Operations Control Configurator

2023 R2

Contents

Welcome to Operations Control Configurator

Welcome to the Operations Control Configurator Documentation!

This comprehensive guide will walk you through the essential steps and functionalities of the Configurator tool. With Configurator, you can deploy and configure various components of AVEVA System Platform seamlessly.

Important Notes: Components available in the Configurator depend upon the products installed on your system and available for configuration. Interdependencies among product pages and individual plugins will also affect the state of components in the Configurator.

The Configurator composition is dynamic whereas this Configurator help is meant to be comprehensive. Configurator product pages and individual plugins documented in this help might not match the Configurator as it appears for your specific product installation.

Legal Information

Publication date: Friday, November 8, 2024

Publication ID: 1283886

Contact information

AVEVA Group Limited
High Cross
Madingley Road
Cambridge
CB3 0HB. UK

https://sw.aveva.com/

For information on how to contact sales and customer training, see https://sw.aveva.com/contact.

For information on how to contact technical support, see https://sw.aveva.com/support.

To access the AVEVA Knowledge and Support center, visit https://softwaresupport.aveva.com.

What's new in Configurator?

This initial release of the Operations Control Configurator help describes Configurator features and behaviors. Following are descriptions of changes to this help and to the Configurator itself.

2023

This is the initial release of the Configurator on-line help. The highlights of this document are as follows:

- Getting started with Configurator
- Common Platform services and plugins
- Advanced configuration
- Configuring System Platform components
- Identity Manager registration
- Documentation enhancements

Additional topics provide guidance specific to configuring AVEVA Operations Control connected experience.

AVEVA Operations Control connected experience - products

An initial set of AVEVA products have been enabled to use the AVEVA Operations Control connected experience, with focus on AVEVA System Platform. Operations Control connected experience has been enabled in the following products. See Getting Started with AVEVA Operations Control for more information.

Operations Control connected experience-enabled products

- AVEVA Industrial Application Server
- AVEVA Operations Management Interface (OMI)
  - OMI web client
- AVEVA InTouch HMI
  - InTouch Web Client
  - InTouch Access Anywhere
- AVEVA Historian
- AVEVA Historian Client
- AVEVA Insight
- Development Studio
- Integration Studio

For information about working with both products that have implemented Operations Control connected experience and those that have not, see Operations Control connected experience - product co-existence

Get started with Configurator

The Configurator allows you to deploy the various components of System Platform and related products and to configure the settings for each component. It is available at the end of the product installation process.

Note: You must have administrative rights to use the Configurator.

The Configurator utility includes a product tree that lists all installed product components that require post-installation configuration. It has a set of pages that can be accessed via a directory to the left of the interface.

Configurator behavior

The Configurator composition is dynamic whereas this Configurator help is meant to be comprehensive. Configurator product pages and individual plugins documented in this help might not match the Configurator as it appears for your specific product installation. You likely will see help topics about products or components you have not installed. The Configurator itself will reflect the as-installed products.

The following describes the dynamic nature of Configurator behaviors:

- Components available in the Configurator depend upon the products installed on your system and available for configuration.
- Interdependencies among product pages and individual plugins will also affect the state of components in the Configurator.
- Configuring an interdependent plug-in might not automatically change the dependent plug ins. This means that the status indicators - green (valid configuration), blue or yellow (invalid or re-configuration needed) - might not automatically update.
- In some cases, dependent components might automatically update but could still require user interaction with the tree item of the component or plug-in to update the status indicator.

The following System Platform components and products that can be installed with System Platform may require configuration after installation:

System Platform Components:

- Common Platform
  - License Mode
  - System Management Server
  - Federated Identity Provider
- Industrial Graphic Server
- AVEVA Historian
- AVEVA Enterprise Licensing
- AVEVA System Monitor
- AVEVA InTouch HMI
- AVEVA System Platform

Other Products:

- Manufacturing Execution System
- Work Tasks
- BI Gateway

Access Configurator

After the System Platform installation process finishes running, Configurator starts automatically when you select the **Configure** button. However, installation is not complete until configuration is complete.

You may need to run the Configurator after installation if you add, change or upgrade System Platform components, your licensing model changes, or you switch to a different authentication/security method.

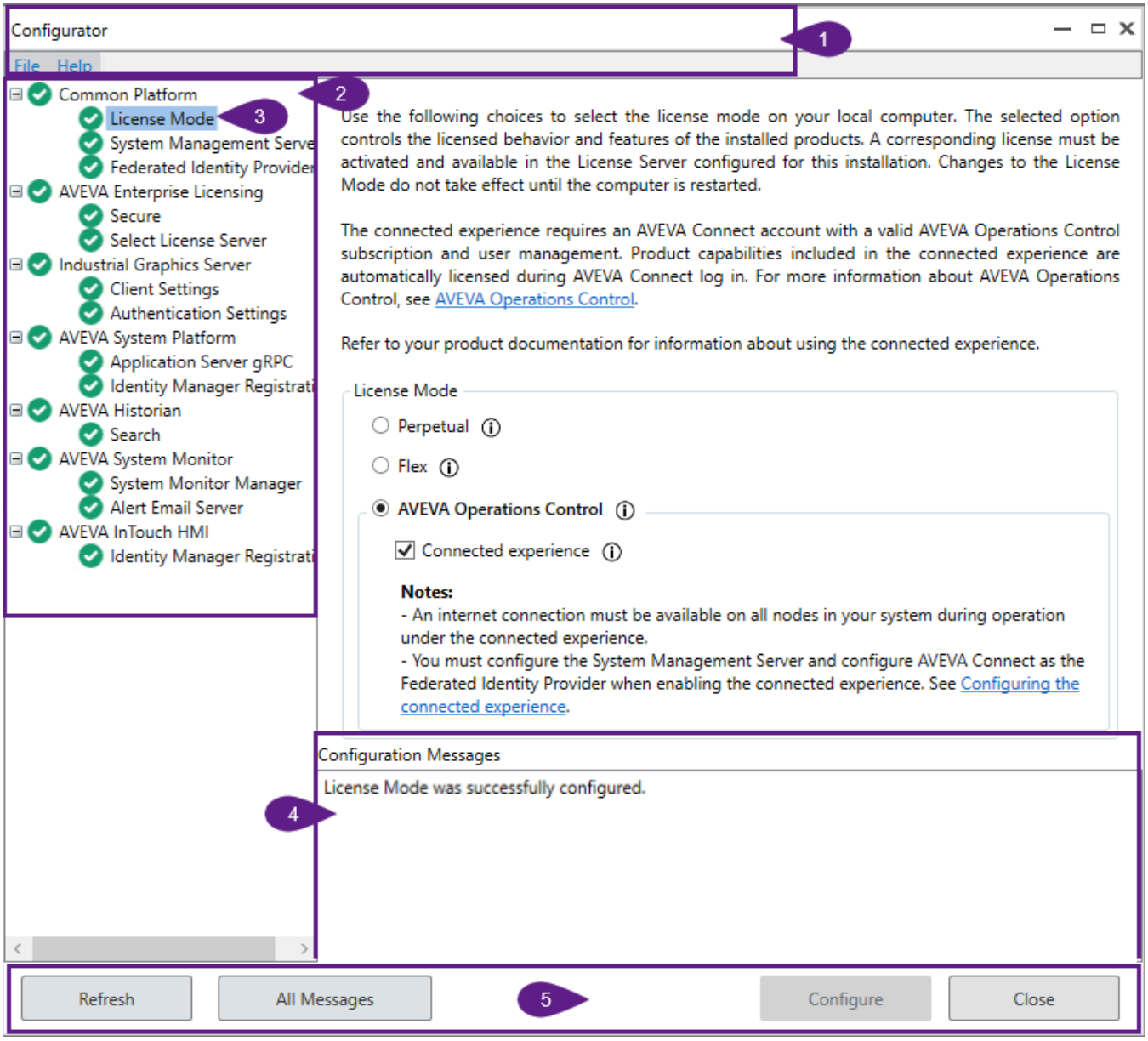
You can start the Configurator at any time by doing any of the following:

- From the Windows **Start** Menu, select **AVEVA** > **Configurator.**
- Launch the **Configurator** application file from Windows Explorer. The default path is:

  C:\Program Files (x86)\Common Files\ArchestrA\Configurator.exe

Navigate the Configurator Interface

The following image depicts the user interface of the **Configurator**.



Refer to the table below descriptions of the Configurator UI elements.

Identification Number	Element	Description
1	Header	Displays the following: Name of the application. **File** menu: There are two options available under the **File** menu: **Remove Trace Logs**: Removes local trace logs. **Exit**: Exits the program. Note that this does not stop any running

Identification Number	Element	Description
		services. **Help** menu: Opens the **About Configurator** window. The **About Configurator** window provides information on version numbers, build date, and legal information.
2	Product Tree	Lists the components for each of the products that require post-installation configuration.
3	License Mode	Displays license mode options that enable or disable features in your licensed products. This page does not acquire or purchase or activate licenses.
4	Configuration Messages	As you perform configuration tasks, messages appear in the **Configuration Messages** box. For more information, see Understand configuration message and status.
5	Command Panel	Displays the following: **Refresh**: Obtains the latest configuration statuses. **All Messages**: Opens the **Configurator Message Lists** window. From the **Configurator Message Lists** window, you can Select **Export to file** to export messages to a txt file, or **Close** to close the window. **Configure**: Executes the configure function. **Close**: Closes the application.

Understand configuration message and status

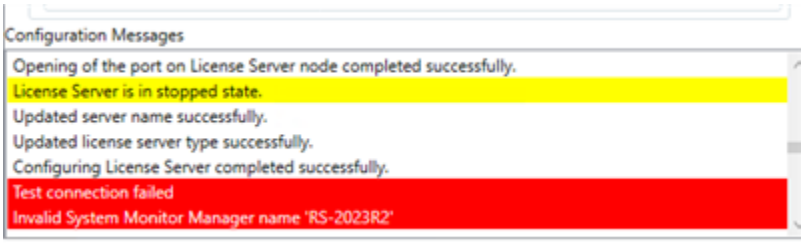
Configuration messages

Each page includes the **Configuration Messages** panel. As you perform configuration tasks, messages appear in the **Configuration Messages** box.

Messages indicating errors are highlighted in red.

Messages indicating warnings are highlighted in yellow.

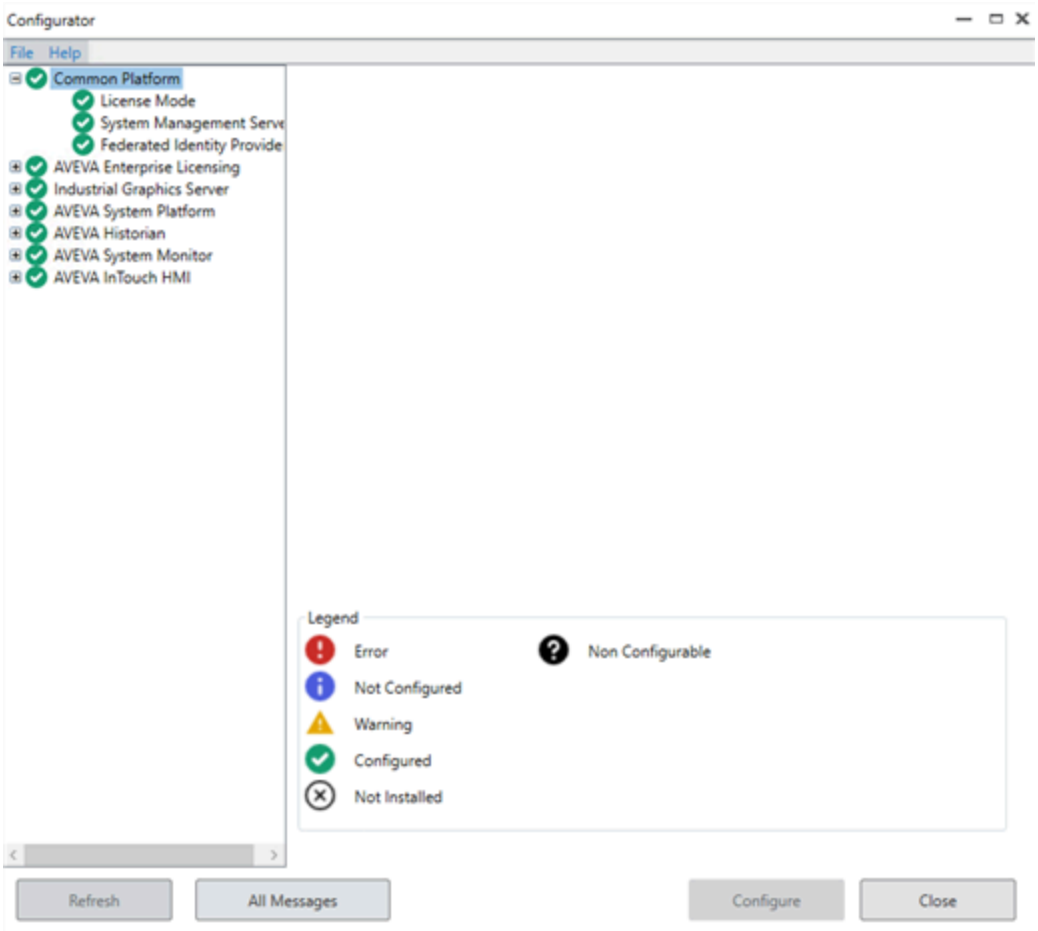
To view additional information about a message, double-click the message. A dialog box appears with the additional information.



Configuration status

The status of each item in the **Configurator** is displayed as items are configured.

The **Legend** is available when a top-level node is selected. It displays descriptions for the available statuses which appear with the configuration entries.



The status indicators are:

- Error - Indicates that an error occurred during configuration.
- Not Configured - Indicates that the feature is installed, but not configured.
- Warning - Indicates that configuration is complete, but with warnings.
- Configured - Indicates that configuration completed successfully.
- Not Installed - Indicates that the feature is not installed.
- Non Configurable - Indicates there is nothing to be configured.

Note: Most features will show as **Not Configured** the first time you open the **Configurator**.

Configure Operations Control with connected experience

Use the Operations Control Configurator to enable connected experience.

Configuration workflow

Contact AVEVA to obtain the appropriate subscriptions, set up an AVEVA Connect account, then open the Configurator, available during product installation or from the Windows **Start** menu. See the linked topics for detailed information about each configuration step in the sequence.

Step 1: Configure license mode. Available modes are: perpetual, flex, Operations Control plus connected experience. Restart the computer.

Note: If you select Operations Control connected experience, you must do so for all nodes in your system.

Step 2: Configure System Management Server (SMS). You can connect to an existing System Management Server (SMS), make your local node the SMS, or proceed without configuring an SMS (not recommended).

Step 3: Configure federated identity provider. You should already have a valid AVEVA Connect account, and you must be an administrator on that account. In this step, you configure "federated" login with AVEVA Connect on any SMS or Redundant SSO (RSSO) machine using the email associated with your AVEVA Connect account.

Step 3a: Configure SMS Advanced, Authentication (optional). Configure authentication using either an embedded browser pop-up dialog or your computer's default browser if one is installed and configured. This step affects single sign on (SSO) behavior with variations between desktop and web-based Operations Control products.

Step 4: Register each installed and licensed product with AVEVA Identity Manager.

AVEVA product implementation

The following products have implemented the initial release of AVEVA Operations Control connected experience as of System Platform 2023 R2:

- Application Server
- AVEVA Operations Management Interface (OMI)
  - OMI web client
- InTouch HMI
  - InTouch Web Client
  - InTouch Access Anywhere
- AVEVA Historian
- AVEVA Historian Client
- AVEVA Insight
- Development Studio

- Integration Studio

For information about working with AVEVA products that have not yet implemented AVEVA Operations Control connected experience, see Operations Control connected experience - product co-existence.

Any product available through AVEVA Connect will participate in the single sign-on functionality as part of AVEVA Operations Control connected experience.

Step 1: Configure license mode

To configure the license mode on your computer:

1. Open the Configurator and select **License Mode** in the left pane.

   For more information see License Mode.
2. Select the **AVEVA Operations Control radio button** and the **connected experience checkbox** to configure Operations Control connected experience on your local computer. The option you select controls the licensed behavior and features of the installed products.

   A corresponding license must be activated and available in the License Server configured for this installation.

   Connected experience requires an CONNECT account with a valid Operations Control subscription and user management.

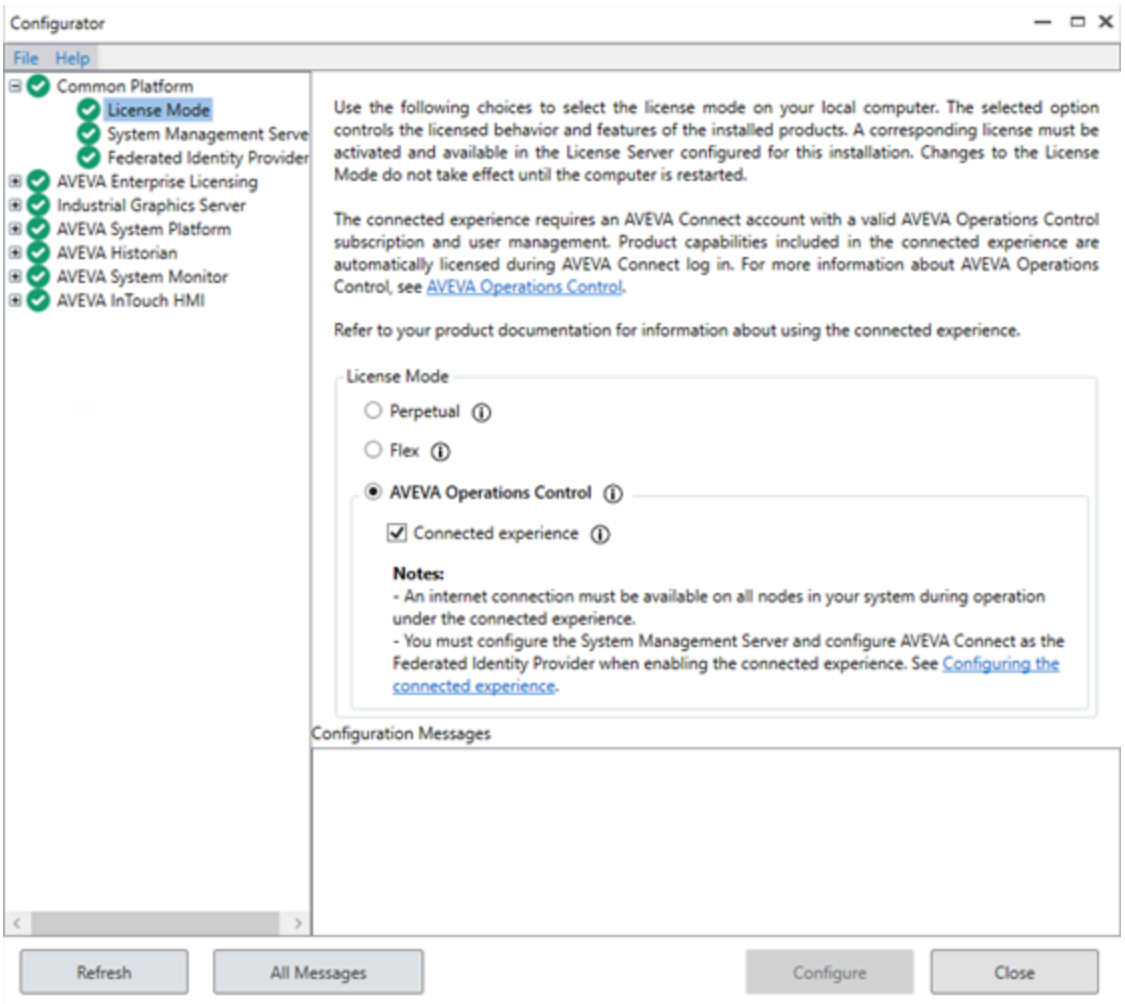
   Product capabilities included in connected experience are automatically licensed during CONNECT log in.

   Your product documentation provides product-specific information about using connected experience.
3. Click the **Configure** button.
4. Restart your computer. Changes to the License Mode do not take effect until the computer is restarted.

Notes:

An internet connection must be available on all nodes in your system during operation under the connected experience.

You must configure the System Management Server and configure AVEVA Connect as the Federated Identity Provider when enabling connected experience - steps 2 and 3 in this workflow.



License mode definitions:

Perpetual: A specific AVEVA product license purchased for use in perpetuity. These licenses typically are managed with the AVEVA Enterprise License Manager.

Flex: An "a la carte" subscription license for a range of AVEVA products. Purchase Flex credits to license use of any AVEVA cloud, hybrid or on-premises products for a recurring period.

AVEVA Operations Control: A subscription license for at least one of two AVEVA Operations Control packages (Edge, Supervisory); includes unlimited use of all products in the product package for your defined set of users.

Connected experience: Select to enable a Single Sign-on (SSO) experience across all Operations Control products on this node with AVEVA Connect cloud capabilities, available in the products by default.

Configuration Notes:

Subscription: The connected experience requires an AVEVA Connect account with a valid Operations Control subscription and user management.

Unified User Management: Selecting connected experience option enables the behavior of all Operations Control products on this node to require sign in authentication with AVEVA Connect when starting the first product on the node. Products on the node subsequently started will authenticate using SSO. AVEVA Connect-based authorization is the only security mode available under connected experience.

Compatibility across nodes: The connected experience must be enabled on all nodes in your system. Applications previously built on nodes not enabled for the Connected Experience must be reconfigured to

function in the Connected Experience environment.

You can deselect the connected experience at any time, but the connected experience must be disabled on all nodes in your system. Applications built under the connected experience must be reconfigured to function under a non-connected experience environment including both authentication methods and product licensing.

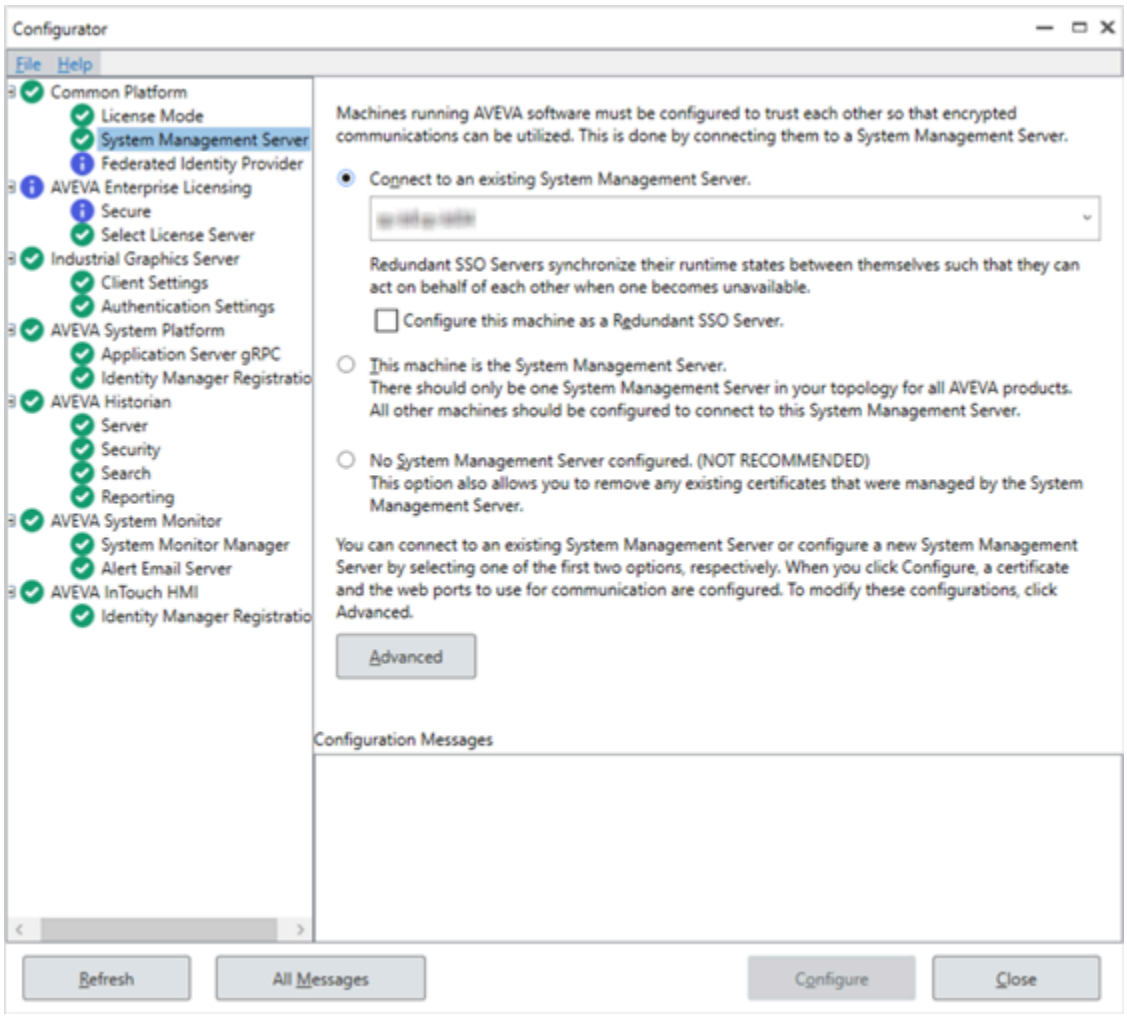
Step 2: Configure System Management Server (SMS)

The System Management Server must be configured to use AVEVA Operations Control connected experience. The "No System Management Server configured" is documented here as a valid option - not recommended - it does not support connected experience.

To configure the System Management Server:

1. In the Configurator, select **System Management Server** under **Common Platform** in the left pane.

   Note: If you are prompted for user credentials for the System Management Server, use the following format to enter the user name: **DomainName\UserName**. The prompt for user credentials may be displayed if you have domain admin privileges but are not an admin on the local machine. You must be a member of the **Administrators** or **aaAdministrators** OS group to configure the System Management Server.



You can connect to an existing System Management Server (SMS), make this node the SMS, or proceed

without configuring an SMS (not recommended). Any time you change the SMS configuration, you must also reconfigure Identity Manager registration and the Application Server gRPC setting must also be reconfigured anytime you change the SMS configuration.

- **Connect to an existing System Management Server** (default)**:** The Configurator looks for an existing System Management Server (SMS) on the network. If any are found, they are displayed in a drop down list. Select the server you want to use or enter the machine name of the server. All computers in your System Platform topology should connect to the same server.

  The machine name must comply with Active Directory naming conventions. Windows does not permit computer names that exceed 15 characters, and you cannot specify a DNS host name that differs from the NETBIOS host name. The maximum length of the host name and of the fully qualified domain name (FQDN) is 63 bytes per label and 255 bytes per FQDN. For more information, refer to the following Microsoft information page that provides Active Directory naming conventions and name/character limitations:

  https://docs.microsoft.com/en-us/troubleshoot/windows-server/identity/naming-conventions-for-computer-domain-site-ou

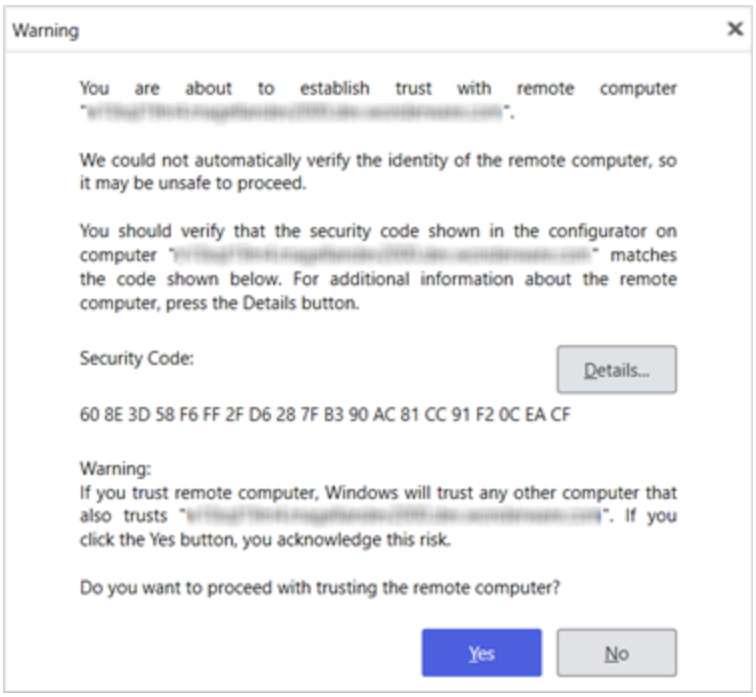
  - **Configure this machine as a redundant SSO Server.** If you configure the node to connect to an existing SMS, you can configure the node as a redundant SSO (single sign-on) Server. See Redundant SSO Configuration for additional information.
- **This machine is the System Management Server:** Select this option if this computer will be the System Management Server. Make sure that you are configuring only one SMS for your entire system. All other computers in your System Platform topology should be configured to connect to this server by using the **Connect to an existing System Management Server** option. A security code is shown when you configure this option. When you configure other nodes using the "Connect to an existing System Management Server" option, verify that the codes match. You can view the certificate by clicking the **Details...** button.
- **No System Management Server configured. (NOT RECOMMENDED):** Select this option to set up your computer without encryption and secure communications. If the System Management Server is not configured, an option that allows SuiteLink connections to use unencrypted communications is automatically enabled.

  Even if you do not configure an SMS for this node, you can still configure the System Management Server for other computers in the topology to use. You can also use this option to remove any previously installed certificates that were managed by the System Management Server.

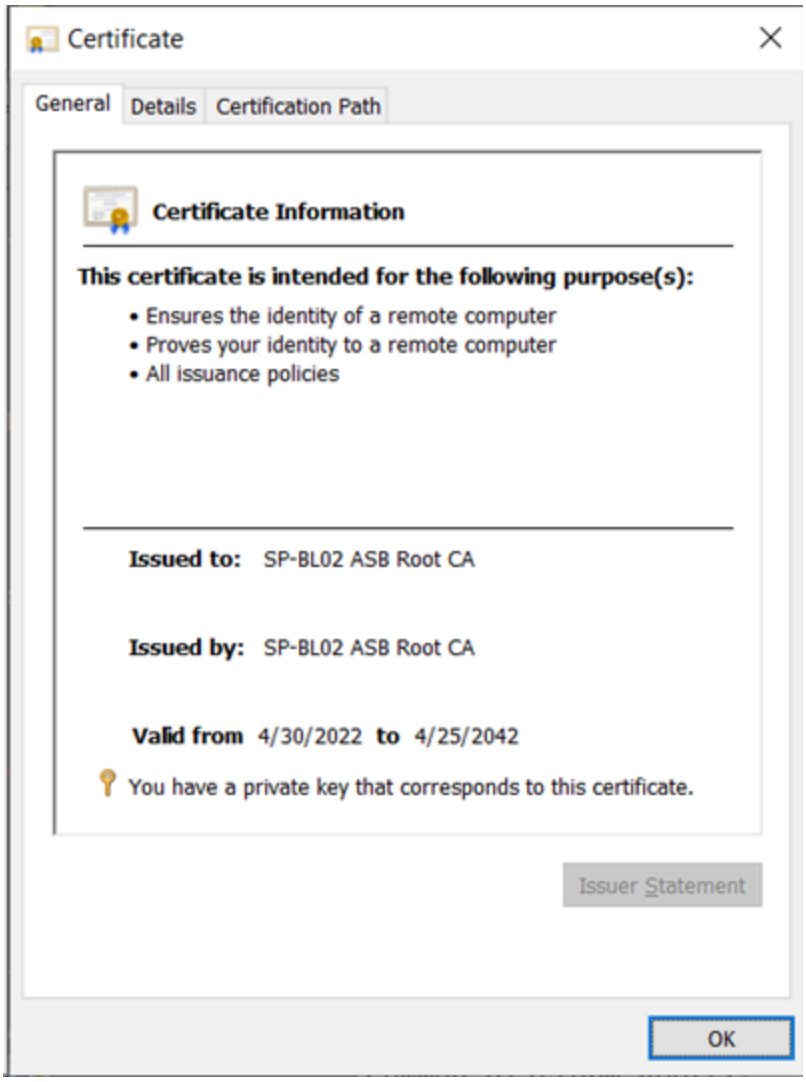
  Important! Every redundant Application Server run-time node must use the System Management Server if data is being historized. Redundant nodes have an instance of HCAP running, which is used to synchronize tags and store-and-forward data between redundant AppEngines. In System Platform 2023 R2 SP1, secure communication is required for HCAP and multi-galaxy communications (MGC), and thus, redundant nodes will not function without the SMS.

  If the SMS is not configured, there will be data loss, as well as warnings and error messages. SMS configuration is required for connected experience to work.

2. Select the **Advanced** button for additional configuration options. These include setting port numbers, adding a security certificate, and setting the SuiteLink communication mode. See Advanced Configuration for details.
3. Press the **Configure** button.
   - If you are connecting to an existing System Management Server, the Security Warning window is displayed:



By establishing trust between machines, communications can pass freely. This will be a security concern if you are not sure of the identity of the remote computer. If you have any doubt about the computer you are connecting to, verify the security code and certificate details by selecting the **Details...** button in the **Advanced Configuration** dialog to open the certificate.



4. Select the next item in the left pane that requires configuration. When all required items have been configured, press the **Close** button to complete installation.

Step 3: Configure federated identity provider

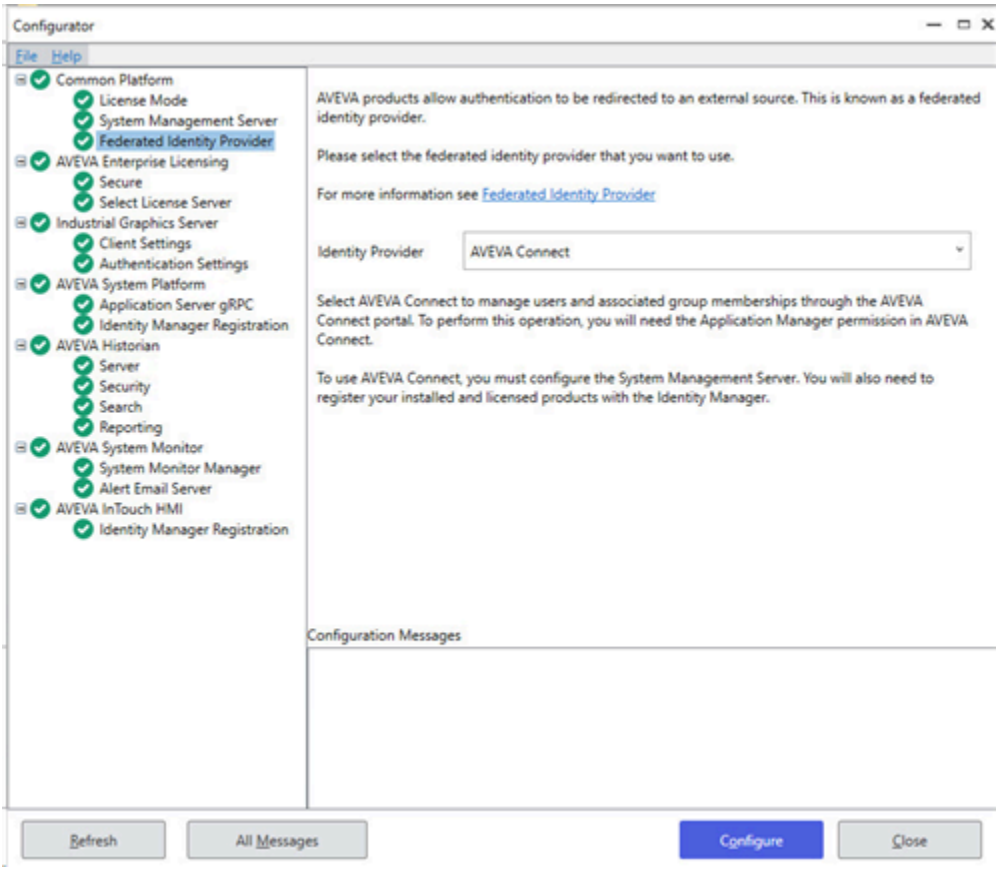
To configure the Federated Identity Provider

1. Prepare the Federated Identity Provider prerequisites.
   a. For a federated identity connection, you need a valid AVEVA Connect account, and you must be an administrator on that account.
   b. This step only applies to the node where this machine is the configured System Management Server or Redundant SSO. If a node is connecting to an existing System Management Server and is not a Redundant SSO, configuring the Federated Identity Provider is not required.
2. Select **Federated Identity Provider** in the left pane, under **Common Platform.**

   The Identity Manager component in the Platform Common Services (PCS) Framework available on the System Management Server (SMS) and Redundant SSO (RSSO) machines can be configured for "federated"

login with AVEVA Connect. This means that a user can enter their email address as registered with an AVEVA Connect account into the Identity Manager login form, at which point they are redirected to AVEVA Connect so they can log in. At present, for Operations Control connected experience, only federation to AVEVA Connect is supported and Azure AD is not supported.

If you set the Federated Identity Provider to "None" you can use AVEVA Identity Manager or local identity providers such as Windows authentication, but you will no longer have a connected experience configuration.



3. Select the appropriate AVEVA Connect account.

   If you have multiple AVEVA Connect accounts, then after the authentication, an account selection dialog listing multiple AVEVA Connect accounts will be displayed. Select the account with which you want to be federated.

   If you are part of only one AVEVA Connect account, then the account selection dialog will not be displayed.

4. Provide your AVEVA Connect credentials when requested.

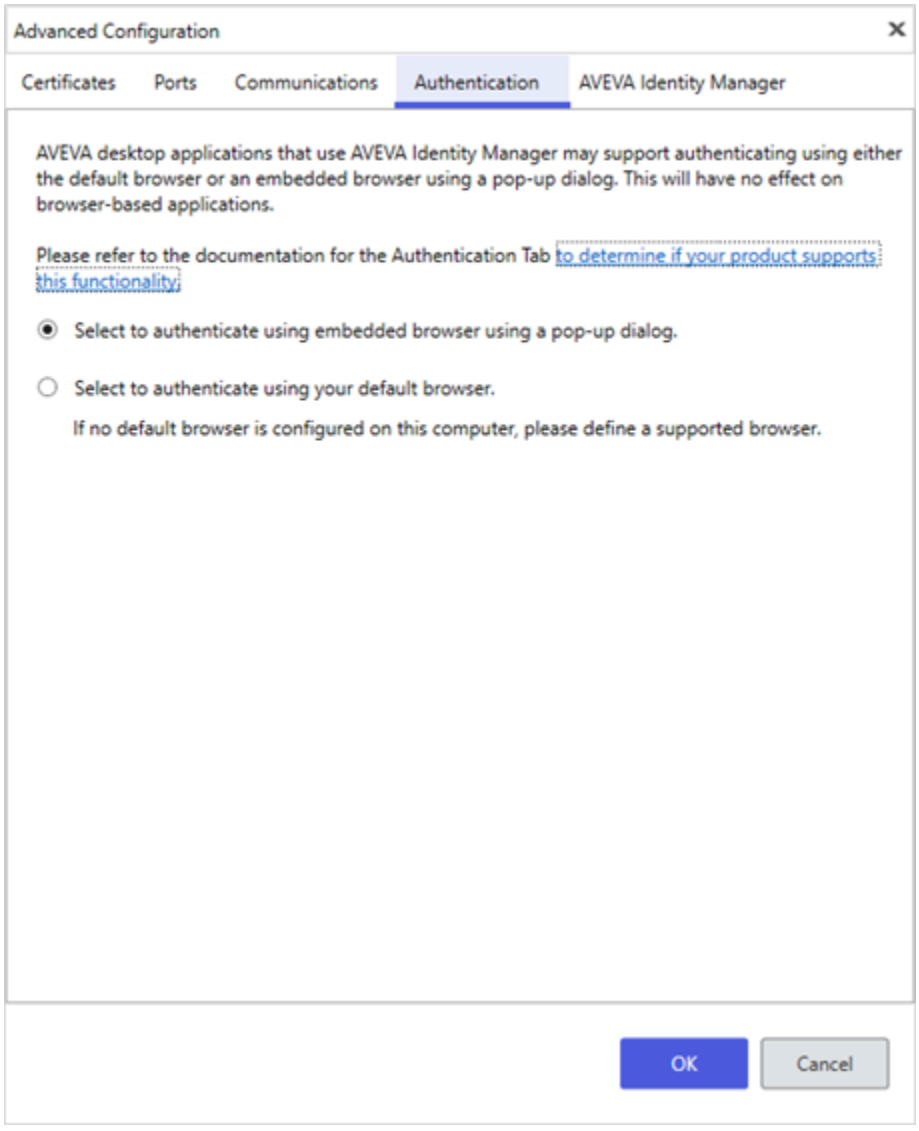
Note: If you are configuring a Redundant SSO Server, it is important to select the same AVEVA Connect account that was configured on the System Management Server.

Step 3a: Configure SMS Advanced, Authentication (optional)

To configure the authentication dialog

1. Select **System Management Server** then click the **Advanced** button and select the **Authentication** tab.

2. Select the authentication option. Each option will exhibit different single sign on (SSO) behaviors across desktop and web based Ops control products.
   - Select to authenticate using an embedded pop-up browser: This option displays the AVEVA Identity Manager login page in an embedded browser using a pop-up window when you are prompted to authenticate.
   - Select to authenticate using your default browser: This option displays the AVEVA Identity Manager login page in your default browser when you are prompted to authenticate.



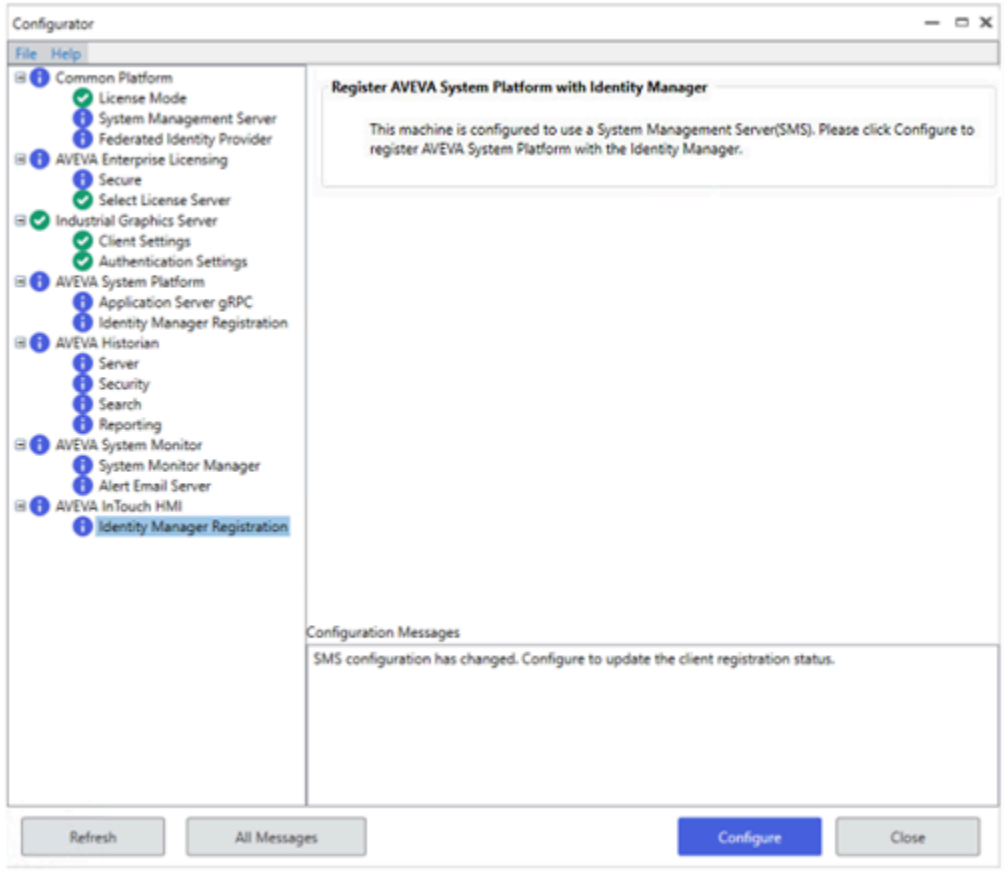
Note: The default behavior - an embedded pop-up dialog - is best for a machine that does not have a default browser configured, or in a restricted environment, or where no browser is installed. Selecting to use your computer's default browser will support all other uses. For more information, see Embedded browser pop-up versus default browser.

Step 4: Register each installed and licensed product with AVEVA Identity Manager

To register products with AVEVA Identity Manager

1. Complete or verify preliminary steps before registering your products.
   a. Enable AVEVA Operations Control connected experience as your license mode.
   b. Configure the System Management Server.
   c. Configure a Federated Identity Provider.
2. Navigate in the Configurator left pane to the product you want to register. Select **Identity Manager Registration** to access the registration page. This page will differ slightly from product to product.

   Example: InTouch registration page:



3. Click **Configure**.

Note: If the SMS configuration changes, you may need to update the federated identity provider configuration and you must re-register each installed product with the AVEVA Identity Manager.

Common Platform

This chapter describes the different components of **Common Platform** and its plugins**.**

Common Platform services include the following components:

- License Mode
- System Management Server
- Federated Identity Provider

License Mode

You can configure the **License Mode** in the **Configurator** under the **Common Platform** tab.

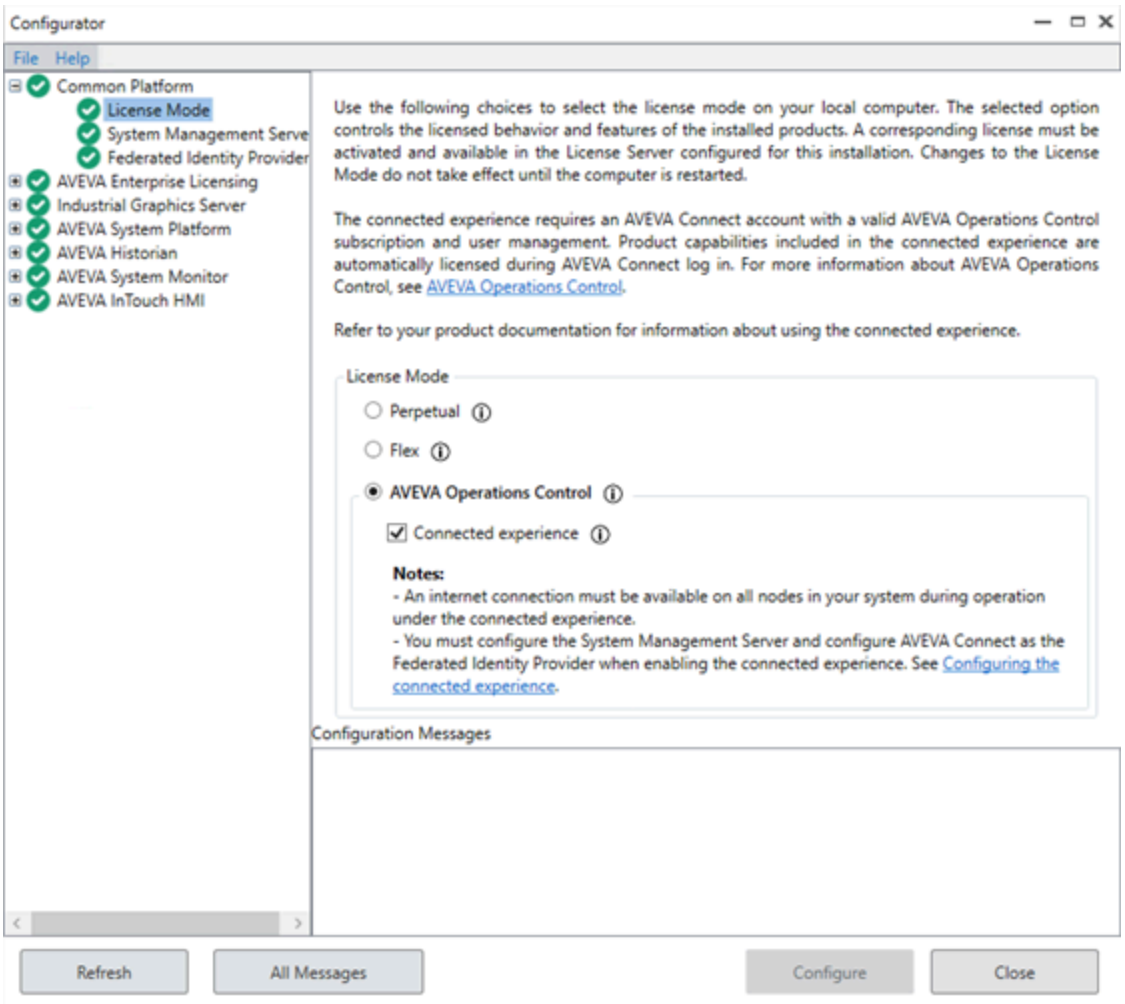
Note: License mode changes do not take effect until the computer is restarted.

Important information about configuring a license mode

Product capabilities and behaviors: Selecting a license mode enables product capabilities and directs the behavior of specific products, but does not select or activate a specific license. Installing and setting up licenses are separate from the license mode. Refer to individual product documentation for information about installing and setting up licenses for that product.

Products affected by license mode configuration: Product behaviors directed by the selection of a license mode may not be applicable to all installed products. The Configurator is a common framework and license mode selection might not apply to a product you have installed and want to configure.

For information on Operations Control connected experience implementation, see Operations Control connected experience - product co-existence.



License mode options

The following **License Mode** options are available:

- **Perpetual:** A specific AVEVA product license purchased for use in perpetuity.
- **Flex:** Choose subscription license separately for a range of AVEVA products. Purchase Flex credits to license use of any AVEVA cloud, hybrid or on-premises products for a recurring period.
- **AVEVA Operations Control:** A subscription license for at least one of two AVEVA Operations Control packages (Edge, Supervisory); includes unlimited use of all products in the product package for your defined set of users.
  - **Connected experience**: Enables Single Sign-on (SSO) experience across all Operations Control products for that node with AVEVA Connect cloud capabilities.

System Management Server

AVEVA software products require post-installation configuration in order to identify servers, use encrypted communications, and enable other product functionality. Configure your products using the Configurator after you have installed them. The Configurator lists all product components that require post-installation

configuration.

Note: Configuring a System Management Server (SMS) is highly recommended to ensure the security of your System Platform. It is required for Application Server nodes 1) when redundancy is enabled, or 2) when implementing Multi-Galaxy Communications. All nodes should be configured to point to a single SMS node or communication between nodes may not succeed.

System Management Server overview

The System Management Server (SMS) allows encrypted communication between machines. Encrypted communications can be used when a trust relationship between one or more machines running AVEVA products is established. This is achieved through the System Management Server by utilizing certificates.

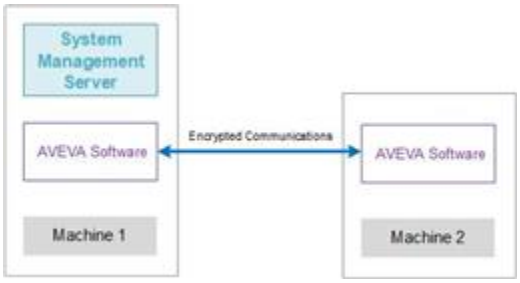
Only one of the machines in the network is identified and configured as a System Management Server. Machines running AVEVA products can then connect to that single System Management Server to establish trust and configure encrypted communications.

Note: To connect to the System Management Server, you need to be a member of either the "aaAdministrators" or the "Administrators" group on the machine where the System Management Server is installed.

Install System Management Server

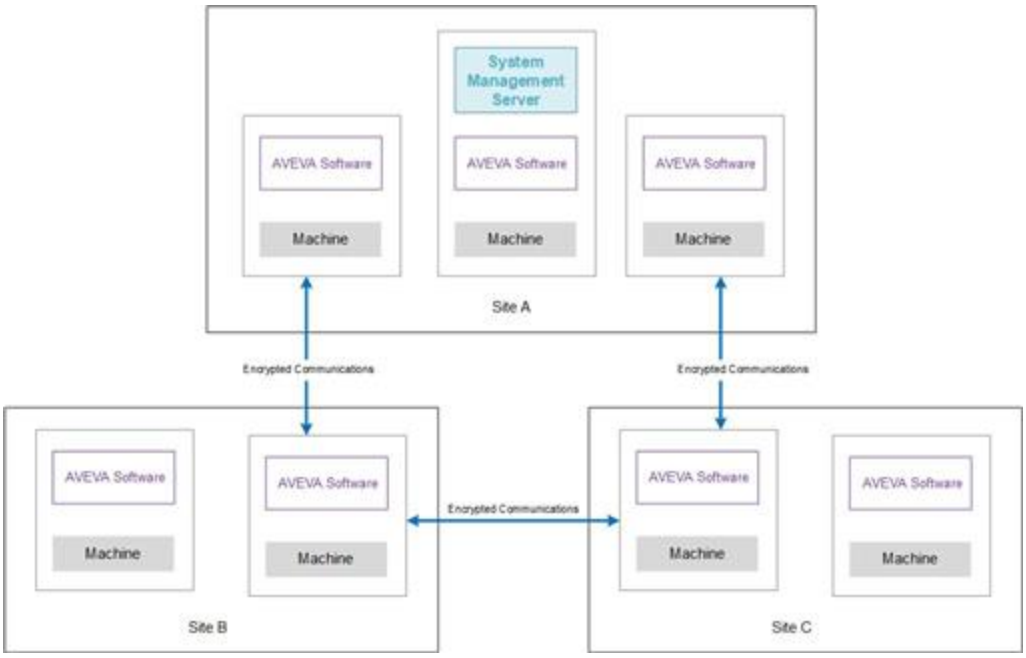
Regardless of the size of your system setup, only one System Management Server is required for encrypted communication. System Management Server can be installed on one of the machines running an AVEVA application or on a separate machine on the network.

Note: You need to include only one System Management Server in your entire system. If other AVEVA products are installed, confirm that System Management Server has not been configured elsewhere before proceeding, as communication disruptions may occur.



System Management Server can also be installed in a large, multi-site environment running multiple AVEVA products. In such systems, the location of the System Management Server may be governed by one or more products. However, all AVEVA products should be able to connect to the System Management Server so that certificates can be renewed when required.

An example configuration of a multi-site system is shown below:



Redundant SSO server

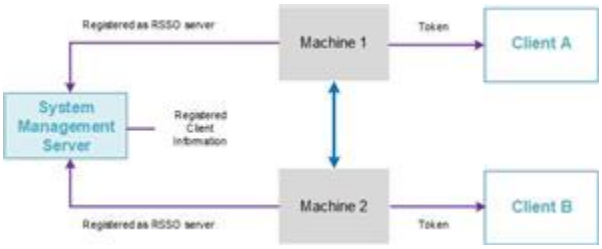
You can configure a machine that connects to an existing System Management Server as a Redundant Single Sign-On (RSSO) server. When you select the System Management Server and configure the current machine, the SSO capability from the System Management Server is shared with the RSSO server.

The purpose of setting up RSSO servers is to:

- distribute the workload between RSSO servers
- eliminate single point of failure

Note: Not all AVEVA products make use of the Redundant SSO Server functionality. Refer to your product documentation to see if this feature is supported.

The following diagram illustrates the working of RSSO servers:



A brief description of the steps in the above workflow is given below:

1. Machine 1 and Machine 2 connect to an existing System Management Server and are configured as RSSO servers using the Configurator.
2. Client A and Client B are registered with the System Management Server.
3. When a workflow is initiated on Client A, it requests a token from Machine 1.
4. Machine 1 sends a token to Client A as if it were sent from the System Management Server.

5. When a workflow is initiated on Client B, it requests a token from Machine 2.
6. Machine 2 sends a token to Client B as if it were sent from the System Management Server.

Note: The client needs to be configured manually to select the RSSO server with which it will communicate for obtaining a token.

The main difference between the System Management Server and the Redundant Single Sign-On (RSSO) server is that a client can register only with the System Management Server, not with the RSSO server. If you configure RSSO servers, it is recommended that the clients communicate with an RSSO server to obtain a token.

A workflow is initiated and completed on a single RSSO server; it cannot be split between RSSO servers. Subsequent client requests for a token should be made to the RSSO server that issued the original token. In addition, token renewal is also possible only with the same RSSO server.

If the original RSSO becomes unavailable, a new token needs to be requested from another, available RSSO server.

An RSSO server can run independently without the System Management Server, provided that the latest client / resource configurations have already been synchronized.

Note: Configuration such as client registration can only be made with the SMS. RSSO does not accept configuration requests.

Configure a System Management Server

You can complete the following tasks in the Configurator:

- Configure the System Management Server
- Connect to a System Management Server

In addition to the above tasks, you can configure **Advanced** settings.

If the System Management Server configuration is changed, you must re-register the Identity Manager for Application Server and InTouch, and reconfigure Application Server gRPC.

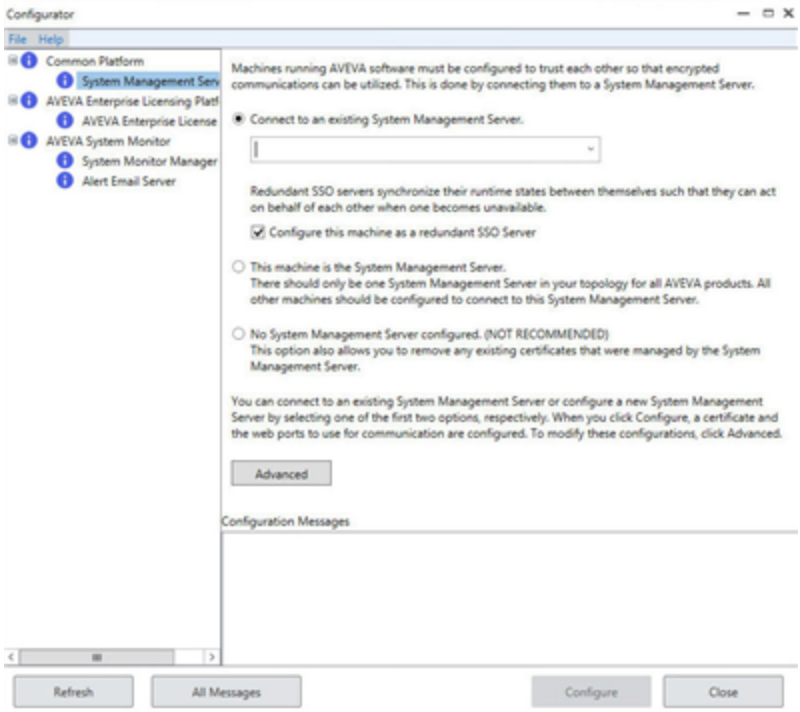
Note: If the System Management Server is not configured, capabilities such as connected experience, Web OMI, Azure AD/ CONNECT federation, Application Server redundancy, and Multi-Galaxy Communications will not be available.

Connect a machine to a System Management Server

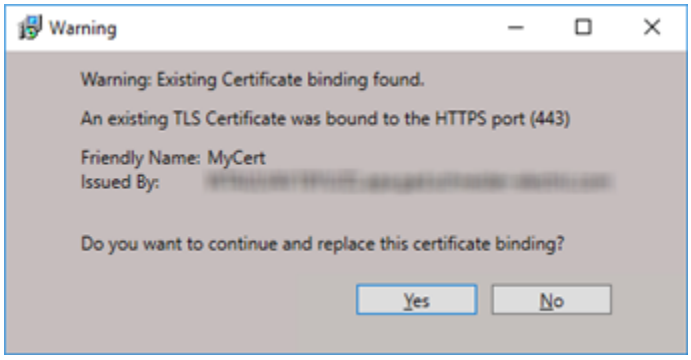
Machines running AVEVA products need to connect to a System Management Server via a configured certificate in order to use encrypted communication.

To connect a machine to a System Management Server

1. Start the Configurator on the machine you wish to connect. The Configurator screen is displayed.

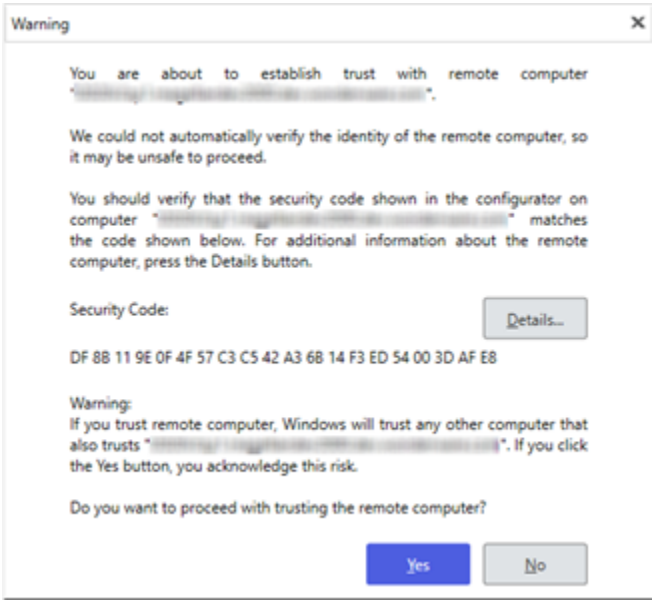


2. In the left pane, select **Common Platform > System Management Server**.
3. If you wish to connect to an already existing System Management Server, select the **Connect to an existing System Management Server**.
4. From the list of System Management Servers available, select the required System Management Server. Note that the list displays all machines on the network that have been configured to function as System Management Server. In most cases, there is only one System Management Server.
5. If you wish to configure a machine as a Redundant SSO (RSSO) server, under **Connect to an existing System Management Server,** select **Configure this machine as a Redundant SSO Server.**
6. Select **Configure**. The System Management Server configurator verifies the configuration, and if any conflicting certificate configuration or communications port binding is detected, the following **Warning** message is displayed.



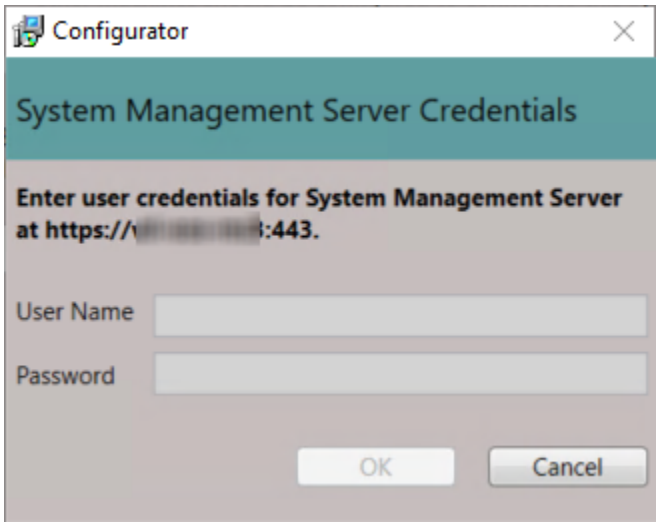
7. Selecting **No** results in the following message being displayed in the **Configuration Messages** area, and the machine will not be connected to the System Management Server.

8. Selecting **Yes** replaces the binding. By default, the root certificate is downloaded from the System Management Server. This is possible only when the **Automatically Generated** certificate option is selected on the **Advanced** page. The following message is displayed.



9. Review the message carefully before you select **Yes**. Selecting **No** cancels the configuration process.
10. Select **Details**, to view more information about the certificate.

    If you are not a member of the "aaAdministrators" or "Administrators" group on the System Management Server, a dialog box prompting you to log on to the System Management Server with administrative credentials is displayed. Enter the credentials of a user that is a member of the "aaAdministrators" or "Administrators" group on the System Management Server and select **OK**.



Note: If you have configured a communications proxy on the server where the System Management Server is installed, contact the AVEVA Global Customer Support team for information about installing and connecting

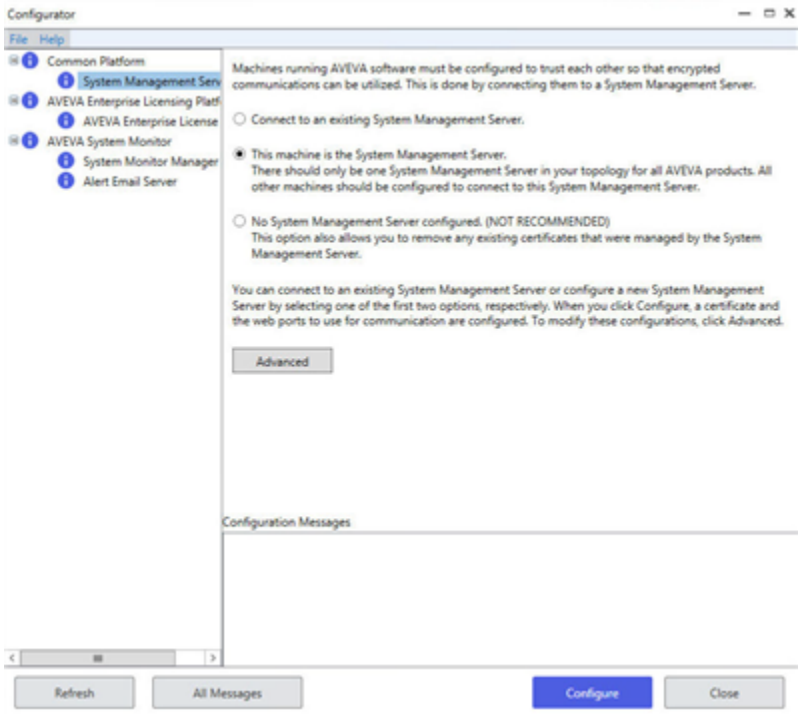
to the System Management Server.

11. The **Configuration Messages** area displays the steps in the configuration process and the progress. If the configuration is unsuccessful, you can view details of the errors in System Management Server.
12. Select **Close** to exit the Configurator.

Configure the System Management Server

To configure the System Management Server

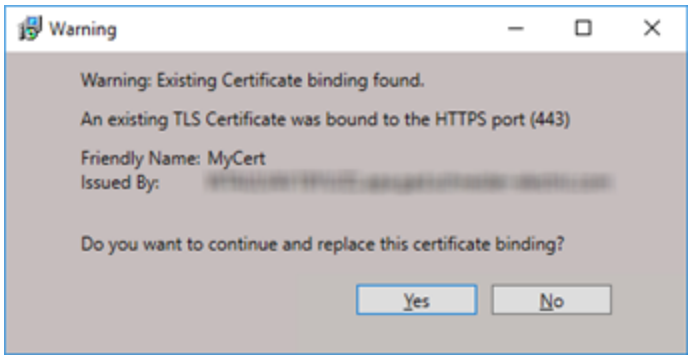
1. Start the Configurator. The Configurator screen is displayed.



2. In the left pane, select **Common Platform > System Management Server**.
3. Select **This machine is the System Management Server**. Review the notes on the screen before you start the configuration.

   Note: You should include only one System Management Server in your entire system. If other AVEVA products are installed, make sure that a System Management Server has not been configured elsewhere before proceeding as communication disruptions may occur.
4. Select **Configure**.
5. Select **Yes** for the **Warning** message after you confirm there is only one System Management Server in your entire system. If other AVEVA products are installed, make sure that a System Management Server has not been configured elsewhere before proceeding as communication disruptions may occur.

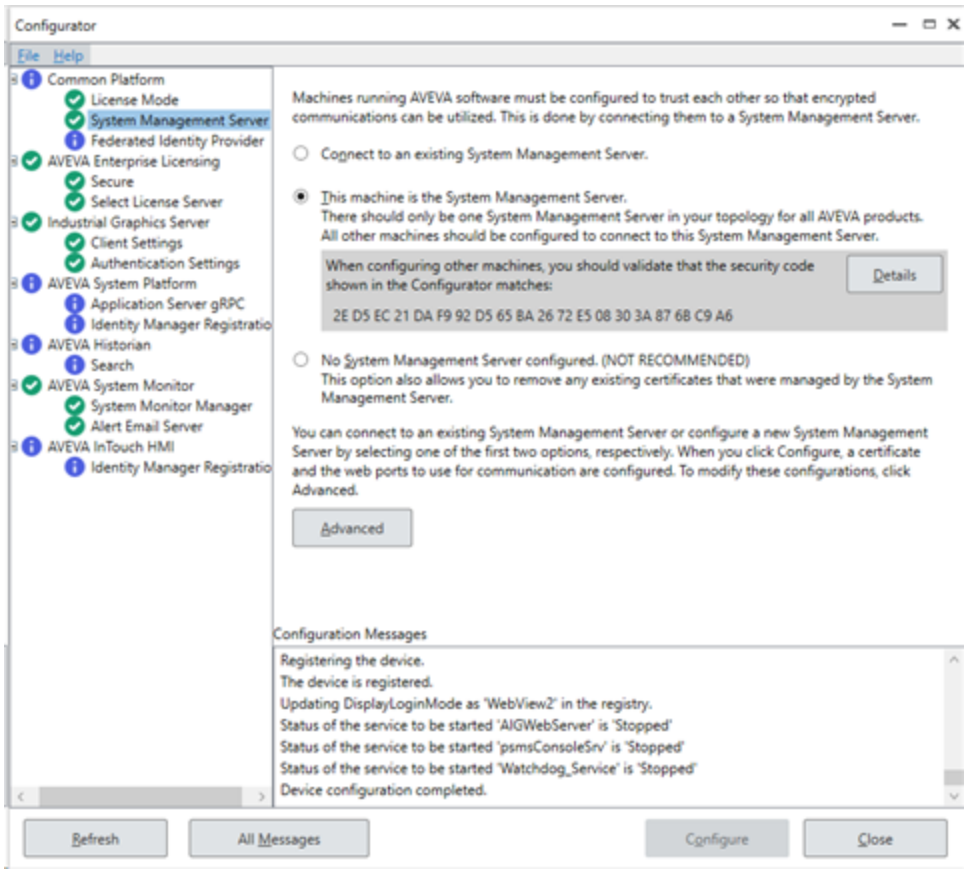
   The System Management Server configurator verifies the configuration, and if any conflicting certificate or communications port binding is detected, the following **Warning** message is displayed.



Note: If you change the System Management Server address, you must re-register all installed products.

6. Selecting **No** results in the following message being displayed in the **Configuration Messages** area, and the machine will not be connected to the System Management Server.

7. Selecting **Yes** replaces the binding. The Configurator will start configuring the System Management Server.
8. On successful configuration, the message **Device configuration completed** is displayed. The security code is displayed in the Configurator as shown below. It is recommended that you make a note of the security code because you will need to verify the security code when you add other machines to this System Management Console.
9. Select **Details,** to view more information about the certificate.



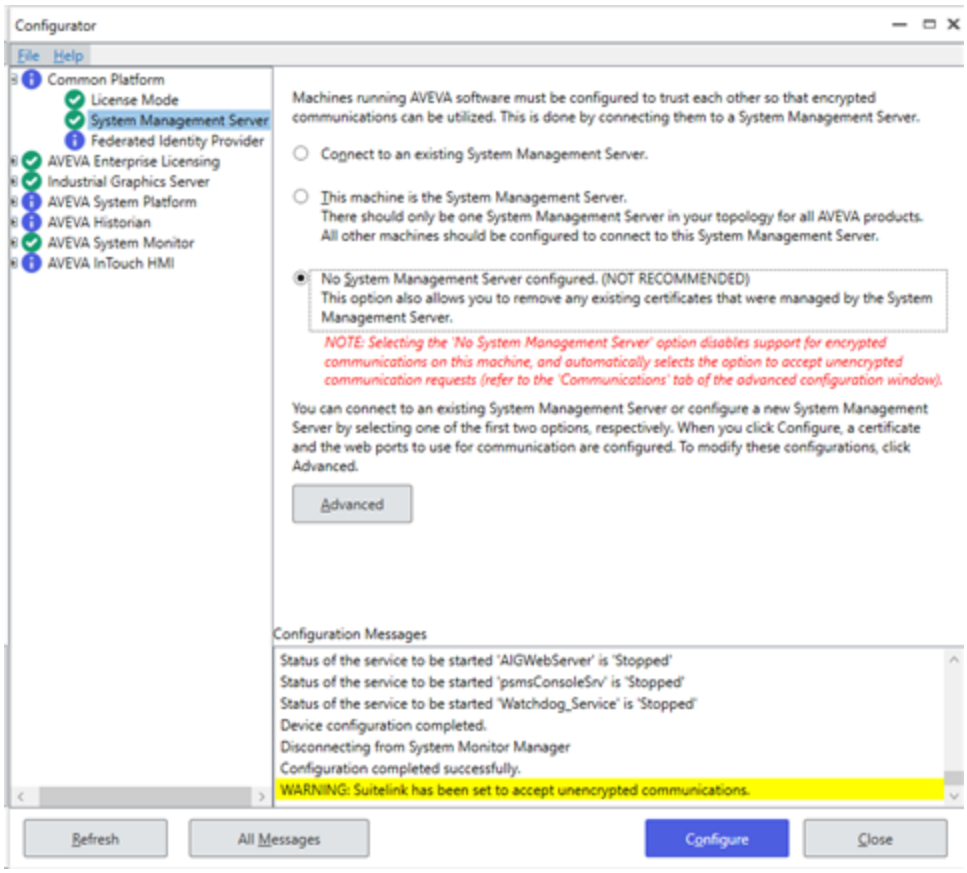
If the configuration is unsuccessful, you can view details of the errors in the System Management Server.

10. Select **Close** to exit the Configurator.

Run products without a System Management Server

To run AVEVA products without a System Management Server configured

1. Start the Configurator.
2. In the left pane, Select **Common Platform > System Management Server**.
3. Select **No System Management Server configured**. Selecting this option results in each individual AVEVA product managing their secure communications, which may or may not be available without the System Management Server.



Note: This procedure is not recommended. It is intended for temporary troubleshooting purposes.

Advanced Configuration

If you have already configured a System Management Server or have selected a System Management Server to connect to, the configuration may be modified if it is required.

To modify an existing configuration

- Select **Advanced**. The **Advanced Configuration** dialog is displayed.

The **Advanced Configuration** window consists of the following tabs:

- Certificate: To configure the certificate for secure communications.
- Ports: To configuring the http and https communication ports.
- Communications: To enable or disable the ability to use a non-encrypted channel for SuiteLink communications, and limiting which users have access to NMX communications.
- Authentication: To enable browser to authenticate user.

Certificates tab

System Management Server uses a security certificate to ensure that communication between nodes is encrypted. The **Certificates** tab includes the following configurable fields:

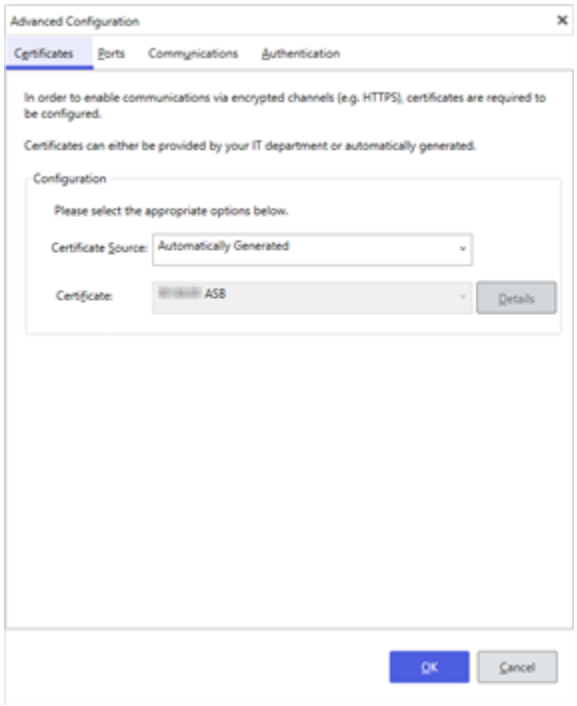
- Certificate Source: Select either **Automatically Generated** (default), or **Provided by IT**. If your IT department is providing the certificate, select **Import** and navigate to the certificate file.
- Certificate: The certificate name is displayed. If you imported a certificate, select **Details** to know more. The certificate is periodically renewed through an automatic update process, both on the server node and on remote nodes.
- System Management Server: If you are connecting to an existing System Management Server, the name and port number of the server you selected is shown.

To configure the certificate for secure communications

1. If you want the Configurator to generate a certificate, select **Automatically Generated** from the **Certificate Source** list. By default, automatically generated is selected. The **Certificate** field is disabled if the Automatically Generated option is selected, or if certificates generated earlier have been deleted. To view more information about the certificate, select **Details**.

   Note: Automatically generated certificates are renewed automatically.

2. If you want to use a certificate generated by your IT Department, select **Provided by IT (import/select)** from the **Certificate Source** list.



3. From the **Certificate** list, select the certificate you want to use.
4. Select **Import** to use a certificate not listed in the **Certificate** list. The **Import Certificate** dialog is displayed.

5. In the **Certificate file** field, browse to select a certificate.
6. From the **Certificate Store** list, select the type of certificate – **Root**, **Intermediate**, or **Personal**. The certificate is configured to be used for encrypting communication channels.

   Depending upon the type selected here, the certificate is stored in the **Certificate Store** identified by the certificate type.
7. In the **Password** field, type the password for the selected certificate Store. The Certificate Store does not have a password. This is the optional password for the certificate being imported.
8. Select **OK** to save the details and close the **Import Certificate** dialog.

   Note: The IT Department needs to renew certificates they generate as and when required.
9. Select **Details**, to view the details of the certificate.

   The **System Management Server** field is displayed only if you have selected the **Connect to an existing System Management Server** option in the previous screen. You can use this field to change to a different System Management Server. From the **System Management Server** list, select the machine on which you want the certificate to be generated.

   Note: You can only specify a computer name or a fully-qualified domain name for the System Management Server. It is recommended that you always use a fully-qualified domain name to identify the SMS. Specifying the name in a different format, for example an IP address, may result in errors.

Ports tab

The System Management Server uses HTTP and HTTPS for communications with AVEVA software. Remote nodes must be configured with the same port numbers as configured here. By default, the System Management Server uses HTTP port 80 and HTTPS port 443. Generally, you can use the default settings. Select the **Advanced** button, then select the **Ports** tab and edit the port numbers as needed.

To configure the HTTP and HTTPS communication ports

This is the port number on which the System Management Server is configured and is automatically populated. It is recommended that you also check the port number manually.

1. Select the **HTTP Port** and **HTTPS Port**. The defaults are 80 and 443, respectively.

These ports are local ports on the current machine, which are used by web services and clients connecting to this machine.

Note: If you change the default ports you need to
(i) restart the machine for the change to take effect, and
(ii) update the port number(s) on all client products that point to servers running on this machine. This excludes the System Management Server because it discovers port numbers automatically.

HTTP and HTTPS ports range from 0 to 65535. Within this range, you may choose any port that has not been blocked or is currently in use. Otherwise, you will receive "Port number conflict" error.

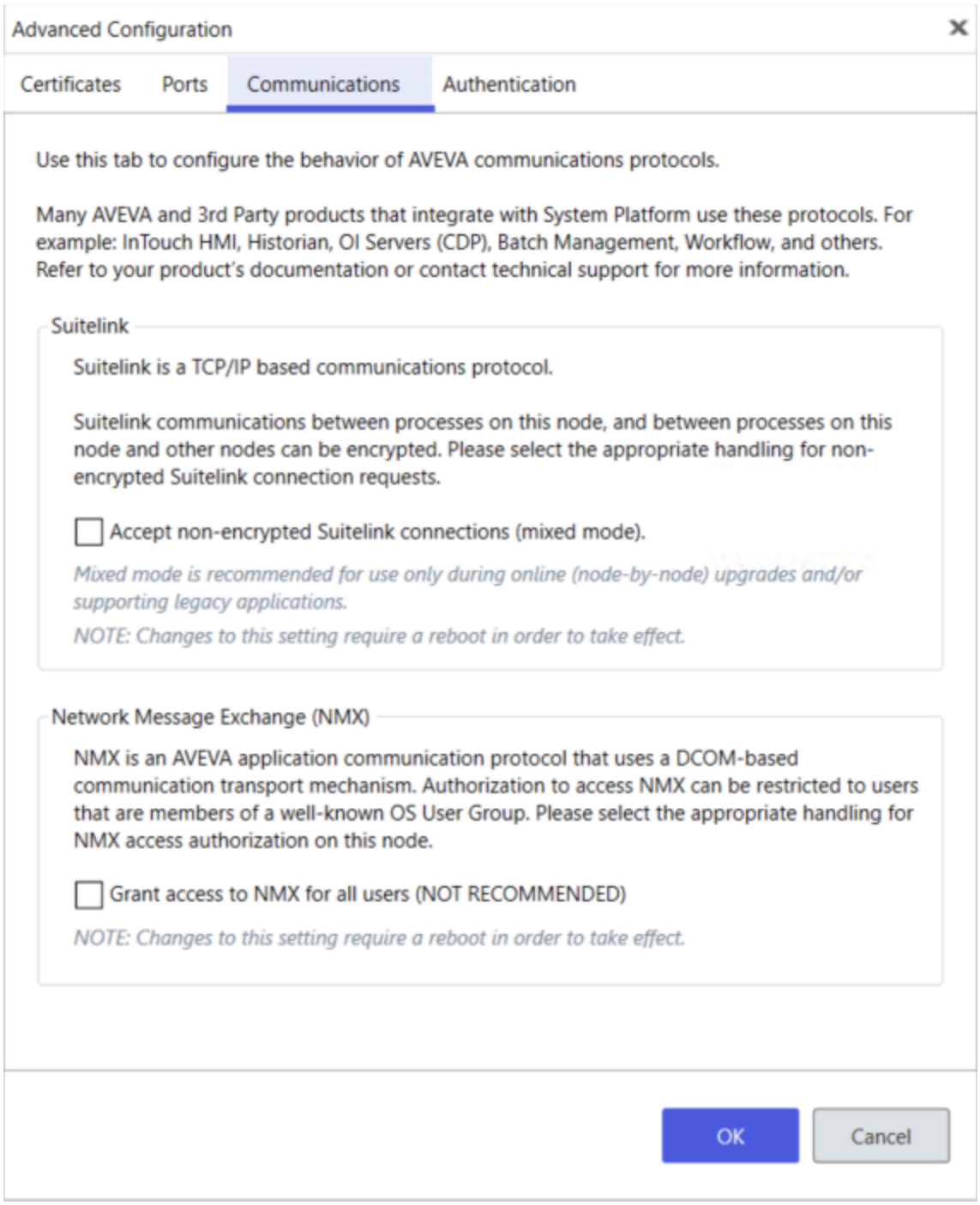
2. Select **OK** to save your settings. The Configurator's main screen is displayed.
3. Select **Configure**.

   The **Configuration Messages** area displays the steps in the configuration process and the progress. Upon successful configuration, the crtificate is generated on the local machine and signed by the selected System Management Server. The server name is displayed in the **Certificate** field of the **Advanced Configuration** dialog. If the configuration is unsuccessful, view details of the errors in the Operations Control Management Console.

Communications tab

The Communications tab allows you to configure the behavior of the AVEVA communications protocol. The **Communications** tab includes the following configurable fields:

- SuiteLink: TCP/IP based communication protocol
- Network Message Exchange (NMX): AVEVA application communication protocol



Note: The **Communications** tab will be hidden if you do not install a product that uses Suitelink or NMX communications.

SuiteLink mixed mode setting

Prior to System Platform 2023, enabling the System Management Server, either by connecting to an existing server or by setting this machine as the System Management Server resulted in the following behavior for SuiteLink connections:

- The system first attempted to make a secure connection between a SuiteLink client and the SuiteLink server.

- If a secure connection could not be established, an unsecured SuiteLink connection was made. Users were not notified if the SuiteLink connection was not secure.

As of System Platform 2023, the System Platform Configurator includes an option to force all communications to be encrypted for SuiteLink connections.

- Mixed mode enabled: This is the default setting if you are upgrading a node from a prior release. With the checkbox set to true (checked), the behavior described above is used, in which unsecured connections are allowed. This mimics legacy System Platform behavior, prior to the System Platform 2023 release. This setting is NOT RECOMMENDED except for the use cases listed below.
- Mixed mode disabled: This is the default setting for new installations. With the checkbox set to false (unchecked), client connections to the SuiteLink server are only successful if the connection is secured, that is both nodes must configured to use the System Management Server. This option ensures that the connection between the SuiteLink Server and SuiteLink clients is always secure (encrypted). If a secure connection is not available, the connection will not be allowed. A secure connection between client and server is only possible if both are configured to use the System Management Server.

Mixed mode use cases

Mixed mode is recommended for use under the following conditions:

- While upgrading an existing System Platform installation (performing a node-by-node upgrade). Reset the mode to disable mixed mode after the upgrade is complete.
- To support legacy applications that do not use encrypted SuiteLink communications.

Note: Whenever the SuiteLink communication mode is changed, a system restart is required before the new mode will take effect.

NMX user access setting

The AVEVA Network Message Exchange (NMX) is an application communication protocol that leverages a DCOM-based transport mechanism for communication between nodes. For new installations, the default setting is to disable access for all users to NMX communications. If you are upgrading an existing System Platform installation, access for all users is enabled by default. Reset the mode to restrict access after you complete the node-by-node upgrade.

- Enable access to NMX for all users: This is the default setting if you are upgrading a node from a prior release. Allowing access for all users is NOT RECOMMENDED except for the use cases listed below.
- Disable access to NMX for all users: This is the default setting for new installations. With the checkbox set to false (unchecked), NMX communication is allowed only for the users and accounts that require it. NMX access is allowed for:
  - Members of the OS User Group aaRuntimeUsers
  - Members of the OS Administrators group
  - The System Platform Network Account
  - The local system account (NT System)

Access to NMX for all users use cases

Access for all users is recommended for use under the following conditions:

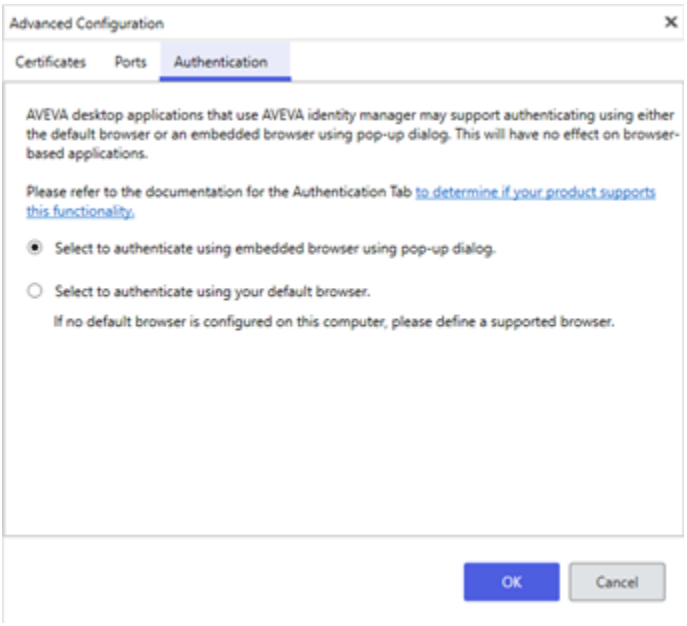
- While upgrading an existing System Platform installation (performing a node-by-node upgrade). Reset the mode to disable access for all users after the upgrade is complete.
- To support legacy applications that require access for all users.

Note: Whenever the NMX mode is changed, a system restart is required before the new mode will take effect.

Authentication tab

The Authentication tab allows you to authenticate using two options:

- Select to authenticate using embedded browser using pop-up dialog: This option displays the AVEVA Identity Manager login page in an embedded browser using a pop-up window when you are prompted to authenticate.
- Select to authenticate using your default browser: This option displays the AVEVA Identity Manager login page in your default browser when you are prompted to authenticate.



Note: The default behavior - an embedded pop-up dialog - is best for a machine that has no browser installed. Selecting to use your computer's default browser will support all other uses.

Federated Identity Provider

Federated identity is a method of connecting a user's identity across multiple separate identity management systems. Users can move between systems while maintaining security. It allows authorized users to access multiple applications and domains using a single set of credentials.

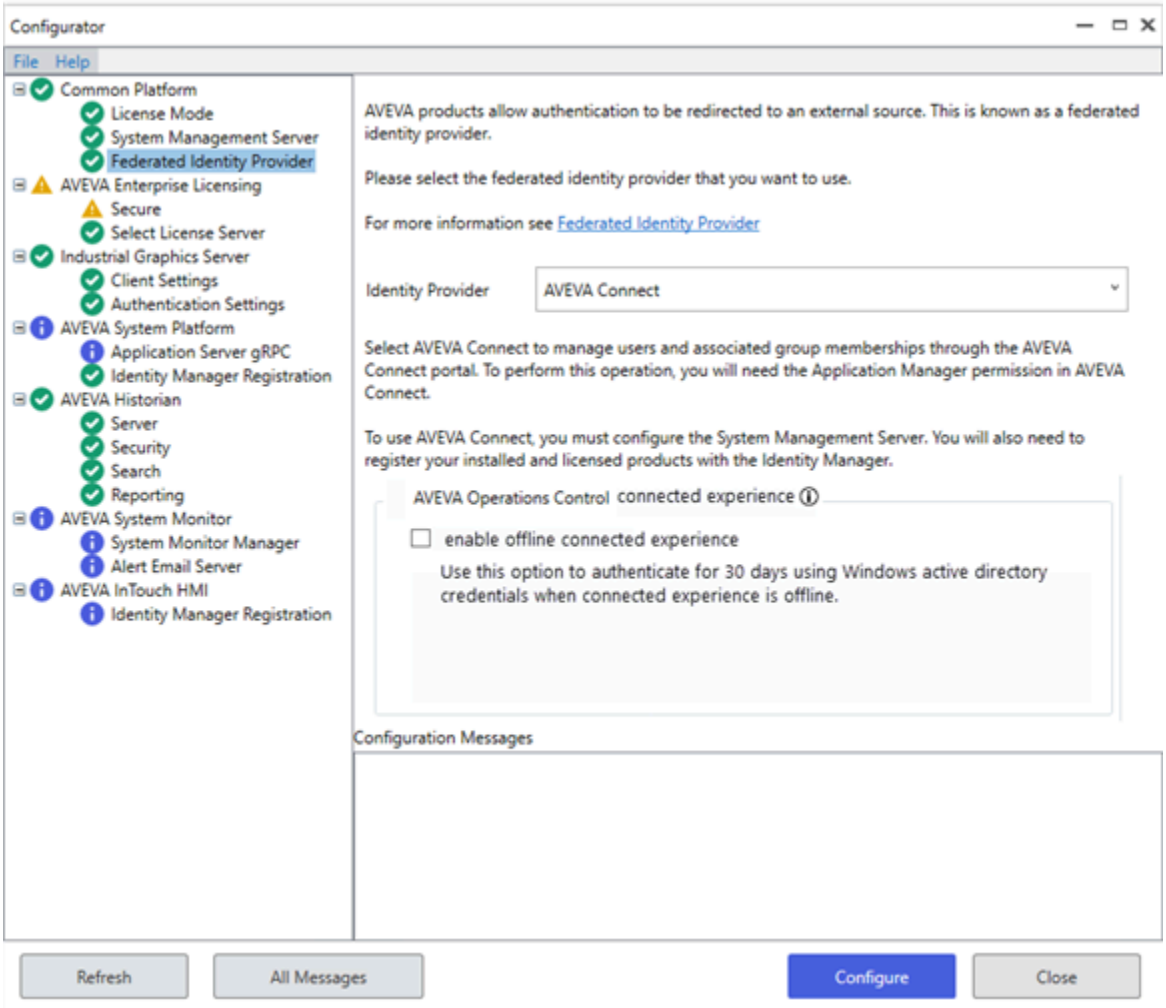
Note: An internet connection must be available on all nodes in your system during operation under the connected experience including authentication. If your system is offline or you have otherwise lost connection with CONNECT, see Offline connected experience for information about offline options.

The Federated Identity Provider plugin registers on-premises AVEVA Identity Manager server with the external identity provider (Azure AD or AVEVA Connect), establishing a trust-based relationship between them. The user

authentication is delegated to the external identity provider.

When you launch an AVEVA product on a node that's configured to be a connected experience node, you are prompted to authenticate via one of the two authentication user experiences (as configured) using their federated ID with AVEVA Connect. This requires your Active Directory to be federated or synced with your AVEVA Connect account. AIM acts as a middle layer for all the session and authentication redirects and capabilities.

All on-premises Operations Control products are required to use AIM as a local identity provider to run in Operations Control mode. AIM is configured to federate with CONNECT and CONNECT is federated with your identity provider. All cloud services use AVEVA Connect as an identity provider, and it can be configured to federate to your Azure AD or other identity provider. This is required only for connected experience. For non-connected experience, it is optional.



Before you register your product with the federated identity provider, ensure the following:

- Enable AVEVA Operations Control connected experience as your license mode
- Configure System Management Server (SMS)

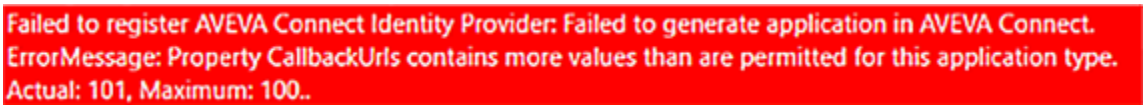
For more information about AVEVA Identity Manager refer to the following topics:

- AVEVA Identity Manager guide
- Key Concepts of Identity Manager

- Certificates
- Identity Provider Options- Azure AD authentication, AVEVA Connect authentication
- Federated Identity Provider Workflow
- Complete Federated Identity Provider configuration

Troubleshooting connection problems

The Federated Identity Provider plugin supports registering up to 100 System Management Servers (SMS) or Redundant SSO Servers (RSSO) with an AVEVA Connect account. If you exceed this limit, the Configurator displays the following error message:



To continue with the registration process, do these steps (detailed instructions follow).

1. Delete stale or unused application URLs from your AVEVA Connect account.

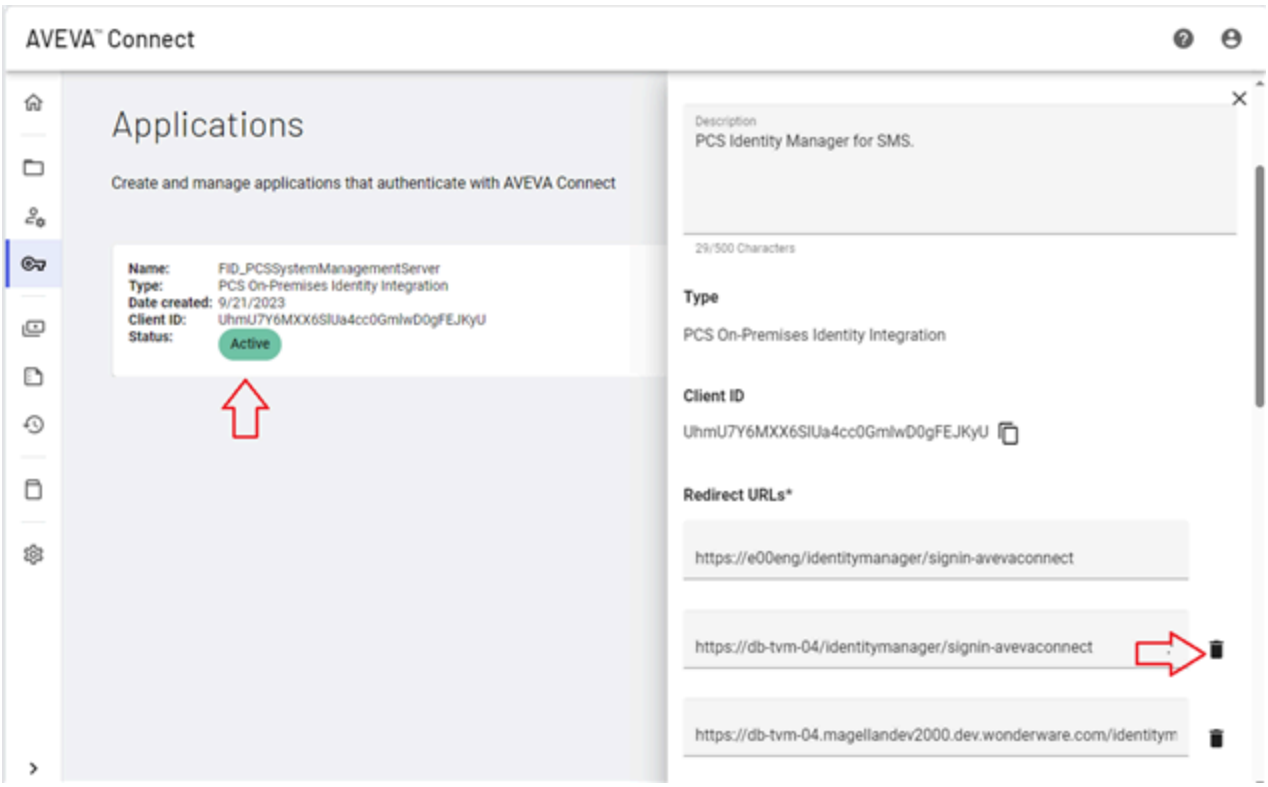
This step alone could resolve a limitation issue. If not, proceed with the following steps.

1. Acquire an access token
2. Configure an application
3. Add URL's to an existing application
4. Add a new application
5. Register the System Management Server or Redundant SSO Server with AVEVA Connect via Powershell

To delete stale or unused application URLs from AVEVA Connect

1. Log into your AVEVA Connect account.

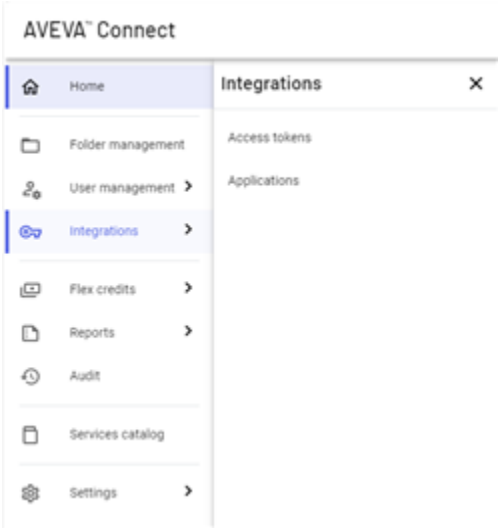
   Note: You must be an administrator on your AVEVA Connect account to perform this operation.
2. Click an application. The **Edit Application** slide-in pane appears.
3. Scroll down to the listed Redirect and Log out URLs.
4. Click the delete (trash can) icon to delete a URL.



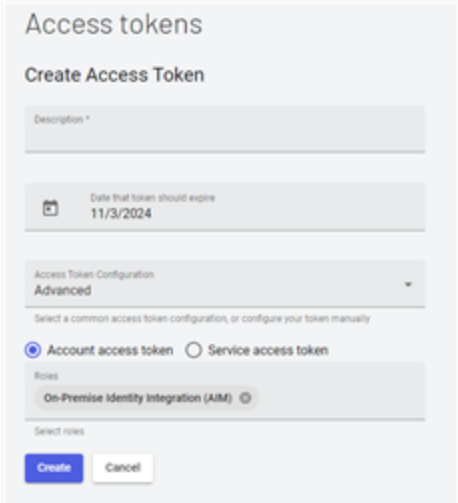
5. Repeat step 4 for all stale or unused URLs for each application.

To acquire an access token

1. Open the browser and navigate to AVEVA Connect.
2. Sign in with your user credentials, and if prompted, select the appropriate account.
3. Select **Integrations** from the left navigation pane.



4. Select **Access tokens** and then select **Create access token** to create a new access token.



5. For **Access Token Configuration**, select **Advanced**.
6. Select **Account access token** option.

   Ensure that the **Roles** include **On-Premise Identity Integration (AIM)** and record the access token.This is required later during the registration process.

To configure an application

Link the redirect URL's and logout URL's with an application. Each application can support 100 redirect URL's and 100 logout URL's.

1. Select **Integrations** from the left navigation pane.
2. Select **Applications**.

   By default, the screen displays "FID_PCSSystemManagementServer" application. This application is automatically created by the Federated Identity Provider configurator plugin.

To add URLs to an existing application

1. If you have any other applications listed other than the default application, select the other application.
2. Confirm whether the application **Type** is set to "PCS On-Premises Identity Integration".

   If the application **Type** is not set to "PCS On-Premises Identity Integration", ignore the application as it was created for a different purpose.
3. Scroll through the redirect URLs and select **Add redirect URL**.
4. Add a redirect URL in the format "https://{fqdn}/identitymanager/signin-avevaconnect" (where {fqdn} is your fully qualified domain name. i.e. mycomputer.mydomain.com).
5. Scroll through the logout URLs and select **Add logout URL**.
6. Add a logout URL in the format "https://{fqdn}/identitymanager/signedout-callback-avevaconnect" (where {fqdn} is your fully qualified domain name. i.e. mycomputer.mydomain.com).
7. Record the **Client ID** for the application.

To add a new application

If the application "FID_PCSSystemManagementServer" is the only application, or if the other application has also reached the limit of 100 redirect URLs and 100 logout URLs, then create a new application before adding in your

redirect and logout URL's.

1. Select **Create application** to create a new application for AIM integration.
2. Select the **Type** as"PCS On-Premises Identity Integration".
3. Record the **Client ID** field. This is required later during the registration process.
4. Scroll through the redirect URLs and select **Add redirect URL**.
5. Add a redirect URL in the format "https://{fqdn}/identitymanager/signin-avevaconnect" (where {fqdn} is your fully qualified domain name. i.e. mycomputer.mydomain.com).
6. Scroll through the logout URLs and select **Add logout URL**.
7. Add a logout URL in the format "https://{fqdn}/identitymanager/signedout-callback-avevaconnect" (where {fqdn} is your fully qualified domain name. i.e. mycomputer.mydomain.com).

To register the System Management Server or Redundant SSO Server with AVEVA Connect via Powershell

On the computer that is configured as the System Management Server (or RSSO), launch Powershell as an administrator and run the following commands:

```
$AccessToken = ConvertTo-SecureString -String "********" -AsPlainText -Force Add-
PcsAuthenticationProvider -name AvevaConnect -ClientID ******** -Endpoint
https://signin.connect.aveva.com -ServicesEndpoint https://services..aveva.com/
-AccessToken $AccessToken
```

Configure System Platform components

Configure System Platform components using the Configurator dialog box after installation. Configurator includes a product tree that lists the components for each of the products that require post-installation configuration. It has a set of pages that can be accessed via a directory to the left of the interface.

Register your product with Identity Manager

The AVEVA Identity Manager (AIM) is a standalone authentication server that allows users to log into AVEVA products using a standard user experience. This makes use of the industry standard OpenID Connect protocol. Before you register your product with Identity manager, ensure you have configured the System Management Server.

For AVEVA Identity Manager registration, refer to the product documentation, as each product has its own registration page.

Note: If you change the System Management Server address, you must re-register all installed products.

Configure Industrial Graphics Server

The **Industrial Graphic Server** is installed whenever the **InTouch** run-time component is installed on a node, and lets users view **InTouch HMI** applications in a web browser.

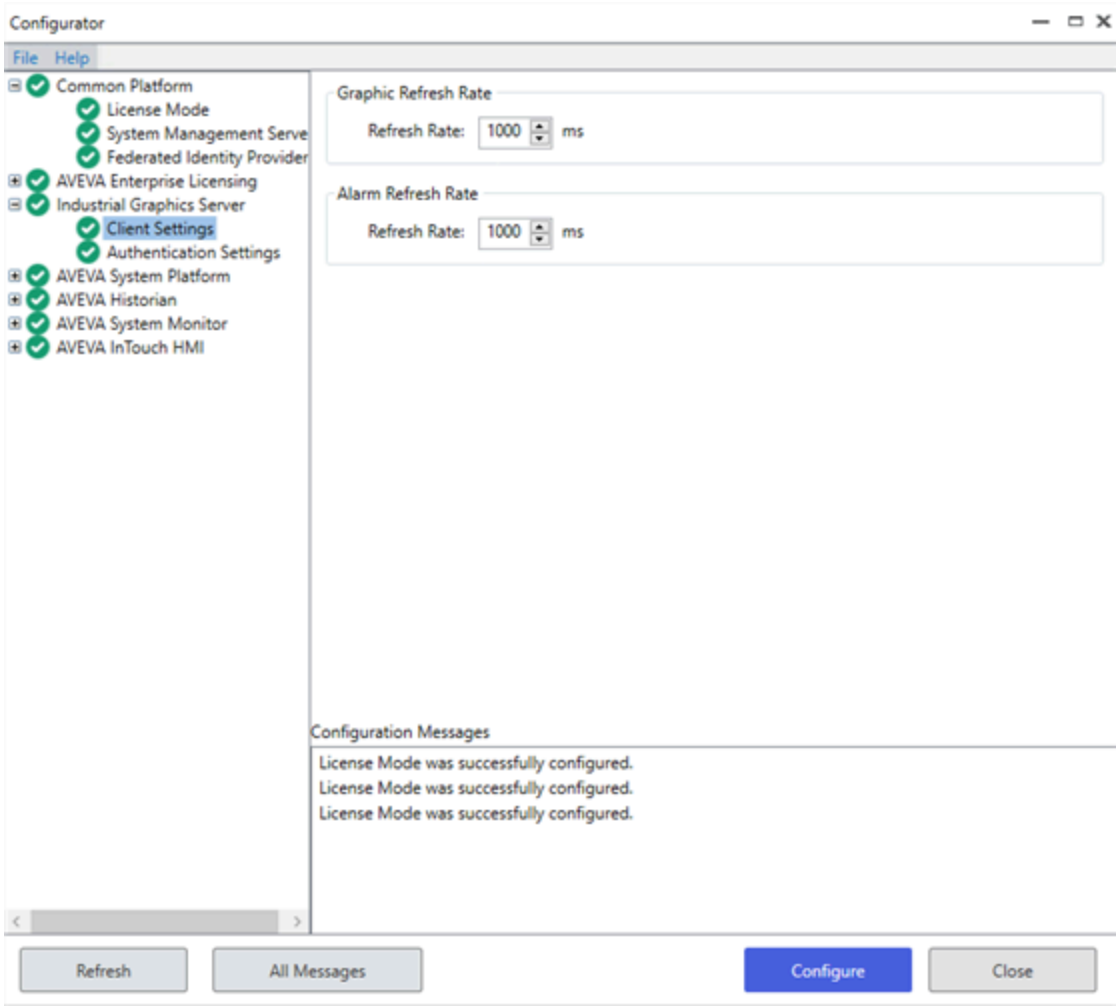
There are two configuration items for the **Industrial Graphic Server**:

- **Client Settings**: This sets how frequently the Web Client refreshes graphics and alarms.
- **Authentication Settings**: This establishes the credentials that the Web Client will use for connecting to the web server.

Client Settings

To configure Client Settings

1. On the left navigation pane, expand **Industrial Graphics Server**, and select **Client Settings**.



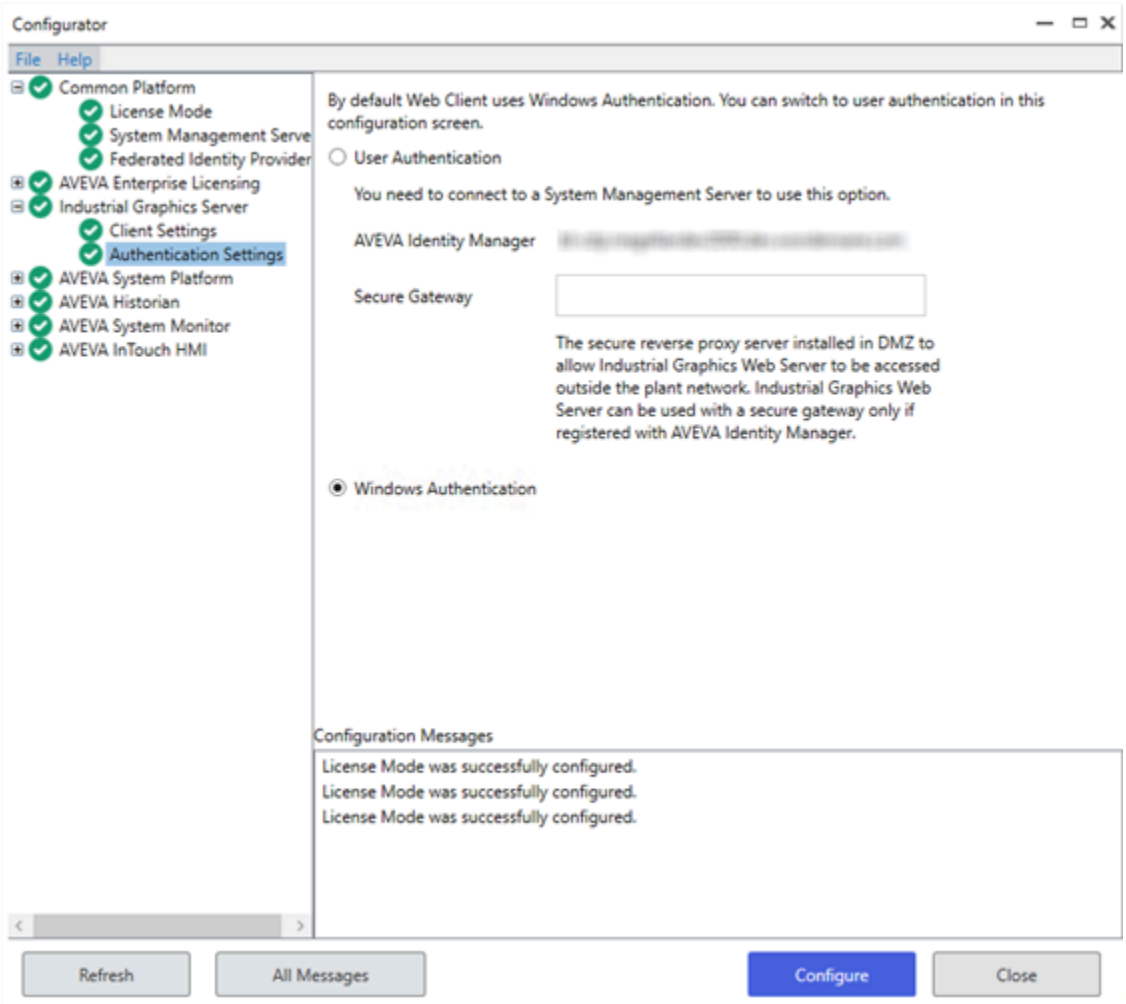
2. Under **Graphic Refresh Rate**, set the screen refresh interval. This determines how frequently the web browser will query the web server for graphic data. A longer interval reduces network traffic and may be needed for very low-bandwidth networks or intermittent connections.
   - Default: 1000 ms (1 second)
   - Minimum: 250 ms
   - Maximum: 60000 ms (60 seconds)

   Note: The **Graphic Refresh Rate** cannot be less than the **Alarm Refresh Rate**. If you lengthen the **Graphic Refresh Rate**, the **Alarm Refresh Rate** will automatically synchronize with the **Graphic Refresh Rate**.
3. Under **Alarm Refresh Rate**, set the alarm refresh interval. This determines how frequently the web browser will query the web server for alarm data. By default, the **Alarm Refresh Rate** is the same as the **Graphic Refresh Rate**. You can make the refresh interval longer for alarms than for graphics, but the **Alarm Refresh Rate** cannot be shorter than the **Graphic Refresh Rate**. A longer interval may be needed for very low-bandwidth networks or intermittent connections.
   - Default: 1000 ms (1 second)
   - Minimum: **Graphic Refresh Rate**
   - Maximum: 60000 ms (60 seconds)

Authentication Settings

To configure Authentication Settings

1. On the left navigation pane, expand **Industrial Graphics Server,** and select **Authentication Settings.**



   There are two options:

   - **User Authentication**. This lets you configure the Web Client to use Single Sign-On using the **AVEVA Identity Manager**. The **System Management Server** must be configured before selecting this option, and is used as the **AVEVA Identity Manager**.
   - **Windows Authentication** (default). Skip to step 3 if you are using **Windows Authentication**.

2. **User Authentication configuration (optional):** To allow access outside the plant network, enter the **Secure Gateway** URL, which is a secure reverse proxy server installed in the DMZ.
3. Select **Configure**.
4. Select the next item in the left pane that requires configuration. When all required items have been configured, select **Close** to complete installation.

Configure AVEVA Historian

You can use the Configurator to configure **AVEVA Historian** settings.

The configuration items for AVEVA Historian are:

- **Server**
- **Security**
- **Search**
- **Reporting**

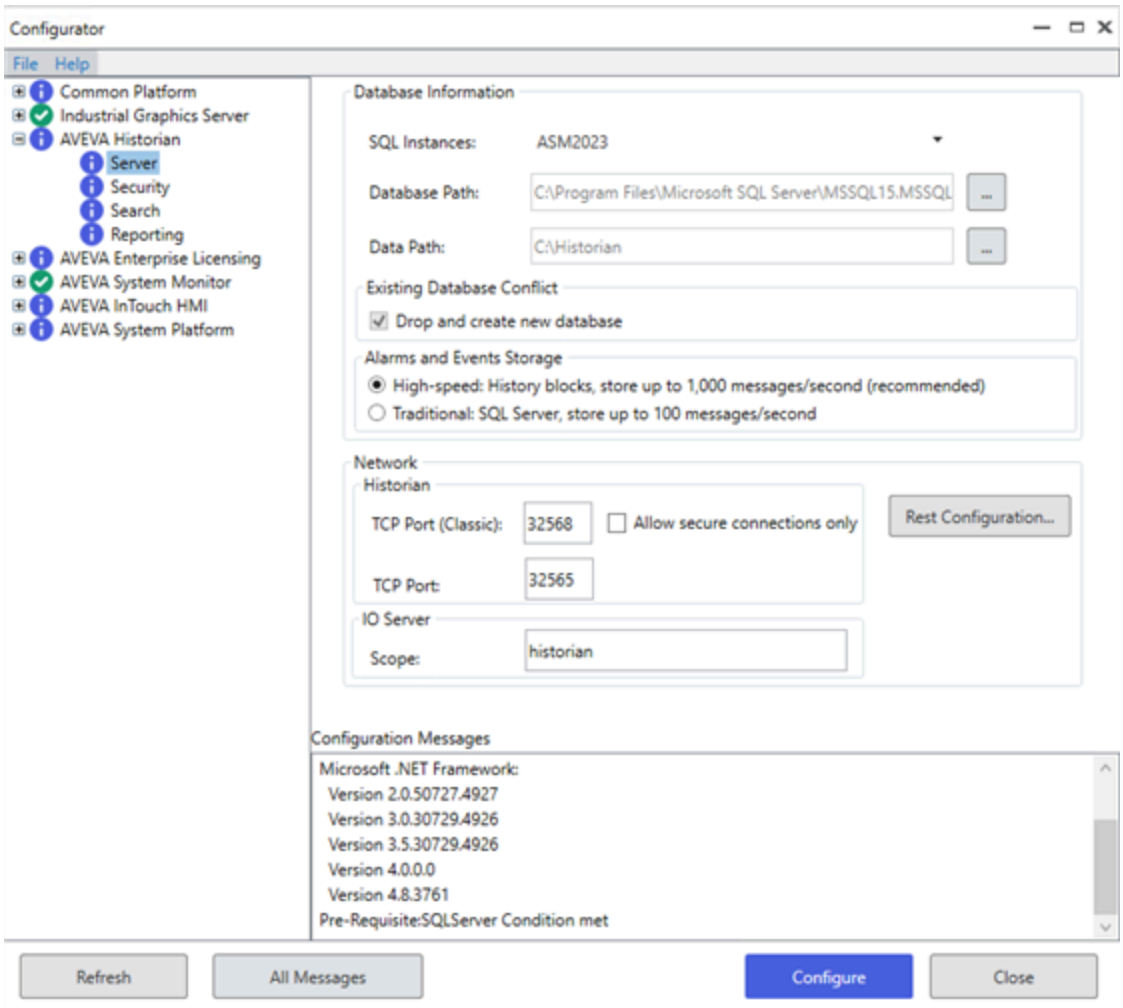
Note: Before running the Configurator, be sure SQL Server is installed and running. Also, be sure you have SQL Server administrator rights.

Server

To configure Server settings

Important: Most server settings cannot be changed while **Historian** is running. To change most server settings after initial configuration, you must first shut down and disable the historian using the **Management Console**. After making the change, restart and enable the historian.

1. On the left navigation pane, expand **AVEVA Historian**, and select **Server.**

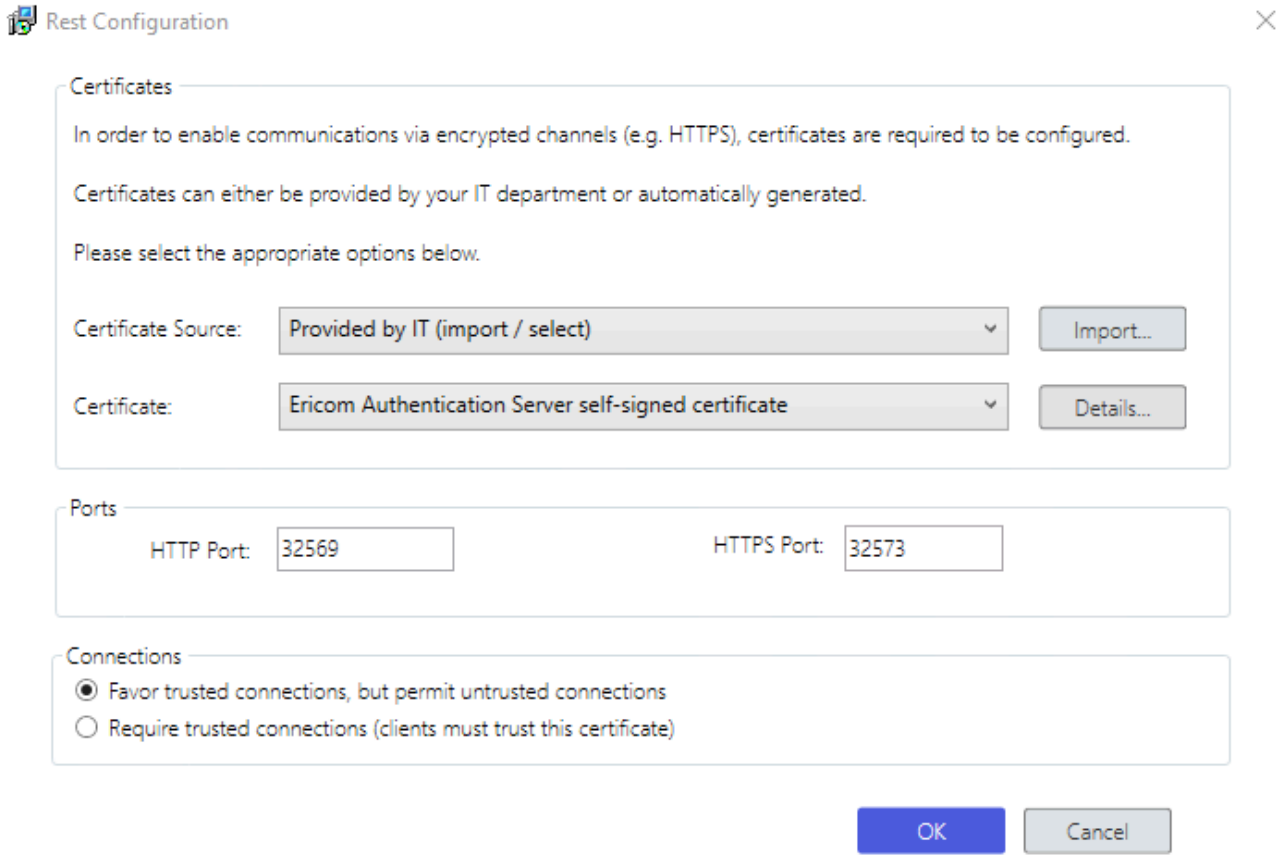


2. Under **Database Information**, specify the **SQL Instances**, **Database Path** and **Data Path**.
   - **SQL Instances**
     Name the SQL Instance associated with this historian.
   - **Database Path**
     Unless you have specific requirements, keep the default SQL Server database path. The default is tied to your SQL Server installation and is the path where the configuration database is deployed. If you need to change the default path, select the ellipsis button to specify a different directory in which to install the historian database files.
3. Under **Existing Database Conflict**, read the notices, if any.
   If the database is created for the first time, then this option is not available. When reconfiguration is done, then the **Drop and Create New Database** option is available. If you select this check box, then the existing database is dropped and a new database is created. If this check box is cleared, then the database is not dropped, but configured for changes, if any.
4. Under **Alarms and Events Storage**, configure how you want to store alarm and events.
   - **High-speed (default/recommended)**
     The high-speed setting for storing alarms and events in history blocks provides several advantages. You can manage the data using simple operations such as moving, copying, or deleting folders, instead of using database management software. With this storage method, you no longer need to purge to sustain storage. This method offers significantly higher storage rates. Also, the capacity for alarm and event

storage is only limited by disk space, not by insertion rate.

- **Traditional**
  The traditional setting stores alarms and events in the A2ALMDB SQL Server database. This works well for smaller applications. Alarm and event data stored in the A2ALMDB database can be retrieved using SQL queries. You can also use SQL Server tools, such as Reporting Services, to query alarm and event history.

5. Under **Network**, accept the default Historian TCP ports or change these settings. The ports you specify are added to the exclusions list of Windows Firewall. You must manually add these ports as exclusions if you use another hardware or software firewall.
   - **TCP Port (Classic)** is used for receiving data from another system using Historian version 2023 or earlier. If you are sending data to Historian from an Application Engine, Remote IDAS or from another Historian, you must specify this port as part of the connection settings on those source systems.
   - **TCP Port** is used for receiving data from another system using Historian version 2023 R2 or later. If you are sending data to Historian from an Application Engine, Remote IDAS or from another Historian, you must specify this port as part of the connection settings on those source systems.
6. Select **Allow secure connections only** to only allow connections to nodes trusted by the System Management Server.
7. Select **Rest Configuration** to configure remote access to the Historian REST API and Historian Client Web. The **Rest Configuration** dialog displays.



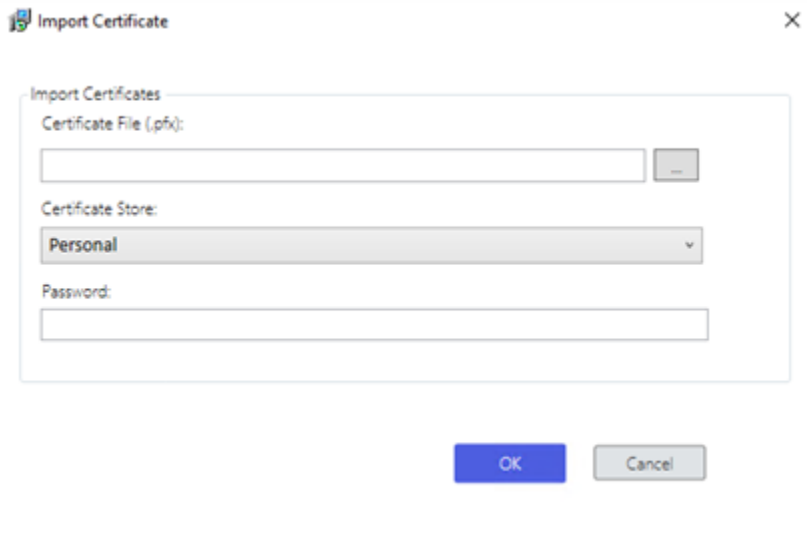
To configure the HTTPS connection, a certificate is required. You can use a certificate provided by your IT department, or you can use a self-signed certificate generated by the configurator.

a. To use a certificate provided by your IT department, select "Provided by IT (import / select)" as the

Certificate Source.

a. If the certificate is already installed on the system, select the appropriate **Certificate** from the list.

b. If you have been provided with a certificate but it is not yet installed on the system, select **Import...**. The **Import Certificate** dialog displays.



Select ... to browse and select the certificate file, which has a .pfx file extension.

c. Select the **Certificate Store** in which to save the Certificate, as directed by your IT department.

d. Enter the **Certificate** password and select **OK** when all the information is correct.

b. To use a self-signed certificate, select "Automatically Generated" as the **Certificate Source**. The name of the **Certificate** is automatically selected for you and cannot be changed.

Using a self-signed certificate makes it easier to configure the server, but it makes the remote browsing experience more complicated, with users receive security warnings in their browser until the certificate is "trusted" on their system.

Note: After configuring the Historian with an automatically generated self-signed certificate, when you visit this dialog again, the **Certificate Source** is "Provided by IT (import / select)". This is because the certificate is installed on the system after configuration, and can now be selected from the **Certificate** list.

---

c. Enter the port numbers to use for the **HTTPS Port** and the **HTTP Port**. These ports are used for data queries via Insight or the Historian REST API to the Historian Server.

Note: To allow the correct functioning of the Alarm Control History Blocks, the firewall must be configured to permit inbound and outbound network traffic on these ports.

---

d. The **Connections** option determines what happens when a connection is made to Historian Client Web over the untrusted (HTTP) port. Select one of the following options:

a. **Favor trusted connections, but permit untrusted connections.** When this option is selected, users at run time are informed there is a trusted connection available, and they can decide whether to use the trusted or untrusted connection. For more information about the run-time options, refer to the *Historian Administrator Guide*.

b. **Require trusted connections (clients must trust this certificate)**. When this option is selected, if you are using a certificate from a trusted authority, users are redirected to the HTTPS connection. If you are using an untrusted certificate, such as a self-signed certificate, an informational message is

displayed that directs users how to proceed. For more information about this message and how users can proceed, refer to the *Historian Administrator Guide*.

e. Select **OK** to accept the selected options, then select **Configure** to apply any changes to the system.

Using HTTPS Instead of HTTP for Historian Client, Historian Client Web, and REST APIs

Typically, customers using Historian Client Web or the REST API can connect to a Historian server from a Historian Client or other client application using an unencrypted (HTTP) connection. (Even without an encrypted connection, the user credentials exchanged during login are still encrypted.) You can also use an encrypted connection (HTTPS) for the REST API, and this requires configuring an X.509 certificate for TLS (transport layer security).

About TLS, HTTPS, and X.509 Certificates

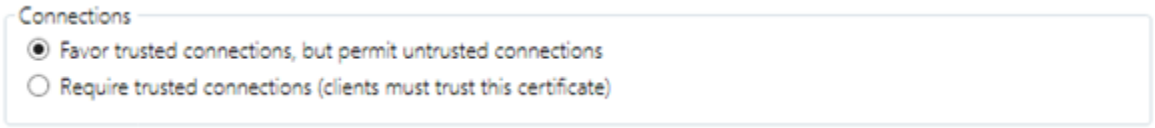
TLS allows for encrypted authentication credentials to be passed between a server and client. A certificate containing a private key is passed between the client and server to verify identification and allow access.

Using HTTPS ensures that communication between the client and server is encrypted, helping to prevent third parties from stealing or tampering with your data.

To configure the HTTPS connection to the Historian, you need an X.509 certificate. The certificate can be from a trusted authority or a self-signed certificate. During the installation and configuration of the Historian, you can import a certificate from a trusted authority if you have one, otherwise the configurator can create a self-signed certificate for you.

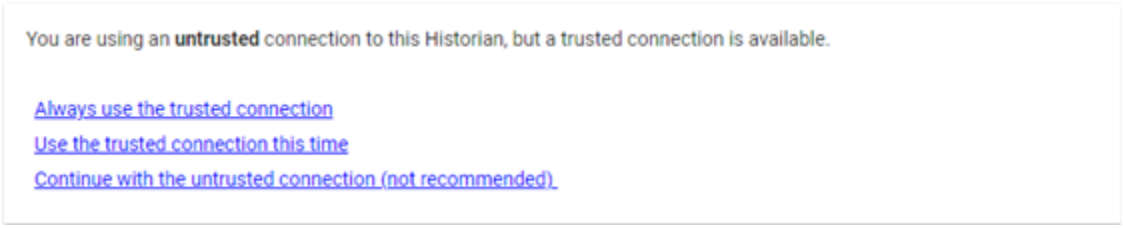
About Configuring Security

When you configure the Historian server, you choose one of two options to control what happens when a user connects using the unencrypted (HTTP) connection:



1. **Favor trusted connections, but permit untrusted connections**

   When this option is selected, users are informed there is a trusted connection available, and they can decide how to proceed using one of three options:



   - **Always use the trusted connection**

     If the user clicks this link, their browser will be permanently redirected to the HTTPS connection. Any future attempts to use the HTTP connection with the same browser are automatically redirected to the HTTPS connection without a prompt.

   - **Use the trusted connection this time**

     Clicking this link redirects the browser to the HTTPS connection, but only for this session. The next time a connection is made in a new browser session, the user is prompted to choose again.

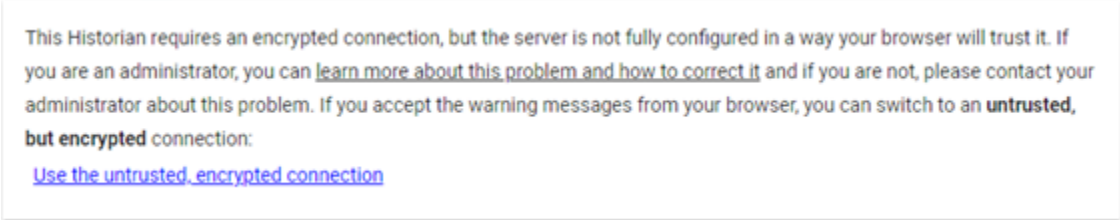
- **Continue with the untrusted connection (not recommended)**

  If the user clicks this link, the browser continues using the HTTP connection, but only for this session. The next time a connection is made in a new browser session, the user is prompted to choose again.

2. **Require trusted connections (clients must trust this certificate)**

   When this option is selected, if you are using a certificate from a trusted authority, users are redirected to the HTTPS connection.

   If you are using an untrusted certificate, such as a self-signed certificate, the following informational message is displayed:

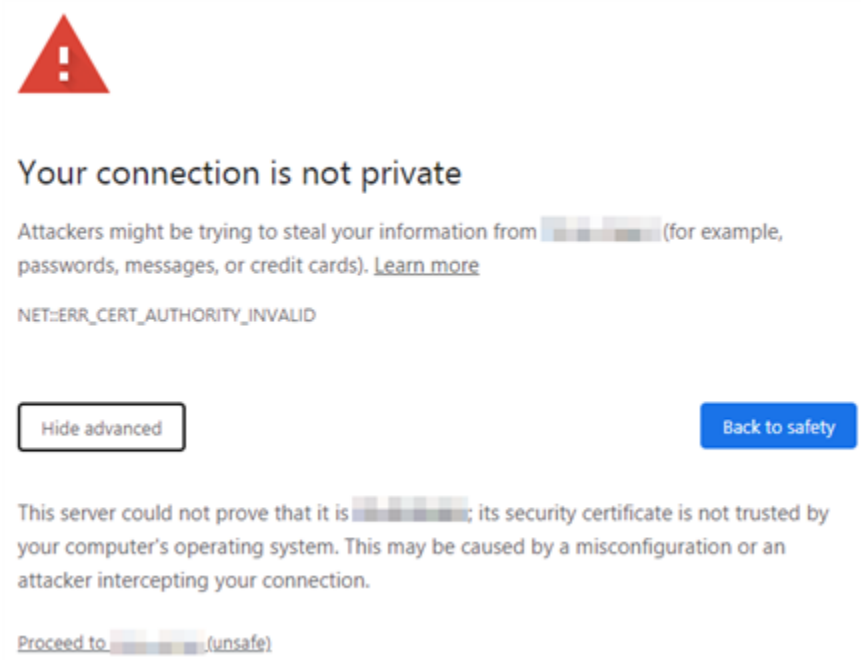
   Users can click **Use the untrusted, encrypted connection** to use the HTTPS connection.

   Warning: It is important to understand the risks associated with using an untrusted self-signed certificate. The browser warnings encountered while using a self-signed certificate could also indicate that the server has been compromised or hijacked by a third party. To avoid the risk of conditioning users to ignore important security warnings, follow the steps in the next section to enable remote clients to trust the self-signed certificate.

   Using a Self-Signed Certificate

If you choose to use a self-signed certificate with the Historian, you are responsible for configuring all clients to trust that certificate. Clients that haven't trusted the certificate see a security warning in their browser.

For example, if you configure your Historian using a self-signed certificate, users connecting with the Google Chrome browser see a warning message similar to the following:



Enabling Trust for a Self-Signed Certificate

A self-signed certificate needs to be "trusted" for the certificate to work without warnings when you access AVEVA Historian Client Web in your browser. Trusting the certificate involves two steps:

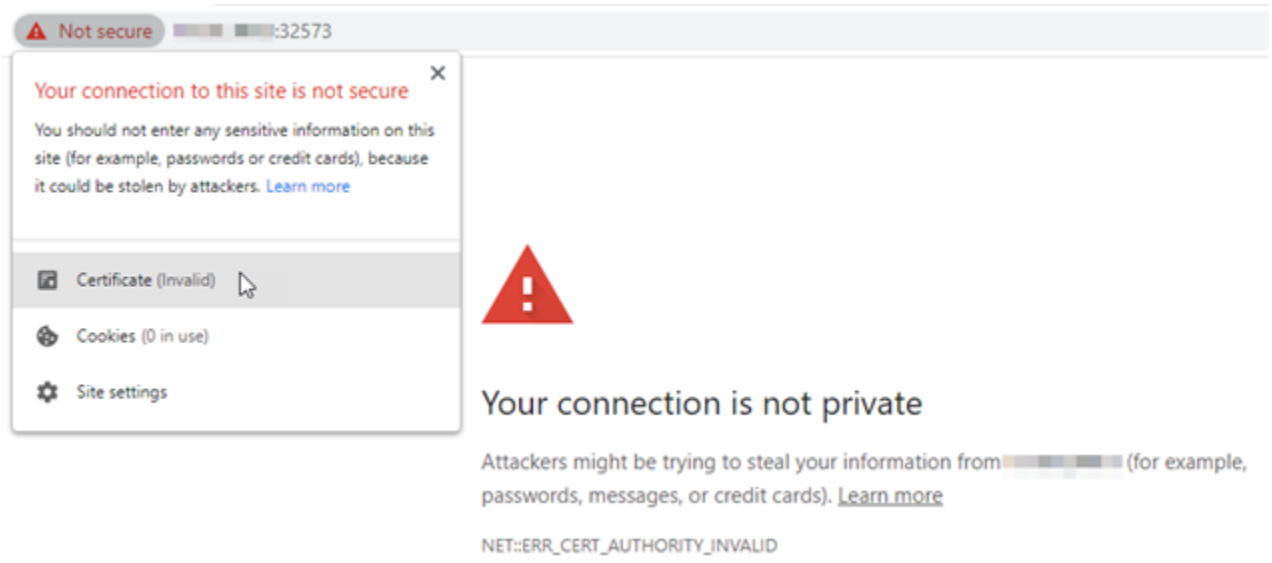
1. Acquire a copy of the certificate.
2. Install the certificate into the trusted root certificate store.

Acquiring a Copy of the Self-Signed Certificate

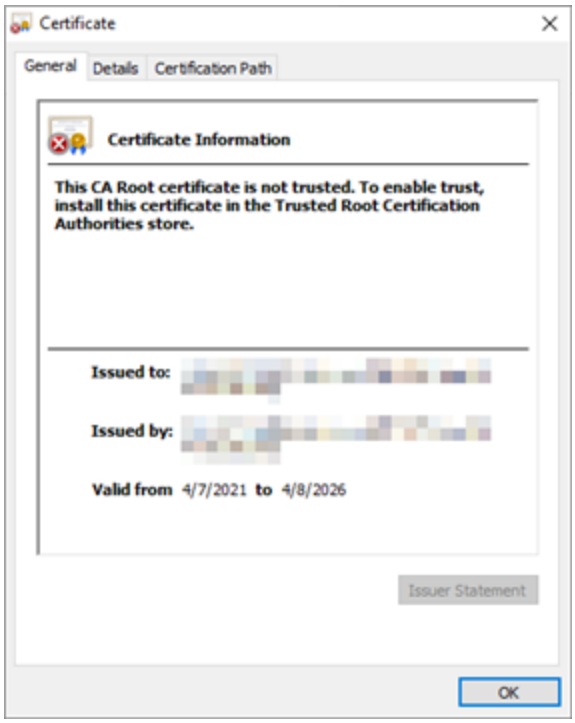
Before you can trust a self-signed certificate, you need a copy of the certificate on your system. If you already have a copy of the certificate, proceed to Trusting a Self-Signed Certificate.

To obtain a copy of the self-signed certificate:

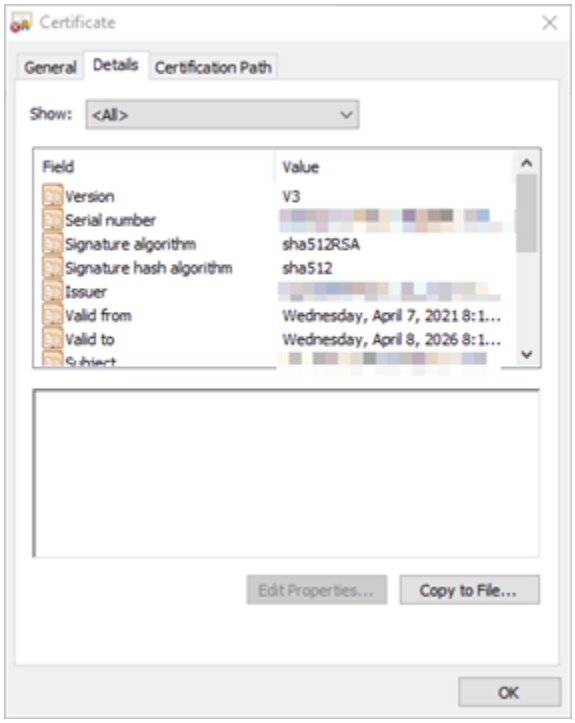
1. In your browser, browse to the AVEVA Historian Client Web URL.
2. In the address bar, click on the warning message indicating your connection is not secure.



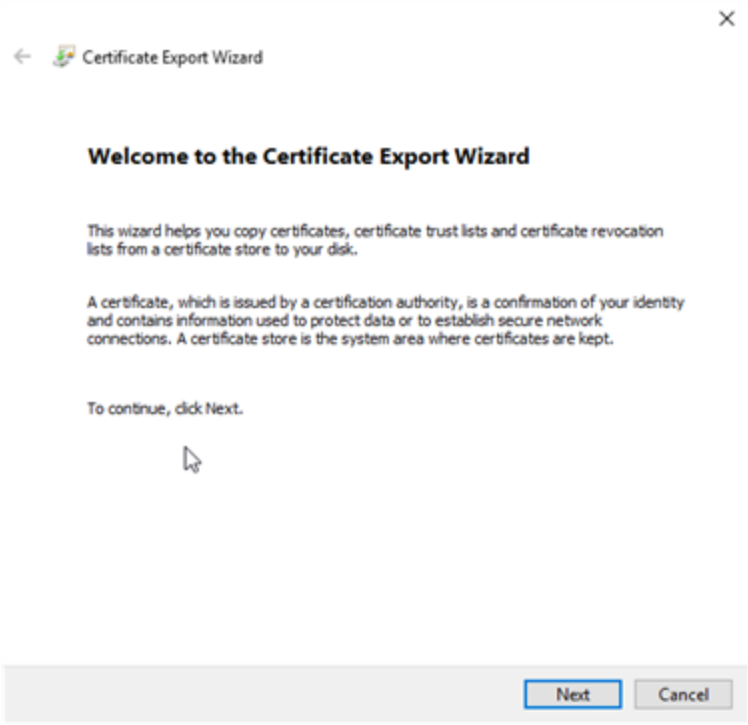
3. Click **Certificate (Invalid)**. The **Certificate** details dialog displays:



4. To trust the certificate, first you must save a copy. Select the **Details** tab.

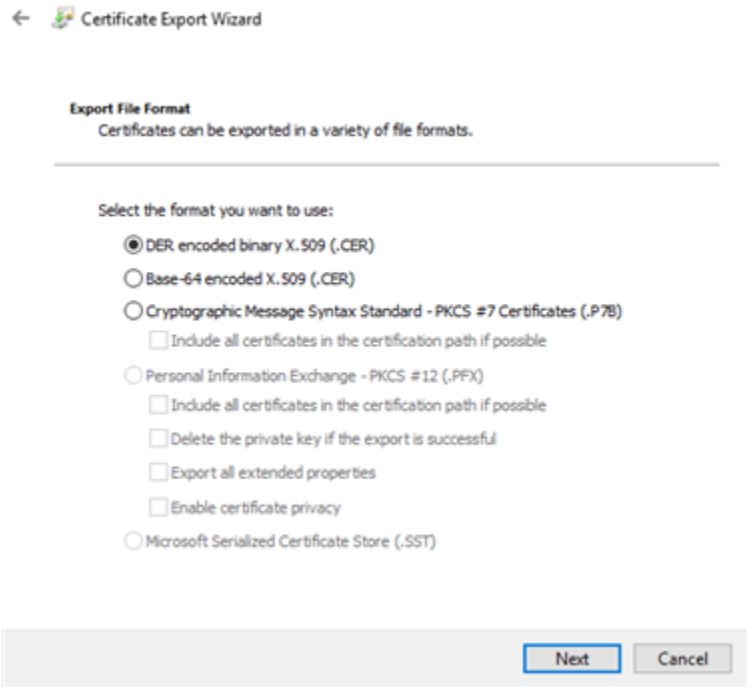


5. Click **Copy to File...**. The **Certificate Export Wizard** displays:



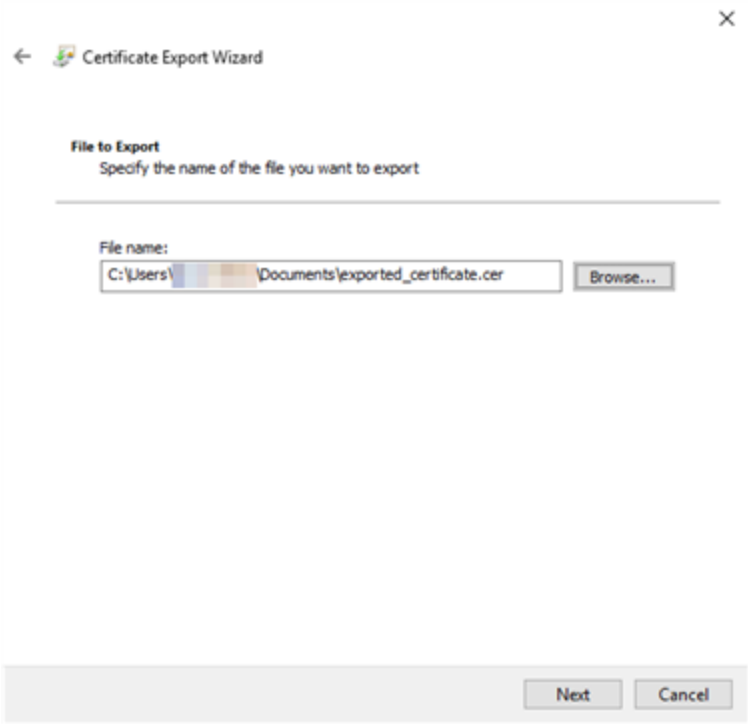
Click **Next**.

6. Select **DER encoded binary X.509 (.CER)** as the export file format:



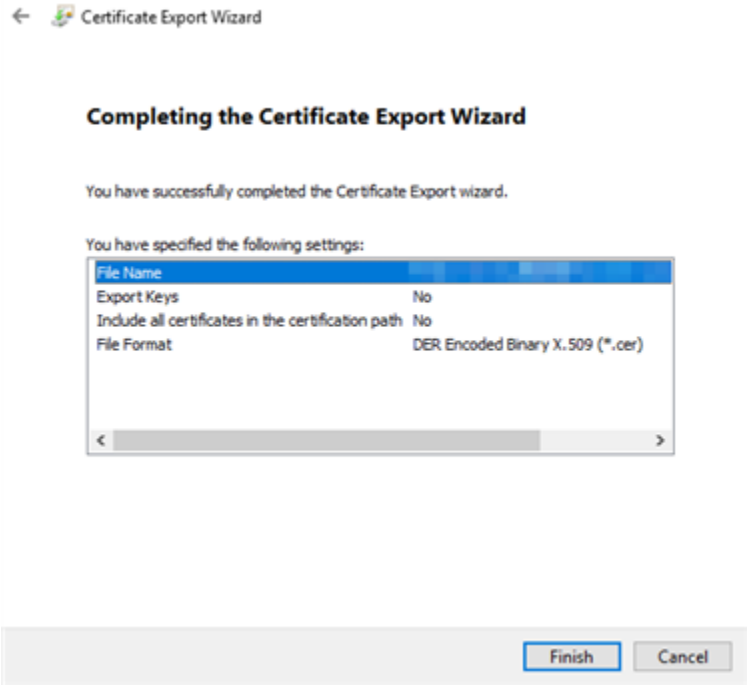
Click **Next**.

7. Click **Browse...** and choose a location to save the exported certificate.



Click **Next**.

8. Click **Finish** to export the certificate to the selected file:

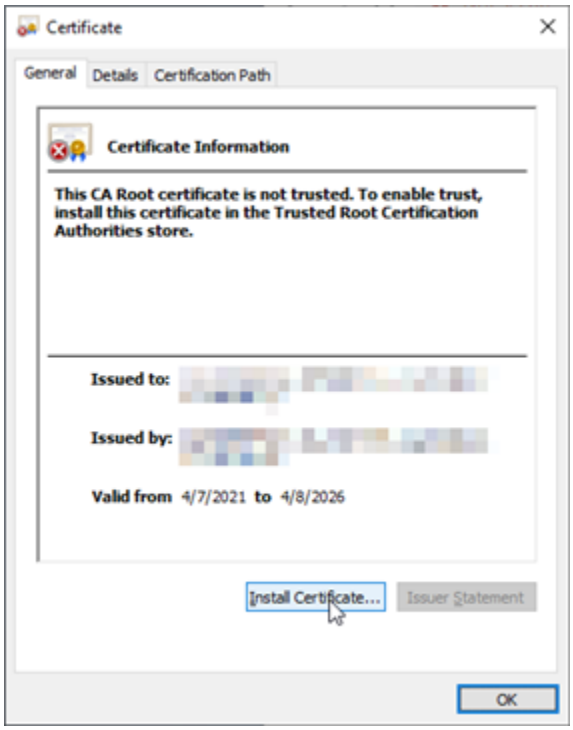


Trusting a Self-Signed Certificate

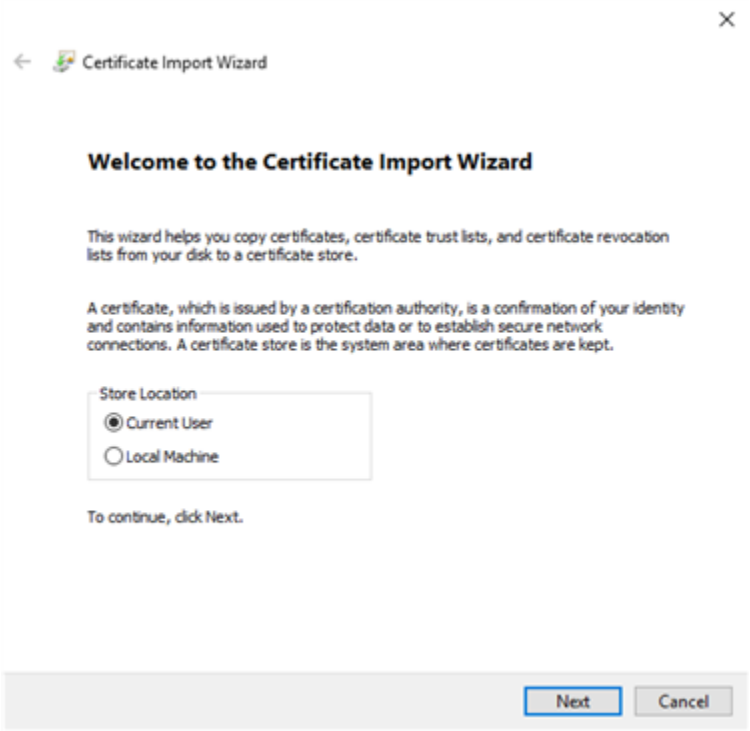
If the AVEVA Historian is configured with a self-signed certificate for TLS encryption, the certificate needs to be trusted on all client machines to avoid warning messages while using AVEVA Historian Client Web. To accomplish this, install the certificate into the trusted root certificate store on each client machine.

To install a self-signed certificate into the trusted root certificate store:

1. Locate and open the certificate file in Windows Explorer. The Certificate dialog displays:



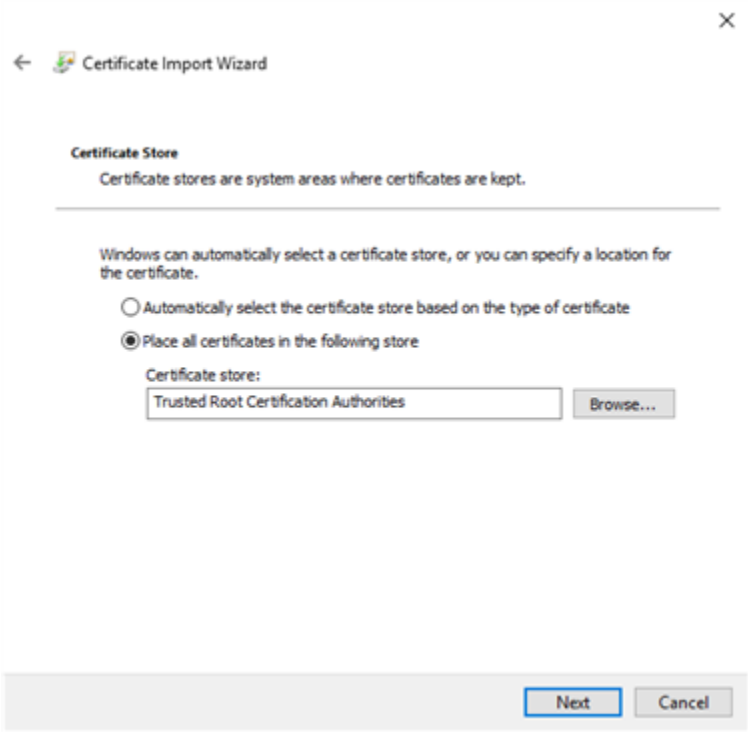
2. Select **Install Certificate...**. The Certificate Import Wizard displays:



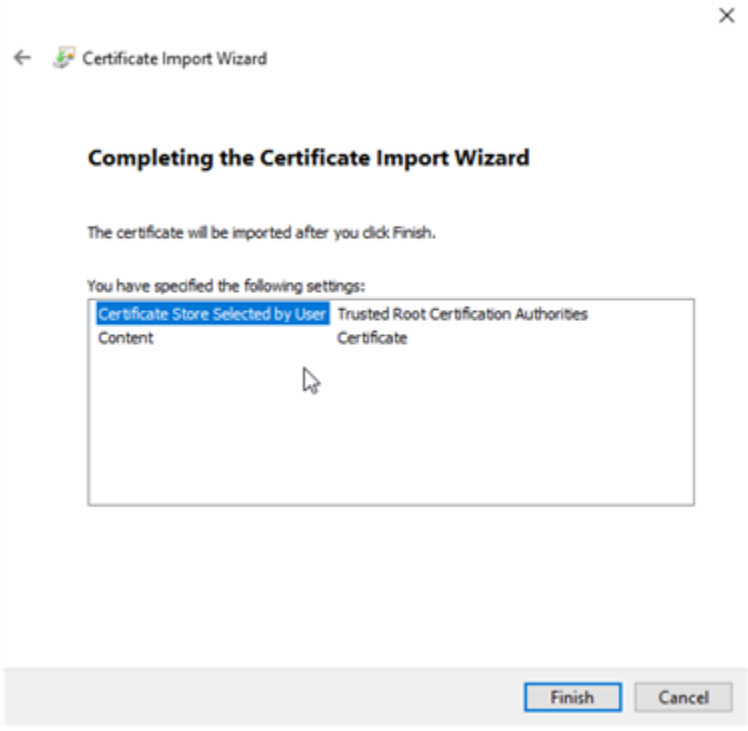
3. Select **Current User** to install the certificate for only the current user, or **Local Machine** to install the certificate for all users on this system.

Note: The **Local Machine** option requires administrative access to the system. If you do not have administrative access, select **Current User**.

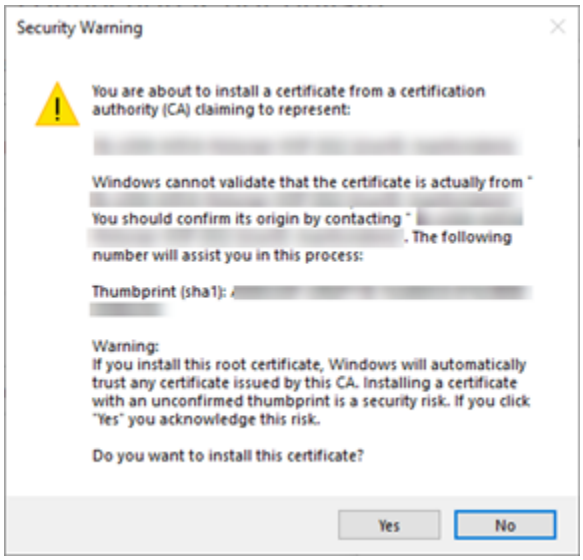
Click **Next**. The **Certificate Store** dialog displays:



4. Select **Place all certificates in the following store**. Click **Browse...** and select **Trusted Root Certification Authorities** as the **Certificate store**.
5. Click **Next.** The **Completing the Certificate Import Wizard** dialog displays:



6. Click **Finish** to complete the Certificate Import Wizard. A security warning displays:

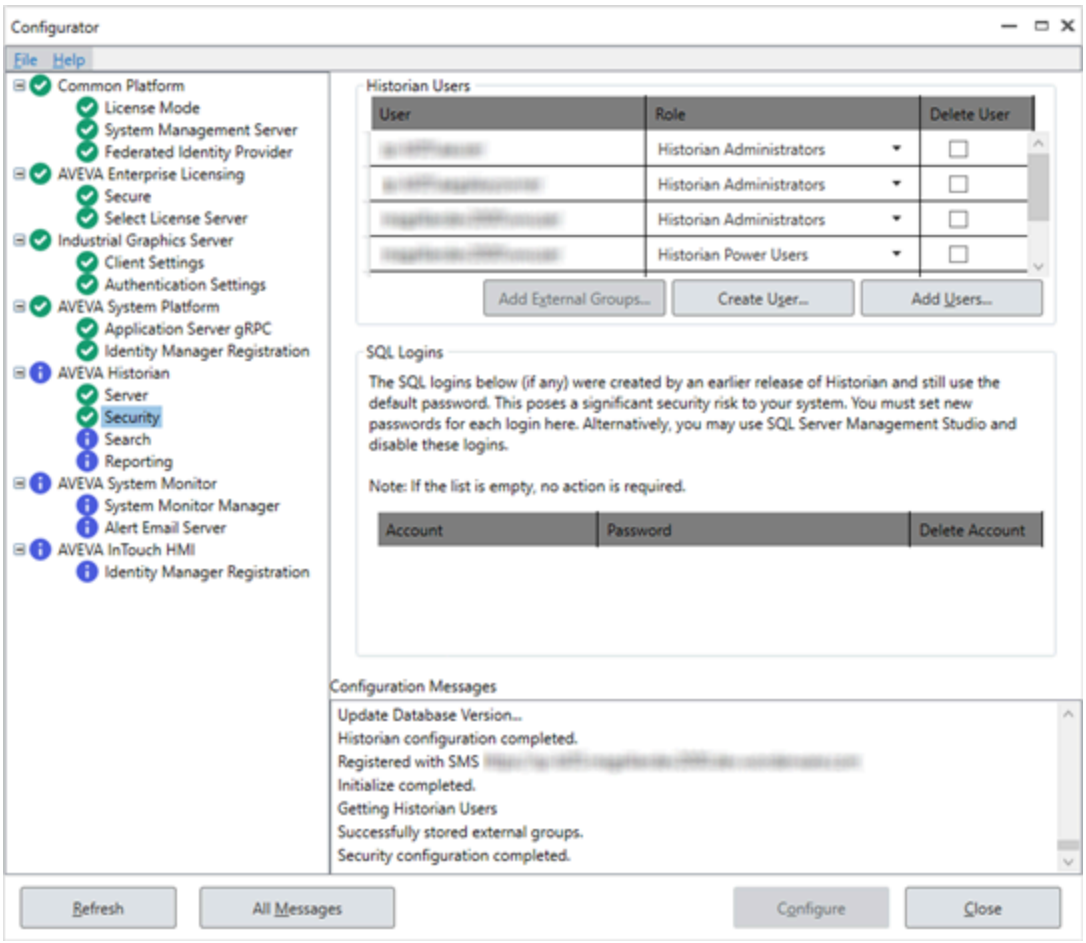


Click **Yes** to acknowledge the warning. The certificate is now trusted on your machine.

Security

To configure Security settings

1. On the left navigation pane, expand **AVEVA Historian**, and select **Security**.



2. Under **Historian Users**, review the existing users and roles for this server. Make adjustments to the list as needed:
   - To create a new user account, select **Create Users** and then specify account details.
   - To add existing user accounts to this list, select **Add Users** and then select the account criteria to use.
   - If you don't need this account anymore, mark the **Delete User** check box.
3. If you have configured an AVEVA Identity Manager server, select **Add External Groups**.

   The **Configure External Groups** dialog appears. To configure external groups:

   a. The Identity Provider Node field is automatically populated with the address of the AVEVA Identity Manager server based on the System Management Server configuration. Click **Get Groups**. The **Connect Groups** dialog appears. Select the groups you want to add and click **Add**.

   b. The groups are retrieved from the AVEVA Identity Manager server and shown in the **Connect Groups - Historian Role** section. For each external group, select from the dropdown which Historian role the group will have.

   c. Select **Save.**
4. Under **SQL Logins**, do one of the following to ensure your SQL Server logins are secure:
   - If you want to keep using a default account listed, type a new password.
   - If you don't need this account, mark the **Delete Account** check box.

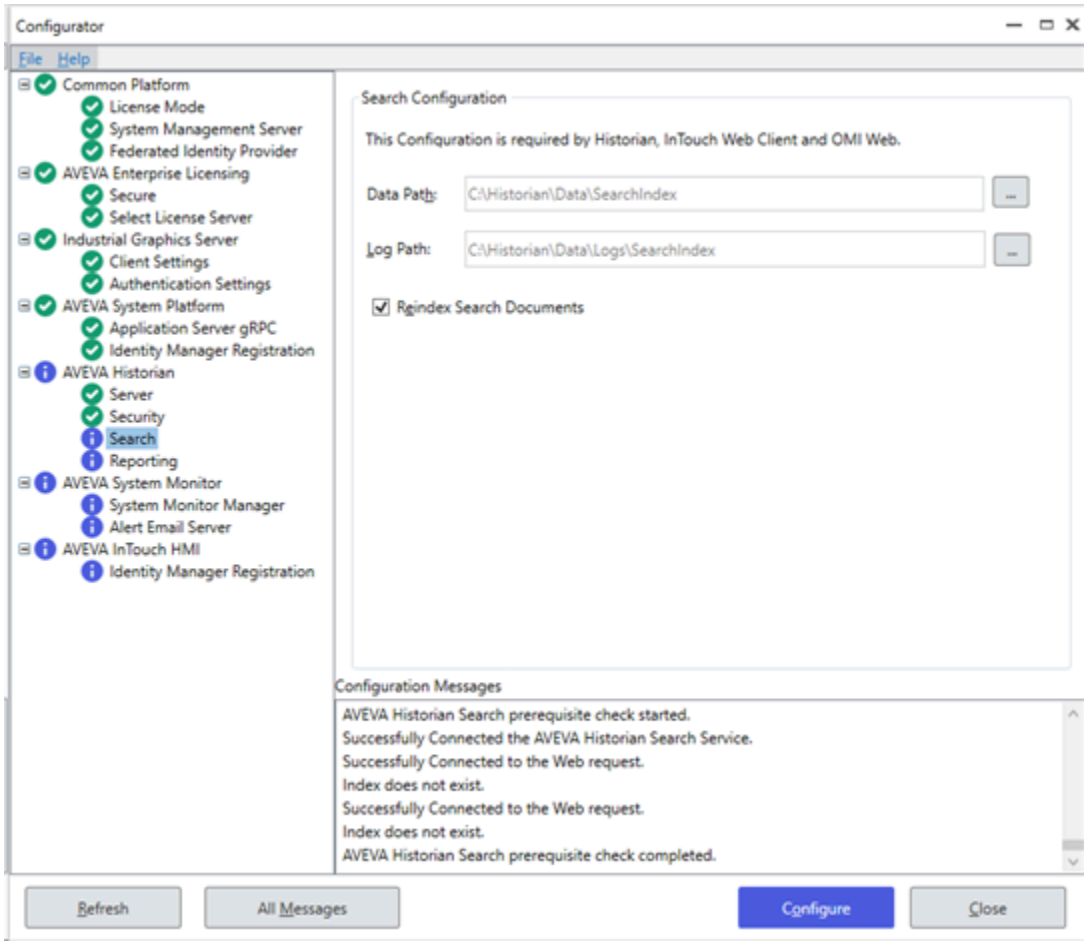
   Note: Secure Development Lifecycle (SDL) guidelines recommend against using automatically created users like aaUser and aaAdminUser with well-known or publicly documented passwords.

When you migrate from an older version of the Historian Server, this area is populated with all preexisting SQL Server accounts and gives you the option to change account password and to delete unused accounts to ensure strong security for your system.

Search

To configure Search settings

1. On the left navigation pane, expand **AVEVA Historian,** and select **Search**.



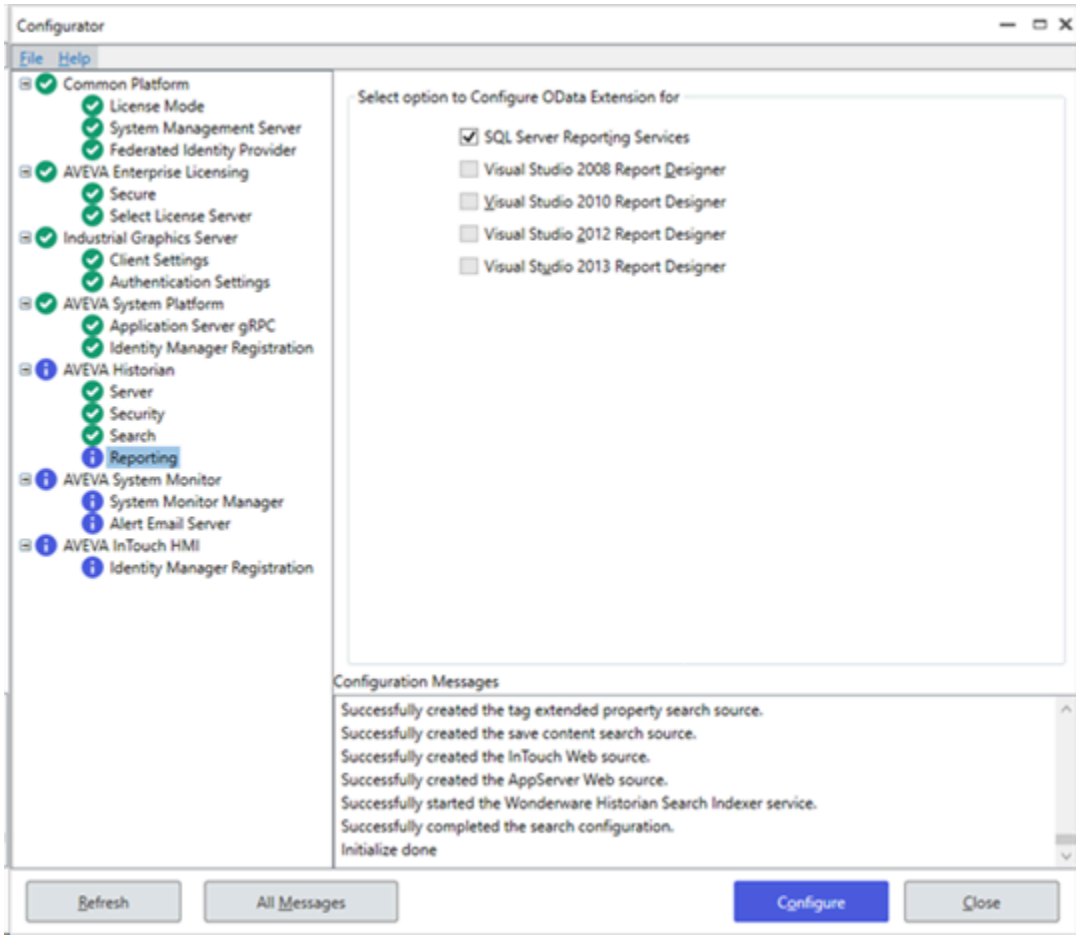
2. Under **Search Configuration**, specify file locations:
   - **Data Path**
     Accept the default path, or select the ellipsis button to specify a different directory for the historian history blocks.

     Make sure that you have plenty of space on this drive most of your plant data will be stored here. (The SQL Server database files typically take less disk space.)
   - **Log Path**
     Accept the default path, or select the ellipsis button to specify a different directory for the log files.
   - Mark the **Reindex Search Documents** check box to create a new index of all existing tags.

Reporting

To configure Reporting settings

1. On the left navigation pane, expand **AVEVA Historian**, and select **Reporting**.



2. Select the appropriate check boxes to configure OData extensions for SQL Reporting Services or Visual Studio Report Designer on your system.
3. Select **Configure**.

   The **Processing SQL Script** dialog box appears. You can see the historian database configuration scripts running. Multiple scripts run during the configuration.
4. After the system finishes running the SQL scripts, the **AVEVA Historian** node and Historian **Server** node are shown with a green status indicator if the database is successfully configured.
5. Select **All Messages** to see all the configuration messages.
6. Select the next item in the left pane that requires configuration. When all required items have been configured, select **Close** to complete installation.

Configure AVEVA Enterprise Licensing

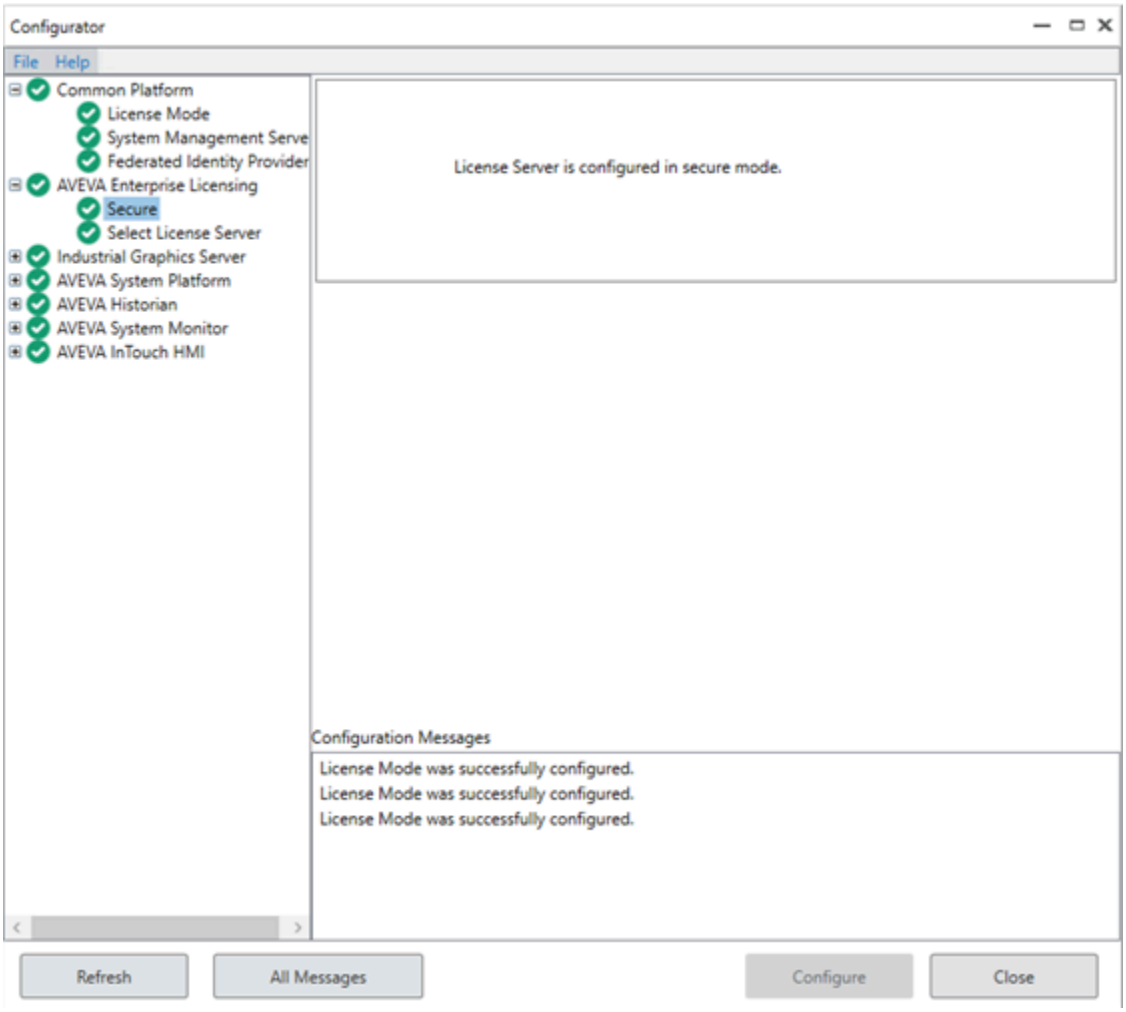
There are two configuration items for the **AVEVA Enterprise Licensing**:

- **Secure**
- **Select License Server**

Secure

To configure License Sever in secure mode

1. On the left navigation pane, expand **AVEVA Enterprise Licensing** , and select **Secure**.
   The configuration screen appears.

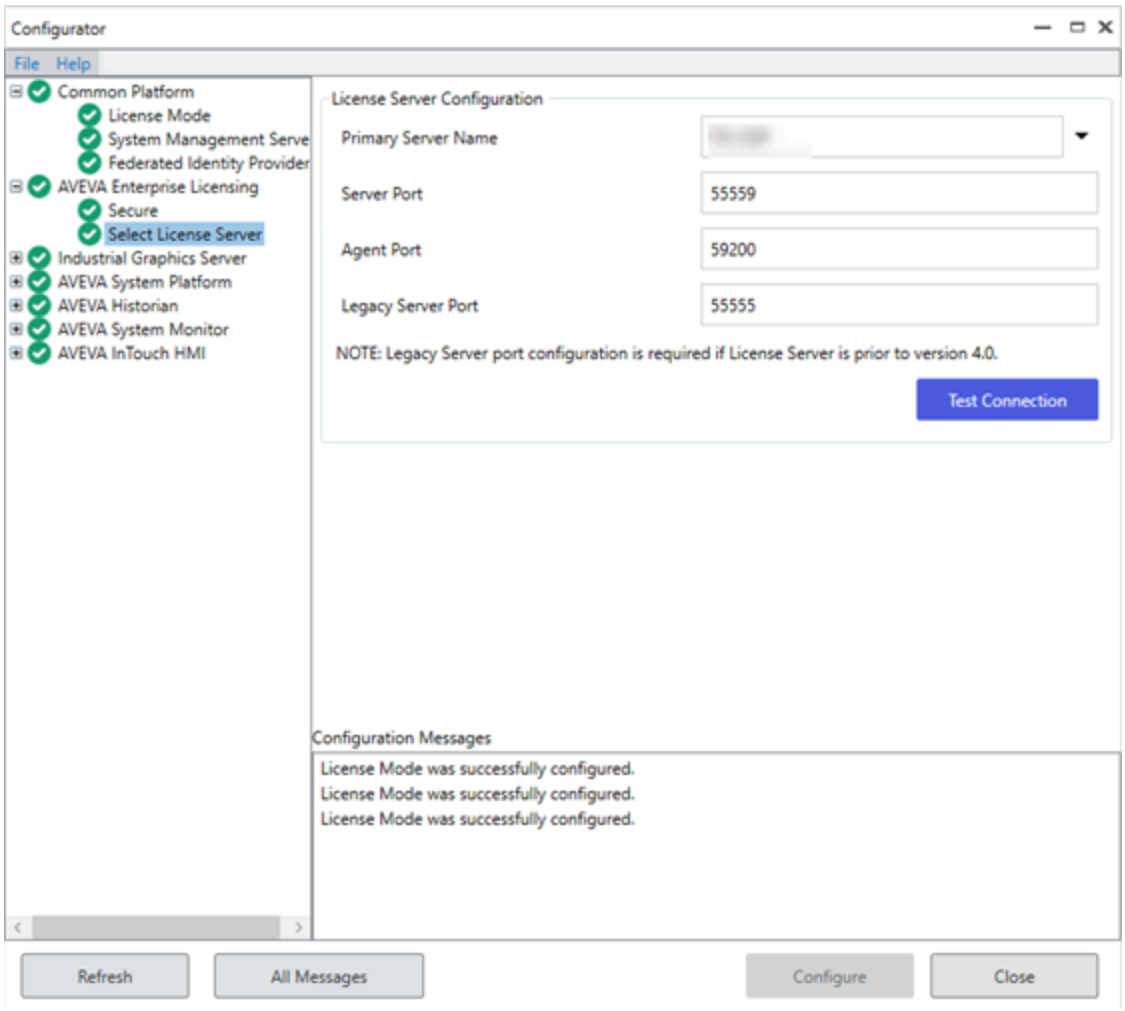


2. Select **Configure**.
   License Server is successfully configured in secure mode.

Select License Sever

To configure AVEVA Enterprise Licensing

1. In the left navigation pane, expand **AVEVA Enterprise Licensing** , and select **Select License Server**.



Then, in the right pane enter:

- **Primary Server Name**: if the License Server is not installed on the local node, enter the License Server name, or select a server name from the drop down list of previously-configured License Servers (if any).

  Note: This is the IP address/machine name of the server that hosts the relevant licenses.

- **Server Port**: Enter the server port number. The default port number is 55559.
- **Agent Port**: Enter the license server agent port number. The default port number is 59200 (for WCF communication) or 59201 (for gRPC communication).
- **Legacy Server Port**: Enter the legacy license server port number. The default port number is 55555.

  Note: Legacy Server Port configuration is required if License Server is prior to version 4.0

2. Select **Test Connection** to verify the details are correct.

   If the connection test succeeds, go to step 3.

   If the test fails,messages indicating errors are highlighted in the **Configuration Messages** box. Verify your information and repeat the test.

3. Select **Configure**.

   The license(s) are released from the host machine.

Note: You can configure the License server even when the specified primary server is unavailable

Configure AVEVA System Monitor

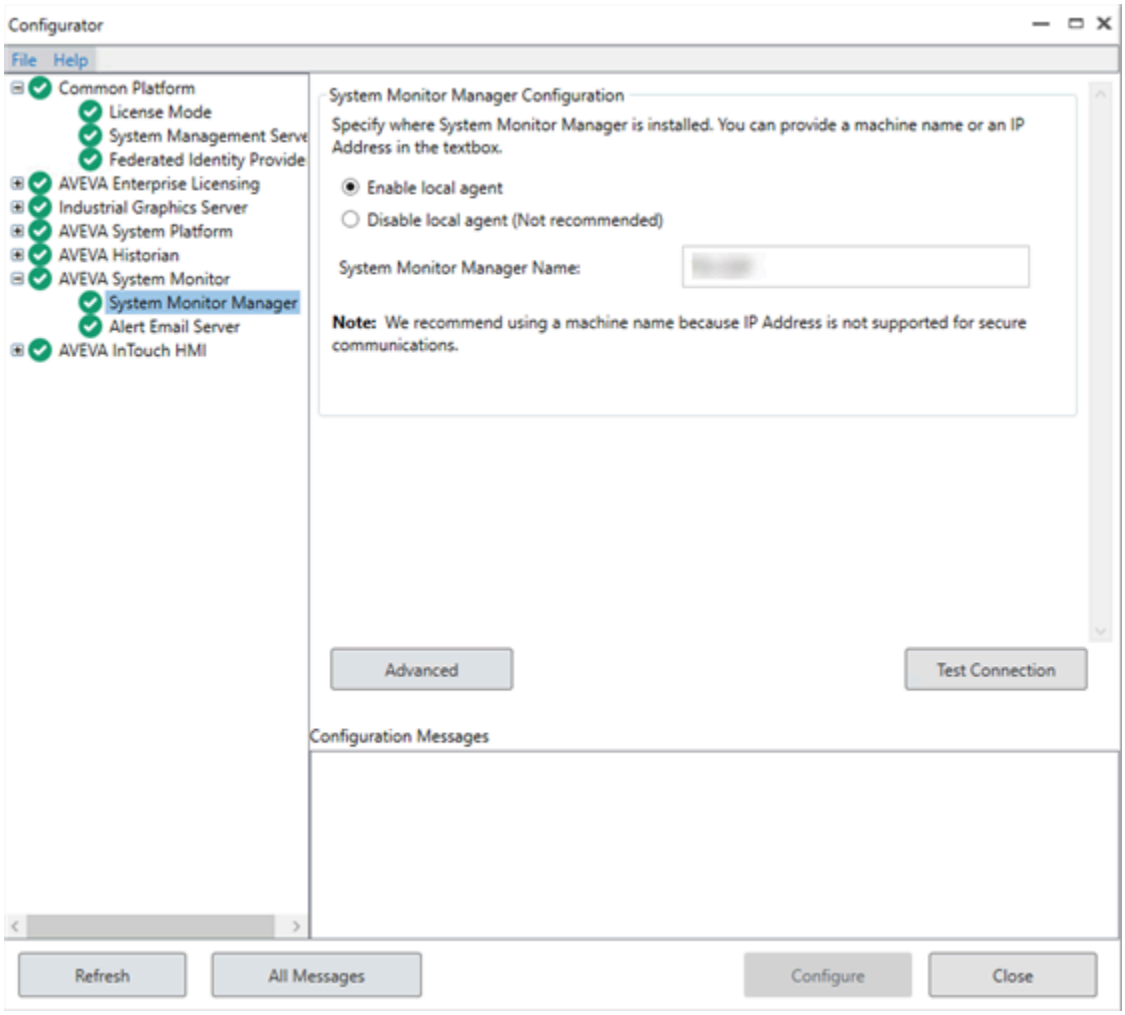
There are two configuration items for the **AVEVA System Monitor:**

- **System Monitor Manager:** It specifies where **System Monitor Manager** is installed. You can provide the machine name or the IP address in the **System Monitor Manager Name** field.
- **Alert Email Server:** The name of the email server and accounts that will be used to send and receive alerts from the **System Monitor Manager**. This is configured on the **System Monitor Manager** node only.

System Monitor Manager

To configure System Monitor Manager

1. On the left navigation pane, expand **AVEVA System Monitor**, and select **System Monitor Manager**.



- If the System Platform node does not include Historian or MES, the initial **System Monitor Manager Configuration** window contains a single field for the **System Monitor Manager** name (node name).
- If the System Platform node includes Historian or MES, the initial **System Monitor Manager Configuration** window contains additional fields to define credentials for MES and/or the Historian.

2. In the **System Monitor Manager Name** field, enter either the computer name (preferred) or IP address of the node that will act as the **System Monitor Manager**. If you are configuring the current node as the **System Monitor Manager**, enter its name or IP address. If you have configured secure communications for the **Common Platform**, the machine name must be used (IP address is not supported for secure communications).

   See the *AVEVA System Monitor User Guide* for additional information.

   Note: TCP/IP is used for communications between **System Monitor Agents** and the **System Monitor Manager**. Use the **Advanced Configuration** dialog to configure the TCP/IP port numbers.

3. Select **Test Connection** to check that the node you are configuring can reach the **System Monitor Manager** node.
4. Select **Configure**.
5. Select the next item in the left pane that requires configuration. When all required items have been configured, select **Close** to complete installation.

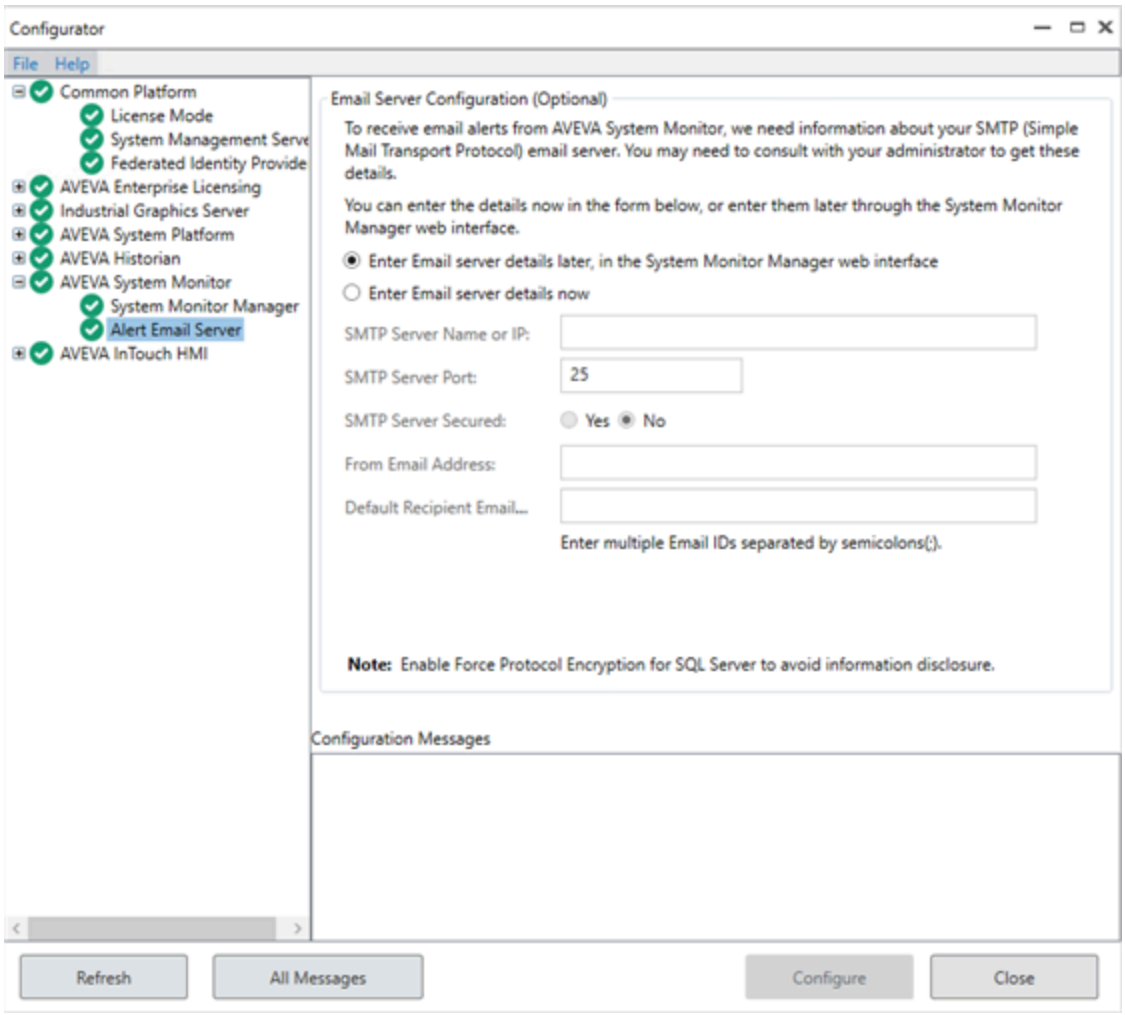
Alert Email Server

Configuring an **Alert Email Server** is optional. This procedure establishes an existing email server that the **System Monitor Manager** can use to send alerts. This is configured on the **System Monitor Manager** node only.

Note: You must have SQL Server sysadmin rights to configure the email server. No warning will be displayed, but without the proper user rights, configuration changes you make to the **Alert Email Server** in the Configurator will not be accepted.

To configure Alert Email Server settings

1. On the left navigation pane, expand **AVEVA System Monitor**, and select **Alert Email Server.**



2. Do one of the following:
   - To skip email server configuration, select **Enter Email server details later, in the System Monitor Manager web interface**.
   - To configure the email server, select **Enter Email server details now**.

   Note: If you configure the option to skip email server configuration and close the Configurator, the option to enter email server details will be disabled if you re-run the Configurator next time. You will need to enter email server details through the **System Monitor Manager** web interface.
3. In the **SMTP Server Name or IP** field, enter either the computer name or IP address of the email server to be used for **System Monitor** alerts.
4. In the **SMTP Server Port** field, enter the port number of the email server (default: **25**).
   - Use port number **25** for an unsecured SMTP server.
   - Use port number **465** for a secured SMTP server.

   See the *AVEVA System Monitor User Guide* for additional configuration information.
5. In the **SMTP Server Secured** field, select **Yes** if the SMTP server is secured. Select **No** if the SMTP server is not secured.
6. If you are using a secured email server, then enter the user name and password to access the server.

   Note: The user name and password field are only applicable to a secured email server.

7. In the **From Email ID** field, enter the email address that will be used to send system alerts from the **System Monitor**.
8. In the **Default Recipient Email ID** field, enter the email address(es) that will receive system alerts from the **System Monitor**.
9. Select **Configure.**
10. Select the next item in the left pane that requires configuration. When all required items have been configured, select **Close** to complete installation

Configure AVEVA InTouch HMI

There is a single configuration item for the **AVEVA InTouch HMI**:

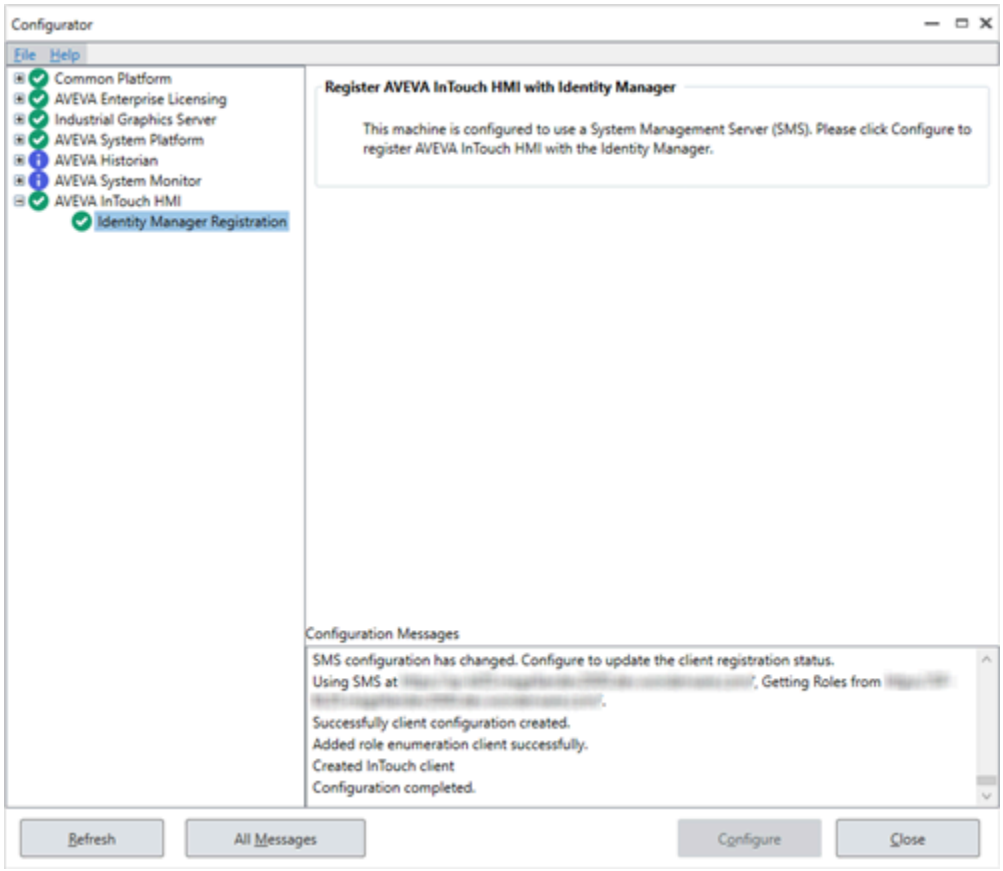
- **Identity Manager Registration**

Identity Manager Registration

Note: Anytime the SMS configuration is changed, you must re-register the Identity Manager.

To configure Identity Manager Registration

1. On the left navigation pane, expand **AVEVA InTouch HMI**, and select **Identity Manager Registration**.



The **Identity Manager Registration** tab allows you to register InTouch products with AVEVA Identity Manager

authentication service.

Note: Client registration of WindowMaker and WindowViewer with AVEVA Identity Manager is required for connected experience mode. When the below requirements are met, the **Configure** button will be enabled:

- In the **System Management Server** of the Configurator, **This machine is the System Management Server** is selected, or connected to an existing System Management Server. InTouch Client registration is not configurable if **No System Management Server configured** is selected in the System Management Server.
- AVEVA Identity Manager service is configured to federate user authentication with AVEVA Connect.

2. Select **Configure** to register InTouch products with AVEVA Identity Manager authentication service.

   The **Configure** button will be disabled if InTouch registration is already configured on that node.

Configure AVEVA System Platform

Important! A single System Management Server (SMS) should be configured for your System Platform environment. The SMS is required to support Application Server redundancy and Multi-Galaxy Communication.

There are two configuration items for the **AVEVA System Platform:**

- **Application Server gRPC**
- **Identity Manager Registration**

Application Server gRPC

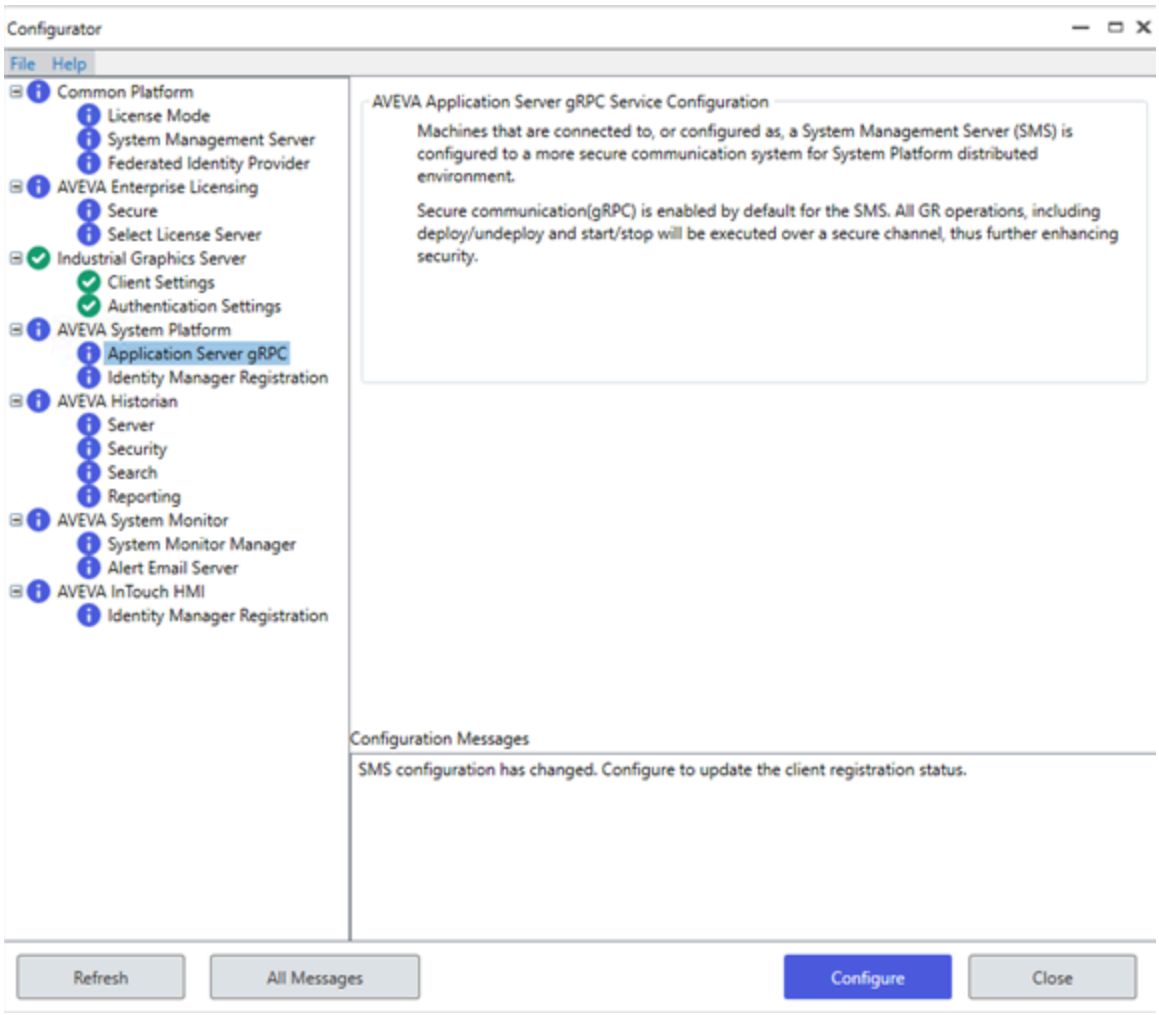
Machines that are connected to, or configured as, a System Management Server (SMS) can be configured to a more secure communication system for our distributed environment.

gRPC is automatically enabled when you click the **Configure** button. This causes all GR operations, including deploy/undeploy and start/stop to be executed over a secure channel, thus further enhancing the security. With this setting enabled, communications use the more secure gRPC protocol instead of DCOM. gRPC should always remain enabled.

Note: Anytime the SMS configuration is changed, you must reconfigure the gRPC plugin.

To configure Application Server gRPC service

1. On the left navigation pane, expand **AVEVA System Platform**, and select **Application Server gRPC.**



2. Click **Configure** to automatically to enable gRPC for Application Server.

Identity Manager Registration

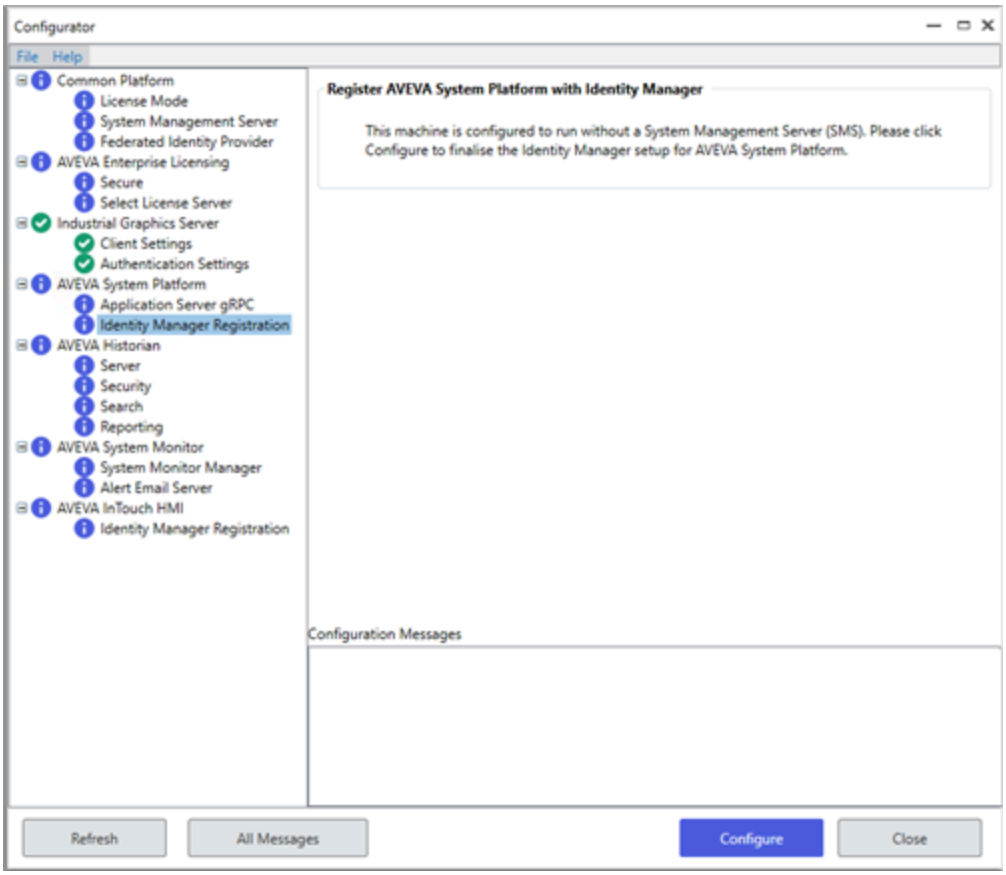
The AVEVA Identity Manager (AIM) is a standalone authentication server that exposes an OpenID Connect endpoint. The System Management Server must be configured before using AIM; this is typically done during product installation via the Configurator, but can also be done by running the Configurator application as a standalone.

Note: Anytime the SMS configuration is changed, you must re-register the Identity Manager.

AVEVA Identity Manager (AIM) registration is required to use Azure AD or AVEVA Connect. This registers your licensed product name with local identity management to allow federation to Azure AD and AVEVA Connect.

Note: When you open an existing galaxy in the IDE that has the security mode set to Authentication providers (using Azure AD), you must set the security mode to “None” (when in non-connected mode), prior to opening the galaxy in connected experience mode.

Select **Configure** to register your licensed product with AIM.



Operations Control connected experience - product co-existence

If you configure your system to use AVEVA Operations Control connected experience, the Federated Identity Provider configurator plugin must be configured to use CONNECT

However, a subset of AVEVA products that interoperate with System Platform use AVEVA Identity Manager but don’t support using CONNECT as a federated identity provider. Other products, such as AVEVA Industrial Application Server and Operations Management Interface (OMI), support CONNECT as a federated identity provider through AVEVA Identity Manager outside of connected experience.

Different product suites that function with the Operations Control common infrastructure including AVEVA Manufacturing Execution System (MES) add ons are not enabled to operate with connected experience in the System Platform 2023 R2 version - the first iteration of connected experience.

A system can contain only one System Management Server. This means that if you want to use these products with System Platform 2023 R2, you cannot use connected experience mode.

Individual products provide alternative settings such as:

- Using an embedded browser pop-up authentication method in the System Management Server configuration.
- Installing a non-participating product on a separate node with its own System Management Server.

Product co-existence will evolve in future releases.

AVEVA Group plc
High Cross
Madingley Road
Cambridge
CB3 0HB
UK

Tel +44 (0)1223 556655

www.aveva.com
To find your local AVEVA office, visit **www.aveva.com/offices**