F.D.A. 21 C.F.R. Part 11

Overview of 21 C.F.R. Part 11

21 C.F.R. Part 11 (Title 21 Code Of Federal Regulations, Part 11) refers to regulations administered by the United States Food and Drug Administration (FDA) imposed on regulated organizations, such as drug and medical device manufacturers as well as biotech companies. These regulations refer to electronic records and electronic signatures such as production settings and the person who made the setting changes. These electronic records and electronic signatures are considered trustworthy, reliable and equivalent to paper records[1].

This regulation applies to recording and submission of production information sent to the FDA (United States Food and Drug Administration). The regulation requires implementation of controls, audits trails, system validation and electronic signatures involving electronic data. 21 C.F.R. Part 11 was targeted to be deployed in drug and biological product production, not food production. However, 21 C.F.R. Part 11 may be required with food production in the food products if the food products contain ingredients that could be unsafe.

21 C.F.R. was initially enacted into law in August, 1997. The legal authority is 21 U.S.C. 321-393 (Regulation of Food, Drug and Cosmetic Products) and 42 U.S.C. §262 (Regulation of Biological Products). 21 C.F.R. Part 11 was initially published in the Federal Register 62 FR 13464 (Volume 62, Page 13464) on March 20, 1997.

There are several sections to 21 C.F.R. Part 11. These sections include:

21 C.F.R. Part 11

Subpart A - General Provisions

Sec.

11.1 Scope.

Defines where the use of electronic records are required. Note that the computer systems, software and documentation maintained are subject to inspection by the Food and Drug Administration.

11.2 Implementation.

Allows for the use of electronic records in lieu of paper records as long as recording requirements are met.

11.3 Definitions.

Defines terms such as biometrics, a closed system (access to the system is only allowed by persons responsible for the content of electronic records), digital signatures, electronic records, electronic signatures, handwritten signature, and an open system (where access to the system is not restricted to persons responsible for the content of electronic records).

Subpart B - Electronic Records

11.10 Controls for closed systems.

Defines procedures to implement a closed system and ensuring authenticity, integrity and confidentiality of electronics records.

11.30 Controls for open systems.

Defines procedures to implement an open system and ensuring authenticity, integrity and confidentiality of electronics records.

11.50 Signature manifestations.

---

[1] Ref. Title 21 CFR Part §11, section 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.

Defines signature requirements such as the printed name, date and time and the meaning of the signature.

11.70 Signature/record linking.
Linking of the electronic signatures to the electronic records to ensure the authenticity of the action.

Subpart C - Electronic Signatures

11.100 General requirements.
Requirement that the electronic signature be unique to one individual and not used by anyone else and ensure that an electronic signature is equivalent to a legally binding handwritten signature

11.200 Electronic signature components and controls.
Defines electronic signatures based on biometrics (e.g. fingerprint) or non-biometrics. For non-biometrics, the electronic signature must have at least two distinct identification components such as an identification code and a password. When there are multiple electronic signatures required in a single continuous period, there must be first an electronic signature with two distinct identification component and afterward at lase one electronic signature component that is executed only by one individual.

11.300 Controls for identification codes/passwords.
Requires that no two (or more) individuals can have the same combination of identification code and password. If there is a lost, stolen, missing or otherwise compromised identification code or password information, there is a requirement to issue a temporary or permanent replacement. Transactional safeguards are required to prevent unauthorized use of identification codes and passwords.

Since 21 C.F.R. Part 11 defines that an electronic record is considered the equivalent of a full handwritten signature and initials, and may be used instead of paper records, the use of electronic records and electronic signature has grown tremendously in the automation industry, including with applications that are not pharmaceutical or biological product manufacturing.

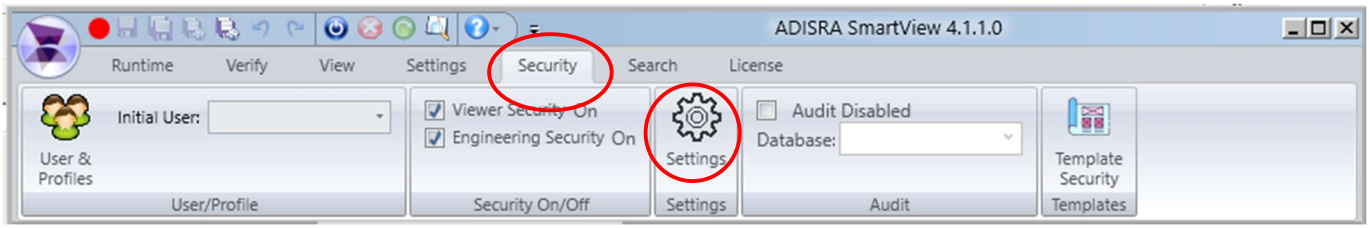
Implementing Electronic Signature in ADISRA SmartView

To implement Electronic Signatures in ADISRA SmartView, there are three configuration steps that need to be implemented.

Step 1: Enable the Security System

ADISRA SmartView had its own built-in security system which you can use to configure Users, Profiles and Passwords. Additionally, you can use an LDAP Domain Security Server as an alternative to the ADISRA SmartView security system.

To use the ADISRA SmartView security system, open the Engineering Environment. In the top ribbon the Engineering Environment, there is a Security tab. Click on the Security tab to open the Security settings. By default, the Engineering Security On checkbox is unchecked. It is recommended to add security to both the Runtime as well as the Engineering Environment. This is done by checking the Engineering Security On checkbox in the Security On/Off section.



Security System Settings

In the Security Settings checkbox, there are several checkboxes that can be used to configure the Security settings for your project. These include:

- **Logoff after xx minutes idle**

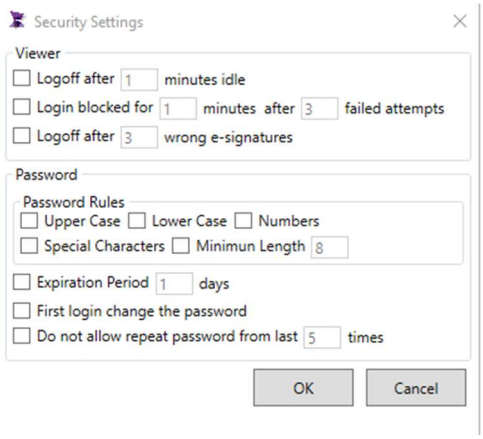
This setting, if checked, will log off the user after there is no more user activity within xx minutes.

- **Login blocked for xx minutes after yy failed attempts**
  This setting, if checked, will not allow a user to attempt to log in to the system after a specified number of failed attempts.

- **Logoff after xx wrong e-signatures**
  This setting, if checked, will automatically log off the user if a setting changes was attempted to be made but there was an invalid e-signature verification made after xx attempts

- **Password Rules**
  There are several Password rule settings that define the type and length of characters required for a password, as well as the expiration period for a password. For an electronic signature application, it is suggested that you use password rules that the various rules (upper & lower characters, numbers and special characters and minimum length to make to password virtually impossible for an unauthorized user to hack.

  Note: Both the User Name and Password are case sensitive



Security Settings

Next, you can add Users and Profiles to the project. To do this, click on the Users and Profiles button.

Security System Settings

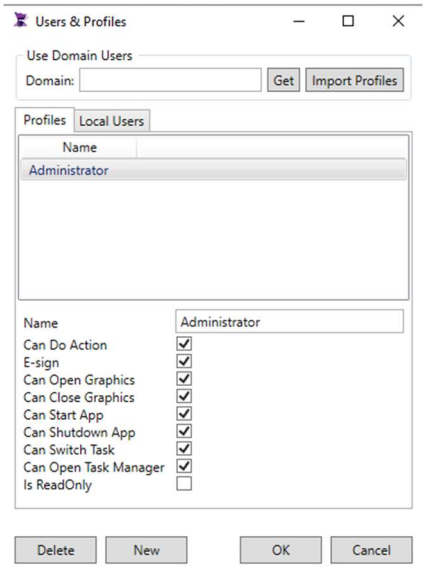
This will open a Users & Profiles dialog box. A User is the name or identifier of a unique individual. Every User must have a unique User name. Every User will have their own unique password that meets the Security Settings requirements set in the Password Rules in the Security Settings dialog box.

A Profile is a grouping of Users, such as Operators, Administrators, Managers, etc. When you configure a graphical object to e-sign, you enable the object e-signature ability by one or more Profiles, not by a User name.

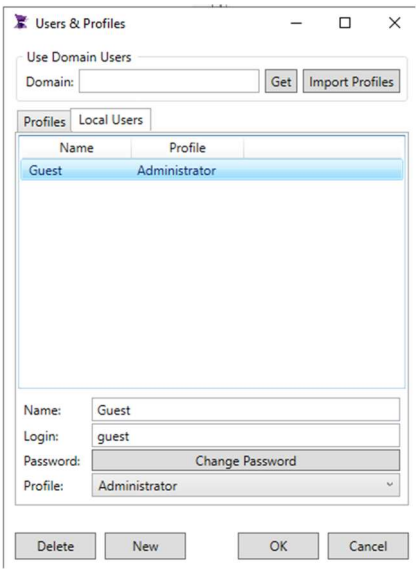
Note in the Users & Profiles dialog box, there is a tab for Profile settings and a tab for User settings. In the Profile settings of this dialog box, there are settings (check boxes) to allow certain actions by a User that is part of a

Profile. For example, there is a E-sign checkbox that will require an e-signature verification before any action is executed when activating the object such as a button or slider, or entering a value into a textbox.

With the Local Users tab, you can add or delete users, or change a User's password. The User names and Passwords (and Profiles) are stored in an encrypted file in the Project folder. Note that any new User added will need to meet the Password Rules requirement. You can also select the initial user in the User/Profile dialog box



Users & Profiles Settings - Profiles

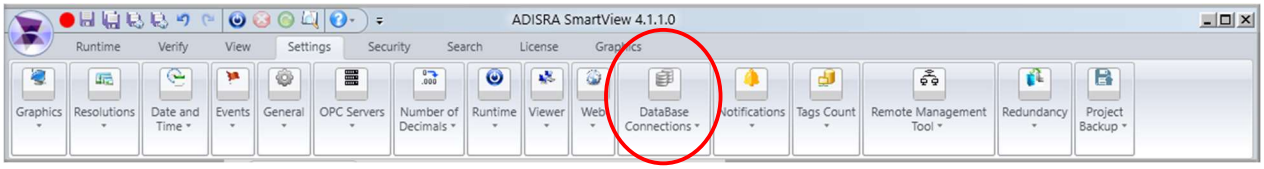


Users & Profiles Settings - Users

Step 2: Configure an Audit Database

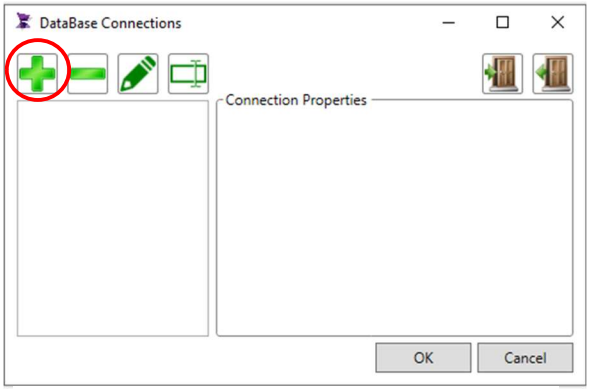
All activities that requires an e-signature (e.g. changing operational setting such as time, temperature, ingredients) are recorded in a SQL database, not a proprietary file system. In ADISRA SmartView, this SQL table to store e-signature activity is called an Audit database. To set up an Audit database, you need to implement the following steps:

a) Configure a SQL database
To configure a SQL database, you first need to open the Engineering Environment of ADISRA SmartView, and in the main ribbon (top portion), you need to click on the Database Connections tab.



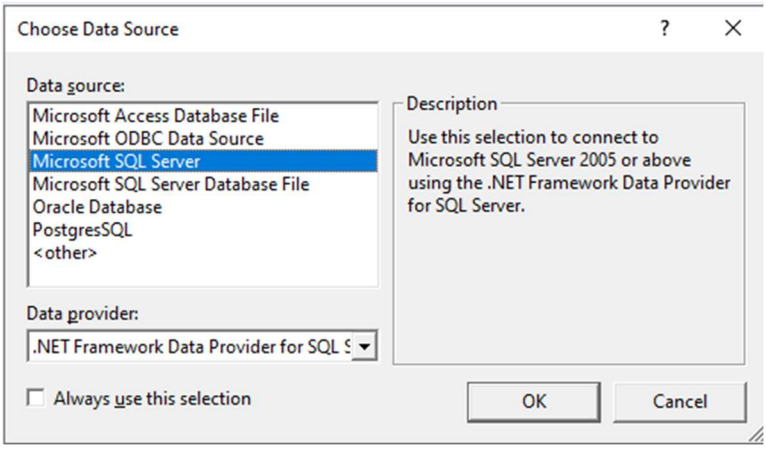
Main Ribbon

Once you do this, it will open a Database Connections dialog box. Click on the **+** symbol in the upper left corner to add a new SQL database table.



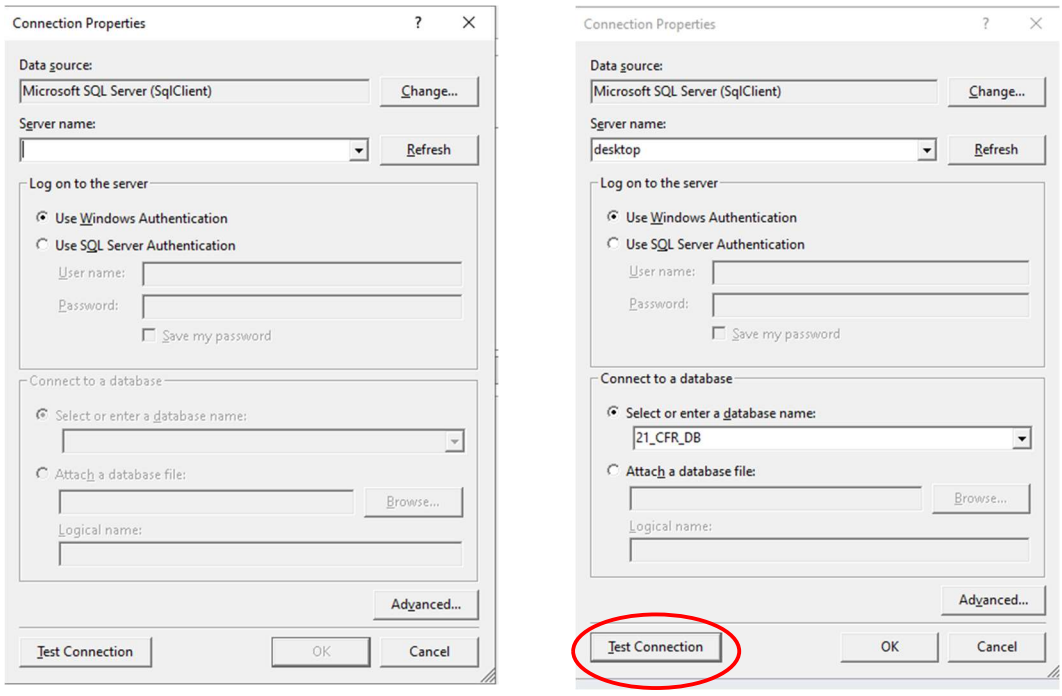
Database Connections Dialog Box

Next, you will choose the Data Source. Note that there are different Data Sources supported in ADISRA SmartView, such as Microsoft SQL Server, Microsoft Access, Microsoft ODBC, Oracle and PostgresSQL. In this example, the Microsoft SQL Server database connection was specified.



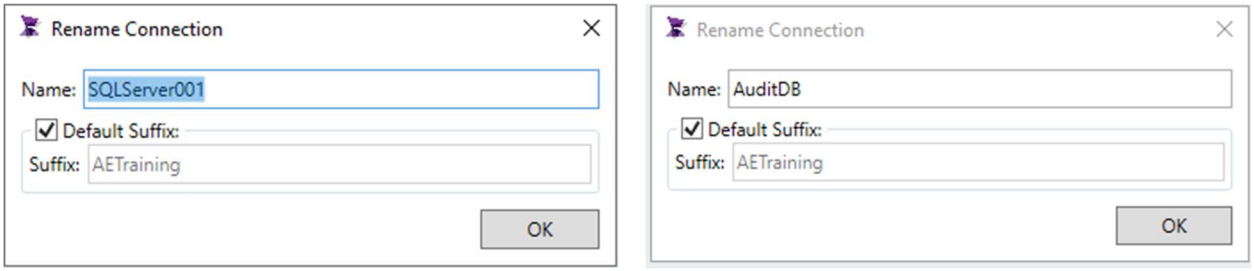
Database Source Dialog Box

When you click on the OK button, this will open a Connections Properties dialog box to allow you to define the Database Server (name) you want to use. Specify the Database Server name, the Authentication method and the Database name. Once these values are specified, there is a Test Connection button on the bottom left side of the Connection Properties dialog box that can be pressed to validate the connection to the database.



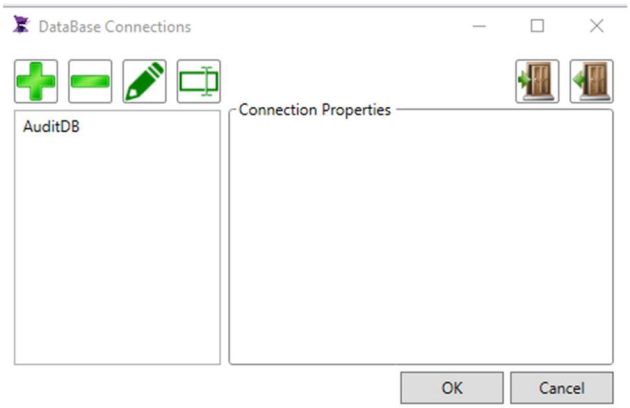
Database Connection Properties

Finally, when you click on the **OK** button at bottom section of the Connection Properties dialog box, it will close the Connection Properties dialog box and open a Rename Connection Dialog box that allows you to rename the database connection in ADISRA SmartView. In this example, the database connection was named AuditDB. Click on the **OK** button when done renaming the Database Connection.



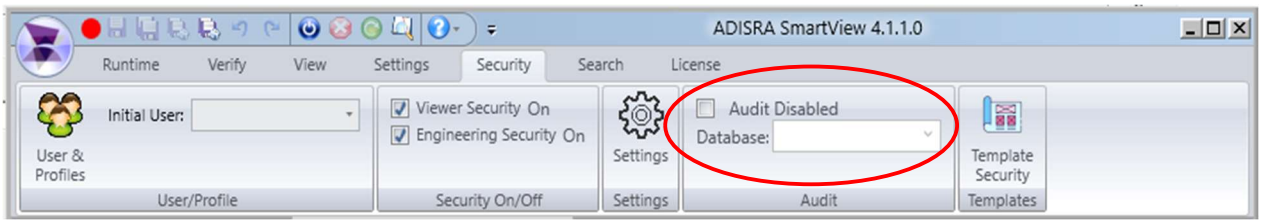
Rename Connection Dialog Box

After you click OK, the new database connection (AuditDB) will be shown in the Database Connections dialog box.

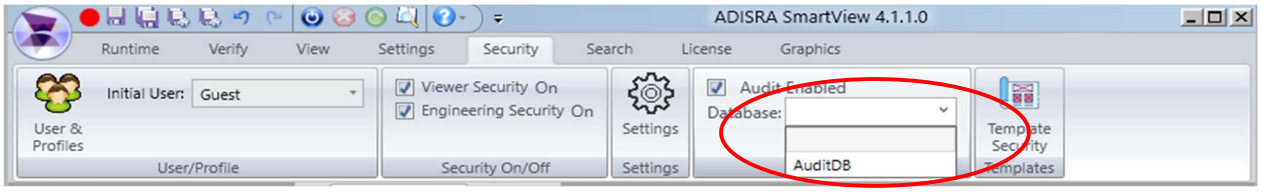


Database Connections Dialog Box

b) Configure ADISRA SmartView to use the database for the Audit log
This final step in this part is fairly simple. You open the Security tab in the top ribbon and go to the Audit settings. If the Audit Enabled checkbox is unchecked, you need to check it to enable the Audit logging.



Security System Settings

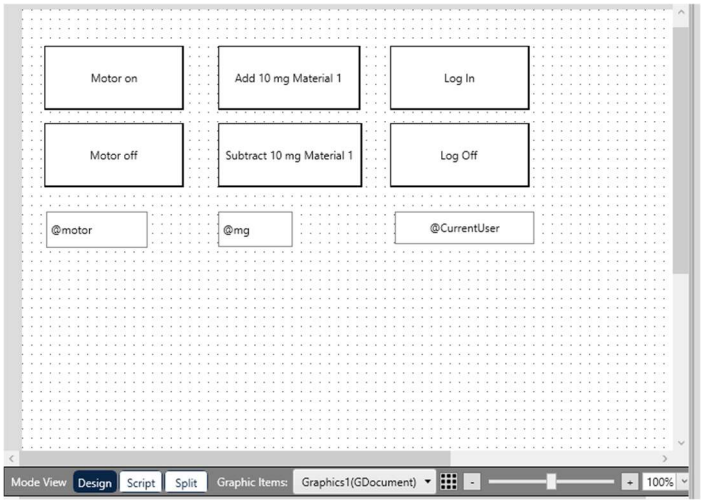


Security System Settings

Once the Audit Enabled checkbox is checked, you can click on the Database combo-box to select the database you want to use. In this example, we will select the AuditDB database.

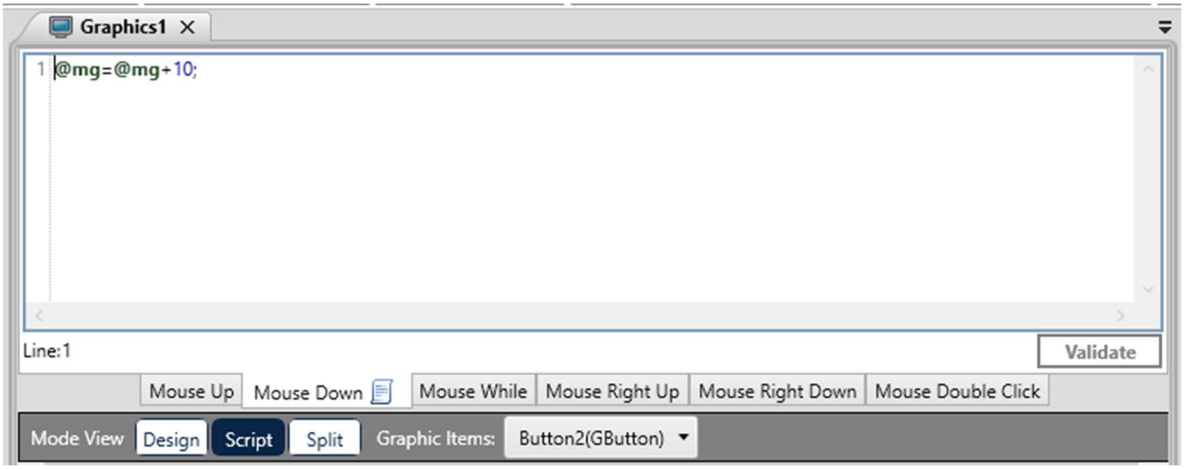
Step 3: Configure an Screen Object

The next step is to add an e-signature requirement to a graphic object that will make changes to the process settings, requiring e-signature verification. In this example, there are six (6) buttons. The first two sets of buttons are for turning a motor on/off and for adding/removing ingredients from the product during production. The last set of buttons are for the user to login and logoff. When one of the first two (2) sets of buttons is pushed at runtime, an e-signature verification is required. Below each set of buttons is a textbox to confirm the motors status, the total milligrams of an ingredient and the current user, which is a system tag named CurrentUser.



Graphics Screen

Let's examine the top middle button which adds 10 mg (milligrams) of material 1 to the production batch. This is a button object.

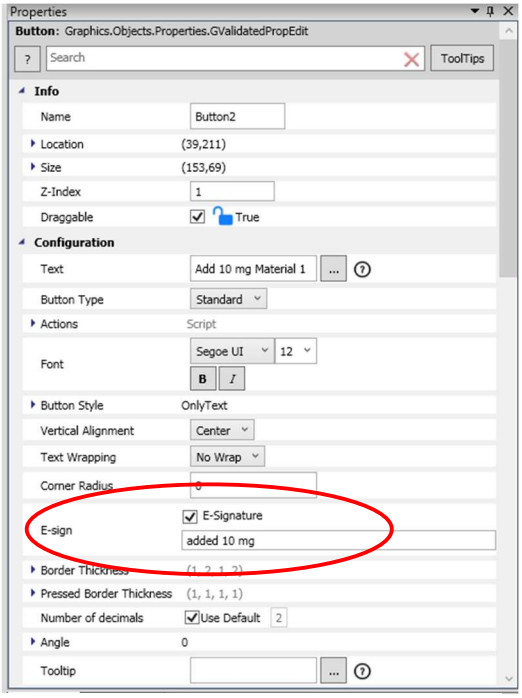


Button Script

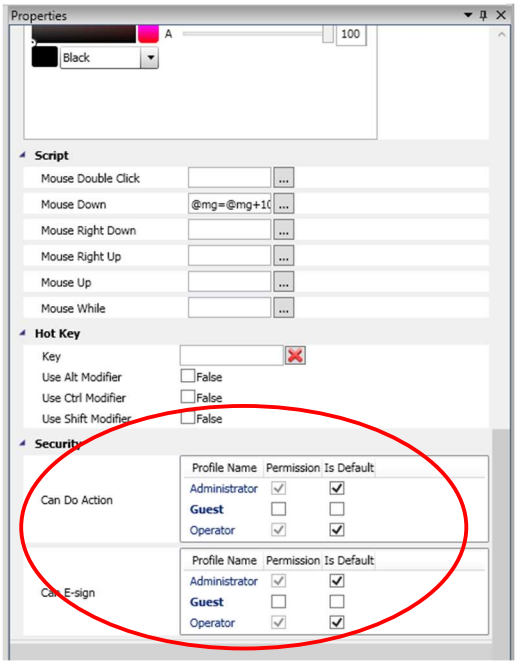
In the button object **Mouse Down** script section, there is code that adds 10 (10 milligrams) of material to the production batch.

Note: if you are using a button with e-signature, you should put the Script in the Mouse Down section, otherwise, it will not execute unless you use a System Security system function in the Mouse Up section. (This will be covered in more detail later).

In the button that is used to add 10 mg of material (top, middle column), there is a Properties dialog box for the button object. Normally this is on the right side of the Engineering Environment.



Button Object Properties Box



Button Object Properties Box

In the top part of the Button Properties dialog box (left side graphic above), there is an E-Sign (electronic signature) checkbox. You will need to check this if you want to have the button object confirm the electronics signature. In the field below, (added 10 mg in this example) is a message that will be written to the audit log when the e-signature is confirmed.

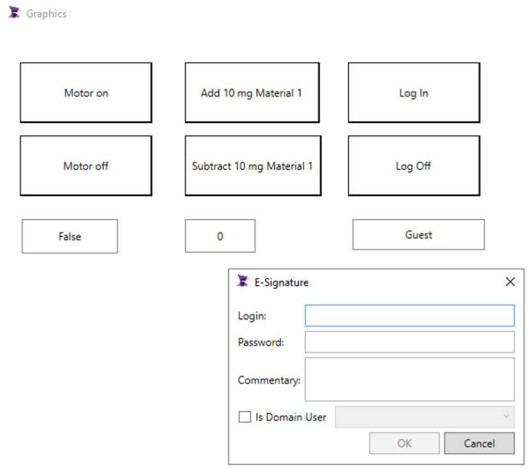
In the lower part of the Button Properties dialog box (right side graphic above), there are some Security settings sections: Can Do Action and Can e-Sign. The Can Do section determines which User Profile can perform an action by clicking on the button. The Can E-Sign section determines which User Profile can electronically sign for the button action to take place. If, for example a button object has the Guest Profile Can E-sign checkbox checked, when a user clicks on the button to initiate the button action, the a e-signature authentication dialog box will appear that will require a User who is part of a Profile that can e-sign to enter their User Name and Password to allow the button object to execute. After it is done executing, it will return back to the User (in this example, Guest).

E-sign checkbox	**Can Do Action**	**Can E-sign**	**Result**
Checked	Unchecked for User Profile	Unchecked for User Profile	Will not take action
Checked	Checked for User Profile	Unchecked for User Profile	Requires a User as part of Profile that can e-sign to confirm e-sign credentials. After button script is executed, the original user is back in control.
Checked	Checked for User Profile	Checked for User Profile	Will allow the current User, even with no password to e-sign.** See notes below.

Notes:

1. All transaction will be recorded in the Audit database
2. **** Be sure that only the Profiles which are configured with Can E-sign privileges are configured to Can E-sign in the Security Settings of the Properties dialog box of an object.**

The following is an example of a run-time e-signature confirmation. Note that in this example, the logged in User was Guest, part of the Guest Profile and had no e-signature privileges. Since the Can Do Action button was checked in the Properties dialog box, while Guest could not initiate the action, another User who was part of a Profile that had e-sign privileges could e-sign and the button action would take place/



Graphics Screen

The following is an example of data that is stored in the Audit database. The **action** field describes the action that took place (e.g. logging in, logging out or an e-sign activity) and a message field. The timestamp is in **ticks**, which is a one-hundred (100) nanosecond time interval from12:00:00 midnight on January 1, 0001 in the Gregorian calendar.

	id	user_loqin	action	messaqe	comment	timestamp
	0	john	login	Login accepted		6386166355960...
	13	john	e-sign	added 10 mg		6386166731282...
	15	john	e-sign	added 10 mg		6386166738585...
	16	john	login failed	Login failed		6386166829880...

Audit Database

In the Log In button, the following command was used: SVSecurity.Login();
In the Log off button, the following command is used: SVSecurity.Logoff();
In this example, there were three (3) Profiles created for this application, Administrator, Operator and Guest. Guest is the User activated when you log off.

In addition, ADISRA SmartView provides SVSecurity that can be used programically with certain objects to execute the e-signature function in the **On-Up** action section or with graphics objects that do not natively have e-signature configuration settings. These System Functions include:

Function	
SVSecurity.ShowEsignWindow	Shows the e-sign dialog box. If the User is part of a Profile that can e-sign and their credentials are entered correct, the function will return a Boolean True value.
SVSecurity.ValidateEsign	Passes e-sign credentials in a function and validates if the credentials are correct (return a Boolean True value if correct).

Summary
If you are configuring an application for manufacturing of pharmaceutical or biotech products, or for medical devices, you will need comply with the e-signature requirements of 21 C.F.R. Part 11 requirements. But many other companies, such as food and beverage manufacturers, also use e-signature for configuration settings so they can track production setting changes. Since the implementation of 21 C.F.R. Part 11 in 1979, the use of e-signature technology had been used in a wide diversity of applications.

E-signature technology is built into ADISRA SmartView and can be easily implemented to meet your production and business requirements. Please note that while e-signature technology is built into ADISRA SmartView for easy configuration, it is also the implementation of this technology that needs to meet FDA requirements. For any questions, please contact ADISRA.