AVEVA™
ArchestrA Protocols User's Guide

Publication date: Tuesday, December 1, 2020

Contact Information

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

https://sw.aveva.com/

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

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

Contents

Chapter 1 Welcome 5
Documentation Conventions 5
Technical Support 5
Chapter 2 Supported Protocols 7
Supported Protocols Secure SuiteLink 7
SuiteLink Features 7
Secured SuiteLink Connection 7
Configuring the System Management Server 9
System Requirements for SuiteLink 11
Time Stamping 12
DDE/FastDDE 12
DDE 12
FastDDE 13
ArchestrA Message Exchange 13
OPC 13
OPC UA 13
MQTT 14

CHAPTER 1

Welcome

This guide provides background information on the primary communication protocols used between different components.

A protocol is a set of rules and standards for enabling computers to connect and exchange data over a network.

This guide includes information on setting up and using some of these protocols.

You can view this document online or you can print it, in part or whole, by using the Adobe Acrobat Reader's print facility.

Documentation Conventions

This documentation uses the following conventions:

Convention	**Used for**
Initial Capitals	Paths and file names.
Bold	Menus, commands, dialog box names, and dialog box options.
`Monospace`	Code samples and display text.

Technical Support

Before you contact Technical Support, refer to the relevant section(s) in this documentation for a possible solution to the problem. If you need to contact technical support for help, have the following information ready:

- The type and version of the operating system you are using. For example, Microsoft Windows XP, SP1.
- Details of how to recreate the problem.
- The exact wording of the error messages you saw.
- Any relevant output listing from the Log Viewer or any other diagnostic applications.
- Details of what you did to try to solve the problem(s) and your results.
- If known, the Technical Support case number assigned to your problem, if this is an ongoing problem.

CHAPTER 2

Supported Protocols

Secure SuiteLink

Secure SuiteLink uses a TCP/IP based communication protocol. It is designed specifically to meet industrial needs, such as data integrity, high throughput, and easier diagnostics. This protocol standard is supported on Microsoft Windows NT 4.0 or later.

Secure SuiteLink is not a replacement for DDE, FastDDE, or NetDDE. Each connection between a client and a server depends on your network situation.

SuiteLink Features

SuiteLink is designed specifically for high speed industrial applications and provides the following features:

- Value Time Quality (VTQ) places a time stamp and quality indicator on all data values delivered to VTQ-aware clients.
- Extensive diagnostics, including server loading, computer resource consumption, and network transport, are made accessible through the Microsoft Windows NT operating system performance monitor. This feature is critical for the maintenance of distributed industrial networks.
- Consistent high data volumes can be maintained between applications when applications are on a single node or distributed over a large node count.
- The network transport protocol is TCP/IP using Microsoft's standard WinSock interface. You do not have to create shares for SuiteLink I/O Servers.

Secured SuiteLink Connection

To ensure a higher level of confidentiality and privacy, SuiteLink communication between a SuiteLink server and a SuiteLink client can now be encrypted. For the SuiteLink server and client to use encrypted communication, the ASB Runtime Components feature must be selected in the SuiteLink 3.0 installation.

Configuring a Secure SuiteLink Connection

Follow the steps described below to configure a secure SuiteLink connection.

Step 1: Set up and Register with the System Management Server

a. **Setting up the Management Server:** A computer with the application environment is designated as the System Management Server. The system management server node holds and distributes the security related information to the other nodes in the environment. The security information is in the form of server certificates.

b. **Registering with the System Management Server**: All the nodes which needs to securely communicate with one another will have to register with the management server node. All the nodes registered with the management server node is grouped together, and can communicate securely with one another.

Use the Configurator to configure the ASB Management Server point to the Management Server on the GR node. For additional information, refer the section *Configuring Machine Trust* in the OI Core Communications Driver Help.

Step 2: Server Initialization

To ensure interoperability, the SuiteLink infrastructure continues to support and allow both encrypted and non-encrypted communication.

The table below describes the communication between the applications using the encrypted and/or non-encrypted SuiteLink protocol. Consider the communication between the encrypted/non-encrypted Client (say, InTouch) with the encrypted/non-encrypted Server (say, OI Server).

SuiteLink (SL) Communications	Encrypted Client	Non-encrypted Client
Encrypted Server	Secure, encrypted	Not secure, not encrypted
Non-encrypted Server	Not secure, not encrypted	Not secure, not encrypted

If the authentication fails between the Client and the Server, or if the Client or Server do not have access to the Certificate store, the system continues with the non-encrypted connection as a fallback.

Accessing Server as a Standard User

When accessing the server as a standard user, you cannot establish a secure SuiteLink channel. For a secure, encrypted communication workflow, the standard user should be added to the 'ArchestrAWebHosting' user group on the server side.

For more information about adding users to user-groups, refer to the Windows-specific documentation.

Step 3: Establishing the secure communication channel

Using the configuration performed with the above steps, the server and client will establish an encrypted SuiteLink connection. If an error is encountered during any of the above steps, the connection is terminated either by the Client or the Server.

SuiteLink Install/Upgrade Scenarios

Current Version	Install/Upgrade Process	Version upgrading to	Notes
Prior to WSP < WSP 2017 Update 3 *Unencrypted*	Upgrade using WSP 2017 Update 3 Install	WSP 2017 Update 3 *Encrypted*	The SuiteLink component is installed silently, and is active. Use the Configurator to manage certificates.
OI Core 1.x., 2.x *Unencrypted*	a) Upgrade using OI Core 3.0 install	OI Core 3.0 *Unencrypted*	This is a standalone SuiteLink install. First, upgrade to OI Core 3.0. Then, install the Secure SuiteLink and PCS 4.3 components. Use the Configurator to manage certificates.
	b) SuiteLink 3.0 install	OI Core 3.0 + PCS 4.3 *Encrypted*	

Configuring the System Management Server

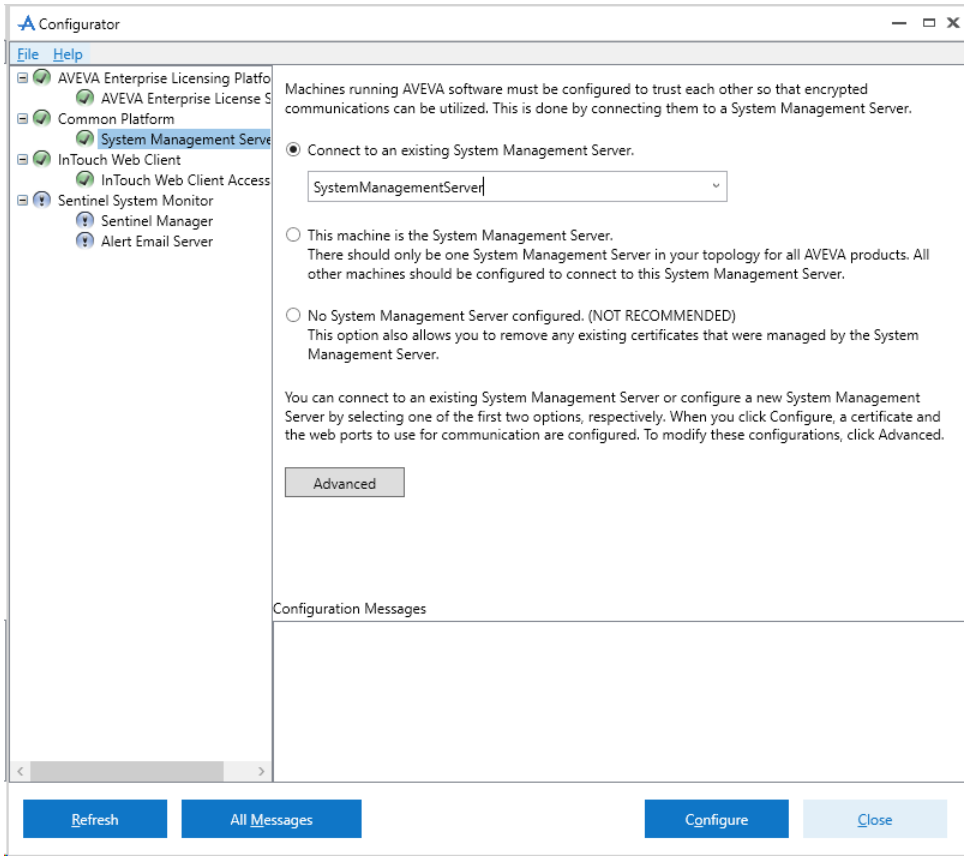
System Platform 2017 Update 3 incorporates new security measures, including support for the TLS 1.2 protocol for secure encrypted communications between nodes, single sign on (SSO), and certificate management. These features are enabled through a component of the ASB Runtime called the **System Management Server**. To enable security, every System Platform node must communicate with the System Management Server, and there should only be a single System Management Server in your System Platform topology. The System Management Server stores shared security certificates and establishes a trust relationship between machines.

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

To configure the System Management Server

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

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

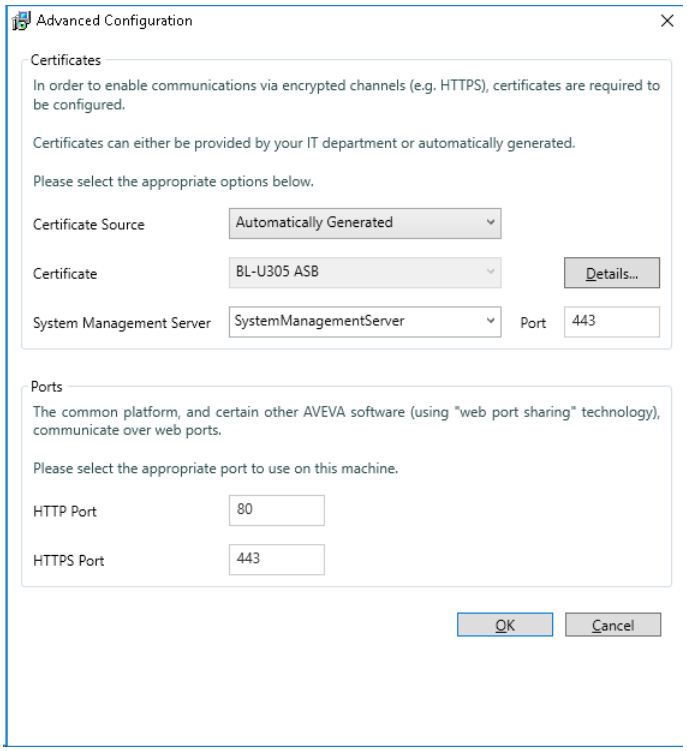


Note: The Configurator is automatically invoked when installation completes. You can also start the Configurator at any time after from the Windows Start menu on any System Platform node.

2. You are presented with three choices:

- **Connect to an existing System Management Server:** This is the default option. The System Platform discovery service looks for any existing System Management Servers on its network. If any are found, they will be displayed in a drop down list. Select the server you want to use, or enter the machine name of the server. All computers in your System Platform topology should connect to the same server.
- **This machine is the System Management Server:** Select this option if this computer will be the System Management Server. All other computers in your System Platform topology should the be configured to connect to this server by using the **Connect to an existing System Management Server** option.
- **No System Management Server configured. (NOT RECOMMENDED):** Select this option to set up your computer without encryption and secure communications. You can still configure other computers in the topology to use a System Management Server.

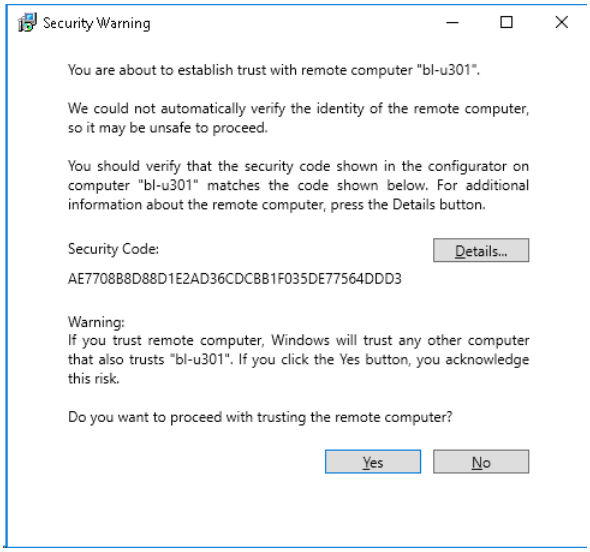
3. **Advanced settings:** This opens the **Advanced Configuration** dialog window.



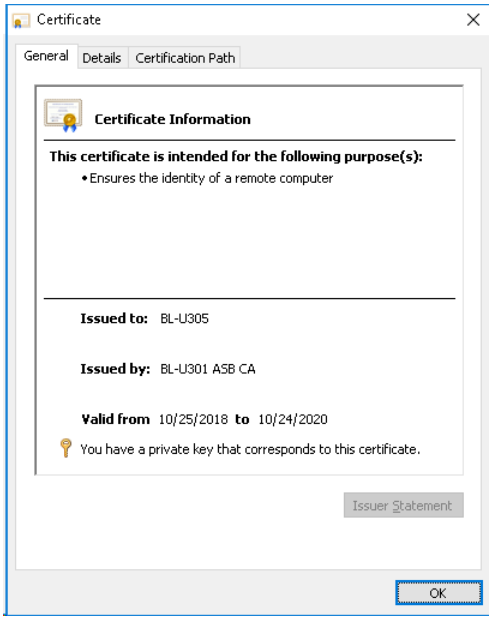
- **Certificate Source:** Select either **Automatically Generated** (default), or **Provided by IT.** If your IT department is providing the certificate, press the **Import** button and navigate to the certificate file. For more information, see Import a Certificate.

  Certificate: The certificate name is displayed. If you imported a certificate, you view it by pressing the **Details** button. The certificate is periodically renewed through an automatic update process, both on the server node and on remote nodes.
- **System Management Server:** If you are connecting to an existing System Management Server, the name and port number of the server you selected is shown.
- **Common Platform Ports:** The ports for the common platform are used for communications with certain AVEVA software, such as the Sentinel System Monitor. Generally, you can use the default settings. Remote nodes must be configured with the same port numbers as configured here. Click the **Advanced** button, then edit the port numbers as needed.
  Default HTTP port: 80
  Default HTTPS port: 443

4. Press the **Configure** button. A Security Warning window is displayed:



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



5. Select the next item in the left pane that requires configuration. When all required items have been configured, press the **Close** button to complete installation. See System Restart after Configuration.

System Requirements for SuiteLink

This section describes the hardware, software, and installation requirements for SuiteLink.

Hardware Requirements

The following is a list of the hardware required to run the SuiteLink component.

- Computer with 2 gigahertz (GHz) or higher processor clock speed.

- 1 gigabyte (GB) of RAM or higher (512 MB minimum supported; may limit performance and some features).
- 8 gigabytes (GB) of available hard disk space.

Software Requirements

The following is the list of the software required to run the SuiteLink.

- Windows XP SP3 Professional edition (32-bit).
- Windows 2003 SP2 Standard and Enterprise editions (32-bit).
- Windows Vista SP2 Business and Ultimate editions (32-bit and 64-bit).
- Windows 2008 SP2 Standard and Enterprise editions (32-bit and 64-bit).
- Windows 2008 R2 SP1 Standard and Enterprise editions (64-bit).
- Windows 7 SP1 Professional and Ultimate editions (32-bit and 64-bit).

Microsoft Internet Explorer 6.0 or later is recommended on the computer where the product is installed.

Installation Requirements

The following installation requirements are prerequisites for the SuiteLink to work properly:

- Local administrator privileges are required to install the update.
- Microsoft WoW64 emulation component must be available on any 64-bit platform.

Time Stamping

SuiteLink allows for the passing of time stamping information with process data. The SuiteLink time stamp is a 64-bit data structure representing the number of 100-nanosecond intervals since January 1, 1901 in Greenwich Mean Time. This matches the Microsoft FILETIME specification. Conversion to and from local time is the responsibility of the application layer. All time stamps carried in the SuiteLink protocol are in GMT.

DDE/FastDDE

The DDE/FastDDE communication protocols allow communication between a client and a server. Dynamic Data Exchange (DDE) protocol is developed by Microsoft whereas FastDDE protocol is proprietary to Wonderware. For DDE/FastDDE communications the OI Server must be activated in Desktop mode (must start from command line).

DDE

DDE is a communications protocol that allow applications in the Windows environment to send/receive data and instructions to/from each other. It implements a Client-Server relationship between two concurrently running applications.

The server application provides data and accepts requests from any other application interested in its data. Requesting applications are called clients. Some applications such as InTouch and Microsoft Excel can simultaneously be both a client and a server.

Note: On Windows Vista and later operating systems, Local DDE is supported only when the OI Server is activated from its executable file or launched from InTouch. Local DDE is not supported when the OI Server is activated from the SMC.

FastDDE

FastDDE provides a means of packing multiple DDE messages into a single message. This packing improves efficiency and performance by reducing the total number of DDE transactions required between a client and a server.

Although FastDDE has extended the usefulness of DDE for our industry, this extension is being pushed to its performance constraints in distributed environments.

ArchestrA Message Exchange

Message Exchange is a proprietary communication protocol used by the ArchestrA infrastructure. It provides data communication across ArchestrA's object-based system.

OPC

OPC (originally OLE for Process Control, now Open Platform Communications) is a non-proprietary set of standard interfaces based on Microsoft's OLE/COM technology. This standard makes possible interoperability between automation/control applications, field systems/devices, and business/office applications.

Avoiding the traditional requirement of software/application developers to write custom drivers to exchange data with field devices, OPC defines a common, high-performance interface that permits this work to be done once, and then easily reused by HMI, SCADA, control, and custom applications.

Over a network, OPC uses DCOM (Distributed COM) for remote communications.

OPC UA

OPC Unified Architecture (OPC UA) is an industrial machine-to-machine communication protocol for interoperability. It provides process control with enhanced security, advanced communication, security, and information models, and cross-platform connectivity.

OPC UA is implemented as a client in OI Gateway.

OPC UA differs significantly from OPC. The following provides the key differences between classic OPC and OPC UA.

Classic OPC	**OPC UA**
Uses the COM/DCOM technology of Microsoft to communicate. It does not have configurable time-outs. It depends on the DCOM time-out, which is configured in the system.	Uses a services architecture to export data, which improves the ease of communication and connectivity.
Is dependent on Windows operating systems.	Is platform independent and can connect to a wide variety of devices and platforms.
Has limited security.	Has built-in security.
No built-in capabilities to handle problems, such as lost messages.	Has built-in capabilities to handle problems, such as lost messages.

MQTT

MQTT, formerly called Message Queuing Telemetry Transport, is a publish/subscribe messaging protocol for use over TCP/IP. MQTT is designed to ensure that devices can communicate with each other while minimizing power and bandwidth requirements. It is a simple messaging protocol that is well-suited for use with devices that rely on slow or unreliable networks.

The MQTT protocol is an application layer specification, and has been published as standard ISO/IEC PRF 20922. MQTT uses a Publish-Subscribe mechanism which requires a mediating broker. The publishers send data to the broker, and subscribing clients receive data published to the broker. Only clients that have subscribed to a particular topic receive messages about that topic. The protocol supports bidirectional communication such that a device that is a publisher can also receive updates.