Proficy Plant Applications 2022

Electronic Signature

We want to hear from you. If you have any comments, questions, or suggestions about our documentation, send them to the following email address:

doc@ge.com

Table of Contents

Electronic Signatures

The Electronic Signature (eSig) option provides a highly secure environment by requiring that operators electronically "sign" for all database process changes resulting from data entry and alarm acknowledgement. Electronic signatures uniquely identify the user making the change, and can optionally require the electronic signature of another person to verify the change. Operators no longer need to use paper and pen to record and sign for their actions, and the possibility of losing or damaging such records is essentially eliminated.

With the eSig option, detailed permanent records of operator actions are now written to and stored in a relational database. You can query and report on these records, and then use this data to provide a comprehensive audit trail detailing the history of your process. The electronic signature audit trail provides greater versatility than paper trails. You can query and analyze data quickly and conveniently. Additionally, record tracking through electronic signatures increases security for process changes and alarm acknowledgements.

The electronic signature capability also addresses the needs of Plant Applications users who must conform to the 21 CFR Part 11 United States FDA government regulation. Using the feature by itself does not ensure compliance; however, applications built using the Electronic Signature option can help provide the necessary electronic verification needed to satisfy the requirements of this regulation. For more information, see Understanding 21 CFR Part 11.

What are Electronic Signatures?

Electronic signatures are the computer-generated, legally binding equivalents of handwritten signatures. They uniquely identify the person(s) responsible for an action.

An electronic record is generated each time an action is signed for. Electronic records consist of the name of the person(s) involved in the signing process, and other details, such as the type of action performed. Electronic records are written to the ESignature table in the Plant Applications database, and retained as a permanent record of a signed action.

Depending on how your displays are configured, a signed action may require a supervisor or another operator to verify or validate the action performed by an operator. The concepts of *User* and *Approver* provide the foundation of understanding how electronic signatures work in Plant Applications.

An electronic signature is either a *User* signature or a *Approver* signature:

- **User** signature – the operator (the "performer") that initiated the action must electronically sign for that action.

- **Approver** signature – the operator (the "performer") that initiated the action must electronically sign for that action and another individual (the "approver") must electronically sign to validate the action. The action is not initiated until both signatures are entered. To require an approver signature, the approver must have a minimum of manager rights to a security group assigned to the display or, if no security group has been assigned to the display, the approver must have a minimum of manager rights to the Administrator security group.

  NOTE: The person who performs an action cannot be the same person who verifies the action.

A signature consists of two components that uniquely identify the signer: a user name and a password. When the operator performs an action or verifies an action, a dialog box appears in which the operator must enter these two identifiers:

- **User Name:** Name of the user performing the action or verifying the action.

- **Password:** Password for the user performing the action or verifying the action.

> **NOTE:** *If an operator's Plant Applications user account was established using Windows security, his Plant Applications user name and password are the same as his Windows user name and password.*
>
> *For information about creating Plant Applications site users, please see, Add Site Users.*

When an operator performs or verifies an action, he can optionally enter a comment related to that action. The operator can select or change a pre-defined comment, or enter an original one.

What Determines a Signed Action?

Operators can perform many actions in the Plant Applications Client program. The following table details the actions that will require an electronic signature when electronic signing is enabled in Plant Applications.

Display	Action requiring electronic signing
Autolog	• Changing a test value. • Changing the status of an event (for example, changing from the status Complete to Inventory). • Inserting, updating, or deleting a product change. • Editing any production event information.
Downtime	• Inserting, updating or deleting a downtime event.
Genealogy View	• Editing an event. • Moving an event into the staged or running position. • Linking parent/child events.
Sequence of Events	• Editing any event. • Inserting a user-defined event.
Waste	• Inserting, updating, or deleting a waste event.
Alarm View	• Updating or acknowledging an alarm.

Tracking Electronic Signatures

Each time an operator signs for an action, a detailed electronic record is written to the electronic signature audit trail. Records written to the electronic signature audit trail:

- Ensure a tamper-resistant, time-stamped, permanent record of operator actions.

- Include the user names and full names of all operators and supervisors involved in signing and verifying actions.

- Include all comments entered by the operators and supervisors involved in signing and verifying actions.

- Are recorded in a relational database.

Getting Started

This section presents an overview of the tasks required to implement the Electronic Signature option. It contains a brief description of how the option is licensed from GE Intelligent Platforms. Most importantly, this section contains information and suggested strategies on implementing the security necessary to use the Electronic Signature option. It includes the following topics:

- Implementing Electronic Signatures

- License and Key Checking

- Using Windows User Accounts

Electronic Signature

- [Database Changes](#)
- [Electronic Signature Dialog Box](#)

Understanding 21 CFR Part 11

21 CFR Part 11 is a United States Government Food and Drug Administration (FDA)-mandated regulation that requires all electronic records and signatures, paperless records, and reporting procedures related to the manufacture of a product be captured and stored securely for businesses under its control, such as the Bio-Pharmaceutical and Food and Beverage industries. This regulation requires the protection, accuracy, and quick retrieval of all records. Secured, computer-generated, time-stamped audit trails must be available to independently record the date and time of operator actions that modify the manufacturing process.

Electronic records can be used to identify the ingredients and people involved in the production and distribution of regulated substances, such as prescription drugs. Additionally, electronic records ensure accuracy, reliability, and security in data collection and record keeping.

Regulated industries that fail to meet 21 CFR Part 11 compliance risk the chance of Inspectional Observations (483s), warning letters, or the authorized shutdown of one or more operations.

The Electronic Signature option included with Plant Applications allows you to design an application that helps meet the demands of this regulation. The paperless environment that results from using this feature benefits you with faster information exchange, improved ability to integrate, trend, and search data, a reduction in errors, and reduced data storage costs.

Using Our 21 CFR Part 11 Services

GE Intelligent Platforms offers 21 CFR Part 11 consulting services to assist you with your goal of achieving 21 CFR Part 11 compliance. Using these services, you can reduce the time, effort, and expense of developing, implementing, and maintaining a compliant solution to meet the regulation. These services include:

- Training
- Assessment
- Detailed Detection
- Maintenance

For more information, contact your GE Intelligent Platforms representative.

Implementing Electronic Signatures

The following provides an overview of the steps necessary to implement electronic signatures in Plant Applications.

To implement Electronic Signatures:

1. Ensure that the Proficy server has a hardware key that has been configured with the Electronic Signature option enabled. Contact your GE Intelligent Platforms sales representative for licensing information.

2. Create site users and user groups. For more information, see Security Management.

3. Modify the following site parameters:

   - PointVerification
   - ESignatureInactivityPeriod
   - ESignatureRequireAuthentication
   - ApproverDefaultReasonTreeId
   - ApproverDefaultReasonId
   - UserDefaultReasonTreeId
   - UserDefaultReasonId

4. Enable electronic signatures on the various Plant Applications features.

   - Events
   - User-defined events
   - Alarms
   - Variables
   - Autolog
   - Downtime
   - Waste
   - Genealogy View

License and Key Checking

To use the Electronic Signature option, you must purchase the option from GE Intelligent Platforms and receive hardware keys with this functionality enabled. You must install the keys on the Proficy server.

When the Electronic Signature option is enabled, you may be required to sign for actions you perform during run time. When the Electronic Signature option is disabled, you can perform actions without needing to sign for them.

Database Changes

To support electronic signatures in Plant Applications, a new column, Signature_ID has been added to the following tables in the Plant Applications database:

- Tests and Test_History tables

- Events and Event_History tables

- Event_Details and Event_Detail_History tables

- Timed_Event_Details and Timed_Event_Detail_History tables

- Waste_Event_Details and Waste_Event_Detail_History tables

- Sheet_Columns and Sheet_Column_History tables

Electronic Signature
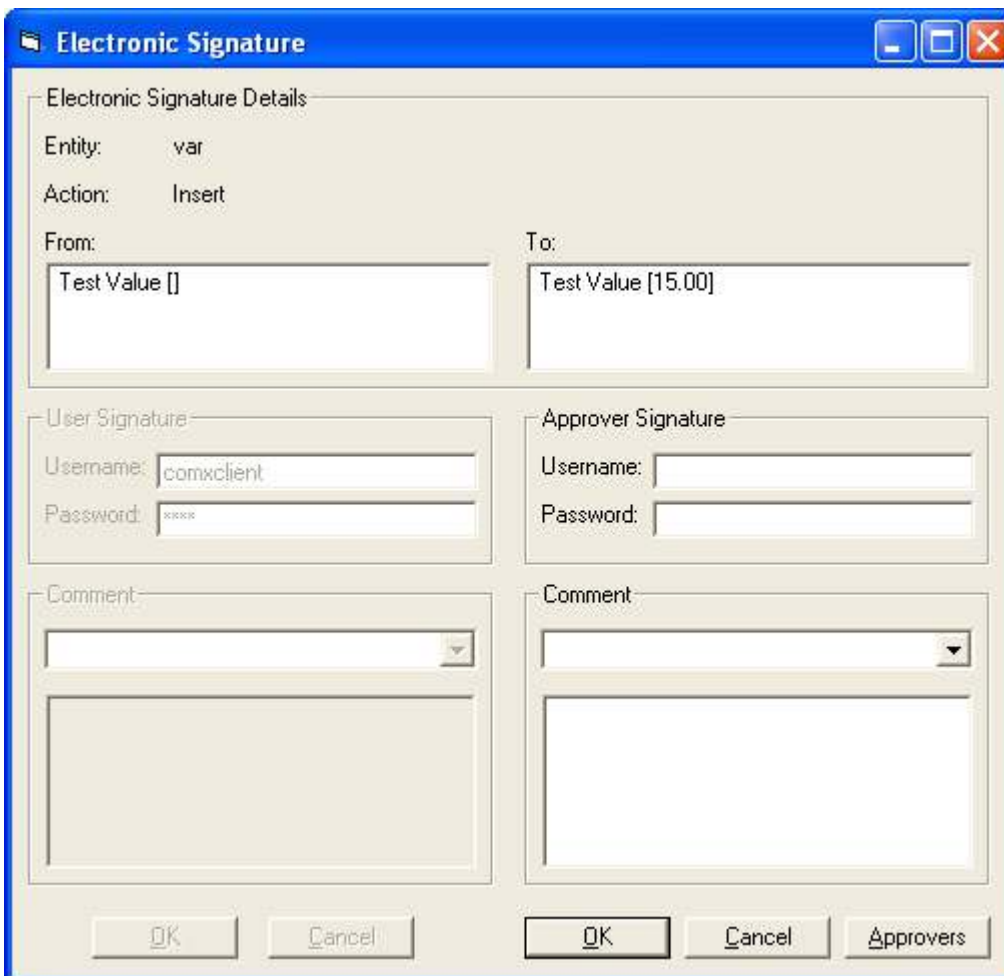
- Production_Starts and Production_Starts_History tables
- PrdExec_Input_Event table

Additionally, a new column, ESignature_Level, has been added to Alarm_Templates table.

Electronic Signature Dialog Box

The Electronic Signature dialog box appears each time an operator performs an action that requires an electronic signature. If the object or action requires a User signature, the User Signature section will be available for input. If the object or action requires Approver signature, the Approver Signature section will become available for input after the User information has been completed.

After a successful authentication, a new row is added to the ESignature table in the Plant Applications database.

Electronic Signature Dialog Box after User authentication and requiring Approver authentication

The following information explains each section of the Electronic Signature dialog box:

Electronic Signature Details: This section of the dialog box describes the action to be signed for.

- **Entity:** The entity that required the electronic signature.
- **Action:** The action that was performed that required approval.
- **From:** The original value or status of the entity that was changed.

5

- **To:** The change that was made.

User Signature: This section of the dialog box is available for input of the User information.

**Approver Signature:** This section of the dialog box becomes available:

- If an approver signature is required

    -and-

- After the user has supplied the correct User Signature information and clicked **OK**.

Username: The user name (and domain, if necessary) of the User or Approver. If Windows user account information is being used, the user types his Windows user account name; otherwise, he types his Plant Applications user name. If ESignatureRequireAuthentication site parameter is set to True, then after signing the first time, the User's user name will be provided and only a password will need to be provided.

Password: The password of the User or Approver. If Windows user account information is being used, the user types his Windows user account password; otherwise, he types his Plant Applications password.

Comment: This section of the dialog box displays the reason and provides an area where you can type additional information or paste a file, such as a text file. The reason specified by the UserDefaultReasonId site parameter or ApproverDefaultReasonID site parameter is displayed in the list, which contains all reasons that belong to the reason tree specified by the UserReasonTreeId site parameter or ApproverReasonTreeId site parameter.

Approvers button: Click this button to open the **Approvers** dialog box to view a list of site users who have Approver authority. This dialog box only displays a list of Approvers. You cannot select an Approver from the list. Click the **Close** button to close the dialog box.
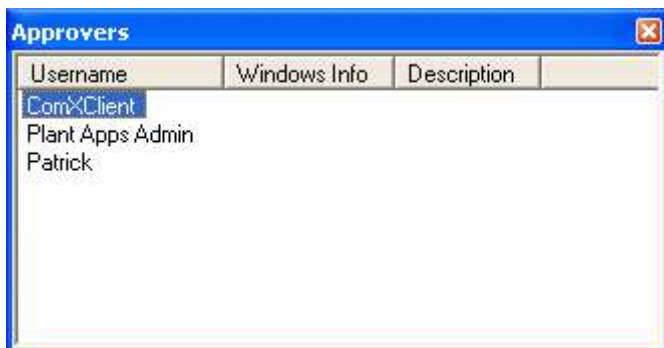
Approvers Dialog Box

Using Windows User Accounts

We encourage you to use Windows user accounts to provide a more robust security environment, as either part of a strategy to reach 21 CFR Part 11 compliance or as a means to provide an additional level of security within any operation. By leveraging this functionality, you can add password expiration control and account lockout to your overall security environment.

If you want to build an application with the goal of achieving compliance with the 21 CFR Part 11 regulation, we strongly encourage you to use Windows user accounts when using the Electronic Signature option within Plant Applications. Windows user accounts allow for password expiration and account lockout, which ensures a more secure signing environment. When your Windows password expires, you can change it without leaving Plant Applications, either when you log in or when you enter an electronic signature. For more information, see the site parameter **EnableChangePasswordDialog** in the topic, Plant Applications Site Parameters.

Password Expiration Considerations

When a user logs in or enters an electronic signature at run time:

- If the Windows password has expired, the user is notified and prompted to change the password.

- If the Windows password is about to expire, a notification message displays, reminding the user to change the password.

If you do not want passwords to expire, you can enable the Password Never Expires option in the Windows security configuration. If you do not want operators to change passwords, you can enable the User Cannot Change Password option in the Windows security configuration.

To enable users to change their Windows security password, the site parameter, **EnableChangePasswordDialog**, must be set to **True**. For more information, see Plant Applications Site Parameters.

Account Lockout

The application developer can set an account lockout threshold, which prevents a user from accessing the account after he enters an incorrect user name or password beyond the number of acceptable times.

When a user logs in or enters an electronic signature at run time, he receives an error if the account has been disabled. The application developer can configure the message to display with the error, such as a telephone number or the name of a contact person; otherwise, a general message displays.

To determine the number of login attempts, you must set the site parameter, **MaxLoginAttempts**. For more information, see Plant Applications Site Parameters.

Additional Considerations

This section contains some suggested strategies for configuring a 21 CFR Part 11 environment.

Disabling the Ability to Change the System Time:

Application developers may want to disable an operator's ability to change the system time by removing the "Change the system time" user right from the appropriate user accounts in Windows security. By doing so, you can prevent inaccurate timestamps from entering the audit trail.

Enabling Auditing in the Windows Security System:

Application developers who want to monitor Windows security events, such as logon and logoff, should enable auditing in the Windows Local Security Policy. You can display these events in the Windows Event Viewer's security log.

Configuring Electronic Signatures

This section introduces the tasks the application developer must complete to enable electronic signatures in Plant Applications. The topics covered in this section include configuring electronic signature for:

- The Plant Applications Administrator program
- The Plant Applications Client program
- Events
- Variables
- Alarms
- Genealogy View
- Waste
- Downtime
- Sequence of Events

Configuring Electronic Signature for the Administrator

To enable the Electronic Signature option:

1. Add site users.

2. If you want to use Windows user account information, you must:

    a. Import the users Window user account information.

    b. Set the WindowsAuthentication site parameter to **True**.

3. Set the PointVerification site parameter to **True**.

In addition to adding site users, there are site parameters that must be set in the Plant Applications Administrator if you want to require an electronic signature when making certain changes in the Administrator.

*NOTE: You must have **Administrator** access in the **Administrator security group** to edit site parameters.*

ESignatureInactivityPeriod Site Parameter

This site parameter applies to both the Plant Applications Administrator and Client programs. The value entered for this site parameter is the number of minutes a user has, following an authentication, to make additional changes without having to authenticate again. For example, let's say the site parameter is set to **2**. After you make a change and authenticate that change, you have two minutes to make additional changes without having to authenticate the changes. Additionally, any change you make within the two minutes will reset the clock to give you another two minutes.

NOTE: The site parameter applies only to user-level authorization. Approver-level authorization will still be required regardless of how this site parameter is set.

PointVerification Site Parameter

If the PointVerification site parameter is set to **True**, when certain changes are made in the Plant Applications Administrator program, the user who made the change will have to verify his or her identity by entering their user name and password in the User Level Authentication dialog box.

Additionally, when this site parameter is set to **True**, the 🔒 **Unauthenticate** button will be enabled on the Plant Applications Administrator toolbar.

To further enhance this feature, you can edit the ESignatureInactivityPeriod site parameter.

*NOTE: You must have **Administrator** access in the **Administrator security group** to edit site parameters.*

WindowsAuthentication Site Parameter

*NOTE: This site parameter must be **True** if you want to use the Windows Info and Mixed Mode options that are available when adding or editing a site user's properties.*

If this site parameter is set to **True** and you imported the user's Windows information and you selected the Mixed Mode option, then the user can log in with either their Plant Applications name and password or their Windows name and password. When the user starts either the Administrator or Client program, Plant Applications will use their Windows name and password to automatically log them in.

If this site parameter is set to **True** and you imported the user's Windows information and you did not select the Mixed Mode option, then the user must log in using their Windows name and password. When the user starts either the Administrator or Client program, Plant Applications will use their Windows name and password to automatically log them in.

If this site parameter is set to **False**, then the user must log in with their Plant Applications name and password, even if the Windows Info was provided for the site user.

*NOTE: You must have **Administrator** access in the **Administrator security group** to edit site parameters.*

Unauthenticate Button in the Administrator Program

The 🔒 **Unauthenticate** button becomes active on the Plant Applications Administrator toolbar when the PointVerification site parameter has been set to True.

Click the **Unauthenticate** button to require verification of any changes made, regardless of the value in the **ESignatureInactivityPeriod** site parameter.

If you need to leave your workstation for a brief period, you can click the **Unauthenticate** button to ensure that any additional changes will require user verification. This helps prevent unauthorized changes.

Configuring Electronic Signature for the Client

To enable electronic signatures in the Plant Applications Client program:

1. Add site users.

2. If you want to use Windows user account information, you must:

   a. Import the users Window user account information.

   b. Set the WindowsAuthentication site parameter to **True**.

3. Edit site parameter values.

4. Set display options for individual displays.

Assigning Reasons to Approver Signatures

You can choose to provide a reason for Approver authentication. Whenever an Approver signature is provided, a default reason can be automatically attached to the signature.

*NOTE: You must have **Administrator** access in the **Administrator security group** to edit site parameters.*

The following site parameters must be configured to automatically provide a reason for an Approver signature.

- **ApproverDefaultReasonId:** Use this display option to specify a default approver-level reason. Before you can specify a default reason, you must first specify a default reason tree in the ApproverReasonTreeId display option. For information about reason trees, see Reason Trees.

- **ApproverReasonTreeId:** Use this display option to specify a default approver-level reason tree. You must first select a reason tree before you can specify a reason for the ApproverDefaultReasonId display option. For information about reason trees, see Reason Trees.

NOTE: In versions prior to 4.3, ApproverDefaultReasonId, ApproverReasonTreeId, UserDefaultReasonId, and UserReasonTreeId were display options, rather than site parameters. To support earlier versions (pre-4.3), they are still listed as site parameters. However, for 4.3 versions and later, setting them as display options will have no effect on the display. They must be configured as site parameters.

Assigning Reasons to User Signatures

You can choose to provide a reason for User authentication. Whenever a User signature is provided, a default reason can be automatically attached to the signature.

*NOTE: You must have **Administrator** access in the **Administrator security group** to edit site parameters.*

The following site parameters must be configured to automatically provide a reason for an User signature.

- **UserDefaultReasonId:** Use this display option to specify a default User-level reason. Before you can specify a default reason, you must first specify a default reason tree in the UserReasonTreeId display option. For information about reason trees, see Reason Trees.

- **UserReasonTreeId:** Use this display option to specify a default User-level reason tree. You must first select a reason tree before you can specify a reason for the UserDefaultReasonId display option. For information about reason trees, see Reason Trees.

NOTE: In versions prior to 4.3, ApproverDefaultReasonId, ApproverReasonTreeId, UserDefaultReasonId, and UserReasonTreeId were display options, rather than site parameters. To support earlier versions (pre-4.3), they are still listed as site parameters. However, for 4.3 versions and later, setting them as display options will have no effect on the display. They must be configured as site parameters.

ESignatureRequireAuthentication Site Parameter

If set to **True**, this site parameter overrides the ESignatureInactivityPeriod site parameter. In other words, every change will require user verification regardless of the value set in the ESignatureInactivityPeriod site parameter. However, if the ESignatureRequireAuthentication is set to **True**, then you will need to supply only your password for each user-level verification. Your user name will already be filled in for you. However, anything that requires approver-level verification will still require a name and password.

*NOTE: You must have **Administrator** access in the **Administrator security group** to edit site parameters.*

Unauthenticate Button in the Client Program

The 🔒 **Unauthenticate** button is a security feature that helps ensure the integrity of your data. If you activate this feature, verification will be required for any changes made.

To help prevent unauthorized changes, you can click the **Unauthenticate** button to ensure that any changes will require user verification. This helps prevent unauthorized changes, in the event you leave your workstation unattended.

After a change has been approved, the **Unauthenticate** button becomes active. After you click the **Unauthenticate** button, it is not available unless a change has been made.

If Data Security User sign-off or Data Security Approver sign-off has been given, any changes will reset the sign-off status to **<Unapproved>**.

*The **Unauthenticate** feature will be available only if electronic signature authorization is required for some element of the display, such as variables or products.*

To activate the Unauthenticate feature:

- From the **File** menu, select **Unauthenticate**.

  - or -

  On the toolbar, click the 🔒 **Unauthenticate** button.

Configuring Electronic Signature for Displays

Electronic signatures (e-signatures) help you monitor and authorize changes to data. By using electronic signatures, you can see who changed data and require separate authorization before changes can be made.

There are two levels of authorization: user level and approver level:

- **User level** requires the current user to sign off when certain changes have been made.

- **Approver level** requires the current user to sign off, followed by sign-off from an approved manager, other than the current user and with at least Manager access.

You can enable authorization for changes to individual variables within a display or for changes to events or product changes.

AutoLog and Electronic Signature

In an Autolog display, the following actions will open the Electronic Signature dialog box.

- Inserting or editing a test value for a variable, if the variable has electronic signature enabled. See Configuring Electronic Signature for Variables

- Changing the status of an event or editing an event that has electronic signature enabled. See Configuring Electronic Signature for Product Changes and Events.

- Inserting, updating, or deleting a product change, if the product change event has electronic signature enabled. See Configuring Electronic Signature for Product Changes and Events.

- Inserting, updating, or deleting a column in a time-based Autolog display if the product Events electronic signature is enabled. See Configuring Electronic Signature for Product Changes and Events.

In addition, Autolog displays have four display options that provide added data security.

- **DisplayDataSecurityApprover:** Setting this display option to **True** will add a column heading titled "Data Security Approver" in the Autolog display. To activate this, you must enable e-signature for events on the **General** tab of the **Product Properties** dialog box. Additionally, a table, "Data Security," will be displayed on the Event Details report if the column has been locked. This option must be set to True if electronic signature is being used for Approver verification. To enable electronic signature, see Configuring Electronic Signature for Product Changes and Events.

- **DisplayESignatureLevel:** Setting this display option to **True** will add a column displaying the level of authorization required for changes made to individual variables that have electronic signature configured.

- **DisplayDataSecurityUser:** Setting this display option to **True** will add a column heading titled "Data Security User" to the Autolog display. To activate this, you must enable e-signature for events on the **General** tab of the **Product Properties** dialog box. Additionally, a table, "Data Security," will be displayed on the Event Details report if the column has been locked.. This option must be set to True if electronic signature is being used for User verification. To enable electronic signature, see Configuring Electronic Signature for Product Changes and Events.

- **DataSecurityLockApprovedColumns:** Setting this option to **User Level** or **Approver Level** will lock the columns after authorization and not allow any changes to be made to the columns.

Genealogy and Electronic Signature

In a Genealogy View display when you edit an event by changing its status or using the common dialog, it gets the signature level from the product for that event. When you move events between running, staged, completed, unloaded,and so on, the event the signature level is determined by the **ESignatureLevel** display option. When you add or edit a genealogy link, the signature level is determined by the **ESignatureLevel** display option.

ESignatureLevel Display Option:

You can select either **None** (0), **User Level** (1), or **Approver Level** (2). If you select **Approver Level**, any changes to a Genealogy display will require both a user-level authorization and an approver-level authorization.

Sequence of Events and Electronic Signature

Electronic signature in a Sequence of Events display is controlled by the configuration of the event, such as downtime or alarms.

Inserting a user-defined event or using the detail panel to edit or delete a user-defined event will open the Electronic Signature dialog box. For more information, see Configuring Electronic Signature for UDEs.

Using the detail panel to edit any event will also open the Electronic Signature dialog box.

*NOTE: To view the detail panel, the **DisplayDetailPanel** display option must be set to **True**.*

Configuring Electronic Signature for Product Changes and Events

You can enable electronic signatures for both product changes and events. You can specify either user-level or approver-level signatures when inserting, deleting or editing events.

*In an Autolog display, the column headings, **Data Security User** and **Data Security Approver**, are controlled by display options, **DisplayDataSecurityUser** and **DisplayDataSecurityApprover**. Even though you see these column headings, you must still*

*configure electronic signatures for events or product changes. However, you must set these display options to **True** in order for e-signatures to work.*

1. In the Plant Applications Administrator, expand the Server Manager tree.

2. Expand **Product Management**.

3. Expand **Product Families**.

4. Expand the desired product family.

5. Double-click the desired product. The **Product Properties for <*product name*>** dialog box appears.

6. On the **General** tab, under **E-Signature Levels**:

   o To require electronic signature for events, select **User Level** or **Approver Level** from the **Events** list. You must select one of these options if you want to require user or approver sign-off in Autolog.
   o To require electronic signature for product changes, select **User Level** or **Approver Level** from the **Product Changes** list.

Configuring Electronic Signature for Variables

You can require electronic signatures when test data is entered or changed for variables. You can specify either user-level or approver-level signatures.

Electronic signatures specified for a specification takes precedence over any electronic signatures specified for a variable.

To require electronic signatures for changes to variables:

1. In the Plant Applications Administrator, expand the Server Manager tree.

2. Expand **Plant Model**.

3. Expand the desired **Department**, **Production Line**, **Production Unit**, and **Variable Group**.

4. Double-click the desired variable. The Variable Sheet appears.

5. Scroll to the **ESignature Level** column and select **User Level** to require only the user to sign off, or select **Approver Level** to require both the user and an approver to sign off on any changes made to the variable.

If the column is not visible, click the Column/Row Visibility button to open the Column/Row Visibility dialog box.

Configuring Electronic Signature for Alarms

If you've enabled electronic signature in the alarm template, updating an alarm or acknowledging an alarm in a display will open the Electronic Signature dialog box.

To enable electronic signatures for alarms:

1. In the Server Manager tree, click to expand **Global Configuration**.

2. Right-click **Administer Alarms** and choose **Administer Alarms**. The **Alarm Configuration** dialog box appears.

3. Click the **Search Template** tab to search for a template to edit, or click **Add Template**.

4. Click the **Details** tab and select **User Level** or **Approver Level** from the **Electronic Signature Configuration** list.

Configuring Electronic Signature for UDEs

You can require electronic signatures for user-defined events. You can specify either user-level or approver-level signatures.

To enable electronic signatures for user-defined events:

1. Configure the user-defined event.

2. In the **User Defined Event Configuration** dialog box, click the **General** tab and select either **User Level** or **Approver Level** from the **Electronic Signature Level** list.

Configuring Electronic Signature for Downtime

Inserting, deleting, or editing downtime events in a Downtime display will open the Electronic Signature dialog box.

To enable electronic signature for downtime:

1. Configure a downtime event on the production unit.

2. In the **Event Configuration** dialog box, on the **Enable Events** tab, do the following:

    a. Under **Events Enabled On This Unit**, select the downtime event and click **Event Properties**. The **Downtime Configuration** dialog box appears.

    b. Click the **Other** tab.

    c. Select either **User Level** or **Approver Level** from the **Electronic Signature** list.

    d. Close the **Downtime Configuration** dialog box.

3. Close the **Event Configuration** dialog box.

Configuring Electronic Signature for Waste

In the Waste display, editing waste events will open the Electronic Signature dialog box. If the waste event requires an Approver signature, the Extended Edit dialog box will open.

To enable electronic signature for waste:

1. Configure a waste event on the production unit.

2. In the **Event Configuration** dialog box, on the **Enable Events** tab, do the following:

    a. Under **Events Enabled On This Unit**, select the downtime event and click **Event Properties**. The **Waste Configuration** dialog box appears.

    b. Click the **Other** tab.

    c. Select either User Level or Approver Level from the Electronic Signature list.

    d. Close the Waste Configuration dialog box.

3. Close the **Event Configuration** dialog box.

Electronic Signature in Web Reports

The following web reports and web parts can be configured to display electronic signature information:

Web Applications

- Alarm Detail

14

Electronic Signature

- Downtime Detail
- Event Detail
- User-defined Event Detail
- Waste Detail
- Batch Summary
- Procedure Detail

ASP Reports

- Production Listing
- OEE Summary
- Event History Color
- Event History Grid
- Time History Color
- Time History Grid

Electronic Signatures on Web Applications

By default, electronic signature information is not displayed on web applications, unless the web application was accessed from another report that was displaying electronic signature information. In other words, the parent report passes the eSig parameter to any child reports.

If electronic signature information is specified to be displayed, an **Electronic Signature** table will provide the following information.

- **User:** The user name of the person who provided the user-level verification.
- **User Reason:** The reason selected in the Electronic Signature dialog box.
- **User Comment:** The user comment entered in the Electronic Signature dialog box.
- **Approver:** The user name of the person who provided approver-level verification.
- **Approver Reason:** The reason selected in the Electronic Signature dialog box.
- **Approver Comment:** The approver comment entered in the Electronic Signature dialog box.

If you have configured electronic signature for product changes and events, a **Data Security** table will provide the following information.

- **User:** The user name of the person who provided user sign-off for the product change or event.
- **User Reason:** The reason for the sign-off. See Assigning Reasons to User Signatures.
- **Approver:** The user name of the person who provided user sign-off for the product change or event.
- **Approver Reason:** The reason for the sign-off. See Assigning Reasons to Approver Signatures.

If any of this information is not provided (for example, if approver verification is not required), then the rows will not be displayed. If electronic signature has not been configured, then no electronic signature table will be displayed.

For reports that provide detail information for individual variables, an additional row will be added under the variable that will display electronic signature information.

To display electronic signature information:

1. On the reports toolbar, click the Properties icon. The **Options** dialog box appears.

2. Select the **Display Electronic Signature Information** check box.

3. Click **Ok**. The Electronic Signature information will be displayed.

Electronic Signatures on ASP Reports

Certain ASP reports, which are identified with , have an additional option available when you configure the report, either in the Web Server client or in the Web Server Administrator. Selecting the **Display E-Signature On Report** check box will add two additional columns to the report: User and Approver.

To display electronic signature information:

1. Configure the report. For more information, see:

   o Editing Report Parameters
   o Creating an Ad hoc Report
   o Creating a New Report Definition

2. On the **Options** tab, select the **Display E-Signature On Report** check box.