# AVEVA

AVEVA™ System Platform
formerly Wonderware

Installation Guide

Version 2020 R2 SP1

Publication date: Wednesday, October 20, 2021

# Contact Information

AVEVA Group plc
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.

# Contents

## Chapter 8   AVEVA Historian Server Installation and Configuration. . . . . . . . . . . . . .  136

## Chapter 9   AVEVA Historian Client Information. . . . . . . . . . . . . . . . . . . . . . . . . . . .  148

## Chapter 10   AVEVA Historian Client Installation and Configuration. . . . . . . . . . . . . .  150

## Appendix A   Using Silent Installation. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .  153

# Preparing for System Platform Installation

This guide describes how to install the AVEVA™ System Platform, formerly Wonderware.

You can use the System Platform installation program to install the entire suite of products, or any of the component products.

Before you begin the installation program, you need to prepare your system, and you should plan your installation according to the two installation types available to you, product-based and role-based. See Selecting a Type of Installation for additional information.

Make sure that your computer meets or exceeds the hardware and software requirements. System Platform 2020 R2 SP1 is not supported on 32-bit operating systems or 32-bit versions of SQL Server. If the installed SQL Server version is not compatible for any reason, installation stops and an error message is displayed. For more information, see Unsupported SQL Server Version Error Message.

## Important Notice: Windows Updates

**Before installing System Platform, download and install the latest Microsoft updates** to enhance security and ensure product compatibility. Allow the Windows update process to finish before you start installing System Platform. This recommendation applies to all Windows versions.

## Important Notice for for Highly Secured Environments (TLS 1.2 Exclusively)

**Affected Systems**

This information is applicable to a small subset of highly secured environments, in which operating systems and supporting networks have been configured to enable TLS 1.2 and where TLS 1.0 and 1.1 have been purposefully disabled. In these rare instances, some additional configuration is required to ensure that System Platform will work as expected.

System Platform 2020 R2 SP1 includes various measures to strengthen security, including the ability to leverage the latest version of transport layer security (TLS 1.2), provided that TLS 1.2 has been enabled and configured in the host operating system.

As of the System Platform 2020 R2 SP1 release date, Microsoft Windows Server 2016 does not support TLS 1.2 by default. You must enable it by applying Microsoft updates and several manual edits to the system registry. The

tasks of applying all Microsoft updates and editing the system registry must be completed **before** you install System Platform 2020 R2 SP1. These instructions also apply to any other software products that support TLS 1.2. Follow the instructions listed below.

**If you are required to enable TLS 1.2 and disable TLS 1.0 and TLS 1.1:**

1. Before installing System Platform 2020 R2 SP1 on a Windows Server 2016 computer, make sure that your computer is up to date by downloading and installing all applicable Microsoft updates.

2. If required by the updates, restart your computer.

3. Edit the system registry. The .REG file shown below sets registry keys to their safest values.
   For additional information about these registry changes, see https://docs.microsoft.com/en-us/dotnet/framework/network-programming/tls#configuring-security-via-the-windows-registry.

   ```
   Windows Registry Editor Version 5.00

   [HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\.NETFramework\v4.0.30319]

   "SystemDefaultTlsVersions"=dword:00000001

   "SchUseStrongCrypto"=dword:00000001

   [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319]

   "SystemDefaultTlsVersions"=dword:00000001

   "SchUseStrongCrypto"=dword:00000001
   ```

4. Restart your computer to ensure that all changes take effect.

5. Install System Platform 2020 R2 SP1.

# License Installation and Activation

A valid product license is required to enable product functionality. The AVEVA Enterprise License Server and Enterprise License Manager are automatically selected when you select Application Server or InTouch, or any role (if you select About Role-Based Installation) that includes the Application Server Galaxy Repository. In some cases, such as when you install a Runtime Client, the Galaxy Repository is installed "silently" (without any notice it is being installed).

While the Application Server Galaxy Repository is selected for installation, you cannot deselect the Enterprise License components. The License Server and License Manager are installed on the Galaxy Repository node by default.

**Note:** If you are using a workgroup, the License Manager and License Server must be installed on the same node.

You will need to configure the License Server and activate your product licenses before using the products you install. For detailed information about product licensing and activation, refer to the *AVEVA Enterprise Licensing Guide* (**AELicenseManagerGuide.pdf**). You can access it after installation is complete from the AVEVA Enterprise License Manager node, under the **AVEVA start directory**.

**AVEVA Enterprise Licensing**

The AVEVA Enterprise License Server acquires, stores, and serves licenses for all installed AVEVA software, including all System Platform products. The AVEVA Enterprise License Server and Manager work together to provide centralized management of all your product licenses.

For products and roles that do not install the License Server on the same node, you will have to provide the location (node name) of the License Server.

The basic product installation and license activation workflow is:

1. Install System Products, along with the AVEVA Enterprise License Server and License Manager. See Installing System Platform.

2. Configure the AVEVA Enterprise License Server (and Historian, if installed). See Configuring the AVEVA Enterprise License Server Location.

3. Start the License Manager. The License Manager is browser-based, and is located in the AVEVA folder (Start > AVEVA > Enterprise License Manager). The License Manager uses the following URL: **http://localhost/AELicenseManager**

   **Note:** If you are running the License Manager from a remote node (not the License Server/Galaxy Repository node), substitute the node name for **localhost**.

   The License Manager opens in your browser.

4. If a License Server is displayed, click on it to select it. If no License Servers are displayed, click the **Add Server** button, and then enter the computer name of the License Server, or select the computer name from the drop down.
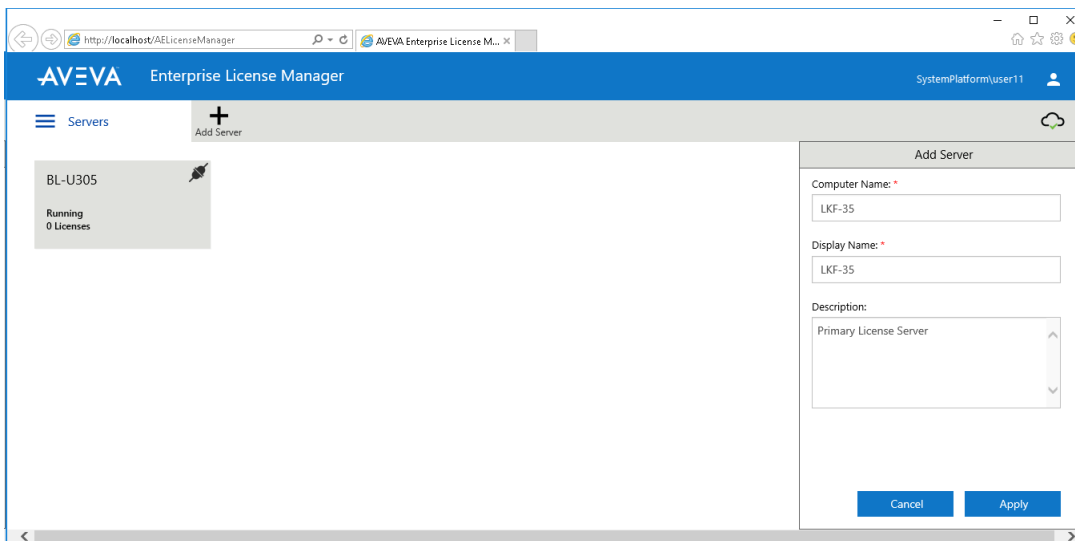


5. Refer to the *AVEVA Enterprise Licensing Help* for options and procedures to activate licenses.

   **Note:** Changes to licensing, such as switching license servers or activating a new license, should not be done for a product that is already running. Depending on the product, it may take up to 30 minutes to acquire a new or changed license. To immediately acquire a license, restart the affected product. However, product interdependencies may require you to restart the node to force the immediate acquisition of the license.

# AVEVA System Monitor Installation

The AVEVA System Monitor constantly checks the License Server to ensure that it is accessible. In the event that the software on a node is unable to acquire a license, the System Monitor sends a warning so you can quickly fix licensing acquisition issues to ensure that operations are not interrupted.

The AVEVA System Monitor consists of the following components:

- **System Monitor Agent:** The System Monitor Agent maintains the manifest of user-defined rules, handles monitoring of the machine to detect unhealthy conditions, and securely communicates with the System Monitor Manager to report those conditions. The System Monitor Agent is installed by the System Monitor Agent Install Manager on every System Platform node, including the System Monitor Manager node. The System Monitor Agent communicates with the System Monitor to monitor the license acquisition from the node to the license server.

- **System Monitor Manager:** The System Monitor is automatically selected for installation whenever the Galaxy Repository feature is selected. Note that you can use the Customize Installation option to deselect the System Monitor, and then select for installation on a different node. The System Monitor also has an SMTP server that can send email notifications if a process it is monitoring requires attention.

For each System Platform node, configuration of the System Monitor is required after installation. The System Monitor Agent on each System Platform node must be configured to point to the System Monitor node. The System Monitor node must be configured to point to itself (the System Monitor Manager Name is the node name). The System Monitor Manager node also requires configuration of its SMTP server and email addresses for notifications. See Advanced System Monitor Configuration for additional information.

In addition to the license monitoring functionality that the System Monitor provides by default, your System Platform licenses include the ability to configure System Monitor on a single node to monitor and manage the performance and availability of the core AVEVA software, the engineered software application(s), and the related hardware and network infrastructure. To configure this additional functionality, see the *AVEVA System Monitor User Guide*.

---

**Important:** If you have a System Monitor license and are running a full version of SQL Server (not Express), you can configure System Monitor Reports. This feature is only available for fully-licensed System Monitor installations, not basic mode, and is not available if you are running SQL Server Express. If your System Monitor installation will be fully licensed, the SQL Server Reporting Services (SSRS) server should be configured and the services started before initiating installation of the System Monitor Manager. This will enable deployment of System Monitor Reports. If SSRS is not configured before installation of the System Monitor Manager, reports will have to be manually deployed. See the *AVEVA System Monitor User Guide* for additional information.

---

# Supported Operating Systems for System Platform 2020 R2 SP1

**Important! System Platform 2020 R2 SP1 supports 64-bit operating systems only.**

The following operating systems (64-bit only) were supported at the time of release of System Platform 2020 R2 SP1:

- Windows 8.1 Enterprise, Professional

- Windows 10 1909 SAC Enterprise and IoT Enterprise

- Windows 10 2004 SAC Professional, Enterprise, and IoT Enterprise

- Windows 10 20H1 SAC Professional, Enterprise, and IoT Enterprise

- Windows 10 20H2 SAC Professional, Enterprise, and IoT Enterprise

- Windows 10 LTSB Enterprise, IoT Enterprise 2015 (1507 (RTM)) - with Extended Support

- Windows 10 LTSB Enterprise, IoT Enterprise 2016 (1607)

- Windows 10 LTSC Enterprise, IoT Enterprise 2019 (1809)

- Windows Server 2012 Data Center (Not Standard Edition)

- Windows Server 2012 R2 Standard and Data Center

- Windows Server 2012 R2 Embedded (64-bit) (Full image)

- Windows Server 2016 LTSC Standard and Datacenter

- Windows Server 2019 LTSC (Datacenter, Essentials, Standard)

- Windows Server IoT 2016 LTSC

- Windows Server IoT 2019 LTSC

> **Note:** System Platform 2020 R2 SP1 is not supported on any Windows 10 version prior to version 1909. For Windows 10 Professional, the minimum version is 2004.

## Supported Operating Systems for InTouch Access Anywhere Server and Secure Gateway

The following operating systems (64-bit only) were supported at the time of release of System Platform 2020 R2 SP1 for InTouch Access Anywhere server nodes. This includes Secure Gateway and InTouch Access Anywhere Server:

- Windows 8.1 Enterprise, Professional

- Windows 10 1909 SAC Enterprise and IoT Enterprise

- Windows 10 2004 SAC Professional, Enterprise, and IoT Enterprise

- Windows 10 20H1 SAC Professional, Enterprise, and IoT Enterprise

- Windows 10 20H2 SAC Professional, Enterprise, and IoT Enterprise

- Windows 10 LTSB Enterprise, IoT Enterprise 2015 (1507 (RTM)) - with Extended Support

- Windows 10 LTSB Enterprise, IoT Enterprise 2016 (1607)

- Windows 10 LTSC Enterprise, IoT Enterprise 2019 (1809)

- Windows Server 2012 Data Center (Not Standard Edition)

- Windows Server 2012 R2 Standard and Data Center

- Windows Server 2016 LTSC Standard and Datacenter

- Windows Server 2019 LTSC (Datacenter, Essentials, Standard)

- Windows Server IoT 2016 LTSC

- Windows Server IoT 2019 LTSC

## Supported InTouch Access Anywhere Clients

InTouch Access Anywhere can run in any HTML5-capable browser, including but not limited to:

- Google Chrome version 72.0.3626 and newer

- Firefox version 60.9 ESR and newer

- Microsoft Edge version 40.15063 and newer

- Safari version 11 and newer (Mac and iOS only, not Windows)

- Opera version 50 (2018) and newer

# System Sizing Guidelines

The following table provides guidelines for hardware configurations suitable for System Platform 2020 R2 SP1, based on application size. These guidelines are subject to the limitations of your Windows operating system, and if applicable, to the SQL Server edition (Express, Standard, or Enterprise). See the Technology Matrix on the AVEVA Global Customer Support website for supported versions of Windows operating systems and SQL Server.

- The Intel Itanium 2 processor is not supported.

- An HD display is recommended for engineering tools such as the Integrated Development Environment (IDE).

- A Windows Server operating system is required for large installations.

- A 64-bit operating system is required, regardless of system size.

- SQL Server Express is not supported for installations with more than 25,000 I/O per node (small installations only).

- Pagefile.sys, the Windows paging file (also called the swap file or virtual memory file), must be enabled. The Windows default setting is enabled.

The following guidelines are provided for reference only. The system configuration required for your application will depend on multiple factors, including but not limited to the size and complexity of the application, and the features and components used.

| Application | Level | Logical Processors | RAM | Free Disk Space | Network Speed |
|---|---|---|---|---|---|
| **Application Server Nodes** | | | | | |
| **Small Application** (1 - 25,000 I/O per Node) | Minimum | 4 | 2 GB | 100 GB | 100 Mbps |
| | Recommended | 8 | 4 GB | 200 GB | 1 Gbps |
| **Medium Application** (25,000- 50,000 I/O per Node) | Minimum | 8 | 8 GB | 200 GB | 1 Gbps |
| | Recommended | 16 | 12 GB | 500 GB | 1 Gbps |
| **Large Application** (> 50,000 I/O per Node) | Minimum | 16 | 16 GB | 500 GB | 1 Gbps |
| | Recommended | 32 | 24 GB | 1 TB | Dual 1 Gbps |
| **Galaxy Repository Nodes** | | | | | |
| **Small Galaxy** (1 - 50,000 I/O per Node) | Minimum | 4 | 2 GB | 100 GB | 100 Mbps |
| | Recommended | 8 | 4 GB | 200 GB | 1 Gbps |
| **Medium Galaxy** (50,000 - 200,000 I/O per Node) | Minimum | 8 | 8 GB | 200 GB | 1 Gbps |
| | Recommended | 16 | 12 GB | 500 GB | 1 Gbps |
| **Large Galaxy** (> 200,000 I/O per Node) | Minimum | 16 | 16 GB | 500 GB | 1 Gbps |
| | Recommended | 32 | 24 GB | 1 TB | Dual 1 Gbps |

| Application | Level | Logical Processors | RAM | Free Disk Space | Network Speed |
|---|---|---|---|---|---|
| **Historian Server Nodes** | | | | | |
| **Small Historian** (1 - 50,000 Historized Tags per Node) | Minimum | 4 | 2 GB | 100 GB | 100 Mbps |
| | Recommended | 8 | 4 GB | 200 GB | 1 Gbps |
| **Medium Application** (50,000 - 200,000 Historized Tags per Node) | Minimum | 8 | 8 GB | 200 GB | 1 Gbps |
| | Recommended | 16 | 12 GB | 500 GB | 1 Gbps |
| **Large Application** (> 200,000 Historized Tags per Node) | Minimum | 16 | 16 GB | 500 GB | 1 Gbps |
| | Recommended | 32 | 24 GB | 1 TB | Dual 1 Gbps |
| **Thin Client Nodes** | | | | | |
| RDP clients, ITAA browsers, mobile devices | Minimum | 2 | 512 MB | N/A | 100 Mbps |
| | Recommended | 4 | 2 GB | N/A | 100 Mbps |
| **Client Nodes** | | | | | |
| WindowViewer, ViewApp, Historian Client, Remote IDE | Minimum | 4 | 1 GB | 100 GB | 100 Mbps |
| | Recommended | 8 | 4 GB | 200 GB | 1 Gbps |
| **Remote Desktop Server Nodes** | | | | | |
| Basic RDS, ITAA Server Supports up to 15 concurrent remote sessions | Minimum | 8 | 8 GB | 200 GB | 1 Gbps |
| | Recommended | 16 | 12 GB | 500 GB | 1 Gbps |
| Large RDS, ITAA Server Supports up to 30 concurrent remote sessions | Minimum | 16 | 16 GB | 500 GB | 1 Gbps |
| | Recommended | 32 | 24 GB | 1 TB | Dual 1 Gbps |
| **All-In-One Nodes** (all products on a single node) | | | | | |
| Small Application: 1,000 I/O max | Minimum | 8 | 8 GB | 200 GB | 100 Mbps |
| | Recommended | 12 | 12 GB | 500 GB | 1 Gbps |
| Medium Application: 20,000 I/O max | Minimum | 12 | 16 GB | 500 GB | 1 Gpbs |
| | Recommended | 16 | 32 GB | 1 TB | 1 Gbps |
| Large Application 100,000 I/O max | Minimum | 20 | 32 GB | 2 TB | 1Gbps |
| | Recommended | 24 | 64 GB | 4 TB | 1 Gbps |

1) To calculate the number of logical processors: multiply the number of physical cores by the number of threads each core can run. A four core CPU that runs two threads per core provides eight logical processors. The terms "Hyper-Threading and "simultaneous multithreading" (SMT) are also used to describe logical processors.
2) SSD drives are highly recommended.
3) In redundant environments, increase CPU and RAM to maintain a maximum of 40% typical resource utilization.
4) For optimal performance of all-in-one nodes, a high clock speed (>2.8 GHz) is recommended.
5) For Application Server platform nodes, it is recommended that you deploy no more than two AppEngines per logical processor (typically one primary AppEngine and one backup).
6) For large applications on all-in-one nodes, dual XEON processors are recommended.

# Supported and Recommended Node Hardware Types

| Product | Server Node | Thin Client-Server Node | Client Node | Thin Client | All-In-One |
|---|---|---|---|---|---|
| Application Server | | | | | |
| Galaxy Repository | Preferred | Supported | Supported | No | Supported |
| Application Engine | Preferred | Supported | Supported | No | Supported |
| IDE | Preferred | Supported | Supported | RDP | Supported |
| AVEVA OMI ViewApp Runtime | Supported | Supported | Preferred | ITAA/RDP | Supported |
| InTouch Standalone | | | | | |
| WindowMaker (No Modern Apps) | Supported | Supported | Preferred | RDP | Supported |
| WindowMaker (with Modern Apps) | Preferred | Supported | Supported | RDP | Supported |
| WindowViewer / InTouch ViewApp (runtime only) | Supported | Supported | Preferred | ITAA/RDP | Supported |
| InTouch for System Platform | | | | | |
| WindowMaker (with Managed Apps) | Preferred | Supported | Supported | RDP | Supported |
| WindowViewer / InTouch ViewApp (runtime only) | Supported | Supported | Preferred | ITAA/RDP | Supported |
| InTouch Access Anywhere | | | | | |
| InTouch Access Anywhere Server | Supported | Preferred | No | No | Supported |
| InTouch Access Anywhere Client (HTML5 Browser) | Browser | Browser | Browser | Browser | Browser |
| InTouch Access Anywhere Secure Gateway | Supported | No | No | No | No |
| Historian | | | | | |
| Historian Server | Preferred | Supported | Supported | No | Supported |
| AVEVA Insight | Browser | Browser | Browser | Browser | Browser |
| Historian Client | Supported | Supported | Preferred | RDP | Supported |
| Support Components | | | | | |
| OI Gateway | Preferred | Supported | Supported | No | Supported |
| AVEVA Enterprise License Server | Preferred | Supported | Supported | No | Supported |
| AVEVA Enterprise License Manager | Preferred | Supported | Supported | No | Supported |
| AVEVA Enterprise License Manager Client | Browser | Browser | Browser | Browser | Browser |

# Required Installation Order of Additional Products

Some AVEVA products released prior to System Platform 2020 R2 SP1 must be installed before you install System Platform. These are:

- Alarm Adviser (2014 R2 SP1 and prior versions)

- Intelligence (2017 SP1 and prior versions)

- Recipe Manager Plus (2017 Update 1 and prior versions)

- Skelta BPM (2017 R2 Update 1 and prior versions)

If any of the above products will be installed on the same system as System Platform 2020 R2 SP1:

1. Install the product (Alarm Adviser, Intelligence, etc.) first.

2. Then, install System Platform 2020 R2 SP1.

InBatch 2017 or prior versions must installed **after** installing System Platform 2020 R2 SP1.

1. Install System Platform 2020 R2 SP1.

2. Then, install InBatch.

# Common Components

System Platform 2020 R2 SP1 includes several shared modules that are needed for the products to operate. You will see some or all of the following common components listed under **Programs and Features** in the Windows **Control Panel** after installation is complete, depending on your installation selections for the node:

| Component | Version | Required/ Optional |
|---|---|---|
| AVEVA Communication Drivers Pack 2020 R2 | 7.2.000 | Required |
| Platform Common Services 4.6.2 | 4.6.21215.1 | Required |
| AVEVA Enterprise License Manager | 3.7.00000 | Required |
| AVEVA Enterprise License Server | 3.7.00002 | Optional (see note) |
| AVEVA Enterprise Licensing Platform | 3.7.00002 | Required |
| System Monitor Agent Install Manager | 1.4.0 | Required |
| System Monitor Manager | 1.4.0 | Optional |

**Note:** The License Server is required on nodes with the Galaxy Repository.

# Windows Network Configuration

If you are installing System Platform products on more than one node, we recommend that you use domain based networking. Domain based (client-server) networks provide better user account security and management than workgroup based (peer to peer) networks.

System Platform does not support mixed Windows workgroup/domain environments. While workgroups are supported, you cannot use workgroup nodes within a domain environment.

**Note:** Do not install the Galaxy Repository on a computer that is used as a domain controller or an Active Directory server.

Operations that rely on inter-node communications may not function correctly in a workgroup based Application Server installation. Examples of this type operation include connecting to a remote IDE, or viewing the status of a remote platform.

If you must use workgroup based networking, you can avoid communications issues by enabling "everyone permissions" for anonymous users. To enable these permissions, go to:

```
Local Security Policy > Local Policies > Security Options > Network Access: Let everyone
permissions apply to anonymous.
```

# Web Help Display and Video Playback

**Web Help - Browser-based User Assistance**

Web help components have been delivered in this release. Web help opens in the default browser on your local computer. Help displayed in a browser allows more dynamic and searchable user assistance including standard web browser navigation and tutorial videos.

Typically, help content is installed on your local machine as part of the documentation library, and displays in your browser without requiring an Internet connection. When you install the Application Server IDE, a link to the AVEVA OMI Web Help is added to the Windows start menu. To open the help, use one of the following methods (depending on the editor/UI you are using):

- Press F1 from the ViewApp editor, Screen Profile editor, or Layout editor.

- From the System Platform IDE, select a Layout, ViewApp, Screen Profile, AVEVA OMI app, or External Content object and:

  - press Ctrl+F1, or

  - right-click, then select Help from the short-cut menu.

- To open AVEVA OMI help from its installed location:

  C:\Program Files (x86)\ArchestrA\Framework\Docs\1033\NGX\index.htm

- To open AVEVA OMI help from the start menu, go to:

  Start > AVEVA Documentation > AVEVA OMI Help

**Browser Requirements and Recommendations**

Internet Explorer is recommended.

- Microsoft Edge will not load help content, unless you use the "Open with Internet Explorer" option in the Edge browser.

- Chrome and Chromium-based browsers, such as Vivaldi, will not load help content unless you install and use an IE-rendering extension (for example, IE Tab).

### Browser Permissions for Displaying Web Help

Each browser and Windows operating system combination has its own security permissions. Using Internet Explorer as an example, you may see a dialog requesting that you "Allow blocked content" each time you invoke the web help. This dialog is triggered by the presence in the help system of JavaScript components that control internal navigation and topic display elements such as pop-up or in-place-expanding display blocks that contain text and graphical images. The text and image content is itself non-active.

You can accept each occurrence of this dialog, or you can set the following option in Internet Explorer, depending on your IT security requirements: In Internet Options, click the Advanced tab, then navigate to the Security section. Enable the "Allow active content to run in files on My Computer." Permissions and security settings will vary depending on your specific browser.

### Playback of Tutorial Videos

The web help may contain a number of brief tutorial videos. To play these videos, you must have Microsoft Media Player installed on your local machine. In Windows Server operating systems, you must enable the "Desktop Experience" feature using Server Manager.

Internet Explorer (or IE-rendering in other browsers) may be required for viewing video content. If using a browser other than Internet Explorer without IE rendering enabled, videos may not be visible.

## System Platform Prerequisites

### Operating System and SQL Server

A 64-bit Windows operating system is required for installing and running System Platform 2020 R2 SP1 and its component products. Some System Platform 2020 R2 SP1 components, such as the Application Server Galaxy Repository and the AVEVA Historian, formerly Wonderware, also require a 64-bit version of Microsoft SQL.

Check the [AVEVA GCS Technology Matrix](#) website for more information about supported Windows and SQL Server versions for the System Platform 2020 R2 SP1 component products you are installing.

**Note:** If you are using silent (command line) installation, all prerequisites, including the .NET Framework and SQL Server, **must** be installed before launching the System Platform setup program. See [Using Silent Installation](#) for more information.

### .NET Framework

- System Platform requires **Microsoft .NET® Framework 4.8**. Prior to any other installation task, System Platform checks if .NET version 4.8 is installed. If it is not, you are prompted to allow its installation. A system restart may be required when .NET installation is complete. If the System Platform installation program does not automatically resume after the system restart, you will need to restart it manually.
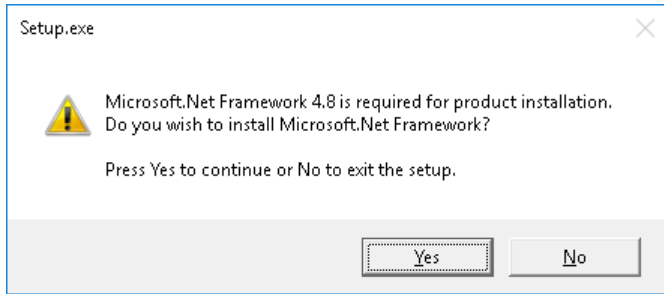
- If an error occurs during setup that stops .NET Framework 4.8 installation, you can try manually installing from the System Platform installation DVD:

  **\InstallFiles\Redist\DOTNET\4.8\NDP48-x86-x64-AllOS-ENU.exe**

**To check installed .NET versions:**

Open a command prompt and enter
**cmd /k reg query "HKLM\SOFTWARE\Microsoft\NET Framework Setup\NDP" /s /v Version**

The installed versions of .NET are listed.

**Prerequisites Automatically Installed by System Platform**

The System Platform installation program analyzes the software installed on your computer and lists any software that is required but not currently installed, and any installed software that is incompatible. The following prerequisites are installed by the System Platform installation program, if not already present on the system:

- **Microsoft .NET® Framework 4.8**

- **SQL Server**: SQL Server is required for products or roles that you select for installation that include GR node or Historian Server. If a supported version of SQL Server is not found, you are given the option to install **SQL Server 2017 Express** as part of System Platform installation. However, SQL Server Express supports only small installations with less than 25,000 I/O per node.
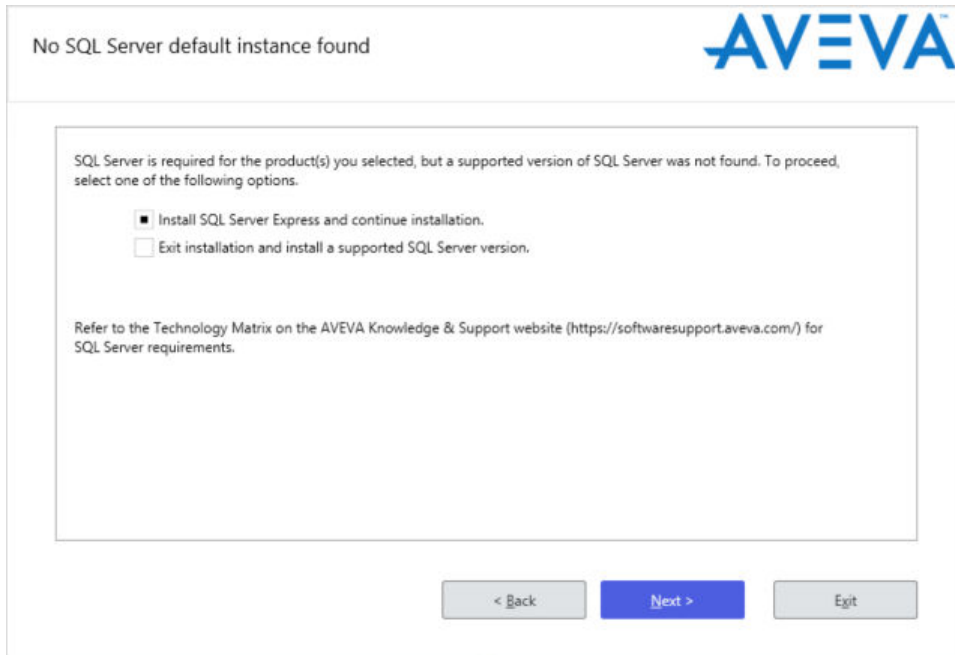
If you have a medium or large installation, a copy of **SQL Server 2017 Standard Edition** is supplied with System Platform. You must install it or another supported version of SQL Server separately, before you install System Platform. See the Technology Matrix on the AVEVA Global Customer Support website for the current list of supported SQL Server versions.

If you do not want to install SQL Server, and you have product or role selections that include the GR node by default, you can select the **Customize Installation** checkbox and deselect the **Galaxy_Repository**. However, this will limit any database-related product functionality, such as the Application Server IDE, that uses the Galaxy Repository.

See SQL Server Requirements for more information about the limitations of using SQL Server Express instead of a standard or enterprise edition.

The following tables summarize which System Platform products and roles require SQL Server.

| Product Selections | SQL Required |
|---|---|
| Application Server | Yes |
| Application Server and AVEVA OMI Runtime | No |
| Application Server Development | No |
| Application Server Galaxy Repository | Yes |
| InTouch HMI | Yes |
| InTouch Development and Runtime | Yes |
| InTouch Runtime Only | No |
| InTouch Access Anywhere Server | No |

| Product Selections | SQL Required |
|---|---|
| InTouch Access Anywhere Secure Gateway | No |
| InTouch Access Anywhere Authentication Server | No |
| Historian | Yes |
| Historian Client | No |
| Licensing | No |
| **Role Selections** | **SQL Required** |
| Runtime Client | No |
| Remote System Platform Development Client | No |
| System Platform Development Server | Yes |
| • Without Galaxy Repository (custom installation) | No |
| Historian Server Node | Yes |
| Historian Client Node | No |
| InTouch Access Anywhere Secure Gateway Node | No |
| All-In-One-Node | Yes |
| • Without Galaxy Repository and Historian Server (custom installation) | No |

**Note:** System Platform will allow you to install an InTouch development system without a Galaxy Repository. However, InTouch Modern Applications will not work without the Galaxy Repository.

While installing System Platform, if the logged-on user (the installer) is not a SQL Server administrator, the **SQL Access Configurator** opens (the dialog box is labeled "**aaConfig SQL**") and requests SQL Server administrator credentials. Enter valid SQL Server administrator credentials when requested. For more information about setting user privileges with the **SQL Access Configurator**, see Setting the SQL Server Security Mode. For more information about SQL Server installation, see About SQL Server Requirements.

The System Platform installation program installs both system-specific and product-specific prerequisites. It also checks for incompatible software that will prevent installation from proceeding, (for example, if InTouch Access Anywhere was previously installed). You do not have to exit from the System Platform installation program to install the prerequisite software, with the exception of standard or enterprise versions of SQL Server. You will need to exit and perform any uninstall operations that are indicated before continuing with installation.

For information on prerequisites and software requirements for the specific products, see the System Platform Readme, the Readme files of the specific products located in your documentation directory, or the specific product information chapter in this installation guide.

## About SQL Server Requirements

The exception to the prerequisites installation workflow is the SQL Server requirement for System Platform products. In most cases, SQL Server is required when you install:

- Application Server
- Historian
- InTouch HMI (when used with modern applications)

If a supported version of SQL Server is not already installed, you must exit the installation program, install the supported SQL Server version, then resume the installation. We recommend that you install and configure the supported SQL Server version before you begin the System Platform installation program.

**Note:** If you are installing a small system (less than 25,000 I/O), you can use SQL Server Express instead of a standard version of SQL Server. You can elect to install SQL Server Express as part of the System Platform installation process; you do not have to install it separately.

For more information about SQL Server prerequisites, see SQL Server Requirements.

## Unsupported SQL Server Version Error Message

If an error message about an unsupported SQL Server version is displayed while installing System Platform, check the following:

- Your installed version of SQL Server is no longer supported, for example, SQL Server 2008.
  - **How to fix:** Upgrade SQL Server to a supported version. Refer to the following Microsoft resource for more information: Upgrade SQL Server.
- Your installed version of SQL Server is supported but requires a service pack. For example, you have SQL Server 2014 but Service Pack 3 is not installed.
  - **How to Fix**: Download and install the required Microsoft SQL Server service pack.
- You have a 32-bit version of SQL Server installed.
  - **How to Fix:** See "*Install/Uninstall and Galaxy Migration Issues*" in the System Platform 2020 R2 SP1 Readme, and refer to Issue 1249251.

# Selecting a Type of Installation

The System Platform installation program offers you a choice of two types of installation— product-based or role-based.

## About Product-Based Installation

Product-based installation provides a combination of features not specific to a node. This is the preferred installation type for a stand-alone product installation.

If you are familiar with System Platform products and their associated components, you can opt for a product-based installation, and then choose the components that you need. For example if you need to install InTouch® with the default options, then select a product-based installation.

**Important:** Product-based installation includes an option to install the InTouch Access Anywhere Secure Gateway. The Secure Gateway can only be installed on a computer running a supported version of the Windows Server operating system (minimum: Windows Server 2012). To ensure security, no other System Platform components should be installed on the node.

In the table below, components that are selected by default when you select the corresponding product are indicated by the letters **R** (for required), and **O** (for optional). Required means that the component must remain selected to install the product. Optional means that you can deselect the component and retain the remaining product functionality. Products definitions (columns 2 through 9) are as follows:

- **AS + GR:** Application Server (with Galaxy Repository)
- **AS no GR:** Application Server (without Galaxy Repository)
- **IT:** InTouch (HMI)
- **ITAA:** InTouch Access Anywhere
- **ITAA SG:** InTouch Access Anywhere Secure Gateway
- **ITAA AS:** InTouch Access Anywhere Authentication Server
- **HS:** Historian Server
- **HC:** Historian Client

| Product / Component | AS + GR | AS w/o GR | IT | ITAA | ITAA SG | ITAA AS | HS | HC |
|---|---|---|---|---|---|---|---|---|
| **System Platform** | R | R | R | R | | | R | |
| • ASB Runtime | R | O | R | | | | O | |
| • ASB Service Repository | | | | | | | | |
| **Application Server** | R | R | R | R | | | | |
| • Bootstrap | O | O | R | | | | | |
| • IDE | O | O | O | | | | | |
| • Galaxy Repository | | | | | | | | |
| Insight Publisher | | | R | R | | | | |

| Product / Component | AS + GR | AS w/o GR | IT | ITAA | ITAA SG | ITAA AS | HS | HC |
|---|---|---|---|---|---|---|---|---|
| **InTouch HMI** | | | R | R | | | | |
| • Runtime | | | O | R | | | | |
| • Development | | | R | R | | | | |
| • Alarm DB Logger | | | O | R | | | | |
| • Demo Apps | | | O | R | | | | |
| • Recipe Manager | | | O | R | | | | |
| • SQL Access | | | O | R | | | | |
| • 16 PenTrend | | | R | | | | | |
| • Symbol Factory | | | R | | | | | |
| • Industrial Graphics Server (InTouch Web Client) | | | | | | | | |
| • OI Gateway | | | | | | | | |
| **InTouch Access Anywhere** | | | | R | R | R | | |
| • ITAA Server | | | | | | | | |
| • ITAA Secure Gateway | | | | | | | | |
| • ITAA Authentication | | | | | | | | |
| **Historian** | | | | | | | R | |
| • Historian Server | | | | | | | R | |
| • IDAS | | | | | | | R | |
| • Active Event | | | | | | | R | |
| • Configuration Tools | | | | | | | R | |
| • Historian Extensions | | | | | | | | |
| **Historian Client** | R | R | R | R | | | | R |
| • Trend/Query Clients | | | | | | | | |
| • Microsoft Add-Ins | | | | | | | | |
| **Licensing** | R | O | R | O | | | | |
| • License Manager | R | O | R | O | | | | |
| • License Server | | | | | | | | |
| Client Components | R | R | R | R | | | | |
| Server Components | R | R | R | R | | | | |
| OI Server Simulator | R | R | R | R | | | | |

| Product / Component | AS + GR | AS w/o GR | IT | ITAA | ITAA SG | ITAA AS | HS | HC |
|---|---|---|---|---|---|---|---|---|
| **System Monitor**<br><br>• System Monitor Manager<br><br>• System Monitor Agent | R<br><br>R | R | R | R | O | O | R | R |

**R** = Required

**O** = Optional

# About Role-Based Installation

Role-based installation provides a combination of features specific to a node. If you are uncertain about the specific products or components you need, but you know what role your computer will play, you can opt for a role-based installation. For example, if your computer is a run-time node or a development node, you can select those roles in the role-based installation program. The System Platform installation program will install all components required for the roles that you have selected. It is recommended that you define the node you are installing and select the appropriate role before starting the installation program. During the installation, you can click a role to see its description, as described in Installing System Platform.

**Important:** Role-based installation includes an option to install an InTouch Access Anywhere Secure Gateway node. The Secure Gateway can only be installed on a computer running a supported version of the Windows Server operating system (minimum: Windows Server 2012). To ensure security, no other System Platform components should be installed on the node.

In the table below, components that are selected by default when you select the corresponding product are indicated by the letters **R** (for required), and **O** (for optional). Required means that the component must remain selected to install the product. Optional means that you can deselect the component and retain the remaining product functionality.

**Note:** In some cases, you can still deselect a product category to remove all components under it, even if components are marked as required. For example, if you are installing a System Platform Development Server, and will be using the AVEVA OMI run time only, you can deselect the InTouch HMI category to remove all the components listed under it, including components that are marked as required. As another example, if you are installing Security Server, it is possible to deselect the ASB Management Server, but the resulting installed product will not result in a Security Server.

Products definitions (columns 2 through 9) are as follows:

- **RT Client:** Runtime Client. Install only the necessary components required to run a visualization client, Historian client, and Application Server server run-time components.

- **Dev Client:** Remote System Development Workstation. Install the components required for a remote engineering development workstation with only the required components to allow the node to connect to an existing development server; GR is not installed by default. It allows development and testing of InTouch and System Platform applications.

- **Dev Servr:** System Platform Development Server. Install the components required to host the development server, and develop and test InTouch and System Platform applications.

- **HS Node:** Historian Server Node. Install the necessary components to store historical data in a System Platform environment.

- **HC Node:** Historian Client Node. Install the components required to connect to an existing Historian Server and analyze the data.

- **ITAA SG:** InTouch Access Anywhere Secure Gateway Node. Install the components to access InTouch applications hosted on Terminal Servers by using HTML5 compatible web browsers. This component cannot be installed on a computer that has other System Platform components installed.

- **Lic Srvr:** License Server. Installs the components required to create a stand-alone license server that installed products on other nodes can access for their licenses.

- **Sys Mtr:** System Monitor Manager . Installs the System Monitor Manager and Agent components. The System Manager monitors the License Server. It also includes a single node license to monitor the health of the computer on which it is installed.

**Note:** The System Monitor Manager is automatically selected for installation whenever the Galaxy Repository component is selected. You use the "Customize Installation" dialog to deselect it. The System Monitor Agent automatically installs on all System Platform nodes. It cannot be deselected and is a required component.

Not Listed: The following roles are not defined in the table below:

- **All-in-One Node:** All products, except InTouch Anywhere, are installed on a single node.

- **Custom:** Allows you to customize the components that are installed. No components are selected by default; you must select any component that you want to install.

| Role | RT Client | Dev Client | Dev Servr | HS Node | HC Node | ITAA SG | Lic Srvr | Snt Mgr |
|---|---|---|---|---|---|---|---|---|
| **System Platform**<br>• ASB Runtime<br>• ASB Service Repository | R | R | R<br>R | R | R | | | |
| **Application Server**<br>• Bootstrap<br>• IDE<br>• Galaxy Repository | R | R<br>R | R<br>R<br>O | O | O | | | |
| Insight Publisher | R | R | R | | | | | |

| Role | RT Client | Dev Client | Dev Servr | HS Node | HC Node | ITAA SG | Lic Srvr | Snt Mgr |
|---|---|---|---|---|---|---|---|---|
| **InTouch HMI** | R | R | R | R | | | | |
| • Runtime | R | O | O | R | | | | |
| • Development | O | R | R | R | | | | |
| • Alarm DB Logger | O | O | O | R | | | | |
| • Demo Apps | O | O | O | R | | | | |
| • Recipe Manager | R | O | O | R | | | | |
| • SQL Access | | O | O | | | | | |
| • 16 PenTrend | | R | R | | | | | |
| • Symbol Factory | | | | | | | | |
| • Industrial Graphics Server (InTouch Web Client) | | | | | | | | |
| **InTouch Access Anywhere** | | | | | | R | | |
| • ITAA Server | | | | | | | | |
| • ITAA Secure Gateway | | | | | | | | |
| • ITAA Authentication | | | | | | | | |
| **Historian** | | | | R | | | | |
| • Historian Server | | | | R | | | | |
| • IDAS | | | | R | | | | |
| • Active Event | | | | R | | | | |
| • Configuration Tools | | | | R | | | | |
| • Historian Extensions | | | | | | | | |
| **Historian Client** | R | R | R | R | R | | | |
| • Trend/Query Clients | | | | | | | | |
| • Microsoft Add-Ins | | | | | | | | |
| **Licensing** | O | O | R | | O | | R | |
| • License Manager | O | O | R | | | | | |
| • License Server | | | | | | | | |

| Role | RT Client | Dev Client | Dev Servr | HS Node | HC Node | ITAA SG | Lic Srvr | Snt Mgr |
|---|---|---|---|---|---|---|---|---|
| **Operation Integration** | R | R | R | R | R | | | |
| • Client Components | R | R | R | R | R | | | |
| • Server Components | R | R | R | R | R | | | |
| • OI Server Simulator | R | R | R | R | | | | |
| • OI Gateway | | | | | | | | |
| **System Monitor** | R | R | R | R | R | R | R | R |
| • System Monitor Manager | | | R | | | | | R |
| • System Monitor Agent | | | | | | | | |

**R** = Required

**O** = Optional

# Network Account

The Network Account is a user name and password combination that enables inter-node communication between all System Platform computers. You must specify the same Network Account on every node when you install the System Platform components for the first time on computers that communicate with each other.

Wherever a Network Account is required, the System Platform Installation dialog box appears and you will need to provide a valid user name and password.

**WARNING! The Network Account is a Windows operating system account located on the local computer or on a domain. Do not delete this account with operating system account management tools. If you do, System Platform software may stop functioning properly.**

- If no other System Platform software is installed on the computer, you are prompted to create a new Network Account or specify an existing user account during the System Platform installation.

- If you use an existing account, it must have a permanent password that does not expire, and the password cannot be changed. By default, the local machine name is displayed. To use a domain user account, enter the short domain name. Do not use the fully qualified domain name (FQDN). For example, use "DomainName" and not "DomainName.com" or "DomainName.local."

**Important:** To enhance security, the Network Account is blocked from logging on to the Galaxy locally or through Remote Desktop Services by default. This is configured in the operating system user rights management.

## About Network Account Privileges

When you install System Platform, you can choose to have the system automatically create the Network Account as a local account. The Network Account cannot be used to interactively log on to the computer.

If you specify a pre-existing user account as the Network, it is added to the group aaAdministrators. Any SQL Server privileges that Application Server requires are also added. See SQL Server Rights Requirements for more information.

---

**Note:** Members of the aaAdministrators group do not have system admin privileges.

---

See Modifying the Network Account if you need to change or recreate the Network Account.

**System Platform Upgrade**

If you are upgrading from an earlier version of System Platform, and the existing Network Account (called ArchestrA User in prior releases) is a system Administrator, you are prompted to:

- Remove the Network Account from the Administrators group to enhance security.

- Keep the Network Account as a system Administrator. You may want to keep the Network Account as a system Administrator, if it is leveraged by other applications and needs elevated privileges.

See Upgrading System Platform for more information.

# Installing System Platform

**IMPORTANT!** We strongly recommend that you log into Windows as a user with administrative privileges when launching setup.exe. Once all selected System Platform products are installed and configured, you can use a lower-privileged account to operate the system.

If you use a standard user account with temporary administrator credentials instead of an administrator account to run setup.exe, a registry flag associated with the temporary administrator account may remain after the system prompts for a mid-installation restart. This flag is used to notify the operating system that setup should resume the next time that particular user logs into the system. Since product installation may have already completed the next time the user logs in, the "modify" setup screen appears instead. If this occurs, simply cancel the modify setup screen. This scenario, if it occurs, will only happen once, since the registry flag will be cleared. This will not affect the products or their installation.

You can select a product-based or a role-based installation for your computer.

**Note:** Prerequisites are installed as part of product installation and not in a separate workflow.

**Compatibility Alert**

If AVEVA™ Manufacturing Execution System or certain versions of AVEVA™ Recipe Management are detected on the node, you will be prompted during installation to apply a patch to the products to ensure compatibility with System Platform 2020 R2 SP1. The patch is required for:

- Manufacturing Execution System 6.2.0. Older versions must be updated to version 6.2 and then patched.

- Recipe Management 4.5.0 and 4.6.0. These two most recent versions must be patched. Versions prior to 4.5 are compatible with System Platform 2020 R2 SP1 and do not require patching.

**To install System Platform**

1. Insert the DVD into your DVD-ROM drive. Navigate to the root directory of the DVD and run setup.exe. Depending on your computer's security settings, Windows User Access Control may ask for permission to run the installation program. Allow it to run, and the startup screen appears.

    If your computer is configured to allow AutoRun, setup.exe may start immediately after inserting the DVD.

    - If the operating system is not supported, you blocked from continuing. A 64-bit operating system is required. For additional information about supported operating systems, see Supported Operating Systems for System Platform 2020 R2 SP1

    - If the operating system is supported, basic installation requirements are checked. .NET Framework 4.8 is installed if it or a later version is not already present.

> **Note:** You are prompted to restart your computer after the .NET Framework is installed. You may need to manually restart the setup program. If the .NET Framework does not install successfully, see System Platform Prerequisites for additional information.

2. You are prompted to manually confirm that your operating system is compatible with System Platform. Refer to the System Platform Readme (for a list of compatible operating systems, as of the System Platform 2020 R2 SP1 release), or the Technology Matrix in the AVEVA Global Customer Support website (for an updated list of compatible operating systems, including newly-released Windows versions).

> **Note:** This compatibility check was added to System Platform 2020 R2 SP1, to ensure installation is not blocked for compatible Windows versions released after the System Platform release, under Microsoft's Long-Term Servicing Channel (LTSC) and Semi-Annual Channel (SAC).
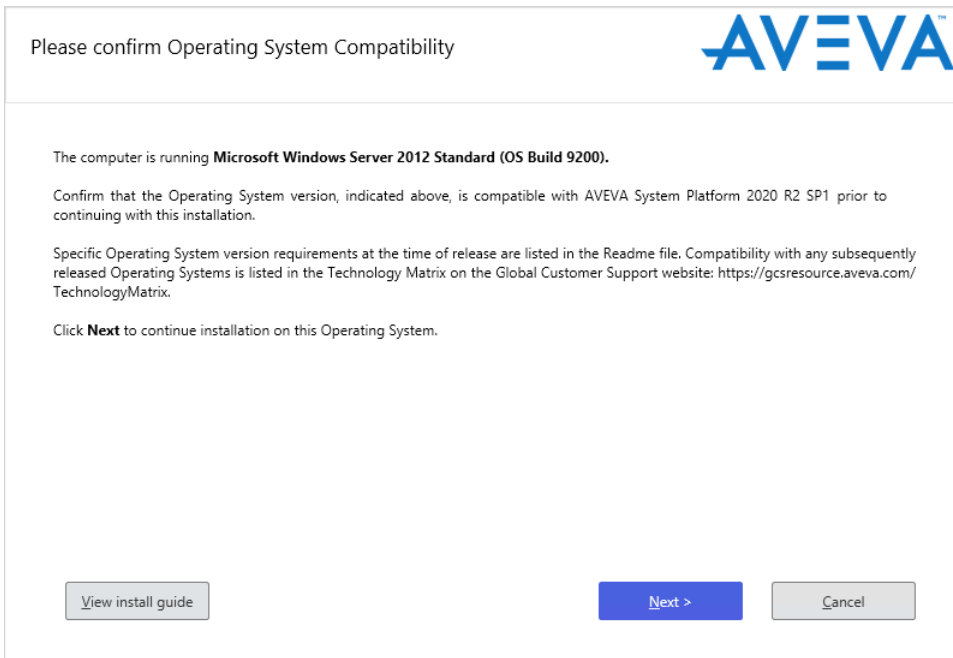


3. After some automatic configuration occurs, the select installation mode dialog box appears.
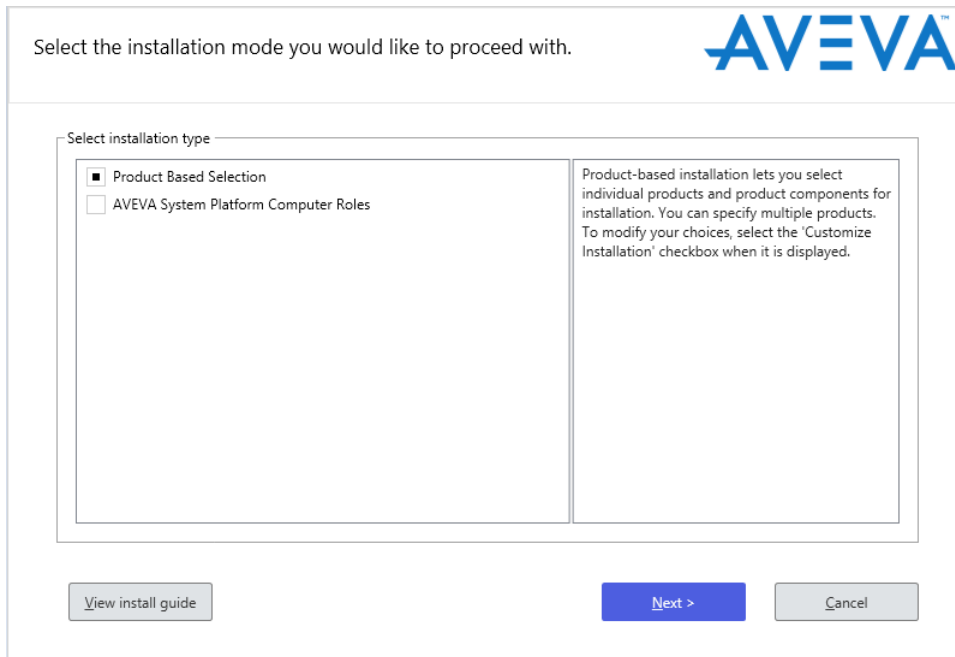
4. Select whether you want a product-based or a computer role-based installation, and then click **Next.** The select options dialog box appears. Its appearance will vary, depending on whether you chose product-based or role-based installation.

   ▪ For information about product-based installation, see About Product-Based Installation.

   ▪ For information about role-based installation, see About Role-Based Installation.

   ▪ If you are installing any of the InTouch Access Anywhere options available under Product-Based Installation, see Installing InTouch Access Anywhere.

   If you select the **Product Based Selection** option, the product based installation dialog box appears. Select the product(s) you want to install on the node.
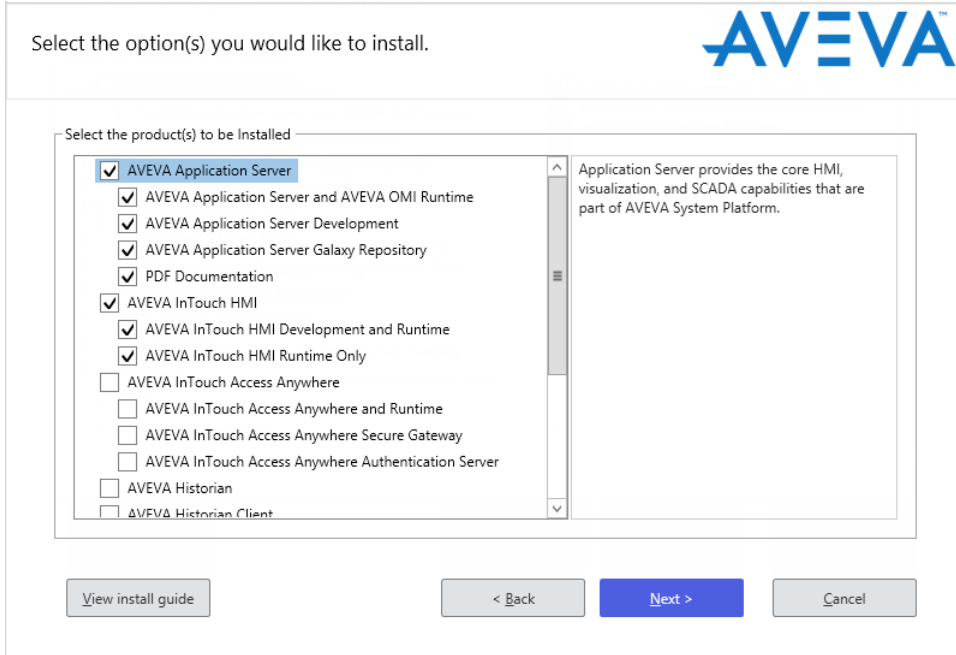
If you select the **System Platform Computer Roles** option, the role based installation dialog box appears. Select the role(s) you want to install on the node.
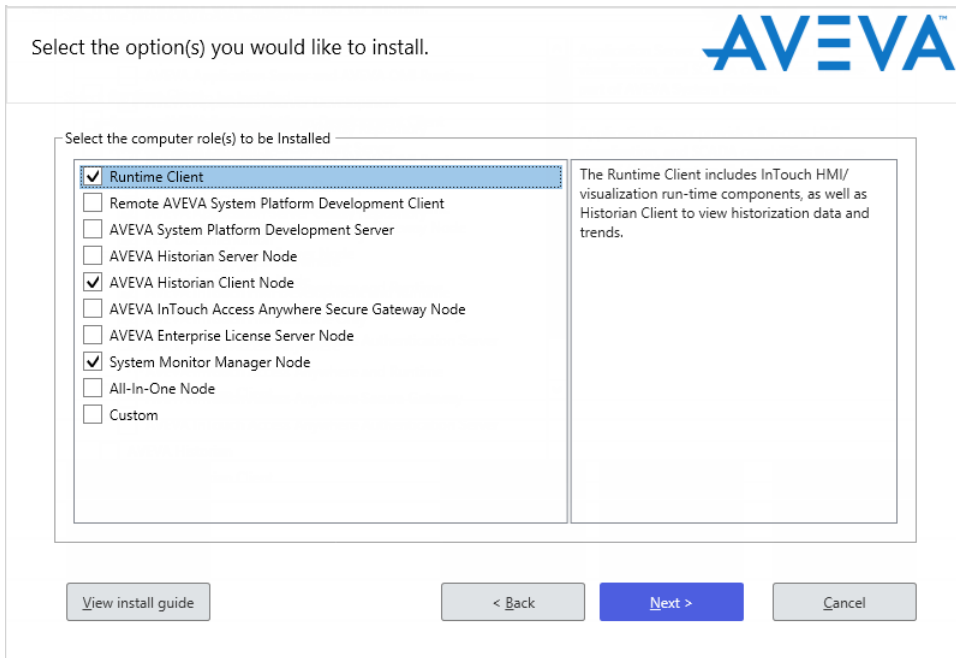


You can select multiple products or roles. All the selected components will be installed together. If you are installing InTouch Access Anywhere Secure Gateway, it should be installed by itself, without any other System Platform components.

5. When you select the Galaxy Repository for installation, the following components are automatically selected for installation and cannot be deselected:

- **Platform Common Services Framework**. The PCS Framework includes a System Management Server, used for establishing a trust relationship between machines. See Configuring the System Management Server for additional information.

- **AVEVA Enterprise Licensing Framework**. Every node should be configured to point to a single License Server. See Configuring the AVEVA Enterprise License Server Location for additional information.

- **AVEVA System Monitor**. Every node should be configured to point to a single System Monitor Manager. See Configuring the AVEVA System Monitor for additional information.

---

**Note:** If you have multiple Galaxy Repository nodes, the **Configurator** lets you select which node(s) to use for the above components at the end of installation. See Configuring System Platform Components for more information.

---

6. After you have made your product or role selections and click **Next**, an important notification appears.

   The notification screen describes important security-related changes in this release of System Platform related to third-party components that are installed to support System Platform. Components that are near or beyond their official support dates are not installed, unless you explicitly choose to install them. These changes have been implemented to improve System Platform security.



7. Click **Next** to proceed. The verify selection dialog box appears.

   - To make changes to your selections or to install out-of-support components, select the **Customize Installation** check box. You can change your selections to:

   - Install the out-of-support components if you are migrating a project with custom-built executable components that leverage these components (NOT RECOMMENDED). See step 8 for additional information.

   - Install other components, such as the InTouch 16-Pen Trend Wizard supplementary component. See step 9 for additional InTouch information.

- Remove components from a node in multi-node Application Server configurations, such as the IDE or Galaxy Repository.

▪ To proceed with your selections without making any changes, click **Next**.
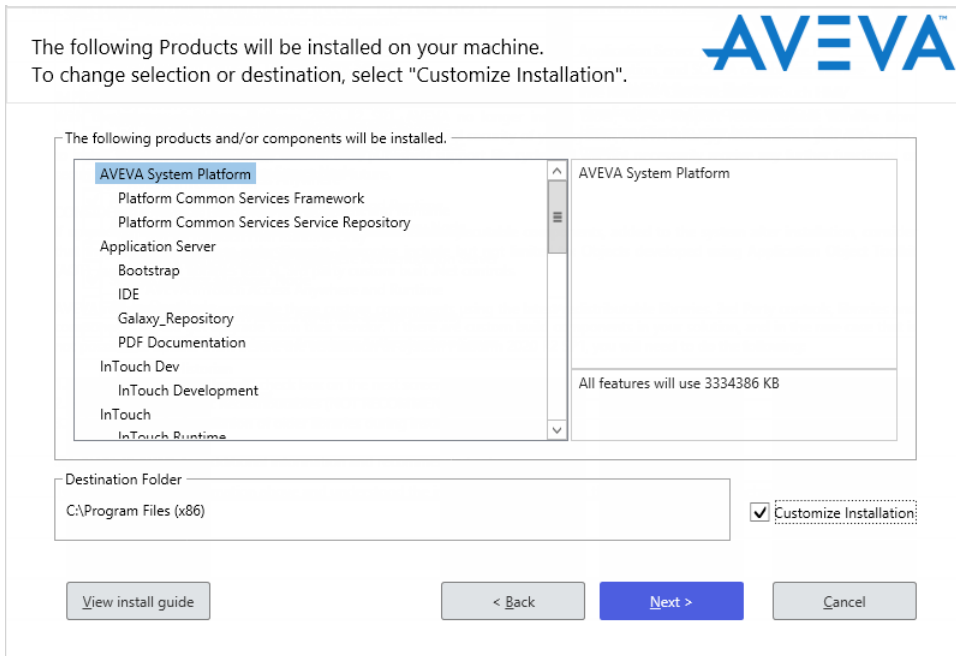


8. **Optional installation of out-of-support assemblies:** Security changes in this release include the removal of certain assemblies from Microsoft and other third-parties that have reached their end-of-life and are now out of support. Installing these assemblies may increase your security risk. Some assemblies have been removed completely as they are no longer needed to support System Platform installation. Other assemblies and executables, listed in the following table, are still included with the installation media. You are given the option to install the following assemblies if needed to support custom-built objects that you may be migrating to the new system. Select the checkbox to install them.
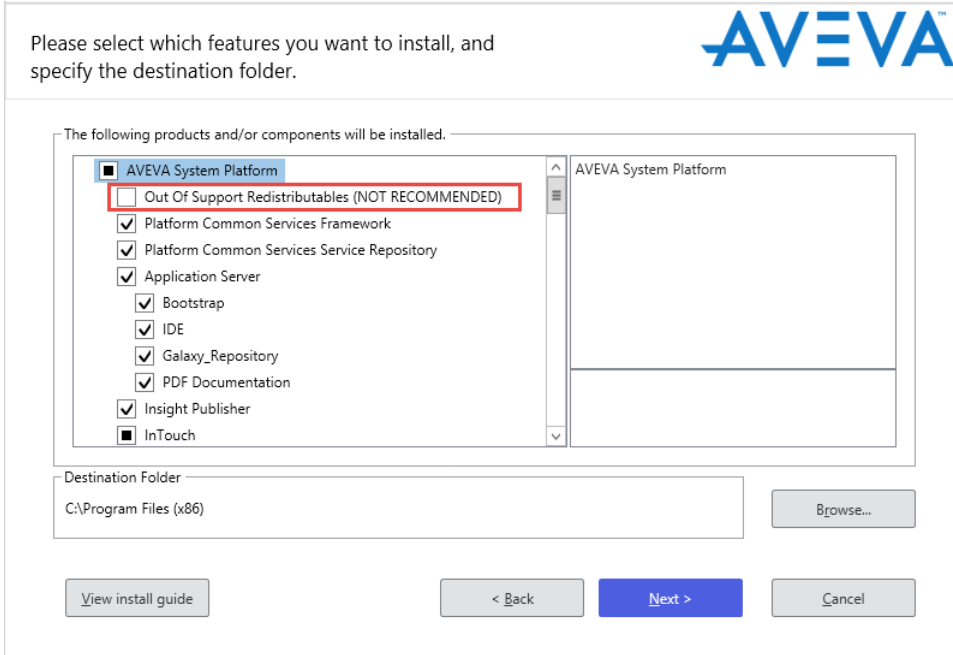
**Important:** Do not elect to install these components unless absolutely required. Instead, AVEVA recommends that you recompile any custom components using the latest redistributable libraries, and/or contact vendor for up-to-date versions.

| Redistributable Description | Folder/Assembly Name |
| --- | --- |
| Microsoft SQL Server 2012 Management Objects SP2 (11.2.5058.0) | SQL2012SP2FeaturePack\ SharedManagementObjects.msi (x64 and x86 versions) <br><br> SQL2012SP2FeaturePack\ SQLSysClrTypes.msi (x64 and x86 versions) |
| Microsoft Visual C++ 2008 Redistributable | VC90SP1/vcredist_x86.exe |
| Microsoft Visual C++ 2010 Redistributable | VC10SP1/vcredist_x64.exe <br><br> VC10SP1/vcredist_x86.exe |

**Note:** You can locate these assemblies on the installation DVD under the **InstallFiles\OutOfSupportRedist** folder. If you select the option to install them now, they will be automatically installed during the installation process.

**Important: Installation of out-of-support assemblies is NOT recommended.**

Instead of installing the out-of-support assemblies, we recommend that you use currently-supported software versions to rebuild any custom ApplicationObjects or applications. You may elect include these out-of-support components when you install System Platform if you will be migrating a project that contains:

• Custom ApplicationObjects built with the Application Object Toolkit

• Remote Response Ojbects

• The discontinued ApplicationObjects $FieldReference or $Switch

- Custom script libraries or custom .NET controls built with these out-of-support components

- Any other component that leverages the out-of-support assemblies

  **Note:** If you do not install the out-of-support assemblies and import objects that have dependencies on them, you may see errors from the aaPim and WWPackageServer components while importing the objects.

9. **Optional installation of InTouch Supplementary Components:** When the **customize installation** dialog box appears, scroll down to the **InTouch Supplementary Components** section to install **InTouch HMI** supplementary components or make other changes.
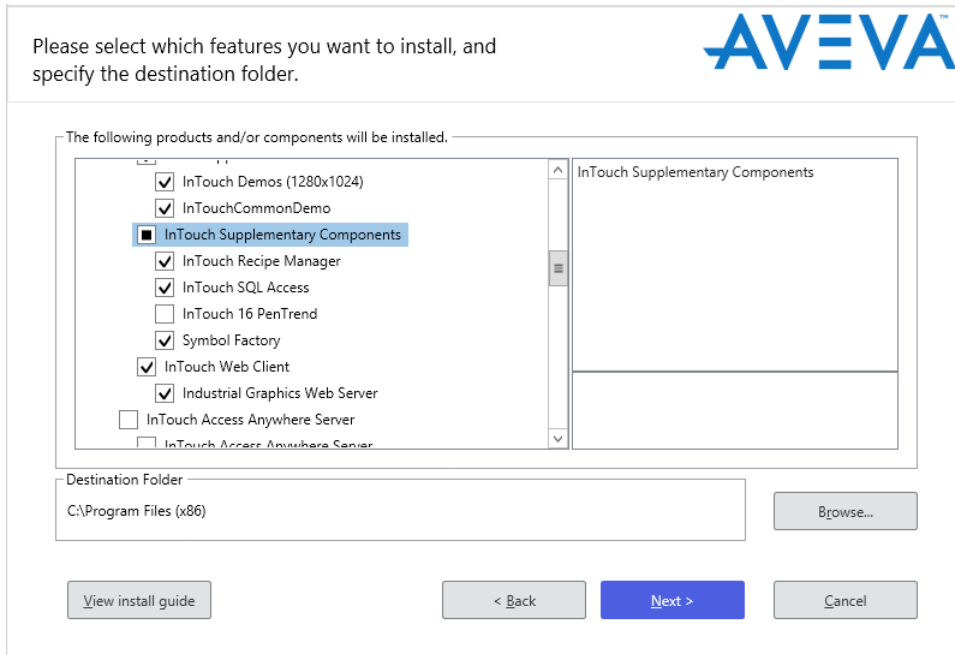


- ▪ Select **InTouch 16 PenTrend** from the list.

- ▪ Make any other product and component selections.

- ▪ You can click **Browse** on the customize installation dialog box to change the program installation destination folder.

  Click **Next** to continue the remainder of the installation procedure.

10. **Optional installation of AVEVA Communication Drivers:** When you select Application Server or InTouch HMI for installation, the AVEVA Communication Drivers Pack Simulator (SIM) and Gateway are also selected for installation. Select **Customize Installation** and then scroll down to add any other drivers that you need.
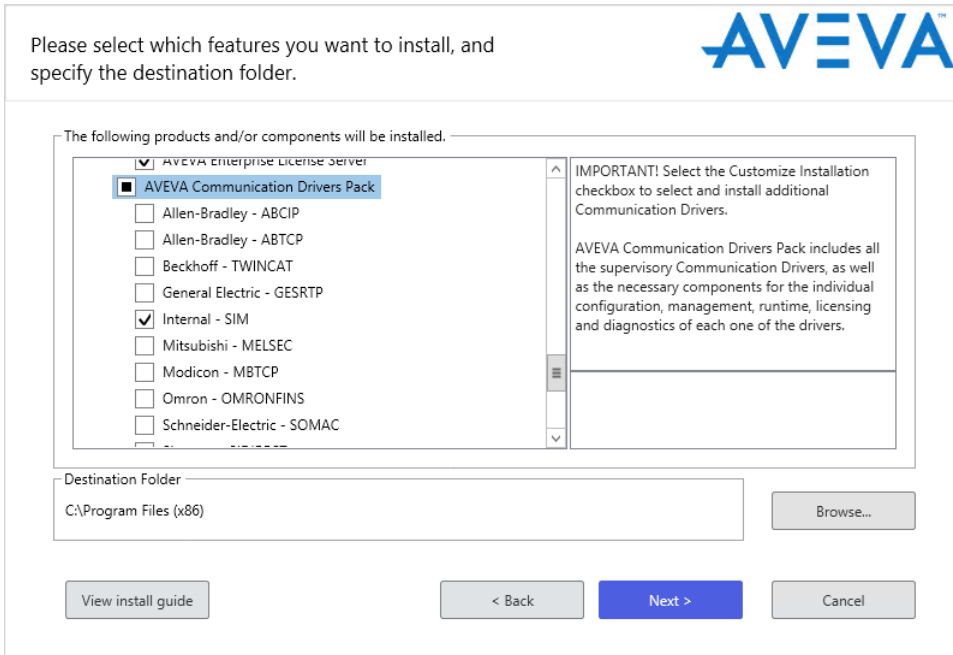
11. If you have selected an **InTouch HMI** features, the language selection dialog box appears. Select the language for your InTouch HMI installation. The InTouch language versions are supported only for the matching operating system language. For example, the German version of the InTouch HMI is only supported on the German operating system.
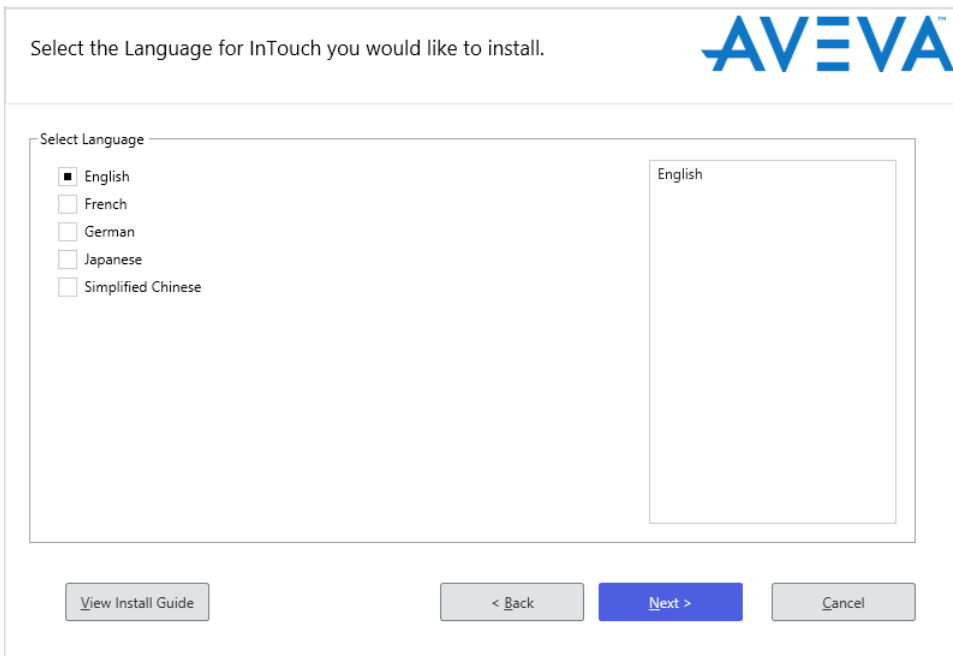


12. Click **Next**. The **End User License Agreement** dialog box appears.
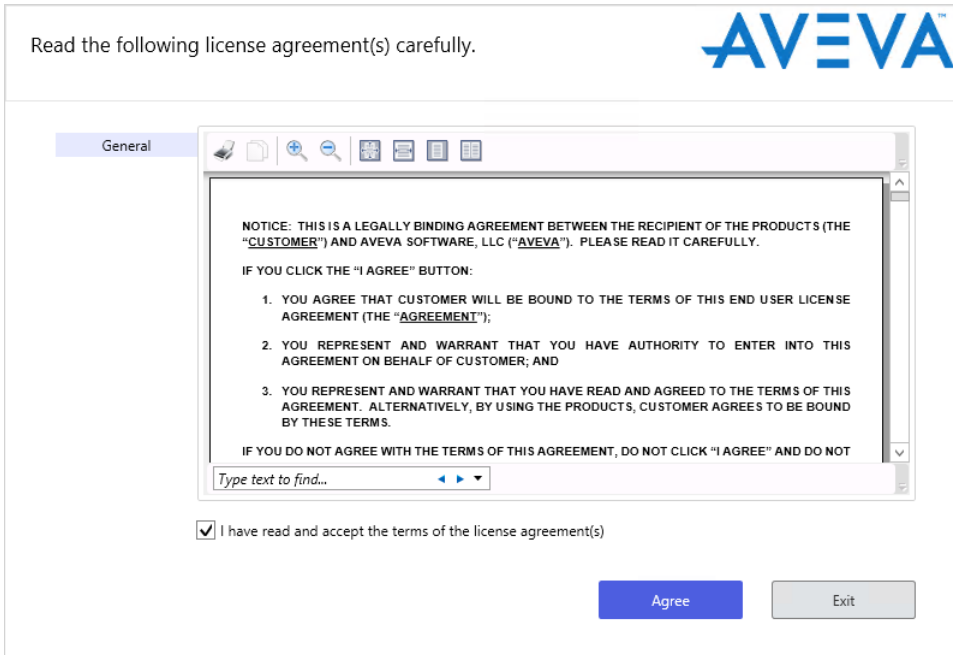
13. Review the license(s). Click **I have read and accept the terms of the license agreement(s)**, and then click **Agree.**

14. If the products or roles you selected require it, the **Off Node Communications** (Network Account) dialog box appears.

   **Note:** If a Network Account for off-node communications is NOT required (for example, if you are only installing Historian Client), you will be prompted to click **Install**. If this is the case, skip to step 18.
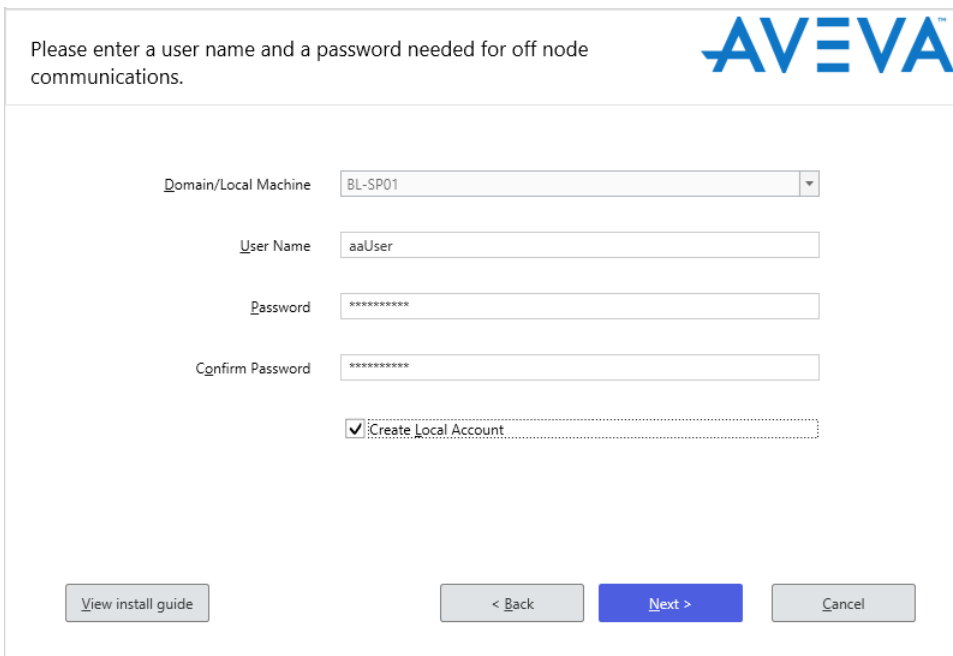
15. Specify a new or pre-existing Network Account for off-node communications. This account is used for encrypted communication between different System Platform nodes and software components. See Network Account for more information.

    ▪ To select an existing account, clear the **Create Local Account** check box. When you clear the check box, the **Domain/Local Machine** text box displays the default domain name. Specify a different domain/local machine name if necessary. Then, enter the user name and password for the existing Network Account. Click **Next** to complete the Network Account setup.

    ▪ To create a new account, click the **Create Local Account** check box if not already selected. By default, the **Domain/Local Machine** box displays your computer name. Then, enter a user name and password.

    ▪ Network Accounts must meet the following requirements:

    • The account must have a permanent password that does not expire.

    • The account must have a password that cannot be changed.

    **Note:** If necessary, you can change the Network Account credentials through the **Change Network Account** utility. The Start Menu includes a short cut to the utility. It is listed under the **AVEVA** folder.

16. If the products or roles you selected require Microsoft SQL Server, and a supported version of SQL Server is not already installed, you will be prompted to select either automatic installation of SQL Server Express, or to exit and manually install a full version of SQL Server.
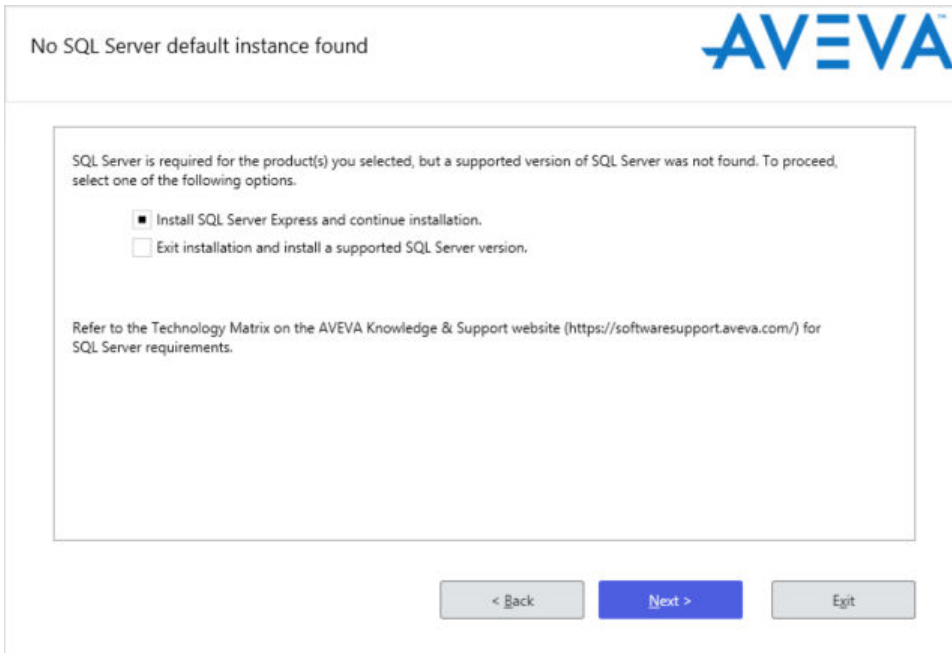


**Caution:** If you select SQL Server Express, System Platform will automatically grant you (the logged in user) SQL sysadmin privileges. This level of access is required to proceed with SQL Server Express installation. You will retain sysadmin privileges even after installation. If you need to remove sysadmin privileges from the logged in account, be sure to create a sysadmin account first.

    ▪ Click **Yes** to use SQL Server Express. SQL Server Express is adequate for systems with less than 25,000 IO. It will be installed automatically along with the other prerequisites and the selected System Platform components.

- Click **No** to skip SQL Server Express installation. Then, click **Exit** and manually install SQL Server. System Platform for medium and large installations includes a separate DVD with a full version of SQL Server 2017 Standard. However, you can install any supported version of SQL Server. See the AVEVA Global Customer Support (GCS) [Technology Matrix](#) for a list of supported SQL Server versions.

    When you have finished SQL Server installation, restart the System Platform installation program.

17. A list of missing prerequisite components (if any) and the System Platform products to be installed are displayed.
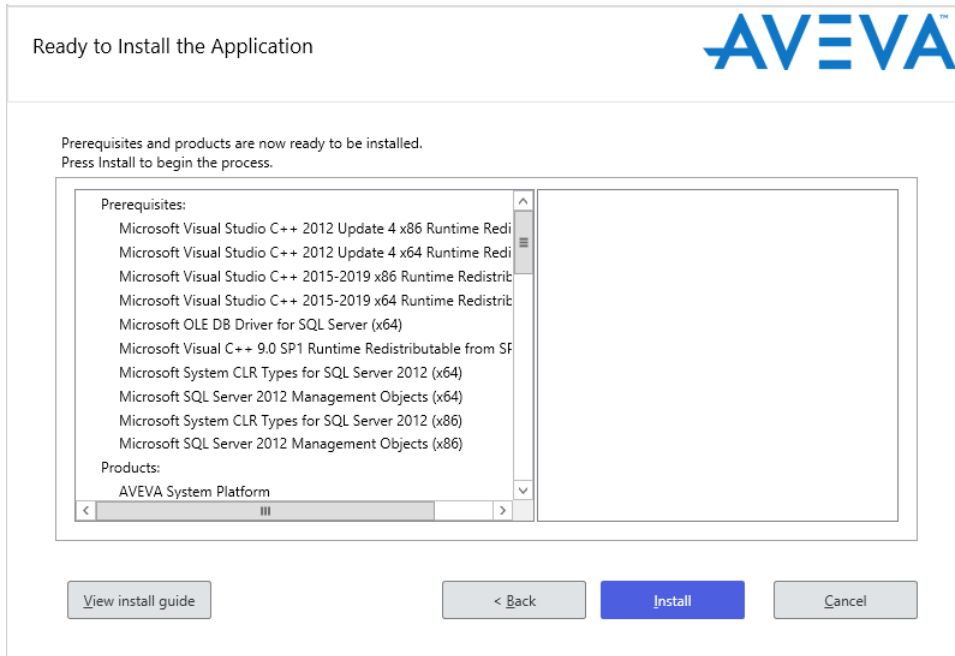


**Note:** Any prerequisites required for the products selected for installation will be listed above the list of products and components. The prerequisites will be installed first, and the product and components will be installed immediately after installation of the prerequisites has finished. If you elected to install SQL Server Express, it will be installed along with any other prerequisites.

18. Click **Install** to proceed. The progress bar appears.
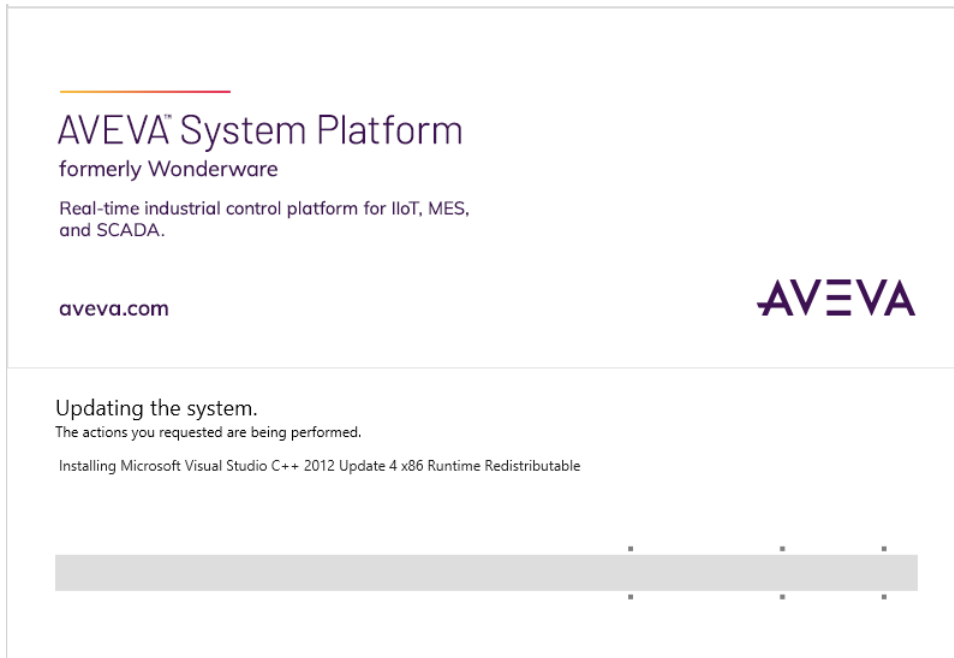
19. After the installation is over, the **installation completed** dialog box appears.
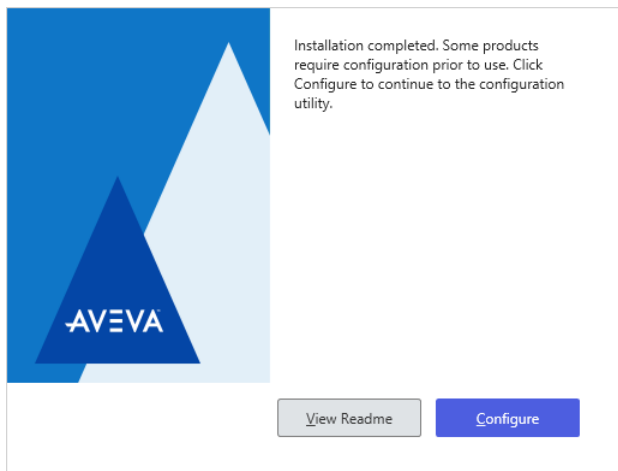


- Select **View Readme** for important information, including hardware and software requirements, new features, and known and resolved issues.

- Select **Configure** to continue. See Configuring System Platform Components for the final steps to complete installation .

# Configuring System Platform Components

The AVEVA Enterprise License Server, security (System Management Server), and the Historian Server require post-installation configuration for initial setup. You need to configure your products using the **Configurator** dialog box after you have installed them. The **Configurator** dialog box lists all product components that require post-installation configuration. You can configure the locations for the product database and the data files.

You must have administrative rights to use the **Configurator**.

**To start the Configurator**

- Click **Configure** on the final installation dialog box. The **Configurator** dialog box appears. The product feature tree expands by default. Most features will show as *Not Configured* the first time you open the Configurator.

- You can also start the Configurator at any time from the Windows Start menu.
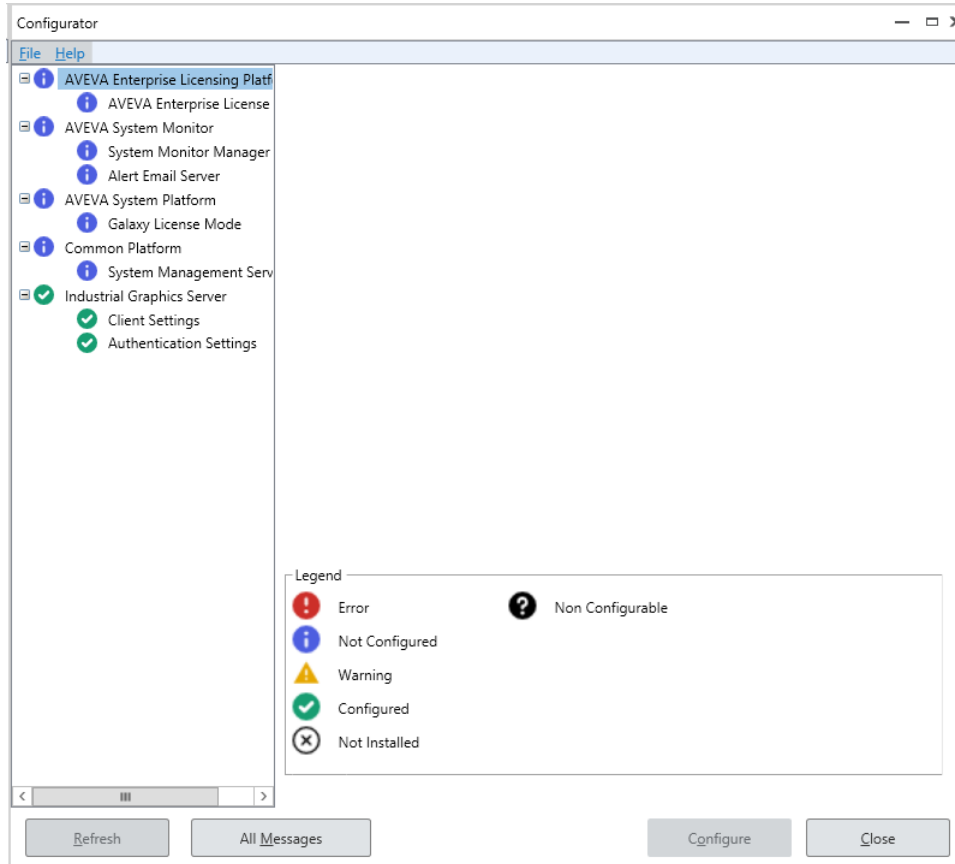


The status of each item in the **Configurator** is displayed when the Configuration opens and as items are configured. The status indicators are:

- 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.

## Configuring the System Management Server

Security measures for System Platform 2020 R2 SP1 include support for the TLS 1.2 protocol for secure encrypted communications between nodes, single sign on (SSO), and certificate management. These features, available since the release of System Platform 2017 Update 3, are enabled through a component of the Common Platform called the **System Management Server**. To enable security, every System Platform node must communicate with

the System Management Server, and there should only be a single System Management Server in your System Platform topology. The System Management Server stores shared security certificates and establishes a trust relationship between machines.

If some nodes have not been upgraded to System Platform 2017 Update 3 or later, communication with those older nodes will continue to utilize unsecured communication. However, communication between nodes running System Platform 2017 Update 3 or later will be encrypted, as long as the nodes are configured to communication with the System Management Server.

**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. For more information, see User Credentials for Configuring the System Management Server.
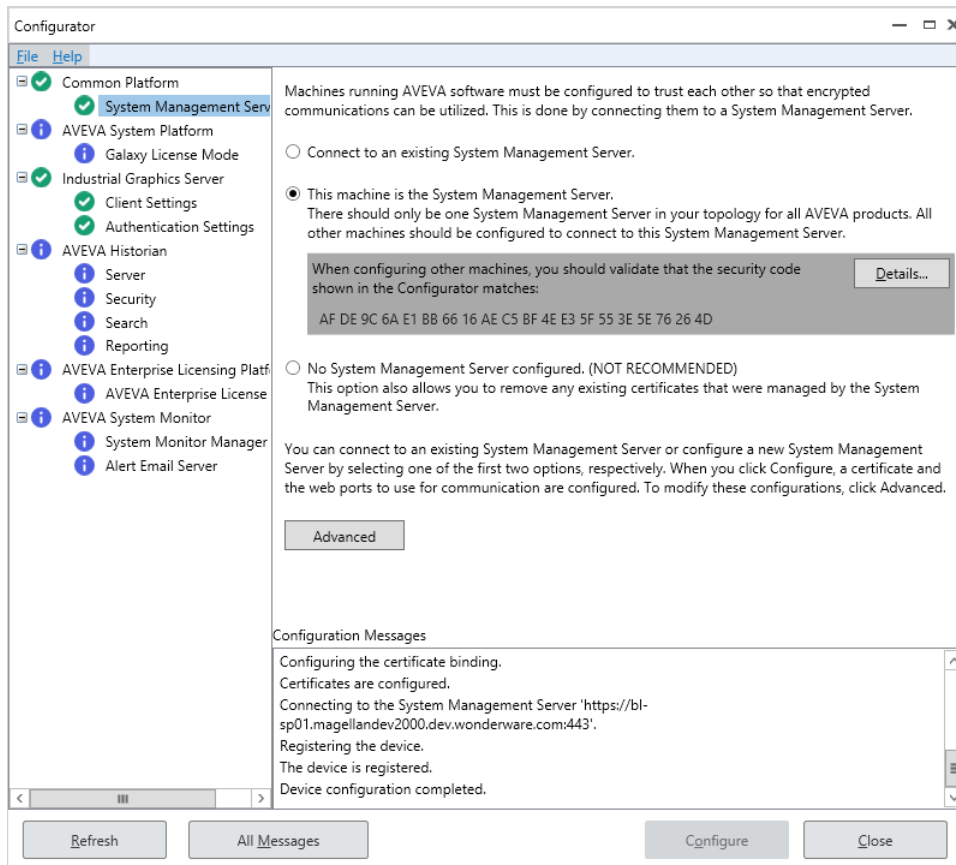


2. You are presented with three choices:

   ▪ **Connect to an existing System Management Server:** This is the default option. The System Platform discovery service looks for an existing System Management Server on its 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

**Note:** The **redundant SSO server** option is not implemented and is not configurable in System Platform 2020 R2 SP1.

- **This machine is the System Management Server:** Select this option if this computer will be the System Management Server. 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. You can still configure other computers in the topology to use a System Management Server.

3. **Advanced settings:** This opens the **Advanced Configuration** dialog window.
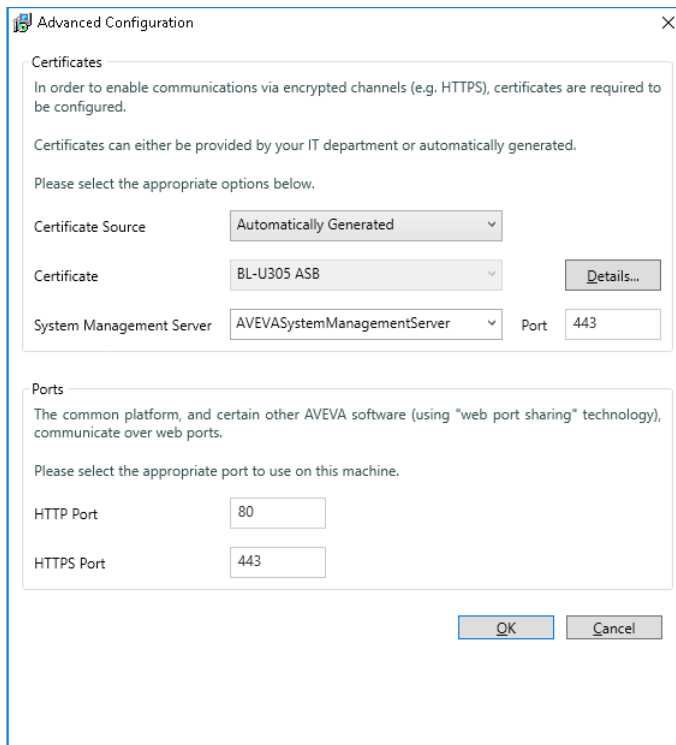


- **Certificate Source:** Select either **Automatically Generated** (default), or **Provided by IT.** If your IT department is providing the certificate, press the **Import** button and navigate to the certificate file. For more information, see Import a Certificate.

**Certificate:** The certificate name is displayed. If you imported a certificate, you view it by pressing the **Details** button. 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.

- **Common Platform Ports:** The ports for the common platform are used for communications with certain AVEVA software, such as the AVEVA System Monitor. Generally, you can use the default settings. Remote nodes must be configured with the same port numbers as configured here. To change the default ports, click the **Advanced** button, then edit the port numbers as needed. See Changing Ports for the System Management Server for more information.

  Default HTTP port: 80

  Default HTTPS port: 443

  Some Application Server communications drivers require some additional, manual configuration if you change the default port(s) used for the System Management Server. This manual configuration is required if you changed a port for the System Management Server and are using either the MQTT Communications Driver or the Auto Build function in Application Server. See Changing Ports for the System Management Server for more information.

  > **Important!** If you have installed InTouch Access Anywhere Secure Gateway on the same node as other System Platform components, there will be a port conflict if you keep the default port settings for System Management Server. You can either (1) change the Common Platform Port number(s) in the **Advanced Configuration** dialog to proceed or, (2) edit the configuration file for the Secure Gateway. See Configuring Ports for the InTouch Access Anywhere Secure Gateway for information on changing the port number.

4. Press the **Configure** button.

   - If you are connecting to an existing System Management Server, the Security Warning window is displayed:
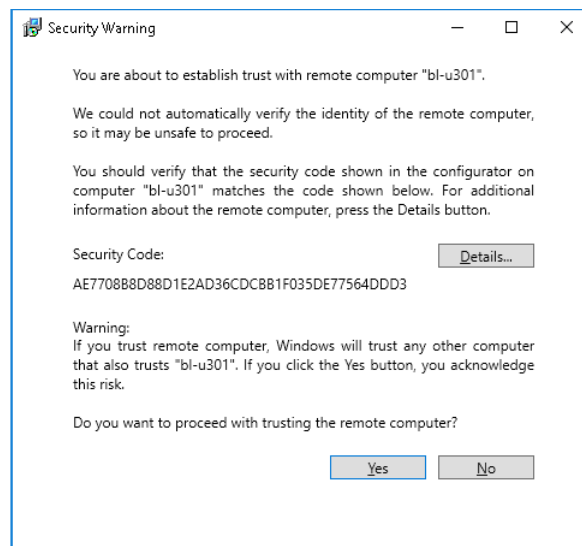


By establishing trust between machines, communications can pass freely. This will be a security concern if you are not sure of the identity of the remote computer. If you have any doubt about the computer you are connecting to, verify the security code and certificate details by selecting the **Details...** button in the Advanced Configuration dialog to open the certificate.
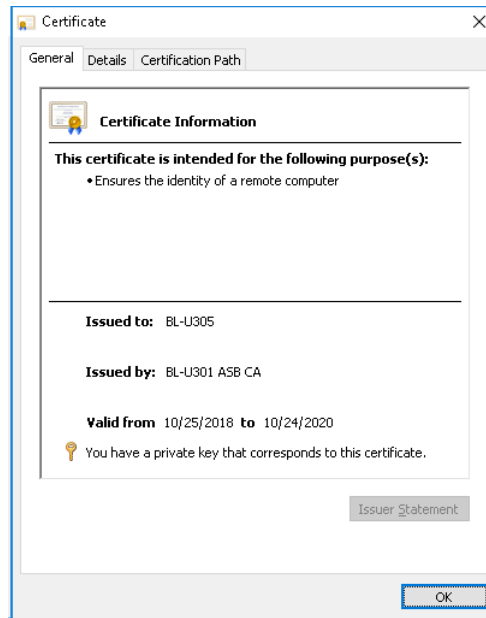
5. Select the next item in the left pane that requires configuration. When all required items have been configured, press the **Close** button to complete installation. See [System Restart after Configuration](#).

## Changing Ports for the System Management Server

Some communication drivers used with Application Server require additional, manual configuration if you change one or both of the default port(s) used for the System Management Server during initial configuration, or a port used by the System Management Server is changed at any time after that. This additional configuration is required if you use either of the following:

- The **Auto Build** function in Application Server. The Auto Build function uses either the ABCIP or SIDirect Communications Driver.

- **MQTT** Communications Driver.

This configuration is not required if you do not change the default System Management ports (HTTP port 80 and HTTPS port 443). However, if a non-default port is configured and then changed back to the default port number, manual configuration is required.

Configure the ports after you have completed all installation and configuration steps, and anytime you change a port number for the System Management System.

**To configure a port for System Management Server**

1. As Administrator, open a command prompt or Windows PowerShell window.

2. Run the following command:

   - If you changed the HTTP port, run this command:
     ```
     netsh http add urlacl url=http://localhost:<changed HTTP port number>/oi/
     user=”NT SERVICE\GDIWebServer”
     ```

   - If you changed the HTTPS port, run this command:
     ```
     netsh http add urlacl url=https://localhost:<changed HTTPS port number>/oi/
     user=”NT SERVICE\GDIWebServer”
     ```

3. Open the Windows Control Panel and select **Services.**

4. Select **Aveva Communication Backend Service** and restart the service.

## Import a Certificate

To import a signed CA certificate, select the **Provided by IT** option from the **Certificate Source** drop down menu. The Import Certificate dialog window opens.
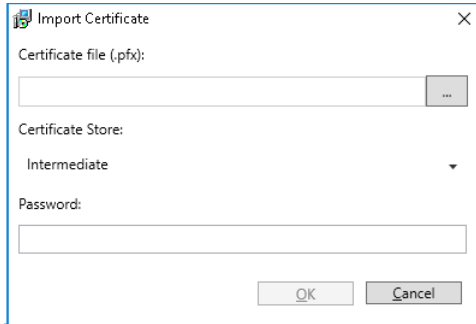


1. Navigate to the Certificate file by pressing the browser ⟨...⟩ button. Select the Certificate file and press **Open**. The Certificate file must have a .PFX extension.

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

3. Enter the Certificate password.

## User Credentials for Configuring the System Management Server

In some circumstances, when configuring the System Management Server, you may be prompted to enter your user credentials. This may happen if the logged in user does not belong to the **aaAdministrators** or **Administrators** OS group. If you are a member of either of these groups, enter your user name as **DomainName \UserName**.

If you are not a member of **aaAdministrators** or **Administrators** on the local machine, you can obtain configuration privileges by editing the file **appsettings.json**, and adding the name of the OS group to the file. The full path for this file is:
C:\Program Files (x86)\AVEVA\Platform Common Services\Management Server\appsettings.json.

To add configuration privileges for the System Management Server to an OS group, add the name of the OS group to the json file, after "aaAdministrators."

```
"AppSetting": {
"AllowGroups": [
"aaAdministrators",
"insert new group name here"
]
```

## Configuring the Galaxy License Mode

The Galaxy License Mode sets licensing mode for the Galaxy Repository. This can be perpetual (Non-Flex) license mode or subscription (Flex) license mode. This setting must match the type of license that has been activated for the License Server. The default setting is Non-Flex mode.

**To configure the Galaxy License Mode**

1. In the Configurator, select **Galaxy License Mode** under **AVEVA System Platform** in the left pane.
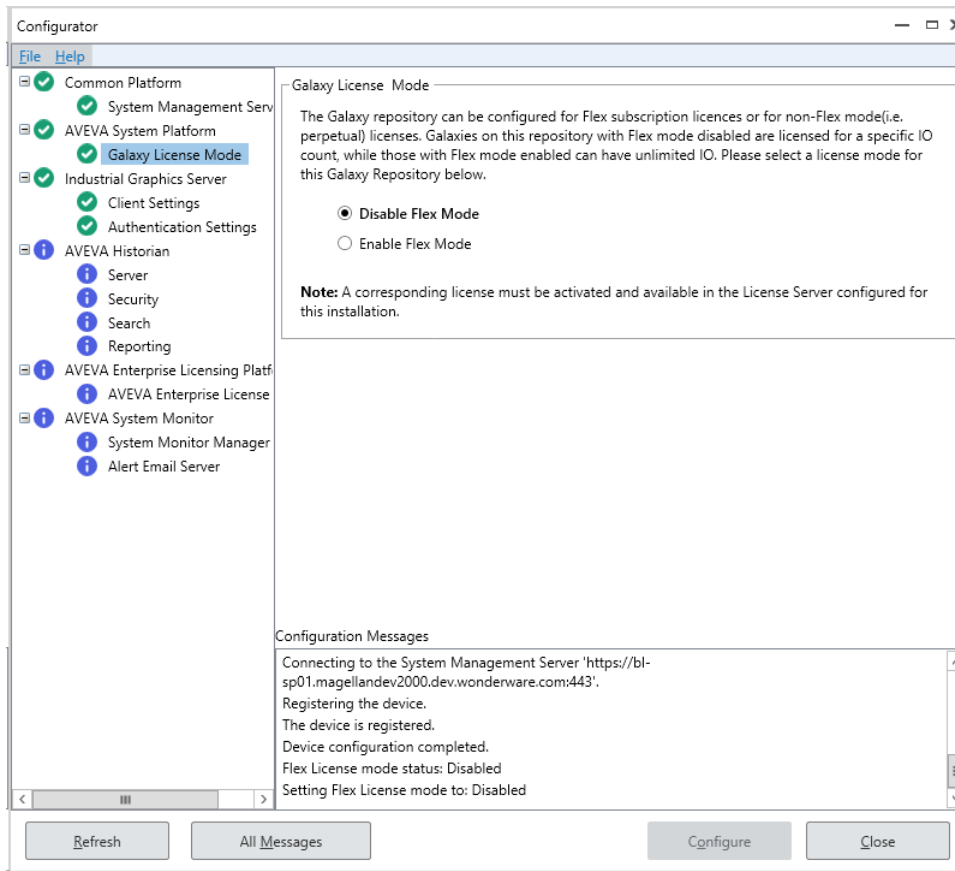
2. Select the licensing mode to used for the Galaxy Repository:

   ▪ **Disable Flex Mode:** Select this mode if you are using perpetual licenses (non-Flex).

   ▪ **Enable Flex Mode:** Select this mode if you are using subscription-based Flex licenses.

   **Note:** Once the licensing mode has been configured, changing modes will require a restart of the GR process.

3. 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. See System Restart after Configuration.

## Configuring the Industrial Graphic 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.

   **Note:** If a System Management Server is configured, the InTouch Web Client will use the security certificate and utilize the HTTPS protocol for secure communications. See Configuring the System Management Server for additional information.

**To configure Client Settings**

1. 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.

2. 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)

**To configure Authentication Settings**

1. In the Configurator, select **Authentication Settings**. There are two options:

   - **Windows Authentication** (default). Skip to step 3 if you are using Windows Authentication.

   - **User Authentication**. User Authentication 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.

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. Press the **Configure** button.

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. See System Restart after Configuration.

## Configuring Databases and Data File Locations

You can use the Configurator to configure Historian settings.

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

You can start the Configurator at any time from the Windows Start menu on the Historian computer.

- To configure Common Platform (PCS) settings, see Configuring the System Management Server.

- To configure licensing, see Configuring the AVEVA Enterprise License Server Location.

**To configure the databases and data file folders**

1. Start Configurator from the Start menu.

2. In the left pane, click **Server**. Then configure the databases as follows.
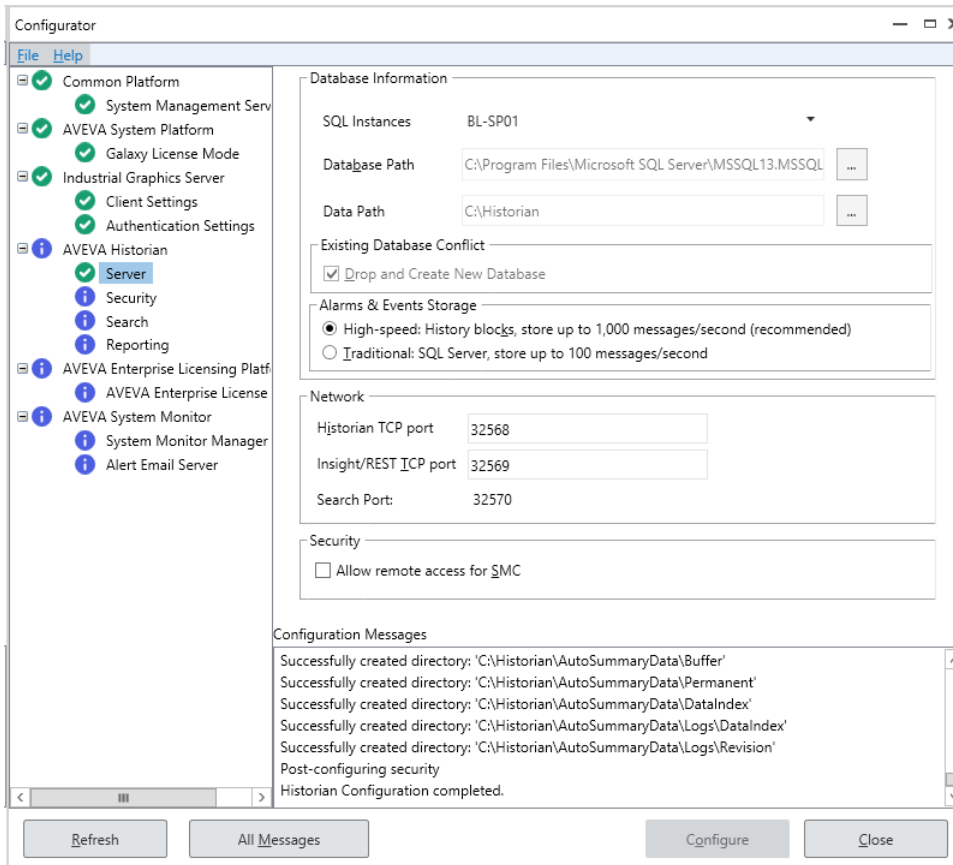


a. Under **Database Information**, specify the SQL Instances and database path.

- **SQL Instance**
  Name the SQL Instance associated with this historian.

- **Database Path**
  Unless you have specific requirements, keep the default SQL Server database path. This is the path where the configuration database is deployed. Click the ellipsis button to specify a different directory in which to install the historian database files.

b. Under **Existing Database Conflict**, read any notices.
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.

c. Under **Alarms & Events Storage**, configure how you want to store alarm and events.

**Important:** If you want to change this setting later after the Historian is running, you must first shut down and disable the historian using the Management Console. Then, after making the change, you can restart and enable the historian.

- **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.

d.  Under **Network**, accept the default ports or change these settings. The ports you specify are added to the exclusions list of Windows Firewall.

- **Historian TCP port** is used for replication data.
  If you are configuring a tiered historian server, specify the port number for tag replication between the tier-1 and tier-2 servers. You must use the same port for all the tier-1 and tier-2 systems working together in the tiered configuration.

- **Insight/REST TCP port** is used for data queries via Insight or the Historian REST API to the Historian Server.
  Type the number for the port used by Insight and REST interface queries.

  **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 the InSight\Rest TCP Port.

- **Search port** is used for data searches. This field is for reference only.

e.  Under **Security**, Check the box if you want to allow remote access of this server's System Management Console (SMC).

When you check **Allow Remote Access for SMC**, Historian allows remote connection to the SMC. Specifically, this allows remote launch and remote activation permissions for the aahCfgSvc and aahEventSvc Historian COM services. (By default, these are set to local launch and local activation.) The permissions are limited to the aaAdministrators, aaPowerUsers, and aaUsers groups. Anyone who is not a member of these groups on the server will not see that Historian remotely via SMC.

3.  In the left pane, click **Security**. Configure the security options as follows.
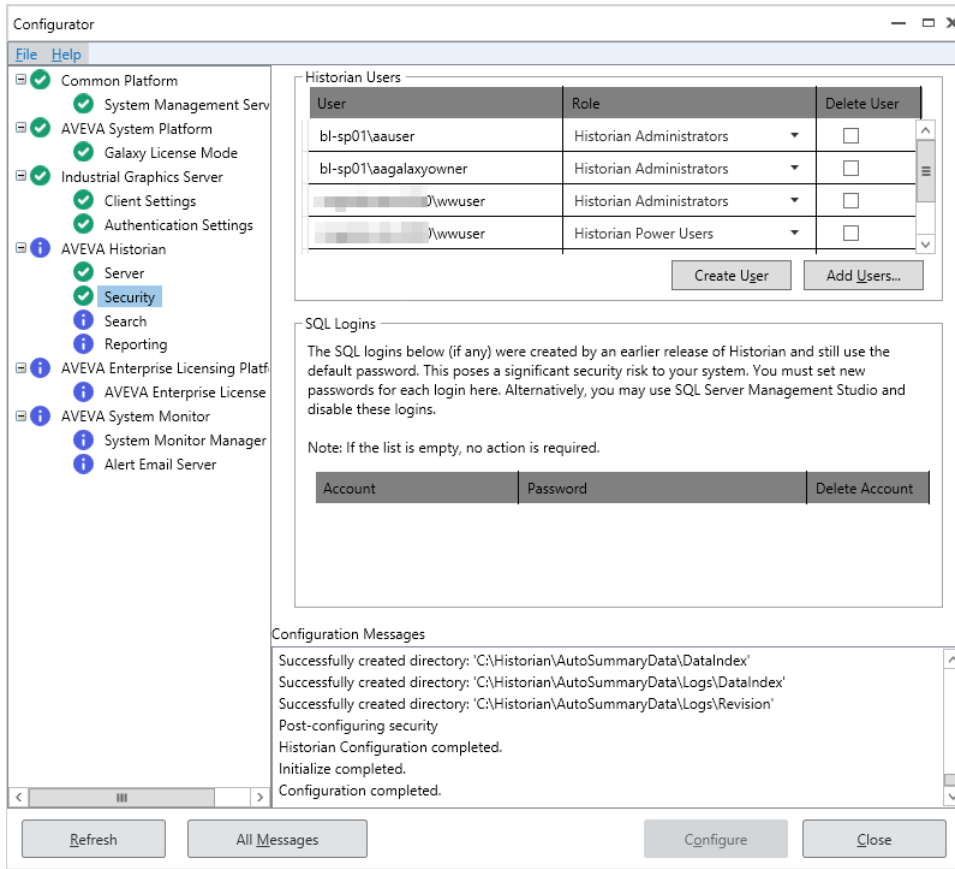
a. Under **Historian Users**, review the existing users and roles for this server. Make adjustments to the list as needed:

- To create a new user account, click **Create Users** and then specify account details.

- To add existing user accounts to this list, click **Add Users** and then select the account criteria to use.

- If you don't need this account anymore, mark the **Delete Account** check box.

b. 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.

4. In the left pane, click **Search**. Then configure the search options as follows.
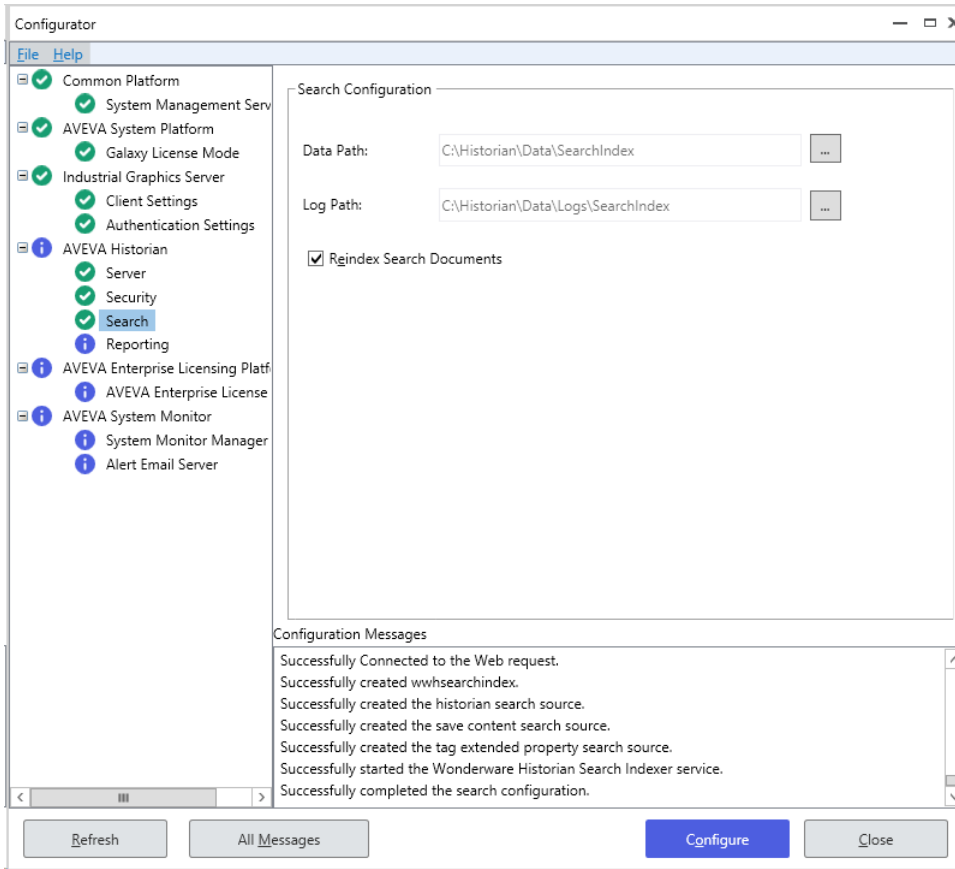
Under **Search Configuration**, specify file locations.

- **Data Path**
  Accept the default path, or click 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 click 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.

5. In the left pane, click **Reporting**. Then mark the appropriate check boxes to configure OData extensions for SQL Reporting Studio or Visual Studio Report Designer on your system.
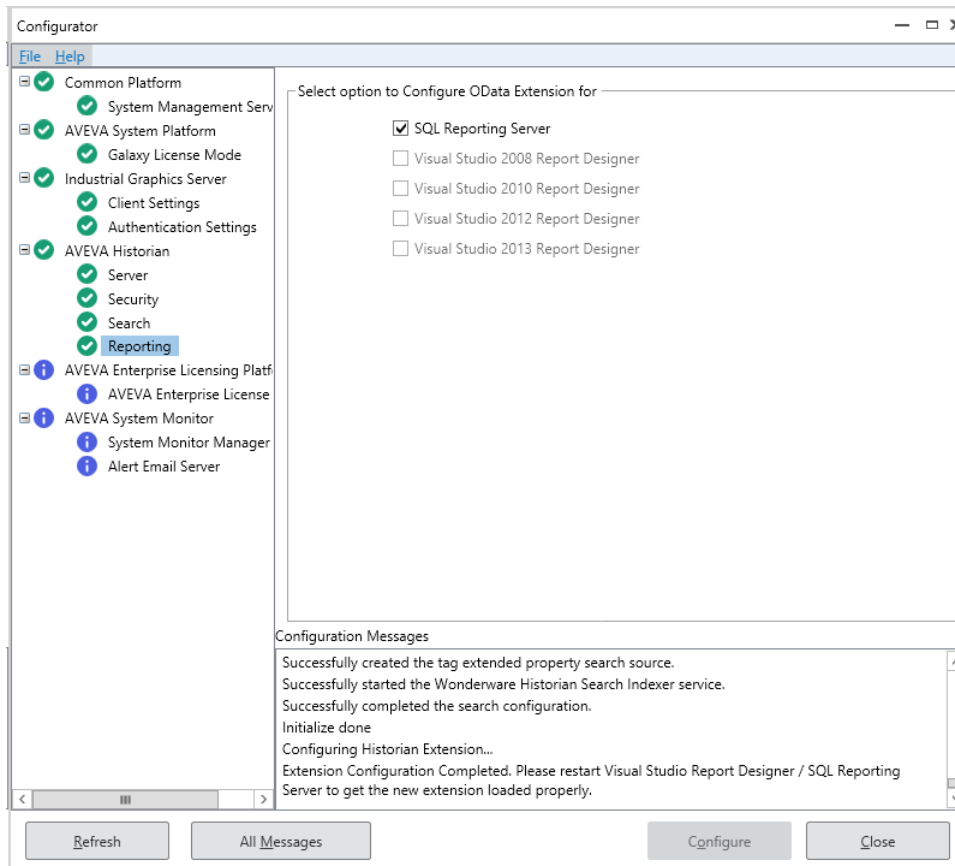
6. In the **Configuration Messages** area, read messages regarding prerequisite checks, current configuration state, and configuration activities that are logged.

7. Click **Configure**. The Processing SQL Script dialog box appears. You can see the historian database configuration scripts running. Multiple scripts run during the configuration.

8. After the system finishes running the SQL scripts, the Historian node and Historian Server node are shown with a green status indicator if the database is successfully configured.

9. Click **All Messages** to see all the configuration messages.

# Configuring the AVEVA Enterprise License Server Location

Detailed information about configuring the AVEVA Enterprise License Server is contained in the *AVEVA Enterprise License Platform Guide.* This guide can be accessed from the AVEVA Enterprise License Manager (see License Installation and Activation for additional information). The basic steps to configure the location of the AVEVA Enterprise License Server are:

1. In the left pane, select **AVEVA Enterprise 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).

   ▪ **Server Port:** default is 55555.

   ▪ **Agent Port:** default is 59200.

**Note:** To see if the license server can be found after entering the Server Name and Port, you can press **Test Connection**.

- **Backup:** If you have configured a backup server (secondary server), select the checkbox to enable backup. Then, enter the secondary server name.

2. Press the **Configure** button.
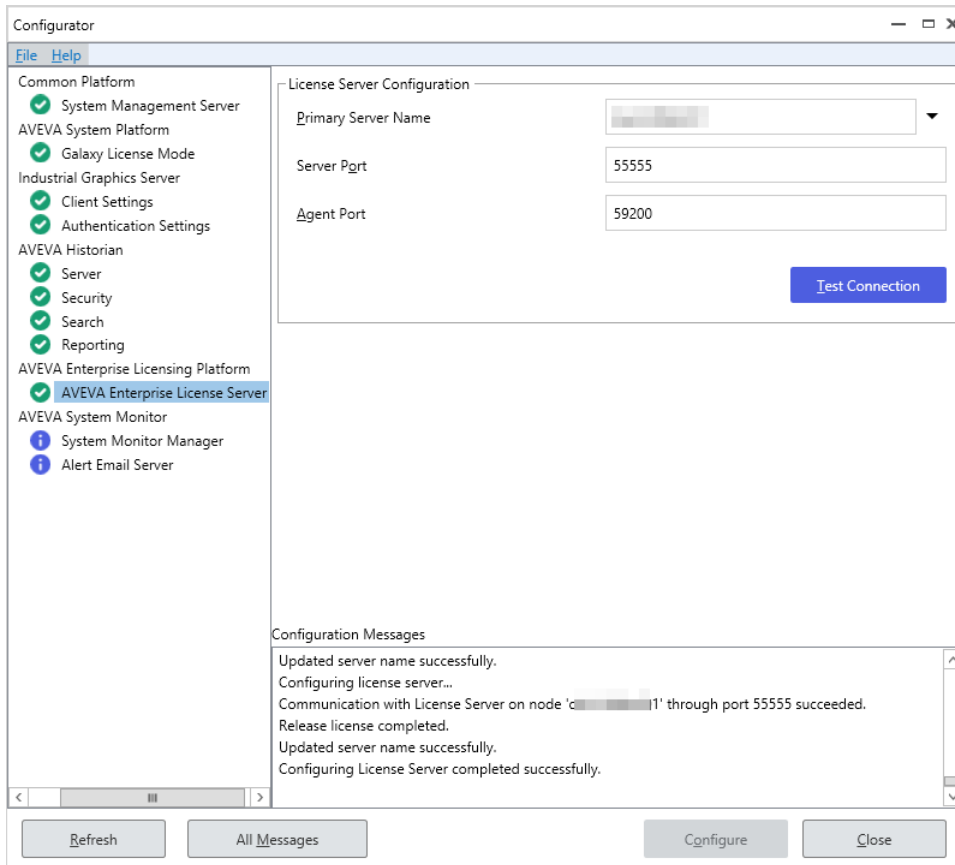


**Note:** If you change a license server name after configuring it, you are prompted to release licenses from the old server name.

3. 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. See System Restart after Configuration.

## Configuring the AVEVA System Monitor

The AVEVA System Monitor contains two configuration items:

- **System Monitor Manager**: The System Monitor Manager configuration item specifies the name of the System Monitor Manager node. By default, the System Monitor Manager is selected for installation on the Galaxy Repository node, but you have to configure the name of the System Monitor Manager on each node in the System Platform topology. This allows the System Monitor Agent, which is automatically installed on each System Platform node, to communicate with the System Monitor Manager node. There should be only one System Monitor Manager node in a System Platform topology. See AVEVA System Monitor Installation for more information.

- **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. You must have SQL Server administrator rights to configure the email server. The email server sends email alerts generated by the System Monitor Manager to notify personnel that an issue has been detected and may require attention.

## System Monitor Manager Configuration

By default, the System Monitor Manager is installed on the Galaxy Repository node. There should only be one System Monitor Manager per System Platform topology, and each node should be configured to point to it.

1. In the Configurator, select **System Monitor Manager**, under **AVEVA System Monitor**.

   ▪ 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.
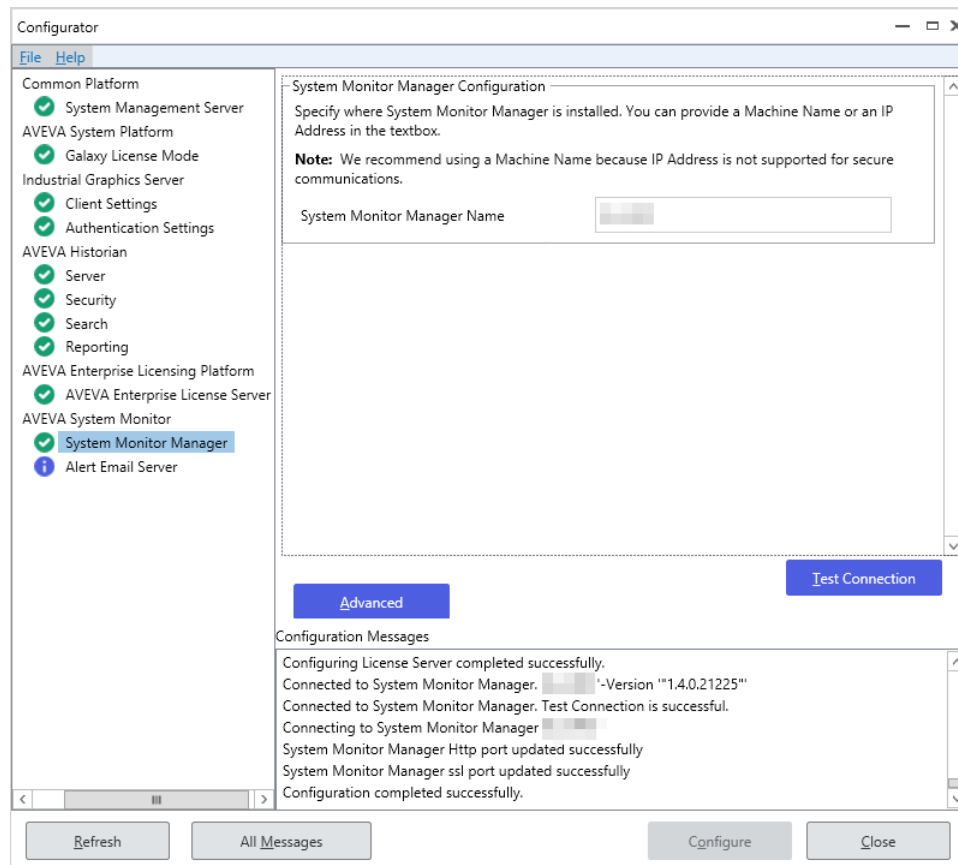


2. In the **System Monitor Manager Name** field, enter either the computer name (preferred) or IP address of the node that will act as the **System Monitor Manager**. If you are configuring the current node as the System Monitor Manager, enter its name or IP address. If you have configured secure communications 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** settings configuration dialog to configure the TCP/IP port numbers. See Advanced System Monitor Configuration for additional information.

3. If either Historian or MES is installed on the node, the Configurator detects the installation. It allows you to specify credentials for these programs to use to increase security. If MES or Historian is not installed, credential fields are not displayed and you can skip this step.

   ▪ **If MES is installed on the node:** To enable secure communication between MES and the System Monitor Manager, select the checkbox next to "Enter the MES credentials." If you do not select the checkbox, communication between MES and the System Monitor Manager is unsecured.

   If you selected the checkbox, enter the user name and password of a configured MES user. The System Monitor Manager uses the configured user to communicate with MES.

   ▪ **If the Historian is installed on the node:** To enable secure communication between the Historian and the System Monitor Manager, select the checkbox next to "Enter the Historian credentials." If you do not select the checkbox, communication between the Historian and the System Monitor Manager is unsecured.

   If you selected the checkbox, enter the user name and password that was configured for the **Network Account**. The System Monitor Manager uses the Network Account to communicate with the Historian. See Network Account for more information.

4. You can use the **Test Connection** button to check that the node you are configuring can reach the System Monitor Manager node.

5. Press the **Configure** button.

6. 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. See System Restart after Configuration.

## Advanced System Monitor Configuration

An instance of the System Monitor Agent is installed on every node. Each agent communicates with the System Monitor Manager through TCP/IP and uses the Common Platform settings. Each System Monitor Agent must use the same port number that was configured for the System Monitor Management Server. See Configuring the System Management Server for additional information.

If you have changed the default port settings for the System Management Server, use the **Advanced Configuration** settings to configure the TCP/IP port numbers for the System Monitor.

**To configure the System Monitor Manager TCP/IP Port Numbers**

**Note:** Configure the **System Management Server** before you configure the System Monitor Manager ports.

1. In the Configurator, select the **System Monitor Manager** entry, under **AVEVA System Monitor**.

2. Click the **Advanced** button. The Advanced Configuration dialog window opens.
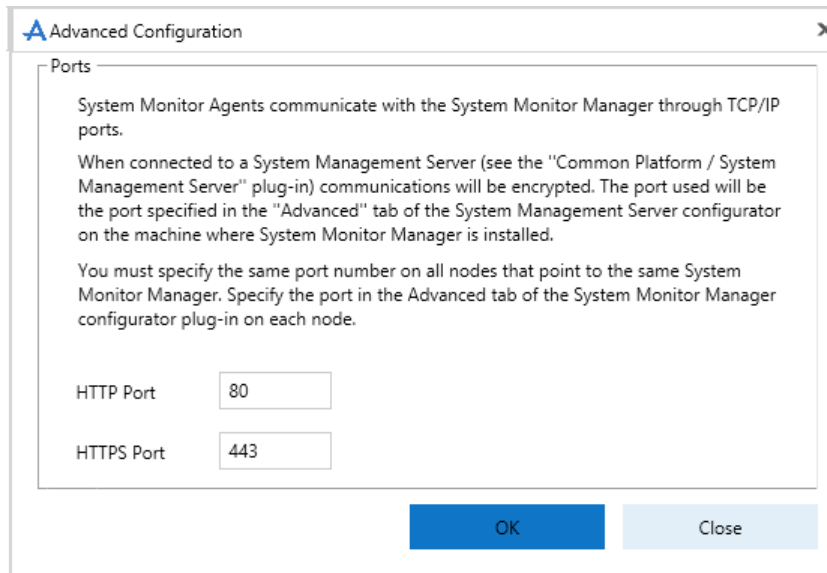
3. Set the port number. Unless you changed default port numbers, no changes should be needed.

   ▪ If System Platform is configured to use a secure mode of operations, that is, if the System Management Server option is configured, set the SSL port to the same number that was configured for Common Platform communications. The default SSL port is 443.

   ▪ If security is not configured for System Platform, that is, if no System Management Server option is configured, set the HTTP port to the same number that was configured for Common Platform communications. The default HTTP port is 80.

4. Press **OK**, and then **Close** to exit **Advanced Configuration**.

5. 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. See System Restart after Configuration.

## Email Server Configuration

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.

1. In the Configurator, select **Alert Email Server**, under **AVEVA System Monitor**.
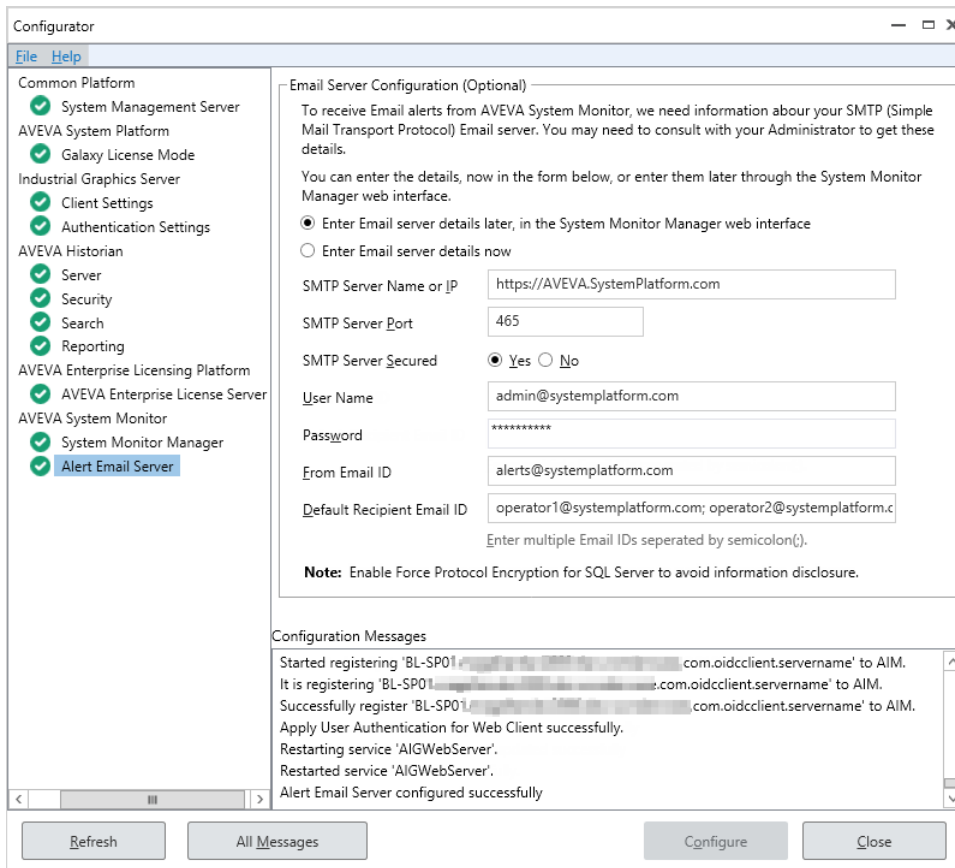
2. Select one of the email alert details options.

   ▪ To skip email server configuration, choose the option to enter email server details in the System Monitor Manager web interface.

   ▪ To configure the email server, choose the option to "Enter Email server details now."

1. 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.

2. 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.

3. In the **SMTP Server Secured** field, enter **yes** if the server is secured, or **no** if it is not.

4. **If you are using a secured email server**, enter the user name and password to access the server. The user name and password field are only applicable to a secured email server.

5. In the **From Email ID** field, enter the email address that will be used to send system alerts from the System Monitor.

6. In the **Default Recipient Email ID** field, enter the email address(es) that will receive system alerts from the System Monitor.

7. Press the **Configure** button.

8. 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. See System Restart after Configuration.

## System Restart after Configuration

When you have configured all the listed components, click **Close**. The system will prompt you to restart. You can restart now or later.
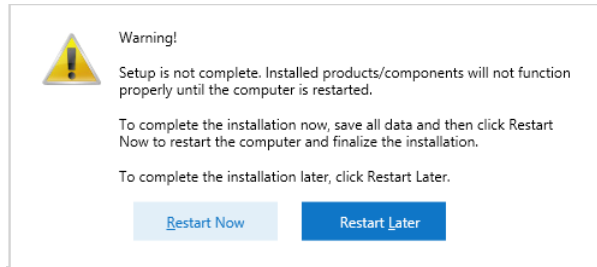


**Note:** The installed programs may not function properly until you restart the system.

After the system restarts, and before you start using System Platform, make sure that you have activated your product licenses. See License Installation and Activation.

# Installing InTouch Access Anywhere

InTouch Access Anywhere does not allow you to remotely install it. Therefore, you must run the installation program locally for each instance.

Three InTouch Access Anywhere installation options are available from the System Platform product-based installation menu. These can be installed separately or together.

- Install InTouch Access Anywhere Server
- Secure Gateway Installation
- Install the Secure Gateway and Authentication Server Separately or Together

See the following documents for for additional information, including configuration steps that should be performed prior to installation. These documents are located on the System Platform Installation DVD under InstallFiles\CD-Intouch\UserDocs.

- *InTouch Access Anywhere Secure Gateway Administrator Manual* (file name: ITAA_Server_AdminManual.pdf)
- *InTouch Access Server Administrator Manual* (file name: ITAA_Gateway_AdminManual.pdf)

Before installing the InTouch Access Anywhere server, verify the following requirements have been met:

- The computer that will host the InTouch Access Anywhere server must be running a 64-bit version of Windows Server.
  - Windows Server 2012 Data Center
  - Windows Server 2012 R2 Data Center and Standard
  - Windows Server 2016 Data Center and Standard
  - Windows Server 2019 Data Center, Essentials and Standard
  - Windows Server IoT 2019

> **Note**: Embedded operating systems are not supported by InTouch Access Anywhere Server.

- .NET Framework 4.8 or later must be installed on the computer that will host the InTouch Access Anywhere server. You can allow the setup program to install it automatically if it is not present. See System Platform Prerequisites for detailed information.

- InTouch applications must be built with version 10.6 or later to be viewed through InTouch Access Anywhere

- The InTouch Access Anywhere server must be installed on the same computer that hosts InTouch WindowViewer.

- Remote Desktop Services must be configured on the host computer.

> **Important**: InTouch Access Anywhere leverages RDP and translates RDP to WebSockets. RDS access must be enabled on the computer hosting InTouch Access Anywhere.

- Make sure the anticipated users of InTouch Access Anywhere are members of the Remote Desktop Users group to be granted the right to log on to the Access Anywhere server remotely.

- The host computer's firewall is configured to permit inbound and outbound network traffic on port 8080.

  Make sure no other application installed on the InTouch Access Anywhere server also uses port 8080.

- On host computers running Windows Server 2012, the InTouch WindowViewer executable file (view.exe) must be added to the host computer's RemoteApp list and configured to support command-line arguments.

- The corresponding TSE (RDS) Concurrent license is activated on the host computer.

- If upgrading to a newer version of InTouch Access Anywhere, first back up any custom components of the existing installation, then uninstall the existing version before installing the new version.

- InTouch Access Anywhere Server cannot be installed on computers in which the host name contains non-English characters.

- InTouch applications cannot be listed by InTouch Access Anywhere if application names or folder paths contain an ampersand (&) character.

## Install InTouch Access Anywhere Server

A basic installation of the InTouch Access Anywhere Server usually takes about five minutes. When you select the InTouch Access Anywhere Server, several InTouch run-time and complementary components are auto-selected. These are required for installation with the InTouch Access Anywhere Server, and include:

- Insight Publisher

- InTouch Runtime

- InTouch Alarm DB Logger (Alarm Logger and Purge Archive components)

- InTouch Supplementary Components (Recipe Manager, SQL Access, and Symbol Factory)

- InTouch Web Client

Make sure that all installation prerequisites have been met before starting the installation procedure. The following procedure explains the basic steps to install the InTouch Access Anywhere Server on a computer running a supported version of Windows Server.

Before placing InTouch Access Anywhere into a secure, production environment, you may want to do some internal testing. Install All Components on a Single Server describes an alternative installation method to place

the InTouch Access Anywhere Server, the Secure Gateway, and the Authentication Server on a single server computer.

**To install InTouch Access Anywhere Server**

1. Log on as a Windows administrator on the computer where you are installing InTouch Access Anywhere Server.

2. Insert the System Platform DVD in your computer and run **setup.exe**.

3. Select **Product-Based Selection**.

4. Select **InTouch Access Anywhere Server**. You will see the additional components auto-selected. Click **Next** to continue.
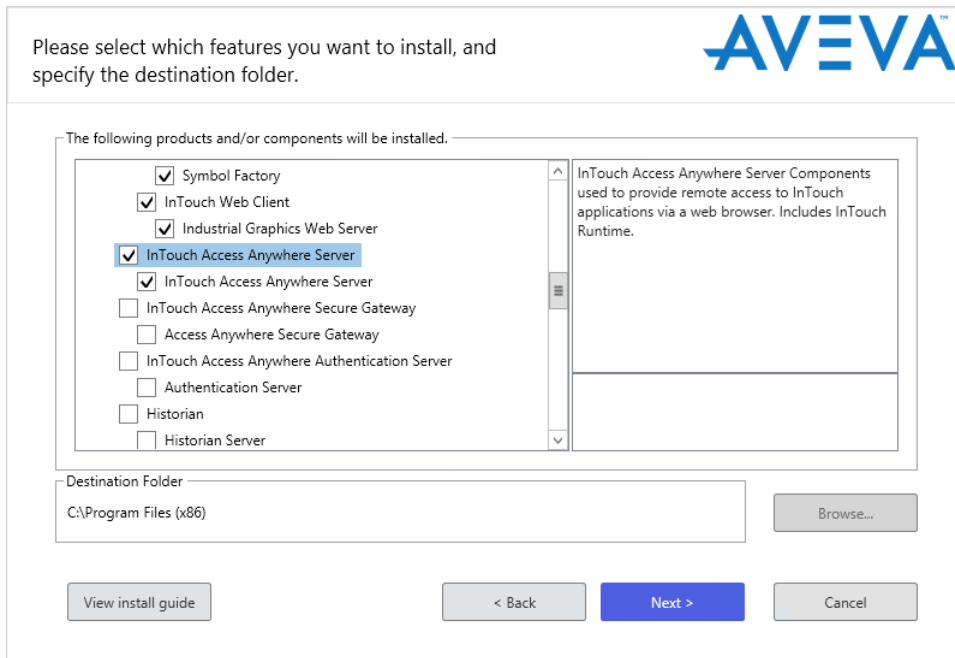


5. Click **Next** on the dialog box that shows the components to be installed.

6. Select the check box that acknowledges you have read and accepted the terms of the license agreement and select **Agree**.

7. Click **Install** to begin installing InTouch Access Anywhere and InTouch Runtime.

8. A horizontal bar shows the progress of the installation.

9. Click **Finish** to complete the installation.

10. Configure (or disable) the Windows Firewall for use with InTouch Access Anywhere. For details, see **Configuring a Firewall Program Exception** in the *InTouch Access Server Administrator Manual*.

## Secure Gateway Installation

This section describes the procedure to install the Secure Gateway on a computer running a supported version of Windows server. The Secure Gateway supports other installation configurations. For more information, see **Other Secure Gateway Installation Configurations** in the *InTouch Access Anywhere Secure Gateway Administrator Manual*.

After verifying all installation prerequisites, start the installation procedure.

**Note**: Secure Gateway cannot be upgraded by installing a newer version on a computer hosting an existing version. The existing version of Secure Gateway must be uninstalled first before attempting to install another version on the same computer. To uninstall Secure Gateway, see Uninstall a System Platform Component.

**To install InTouch Access Anywhere Secure Gateway**

1. Insert the System Platform DVD in your computer and run **setup.exe**.

2. Select **Product-Based Selection**.

3. Select **InTouch Access Anywhere Secure Gateway**, then click **Next**.
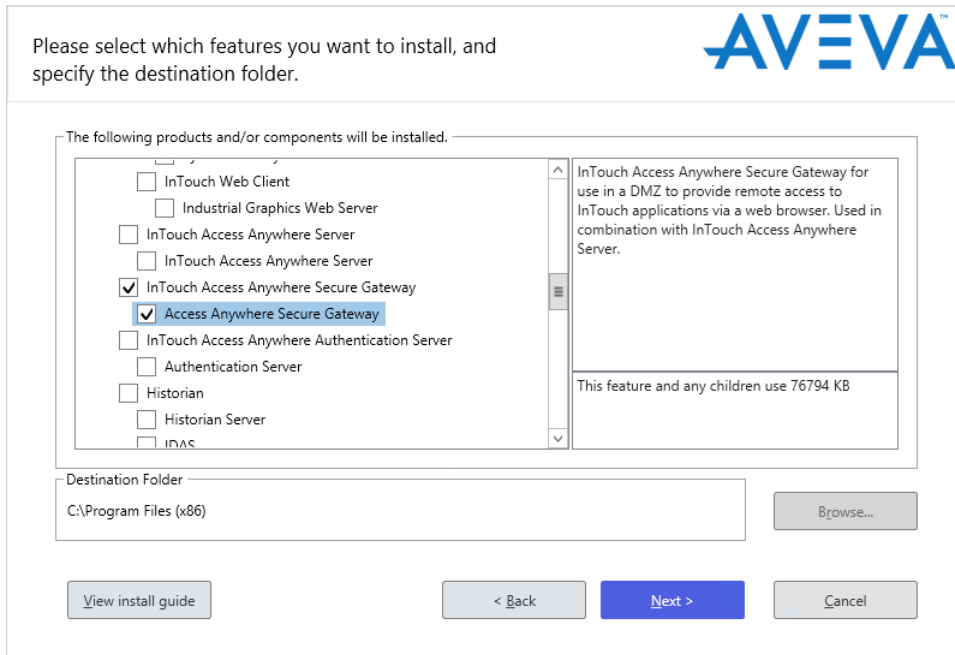


4. A checkbox appears that lets you customize installation. Select this if you wish to change the default installation folder.

   Otherwise, the Secure Gateway is installed to the default installation folder, C:\Program Files (x86).

5. Accept the license agreement by selecting the **I have read and accept the terms of the license agreement** option, and then click **Agree.**

   The **Ready to Install the Application** screen appears.

6. Review the installation details and click **Install**.

7. Click **Finish** after the installer indicates that the **Installation has completed successfully**.

## Configuring Ports for the InTouch Access Anywhere Secure Gateway

The InTouch Access Anywhere Secure Gateway uses several ports for communication. The following ports are used and must be configured on the computer hosting the Secure Gateway if a conflict exists:

- Port 443 (default): This is a dedicated port between the Secure Gateway Server and the external network. Check for port conflicts, and change port numbers if necessary. This is a common port that is also used by:

- Microsoft Internet Information Services (IIS).

- Remote Desktop, if Remote Desktop itself is enabled.

- System Management Server, if a System Platform product (Application Server, InTouch HMI, Historian, etc.) is installed on the same computer as the Secure Gateway Server.

- Port 8080: A port between the Secure Gateway Server and the InTouch Access Anywhere Server. The default port number is 8080, and can be changed.

- Port 80: The Secure Gateway includes an HTTP proxy that listens on port 80 by default. The port can be disabled after installing the Secure Gateway.

**Resolving Secure Gateway Port Conflicts**

A complete list of ports used by System Platform products and components is provided in an Appendix to this document: Ports Used by System Platform Products. Refer to that list when modifying default port settings to ensure that you are not creating a new conflict.

The System Management Server is a required component for running System Platform products. By default, it uses port 443, the same as the Secure Gateway default. Therefore, a conflict results if you are installing any other System Platform component products on the same node as the Secure Gateway. You must change the port number for either the System Management Server or the Secure Gateway. If you change the System Management Server port, you must also change the port number for the System Monitor. In addition, other System Platform nodes must be configured to use the same System Management Server port.

- Port assignments for both the System Management Server and the System Monitor can be changed during System Platform configuration, immediately following installation. See Configuring the System Management Server and Configuring the AVEVA System Monitor for more information about changing the port numbers for these components.

- To change the port number for the InTouch Access Anywhere Secure Gateway:

  a. Locate the Secure Gateway configuration file, **EricomSecureGateway.Config** and open it for editing. The default file location is:
  C:\Program Files (x86)\Wonderware\InTouch Access Anywhere Secure Gateway\InTouch Access Anywhere Secure Gateway

  b. Change the value for the SecuredPort to a different, unused port number. The Secure Gateway does not permit port sharing.

  c. Save the file.

- Refer to the *InTouch Access Anywhere Secure Gateway Administrator Guide*, located in the AVEVA Documentation folder for additional information.

- If Microsoft IIS is running on the same server that will host the Secure Gateway, either change the IIS ports to values other than 80 and 443, or change the Secure Gateway port to a value other than 443 and disable the HTTP auto redirect feature after the installation. If there is a port conflict on either the HTTP or HTTPS port, the Secure Gateway does not operate properly.

# Install the Secure Gateway and Authentication Server Separately or Together

The Authentication Server provides an additional layer of security by authenticating end-users before they can contact the Access Anywhere server. When the Authentication Server is enabled, only domain users will be able

to authenticate. Local system users (such as Administrator) will not be able to logon through the Authentication Server. The Authentication server is an optional InTouch Access Anywhere component and is disabled by default.

The Secure Gateway and Authentication servers can be installed separately or together on one of the supported Windows Server operating systems, or on a Windows workstation running 64-bit versions of Windows 8.1 Professional or Enterprise, or Windows 10 Professional or Enterprise, Build 1909 and later. Follow these requirements when installing the Authentication server:

- The Authentication Server must be installed on a computer that is a member of the domain that it will use to authenticate users.

- The Authentication server can only be configured for one domain at a time.

- The Authentication server should be installed on the safe side of a firewall rather than the DMZ for best security practice.

**To install the Secure Gateway and Authentication server on the same or separate computers**

1. Log on as a Windows administrator of the computer that will host either the Secure Gateway, the Authentication server, or both.

2. Insert the System Platform DVD in your computer and run **setup.exe**.

3. Select **Product-Based Selection**.

4. Determine how you want to install the Secure Gateway and the Authentication server.

   **Install the Secure Gateway and the Authentication server on separate computers**

   - Install the Secure Gateway by following the steps described in [Secure Gateway Installation](#). The Authentication server must be configured by setting options from the Secure Gateway Configuration portal.

   - Install the Authentication server on another computer that meets the requirements listed above this procedure.

   **Install the Secure Gateway and the Authentication server together on the same computer**

   - Select the Secure Gateway and Authentication server options from the installation dialog box and following the installation instructions.
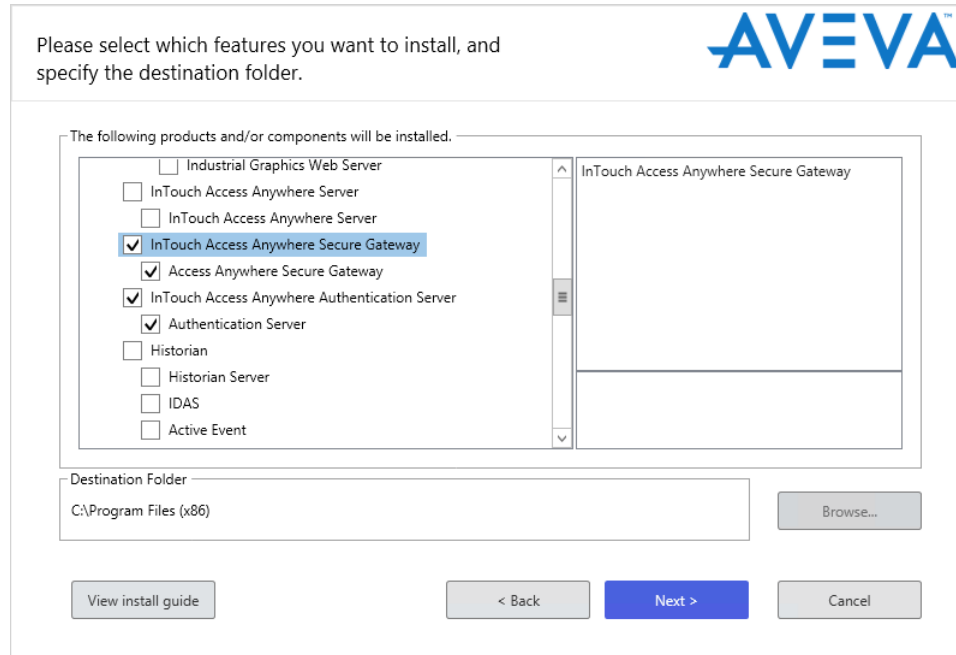
5. After installing the Authentication server and the Secure Gateway, see the section, **Built-In Authentication Server**, in the *InTouch Access Anywhere Secure Gateway Administrator Manual* for descriptions of the options to configure the Secure Gateway to work with an Authentication server.

## Install All Components on a Single Server

All InTouch Access Anywhere server components can be installed on a single computer running a supported version of Windows server. The Secure Gateway, the Authentication server, and the InTouch Access Anywhere server can be installed simultaneously.

**To install all InTouch Access Anywhere Components on a single server**

1. Log on as a Windows administrator on the computer where you are installing InTouch Access Anywhere.

2. Insert the System Platform DVD in your computer and run **setup.exe**.

3. Select **Product-Based Selection** and select the checkbox for each of the three InTouch Access Anywhere installation options:

   - Install InTouch Access Anywhere Server

   - Secure Gateway Installation

   - Install the Secure Gateway and Authentication Server Separately or Together
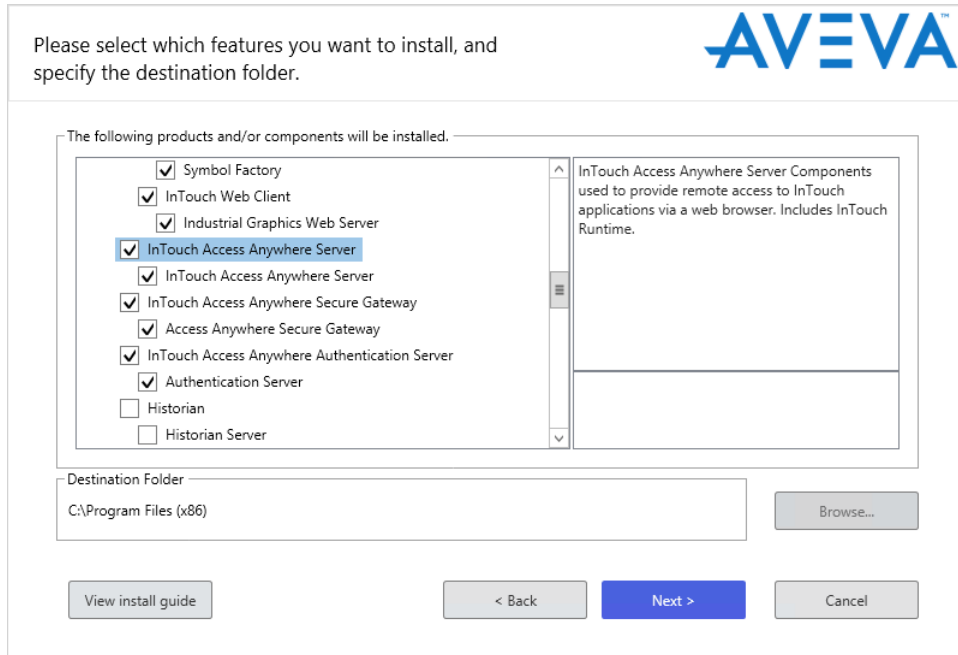
4. Click **Next** on the dialog box that shows all components have been select to be installed.

5. Select the check box that acknowledges you have read and accepted the terms of the license agreement and select **Agree**.

6. Click **Install** to begin installing the InTouch Access Anywhere components.

   A horizontal bar shows the progress of the installation.

7. Click **Finish** to complete the installation.

# Modifying an Installation

You can change the System Platform components installed on your computer. You can add new components or remove the existing ones. You can modify any component of System Platform.

You must have the installation DVD inserted in the DVD-ROM drive before you can modify a program.

**To modify an installation**

1. Select the **Modify** option from the System Platform **Modify, Repair or Remove Installation** dialog box. You can open the dialog by doing either of the following:

   ▪ Run Setup.exe from the System Platform installation DVD.

   ▪ Navigate to **Uninstall or Change a Program** in the Windows **Control Panel.** Then, select any System Platform component and then click the **Uninstall/Change** button.

   > **Note:** The name of the **Uninstall/Change** option may vary depending on which Windows operating system is installed on your computer.
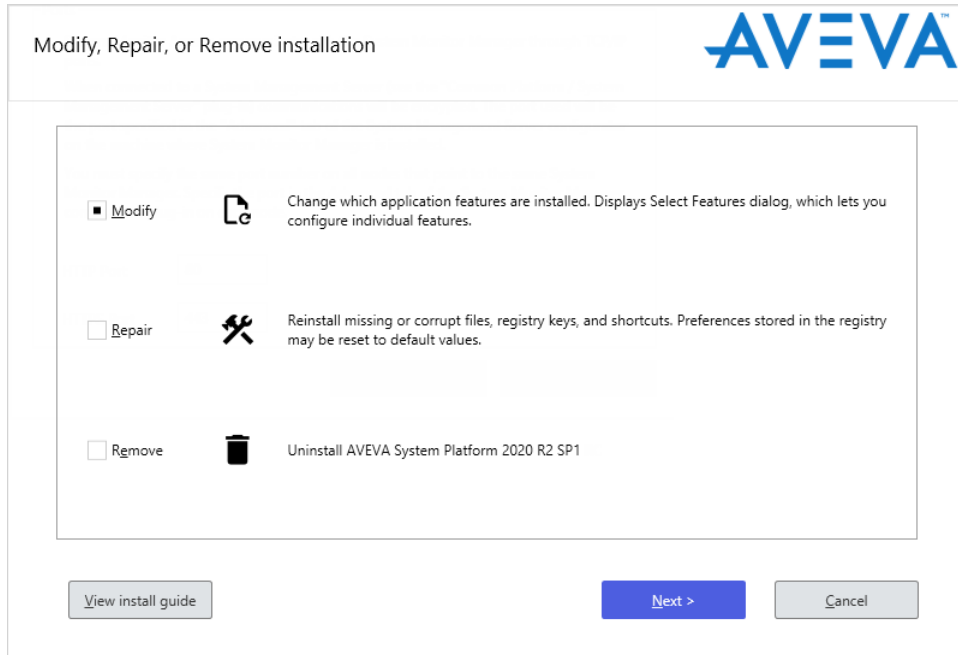
2. Click the **Modify** option, and then click **Next**.

3. A message describing functional changes to System Platform installation behavior, and considerations for existing projects, is displayed. Read and acknowledge this message, then click **Next** to proceed. The list of System Platform components appears.
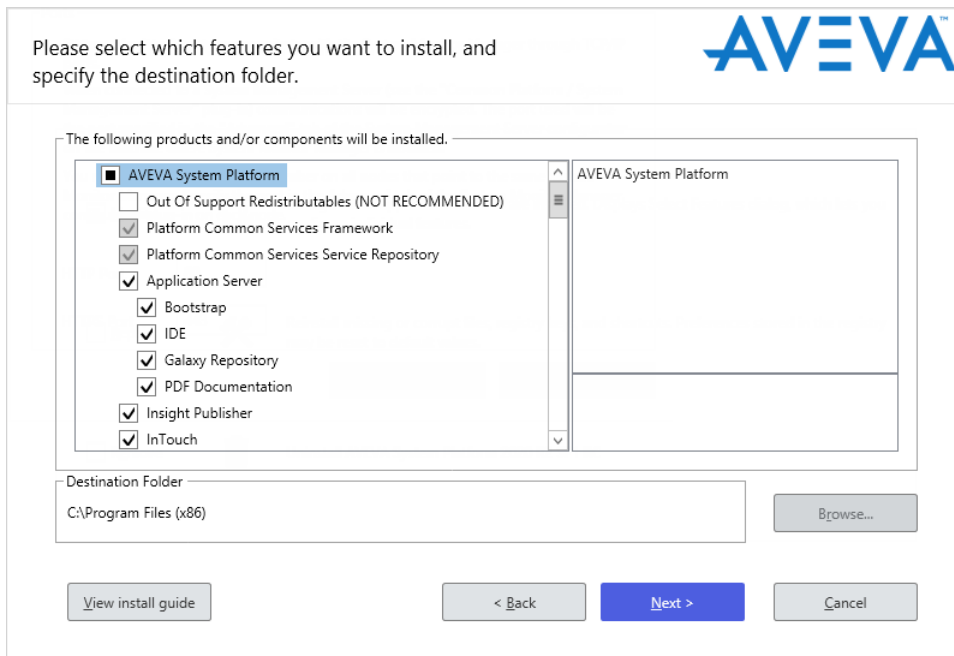


4. Select or clear the components that you want to add or remove, and then click **Next**. The verify change dialog box appears.

5. Click **Modify**. The selected components are added or removed. If the added components require configuration, the **Configurator** opens. If not, the complete modification dialog box appears. See Configuring System Platform Components for information about the **Configurator**.

6. Click **Finish**.

---

**Note:** The system may not prompt you to restart the system after Modify is successful. However, if you have added a new product or feature, a system restart is recommended.

---

# Repairing an Installation

You can repair the installation of any System Platform component to fix missing or corrupt files, registry keys or shortcuts. You can also reset the registry key to the default value.

You must have the installation DVD inserted in the DVD-ROM drive before you can repair a System Platform installation.

**To repair an installation**

1. Select the **Repair** option from the System Platform **Modify, Repair or Remove Installation** dialog box. You can open the dialog by doing either of the following:

   - Run Setup.exe from the System Platform installation DVD.

   - Navigate to **Uninstall or Change a Program** in the Windows **Control Panel.** Then, select any System Platform component and then click the **Uninstall/Change** button.

     ---

     **Note:** The name of the **Uninstall/Change** option may vary depending on which Windows operating system is installed on your computer.

     ---
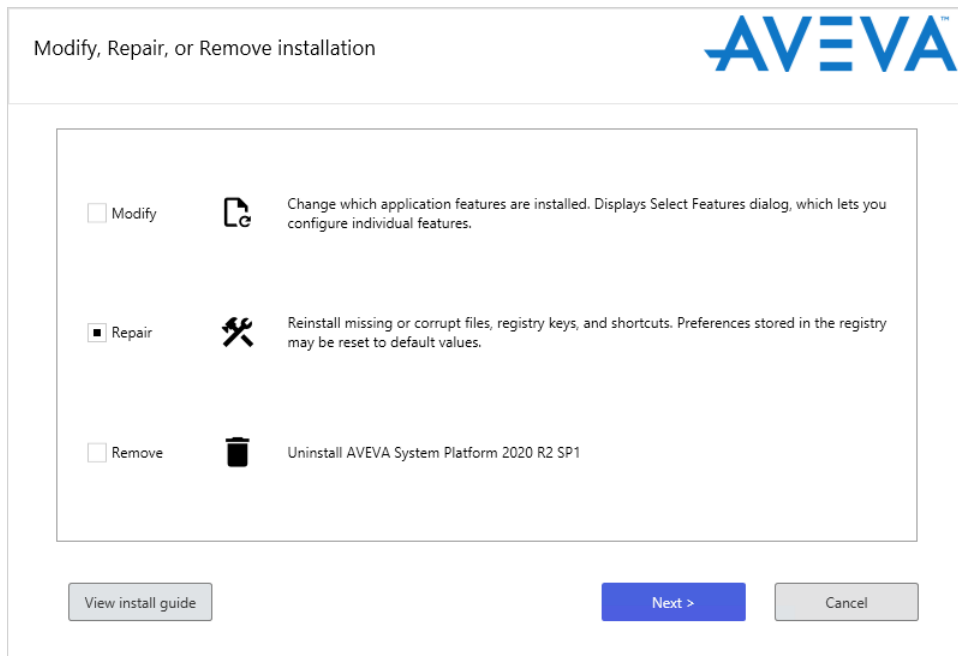


2. Select the **Repair** option, the click **Next**. The **Confirm Repair** dialog box appears.

Confirm Repair

Click Repair to repair the installation of AVEVA System Platform 2020 R2 SP1

Click Cancel to exit the wizard.

| View install guide | | < Back | Repair | Cancel |
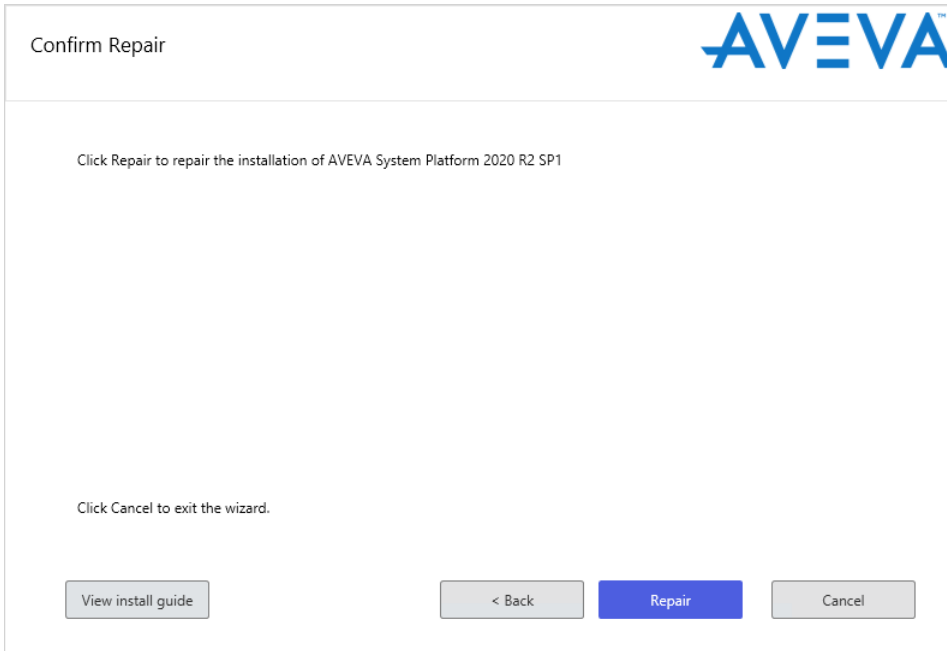
3. Click the **Repair** button. A message describing functional changes to System Platform installation behavior, and considerations for existing projects, is displayed. Read and acknowledge this message, then click **Next** to proceed.

4. If any System Platform services are running, the **Stop Running Services** dialog box appears. Click the **Stop Services** button to proceed.

Stop Running Services

The following services need to be stopped to proceed further.

| Service Name | Status |
|---|---|
| ArchestrA Platform Install Manager | Running |
| ArchestrA Watchdog Service | Running |
| InTouch IData Service | Running |
| AVEVA Historian Configuration | Running |
| AVEVA Historian Client Access Point | Running |
| AVEVA Historian System Driver | Running |
| AVEVA Historian Event System | Running |
| AVEVA Historian IOServer | Running |
| AVEVA Historian Manual Storage | Running |
| AVEVA Historian Storage | Running |
| AVEVA Historian Indexing | Running |
| SQL Server (MSSQLSERVER) | Running |
| AVEVA Historian Search Indexer | Running |

| Stop Services | | < Back | Next > | Cancel |

5. When all services stop, the **Next** button becomes active. Click the button to proceed.
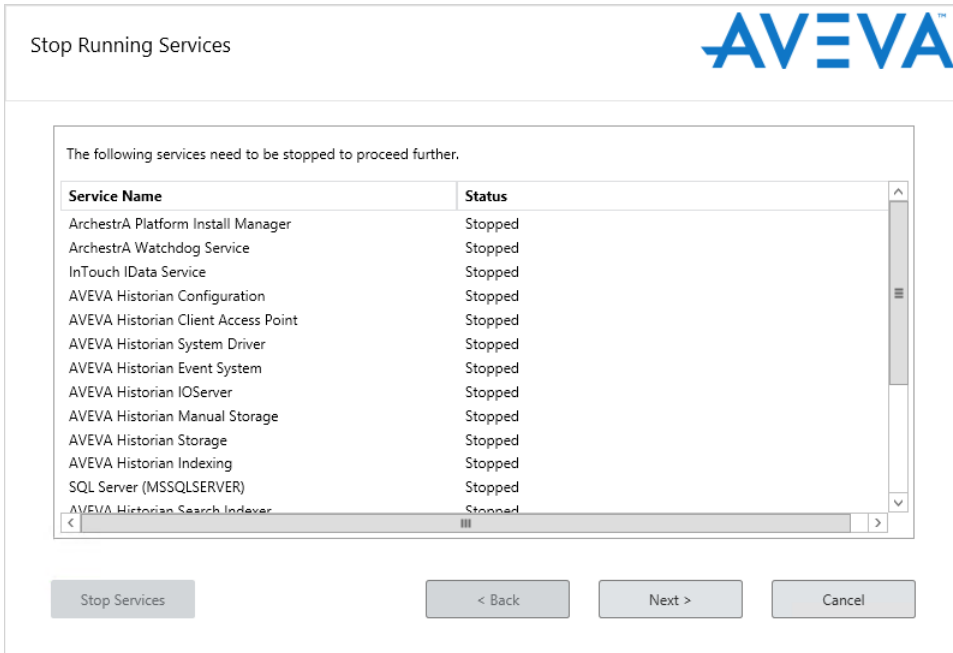
6. A progress bar is displayed as the system updates and repairs itself.

7. When the update has finished, the **Process Complete** dialog box appears.Click **Finish** to close the dialog box and complete the process.
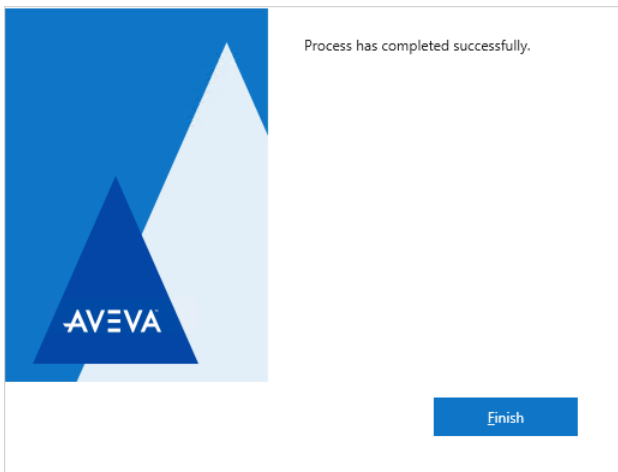


# Uninstalling AVEVA System Platform

## Uninstall a System Platform Component

You can uninstall any System Platform component that is installed on your computer.

**To uninstall a System Platform component**

1. Click the **Uninstall or Change a Program** option in Windows **Control Panel**. The list of software installed on your computer appears.

2. Select the System Platform component that you want to uninstall, and then click the **Uninstall/Change** button. The **Modify, Repair or Remove Installation** dialog box appears.
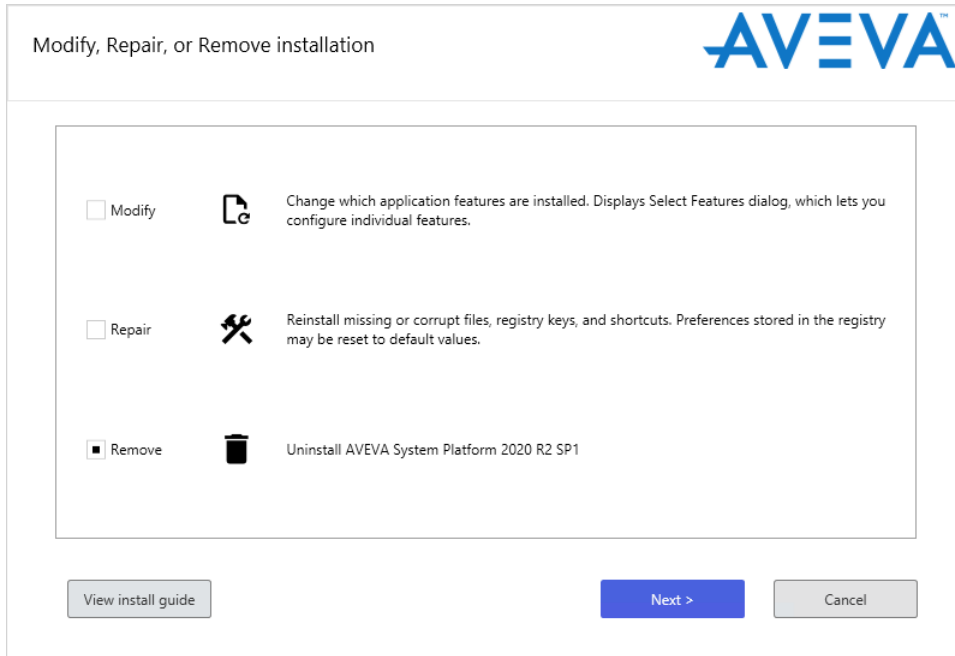


3. Click the **Remove** option, and then click **Next**. The confirmation dialog box appears.

4. Click **Uninstall**. The component is uninstalled and the complete uninstallation dialog box appears.

5. Click **Finish**.

## Uninstall All Components

**To uninstall AVEVA System Platform (remove all components)**

Begin by opening the Windows **Control Panel**, and select **Programs and Features**. Uninstall components by selecting the component, and then click **Uninstall**. You must uninstall components in the following order:

**Note:** Ignore components that are listed below if they have not been installed on your system.

1. AVEVA Application Server

2. AVEVA InTouch HMI

3. InsightPublisher

4. AVEVA Historian

5. AVEVA Historian Client

6. AVEVA Communications Drivers Pack

7. Platform Common Services

8. System Monitor Manager

9. System Monitor Agent Install Manager

10. AVEVA Enterprise License Manager

11. AVEVA Enterprise License Server

12. AVEVA Enterprise Licensing

13. AVEVA Enterprise Licensing (x86)

# Upgrading System Platform

Direct upgrade to System Platform 2020 R2 SP1 is supported from System Platform 2014 R2 SP1 and later versions.

The upgrade process lets you upgrade only components that were previously installed. You cannot choose to add components that were not already installed, and you cannot deselect components. That is, if a newer version of a component is included on the installation DVD, the previously installed component is automatically upgraded.

After the upgrade is complete, you can add new components or remove existing components, as needed.

**Important Upgrade Information**

- **64-bit operating system required:** A 64-bit operating system is required to install System Platform 2020 R2 SP1.

- **64-bit SQL Server required:** For components that require SQL Server, such as Application Server and Historian, you must have a 64-bit version of SQL Server installed.

- **.NET Framework:** System Platform 2020 R2 SP1 requires .NET Framework 4.8. If your system does not have this version or a newer version installed, the .NET Framework will be installed prior to product installation. A restart may be required, after which setup.exe will resume automatically. See System Platform Prerequisites for additional information.

- **Licensing Change:** If you are upgrading from System Platform 2014 R2 SP1, you will be changing to the new licensing system. This new "Activated License System" requires a License Server to be hosted on a machine that can be accessed by all nodes in the system. Additional license servers can be installed for more granular licensing management or redundancy.

  Since the License Server is a new component, it is not added during the upgrade process. Upgrade the Galaxy Repository node first, and then use the **Modify** workflow to add the License Server after the node has been upgraded. See License Installation and Activation for additional information.

  Only one License Server is required per overall system.

  **Note:** The Galaxy Repository node is the default installation location for the License Server. You can, however, select a different node, or install the License Server on a standalone node, depending on your system size and architecture.

- **Network Account:** In System Platform 2017 Update 2 and prior releases, the Network Account (previously called the ArchestrA User) was a member of the system Administrators group. Starting with System Platform 2017 Update 3, the Network Account was removed the Administrators group to enhance system security.

  When you upgrade from System Platform 2017 Update 2 or an earlier version, a security warning asks if you want to remove the Network Account from the Administrators group. This is the best option for security. However, you can leave the Network Account as a system administrator, if the account is used by another application and if removing administrator rights will affect that application.

- **AVEVA System Monitor:** The System Monitor Manager tracks the availability of the License Server and provides email notification of its status to ensure uninterrupted system operations. A System Monitor agent,

also called the Sentinel Agent, is installed on each node and communicates with the System Monitor Manager if there is an issue with the connection between the System Platform node and the License Server.

The System Monitor Manager is not automatically added during the upgrade process. To add the System Monitor Manager, upgrade the Galaxy Repository node first, and then use the **Modify** workflow to add the System Monitor Manager when the upgrade completes. The System Monitor agent is automatically added to each upgraded node. Configure the System Monitor agent on each remote node to point to the System Monitor Manager. See AVEVA System Monitor Installation for additional information.

Only one System Monitor Manager is required per overall system.

- **InTouch Access Anywhere:** If you plan to upgrade System Platform on a computer that has InTouch Access Anywhere Server or InTouch Access Anywhere Gateway installed, you must first uninstall the InTouch Access Anywhere Server or Gateway. Then, upgrade System Platform and finally, reinstall InTouch Access Anywhere. Note that the uninstall/reinstall process normally takes only several minutes.

- **Common Platform:** The System Management Server, a security component, was added for System Platform 2017 Update 3. If you are upgrading from a prior version that did not have the System Management Server, it is automatically installed on the GR node when you upgrade to System Platform 2020 R2 SP1. There should be only one System Management Server in your System Platform topology, and every node should be configured to point to it. See Configuring the System Management Server for additional information. If some nodes will not be upgraded, communication with non-upgraded nodes will continue to use legacy communication protocols.

  In multi-galaxy environments, configure only one GR node as the System Management Server, and configure the other nodes to point to it.

### About the Modify Workflow

The upgrade process can only upgrade System Platform components that are already installed on your system. Since upgrading may introduce new components that were not part of prior releases, you need to run setup.exe and launch the **Modify** option to install new components that may not have been available in prior versions of System Platform. The components that you may need to install through the **Modify** option include:

- AVEVA System Monitor Manager
- AVEVA License Server

### To add components through the Modify option

1. Upgrade the node and configure it.
2. Run the installation program again from the installation DVD (setup.exe).
3. Select the **Modify** option.
4. Select the component(s) you want to install.

### To upgrade a System Platform component

**Note:** Upgrade the GR node first, followed by remote IDE nodes, and then run-time nodes. See Upgrading an IDE-only Node and Upgrading Run-Time Nodes for additional information.

1. Insert the DVD into your DVD-ROM drive and run setup.exe to start the set-up program. The startup screen appears, followed by the upgrade feature dialog box that lists any prerequisites and products to be upgraded. If new version of the .NET Framework is required, it is installed first and then setup resumes after a restart.
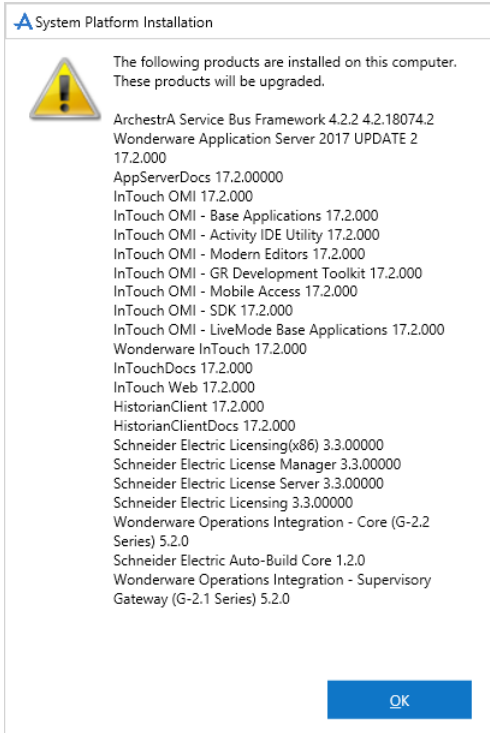
**Note:** You can only upgrade the products that are already installed, and you will not be able to install additional products during the upgrade process.

2. Click **OK** to proceed. A list of all System Platform components appears. The installed components that need to be upgraded are selected and disabled. You cannot clear these check boxes or select more components during the upgrade.
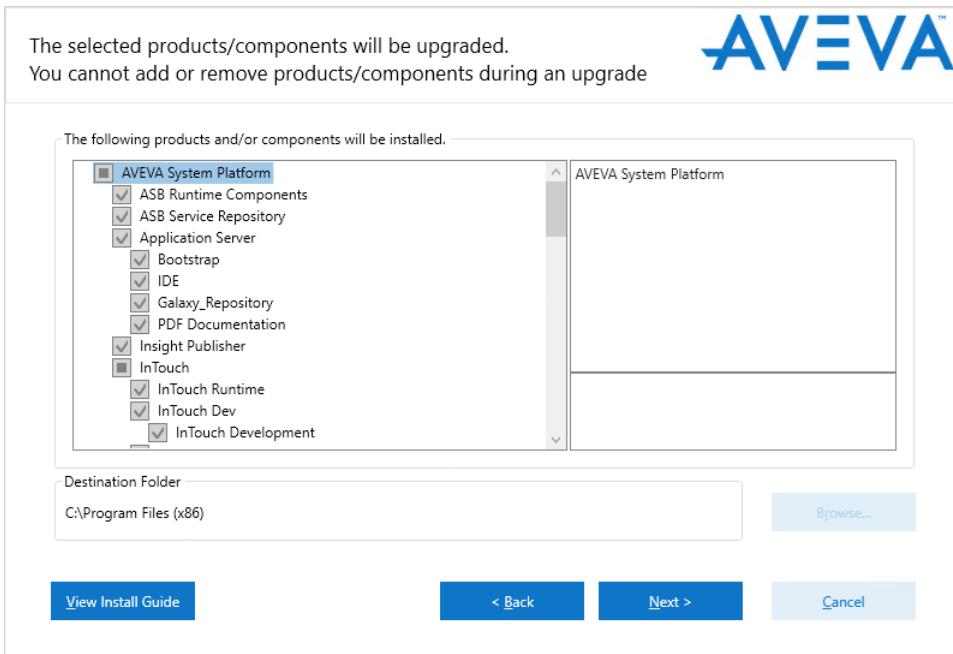


3. Click **Next**. If you are upgrading from System Platform 2017 Update 2 or a prior version, a security warning is displayed.

- To improve security, leave the checkbox selected (default option). This removes the Network Account from the system Administrators group.

- If you have other applications that use the Network Account, and the account needs Administrator access to function properly, deselect the checkbox. The Network Account permissions will not change.
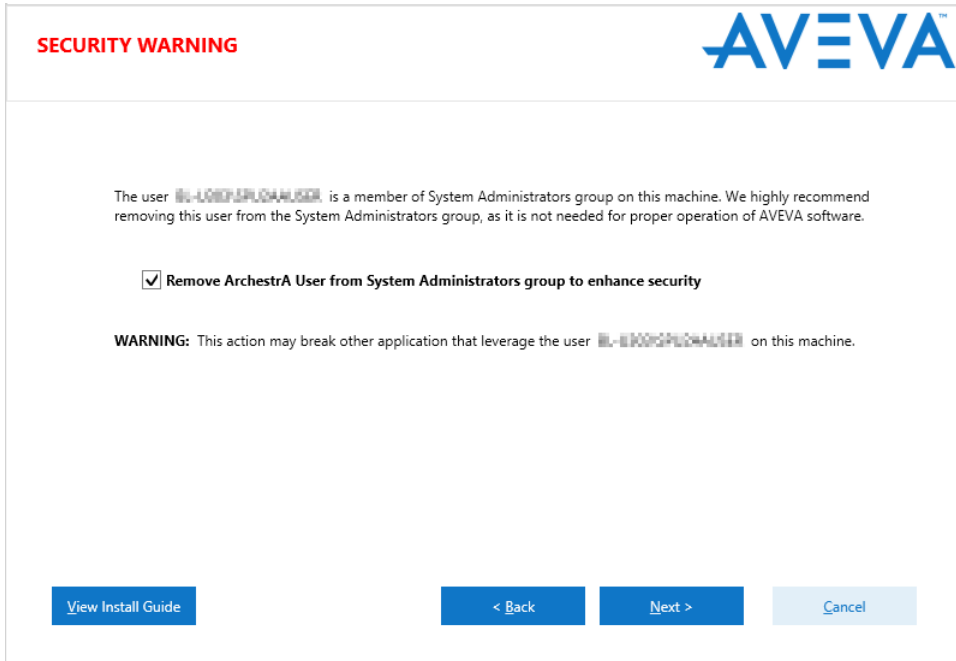


4. You may get a message to stop one or more running processes or services before proceeding, such as the ArchestrA Watchdog Service. If this occurs, click **Stop Services**, and when the processes stop, click **Next**.
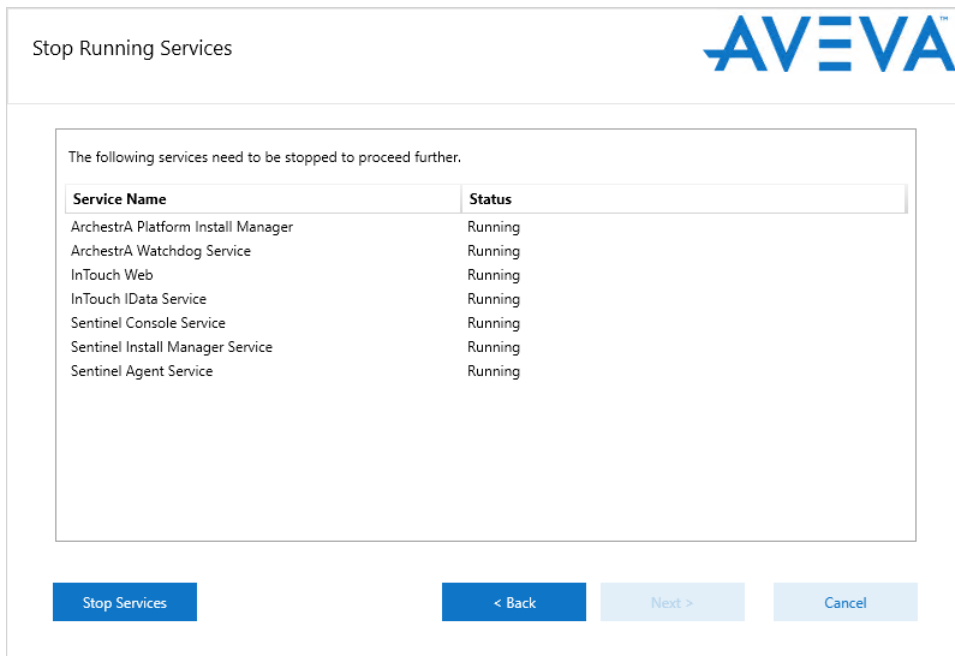


5. Another list of recommended steps to take before upgrading may be shown, such as backing up Galaxies. Complete the recommended steps, then click **Next**.

6. The upgrade dialog box appears.
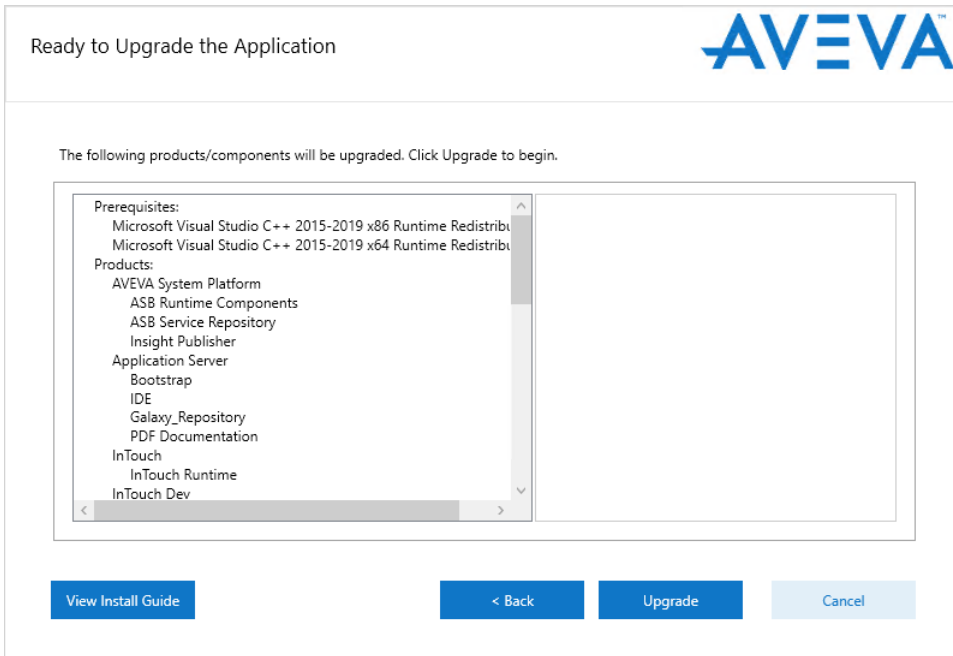


7. Click **Upgrade** to proceed with the upgrade. The progress bar appears.
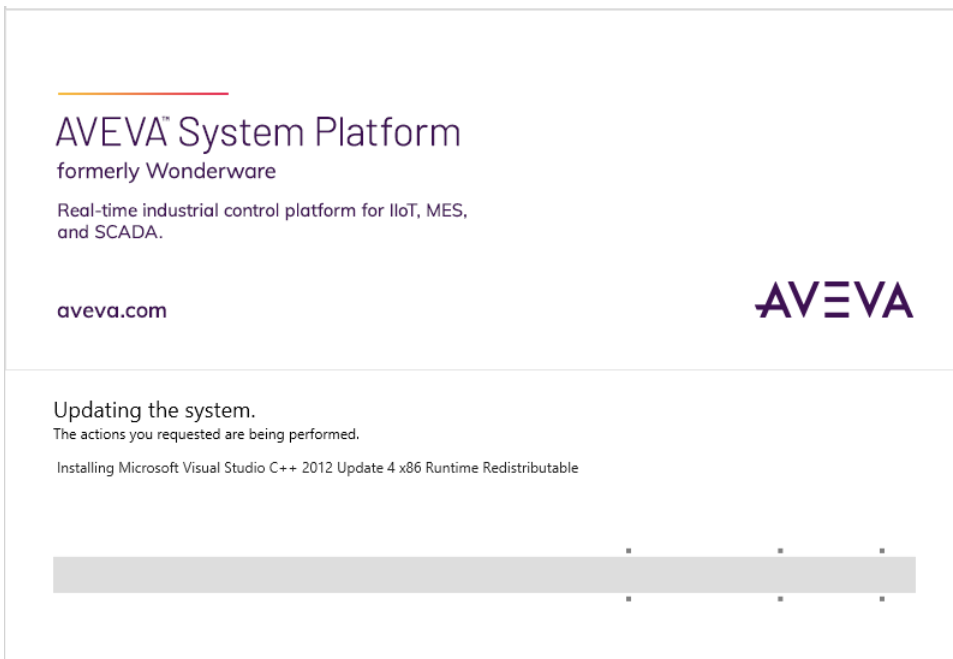


8. After the installation is over, the **Configurator** starts. Any items that were previously configured retain their configurations. If new items require configuration, configure them now. See Configuring System Platform Components for more information.

- Select **View Readme** for important information about System Platform 2020 R2 SP1, including hardware and software requirements, new features, and known and resolved issues.

**Note:** You may see a **Cybersecurity Notice** that instances of a Microsoft XML processing library were found. For information on removing MSMXML 4.0, see the Microsoft Support web page: https://support.microsoft.com/en-us/help/925672/ms06-061-security-update-for-microsoft-xml-core-services-4-0-sp2
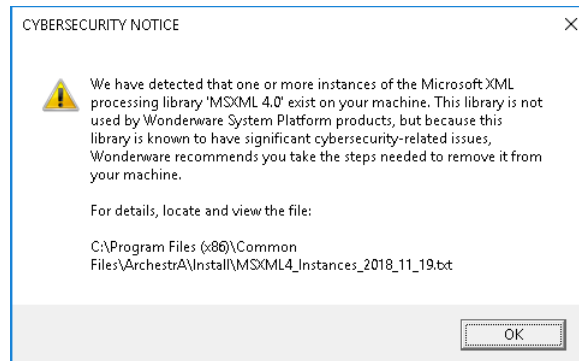


If you are upgrading from a prior version of Application Server, and a galaxy is deployed, the Galaxy Patcher will start as soon as you connect to the galaxy from the Application Server IDE. Undeployed galaxies are not patched until you connect to them.

**Important:** Galaxy patching may take several minutes. Do not shut down the node while the patching operation is in progress.

- If you are upgrading from System Platform 2014R2 SP1, a new icon for the **Application Manager** is installed on the desktop. Use Application Manager to select and run deployed AVEVA OMI ViewApps.

AVEVA

## Chapter 3

# Security and Permissions

## Enhanced Security for Connecting to a Galaxy

Users must belong to the OS group **aaConfigTools** to connect to a Galaxy from the IDE. Assign users to this group as needed through the **Windows Control Panel**.

## Modifying the Network Account

After you install the System Platform, you can use the **Change Network Account** utility to change or recreate the Network Account. The **Change Network Account Utility** is a tool to manage credentials for node-to-node communications between System Platform computers. See Network Account for more information. A short cut to the **Change Network Account** utility is created in the **AVEVA** folder after you install the System Platform products.

After opening the utility, select the domain name from the drop down menu if necessary. If the domain name does not appear on the drop down menu, enter the short domain name. Do not use the fully qualified domain name (FQDN). For example, use "DomainName" and not "DomainName.com" or "DomainName.local."

To run the utility from the command line, open the command window as Administrator. See Change the Network Account from the CLI for more information. You must have administrator privileges to run the utility through the GUI or from the command line.

**Important:** When you change or recreate the Network Account, a system restart is required. Close all applications and click OK to proceed.

**Note:** If you recreate the user account using the Change Network Account utility, the Microsoft Windows security component on the computer can take several minutes to update this information on the Galaxy Repository node. Until that occurs, inter-node communications may not function properly. Restarting the Galaxy Repository node updates this information immediately.

### Change the Network Account from the CLI

You can run the **Change Network Account** utility from the command line by invoking aaAdminUser.exe. If you open aaAdminUser.exe from a command prompt without any flags, it opens the Change Network Account GUI. If you open aaAdminUser.exe with flags, it runs from the command prompt. Any changes require that you restart the computer to complete the change.

The default installed location for aaAdminUser.exe is:
C:\Program Files (x86)\Common Files\ArchestrA.

**Note:** As is the case for the Change Network Account utility, you must have system administrator privileges to run aaAdminUser.exe from the command prompt.

Options you can specify with aaAdminUser.exe are:

| Option | Flag | Example |
| --- | --- | --- |
| Help | /h, -h, or /? | aaAdminUser.exe /h |
| User name | -u | aaAdminUser.exe **-u user** -p password |
| Account password | -p | aaAdminUser.exe -u user -**p password** |
| Create local account | -c | aaAdminUser.exe -user -p password **-c** |
| Domain account | -d | aaAdminUser.exe -user -p password **-d example.com** |
| Open GUI | <none> | When no flags are specified, the **Change Network Account utility (GUI) opens** |

# SQL Server Rights Requirements

When you install a Galaxy Repository or Historian node, the installation process creates or modifies new user groups, SQL Server logins, and a user account (Network Account). These provide support for Galaxy communications, system security, and connection to SQL Server. The new/modified SQL Server logins used by System Platform are:

- <NodeName>\aaAdministrators
- <NodeName>\aaGalaxyOwner
- NT AUTHORITY\SYSTEM

The Network Account, created when you installed Application Server, is required for Galaxy operations. This account:

- Is a member of the System Platform aaAdministrators group.
- Has one of the following SQL Server roles:
  - Has the SQL Server bulkadmin role, if Enhanced Security Mode is enabled (default).
  - Has the SQL Server sysadmin role, if Legacy Security Mode is enabled.

See [Network Account](#) and [Setting the SQL Server Security Mode](#) for additional information.

The automated process that creates the aaAdministrators group, Network Account, and aaGalaxyOwner user account also provides the rights required for operations within the GR. The aaAdministrators group, Network Account, and aaGalaxyOwner user account must all be present and enabled for Galaxy operations.

**Caution:** aaGalaxyOwner and ASBService are reserved OS user names. aaAdministrators and ASBSolution are reserved OS group names. Do not create users or groups with these names.

**Note:** The aaGalaxyOwner account is the owner (dbo) of all Galaxy databases in your system. It does not have a system login.

AVEVA™ System Platform Installation Guide
Chapter 3 – Security and Permissions

- If you accidentally delete the aaAdministrators group or the Network Account from the Windows operating system, you can run either the **Change Network Account** utility or the **SQL Access Configurator** to restore it. You can access these utilities from the **Start Menu**, under the **AVEVA** folder.

- If you accidentally delete the aaGalaxyOwner account from the Windows operating system, you must run the **SQL Access Configurator** to restore it.

- If you accidentally delete the aaAdministrators group, Network Account, or aaGalaxyOwner from the SQL Server security logons, you must run the **SQL Access Configurator** to restore it.

# Setting the SQL Server Security Mode

If you are a SQL administrator, you can use the **SQL Access Configurator** to set user privileges within SQL Server for accessing and using Galaxy databases (the Galaxy Repository). A short cut to the **SQL Access Configurator** is created in the **AVEVA** folder when you install **Application Server** or **Historian**.
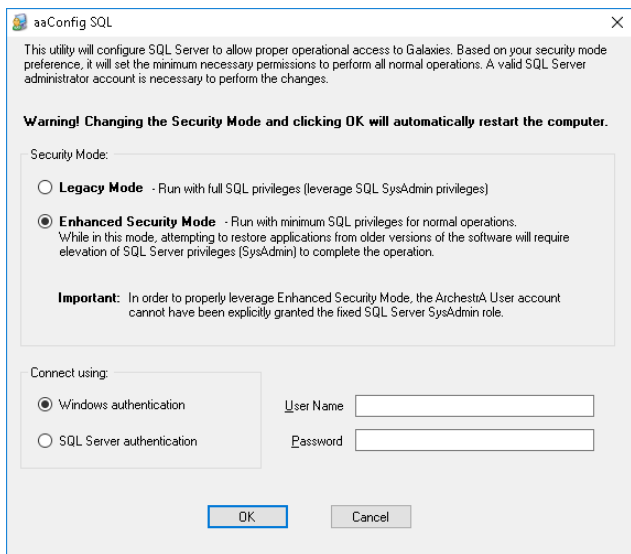


User privileges are determined by the security mode. Two security modes are available:

- **Legacy Mode.** Authenticated users have the sysadmin privilege and are not restricted from any SQL Server activity, including creating, modifying, and deleting any SQL Server database.

  Select Legacy mode to ensure that users can perform all Galaxy operations. If users will frequently be restoring Galaxies created with previous versions of Application Server, this may be the preferred setting.

- **Enhanced Security Mode.** This is the default setting. This mode removes the sysadmin privilege from Application Server users, and retains only the minimum privileges needed for normal operations.

  Select Enhanced Security mode for compliance with corporate or other IT security requirements or guidelines.

  If you use Enhanced Security Mode, you may be prompted to provide SQL sysadmin user credentials when restoring a Galaxy that was created with an older version of Application Server. You do not need sysadmin credentials to restore Galaxies created with the current version of Application Server.

  Enhanced Security Mode removes the SQL **sysadmin** role from, and adds the **bulkadmin** role to the following SQL logins:

- NTAUTHORITY\SYSTEM

- <NodeName>aaAdminstrators (local security group that contains the Network Account)

**To change the SQL security mode with the SQL Access Configurator**

WARNING! The SQL Access Configurator automatically restarts the computer to ensure system stability. If you press OK, you will not be able to cancel the restart.

1. Select the SQL Server security mode:

   - **Legacy Mode**.

   - **Enhanced Security Mode** (default).

2. Select the authentication type:

   - **Windows authentication**.

   - **SQL Server authentication**.

3. Provide SQL sysadmin login credentials (User Name and Password).

4. Click **OK**. The system will restart automatically.

5. Optional: If you selected **Enhanced Security Mode**, open SQL Server Management Studio and look under **Security\Logins.** Check that the NTAUTHORITY\SYSTEM and <NodeName>aaAdminstrators logins do **not** have the sysadmin server role.

Note: The system performs a check prior to changing to Enhanced Security Mode. This is to ensure that at least one account will exist with the SQL sysadmin privilege after the change. If the system check determines that no accounts with the SQL sysadmin privilege will remain after changing modes, an error message will be displayed and security will remain in Legacy Mode.

# Restoring Required SQL Server Accounts

If you delete the aaAdministrators group, Network Account, or the aaGalaxyOwner account, restore them by running the **SQL Access Configurator**. You do not have to do anything else to restore the missing group or account. The missing group or account is created automatically when you run the utility. Running the utility does force a system restart, however, even if you retain the same security configuration.

# Setting the FIPS Security Policy Option

Application Server does not support the FIPS (Federal Information Processing Standards) security policy option in Microsoft Windows.The Federal Information Processing Standards are United States Government standards that provide a benchmark for implementing cryptographic software. If your system has FIPS enabled in the Local Security Policy settings, you should disable it. The security setting for FIPS is listed under Security Settings> Local Policies> Security Options> System cryptography, or as part of Group Policy.

## Chapter 4

# Configuring SQL Server

## SQL Server Requirements

System Platform 2020 R2 requires a 64-bit version of SQL Server. In a typical configuration, you should install Microsoft SQL Server before you install Application Server. It is important to take into consideration the requirements of the different versions of SQL Server. Follow Microsoft installation instructions for your particular edition of SQL Server. See TechNote TN548, available on the AVEVA Global Customer Support web site, for detailed SQL Server installation instructions. While TechNote TN548 describes the installation process for SQL Server 2012, the installation process is similar for other versions of SQL Server.

If no version of SQL Server is installed on your system when you install System Platform, and you install a product or role that includes either Historian Server or a Galaxy Repository, you can choose to allow System Platform to automatically install SQL Server 2017 Express as it installs other prerequisites.

**Note:** SQL Server Express is limited for use with small installations only (25,000 I/O per node or less). For information about the versions of SQL Server supported by Application Server and other System Platform products, see the *System Platform Readme*.

**Supported SQL Server Versions (64-bit only)**

- SQL Server Express 2012 SP4-SSMSE (small systems only)
- SQL Server 2012 SP4 Standard or Enterprise
- SQL Server Express 2014 SP3-SSMSE (small systems only)
- SQL Server 2014 SP3 Standard or Enterprise
- SQL Server Express 2016 SP2 (or SP2 plus all cumulative updates)-SSMSE (small systems only
- SQL Server 2016 Standard or Enterprise SP2 (or SP2 plus all cumulative updates)
- [DEFAULT] SQL Server 2017 Express Core or Express with Advanced Tools and all cumulative updates (small systems only)
- SQL Server 2017 Standard or Enterprise with all cumulative updates
- SQL Server 2019 Express (small systems only)
- SQL Server 2019 Standard or Enterprise, no Service Pack

For more information about specific requirements for SQL Server configuration, see SQL Server Rights Requirements, or see the Microsoft documentation available online.

- A supported version of SQL Server must be installed on the computer designated as the Galaxy Repository (GR) node before you install Application Server. If you select a product or role that requires the Galaxy Repository, and SQL Server is not installed on the computer, you have the option to install SQL Server Express 2017.

- You cannot install and use a GR on a computer that has both Microsoft SQL Server 2000 and Microsoft SQL Server 2008 or later versions installed.

- The GR locks the SQL Server maximum memory usage to 65% of the computer's physical memory.

- TCP/IP must be enabled on the computer hosting a SQL Server database. The TCP/IP protocol setting can be verified from the SQL Server Network Configuration under SQL Server Configuration Manager. Do the following steps to enable TCP/IP.

**To enable the TCP/IP protocol for the SQL Server database instance**

1. Open the **SQL Server Configuration Manager**.

2. In the tree pane, click **SQL Server Services**.

3. If any services are displayed in the results pane, verify that each service under is in the **Running** state.

   If a service is **Stopped**, right-click the name of the service, and click **Start**.

4. In the tree pane, click **SQL Server Network Configuration** to expand it, and then click **Protocols** for **MSSQLServer/**<InstanceName>.

   If you specified the default instance during installation, the instance name will be **MSSQLSERVER**.

5. In the results pane, verify that each protocol is **Enabled**:

   - Shared Memory
   - Named Pipes
   - TCP/IP

     If **Disabled** appears, right-click on the protocol name and enable it.

6. In the tree pane, click **SQL Native Client Configuration** to expand it, and then click **Client Protocols**.

7. In the results pane, verify that each client protocol is **Enabled:**

   - Shared Memory
   - Named Pipes
   - TCP/IP

     If **Disabled** appears, right-click on the protocol name and enable it.

8. If you had to enable any services:

   a. Start **Task Manager**.

   b. Go to the **Services** tab.

   c. Restart **MSSQLServer/**<InstanceName>.

# Working with SQL Server Versions

The installation workflow will vary, depending on whether or not SQL Server is already installed. The version of SQL Server that is installed can also make a difference in the workflow. If SQL Server is not already installed, the System Platform installation program will install a 64-bit version of SQL Server Express. This is adequate for small configurations, but not for medium and large configurations. For these, install SQL Server before installing System Platform. The following workflow scenarios are described:

- SQL Server not found on node: small configuration

- SQL Server not found on node: medium and larger configurations

- Compatible version of SQL Server already installed

- New (untested) version of SQL Server already installed

- Incompatible version of SQL Server already installed

**Note:** Nodes are defined as follows: Small = up to 25,000 I/O per node; Medium = 25,000 to 50,000 I/O per node; Large = 50,000 to 400,000 I/O per node.

## SQL Server not found on node: small configuration

If you install the Application Server Galaxy Repository and SQL Server is not found on the computer, SQL Server 2017 Express (64-bit) is installed as part of the installation process. This version of SQL Server is suited for small configurations, and is best for a single-node system. A small configuration is defined as one that has less than 25,000 I/O. See the *System Platform Readme* for additional information.

## SQL Server not found on node: medium and larger configurations

For medium and larger systems, the following 64-bit versions of SQL Server are supported:

- SQL Server 2012 SP4 Standard or Enterprise

- SQL Server 2014 SP3 Standard or Enterprise

- SQL Server 2016 Standard or Enterprise SP2 (or SP2 plus all cumulative updates)

- SQL Server 2017 Standard or Enterprise with all cumulative updates

- SQL Server 2019 Standard or Enterprise, no Service Pack

See the *System Platform Readme* for additional information.

For more information about the comparative capabilities of SQL Server versions, see the following URL:

https://docs.microsoft.com/en-us/sql/sql-server/editions-and-components-of-sql-server-version-15?view=sql-server-ver15

## Compatible version of SQL Server already installed

If a compatible version of SQL Server is already installed, System Platform installation will continue without interruption (SQL Server Express 2017 is not installed).

## New version of SQL Server already installed

If a new version of SQL Server is already installed that has not yet been fully tested with System Platform 2020 R2 SP1 products, a warning is displayed stating that the installed SQL version has not yet been tested. You can proceed with the installation, but we recommend that you contact AVEVA Global Customer Support before proceeding to check if any issues have been found.

## Incompatible version of SQL Server already installed

If an older version of SQL Server is already installed that is not supported with the current version of System Platform products, installation will stop and a warning will be displayed stating the SQL Server version is not compatible. You must upgrade to a supported version of SQL Server before you can resume installation.

# Using a Non-Default Port for SQL Server

The default port for SQL Server is 1433. If you want to use a different port number, use **SQL Server Configuration Manager** to set the port number.

If you are using the SQLData object to store and retrieve data, you will need to enter the non-default SQL Server port number as you enter other database connection information. See the SQLData Object help file, available through the System Platform IDE, for additional information.

**To change to a non-default SQL Server port number**

1. If you are upgrading from a prior version of System Platform, upgrade all nodes. See Basic Upgrade Sequence for more information. If this is a new installation, continue to step 2.

2. Launch SQL Server Configuration Manager.

3. Select **SQL Server Network Configuration**, then select **Protocols for MSSQLSERVER**.

4. In the list of protocol names to the right, select and open **TCP/IP Properties**.
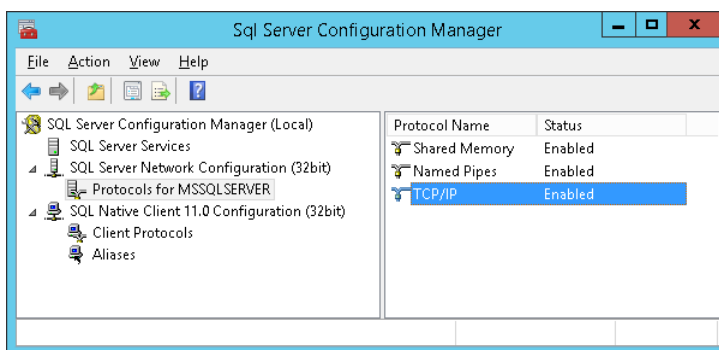


5. In the **TCP/IP Addresses** tab, scroll down to **IPAll**.
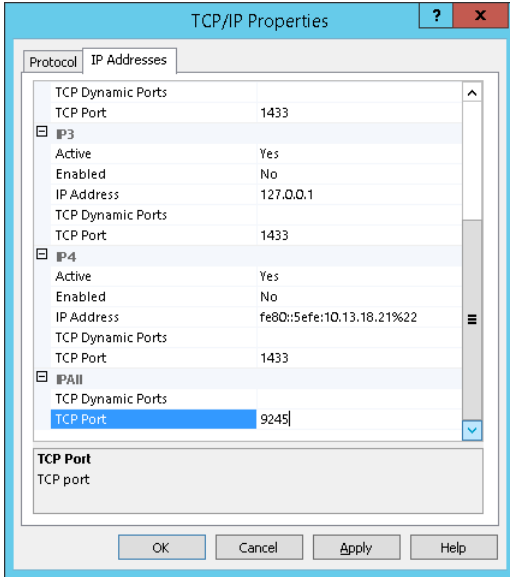
6.  Change the TCP Port number from 1433 to the desired number.

7.  Click **OK** or **Apply** to commit the changes.

8.  Reboot the GR node.

# Setting a Windows Firewall Exception for the SQL Server Port

You will need to set a Windows Firewall exception for a non-default SQL Server port number if you are using a remote node. Without access through the firewall, remote nodes will be unable to connect to the database.

**To allow access through the Windows Firewall**

1.  Open **Allow an app through Windows Firewall**.

2.  Select SQLServer from the list of applications. Double click to open the **Edit a Port** window.

3.  Change the port number to match the port number listed in **SQL Server Configuration Manager**.

4.  Click **Network types...** and select the checkbox that matches the network type to which you are connected (typically Domain).

# AVEVA

# AVEVA Application Server Upgrade

Direct upgrade to AVEVA Application Server 2020 R2 SP1 is supported from Application Server 2014 R2 SP1 and later versions.

## About Upgrading Application Server

**Important:** Direct upgrade to Application Server 2020 R2 SP1 is supported from Application Server 2014 R2 SP1 and later, up through and including Application Server 2020. Your system must meet the minimum system requirements, including operating system version, SQL Server version, and .NET Framework version. Note that only 64-bit operating systems are supported. For more information, see Supported Operating Systems for System Platform 2020 R2 SP1, the System Platform Readme, and the website.

**Note:** Users must belong to the OS group **aaConfigTools** to connect to a Galaxy from the IDE. Assign users to this group as needed through the **Windows** Users must belong to the OS group **aaConfigTools** to connect to a Galaxy from the IDE. Assign users to this group as needed through the **Windows Control Panel**.

**Important Upgrade Information**

- **64-bit operating system required:** A 64-bit operating system is required to install System Platform 2020 R2 SP1.

- **64-bit SQL Server required:** For components that require SQL Server, such as Application Server and Historian, you must have a 64-bit version of SQL Server installed.

- **.NET Framework:** System Platform 2020 R2 SP1 requires .NET Framework 4.8. If your system does not have this version or a newer version installed, the .NET Framework will be installed prior to product installation. A restart may be required, after which setup.exe will resume automatically. See System Platform Prerequisites for additional information.

- **Licensing Change:** If you are upgrading from System Platform 2014 R2 SP1, you will be changing to the new licensing system. This new "Activated License System" requires a License Server to be hosted on a machine that can be accessed by all nodes in the system. Additional license servers can be installed for more granular licensing management or redundancy.

  Since the License Server is a new component, it is not added during the upgrade process. Upgrade the Galaxy Repository node first, and then use the **Modify** workflow to add the License Server after the node has been upgraded. See License Installation and Activation for additional information.

  Only one License Server is required per overall system.

**Note:** The Galaxy Repository node is the default installation location for the License Server. You can, however, select a different node, or install the License Server on a standalone node, depending on your system size and architecture.

- **Network Account:** In System Platform 2017 Update 2 and prior releases, the Network Account (previously called the ArchestrA User) was a member of the system Administrators group. Starting with System Platform 2017 Update 3, the Network Account was removed the Administrators group to enhance system security.

  When you upgrade from System Platform 2017 Update 2 or an earlier version, a security warning asks if you want to remove the Network Account from the Administrators group. This is the best option for security. However, you can leave the Network Account as a system administrator, if the account is used by another application and if removing administrator rights will affect that application.

- **AVEVA System Monitor:** The System Monitor Manager tracks the availability of the License Server and provides email notification of its status to ensure uninterrupted system operations. A System Monitor agent, also called the Sentinel Agent, is installed on each node and communicates with the System Monitor Manager if there is an issue with the connection between the System Platform node and the License Server.

  The System Monitor Manager is not automatically added during the upgrade process. To add the System Monitor Manager, upgrade the Galaxy Repository node first, and then use the **Modify** workflow to add the System Monitor Manager when the upgrade completes. The System Monitor agent is automatically added to each upgraded node. Configure the System Monitor agent on each remote node to point to the System Monitor Manager. See AVEVA System Monitor Installation for additional information.

  Only one System Monitor Manager is required per overall system.

- **InTouch Access Anywhere:** If you plan to upgrade System Platform on a computer that has InTouch Access Anywhere Server or InTouch Access Anywhere Gateway installed, you must first uninstall the InTouch Access Anywhere Server or Gateway. Then, upgrade System Platform and finally, reinstall InTouch Access Anywhere. Note that the uninstall/reinstall process normally takes only several minutes.

- **Common Platform:** The System Management Server, a security component, was added for System Platform 2017 Update 3. If you are upgrading from a prior version that did not have the System Management Server, it is automatically installed on the GR node when you upgrade to System Platform 2020 R2 SP1. There should be only one System Management Server in your System Platform topology, and every node should be configured to point to it. See Configuring the System Management Server for additional information. If some nodes will not be upgraded, communication with non-upgraded nodes will continue to use legacy communication protocols.

  In multi-galaxy environments, configure only one GR node as the System Management Server, and configure the other nodes to point to it.

### About the Modify Workflow

The upgrade process can only upgrade System Platform components that are already installed on your system. Since upgrading may introduce new components that were not part of prior releases, you need to run setup.exe and launch the **Modify** option to install new components that may not have been available in prior versions of System Platform. The components that you may need to install through the **Modify** option include:

- AVEVA System Monitor Manager
- AVEVA License Server

### To add components through the Modify option

1. Upgrade the node and configure it.

2. Run the installation program again from the installation DVD (setup.exe).

3. Select the **Modify** option.

4. Select the component(s) you want to install.

If you plan to upgrade system components in addition to Application Server, keep the following in mind:

- After Application Server is installed, operating system migration is not supported, with the following upgrade exceptions:

  - Windows 8.1 to Windows 10

  - Windows Server 2012 to Windows Server 2012 R2

  Other than the above exceptions, System Platform products must be uninstalled prior to upgrading the operating system.

- You can upgrade SQL Server after Application Server is installed. Refer to Microsoft's SQL Server resources for guidelines and procedures.

  To upgrade SQL Server after Application Server is installed, we recommend that you undeploy any galaxies deployed on the relevant computer, and that you undeploy all Platform Common Services. For more information, see the *Application Server User Guide*.

You can upgrade the following Application Server components:

- Bootstrap

  You will see a warning message if you attempt to upgrade a computer with a deployed WinPlatform. You have the choice to continue with the upgrade or to cancel. If you continue with the Bootstrap upgrade, the deployed WinPlatform object is removed from run time and upgraded.

  If an InTouchViewApp instance is deployed for a managed InTouch application, the folder is undeployed and deleted. You are prompted to stop InTouch WindowViewer from running the managed application.

- IDE and Bootstrap

  You will see a warning message if you attempt to upgrade a computer with a deployed WinPlatform. You have the choice to continue with the upgrade or to cancel. If you continue with the upgrade, the current IDE and Bootstrap are removed and the new versions are installed.

  If an installed InTouchViewApp instance is deployed for a managed InTouch application, the folder is undeployed and deleted. You are prompted to stop InTouch WindowViewer from running the managed application.

- Galaxy Repository (GR) and Bootstrap

  You will see a warning message if you attempt to upgrade a computer with a deployed WinPlatform or a client application is connected to the GR node. You can choose to continue with the upgrade or to cancel. If you continue, the components are removed and upgraded.

  Upgraded IDE/Client nodes cannot connect to a non-upgraded GR node. The GR node is undeployed before it is upgraded.

- IDE, GR, and Bootstrap

  A warning message is displayed if you attempt to upgrade a computer with a deployed WinPlatform or if a client application is connected to the GR node. You can choose to continue with the upgrade or to cancel. If you continue, all components are removed and upgraded.

- Run-time node

  Upgrading the Bootstrap on any computer removes the running WinPlatform and AppEngine. Both of these system objects are marked as undeployed if they are running on any Galaxy node.

  **Note:** No system objects are removed on non-GR nodes when migrating from earlier versions of Application Server.

If a remote node is disconnected from the GR node, or if you upgrade the remote node before you upgrade the GR node, the remote Platform is not marked as undeployed. You must undeploy and redeploy the Platform.

The run-time functionality of Application Server continues throughout the upgrade process, except during a run-time node upgrade. Configuration, however, must be done using components that are at the same version level. For example, you cannot use the Galaxy Browser in the InTouch HMI on a non-upgraded node to view or select attributes from an upgraded Galaxy. You can, though, view or modify run-time data using an InTouch window or the Object Viewer.

Special considerations apply if you are upgrading both the Application Server and the Historian. For more information about upgrading the Historian, see <u>Upgrading from a Previous Version</u>.

## Windows Upgrades

If you plan to upgrade system components in addition to Application Server, keep the following in mind:

After Application Server is installed, operating system migration is not supported, with the following upgrade exception:

- Windows 8.1 to Windows 10
- Windows Server 2012 to Windows Server 2012 R2

Other than the above exception, System Platform products must be uninstalled prior to upgrading the operating system.

## SQL Server Upgrades

You can upgrade SQL Server after Application Server is installed, provided that the version of SQL Server that is installed is supported by Application Server. Refer to Microsoft's SQL Server resources for guidelines and procedures.

To upgrade SQL Server after Application Server is installed, we recommend that you undeploy any galaxies deployed on the relevant computer, and that you undeploy all Platform Common Services (previously called ASB services). For more information, see the *Application Server User Guide*.

## Issues with Legacy Common Components

Application Server uses the latest version of the System Platform common components, which are installed to the following folder:

C:\Program Files (x86)\Common Files\ArchestrA

Legacy common components are installed to the following folder:

C:\Program Files (x86)\FactorySuite\Common

It is possible to install duplicate common components on a computer if you install an System Platform product that still uses the legacy common components after you install Application Server. Unexpected behavior can

occur if duplicate common components are installed. The system components may not run properly, or may not run at all. Contact technical support for further assistance.

# Basic Upgrade Sequence

**Important:** Back up the Galaxy before starting an upgrade. Also, upload any run-time changes for critical objects. You cannot upload any run-time change from non-upgraded nodes after you upgrade the system.

.NET Framework 4.8 is installed if it or a later version is not already present. You will be prompted to restart your computer after the .NET framework is installed.

The basic upgrade steps are:

1. **Upgrade your hardware and prerequisite software** such as the operating system or Microsoft SQL Server to the required versions. For information on hardware and software requirements, see the *System Platform Readme* file.

   If you are upgrading the SQL Server database on the GR node, you must undeploy the GR node before starting the SQL Server upgrade.

2. **Upgrade and configure the GR node.** If you are upgrading from System Platform 2017 Update 2 or prior version, the Common Platform System Management Server is automatically installed on the GR node. For more information, see Upgrading a Galaxy Repository Node.

3. **Upgrade and configure at least one IDE installation.** If you upgrade the GR node, that IDE installation is upgraded. However, if you have any IDE-only nodes, you will have to upgrade them separately. For more information, see Upgrading an IDE-only Node.

4. **Migrate the Galaxy database.** Connect to the upgraded GR node from the upgraded IDE to migrate the galaxy to the new version automatically.

5. **Deploy the GR Platform.**

6. **Upgrade and configure run-time nodes.**

   ▪ Upgrade non-redundant run-time nodes one at a time and redeploy them. For more information, see Upgrading Run-Time Nodes.

   ▪ Upgrade redundant pairs one at a time. For more information, see Upgrading Redundant Pairs.

If you upgrade a remote Platform node before you migrate the Galaxy database, the remote Platform and hosted objects show the software upgrade pending icon after you migrate and deploy the Galaxy. To resolve this, undeploy and redeploy the remote Platform.

**Important:** After you have upgraded the GR node to Application Server 2020 R2 SP1, you will not be able to deploy or undeploy from the GR node to non-upgraded remote nodes. Also, an IDE node that has been upgraded will not be able to connect to a GR node that has not been upgraded.

**Note:** As long as the operating system and SQL requirements are met, upgrade is supported.

# Upgrading a Galaxy Repository Node

**Important:** Upgrade the GR node before upgrading other nodes.

When you upgrade a GR node, the local Platform and all hosted objects are undeployed and the database schema is migrated from the existing schema to the Application Server 2020 R2 SP1 schema. Existing data from the GR is also migrated to the new schema.

You must upgrade all Application Server components (IDE, Bootstrap, and GR) to the same version that are installed on the GR node.

### SQL Server Considerations

If the GR node contains less than the recommended RAM amount, system performance may be impacted as SQL Server will use more CPU to compensate for the lower amount of available memory. To improve system performance, set the SQL Server minimum memory (min server memory) to 1/3 of total physical memory. See the *Application Server User Guide*, "Allocating Galaxy Repository Node Memory," for additional information.

### To upgrade the GR node

1. Review the status of objects deployed in the system and take appropriate action, if needed.

2. Run Setup.exe from the DVD. See Upgrading System Platform for information about the installation process.

   **Note:** If you are upgrading from System Platform 2014 R2 SP1, the License Server and Manager will be automatically selected and installed during the upgrade the process (GR node only). If you are upgrading from System Platform 2017 Update 2 or earlier, you can optionally add the **AVEVA System Monitor** at this point. Adding or deleting other components requires that you run the **Modify** workflow after the upgrade process is complete. Components that cannot be selected or deselected are locked and can only be added or removed through the **Modify** workflow. See Modifying an Installation for more information.

3. When the **Installation Complete** dialog box appears, click **Configure** to continue. See Configuring System Platform Components for more information.

   **Important:** Configure all GR nodes in multi-galaxy environments to point to a single System Management Server.

4. Close the **Configurator** and restart the computer to complete the upgrade. See System Restart after Configuration.

5. When the GR node has been upgraded, open the IDE and connect to the galaxy. The galaxy will be automatically migrated to System Platform 2020 R2 SP1.

   **Note:** If you are using a remote IDE node to connect to the galaxy, make sure that you have upgraded the IDE node before connecting to the galaxy.

## Upgrading an IDE-only Node

**Important:** Upgrade the GR node before upgrading IDE-only nodes.

If you have IDE-only installations on nodes other than the GR node, you need to upgrade them separately.

**Important:** An IDE node that has been upgraded will not be able to connect to a GR node that has not been upgraded. Conversely, an IDE node that has not been upgraded cannot connect to a GR node that has been upgraded.

### To upgrade an IDE-only node

1. Run Setup.exe from the DVD. See Upgrading System Platform for information about the installation process.

   When the **Installation Complete** dialog box appears, click **Configure** to continue.

2. **Configuration:** Configure licensing, the System Management Server, and other installed features, such as the Historian and the InTouch Web Client.

   ▪ Configure the System Management Server to point to the GR node. See [Configuring the System Management Server](#) for additional information.

   ▪ Under AVEVA System Monitor, enter the name of the node that has the System Monitor Manager installed. By default, it is installed on the GR node. See [Advanced System Monitor Configuration](#) for additional information.

3. When prompted, click **Restart Now** to complete the upgrade.

# Migrating the Galaxy Database

To migrate the database:

- The IDE you use to migrate the database must be the current version.

- The GR node must already be upgraded to the current version.

Make sure that all connections to the Galaxy database are closed before migrating the database.

After you migrate the Galaxy, deployed objects on a non-upgraded node are marked with pending software upgrade status.

### SQL Server Considerations

If the GR node contains less than the recommended RAM amount, system performance may be impacted as SQL Server will use more CPU to compensate for the lower amount of available memory. To improve system performance, set the SQL Server minimum memory (min server memory) to 1/3 of total physical memory. See the *Application Server User Guide*, "Allocating Galaxy Repository Node Memory," for additional information.

### To migrate the Galaxy database

1. Start the IDE.

2. Connect to the Galaxy database to migrate. You are prompted to migrate it.

3. Follow the prompts to complete the migration.

### Migration errors

Migration of a very large Galaxy may fail, with various (and sometimes misleading) warnings and errors displayed in the Logger. This is due to the Galaxy database transaction log expanding over its maximum allocated size.

Before making the changes described here, use the Event Viewer to check if the transaction log is full. If you confirm that the transaction log has exceeded its maximum file size restriction, remove the restriction as follows:

1. In SQL Server Management Studio, right click the **Galaxy database**, then click **Properties** on the shortcut menu.

2. In the **Database Properties** dialog, select the **Files** page.

3. Locate **Log ...** in the **File Type** column.

4. Click the ellipsis (**...**) button in the **Autogrowth** column on the same line.

5. In the **Change Autogrowth for Base_Application_Server_log** dialog, click the **Unrestricted File Growth** radio button under the **Maximum File Size** parameter, then click **OK**.

6. After the Galaxy migration is finished, repeat steps 1 through 5 to reinstate the file size limit on the transaction log.

# Upgrading Run-Time Nodes

**Important:** Upgrade the GR node and any IDE-only nodes before upgrading run-time nodes.

After you upgrade the GR and IDE, all run-time nodes continue to run. This enables you to upgrade the run-time nodes individually when it is convenient.

**Important:** After you have upgraded the GR node, and you have migrated the galaxy, you will not be able to deploy or undeploy from the GR node to remote nodes which have not yet been upgraded. Once remote node upgrade is complete, deployment functionality returns. Also, an upgraded IDE node will not be able to connect to a GR node that has not been upgraded.

Upgrading a run-time node will remove (undeploy) any deployed Platforms from that node.

After you upgrade and then deploy a run-time node, it continues to function with other run-time nodes as long as the other nodes are the current version or from the previous version.

The run-time node does not function while you are upgrading it. You cannot roll back the upgrade.

After you upgrade the run-time node and all hosted objects, you need to redeploy the WinPlatform and all hosted objects to the node.

The GR node migration fails if the GR node is used as a run-time node for another GR.

**To upgrade a run-time node**

1. Run Setup.exe from the DVD. See Upgrading System Platform for information about the installation process.

   When the **Installation Complete** dialog box appears, click **Configure** to continue.

2. **Configuration:** Configure licensing, the System Management Server, and other installed features, such as the Historian and the InTouch Web Client.

   ▪ Configure the System Management Server to point to the GR node. See Configuring the System Management Server for additional information.

   ▪ Configure the AVEVA System Monitor to point to the System Monitor Manager node. By default, this is the GR node. See Advanced System Monitor Configuration for additional information.

3. When prompted, click **Restart Now** to complete the upgrade.

# Upgrading Redundant Pairs

You can reduce plant down time by upgrading the two partner nodes in a redundant pair, one at a time.

Platforms hosting redundant pairs may be deployed even when a partner platform is not the same software version as the Galaxy Repository (GR) platform, or is in the Software Upgrade Pending (SUP) state.

When upgrading a redundant pair, we recommend upgrading the standby partner first. This way, only one failover of the redundant engines is needed, thus minimizing the period of time in which process data is not collected. After upgrading the first node, upgrade the second as soon as possible. When only one node is upgraded, backup and failover are not available. Both nodes must be at the same software version to enable redundancy.

The following table illustrates the workflow for upgrading a Galaxy Repository and one redundant pair, consisting of different nodes, from software version 1 (v1) to version 2 (v2). Action items are shaded. In this example, the redundant pair is comprised of Node B and Node C, as a redundant Application Engine is hosted by the platform on each node. Use the Platform Manager to determine which platform (P1 or P2) is hosting the active Application Engine. See the Platform Manager User's Guide for additional information.

**To upgrade a redundant pair**

Follow the actions listed in the table to upgrade a GR node and redundant pair. These instructions assume an initial state where the primary engine (E1) is active. At the conclusion of this procedure, all three nodes are upgraded and the backup engine (E1b) is active.

| | Node A<br><br>Galaxy Repository (GR)<br>Platform 0 (P0) | | Node B<br><br>Primary AppEngine (E1)<br>Platform 1 (P1) | | Node C<br><br>Backup AppEngine (E1b)<br>Platform 2 (P2) | |
|---|---|---|---|---|---|---|
| Step | Action | Resulting State | Action | Resulting State | Action | Resulting State |
| --- | (Initial state) | Deployed. | | E1 Deployed – Active. | | E1b Deployed – Standby. |
| 1 | Upload run-time changes | Changes made at run-time now stored in the database. | | | | |
| 2 | Upgrade (with AppServer deployed but shut down) | All objects on P0 become undeployed. | | | | |
| 3 | Reboot when prompted | Software is now at v2. | | | | |
| 4 | Open IDE and migrate database | Galaxy database now at v2.<br><br>IDE shows P1 and P2 in SUP state. | | | | |

| | Node A<br><br>Galaxy Repository (GR)<br>Platform 0 (P0) | | Node B<br><br>Primary AppEngine (E1)<br>Platform 1 (P1) | | Node C<br><br>Backup AppEngine (E1b)<br>Platform 2 (P2) | |
|---|---|---|---|---|---|---|
| **Step** | **Action** | **Resulting State** | **Action** | **Resulting State** | **Action** | **Resulting State** |
| 5 | Optional: Open and migrate InTouch ViewApps | InTouch ViewApps now at v2. | | | | |
| 6 | Cascade deploy P0 | All objects on P0 are deployed. | | | | |
| 7 | | | | | Upgrade (with AppServer deployed but shut down) | P2 and its hosted engines and objects become undeployed. |
| 8 | | | | E1 becomes undeployed. E1 shows as undeployed, but objects under E1 show as deployed. | Cascade Deploy P2<br><br>**Note:** This action results in a brief downtime for objects on E1 and E1b as E1 becomes undeployed (a few seconds to a few minutes, depending on number of objects). | E1b becomes active; hosted objects are now running under v2.<br><br>**Note:** E1b does NOT start from the check-pointed state of non-upgraded E1. |

| | Node A<br><br>Galaxy Repository (GR)<br>Platform 0 (P0) | | Node B<br><br>Primary AppEngine (E1)<br>Platform 1 (P1) | | Node C<br><br>Backup AppEngine (E1b)<br>Platform 2 (P2) | |
|---|---|---|---|---|---|---|
| Step | Action | Resulting State | Action | Resulting State | Action | Resulting State |
| 9 | | | Upgrade (with AppServer deployed but shut down) | P1 becomes undeployed. | | |
| 10 | | | Cascade deploy P1 | E1 is deployed as part of P1 deployment.<br><br>E1 starts as standby and fully syncs with active engine. | | No down-time for objects on E1b as E1b continues to run as active. |
| --- | Final state | Deployed. | | E1 Deployed – Standby. | | E1b Deployed – Active. |

After you have upgraded to System Platform 2020 R2 SP1, you can enable CPU load balancing to improve the performance of redundant AppEngines during failover. See the *Application Server User Guide*, Working with Redundancy, for additional information.

The following table describes the behaviors associated with specific upgrade actions and states.

| Action or State | Behavior |
|---|---|
| Cascade deploy a Platform after upgrade | If the upgraded platform hosts a backup redundant engine with a partner in the SUP state, then during the deploy operation, it will extract the hosted objects from the partner and deploy them along with the backup redundant engine. |
| Deploy a redundant engine with a partner in the SUP state. | The deploy operation is always a Cascade Deploy. |
| Multi-selection for a cascade deployment includes a redundant engine with a partner in SUP state | The cascade deploy operation skips the redundant engine in SUP state and logs a message. |

| Action or State | Behavior |
|---|---|
| Select a backup redundant partner engine for deployment | The backup redundant engine extracts the hosted objects from the primary redundant engine and deploys them along with the backup redundant engine. |
| | The hosted objects are under the primary redundant engine on a partner platform which is in SUP state. The hosted objects will be forced to deploy with the newer software version during the deployment of the backup redundant engine. |
| | A dialog displays with the option to continue deployment or to cancel. |
| Partner engine is deployed but not reachable or not ready to sync. | Redundant engine deployment fails. |
| Partner engine has older software version. | The partner engine is detected and recognized as having an older software version. It is automatically stopped and unregistered. |
| | Primary engine transitions into **Active – Partner not Upgraded** redundancy status. |
| | Primary and backup partners cannot sync, but references to a redundant engine with this status—or with **Active** or **Active – Standby not Available** redundancy statuses—will resolve. |
| | Application Objects can be deployed to a redundant partner with **Active – Partner Not Upgraded** redundancy status. |
| | You will not be able to deploy the partner engine until you have upgraded it. |

# Upgrade Considerations for Multi-Galaxy Communication

**Important:** In multi-galaxy environments, add a System Management Server to only one GR node, and configure the other nodes to point to it. See Configuring the System Management Server for additional information.

Setting up a multiple galaxy environment requires a unique name for each galaxy in the environment. This may require you to rename one or more galaxies if you plan to include galaxies with the same name in your multi-galaxy communication environment. We recommend performing all necessary renaming prior to upgrading System Platform. This will prepare your galaxies for use in a multi-galaxy environment without disrupting the upgrade workflow.

**Important:** It is very important that you follow the galaxy name change procedure provided in the following steps and in the *Application Server User Guide*. You must create a new galaxy with a new, unique name, from a backup .cab file rather than creating a galaxy and performing a restore of the backup .cab file.

For more information about creating and backing up galaxies, see "Getting Started with the IDE," and "Managing Galaxies," in the *Application Server User Guide*.

**To rename a galaxy for use in a multi-galaxy environment**

1. Select a galaxy with a duplicate name, undeploy it and back it up to create a .cab file.

2. Use the .cab file as a "template" by placing it in C:\Program Files (x86)\ArchestrA\Framework\Bin \BackupGalaxies.

3. Create a new galaxy with a new name, based on the backup .cab file. The name must be unique, not in use anywhere else in the multi-galaxy environment.

4. Repeat the preceding steps for each galaxy to be renamed with a unique name.

5. Redeploy each newly created galaxy.

6. Delete the original galaxy from the GR node.

7. Upgrade to Application Server 2020 R2 SP1.

Your galaxy can now be configured for use in a multi-galaxy environment.

# Chapter 6

# AVEVA InTouch HMI Requirements and Prerequisites

You need to meet the requirements and prerequisites for products.

## Installing OI Gateway and Upgrading from FS Gateway

Operations Integration Gateway (OI Gateway) is automatically installed as an InTouch component when InTouch is selected for installation. OI Gateway replaces Factory Suite (FS) Gateway, which was supplied with prior versions of System Platform. Like FS Gateway, OI Gateway acts as a communications protocol converter, provides OPC connectivity and also supports OPC UA connectivity. Default configurations for both OPC and OPC UA are included.

See the *Operations Integration Gateway Help* for information about connecting to OPC and OPC UA servers, as well as for information about linking clients and data sources that communicate using different protocols.

In addition to installing OI Gateway as part of installing InTouch, you can install OI Gateway as a stand-alone application. There are three common installation scenarios:

| "Clean" System without OI Gateway or FS Gateway | Older version of OI Gateway is installed | FS Gateway is installed |
|---|---|---|
| OI Gateway is installed as part of InTouch installation. | The System Platform installation program upgrades the existing OI Gateway version to the new version and exits.<br><br>Restart the System Platform installation program after OI Gateway has been upgraded.<br><br>This installs the remaining System Platform components, including InTouch. | The installation program removes FS Gateway, but saves the existing FS Gateway configuration.<br><br>Two instances of OI Gateway are installed. The existing FS Gateway is replaced by the second OI Gateway instance, which uses the existing FS Gateway application name.<br><br>After the upgrade to System Platform 2020 R2 SP1 is complete, activate the instance that has replaced FS Gateway.<br><br>There is no change in behavior for InTouch users that use the pre-existing OPC access name. |

| "Clean" System without OI Gateway or FS Gateway | Older version of OI Gateway is installed | FS Gateway is installed |
|---|---|---|
|  |  | See Compatibility with Existing FS Gateway Applications. |

# Compatibility with Existing FS Gateway Applications

If you are upgrading from InTouch 2014 R2 SP1 where FSGateway has been installed, OI Gateway will continue to maintain the FSGateway application name in the Access Name definition. The application name is preserved to enhance compatibility with existing applications.

- If you are upgrading from InTouch 2014 R2 SP1, FS Gateway will appear in the SMC (System Management Console) under DAManager.
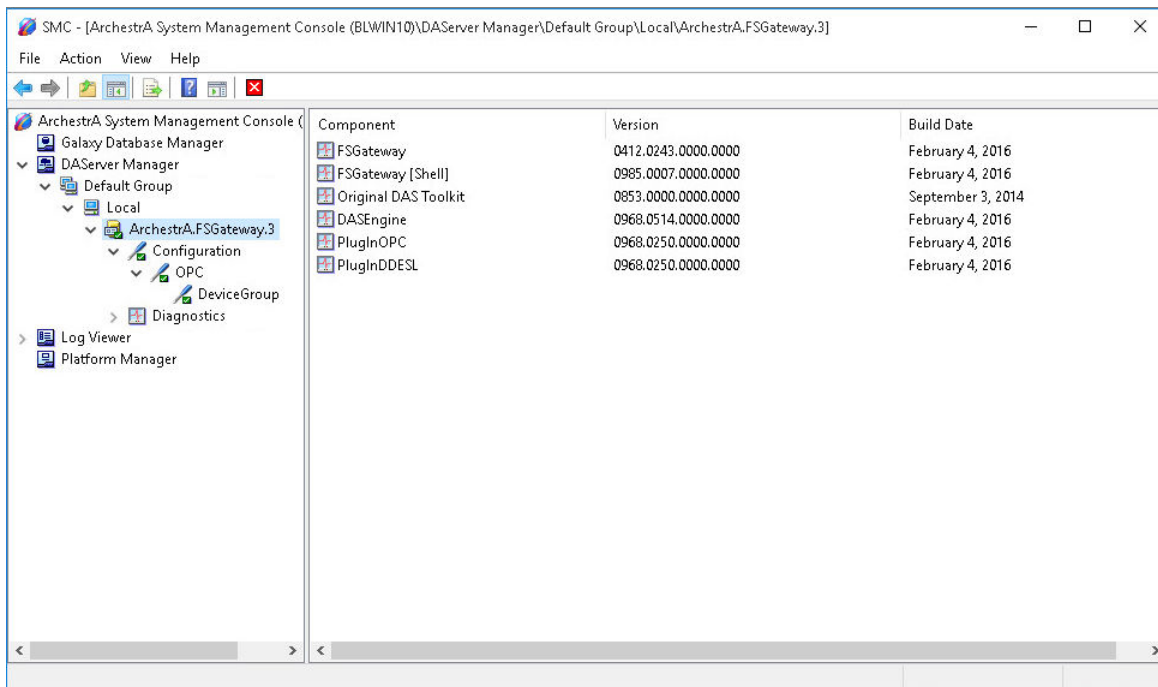


- After upgrading from InTouch 2014 R2 SP1, two new Gateway servers are installed. The first OI Gateway is installed under Operations Integration Supervisory Servers as OI.GATEWAY.n. A second instance replaces the existing FS Gateway instance, but preserves the existing configuration and name, even though FS Gateway has been deleted and the new OI Gateway has been installed in its place. Since the new gateway instance is in a deactivated state, you must activate it (select the instance, right-click, and select "Activate Server").

Note that the component names are changed from "FSGateway" to "Gateway." This does not affect references or change the behavior of the gateway.
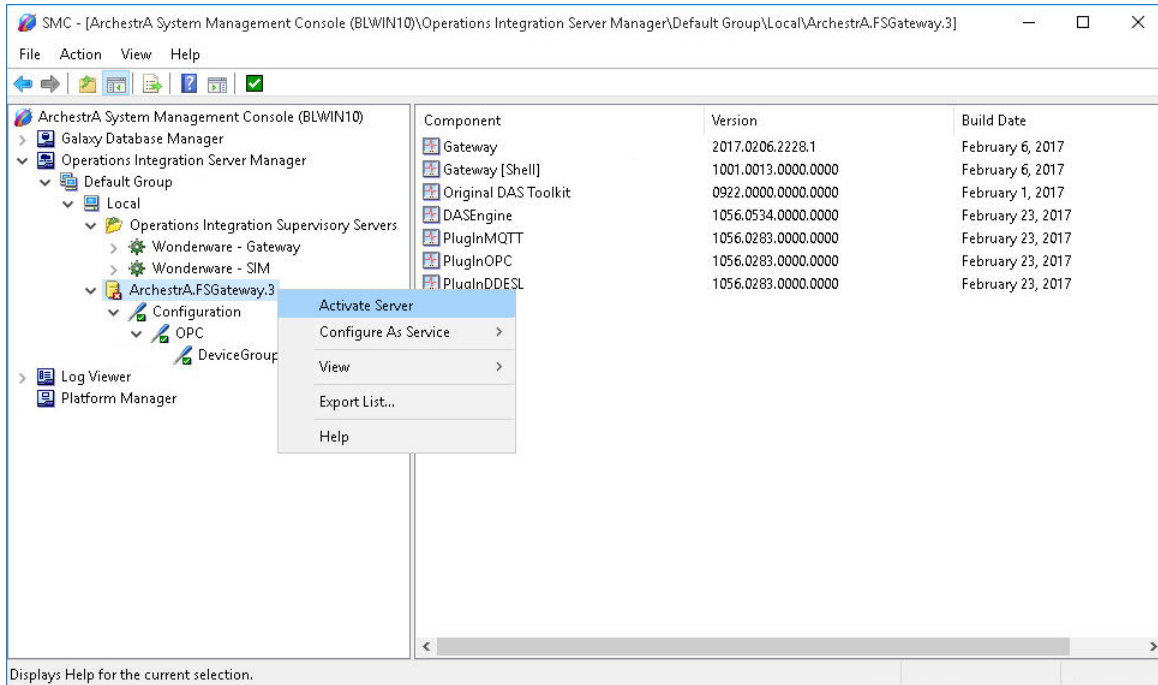
# Product Licensing

**NOTICE: LIMITATIONS TO LICENSING FOR INTOUCH AND APPLICATION SERVER:**

**PROPER USE OF LICENSED PRODUCTS MUST BE STRICTLY FOLLOWED TO ENSURE A FULLY FUNCTIONING PRODUCTION SYSTEM. READ THIS ENTIRE NOTICE.**

If you are licensed for System Platform or the Application Server, you can use all the functionality in these products, up to the limits in your license files.

If you are licensed for only InTouch development and run time, you are licensed to use:

- All InTouch product software capabilities

- InTouch tags up to the licensed limit

- Industrial Graphics

- System Platform IDE

> **Important:** You are not licensed to use or deploy in production any Object templates in the System Platform IDE other than InTouchViewApp Object.

However, you can use the additional functionality in the Application Server in a Demo mode as you learn about its capabilities and consider the advantages of upgrading to a full System Platform license.

You can use most or all of System Platform products in a demonstration, or "Demo," mode. Demo mode lets you learn about and experience the full breadth of System Platform products, technology, and capabilities without requiring a legal license file to run the software.

You can use the License Information utility to see whether the current local or remote I/O counts exceed the maximum specified by your product license.To view license information from the System Platform IDE, on the **Help** menu, click **About**, and then click **View License**.
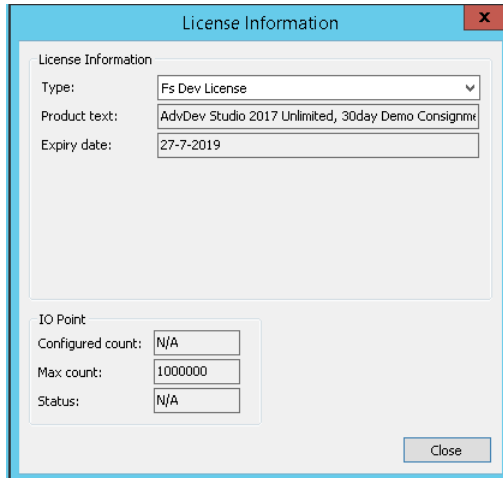
In addition, carefully read the *License Certificate* documentation, which describes the licensed products you received. The *License Certificate* is included with your Licensing CD.

---

**Important:** Attempting to deploy unlicensed functionality to a production environment is illegal and results in problems when upgrading to a future version. Deploying unlicensed functionality is not supported.

---

For further explanation of licensing compliance, see Appendix B of the *InTouch Data Management Guide* installed with the software. Or, contact your local AVEVA distributor or AVEVA Technical Support.

## FS Gateway Installation Scenarios

The following table shows the possible combinations for installing FS Gateway and System Platform. See the *System Platform Readme* and the *InTouch Readme* for information about upgrading and migrating to System Platform 2020 R2 SP1 with InTouch HMI 2020 R2 SP1 from earlier versions of InTouch.

| I have... | I want to... | |
|---|---|---|
| | **Install FS Gateway 3.0 SP2 Stand-alone** | **Install System Platform 2020 R2 SP1 with InTouch and FS Gateway 3.0 SP2** |
| **A clean system** | • FS Gateway is preconfigured with a predefined OPC access Name.<br>• FS Gateway is installed as stand-alone product.<br>• FS Gateway appears in Uninstall/ Change Programs. | • FS Gateway is preconfigured with a predefined OPC access Name.<br>• FS Gateway is installed as a hidden feature.<br>• InTouch appears in Uninstall/ Change Programs. |

| I have... | I want to... | |
|---|---|---|
| | **Install FS Gateway 3.0 SP2 Stand-alone** | **Install System Platform 2020 R2 SP1 with InTouch and FS Gateway 3.0 SP2** |
| **FS Gateway 2.0.0 or previous installed (Stand-alone)** | • Existing FS Gateway Configuration is retained.<br>• FS Gateway is upgraded.<br>• FS Gateway appears in Uninstall/ Change Programs. | • Existing FS Gateway Configuration is retained.<br>• InTouch is installed.<br>• FS Gateway is installed as a hidden feature.<br>• FS Gateway is upgraded.<br>• FS Gateway appears in Uninstall/ Change Programs.<br>• InTouch appears in Uninstall/ Change Programs. |
| **InTouch 10.0.0 or previous installed** | • FS Gateway is preconfigured with a predefined OPC access Name.<br>• FS Gateway is installed as stand-alone product.<br>• FS Gateway appears in Uninstall/ Change Programs.<br>• InTouch appears in Uninstall/ Change Programs. | • FS Gateway is preconfigured with a predefined OPC access Name.<br>• FS Gateway is installed as a hidden feature.<br>• InTouch is upgraded.<br>• InTouch appears in Uninstall/ Change Programs. |
| **FS Gateway 2.0.0 (Stand-alone) or previous and InTouch 10.0.0 or previous** | • Existing FS Gateway Configuration is retained.<br>• FS Gateway is upgraded.<br>• FS Gateway appears in Uninstall/ Change Programs.<br>• InTouch appears in Uninstall/ Change Programs. | • Existing FS Gateway Configuration is retained.<br>• FS Gateway is upgraded.<br>• InTouch is upgraded.<br>• FS Gateway appears in Uninstall/ Change Programs.<br>• InTouch appears in Uninstall/ Change Programs. |

| I have... | I want to... | |
|---|---|---|
| | **Install FS Gateway 3.0 SP2 Stand-alone** | **Install System Platform 2020 R2 SP1 with InTouch and FS Gateway 3.0 SP2** |
| **FS Gateway 2.0.1 Stand-alone** | • Existing FS Gateway Configuration is retained.<br>• FS Gateway is upgraded.<br>• FS Gateway appears in Uninstall/Change Programs. | • Existing FS Gateway Configuration is retained.<br>• FS Gateway is installed as a hidden feature.<br>• InTouch is installed.<br>• FS Gateway appears in Uninstall/Change Programs.<br>• InTouch appears in Uninstall/Change Programs. |
| **System Platform 2012 with InTouch 10.5 and FS Gateway 2.0.1** | • FS Gateway 2.0.1 must be manually uninstalled (after doing this, it is equivalent to installing FS Gateway on a clean system). | • Existing FS Gateway Configuration is retained.<br>• FS Gateway is installed as a hidden feature.<br>• InTouch is upgraded.<br>• InTouch appears in Uninstall/Change Programs. |
| **FS Gateway 3.0.0 Stand-alone** | • FS Gateway is preconfigured with a predefined OPC access Name.<br>• FS Gateway is installed as stand-alone product.<br>• FS Gateway appears in Uninstall/Change Programs. | • Existing FS Gateway Configuration is retained.<br>• InTouch is installed.<br>• FS Gateway is installed as a hidden feature.<br>• FS Gateway appears in Uninstall/Change Programs.<br>• InTouch appears in Uninstall/Change Programs. |
| **System Platform 2012 R2 with InTouch 10.6 and FS Gateway 3.0.0** | • Existing FS Gateway Configuration is retained.<br>• FS Gateway is installed as stand-alone product.<br>• FS Gateway appears in Uninstall/Change Programs.<br>• InTouch appears in Uninstall/Change Programs. | • Existing FS Gateway Configuration is retained.<br>• InTouch is installed.<br>• FS Gateway is installed as a hidden feature.<br>• FS Gateway appears in Uninstall/Change Programs.<br>• InTouch appears in Uninstall/Change Programs. |

Chapter 7

# AVEVA Historian Server Requirements and Recommendations

For the AVEVA Historian to achieve maximum performance, make sure your hardware and software meet the following requirements. Because the Historian is a high-performance relational database, it is also important to size your system to handle the level of data that you expect to store.

The Historian is tightly integrated with Microsoft products, and a working knowledge of both Microsoft SQL Server and Microsoft Windows operating systems is required. For more information on Microsoft SQL Server or Windows operating systems, see your Microsoft documentation.

## Server Requirements

The minimum hardware and software requirements for the Historian are based on the tag count and the anticipated data throughput rate. These requirements are divided into four levels, which are outlined in this section.

You need to ensure that the memory that SQL Server reserves for the Historian is adequate for the expected load. Based on your particular environment, you may need to adjust the SQL Server MemToLeave allocation. For more information on MemToLeave, see the Microsoft documentation.

You can install the Historian on operating systems that have the User Account Control (UAC) turned on.

If you are running the Historian on a virtual server, the historian must have an adequate CPU, adequate network memory, and disk I/O resources at all times. Overloading the virtual server leads to unpredictable behavior. See System Sizing Guidelines for general hardware requirements.

**Operating Systems**

Any supported 64-bit operating system. See the AVEVA Global Customer Support (GCS) Technology Matrix.

**Microsoft SQL Server**

For supported 64-bit Microsoft SQL Server versions, see the AVEVA GCS Technology Matrix.

**Disk Space**

- 300 MB of free disk space to install the Historian
- Appropriate space for history block storage. For more information, see Disk Sizing and Data Storage.

### Level 1 Server - Hardware

A Level 1 server can handle a load of about 5,000 tags. For example, 2,600 analogs, 2,200 discretes, 300 strings, and 20 non-I/O Server (manual) tags.

When replicating to AVEVA Insight, each Level 1 server can support up to 15,000 tags and 5,000 values per second.

The requirements are:

- Processor:
  - Minimum: P4 3.2 GHz CPU
  - Recommended: dual-core CPU
- RAM:
  - Minimum: 2 GB
  - Recommended: 4 GB
- 100 Mbps network interface card (NIC)

### Level 2 Server - Hardware

A Level 2 server can handle a load of about 100,000 tags, with 50% analog, 45% discrete, and 5% string tags. The requirements are:

- Processor:
  - Minimum: P4 3.0 GHz dual CPU
  - Recommended: quad-core CPU
- RAM:
  - Minimum: 4 GB
  - Recommended: 8 GB
- 1 Gbps network interface card (NIC)

### Level 3 Server - Hardware

A Level 3 server can handle a load of 150,000 tags, with 50% analog, 45% discrete, and 5% string tags. The requirements are:

- Processor:
  - Minimum: P4 2.7 GHz Xeon quad CPU
  - Recommended: dual processor, quad-core CPUs
- RAM:
  - Minimum: 6 GB
  - Recommended: 12 GB
- 1 Gbps network interface card

**Level 4 Server - Hardware**

A Level 4 server can handle a load of 2,000,000 tags, with 50% analog, 45% discrete, and 5% string tags. The requirements are:

- Processor:
    - Recommended: two quad-core CPUs
- RAM:
    - Minimum: 24 GB
    - Recommended: 48GB
- 1 Gbps network interface card

A performance report for different historian systems is provided in [System Sizing Examples](#).

## High Availability Support

The Historian provides built-in support for Stratus ft3500 fault-tolerant servers. Other high availability features include:

- Tiering - using the "replication" functionality with a small "local" Historian on site that replicates to two "tier 2" Historians.

- Virtualization - using HyperV or VMware high availability options with Historian running on a virtual machine. For more information, see the *System Platform in a Virtualized Environment Implementation Guide*.

- Redundancy - the Application Server can send data to two Historians at once and maintains independent store-and-forward channels to each.

# Requirements for Historian Management Tools

The management tools include the Historian System Management Console and the Historian Database Export/Import Utility. If you are installing the tools on a remote computer, the following requirements apply:

- Any supported operating system. See the AVEVA Global Customer Support (GCS) [Technology Matrix](#).

- MDAC 2.7

- Any supported browser. See the AVEVA GCS [Technology Matrix](#).

- 20 MB of free disk space

    **Note:** The Historian Data Importer is installed as part of the server installation.

# Remote IDAS Requirements

A remote IDAS runs on all supported operating systems: domain member, stand-alone workstation, or server.

To determine the CPU and memory needed for a remote IDAS, use the same guidelines of the Historian computer. For more information, see [Server Requirements](#).

The IDAS computer does not necessarily have to be as powerful as the server computer, because it will not be performing all of the same functions (for example, processing SQL Server transactions), but it should be powerful enough to handle the tag load that you expect.

The amount of free disk space required depends on whether or not you will have store-and-forward enabled for the IDAS. If store-and-forward is enabled, you need to make sure that the disk space on the remote IDAS computer is sufficient to store cached data if the network connection to the historian fails. Estimate the disk space requirements for a remote IDAS as that of the historian. For more information, see Disk Space Requirements for Historical Data Files.

A remote IDAS configured for store-and-forward has more stringent requirements on memory to ensure that the IDAS local storage engine has sufficient resources to run properly. In general, estimate memory requirements for a remote IDAS configured for store-and-forward the same as you would for a historian having the corresponding tag count.

## Security Considerations for a Remote IDAS

If you set up a remote IDAS, you need to configure security settings that allow access permissions between the remote IDAS and the Historian. For example, the historian needs to access the remote computer to start and stop the IDAS. Also, the remote IDAS needs to access the historian computer to send data. These are administrative tasks, which require administrative permissions.

When you install the historian, you must specify an administrative user account under which all of the historian services run. Make sure that this same user account is added to the Administrators security group on the remote IDAS computer. The existence of the same administrative user account on both the computers, allows the historian to access the remote IDAS, and vice versa.

**Note:** A remote IDAS only requires the same administrative account to exist on the local computer and the historian. It is not required for you to log on to the remote IDAS computer using the administrator account.

If you change the Windows login using the System Management Console, after installing the historian, make sure that the user account change is reflected on the remote IDAS computer.

If you are running the historian in a domain environment (recommended), you can create the administrative user account on the domain controller and add the account to the Administrators group on the historian computer and the remote IDAS computer. Do not create a local user on any computer with the same name and/or password as the administrative user account.

If you are running a remote IDAS in a workgroup environment, there is no centralized management and authentication of user accounts (no domain controller). Create the same administrative user account on each individual computer running a historian component. For example, if you have a computer running the historian and plan to install remote IDASs on two other computers, create the user account (that is, matching user names and passwords) on all three computers.

For information on workgroups, domains, creating user accounts, and adding accounts to the Administrators security group, see your Microsoft operating system documentation.

## Disk Sizing and Data Storage

A number of storage-related questions must be answered when setting up the Historian. They include:

- How important is the data? Is it acceptable that four weeks of data is stored online and is then over-written?
- How important is the configuration and event data? This type of information is stored in the Microsoft SQL Server database.
- How often is data in the Microsoft SQL Server database changing?

- Is anyone in the organization going to require operating data that is older than a month? Older than a year?

- How much is the SQL Server component of the historian expected to be used (for example, for the event system)?

- How long can the system be off-line because of a component failure?

- What happens if the system stops storing data?

- What happens if stored data is lost because of a hard drive failure?

- Can the server equipment be taken off-line to perform repairs?

Ask yourself questions like these to help you determine disk space requirements and how you should plan to protect your data.

A performance report for different historian systems is provided in System Sizing Examples.

## General Hardware Recommendations for Storage

The following are the general recommendations for the hardware used for storage:

- SCSI drives configured using hardware RAID is optimum. The disk space required is a function of data rate and the desired history duration.

- NTFS is the only officially supported file system for a production environment.

## Planning for Disk Space Requirements

There are a number of factors to consider when estimating the amount of disk space required to run the Historian:

- Disk space required to install the required software components and files needed to run the historian.

- Disk space required to store the historian database files.

- Disk space required to store the historian data files.

- If a remote IDAS is used, the disk space required on the local IDAS computer to store cached data if the network connection to the historian fails.

- We recommend that you keep sufficient free disk space (around 20%) so that you can run a disk defragmenting utility without negatively affecting the historian performance.

A performance report for different historian systems is provided in System Sizing Examples.

## Disk Space Requirements for Database Files

The Historian installation program adds the Runtime and Holding databases to the Microsoft SQL Server by default. If you choose to store events to SQL Server, the A2ALMDB database is created.

**Note:** Historical plant data is not stored in the database files. This type of data is stored in special files called history blocks.

- The Runtime database stores all historian configuration data and classic event data. The information in the Runtime database is stored to disk as a database file named RuntimeDat_116_*<server_name>*.mdf. Its associated log file is RuntimeLog_116_*<server_name>*.ldf.

The configuration data in the database file remains relatively static and usually never causes the file size to go above 20 MB. However, if you set up classic events, records of event detections and the results of any data summaries or snapshots increase the size of the Runtime database file because the tables are filling up. Also, entries are created in the log file for event-related transactions. If the database files are set to auto-size, the Runtime database file expands to accommodate event-related data until the hard drive is full.

**Note:** In a 2,000,000 tag system, 2.5 GB of space should be preallocated for data files when modification tracking is not used. When modification tracking is used, 20 GB should be preallocated.

- The Holding database temporarily stores tag definitions being imported from InTouch® HMI software. The information in the Holding database is stored to a database file named HoldingDat_116_<*server_name*>.mdf. Its associated log file is HoldingLog_116_<*server_name*>.ldf.

- The A2ALMDB database stores alarm and event data. The information in the A2ALMDB database is stored to a database file named A2LMDat_115_<*server_name*>.mdf. Its associated log file is A2ALMDB_LOG.ldf.

The Runtime and Holding databases are set to automatically expand at a 10% rate (the default).

You cannot change these defaults during the installation. The databases can be resized later using Microsoft SQL Server utilities. For more information on sizing databases, see your Microsoft SQL Server documentation for guidelines.

**Note:** If you are upgrading a previous version of the Historian, the installation program needs space to save a copy of the old Runtime database while it creates the new one. To upgrade, the database space required is twice the size of the old database, plus the database size for the new install.

## Disk Space Requirements for Historical Data Files

The Historian stores historical plant data to hard disk in special files called history blocks. When you install the historian, you are required to specify a storage location (directory) in which these files will be dynamically created and subsequently filled. You must have at least 200 MB of free disk space for these files to install the historian.

After the historian is up and running, when the free space on the drive containing the storage directory drops below a minimum threshold, the oldest data is overwritten. It is very important that you allocate enough disk space to store your plant data for the desired length of time.

The amount of data that can be stored to disk before running out of space is dependent upon the number of tag values that are stored and how often they are stored. That is, the more tags you have, the fewer values you can store per tag before you need to archive off the oldest data. Likewise, the higher the specified storage rate per tag, the faster the system runs out of space.

**Important:** You must have sufficient disk space in the circular storage area to hold at least two full history blocks, plus the space specified for the minimum threshold for the circular storage area. Use the System Management Console to view or change the minimum threshold value.

A performance report for different historian systems is provided in System Sizing Examples.

## Storage and Network Transmission Sizes for Tags

The following table lists the storage and network transmission sizes for various tag types.

| Tag Type | Storage Engine - Storage Item Size (Bytes) | Storage Engine - Network Transmission Item Size (Bytes) |
|---|---|---|
| Analog - Integer | 8 | 34 |
| Analog - Floating Point | 8 | 34 |
| Analog - Double | 12 | 38 |
| Discrete | 5 | 31 |
| String | 5+AvgStringLength | (5+AvgStringLength)+26 |
| Analog Summary | 37 | 63 |
| Discrete State Summary | 40 | 66 |
| Analog State Summary | 28 * NumberOfStates | (28*NumberOfStates)+26 |
| String State Summary | (28+AvgStringLength) * NumberOfStates | ((28+AvgStringLength) * NumberOfStates)+26 |
| Alarm | 325 | 6061 |
| Acknowledgement | 325 | 6066 |
| Event | 300 | 5048 |

The storage size is used for estimating the space required for storage.

The network transmission size is used for calculating the network bandwidth required between HCAL and the historian.

If you enable compression on the AppEngine from which events are originating, then the network size is reduced by approximately 80%.

For alarms and events, the network transmission size assumes that the average name length for each of the alarm properties is 20 characters.

The following table provides some sizing examples.

| Tag Type | Storage Engine - Storage Item Size (Bytes) | Storage Engine - Network Transmission Item Size (Bytes) |
|---|---|---|
| String Tags (32 byte string) | 5+32 = 37 | (5+32)+26 = 63 |
| State Summary for Analog (for 10 states) | 28*10 = 280 | 71*10 = 710 |
| State Summary for Discrete (for 2 states) | 20*2 = 40 | 68*2 = 136 |
| State Summary for String (10 states and 32 byte string) | (1+32)*10 = 330 | (69+32)*10 = 1010 |

**Note:** Current space calculations are different than the calculations used by the classic storage system.

# Disk Space Estimation

This section provides guidance on how to determine the appropriate history block duration. A history block duration can range from 1 hour to 24 hours, with a default of 24 hours.

For retrieval performance, it is better to have longer block durations. However, if the incoming data rate is too high during a 24-hour period, the Original.dat file in which data collects may grow so large that issues occur for history block management and other aspects of the storage subsystem.

We recommend that you tune the history block duration so that the size of the Original.dat file does not exceed 8 GB per history block.

You can estimate how many bytes this data rate generates in one hour by using the following formula:

N kbps = ($N$ / 8) bytes per second = (450 * $N$) bytes per hour

Where N is the transmission item size for the type of data that you are storing. For information on calculating this number, see Storage and Network Transmission Sizes for Tags.

If you multiply this by the history block duration, you can get an estimate of the biggest data file containing streamed and forwarded data, Original.dat.

If that estimate is larger than 8 GB, keep reducing the history block duration until the estimate is under the 8 GB limit.

# Bandwidth Estimation for Streaming Data

The network bandwidth required can be estimated by adding the data transmission rate for all data types and the network overhead. Network overhead is approximately 4% of the total transmission rate, assuming the data rate is above 1000 points/sec. The estimated bandwidth would be the minimum bandwidth required for replication with reliable network (always connected). However, if there are network disconnections/reconnections, using only the minimum required bandwidth would make the "catch-up" process take a long time if possible. It is recommended that you add a 30% safe margin to the estimated bandwidth to ensure that the forwarding process can complete quickly if an unexpected network outage occurs.

The formula for estimated bandwidth is as follows:

$Bandwidth_{Streaming}$ = 1.04 * 8 * $\Sigma_{Each\ Tag\ Type}$ (Data Rate * Transmission Item Size)

$Bandwidth_{RecommendedStreaming}$ = 1.3 * $Bandwidth_{Streaming}$

For example, with the following replication configuration:

1. Simple Replication - 798 4-byte analog tags changing every second.

2. Simple Replication - 815 discrete tags changing every second.

3. Simple Replication - 187 string tags (20 bytes string) every second.

4. 1 Minute Analog Summary - 800 tags

5. 1 Hour Analog Summary - 800 tags

6. 1 Minute State Summary (Analog, 10 states) - 800 tags

7. 1 Hour State Summary (Analog, 10 states) - 800 tags

The average number of bytes transmitted every second for each of the above replication types is as follows. For a table of transmission sizes, see Storage and Network Transmission Sizes for Tags.

1. 798 * 34 = 27132 Bytes

2. 815 * 31 = 25265 Bytes

3. 187 * 52 = 9724 Bytes

4. 800 * 96 / 60 = 1280 Bytes

5. 800 * 96 / 3600 = 21 Bytes

6. 800 * 710 / 60 = 9467 Bytes

7. 800 * 710 / 3600 = 157.8 Bytes

$\text{Bandwidth}_{\text{Streaming}}$ = 1.04 * 8 * (27132 + 25265 + 9724 + 1280 + 21 + 9467 + 158) = 608 Kbps

$\text{Bandwidth}_{\text{RecommendedStreaming}}$ = 1.3 * 608 Kbps = 790 Kbps

# Bandwidth Estimation for Store-and-Forward Data

If there is a network disconnection, HCAL sends data to local storage and later forwards the data to the historian. After the forwarding process starts, HCAL will try to send as much as data as possible with a large packet. The forwarding bandwidth is the bandwidth required to stream the store-and-forward data.

The store-and-forward storage size is the same as for local historian storage. The following table lists the average sizes used for bandwidth estimation used in this example.

| Tag Type | Storage Item Size (Bytes) |
|---|---|
| Discrete Tags | 5 |
| Analog Tags (4 byte data) | 8 |
| String Tags (32 byte string) | 37 |
| Analog Summary (4 byte analog) | 37 |
| State Summary for Analog (for 10 states) | 28 * 10 = 280 |
| State Summary for Discrete (for 2 states) | 20 * 2 = 40 |
| State Summary for String (10 states and 32 byte string) | (1 + 32) * 10 = 330 |

The forwarding bandwidths are calculated using the following formulas:

$\text{Bandwidth}_{\text{Forwarding}}$ = 1.04 * 8 * $\Sigma_{\text{Each Tag Type}}$ (Data Rate * Storage Item Size)

$\text{Bandwidth}_{\text{RecommendedForwarding}}$ = 1.3 * $\text{Bandwidth}_{\text{Forwarding}}$

For this example, if all are stored in the local storage engine and forwarded later, the number of bytes required for every second is as follows:

1. 798 * 8 = 6384 Bytes

2. 815 * 5 = 4075 Bytes

3. 187 * 25 = 4675 Bytes

4. 800 * 37 / 60 = 493 Bytes

5. 800 * 37 / 3600 = 8 Bytes

6. 800 * 280 / 60 = 3733 Bytes

7. 800 * 280 / 3600 = 62 Bytes

$Bandwidth_{Forwarding}$ = 1.04 * 8 * (6384 + 4075 + 4675 + 493 + 8 + 3733 + 62) = 162 Kbps

$Bandwidth_{RecommendedForwarding}$ = 1.3 * 162 Kbps = 211 Kbps

## Time Estimation for Store-and-Forward Data

The actual time taken to forward store-and-forward snapshots depends on the amount of data accumulated and the bandwidth limit. HCAL typically waits for about 30 second to attempt forwarding process after reconnection. It may need to wait for a longer time if the historian is busy.

To simplify the calculation, the following is assumed:

- HCAL can start forwarding immediately without interruption

- The bandwidth is 30% above the data rate before disconnection

The time taken to forward is as follows:

$Time_{Forwarding}$ = $Time_{InStoreforward}$ * $Ratio_{ForwardingDataSize}$ / 0.3

Where $Ratio_{ForwardingDataSize}$ = Forwarding data Size / Streaming data size

For example, the date rate is 1 Mbps and the bandwidth is 1.3 Mbps. Assume you have simple replication for analog tags and store-and-forward data has been accumulating for 1 hour.

$Ratio_{ForwardingDataSize}$ = 8 / 34 = 0.235

$Time_{Forwarding}$ = 60 (minutes) * 0.235 / 0.3 = 47 minutes

## About Data Compression and the Buffer Age Limit

Bandwidth usage is reduced by about 80% if compression is enabled. This assumes that the data rate is high enough to keep the buffer (64K) filled to have better compression ratio. For analog tags, the data rate is roughly 2000 values/second.

When the data rate is low, enabling compression may not be effective. To fill the buffer with low data rate, you can select the **Wait to send incomplete packets** option (BufferAgeLimit attribute) for the AppEngine configuration. This attribute is not applicable to replication.

# Performance Considerations

For a complete Historian system, the following components put a demand on memory.

- Internal historian subsystems, such as the Configuration Manager, data acquisition, and data storage

- The associated Microsoft SQL Server

- The operating system

- Client access (data retrieval), which includes caching

When determining the amount of memory to purchase, remember that adding more memory is the cheapest and easiest thing that you can do to improve performance. Increasing the amount of memory reduces the amount the server has to use virtual memory, thus lowering the load on the storage subsystem. Even if you have a large amount of memory, additional memory is used as additional disk cache, speeding up disk access and therefore file service. Also, processes needed by the server become faster because they are memory-resident.

A major factor in system performance is the amount of plant data you anticipate storing in the system, including considerations about how often that data is stored and retrieved. In general, the more you store, the more often you store it, and the more you retrieve it, the slower the system. The major storage factors affecting the performance of the system are:

- Effective analog flow rate (analog updates per second).
- Period of online data storage required.
- Effective discrete variable flow rate.
- Number of concurrent end users required.
- Complexity of end user queries.
- Number and size of string tags, as well as the effective flow rate of string values.
- Number and duration of string tag retrieval queries, as well as the frequency at which these queries are executed.

A performance report for different historian systems is provided in [System Sizing Examples](System Sizing Examples).

## Server Loading

When a user connects to the Historian with a client, configuration information is immediately requested from the historian. This information includes the tags that the server stores, their descriptions, engineering units, and other tag data. SQL Server reads this information from the database (stored on disk) and places it in memory.

As the user selects time periods to trend, the historian reads data from files located on the disk and prepares the results of the client's data request to be transmitted back to the client. The ability of the server to quickly handle subsequent requests for data from the same client and others is dependent on the server's ability to keep as much information in memory without having to again access data from the disk.

As a higher load is placed for memory, a higher load is placed on the disk I/O system as the server has to use disk caching and read from the data files.

The following table summarizes the loading for various systems.

| System | Load Description |
| --- | --- |
| Acquisition and storage | Base load of the historian. This load exists as long as the system is running. However, this load is not affected by client activity. |
| Retrieval | Variable loading caused by data retrieval from client applications. When the client initially connects, the data requested is configuration data, which is stored in SQL Server. The historian requests data from SQL Server, causing its loading to increase. As the client requests historical data, the disk time increases as information from the data files is transferred to memory. This continues as the client requests additional data. If the client application |

| System | Load Description |
| --- | --- |
|  | requests data that has already been transferred to memory, there is no associated disk activity and transfer of data to memory. |

The server must be able to adequately handle the variation on loading caused by the client applications. To accomplish this, make sure that your hardware is sized so that it can handle the base load created by the acquisition and storage systems and that there are adequate resources still available for the retrieval system.

## IDAS Performance

An IDAS can acquire an unlimited number of real-time data values, from an unlimited number of I/O Servers, each with an unlimited number of topics. However, IDASs are subject to the following limitations.

- The maximum sustained data throughput for any single IDAS is 30,000 items per second for real-time data. For late or old data, the maximum throughput is 9,000 items per second. The total combined throughput (real-time data plus late or old data) cannot exceed 30,000 items per second. For higher-volume applications, you can set up multiple IDASs to serve a single storage subsystem.

- The size of any data value is limited to 64,000 bytes.

- The maximum number of tags supported by any single IDAS is 30,000.

## Tiered Historians

If you are installing a tiered historian, tier-1 nodes use the same basic configuration for the number and types of tags and data collection rates.

The tier 1 configuration should be "delta" data collected and stored:

- 12,000 analog tags every 2 seconds

- 2,900 discrete tags every 2 seconds

- 100 32-character string tags every 30 seconds

For the analog and discrete tags, the averages and value state aggregates are:

- 6000 tags with an hourly calculation performed at the top of each hour

- 6000 tags with 1-minute calculations performed at the top of each minute

plus

- 1500 tags replicated (not aggregated) in tier 2

- 1500 tags stored only in tier 1 (no aggregates or replication)

## Storage Subsystem Performance

The storage subsystem can support a continuous data acquisition rate of 150,000 updates per second. The storage sub-system also supports a burst rate of 300,000 updates per second up to 1 second.

The classic storage subsystem can support a continuous real-time data acquisition rate of 30,000 updates per second and a burst rate of 60,000 updates per second up to 1 second.

The storage subsystem processes all real-time data as a high-priority task that is never interrupted. However, data received from "manual" methods (such as UPDATE/INSERT commands, CSV file imports, or store-and-forward) is handled by a low priority task. If the system is generally busy, then it may take some time for the manual data to be posted.

# Networking Recommendations

The Historian is a highly configurable package that can be set up in many different ways depending on your needs.

The Historian can use any protocol currently supported by Microsoft SQL Server 2012. You can use the default Microsoft SQL Server 2012 protocol (named pipes) with TCP/IP. TCP/IP is required if SuiteLink™ is used.

Do not use the historian computer as a domain controller.

It is highly recommended that you run the historian on a dedicated computer. For example, running the historian on a mail server or an Internet server may impact performance.

Generally, it is recommended that you split the process and IS networks to ensure that the process network does not become overloaded. The following illustration shows one possible network architecture where the historian is the link between the process network and the business LAN/WAN

Data acquisition, PLCs, DCSs, process computers, instruments
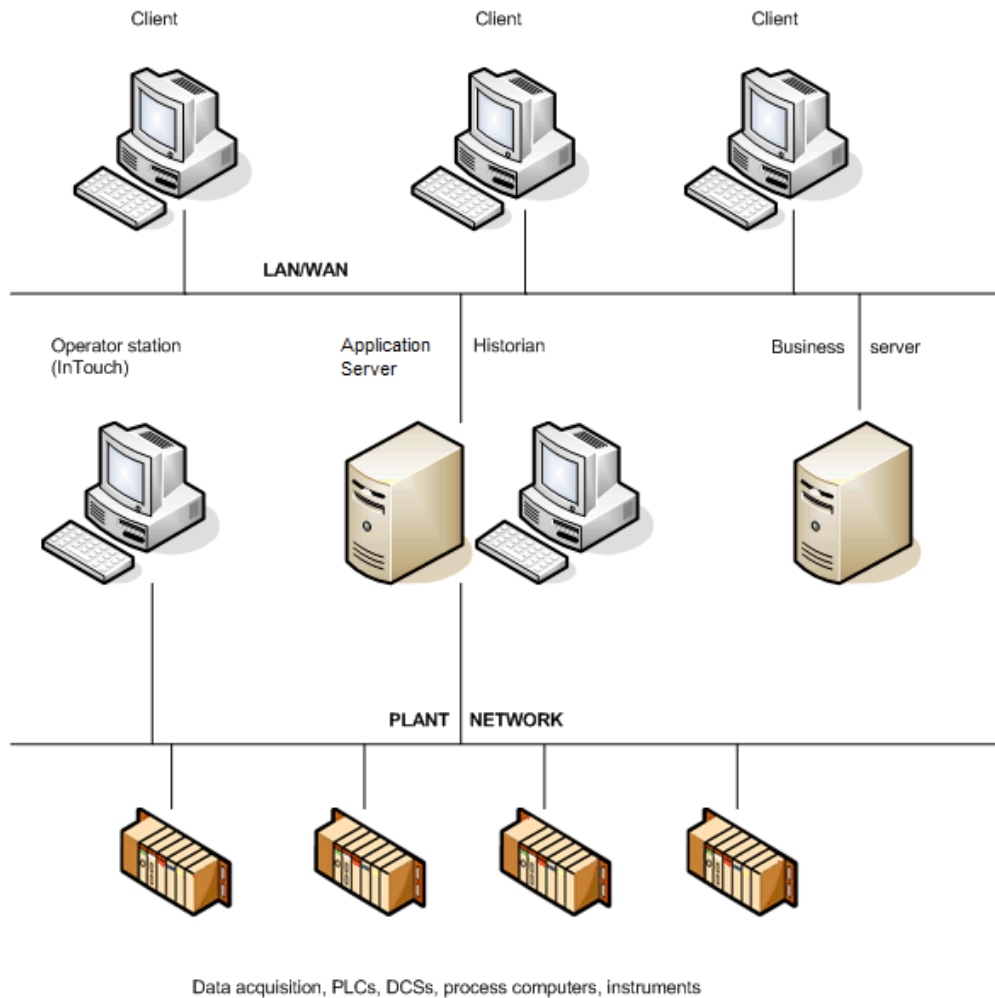
For this architecture, install two network cards on a server computer and configure them to segment the IS network from the process network.

**Note:** All tags to be stored in historian are on "advise" all the time. This may cause heavy load conditions on the process network. Before you install the historian, investigate the possible load impact of installing the historian on your network.

# Client Access

All clients should connect to the Historian using the default Microsoft SQL Server connection. Usually, this means using the name of the computer on which the historian is running as the server name when logging on.

To change the default network protocol used by Microsoft SQL Server to something other than named pipes, configure the client network access using the SQL Server Client Network Utility. For more information, see your Microsoft SQL Server documentation.

# Support for Non-English Operating Systems

The English version of the Historian, the Historian Database Export/Import Utility, and the Historian Data Importer run on localized versions of all the supporting operating systems for the following languages. Set the

regional settings before you install SQL Server. The corresponding version of Microsoft SQL Server for the required language must be used.

- German

- French

- Japanese

- Simplified Chinese

The following entities are not supported in double-byte languages:

- Domain names, user names, and passwords (including SQL Server login names and passwords).

- Names of I/O Server host machines, I/O Server application names, topic names, and item names.

- Any text associated with licensing.

# Integration with Other AVEVA Products

The Historian is an open relational database for plant and process data. Many of the features of the historian allow it to be used with many of other products from AVEVA.

The historian can store data from any application that supports SuiteLink™. Examples of AVEVA applications that can send data to the historian are Application Server, I/O Servers, and InTouch® WindowViewer™.

Any client application that can retrieve information using SQL can retrieve data from Historian. For example, some AVEVA products that can retrieve data by means of SQL queries are the InTouch HMI, Historian Client applications and controls, Manufacturing Execution Module, and InBatch™ products. The Historian further extends SQL to improve the ability to handle time series data.

Also, the Historian I/O Server (aahIOSvrSvc.exe) is an interface for clients to access current data values a historian by means of the SuiteLink protocol. The Historian I/O Server can update items with current values for given topics, providing "real-time" I/O Server functionality.

Finally, you can use InTouch to configure the historian by importing tag definitions and I/O Server definitions from the InTouch Tagname.x file into the Runtime database.

# System Sizing Examples

To help you determine how to size your system, performance reports are provided for different Historian configurations.

**Important:** The information presented here is a guideline only. The actual results in your environment may vary.

## Process Historian Sizing Examples

Performance reports are provided for various levels of a Historian.

### Server 1 (Non-Tiered): 2.4 GHz Single Processor Quad-Core CPU

**Historian Specifications**

- DELL OptiPlex 755 with 2.4 GHz single processor quad-core CPU

- 4 GB RAM

- 512 MB Virtual Memory

- 1 Gbps NIC

- Microsoft SQL Server 2017 Standard Edition

- SQL memory clamped @ 512 MB

- 12-hour history block duration

## Tag Information

Tag count (total) = 5,187

Analog tags = 2,607

Discrete tags = 2,285

String tags = 295

Manual tags = 17

Update rate of +/- 5,000 updates/second

## Remote IDAS

None.

## Event Information

- 3 snapshot events, each having:

    - 1 analog snapshot

    - 1 discrete snapshot

    - 1 string snapshot

- 2 summary events, each having:

    - 1 AVG calculation (1 tag every 8 hours)

    - 1 MAX calculation (1 tag every 8 hours)

    - 1 MIN calculation (1 tag every 8 hours)

    - 1 SUM calculation (1 tag every 8 hours)

- 1 SQL insert every 4 hours

- 2 SQL multi-point updates every hour

## Query Load

For the following seven queries, each are occurring at different times in the hour:

- 1 query (trend):

    - live mode - 1 second update

    - 1-hour duration

    - 10 tags (7 analogs, 3 discretes)

- 1 query: 1-hour range / hour (1 tag)

- 4 queries: 15-minute range / hour (1 tag)

- 1 query: 24-hour report every 24 hours (25 to 30 tags)

### Performance Results

| Category | Value |
|---|---|
| Average CPU load (%) | 1.896 |
| Historian memory (Private Bytes) consumption (MB) | 714 |
| Number of online history blocks | 18 |
| Uncompressed hard drive disk space per history block (MB) | 1002 |

## Server 2 (Non-Tiered): Four Dual-Core 2.7 GHz CPUs

### Historian Specifications

- DELL Precision WorkStation T5400 with four dual-core Intel Xeon 2.7 GHz CPUs

- 4 GB RAM

- 3072 MB Virtual Memory

- 1 Gbps NIC

- Microsoft SQL Server 2017 Standard Edition

- SQL memory clamped @ 1024 MB

- 4-hour history block duration

### Tag Information

Tag count (total) = 63,000

Analog tags = 39,359

Discrete tags = 19,734

String tags = 295

Manual tags = 5,057

Update rate of +/- 30,000 updates/second

### Remote IDAS

One remote IDAS:

- P4 1.7 GHz

- 1 GB RAM

- 34,000 tags via the remote IDAS and the rest via the local IDAS

**Note:** Because this configuration was used for performance and stress testing, the remote IDAS tag count is more than the recommended 30,000 maximum.

## Event Information

- 3 snapshot events, each having:
  - 1 analog snapshot
  - 1 discrete snapshot
  - 1 string snapshot
- 2 summary events, each having:
  - 1 AVG calculation (1 tag every 8 hours)
  - 1 MAX calculation (1 tag every 8 hours)
  - 1 MIN calculation (1 tag every 8 hours)
  - 1 SUM calculation (1 tag every 8 hours)
- 1 SQL insert every 4 hours
- 2 SQL multi-point updates every hour

## Query Load

For the following seven queries, each are occurring at different times in the hour:

- 1 query (trend):
  - live mode - 1 second update
  - 1- hour duration
  - 10 tags (7 analogs, 3 discretes)
- 1 query: 1-hour range / hour (1 tag)
- 4 queries: 15-minute range / hour (1 tag)
- 1 query: 24-hour report every 24 hours (25 to 30 tags)

## Performance Results

| Category | Value |
|---|---|
| Average CPU load (%) | 5.38 |
| Historian memory (Private Bytes) consumption (MB) | 1174 |
| Number of online history blocks | 20 |
| Uncompressed hard drive disk space per history block (GB) | 4.12 |

## Server 3 (Non-Tiered): Four Dual-Core 3.4 GHz CPUs

### Historian Specifications

- DELL PowerEdge 6800 with four dual-core Intel Xeon 3.4 GHz CPUs

- 16 GB RAM

- 4096 MB Virtual Memory

- 1 Gbps NIC

- Microsoft SQL Server 2017 Standard Edition

- SQL memory clamped @ 3967 MB

- 2-hour history block duration

### Tag Information

Tag count (total) = 133,941

Analog tags = 73,600

Discrete tags = 53,560

String tags = 6920

Update rate of +/- 50,000 updates/second

### MDAS

In the total tag count, 4,009 tags originated from Application Server.

### Remote IDAS

Two remote IDASs:

- Remote IDAS 1: P4 1.9 GHz, 1 GB RAM

- Remote IDAS 2: P4 2.5 GHz, 512 MB RAM

44,370 tags via the remote IDAS 1

45,584 tags via the remote IDAS 2

44,383 tags via the local IDAS

**Note:** Because this configuration was used for performance and stress testing, the remote IDAS tag counts are more than the recommended 30,000 maximum.

### Event Information

- 3 snapshot events, each having:

    - 1 analog snapshot

    - 1 discrete snapshot

    - 1 string snapshot

- 2 summary events, each having:

    - 1 AVG calculation (1 tag every 8 hours)

- 1 MAX calculation (1 tag every 8 hours)

    - 1 MIN calculation (1 tag every 8 hours)

    - 1 SUM calculation (1 tag every 8 hours)

- 1 SQL insert every 4 hours
- 2 SQL multi-point updates:

    - 1 every 15 minutes

    - 1 every 30 minutes

### Query Load

For the following seven queries, each are occurring at different times in the hour:

- 1 query (trend):

    - live mode - 1 second update

    - 15-minute duration

    - 15 tags (10 analogs, 5 discretes)

- 1 query: 1-hour range / hour (1 tag)
- 4 queries: 15-minute range / hour (1 tag)
- 1 query: 24-hour report every 24 hours (25 to 30 tags)

### Performance Results

| Category | Value |
| --- | --- |
| Average CPU load (%) | 10 |
| Historian memory (Private Bytes) consumption (MB) | 360 |
| Number of online history blocks | 10 |
| Uncompressed hard drive disk space per history block (average GB) | 1.81 |

## Server 4 (Tier-2): Eight Dual-Core 2.67 GHz CPUs (Hyper Threaded)

### Historian Specifications

- DELL PowerEdge T610 with Eight Dual-Core 2.67 GHz CPUs (Hyper Threaded)
- 48 GB RAM
- 48 GB Virtual Memory
- 1 Gbps NIC
- Windows Server 2019 Data Center Edition
- Microsoft SQL Server 2017 Standard or Enterprise
- SQL memory clamped @ 4096 MB

- 1-hour history block duration

**Tag Information**

Tag count (total) = 2,000,000

Analog tags = 1,000,000

Discrete tags = 900,000

String tags = 100,000

Update rate of +/- 150,000 updates/second

**Query Load**

The following query is occurring at different times in the hour:

- 1 query (trend):
    - live mode - 1 second update
    - 15-minute duration
    - 500 tags (250 analogs, 225 discretes, 25 strings)

**Performance Results**

| Category | Value |
|---|---|
| Average CPU load (%) | 26.444 |
| Historian memory (Private Bytes) consumption (MB) | 11,124 |
| Number of online history blocks | 246 |
| Uncompressed hard drive disk space per history block (average GB) | 10.00 |

# SCADA (Tiered) Historian Sizing Examples

Performance reports are provided for various levels of a multiple Historian SCADA configuration.

## Topology 1: Centralized Tiered Historian Topology on a Slow/Intermittent Network

This topology consists of ten tier-1 historians performing simple and summary replication of the same tags independently to two tier-2 historians. This topology is targeted to reflect the requirements of geographically distributed SCADA applications operating on slow and intermittent networks.
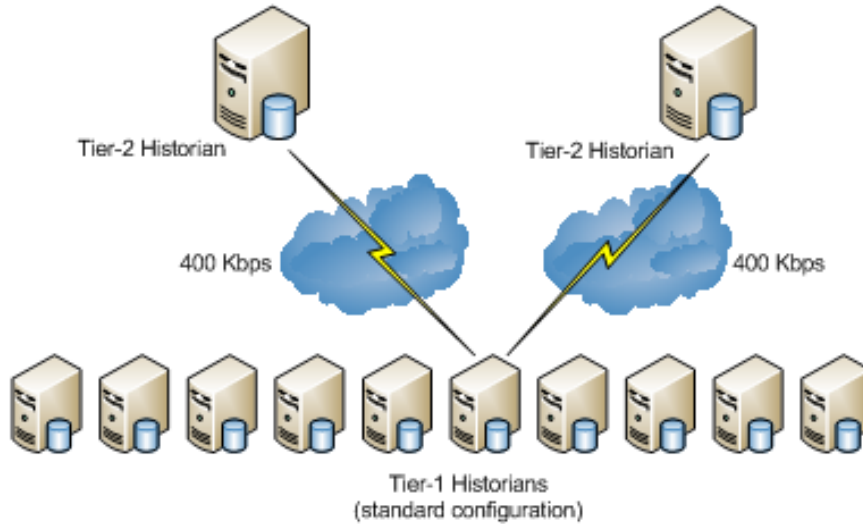
The 400 Kbps data transfer limit reflects a typical data transfer speed between remote locations over the Internet. The data transfer from each tier-1 historian to a tier-2 historian is assumed to be through a dedicated 400 Kbps connection; multiple tier-1 historians do not share the same 400 Kbps connection. It is assumed that the 400 Kbps is a bandwidth that can be fully used.

### Tier 2 Historian Specifications

- DELL PowerEdge 6800 with four dual-core Intel Xeon 3.4 GHz CPUs

- 16 GB RAM with enabled PAE or 4 GB RAM

- Disk I/O subsystem of a 100MB/s throughput, 6 ms access time.

- 100/1000 Base-T network card

- 400 Kbps network connection (actual usable bandwidth)

### Tier 1 Historian Specifications

- DELL Precision WorkStation T5400 with dual processor quad-core Intel Xeon 2.7 GHz CPUs

- 4 GB RAM

- Disk I/O subsystem of a 60MB/s throughput, 16 ms access time.

- 100/1000 Base-T network card

### Loading Information

Assume that the total tag count on the tier-1 historian is 15,000.

The tier-1 historian receives 15,000 tags from I/O Servers of the following types and data rates:

- 12,000 4-byte analog delta tags changing every 2 seconds: (10,000 always fitting the real-time window and 2,000 falling outside of the real-time window being 50 minutes late).

- 2,800 1-byte discrete delta tags changing every 2 seconds

- 200 variable-length string delta tags of 32-character length changing every 30-seconds

The tier-2 historian stores the following:

- 6,000 tags with hourly analog summary calculations performed at the top of each hour (using 6,000 4-byte analog tags as tier-1 tags)

- Another 6,000 tags with 1-minute analog summary calculations performed at the top of each minute (using 6,000 4-byte analog tags as tier-1 tags)

- 1,500 tags replicated (as simple replication) to tier-2 (using 1,400 1-byte discrete tags and 100 variable-length string delta tags as tier-1 tags)

- Another 1,500 tags only stored on tier-1 (using 1,400 1-byte discrete tags and 100 variable-length string delta tags as tier-1 tags)

### Performance Results for the Tier-2 Historian

| Category | Value |
| --- | --- |
| Average CPU load (%) (with no queries executing) | 1% |
| Historian memory (Virtual Bytes) consumption (GB) | 3.05 GB |
| Number of online history blocks | 312 |
| Uncompressed hard drive disk space per history block (average MB) | 888 MB |

### Latency Results

| Category | Value |
| --- | --- |
| Fastload (1 day fastload) | 10.33 hours |
| Simple replication | 4 seconds |
| Summary replication | 4.6 seconds |

Latency is the difference in time between when the value is received by the tier-1 historian and when it is received by the tier-2 historian.

## Topology 2: Centralized Tiered Historian Topology for a Single Physical Location

A 100 Mbps data transfer limit reflects a typical data transfer speed within one location, but distributed over several buildings. In this case the 100 Mbps bandwidth is a physical characteristic of the connection. It is assumed that up to 33% of that physical bandwidth can be used.
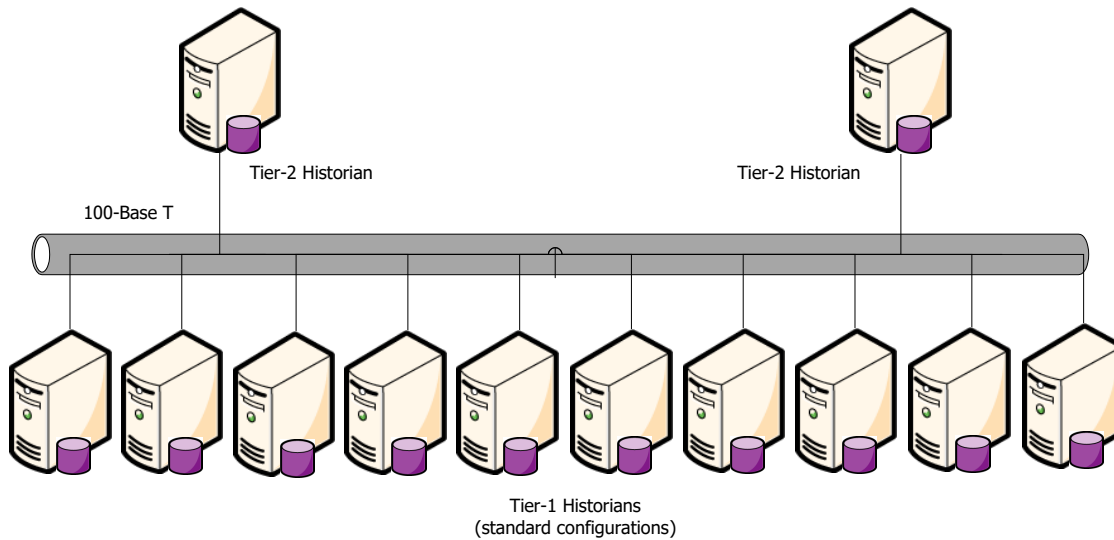
Tier-1 Historians
(standard configurations)

## Tier 2 Historian Specifications

- DELL PowerEdge 6800 with four dual-core Intel Xeon 3.4 GHz CPUs

- 16 GB RAM with enabled PAE or 4 GB RAM

- Disk I/O subsystem of a 100MB/s throughput, 6 ms access time.

- 100/1000 Base-T network card

- 100 Kbps network connection (actual usable bandwidth)

## Tier 1 Historian Specifications

- DELL Precision WorkStation T5400 with dual processor quad-core Intel Xeon 2.7 GHz CPUs

- 4 GB RAM

- Disk I/O subsystem of a 60MB/s throughput, 16 ms access time.

- 100/1000Base-T network card

## Loading Information

Assume that the total tag count on the tier-1 historian is 15,000.

The tier-1 historian receives 15,000 tags from I/O Servers of the following types and data rates:

- 12,000 4-byte analog delta tags changing every 2 seconds: (10,000 always fitting the real-time window and 2,000 falling outside of the real-time window being 50 minutes late).

- 2,800 1-byte discrete delta tags changing every 2 seconds

- 200 variable-length string delta tags of 32-character length changing every 30-seconds

The tier-2 historian stores the following:

- 6,000 tags with hourly analog summary calculations performed at the top of each hour (using 6,000 4-byte analog tags as tier-1 tags)

- Another 6,000 tags with 1-minute analog summary calculations performed at the top of each minute (using 6,000 4-byte analog tags as tier-1 tags)

- 1,500 tags replicated (as simple replication) to tier-2 (using 1,400 1-byte discrete tags and 100 variable-length string delta tags as tier-1 tags)

- Another 1,500 tags only stored on tier-1 (using 1,400 1-byte discrete tags and 100 variable-length string delta tags as tier-1 tags)

**Performance Results for the Tier-2 Historian**

| Category | Value |
|---|---|
| Average CPU load (%) (with no queries executing) | 1.55% |
| Historian memory (Virtual Bytes) consumption (GB) | 3.3 GB |
| Number of online history blocks | 312 |
| Uncompressed hard drive disk space per history block (average MB) | 888 MB |

**Latency Results**

| Category | Value |
|---|---|
| Fastload (1 day fastload) | 9.92 hours |
| Simple replication | 1.65 seconds |
| Summary replication | 1.51 seconds |

Latency is the difference in time between when the value is received by the tier-1 historian and when it is received by the tier-2 historian.

## Topology 3: Simple Tiered Historian Topology for a Modem Configuration

In a modem configuration, the network bandwidth between the tier-1 and the tier-2 historians is limited by 56 Kbps. Because the tag count and the replication data rate of the tier-1 historian should be very limited, it would be sufficient to consider only one tier-1 historian performing simple replication to one tier-2 historian over a modem network.
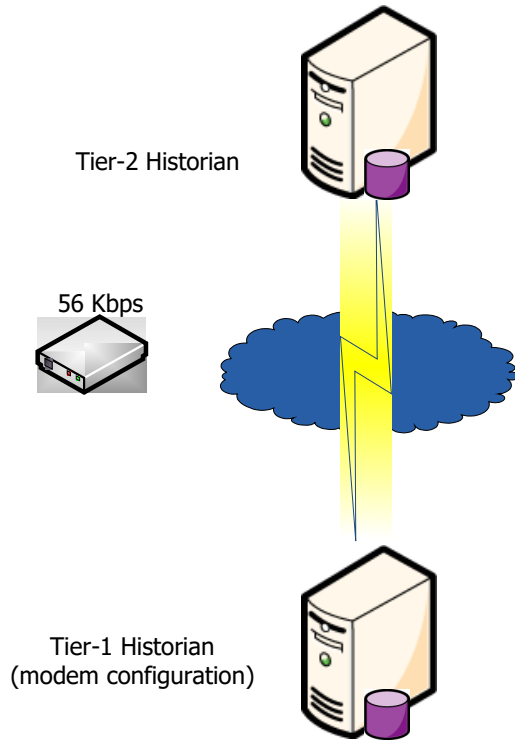
## Tier 2 Historian Specifications

- DELL Precision WorkStation T5400 with dual processor quad-core Intel Xeon 2.7 GHz CPUs

- 4 GB RAM

- Disk I/O subsystem of a 60MB/s throughput, 16 ms access time.

- 100/1000Base-T network card

- 56K modem

## Tier 1 Historian Specifications

- OptiPlex 755 with single processor quad-core CPU 2.4 GHz

- 4 GB RAM

- Disk I/O subsystem of a 60MB/s throughput, 16 ms access time.

- 100/1000Base-T network card

- 56K modem

## Loading Information

In the tier-1 historian modem configuration, the tier-1 historian receives 3,000 tags from I/O Servers of the following types with average update rate 300 items per second:

- 1,500 4-byte analog delta tags (1,400 always fitting the real-time window and 100 falling outside of the real-time window being 50 minutes late)

- 1,350 1-byte discrete delta tags

- 150 variable-length string delta tags of 32 bytes each

## Performance Results for the Tier-2 Historian

| Category | Value |
| --- | --- |
| Average CPU load (%) (with no queries executing) | 1% |
| Historian memory (Virtual Bytes) consumption (GB) | 1.86 GB |
| Number of online history blocks | 30 |
| Uncompressed hard drive disk space per history block (average GB) | 43 MB |

## Latency Results

| Category | Value |
| --- | --- |
| Fastload (1 day fastload) | n/a |
| Simple replication | 5 seconds |
| Summary replication | n/a |

Latency is the difference in time between when the value is received by the tier-1 historian and when it is received by the tier-2 historian.

# AVEVA Historian Server Installation and Configuration

## Preparing for the Historian Installation

A complete AVEVA Historian system consists of the following software components:

- Microsoft SQL Server

- Historian program files, database files, and history data files

- System Management Console, the configuration and control tool

- One or more local or remote IDASs (at least one must be defined)

- Historian documentation.

You should have a definite plan for implementing the historian in your plant environment before you start the installation process. This plan should include the type of network architecture for the historian system, the amount of disk space required for data storage, and the amount of space required for the historian database files and log files.

Also, any administrative security accounts that you specify for either the Microsoft SQL Server or the historian should be accounts that do not change often, if ever. In particular, do not change an administrative password during any part of the installation process.

You must have administrative rights on the local computer to install the historian. The account with which you log on to the computer must also be a sysadmin for the SQL Server or you must be able to provide a sysadmin account for the SQL Server when prompted for it during the installation.

The installation program detects any previous versions of the historian and notifies you of your migration options.

## Microsoft SQL Server Installation

You need to install and run the required version of Microsoft SQL Server before installing the Historian.

Configure the following Microsoft SQL Server options before installing the historian. If you already have Microsoft SQL Server installed, you can run the Microsoft SQL Server setup program to change these options. Microsoft SQL Server options should only be configured by a qualified Windows or SQL Server administrator. For more information, see your Microsoft SQL Server documentation.

- Microsoft Client Utilities must be installed.

- The historian must run with the Microsoft SQL Server default instance name (that is, the computer name).

- During the Database Engine Configuration step of the SQL Server installation, make sure to add the Network Account and/or the local Administrators group as authorized users.

- Remote Microsoft SQL Servers are not supported by the historian.

- For networking support, use named pipes and any other support required at your site. However, you must select at least named pipes and TCP/IP sockets (the defaults). It is highly recommended that you do not modify the default configuration for named pipes and TCP/IP sockets.

- As you select the path to the data files, you must consider that the historian Runtime database will grow, especially if you are going to use the event subsystem (including summaries) or storing data in the ManualAnalog, ManualDiscrete, or ManualString tables.

- The Microsoft SQL Server services should be installed using the local system account. The account you specify should be an account that does not change often, if ever.

- For obvious security reasons, you should not use a blank password for Microsoft SQL Server.

- Both case-sensitive and case-insensitive SQL Servers are supported. However, you should avoid mixing case-sensitive collations in tiered historian topologies.

- The SQL Server e-mail functionality requires a Windows domain user account. You can change the service account after SQL Server is installed. However, it is highly recommended that you use an account for which the password does not change often. For more information on SQL Server e-mail, see your Microsoft SQL Server documentation.

# Historian Installation Features

The Historian installation program allows you to install some of the features of the system separately. The following table describes the various historian features that can be installed. The online help is installed with all the features.

For information on hardware and software requirements for installing any of these features, see the *Historian Readme* file.

| Feature | Description |
| --- | --- |
| Historian | This option installs or re-installs the historian, configuration tools and selected subcomponents. |
| IDAS | An IDAS, which can be used remotely. The IDAS is always installed if you select to install a complete historian. |
| Configuration Tools | The server management tools include Historian Configuration Editor and Historian Management Console. Both of these applications are MMC snap-ins that are contained in the System Management Console. These tools are always installed on the same computer as the historian and can also be installed on a different computer on the network. The Historian Database Export/Import Utility is also an installed configuration tool. |

| Feature | Description |
|---|---|
| ActiveEvent | ActiveEvent is an ActiveX control that allows you to notify the historian classic event system when an event has occurred in another application, such as InTouch HMI software. |
| Insight Client | Historian Insight is a browser client included with the Historian. It is the on-premises version of AVEVA Insight, and provides instant access to production and performance data. |
| Historian Extensions | This option installs historian extensions for OData and SQL Server Reporting Services (SSRS). |

## About Historian Installation

Historian installation is performed in two phases. In the first phase, the installation program performs the following operations:

- Deploys the common components, such as SuiteLink and the License Viewer, unless they are already installed and validated.
- Locates the required version of a running Microsoft SQL Server on the local computer.
- Logs on to the installed Microsoft SQL Server using the account of the person who is currently logged on. This account must be an administrative account on the local computer.
- Checks for required disk space based on the features that you select.
- Creates the historian directories on the hard disk, installs program files for the selected features, and registers components. For more information, see Historian Installation Features.
- Populates the historian program or startup group with icons.

The Database Configuration Utility automatically runs after the historian program file installation is complete. This utility:

- Creates and/or configures the required databases.
- Creates the directory for the history data files (history blocks).

To install the Historian for use in a tiered historian environment, install the Historian on the individual computers, then implement them as described in the "Managing and Configuring Replication" chapter of the *Historian Administration Guide*.

Use the System Platform installation program to install the entire system or any of the features. It is assumed that you are familiar with the installation options. The installation program does not log any errors that may occur.

You must have administrative rights on the local computer to install the historian. The account with which you log on to the computer must also be a sysadmin for the SQL Server or you must be able to provide a sysadmin account for the SQL Server when prompted for it during the installation.

**Important:** Do not install the Historian on a computer named INSQL, because this conflicts with the name of the Historian OLE DB provider and the installation eventually fails.

For detailed instructions on installing, see Installing System Platform.

After the installation completes, configure the server using the instructions in [Configuring Databases and Data File Locations](#).

Refer to the *System Platform Readme* before using the historian.

# Testing the Installation

Test the Historian installation to make sure that everything is installed correctly and is working properly.

**To test the installation**

1. Start the Historian.

2. Start the storage system and check that the system is receiving data from the system tags.

After the historian is installed, no additional configuration is required to run client tools against the server using named pipes. However, you may want to change the system or server configuration using the System Management Console.

# Antivirus Software

After installing the Historian, configure your antivirus software. Be sure to exclude any folder that contains history blocks. Refer to [TechNote TN2865](#), available from the AVEVA Global Customer Support (GCS) web site, for important information about antivirus software. Enter your GCS credentials to access the Tech Note.

# Historian Menu Shortcuts

The following **Start** menu shortcuts are created in the **AVEVA Historian** folder.

- Administration
- Configuration Export and Import
- Data Import
- Historian Client Web
- Query
- Trend

The following **Start** menu shortcuts are created in the **AVEVA** folder:

- Change Network Account
- Configurator
- SQL Access Configurator
- System Platform Management Console

**Note:** If you performed a complete historian installation, the System Management Console is configured so that the local SQL Server is already registered. However, if you only installed the client tools, the console is empty.

# Repairing the Historian

For a repair, the installation program automatically detects if you have an existing copy of the Historian on your computer and then reinstalls missing or corrupt program files, registry keys, and shortcuts.

For detailed repair instructions, see Repairing an Installation.

To repair a database, use the Database Configurator. For more information, see Configuring Databases and Data File Locations.

# Modifying the Historian Installation

You can modify the Historian features that are already installed.

For detailed modification instructions, see Modifying an Installation.

To modify the disk directories for the database files and/or the history data files (history blocks), use the Database Configurator. For more information, see Configuring Databases and Data File Locations.

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

Typically, customers using the Open Data (OData) protocol 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.) It is possible to use an encrypted connection (HTTPS) for OData, but in that case, you must first install and configure a TLS (transport layer security) certificate.

The following sections describe how to install and configure a TLS certificate.

## About TLS Certificates

If you use an HTTPS connection with the Historian, you will need a TLS certificate. The certificate can be from a trusted authority or a self-signed certificate.

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

## Creating Self-Signed Certificates

If you choose to use a self-signed certificate with the Historian, you are responsible for configuring all clients to trust that certificate. Consult you operating system and/or browser documentation for details about how to trust a self-signed certificate.

**To create a self-signed certificate**

- In Windows PowerShell, run this command:
  ```
  New-SelfSignedCertificate -DnsName <hostname> -CertStoreLocation "cert:\LocalMachine
  \My"
  ```

  Where

  - <hostname> is the name or IP address of the computer running Insight.

    **Note:** Remote users of Insight must use the name or IP address used in the certificate while browsing to avoid receiving TLS warnings.

## Acquiring a Certificate Thumbprint

**To acquire a thumbprint (certhash) for your certificate**

1. In Microsoft Management Console (MMC), double-click the certificate to open it.
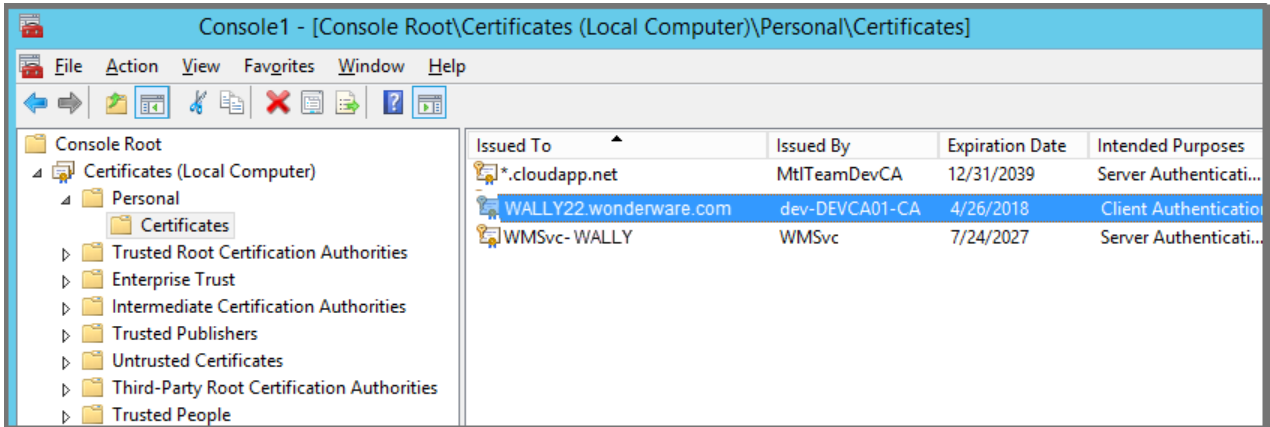


2. From the **Details** tab, select **Thumbprint**.
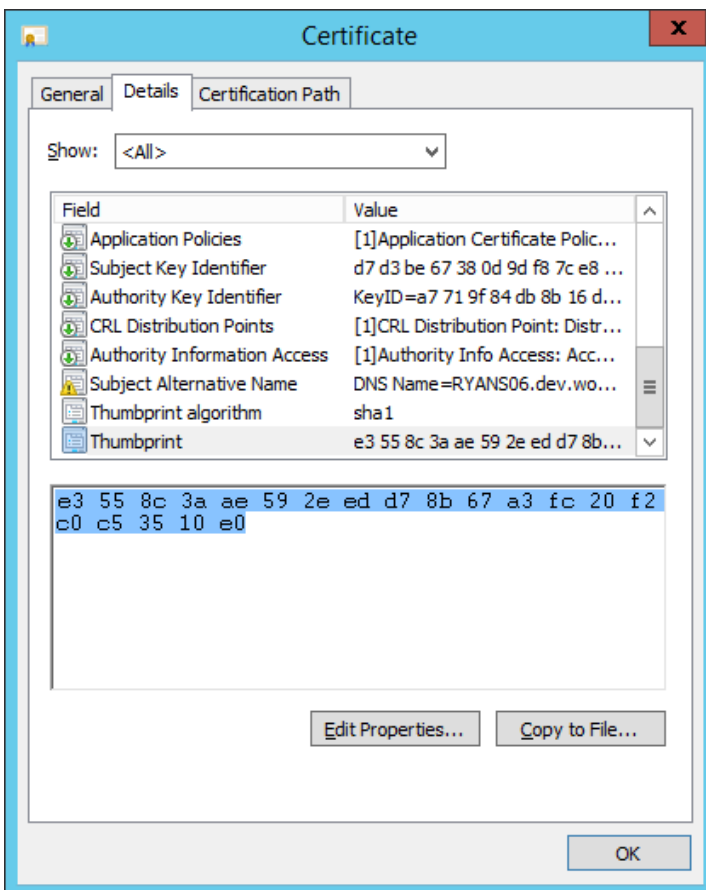


3. Copy the thumbprint and paste it into a text editor, such as Notepad, and remove any spaces from between the hexadecimal digits.

4. Save the file in ANSI format.

5.  Copy the resulting thumbprint for use with the *certhash* parameter when you bind certificates to the port.

## Binding Certificates to Secure Socket Layer Ports

Once you have a certificate to be used for HTTPS communication, you need to bind it to the port used for that communication. The port acts as a self-hosted endpoint for communication with the server.

**To bind a certificate to an SSL port for self-hosting**

- In a command prompt, run this command as administrator (all on one line):
  ```
  netsh http add sslcert ipport=0.0.0.0:<port> appid={12345678-
  db90-4b66-8b01-88f7af2e36bf} certhash=<certificate_hash>
  ```

  For every endpoint mapping, you need to supply three values:

  - ipport -- identifies the ip and port
    Specified as ipport=0.0.0.0:<port>, where the zeros mean all IP addresses on that port. If you are using HTTPS and a gateway, this is port 32569. So, in that case, you would use " 0.0.0.0:32569", which means all IP addresses on port 32569.

  - certhash -- the certificate's thumbprint
    The certhash comes from the specific certificate you're using. Certhash is the identifier that maps the certificate to the specified IP endpoint. This identifier is contained in the TLS certificate (also called a SSL certificate).
    Type your certificate's identifier in this location.

  - AppID -- fixed for HttpListener Hosting
    This value is static, so always use appid={12345678-db90-4b66-8b01-88f7af2e36bf}

  Next, view the binding to confirm the steps above worked.

**To view the binding**

1.  Select the Windows Start button.

2.  In the command box, type the netsh command using this syntax (all on one line):
    ```
    netsh http show sslcert ipport=0.0.0.0:<port>
    ```

    where "<port>" is the port you configured above.

    You will see a display like this one:

## Updating appsettings.json to Enable Secured Mode

Once the binding is completed, you must modify the configuration file (appsettings.json) for AVEVA Historian Client Web to enable secure connections.

**To update the AVEVA Historian Client Web configuration file**

1. Locate the appsettings.json file and open it in a text editor, such as Notepad. The file is located in the `%ProgramFiles(x86)%\Wonderware\HistorianInsight\Server` folder.

2. Locate the *NCHServerUrl* and *ContentsUrl* settings, and update their values to change the URL prefix from `http` to `https` as shown in the following example:

3. Save your changes to appsettings.json.

## Updating the Registry for OWINHost to Start in Secured Mode

Once the binding is completed and the configuration file has been updated, you can modify the Windows Registry to start OWINHost in secured mode.

**To update the Registry**

1. Open Regedit.

2. In the left pane, navigate to this location:
   HKEY_LOCAL_MACHINE\SOFTWARE\ArchestrA\Historian\Setup

3. Update the *GatewayArgs* value as follows:
   GatewayArgs = -port 32569 -secured 1

4. Launch the configurator, and select the **Historian Server** node.

5. Click **Configure**.

   **Note:** To enable the **Configure** button, you may need to temporarily change a configured setting. For example, toggle the **Allow remote access for SMC** setting, click **Configure**, return the setting to its original value, then click **Configure** once more.

6. Restart the **AVEVA Historian Client Web** and **AVEVA Historian Gateway** services.

   You can now use an encrypted connection to the server.

# Uninstalling the Historian

The uninstall program allows you to remove all the historian program files. The Runtime, Holding, and A2ALMDB databases and the history blocks are not deleted.

During the uninstall, you have the option to delete the configuration files (idatacfg_*.dat) created by IDAS and the Configuration Service.

For detailed uninstall instructions, see [Uninstalling AVEVA System Platform](#).

# Upgrading from a Previous Version

You can upgrade directly to the current version of the Historian (2020 R2 SP1) from Historian 2014 R2 (version 11.6.12100) SP1 and later versions.

You should upgrade the Historian Server before upgrading Historian remote IDAS nodes. Remote IDAS nodes that are not upgraded to 2020 R2 SP1 will remain fully functional. However, it is strongly recommended that you upgrade them to 2020 R2 SP1 to incorporate minor improvements and simplify further upgrades and maintenance.

If you have been using replication, when upgrading Historian nodes, upgrade the tier-2 Historian node first and then the tier-1 Historian node. A tier-2 node must use the same release of the Historian, or one release newer than its tier-1 nodes. A tier-1 node cannot replicate to a tier-2 node running an earlier version of the Historian.

## About Database Migration

The data in an existing Runtime database can be migrated to a new Runtime database. The old Runtime database is not deleted. Keep the old database until the Historian migration is validated.

**Important:** Back up the Runtime database before performing the migration.

There is no migration for the content of the Holding database, because this database is used only to temporarily hold data when importing an InTouch data dictionary.

Any configuration data associated with obsolete system tags is not migrated.

For the event subsystem, all SQL-based detectors and actions are migrated to the OLE DB syntax. If you have any custom SQL-based detectors or actions, you need to rewrite them using the OLE DB syntax.

History data that is stored in SQL Server tables (not history blocks) can be migrated after the general upgrade has been performed.

The scripts are created when you first run the database setup utility so that you can run them at any time. The file path is:

**To migrate your database**

1.  On a new Historian server, use SQL Management Studio to:

    a.  Delete any empty Runtime database that was created as part of the installation.

    b.  Restore the old Runtime database from a backup.

2.  Run the Configurator.

3.  In the left pane, select **Historian** and then select **Server**.

4.  Configure the server. See [Configuring Databases and Data File Locations](#) for details.

# Upgrading the Historian Version (Microsoft SQL Server 32-bit)

Beginning with Historian 2020, only 64-bit versions of Microsoft SQL Server are supported. If your existing databases are hosted on a 32-bit version of Microsoft SQL Server, you must migrate them to a 64-bit version.

**To upgrade the Historian when using 32-bit Microsoft SQL Server:**

1.  Shut down and disable the Historian using the Management Console. Any remote IDAS nodes will go into store-and-forward mode.

2.  Back up the Runtime, Holding, and A2ALMDB databases.

3.  Uninstall the 32-bit version of Microsoft SQL Server.

4.  Install a supported 64-bit version of Microsoft SQL Server that is compatible with your database backups.

5.  Restore the Runtime, Holding, and A2ALMDB databases.

6.  Run the System Platform installation program to perform the upgrade. For more information, see [Upgrading System Platform](#).

7.  In the configurator, configure 'Server' without selecting the 'Drop and Create' option. Provide the correct path to the data files for the restored databases. For example, `C:\Program Files\Microsoft SQL Server \MSSQL12.MSSQLSERVER\MSSQL\DATA`.

8.  Configure the remaining components, if not already configured.

9.  Start the Historian. The Historian will start acquiring and storing the store-and-forward data from the existing remote IDASs.

10. After the Historian Server node is upgraded, you can upgrade any remote IDAS nodes.

# Upgrading the Historian Version

Refer to [Upgrading from a Previous Version](#) to see which versions can be directly upgraded to Historian 2020 R2 SP1.

The existing Runtime and A2ALMDB databases are automatically migrated to during the installation, preserving all existing settings and tag configuration.

History blocks created using a previous version of the Historian do not require any migration and can be copied to and used with Historian 2020 R2 SP1, as long as the tags they contain are present in the Runtime database.

**To upgrade the Historian**

1.  Back up the Runtime database.

2.  Shut down and disable the Historian using the Management Console. Any remote IDAS nodes will go into store-and-forward mode.

3.  Run the System Platform installation program to perform the upgrade. For more information, see [Upgrading System Platform](#).

4.  The installation program detects the previous version of the Runtime database and prompts you to keep the existing database or recreate the new database.

5. If you re-create the database, existing Runtime database will not be re-named but will be overwritten with a new Runtime database. If you do not re-create the database, the existing database will remain intact.

6. Finish the installation of the Historian.

7. Restart the computer.

8. Start the Historian. The Historian will start acquiring and storing the store-and-forward data from the existing remote IDASs.

9. After the Historian Server node is upgraded, you can upgrade any remote IDAS nodes.

## Migration of History Data Stored in SQL Server

The normal SQL Server tables in the Runtime database contain configuration data and certain types of history data. History data that is stored in the normal SQL Server tables includes:

- Data in the AnalogManualHistory, DiscreteManualHistory, and StringHistory tables.

- Classic event and summary data, which is stored in the EventHistory, SummaryHistory, SummaryData, AnalogSnapshot, DiscreteSnapshot, and StringSnapshot tables.

These tables can contain hundreds of thousands of rows, if not millions of rows. Depending of the amount of data to be migrated, migrating this data can take a few minutes to many hours, and in some cases, days.

**Important:** You MUST perform the database migration before the server goes back into production, because the history table content will be truncated. Be sure that you have disk space equivalent to two times the size of the Runtime database on the drive to which the history data will be migrated; otherwise, the migration may fail. Back up the Runtime database with the migrated configuration data before migrating the history data.

Chapter 9

# AVEVA Historian Client Information

## About the Historian Client

You can use the Historian Client software to address specific data representation and analysis requirements. The Historian Client software maximizes the value of the data present in the Historian and helps you organize, explore, analyze, present, and distribute process data in a variety of formats.

With the Historian Client software, you can:

- Explore data graphically to find important information

- Analyze data

- Develop and execute ad hoc queries against any data stored in the Historian database

- Visualize the current process state

## Historian Client Components

The Historian Client software comprises of tools that eliminate the need to be familiar with the SQL and provides intuitive point-and-click interfaces to access, analyze, and graph both current and historically acquired time-series data.

### Desktop Applications

The Historian Client software includes the following stand-alone applications:

**Historian Client Trend**

- Allows plotting of historical and recent data over time

- Allows you to compare data over different time periods

**Historian Client Query**

- Allows you to query the Historian database

- Provides complex, built-in queries

- Eliminates the need to be familiar with the database structure or SQL

## Microsoft Office Add-Ins

The Historian Client software includes the following add-ins for Microsoft Excel and Microsoft Word. The add-ins support only 32-bit versions of these applications.

**Historian Client Workbook**

- Allows display and analysis of historical and recent data from a Historian database using the Excel spreadsheet format

**Historian Client Report**

- Allows advanced reporting of historical and recent data from a Historian database using the Word document format

## ActiveX and .NET Controls

The aaHistClientTrend and aaHistClientQuery controls provide the essential functionality of the Historian Client Trend and Historian Client Query. You can use these controls in container applications, such as InTouch® HMI software, Visual Studio (Visual Basic .NET or C#), and Internet Explorer. You can also use Historian Client "building block" controls (such as aaHistClientTagPicker, aaHistClientTimeRangePicker, and so on) in your custom applications.

# Requirements and Recommendations

You must log on to the computer as an administrator to install the Historian Client software. Be sure that you read the hardware and software requirements in the *System Platform Readme* before starting the installation.

# Support for Operating System Language Versions

The English version of the Historian Client software runs on the following operating system languages:

- English
- French
- German
- Japanese
- Simplified Chinese

  **Note:** The SQL Server locale language must be the same as the operating system locale language.

# AVEVA

## Chapter 10

# AVEVA Historian Client Installation and Configuration

The System Platform installation program allows you to install the Historian Client software. The System Platform installation program copies the files from the setup DVD to the target computer.

For more information on the components installed, see [Historian Client Components](#).

## About Historian Client Installation

Before installing the Historian Client software, log on to the computer as an administrator. Before copying the software files, the System Platform installation program checks for the basic system prerequisites.

You can individually select or deselect features of Historian Client for installation. These are:

- Trend/Query Clients: This feature lets you view and analyze data and trends.
- Microsoft Office (32-bit) Add-ins: This feature installs Historian Client add-ins for Microsoft Word and Excel. You must have a 32-bit version of these programs installed.
- PDF Documents

The System Platform installation program checks if a Microsoft Excel process is running. If Excel is running, a message appears informing you that an Excel process and the aaHistClientReportingService.exe service are running.

To continue with the installation, you need to manually stop the services and click **Retry**. Click **Close** if you want to stop the installation.

**Note:** In some cases, depending upon the operating system and the prerequisite, you may have to restart the system after the prerequisites are installed. In such cases, the setup automatically continues after the restart.

For instructions on installing the Historian Client software files, see [Installing System Platform](#).

After the Historian Client software is installed on the computer, you must install the Language Packs manually.

## Using Historian Client Software with Roaming Profiles

If your network environment uses roaming user profiles, you must change a registry key so that changes to any Historian Client software options are saved in the user profiles.

To save software options in the roaming user's profile, add a DWORD key named "EnableRoaming" to the user's HKEY_CURRENT_USER\Software\ArchestrA\ActiveFactory registry folder and change its value to 1.

# Repairing the Historian Client Installation

You can use the System Platform installation program to repair corrupt files of the installed features. For more information, see [Repairing an Installation](#).

**Note:** You can also use the standard Windows **Uninstall/Change Programs** feature from the Control Panel to repair the Historian Client software installation.

# Uninstalling Historian Client

You can use the System Platform installation program to remove the Historian Client software that exists on your computer. For more information, see [Uninstalling AVEVA System Platform](#).

**Note:** You can also use the standard Windows **Uninstall/Change Programs** feature from the Control Panel to remove the Historian Client software installation.

# Upgrading from a Previous Version

You can upgrade directly to the current version of the Historian (2020 R2 SP1) from Historian 2014 R2 (version 11.6.12100) SP1 and later versions.

You should upgrade the Historian Server before upgrading Historian remote IDAS nodes. Remote IDAS nodes that are not upgraded will remain fully functional. However, it is strongly recommended that you upgrade them to Historian 2020 R2 SP1 to incorporate minor improvements and simplify further upgrades and maintenance.

If you have been using replication, when upgrading historian nodes, upgrade the tier-2 historian node first and then the tier-1 historian node.

**Upgrading From a Version Earlier Than Historian 2014 R2**

You must make some changes manually if you need to upgrade from a version of Historian prior to version 2014 R2. When you run the Configurator, it generates SQL scripts that you can use for manually migrating older releases.

**To upgrade from an earlier version of Historian (before v.2014 R2)**

1. Install Historian 2020 R2 SP1 and run Configurator.

2. From the System Management Console, shutdown and disable Historian.

3. Locate SQL scripts that you'll need for intermediate migration in this folder:

    **C:\ProgramData\ArchestrA\Historian\Install\Scripts**

4. From SQL Server Management Studio:

    a. Drop the Runtime database.

    b. Restore a backup of the Runtime from your previous version of Historian.

5. Disable any triggers or constraints that would prevent schema changes. This prepares your database for changes.

6. Run the scripts you need to update Historian.

   If you are upgrading from a much older version, you may have to run scripts to incrementally upgrade versions.Run the scripts in the order they appear (when sorted alphanumerically).

7. Restore any changes (triggers and other constraints) that you made to settings in step #5.

8. Shut down the old server's remote IDAS.

9. From the new server, force an update to the remote IDAS configuration.

# Appendix A

# Using Silent Installation

System Platform supports silent (command line) installation. This feature uses plain text files called "Response Files" and enables you to install System Platform products without user interaction.

**Important: If prerequisite software is required for the System Platform products you are installing, all prerequisites must be installed before starting silent installation.**

Prerequisite software includes .NET Framework and SQL Server. Details about prerequisite software are provided in System Platform Prerequisites. See SQL Server Requirements for additional information about supported versions of SQL Server.

Setup.exe is run from the command line and accepts as an argument the name and path of a response file containing pre-scripted responses to System Platform installation prompts.

System Platform 2020 R2 SP1 incorporates a functional change to the installation workflow. By default, some redistributable libraries from Microsoft and other vendors are not installed by default because of the support status of these libraries. **You must acknowledge this change to successfully install System Platform.** This applies both to GUI-based installation and to silent installation. See Response File Entry to Acknowledge Installation Change Information (Redistributable Libraries).

Additionally, a patch for AVEVA Manufacturing Execution System and certain versions of AVEVA Recipe Management is required to ensure compatibility with System Platform 2020 R2 SP1. **You must acknowledge this requirement to successfully install System Platform.** See Response File Entry to Acknowledge Compatibility Requirement for more information.

**Important:** Use silent installation only to install a new system or upgrade an existing one. Adding or removing components during an upgrade is NOT supported.

## Starting Silent Installation

To run silent installation, open a command prompt using **Run as administrator**. The basic syntax of the silent installation command consists of the full path to the setup.exe file (typically the DVD drive designation on your local computer), the command line switch for silent installation, and the full path to the response file. In the examples that follow, C:\ is the system drive and D:\ is the DVD drive.

To see descriptions of the switches and options available, enter **/?** after the setup command.

```
D:\setup.exe /?
Setup.exe will install products in UI and Silent mode.
Setup.exe [/silent] [/silentmodify] [/silentrepair] [/silentuninstall]
[/silentnoreboot] [/silentpatch] [/mingui] [responsefile] [/nowait]
/silent specifies the installation is silent Install
```

```
and doesn't show UI.
/silentmodify specifies the installation is silent modify
and doesn't show UI.
/silentrepair specifies the installation is silent repair
and doesn't show UI.
/silentuninstall specifies this is silent uninstall.
/silentnoreboot specifies the installation is silent Install
and doesn't show UI with no reboot.
/silentpatch specifies the installation is silent patch Install.
/mingui specifies the installation is silent with mingui.
/nowait specifies with silent Install/modify/repair/uninstall
with immediate return to command line.
responsefile specifies the response file.
Examples:
setup.exe /silent responsefile.txt
setup.exe /silentmodify responsefile.txt
setup.exe /silentrepair {productguid}
setup.exe /silentrepair {productguid}.{ownerguid}
setup.exe /silentuninstall {productguid}
setup.exe /silentnoreboot responsefile.txt
setup.exe /silentpatch
setup.exe /mingui responsefile.txt
setup.exe /silent responsefile.txt /nowait
setup.exe /silentmodify responsefile.txt /nowait
setup.exe /silentrepair {productguid} /nowait
setup.exe /silentrepair {productguid}.{ownerguid} /nowait
setup.exe /silentuninstall {productguid} /nowait
```

**Silent installation syntax:**

```
D:\setup.exe /silent "<path\response-file-name>"
```

Note that the full filespec of the response file (filename plus location of file) must be included. For example:

```
D:\setup.exe /silent "C:\docs\WSPInstall\response.txt"
```

The /silent switch completely disables the graphical user interface of Setup.exe. There is no input from or feedback to the end user. However, the installation will output progress to a log file. The log is usually found here:

```
C:\Program Files (x86)\Common Files\ArchestrA\Install\ {<FolderName>}
\ILog<timestamp>.log
```

**Silent installation with minimal GUI syntax:**

```
D:\setup.exe /MINGUI <path\response-file-name>
```

Running setup with the /MINGUI switch will cause setup to install without any input from the end user, but it will display the progress of the installation on screen.

**Silent installation with automatic system restart disabled:**

```
D:\setup.exe /silentnoreboot <path\response-file-name>
```

Running with the /silentnoreboot switch will keep the command window open so you can preserve messages from the installation process. A manual reboot will be required after installation completes.

**Silent installation command-line help:**

```
D:\setup.exe /?
```

Running setup with the /? switch will display the silent installation command-line help.

# Using Response Files

Response files are plain text files. They specify which System Platform products, and even which features of a product that Setup.exe will install. For example, one response file could be used to install the components for a run-time environment. A different response file might be used to install the components for a development server.

Response files can install more than one product at a time, enabling you to install all the necessary products for a given role.

Because the user will get little feedback on error conditions, it is necessary for the user to perform the following checks before installing via command line:

1. The operating system must be a supported version with all of the correct service packs.

2. SQL Server must be a supported version.

3. The user running installation must have administrator rights.

4. SQL Server SysAdmin permissions must be configured. See Configure SQL SysAdmin Permissions for more information.

5. You must acknowledge the changes to System Platform 2020 R2 SP1, as compared to prior versions, regarding which redistributable assemblies are installed. To acknowledge this, set the parameter "OutOfSupportRedistConsentForm.SRedistConsent=true" in the response file. See Response File Entry to Acknowledge Installation Change Information (Redistributable Libraries) for more information.

6. You must acknowledge that a patch may be needed to ensure compatibility with AVEVA Manufacturing Execution System and AVEVA Recipe Management, even if you do not have these products installed. To acknowledge this, set the parameter "CompatibilityAlert.SProductCompatibilityConsent=true" in the response file. See Response File Entry to Acknowledge Compatibility Requirement for more information.

   If it is needed, apply the patch(es) to Manufacturing Execution System and/or Recipe Management, not to System Platform. See the *Compatibility Readme,* located in the **InstallFiles>CoexistenceUpdates** folder on the System Platform Installation media for more information.

Any issues that would stop a normal GUI-based installation, such as the presence of incompatible software, will also prevent successful completion of a command-line installation. You can keep the command prompt open during installation by specifying the **/silentnoreboot** switch. This will let you view messages related to installation issues. Installation messages are lost when the system restarts. With the **/silentnoreboot** switch, you will need to manually restart the system after installation completes. If you allow the system to restart automatically, as it will if you use the **/silent** switch, you can search the log file for error conditions that may have stopped the installation from completing successfully.

**Note:** If the GUI installer would install any necessary prerequisites, the command line installer will also install these items.

All the sample response files contain information to create the Network Account for system communication. If another System Platform product was previously installed and the the Network Account was already created, subsequent installations will retain the original Network Account. A new account is not created.

For example, under those conditions, Setup.exe ignores the following properties in the response file:

```
AdminUserForm.SUserName
AdminUserForm.SPassword
AdminUserForm.SCreateLocal
AdminUserForm.SDomainName
```

```
AdminUserForm.SEnhancedSecurity
```

A good approach for testing is to first run the setup.exe in GUI mode on a typical computer and confirm that no incompatibilities exist that would stop the installation, then cancel and run by command line.

**Note:** If the GUI-based installation requires a system restart after the installation is complete, installing by command line will also require a system restart. Using the **/silent** switch allows the system to restart automatically. The **/silentnoreboot** switch suppresses the automatic restart, but will require a manual restart.

## Configure SQL SysAdmin Permissions

The information in this section applies only if the logged-in Windows user for installation does not have SQL SysAdmin permissions. If this is the case, use one of the following options.

**Option 1: Use SQL authentication (SA).** Add the following properties to the response file and configure them as indicated:

```
ConfigureSQL.SUserName=<SA User>
ConfigureSQL.SPassword=<SA Password>
ConfigureSQL.SQLAuthentication=true
```

**Option 2: Provide a Windows User who has SQL SysAdmin permissions.** Add the following properties to the response file and configure them as indicated:

```
ConfigureSQL.SUserName=<DOMAIN\USER>
ConfigureSQL.SPassword=<PASSWORD>
ConfigureSQL.SQLAuthentication=false
```

# Creating a Response File

Response files consist of an INSTALL section and a CONFIGURATOR section. See Response File Samples for examples that you can use after making minor edits.

**Install Section**

The INSTALL section defines the items that would be selected through the GUI installation dialog windows. These are:

- The root installation directory. The default path is C:\Program Files (x86).
  - Example:

    **FeatureForm.SInstallDir**=C:\Program Files (x86)
- The Network Account (name and password), used for inter-node and inter-product communications.
  - Example:

    **AdminUserForm.SUserName**=NetworkAccount

    **AdminUserForm.SPassword**=Password123
  - Other Settings (not included in Response File Samples; add these manually if needed):

    **AdminUserForm.SDomainName**=YourDomain

    **AdminUserForm.SEnhancedSecurity**=True/False
    - If True, the Network Account is NOT added to the system Administrators group.
    - If False, the Network Account is added to the system Administrators group.

- Acknowledgement of change to installation behavior:

  - **OutOfSupportRedistConsentForm.SRedistConsent**=false

  - Setting the parameter to true indicates that you acknowledge this information. If the parameter is left at its default, installation fails. See [Response File Entry to Acknowledge Installation Change Information (Redistributable Libraries)](#) for more information.

- Acknowledgement that a patch may be required for AVEVA Manufacturing Execution System and AVEVA Recipe Management to ensure compatibility with System Platform:

  - **CompatibilityAlert.SProductCompatibilityConsent**=false

  - Setting the parameter to true indicates that you acknowledge this information. If the parameter is left at its default, installation fails. See [Response File Entry to Acknowledge Compatibility Requirement](#) for more information.

- The components and related requirements that will be installed. You can specify by inclusion or exclusion:

  - Install by inclusion example:

  **FeatureForm.SFeatureList**=AVEVA System Platform.ASBRuntime,Application Server.Bootstrap,Application Server.IDE

  - To specify products by exclusion, first add ALL products with an inclusion statement, then list the ones that should be left out.
    Install by exclusion example:

  **FeatureForm.SFeatureList=ALL**

  **FeatureForm.SExcludeFeatureList**=InTouch Access Anywhere Secure Gateway.SecurityServer_Files,InTouch Access Anywhere Authentication

- Use the following language setting when installing System Platform on a non-English operating system:

  - Example:

  **LanguageForm.Language**=French

  Other options are German, Japanese, and SimplifiedChinese

## Configurator Section

The CONFIGURATOR section defines the components that would be configured through the Configurator GUI. These include the following:

- Product licensing example (to install a license server, define the license server name and port number):

  **AVEVA Enterprise Licensing.LicAPI2.NewServerName**=SE_LICENSE_SERVER_NAME

  **AVEVA Enterprise Licensing.LicAPI2.NewPortNumber**=55555

- ASB runtime examples. These entries are used to configure the System Management Server.

  **Common Platform.ASBRuntime.HttpPort** = 80

  **Common Platform.ASBRuntime.HttpsPort** = 443

  **Common Platform.ASBRuntime.ManagementServerPort** = 443

  **Common Platform.ASBRuntime.ManagementServerName** = MachineName

  **Common Platform.ASBRuntime.AsbManagedCertificates** = true

**Common Platform.ASBRuntime.BindingCertificateThumbprint** = thumbprint (optional required if AsbManagedCertificates = false, otherwise remove this parameter)

**Common Platform.ASBRuntime.UserName** = username

**Common Platform.ASBRuntime.Password** = password

- AVEVA System Monitor examples. These entries are used to configure the System Monitor Manager and Agent, formerly called Sentinel Manager and Agent.

    **AVEVA System Monitor.System Monitor Manager.AgentServerName**=ServerName

    **AVEVA System Monitor.System Monitor Manager.HttpPort** =httpPort (optional, if required input the httpPort value, otherwise remove this parameter (plugin will use the default httpPort value))

    **AVEVA System Monitor.System Monitor Manager.SslPort** =sslPort (optional, if required input the sslport value, otherwise remove this parameter (plugin will use the default sslPort value))

    **AVEVA System Monitor.Alert Email Server.SmtpOneClickConfigure** = false (set true, if the SMTP email server details enter later from System Monitor web interface and remove SmtpServerNameorIp,SmtpServerPort,SmtpServerSecured,SmtpUserName,SmtpPassword, SmtpFromRecipientEmailID and SmtpRecipientEmailID)

    **AVEVA System Monitor.Alert Email Server.SmtpServerNameorIp** = MachineName or IP Address

    **AVEVA System Monitor.Alert Email Server.SmtpServerPort** = portNo

    **AVEVA System Monitor.Alert Email Server.SmtpServerSecured** = false (set true, if the SMTP server needs user credentials to access the SMTP server)

    **AVEVA System Monitor.Alert Email Server.SmtpUserName** = username

    **AVEVA System Monitor.Alert Email Server.SmtpPassword** = password (UserName and Password parameters are not required, if the SMTP server needs user credentials to access the SMTP, you can remove the parameters if they are not required)

    **AVEVA System Monitor.Alert Email Server.SmtpFromRecipientEmailID** = from_EmailID

    **AVEVA System Monitor.Alert Email Server.SmtpRecipientEmailID** = email address for receiving alerts from the System Monitor Manager. Use a semicolon to separate multiple addresses

    **AVEVA System Monitor.Alert Email Server.HttpPort** =httpPort (optional, if required input the httpPort value, otherwise remove this parameter (plugin will use the default httpPort value))

    **AVEVA System Monitor.Alert Email Server.SslPort** =sslPort (optional, if required input the sslport value, otherwise remove this parameter (plugin will use the default sslPort value))

- Historian examples. These entries are used to configure the Historian.

    **AVEVA Historian.Historian.SilentTCPPort**=32568

    **AVEVA Historian.Historian.SilentchkBoxAutoStartHistorian**=true

    **AVEVA Historian.Historian.SilentDBOption**=REBUILD

    **AVEVA Historian.Historian.SilentDBPath**=C:\Program Files\Microsoft SQL Server\MSSQL10.SERVER \MSSQL\DATA

    **AVEVA Historian.Historian.SilentDataPath**=C:\Historian

    **AVEVA Historian.Historian.SilentSQLUserName**=SQLUserName

**AVEVA Historian.Historian.SilentSQLPassword**=SQLUserPW

**AVEVA Historian.Historian.SilentBlockStorageMode**=1

**AVEVA Historian.Search.SilentSearchInstall**=true

**AVEVA Historian.Extensions.SilentExtensionInstall**=true

# Response File Entry to Acknowledge Installation Change Information (Redistributable Libraries)

This release of System Platform does not install certain components from Microsoft and other third-parties that were installed in prior versions because they are now out-of-support. If you have custom-built objects or controls that rely on these components, you can still choose to install them. However, you must acknowledge this change before you can install System Platform. The GUI-based installation process displays a form describing the change in behavior. Silent install of System Platform requires that you change the setting of a parameter, as described below:

**IMPORTANT CHANGE TO INSTALLATION BEHAVIOR**

With this release of System Platform, AVEVA no longer installs older, out-of-support redistributable libraries from Microsoft or other vendors. For the long term sustainability and security of your system, AVEVA strongly recommends that you do not elect to install these libraries, which are outside their published support life cycle and will not necessarily receive any further functional or security-related fixes from their vendors in the future.

**CONSIDERATIONS FOR EXISTING PROJECTS**

If upgrading an existing project which includes custom-built executable components, which were added to the system after installation, consider that they may rely on these older libraries. Examples include but are not limited to:

- Objects developed using the Application Object Toolkit (AOT)

- Custom script libraries (DLLs)

- Third-party custom-built .NET controls

AVEVA recommends you recompile these custom components using the latest redistributable libraries. You should request updates/upgrades for third-party controls, libraries, and components from their vendors.

**Set the following parameter to true in your response file to indicate that you have read and acknowledged this information:**

`OutOfSupportRedistConsentForm.SRedistConsent=true`

Installation will not succeed if the parameter is left at its default value, if the parameter is not present in the response file, or if the parameter has an invalid configuration.

# Response File Entry to Install Out-of-Support Redistributables

If there are custom-built components in your solution, and in the rare case that you cannot update them before installing System Platform, you can install them silently by adding a parameter, "AVEVA System Platform.RedistInstall" to the SFeatureList, in the <Install> section of your response file:

**FeatureForm.SFeatureList**=**AVEVA System Platform.RedistInstall,**AVEVA System Platform.ASBRuntime,AVEVA System Platform.ASBServiceRepository,Application Server.Bootstrap,Application Server.Galaxy_Repository,AVEVA

Enterprise Licensing Platform.AELicenseManager,AVEVA Enterprise Licensing Platform.AELicenseServer,AVEVA System Monitor.SIM,AVEVA System Monitor.PSMSConsoleService

See [Response File Entry to Acknowledge Installation Change Information (Redistributable Libraries)](#) for more information about out-of-support redistributables and the limited number of reasons to install them.

## Response File Entry to Acknowledge Compatibility Requirement

A patch must be applied to the following products and versions to ensure compatibility with System Platform 2020 R2 SP1:

- Manufacturing Execution System 6.2.0. Older versions must be updated to version 6.2 and then patched.

- Recipe Management 4.5.0 and 4.6.0. These two most recent versions must be patched. Versions prior to 4.5 are compatible with System Platform 2020 R2 SP1 and do not require patching.

Even if your system does not include Manufacturing Execution System or Recipe Management, you must acknowledge that you are aware of this potential incompatibility and the need to fix it by applying the patch. The GUI-based installation process displays an alert if it detects either of these products on the node where you are installing System Platform. Please review the *Compatibility Readme*, located in the **InstallFiles>CoexistenceUpdates** folder on the System Platform Installation media for more information.

Silent installation of System Platform requires that you change the setting of a parameter, as described below, whether or not the products are installed:

**Set the following parameter to true in your response file to indicate that you have read and acknowledged this information:**

```
CompatibilityAlert.SProductCompatibilityConsent=true
```

Installation will not succeed if the parameter is left at its default value, if the parameter is not present in the response file, or if the parameter has an invalid configuration.

## Response File Entries to Configure the License Server

You can configure licensing through the silent install process by using a response .txt file. To configure the License Server, add the following entry to your .txt response file:

```
<configurator>
AVEVA Enterprise Licensing Platform.LicAPI2.NewServerName=SE_LICENSE_SERVER_NAME
AVEVA Enterprise Licensing Platform.LicAPI2.NewPortNumber=55555
</configurator>
```

Replace "SE_LICENSE_SERVER_NAME" with the name of your License Server. If you need change the port number, replace the default entry "55555" with the new port number.

## Response File Entries to Configure the System Management Server

The System Management Server (SMS) is used to establish machine trust between nodes. See [Configuring the System Management Server](#) for additional information. To configure the SMS silently, add the following entries to your .txt response file:

```
<configurator>

Common Platform.ASBRuntime.HttpPort=80

Common Platform.ASBRuntime.HttpsPort=443
```

```
Common Platform.ASBRuntime.ManagementServerPort=443
```

```
Common Platform.ASBRuntime.ManagementServerName=MachineName (input the Managment Server
name if need to configure to this Community Management Server)
```

```
Common Platform.ASBRuntime.AsbManagedCertificates=true
```

```
Common Platform.ASBRuntime.BindingCertificateThumbprint=thumbprint (optional required if
AsbManagedCertificates = false, otherwise remove this parameter)
```

```
Common Platform.ASBRuntime.UserName=username
```

```
Common Platform.ASBRuntime.Password=password (UserName and Password parameters are not
required if the current logged in user is authenticated to access the Management Server,
you can remove the parameters if they are not required)
```

```
Common Platform.ASBRuntime.IsRedundantSsoServer = true (Note: ensure ManagementServerName
to be the remote node machine name, not the local node machine name)
```

```
AVEVA System Monitor.System Monitor Manager.AgentServerName=ServerName
```

```
</configurator>
```

- **HttpPort** and **HttpsPort:** Edit the port numbers if necessary.

- **ManagementServerName:** Replace ManagementServerName with the name of the SMS node.

- **AsbManagedCertificates:** If you do not want the SMS to manage certificates, set the AsbManagedCertificates parameter to false. Note that if AsbManagedCertificates is false, you must enter the thumbprint value for the BindingCertificateThumbprint parameter. For information about acquiring a certificate thumbprint, see Using HTTPS Instead of HTTP for Historian Client, Insight, and REST APIs.

- **UserName and Password:** If you have not have a Network Account already configured, you must add the user name and password. If the Network Account already exists, the username and password parameters are ignored.

- **IsRedundantSsoServer:** The Redundant SSO Server feature is not available in this release. The IsRedundantSsoServer parameter is therefore ignored.

# Response File Samples

The response file samples are provided as .txt files on the installation DVD within the following directory path:
```
\InstallFiles\ResponseFiles\Samples\
```

These samples can be used as templates to initiate the installation of certain products or features during the silent install process.

**To use the response file samples as templates**

1. In Notepad or a similar text editor, open the appropriate response .txt file from the installation DVD. Refer to the Role-Based Response Files or the Product-Based Response Files sections to determine the correct .txt file to use.

2. Edit the response file as necessary.

   a. Edit the UserName, Password and CreateLocal (true or false) responses. The templates contain sample responses on these lines. Delete the sample responses, located to the right of the equal sign (=), and replace with your own response.

b. If you install Historian components, provide the SQL Server user name and password.

c. Acknowledge the change to the installation of out-of-support third party libraries by setting OutOfSupportRedistConsentForm.SRedistConsent to true. For important details, see Response File Entry to Acknowledge Installation Change Information (Redistributable Libraries).

d. Acknowledge that a patch to Manufacturing Execution System and/or Recipe Management may be needed to ensure compatibility with System Platform by setting CompatibilityAlert.SProductCompatibilityConsent to true. For important details, see Response File Entry to Acknowledge Compatibility Requirement.

3. Save the file to a directory on your local computer. Note the path and full name of the file.

4. From the command line, type the install command and provide the path and filename of the response file you want to use.

Example: `D:\setup.exe /silent c:\Documents\DevNode.txt`.

In this example, the setup.exe file is in the root directory of the DVD, and the development node response file is on the local C: drive in the specified directory.

5. Press **Enter** to start the specified installation.

## Role-Based Response Files

The following response files install and configure System Platform products to perform the functions of specific roles. All response files listed here can be found on the installation DVD under **InstallFiles\ResponseFiles \Samples**.

| Response File | Description |
|---|---|
| All | Installs and configures every product included with System Platform, except InTouch Access Anywhere Secure Gateway and InTouch Access Anywhere Authentication Server. Since this response file installs the Galaxy Repository, the License Server, System Management Server, and System Monitor Manager are also installed. |
| AVEVA Enterprise License Server Node | Installs and configures the AVEVA License Server, System Monitor Manager and other required components. The License Manager is not installed. |
| AVEVA Historian Client Node | Installs and configures the components required to connect to an existing Historian Server, analyze the data, and provide Application Server run-time components. |
| AVEVA Historian Server Node | Installs and configures the components required to host a Historian server, analyze the data with a Historian Client, and provide Application Server run-time components. |
| AVEVA InTouch Access Anywhere Secure Gateway Node | Installs and configures the AVEVA InTouch Access Anywhere Secure Gateway. No other components are installed. |

| Response File | Description |
|---|---|
| AVEVA System Platform Development Server | Installs and configures the components required to host the development server, in order to develop and test InTouch HMI and AVEVA OMI applications.<br><br>This response file includes the Galaxy Repository, License Server, System Monitor Manager, and System Management Server. |
| Remote AVEVA System Platform Development Client | Installs and configures the components required to connect to an existing development server in order to develop and test InTouch and System Platform applications. |
| Runtime Client | Installs and configures the components required to run InTouch HMI, the Historian client, and AppObject server run time. |
| System Monitor Manager Node | Installs and configures the System Monitor Manager and other required components. |

## Product-Based Response Files

The following response files install and configure the selected product or products of System Platform. All response files listed here can be found on the installation DVD under **InstallFiles\ResponseFiles\Samples**.

| Response File | Description |
|---|---|
| AVEVA Application Server | Installs and configures the components needed for Application Server run time and development. Since this response file installs the Galaxy Repository, the License Server, System Management Server, and System Monitor Manager are also installed. |
| AVEVA Application Server and AVEVA OMI Runtime | Installs and configures the components needed for Application Server and AVEVA OMI run-time. |
| AVEVA Application Server Development | Installs and configures the components needed for Application Server development. |
| AVEVA Application Server Galaxy Repository | Installs and configures the components needed for the Galaxy Repository. Since this response file installs the Galaxy Repository, the License Server, System Management Server, and System Monitor Manager are also installed. |
| AVEVA Enterprise License Server Node | Installs and configures the AVEVA License Server and System Monitor Manager and other required components. |
| AVEVA Historian | Installs and configures the components needed for the Historian. |
| AVEVA Historian Client | Installs and configures the components needed for the Historian Client. |

| Response File | Description |
|---|---|
| AVEVA InTouch HMI | Installs and configures the components needed for InTouch run time and development. Since this response file installs the Galaxy Repository, it also installs the License Server, System Management Server, and System Monitor Manager. |
| AVEVA InTouch HMI Development and Runtime | Installs and configures the components needed for InTouch run time and development. Since this response file installs the Galaxy Repository, it also installs the License Server, System Management Server, and System Monitor Manager. |
| AVEVA InTouch HMI Runtime Only | Installs and configures the components needed for InTouch run time only. |
| AVEVA InTouch Access Anywhere and Runtime | Installs and configures the components needed to run InTouch Access Anywhere and the InTouch run-time. |
| AVEVA InTouch Access Anywhere Authentication Server | Installs and configures the InTouch Access Anywhere Authentication Server. No other components are installed. |
| AVEVA InTouch Access Anywhere Secure Gateway | Installs the InTouch Access Anywhere Secure Gateway. No other components are installed. |
| AVEVA Enterprise Licensing Platform | Installs the AVEVA License Server, License Manager, System Monitor Manager and other required components. |
| System Monitor Manager | Installs the System Monitor Manager and other required components. |

# Appendix B

# Single Product Installation

You can create an alternative installation media source if you are installing only Historian, Historian Client, or the Application Server runtime, and you want to reduce network usage. This alternative installation source will be much smaller than the full set of installation files, and thus will be easier to send to remote locations. This is of particular value if your network connection to the remote site is slow or unreliable, and any of the following, or similar circumstances, apply:

- You have multiple nodes at a remote site on which you want to install only Historian, Historian Client, or the Application Server runtime.

- A firewall at the remote site restricts most off-site access, and having a local copy of the installation files is easier to manage than having to modify the firewall.

- Installing from a WAN-based share is impossible due to the speed or reliability of the network connection.

With this procedure, you will:

1. Create a new installation source that contains a subset of the installation files contained on the System Platform installation DVD.

2. Install Historian, Historian Client, or the Application Server runtime from this subset of files.

Copying the files, rather than installing from a remote location, eliminates the possibility of a time-out during installation.

## Guidelines for Creating a Compact Installation Source

**Important:** This process can only be used for installing Historian, Historian Client, or the Application Server runtime. Other product configurations are not supported.

The workflow for creating the compact installation source is:

1. Copy the entire contents of the System Platform installation DVD.

2. Delete language and product components that are not needed.

3. Copy the directory containing the remaining components to either:

   ▪ To the node where you will install the product.

   ▪ To a CD or DVD to be used as the installation disk.

When you run the installation program, components that were deleted will show as disabled (grayed-out) and unavailable for selection.

## Upgrading from a Previous Version

Do not delete folders for products that are already installed. The upgrade process will not complete if you do not upgrade all products previously installed on the node. For example, if both Historian and Historian Client are installed on the node, you must upgrade both.

# Preparation for Installing a Single Product

To install Historian, Historian Client, Application Server, or InTouch, you can choose not to install or copy unnecessary files.

- The root directory contains the installation program (setup.exe) and several document files. Two files in the root directory are absolutely required: Autorun.inf (1 KB) and Setup.exe (about 2,200 KB). The remaining files are documents: *Getting Started with AVEVA Licensing*, the *System Platform Installation Guide*, the *System Platform Virtual Implementation Guide*, the *System Platform Getting Started Guide*, and the *System Platform Readme*.

- The entire InstallITK folder (about 9 MB) is required.

The following table shows which subfolders in the InstallFiles folder are required for Historian, Historian Client, Application Server (including AVEVA OMI run time), and InTouch HMI development and run time. You can delete folders that are not required for the product you are installing. All file and folder sizes are approximate and provided for reference only.

| InstallFiles Folder (Component) | Approx Folder Size | Historian | Historian Client | Application Server | InTouch (Run time only or run time and development) |
|---|---|---|---|---|---|
| CD-ApplicationServer | 1.44 GB | **Required** | Optional | **Required** | **Required** |
| CD-ASBFramework | 361 MB | **Required** | **Required** | **Required** | **Required** |
| CD-Gateway | 67 MB | Optional | Optional | Optional | Optional |
| CD-Historian | 539 MB | **Required** | Optional | Optional | Optional |
| CD-HistorianClient | 56 MB | Optional | **Required** | **Required** | **Required** |
| CD-InSightPublisher | 30 MB | Optional | Optional | Optional | Optional |
| CD-Intouch | 369 MB | Optional | Optional | Optional | **Required** for English |
| If InTouch is required, delete language folders that are not needed (CD-InTouch = English). CD-IntouchCommon and CD-IntouchWebClient are required when InTouch is installed (all languages). | | | | | |
| CD-IntouchCommon | 334 MB | Optional | Optional | Optional | **Required** |
| CD-IntouchFrench | 354 MB | Optional | Optional | Optional | **Required** for French |
| CD-IntouchGerman | 350 MB | Optional | Optional | Optional | **Required** for German |

| InstallFiles Folder (Component) | Approx Folder Size | Historian | Historian Client | Application Server | InTouch (Run time only or run time and development) |
|---|---|---|---|---|---|
| CD-Intouch Japanese | 356 MB | Optional | Optional | Optional | **Required** for Japanese |
| CD-Intouch SChinese | 359 MB | Optional | Optional | Optional | **Required** for Chinese |
| CD-IntouchWebClient | 79 MB | Optional | Optional | Optional | **Required** |
| CD-IntouchWebClient is required when InTouch is installed (all languages). | | | | | |
| CD-Language Assistant | 162 MB | Optional | Optional | Optional | Optional |
| CD-LicAPI | 113 MB | **Required** | **Required** | **Required** | **Required** |
| CD-Licensing | 115 MB | **Required** | **Required** | **Required** | **Required** |
| CD-NGVisualization | 443 MB | Optional | Optional | **Required** | **Required** |
| CD-OIEngine | 157 MB | **Required** | **Required** | **Required** | **Required** |
| CD-OIGATEWAY | 20 MB | **Required** | **Required** | **Required** | **Required** |
| CD-SentinelAim | 7 MB | **Required** | **Required** | **Required** | **Required** |
| CD-SentinelManager | 33 MB | Optional | Optional | Optional | Optional |
| CD-Server | 50 MB | **Required** | Optional | Optional | Optional |
| CD-UnsupportedRedist | 0 MB | Optional | Optional | Optional | Optional |
| CoexistenceUpdates More details shown below | 258 MB | Optional | Optional | Optional | Optional |
| External | 2 MB | **Required** | **Required** | **Required** | **Required** |
| OutofSupportRedist More details shown below | 41 MB | Optional | Optional | Optional | Optional |
| Redist | 538 MB | See note (DOTNET) | See note (DOTNET) | See note (DOTNET) | See note (DOTNET) |
| • DOTNET | 175 MB | Optional | Optional | Optional | Optional |
| **If** .NET version 4.8 or higher is already installed, you can remove the DOTNET folder from Redist. | | | | | |
| • MSOLEDBSQL | 11 MB | **Required** | **Required** | **Required** | **Required** |
| • PreReqInstaller | 0 MB | **Required** | **Required** | **Required** | **Required** |

| InstallFiles Folder (Component) | Approx Folder Size | Historian | Historian Client | Application Server | InTouch (Run time only or run time and development) |
|---|---|---|---|---|---|
| • SQL2017EXPRESSCORE | 275 MB | Optional | Optional | Optional | Optional |
| See **Note**, below, about removing subfolder SQL2017EXPRESSCORE from Redist. | | | | | |
| • VC2012U4 | 13 MB | **Required** | **Required** | **Required** | **Required** |
| • VC2013U4 | 26 MB | **Required** | **Required** | **Required** | **Required** |
| • VC2019 | 37 MB | **Required** | **Required** | **Required** | **Required** |
| ResponseFiles | 0 MB | **Required** | **Required** | **Required** | **Required** |
| Support | 0 MB | **Required** | **Required** | **Required** | **Required** |
| UpgradeSupport | 38 MB | **Required** | **Required** | **Required** | **Required** |

**Note:** The Redist folder contains SQL Server Express in folder SQL2017EXPRESSCORE. You can remove Redist if:
- You are installing Historian Client. SQL Server is not required.
- You are installing Application Server, InTouch, or Historian, and SQL Server is already installed.
See [SQL Server Requirements](#) for information about supported versions of SQL Server.

**CoexistenceUpdates:** If AVEVA™ Manufacturing Execution System or certain versions of AVEVA™ Recipe Management are present, you may need the contents of this folder to ensure compatibility with System Platform 2020 R2 SP1. Affected products are:

- Manufacturing Execution System 6.2.0. Older versions must be updated to version 6.2 and then patched.

- Recipe Management 4.5.0 and 4.6.0. These two most recent versions must be patched. Versions prior to 4.5 are compatible with System Platform 2020 R2 SP1 and do not require patching.

  **Out-of-Support assemblies:** If needed for compatibility with migrated galaxies or custom objects, you may need to include this folder which includes the following assemblies:

| Redistributable Description | Folder/Assembly Name |
|---|---|
| Microsoft SQL Server 2012 Management Objects SP2 (11.2.5058.0) | SQL2012SP2FeaturePack\ SharedManagementObjects.msi (x64 and x86 versions)<br><br>SQL2012SP2FeaturePack\ SQLSysClrTypes.msi (x64 and x86 versions) |
| Microsoft Visual C++ 2008 Redistributable | VC90SP1/vcredist_x86.exe |
| Microsoft Visual C++ 2010 Redistributable | VC10SP1/vcredist_x64.exe<br>VC10SP1/vcredist_x86.exe |

## Optional Folder for Historian

The CD-InTouch folder contains a database purge utility that Historian uses (this utility is not called when block-based event history is utilized). Without this folder, Historian cannot purge the A2ALMDB alarm database and an error will be generated (this does not occur with block-based history). If you are installing Historian Client only, this utility is not called and the folder can be deleted without any issues.

**Note:** If you are installing Historian and the CD-Intouch has been deleted, you will not be able to purge the A2ALMDB alarm database and an error will be generated (does not apply if you are using block-based history). However, the installation will complete successfully.

# Creating the Installation Source and Installing the Selected Component

**To create an installation source**

1. Copy the entire contents of the System Platform installation DVD to a local folder on your computer or to a network share location.

   This location will be used to prepare for the installation or upgrade of the product you are installing.

   **Important:** You must copy the entire DVD. The root directory from the DVD and all files in it must be in place and completely intact.

2. Navigate to the location where you copied the DVD. Delete the files, components and language folders that you do not need.

   Now you are ready to install or upgrade the product(s) using either of the methods described below.

**To install or upgrade a single product**

Direct installation from the copy location (install locally or on a different network node):

1. Remove the original System Platform installation DVD from the drive.

   **Important:** When you run setup.exe, it checks for the System Platform installation DVD. If the installation DVD is available, it will be used instead of the copy location.

2. Navigate to the copy location.

3. Make sure you have deleted the folders you do not need.

4. Run setup.exe. Components that were deleted will be grayed-out and unavailable for installation.

5. If this is a new installation (not an upgrade), select the target location when you are prompted.

Installation from a CD or DVD:

1. Create a CD or DVD from the copy location after deleting the folders you do not need.

2. Run setup.exe from the CD/DVD on each node. Components that were deleted will be grayed-out and unavailable for installation.

# Ports Used by System Platform Products

## System Platform Ports

The following table lists ports used by System Platform products.

| Product | Process Name | Port | Add'l Port | Config-urable | Description | Protocol |
|---|---|---|---|---|---|---|
| Application Server | aaBootstrap.exe | 30000 | | Yes | Local redundancy primary port (WinPlatform) | TCP and UDP |
| | | 30001 | | Yes | Local redundancy message port (WinPlatform) | TCP |
| | | 49152 to 65535 | | No | DCOM Port Range | TCPV6 |
| | | 135 | | No | DCOM and RPC | TCP |
| | | 139 | | No | DCOM and Netbios (Bootstrap) | TCP |
| | | 445 | | No | DCOM and Netbios (Bootstrap) | TCP |
| | aaGlobalDataCache MonitorSvr.exe | 49152 to 65535 | | No | DCOM Port Range | TCPV6 |
| | aaGR.exe | 49152 to 65535 | | No | DCOM Port Range | TCPV6 |
| | | 8090 | | Yes | Configurable through registry: HKLM \SOFTWARE \ArchestrA \Framework \Remoting with key "defaultPort" and | TCP |

| Product | Process Name | Port | Add'l Port | Config-urable | Description | Protocol |
|---------|-------------|------|-----------|---------------|-------------|----------|
| | | | | | Value as <port number> string | |
| | | 49152 to 65535 | | No | DCOM Port Range | TCP and TCPV6 |
| | aaEngine.exe | 32568 | | Yes | "TCP Port" (WinPlatform Engine advanced settings) | TCP |
| | aaObjectViewer.exe | 49152 to 65535 | | No | DCOM Port Range | TCPV6 |
| | aaPIM.exe | 49152 to 65535 | | No | DCOM Port Range | TCPV6 |
| | aaPlatformInfoSvr.exe | 49152 to 65535 | | No | DCOM Port Range | TCPV6 |
| | aaUserValidator.exe | 49152 to 65535 | | No | DCOM Port Range | TCPV6 |
| | NmxSvc.exe | 5026 | | Yes | Message Exchange port number (WinPlatform) | TCP |
| | Multi Galaxy | 808 | | No | ASBMxDataProvider Service | TCP |
| | | 808 | | No | Galaxy Pairing | TCP |
| | | 808 | | No | ASBGRBrowsing Service | TCP |
| | | 808 | | No | ASBAuthentication Service | TCP |
| PCS | | 808 | 4600 | Yes | ASBOPCUAClient Service, ASB Core Service and others who use net tcp port sharing service (808 port) | TCP |
| PCS/ Historian | | 3575 | | Yes | Event Service | TCP |
| PCS/ Historian Service (PCS InProc Hosting) | | 3586 | | Yes | EventHistorian Service | TCP |

| Product | Process Name | Port | Add'l Port | Config-urable | Description | Protocol |
|---|---|---|---|---|---|---|
| PCS | PCS.IdentityManager. Host.exe SSDP | 1900 | | Yes | | UDP |
| | Asb.Discovery.exe, PCS.IdentityManager .Host.exe | 443 | | Yes | | HTTPS |
| | | 7084 | | Yes | System authentication (Only available during node registration) | TCP |
| | | 7085 | | Yes | System authentication (Only available during node pairing) | TCP |
| | Asb.Watchdog.exe, Asb.ServiceManager .exe, PCS.IdentityManager .Host.exe | 80 | | Yes | | HTTP |
| | | any | | Yes | OPC UA Server | TCP |
| Historian | | 135 | | | MDAS -Used by client nodes prior to ASP 2012 R2 | TCP and UDP |
| | | 136 | | | IDAS and Remote IDAS prior to Historian 2017 | TCP and UDP |
| | | 137 | | | IDAS and Remote IDAS prior to Historian 2017 | TCP and UDP |
| | | 138 | | | IDAS and Remote IDAS prior to Historian 2017 | TCP and UDP |
| | | 139 | | | IDAS and Remote IDAS prior to Historian 2017 | TCP and UDP |
| | | 445 | | | File and printer sharing | TCP |
| | | 445 | | | Remote IDAS prior to Historian 2017 | TCP and UDP |

| Product | Process Name | Port | Add'l Port | Config-urable | Description | Protocol |
|---|---|---|---|---|---|---|
| | | 1433 | | Yes | SQL Server - Used by Historian Client. Historian and Historian Client 2017 and later support non-default ports. | TCP |
| | | 1434 | | | SQL Server Browser | UDP |
| | aahClientAccess Point.exe | 32568 | | Yes | Historian, Remote IDAS 2017 and later, and Redundant AppServer node./ HCAL/HCAP | TCP |
| Historian Insight, OData | aahGateway.exe | 32569 | | Yes | Configured in Historian System Parameter "GatewayTcpPort."Configurable in Historian 2017 and later | TCP |
| Licensing | License Manager | 80 | | Yes | License Manager | |
| | License Server Core Service | 55555 | | Yes | License Server Core Service | |
| | License Agent | 59200 | | Yes | License Agent | |
| | License Manager to Activation server outbound | 443 | | Yes | License Manager to Activation server outbound | |
| OI Server | SI Direct | 102 | | | OI Server | |
| | MBTCP | 502 | | | OI Server | |
| | ABTCP | 2221 | | | OI Server | |
| | | 2222 | | | OI Server | |
| | | 2223 | | | OI Server | |
| | S/L OI Servers | 5413 | | | OI Server | |
| | DBServer | 5481 | | Yes | ATS | TCP |
| | ABCIP | 44818 | | | OI Server | TCP |
| | GESRTP OI Server | 18245 | | | OI Server | |

| Product | Process Name | Port | Add'l Port | Config-urable | Description | Protocol |
|---|---|---|---|---|---|---|
| OI Gateway | OI Gateway | 1883, 8883 | | Yes | OI Gateway MQTT connectivity | |
| InTouch Access Anywhere | AccessServer64. exe | 8080 | | | Server | TCP |
| | | 57733 | | | Server | TCP |
| | | 57734 | | | Server | TCP |
| | | 57735 | | | Server | TCP |
| | | 3399 | | | Server | TCP |
| | EricomSecure Gateway.exe | 443 | | | Secure Gateway | TCP |
| | | 57111 | | | Secure Gateway | UDP |
| Intouch Web Client | InTouchWeb. ContentHost.exe | 60152 | 60153 | | InTouch Web Client | TCP |
| | InTouchWeb.Host. exe | 60236 | 60237 60238 60311 60312 | | InTouch Web Client | TCP |
| | InTouchWeb.Server. exe | 60161 | 60162 | | InTouch Web Client | TCP |
| Intouch | InTouchDataService. exe, used for InTouchiData | 58398 | 60118 | | InTouchiData | TCP |
| Suitelink | | 5413 | | | | TCP |
| | | 49152 to 65000 | | | | TCP |
| Alarm Logger | aaLogger.exe | 1041 | | | Alarm Logger | TCP |
| | | 5004 | | | Alarm Logger | TCP |
| | Alg.exe | 1087 | | | Alarm Logger | TCP |
| Alarm Manager | Alarmmgr.exe | 51218 | | | | TCP |
| System Monitor | | 80 | | Yes | HTTP | |
| | | 443 | | Yes | HTTPS | |
| | | 25 | | Yes | SMTP | |
| | | 587 | | Yes | SMTPS | |

# Appendix D

# Common System Platform Processes

## AVEVA System Platform Processes

The following table describes AVEVA Application Server other required System Platform processes. For a description of services associated the the AVEVA Historian, see the *AVEVA Historian Administration Guide*.

| Service/Process Name | Executable Name | Description |
| --- | --- | --- |
| **Application Server/ArchestrA Services** | | |
| ArchestrA Bootstrap (aaBootstrap) | aaBootstrap.exe | Utility to bootstrap an ArchestrA run time to support code-module deployment and process monitoring. |
| Engine Module (aaEngine) | aaEngine.exe | Supports the creation, deletion, startup, and shutdown of objects hosted by the Engine object as the hosted objects are deployed and undeployed. |
| ArchestrA Galaxy Repository (aaGR) | aaGR.exe | The Galaxy Repository service to process requests to the ArchestrA configuration subsystem. |
| ArchestrA Global Data Cache Monitor Server (aaGlobaldata CacheMonitorSvr) | aaGlobaldata CacheMonitorSvr.exe | Global Data Cache Monitor service to process file change notifications. |
| ArchestrA Logger Service (aaLogger) | aaLogger.exe | Receives log messages from System Platform component products and stores them in a file. |
| ArchestrA User Validator (aaUserValidator) | aaUserValidator.exe | User validator service to process user validations for the ArchestrA framework. |
| Platform Info Server Module (aaPlatformInfoSvr) | aaPlatformInfoSvr.exe | Server module for the Network Account. |

| Service/Process Name | Executable Name | Description |
|---|---|---|
| **PCS/ASB Services** | | |
| PCS Framework Server Launcher Service | Asb.Service Manager.exe | Starts and stops hosted services on behalf of the watchdog. The Watchdog is a high-privilege process, which for security purposes, is not intended for hosted services. Therefore, the Watchdog delegates the tasks of starting and stopping monitored services to this lower-privileged process. |
| PCS Framework Watchdog Service | Asb.Watchdog.exe | Ensure services that provide discoverable endpoints are running. The Watchdog is for responsible for starting these services, monitors their health, restarts them as needed, and stops them when the Watchdog stops. The Watchdog also hosts other services such as the Deploy Service and Service Content Provider. |
| **Licensing Services** | | |
| License Server Agent Service | LicServer.Windows Service.exe | Provides the data model to operate the License Server. |
| License Server Core Service | AELicServer.exe | Provides the data model for the FNE Manager. |
| License Manager Web Service | LMWeb.Windows Service.exe | Provides web access for the License Manager. |

For more information on Windows services, see your Microsoft documentation.

# AVEVA

## Appendix E

# User Accounts and Groups Created by System Platform Installation

This section describes the user accounts and groups used by System Platform It is divided by product.

## Application Server OS Groups and Accounts

For System Platform 2020 R2 SP1, Application Server creates and uses the following user accounts, service accounts, and user groups.

| Name | Category | Description |
|------|----------|-------------|
| aaConfigTools | Group | Provides permissions to users to connect to a Galaxy from the IDE. |
| Performance Monitor Users | Group | Membership in the Performance Monitor Users group allows the Network Account to function without elevated privileges. See Network Account Membership, below, for more information. |
| PSMS Administrators | Group | Membership in the PSMS Administrators group allows the Network Account to function without elevated privileges. See Network Account Membership, below, for more information. |
| aaGalaxyOwner | User Account | This user account is the owner (dbo) of all Galaxy databases in your system. |
| NT SERVICE\ aaPIM | Windows Service Account | This is the platform installation manager. It is responsible for installing platforms. It is added to the Administrators group as a service account. |

**Network Account Membership**

The Network Account, also known as the ArchestrA Account, is used for off-line communications between System Platform nodes. To support Application Server, it may have membership in some or all of the following OS Groups, with the requirements and limitations as described below. Note that membership in some of these groups is dependent on whether or not this is a new installation or an upgrade of an older version of System Platform.

| Group Name | Description |
|---|---|
| Administrators | The Network Account will be part of the Administrators group ONLY if you are upgrading from System Platform 2017 Update 2 or prior release. If only Application Server is installed, you can remove the Network Account from this group. |
| Distributed COM Users | The Network Account will be part of the Distributed COM Users group ONLY if you are upgrading from System Platform 2017 Update 2 or prior release. If only Application Server is installed, you can remove the Network Account from this group. |
| Performance Monitor Users | This is a new OS Group added for System Platform 2017 Update 3 and later releases. It allows the Network Account to function without elevated privileges. Do not remove this group, and do not remove the Network Account from this group. |
| PSMS Administrators | This is a new OS Group added for System Platform 2017 Update 3 and later releases. It allows the Network Account to function without elevated privileges. Do not remove this group, and do not remove the Network Account from this group. |

## InTouch HMI OS Groups and Accounts

For System Platform 2020 R2 SP1, InTouch HMI creates and uses the following user accounts, service accounts, and user groups.

| Name | Category | Description |
|---|---|---|
| aaInTouchUsers | Group | Membership in this user group is required for viewing graphics from an application in the web browser. |
| ArchestrA WebHosting | Group | This user group supports the HTTPS protocol for the InTouch Web Client. |
| ASBSolution | Group | This user group provides the File System and Registry permissions required by the PCS (a.k.a ASB) Framework. |
| Administrators | Group | The Network Account may be included in the Administrators group if you have upgraded from version System Platform 2017 Update 2 or earlier. |
| NT SERVICE\ InTouchData Service | Windows Service Account | This Service Account is used by the InTouch Web Client or AVEVA OMI ViewApps to access InTouch tags. |
| NT SERVICE\ InTouchWeb | Windows Service Account | This Service Account is used by the InTouch Web Client to browse application graphics from a web browser. |

# InTouch Web Client OS Groups and Accounts

To support the HTTPS protocol for InTouch Web Client, Service Accounts added for InTouch HMI are given membership in the following OS Groups:

| Group | Account | Description |
|---|---|---|
| ArchestrAWeb Hosting | InTouchData Service | You can remove these service accounts from group if you are not using the InTouch Web Client or accessing InTouch tags from an AVEVA OMI ViewApp . |
| | InTouchWeb | |
| ASBSolution | InTouchData Service | You can remove these service accounts from the group if you are not using the InTouch Web Client or accessing InTouch tags from an AVEVA OMI ViewApp. |
| | InTouchWeb | |
| Performance Monitor Users | Network Account | This is a new OS Group added for System Platform 2017 Update 3 and later releases. It allows the Network Account to function without elevated privileges. Do not remove this group, and do not remove the Network Account from this group. |
| PSMS Administrators | Network Account | This is a new OS Group added for System Platform 2017 Update 3 and later releases. It allows the Network Account to function without elevated privileges. Do not remove this group, and do not remove the Network Account from this group. |

# Historian Server OS Groups and Accounts

For System Platform 2020 R2 SP1, Historian Server creates and uses the following user accounts, service accounts, and user groups.

| Name | Category | Description |
|---|---|---|
| aaAdministrators | Group | This user group provides read/write access for Historian Data, Batch Logon Privilege, write access to ArchestrA registry Hive and additional privileges on Runtime Database. A SQLServer service account (MSSQLServer) is added to this group to allow permitted users to perform data insertion to Historian through SQL. |
| aaPowerUsers | Group | Membership in this user group provides read/write access for Historian Data and Batch Logon Privilege. This user group also supports the HTTPS protocol for the InTouch Web Client. |

| Name | Category | Description |
|------|----------|-------------|
| aaReplicationUsers | Group | Membership in this user group allows its members to replicate data (Tier 2), and provides Batch Logon privilege. |
| aaUsers | Group | Membership in this user group provides read access for Historian data. |
| NT SERVICE\ aahClientAccessPoint | Windows Service Account | The Client Point Access Point Service is the data ingest layer. |
| NT SERVICE\ aahSearch Indexer | Windows Service Account | The Search Indexer Service indexes the tags to Historian Server. |
| NT SERVICE\ InSQLConfiguration | Windows Service Account | The InSQL Configuration Service manages the Historian Services. |
| NT SERVICE\ InSQLEvent System | Windows Service Account | The InSQL Event Service is the account for the Classic Event System service. |
| NT SERVICE\ InSQLManual Storage | Windows Service Account | The InSQL Manual Storage Service is the data import service that processes CSV file imports. |
| NT SERVICE\ InSQLStorage | Windows Service Account | The InSQL Storage Service is the Classic Storage Service that transforms data from the legacy IDAS service. |
| NT SERVICE\ InSQLIndexing | Windows Service Account | The InSQL Indexing Service is for indexing the History Blocks. |
| NT SERVICE\ InSQLIOServer | Windows Service Account | The InSQL IO Service provides access to data through Suitelink. |
| NT SERVICE\ InSQLSystemDriver | Windows Service Account | The InSQL System Driver Service captures data for System Tags. |
| NT SERVICE\ aahInSight | Windows Service Account | The aahInSight Service is for AVEVA InSight. |
| NT SERVICE\ aahSupervisor | Windows Service Account | The aahSupervisor Service is for the InSight Publisher host process. |

## Historian Account Group Membership

The following accounts and groups support Historian functionality

| Group | Account | Description |
|---|---|---|
| ArchestrAWeb Hosting | aahClientAccessPoint | aahClientAccessPoint is added to this group to allow access to the PCS certificate used for encrypting the transport. |
|  | InSQLIOServer | InSQLIOServer is added to this group to allow Secure Suitelink communication. |
| Performance Monitor Users | Historian Service (multiple Windows Service Accounts) | The Historian services are added to this group to acquire the performance counter information that will be historized as system tags. |
| Performance Log Users | Historian Service (multiple Windows Service Accounts) | The Historian services are added to this group to allow logging performance counters. |

## Platform Common Services Accounts and OS Groups

For System Platform 2020 R2 SP1, Platform Common Services, also referred to as ASB, creates and uses the following user accounts, service accounts, and user groups.

| Name | Category | Description |
|---|---|---|
| AsbCoreServices | Group | This user group contains the file system and registry permissions required by the core services of the PCS (ASB) framework. Since these processes are started by the ASB Watchdog, the only user account in this group should be the NT SERVICE\Watchdog_Service virtual service account. |
| ArchestrAWeb Hosting | Group | Members of this user group can listen to the shared HTTP (default=80) and HTTPS ports (default=443). Members of this group also have access to the private key of the security certificate used to bind to the HTTPS port. <br><br> To enable a secure SuiteLink connection, add the standard user to this group on the server side. For details, see the *AVEVA Communication Drivers Pack User Guide*, "Secured SuiteLink Connection" for details, available at [Installation Media]\InstallFiles\CD-OIEngine\Docs\OICore.pdf |
| ASBSolution | Group | Membership in this user group provides the File System and Registry permissions required by the PCS/ASB Framework. |

| Name | Category | Description |
|------|----------|-------------|
| NT SERVICE\ Watchdog_Service | Windows Service Account | Watchdog_Service runs as a high-privileged virtual service account. The group policy for this service requires AeServiceLogonRight. |
| NT SERVICE\ AsbService Manager | Windows Service Account | AsbServiceManager runs as the low-privileged virtual service account. The group policy for this service requires AeServiceLogonRight. |
| ASBCertificate RenewalService | Local Service Account | ASBCertificateRenewalService runs a local account, and is normally in a stopped state. It is only triggered by the Asb.Watchdog process, based on the validity of the local certificate. When the certificate is renewed, the service is stopped. The group policy for this service requires AeServiceLogonRight. |
| NT SERVICE\ AIMTokenHost | Windows Service Account | AIMTokenHost runs as a virtual service account once the System Management Server is configured. This is for the PCS.IdentityManager.Host. |
| NT SERVICE\ ArchestraData Store | Windows Service Account | ArchestraDataStore runs as a virtual service account. It starts and should continue to run once the installation is complete. |

## PCS Account Group Membership

The following accounts and groups support Historian functionality

| Group | Account | Description |
|-------|---------|-------------|
| ArchestrAWeb Hosting | AIMTokenHost | All processes which need access to the private key of certificates should be part of the ArchestrAWebHosting user group. |
| | AsbService Manager | To enable a secure SuiteLink connection, add the standard user to this group on the server side. For details, see the *AVEVA Communication Drivers Pack User Guide*, "Secured SuiteLink Connection," available at [Installation Media]\InstallFiles\CD-OIEngine\Docs \OICore.pdf. |
| ASBSolution | InTouchData Service | These two Windows Service Accounts are not technically PCS services, but are added to this group to support the InTouch Web Client. |
| | InTouchWeb | |

| Group | Account | Description |
|-------|---------|-------------|
| Users | AsbService Manager | NT SERVICE\AsbServiceManager is added to Users group is for backward compatibility. The legacy ASBService user was part of the Users group, and was replaced by the AsbServiceManager as of ASB version 4.2. If not needed for compatibility, AsbServiceManager can be removed. |

## AVEVA License Manager OS Groups and Accounts

For System Platform 2020 R2 SP1, AVEVA License Manager installs the following User Group. No users are added to the group by default. This group can be deleted if the user(s) accessing the License Server and License Manager is an administrator on that computer.

| Name | Category | Description |
|------|----------|-------------|
| AELicMgr | Group | Members of this group are granted non-administrator permission to access the License Server and/or License Manager installed on that node. |

## System Monitor OS Groups and Accounts

For System Platform 2020 R2 SP1, AVEVA System Monitor creates and uses the following service accounts.

| Name | Category | Description |
|------|----------|-------------|
| NT SERVICE\ psmsconsolSrv | Windows Service Account | These Windows services are added to the local Administrators user group when System Monitor is installed. |
| NT SERVICE\ simHostSrv | | |
| NT SERVICE\ adpHostSrv | | |

# Index