



AVEVA™
Protocols User Guide

© 2022 AVEVA Group plc and its subsidiaries. All rights reserved.

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

Although precaution has been taken in the preparation of this documentation, AVEVA assumes no responsibility for errors or omissions. The information in this documentation is subject to change without notice and does not represent a commitment on the part of AVEVA. The software described in this documentation is furnished under a license agreement. This software may be used or copied only in accordance with the terms of such license agreement.

ArchestrA, Avantis, Citect, DYNsIM, eDNA, EYESIM, InBatch, InduSoft, InStep, IntelaTrac, InTouch, OASyS, PIPEPHASE, PRISM, PRO/II, PROVISION, ROMeo, SIM4ME, SimCentral, SimSci, Skelta, SmartGlance, Spiral Software, WindowMaker, WindowViewer, and Wonderware are trademarks of AVEVA and/or its subsidiaries. An extensive listing of AVEVA trademarks can be found at: <https://sw.aveva.com/legal> <https://sw.aveva.com/legal>. All other brands may be trademarks of their respective owners.

Publication date: Friday, June 10, 2022

Contact Information

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

<https://sw.aveva.com/>

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

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

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

Contents

Chapter 1 Welcome 4

Documentation Conventions4

Technical Support4

Chapter 2 Supported Protocols 5

SuiteLink.....5

 SuiteLink Features 5

 Secured SuiteLink Connection..... 5

 Common Platform 7

 Hardware and Software Requirements..... 8

 Time Stamping..... 8

DDE, FastDDE, and NetDDE8

 DDE 8

 FastDDE 9

Message Exchange9

OPC9

OPC UA.....9

MQTT10

Chapter 1

Welcome

This guide provides background information on the primary communication protocols used between components of AVEVA products, formerly Wonderware.

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.

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

AVEVA Technical Support offers a variety of support options to answer any questions on AVEVA products and their implementation.

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, Windows 10 version 1903, 64-bit.
- 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

The following section lists the supported protocols.

SuiteLink

SuiteLink uses a TCP/IP based communication protocol. SuiteLink 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.

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 nodes which needs to securely communicate with one another will have to register with the management server node. All nodes registered with the management server node are 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 Core Communication Drivers 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 <i>Unencrypted</i>	Upgrade using WSP 2017 Update 3 Install	WSP 2017 Update 3 <i>Encrypted</i>	The SuiteLink component is installed silently, and is active. Use the Configurator to manage certificates.
OI Core 1.x., 2.x <i>Unencrypted</i>	a) Upgrade using OI Core 3.0 install	OI Core 3.0 <i>Unencrypted</i>	This is a standalone SuiteLink install. First, upgrade to OI Core 3.0. Then, install the Secure SuiteLink and PCS 4.3 components.
	b) SuiteLink 3.0 install	OI Core 3.0 + PCS 4.3 <i>Encrypted</i>	Use the Configurator to manage certificates.

Common Platform

Common Platform services include the **System Management Server (SMS)**. The SMS is used to implement important security measures for System Platform 2023. These include:

- Setting port numbers for inter-node communications: See Ports Tab for more information.
- Setting the SuiteLink security mode and user access to the AVEVA Network Message Exchange.
 - Communication over a SuiteLink connection can be configured to use only encrypted (secure) communications, or to allow unencrypted communications, if a secure (TLS) connection cannot be established. SuiteLink is used for a number of different applications in System Platform.
 - The AVEVA Network Message Exchange (NMX) is an application communication protocol that leverages a DCOM-based transport mechanism for communication between nodes.

For information about configuring SuiteLink security and NMX access, select the Advanced Configuration button and go to the Communications Tab.

- Certificate management: See Import a Certificate for more information.
- User authentication via the OpenID connect standard, which allows single sign on (SSO) via an external identity provider. See Authentication Provider Configuration for more information.

To enable security, every System Platform node must communicate with the System Management Server. There should only be one System Management Server in your System Platform topology, otherwise, communication disruptions may occur. The System Management Server stores shared security certificates and establishes a trust relationship between machines. You can configure one additional node as a redundant SSO server, which functions as a backup for single sign-on if the System Management Server cannot be reached.

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

For more information about configuring the System Management Server with an authentication provider, see *Designing a Robust SSO System with an External Authentication Provider*.

Hardware and Software Requirements

You must have the following installed to use SuiteLink for data communications.

- Windows NT 4.0 or later
- TCP/IP installed and configured

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, and NetDDE

The DDE protocols used by AVEVA products are DDE, FastDDE, and NetDDE.

DDE

Dynamic Data Exchange (DDE) is a Microsoft communications protocol that lets applications in the Windows environment send/receive data and instructions to/from each other. DDE 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: InBatch does not support DDE/NetDDE connections to the I/O Servers, including InControl. For those connections, SuiteLink must be used.

Requests for data can be one of two types: one-time requests or permanent data links. With one-time requests, the client program requests a "snapshot" of the desired data from the server application. An example of a one-time request is a program, such as Excel, running a report-generating macro. The macro opens a channel to another application, requests specific data, closes the channel, and uses the data to generate the report.

Permanent data links are called "hot links." When a client application sets up a hot link to another application it requests the server application to notify the client whenever a specific item's data value changes. Permanent data links remain active until either the client or server program terminates the link or the conversation. Permanent data links are a very efficient means of exchanging data because, once the link has been established, no communication occurs until the specified data value changes. System Platform components can use DDE to communicate with I/O device drivers and other DDE application programs.

FastDDE

FastDDE provides a means of packing many AVEVA DDE messages into a single Microsoft DDE message. Message packing improves efficiency and performance by reducing the number of DDE transactions required between client and server.

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.