Aspen InfoPlus.21 OPC UA Server

User's Guide

Version: V14.3 May 2024

Aspen Technology, Inc.
20 Crosby Drive
Bedford, MA 01730
USA
Phone: + (781) 221-6400
Toll Free: (1) (888) 996-7100
http://www.aspentech.com

Contents

1 Overview

AspenTech provides an OPC UA compliant server-side component known as the Aspen InfoPlus.21® OPC UA Server. The InfoPlus.21 OPC UA Server allows OPC UA compliant client applications to exchange data with InfoPlus.21 (IP21). See the "2 Concepts" chapter for more details.

UA stands for "Unified Architecture," which is a technology developed by the OPC Foundation. The OPC Foundation is an organization that maintains open standards for open connectivity in industrial automation and the enterprise systems that support industry. Interoperability is assured through the creation and maintenance of open standards specifications.

This manual provides information required by personnel responsible for the installation and maintenance of InfoPlus.21 systems that communicate with OPC UA clients. The reader is expected to have a working vocabulary of both InfoPlus.21 and OPC UA terminology.

The InfoPlus.21 UA Server may be configured to perform the operations listed below to meet the requirements of an installation. The capabilities may be limited by a particular OPC UA client.

Get Data

InfoPlus.21 UA Server allows UA clients to get values contained in an InfoPlus.21 database. It supports reading current and historical values. OPC UA subscriptions may be defined to acquire data on value change notifications.

Note: InfoPlus.21 OPC UA does not support percent deadbands. Percent deadbands apply only for variables having a EURange Property, which currently is not configurable. Absolute deadbands do not require the EURange Property and are supported by AspenTech's OPC UA server.

Put Data

InfoPlus.21 UA Server allows UA clients to change values in an InfoPlus.21 database.

Access Control

It supports access control integrated with Windows user authenticated when the security feature is enabled in InfoPlus.21.

2 Concepts

General Concepts

Here are some general concepts regarding the InfoPlus.21® OPC UA Server.

- It is based on the UA standard as published by the OPC Foundation.
- It leverages the UA SDK developed by the OPC Foundation.
- It delivers a subset of the complete functionality proposed by the UA standard.
- It allows a client application to discover, connect, read, and write data to/from InfoPlus.21.
- It registers itself into the standard UA Discovery Server, thus allowing it to easily be discovered by client applications.
- It supports event-driven subscriptions to data changes.
- It supports reading historical data from InfoPlus.21.

OPC UA Stack

The InfoPlus.21 OPC UA Server uses V1.04 .Net-based OPC UA Stack & SDK from the OPC Foundation. The V1.04 OPC UA Stack & SDK from the OPC Foundation is based on OPC UA Specification V1.04. Please refer to the OPC Foundation website for more details on OPC UA Specification V1.04.

Advanced Concepts

Here are some advanced concepts regarding the InfoPlus.21 OPC UA Server.

- It supports the UA security model, such as tamperproof encrypted client-server communications. To learn more, please see "**Message Security in OPC UA**," later in this chapter.
- It complies with the InfoPlus.21 security model by impersonating the client-side user account when accessing InfoPlus.21.
- It provides two means for working with data, DA and RAW. For more, please see "**Choosing a Tag Folder**," later in this chapter.

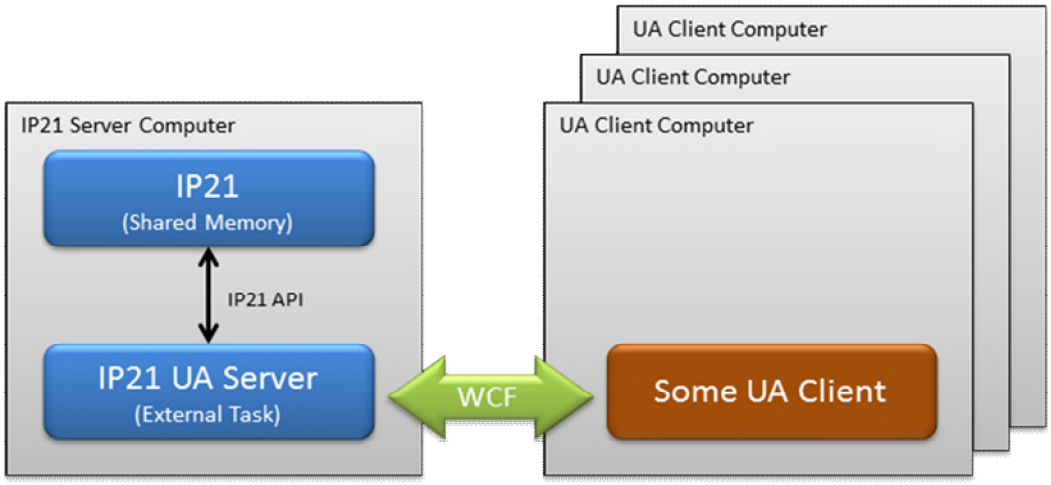
- It can communicate via OPC.TCP protocol.

Architecture

The InfoPlus.21 UA Server is a set of software components that allow InfoPlus.21 to exchange data with OPC UA compliant clients. The components are delivered as .NET framework assemblies and are developed in either the C# or C++ language. The components that facilitate this feature are delivered in the form of executable modules known as "assemblies" in the lingo of Microsoft .NET development. The assemblies are comprised of both dynamic link libraries (DLLs) and executables (EXEs).

The IP21OpcUAServerHost.exe is an InfoPlus.21 Task Service that automatically runs when InfoPlus.21 is started. This means that the InfoPlus.21 UA Server is available immediately by UA client connections.

Below is a depiction of Aspen InfoPlus.21 OPC UA Server architecture.



Message Security in OPC UA

The OPC UA specification supports message security to ensure tamperproof exchange of messages between client and server, including optional encryption of the transferred data. It relies on digital certificates to “sign” each data packet that is exchanged. A digital certificate is a data structure that is created by a certificate authority and can be designated as “trusted” on a computer.

Digital certificates, known as application instance certificates, are created during application installation (or setup) to uniquely identify the application instance. Every OPC UA client and server must have an application instance certificate.

The message security is based on Security Level and Security Policy. The security level and policy determine how all incoming messages are going to be signed and encrypted between the InfoPlus.21 OPC UA Server and the OPC UA Client.

The InfoPlus.21 OPC UA Server is designed to support three levels of message security:

Security Level	Description
None	No signing is performed. The message packet is transmitted in clear text and could be altered in transit, without being detected.
Sign	The message packet is signed such that it will be detected if the message is tampered with in transit. The data is not encrypted; it is transmitted in clear text.
SignAndEncrypt	The message packet is signed such that it will be detected if the message is tampered with in transit. The data is also encrypted; it cannot be deciphered while in transit.

The security policies in OPC UA Specification V1.04 are based on SHA256 hashing algorithms. The InfoPlus.21 OPC UA server supports all SHA256 endpoints shown below:

Security Mode	Security Policy
Sign	Basic256Sha256
Sign	Aes128_Sha256_RsaOaep
Sign	Aes256_Sha256_RsaPss
SignAndEncrypt	Basic256Sha256
SignAndEncrypt	Aes128_Sha256_RsaOaep
SignAndEncrypt	Aes256_Sha256_RsaPss

HTTP endpoints are not supported in OPC UA Specification V1.04, so the InfoPlus.21 OPC UA server will no longer support HTTP endpoints.

When connecting to a UA server, the UA client decides what message security level and policy to use, though some UA servers may not support all levels and policies. During the process of establishing a communication session, the client and server exchange certificates.

If a certificate is rejected by either the client or the server, a communication session is not established. Certificates may be rejected by either party if the certificate is not found in a trusted store, expired, from another computer, or other reasons. The failed trust relationship must be resolved to allow a successful connection. See *Configuring Security Certificates* below to learn about ways to resolve certificates.

After a certificate has been rejected, the InfoPlus.21 UA Server stores rejected certificates in folder:

```
%CommonApplicationData%\OPC Foundation\CertificateStores\RejectedCertificates
```

When attempting to connect to an InfoPlus.21 UA Server, if either Sign or SignAndEncrypt is used, the server will reject the certificate upon the first connection attempt. Usually this is indicated by error 6 2 concepts code BadSecureChannelClosed. A copy of the client-side certificate will be stored in the InfoPlus.21 **Rejected Certificates** folder at path:

```
%CommonApplicationData%\OPCFoundation\CertificateStores\RejectedCertificates
```

Configuring Security Certificates

The OPC UA architecture relies on security certificates to protect data as it is transferred across a network. Depending on the type of OPC UA client or server, it may be necessary to configure the certificates to permit successful communication.

The certificate of the InfoPlus.21 OPC UA server is installed in standard store.

Certificate Name	Certificate Store Type	Certificate Location	Trust List Location
AspenTech InfoPlus21 OPC UA Server	Directory	%CommonApplicationData%\OPC Foundation\CertificateStores\MachineDefault	%CommonApplicationData%\OPC Foundation\CertificateStores\UA Applications

Configuring Certificates – Recommended Method

To allow a UA server to accept future connections from a client, the certificate must be moved from the rejected folder into the trusted UA certificate folder. To do this, use the OPC Foundation's UA Configuration tool (see "**UA Configuration Tool**" on page 23).

A simple way to configure the application instance certificates is to:

1. Attempt to connect to the desired UA server using either the "Sign" or "SignAndEncrypt" message security level. The attempt will fail since the applications do not trust each other, but the certificates will exist in the Rejected Certificates stores.

   Note: If you choose **None**, and the UA Server is configured to support **None**, then there is no need to bother configuring certificates on the server side.

2. On the InfoPlus.21 UA server computer, start the OPC Foundation's UA Configuration tool, then follow these steps:
   - Select the **Manage Security** tab.
   - Select the UA server executable (EXE) file from the **Applications To Manage** drop down. If it does not appear, then perform steps a and b, below, otherwise skip to step 3.
     a. Click the **Find** button, and then navigate to find the executable file where it was installed. For example, the InfoPlus.21 UA Server is named, "IP21OpcUAServerHost.exe" and is found in the folder where the InfoPlus.21 binaries are installed, such as {ProgramFiles}\AspenTech \InfoPlus.21\db21\code. Select the executable file, and then click **Open**.

     b. Click **OK** to close the **Modify Application Information** window that appears afterward.

3. Click **Select Certificate to Trust**, and then select **Directory** from the Store Type drop down.
4. Pick the appropriate rejected certificate store from the Store Path drop down. If it does not appear in the list, then use the Browse button to find this folder and choose it. The InfoPlus.21 UA server uses standard store in:

```
%CommonApplicationData%\OPC Foundation\CertificateStores\RejectedCertificates
```

5 Find the certificate from the client application that was rejected earlier, select it, and then click **OK**.

The client application's certificate is now trusted, so you should be able to successfully connect to the InfoPlus.21 UA Server.

If needed, you can use this same technique to allow a UA client application to trust a server. You will need to use the **Find** button to locate the client application.

Configuring Certificates – Alternate Method 1

There is an alternate, yet cumbersome, method for working with certificates using the Certificate Manager that is available in Microsoft Windows.

1 Launch the Microsoft Management Console. Do this by entering "mmc" in the Start | Run (or in a command window).

2 Choose File | Add/Remove Snap-in, and then choose "Certificates".

3 Click Add, and then use the wizard to create a "Computer account". This will load the computer certificates into the tree.

4 To install a rejected certificate, expand the **UA Application** folder, then right-click **Certificates** to see a context menu.

5 Choose **All Tasks**, then **Import**, and then navigate to the location where rejected certificates are stored on disk. For the InfoPlus.21 UA Server, this would be in:

```
%CommonApplicationData%\OPC Foundation\CertificateStores\RejectedCertificates
```

6 Change the file extension filter of the Open File window to show all files (All Files (*.*)), then choose the desired certificate, which probably has a .DER file extension.

7 Complete the wizard to load the certificate. After this operation, the once rejected certificate is now trusted by the UA client applications.

Configuring Certificates – Alternate Method 2

There is yet another way to configure certificates using the UA Configuration tool. This involves using the **View Certificate** button on **Manage Certificates** tab to find the rejected certificate, then copy it using the **Copy** option right mouse click, and then paste it into the appropriate destination certificate store, using the **Paste** option right mouse click.

Configuring Certificates – Alternate Method 3

Finally, there is yet another way to configure certificates by proactively copying all UA client certificates to the appropriate trusted certificate folder on the InfoPlus.21 UA Server computer. This method is cumbersome, but only needs to be done once and avoids the two-step process of causing a client connection failure, then using the UA Configuration tool to trust the certificate. In this case, you are pre-loading all client certificates so they will be found the first time a client attempts to connect to an InfoPlus.21 UA Server.

Resolving Certificates Automatically

Depending on how a UA client or server was implemented, there might be ways to configure a UA application to automatically handle certificate resolution. For example, client applications that provide a user interface might prompt the user to accept and incoming server-side certificates. Some applications might support the ability to automatically accept incoming certificates, but this risky as it might allow an unintended connection to succeed.

One simple way to auto-accept certificates on a UA server is to modify the UA configuration file to change the rejected folder location to the trusted folder location. Thus, when a client's certificate is rejected, the rejected certificate is copied to the trusted location, thus the next connection attempt should succeed.

Access Control Security

Several levels of access control security are provided by InfoPlus.21 UA server.

Built-in OPC UA Access Control

OPC UA itself provides access control to the following application objects:

Description	Doc References	Page
The UA server's OPC UA configuration file	OPC UA Application Configuration File	16
The UA server's executable file	n/a	n/a
The UA server's certificate	Message Security in OPC UA	4

To configure, click the **Manage Application Permissions** on the **Manage Application** tab on the UA Configuration tool.

If experiencing connection problems, verify the user's access permissions.

Application Specific Access Control

Some UA server vendors may provide their own proprietary access control security within their application. This would control access to objects internal to the server application. For example, InfoPlus.21 has access control features that integrate with the Microsoft Windows authentication. Thus, the InfoPlus.21 UA server also supports this security feature. To use it, the UA client must be configured to pass the user's identity to the server. For details, see "**User Authentication**" on page 16.

If experiencing connection problems, verify the user's access permissions in the UA server.

NodeID

Tags are identified using the NodeID, a unique identifier. The NodeId is a text value. Each tag has a NodeId. The format depends on the UA server.

For example, the NodeId of a value of a tag named ATCAI from the DA folder in InfoPlus.21 UA server might be:

ns=2;b=AAAAAAEAAAAeCAAAAABZdMsDAAA=

NodeId is the standard used by 3rd party OPC UA clients for reading or writing tag values into InfoPlus.21 OPC UA server.

InfoPlus.21 provides a tool named Aspen OPC UA Explorer for reading NodeIds of tags. You can access it through the Start menu.

Third-party tools exist that can help, such as the US Sample Client application provided by the OPC Foundation.

Browse Paths

Some OPC UA clients, like Aspen CIM-IO Interface for OPC UA, can use browse paths as an alternative to NodeId, for reading or writing values into InfoPlus.21 tags. Browse paths are non-localized human readable text values that identify the location of a value in a UA server. The format depends on the UA server, but generally represents a hierarchical path of the form:

```
/Objects/{NamespaceIndex}:nodeLeve1Name/
{NamespaceIndex}:nodeLeve2Name/...
```

For example, the path to a value in an InfoPlus.21 UA server might be:

```
/Objects/2:DA/2:IP_AnalogDef/2:TestRecord/2:Measurement
```

The NamespaceIndex is a number that indicates to which namespace the following node name belongs. OPC UA groups names with namespaces to avoid name clashes.

InfoPlus.21 provides a tool named Aspen OPC UA Explorer for discovering browse paths. You can access it through the Start menu.

Third party tools exist that can help, such as the UA Sample Client application provided by the OPC Foundation.

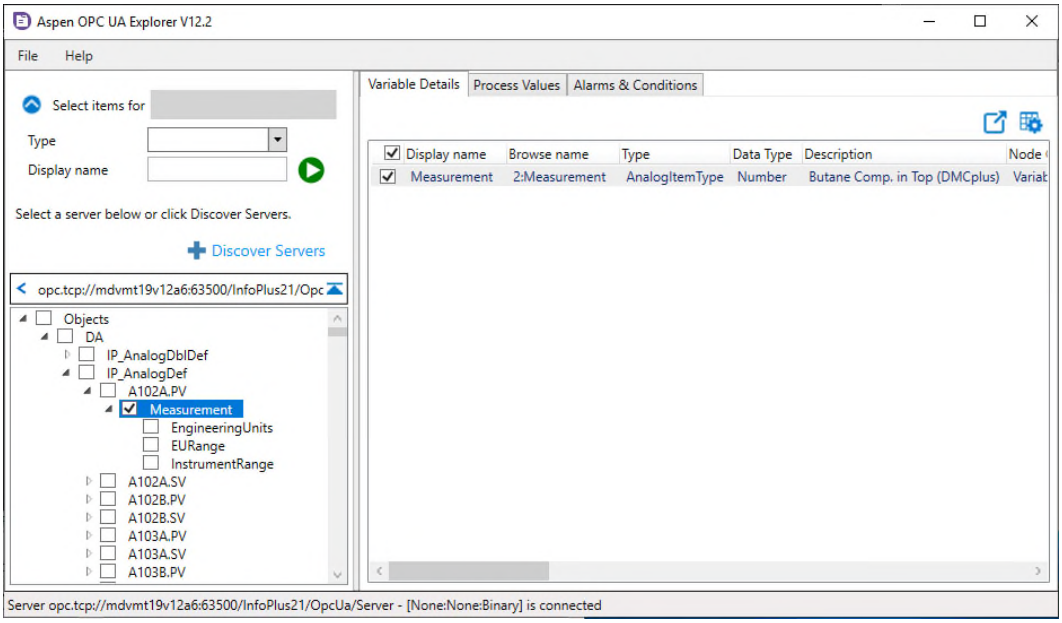
Choosing a Tag Folder

When browsing the IP.21 UA Server namespace for tags, it is important to understand the layout of the folders. The IP.21 UA Server provides two separate folders for navigating the tags, the DA and RAW folders.

The DA folder represents a filtered view by including only a subset of the IP.21 records. Specifically, it contains only those records categorized as "data access", such as IP_AnalogDef, IP_DiscreteDef, and IP_TextDef. When showing tags under the DA folder, only a subset of the attributes (fields) are available. Only those attributes related to data access are available, such as

Measurement, EngineeringUnits, and EURange. Measurement includes Value, StatusCode, SourceTimestamp, and ServerTimestamp.

For example, A102A.PV record of type IP_AnalogDef, contains a Measurement node, as shown below.



By default, every tag in the DA branch has only one process measurement. The IP.21 IOPC UA server makes use of the default MAP record for process measurement.

The RAW folder represents an unfiltered view of all the IP.21 records. Under this folder, all IP.21 fields are available as attributes on the UA node.

Using the DA Folder

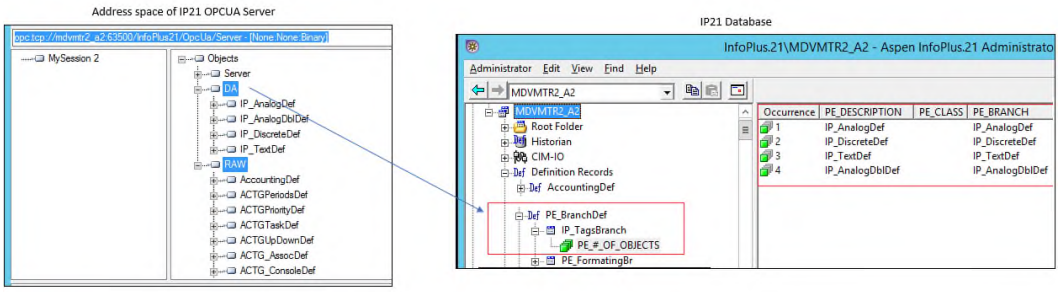
To reference items under the DA folder, prefix the UA browse path with "/Objects/2:DA", such as "/Objects/2:DA/2:IP_AnalogDef/2:MyAnalogTag/2:Measurement". Notice the namespace index of 2 used here.

Using the RAW Folder

To reference items under the RAW folder, prefix the UA browse path with "/Objects/2:RAW", such as "/Objects/3:RAW/3:IP_AnalogDef/3:MyAnalogTag/3:IP_INPUT_VALUE". Notice the namespace index of 3 used here.

Exposing Custom IP21 Records as DA Measurement Tags

To expose a custom IP21 record as a measurement tag from the DA branch of the InfoPlus.21 OPC UA server, the custom IP21 record should be defined in the IP_TagsBranch record in PE_BranchDef record, as shown below.



The InfoPlus.21 OPC UA server expects the following fields to have values in the default map record of every definition record that appears in the DA branch.

- MAP_CurrentValue
- MAP_CurrentQuality
- MAP_CurrentTimeStamp
- MAP_Description
- MAP_Units
- MAP_Base
- MAP_Range
- MAP_HistoryValue
- MAP_Quality
- MAP_TimeStamp

Supporting Multiple Measurements in DA Tag

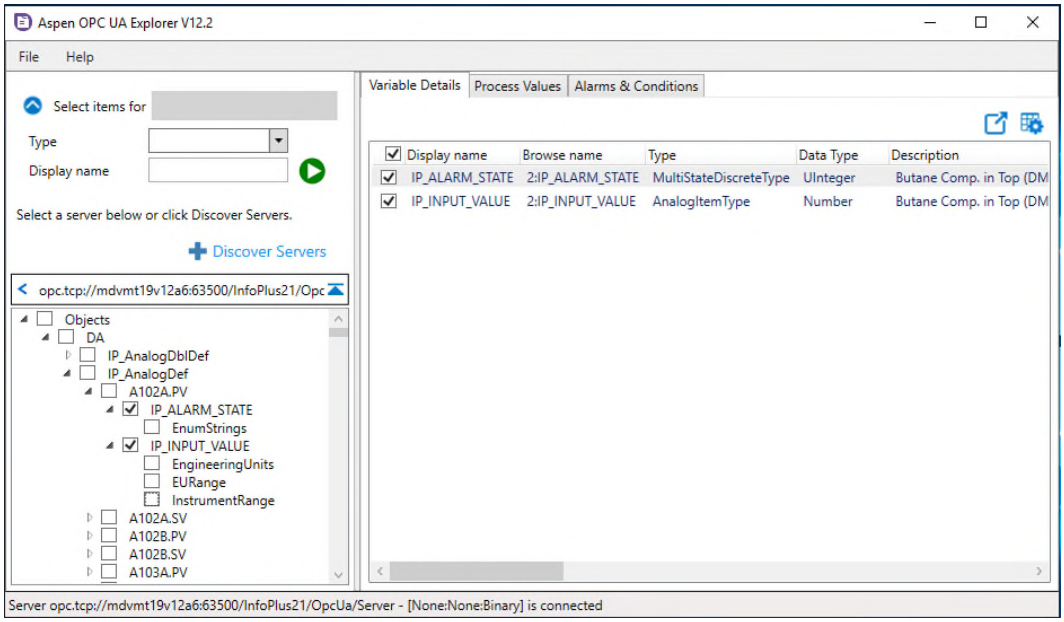
An IP.21 record can be configured to store and historize process values from multiple devices into different fields of the same IP.21 record. Such IP.21 records can be exposed as data access tags with multiple measurements in the DA node of the IP.21 OPC UA Server. Each measurement must have a separate and well-defined MAP record to qualify as a measurement.

The application configuration file of IP.21 OPC UA Server, IP21OpcUAServerHost.exe.config, has a setting named **'EnableMulitpleDAMeasurement'** to enable tags in the DA folder to have multiple measurements.

EnableMultipleDAMeasurement: True

- The IP.21 field name configured in the MAP_CurrentValue field of the map record is used as the measurement name.
- The IP.21 field name configured in the MAP_CurrentValue field of the map record is used as the DisplayName attribute of the measurement.
- The BrowseName attribute of the measurement is composed of namespaceindex of DA branch(2), followed by ':', followed by IP.21 field name configured in the MAP_CurrentValue field of the map record.
- The IP.21 field name configured in the MAP_Description field of the map record is used as the measurement description.

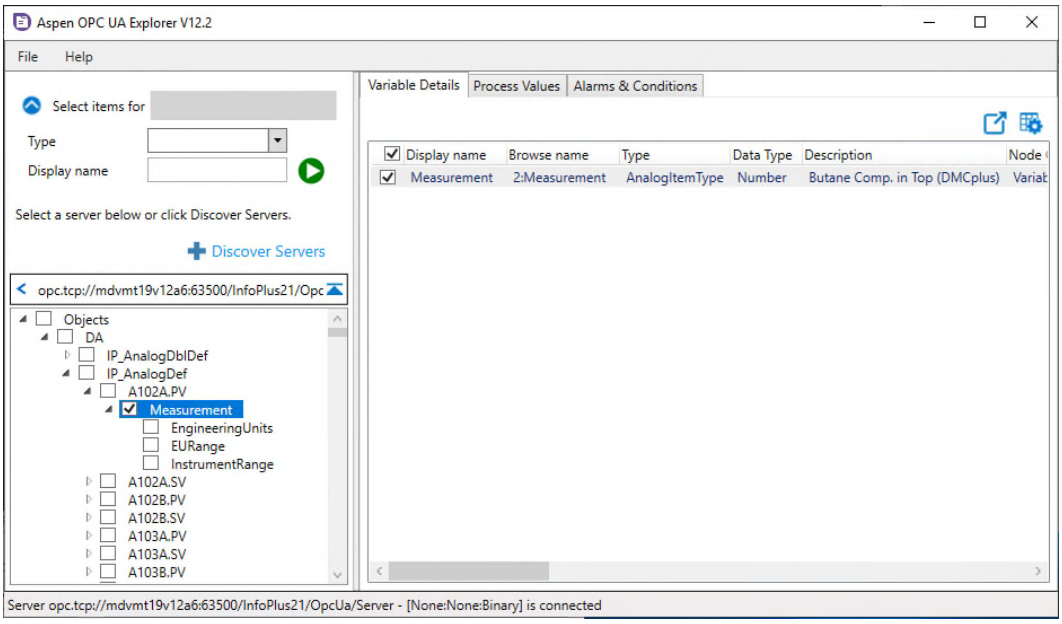
For example, the IP_AnalogDef records have two different measurements, IP_ALARM_STATE and IP_INPUT_VALUE, which are defined with two different map records, IP_AnalogAlmMap and IP_AnalogMap, respectively.



EnableMultipleDAMeasurement: False

Every tag in the DA branch has only one process measurement. The IP.21 IOPC UA server makes use of the default MAP record to expose an IP.21 record as a process measurement.

For example, A102A.PV record of type IP_AnalogDef, contains a single Measurement node as shown below.


Aspen OPC UA Explorer V12.2
File
Help
Select items for
Type
Display name
Select a server below or click Discover Servers.
Discover Servers
opc.tcp://mdvmt19v12a6:63500/InfoPlus21/Opc
Objects
DA
IP_AnalogDblDef
IP_AnalogDef
A102A.PV
Measurement
EngineeringUnits
EURange
InstrumentRange
A102A.SV
A102B.PV
A102B.SV
A103A.PV
A103A.SV
A103B.PV
Variable Details
Process Values
Alarms & Conditions
Display name
Browse name
Type
Data Type
Description
Node
Measurement
2:Measurement
AnalogItemType
Number
Butane Comp. in Top (DMCplus)
Variat
Server opc.tcp://mdvmt19v12a6:63500/InfoPlus21/OpcUa/Server - [None:None:Binary] is connected

3 Configuration

Various configuration settings are associated with the InfoPlus.21® UA Server as described below.

Firewall Configuration

If a site uses software to control access to computer network ports, such as firewall management, then configuration steps may be needed to allow a UA Client to connect to an InfoPlus.21 UA server on another computer. Some UA servers automatically configure the firewall ports during installation. This is true for the InfoPlus.21 UA Server. However, if connection problems are encountered, then the firewall rules on both the client computer and the InfoPlus.21 UA server computer may need to be modified to open the appropriate ports. Since each UA server uses its own port numbers, refer to the documentation provided by the UA server vendor to learn the port numbers.

One easy way to configure the firewall is to use the UA Configuration tool, as follows:

1. Launch the UA Configuration tool. (See "**UA Configuration Tool**" on page 23.)
2. Select the **Manage Application** tab.
3. Use the **Find** button to navigate to the folder where the UA application was installed, and then select the executable file. For InfoPlus.21, such files exist in **%PROGRAMFILES%\AspenTech\InfoPlus.21\db21\code**.
4. The UA server file is named: **IP21OpcUAServerHost.exe**.
5. Click the **Manage Firewall Access** button, select the check boxes for **Ports Used by Application**, and then click **Done**.

Application Instance Certificates

To learn about application instance certificates, see "**Message Security in OPC UA**" on page 4.

Configuration Files

The InfoPlus.21 UA Server provides the following configuration files to control the runtime behavior of the system.

Application Configuration File

The file **%PROGRAMFILES%\AspenTech\InfoPlus.21\db21\code\IP21OpcUAServerHost.exe.config** stores configuration information required by the InfoPlus.21 UA Server. This file does not normally need to be modified.

OPC UA Application Configuration File

The InfoPlus.21 UA Server uses technology provided by the OPC Foundation, known as the OPC UA SDK. This technology is delivered as redistributable DLLs included with the InfoPlus.21 installation. The technology uses a file, known as the OPC UA Application Configuration file to store certain parameters, including security and transport configuration. The file is named **tsk_opcua_server.opcua.config.xml** and is normally located in the InfoPlus.21 group200 folder under the Windows folder **%CommonApplicationData%\AspenTech\InfoPlus.21\db21\group200**. The exact location of the file can be determined by viewing the FilePath setting in the Application Configuration File (described just above).

Normally you would not view or edit this file manually, but instead use the OPC UA Configuration tool. For details, see "**UA Configuration Tool**" on page 23.

Logging Configuration File

Please read the section "**Diagnostic Log**" on page 21.

User Authentication

Aspen InfoPlus.21 UA server does not accept connections from anonymous client user accounts. Therefore, to connect, a valid Windows user account and password must be supplied when configuring a UA client connection. Please refer to the steps provided by the UA client vendor for setting and passing user credentials.

Endpoint Configuration

The base endpoint URL of the Aspen InfoPlus.21 UA server is specified in the OPC UA Configuration file **tsk_opcua_server.opcua.config.xml**.

The endpoint URL is defined as below:

```
<BaseAddresses xmlns:d3p1="http://opcfoundation.org/UA/2008/02/Types.xsd">
  <d3p1:String>opc.tcp://localhost:63500/InfoPlus21/OpcUa/Server</d3p1:String>
</BaseAddresses>
```

There are various options available with the OPC UA clients to discover the endpoint of the Aspen InfoPlus.21 OPC UA server, such as querying the endpoints from the Local Discover server or directly querying the endpoints from the Discovery URL of Aspen InfoPlus.21 OPC UA Server.

The base endpoint URL of the Aspen InfoPlus.21 OPC UA server should be modified to contain the actual host name instead of localhost if OPC UA clients are using the discovery URL of the Aspen InfoPlus.21 server, as shown below.

```
<BaseAddresses xmlns:d3p1="http://opcfoundation.org/UA/2008/02/Types.xsd">
  <d3p1:String>opc.tcp://hostname:63500/InfoPlus21/OpcUa/Server</d3p1:String>
</BaseAddresses>
```

4 Connecting

This section describes how connect a UA client to an InfoPlus.21® UA Server to get or put data values:

Prerequisites

1 Install and configure a UA client.

A UA client application is required for accessing data in the InfoPlus.21 UA Server. There are several options for acquiring a UA client:

- Use the Aspen Cim-IO™ UA Client (useful for testing the InfoPlus.21 UA Server or for transferring data between two InfoPlus.21 systems).
- Install and configure a third-party UA client. Some free or trial applications exist.

2 Open Firewall Ports.

In most cases, this step can be skipped because firewalls ports are automatically configured when a UA server is installed. However, if connection problems arise, then firewall configuration may be necessary.

Discovery

The OPC UA Local Discovery server from the OPC Foundation is distributed as part of the InfoPlus.21 server installation.

The OPC UA Local Discovery server is installed as a Windows service.

The InfoPlus.21 OPC UA server running on a node registers itself, periodically, with the Local Discovery server on that node.

The OPC UA Local Discovery server allows OPC UA Client applications to discover all OPC UA servers running on that node.

If the OPC UA Client application is unable to discover the InfoPlus.21 OPC UA server, then it is most certainly due to lack of certificate trust between the OPC UA Local Discovery server and the InfoPlus.21 OPC UA server.

The OPC UA Local Discovery server may reject the certificate of the InfoPlus.21 OPC UA server. In such case, the rejected certificate of the

InfoPlus.21 OPC UA server will be stored at the following location: **C:\ProgramData\OPC Foundation\UA\Discovery\pki\rejected**.

To establish trust between OPC UA Local Discovery server and the InfoPlus.21 OPC UA server's certificate, the certificate should be moved to the trust list of the OPC UA Local Discovery server at the following location: **C:\ProgramData\OPC Foundation\UA\Discovery\pki\trusted\certs**.

The Windows service for OPC UA Local Discovery server should be restarted to take effect.

Connecting and Reading Data

The example steps below show how to manually read a value from the InfoPlus.21 UA Server. The example uses the OPC UA Foundation's Sample Client application.

1 Connect to the InfoPlus.21 UA Server

a. Launch the OPC UA Sample Client.

b. Click **Discovery**, then **Servers**.

c. Specify the host (computer) name of the InfoPlus.21 server, then click **Discover**.

d. Select **AspenTech InfoPlus.21 OPC UA Server**, then click **OK.**

e. Click **Connect**.

f. From the **Server Configuration** dialog box, specify the protocol as opc.tcp, security mode as SignAndEncrypt, and security policy as Basic128Rsa15, then click **OK**.

g. In the **Open Session** dialog, specify the authentication mode as **UserName**, then specify a Windows username and password. The username should be fully qualified, such as corp\myname.

h. Click **OK**, and then if prompted, accept the server's certificate.

i. If you get the error **BadSecureChannelClosed**, it is because we have not yet configured the InfoPlus.21 server to trust our client's certificate. Follow the steps in "xxx", xxx to add the UA Sample Client's certificate to the list of trusted ones.

2 Read an InfoPlus.21 Tag Value

a. Expand the **DA** folder in the right panel, then expand **IP_AnalogDef**.

b. Expand the tag **ATCAI**, then right-click on **Measurement** and select **Read**.

c. Click **Next**, then click Read. Continue to click **Read** to get updated values.

Note: The fields used for the **Measurement** attribute are determined by the map record. The IP.21 UA Server expects the following fields to have values in the map record for any definition record that appears in the DA branch: MAP_CurrentValue, MAP_CurrentQuality, MAP_CurrentTimeStamp. MAP_Description, MAP_Units, MAP_Base, MAP_Range, MAP_HistoryValue, MAP_Quality, MAP_TimeStamp.

5 Diagnostics

The InfoPlus.21® UA Server produces diagnostic information to help diagnose problems.

Diagnostic Logging

The InfoPlus.21 UA Server provides diagnostic log messages to help diagnose issues. Use the InfoPlus.21 Manager™ to view the output and error files produced by **TSK_OPCUA_SVR**.

The logging system is based on log4net. Log4net is a user-configurable logging service capable of writing to a variety of logs. These logs contain the greatest amount of detail about operational problems encountered by the InfoPlus.21 UA Server. The information in the log is most useful to experienced users and Aspen Technology support personnel.

The log verbosity is controlled by the following levels:

Log Level	Description
FATAL	Only logs serious unrecoverable errors.
ERROR	Logs errors and the levels above.
WARN	Logs warnings and the levels above.
INFO	Logs informational messages and the levels above.
DEBUG	Logs debug messages and the levels above. This will produce significant amount of log entries and can affect performance of the application.
TRACE	Logs trace messages (very detailed) and the levels above. This will produce the highest amount of log entries and can affect performance of the application.

By default, the InfoPlus.21 UA Server logs only warning messages and higher. It logs to the following locations:

Log Type	Location	Levels Logged
Standard Output	Group200\TSK_OPCU_SVR.OUT	INFO to FATAL
Rolling File Log	%CommonApplicationData%\ AspenTech\DiagnosticLogs\ InfoPlus.21\OpcUaServer\ IP21OpcUaServer.log.txt	TRACE to FATAL

The InfoPlus.21 UA Server is installed with a default log4net configuration file that may be modified to suit the requirements of each site. The log4net configuration file is **%ALLUSERSPROFILE%\AspenTech\InfoPlus.21\db21\group200\tsk_opcua_server.log4net.config.xml**. This file is in XML format and can be edited with a standard editor, such as Windows Notepad. **Note:** You must launch the editor with elevated (as Administrator) security in order to save to this folder location. To control the verbosity of the messages, open the file for editing, and then change the default log level in the <root> section. For example, change the line:

```
<level value="WARN" />
```

To

```
<level value="INFO" />
```

Detailed instructions to configure log4net are available at the log4net home page, http://logging.apache.org/log4net/index.html.

If low-level diagnostic information is required, the OPC UA SDK Diagnostic Log (described later below) may be consulted.

Viewing Diagnostic Trace Log Messages

The InfoPlus.21 UA Server diagnostic logging system can be used as a testing tool to help verify behavior and to better understand the processing flow of the application. To interactively watch the log events, you need the free tool, such as one named DebugView from this link (http://technet.microsoft.com/en-us/sysinternals/bb896647). After launching it, enable the flag for "Capture Global Win32" under the Capture menu. On Windows 2008, you need to run elevated (as Administrator).

To enable logging such that you can view detailed log messages as TSK_OPCU_SVC operates, you must configure the logging settings (log4net settings) inside the **tsk_opcu.log4net.config.xml** file, as described earlier. You must add a TraceAppender. Configuring a TraceAppender is outside the scope of this document, so please refer to the log4net online documentation. Once the TraceAppender has been added, to enable trace-level logging, change the line <level value="WARN" /> to <level value="TRACE" />. The **tsk_opcu.log4net.config.xml** file is located in folder **%CommonApplicationData%\AspenTech\InfoPlus.21\db21\group200**.

Note: TRACE level logging is very verbose, so consider setting the level to DEBUG to see fewer messages. Be sure to set the logging level back to "WARN" when finished.

OPC UA SDK Diagnostic Log

There is yet another source of low-level diagnostic logging provided. The OPC Foundation's OPC UA SDK provides additional logging capability. This log typically contains low-level communication entries. The log file can be found at path: %CommonApplicationData%\AspenTech\DiagnosticLogs\InfoPlus.21\OpcUaServer\IP21OpcUAServerHost.log.

The logging capability can be changed by editing the **TraceConfiguration** section of the OPC UA Application Configuration File (see "**OPC UA Application Configuration File**" on page 16). The table below gives the possible **TraceMasks** values.

Value	Meaning
0	Do not output any messages
1	Output error messages
2	Output informational messages
4	Output stack traces
8	Output basic messages for service calls
16	Output detailed messages for service calls
32	Output basic messages for each operation
64	Output detailed messages for each operation
128	Output messages related to application initialization or shutdown
256	Output messages related to a call to an external system
512	Output messages related to security.

A combination of the above **TraceMasks** values may be selected by adding the desired values together.

OPC UA Tools

There are various tools available that can help manage the OPC UA applications. Some of these are highlighted below.

UA Configuration Tool

Use the OPC Foundation's UA Configuration tool to manage various settings for a UA client or server application. This tool is redistributed as part of the InfoPlus.21 installation, and can be launched by choosing **UA Configuration Tool** listed under **OPC Foundation** on the Windows **Start** menu.

The tool helps to configure security settings and to manage certificates. It also helps set firewall access and application access permissions. It does this by changing settings in the OPC UA Configuration file that is associated with the UA client or server application. (See "**OPC UA Application Configuration File**" on page 16).

Troubleshooting Server Connections

Below are steps to detect and resolve failures.

To detect failures:

Description	Doc References	Page
View the diagnostic logs	Diagnostic Logging	21

To resolve failures:

Description	Doc References	Page
Verify the firewall ports	Firewall Configuration	15
Check for certificate issues	Configuring Security Certificates	6
Check OPC UA access control	Built-in OPC UA Access Control	8
Check UA server application access control	Application Specific Access Control	8
Check for browse path problems	Browse Paths	9