: Blocks User if maximum number of invalid login attempts have been made.
- Store Password History: A range of the last 0-5 passwords can be stored to make sure the user does not repeat an already used one.
- · Auto Log Off: User is logged off the system for inactivity or expiration date.
- Audit Trail Data: Security-relevant chronological record or set of records that provide documentary evidence of the sequence of activities that
  have affected at any time a specific operation.

# **Project Configuration**

## Audit Trail

Audit trails should be generated independently of the operator and include the local date and time of the actions that alter the record. They cannot overwrite the old data, and they must be stored as long as the record itself is stored.

To use the Audit Trail function, you must enable it. Go to **Edit** > **Alarms** > **Groups**, and click on the Settings button.

$\int$	Groups	Areas	Items						
	Audit Trail: Settin	s Initial d	isable time: 00:00:00	Life Time: 0	days 🧧 Log Use	r FullName			
	Ignore	Alarms During Time	eDeadband: 🦲 En	able Limits by Shift: 🧧					
	Drag a column head	er here to group	_	-	_		_	-	Filter by Name:
	Name	Acklequired AckreTimeDeadband Sound Show LogEvents Colors NotificationMethod Description							
*									
4	Warning	No		None	List	Active	ActiveFg=#FFF0000;Active		Warning messages that don't require acknowledge
	Critical	Yes		Веер		ActiveAck	ActiveFg=#FFFF0000;Active		Critical messages that require acknowledge
	AuditTrail	No		None	None	Active	ActiveFg=#FFFF0000;Active		Audit trail log

A popup display will open with many checkboxes. Besides the Enable option, you can choose which actions will be stored in the Audit Trail database. The options are as follows:

- · User Logon/Logoff: Stores informational data on user login/logout.
- · Open/Close Displays: Stores informational data when displays are open or closed.
- Remote Connections: Stores information on remote client connections (Smart/Rich Clients).
- Custom Messages: Stores added custom messages.
- Tag Changes: Stores informational data of every tag change.
- Datasets (Insert/Updates or All Commands): Stores information on datasets.
- Operator Actions: Stores information on operator actions.
- · Save Reports: Stores information when the save command is executed.
- System Warnings: Stores information related to the system.

For every project update indicated above, crucial information is stored alongside the event info in the Alarm Historian database columns:

Active Time 🔹	Condition	UserName	Message	ŀ
2/13/2020 10:53:02	OpenCloseDisplays	Administrator	Display was opened: MainPage; RichClient	
2/13/2020 10:53:02	OpenCloseDisplays	Administrator	Display was opened: MainPage; RichClient	
2/13/2020 10:53:02	OpenCloseDisplays	Administrator	Display was closed: MainPage; RichClient	
2/13/2020 10:53:02	OpenCloseDisplays	Administrator	Display was closed: MainPage; RichClient	
2/13/2020 10:51:15	OpenCloseDisplays	Administrator	Display was closed: LogOn; RichClient	
2/13/2020 10:51:15	LogonLogoffSecurity	Administrator	Logged user: Administrator; 127.0.0.1\RichClient	
2/13/2020 10:51:15	OperatorActions	Guest	Value was set: Client.InputUserName; Administrator; RichClient	
2/13/2020 10:51:09	OpenCloseDisplays	Guest	Display was opened: LogOn; RichClient	
2/13/2020 10:51:03	OpenCloseDisplays	Guest	Display was opened: Header; RichClient	
2/13/2020 10:51:03	OpenCloseDisplays	Guest	Display was opened: MainPage; RichClient	
2/13/2020 10:51:00	SystemWarnings		DataSet was started	
2/13/2020 10:51:00	LogonLogoffSecurity	Guest	Logged user: Guest; 127.0.0.1\RichClient	
2/13/2020 10:50:57	SystemWarnings		Server was started	
2/13/2020 10:50:57	SystemWarnings		Alarm was started	

- UserName: Indicates the user that was logged in at the time an event happened.
- ActiveTime Ticks: Date and time in which the event happened. It's worth mentioning that despite this data being stored as Ticks in the database, the product is smart enough to automatically convert it to DateTime when it shows on a Display.
- Message: Detailed information on the event. It changes according to the event.
- Condition: Indicate which Audit Trail selection field the event came from.

## **Exporting Reports**

To comply with the regulation, the software must be able to export digital and physical copies of Reports.

To create or edit a report:

- Go to Edit > Reports > Reports
- Select a report name or select the insert row (first row)
- Enter or select information, as needed



- Name: Enter a name for the report. The system will let you know if the name is not valid.
- Padding: Use padding when replacing a tag name with its value (the field starts with enough space for the same number of characters as the tag name):
  - <sup>o</sup> Compact Removes any extra characters and displays only the tag
  - PadRight Adds an extra space for each character to the right of the tag
  - PadLeft Adds an extra space for each character to the left of the tag
- SaveFormat: Selects the report format: XPS, HTML, Unicode, ASCII, PDF
- SaveFileName: Enter a string with {ObjectProperties}. Use the full path
- SaveTrigger: Enter an object property as the trigger
- Append: Enter the file that appends the report
- Size: The size of the report
- EditSecurity: Check which user groups can edit the report
- Header: Choose another report as the Header
- Footer: Choose another report as the Footer
- Legacy: Read-only. Shows if the report is a legacy
- Description: Enter a description of the report

It is possible to add several runtime objects to a Report. Some examples are:

- Tag values and properties.
- Client and Server property information.
- Symbols (TrendCharts are added as a symbol).
- Tables and DataGrids can be dynamically colored and translated according to the project's localization setting.

The Report is saved using one of the following methods:

```
@Report.<ReportName>.Save
// Property used to trigger the save report action
@Report.<ReportName>.SaveCommand(int Orientation)
// Orientation = 0 or blank -- Portrait Mode
// Orientation = 1 -- Landscape Mode
// saves the selected report into the path indicated by the SaveFileName property
```

# Security

#### **User Permissions**

Under Security > Permissions, it is possible to allow/disallow a user to edit different project tabs in the Engineering Environment. The available options are shown in the image below.

	Users	missions	Policies	RuntimeUsers	
Γ	Drag a column heade	er here to group			
	Name	Edit	Run		
	Administrator	Unrestricted;	Unrestricted;	Administrator group	
	Guest	Unrestricted;	Unrestricted;	Guest group	
	Maintenance	Unrestricted;	Unrestricted;	Maintenance group	
	Enginnering	Unrestricted;	Unrestricted;	Engineering group	
	Supervisor	Unrestricted;	Unrestricted;	Supervisor group	
<u>s</u>	Operator	Edit	Startup; Clien	Operator group	
	User	📒 Unres	tricted	Darat	
	Group8			Keset	
	Group9	🦰 EditTa	igs 🧧	Historian	
	Group10	🦲 Securi	ity 🛛	Alarms	
	Group11	Script	c 🛛	Devices	
	Group12		· ·		
	Group13	🦲 Datas	ets 🛛	Displays	
	Group14	🦲 Repor	ts 🧧	Startup	
	Group15	- Dublic	L .	Cattings	
	Group16	Publis	an (4	- settings	
	Group17	🦰 Notes		CreateTags	
	Group18		1		

It is also possible to allow/disallow a user to perform different actions during Runtime.

	Users	missions	Policies	RuntimeUsers				
Γ	Drag a column header here to group							
	Name	Edit	Run					
	Administrator	Unrestricted;	Unrestricted;	Administrator group				
	Guest	Unrestricted;	Unrestricted;	Guest group				
	Maintenance	Unrestricted;	Unrestricted;	Maintenance group				
	Enginnering	Unrestricted;	Unrestricted;	Engineering group				
	Supervisor	Unrestricted;	Unrestricted;	Supervisor group				
<b>S</b>	Operator		Run	Operator group				
	User	Unrestricted;	- 	tricted				
	Group8			Reset				
	Group9		🦰 Test	Startup				
	Group10		🦲 Shutd	own 📈 ClientStart				
	Group11		Client	Shutdown - StartTools				
	Group12							
	Group13		🔁 ToolsS	SetValues 😿 CreateUsers				
	Group14		🦰 Switch	hApplication 🖌 WebAccess				
	Group15							

To apply a created permission to a user, go to Security > Users (Permissions Columns), and select the desired option.

Password

## 2.3.1 User Policies

Under Security > Policies, there are three main configuration columns that can be important for CFR 11 compliance.

- Identification: Contains several password configuration options, detailed below:
  - Allow Password Change: Indicates if a user, other than an administrator, can change its own password.
  - Password Min Length: Minimum character length for password (0 means no restrictions).
  - Block On Invalid Attempts: Maximum number of login attempts before blocking user (0 means no restrictions).
  - Allow Share User: Indicates if user can be shared between stations.
  - ° UserName Min Length: Minimum character length for username (0 means no restrictions).
  - Password History: Remember last passwords (Range: 0-5).
  - Min Password Age: Minimum password age in hours (0 means no restrictions).
  - Max Password Age: Maximum password age in hours (0 means no restrictions).
  - Block Aging: Maximum blocking age in hours (0 means no restrictions).
- ESign: When enabled, a password will be requested for Action Dynamics with eSign. The password remains valid for a specified timeout time (in minutes).

Dynamics, object:	TextBox (4)			Close
<ul> <li>Action</li> <li>Shine</li> <li>TextIO</li> <li>Security</li> <li>TextColor</li> <li>LineColor</li> <li>FillColor</li> <li>Visibility</li> <li>MoveDrag</li> <li>Scale</li> <li>Rotate</li> <li>Skew</li> </ul>	Disable: Verify permissions Administrator Enginnering User Confirm message: ESign required	Guest Supervisor	<ul> <li>Maintenance</li> <li>Operator</li> </ul>	

• Session: User can be logged off according to a determined Inactivity Time (in minutes) and/or after a maximum session duration (in hours).

Session								
Session								
AutoLogOff	Both 💌							
DurationHours	120							

To apply a created session configuration to a User, go to Security > Users (Policies Columns), and select the desired option.

	Users Per	rmissions Policies Ru	untimeUsers	
	Drag a column head	er here to group		
	Name	Permissions	Password	Policy [ lo
*				
ø	Administrator	Administrator;	*****	Defai 💌
	User	User;	*****	Default
	Guest	Guest;	*****	Enhanced
				Settings4 Settings5 Settings6 Settings7

#### **Runtime Users**

This is a type of user that exists only during an application's Runtime period. The user can be created during the Engineering process (in *Security* > *Runti meUsers*) or during runtime (via code).

Below you can find more details regarding the available RuntimeUser methods in the Security namespace.

```
@Security.NewRuntimeUser(string name, out int errorCode)
// Creates a new RuntimeUser
// name: User Name
// errorCode: Error code (output)
// Returns: String containing the error message (if error) or empty (if not error)
@Security.AddRuntimeUser(string name, string permissionsStr, string password, string passwordHint, string
policyStr, string profilePhone, string profileCompleteName, bool oneTimePassword)
// Add Runtime User
// name: User Name
// permissions Str: Permissions
// password: Password
// passwordHint: Password hint
// policyStr: Policy
// profileEmail: Profile email
// profilePhone: Profile phone
// profileCompleteName: Profile complete name
// oneTimePassword: flag (true or false) to set a One Time Password setting. If true, a password change is
required after first login
// Returns: String containing error message (if error) or empty (if not error)
```

The RuntimeUsers are stored in its own database found at **Databases** > **DBs**.

🇱 🛀 💽 🕕	$\hat{\boldsymbol{\zeta}}$	DBs Tabl	es Queries File				
Edit <sup>Draw Run Into</sup>		Available Providers: SQ	Lite Data Provider	•			
Jags	D	atabase connection: Create new					
		Drag a column header h	ere to group		Filter by Name:		
G Security	ſ	ID Name	Provider	Database	ConnectionString		
- occarty	3	Retentive	System.Data.SQLite	SQLite	Provider=System.Data.SQLite;Data Source=_ExecutionPathAndName_dbRetentive		
	🗢 2	RuntimeUsers	System.Data.SQLite	SQLite	Provider=System.Data.SQLite;Data Source=_ExecutionPathAndNamedbRuntimeUsers		
<b>11</b>	1	AlarmHistorian	System.Data.SQLite	SQLite	Provider=System.Data.SQLite;Data Source=_ExecutionPathAndNamedbAlarm;Store and F		
Le Devices	0	TagHistorian	System.Data.SQLite	SQLite	Provider=System.Data.SQLite;Data Source=_ExecutionPathAndNamedbHistorian		
Alarms							

#### **Windows Authentication**

To use Windows Authentication, select the checkbox 'Use only Windows Authentication' in Run > Startup and configure which port will be used for authentication in PortWA.

Startup		
Startup Settings		
UserName: Guest	🥮 Password:	
Project server: localhost		
Port: 3101	PortWA: 3102 🧭 Use Only Window	s Authentication
Startup computer: 🧕 Local	Execution Path: • Project Path	
<ul> <li>Project Ser</li> </ul>	ver 🥏 Custom:	
	Due Madula	
Module Information	Alarms Covices	Reports
🥥 🦉 Property Watch	🖌 Datasets 📈 Historian 🐰	Displays
🤤 🧧 Trace Window	Scripts	OPCServer
Hat Start		Rup Startup
Hotstart		Kunstartup
Status: Project		
F Fash	e online configuration	
	e online configuration	

In this case, you will use the configured users for the Active Directory login. If the windows OS has the same name that was created in *Security* > *Permiss ion*, the application will use the permissions configured for this user. Otherwise, it will use the permissions for the Guest user.