AVEVA™ System Platform 2023 R2 Patch 01 Readme

Last revision: 6/21/2024

In This Document

Included in this patch -- 2023 R2 Patch 01

This document contains important information about AVEVA™ System Platform 2023 R2 Patch 01, which includes the products listed below. The Readme file for System Platform 2023 R2 is included below, following the Patch 01 documentation corrections.

Program Name	Version
AVEVA Application Server and AVEVA OMI 2023 R2 P01	23.1.001
AVEVA Communication Drivers Pack	23.02.001
AVEVA Historian 2023 R2 P01	23.1.001
AVEVA Historian Client 2023 R2 P01	23.1.001
AVEVA InTouch HMI 2023 R2 P01 (all languages)	23.1.001
AVEVA Platform Common Services 8.0.2	8.0.2
Operations Control Logger	23.1.001

Review the individual product Readme files for details regarding product-specific known and resolved issues. When you extract the patch installation files, the product Readme files are extracted to individual folders. The Readme files are also posted on the AVEVA Global Customer Support (GCS) website. Readme files from previous releases of System Platform and its component products are also posted on the AVEVA Global Customer Support (GCS) website, along with additional technical information about System Platform. For the latest updates related to supported operating systems and databases, see the GCS Technology Matrix.

About this patch release -- 2023 R2 Patch 01

This patch release includes the following changes:

- Incorporation of hot fixes for all products
- Miscellaneous bug fixes
- Improvements to the OMI web client. See the *Application Server and AVEVA OMI 2023 R2 Patch 01 Readme* for more information.

Supported System Platform Versions for Product Upgrade

This patch can only be applied to System Platform 2023 R2.

Important! System Platform does not support mixed Windows workgroup/domain environments. As stated in the *System Platform 2023 R2 Installation Guide*, although workgroups are supported, domain-based networking is recommended. However, you cannot use workgroup nodes within a domain environment.

Readme Files for Other Products in this Release

The extracted patch files include a ReadMe directory with the Readme files for each individual component product. To access the product Readme files, navigate to the applicable folder under the ReadMe directory. Review the known and resolved issues contained in each file as applicable.

Resolved issues -- 2023 R2 Patch 01

See the product-specific ReadMe files (in the ReadMe directory, as described above) for issues resolved in this patch release. The table below shows issues

resolved in components that are shared between two or more products and issues that were resolved too late to be included in the Readme file for their product.

Original Issue	Case/SR Number	Description
IMS 3199110	960396336	In the Industrial Graphic Editor, trying to create a script by selecting **Scripts (Collection)** from the **Properties** tab did not work. You could not type anything in the body of the script and warning messages were written to the logger.
IMS 3022955	960377542	After migrating a galaxy from System Platform 2023 Patch 03 to 2023R2, some graphics that were attached to object templates could not be opened in the Industrial Graphic Editor. Trying to open the graphic caused the message *Graphic Not Available*.
IMS 3034154	960374098	In InTouch, signing in using a smart card for authentication took approximately one minute. While the issue occurred in InTouch, the fix for it is in Application Server.

InTouch HMI Resolved Issues and Known Issues

InTouch HMI Resolved Issues

In addition to the fixes listed in the InTouch HMI 2023 R2 P01 Readme file, InTouch includes fixes for the issues listed in the following table. These issues were fixed too late to be included in the InTouch Readme.

Original Issue	Case/SR Number	Description
IMS-3054559	960384212	InTouch HMI was logging null values to Historian for the tags that had initialization value set to 0.
IMS-3058936	960380845	In InTouch HMI runtime, when multimonitor screen was used, the maximize option did not cover the complete resolution of the screens.
IMS-3183859	960392314	The Galaxy Browser window did not show all properties for Trend Client Control and **Show all properties** checkbox was disabled.
IMS-3280020	960402885	WindowMaker printout had an unusual background if Images/Graphics were selected as HTML file.
IMS-3287663	960409213	There was a handle leak on Alarm Client Control when the RunQuery() method was called.
IMS-3292969	960406554	Post-upgrade from InTouch HMI 2020 R2 P01 to InTouch HMI 2023 R2, the Web widget could not be opened in the Azure Power Application.
IMS-3302540	960412777	Status element in Industraial Graphic did not expose properties in scripts which resulted in warnings. Also, could not add a 'dot' after the status element name in a script.
IMS-3303422	960407542	The SQLSelect() function did not work if a string was used with the WhereExpr parameter.
IMS-3307715	960414467	On a Chinese install of InTouch HMI, the help file of Industrial Graphic Editor was in German language instead of Chinese.
IMS-3337421	960420385	When tried to zoom-out an Industrial Graphic symbol or set to fit to window, the graphic changed to red-X and it could not be recovered later.
IMS-3341495	960413176	Post-upgrade from InTouch HMI 2017 U3 SP1 to InTouch HMI 2023 R2, there were issues navigating to some of the windows.

InTouch HMI Known Issues

The following are the known issues that remain in the release of InTouch HMI 2023 R2 P01.

Issue ID	Description
3298289	Insight screen showed blank when tried to publish data from InTouch HMI. **Workaround:** 1. Go to **C:\Program Files (x86)\Wonderware\Intouch\InsightPublisher\x64** and open the **aahCloudConfigurator.exe.config** file. 2. Update the following values: • <add key="PublisherProcess" value="C:\Program Files (x86)\Wonderware\InTouch\InsightPublisher\x64\aahInTouchTagImport.exe" /> • <add key="PublisherPrerequisite" value="C:\Program Files (x86)\Wonderware\InTouch\InsightPublisher\x64\aahPublisherPrerequisites.dll" /> 3. Relaunch the publisher.

Documentation corrections

This section lists pending corrections to System Platform documentation. These changes will appear in the next product release.

In the System Platform Installation Guide

Location	Existing Text	Change
System Platform Installation Guide (System Platform 2023 R2) Modifying an Installation (page 133)	Step 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.	Add step 7 after the note. Step 7 After the modify operation has finished and you have rebooted the system, re-install any patches or hotfixes that were previously installed. This ensures that the new components are patched to the same level as the previously installed components. If the patch installation informs you that the patch is already installed, continue with the installation anyway. There is no harm in installing a patch a second time.
System Platform Installation Guide (System Platform 2023 R2) Repairing an Installation (page 135)	Step 7 When the update has finished, the Process Complete dialog box appears. Click **Finish** to close the dialog box and complete the process.	Add step 8. The repair process may overwrite patched files with unpatched earlier versions of the files. After the repair process has finished, re-install any patches or hotfixes that were previously installed. If the patch installation informs you that the patch is already installed, continue with the installation anyway. There is no harm in installing a patch a second time.

-- End of Patch 01 ReadMe --

AVEVA™ System Platform 2023 R2 ReadMe

Last revision: 12/19/2023

This document contains important information about AVEVA System Platform 2023 R2.

Included in This Release

Program Name	Version

AVEVA Application Server 2023 R2, including AVEVA OMI	23.1.000
AVEVA Communication Drivers Pack 2023 R2	23.02.000
AVEVA Enterprise License Manager 4.0.1	4.0.1
AVEVA Enterprise License Server 4.0.1	4.0.1
AVEVA Enterprise Licensing Platform 4.0.1	4.0.1
AVEVA Enterprise Licensing Platform(x86) 4.0.1	4.0.1
AVEVA Enterprise License Server Legacy Support 4.0.1	4.0.1
AVEVA Help	23.1.000
AVEVA Historian 2023 R2	23.1.000
AVEVA Historian Client 2023 R2	23.1.000
AVEVA InTouch HMI 2023 R2	23.1.000
AVEVA InTouch Access Anywhere Server 2023 R2	23.1.000
AVEVA InTouch Access Anywhere Secure Gateway 2023 R2	23.1.000
AVEVA Platform Common Services 8.0.1	8.0.23345.1
System Monitor Agent Install Manager 1.5	1.5.0
System Monitor Manager 1.5	1.5.0
Operations Control Logger	23.1.000
Operations Control Management Console	23.1.000

New in System Platform 2023 R2

System Platform 2023 R2 includes the following features, as well as miscellaneous bug and security fixes.

Operations Control and the Connected Experience

AVEVA Operations Control is an industrial software subscription to one or more of two packages that provides access across both on-premises and cloud applications. This flexibility provides multiple configuration, architecture, and deployment options that support your objectives and meet your requirements.

Adding connected experience to an Operations Control subscription provides the security of federated identity management for authentication and authorization, superseding the segmented approach of individual product security configurations. A per-user common identity is configured, authenticated, and managed through AVEVA Connect.

The *Getting Started Guide* describes AVEVA Operations Control and connected experience, how Operations Control differs from perpetual and flex license modes, and benefits of the Operations Control mode with connected experience. You can access it at: Welcome to AVEVA™ Operations Control (zoominsoftware.io)

Changes to the Default TCP port for Communication with Historian Server

The default TCP port for communication with Historian server has been changed to 32565. This is configurable and is used for data replication and communication with remote IDAS version 2023 R2 and later (which implies gRPC communication). The Classic Historian TCP port - 32568, for WCF communication, was used for data replication and remote IDAS communication with Historian versions 2023 and earlier, and remains for compatibility with previous versions.

Support for Import of SVG as an Industrial Graphic

The Industrial Graphic Editor supports import of Scalable Vector Graphics (SVG) as Industrial Graphics. You can perform the following:

- Import an SVG into the Industrial Graphic Editor. The graphic elements automatically get converted to an Industrial Graphic, which can include many primitives.
- Insert the SVG while using the **Image** icon from the **Tools** panel of the Industrial Graphic Editor.
- Use SVG for the **UpImage** and **DownImage** on a button.

- Use SVG for the **Quality & Status** display icons under **Styles** configuration.

New in Application Server and AVEVA OMI 2023 R2

Application Server 2023 R2 includes a number of new features, hot fixes, and provides support for the latest versions of Microsoft products. Refer to the GCS Technology Matrix for the list of supported Microsoft products.

Improved User Interface

The System Platform IDE has an improved user interface that provides object status at a glance.

New OMI Web Client

The web client for use with OMI ViewApps is completely new. The new client offers better performance, a look and feel more like the desktop client, and an easier way to make ViewApps available from a browser: you just assign them to an instance of the new WebViewEngine object type. The OMI web client is suppored with the latest versions of the Google Chrome and Microsoft Edge browsers.

OPC UA Scripting

You can now use Application Server object scripts and/or Industrial Graphics scripts to call OPC UA servers. Method calls are executed in the OPC UA server through the OPC UA client, are supported through the OPC client in the OI Gateway Communication Driver.

Alarm Latching and Alarm Dismiss

Latching is a new alarm state that can be enabled for a Galaxy. When latching is enabled, an acknowledged alarm that has returned to a normal value will continue to be displayed in the LATCHED alarm state. Alarms go to the LATCHED state if you ACK an alarm from UNACK_RTN state or return an alarm from ACK state. LATCHED alarms continue to be displayed to show that the alarms did occur. A dismiss command will return alarms that are in the LATCHED state to normal.

New in InTouch HMI 2023 R2

InTouch HMI 2023 R2 (Version 23.1.000) includes a number of new features, hot fixes, and provides support for the latest versions of Microsoft products. Refer to the GCS Technology Matrix for the list of supported Microsoft products.

Alarm Latching and Alarm Dismiss

If the Alarm latching feature is enabled, an acknowledged alarm that has returned to a normal value will continue to be displayed in the LATCHED alarm state. LATCHED alarms can be displayed in the current alarms mode to show that the alarms did occur. Alarms go to the LATCHED state when:

- ACK an alarm from UNACK_RTN state.

  Or

- Return an alarm from ACK state.

To view the LATCHED state, enable the LATCHED state in the **Alarms and events** configuration screen of the IDE. You can dismiss the LATCHED alarms to remove the LATCHED alarms from the current mode of the Alarm Client Control grid. The dismissed LATCHED alarms would be visible in the recent mode of the Alarm Client Control.

Credential Manager

Use the Credential Manager utility to securely store and manage login credentials. You can retrieve the stored credentials (from AVEVA Application Manager for standalone applications, and from the Application Server for managed applications) for authenticating access to other components in WindowMaker, WindowViewer, and Alarm utilities.

By default, all named credentials are added to the Administrators group. In addition, we recommend you to add groups that the users running the application belong. This will allow the users to access the credentials even when running the application in a non-administrator mode, such as WindowViewer.

Changes to the Default TCP port for Communication with Historian Server

The default TCP port for communication with Historian server has been changed to 32565. This is configurable and is used for data replication and communication with remote IDAS version 2023 R2 and later. The Classic Historian TCP port - 32568, was used for data replication and remote IDAS communication with Historian versions 2023 and earlier, and remains for compatibility with previous versions.

OPC UA Enhancements

A new option **External providers** has now been added under **Tag dictionary**, that lists all the OPC UA server connections configured in the Gateway

Communication Driver present on the same machine. Using this option, you can avoid several manual steps and create access names and InTouch tags for OPC UA item references easily. You can create the tags by just dragging and dropping from the **External providers** pane to the new **Model – Tagname** pane, that displays all the alarm groups and tags of the InTouch application.

Create Graphic Elements and Industrial Graphics using InTouch Tags

A **Model – Tagname** tab has been added in the **Properties** configuration pane of the Industrial Graphic Editor which displays all the tags available in the InTouch application. You can simply drag and drop the tags to the canvas to create graphic elements or Industrial Graphics. When creating multiple symbols at a time, the dot field property will be bounded automatically. This method simplifies the graphic development workflow and significantly reduces the application development time.

Embed an Industrial Graphic from the Toolbox Tab of Industrial Graphic Editor

You can embed an existing Industrial Graphic into current graphic using the **Toolbox** tab located in the **Properties** configuration pane of the Industrial Graphic Editor. The **Toolbox** tab displays all the Industrial Graphics available in the InTouch library. Once you have embedded the graphic, you can then edit it like any other component of the graphic.

Support for Import of SVG as an Industrial Graphic

The Industrial Graphic Editor supports import of Scalable Vector Graphics (SVG) as Industrial Graphics. You can perform the following:

- Import an SVG into the Industrial Graphic Editor. The graphic elements automatically get converted to an Industrial Graphic, which can include many primitives.
- Insert the SVG while using the **Image** icon from the **Tools** panel of the Industrial Graphic Editor.
- Use SVG for the **UpImage** and **DownImage** on a button.
- Use SVG for the **Quality & Status** display icons under **Styles** configuration.

Support for User Defined Types (UDTs) in InTouch

This feature supports the following:

- Manually create one or more UDTs, with nesting up to six levels.
- Manually create one or more UDT instances from a UDT.
- Bind individual UDT instance members to I/O.
- Reference individual UDT instance members in Industrial Graphics symbols.
- Import and export UDT to a JSON file.
- Edit UDT in bulk using external JSON editor.
- Edit and override UDT Properties except Name and Type.
- Changes in a data type are reflected immediately in the **User Defined Type** view.
- Configure the owning object of an embedded graphic and point to an UDT instance. During run time, the me. relative reference is replaced by the UDT instance. You can also update the owning object to a different UDT instance during run time.
- Intellisense for UDT instances lists all members and member data structures for the immediate level only. The Industrial Graphic Editor supports intellisense in scripting, animation, and custom properties. Native InTouch supports intellisense in scripting only.
- You can configure UDTs in Industrial Graphic animations and native InTouch animations.
- You can configure UDTs in an Industrial Graphic script and a native InTouch script.
- Update the alarm properties in the **Properties** grid. In the WindowViewer, you can view the members of an instance that are generating alarms and display them in an Alarm Client Control.
- The UDT members of an instance can log data to LGH files or the Historian, as with other InTouch tags.
- The UDT member of an instance behaves the same as other InTouch tags in the MapApp.
- The UDT member of an instance works the same as other InTouch tags in the Web Client.

Introducing the new Unified Identity

AVEVA Unified Identity enables Single Sign-On (SSO) for all Operations Control products on a given node with AVEVA Connect cloud capabilities. It supports common user authentication, authorization, and access entitlements across AVEVA Operations Control products. It includes:

- User Authentication via a single common user ID, configured and managed within AVEVA Connect.

- User Authorization via roles, groups, and rules (allow/deny).
- Single Sign-On: After you sign-on to a supported product, subsequent sign-ons to that product or other supported products on the node are automatic.

The connected experience requires access to the AVEVA Connect cloud repository from each node where you want to use it.

Option to secure InTouch application folder

To restrict access to the applications folder for Standalone applications, a new check box has been introduced in Application Manager under **Tools** > **Security**. When the security feature is enabled on a node, strict read and write permissions are applied to the InTouch View Application.

Update default local working directory for NAD and Managed InTouch application

An option **Enable local working directory integrity check for Managed and NAD InTouch Applications** has been added in the Application Manager, under **Tools** > **Node properties** > **Security**. If this option is enabled,when launching WindowViewer for a Managed InTouch application andr NAD application, a file time stamp and file content hash comparison is performed between the deployed application and the application in the local working directory. If the files do not match, WindowViewer will copy the deployed application to the local working directory and run the application.

New Features in Historian 2023 R2

AVEVA Operations Control connected experience sign-on support

Historian supports the AVEVA Operations Control connected experience with AVEVA System Platform.

The server must be configured with an advanced license to retrieve data for expressions.

Note that the following still require Windows credentials:

- HTTP communication (HTTPS is required)
- Replication
- SDK connection using Classic Historian (WCF)
- Managing Historian with System Management Server

Changes to default Historian communications protocol and ports

The Historian communications protocol has been updated. The port for the new protocol is 32565 by default. The previous port, 32568, is supported as a legacy port for connecting servers that are running older software that doesn't support the new protocol.

Tier 1 Historians, AppEngines, and Platforms that support the new protocol and use the default 32568 port are updated automatically when the software is updated to the latest version. The local IDAS is also updated automatically. Existing connections that use legacy custom ports will need to be updated manually. External firewalls may need to be updated to allow connections on the new port.

- For a remote IDAS, change the port with the remote IDAS configurator.
- Update replication servers via the OCMC.
- Update application servers that use old ports in the engine definitions in the Galaxy.

Connecting servers that support the new protocol but are still using a custom legacy port will show as using the HCAL (Classic) protocol on the Data Acquisition page. (Note that connecting servers on older software will also use the HCAL (Classic) protocol. This is expected. Older software does not support the new protocol, and should still connect on the legacy port and use the classic protocol.)

If you have connecting servers that support the new protocol but still use the legacy port, the following warning appears once each hour in the Operations Control Logger:

```
The Historian Client Access Point running on XXX:XXX is an older version using a legacy protocol. Please update the port in the connection definition to point to the new Historian Client Access Point (port 32565 by default).
```

For more information, see the following sections in the *Historian Administrator Guide*:

- *IDAS Security and Firewalls*
- *Configuring IDAS on a Remote Node*

Tags support multiple languages in Historian Client Web, Historian Client Query, and Historian Client Trend

You can now configure multiple translations for the same tag in Historian Client Web, Historian Client Query, and Historian Client Trend.

The language for these applications will be set automatically based on the operating system or browser language.

HTTPS-based communications

Internal Historian network communication is more secure and easily integrated with HTTP proxies.

Live data via iData

View latest historical values as the “live” values on OMI displays.

Alarm grid filter and sort in Historian Client Web

Browser-based alarm history in Historian Client Web supports more filtering and sorting options.

Historian Client Web / Excel integration

Easily transition from Historian Client Web charts to detailed analysis in Excel.

New look for Historian Client Web

The Historian Client Web interface is updated to be more powerful and easier to use.

Export / import Historian Client Web content

Include saved charts in CSV configuration import/export.

New features in Historian Client 2023 R2

Ad-Hoc expressions in Trend

Historian Client Desktop Trend control and its embedded ActiveX controls now support Ad-Hoc expressions. The Expression application and pane now appear in the Tag Picker with the Textbox editor.

For embedded ActiveX controls, scripting is supported for ad-hoc expressions in InTouch applications.

Ad-hoc expressions are supported with both SQL and REST connections.

Expanded ad-hoc expression functions

New functions added to ad hoc expressions make results simpler and more valuable.

Runtime language switching

Runtime language switching is supported for Trend Control, Query Control, Embedded control, and the Excel and Word ActiveX controls. It's supported for the following fields:

- Description
- EngineeringUnit
- Message On/Message Off
- Alias

If there is no value for the requested language for a field, the default language is used.

Improved Trend control for InTouch

Configuration is simplified for the Trend control within InTouch. The control is available in the graphic editor and can be placed in InTouch directly.

AVEVA Identity Manager Server login

Trend and Query support single sign-on authentication with AVEVA Identity Manager. This is restricted to REST-based connections and is not available for SQL-based connections.

Additional script functions for OMI Trend App and Graphic Editor support

The event tags TagAdded and TagRemoved have been added and are available at the Graphic level and in the HistoricalTrendApp control.

General performance improvements

Performance has been improved across the Historian Client controls.

Microsoft Office Historian Client Workbook improvements

The classic Historian Client Workbook add-in has been updated. Note the following:

- Microsoft Office is optional. If you install Office after installing Historian Client, the Historian Client add-ins do not appear in the list of Office add-ins. Run the Historian Client installation program and repair the installation to load the Office add-ins.
- When you perform a custom installation of Microsoft Office (32-bit), you must install Office Shared Features and Office Tools so that the Historian add-ins for Workbook or Report can be loaded.

  Note: Make sure that you are not using the 64-bit version of Microsoft Office.

Tool for migrating from Historian Client Workbook to the newer Excel task pane add-in

The Excel Migration Tool updates Excel workbooks created in Historian Client Workbook to formulas compatible with the newer Historian Excel task pane add-in.

This tool is supported for files created in Excel 2016 or later.

For more details, see the *Migrate data from Historian Client Workbook to the Excel add-in* section in the *AVEVA Historian Client User Guide*.

New in Communication Drivers 2023R2

OPC UA Methods Support

Client applications (such as Application Server) can call a method in an OPC UA server through the OPC UA client in the Gateway Communication Driver.

About This Release

Related Topics

Supported System Platform Versions for Product Upgrade

Supported System Platform Versions for Migration

Security Changes Related to End-of-Life Third-Party Components

Application Object Toolkit

Name Changes to Graphics and Graphic Toolsets

Readme Files for Other Products in this Release

Supported System Platform Versions for Product Upgrade

You can upgrade directly to System Platform 2023 R2 from System Platform 2017 or later, provided the prior version was installed on a 64-bit operating system.

Upgrades to System Platform 2023 R2 are NOT supported from the following System Platform versions:

- System Platform **Enterprise** 2023
- System Platform 2020 R2 **CR1** and **CR2**

Limitations

All existing, installed products on a node must be upgraded to the same version. Upgrading is defined as installing a newer version of the software when a previous version of the software exists. An upgrade is possible when the system requirements (operating system, SQL Server, .NET Framework) are met. The upgrade process will properly remove or uninstall the previous software version and install the new version. For versions older than the current and previous licensed versions, only the latest service pack or patch versions are tested. For distributed systems, some products must be upgraded in a particular order. For more information, see upgrade information for each product in the *System Platform Installation Guide*.

IMPORTANT! Back up any relevant application configuration files and databases before you start an upgrade or migration.

IMPORTANT! System Platform does not support mixed Windows workgroup/domain environments. Although workgroups are supported, domain-based networking is recommended. However, you cannot use workgroup nodes within a domain environment.

Operating System Compatibility

The earliest versions of Windows that support System Platform 2023 R2 are:

- Long Term Servicing Channel
  - Windows 10 Enterprise, IoT Enterprise 2015 LTSB (1507)
  - Windows Server 2016 LTSC Standard and Datacenter
- General Availability Channel:
  - Windows 10 21H2 Pro, Enterprise, and IoT Enterprise

See the GCS Technology Matrix for complete information about operating systems that you can use with System Platform 2023 R2 products.

Supported System Platform Versions for Migration

You can migrate user-created content (for example, .cab files, .aaPKG files, Historian databases, etc.) to System Platform 2023R2, as long as the content was created in one of the following product versions:

- System Platform: Version 4.5 or newer
- Application Server: Version 2.5 or newer
- InTouch HMI: Version 7.11 P07 or newer
- Historian Server: Version 9.0 P02 or newer
- Historian Clients: Version 9.2 or newer
- FS Gateway: Version 1.5 or newer

Security Changes Related to End-of-Life Third-Party Components

Security changes in System Platform 2023 and later include the removal of certain assemblies from Microsoft that have reached their end-of-life and are now out of support. These assemblies may pose a security risk and are no longer needed to support System Platform installation. The removed assemblies include:

- Microsoft SQL Server 2012 Management Objects SP2 (11.2.5058.0)
- Microsoft Visual C++ 2008 Redistributable
- Microsoft Visual C++ 2010 Redistributable

System Platform components that may be affected: The flexibility of System Platform allows extensive customization, which could potentially involve these libraries. It is important to note that components that do not reference the removed libraries are not affected. System Platform components that may be affected include:

- Custom or third-party base templates built with the Application Object Toolkit, if they reference any of the removed libraries.
- The discontinued ApplicationObjects $FieldReference and $Switch
- Custom script libraries (DLLs) or custom .NET controls built with these out-of-support components.
- Any other component that leverages the out-of-support assemblies.
- Remote Response Objects (RRO).

If you are upgrading an existing System Platform installation, the out-of-support libraries are retained if they are already present, ensuring ongoing functionality. However, clean installations of System Platform 2023 R2 will not include the libraries, and this could affect any imported/migrated applications that rely on them.

For ways to take remedial action to avoid any problems with components that may be affected by the removal of the out-of-support libraries, see the *System Platform Installation Guide*.

Important! Installation of out-of-support assemblies is NOT recommended.

Server-based Licensing

AVEVA System Platform uses the **server-based licensing** subsystem introduced in System Platform 2017. This licensing subsystem provides **centralized license management**, and replaces the file-based licensing system that was used in prior releases. Licenses must be activated before use.

If you are upgrading from Wonderware System Platform 2014 R2 SP1 (with or without patches), you must first install and configure a license server node, and activate the licenses to ensure continuous plant operation. The license server is typically installed on the Galaxy Repository node, but you can use a dedicated license server. See the "License Installation and Activation" section of the *System Platform Installation Guide*.

Application Object Toolkit

Microsoft .NET Framework 4.8 or later is required for System Platform 2023 R2. When the System Platform installation process begins, it automatically checks

the .NET version and installs the correct version if needed.

The Application Object Toolkit (AOT) is not included in the System Platform 2023 R2 release, but if you use AOT to build objects for Application Server, check that you have installed and configured the developer pack for .NET Framework 4.8 when you create your AOT solution in Visual Studio.

Name Changes to Graphics and Graphic Toolsets

As of System Platform 2023, the System Platform IDE changes the names of some of the toolsets and graphics included in the Graphics Toolbox. The affected toolsets and graphics are in the path
_Default Content > 3. Graphics > Icon Library

- The "SE_" prefix is removed from all graphic names in the SE_Branding toolset, and the toolset name is changed to "Branding." The full path to the renamed toolset and graphics is:
  _Default Content > 3. Graphics > Icon Library > Branding

  The SE_Branding toolset is now simply Branding, SE_Domain_Pictograms is now Domain_Pictograms, and so on.
- The "WW_" prefix is removed from the WW_Icons toolset, and the WW_Logo and WW_Logo_Tbit graphics are removed. The toolset name is changed to "Icons." The full path to the renamed toolset and graphics is:
  _Default Content > 3. Graphics > Icon Library > Icons

  The new Icons toolset contains only one graphic named AVEVA_Logo. This graphic is new for System Platform 2023.

Existing galaxies that were created before System Platform 2023 will continue to contain the previous toolset and graphic names; you do not need to change any existing graphics or layouts that use any of these graphics under the SE_* or WW_* name.

New galaxies created after an upgrade to System Platform 2023 or 2023 R2 will contain only the new graphics.

Except for replacing the old WW_Logo graphics with AVEVA_Logo, this is a name change only. The graphics themselves have not changed.

Readme Files for Other Products in this Release

To access individual product Readme files, insert the System Platform installation DVD and navigate to the applicable folder under the **InstallFiles** directory. Review the known and resolved issues contained in each Readme file for the component products updated for this release:

Product	**Location on Installation DVD**
Application Server	InstallFiles/CD-ApplicationServer/UserDocs/English/Readme.html
InTouch HMI	InstallFiles/CD-Intouch/Readme.html
Historian Server	InstallFiles/CD-Historian/Readme.html
Historian Client	InstallFiles/CD-HistorianClient/Readme.html
InTouch Access Anywhere	InstallFiles/CD-Server/Readme.html

Important Notice: Windows Updates

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

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.

How to Find the Latest Product Requirements and Compatibility Information

For important information about this product release, go to the AVEVA Global Customer Support (GCS) website. Information on the GCS website includes product requirements and compatibility, as well as downloads from previous releases. After you log in, you can filter search results by product name and the release/version.

The GCS Product Hub contains Readme files, videos, and product downloads from previous product releases.

- The GCS Technology Matrix is a searchable database that contains the latest product information. Enter the product name in the search bar, then select the current release to view:
  - **Product Information:** version name, number, release date, etc.
  - **Product Notes:** key release information, new features, and updates
  - **OS Compatibility:** list of compatible Windows and Windows Server versions
  - **Database Compatibility:** list of compatible SQL Server and other database product versions
  - **Virtualization Compatibility:** list of compatible virtualization software products and versions
  - **Product Coexistence:** list of products that can be installed on the same computer
  - **Product Compatibility and Interoperability:** list of products that can operate together and communicate with each other through a common message protocol

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 and Older
- 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

AVEVA OMI SDK

The AVEVA OMI Software Developer Kit (SDK) provides programmatic access to component APIs and namespaces. Using the methods and properties that these provide, you can build your own custom AVEVA OMI applications. Users can then add these custom apps to their ViewApps, the same way that they can add the AVEVA OMI apps that are included with Application Server.

When you install the System Platform IDE, the AVEVA OMI SDK is automatically installed, including samples and libraries. A link to the AVEVA OMI SDK Web Help is added to the Windows start menu. You can also open the OMI SDK Help via AVEVA Help, accessible from the Windows Start Menu, under AVEVA.

- The default installed location of the SDK is:

  C:\Program Files (x86)\ArchestrA\Framework\AcfSdk

System Platform Installation

For detailed installation instructions in English, see the *AVEVA System Platform Installation Guide* (SP_Install_Guide.pdf). The Installation Guide pdf file is located in the root directory of the System Platform installation DVD.

Before Installing System Platform

Important! Installing System Platform on a computer used as a domain controller is not supported.
For more information, see the Microsoft Security Best Practices Checklist.

Some AVEVA products released prior to System Platform 2023 R2 must be installed BEFORE you install System Platform, if the product will be installed on the same node as 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)

About the Network User Account

The Network User Account, previously called the ArchestrA User or AdminUser Account, is a user name and password combination that enables inter-node communication between computers in a System Platform environment. You must specify the same user account on every node when you install the System Platform components for the first time on computers that communicate with each other.

WARNING! The Network User 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 that uses the account may stop functioning properly.

- If the Network User Account has not previously been configured, you will be prompted to configure it during the System Platform installation. You must specify a user name, password, and domain.
- If you use an existing user account, it should have a permanent password that does not expire, and the password should not be changed.

After you install a System Platform component, you can use the Change Network Account utility to change or re-create the Network User Account. The AVEVA Start menu contains a shortcut to the utility.

You must have Administrator privileges to use the Change Network Account utility. For more information, see the Change Network Account utility help, available from within the utility.

Note: If you re-create 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 node. Until that occurs, some System Platform components may not function properly. Restarting the Galaxy node updates this information immediately.

System Monitor Installation and Configuration

We highly recommend the following System Monitor installation and configuration sequence. For more information and details, please see “Configuring the System Monitor Agent" and "Configuring the System Monitor Manager” in the *System Platform Installation Guide* (SP_Install_Guide.pdf).

1. Install System Platform.
2. Start the Configurator:
    a. Configure the Common Platform, including the System Management Server (SMS) and license type, on all nodes. Only one SMS node should be configured per System Platform installation; configure all other System Platform nodes to point to the SMS node.
    b. Configure the AVEVA System Monitor on all nodes. Only one System Monitor node should be configured per System Platform installation; configure all other System Platform nodes to point to the System Monitor node.
    c. Configure the Alert Email Server on the System Monitor Manager node.
    d. Configure the remaining product plug-ins.
    e. Restart your system.

Re-Connecting to System Management Server after Hardware Replacement or VM Restoration

If you connect a machine to the System Management Server and then later replace the machine due to hardware failure, or restore the VM to a state prior to that connection without first disconnecting the machine from the System Management Server, you will not be able to reconnect that same machine to the System Management Server.

Cause:

To protect the security of the system, the System Management Server uniquely identifies each machine that connects to it. If an intruder attempts to pretend to be that machine (spoofing) and re-registers with that machine’s name, the System Management Server will detect the mismatched identity and reject the suspected intruder’s registration.

Solution:

- Before replacing a connected machine, and/or restoring the connected VM to a pre-connected state, run the Configurator on that machine and disconnect it from the System Management Server.
- If that is not possible (i.e., the machine is no longer available due to hardware failure), then you will need to remove the connection information on the System Management Server manually:

  After attempting to reconnect the machine, the logger will contain the warning:

  “ArchestrA.CertificateManager: Please un-register the device <device name> from management server. Use the (Remove-AsbDevice) script to remove the device registration”

The PowerShell command will remove the machine's connection information from the System Management Server. We recommend that you contact your support team, or AVEVA Global Customer Support (GCS), for assistance with executing this command.

Licensing Information

Once installed, a link to the AVEVA Enterprise License Manager can be found in the **\AVEVA** folder on the **Start** menu.

It can also be accessed by pointing your browser to the following URL:

```
http://<nodename>/AELicenseManager
```

where <nodename> is localhost or the name of the node where the AVEVA Enterprise License Manager is installed.

License Server

The AVEVA Enterprise License Server can be installed separately from the AVEVA Enterprise License Manager.

Running Both InTouch HMI and AVEVA OMI in a Session on an RDS Server

In System Platform 2023 R2, running both InTouch HMI and AVEVA OMI in a session on an RDS Server will attempt to acquire two (2) Supervisory Client Server (unlimited) licenses instead of one (1).

If you have purchased a Supervisory Client Server license (unlimited RDP sessions on a single server) and then run both InTouch HMI and AVEVA OMI simultaneously, there can be issues acquiring the server license due to differences in how the license is handled between the two. The order of startup will impact the results.

This behavior is seen in only a limited number of instances, only when you have purchased a subscription license. If you do see this behavior, change the order of InTouch HMI and AVEVA OMI startup.

If this behavior continues, contact AVEVA Software Global Customer Support (GCS), describe the behavior, and request a temporary license, typically valid for 60-days.

AVEVA OMI and InTouch HMI ViewApp License Reservation Device Name for Client Devices, RDP Servers, and Users

License Reservation

Reserving a license for a specific device ensures a license will be available for that specific device whenever it is needed, regardless of the number of devices connected to the system. Keep in mind, each license can only be reserved to a single device, so if the device names are unknown ahead of time, it's better to not use reservations and instead allow the licenses to be acquired on a first-come, first-serve basis.

User-based License Reservation

In the AVEVA Enterprise License Manager license reservation page, it is possible to mark a license to be reserved to a specific user. While the reservation page allows this particular configuration, it's important to know that neither AVEVA OMI nor InTouch HMI ViewApps support user-based license reservations. The end-result will be the inability for the software to acquire the license reserved. Therefore, only use device-based reservations for Supervisory Client licenses.

Device-based License Reservation

When reserving a Supervisory Client license for a specific device, the Device Name needs to be the name of the computer running the InTouch HMI/AVEVA OMI ViewApp. In the case where the ViewApp is running inside of a Remote Desktop Session, on an RDS (aka: Terminal Server), then the Device Name needs to follow this naming pattern:

<RDSHostName>-<RDPClientName>-<index>

where RDSHostName is the name of the Remote Desktop Server (aka: RDS or Terminal Server), and RDPClientName is the name of the PC running the RDP client software, and "index" is 1, unless there will be multiple RDP sessions from a single client machine, in which case the index should be incremented (starting at 1) for each reservation for that specific RDP client, up to the total number of RDP sessions from that specific RDP client.

Reservation Examples

Situation: A computer with a hostname of "ControlRoomA" runs AVEVA OMI

Device Name: "ControlRoomA"

Situation: A computer with a hostname of "ControlRoomB" running a single Remote Desktop Client (RDP), connecting to the Remote Desktop Server (aka: Terminal Server) with a hostname of "PrimaryRDS"

Device Name: "PrimaryRDS-ControlRoomB-1"

Situation: Two computers with hostnames "SupervisorPC1" and "LineMgrA", respectively, each running a single Remote Desktop Client (RDP) connecting to the Remote Desktop Server (aka: Terminal Server) with a hostname of "PrimaryRDS"

Device Names:

- License Reservation 1: "PrimaryRDS-SupervisorPC1-1"
- License Reservation 2: "PrimaryRDS-LineMgrA-1"

Situation: A computer with a hostname of "ExecutiveDesktop" running four (4) Remote Desktop Clients (RDPs), connecting to the Remote Desktop Server (aka: Terminal Server) with a hostname of "PrimaryRDS"

Device Names:

- License Reservation 1: "PrimaryRDS-ExecutiveDesktop-1"
- License Reservation 2: "PrimaryRDS-ExecutiveDesktop-2"
- License Reservation 3: "PrimaryRDS-ExecutiveDesktop-3"
- License Reservation 4: "PrimaryRDS-ExecutiveDesktop-4"

AVEVA Enterprise Licensing Support for High Availability (HA) and Disaster Recovery (DR) in Virtual Environments

Virtual Environments: License Servers are supported in virtual environments. However, under certain circumstances, such as transferring a license from one virtual environment to another, the License Server may interpret the transfer as an improper move and therefore go into grace period.

- High Availability (HA) in VMWare and Hyper-V virtual environments **does not activate licensing grace period during a failover** as monitored environmental variables do not change.
- Disaster Recovery (DR) in VMWare and Hyper-V virtual environments **activates a licensing grace period** as monitored environmental variables do change.

High Availability: License Servers in a High Availability virtual environment are supported in specific topologies. Basic redundancy topologies are described in the AVEVA Enterprise Licensing online help.

Disaster Recovery: License Servers in a Disaster Recovery virtual environment will go into a grace period during DR activities. This is because DR activities are similar to an improper move of licenses and will trigger a grace period.

To avoid a grace period trigger in a DR virtual environment, we recommend that you run the License Server outside the virtualized DR environment and use a redundant License Server configuration through the functionality built into the License Server software. Another option is to purchase Disaster Recovery licenses at a discounted rate and establish a backup License Server with these additional licenses.

In all environments, we recommend you install and run the AVEVA System Monitor to monitor licensing functionality and view alerts on issues such as a License Server going into grace period or licenses expiring.

Antivirus Software

Antivirus Software should be implemented as part of a defense-in-depth strategy to secure your Industrial Control Systems. TechNote TN2865, available from the AVEVA Global Customer Support (GCS) web site, lists important information about antivirus software. Enter your GCS credentials to access the TechNote.

https://softwaresupportsp.aveva.com/#/okmimarticle/docid/tn2865

Known Issues

The following important known issues are listed by their assigned reference number in ascending order. Additional known issues are documented in the product-specific Readme files.

PCS and MGC Issues

PCS: Platform Common Services

MGC: Multi-Galaxy Communication

Issue Number	Description
IMS 1586624	The logger will repeatedly display error/exception messages from the "view" component if a multi-galaxy pairing is broken for any reason, and then an InTouch HMI Managed ViewApp is launched that contains cross-references to tags in another galaxy. **Workaround:** Since the exceptions are caused by the broken galaxy pairing, simply pair the galaxies again. The exceptions will no longer be logged.
IMS 2829309	If you are using the connected experience for security and you close the browser window where you signed in when starting an OMI ViewApp, you may see one of these symptoms when signing out of the ViewApp: The sign out option may not appear; no users may show as signed in; if there are multiple connected users, you may be able to sign out as a different user; or you may see a message saying that sign out did not succeed even though it did. **Workaround**: Either have the System Administrator change the authentication browser option in the configurator (found under **Common Platform** > **System Manager Server** > **Advanced** > **Authentication**) to use the embedded browser pop-up dialog box, or keep the sign-in browser window open the entire time you are using the OMI ViewApp. Sign out then functions correctly.

TFS 1263702	When upgrading from a node with Platform Common Services (PCS) 4.3.3 installed, such as the case when upgrading from System Platform 2017 Update 3 SP1 or installing on a node with RMP 2017 Update 2, errors are logged while deploying the OPCUA service. However, the service is deployed successfully. The errors are similar to the following:
	`Application certificate does not have an application URI: CN=AZURE2019`
	`Failed! UnifiedAutomation.UaBase.StatusException: Application certificate does not have an application URI: CN=AZURE2019`
	`at UnifiedAutomation.UaBase.ApplicationInstanceBase.LoadApplicationCertificate (ApplicationDescription application, String hostName, Boolean silent)`
	`at UnifiedAutomation.UaBase.ApplicationInstanceBase.CheckConfiguration(Boolean silent)`
	`at UnifiedAutomation.UaBase.ApplicationInstance.Start(ServerBase server, WaitCallback callback, Object userData, Boolean silent)`
	`at PCS.Provider.OpcUa.UaServerHostedService.StartApplication()`
	`at PCS.Provider.OpcUa.UaServerHostedService.<ExecuteAsync>d__7.MoveNext()`
	
	Workaround:
	1. Upgrade all nodes and install and configure PCS 4.4 on each.
	2. On the node that will function as the OPC UA Server, select the "No System Management Server configured" option and finish configuration.
	3. Start the Configurator again (reboot if necessary), and configure the System Management Server option as applicable for your system.

IMS 2658043	In an installation which uses workgroups and has MultiCast-DNS enabled, upgrading from an earlier version to PCS 8.0 (for example, during an upgrade to System Platform 2023R2) causes an issue with the PCS certificate. This causes secure communication with the SMS to fail. The SMS falls back to using non-secure communication. This causes error messages to be written continuously to the logger on all remote nodes. **Workaround**: Perform the following procedure on all nodes, including the SMS node: 1. Open the Configurator and, under **Common Platform**, select **System Management Server**. 2. Select **No System Management Server configured** and select **Configure**. 3. Close the Configurator and reboot the node. 4. After the reboot, open the Configurator again and set the System Management Server back to the correct selection: **This machine is the System Management Server** on the SMS and **Connect to an existing System Management Server** on all other nodes. Select **Configure**. 5. Close the Configurator and reboot the node.

Communication Driver Pack Issues

Issue Number	Description
IMS 1578426	When attempting to establish a secure, encrypted SuiteLink connection, an error may be generated and the connection is terminated (by either the Client or Server). This condition will occur if the standard user has not been added as a member of the 'ArchestrAWebHosting' user group. **Workaround:** For a secure, encrypted communications over SuiteLink, add the standard user to the 'ArchestrAWebHosting' user group on the server side. For details, see the *AVEVA Communication Drivers Pack Help*, "Secure SuiteLink Connection," available after installation in the AVEVA Help application.
IMS 1435622 TFS-1355437	If the Gateway Communication Driver (v4.0-v6.0) is installed on a machine and you try to upgrade to System Platform 2020 R2 SP1, then the Gateway Communication Driver gets uninstalled. **Workaround:** Use **Modify** install option in System Platform 2020 R2 SP1 and select Standards - Gateway to install on the machine. **Note:** If you install the Gateway Communication Driver using System Platform 2020, System Platform 2020 R2, or Wonderware System Platform 2017 U3 SP1 (along with InTouch and Application Server), then there is no issue in upgrading the Gateway Communication Driver using System Platform 2020 R2 SP1.

Installation, Upgrade and Galaxy Migration Issues

Issue Number	Description
IMS 2967085	During an upgrade to System Platform 2023R2, you may receive an error message from the LicAPISvcProxy.NET service that starts: `Failed to communicate with AVEVA Enterprise License Product Service`. This is caused by an upgraded component trying to acquire a license before the Licensing service has started. **Workaround**: None needed. The error will resolve itself once the upgrade is complete and the node is rebooted.
IMS 2917871	After an upgrade, the AVEVA Insight Supervisor service is not set to start automatically. **Workaround**: After the upgrade, open the Windows **Services** dialog box. In the list of services, right-click the AVEVA Insight Supervisor service. Select **Properties** and, on the **General** tab, set the **Startup type** to Automatic.
IMS 2840477	When you run setup to upgrade from System Platform 2023 or other version to System Platform 2023 R2 and reach the "Ready to Upgrade the Application" form, but then select **Back**, setup may not navigate to the previous page. This happens because the previous page is a prerequisite check. Since all prerequisites have been satisfied, the setup program remains on the "Ready to Upgrade" form. **Workaround:** If you wish to return to a prior point in the upgrade process, press the **Cancel** button and restart the setup program.
IMS 1958954	After upgrading from a prior version to System Platform 2023, Windows start menu icons from the prior version of System Platform may be displayed instead of the new System Platform icons. This may affect the icons for all System Platform products and components, including the Operations Control Management Console, Trend App, and InTouch HMI WindowMaker. This is an operating system cache issue that affects newer versions of Windows. There is no impact to the functionality of the products, and all new System Platform features will work as expected. **Workaround:** You can clear the Windows cache. Note that the cache is owned and managed by the Windows operating system. Therefore, we recommend that you contact Microsoft before using this procedure. 1. Navigate to AppData\Local\Packages\Microsoft.Windows.Search_<AlphaNumericID>\LocalState\AppIconCache\100 and delete all files in the folder. 2. Restart your machine. The updated icons should now appear.
IMS 1925046	After installing or upgrading to System Platform 2023, and then completing configuration of the System Monitor Manager, icons and the UI title bar from the previous version of System Platform are shown for the Operations Control Management Console (OCMC), even if this is a new installation. This also occurs when installing OCMC Standalone and then installing any product that has an older version of OCMC (SMC). The icon in the title bar of the OCMC and the task bar icon revert to old icon. **Workaround:** Use Programs and Features in the Control Panel to repair the Operations Control Management Console.
IMS 1758909 IMS 1739197	MDT AutoSave 5.01a is not supported on System Platform 2023 and System Platform Enterprise 2023.
TFS 1249251	Upgrading to System Platform 2020 or later from a prior version does not succeed if the prior version used a 32-bit version of SQL Server. Support for 32-bit SQL Server was discontinued for the System Platform 2020 release.

Workarounds: Two methods for upgrading System Platform and migrating galaxies are listed below. Use the first method if you will use SQL Server Express, included with System Platform. Use the second method if you will be installing a 64-bit full version of SQL Server in place of a 32-bit version.

Method 1 (install SQL Server Express as part of System Platform installation):

1. Detach the galaxy databases through SQL Server Management Studio.
2. Back up the database files by copying the Galaxy folder in the path:
   C:\Program Files (x86)\ArchestrA\Framework\FileRepository\
3. Uninstall the 32-bit version of SQL Server Express.
4. Launch the System Platform 2020 installation program (setup.exe), and allow it to install SQL Server Express 2017 (64-bit).
5. Restore the Galaxy folder to the path:
   C:\Program Files (x86)\ArchestrA\Framework\FileRepository\
6. Attach the previously detached Galaxy database files.
7. Restart the aaGR and Watchdog services.
8. Launch the IDE, then connect to the galaxy and migrate it.

   Galaxy migration should succeed without any issues.

Method 2 (install full version of SQL Server):

1. Detach the galaxy databases through SQL Server Management Studio and make a backup (see Considerations for SQL Server for information about SQL Server Management Studio).
2. Uninstall the existing 32-bit version of SQL Server.
3. Install a supported 64-bit version SQL Server.
4. Attach the previously detached Galaxy database files.
5. Launch the System Platform 2020 installation program (setup.exe) and allow it to upgrade your products.
6. After upgrade is complete, launch the IDE, then connect to the galaxy and migrate it.

   Galaxy migration should succeed without any issues.

AVEVA OMI Issues

Issue Number	Description
IMS 1212168	On Windows 10 operating systems, layouts created in System Platform 2020 with non-English OS/regional settings show a warning and do not open when migrated to System Platform 2020 R2 or 2020 R2 SP1. **Workaround:** Before migrating the galaxy, make sure the operating system locale is set appropriately by following these steps: 1. Open the Windows **Control Panel** and select **Region**. 2. Select the **Administration** tab when the **Region** popup opens. The Administration tab contains two buttons: • **Copy settings** • **Change system locale** 3. Select **Copy settings** and then mark the checkboxes to copy current settings to "Welcome screen and system accounts," and "New user accounts." 4. Select **Change system locale** and then choose the applicable locale from the dropdown list.
TFS 1369154	Under certain circumstances, an instance derived from a template with an invalid reference will not show a warning during design time. This can occur if the following occurs: 1. A symbol is added to the Graphic Toolbox with an undefined relative reference, for example, “Me.Attribute001,” where Attribute001 has not been created yet. 2. The symbol is then added to a layout. 3. The layout is linked to a UDO (User Defined Object) template. When the template is saved, no warning is displayed. 4. When an asset is derived from the template, no warning is displayed for the instance either.

Result: Although no warnings are issued during design time, when you create and then deploy a ViewApp with the linked layout, and show the linked layout in any screen, an error message will be displayed at run time (or in Preview Mode) that will allow you to troubleshoot and correct the error. The message will be similar to:

Element 'TEXT1' in Symbol 'UDO_001.S1' has Configuration error: Invalid reference 'Galaxy1:Me.Attribute001' with owning object 'UDO_001' does not exist.

TFS 1160616

If an admin user logs in, launches a ViewApp, and then logs off the system while leaving the ViewApp running, registry keys are unloaded in the profile of the user account. This results in continuous errors from CheckPointFileServer in the logger similar to: ""INVALID HRESULT LINE765 File CheckPointFile.cpp hResult 80003fa after logging off and logging on as different users (non-admin)."

Cause: This is a known Microsoft issue. This problem typically occurs after an administrator uses a service account to log in to the server for an interactive session, and then logs off. For example, an administrator may log in to a Web Front End (WFE) server by using the farm account, and then log off. This activity forces the registry keys to be unloaded in the profile of that account, and makes the keys unavailable for future use. Microsoft recommends using either of the following workarounds to resolve this issue. For more information, see:

"800703fa Illegal operation attempted on a registry key" error

A COM+ application may stop working on Windows Server 2008 when the identity user logs off

Workaround 1: Do not log in to the server for interactive sessions by using a service account.

Workaround 2: Disable the related Windows User Profile Service feature as follows:

1. Open the Group Policy editor (Gpedit.msc) on the affected server.

2. Open the User Profiles folder in the following path:

Computer Configuration > Administrative Templates > System > User Profiles

3. Locate the **"Do not forcefully unload the user registry at user logoff"** setting.

4. Change the setting to **Enabled**.

CR L00150114

SR59513303: TheGetCPTimeStamp() scripting method, when used in an AVEVA OMI action or named script within a symbol, does not return the timestamp at run time. Instead, it returns characters for the timestamp format, such as "mm/dd/yyyy hh:mm:ss." No errors or warnings will appear in the logger. This is similar to issue 777504, listed below.

Workaround: Use the GetCPTimeStamp() method in an object script instead of a symbol script.

Missing NavTree

After upgrading or migrating an AVEVA OMI ViewApp from 2017, a warning message states that the NavTree entity could not be found. In 2017 Update 1, this navigation object has changed and is now called "NavTreeControl."

Workaround 1: To replace the NavTree object in a ViewApp or Layout when upgrading from System Platform 2017:

1. Open the ViewApp or Layout that shows the warning.

2. In the ViewApp or Layout editor, look in the **Actions** list for all references to "NavTree." An icon showing "Content not available" will be displayed for these references.

3. To see the entire action list for a ViewApp, toggle the **Actions for Primary** switch to show **Actions for Home** (does not apply to the Layout editor).

a. Replace the NavTree object with the new NavTreeControl.

b. Search for NavTreeControl under the Toolbox tab.

4. Drag the NavTreeControl onto the pane to replace the NavTree.

5. Confirm that you want to replace the content, then save the ViewApp or Layout and close the editor.

6. Verify Layouts and ViewApps no longer show any warnings related to the NavTree.

7. Deploy the ViewApp.

Workaround 2: To replace references to NavTree when importing packages from System Platform 2017:

1. Launch the IDE and open the "Find" dialog.
2. Search for "NavTree" using the default search settings.

   If the package file contains the obsolete NavTree object, it will be listed in the search results.
3. Double-click the NavTree search result, which will select the NavTree object in the Graphic Toolbox.
4. Delete the NavTree object from the Graphic Toolbox.
5. Use **Workaround 1** to replace the NavTree object with the new NavTreeControl object.

TFS 774717 When an AVEVA OMI application (View.exe) that uses one of the following web controls is run in 4K mode or on multiple 1080p monitors, under certain circumstances the application may stop responding:

- InSightApp
- MapApp
- WWWebAppControls

Workaround: When running a ViewApp that uses a web control on a 4K monitor, set the monitor resolution to 2560 x1440 or less. When running the ViewApp on 1080p monitors, do not attempt to span multiple monitors.

TFS 777504 The GetCPQuality() scripting method is not supported in AVEVA OMI. If used in a ViewApp, it always returns quality = 0 (bad quality). This is similar to issue L00150114, listed above.

TFS 781006 If an invalid custom property is added to a symbol, no warning is logged in the Operations Control Management Console, even though no value is displayed for the custom property.

TFS 781620 The Height and Width properties of a group with text elements do not change in accordance with changes made to the label font size, and are not rendered correctly.

TFS 784470 Tooltip animations that contain multiple lines of text with line breaks may not display properly in deployed ViewApp.

TFS 784474 A tooltip may partially cover the element with which it is associated in the deployed ViewApp.

TFS 787192 When OSGroup security mode is used, the VerifiedWrite dialog is not displayed when you modify the value of a VerifiedWrite attribute from a combobox, if you first attempted to perform the VerifiedWrite without having the correct security credentials.

TFS 789958 On some high resolution tablet devices, such as the Surface Pro 4, object names in the System Platform IDE may have insufficient line spacing between items, which can make it harder to read object names.

TFS 794383 When a custom property is changed from public to private, the change does not have any affect, and the value of the private custom property is shown at run time (private values should not be shown). Similar situations occur when:

- An override values for a custom property that is later made private. The override is also shown at run time.
- An override is applied to a custom property, and later the custom property is locked (can no longer be overridden). When the ViewApp is redeployed, the override value is still shown.

Workaround: Manually validate the outermost symbol and then deploy the ViewApp.

IMS-1989484 After galaxy migration, if a linked symbol information is unavailable, the layout validator cannot process the linked symbol. This can result in the layout in warning state. Immediately connecting to the galaxy will display a warning state and empty symbol preview for the specific unprocessed linked symbol.

Workaround: After the migration completes, connect to the galaxy and open the layout in warning state. Identify the symbols showing empty previews, validate those symbols only, then validate the layout to resolve the issue. You do not need to validate all symbols, only those symbols with missing previews in the layout.

IMS-1989662 Some alarm field localizations might not appear in the Alarm Control in InTouch HMI and AVEVA OMI when running in **Historical Alarms and Events** client mode.

When running the Alarm Control, either as an embedded symbol in InTouch HMI or in AVEVA OMI, or as an AlarmApp in AVEVA OMI configured to run in **Historical Alarms, Historical Events, or Historical Alarms and Events** modes, some alarm field localizations may not load even if present in the galaxy translation files. This occurs when the control is configured to display alarms from the History Blocks database. Following are the known cases (Alarm/Event types) where the localizations fail to load at runtime:

1. For user write operations (User.Write) and events, the AlarmComment field is only partially localized in an Alarm App configured to view **Historical Alarms and Events.**

2. For a Boolean alarm (Alarm.Set, Alarm.Clear) events, the AlarmComment, Limit and Value field localizations are not displayed in an Alarm App configured to view **Historical Alarms and Events,**.

3. For Boolean write operations from an I/O reference (Application.Write) events, the AlarmComment and Value field localizations are not displayed in an Alarm App configured to view **Historical Alarms and Events**.

IMS-1991749 After installing and configuring System Platform 2023 or rebooting the system, the following message will be logged in the Operations Control Logger, "AnnounceOnline could not announce to local discovery service due to communication error," when the InTouchIDataService is unable to connect to the Discovery Service. This can occur if the InTouchIDataService starts before the Local Discovery Service. This message will not be logged after the Discovery Service starts. There is no functional loss once all services have started.

IMS 2918856 In some cases, in the OMI web client, the Trend Pen graphic element and the HistoricalTrendApp OMI ViewApp cannot retrieve historical data. There are two reasons for this:

- The Historian Server node name and port are not set in the application settings file for the proxy server on the WebViewEngine platform.
- The Historian Server does not use the security certificate from the System Management Server. This means the web client does not have a trust relationship with the Historian Server and will not accept data from it.

Perform workaround 1 to correct the first issue. For the second issue, perform one of the two procedures in workaround 2.

Workaround 1: Update the application settings file for the WebViewEngine:

1. On the WebViewEngine node, in a text editor, open the file **C:\Program Files (x86)\Common Files\ArchestrA\Services\proxyserver\appsettings.json**.
2. Find this section of the file:

```
"history-data": {
        "HttpRequest": {
          "Version": "1.1",
          "VersionPolicy": "RequestVersionExact"
        },
        "Destinations": {
          "destination1": {
            "Address": "https://localhost:32573/"
```

3. Change `localhost` to the name of the node where the Historian Server is installed. If Historian is not using the default port of 32573, also set the correct port number. Save and close the file.

Workaround 2: To fix the security certificate issue, you have two choices.

- Install a certificate on every remote node that will use the OMI web client. You do not need to shut down or disable the Historian to do this, but each node or remote device must have the certificate installed before it can use the OMI web client.
- Change the Historian Server node to use the certificate of the System Management Server. You need to shut down and disable the Historian during the change, but this method requires changes only on the Historian Server node.

Decide on the method you wish to use and follow the appropriate procedure below. You need to follow **only one** of these procedures.

To install the certificate on a Windows node or remote device:

Note: Depending on your organization's network configuration, your IT department may be able to install the certificate on all devices remotely. Users would not then need to perform this procedure.

1. On the web client node, in a supported web browser, go to `https://<historian_node>:32573/`.

   (If the Historian is not using the default port of 32573, use the Historian port number for your installation.)
2. Select the **Not secure** message, then, in the dialog box that opens, select **Certificate is not valid**.
3. On the **Certificate Viewer** dialog box, on the **Details** tab, under **Certificate Hierarchy**, select the line that ends in **... CA**. Select **Export**.
4. Save the certificate to a file. You can place it in any folder and give it any name, but do not change the file type.
5. Install the certificate. You can do this either by executing the certificate file you just created, or by opening the Windows Certificate Manager from the Start menu. Once you have started the process, follow the wizard prompts and place the certificate in the Trusted Root Certification Authorities store.
6. Close and re-open the browser. You should now be able to open the OMI web client, start the VIewApp, and see historical data.

Note: For remote devices which use an operating system other than Windows, see the manufacturer's instructions for installing a certificate.

To change the certificate on the Historian Server node:

1. On the Historian Server node, use the OCMC to stop and disable the Historian:
   a. Start the OCMC and expand the **Historian** node in the left pane until you see the Historian Server node name.
   b. Expand the node name. Right-click **Management Console**, select **All Tasks**, and select **Shutdown (and disable) Historian**.
   c. On the **Shutdown and Disable Historian** dialog box, make sure the node name is correct and select **OK**.
2. From the Windows start menu, select **AVEVA**, then **Configurator**.
3. Under **AVEVA Historian**, select **Server**. Select **Rest Configuration**.

   The **Rest Configuration** dialog box opens.

4. For **Certificate Source**, select **Provided by IT**.
5. In **Certificate**, select `<hostname> ASB`, where *<hostname>* is the name of the node where the Historian Server is installed.
6. Select **OK**, then select **Configure**.
7. Select **Close** to close the Configurator.
8. In the OCMC, restart the Historian:
    a. Expand the Historian node again.
    b. Right-click **Management Console**, select **All Tasks**, and select **Enable (allow to run) Historian**.

IMS 2968494	Basic translation is supported for trend controls using an SQL connection. This translates the descriptions of tags as well as the user interface of the trend control. However, you can more fully use the translation capabilities to the trend control by connecting to the Historian using the REST oData interface. Using the REST oData interface expands the translation capabilities to include the translation of descriptions, engineering units and Boolean on/off messages.

AVEVA Industrial Graphic Editor Issues

Issue Number	Description
IMS 2003461	In the Industrial Graphic Editor, the largest allowable X and Y co-ordinates for a graphic element are 4096. You cannot position the top-left corner of a graphic element--such as a rectangle, an Industrial Graphic, or an image--beyond that location. However, you can define graphic elements that extend to the right of or lower than this limit. These elements may extend past the visible part of the Graphic Editor canvas, but will still appear correctly if you place the graphic in a layout pane. You also cannot enter a value higher than 4096 for the width or height of a graphic element. As a workaround, you can exceed this limit by selecting the element and using the sizing handles to expand it to the size you want.

InTouch HMI Issues

The following known issues are in addition to those documented in the InTouch HMI Readme.

Issue Number	Description
-	On a fresh installation of System Platform 2023, you may notice the following issues related to Secure Suitelink Connection: • The Suitelink client does not connect to the WindowViewer • The Web Client does not bind to InTouch tag. • When WindowViewer is launched, the system displays the SuiteLink error message in the Logger. **Workaround:** To ensure connectivity between the Suitelink client and the WindowViewer: • Enable System Management Server in the Configurator. • Configure Secure Suitelink connection (V3). • Enable Unsecure Suitelink connection (V2) fall back. For more information, see *Configuring a Secure Suitelink Communication* in the AVEVA InTouch HMI Help.
1928318	When the Supertag instances are created by importing from a .CSV file, the imported Supertags are not displayed in the Supertags pane of the WindowMaker. **Workaround:** The Supertag instances created by importing from a .CSV file can be viewed in the tag dictionary.
IMS 1488851	Post-upgrade from InTouch HMI 2017 U3 SP1 to InTouch HMI 2020 R2 SP1, the following warning message is logged in the LogViewer: “Unable to start the aaServiceHost Could not load file or assembly 'PCS.Client.Discovery, Version=1.3.1.0, Culture=neutral, PublicKeyToken=23106a86e706d0ae' or one of its dependencies. The system cannot find the file specified.” This has no functional impact. However, restarting the system will resolve the message.
IMS 2886663	After you upgrade PCS from 7.0.1 to 8.0, InTouchDataService continually writes warning messages to the logger. These messages occur, on average, about every 30 seconds.

	There is no loss of functionality from this issue. Other than generating the warning message, InTouchDataService continues to operate normally.
IMS 2917871	After an upgrade, if InTouch and Historian are installed on the same node, InTouch ViewApps published to AVEVA Insight may not show tag data. This is because an XML configuration file for the ViewApp is inadvertently deleted during Historian configuration. **Workaround**: Republish each affected InTouch ViewApp.
IMS 2968494	Basic translation is supported for trend controls using an SQL connection. This translates the descriptions of tags as well as the user interface of the trend control. However, you can more fully use the translation capabilities for the trend control by connecting to the Historian using the REST oData interface. Using the REST oData interface expands the translation capabilities to include the translation of descriptions, engineering units and Boolean on/off messages.

InTouch Access Anywhere Issues

The following known issue is in addition to those documented in the InTouch Access Anywhere Readme.

Issue Number	Description
TFS 1280717	InTouch Access Anywhere cannot be removed through the **Modify** workflow. An error message is displayed that states, "To install this product, please run Setup.exe. The setup will now exit." **Workaround:** Select the **Remove** workflow, instead of Modify, from the Maintenance dialog. This successfully deletes InTouch Access Anywhere and its components.

Licensing Issues

Issue Number	Description
TFS 1300491	Activating OI Gateway consumes a license even though OI Gateway does not require a license unless the MQTT component has been configured and is in use. **Workaround:** Reserve a license for each Communication Driver (OI Server) that requires a license. No licenses will then be available because they are reserved to other Communication Drivers. When OI Gateway is activated but not using MQTT, no license will be consumed by OI Gateway. OI Gateway will run without interruption.
TFS 1241116	MES 2017/2017 R2 may not acquire a trial license when installed with System Platform 2020. This is due to a file path name change for the TrialLicensePool that is part of the System Platform 2020 release. This issue only occurs if you are using a trial license. For both MES 2017 and MES 2017 R2, the file path for the TrialLicensePool folder is: C:\ProgramData\Schneider Electric\Licensing\TrialLicensePool For System Platform 2020, the file path for the TrialLicensePool folder is: C:\ProgramData\AVEVA\Licensing\TrialLicensePool **Workarounds:** Use one of the following workarounds. • If only the file path "C:\ProgramData\Schneider Electric\Licensing\TrialLicensePool" is on your system, change the name of the "Schneider Electric" folder in the file path to "AVEVA." No other change is needed. • If both file paths exist on your system, copy the trial license from "C:\ProgramData\Schneider Electric\Licensing\TrialLicensePool" to "C:\ProgramData\AVEVA\Licensing\TrialLicensePool." No other change is needed If the AVEVA License Manager is open while you are moving the license file or renaming the file path, you may see a series of error messages. However, these will clear once the trial license is acquired. You can avoid this by closing the License Manager prior to renaming or moving the file.
TFS 793643	If you have not set a default browser, and you install System Platform with AVEVA Enterprise licensing selected, clicking the AVEVA Enterprise License Manager shortcut does not open the License Manager in the browser as it should. Instead, the shortcut opens in Windows Explorer. From Windows Explorer, you cannot open License Manager (the OK button is inactive). **Workaround:** Follow the instructions for your operating system to set the default browser, and then open the AVEVA Enterprise License Manager from the shortcut, **or**: Open your browser and copy the shortcut link, http://localhost/AELicenseManager, directly into the browser's address bar.
TFS 779958	When the same license is acquired on both a local node and in an RDP session that originates from the same node, the License Manager may not show all the licenses that have been acquired. This occurs even though the licenses are counted properly on the license server. The license count that you see applies only to the node you are viewing. Thus, once you reach your maximum number of licenses, you will not be

able to acquire additional licenses, even though the license manager may indicate that more licenses are available.

System Monitor Issues

The following known issues are in addition to those documented in the AVEVA System Monitor Readme.

Issue Number	Description
1436013	Email alerts cannot be sent through secured SMTP.
1511692	Post Install -> Reboot, ASM has an alert that Bootstrap is not running that does not update to show Bootstrap IS running. **Workaround:** Resolve the Bootstrap alert. It will not shows the incorrect status again.

AVEVA Alarm Control Issues

If you create a filter for a history block query that results in no matches, "Not Connected" appears in the status bar and a warning is logged in the Logger. The status bar should show "Connected" even though no matches are returned.

AVEVA Edge Co-Existence Issues

AVEVA Edge is not a component product of System Platform, but is sometimes installed with it.

Issue Number	Description
TFS 1342283	If you attempt to upgrade a computer to System Platform 2020 R2 from System Platform 2020, and AVEVA Edge 2020 is installed on the same computer, an error message may be displayed that warns of an incompatibility. This will occur during the upgrade if certain registry values are incorrect, and the upgrade installation will be blocked. **Workaround:** Use regedit to enter the correct registry values. Location: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\ArchestrA\Framework 1. Change the value of InstallPath to “C:\Program Files (x86)\ArchestrA\Framework\” (add the final backslash character) 2. Change the value of TargetInstallPath to “C:\Program Files (x86)\ArchestrA\” (add “ArchestrA\”)

Documentation

Most System Platform help documents are provided as PDF and web help documents.

- The System Platform Installation Guide is located in the root folder of the installation DVD.
- Use the Start Menu to access Application Server, InTouch HMI, Historian, and other System Platform PDF documents in the AVEVA Documents folder.
- Online help can be viewed in your browser using the AVEVA Products Help Viewer.
    - To launch the Help Viewer from the Windows Start menu, select **AVEVA**, then select **AVEVA Help**.
    - The Online Help can also be accessed directly from the various System Platform applications, including Application Server (System Platform IDE), InTouch HMI (WindowMaker), and Historian.