



# AVEVA™ System Platform Installation

2023 R2 P01

© 2015-2024 AVEVA Group Limited and its subsidiaries. All rights reserved.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, mechanical, photocopying, recording, or otherwise, without the prior written permission of AVEVA Group Limited. No liability is assumed with respect to the use of the information contained herein.

Although precaution has been taken in the preparation of this documentation, AVEVA assumes no responsibility for errors or omissions. The information in this documentation is subject to change without notice and does not represent a commitment on the part of AVEVA. The software described in this documentation is furnished under a license agreement. This software may be used or copied only in accordance with the terms of such license agreement. AVEVA, the AVEVA logo and logotype, OSIsoft, the OSIsoft logo and logotype, Archedra, Avantis, Citect, DYNsIM, eDNA, EYESIM, InBatch, InduSoft, InStep, IntelaTrac, InTouch, Managed PI, OASyS, OSIsoft Advanced Services, OSIsoft Cloud Services, OSIsoft Connected Services, OSIsoft EDS, PIPEPHASE, PI ACE, PI Advanced Computing Engine, PI AF SDK, PI API, PI Asset Framework, PI Audit Viewer, PI Builder, PI Cloud Connect, PI Connectors, PI Data Archive, PI DataLink, PI DataLink Server, PI Developers Club, PI Integrator for Business Analytics, PI Interfaces, PI JDBC Driver, PI Manual Logger, PI Notifications, PI ODBC Driver, PI OLEDB Enterprise, PI OLEDB Provider, PI OPC DA Server, PI OPC HDA Server, PI ProcessBook, PI SDK, PI Server, PI Square, PI System, PI System Access, PI Vision, PI Visualization Suite, PI Web API, PI WebParts, PI Web Services, PRISM, PRO/II, PROVISION, ROMEo, RLINK, RtReports, SIM4ME, SimCentral, SimSci, Skelta, SmartGlance, Spiral Software, WindowMaker, WindowViewer, and Wonderware are trademarks of AVEVA and/or its subsidiaries. All other brands may be trademarks of their respective owners.

#### U.S. GOVERNMENT RIGHTS

Use, duplication or disclosure by the U.S. Government is subject to restrictions set forth in the license agreement with AVEVA Group Limited or its subsidiaries and as provided in DFARS 227.7202, DFARS 252.227-7013, FAR 12-212, FAR 52.227-19, or their successors, as applicable.

AVEVA Legal Resources: <https://www.aveva.com/en/legal/>

AVEVA Third Party Software Notices and Licenses: <https://www.aveva.com/en/legal/third-party-software-license/>

# Contents

<b>Welcome to AVEVA System Platform .....</b>	<b>9</b>
<b>Prepare for System Platform installation .....</b>	<b>10</b>
License installation and activation .....	10
AVEVA System Monitor installation .....	11
Select System Platform components .....	12
Supported browsers .....	13
Supported languages .....	13
Supported operating systems .....	14
Supported InTouch Access Anywhere clients .....	15
System sizing guidelines .....	15
Supported and recommended node hardware types .....	18
Required installation order of additional products .....	20
Common components .....	20
Windows network configuration .....	21
AVEVA System Platform help system .....	22
System Platform prerequisites .....	22
SQL Server requirements for System Platform components .....	26
Unsupported SQL Server version error message .....	26
Select a type of installation .....	27
About product-based installation .....	27
About role-based installation .....	30
Network account .....	34
About network account privileges .....	34
<b>Install System Platform .....</b>	<b>35</b>
Install InTouch Access Anywhere .....	40
Install InTouch Access Anywhere Server .....	41
Install Secure Gateway .....	43
Configure ports for the InTouch Access Anywhere Secure Gateway .....	44
Install the Secure Gateway and Authentication Server separately or together .....	45
Install all components on a single server .....	46
<b>Configure System Platform components .....</b>	<b>48</b>
Using the Configurator .....	48
Common Platform Services .....	49
License Mode .....	49
System Management Server .....	50
System Management Server overview .....	50
Install System Management Server .....	50
Redundant SSO server .....	51

Work with Configurator .....	52
Connect a machine to a System Management Server .....	53
Configure the System Management Server .....	55
Run products without a System Management Server .....	57
Advanced Configuration .....	58
Certificates tab .....	58
Ports tab .....	60
Communications tab .....	61
Authentication tab .....	64
Federated Identity Provider .....	64
Troubleshooting connection problems .....	66
<b>Galaxy License Mode Configuration .....</b>	<b>69</b>
<b>Industrial Graphic Server Configuration .....</b>	<b>70</b>
<b>AVEVA Historian Configuration .....</b>	<b>71</b>
Using HTTPS Instead of HTTP for Historian Client, Historian Client Web, and REST APIs .....	76
Enabling Trust for a Self-Signed Certificate .....	78
Acquiring a Copy of the Self-Signed Certificate .....	78
Trusting a Self-Signed Certificate .....	82
<b>AVEVA Enterprise License Server Configuration .....</b>	<b>85</b>
<b>AVEVA System Monitor Configuration .....</b>	<b>86</b>
System Monitor Manager Configuration .....	87
Email Server Configuration .....	88
Advanced System Monitor Configuration .....	90
<b>System Restart after Configuration .....</b>	<b>91</b>
 <b>Upgrade, modify, and repair System Platform .....</b>	 <b>92</b>
<b>AVEVA Application Server upgrade .....</b>	<b>95</b>
About Upgrading Application Server .....	95
Upgradeable Application Server components .....	99
Windows upgrades .....	100
SQL Server upgrades .....	100
Issues with legacy common components .....	100
Basic upgrade sequence .....	100
Upgrade a Galaxy Repository node .....	101
Upgrade an IDE-only node .....	102
Migrate the Galaxy database .....	102
Upgrade run-time nodes .....	103
Upgrade redundant pairs .....	104
Upgrade considerations for multi-galaxy communication .....	107
<b>Modify an installation .....</b>	<b>108</b>
<b>Repair an installation .....</b>	<b>109</b>
 <b>Uninstall AVEVA System Platform .....</b>	 <b>112</b>
<b>Uninstall a System Platform component .....</b>	<b>112</b>
<b>Uninstall all components .....</b>	<b>112</b>

<b>Security and permissions</b>	<b>114</b>
Enhanced security for connecting to a Galaxy	114
Modify the network account	114
Change the network account from the CLI	115
SQL Server rights requirements	115
Set the SQL Server security mode	116
Restore required SQL Server accounts	117
Set the FIPS security policy option	118
<b>Configure SQL Server</b>	<b>119</b>
SQL Server requirements	119
Work with SQL Server versions	120
SQL Server not found on node: small configuration	121
SQL Server not found on node: medium and larger configurations	121
Compatible version of SQL Server already installed	121
New version of SQL Server already installed	121
Incompatible version of SQL Server already installed	122
Use a non-default port for SQL Server	122
Set a Windows firewall exception for the SQL Server port	123
<b>AVEVA InTouch HMI requirements and prerequisites</b>	<b>124</b>
Install the Gateway Communication Driver and upgrade from FS Gateway	124
Compatibility with existing FS Gateway applications	125
OI Gateway installation scenarios	126
<b>AVEVA Historian server requirements and recommendations</b>	<b>129</b>
Server requirements	129
High availability support	131
Requirements for Historian Management tools	131
Remote IDAS requirements	131
Security considerations for a remote IDAS	132
Disk sizing and data storage	132
General hardware recommendations for storage	133
Plan for disk space requirements	133
Disk space requirements for database files	133
Disk space requirements for historical data files	134
Storage and network transmission sizes for tags	134
Disk space estimation	136
Bandwidth estimation for streaming data	136
Bandwidth estimation for store-and-forward data	137
Time estimation for store-and-forward data	138
About data compression and the buffer age limit	138
Performance considerations	139
Server loading	139
IDAS performance	140
Tiered historians	140

Storage subsystem performance .....	141
<b>Networking recommendations .....</b>	<b>141</b>
<b>Client access .....</b>	<b>142</b>
<b>Support for non-English operating systems .....</b>	<b>142</b>
<b>Integration with other AVEVA products .....</b>	<b>143</b>
<b>System sizing examples .....</b>	<b>143</b>
Process Historian sizing examples .....	143
Server 1 (Non-Tiered): 2.4 GHz single processor quad-core CPU .....	143
Historian specifications .....	144
Tag information .....	144
Remote IDAS .....	144
Event information .....	144
Query load .....	144
Performance results .....	145
Server 2 (non-tiered): four dual-core 2.7 GHz CPUs .....	145
Historian specifications .....	145
Tag information .....	145
Remote IDAS .....	146
Event information .....	146
Query load .....	146
Performance results .....	147
Server 3 (non-tiered): four dual-core 3.4 GHz CPUs .....	147
Historian specifications .....	147
Tag information .....	147
MDAS .....	147
Remote IDAS .....	147
Event information .....	148
Query load .....	148
Performance results .....	149
Server 4 (tier-2): eight dual-core 2.67 GHz CPUs (hyper-threaded) .....	149
Historian specifications .....	149
Tag information .....	149
Query load .....	149
Performance results .....	150
SCADA (tiered) historian sizing examples .....	150
Topology 1: centralized tiered Historian topology on a slow/intermittent network .....	150
Tier 2 Historian specifications .....	150
Tier 1 Historian specifications .....	151
Loading information .....	151
Performance results for the tier-2 Historian .....	151
Latency results .....	152
Topology 2: centralized tiered Historian topology for a single physical location .....	152
Tier 2 Historian specifications .....	152
Tier 1 Historian specifications .....	152
Loading Information .....	153
Performance results for the tier-2 Historian .....	153
Latency results .....	153
Topology 3: simple tiered Historian topology for a modem configuration .....	154
Tier 2 historian specifications .....	154

Tier 1 Historian specifications .....	154
Loading information .....	155
Performance results for the tier-2 Historian .....	155
Latency Results .....	155
<b>AVEVA Historian Server installation and configuration .....</b>	<b>156</b>
Prepare for the Historian installation .....	156
Microsoft SQL Server installation .....	156
Historian installation features .....	157
About Historian installation .....	158
Test the installation .....	159
Antivirus software .....	159
Historian menu shortcuts .....	159
Repair Historian .....	160
Modify the Historian installation .....	160
Uninstall Historian .....	160
Upgrade from a previous version .....	160
About database migration .....	160
Upgrade the Historian version (Microsoft SQL Server 32-bit) .....	161
Upgrade the Historian version .....	161
Migration of History data stored in SQL Server .....	162
<b>AVEVA Historian Client information .....</b>	<b>163</b>
About the Historian Client .....	163
Historian Client components .....	163
Desktop applications .....	163
Microsoft Office add-ins .....	163
ActiveX and .NET controls .....	164
Requirements and recommendations .....	164
Support for operating system language versions .....	164
<b>AVEVA Historian Client installation and configuration .....</b>	<b>165</b>
About Historian Client installation .....	165
Use Historian Client software with roaming profiles .....	165
Repair the Historian Client installation .....	166
Uninstall Historian Client .....	166
Upgrade from a previous version .....	166
<b>Use silent installation .....</b>	<b>168</b>
Start silent installation .....	168
Use response files .....	169
Create a response file .....	171
Response file entry to acknowledge installation change information (redistributable libraries) .....	172
Response file entry to acknowledge compatibility requirement .....	173
Response file entries to configure the common platform .....	174
Response file entries to configure the industrial graphic server .....	175

Response file entries to configure Historian .....	176
Response file entries to configure the License Server .....	176
Response file entries to configure System Monitor .....	176
<b>Response file samples .....</b>	<b>177</b>
Role-based response files .....	178
Product-based response files .....	179
 <b>Single product installation .....</b>	 <b>181</b>
<b>Guidelines for creating a compact installation source .....</b>	<b>181</b>
Upgrade from a previous version .....	181
<b>Preparation for installing a single product .....</b>	<b>182</b>
Optional folder for Historian .....	185
<b>Create the installation source and install the selected component .....</b>	<b>185</b>
 <b>Common System Platform processes .....</b>	 <b>186</b>
AVEVA System Platform processes .....	187
 <b>Ports used by System Platform products .....</b>	 <b>190</b>
 <b>User accounts and groups created by System Platform installation .....</b>	 <b>196</b>
Application Server OS groups and accounts .....	196
InTouch HMI OS groups and accounts .....	197
InTouch Web Client OS groups and accounts .....	198
Historian Server OS groups and accounts .....	199
Platform Common Services accounts and OS groups .....	201
AVEVA License Manager OS groups and accounts .....	203
System Monitor OS groups and accounts .....	204



# Welcome to AVEVA System Platform

Welcome to this AVEVA System Platform Installation Guide.

As you use this guide, we really want your feedback, because you are helping us to make this a better product. We will work closely with you to understand what you want out of System Platform so that we can improve future versions. If you experience any difficulty using AVEVA System Platform, please let us know.

Thank you,

*The AVEVA System Platform Team*

# Prepare for System Platform installation

This guide describes how to install AVEVA™ System Platform.

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 [Select a type of installation](#) for additional information.

Make sure that your computer meets or exceeds the hardware and software requirements. System Platform 2023 R2 SP1 is not supported on 32-bit operating systems.

Some System Platform components (Application Server Galaxy Repository, Historian Server, System Monitor) require SQL Server. If you are installing one of these components, and you have a version of SQL Server pre-installed that is not compatible for any reason, installation stops and an error message is displayed. For more information, see [Unsupported SQL Server version error message](#). The System Platform installation process will optionally install SQL Server Express if SQL Server is not detected on your computer.

Apply all relevant Windows patches and updates prior to installing or upgrading System Platform. If SQL Server is required for the products you are installing, apply all cumulative updates at this time also.

## License installation and activation

A valid product license or subscription 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 (see [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). If you are using Operations Control connected experience, subscriptions are managed through CONNECT. An internet connection is required for CONNECT. Note that the License Server is still required for certain server and non-user facing applications, even if you are using Operations Control connected experience.

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 [Install System Platform](#).
2. Configure the common platform services and the System Management Server. See [Common Platform](#).
3. Configure the AVEVA Enterprise License Server (and Historian, if installed). See [Configure AVEVA Enterprise Licensing](#) (and [Configure AVEVA Historian](#)),
4. 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 format for its URL:  
https://<nodename/AELicenseManager  
The License Manager opens in your browser.
5. 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.
6. 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.

---

## Select System Platform components

The following lists show the System Platform components available for installation.

### AVEVA Application Server and OMI Components

- System Platform IDE
- Application Server Galaxy Repository
- Application Server Platform (runtime)
- Operations Management Interface (OMI) ViewApp (runtime)
- OMI Web Server

### AVEVA OMI Apps

- OMI ContentPresenter App
- OMI Map App
- OMI Standard Apps

### AVEVA OMI Widgets

- Carousel Widget
- DataGrid Widget
- QRCode Scanner Widget
- Teamwork Widget
- Web Browser Widget

### AVEVA InTouch HMI and InTouch Access Anywhere Components

- InTouch WindowMaker
- InTouch WindowViewer

- InTouch Web Server (Web Client)
- InTouch Workspaces
- InTouch Access Anywhere Server
- InTouch Access Anywhere Secure Gateway

## AVEVA Historian

- Historian Server (Desktop/Server)
- Historian Client Web (Insight Local)
- Historian Client Desktop
- Insight Publisher

## AVEVA Common Services

- Communication Driver Pack
- Common Services Framework
- AVEVA Enterprise Licensing
- System Monitor

## Supported browsers

---

**Important:** Cookies must be enabled in ALL browsers, even while in private browsing or incognito mode.

---

Supported browsers are used for configuration in AVEVA CONNECT, for downloading System Platform, and for viewing user documentation.

AVEVA System Platform supports the following browsers:

- Google Chrome
- Microsoft Edge, version 79 or newer
- Mozilla Firefox

AVEVA System Platform no longer supports the following browsers:

- Microsoft Internet Explorer 11
- Microsoft Edge, version 78 or older

## Supported languages

We are pleased to provide examples in the following additional languages: French, Spanish, simplified Chinese. They can be enabled and updated by an administrator.

## Supported operating systems

---

**Important! System Platform is supported on 64-bit operating systems only.**

---

System Platform 2023 R2 SP1 is supported on the following Windows client and server operating systems (64-bit only). This list was compiled at the release of System Platform 2023 R2 SP1. Check the [AVEVA GCS](#) web site for the latest information. Apply operating system patches and updates prior to installing or upgrading System Platform.

---

**Note:** The same operating system support applies to InTouch Access Anywhere.

---

Note that when Windows updates run in the background, there is the possibility that different software processes can be adversely affected. Therefore, it is important to schedule the updates to run only during planned shutdown periods.

### Configuring Automatic Windows Updates

If Windows is configured to update automatically, these automatic updates, when running in the background, can disrupt System Platform components, including Application Server and OMI during installation/upgrade, configuration and run-time operations. These updates may cause the IDE, GR, OMI Web Client and related components, and other services to shutdown unexpectedly. Therefore, we recommend that you disable automatic Windows updates, or otherwise ensure the updates will be installed only when System Platform applications are not being actively used.

### Client Operating Systems

#### *Semi-Annual Channel Releases:*

- Windows 10 21H2 Pro, Enterprise, and IoT Enterprise [Microsoft support ends 11 Jun 2024]
- Windows 10 22H2 Pro, Enterprise, and IoT Enterprise [Microsoft support ends 14 Oct 2025]
- Windows 11 21H2 Pro, Enterprise, and IoT Enterprise [Microsoft support ends 8 Oct 2024]
- Windows 11 22H2 Pro, Enterprise, and IoT Enterprise [Microsoft support ends 14 Oct 2025]
- Windows 12 24?? Pro, Enterprise, and IoT Enterprise [End of support date not yet announced]

#### *Long Term Service Channel Releases:*

- Windows 10 Enterprise, IoT Enterprise 2015 LTSB (1507) [Microsoft support ends 14 Oct 2025]
- Windows 10 Enterprise, IoT Enterprise 2016 LTSB (1607) [Microsoft support ends 13 Oct 2026]
- Windows 10 Enterprise, IoT Enterprise 2019 LTSC (1809) [Microsoft support ends 09 Jan 2029]
- Windows 10 Enterprise 2021 LTSC (21H2) [Microsoft support ends 12 Jan 2027]
- Windows 10 IoT Enterprise (Only) 2021 LTSC (21H2) [Microsoft support ends 13 Jan 2032]
- Windows 11 Enterprise, IoT Enterprise 2024 LTSC [End of support not yet announced]

### Server Operating Systems

#### *Long Term Service Channel Releases:*

- Windows Server 2016 LTSC Standard and Datacenter [Microsoft support ends 12 Jan 2027]
- Windows Server 2019 LTSC (Datacenter, Essentials, Standard) [Microsoft support ends 9 Jan 2029]
- Windows Server IoT 2016 LTSC [Microsoft support ends 12 Jan 2027]
- Windows Server IoT 2019 LTSC [Microsoft support ends 9 Jan 2029]
- Windows Server 2022 LTSC Standard and Datacenter [Microsoft support ends 14 Oct 2031]
- Windows Server 2025 LTSC Standard and Datacenter [End of service to be announced]

---

**Note:** System Platform is not supported on any version of Windows prior to Windows 10, or on Windows Server versions prior to 2016.

---

## Supported InTouch Access Anywhere clients

InTouch Access Anywhere has been tested in the following HTML5-capable browsers:

- Google Chrome version 98.0.4758.80 and newer
- Firefox version 96.03 ESR and newer
- Microsoft Edge Non-Chromium
- Microsoft Edge Chromium 97.0.1072.76 and newer
- Safari version 15.2 and newer (Mac and iOS only) (Not Windows)
- Opera version 83.0.4254.16 and newer

## System sizing guidelines

The following table provides guidelines for System Platform hardware configurations, 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 Knowledge and Support Center website (<https://softwaresupport.aveva.com/>) for supported versions of Windows operating systems and SQL Server.

- An HD display is recommended for engineering tools such as the System Platform IDE.
- A 64-bit operating system is required, regardless of system size.
- A Windows Server operating system is required for large installations.
- SQL Server Express is supported only for small systems, that is, installations with less than 25,000 I/O per node.
- Pagefile.sys, the Windows paging file (also called the swap file or virtual memory file), must be enabled. The Windows default setting is enabled.

To access the relevant information from the Technology Matrix, go to the Knowledge and Support Center website, select the Technology Matrix icon, and then enter the name of the System Platform product (for example, Application Server or Historian), or enter the Windows or SQL Server version you wish to use (for example, SQL Server 2022 Standard x64).

## Definitions

In the table below, hardware guidelines for different types of System Platform are listed. Definitions for the terminology used in the table are:

### **Level (Minimum and Recommended)**

Minimum level describes the baseline hardware configuration that will provide at least minimally acceptable performance for the role. Recommended level describes an expanded hardware set that provides improved performance.

### **IDE Node**

IDE nodes are engineering workstations. These are used for creating, editing, and deploying objects.

### **Application Object Server Node**

Application Object Server nodes, also called AOS nodes, are remote run-time nodes. AppEngines, and the objects assigned to them, are deployed from the Galaxy Repository to AOS nodes, where the AppEngines run on the AOS WinPlatform object. Each active AppEngine requires one logical processor and runs as a 32-bit process. We recommend that each AppEngine in a redundant pair is also assigned one logical processor (one for active and one for standby). If redundant AppEngines consume less than 40% of CPU and memory resources, you can allocate one active and one standby AppEngine to a single logical processor. However, if the AppEngines exceed 40% of the computing resources, you run the risk of overleveraging the node (i.e., CPU and/or memory usage hits 100%) when a failover occurs.

### **AOS resource allocation**

Areas are assigned to AppEngines, and objects are assigned to areas. The total number of objects that can be assigned to a single AppEngine is very variable, and depends on the complexity of the objects, including the number of attributes, attribute datatypes, if the object is running scripts, script complexity, and if the object contains graphics (owned graphics will take more memory than linked graphics). In most system configurations, an AppEngine can host anywhere from 5,000 to 50,000 objects, but even this broad range does not cover non-typical configurations, depending on the factors just mentioned (attributes, datatypes, owned graphics, etc.). For example, a single object attribute of datatype BigString can, conceivably, consume 2 GB of memory. All of the areas and objects under them that are assigned to an AppEngine cannot require more than 2 to 3 GB of total memory. Do not forget to take into account CPU, memory, and disk requirements for running Windows when provisioning the AOS nodes. Device Integration objects also run on the AppEngine and consume resources.

### **AOS deployment performance**

When you deploy a galaxy, the GR node is deployed first. After the GR, remote AOS platforms are deployed. Deployment of AppEngines to the AOS platforms is done in parallel. The AppEngines, along with the areas and the objects they contain are deployed serially. Thus, deployment is much quicker if you use multiple AOS nodes, each hosting fewer AppEngines, rather than using a single AOS node to host, for example, 30 active AppEngines. The improvement in deployment performance that you gain by using multiple nodes is nearly linear. Using two AOS nodes instead of one can reduce deployment time by half, using four AOS nodes reduces the time to a quarter, eight nodes reduces the time to an eighth. Once the AppEngines are deployed, deployment of areas and their contained objects to each AppEngine occurs serially. Thus, deployment is much more efficient if you use multiple, AOS nodes that are provisioned with fewer hardware resources, rather than using a few, highly-resourced nodes.

### **Galaxy Repository Node**

Galaxy Repository nodes, also called GR nodes, host the galaxy database. The GR is tightly coupled to a Microsoft SQL Server database.

### **Historian Server Node**

Historian Server nodes host the AVEVA Historian. The Historian is tightly coupled to a Microsoft SQL Server



database.

### Thin Client

Thin clients include smart phones and tablets. In the context of System Platform, thin clients are platforms for web browsers and remote desktop sessions (for example, InTouch Access Anywhere clients).

### Client

In the context of System Platform, clients are computers that can be used to develop and/or view and interact with applications. Remote IDE workstations, as well as for run-time applications like WindowViewer, AVEVA OMI ViewApps, and Historian Insight can be System Platform clients.

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 <sup>1</sup>	RAM <sup>3</sup>	Free Disk Space <sup>2, 3</sup>	Network Speed
<b>Application Object Server (AOS) Nodes <sup>5, 6</sup></b>					
<b>Small AOS Node</b> 1 - 6 AppEngines	Minimum	4	4 GB	100 GB	100 Mbps
	Recommended	8	8 GB	200 GB	1 Gbps
<b>Medium AOS Node</b> 6 - 15 AppEngines	Minimum	8	8 GB	200 GB	1 Gbps
	Recommended	16	16 GB	500 GB	1 Gbps
<b>Large AOS Node</b> 15 - 30 AppEngines	Minimum	16	16 GB	500 GB	1 Gbps
	Recommended	32	24 GB	1 TB	Dual 1 Gbps
<b>Galaxy Repository Nodes</b>					
<b>Small Galaxy</b> 1 - 50,000 I/O per Node	Minimum	4	2 GB	100 GB	100 Mbps
	Recommended	8	4 GB	200 GB	1 Gbps
<b>Medium Galaxy</b> 50,000 - 200,000 I/O per Node	Minimum	8	8 GB	200 GB	1 Gbps
	Recommended	16	12 GB	500 GB	1 Gbps
<b>Large Galaxy</b> > 200,000 I/O per Node	Minimum	16	16 GB	500 GB	1 Gbps
	Recommended	32	24 GB	1 TB	Dual 1 Gbps
<b>Historian Server Nodes</b>					
<b>Small Historian</b> 1 - 50,000 Historized Tags per Node	Minimum	4	2 GB	100 GB	100 Mbps
	Recommended	8	4 GB	200 GB	1 Gbps
<b>Medium Historian</b> 50,000 - 200,000 Historized Tags per Node	Minimum	8	8 GB	200 GB	1 Gbps
	Recommended	16	12 GB	500 GB	1 Gbps
<b>Large Historian</b> > 200,000 Historized	Minimum	16	16 GB	500 GB	1 Gbps

Tags per Node	Recommended	32	24 GB	1 TB	Dual 1 Gbps
<b>Thin Client Node</b>					
RDP clients, InTouch Access Anywhere browsers, mobile devices	Minimum	2	512 MB	N/A	100 Mbps
	Recommended	4	2 GB	N/A	100 Mbps
<b>Client Node</b>					
WindowViewer, ViewApp, Historian Client, Remote IDE	Minimum	4	1 GB	100 GB	100 Mbps
	Recommended	8	4 GB	200 GB	1 Gbps
<b>Remote Desktop Server Nodes</b>					
Basic RDS, InTouch Access Anywhere 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, InTouch Access Anywhere 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
<b>All-in-One Node</b> <sup>4</sup> (all products on a single node)					
<b>Small Application</b> 1,000 I/O max	Minimum	8	8 GB	200 GB	100 Mbps
	Recommended	12	12 GB	500 GB	1 Gbps
<b>Medium Application</b> 20,000 I/O max	Minimum	12	16 GB	500 GB	1 Gbps
	Recommended	16	32 GB	1 TB	1 Gbps
<b>Large Application</b> <sup>7</sup> 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) You can deploy two AppEngines (one active and one standby) per logical processor provided that the CPU and memory load is less than 40% for each AppEngine.

6) Using multiple Application Object Server platform nodes reduces deployment time.

7) 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
ApplicationObject Server (AOS)	Preferred	Supported	Supported	No	Supported
System Platform IDE	Preferred	Supported	Supported	RDP	Supported
AVEVA OMI ViewApp Runtime	Supported	Supported	Preferred	ITAA/RDP	Supported
InTouch HMI Standalone					
InTouch WindowMaker	Supported	Supported	Preferred	RDP	Supported
InTouch WindowViewer / InTouch ViewApp (runtime only)	Supported	Supported	Preferred	ITAA/RDP	Supported
InTouch for System Platform					
InTouch WindowMaker (with Managed Apps)	Preferred	Supported	Supported	RDP	Supported
InTouch 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 2023 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 2023 R2 SP1:

1. Install the product (Alarm Adviser, Intelligence, etc.) first.
2. Then, install System Platform 2023 R2 SP1.

InBatch 2017 or prior versions must installed **after** installing System Platform 2023 R2 SP1.

1. Install System Platform 2023 R2 SP1.
2. Then, install InBatch.

## Common components

System Platform 2023 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 2023 R2 SP1	23.2.100	Required
AVEVA Platform Common Services 8.1	8.1.24278.2	Required

Component	Version	Required/ Optional
AVEVA Help	23.2.000	Optional
AVEVA Enterprise License Manager 4.1.0	4.1.0	Required
AVEVA Enterprise License Server Legacy Support 4.1.0	4.1.0	Optional (see note 1)
AVEVA Enterprise License Server 4.1.0	4.1.0	Optional (see note 2)
AVEVA Enterprise Licensing Platform 4.1.0	4.1.0	Required
AVEVA Enterprise Licensing Platform (x86) 4.1.0	4.1.0	Required
Operations Control Logger	23.2.000	Required
Operations Control Management Console	23.1.000	Required
System Monitor Install Manager 1.6	1.6.0	Optional
System Monitor Manager 1.6	1.6.0	Optional

**Note 1:** Legacy support is required if there are any nodes that are not using Licensing 4.x. If all nodes are using License Server 4.x, and licensing is configured as secure, then legacy support can be removed.

**Note 2:** 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 as 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, open the Local Security Policy app and set network access permissions for anonymous users as follows:

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

Or, you can enter the following command from an administrator command prompt:

```
reg add HKLM\System\CurrentControlSet\Control\Lsa /v EveryoneIncludesAnonymous /t REG_DWORD /d 1
```

## AVEVA System Platform help system

### Web help - browser-based user assistance

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.

You can open help from within the System Platform IDE, InTouch WindowMaker, and other System Platform component products by pressing F1. You can also access the help system from the Windows start menu (located under the AVEVA folder). Or, you can simply enter **AVEVA Help** to locate and open the browser-based help library.

### Supported browsers

- Microsoft Edge Non-Chromium
- Microsoft Edge Chromium 97.0.1072.76 and newer
- Firefox version 96.03 ESR and newer
- Google Chrome version 98.0.4758.80 and newer
- Opera version 83.0.4254.16 and newer

## System Platform prerequisites

### Operating System and SQL Server

A 64-bit Windows operating system is required for installing and running System Platform 2023 R2 SP1 and its component products. Some System Platform 2023 R2 SP1 components, such as the Application Server Galaxy Repository and the AVEVA Historian also require a 64-bit version of Microsoft SQL Server.

Check the [AVEVA GCS Technology Matrix](#) website for more information about supported Windows and SQL Server versions for the System Platform 2023 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 (if required for the components being installed), **must** be installed before launching the System Platform setup program. See [Use silent installation](#) for more information. SQL Server is required for the Galaxy Repository, Historian, and System Monitor.

### .NET Framework

- System Platform requires **Microsoft .NET® Framework 4.8**, plus some additional .NET 8.0 run-time components. Prior to any other installation task, System Platform checks if all the required .NET components

are installed. If 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. The .NET run-time components required for System Platform are:

- .NET Runtime (x64)
- ASP.Net Core Runtime - windows hosting bundle (x64)
- .NET Desktop Runtime (x64)
- If an error occurs during setup that stops the .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**
- In some cases, a higher version of the run-time .NET components may already be installed on your computer than those included on the System Platform installation DVD. Normally, this does not stop installation. However, if your computer has some, but not all, of the required run-time modules that are at a higher version (.NET Runtime, ASP .NET Core Runtime, and .NET Desktop Runtime), an error message is shown and you are prompted to download the latest version of .NET. This is because all of the modules must be at the same version.

#### 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, Historian Server or System Monitor. If a supported version of SQL Server is not found, you are given the option to install **SQL Server 2022 Express Core** (with Advanced Tools) as part of System Platform installation. However, SQL Server Express supports only small installations with less than 25,000 I/O per node. See the [Technology Matrix](#) on the AVEVA Global Customer Support website for the current list of supported SQL Server versions.

No SQL Server default instance found

SQL Server is required for the product(s) you selected, but a supported version of SQL Server was not found. To proceed, select one of the following options.

☒ Install SQL Server Express and continue installation.  
☐ Exit installation and install a supported SQL Server version.

Refer to the Technology Matrix on the AVEVA Global Customer Support website (<https://gcsresource.aveva.com>) for SQL Server requirements.

< Back
Next >
Exit

If you do not want to install SQL Server, and you have products or role selections that include the GR node by default, you can select the **Customize Installation** checkbox and deselect **Galaxy Repository**. However, this will limit any database-related product functionality, such as the AVEVA System Platform 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 (see note)
InTouch Development and Runtime	Yes (see note)
InTouch Runtime Only	No
InTouch Access Anywhere Server	No
InTouch Access Anywhere Secure Gateway	No



Product Selections	SQL Required
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 and SQL Server was installed prior to System Platform, 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 [Set the SQL Server security mode](#). For more information about SQL Server installation, see [SQL Server requirements for System Platform components](#).

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.

## SQL Server requirements for System Platform components

SQL Server is required when any of the following System Platform components are selected for installation:

- Application Server Galaxy Repository (GR)
- Historian Server
- System Monitor Manager

The prerequisites installation workflow diverges if SQL Server is required but not already installed, and you will be prompted to install SQL Server during the installation. At this point, you have a choice of having System Platform install SQL Server 2022 Express Core automatically, or exiting System Platform installation and installing SQL Server before proceeding.

- If you are installing a small system (less than 25,000 I/O), you can allow System Platform to continue installing, and SQL Server Express Core will be installed during the System Platform installation process. You do not have to install SQL Server Express Core separately.
- If you cannot use SQL Server Express due to your system requirements, exit the installation program and install a supported SQL Server version. Resume System Platform installation after you have installed and configured the supported SQL Server version.

To see if one of the SQL Server-required components is selected for installation, click the **Customize Installation** checkbox and scroll through the product/component list. In some cases, you can deselect the SQL Server-dependent component, if you decide that the component is not needed for the product or role you are installing. For some roles and products, you will not be able to deselect the component and still have the functionality required for that particular role or product.

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 2014.
  - **How to fix:** Upgrade SQL Server to a supported version. Refer to the following Microsoft resource for more information: Upgrade SQL Server.  
<https://docs.microsoft.com/en-us/sql/database-engine/install-windows/upgrade-sql-server?view=sql-server-ver15>
- Your installed version of SQL Server is supported but requires a service pack. For example, you have SQL Server 2016 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 Readme, and refer to Issue 1249251.

## Select 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 2016). 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:** AVEVA Application Server and AVEVA OMI Runtime (with Galaxy Repository)
- **AS w/o GR:** AVEVA 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	
PCS Runtime	R	O	R				O	
PCS Service Repository								
Applicati								

Product / Component	AS + GR	AS w/o GR	IT	ITAA	ITAA SG	ITAA AS	HS	HC
on Server Bootstrap IDE Galaxy Repository	R O O	R O O	R R O	R				
Insight Publisher			R	R				
InTouch HMI Runtime Development Alarm DB Logger Demo Apps Recipe Manager SQL Access 16-PenTrend Symbol Factory Industrial Graphics Server (InTouch Web Client) OI Gateway			R O R O O O O O R R R	R R R R R R R				
InTouch Access Anywhere ITAA				R	R	R		

Product / Component	AS + GR	AS w/o GR	IT	ITAA	ITAA SG	ITAA AS	HS	HC
Server ITAA Secure Gateway ITAA Authentic ation								
<b>Historian</b> Historian Server IDAS Active Event Configura tion Tools Historian Extension s							R R R R R	
<b>Historian Client</b> Trend/ Query Clients Microsoft Add-Ins	R	R	R	R				R
<b>Licensing</b> License Manager License Server	R R	O O	R R	O O				
Client Compone nts	R	R	R	R				
Server Compone nts	R	R	R	R				

Product / Component	AS + GR	AS w/o GR	IT	ITAA	ITAA SG	ITAA AS	HS	HC
OI Server Simulator	R	R	R	R				
System Monitor	R							
System Monitor Manager	R	R	R	R	O	O	R	R
System Monitor Agent								

**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 [Install 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 2016). 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 System Management Server, but the resulting installed product will not be 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 AVEVA System Development Client. 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 Srvr:** AVEVA System Platform Development Server. Install the components required to host the development server, and develop and test InTouch and System Platform applications.
- **HS Node:** AVEVA Historian Server Node. Install the necessary components to store historical data in a System Platform environment.
- **HC Node:** AVEVA Historian Client Node. Install the components required to connect to an existing Historian Server and analyze the data.
- **ITAA SG:** AVEVA 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:** AVEVA Enterprise 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 Mon:** System Monitor Manager Node. 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 Srvr	HS Node	HC Node	ITAA SG	Lic Srvr	Sys Mon
<b>System Platform</b> PCS Runtime PCS Service Repository	R	R	R R	R	R			
<b>Application Server</b> Bootstrap IDE Galaxy Repository	R	R R	R R O	O	O			

Role	RT Client	Dev Client	Dev Servr	HS Node	HC Node	ITAA SG	Lic Srvr	Sys Mon
<b>Insight Publisher</b>	R	R	R					
<b>InTouch HMI</b>	R	R	R	R				
Runtime		O	O					
Development	R	R	R	R				
Alarm DB		O	O					
Logger	O	O	O	R				
Demo Apps	O	O	O	R				
Recipe Manager	O	O	O	R				
SQL Access	R	R	R	R				
16-PenTrend								
Symbol Factory								
Industrial Graphics Server (InTouch Web Client)								
<b>InTouch Access Anywhere</b>						R		
ITAA Server								
ITAA Secure Gateway								
ITAA Authentication								
<b>Historian</b>								
Historian Server				R				
IDAS				R				
				R				



Role	RT Client	Dev Client	Dev Servr	HS Node	HC Node	ITAA SG	Lic Srvr	Sys Mon
Active Event Configura tion Tools Historian Extensions				R R				
<b>Historian Client</b> Trend/ Query Clients Microsoft Add-Ins	R	R	R	R	R			
<b>Licensing</b> License Manager License Server	O O	O O	R R		O		R	
<b>Operation Integratio n</b> Client Compone nts Server Compone nts OI Server Simulator OI Gateway	R R R R	R R R R	R R R R	R R R R	R R R			
<b>System Monitor</b> System Monitor Manager System Monitor Agent	R	R	R R	R	R	R	R	R R

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 [Modify 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 either:

- 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 [Upgrade, modify, and repair System Platform](#) for more information.

# Install 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 2023 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 2023 R2 and do not require patching.

## Workspace feature notification for the OMI and InTouch HMI web clients

The AVEVA Historian search and elastic search features are installed to support the Workspace feature for the Operations Management Interface (OMI) and InTouch HMI web clients. Workspace is available if you are using Flex licensing. Therefore, after installation, you may see AVEVA Historian listed as a Windows program, even if you did not install the Historian. Do not uninstall Historian. You can use the Modify workflow to restore the Historian search and elastic search features if you inadvertently uninstalled Historian.

## OMI web client configuration requirements

If you have, or plan on developing, ViewApps that will be used with the OMI web client, there are two configuration requirements that must be met after installing System Platform:

- You must configure a System Management Server. See [Work with Configurator](#) for details.
- You must register System Platform with AVEVA Identity Manager. See [Federated Identity Provider](#) for details.

## 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 are blocked from continuing. A 64-bit operating system is required. For additional information about supported operating systems, see [Supported operating systems](#).
- 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 may be 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.

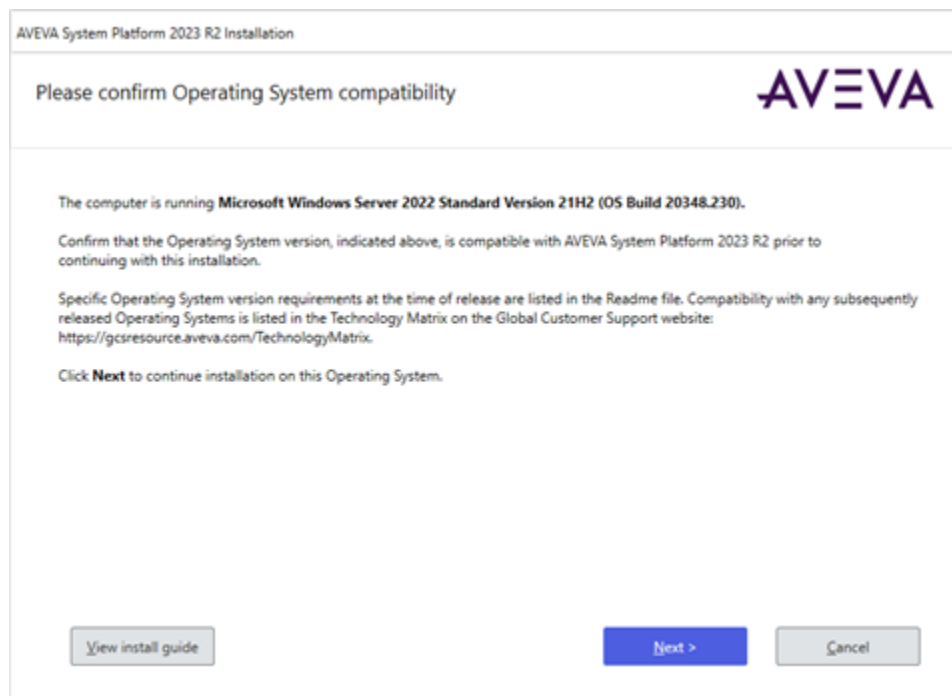
---

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 2023 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 helps to ensure that 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. Select one of the following options:

- Product-based installation.

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 are installing any of the InTouch Access Anywhere options available under Product-Based Installation, see [Install InTouch Access Anywhere](#).

- Role-based installation.

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 (unless you select Custom, in which case all other options are ignored).. If you are installing InTouch Access Anywhere Secure Gateway, it should be installed by itself, without any other System Platform components on the same node.

4. 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 [Common Platform Services](#) for additional information.
  - **AVEVA Enterprise Licensing Framework.** Every node should be configured to point to a single License Server. See [AVEVA Enterprise License Server Configuration](#) for additional information.
  - **AVEVA System Monitor.** Every node should be configured to point to a single System Monitor Manager. See [AVEVA System Monitor Configuration](#) 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 [Configure System Platform components](#) for more information.

---

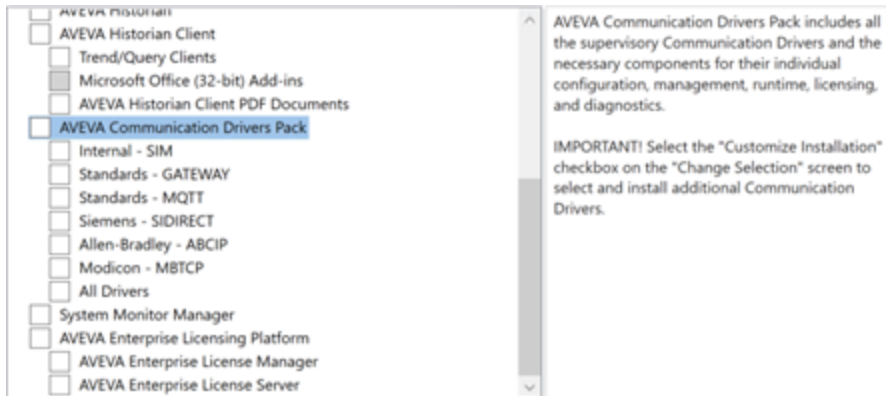
5. Click **Next** to proceed. The verify selection dialog box appears. To make changes to your selections or to change the installation directory, select the **Customize Installation** check box. You can change your selections to:
  - Select Communication Drivers as needed. See step 7 for additional information.
  - Install other components, such as the InTouch 16-Pen Trend Wizard supplementary component. See step 8 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**.

---

**Important!** If you install System Platform to a location other than the default folder, you must set the Access Control List (ACL) for the selected location to avoid file tampering or other malicious activity. Refer to Microsoft's recommendations for setting the ACL for your version of Windows.

---


6. **AVEVA Communication Drivers:** The AVEVA Communication Drivers Pack Simulator (SIM) and Gateway are automatically installed when you install Application Server or InTouch HMI. You can also select some of the commonly-used drivers here. If the driver you need is not listed, you can use the **Customize installation** option to select additional drivers for installation.



7. If you have selected any **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. InTouch HMI language options are:
  - English
  - French
  - German
  - Japanese
  - Simplified Chinese
8. Click **Next**. The **End User License Agreement** dialog box appears.
9. Review the license. Select **I have read and accept the terms of the license agreement(s)**, and then click **Agree**.
10. 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 13.

Please enter a user name and a password needed for off node communications.



Domain/Local Machine

.\

User Name

aaUser

Password

\*\*\*\*\*

Confirm Password

\*\*\*\*\*

☒ Create Local Account

View install guide

< Back

Next >

Cancel

11. 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, select 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 shortcut to the utility. It is listed under the **AVEVA** folder.

---

12. 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:
  - Install SQL Server Express and continue installation. If you select this option, SQL Server Express is installed and then System Platform installation proceeds automatically.

---

**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.

---

  - Exit installation and install a supported SQL Server version. If you select this option, the System Platform installer exits. Manually install SQL Server, and then restart the System Platform installer.

System Platform for medium and large installations includes a separate DVD with a full version of SQL Server 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.

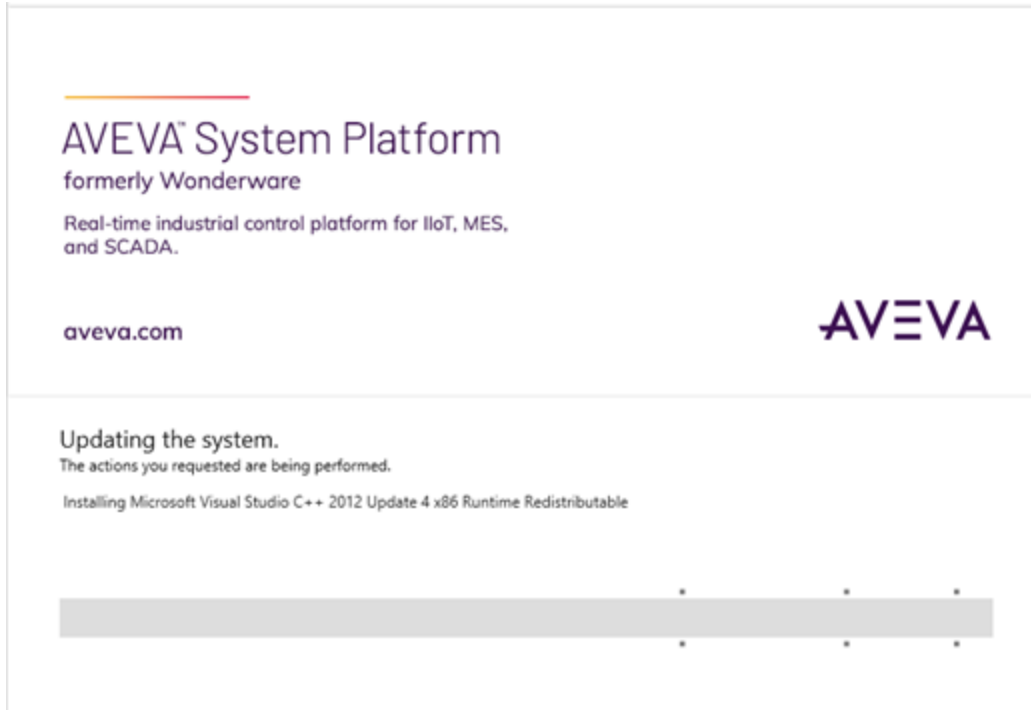
13. A list of missing prerequisite components (if any) and the System Platform products to be installed are displayed.

---

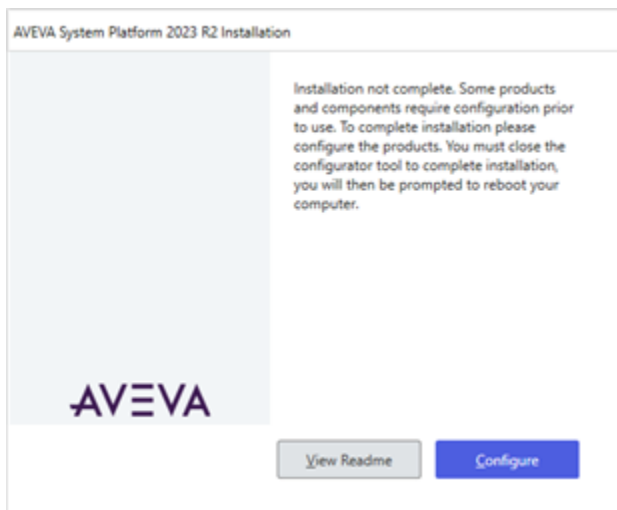
**Note:** Any prerequisites required for the products selected for installation will be listed above the list of products and components. The prerequisites will be installed first, and the product and components will be installed immediately after installation of the prerequisites has finished. If you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

---

Click **Install** to proceed. The progress bar appears.



14. After the installation is over, the dialog box to begin configuration appears.



- To view important information, select **View Readme**. The Readme describes hardware and software requirements, new features, and known and resolved issues. The dialog remains open; you will still need to select **Configure** to continue.
- Select **Configure** to continue. See Get started with Configurator to complete installation.

## Install 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](#)
- [Install Secure Gateway](#)
- [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 compatible 64-bit version of Windows Server. See [Supported operating systems](#) for details.

---

**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 (RDS) 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.
- The corresponding 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

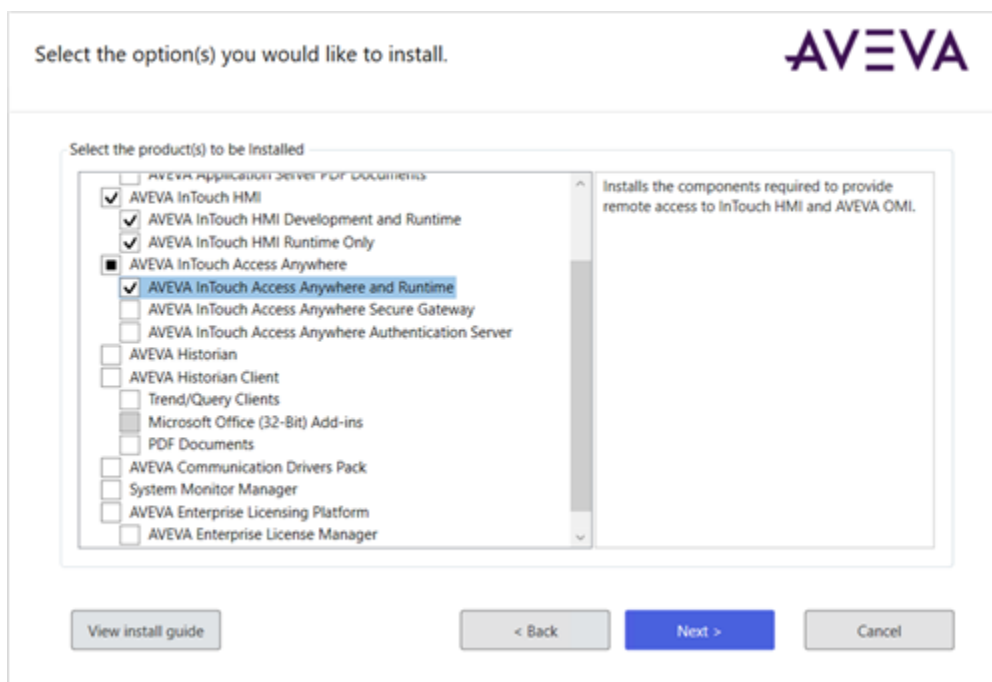
Make sure that all installation prerequisites have been met before starting the installation procedure. The following procedure explains the basic steps to install the InTouch Access Anywhere Server on a computer running a supported version of Windows Server.

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.

**Note:** You cannot upgrade the InTouch Access Anywhere Server directly. The existing version must be uninstalled before you can install a newer version on the same 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*.

## Install Secure Gateway

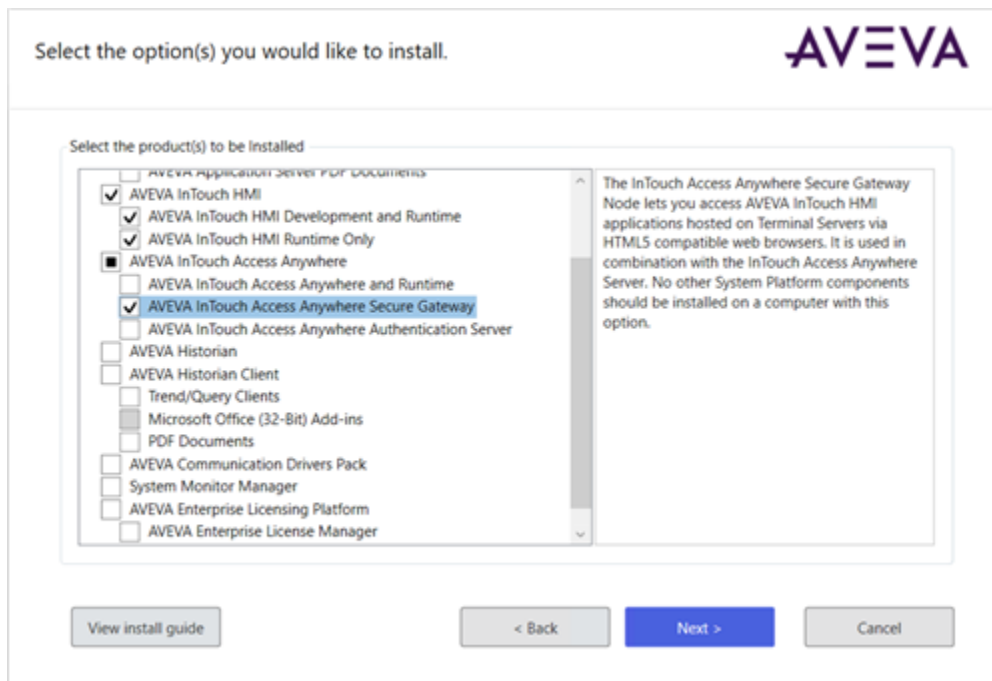
This section describes the procedure to install the Secure Gateway on a computer running a supported version of Windows server. The Secure Gateway supports other installation configurations. For more information, see "Other Secure Gateway Installation Configurations" in the *InTouch Access Anywhere Secure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

After verifying all installation prerequisites, start the installation procedure.

**Note:** You cannot upgrade the Secure Gateway directly. The existing version must be uninstalled before you can install a newer version on the same computer.

### 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 select **Agree**.  
The **Ready to Install the Application** screen appears.

6. Review the installation details and select **Install**.
7. Select **Finish** after the installer indicates that the **Installation has completed successfully**.

## Configure 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

The ports used by System Platform products and components are listed in [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 [Work with Configurator](#) and Configure 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:

1. 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
2. Change the value for the SecuredPort to a different, unused port number. The Secure Gateway does not permit port sharing.
3. 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 Server can be installed separately or together on one of the supported Windows Server operating systems. See [Supported operating systems](#) for details.

- 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 as a best security practice.

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

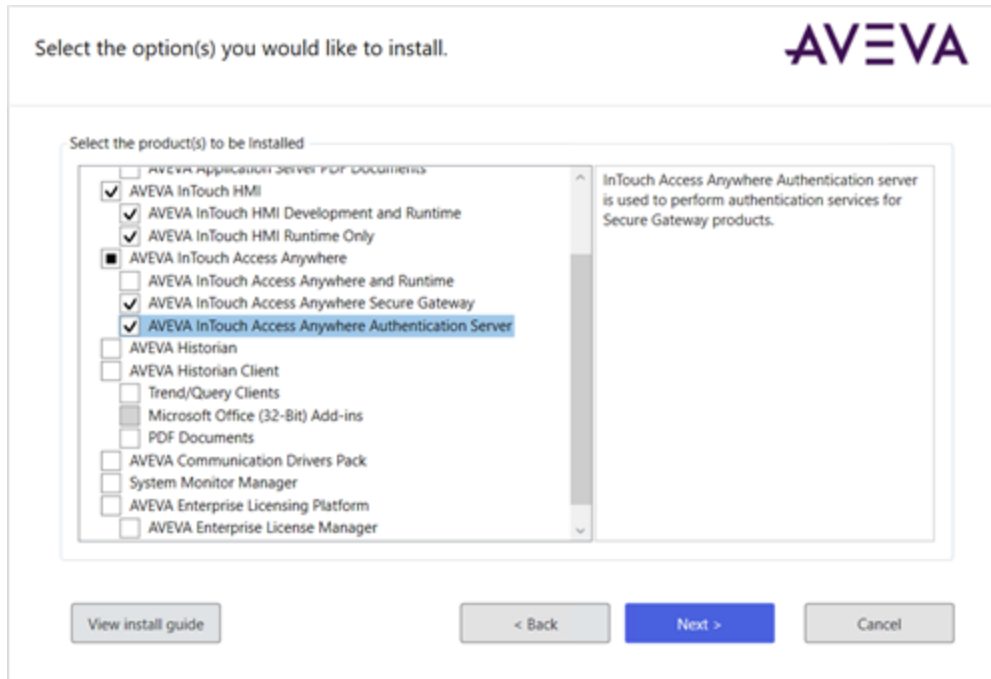
1. Log on as a Windows administrator of the computer that will host either the Secure Gateway, the Authentication server, or both.
2. Insert the System Platform DVD in your computer and run **setup.exe**.
3. Select **Product-Based Selection**.
4. Determine how you want to install the Secure Gateway and the Authentication Server.

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

- Install the Secure Gateway by following the steps described in [Install Secure Gateway](#). 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:
  - AVEVA InTouch Access Anywhere and Runtime
  - AVEVA InTouch Access Anywhere Secure Gateway
  - AVEVA InTouch Access Anywhere Authentication Server

Select the option(s) you would like to install.

AVEVA

Select the product(s) to be installed

<input type="checkbox"/> AVEVA Application Server PDF Documents	InTouch Access Anywhere provides remote access to InTouch HMI and AVEVA OMI applications via a web browser.
<input checked="" type="checkbox"/> AVEVA InTouch HMI	
<input checked="" type="checkbox"/> AVEVA InTouch HMI Development and Runtime	
<input checked="" type="checkbox"/> AVEVA InTouch HMI Runtime Only	
<input checked="" type="checkbox"/> AVEVA InTouch Access Anywhere	
<input checked="" type="checkbox"/> AVEVA InTouch Access Anywhere and Runtime	
<input checked="" type="checkbox"/> AVEVA InTouch Access Anywhere Secure Gateway	
<input checked="" type="checkbox"/> AVEVA InTouch Access Anywhere Authentication Server	
<input type="checkbox"/> AVEVA Historian	
<input type="checkbox"/> AVEVA Historian Client	
<input type="checkbox"/> Trend/Query Clients	
<input type="checkbox"/> Microsoft Office (32-Bit) Add-ins	
<input type="checkbox"/> PDF Documents	
<input type="checkbox"/> AVEVA Communication Drivers Pack	
<input type="checkbox"/> System Monitor Manager	
<input type="checkbox"/> AVEVA Enterprise Licensing Platform	
<input type="checkbox"/> AVEVA Enterprise License Manager	

View install guide

< Back Next > Cancel

4. Click **Next** on the dialog box that shows all components have been selected 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.

# Configure System Platform components

## Using the Configurator

Configure System Platform using the **Configurator** dialog box after installation. You can re-run the **Configurator** as required to make changes to any of the settings for the installed components. 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.

---

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

---







The following System Platform components may require configuration after installation and after making certain changes to an existing system installation:

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

### 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.



## Common Platform Services

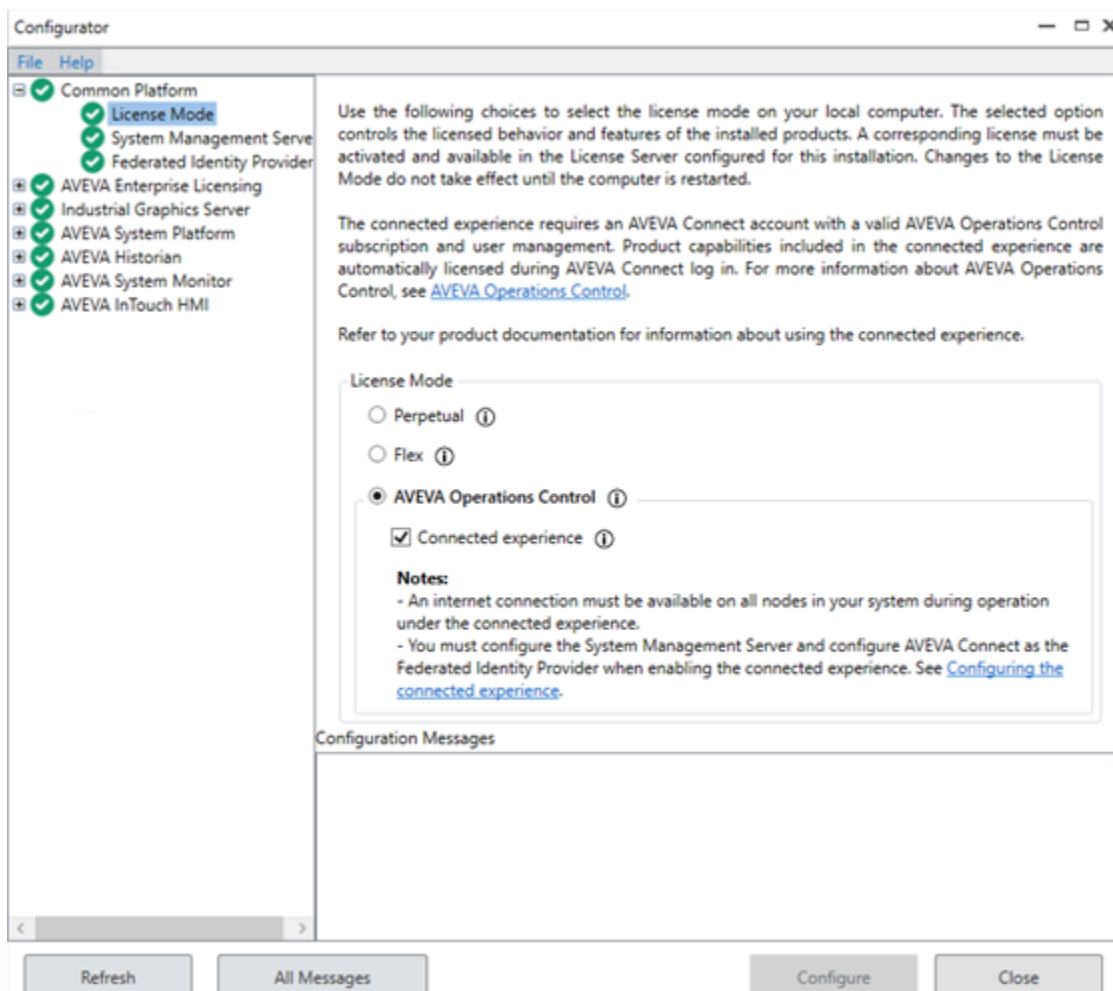
**Common Platform** services are used to set various parameters that control license behavior, user management, and authentication. There are three components to be configured:

**Common Platform** services include the following components:

- [License Mode](#)
- [System Management Server](#)
- [Federated Identity Provider](#)

## License Mode

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



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

- **Perpetual:** A specific AVEVA product license purchased for use in perpetuity.
- **Flex:** Choose subscription license separately for a range of AVEVA products. Purchase Flex credits to license

use of any AVEVA cloud, hybrid or on-premises products for a recurring period.

- **AVEVA Operations Control:** A subscription license for at least one of two AVEVA Operations Control packages (Edge, Supervisory); includes unlimited use of all products in the product package for your defined set of users.
  - **connected experience:** Select to enable a Single Sign-on (SSO) experience across all Operations Control products for that node with CONNECT cloud capabilities.
    - The **connected experience** requires an CONNECT account with a valid Operations Control subscription and user management.
    - Selecting the **connected experience** option enables the behavior of all Operations Control products on that node to require log in authentication with CONNECT when starting the first product on the node. Products on the node subsequently launched will authenticate using SSO. CONNECT-based authorization is the only security mode available under the **connected experience**.
    - The **connected experience** must be enabled on all nodes in your system. Applications previously build on nodes not enabled for the connected experience must be reconfigured to function in the **connected experience** environment.
    - You can deselect the **connected experience** at any time, but the **v** must be disabled on all nodes in your system. Applications built under the **connected experience** must be reconfigured to function under a non-Connected Experience environment including both authentication methods and product license.

## System Management Server

AVEVA software products need post-installation configuration in order to use encrypted communications. You need to configure your products using the Configurator after you have installed them. The Configurator lists all product components that require post-installation configuration.

---

**Note:** Configuring a System Management Server (SMS) is highly recommended to ensure the security of your System Platform. It is required when redundancy is enabled for Application Server nodes.

---

## System Management Server overview

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

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

---

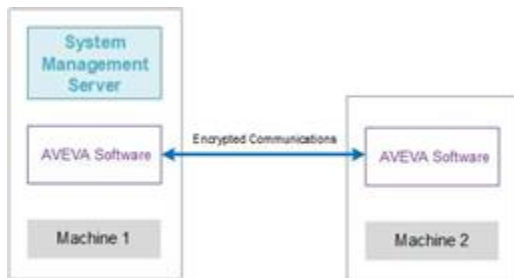
**Note:** To connect to the System Management Server, you need to be a member of either the "aaAdministrators" or the "Administrators" group on the machine where the System Management Server is installed.

---

## Install System Management Server

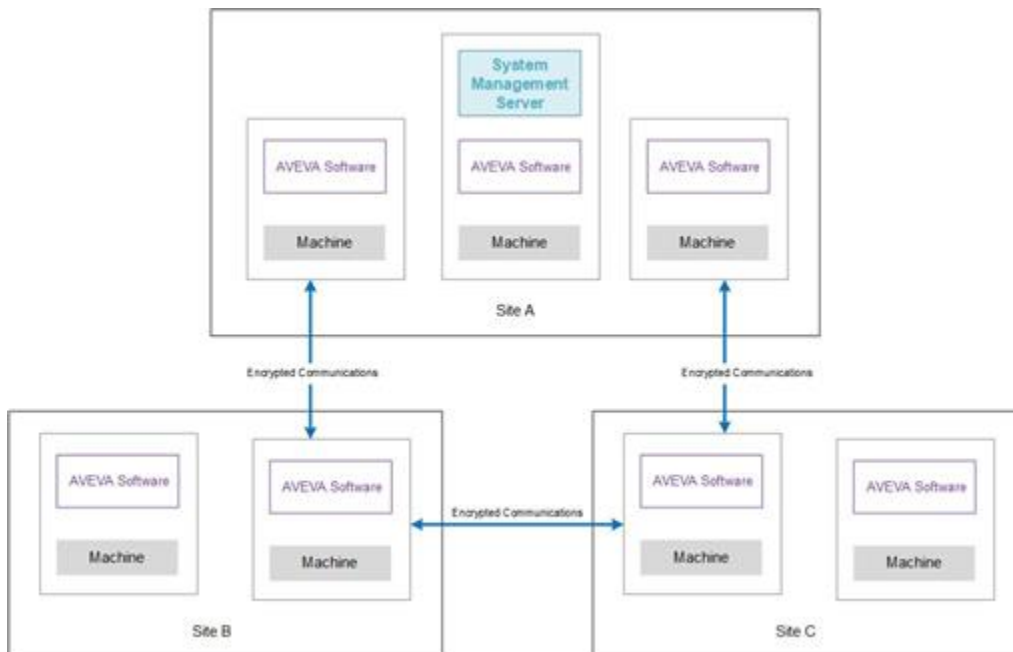
Regardless of the size of your system setup, only one System Management Server is required for encrypted communication. System Management Server can be installed on one of the machines running an AVEVA application or on a separate machine on the network.

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



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

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



## Redundant SSO server

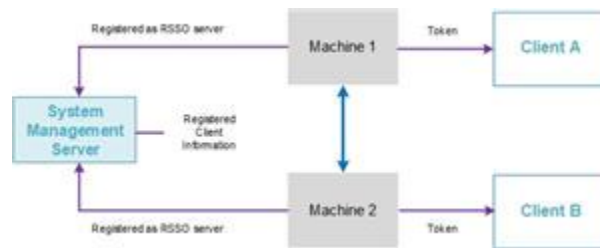
You can configure a machine that connects to an existing System Management Server as a Redundant Single Sign-On (RSSO) server. When you select the System Management Server and configure the current machine, the SSO capability from the System Management Server is shared with the RSSO server.

The purpose of setting up RSSO servers is to:

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

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

The following diagram illustrates the working of RSSO servers:



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

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

---

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

---

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

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

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

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

---

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

---

## Work with Configurator

You can complete the following tasks in the Configurator:

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

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

---

**Note:** If you have other products installed that use the Configurator, the Configurator may be located in a different program group.

If System Management Server is not configured, capabilities like connected experience, Web OMI, Azure AD/CONNECT federation will not be available.

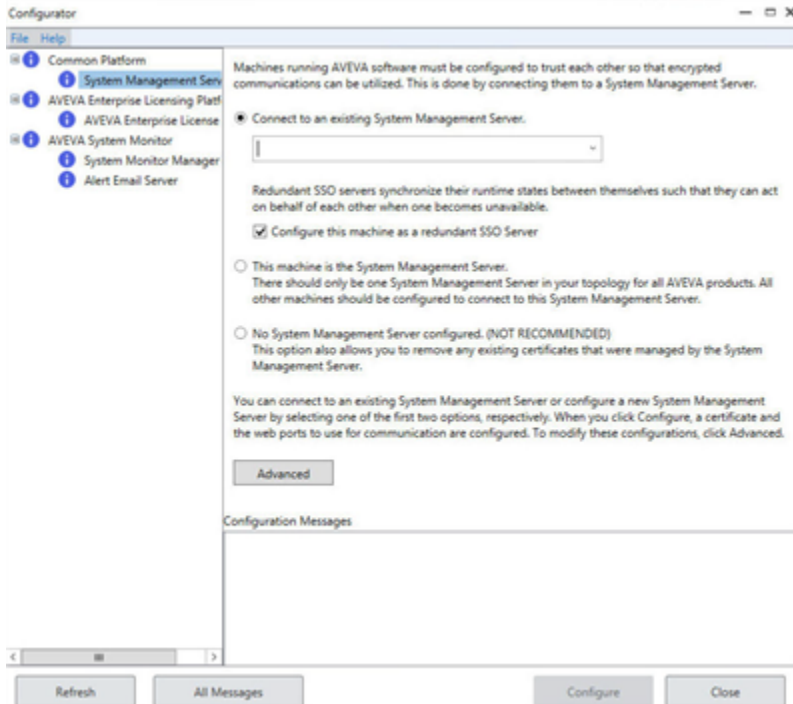
---

## Connect a machine to a System Management Server

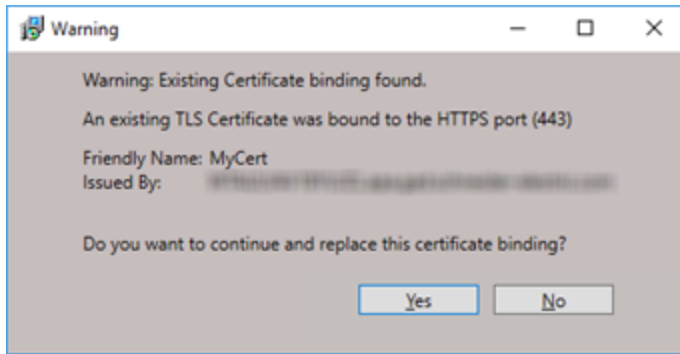
Machines running AVEVA products need to connect to a System Management Server via a configured certificate in order to use encrypted communication.

### To connect a machine to a System Management Server

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



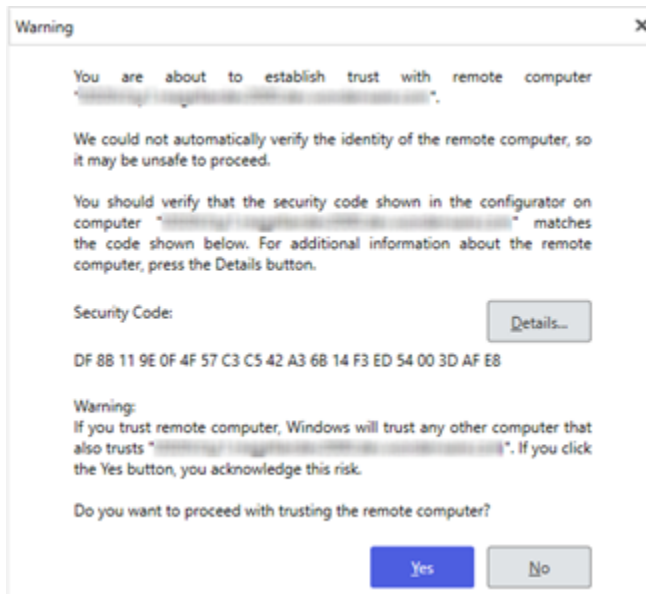
2. In the left pane, select **Common Platform > System Management Server**.
3. If you wish to connect to an already existing System Management Server, select the **Connect to an existing System Management Server**.
4. From the list of System Management Servers available, select the required System Management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



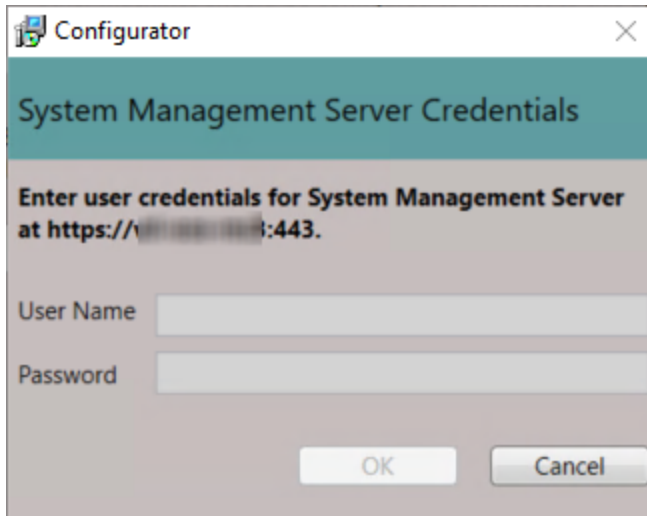
7. Selecting **No** results in the following message being displayed in the **Configuration Messages** area, and the machine will not be connected to the System Management Server.



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



9. Review the message carefully before you select **Yes**. Selecting **No** cancels the configuration process.
  10. Select **Details**, to view more information about the certificate.
- If you are not a member of the "aaAdministrators" or "Administrators" group on the System Management Server, a dialog box prompting you to log on to the System Management Server with administrative credentials is displayed. Enter the credentials of a user that is a member of the "aaAdministrators" or "Administrators" group on the System Management Server and select **OK**.



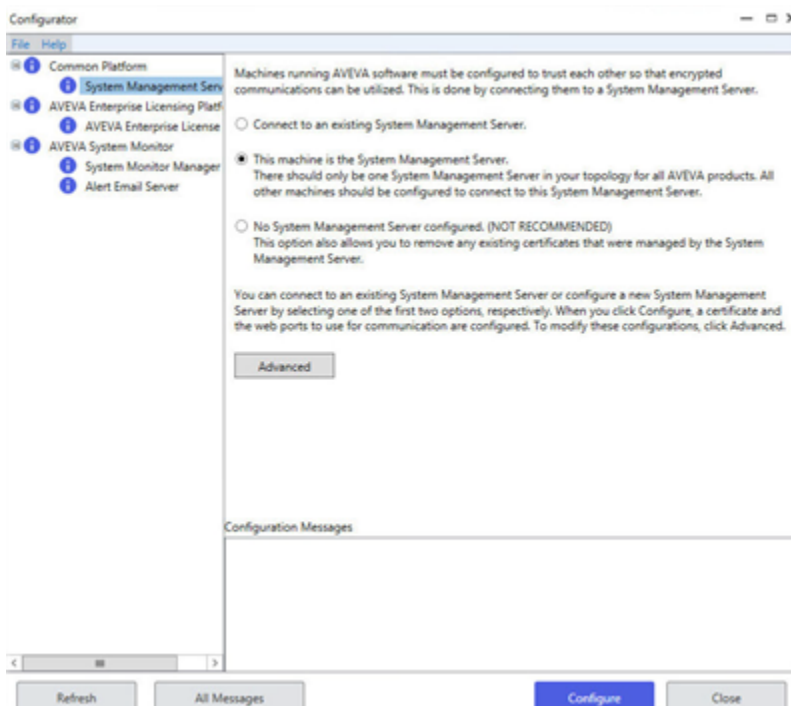
**Note:** If you have configured a communications proxy on the server where the System Management Server is installed, contact the AVEVA Global Customer Support team for information about installing and connecting to the System Management Server.

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

## Configure the System Management Server

### To configure the System Management Server

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





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

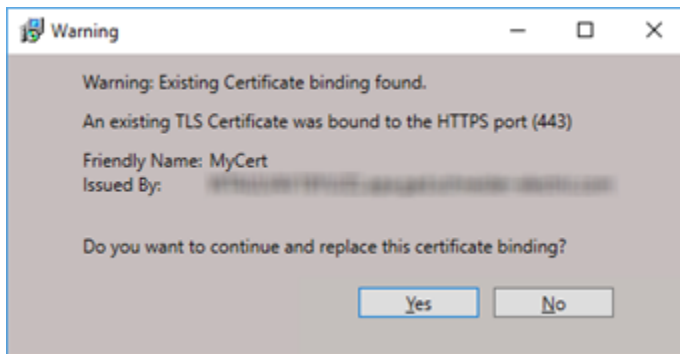
---

**Note:** You should include only one in your entire system. If other AVEVA products are installed, make sure that one has not been configured elsewhere before proceeding as communication disruptions may occur.

---

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

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

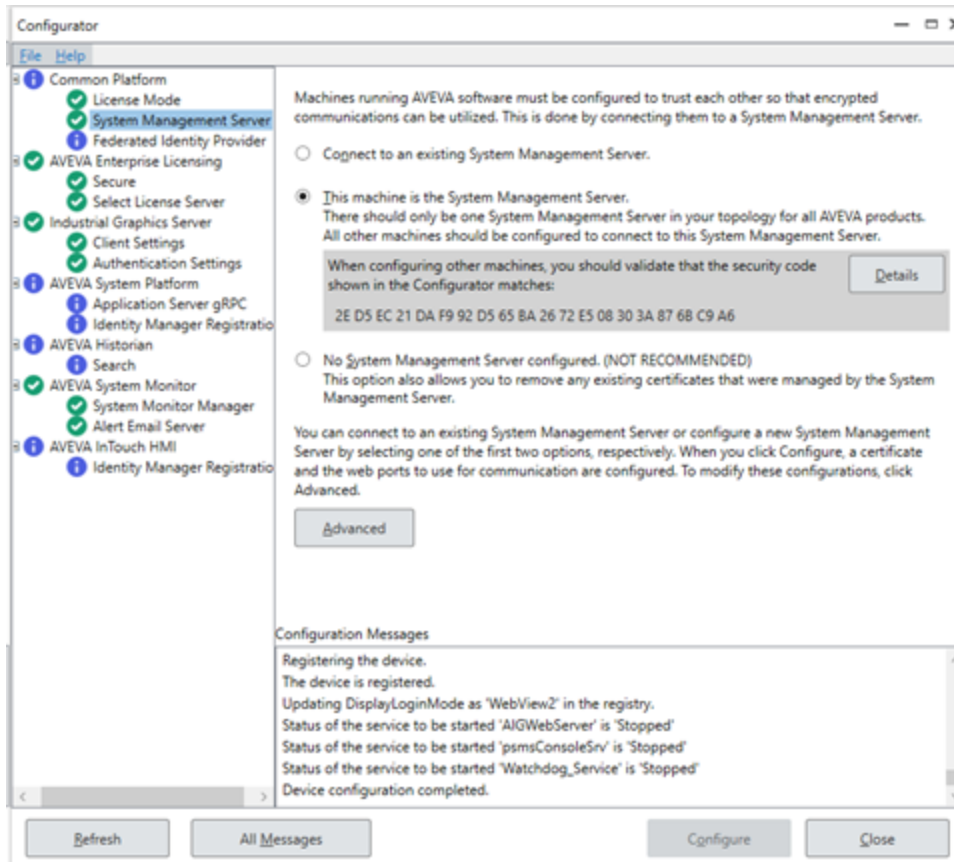


6. Selecting **No** results in the following message being displayed in the **Configuration Messages** area, and the machine will not be connected to the System Management Server.



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





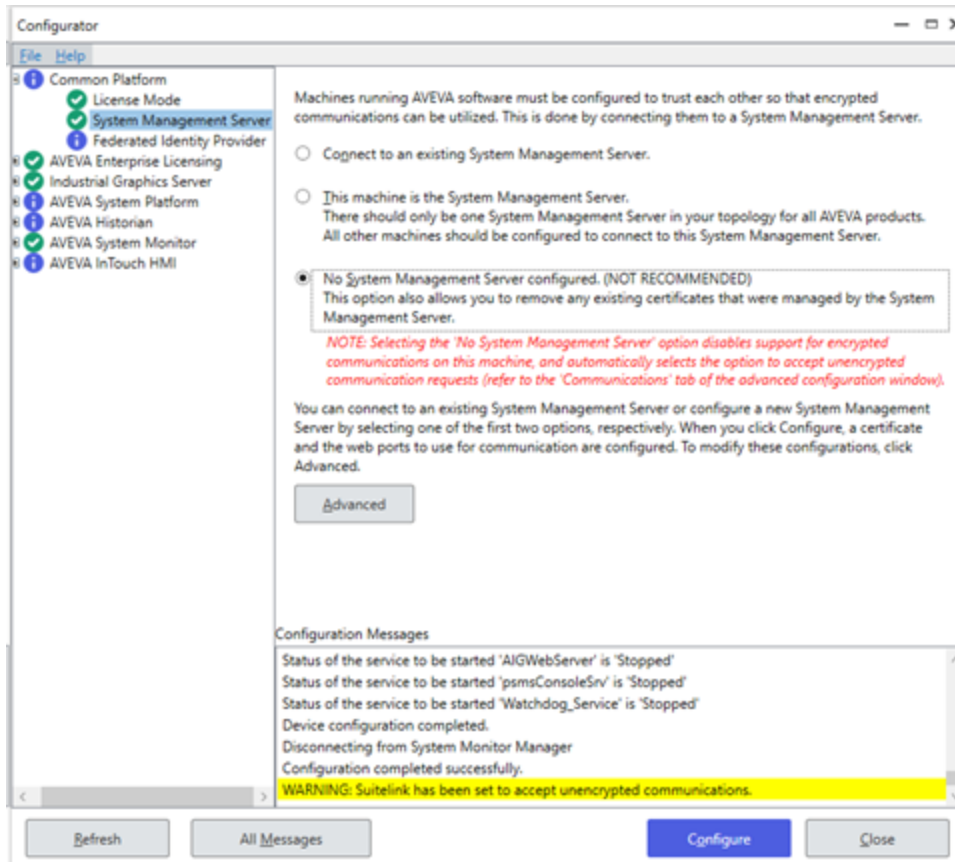
If the configuration is unsuccessful, you can view details of the errors in the System Management Server.

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

## Run products without a System Management Server

### To run AVEVA products without a System Management Server configured

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



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

## Advanced Configuration

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

### To modify an existing configuration

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

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

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

### Certificates tab

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

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

## To configure the certificate for secure communications

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

---

**Note:** Automatically generated certificates are renewed automatically.

---

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

Advanced Configuration

Certificates Ports Communications Authentication

In order to enable communications via encrypted channels (e.g. HTTPS), certificates are required to be configured.

Certificates can either be provided by your IT department or automatically generated.

Configuration

Please select the appropriate options below.

Certificate Source: Automatically Generated

Certificate: [Disabled] ASB Details

OK Cancel

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

5. In the **Certificate file** field, browse to select a certificate.
6. From the **Certificate Store** list, select the type of certificate – **Root**, **Intermediate**, or **Personal**. The certificate is configured to be used for encrypting communication channels.  
Depending upon the type selected here, the certificate is stored in the **Certificate Store** identified by the certificate type.
7. In the **Password** field, type the password for the selected certificate Store. The Certificate Store does not have a password. This is the optional password for the certificate being imported.
8. Select **OK** to save the details and close the **Import Certificate** dialog.

---

**Note:** The IT Department needs to renew certificates they generate as and when required.

---

9. Select **Details**, to view the details of the certificate.

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

---

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

---

## Ports tab

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

### To configure the HTTP and HTTPS communication ports

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

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

Advanced Configuration

Certificates Ports Communications Authentication

The common platform, and certain other AVEVA software (using "web port sharing" technology), communicate over web ports.

Configuration

Please select the appropriate ports to use on this machine.

HTTP Port: 80

HTTPS Port: 443

OK Cancel

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

**Note:** If you change the default ports you need to

(i) restart the machine for the change to take effect, and

(ii) update the port number(s) on all client products that point to servers running on this machine.

This excludes the System Management Server because it discovers port numbers automatically.

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

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

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

## Communications tab

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

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

Advanced Configuration

Certificates

Ports

Communications

Authentication

Use this tab to configure the behavior of AVEVA communications protocols.

Many AVEVA and 3rd Party products that integrate with System Platform use these protocols. For example: InTouch HMI, Historian, OI Servers (CDP), Batch Management, Workflow, and others. Refer to your product's documentation or contact technical support for more information.

Suitelink

Suitelink is a TCP/IP based communications protocol.

Suitelink communications between processes on this node, and between processes on this node and other nodes can be encrypted. Please select the appropriate handling for non-encrypted Suitelink connection requests.

☐ Accept non-encrypted Suitelink connections (mixed mode).

*Mixed mode is recommended for use only during online (node-by-node) upgrades and/or supporting legacy applications.*

*NOTE: Changes to this setting require a reboot in order to take effect.*

Network Message Exchange (NMX)

NMX is an AVEVA application communication protocol that uses a DCOM-based communication transport mechanism. Authorization to access NMX can be restricted to users that are members of a well-known OS User Group. Please select the appropriate handling for NMX access authorization on this node.

☐ Grant access to NMX for all users (NOT RECOMMENDED)

*NOTE: Changes to this setting require a reboot in order to take effect.*

OK

Cancel

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

### SuiteLink mixed mode setting

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

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

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

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

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

### Mixed mode use cases

Mixed mode is recommended for use under the following conditions:

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

---

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

---

### NMX user access setting

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

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

### Access to NMX for all users use cases

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

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

---

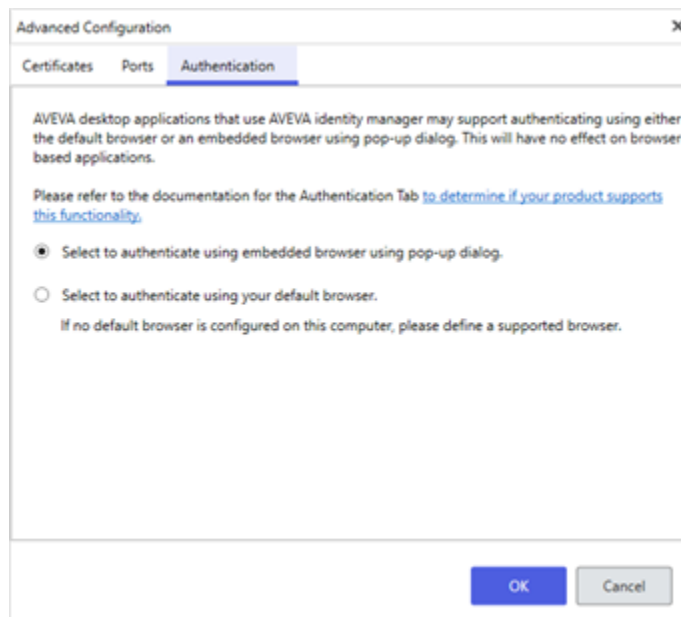
**Note:** Whenever the NMX mode is changed, a system restart is required before the new mode will take effect.

---

## Authentication tab

The Authentication tab allows you to authenticate using two options:

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




---

**Note:** The default behavior - an embedded pop-up dialog - is best. Selecting to use your computer's default browser will support all other uses.

---

## Federated Identity Provider

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

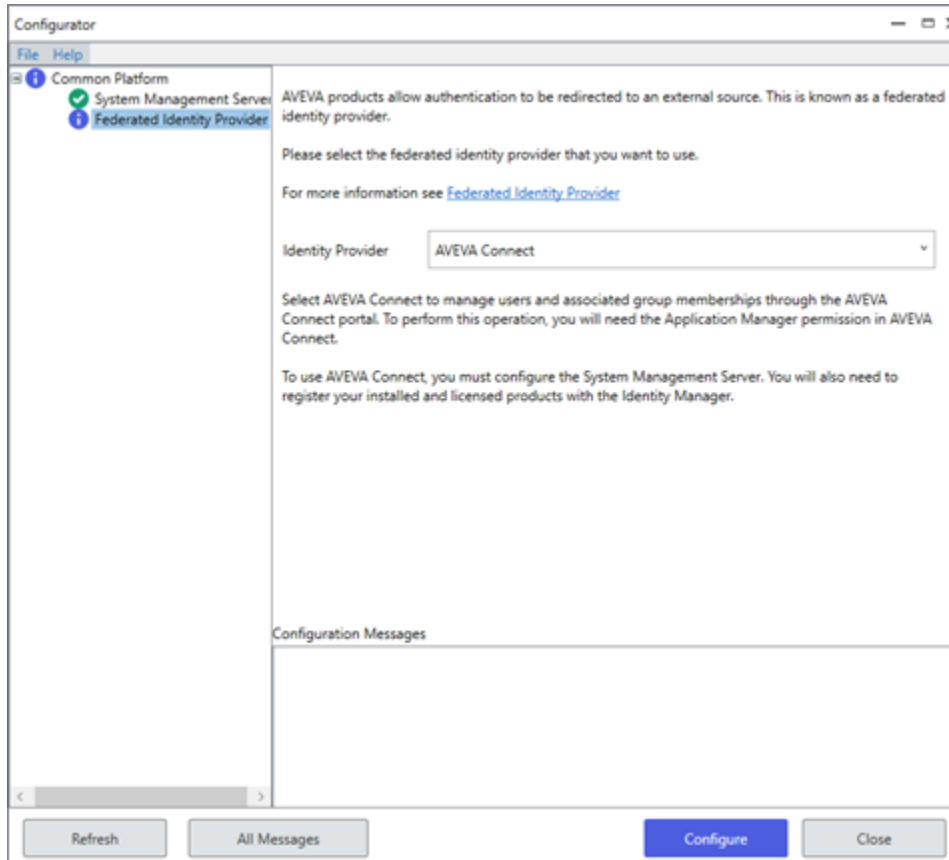
The Federated Identity Provider plugin registers on prem AIM server with the external identity provider (Azure AD or CONNECT), establishing a trust-based relationship between them. The user authentication is delegated to the external identity provider.

When you launch an AVEVA product on a node that's configured to be a connected experience node, you are prompted to authenticate via one of the two authentication user experiences (as configured) using their



federated ID with CONNECT. This requires your Active Directory to be federated or synced with your CONNECT account. AIM acts as a middle layer for all the session and authentication redirects and capabilities.

All on-prem Operations Control products are required to use AIM as a local identity provider to run in Operations Control mode. AIM is configured to federate with CONNECT and CONNECT is federated with your identity provider. All cloud services use CONNECT as an identity provider, and it can be configured to federate to your Azure AD or other identity provider.



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

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

For more information refer to the following links:

- [Key Concepts of Identity Manager](#)
- [Certificates](#)
- [Identity Provider Options- Azure AD authentication, AVEVA Connect authentication](#)
- [Federated Identity Provider Workflow](#)
- [Complete Federated Identity Provider configuration](#)
- [AVEVA Identity Manager guide](#)

## Troubleshooting connection problems

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

Failed to register AVEVA Connect Identity Provider: Failed to generate application in AVEVA Connect.  
ErrorMessage: Property CallbackUrls contains more values than are permitted for this application type.  
Actual: 101, Maximum: 100..

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

1. Delete stale or unused application URLs from your CONNECT account.

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

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

### Delete stale or unused application URLs from CONNECT

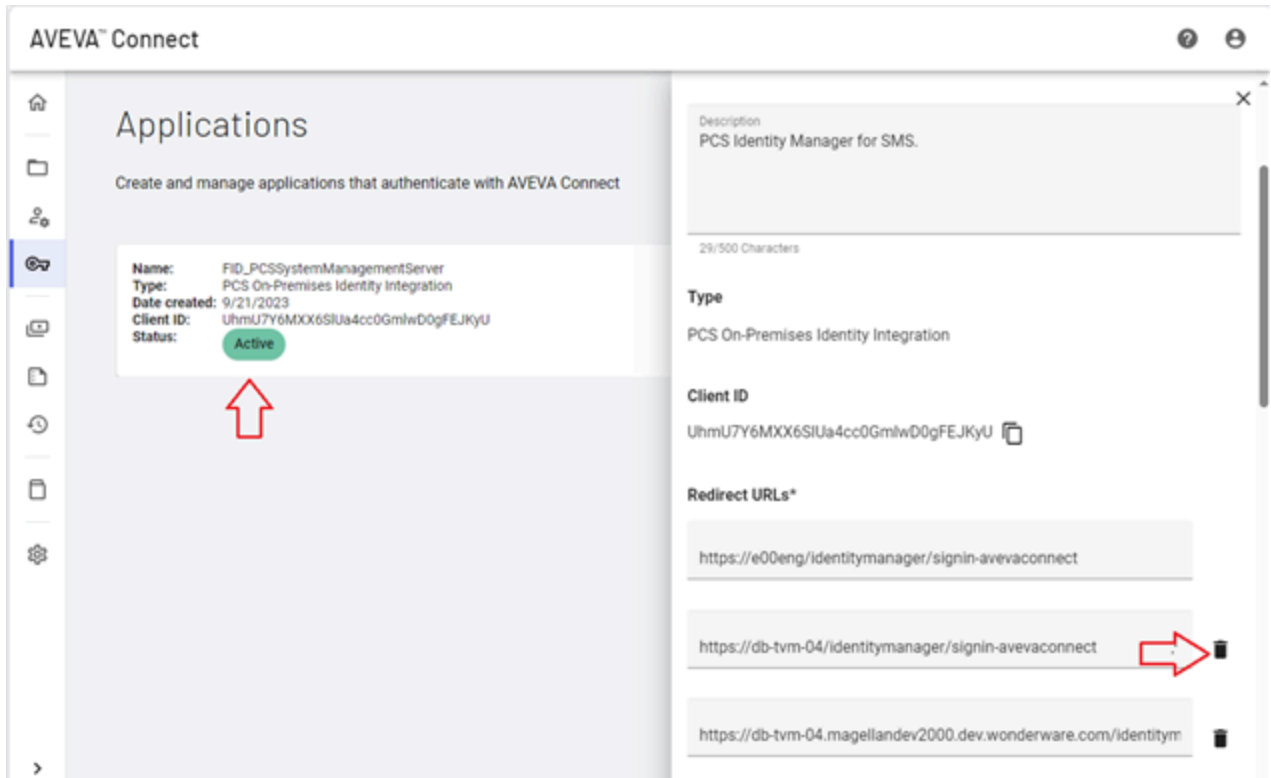
1. Log into your CONNECT account.

---

**Note:** You must be an administrator on your CONNECT account to perform this operation.

---

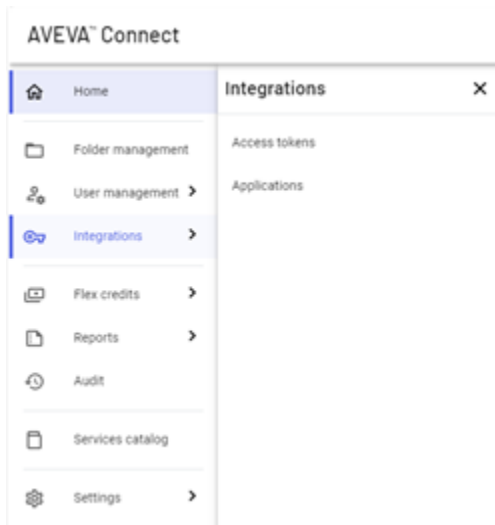
2. Click an application. The **Edit Application** slide-in pane appears.
3. Scroll down to the listed Redirect and Log out URLs.
4. Click the delete (trash can) icon to delete a URL.



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

### Acquire an access token

1. Open the browser and navigate to [CONNECT](#).
2. Sign in with your user credentials, and if prompted, select the appropriate account.
3. Select **Integrations** from the left navigation pane.



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

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

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

## Configure an application

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

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

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

## Add URLs to an existing application

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

## Add a new application

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

redirect and logout URLs.

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

### Register the System Management Server or Redundant SSO Server with CONNECT via Powershell

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

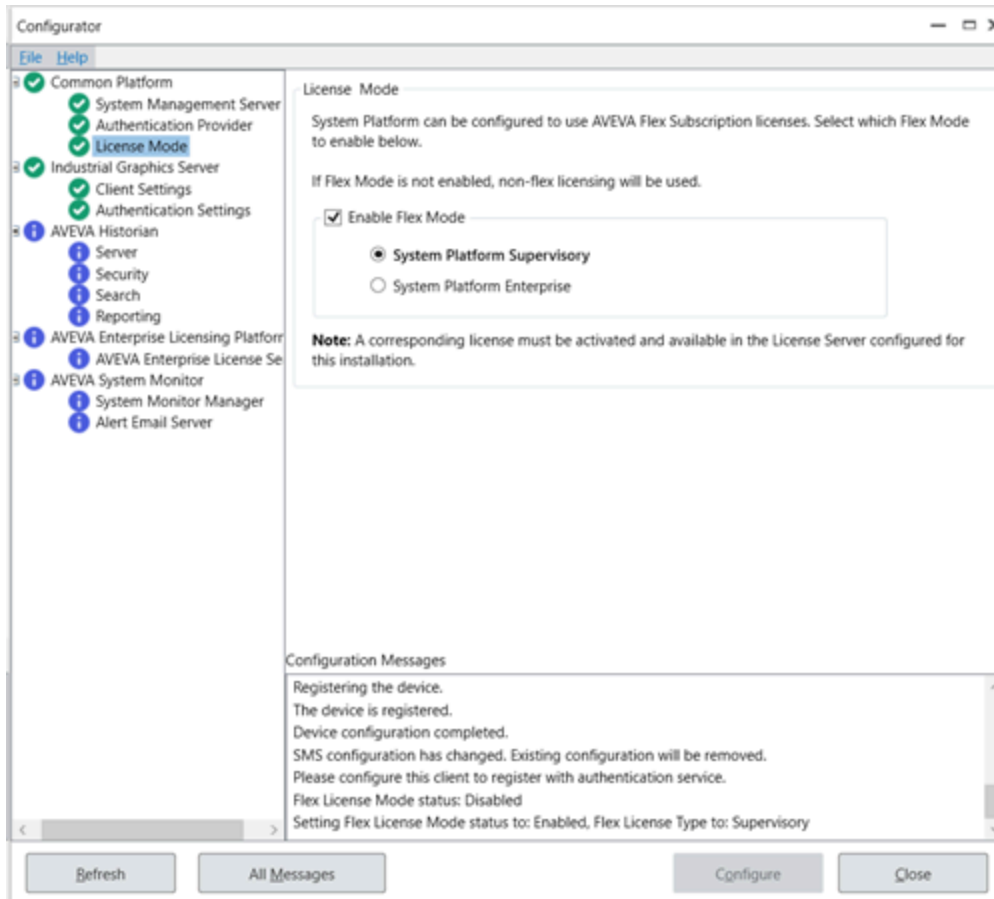
```
$AccessToken = ConvertTo-SecureString -String "*****" -AsPlainText -Force Add-
PcsAuthenticationProvider -name AvevaConnect -ClientID ***** -Endpoint
https://signin.connect.aveva.com -ServicesEndpoint https://services.aveva.com/
-AccessToken $AccessToken
```

## Galaxy License Mode Configuration

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](#).

## Industrial Graphic Server Configuration

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 [Common Platform Services](#) 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](#).

## AVEVA Historian Configuration

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 [Common Platform Services](#).
- To configure licensing, see [AVEVA Enterprise License Server Configuration](#).

## To configure AVEVA Historian:

1. Launch the Configurator from the Start menu. In the left pane, click **Server**.

The screenshot shows the 'Configurator' window with the 'Server' configuration page selected. The left pane shows a tree view with the following items: Common Platform (checked), Industrial Graphics Server (checked), AVEVA Historian (selected), AVEVA Enterprise Licensing Platform, and AVEVA System Monitor. Under 'AVEVA Historian', the 'Server' item is selected, with sub-items: Security, Search, and Reporting. The main pane displays the following configuration options:

- Database Information**
  - SQL Instances: SP-BL01
  - Database Path: C:\Program Files\Microsoft SQL Server\MSSQL15.MSSQL (with ellipsis button)
  - Data Path: C:\Historian (with ellipsis button)
  - Existing Database Conflict
    - ☒ Drop and create new database
  - Alarms and Events Storage
    - ☒ High-speed: History blocks, store up to 1,000 messages/second (recommended)
    - ☐ Traditional: SQL Server, store up to 100 messages/second
- Network**
  - Historian
    - TCP Port (Classic): 32568
    - TCP Port: 32565
- Security**
  - ☐ Allow remote access for OCMC
  - ☐ Allow secure connections only
- Configuration Messages**
  - Microsoft .NET Framework:
    - Version 2.0.50727.4927
    - Version 3.0.30729.4926
    - Version 3.5.30729.4926
    - Version 4.0.0.0
    - Version 4.8.3761
  - Pre-Requisite:SQLServer Condition met

At the bottom of the window, there are four buttons: Refresh, All Messages, Configure, and Close.

2. 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. The default is tied to your SQL Server installation and is the path where the configuration database is deployed. If you need to change the default path, click the ellipsis button to specify a different directory in which to install the historian database files.
3. 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.
4. 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**

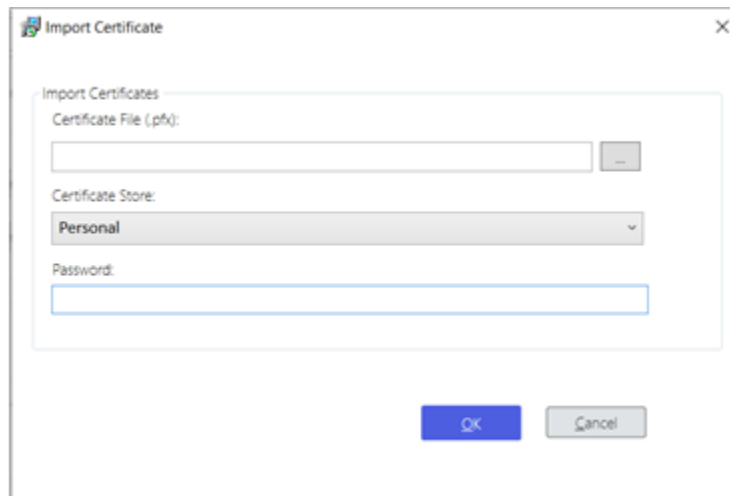
The traditional setting stores alarms and events in the A2ALMDB SQL Server database. This works well for smaller applications. Alarm and event data stored in the A2ALMDB database can be retrieved using SQL queries. You can also use SQL Server tools, such as Reporting Services, to query alarm and event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

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

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

For more details about using enabling encrypted communication for the Historian, see [Using HTTPS Instead of HTTP for Historian Client, Historian Client Web, and REST APIs](#).

- a. To use a certificate provided by your IT department, select "Provided by IT (import / select)" as the **Certificate Source**.
  - a. If the certificate is already installed on the system, select the appropriate **Certificate** from the list.
  - b. If you have been provided with a certificate but it is not yet installed on the system, click **Import...**. The **Import Certificate** dialog displays.



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

- c. Select the **Certificate Store** in which to save the Certificate, as directed by your IT department.
  - d. Enter the **Certificate** password and click **OK** when all the information is correct.
- b. To use a self-signed certificate, select "Automatically Generated" as the **Certificate Source**. The name of the **Certificate** is automatically selected for you and cannot be changed.

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

---

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

---

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

---

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

---

- d. The **Connections** option determines what happens when a connection is made to Historian Client Web over the untrusted (HTTP) port. Select one of the following options:
  - a. **Favor trusted connections, but permit untrusted connections.** When this option is selected, users at run time are informed there is a trusted connection available, and they can decide whether to use the trusted or untrusted connection. For more information about the run-time options, refer to the *Historian Administrator Guide*.
  - b. **Require trusted connections (clients must trust this certificate).** When this option is selected, if you are using a certificate from a trusted authority, users are redirected to the HTTPS connection. If you are using an untrusted certificate, such as a self-signed certificate, an informational message is

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

- e. Click **OK** to accept the selected options, then click **Configure** to apply any changes to the system.

For more information about secure, encrypted communication between nodes, see [Common Platform Services](#).

7. Under **Security**, select **Allow Remote Access for OCMC** if you want to allow remote access of this server's Operations Control Management Console (previously called the System Management Console, or SMC). This option is disabled by default for improved security, and we recommend that you use remote desktop software to administer remote Historian servers.

When you select **Allow Remote Access for OCMC**, Historian allows remote connection to the Operations Control Management Console. 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.

---

**Important:** In 2022, Microsoft released a phased update to address a security issue with DCOM on Windows. After the third phase of this update is applied, administering remote historian servers will no longer be possible using the Operations Control Management Console. Instead, you can administer remote Historian servers by first connecting with the remote desktop software of your choice, and then using the Operations Control Management Console on the remote server.

---

For more up-to-date information about the vulnerability, and a timetable for its phased release, see <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26414>.

---

8. 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:
    - a. To create a new user account, click **Create Users** and then specify account details.
    - b. To add existing user accounts to this list, click **Add Users** and then select the account criteria to use.
    - c. If you don't need this account anymore, mark the **Delete Account** check box.
  - b. If you have configured an AVEVA Identity Manager server, click **Add External Groups**.

The Add External Groups dialog appears. To configure external groups:

- i. The Identity Provider Node field is automatically populated with the address of the AVEVA Identity Manager server based on the System Management Server configuration. Click **Get Groups**. The Connect Groups dialog appears. Select the groups you want to add and click **Add**.
- ii. The groups are retrieved from the AVEVA Identity Manager server and display in the Connect Groups - Historian Role section. For each external group, select from the dropdown which Historian role the group will have.
- iii. Click **Save**.
- c. Under **SQL Logins**, do one of the following to ensure your SQL Server logins are secure:
  - a. If you want to keep using a default account listed, type a new password.
  - b. 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.

---

9. 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.

10. 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.
11. In the **Configuration Messages** area, read messages regarding prerequisite checks, current configuration state, and configuration activities that are logged.
12. Click **Configure**. The **Processing SQL Script** dialog box appears. You can see the historian database configuration scripts running. Multiple scripts run during the configuration.
13. 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.
14. Click **All Messages** to see all the configuration messages.

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

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

### About TLS, HTTPS, and X.509 Certificates

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

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

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

### About Configuring Security

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

Connections

☒ Favor trusted connections, but permit untrusted connections

☐ Require trusted connections (clients must trust this certificate)

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

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

You are using an **untrusted** connection to this Historian, but a trusted connection is available.

[Always use the trusted connection](#)

[Use the trusted connection this time](#)

[Continue with the untrusted connection \(not recommended\)](#)

- **Always use the trusted connection**

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

- **Use the trusted connection this time**

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

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

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

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

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

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

This Historian requires an encrypted connection, but the server is not fully configured in a way your browser will trust it. If you are an administrator, you can [learn more about this problem and how to correct it](#) and if you are not, please contact your administrator about this problem. If you accept the warning messages from your browser, you can switch to an **untrusted, but encrypted** connection:

[Use the untrusted, encrypted connection](#)

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

---

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

---

### Using a Self-Signed Certificate

If you choose to use a self-signed certificate with the Historian, you are responsible for configuring all clients to

trust that certificate. Clients that haven't trusted the certificate see a security warning in their browser.

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



### Your connection is not private

Attackers might be trying to steal your information from [redacted] (for example, passwords, messages, or credit cards). [Learn more](#)

NET::ERR\_CERT\_AUTHORITY\_INVALID

Hide advanced

Back to safety

This server could not prove that it is [redacted]; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

[Proceed to \[redacted\] \(unsafe\)](#)

## Enabling Trust for a Self-Signed Certificate

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

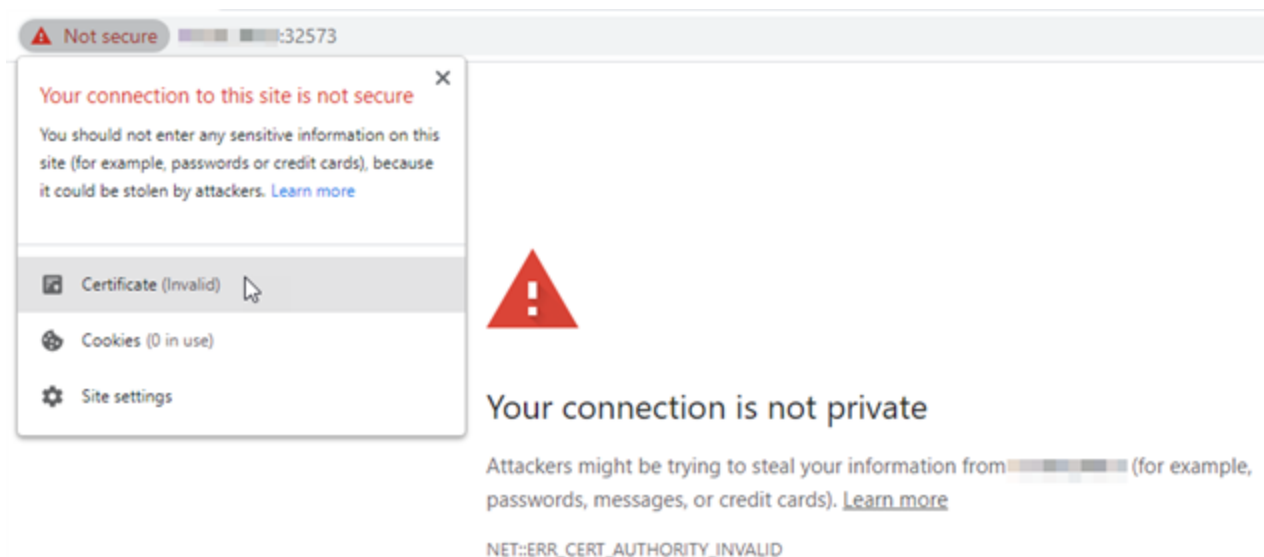
1. Acquire a copy of the certificate.
2. Install the certificate into the trusted root certificate store.

## Acquiring a Copy of the Self-Signed Certificate

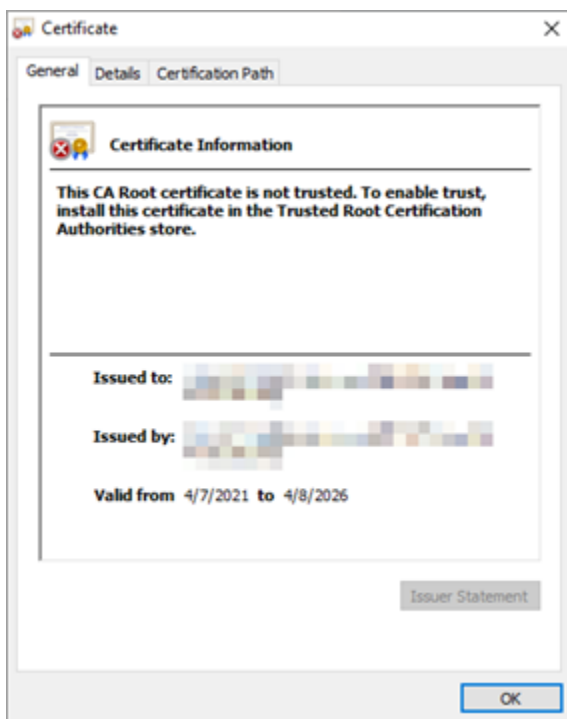
Before you can trust a self-signed certificate, you need a copy of the certificate on your system. If you already have a copy of the certificate, proceed to [Trusting a Self-Signed Certificate](#).

### To obtain a copy of the self-signed certificate:

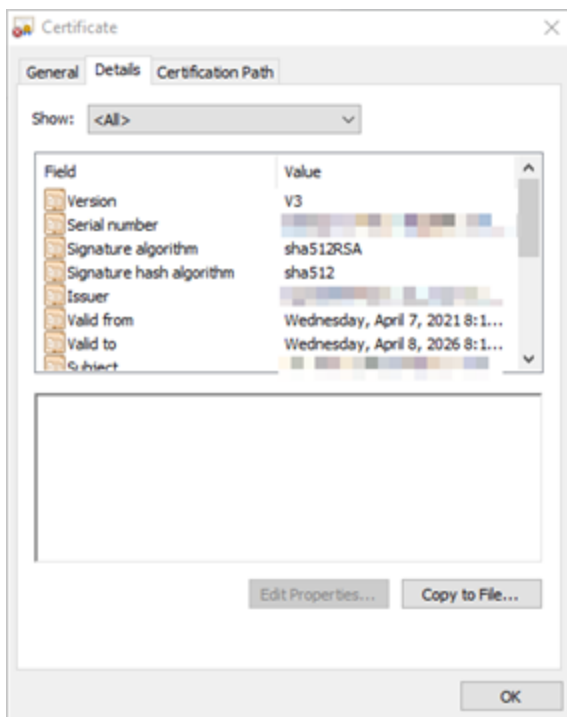
1. In your browser, browse to the AVEVA Historian Client Web URL.
2. In the address bar, click on the warning message indicating your connection is not secure.



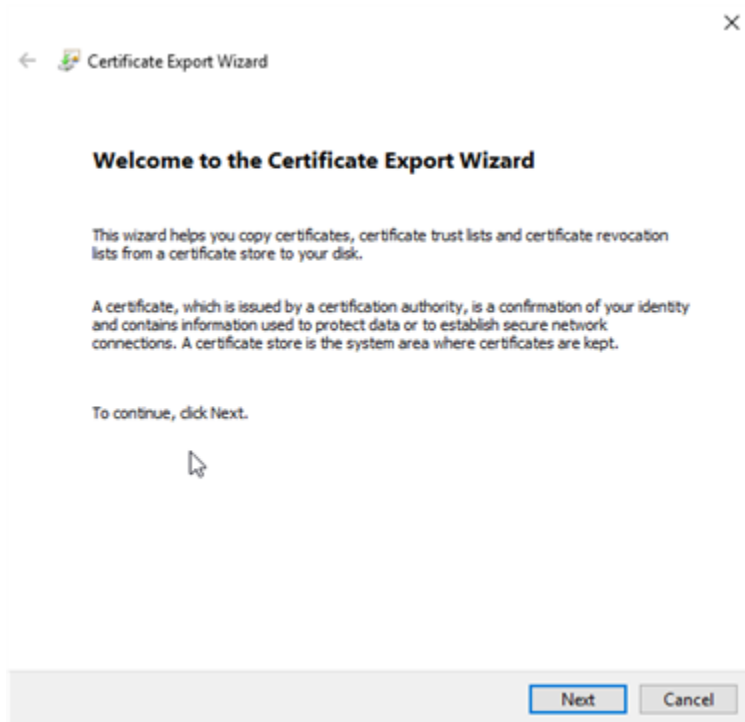
3. Click **Certificate (Invalid)**. The **Certificate** details dialog displays:



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



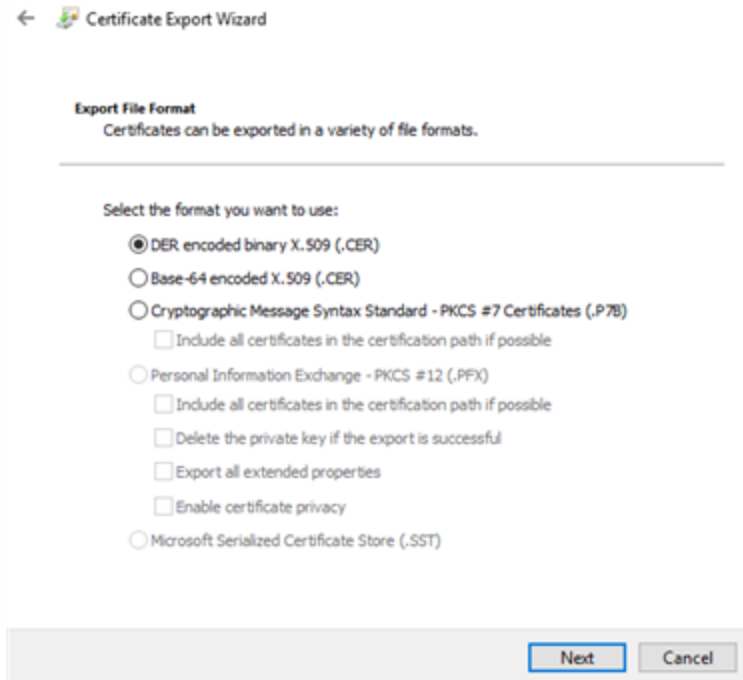
- Click **Copy to File...**. The **Certificate Export Wizard** displays:



Click **Next**.

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





← Certificate Export Wizard

**Export File Format**  
Certificates can be exported in a variety of file formats.

---

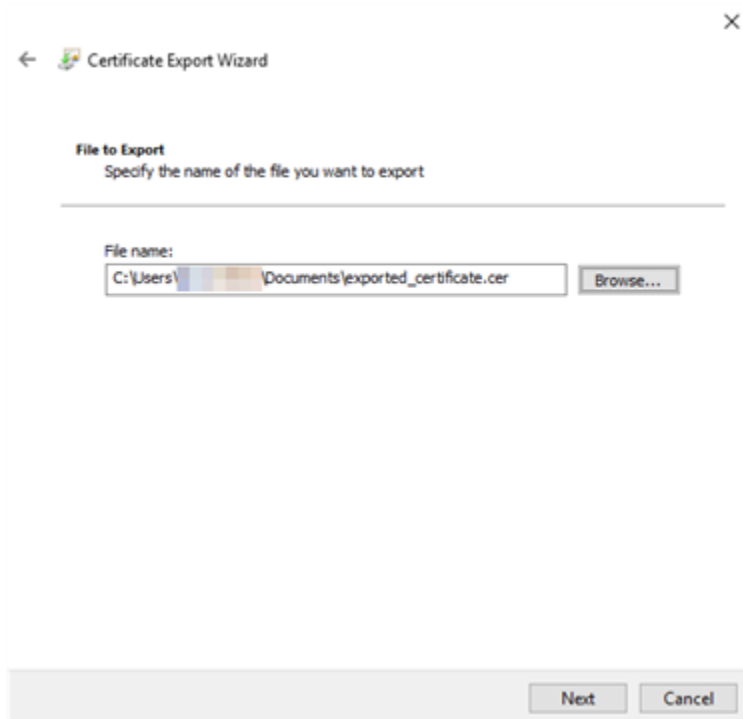
Select the format you want to use:

- ☒ DER encoded binary X.509 (.CER)
- ☐ Base-64 encoded X.509 (.CER)
- ☐ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
  - ☐ Include all certificates in the certification path if possible
- ☐ Personal Information Exchange - PKCS #12 (.PFX)
  - ☐ Include all certificates in the certification path if possible
  - ☐ Delete the private key if the export is successful
  - ☐ Export all extended properties
  - ☐ Enable certificate privacy
- ☐ Microsoft Serialized Certificate Store (.SST)

Next Cancel

Click **Next**.

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



×

← Certificate Export Wizard

**File to Export**  
Specify the name of the file you want to export

---

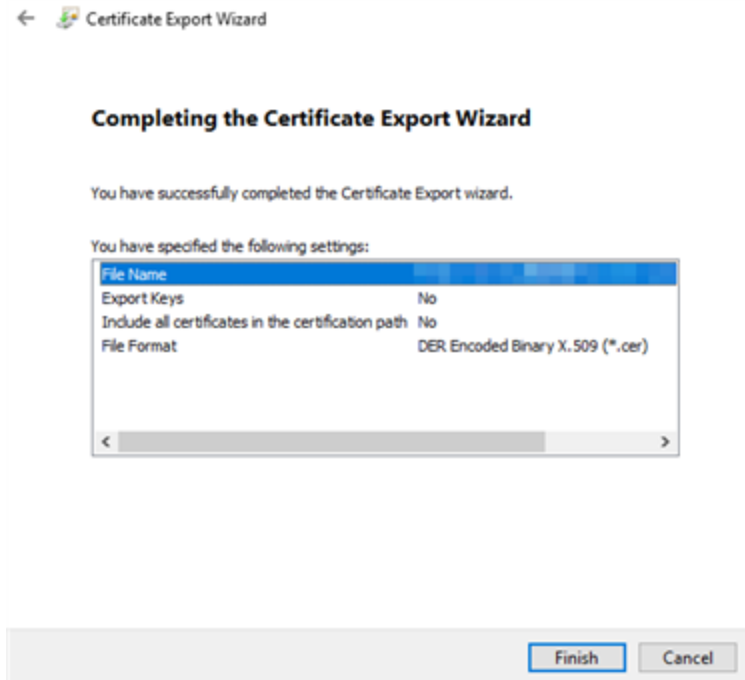
File name:

C:\Users\... Documents\exported\_certificate.cer Browse...

Next Cancel

Click **Next**.

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

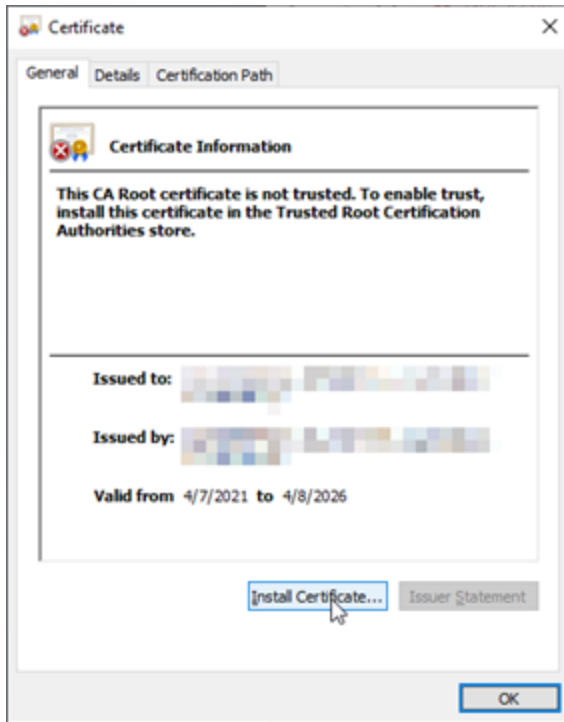


## Trusting a Self-Signed Certificate

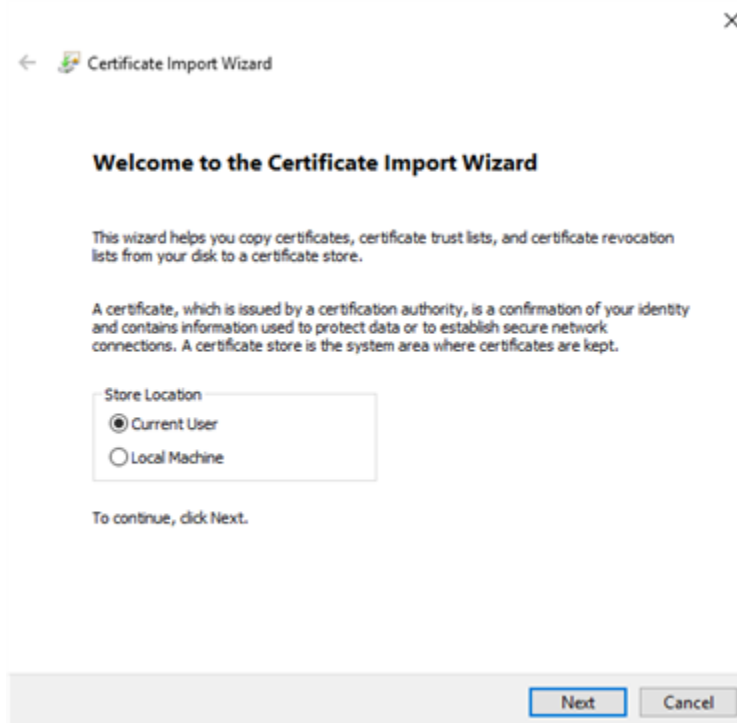
If the AVEVA Historian is configured with a self-signed certificate for TLS encryption, the certificate needs to be trusted on all client machines to avoid warning messages while using AVEVA Historian Client Web. To accomplish this, install the certificate into the trusted root certificate store on each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

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

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



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



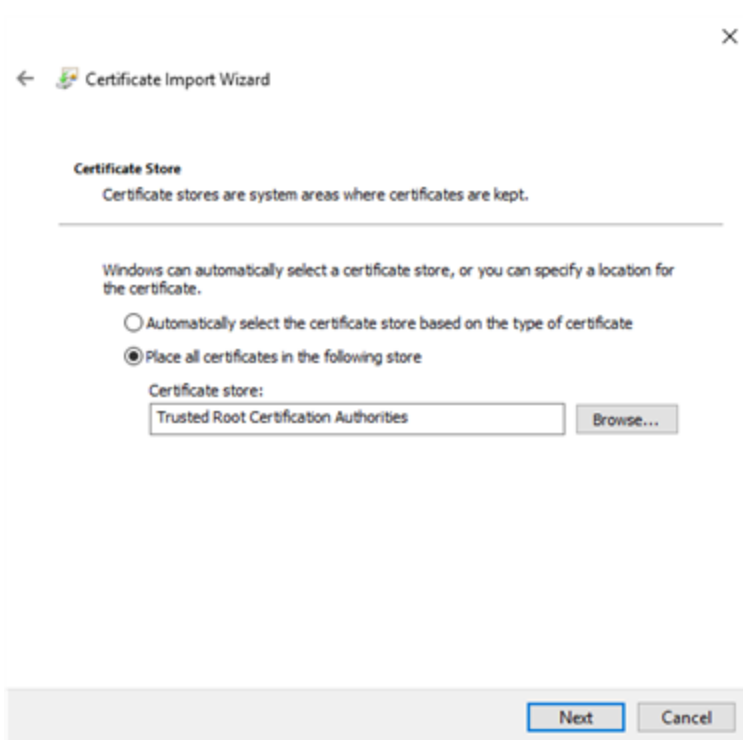
3. Select **Current User** to install the certificate for only the current user, or **Local Machine** to install the certificate for all users on this system.

---

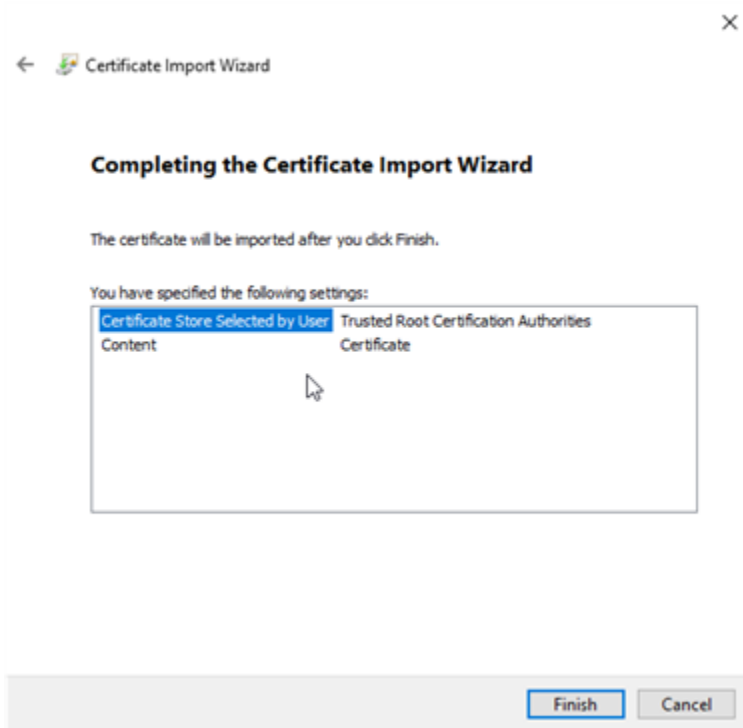
**Note:** The **Local Machine** option requires administrative access to the system. If you do not have administrative access, select **Current User**.

---

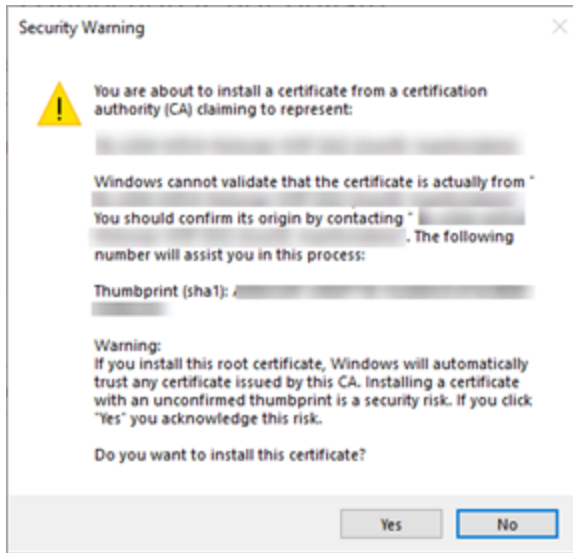
Click **Next**. The **Certificate Store** dialog displays:



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



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



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

## AVEVA Enterprise License Server Configuration

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:

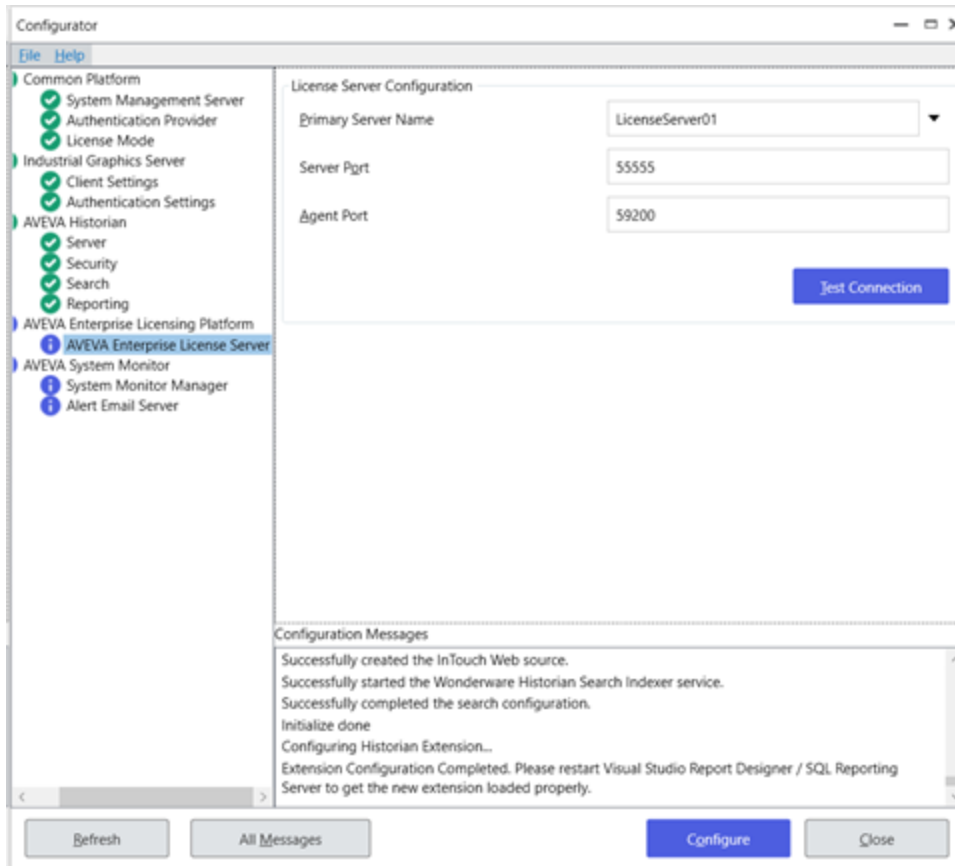
1. In the left pane, select **AVEVA Enterprise License Server**. Then, in the right pane enter:
  - **Primary Server Name:** if the License Server is not installed on the local node, enter the License Server name, or select a server name from the drop down list of previously-configured License Servers (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](#).

## AVEVA System Monitor Configuration

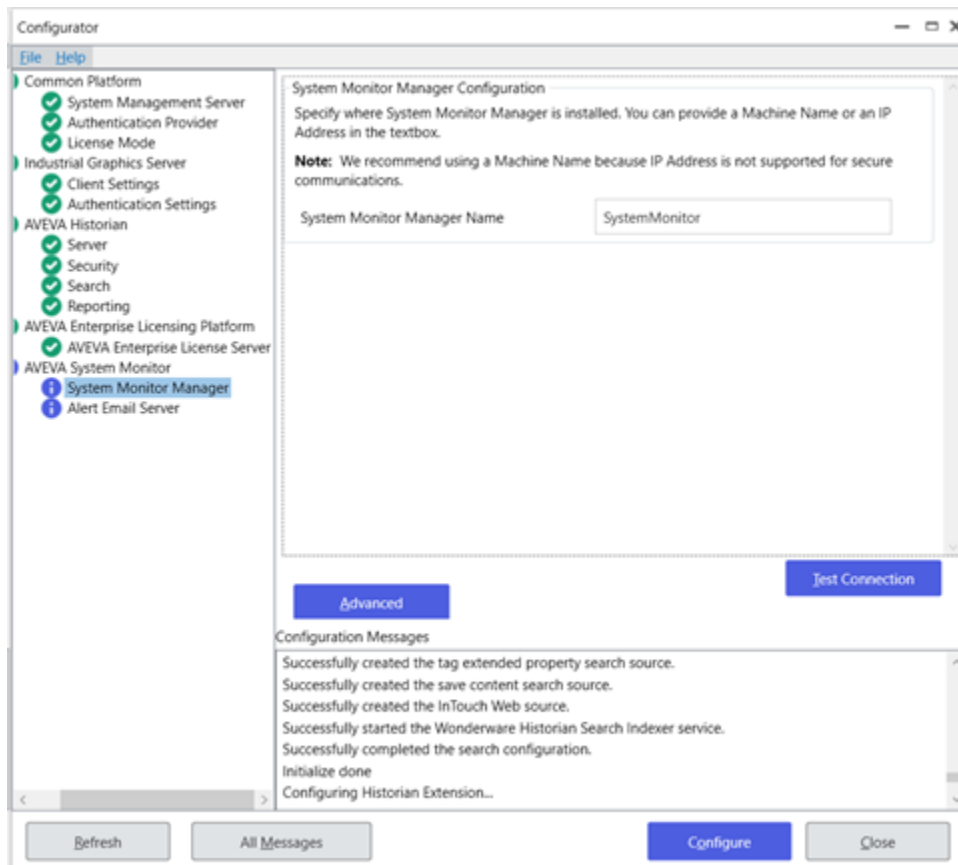
The AVEVA System Monitor contains two configuration items:

- **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](#).

## 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**.



**Configurator**

**File Help**

**Common Platform**

- System Management Server
- Authentication Provider
- License Mode

**Industrial Graphics Server**

- Client Settings
- Authentication Settings

**AVEVA Historian**

- Server
- Security
- Search
- Reporting

**AVEVA Enterprise Licensing Platform**

- AVEVA Enterprise License Server

**AVEVA System Monitor**

- System Monitor Manager
- Alert Email Server**

**Email Server Configuration (Optional)**

To receive email alerts from AVEVA System Monitor, we need information about your SMTP (Simple Mail Transport Protocol) email server. You may need to consult with your administrator to get these details.

You can enter the details now in the form below, or enter them later through the System Monitor Manager web interface.

☐ Enter Email server details later, in the System Monitor Manager web interface

☒ Enter Email server details now

SMTP Server Name or IP:

SMTP Server Port:

SMTP Server Secured: ☐ Yes ☒ No

From Email ID:

Default Recipient Email ID:

Enter multiple Email IDs separated by semicolon(;).

**Note:** Enable Force Protocol Encryption for SQL Server to avoid information disclosure.

**Configuration Messages**

Successfully started the Wonderware Historian Search Indexer service.  
Successfully completed the search configuration.  
Initialize done  
Configuring Historian Extension...  
Extension Configuration Completed. Please restart Visual Studio Report Designer / SQL Reporting Server to get the new extension loaded properly.  
Configuring license server...

**Refresh** **All Messages** **Configure** **Close**

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."
3. In the **SMTP Server Name or IP** field, enter either the computer name or IP address of the email server to be used for System Monitor alerts.
4. In the **SMTP Server Port** field, enter the port number of the email server (default: 25).
  - Use port number 25 for an unsecured SMTP server.
  - Use port number 465 for a secured SMTP server.

See the *AVEVA System Monitor User Guide* for additional configuration information.
5. In the **SMTP Server Secured** field, enter **yes** if the server is secured, or **no** if it is not.
6. 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.
7. In the **From Email ID** field, enter the email address that will be used to send system alerts from the System Monitor.
8. In the **Default Recipient Email ID** field, enter the email address(es) that will receive system alerts from the System Monitor.
9. Press the **Configure** button.
10. 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

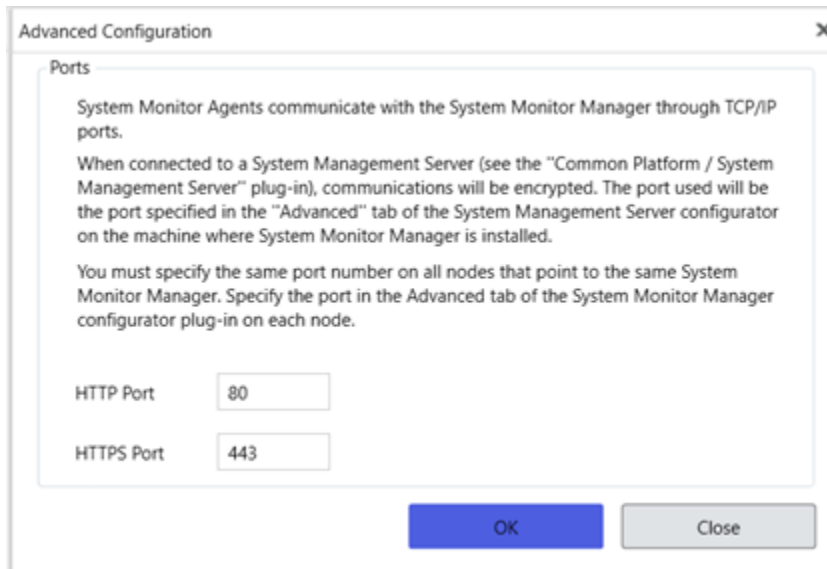
An instance of the System Monitor Agent is installed on every node. Each agent communicates with the System Monitor Manager through TCP/IP and uses the Common Platform settings. Each System Monitor Agent must use the same port number that was configured for the System Monitor Management Server. See [Common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

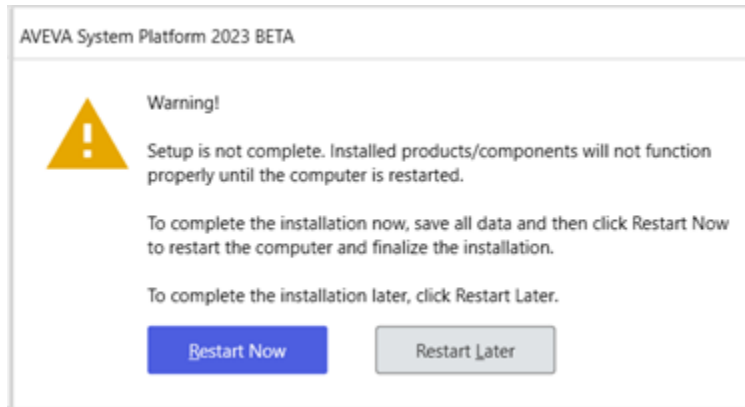
1. In the Configurator, select the **System Monitor Manager** entry, under **AVEVA System Monitor**.
2. Click the **Advanced** button. The **Advanced Configuration** dialog window opens.



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](#).

## 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](#).

# Upgrade, modify, and repair System Platform

**Upgrade to System Platform 2023 R2:** You can upgrade to System Platform 2023 R2 SP1 from System Platform 2017 or newer. If you running a version older than System Platform 2017, you must perform an intermediate upgrade to a version that allows a direct upgrade, and then upgrade to System Platform 2023 R2 SP1.

Migration of Application Server galaxies is supported from all versions, beginning with 4.5, and includes System Platform 2012 and later.

---

**Note:** System Platform Enterprise 2023, and System Platform 2020 R2 Controlled Releases 1 and 2 (CR1 and CR2) cannot be upgraded or migrated to System Platform 2023 R2.

---

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. To enable Operations Control - connected experience, follow the instructions below, and refer to Galaxy migration to support connected experience before you connect to a galaxy.

## Important Upgrade Information

- **64-bit operating system required:** A 64-bit operating system is required to install System Platform 2023 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 2023 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 need to upgrade first to System Platform 2017 as an intermediate step. 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 was a member of the system Administrators group. Starting with System Platform 2017 Update 3, the Network

Account was removed from 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 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 [Configure AVEVA System Monitor](#) for additional information.

Only one System Monitor Manager is required per overall system.

- **Application Server:** Every redundant Application Server run-time node must use the System Management Server if data is being historized. Redundant nodes have an instance of HCAP running, which is used to synchronize tags and store-and-forward data between redundant AppEngines. With the release of System Platform 2023 R2, secure communication is required for HCAP, and thus, redundant nodes will not be able to synchronize data without the SMS.
- **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. After you upgrade System Platform, you can reinstall InTouch Access Anywhere. See [Upgrading InTouch Access Anywhere](#) for details.
- **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 2023 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 [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.

If the System Management Server is not configured for redundant Application Server nodes, there will be data loss, as well as warnings and error messages.

## 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

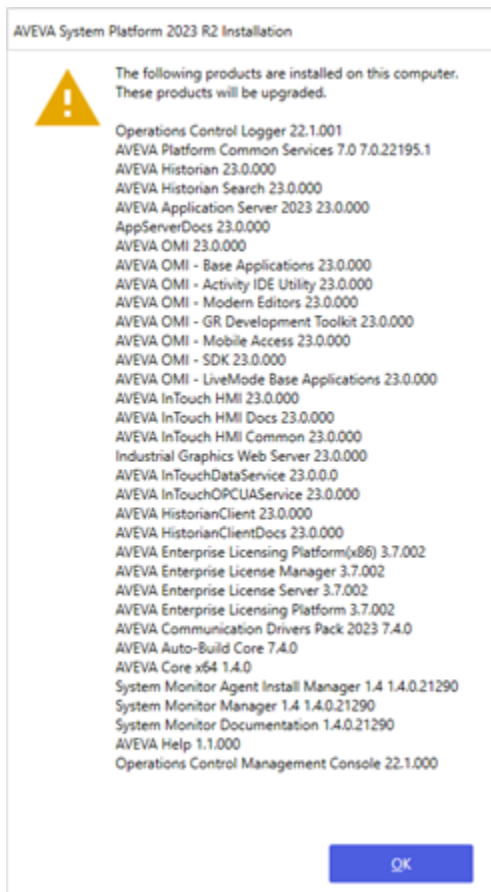
## To add components through the Modify option

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 [Upgrade an IDE-only node](#) and [Upgrade run-time nodes](#) for additional information.

1. 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 and versions to be upgraded. If a 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. Confirm your operating system compatibility, then click **Next** to proceed.
3. A selection list of the products and components to be upgraded is shown. You cannot modify this list. Click **Next** to proceed.
4. Perform any recommended actions, such as backing up your galaxy, then click **Next** to proceed.
5. If required, OI servers are upgraded, then galaxy updates begin after the OI servers are upgraded. If

prompted, click the **Stop Services** button to proceed.

6. After all services stop, click **Next** to proceed.
7. The list of products that will be upgraded is shown. Click **Upgrade** to begin upgrading your system.
8. After the installation is over, the **Configurator** starts. Some items that were previously configured retain their configurations, but you will need to reconfigure certain items including the System Management Server and the Historian (if present).
9. **Important!** If you are upgrading from System Platform 2023 and are using Operations Control - connected experience, and have an existing galaxy that uses the **Authentication providers** security option with Azure AD, you will need to follow the configuration instructions as described in Galaxy migration to support connected experience.

Select **View Readme** for important information about System Platform 2023 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/topic/ms06-061-security-update-for-microsoft-xml-core-services-4-0-sp2-21c429e2-0349-30e5-189a-ca32aea6c2dd>

If you a galaxy is deployed, the Galaxy Patcher will start as soon as you connect to the galaxy from the System Platform 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.

## AVEVA Application Server upgrade

Direct upgrade to AVEVA Application Server 2023 R2 is supported from Application Server 2017 and later versions. However, upgrade is not supported for the following System Platform versions:

- System Platform Enterprise 2023
- System Platform 2020 R2 Controlled Releases 1 (CR1)
- System Platform 2020 R2 Controlled Releases 2 (CR2)

### Authentication Providers with Azure AD - Upgrade to connected experience

If the galaxy security mode is configured for Authentication Providers with Azure AD, the security mode has to be set to “None” (when in non-connected mode), prior to opening the galaxy in connected experience mode.

## About Upgrading Application Server

**Important:** Direct upgrade to Application Server 2023 R2 is supported from Application Server 2017 and later. 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](#), the System Platform Readme, and the [AVEVA Global Customer Support](#) 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**, or you can assign users with an administrator command prompt.

### To assign users through the Control Panel

1. Open the **Control Panel** and select **User Accounts**.
2. Select the user account you want to modify.
3. Click the **Properties** button.
4. In the Properties popup window, select **Group Membership** tab.
5. Select **Other**, under What level of access do you want to grant this user.
6. From the pulldown list, select **aaConfigTools**, then click **OK**.

### To assign users through an administrator command prompt

1. Open a command prompt as administrator.
2. In the command prompt enter:  
`net localgroup aaConfigTools <user name> /add`

## Important Upgrade Information

- **64-bit operating system required:** A 64-bit operating system is required to install System Platform 2023 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 2023 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 need to upgrade first to System Platform 2017 as an intermediate step. 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 was a member of the system Administrators group. Starting with System Platform 2017 Update 3, the Network Account was removed from 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 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 [Configure AVEVA System Monitor](#) for additional information.

Only one System Monitor Manager is required per overall system.

- **Application Server:** Every redundant Application Server run-time node must use the System Management Server if data is being historized. Redundant nodes have an instance of HCAP running, which is used to synchronize tags and store-and-forward data between redundant AppEngines. With the release of System Platform 2023 R2, secure communication is required for HCAP, and thus, redundant nodes will not be able to synchronize data without the SMS.
- **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. After you upgrade System Platform, you can reinstall InTouch Access Anywhere. See [Upgrading InTouch Access Anywhere](#) for details.
- **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 2023 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 [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.

If the System Management Server is not configured for redundant Application Server nodes, there will be data loss, as well as warnings and error messages.

## 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.

- 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 [Upgrade from a previous version](#).

## Upgradeable Application Server components

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 to version 2023 R2.

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 to version 2023 R2.

Upgraded IDE/Client nodes cannot connect to a non-upgraded GR node. The GR node is undeployed before it is upgraded to Application Server 2023 R2.

- 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 to version 2023 R2.

- 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.

---

## Windows upgrades

After Application Server is installed, operating system migration is not supported. If a prior version of System Platform is installed, it 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 [Upgrade 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 [Upgrade 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 [Upgrade run-time nodes](#).
  - Upgrade redundant pairs one at a time. For more information, see [Upgrade 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 2023 R2, 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.

---

## Upgrade 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 2023 R2 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 "Allocating Galaxy Repository Node Memory" in the *Application Server User Guide* 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 [Upgrade, modify, and repair System Platform](#) for information about the installation process.

---

**Note:** 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 [Modify an installation](#) for more information.

---

3. When the **Installation Complete** dialog box appears, click **Configure** to continue. See Get started with

Configurator 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.
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 2023 R2.

---

**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.

---

## Upgrade 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 [Upgrade, modify, and repair 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. See *Get started with Configurator* for details.
3. When prompted, click **Restart Now** to complete the upgrade.

## Migrate 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 "Allocating Galaxy Repository Node Memory" in the *Application Server User Guide* 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, select 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.

## Upgrade 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 [Upgrade, modify, and repair 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. See *Get started with Configurator* for details.
3. When prompted, click **Restart Now** to complete the upgrade.

## Upgrade redundant pairs

---

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

---

If the SMS is not configured, there will be data loss, as well as warnings and error messages.

---

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 is a description of the workflow for upgrading a Galaxy Repository (GR) and one redundant pair of AppEngines (E1 and E1b) from the existing version of System Platform to System Platform 2023 R2 SP1.

- The GR is installed on platform P0.
- The redundant AppEngines are installed on primary platform P1 (active AppEngine E1) and backup platform P2 (standby AppEngine E1b).
- For simplicity, this procedure assumes that each platform has only one engine.

Upgrade the GR first, next, the backup platform, and finally the primary platform.

### Initial State

- All platforms, including the GR, are deployed.
- AppEngine E1 running on Platform P1 is the active engine.
- AppEngine E1b running on Platform P2 is the standby engine.

### Final State

- All nodes are upgraded and deployed.
- AppEngine E1 (Platform P1) is running as the standby engine.
- AppEngine E1b (Platform P2) is running as the active engine.



## Upgrade the GR (P0)

1. **Optional:** If necessary, upload run-time changes to the GR. This saves any changes made during run time to the database.

---

**Caution!** Any configured default values such as set points that are modified at run time will be overwritten if you upload the run-time changes.

---

2. Upgrade the GR node from the current version to System Platform 2023 R2 SP1 with Application Server deployed but shut down.
  - All objects on the GR node become undeployed.
3. Reboot when prompted.
  - System Platform 2023 R2 SP1 is now installed.
4. Open the IDE and migrate the galaxy.
  - The galaxy database is migrated to System Platform 2023 R2 SP1.
  - The IDE shows that platforms P1 and P2 are in SUP (software upgrade pending) state.
5. **Optional:** Open and migrate InTouch ViewApps.
  - InTouch ViewApps are now migrated to System Platform 2023 R2 SP1.
6. Cascade deploy the GR node.
  - All objects on the GR node are now deployed.

## Upgrade Standby Platform (P2)

1. Upgrade the standby platform (P2) hosting the backup AppEngine E1b to System Platform 2023 R2 SP1. Application Server is deployed but shut down.
  - P2 and its hosted engines and objects become undeployed.
2. Cascade deploy P2.
  - AppEngine E1 becomes undeployed but objects under E1 continue to show as deployed.
  - AppEngine E1b becomes active. Hosted objects (shown under E1) are now running under System Platform 2023 R2 SP1. Note that AppEngine E1b does NOT start from the check-pointed state of AppEngine E1, which is still running under the prior version of System Platform.

---

**Caution:** The cascade deployment results in a brief downtime for all objects hosted by the redundant engines E1 and E1b as E1 transitions to undeployed. This downtime can last anywhere from a few seconds to a few minutes, depending on the number of objects.

---

## Upgrade Active Platform (P1)

1. Upgrade (formerly active) platform P1 hosting the backup AppEngine E1 to System Platform 2023 R2 SP1. Application Server is deployed but shut down.
  - P1 becomes undeployed.
2. Cascade deploy P1.
  - AppEngine E1 is deployed as part of platform P1 deployment. E1 starts as the standby AppEngine and fully syncs with active AppEngine E1b.
  - AppEngine E1b continues to run as active.

All nodes have now been upgraded and all platforms and engines are deployed.

- Platform P0 (GR) is deployed.
- Platform P1 is running as backup. AppEngine E1, running on P1, is deployed - standby.
- Platform P2 is running as primary. AppEngine E1b, running P2, is deployed - active.

After you have upgraded to System Platform 2023 R2 SP1, you can enable CPU load balancing to improve the performance of redundant AppEngines during failover. See "Working with Redundancy" in the *Application Server User Guide* 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.
Select a backup redundant partner engine for deployment	<p>The backup redundant engine extracts the hosted objects from the primary redundant engine and deploys them along with the backup redundant engine.</p> <p>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.</p> <p>A dialog displays with the option to continue deployment or to cancel.</p>
Partner engine is deployed but not reachable or not ready to sync.	Redundant engine deployment fails.

Action or State	Behavior
Partner engine has older software version.	<p>The partner engine is detected and recognized as having an older software version. It is automatically stopped and unregistered.</p> <p>Primary engine transitions into <b>Active – Partner not Upgraded</b> redundancy status.</p> <p>Primary and backup partners cannot sync, but references to a redundant engine with this status—or with <b>Active</b> or <b>Active – Standby not Available</b> redundancy statuses—will resolve.</p> <p>Application Objects can be deployed to a redundant partner with <b>Active – Partner Not Upgraded</b> redundancy status.</p> <p>You will not be able to deploy the partner engine until you have upgraded it.</p>

## 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 [Common Platform Services](#) 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 2023 R2.

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

## Modify 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.

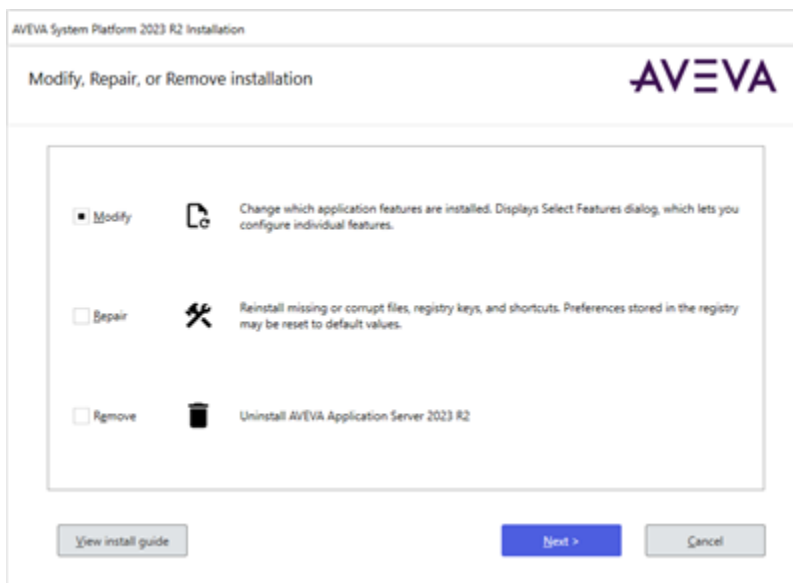
### To modify an installation

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.

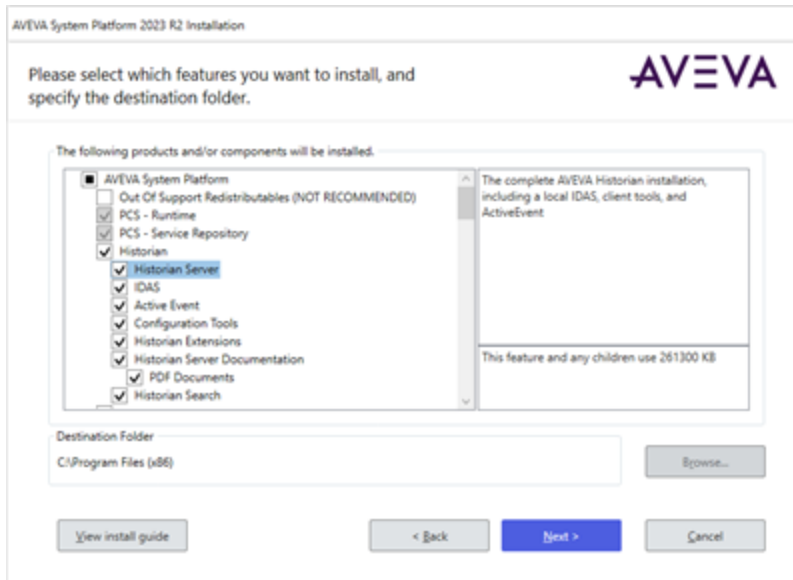
---

**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 Get started with Configurator for information.
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.

## Repair an installation

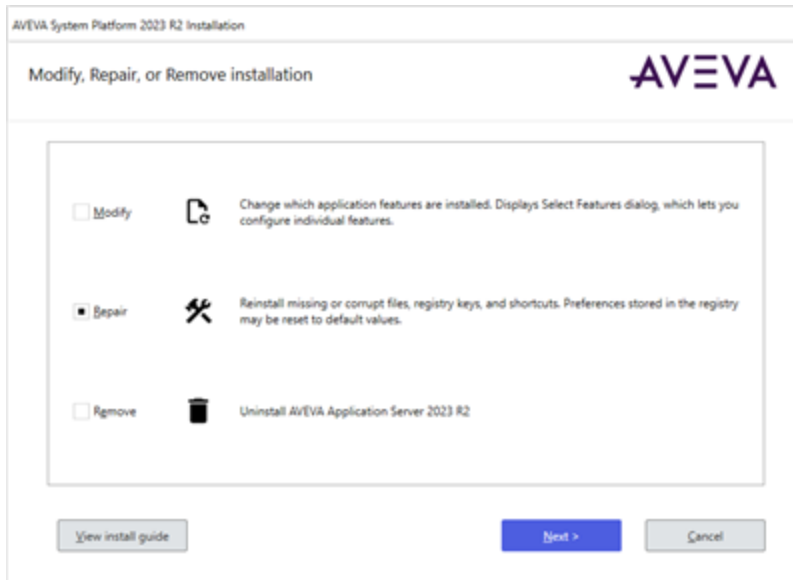
You can repair the installation of any System Platform component to fix missing or corrupt files, registry keys or shortcuts. You can also reset the registry key to the default value.

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

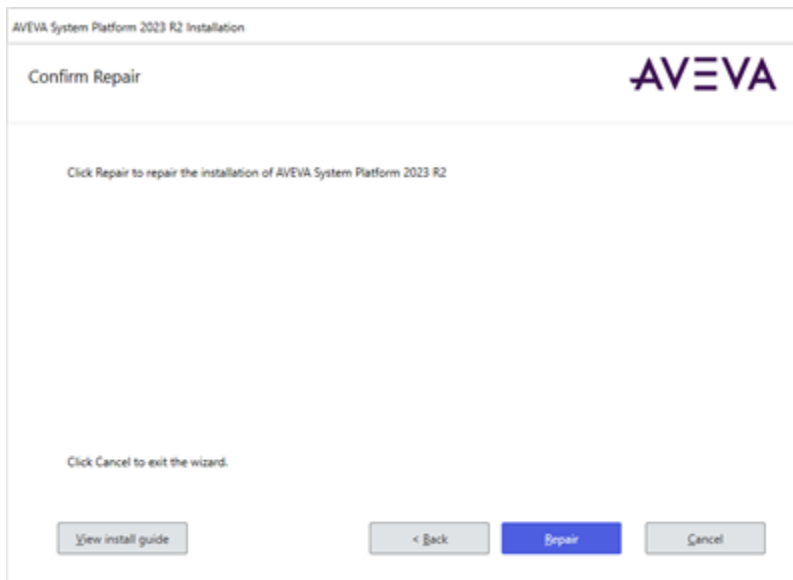
### To repair an installation

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.

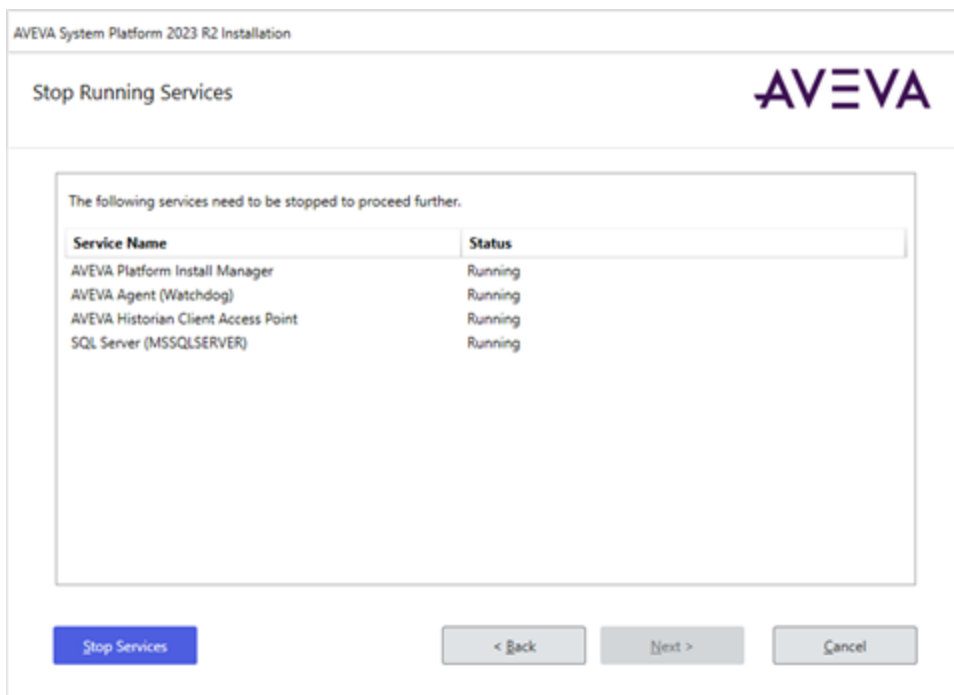
**Note:** The name of the **Uninstall/Change** option may vary depending on which Windows operating system is installed on your computer.



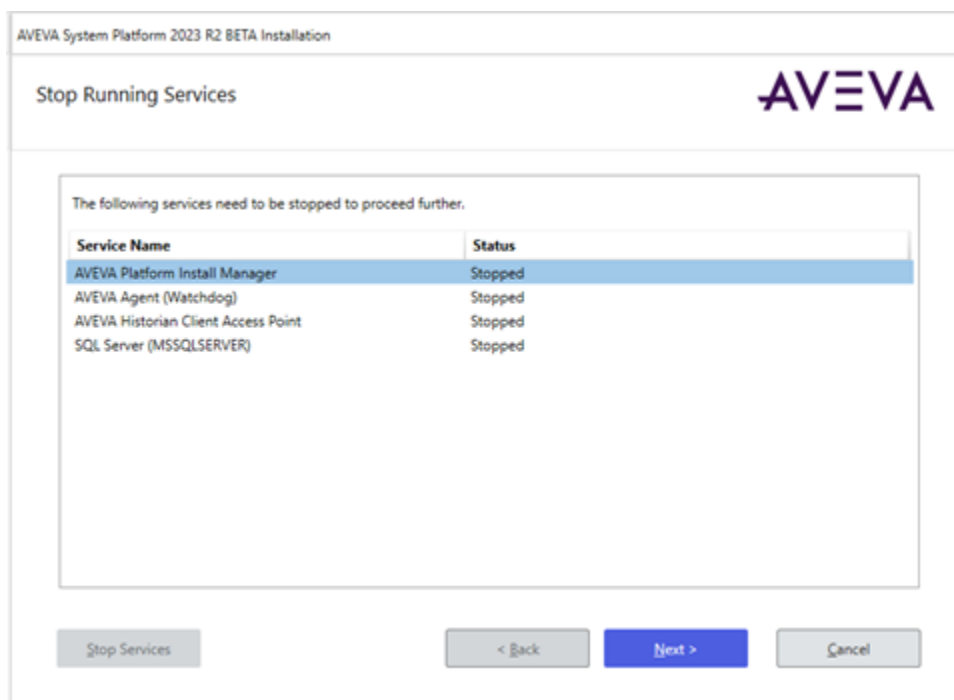
2. Select the **Repair** option, then click **Next**. The **Confirm Repair** dialog box appears.



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.



- When all services stop, the **Next** button becomes active. Click the button to proceed.



- A progress bar is displayed as the system updates and repairs itself.
- When the update has finished, the **Process Complete** dialog box appears. Click **Finish** to close the dialog box and complete the process.

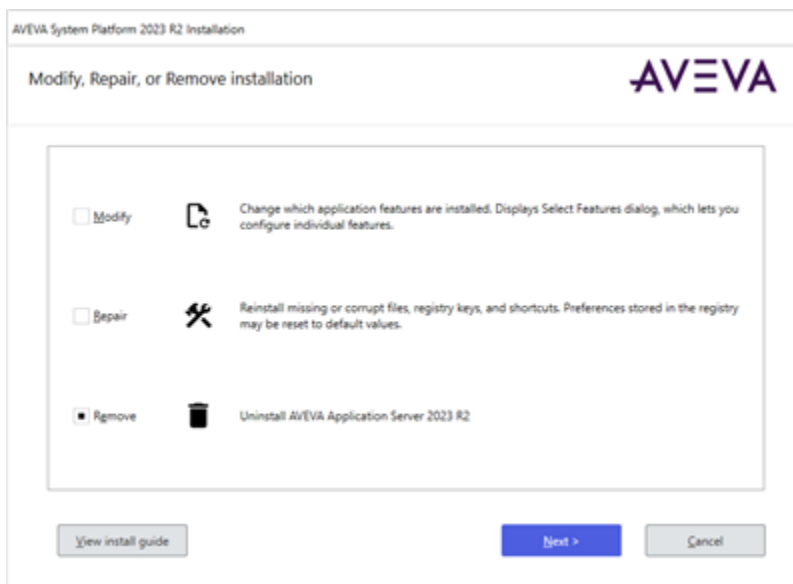
# Uninstall AVEVA System Platform

## 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)

We recommend using the System Platform installation DVD to uninstall System Platform. This is much more efficient than uninstalling each application individually through the Windows **Control Panel**. After you complete the uninstall operation, check the **Control Panel** for any applications that were not caught.

To uninstall from the **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 Platform Common Services
7. System Monitor Manager
8. System Monitor Agent Install Manager
9. AVEVA Communications Drivers Pack
10. AVEVA Enterprise License Manager
11. AVEVA Enterprise License Server
12. AVEVA Enterprise Licensing
13. AVEVA Enterprise Licensing (x86)
14. AVEVA Help

# 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**, or you can assign users with an administrator command prompt.

### To assign users through the Control Panel

1. Open the **Control Panel** and select **User Accounts**.
2. Select the user account you want to modify.
3. Click the **Properties** button.
4. In the Properties popup window, select **Group Membership** tab.
5. Select **Other**, under What level of access do you want to grant this user.
6. From the pulldown list, select **aaConfigTools**, then click **OK**.

### To assign users through an administrator command prompt

1. Open a command prompt as administrator.
2. In the command prompt enter:  
`net localgroup aaConfigTools <user name> /add`

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

## 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 [Set 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.

---

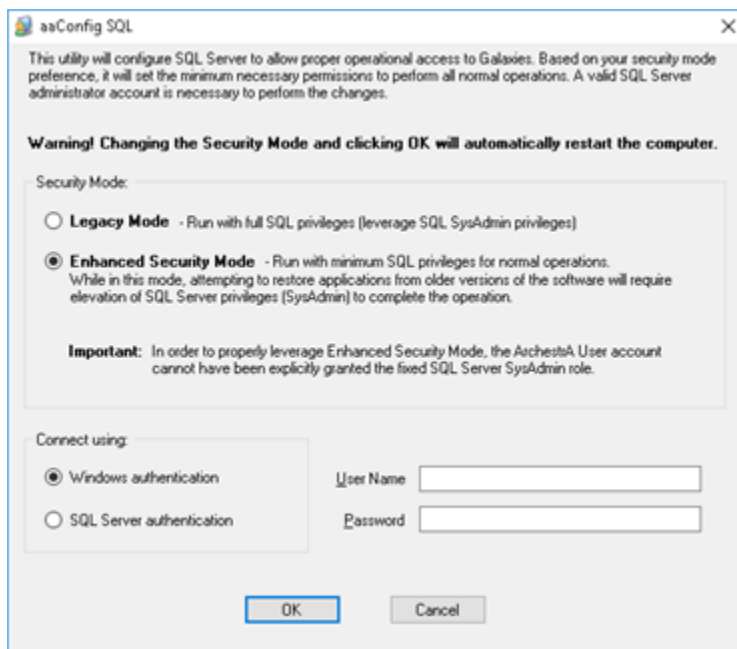
**Note:** The aaGalaxyOwner account is the owner (dbo) of all Galaxy databases in your system. It does not have a system login.

---

- 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.

## Set 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 shortcut 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>aaAdministrators (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** (default).
  - **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>aaAdministrators 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.

---

## Restore 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.

## Set 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.

# Configure SQL Server

## SQL Server requirements

If required for the products/roles you are installing, and you will not be using the version of SQL Server Express supplied with System Platform, install Microsoft SQL Server before installing System Platform. It is important to take into consideration the requirements of the different versions of SQL Server. For detailed SQL Server installation instructions, refer to the Microsoft documentation and the AVEVA TechNote applicable to your version of SQL Server. available on the AVEVA Global Customer Support web site.

- Installing Microsoft SQL Server 2016  
<https://softwaresupportsp.aveva.com/#/okmimarticle/docid/tn000032384>
- Installing Microsoft SQL Server 2019  
<https://softwaresupportsp.aveva.com/#/okmimarticle/docid/tn000032660>

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 2022 Express Core 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

Install all cumulative updates for all versions of SQL Server. Check the [AVEVA Technology Matrix](#) for the latest updates to this list.

- SQL 2016 Express-SSMSE (SP3 plus all cumulative updates) [Microsoft support ends 14 Jul 2026]
- SQL 2016 Standard, Enterprise (SP3 plus all cumulative updates) [Microsoft support ends 14 Jul 2026]
- SQL 2017 Express Core / Express with Advanced Tools) (plus all cumulative updates) [Microsoft support ends 12 Oct 2027]
- SQL 2017 Standard, Enterprise (plus all cumulative updates) [Microsoft support ends 12 Oct 2027]
- SQL 2019 Express Core / Express with Advanced Tools) (plus all cumulative updates) [Microsoft support ends 8 Jan 2030]
- SQL 2019 Standard, Enterprise (plus all cumulative updates) [Microsoft support ends 8 Jan 2030]
- [DEFAULT] SQL 2022 Express Core / Express with Advanced Tools) (plus all cumulative updates) [Microsoft support ends 11 Jan 2033]
- SQL 2022 Standard, Enterprise (plus all CUs) [Microsoft support ends 11 Jan 2033]

To access the relevant information from the Technology Matrix, go to the Knowledge and Support Center website, select the Technology Matrix icon, and then enter the name of the System Platform product (for example, Application Server or Historian), or enter the Windows or SQL Server version you wish to use (for

example, SQL Server 2022 Standard x64).

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 Core 2022.
- 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/IPIf **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/IPIf **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>**.

## Work 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 install SQL Server 2022 Express Core. 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 2022 Express Core 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 2016 Standard or Enterprise SP3 (or SP3 plus all cumulative updates)
- SQL Server 2017 Standard or Enterprise with all cumulative updates
- SQL Server 2019 Standard or Enterprise with all cumulative updates
- SQL Server 2022 Standard or Enterprise with all cumulative updates

See the *System Platform Readme* for additional information.

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

<https://learn.microsoft.com/en-us/sql/sql-server/editions-and-components-of-sql-server-2022?view=sql-server-ver16>

## 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 2022 Express Core 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 2023 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.

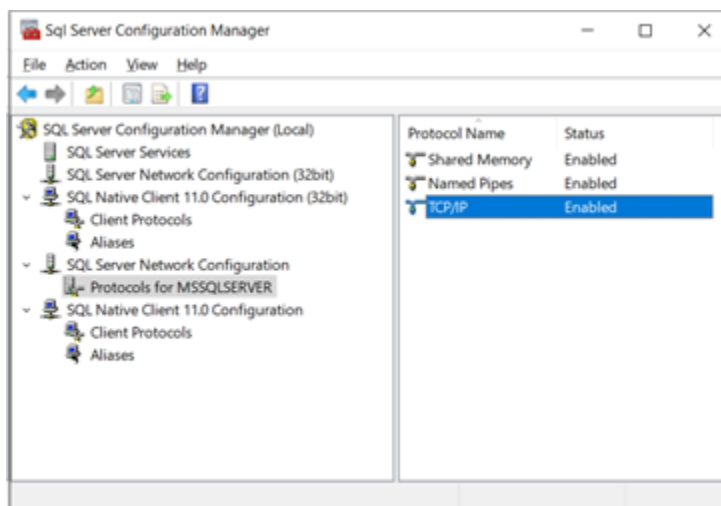
## Use a non-default port for SQL Server

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.

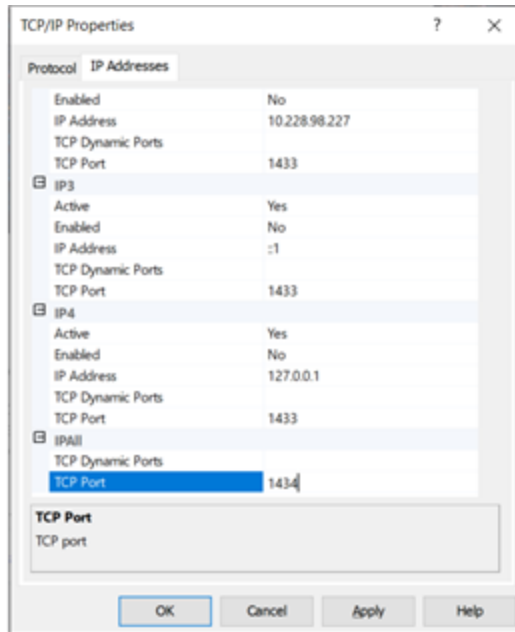
If you are using the SQLData object to store and retrieve data, you will need to enter the non-default SQL Server port number as you enter other database connection information. See the SQLData Object help file, available through the System Platform IDE, for additional information.

### 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.

## Set 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).

For more information, refer to the following Microsoft documentation:

<https://learn.microsoft.com/en-us/sql/sql-server/install/configure-the-windows-firewall-to-allow-sql-server-access?view=sql-server-ver16>

# AVEVA InTouch HMI requirements and prerequisites

You need to meet the requirements and prerequisites for products.

## Install the Gateway Communication Driver and upgrade from FS Gateway

The Gateway Communication Driver (Gateway) is automatically installed as an InTouch component when InTouch is selected for installation. Gateway replaces Factory Suite (FS) Gateway, which was supplied with earlier versions of System Platform. Like FS Gateway, 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 Gateway as part of installing InTouch, you can install Gateway as a stand-alone application. There are three common installation scenarios.

### Scenario 1: "Clean" System without Gateway or FS Gateway

In this scenario, Gateway is installed as part of InTouch installation.

### Scenario 2: Older version of Gateway is installed

The System Platform installation program upgrades the existing Gateway version to the new version and exits.

Restart the System Platform installation program after the Gateway has been upgraded.

This installs the remaining System Platform components, including InTouch.

### Scenario 3: FS Gateway is installed

The System Platform installation program removes FS Gateway, but saves the existing FS Gateway configuration.

Two instances of Gateway are then installed. The existing FS Gateway is replaced by the second Gateway instance, which uses the existing FS Gateway application name.

After the upgrade to System Platform 2023 R2 is complete, activate the instance that has replaced FS Gateway.

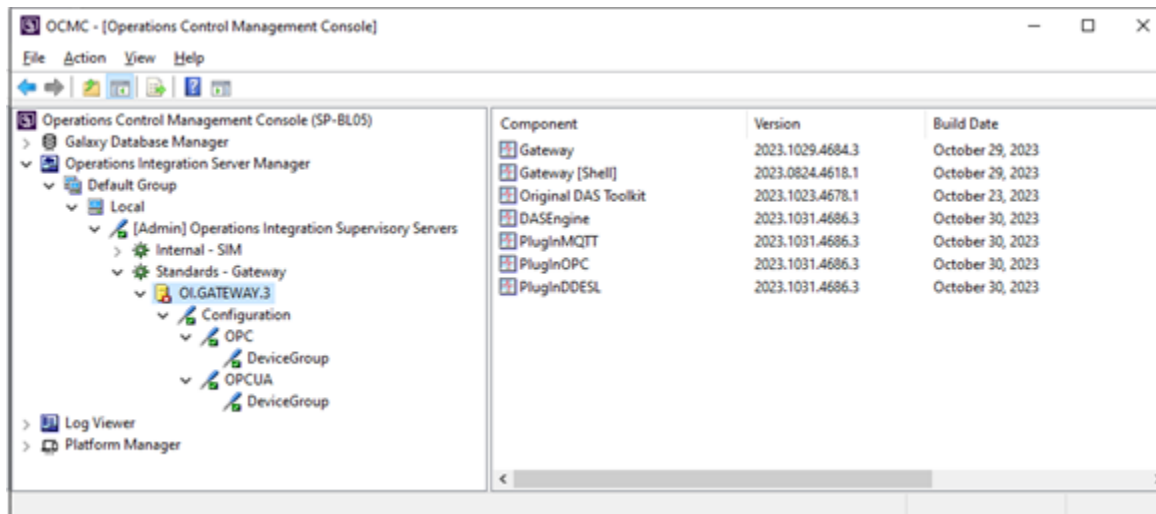
There is no change in behavior for InTouch users that use the pre-existing OPC access name.

See [Compatibility with existing FS Gateway applications](#).

## Compatibility with existing FS Gateway applications

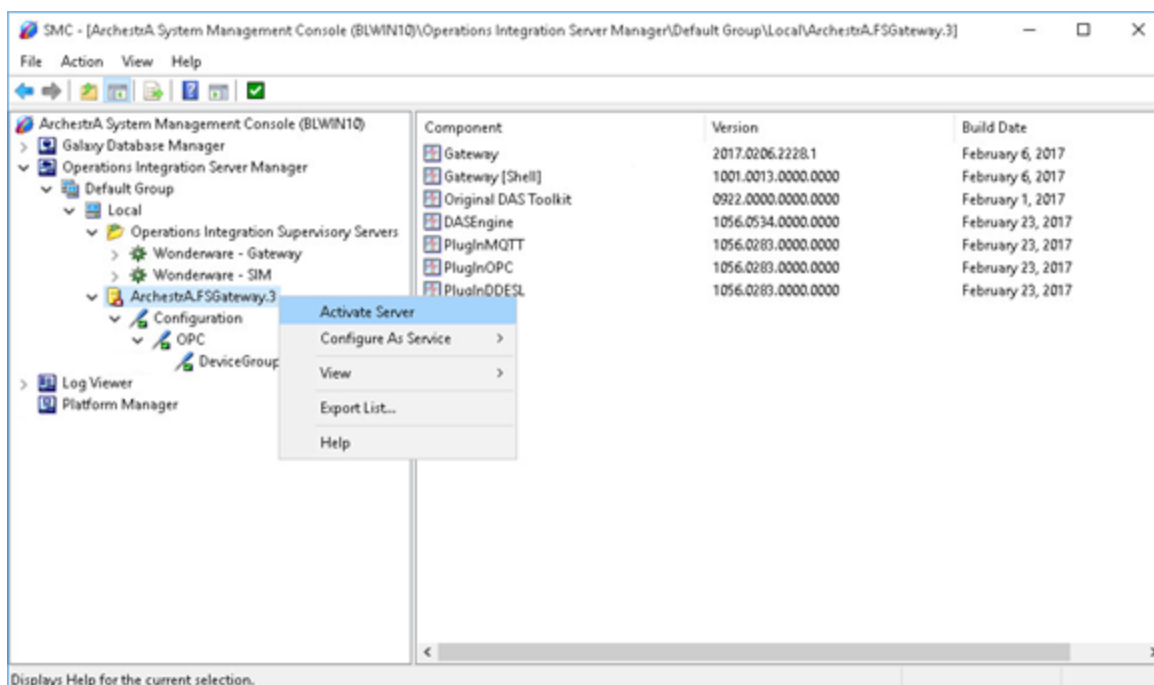
If you are upgrading from InTouch 2014 R2 SP1 where FSGateway has been installed, Gateway will continue to maintain the FSGateway application name in the Access Name definition. The application name is preserved to enhance compatibility with existing applications.

- If you had InTouch 2014 R2 SP1 installed previously, FS Gateway will appear in the Operations Control Management Console (OCMC) under **DAServer Manager**.



- After upgrading from InTouch 2014 R2 SP1, two new Gateway servers are installed. The first 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 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.



## OI Gateway installation scenarios

The following table shows the possible combinations for installing the Gateway Communication Driver and System Platform. See the *System Platform Readme* and the *InTouch Readme* for information about upgrading and migrating to System Platform 2023 R2 SP1 with InTouch HMI 2023 R2 from earlier versions of InTouch.

I have...	I want to...	
	Install Gateway 2023 R2 Stand-alone	Install System Platform 2023 R2 with InTouch and Gateway 2023 R2
<b>A clean system</b>	<ul style="list-style-type: none"> <li>Gateway is preconfigured with a predefined OPC access Name.</li> <li>Gateway is installed as stand-alone product.</li> <li>Gateway appears in Uninstall/Change Programs.</li> </ul>	<ul style="list-style-type: none"> <li>Gateway is preconfigured with a predefined OPC access Name.</li> <li>Gateway is installed as a hidden feature.</li> <li>InTouch appears in Uninstall/Change Programs.</li> </ul>

I have...	I want to...	
<b>FS Gateway 2.0.0 or previous installed (Stand-alone)</b>	<ul style="list-style-type: none"> <li>Existing FS Gateway Configuration is retained.</li> <li>FS Gateway is upgraded to Gateway 2023 R2.</li> <li>Gateway appears in Uninstall/Change Programs.</li> </ul>	<ul style="list-style-type: none"> <li>Existing FS Gateway Configuration is retained.</li> <li>InTouch is installed.</li> <li>Gateway 2023 R2 is installed as a hidden feature.</li> <li>Gateway is upgraded.</li> <li>Gateway appears in Uninstall/Change Programs.</li> <li>InTouch appears in Uninstall/Change Programs.</li> </ul>
<b>InTouch 10.0.0 or previous installed</b>	<ul style="list-style-type: none"> <li>Gateway is preconfigured with a predefined OPC access Name.</li> <li>Gateway is installed as stand-alone product.</li> <li>Gateway appears in Uninstall/Change Programs.</li> <li>InTouch appears in Uninstall/Change Programs.</li> </ul>	<ul style="list-style-type: none"> <li>Gateway is preconfigured with a predefined OPC access Name.</li> <li>Gateway is installed as a hidden feature.</li> <li>InTouch is upgraded.</li> <li>InTouch appears in Uninstall/Change Programs.</li> </ul>
<b>FS Gateway 2.0.0 (Stand-alone) or previous and InTouch 10.0.0 or previous</b>	<ul style="list-style-type: none"> <li>Existing FS Gateway Configuration is retained.</li> <li>FS Gateway is upgraded to Gateway 2023 R2.</li> <li>Gateway appears in Uninstall/Change Programs.</li> <li>InTouch appears in Uninstall/Change Programs.</li> </ul>	<ul style="list-style-type: none"> <li>Existing FS Gateway Configuration is retained.</li> <li>FS Gateway is upgraded to OI Gateway.</li> <li>InTouch is upgraded.</li> <li>Gateway appears in Uninstall/Change Programs.</li> <li>InTouch appears in Uninstall/Change Programs.</li> </ul>
<b>FS Gateway 2.0.1 Stand-alone</b>	<ul style="list-style-type: none"> <li>Existing FS Gateway Configuration is retained.</li> <li>FS Gateway is upgraded to Gateway 2023 R2.</li> <li>Gateway appears in Uninstall/Change Programs.</li> </ul>	<ul style="list-style-type: none"> <li>Existing FS Gateway Configuration is retained.</li> <li>Gateway is installed as a hidden feature.</li> <li>InTouch is installed.</li> <li>Gateway appears in Uninstall/Change Programs.</li> </ul>

I have...	I want to...	
		<ul style="list-style-type: none"> <li>• InTouch appears in Uninstall/Change Programs.</li> </ul>
<b>System Platform 2012 with InTouch 10.5 and FS Gateway 2.0.1</b>	<ul style="list-style-type: none"> <li>• FS Gateway 2.0.1 must be manually uninstalled (after doing this, it is equivalent to installing Gateway2023 R2 on a clean system).</li> </ul>	<ul style="list-style-type: none"> <li>• Existing FS Gateway Configuration is retained.</li> <li>• Gateway is installed as a hidden feature.</li> <li>• InTouch is upgraded.</li> <li>• InTouch appears in Uninstall/Change Programs.</li> </ul>
<b>FS Gateway 3.0.0 Stand-alone</b>	<ul style="list-style-type: none"> <li>• Gateway is preconfigured with a predefined OPC access Name.</li> <li>• Gateway is installed as stand-alone product.</li> <li>• Gateway appears in Uninstall/Change Programs.</li> </ul>	<ul style="list-style-type: none"> <li>• Existing FS Gateway Configuration is retained.</li> <li>• InTouch is installed.</li> <li>• Gateway is installed as a hidden feature.</li> <li>• Gateway appears in Uninstall/Change Programs.</li> <li>• InTouch appears in Uninstall/Change Programs.</li> </ul>
<b>System Platform 2012 R2 with InTouch 10.6 and FS Gateway 3.0.0</b>	<ul style="list-style-type: none"> <li>• Existing FS Gateway Configuration is retained.</li> <li>• Gateway is installed as stand-alone product.</li> <li>• Gateway appears in Uninstall/Change Programs.</li> <li>• InTouch appears in Uninstall/Change Programs.</li> </ul>	<ul style="list-style-type: none"> <li>• Existing FS Gateway Configuration is retained.</li> <li>• InTouch is installed.</li> <li>• Gateway is installed as a hidden feature.</li> <li>• Gateway appears in Uninstall/Change Programs.</li> <li>• InTouch appears in Uninstall/Change Programs.</li> </ul>



# 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: 48 GB
- 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 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](#).
- 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 (I/O data acquisition service) runs on all supported operating systems: domain member, stand-alone workstation, or server. The IDAS accepts data coming from SuiteLink and other I/O sources, and forwards that data to the Historian and other components, such as the Trend Client.

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 Operations Control 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.

## Plan 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 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 A2ALMDBDat\_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 Operations Control 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	6,061
Acknowledgement	325	6,066
Event	300	5,048

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

Tag Type	Storage Engine - Storage Item Size (Bytes)	Storage Engine - Network Transmission Item Size (Bytes)
State Summary for String (10 states and 32 byte string)	$(1+32)*10 = 330$	$(69+32)*10 = 1,010$

**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:

$$N \text{ kbps} = (N / 8) \text{ bytes per second} = (450 * N) \text{ bytes per hour}$$

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:

$$\text{Bandwidth}_{\text{Streaming}} = 1.04 * 8 * S_{\text{Each Tag Type}} (\text{Data Rate} * \text{Transmission Item Size})$$

$$\text{Bandwidth}_{\text{Recommended Streaming}} = 1.3 * \text{Bandwidth}_{\text{Streaming}}$$

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

$\text{Bandwidth}_{\text{RecommendedStreaming}} = 1.3 * 608 \text{ Kbps} = 790$  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:

$\text{Bandwidth}_{\text{Forwarding}} = 1.04 * 8 * S_{\text{Each Tag Type}} (\text{Data Rate} * \text{Storage Item Size})$

$$\text{Bandwidth}_{\text{RecommendedForwarding}} = 1.3 * \text{Bandwidth}_{\text{Forwarding}}$$

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

$$\text{Bandwidth}_{\text{Forwarding}} = 1.04 * 8 * (6384 + 4075 + 4675 + 493 + 8 + 3733 + 62) = 162 \text{ Kbps}$$

$$\text{Bandwidth}_{\text{RecommendedForwarding}} = 1.3 * 162 \text{ Kbps} = 211 \text{ Kbps}$$

## 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:

$$\text{Time}_{\text{Forwarding}} = \text{Time}_{\text{InStoreforward}} * \text{Ratio}_{\text{ForwardingDataSize}} / 0.3$$

Where  $\text{Ratio}_{\text{ForwardingDataSize}} = \text{Forwarding data Size} / \text{Streaming data size}$

For example, the data 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.

$$\text{Ratio}_{\text{ForwardingDataSize}} = 8 / 34 = 0.235$$

$$\text{Time}_{\text{Forwarding}} = 60 \text{ (minutes)} * 0.235 / 0.3 = 47 \text{ minutes}$$

## 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](#).

## 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 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 ( I/O data acquisition service) 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:

- 6,000 tags with an hourly calculation performed at the top of each hour
- 6,000 tags with 1-minute calculations performed at the top of each minute

plus

- 1,500 tags replicated (not aggregated) in tier 2
- 1,500 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

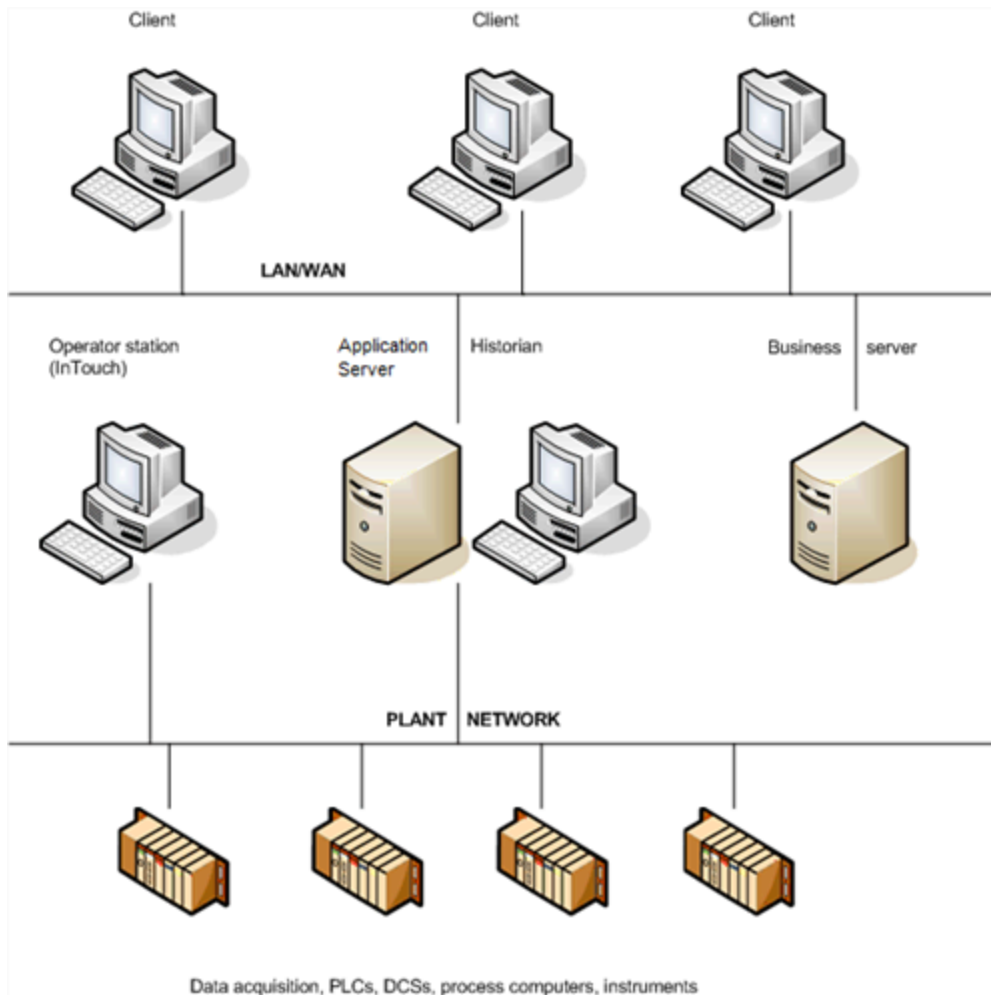
The Historian is a highly configurable package that can be set up in many different ways depending on your needs.

The Historian can use any protocol supported by Microsoft SQL Server. You can use the default Microsoft SQL Server 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



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 the 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 AVEVA™ Batch Management 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 from the 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)	1,002

### 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
- 3,072 MB Virtual Memory
- 1 Gbps NIC
- Microsoft SQL Server 2017 Standard Edition
- SQL memory clamped @ 1,024 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)	1,174
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
- 4,096 MB Virtual Memory
- 1 Gbps NIC
- Microsoft SQL Server 2017 Standard Edition
- SQL memory clamped @ 3,967 MB
- 2-hour history block duration

### Tag information

Tag count (total) = 133,941

Analog tags = 73,600

Discrete tags = 53,560

String tags = 6,920

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

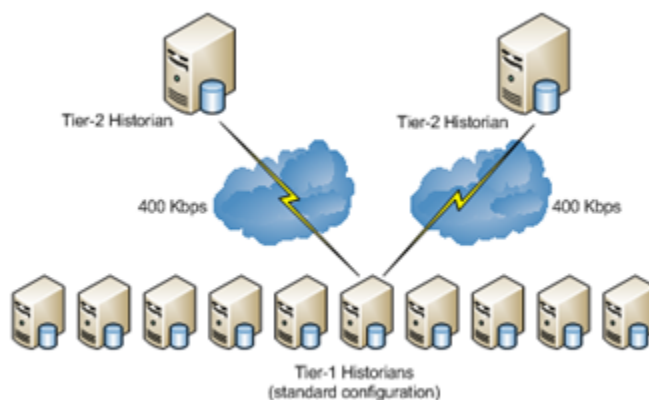
Category	Value
Average CPU load (%)	26.444
Historian memory (Private Bytes) consumption (MB)	11,124
Number of online history blocks	246
Uncompressed hard drive disk space per history block (average GB)	10.00

## 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

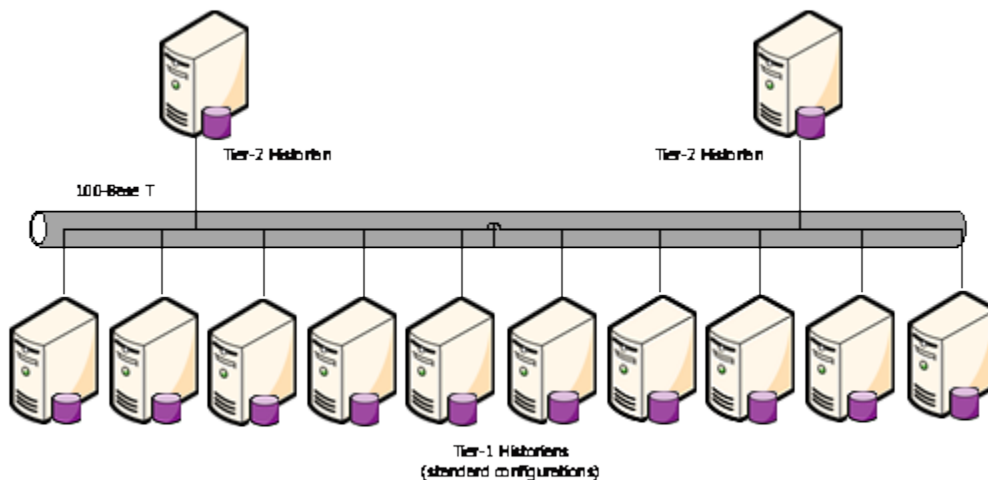
## Latency results

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 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.



- 100/1000 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)	1.55%
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

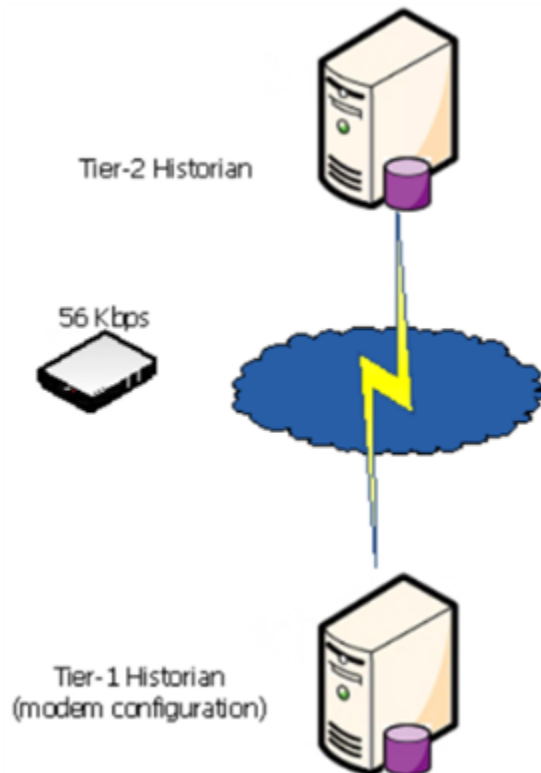
## Latency results

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.
- 100/1000 Base-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.

- 100/1000 Base-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

## Prepare 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 IDAs (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 (I/O data acquisition service), 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 Operations Control 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.
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.

Feature	Description
Historian Client Web	AVEVA Historian Client Web 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 INSQ, because this conflicts with the name of the Historian OLE DB provider and the installation eventually fails.

---

For detailed instructions on installing, see [Install System Platform](#).

After the installation completes, configure the server using the instructions in *Configure AVEVA Historian*.

Refer to the *System Platform Readme* before using the historian.

## Test 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 Operations Control 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
- Operations Control Management Console

---

**Note:** If you performed a complete historian installation, the Operations Control 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.

---

## Repair 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 [Repair an installation](#).

To repair a database, use the System Platform Configurator. For more information, see [Configure AVEVA Historian](#).

## Modify the Historian installation

You can modify the Historian features that are already installed.

For detailed modification instructions, see [Modify 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 [Configure AVEVA Historian](#).

## Uninstall 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 (idatcfg\_\*.dat) created by IDAS and the Configuration Service.

For detailed uninstall instructions, see [Uninstall AVEVA System Platform](#).

## Upgrade from a previous version

You can upgrade directly to the current version of the Historian (2023 R2) from Historian 2017 and later versions.

You should upgrade the Historian Server before upgrading Historian remote IDAS nodes. Remote IDAS nodes that are not upgraded to 2023 R2 will remain fully functional. However, it is strongly recommended that you upgrade them to 2023 R2 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. For more information, see Server configuration details, as described in Configure AVEVA Historian.

## Upgrade 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 Operations Control 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 [Upgrade, modify, and repair 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.

## Upgrade the Historian version

Refer to [Upgrade from a previous version](#) to see which versions can be directly upgraded to Historian 2023 R2.

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 2023 R2, 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 Operations Control 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 [Upgrade, modify, and repair 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, the 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.

# 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 contains a set of tools that eliminate the need to be familiar with the SQL Server, 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 classic add-ins for Microsoft Excel and Microsoft Word. These classic 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.

---

**Note:** Historian data can also be displayed in Excel with the newer task pane add-in. The newer task pane add-in supports 64-bit and 32-bit versions of Excel. No installation is required for this task pane add-in; each user sets it up per the instructions in the *Historian Client Web User Guide*.

---

## 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 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.

---

**Note:** Historian data can also be displayed in Excel via the task pane add-in. The task pane add-in supports 64-bit and 32-bit versions of Excel. No installation is required for the task pane add-in; each user sets it up per the instructions in the *Historian Client Web User Guide*.

---

- 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, manually stop the Excel and aaHistClientReportingService.exe services, and then 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 [Install System Platform](#).

After the Historian Client software is installed on the computer, you must install the Language Packs manually.

## Use 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\ArchestraA\ActiveFactory registry folder and change its value to 1.

## Repair the Historian Client installation

You can use the System Platform installation program to repair corrupt files of the installed features. For more information, see [Repair 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.

---

## Uninstall 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 [Uninstall 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.

---

## Upgrade from a previous version

You can upgrade directly to the current version of the Historian (2023 R2) from Historian 2017 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 2023 R2 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)

Install Historian 2023 R2 and run Configurator.

From the Operations Control Management Console, shutdown and disable Historian.

Locate SQL scripts that you'll need for intermediate migration in this folder:

**C:\ProgramData\Archestra\Historian\Install\Scripts**

From SQL Server Management Studio:

Drop the Runtime database.

Restore a backup of the Runtime from your previous version of Historian.

Disable any triggers or constraints that would prevent schema changes. This prepares your database for changes.

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).

Restore any changes (triggers and other constraints) that you made to settings in step 5.

Shut down the old server's remote IDAS.

From the new server, force an update to the remote IDAS configuration.

# Use 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.

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.

---

**Important:** SQL Server and the .NET Framework are not installed automatically by the command line installer and must be installed before starting silent installation. Other prerequisites are installed automatically.

---

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 2023 R2 SP1 incorporates a functional change to the installation workflow. Redistributable libraries from Microsoft and other vendors that are out-of-support, but may be referenced by legacy Application Server templates or custom components, are not installed and are not present on the installation media. **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 2023 R2 SP1. **You must acknowledge this requirement to successfully install System Platform.** See [Response file entry to acknowledge installation change information \(redistributable libraries\)](#) 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.

---

## Start 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 /silent responsefile.txt /domainname=adminuserdomainname /uname=adminusername
/upwd=adminuserpassword
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 /silent responsefile.txt /domainname=adminuserdomainname /uname=adminusername
/upwd=adminuserpassword /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 path of the response file (filename plus location of file) must be included. For example:

```
D:\setup.exe /silent C:\docs\SPInstall\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.

## Use 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. You must acknowledge the changes to System Platform 2023 R2 SP1, as compared to earlier 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.
5. 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 installation change information \(redistributable libraries\)](#) for more information.

If it is needed, apply the patch(es) to Manufacturing Execution System and/or Recipe Management, not to System Platform.

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:** SQL Server and the .NET Framework are not installed automatically by the command line installer and must be installed before starting silent installation. Other prerequisites are installed automatically.

---

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.

---

# Create 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 include:

- Root installation directory. The default path is C:\Program Files (x86).
  - **FeatureForm.SInstallDir**=C:\Program Files (x86)
- The Network Account (name and password), used for inter-node and inter-product communications.
  - **AdminUserForm.SUserName**=NetworkAccount
  - **AdminUserForm.SPassword**=Password123
- For upgrade only, whether or not to remove Administrator privileges from the Network Account.
  - **RemoveArchestraUser.RemoveA2AFromAdmin**=true
- 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:

- **Common Platform.** Entries to configure the Common Platform components:
  - System Management Server (SMS), which includes:
    - Certificate management
    - Common Platform ports
    - Security settings for SuiteLink and Network Message Exchange (NMX)
  - Authentication Provider (Azure AD)
  - License Mode, which gives you three options:
    - Perpetual
    - Flex mode
    - AVEVA Operations Control. If you select this, you also have the option of enabling connected experience.

See [Response file entries to configure the common platform](#) for more information.
- **Industrial Graphics Server.** See [Response file entries to configure the industrial graphic server](#) for more information.
- **AVEVA Historian.** See [Response file entries to configure Historian](#) for more information.
- **AVEVA Enterprise Licensing Manager.** See [Response file entries to configure the License Server](#) for more information.
- **AVEVA System Monitor Manager.** See [Response file entries to configure System Monitor](#) for details.

## 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. 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. As of the release of System Platform 2023 R2, AVEVA no longer provides these libraries and we strongly recommend that you do not use any libraries that are outside their published support life cycle. Libraries outside their support life cycle 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
- Remote Response Objects (RRO)

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. An update to the Remote Response Object is currently underway. If you use the RRO, we recommend that you delay upgrading your system until the new RRO is available.

**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 acknowledge compatibility requirement

A patch must be applied to the following products and versions to ensure compatibility with System Platform 2023 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 2023 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.

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 common platform

The Common Platform settings are used to:

- Establish machine trust between nodes via the System Management Server. See [System Management Server](#) for additional information.
- Configure a Federated Identity Provider. See [Federated Identity Provider](#) for more information.
- Set the License Mode and license type. See [License Mode](#) for more information.

```
<configurator>
Common Platform.ASBRuntime.HttpPort=80
Common Platform.ASBRuntime.HttpsPort=443
    // Sets the HTTPS port of Aveva web apps running on the local node.
    // Corresponds to the HTTPS Port setting on the Advanced Configuration Ports tab.
Common Platform.ASBRuntime.ManagementServerPort=443
    // Sets the HTTPS port number for a "remote" SMS, and is used only when the SMS is on
    // a different node.
    // Corresponds to the SMS Port setting on the Advanced Configuration Certificates
    // tab.
Common Platform.ASBRuntime.ManagementServerName=<machine name>
    // Enter the System Management Server name if the SMS is on a remote node
Common Platform.ASBRuntime.AsbManagedCertificates=true
Common Platform.ASBRuntime.BindingCertificateThumbprint=<thumbprint>
    // 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
    // Ensure ManagementServerName is the remote node machine name, not the local node
    // machine name.
Common Platform.ASBRuntime.SuitelinkMixedModeEnabled=<true or false>
    // False indicates that Suitelink accepts only encrypted connection requests.
    // True indicates that Suitelink accepts both encrypted and unencrypted connection
    // requests.
    // Setting to true is recommended only during upgrade scenarios or for supporting
    // legacy applications.
Common Platform.ASBRuntime.NmxAllowAllUsers=<true or false>
    // Valid entries are 0 or 1. 0 (false) restricts user access.
    // Set to 0 for new installations. For upgrades should be set to 1, then reset to 0
    // when all nodes have been upgraded.
Common Platform.ASBRuntime.DisplayLoginMode=0
    // Used for AVEVA Identity Manager login dialog
    // 0 - browser not specified (defaults to default system browser)
    // 1 - use WebView2 embedded browser
    // 2 - use system browser)
```

```

Common Platform.Bootstrap.IsAzureADMode=true
// Enables Azure AD as the Authentication Provider
Common Platform.Bootstrap.Endpoint=<AzureEndpoint>
// Sets the Endpoint when Azure AD is enabled as the Authentication Provider
Common Platform.Bootstrap.ClientId=<AzureClientId>
// Sets the Client ID when Azure AD is enabled as the Authentication Provider
Common Platform.Bootstrap.ClientSecret=<AzureClientSecret>
// Sets the Client Secret when Azure AD is the Authentication Provider.
Common Platform.Bootstrap.IsAVEVAConnectMode=true
// Enables AVEVA Connect as the Authentication Provider
Common Platform.Bootstrap.Endpoint="AVEVAConnectEndPoint"
// Sets the Endpoint when AVEVA Connect is enabled as the Authentication Provider
Common Platform.Bootstrap.ClientId=<AVEVAConnectClientId>
// Sets the Client ID when AVEVA Connect is enabled as the Authentication Provider
Common Platform.Bootstrap.ServiceEndpoint=<AVEVAConnectServiceEndpoint>
// Sets the Service Endpoint when AVEVA Connect is enabled as the Authentication
Provider
Common Platform.Bootstrap.AccessToken=<AVEVAConnectAccessToken>
// Sets the Access Token when AVEVA Connect is enabled as the Authentication Provider
Common Platform.AimFidps.ProviderName=None
// None - no external identity provider will be configured
// AzureAd - Azure AD will be configured as the federated identity provider
// AvevaConnect - AVEVA Connect will be configured as the federated identity provider
Common Platform.AimFidps.ClientId= <client Id for AzureAD or AVEVAConnect>
// This parameter is a string and is mandatory. For AVEVA Connect, the Clientid is a
GUID string
Common Platform.AimFidps.ClientSecret= <AzureAD client secret>
// Specifies the client secret for Azure AD only
Common Platform.AimFidps.Endpoint= <AzureAD or AVEVAConnect endpoint URL>
// Specifies the endpoint (URL) for Azure AD or AVEVA Connect. This parameter is
mandatory
Common Platform.AimFidps.AccessToken= <AVEVAConnect Access Token>
// Specifies the AccessToken for AVEVA Connect only
Common Platform.AimFidps.ServicesEndpoint= <AVEVAConnect endpoint>
// Specifies the Service Endpoint for AVEVA Connect only
Common Platform.LicenseModePlugin.Option=<flexmode / non-flexmode / operationscontrol /
opscontrol-connectedexperience>
// Used to set the license mode
// flexmode = Flex
// non-flexmode = Perpetual
// operationscontrol = AVEVA Operations Control
// opscontrol-connectedexperience = enables connected experience (AVEVA Operations is
enabled)
</configurator>

```

## Response file entries to configure the industrial graphic server

The following entries are used to configure the Industrial Graphic Server:

```

<configurator>
Industrial Graphics Server.Authentication Settings.SilentRegisterAIM=<true or false>
// true selects "User Authentication"
// false selects "Windows Authentication"
Industrial Graphics Server.Authentication Settings.SilentITGatewayUrl=<SecureGatewayURL>
Industrial Graphics Server.Authentication Settings.SilentITGatewayUserName=<Domain\

```



```
username>  
Industrial Graphics Server.Authentication Settings.SilentITGatewayPassword=<password>  
</configurator>
```

## Response file entries to configure Historian

The following entries are used to configure the AVEVA Historian:

```
<configurator>  
AVEVA Historian.Historian.SilentTCPPort=32565  
AVEVA Historian.Historian.SilentchkBoxAutoStartHistorian=true  
AVEVA Historian.Historian.SilentDBOption=REBUILD  
AVEVA Historian.Historian.SilentDBPath=C:\Program Files\Microsoft SQL Server\  
MSSQL15.MSSQLSERVER\MSSQL\DATA  
AVEVA Historian.Historian.SilentDataPath=C:\Historian  
AVEVA Historian.Historian.SilentSQLUserName=  
AVEVA Historian.Historian.SilentSQLPassword=  
AVEVA Historian.Historian.SilentBlockStorageMode=1  
AVEVA Historian.Historian.SilentGatewayHTTPPort=32569  
AVEVA Historian.Historian.SilentGatewayHTTPSPort=32573  
AVEVA Historian.Historian.SilentSecuredCommunication=false  
AVEVA Historian.Historian.SilentSelfCertificate=true  
    // If true and SilentCertificateThumbprint is not provided, the certificate is  
    installed automatically)  
AVEVA Historian.Historian.SilentIDDataProviderScope = <historian node>  
    // Unique identifier (prefix) used by IData compliant clients to access historian  
    tags on this particular historian server  
AVEVA Historian.Extensions.SilentExtensionInstall=true  
AVEVA Historian.Search.SilentSearchInstall=true  
AVEVA Historian.Security.SilentSQLUserName=<SqlAdminUser>  
AVEVA Historian.Security.SilentSQLPassword=<Password>  
</configurator>
```

## Response file entries to configure the License Server

The following entries are used to configure the AVEVA Enterprise License Server:

```
<configurator>  
AVEVA Enterprise Licensing.LicAPI2.NewServerName=<license server name>  
AVEVA Enterprise Licensing.LicAPI2.NewPortNumber=55559  
AVEVA Enterprise Licensing.LicAPI2.LegacyPortNumber=55555  
AVEVA Enterprise Licensing.LicAPI2.NewAgentPortNumber=59200  
AVEVA Enterprise Licensing.LicAPI2.EnableBackup=False  
</configurator>
```

**Note:** License mode is set through a Common Platform entry. See [Response file entries to configure the common platform](#) for details.

## Response file entries to configure System Monitor

The following entries are used to configure the AVEVA System Monitor Manager:

```
<configurator>  
AVEVA System Monitor.System Monitor Manager.AgentServerName=ServerName
```



```

AVEVA System Monitor.System Monitor Manager.HttpPort=<httpPort>
// Optional; required only if you are changing the httpPort value.
// If you are using the default, you can remove this parameter and the plugin will
use the default httpPort value.
AVEVA System Monitor.System Monitor Manager.SslPort=<sslPort>
// Optional; required only if you are changing the sslport value.
// If you are using the default, you can remove this parameter and the plugin will
use the default sslPort value.
AVEVA System Monitor.Alert Email Server.SmtpOneClickConfigure=false
// Set to true if you will configure the SMTP email server details later from System
Monitor web interface.
// If you will use the System Monitor web interface to enter the Email Server
details, remove
SmtpServerNameorIp,SmtpServerPort,SmtpServerSecured,SmtpUserName,SmtpPassword,SmtpFrom
mRecipientEmailID and SmtpRecipientEmailID.
AVEVA System Monitor.Alert Email Server.SmtpServerNameorIp=<MachineNameOrIp>
// Remove if SmtpOneClickConfigure=true.
AVEVA System Monitor.Alert Email Server.SmtpServerPort=<portNo>
// Remove if SmtpOneClickConfigure=true.
AVEVA System Monitor.Alert Email Server.SmtpServerSecured =false
// Set to true if the SMTP server needs user credentials to access the SMTP server.
// Remove if SmtpOneClickConfigure=true.
AVEVA System Monitor.Alert Email Server.SmtpUserName=<username>
// Remove if SmtpOneClickConfigure=true.
AVEVA System Monitor.Alert Email Server.SmtpPassword=<password>
// If UserName and Password parameters are not required to access the SMTP server you
can remove the parameters.
// Remove if SmtpOneClickConfigure=true.
AVEVA System Monitor.Alert Email Server.SmtpFromRecipientEmailID=<from_EmailID>
// Remove if SmtpOneClickConfigure=true.
AVEVA System Monitor.Alert Email Server.SmtpRecipientEmailID=<receipientEmailID>
// Provide one or multiple Email Id's separated by semicolon(;).
// Remove if SmtpOneClickConfigure=true.
AVEVA System Monitor.Alert Email Server.HttpPort=<httpPort>
// Optional; required only if you are changing the httpPort value.
// If you are using the default, you can remove this parameter and the plugin will
use the default httpPort value.
AVEVA System Monitor.Alert Email Server.SslPort=<sslPort>
// Optional; required only if you are changing the sslport value.
// If you are using the default, you can remove this parameter and the plugin will
use the default sslPort value.
</configurator>

```

## 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 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-

Response File	Description
	time components.
AVEVA InTouch Access Anywhere Secure Gateway Node	Installs and configures the AVEVA InTouch Access Anywhere Secure Gateway. No other components are installed.
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.  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

Response File	Description
	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.
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.

# 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.

## Upgrade 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	1.57 GB	Required	Optional	Required	Required
CD-ASBFramework	59 MB	Required	Required	Required	Required
CD-AVEVAHelp	40 MB	Required	Required	Required	Required
CD-Gateway	74 MB	Optional	Optional	Optional	Optional
CD-Historian	596 MB	Required	Optional	Optional	Optional
CD-HistorianClient	65 MB	Optional	Required	Required	Required
CD-InTouch	474 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	413 MB	Optional	Optional	Optional	Required
CD-	457 MB	Optional	Optional	Optional	Required for

InstallFiles Folder (Component)	Approx Folder Size	Historian	Historian Client	Application Server	InTouch (Run time only or run time and development)
IntouchFrench					French
CD-IntouchGerman	456 MB	Optional	Optional	Optional	Required for German
CD-IntouchJapanese	457 MB	Optional	Optional	Optional	Required for Japanese
CD-IntouchSChinese	461 MB	Optional	Optional	Optional	Required for Chinese
CD-IntouchWebClient	94 MB	Optional	Optional	Optional	Required
CD-IntouchWebClient is required when InTouch is installed (all languages).					
CD-Language Assistant	105 MB	Optional	Optional	Optional	Optional
CD-LicAPI	68 MB	Required	Required	Required	Required
CD-Licensing	395 MB	Required	Required	Required	Required
CD-NGVisualization	567 MB	Optional	Optional	Required	Required
CD-OCLogger	51 MB	Required	Required	Required	Required
CD-OCMC	1 MB	Required	Required	Required	Required
CD-OIEngine	495 MB	Required	Required	Required	Required
CD-OIGATEWAY	20 MB	Required	Required	Required	Required
CD-SentinelAim	7 MB	Required	Required	Required	Required
CD-SentinelManager	25 MB	Optional	Optional	Optional	Optional
CD-Server	64 MB	Required	Optional	Optional	Optional
CD-VCPServices	105 MB	Required	Required	Required	Required
CoexistenceUpdates	236 MB	Optional	Optional	Optional	Optional

InstallFiles Folder (Component)	Approx Folder Size	Historian	Historian Client	Application Server	InTouch (Run time only or run time and development)
More details shown below					
External	2 MB	Required	Required	Required	Required
Redist	0.98 GB	See note (DOTNET)	See note (DOTNET)	See note (DOTNET)	See note (DOTNET)
DOTNET	475 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
SQLEXPRESS2022CORE	266 MB	Optional	Optional	Optional	Optional
See <b>Note</b> , below, about removing subfolder SQL2022EXPRESSCORE from Redist.					
VC2012U4	13 MB	Required	Required	Required	Required
VC2013U4	26 MB	Required	Required	Required	Required
VC2019	37 MB	Required	Required	Required	Required
VC2022	37 MB	Required	Required	Required	Required
WebView2	150 MB	Required	Required	Required	Required
ResponseFiles	0 MB	Optional	Optional	Optional	Optional
Support	0 MB	Required	Required	Required	Required
UpgradeSupport	38 MB	Required	Required	Required	Required

**Note:** The Redist folder contains SQL Server Express in folder SQLEXPRESS2022CORE. 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 2023 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 2023 R2 SP1 and do not require patching.



## 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.

---

## Create the installation source and install 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.

# Common 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
<b>Application Server/System Platform Services</b>		
AVEVA Bootstrap (aaBootstrap)	aaBootstrap.exe	Utility to bootstrap an Application Server 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.
GalaxyRepository (aaGR)	aaGR.exe	The Galaxy Repository service to process requests to the Application Server configuration subsystem.
AVEVA Global Data Cache Monitor Server (aaGlobaldata CacheMonitorSvr)	aaGlobaldata CacheMonitorSvr.exe	Global Data Cache Monitor service to process file change notifications.
Operations Control Logger Service (aaLogger)	aaLogger.exe	Receives log messages from System Platform component products and stores them in a file.
AVEVA UserValidator (aaUserValidator)	aaUserValidator.exe	User validator service to process user validations for the System Platform framework.
Platform Info Server Module (aaPlatformInfoSvr)	aaPlatformInfoSvr.exe	Server module for the Network Account.
<b>PCS Services</b>		
AVEVA Server Manager (AsbServiceManager)	Asb.ServiceManager.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

Service/Process Name	Executable Name	Description
		hosted services. Therefore, the Watchdog delegates the tasks of starting and stopping monitored services to this lower-privileged process.
AVEVA Watchdog (Watchdog_Service)	Asb.Watchdog.exe	Ensure services that provide discoverable endpoints are running. The Watchdog is 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.
<b>Licensing Services</b>		
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 System Platform processes

The following table describes AVEVA Application Server other required System Platform processes. For a description of services associated with the AVEVA Historian, see the *AVEVA Historian Administration Guide*.

Service/Process Name	Executable Name	Description
<b>Application Server/System Platform Services</b>		
AVEVA Bootstrap (aaBootstrap)	aaBootstrap.exe	Utility to bootstrap an Application Server run time to support code-module deployment and process monitoring.

Service/Process Name	Executable Name	Description
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.
GalaxyRepository (aaGR)	aaGR.exe	The Galaxy Repository service to process requests to the Application Server configuration subsystem.
AVEVA Global Data Cache Monitor Server (aaGlobaldata CacheMonitorSvr)	aaGlobaldata CacheMonitorSvr.exe	Global Data Cache Monitor service to process file change notifications.
Operations Control Logger Service (aaLogger)	aaLogger.exe	Receives log messages from System Platform component products and stores them in a file.
AVEVA UserValidator (aaUserValidator)	aaUserValidator.exe	User validator service to process user validations for the System Platform framework.
Platform Info Server Module (aaPlatformInfoSvr)	aaPlatformInfoSvr.exe	Server module for the Network Account.
<b>PCS/ASB Services</b>		
AVEVA Server Manager (AsbServiceManager)	Asb.ServiceManager.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.
AVEVA Watchdog (Watchdog_Service)	Asb.Watchdog.exe	Ensure services that provide discoverable endpoints are running. The Watchdog is 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

Service/Process Name	Executable Name	Description
		and Service Content Provider.
<b>Licensing Services</b>		
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.

# Ports used by System Platform products

The following tables list the ports used by System Platform products.

**Note:** Firewall settings for all destination ports must allow INBOUND connections.

## Application Server

Port	Can be configured	Protocol	Subsystem	Purpose
135	No	TCP	Bootstrap	DCOM and RPC
139 445	No	TCP	Bootstrap	DCOM and NetBios
443	No	TCP (HTTPS)	AVEVA.AppServer. BootstrapProxy.exe	AVEVA.AppServer. BootstrapProxy.exe
808	Yes	TCP	Multi-Galaxy	Galaxy Pairing ASBAAuthentication Service ASBGRBrowsing Service IOM BLS Service ASMBMxDataProvider Service
5026	Yes	TCP	NMXSVC	NMXSVC
8090	Yes	TCP	aaGR	aaGR
30000 30001	Yes	TCP/UDP TCP	Bootstrap, Redundancy PMC	Local redundancy messaging (WinPlatform)
32568	Yes	TCP	aaEngine.exe	aaEngine.exe
48031	Yes	TCP	Platform Common Services	OPC UA Server
49152 – 65535	No	TCP	aaGlobalDataCache MonitorSvr	DCOM

Port	Can be configured	Protocol	Subsystem	Purpose
			aaGR aaIDE aaObjectViewer aaPIM aaPlatformInfoSvr aaUserValidator Bootstrap	

## AVEVA Historian

Port	Can be configured	Protocol	Subsystem	Purpose
32565	Yes	TCP	aaClientAccessPointNG.exe	Historian Client Access Point NG
32568	Yes	TCP	AVEVA Historian	AVEVA Historian as a real-time service
32569	Yes	TCP (HTTPS)	Insight	Insight on-premise gateway
32573	Yes	TCP (HTTPS)	Historian Secured Gateway	REST communications

## Device Integration (Communication Drivers Pack)

Port	Can be configured	Protocol	Subsystem	Purpose
102	No	TCP	SiDirect OI Server	Siemens PLC communication to OI Server
135	No	TCP	DASEngine, OPC	DCOM and RPC
443	Yes	TCP (HTTPS)	GDIWebServer	MQTT and Auto-Build configuration
502	No	TCP	MBTCP OI Server	Modbus communication to OI Server

Port	Can be configured	Protocol	Subsystem	Purpose
1883 8883	Yes	TCP	MQTT	MQTT broker communication to OI Server
2221 2222 2223	No	TCP	ABTCP OI Server	Allen-Bradley PLC communication to OI Server
5413	No	TCP	SuiteLink	SuiteLink communication
18245	No	TCP	GESRTP OI Server	GE PLC communication to OI Server
44818	No	TCP	ABCIP OI Server	Allen-Bradley CIP PLC communication to OI Server
See note, below	Yes	TCP	OPC UA Services	Remote access to the OPC UA servers

**Note:** The Communication Drivers Pack uses the default OPC ports, which are are configurable. For details, refer to the OPC Foundation documentation:

[https://opcfoundation.github.io/UA-.NETStandard/help/firewall\\_settings.htm](https://opcfoundation.github.io/UA-.NETStandard/help/firewall_settings.htm)

## InTouch

Port	Can be configured	Protocol	Subsystem	Purpose
51218	No	TCP	Alarmmgr.exe	Alarm Manager
48032 – 65000	Yes	TCP	InTouch.OPCUA.Se	InTouch OPC UA



Port	Can be configured	Protocol	Subsystem	Purpose
			rviceHost.exe	

## InTouch Access Anywhere (ITAA)

Port	Can be configured	Protocol	Subsystem	Purpose
443	Yes	TCP	EricomSecureGate way.exe	Secure Gateway
7433	Yes	TCP	EricomAuthenticat ionServer.exe	Access Anywhere Authentication Server
8080	Yes	TCP	EricomSecureGate way.exe AccessServer64.exe	Communication between ITAA Server and ITAA Secure Gateway
57111	No	UDP	EricomSecureGate way.exe	Secure Gateway
57733 57734 57735	No No No	TCP	AccessServer64.exe	Server

## Licensing

Port	Can be configured	Protocol	Subsystem	Purpose
80	Yes	TCP (HTTP)	License Manager	Web Service
443	Yes	TCP	License Manager	License Manager outbound to activation server
50051	Yes	TCP (HTTPS)	Licensing Platform	Serve licensing requests from products
55555	Yes	TCP (HTTP)	License Server	License Server Translator service. Also required to

Port	Can be configured	Protocol	Subsystem	Purpose
				support prior client versions from Server 4.0
55559	Yes	TCP (HTTP/ HTTPS)	License Server	License Server core service
59200	Yes	TCP	License Server	License Server Agent Service
59201	Yes	TCP (HTTPS)	License Server	License Server Agent Service

## OMI Web Client

Port	Can be configured	Protocol	Subsystem	Purpose
80 808	No	TCP (HTTP)	VCP	vcp.services.onpre m.DataAccess.exe vcp.services.onpre m.WebServer.exe
443 80	No	TCP (HTTPS)	VCP	vcp.services.onpre m.frontdoor.exe

## Operations Control Logger

Port	Can be configured	Protocol	Subsystem	Purpose
135	No	TCP	RPC	Used for dynamic port mapping

## Platform Common Services (PCS)

Port	Can be configured	Protocol	Subsystem	Purpose
80	No	TCP (HTTP)	PCS	PCS.ServiceManag er.exe
443	Yes	TCP (HTTPS)	PCS	PCS.Agent.exe(Dis covery)

Port	Can be configured	Protocol	Subsystem	Purpose
				PCS.IdentityManager.Host.exe
808	Yes	TCP	PCS	WCF shared port
1900	No	UDP (SSDP)	PCS	PCS.IdentityManager.Host.exe SSDP
7084 7085	No No	TCP	PCS	System authentication during node registration

## SQL Server

Port	Can be configured	Protocol	Subsystem	Purpose
1433	Yes	TCP	SQL Server	SQL Server
1434	No	UDP	SQL Server	SQL Server browser

## System Monitor

Port	Can be configured	Protocol	Subsystem	Purpose
25	Yes	TCP (SMTP)	System Monitor	SMTP Server
80	Yes	TCP (HTTPS)	System Monitor	Sentinel Console Service
443	Yes	TCP (HTTPS)	System Monitor	Secure Sentinel Console Service
587	Yes	TCP (SMTP)	System Monitor	Secure SMTP Server

# 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 2023 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.
aaRuntimeUsers	Group	In systems where NMX communications have been restricted through a Configurator setting, membership in the aaRuntimeUsers group allows the user or account to access the Network Message Exchange (NMX) for communication between nodes. For details about this Configurator setting, see <a href="#">Communications tab</a> .
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.

Name	Category	Description
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 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 2023 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 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 this 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 this group if you are not using the InTouch Web Client or accessing InTouch tags from an AVEVA OMI ViewApp.
	InTouchWeb	

Group	Account	Description
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 2023 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 System Platform 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.
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 configuration service manages configuration of the historian and general runtime operation.
NT SERVICE\ InSQLEvent System	Windows Service Account	The event system service is the account for the Classic Event System service. It detects user-defined events and performs specified actions.
NT SERVICE\ InSQLManual Storage	Windows Service Account	The Historian Manual Storage service processes late, forwarded, CSV, and manually updated/ inserted data.
NT SERVICE\ InSQLStorage	Windows Service Account	The Historian Storage service is the Classic Storage Service that transforms data from the legacy IDAS service.
NT SERVICE\ InSQLIndexing	Windows Service Account	The Historian Indexing service is for indexing the History Blocks.
NT SERVICE\ InSQLIOServer	Windows Service Account	The Historian IO Server is the Classic IO Service that provides access to data through Suitelink.
NT SERVICE\ InSQLSystemDriver	Windows Service Account	The Historian System Driver Service captures data for System Tags and generates diagnostic information.
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 2023 R2 SP1, Platform Common Services 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 framework. Since these processes are started by the AVEVA 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

Name	Category	Description
		<p>private key of the security certificate used to bind to the HTTPS port.</p> <p>To enable a secure SuiteLink connection, add the standard user to this group on the server side. For details, see "Secured SuiteLink Connection" in the <i>AVEVA Communication Drivers Pack User Guide</i>, available at [Installation Media]\InstallFiles\CD-OIEngine\Docs\OICore.pdf</p>
ASBSolution	Group	Membership in this user group provides the File System and Registry permissions required by the PCS Framework.
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\ OrchestraData Store	Windows Service Account	OrchestraDataStore runs as a virtual service account. It starts and

Name	Category	Description
		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. To enable a secure SuiteLink connection, add the standard user to this group on the server side. For details, see "Secured SuiteLink Connection" in the <i>AVEVA Communication Drivers Pack User Guide</i> , available at [Installation Media]\InstallFiles\CD-OIEngine\Docs\OICore.pdf.
	AsbService Manager	
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	
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 2023 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 2023 R2 SP1, AVEVA System Monitor creates and uses the following service accounts.

Name	Category	Description
NT SERVICE\ psmconsolSrv	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		



**AVEVA Group plc**

High Cross  
Maddingley Road  
Cambridge  
CB3 0HB  
UK

Tel +44 (0)1223 556655

**[www.aveva.com](http://www.aveva.com)**

To find your local AVEVA office, visit **[www.aveva.com/offices](http://www.aveva.com/offices)**

AVEVA believes the information in this publication is correct as of its publication date. As part of continued product development, such information is subject to change without prior notice and is related to the current software release. AVEVA is not responsible for any inadvertent errors. All product names mentioned are the trademarks of their respective holders.