Security

Overview

XLReporter provides the following security and CFR Part11 features:

- **User Accounts**
  Restrict the capability of a user by credentials. See **User Accounts** section.
- **Access Security**
  Apply access Security to restrict templates and reports. See **Access Security** section.
- **Audit Trail**
  Maintain a log of user activity on configuration changes and electronic signatures. See **Audit Trail** section.
- **File Version Control**
  Archive configuration files with versioning and rollback. See **File Version Control** section.
- **Electronic Signatures (eSignatures)**
  Assign users to apply electronic signatures to reports. See **Electronic Signatures** section.

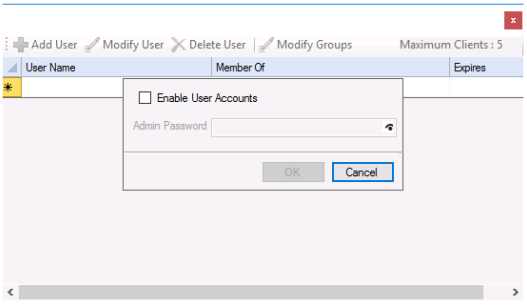
User Accounts

By default, user accounts are disabled. With user accounts disabled, the default user is **Local** which is shown in the bottom left of the **Project Explorer**. This account has no restriction on capability and will exist until user accounts have been enabled.

With user accounts enabled, the capability of users is limited by configuration. User accounts are used in both local and multi-user **Ultimate** editions of **XLReporter**. For example, you may wish to allow a user to view reports but not to generate them on-demand.

Enable User Accounts

From the **Project Explorer** select the **Project** tab and then **User Accounts**. If this is the first time then the following is displayed:



The **Admin Password** is created when user accounts are first enabled.

Enable user accounts by checking **Enable User Accounts**, entering the desired **Admin Password** that will be used if further user account changes are needed, and clicking **OK**. The Admin account cannot be used like any other user account. It is strictly for managing the User Accounts of the project. **Make sure to make a note of the password**. Other Users must be defined in order to close the User Accounts dialog.

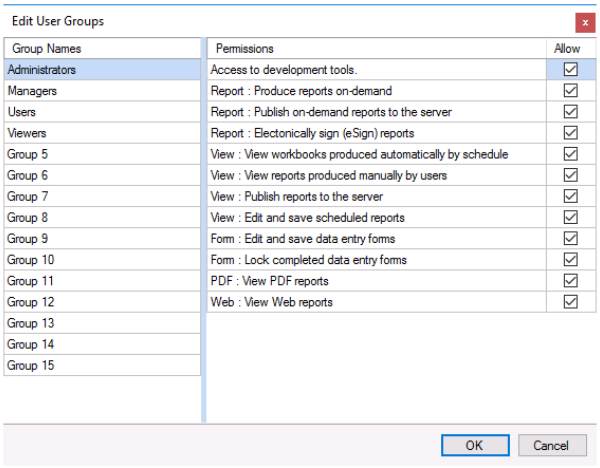
Disable user accounts by entering the Admin Password and unchecking **Enable User Accounts.**

The maximum client count is shown in the top right. The setting is only applicable to the **Ultimate** edition and indicates the maximum number of concurrent users provided by the active software license (also displayed on the **Project Explorer** status window).

Define User Groups

Except for the **Administrators** group, all the **Group Names** can be customized together with the associated **Permissions**.

Select **Modify Groups**.



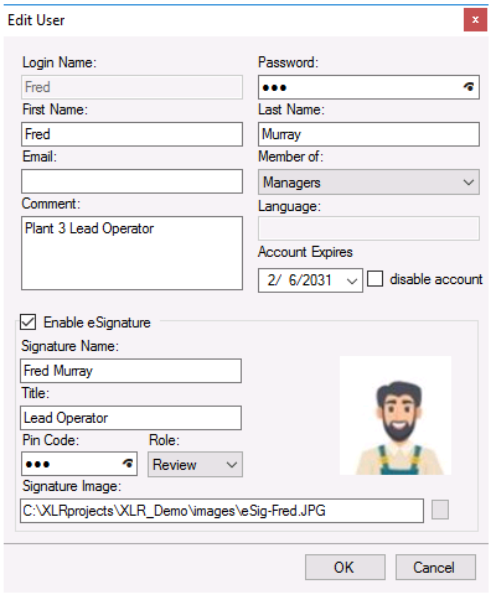
In the left pane are the **Group Names**. Double click a name to edit. Note that the **Administrators** group name cannot be changed.

In the right pane are the **Permissions** assigned to the group. The referenced documents can be found in the Document Library which can be opened from the **Documentation** button in the upper right corner of the **Project Explorer**.

- Access to development tools (see SETUP, **Setup a Project in the Project Explorer**).
- Report: Produce reports on-demand (see REPORT, **Deploy On-Demand Reports**).
- Report: Publish on-demand reports to server (see REPORT, **Deploy On-Demand Reports**).
- Report: Electronically sign (eSign) reports (see **Electronic Signatures (eSignatures)**)
- View: View workbooks produced automatically by schedule (see DISTRIBUTE, **View and Annotate Reports**).
- View: View reports produced manually by users (see DISTRIBUTE, **View and Annotate Reports**)
- View: Publish reports to the server (see REPORT, **Setup the Web Portal**).
- View: Edit and save scheduled reports (see DISTRIBUTE, **View and Annotate Reports**).
- Form: Edit and save data entry forms (see REPORT, **Deploy Data Entry Forms**).
  Form: Lock completed data entry forms (see REPORT, **Deploy Data Entry Forms**).
- PDF: View PDF reports (see DISTRIBUTE, **View and Annotate Reports**).
- Web: View web reports (see DISTRIBUTE, **View and Annotate Reports**).

Define Users

To define a user, click **Add User**.

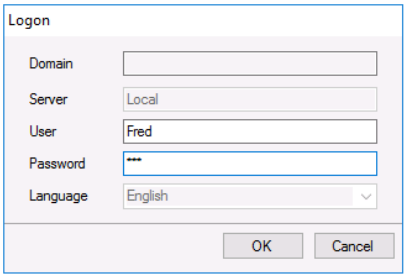


Enter a **Login Name** and assign the user to a **Member Of** a group. The remaining fields are optional. The account will expire on and after the date configured, this feature can be disabled.

Refer to the **Electronic Signature** section for more information on the signature settings.

Log On/Off

When user security is enabled, there are two ways for a user to log on and off. The first is from the **Project Explorer** by clicking **Home Tab**, **Log On/Off** and the second is from the **Team Project Explorer**. In both cases, the user is prompted to specify for a **Protocol** (http or https), a **User** name**,** and **Password**.



Access Security

Report templates are workbook documents and the reports produced from these templates are documents in workbook, PDF, or web format. By default, there is no restriction on opening these documents for viewing and editing. Enabling Access Security will prompt users to enter a password to access the document.

Enable Access Security

To enable Access Security for Workbook or PDF (Web does not support access security), from the **Project Explorer**, select the **Project** tab and then **Security**.

From the **Security** tab, check **Workbook Access Protection** and enter the **Access Code** required to open either a template or a report.

From the **PDF Reports** tab, check **PDF Access Protection** and enter the **Access Code** (see SETUP, **Customize a Project** for more details).

With access security enabled the following will occur:

- When a new template is created, an option to enable access security will be available.
- When a report is created from a template that has access security, either workbook or PDF, the user will be prompted to provide the **Access Code** when the report is viewed.

Please note, this feature is designed to work with **Template Design** set as the *XLReporter Design Studio*.

Audit Trail

The audit trail maintains a log of user activity for the:

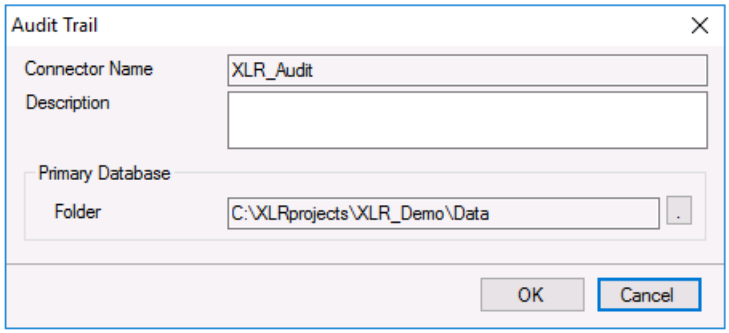
- Alteration of security settings
- Application of an electronic signature (when **Electronic Signatures** are enabled)
- Modification of a configuration file (when **File Version Control** is enabled)

The component requires the **Audit Trail** connector to be defined. To view the user activity, the Audit Trail Viewer is provided.

If User Accounts is not enabled, then the **Local** user is used in the messages of the activity log.
If User Accounts is enabled, then the active username is used.

Enable Audit Trail

From the **Project Explorer**, select the Data tab and choose connectors. **Add** a new connector by selecting *XLReporter* data sources and then *Audit Trail*.

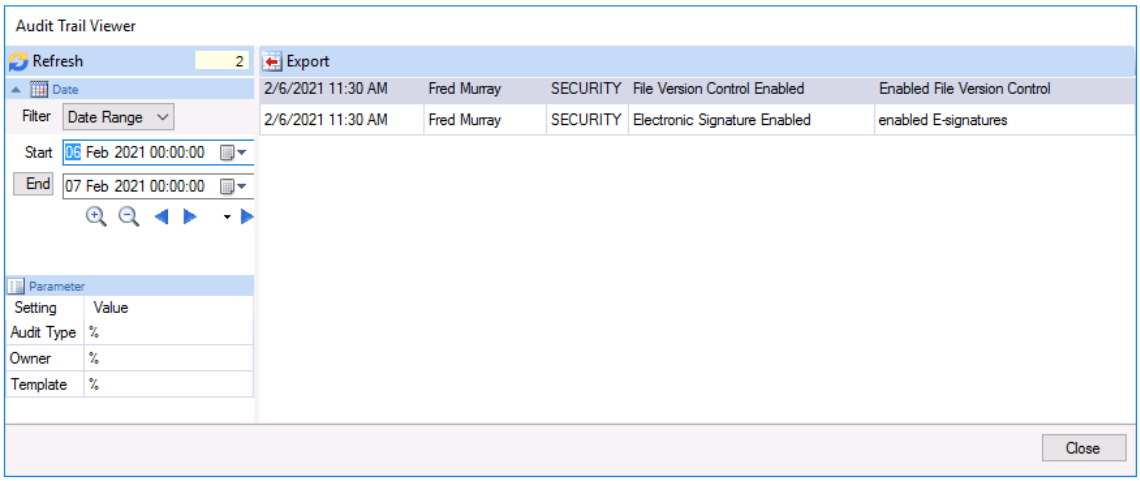


The audit trail database called **Audit.xdb** is created in the *Data* folder of the project. Select the browse […] for a different forlder.
If the database already exists, a prompt to recreate the table(s) in the database will appear. Note that recreating tables will cause all existing content to be erased.

For reference, the addition of the connector to the project is also shown in the Security settings. From **Project Explorer**, select **Project**, **Security**.

Audit Trail Viewer

The audit trail content can be viewed using the Audit Trail Viewer. From the **Project Explorer**, select the **Home** tab and choose **Logs**, **Audit** to view.



In the left pane, filters are used to assist in finding information. Filtering by **Date**, **Audit Type**, **Owner** and **Template** is provided.

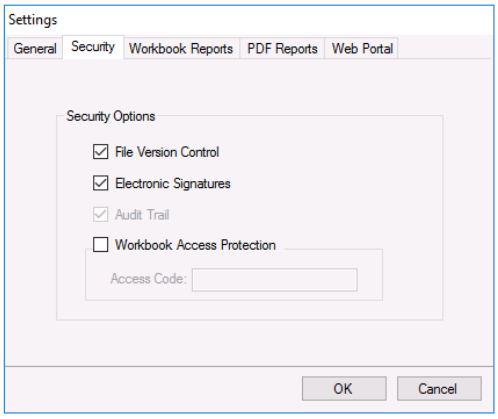
File Version Control

When configuration file changes are performed, **File Version Control** maintains an archive of the configuration files of the project and also provides an audit trail of the user that performed the change.

It is suggested that this option is enabled after the development of the templates is complete.

Enable Version Control

From the **Project Explorer** select the **Project** tab and then **Security.**



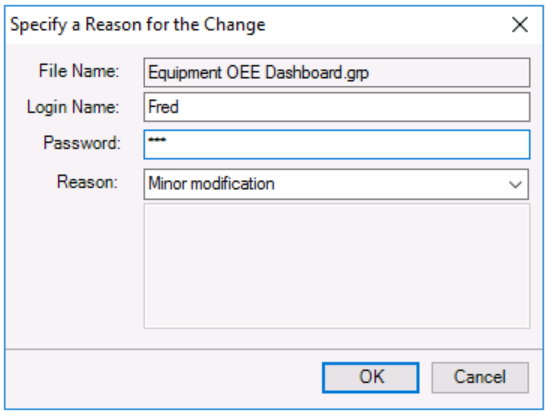
Check **File Version Control** to enable the feature.

This feature requires the **Audit Trail** connector to be defined (see **Audit Trail**). If the connector is not part of the project, then this is indicated on the display.

Applying Version Control

File version control is applied on the save of various report template components which affect the content of the report.

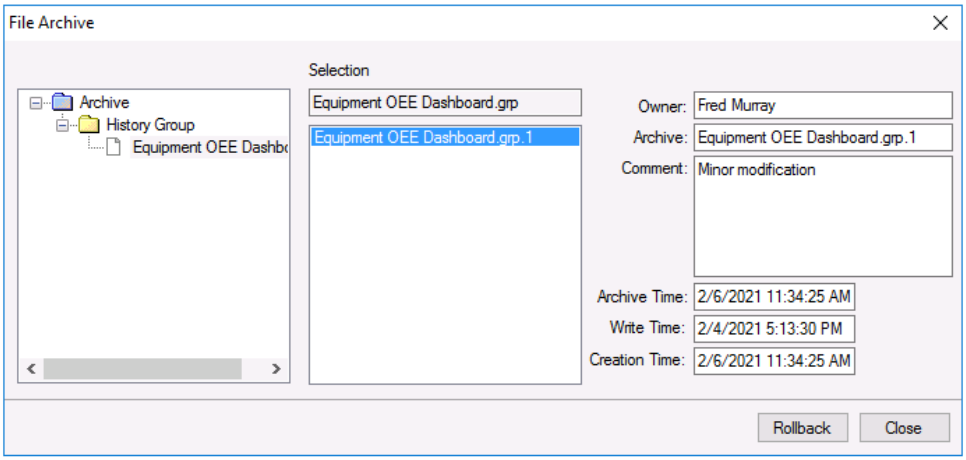
For example, if a template contains a history group connection and the history group content is edited, then the user will be required to specify the reason of the change. This will be performed by the following dialog which appears automatically:



The reason can be selected from a reset list or can be entered by the user. This action will be archived in the audit trail and viewed by the **Audit Trail** viewer

File Archive Viewer

The File Archive viewer is accessed from **Project Explorer**, select the **Tools** tab, and choose **File Archive**.



Under **Archive** are the files that have been changed with File Version active. Selecting a file will display the archive of the file with the naming convention file name followed by a number. Selecting an archive file will show details of who, why and on what date the file was edited.

File Rollback

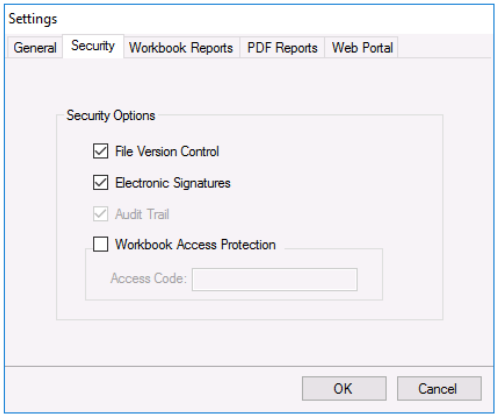
If there is a need to make a file active from the Archive, then select the file and click **Rollback**. A warning will appear which, when accepted with a reason, will make the selected file the active file and log this action to the audit trail.

Electronic Signatures (eSignatures)

Electronic signatures (eSignatures) are a mechanism that allows Users to review and accept completed reports by applying an electronic signature to report documents.

Enable Electronic Signatures

From the **Project Explorer** select the **Project** tab and then **Security.**



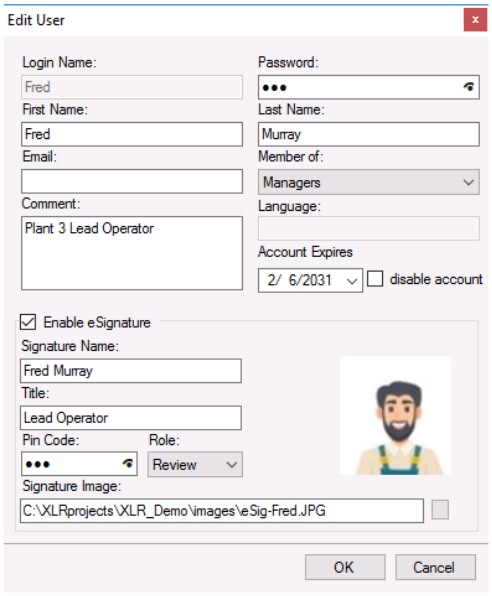
Check **Electronic Signatures** to enable the feature.

This feature requires the **Audit Trail** connector to be defined (see **Audit Trail**). If the connector is not part of the project, then this is indicated on the display.

Add eSignature Credentials to a User

To apply an eSignature, users need to be given the authorization in the **User Account** settings. From the **Project Explorer** select the **Project** tab and then **User Accounts**.

Open the settings of the **User**.



Each user belongs to a user group. If the group permits electronic signatures, then check the **Enable Signature** to configure this user to apply electronic signatures. By default, the **Signature Name** is set to the **Login Name**.

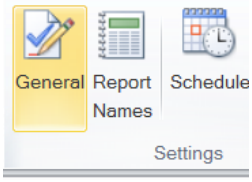
For added security, eSignatures use a 2-step authentication. The first is the **Login Name** and **Password** and the second is the **Pin Code** which will be needed when the User applies the signature.

Each user is assigned a **Role** as *Review*, *Accept*, *Approve or All* which is used when **eSignatures** are added to the template. A report can support a combination of four roles.

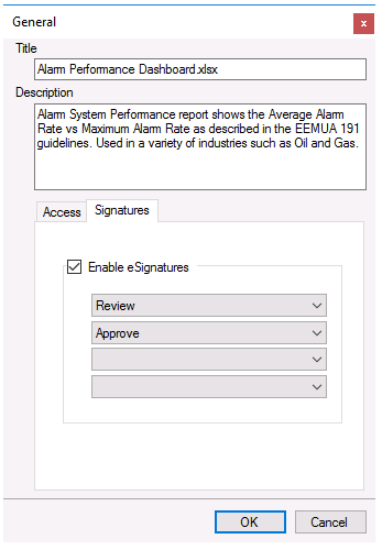
Note that a user can be assigned for *All* roles.

Add eSignatures to a Template

From the **Project Explorer**, select the **Home** tab and choose **Template Studio**. Open a template in the studio and select the **General** settings on the ribbon.



The display shows the groups that can access the report template when it is used on-demand and also the signatures roles that are required when **eSignatures** are applied to the report.



In the above example, two users will be required to complete the eSignature process; one user with *Review* role and one user with *Approve* role.

Produce a Report with eSignatures

Scheduling a template that is configured with eSignatures will automatically produce a report requiring eSignatures.

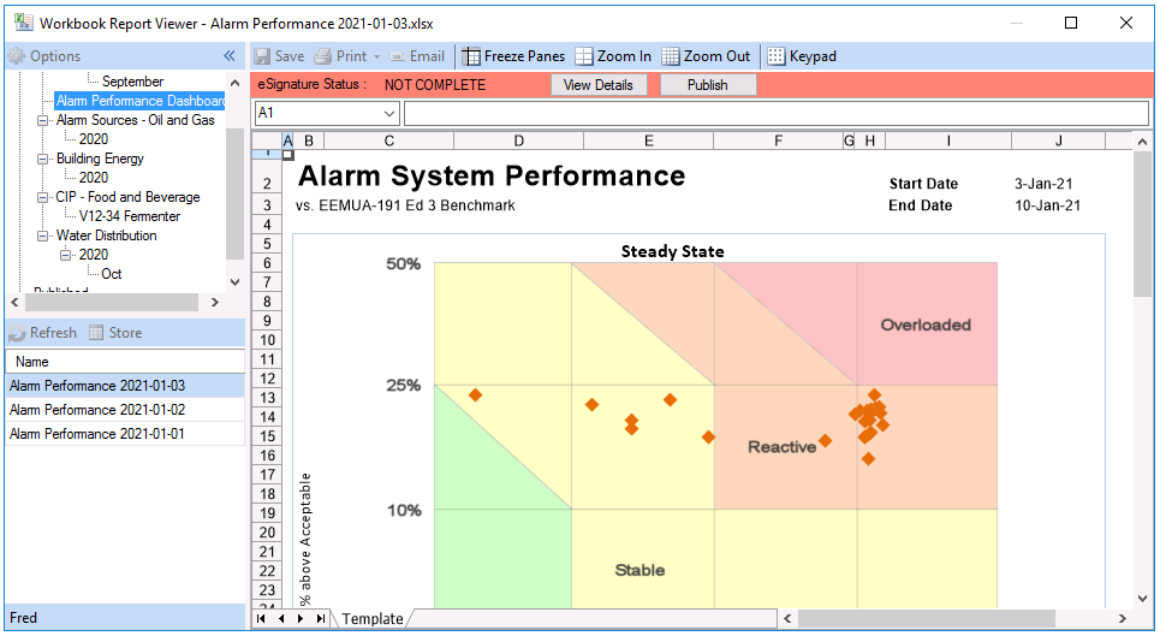
If the report is modified by the scheduler, then any existing signatures will be removed since the signatures were not applied on the completed report. As an example, a report updated periodically over the production of a batch should only be signed when the batch report is complete.

eSignatures Banner

Signatures are assigned to reports in the workbook viewer. From the **Project Explorer**, select the **Home** tab and choose **Workbook Reports**. A similar navigation is from a Team client running on a desktop.

Signature Banner

The signature banner will appear in the viewer if the report being viewed requires eSignatures. Indicating it was generated from a template configured for signatures.

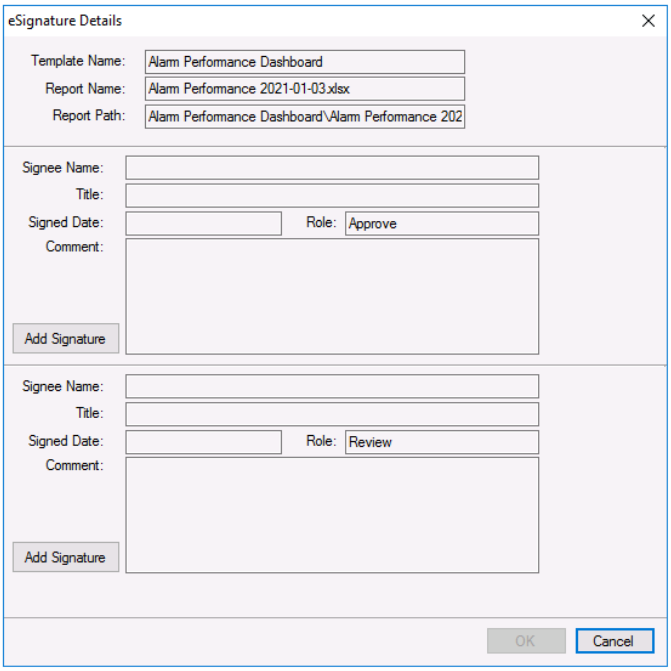


The banner states are:

- Not Visible The report does not require eSignatures
- Red eSignatures have not been entered
- Yellow eSignatures are partially entered
- Green eSignatures are complete

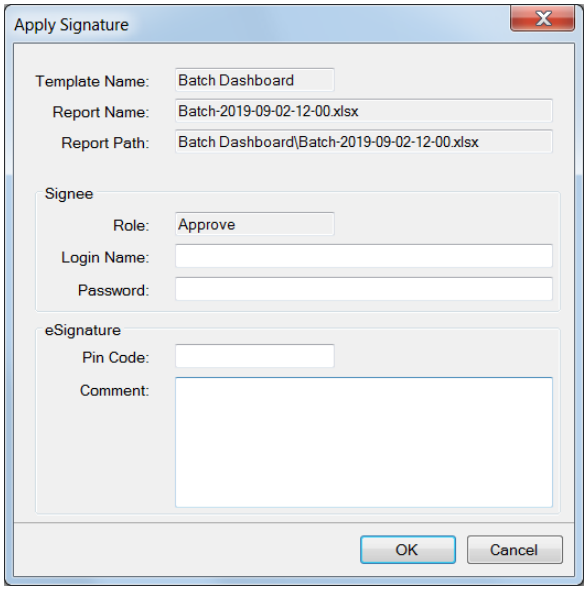
Add eSignatures to a Report

From the banner, click **View Details**.

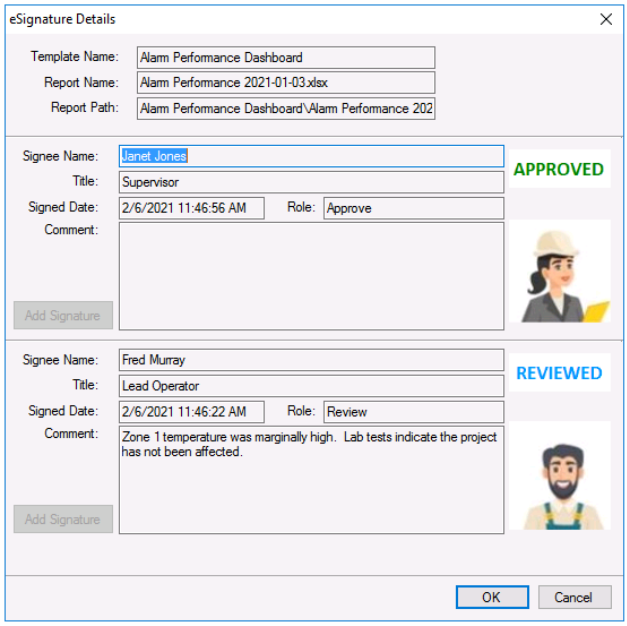


The dialog shows the signatures and any that have already been specified. In the above, the report requires signatures from two Users that have *Approve* and *Review* roles.

Click **Add Signature**.

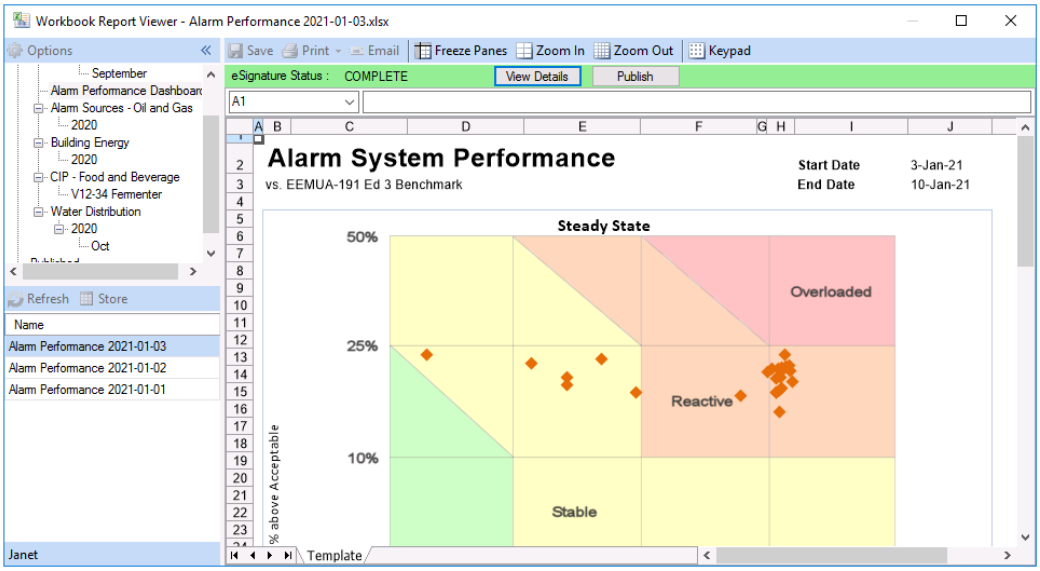


If the active user has the **Role** indicated, then the **Login Name** and **Password** is pre-filled and only the **Pin Code** will be needed. If the active user does not have the **Role** indicated then all the fields are required.



Publish Report with Signatures

At any time, the report can be published with a signature certificate to a PDF file.



Click **Publish Report**. This action will save the workbook and signature certificate to PDF in the directory configured in the project on the server machine when selected from the Workbook Report Viewer on either the server or the **Windows Team Client.**

Customizing the Signature Certificate

The signature certificate can be edited to suit. The template for the certificate is called *certificate.xlsx* as in located in the **_library** folder of the installation.

Note that the template contains a named cell called *certificate_data* which, by default, is location B39. The certificate data is written to the named cell as a single row.