WEDNESDAY, OCTOBER 25, 2023

Implementing claims authentication in AVEVA[™] PI System[™]

Presented By: Ryan Biggins





Ryan Biggins

Senior Technical Support Engineer I

- AVEVA
- ryan.biggins@aveva.com





Improving security with OpenID Connect (OIDC)



Challenge

Security in my AVEVA PI System is unnecessarily complicated

- Servers distributed across workgroups, isolated domains, untrusted domains
- Heavy use of Windows Credential Manager
- Use of PI Trusts (Not recommended)



Solution

Use OpenID Connect (OIDC) authentication and other new features in AVEVA™ PI Server 2023

- New to AVEVA PI Server 2023
- A form of claims authentication
- Uses tokens for access



Benefits

- TLS/SSL to natively encrypt communication for all authentication methods
- Free from the boundaries of a Windows domain/Active Directory
- Can federate to your organization's existing identity provider (IdP)

Agenda

- New AVEVA PI Server features overview
- TLS/SSL certificates
- OpenID Connect
- Installation/upgrade considerations
- Managing security access
- Troubleshooting
- Questions

Relevant new AVEVA PI Server features

- Support for TLS/SSL certificates
 - Natively encrypts communication for all AVEVA PI System authentication methods (OIDC, Windows, PI Trust)
- OpenID Connect (OIDC) authentication
 - A form of claims authentication
 - Possible through the AVEVA Identity Manager (AIM) service and an identity provider (IdP) of choice

Note: AVEVA PI Server 2023 requires you to be on AVEVA[™] Flex

TLS/SSL certificates



TLS/SSL certificates

- Transport Layer Security (TLS):
 - Cryptographic protocol that involves certificates
 - Previous iterations were known as Secure Sockets Layer (SSL)
- Natively encrypts communication in AVEVA PI System for all different authentication methods
- Same technology is used to secure communication with websites
 - HTTPS protocol requires a TLS/SSL certificate
- Issued by a certificate authority (CA)
- Need to be trusted by all clients that connect
- Applications (PI DA, asset framework, AVEVA Identity Manager (AIM)) that are installed on the same server can share the same certificate
- Optional feature for PI Server; Required if using OIDC authentication

Certificates in AVEVA[™] PI System[™]

Which AVEVA PI System components now support TLS/SSL?

Newly Supported:

- Data archive
- Asset framework
- AIM

Already Supported:

- AVEVA™ PI Vision™
- PI Web API
- AVEVA PI Integrator for Business Analytics
- Several others (mostly web-based)

Which certificate authority (CA) is best?

In order of preference/strength

- 1. Third-party CA (Issued by GlobalSign, DigiCert, GoDaddy, etc.)
 - Preferred if users and applications are spread across multiple untrusted domains
 - Preferred if accessing the application from outside the corporate network
 - Most servers/computers will trust these certs automatically
 - Incur a cost to obtain
- 2. Enterprise CA (Issued by your domain/IT)
 - Preferred if users and applications are mostly contained within the same domain forest
 - Servers/computers within the corporate domain forest will trust these certs automatically
- 3. Self-signed (Issued by your server)
 - Not recommended for corporate deployment
 - These certs are trusted only on the local server or to any server onto which it is imported

Choose the option that makes the most sense for your deployment

AVEVA PI System Data Archive or Asset Framework (AF)

Select certificate during installation

AVEVA PI Server 2023 Ir	nstaller (Administrator) —		×
Certificates Selection Select certificates for se	rver communication.		About
Welcome Feature Selection Feature Rules Data Archive Certificates Selection PI to Data Hub PI to Data Hub Rules Service Accounts Summary Installation Progress Complete	TLS Certificate Configure certificate for TLS Encryption. SSL Certificate thumbprint: Select Remove Click Select to choose a new certificate.		0
	< Back Next >	Cano	el



AVEVA PI System Data Archive

Change certificate at a later time (Using pidiag)

• pidiag -tls -r <thumbprint> (or pidiag -tls --register <thumbprint>)

Certificate	×
General Details Certification Path	
Certificate Information	
This certificate is intended for the following purpose(s): • Ensures the identity of a remote computer	
Server Name	
Issued to:	
Issued by: Issuing CA Valid from 7/10/2023 to 7/0/2025	
You have a private key that corresponds to this certificate.	
Issuer Statement	
OK	

AVEVA PI System Data Archive

Change certificate at a later time (Using pidiag)

pidiag -tls -r <thumbprint> (or pidiag -tls --register <thumbprint>)

General Details Certification Path Show: <all></all>	
General Details Certification Path Show: <all></all>	
Show: <all></all>	
	Ť
Field Val Subject Key Identifier DN Subject Alternative Name DN Authority Key Identifier Ke CRL Distribution Points [1] Authority Information Access [1] Thumbprint c6 Friendly name Intervention Access	Ilue VS Name= VID= VICL Distribution Point: Distr JAuthority Info Access: Acc See7caa453f76629664fbc0 V



AVEVA PI System Data Archive

Verify current certificate (Using pidiag)

pidiag -tls -y (or pidiag -tls --verify)



AVEVA PI System Asset Framework (AF)

Change certificate at a later time (Using AFDiag)

AFDiag /CT:<thumbprint> (or AFDiag /CertificateThumbprint:<thumbprint>)

Certificate	×
General Details Certification Path	
Certificate Information	
This certificate is intended for the following purpose(s): • Ensures the identity of a remote computer	
Server Name	
Issued to:	
Issued by:	
Valid from 7/10/2023 to 7/9/2025	
$\ref{eq: product}$ You have a private key that corresponds to this certificate.	
Issuer Statement	
OK	

AVEVA PI System Asset Framework (AF)

Change certificate at a later time (Using AFDiag)

AFDiag /CT:<thumbprint> (or AFDiag /CertificateThumbprint:<thumbprint>)

📃 Certificate	×	
Gen 📃 Certificate		×
General Details Certification Path	1	
Show: <all></all>	~	
Field	Value DNS Name = KeyID =0e4c09baa5e01b1f19 [1]CRL Distribution Point: Distr [1]Authority Info Access: Acc e88ea19429543ee3cd4be501	•
e88ea19429543ee3cd4be	501d83f6ad6cb21f127	
E	dit Properties Copy to File	
	ОК	



AVEVA PI System Asset Framework (AF)

Verify current certificate (Using registry)

- Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AFService
- CERTIFICATETHUMBPRINT

🔡 Registry Editor			- 🗆 ×
File Edit View Favorites Help		1450	
	E\SYSTEM\CurrentControlSet\Service	s\AFService	
V Computer	^ Name	Туре	Data
> HKEY_CLASSES_ROOT	ab (Default)	REG_SZ	(value not set)
	Dertificatethumbprint	REG_SZ	e88ea19429543ee3cd4be501d83f6ad6cb21f127
	ab Description	REG_SZ	Provides ability for clients to read and write PI AF d
HARDWARE	ab DisplayName	REG_SZ	PI AF Application Service
SAM	300 ErrorControl	REG_DWORD	0x00000000 (0)
SECURITY	ab ImagePath	REG_EXPAND_SZ	"C:\Program Files\PIPC\AF\AFService.exe"
> SOFTWARE	(ab) ObjectName	REG_SZ	NT SERVICE\AFService
SYSTEM	🐯 ServiceSidType	REG_DWORD	0x00000001 (1)
> ActivationBroker	🐯 Start	REG_DWORD	0x0000002 (2)
> ControlSet001	🐯 Type	REG_DWORD	0x00000010 (16)
> ControlSet002			
CurrentControlSet			
> Control			
> Enum	~		
< >>	•		

AVEVA Identity Manager (AIM)

Select certificate through configurator



AVEVA Identity Manager (AIM)

Select certificate through configurator

Advanced Conf	figuration				X
Certificates	Ports				
In order to e be configure	nable comn ed.	nunications via encrypted channels (e.g. HT	TPS), cer	tificates an	e required to
Certificates o	ion	e provided by your IT department or autom	natically g	generated.	
Please	select the a	ppropriate options below.			
Certific	ate Source:	Provided by IT (import / select)		*	Import
Certifi	cate:	RBIGGINS-PITEST		~	Details
		RBIGGINS-PITEST	N		
		RBIGGINS-PITEST ASB OPC UA Server	3		
		WMSVC-SHA2			
				ок	Cancel

OpenID Connect (OIDC) authentication

Claims in AVEVA PI System



OpenID Connect (OIDC) authentication

- Authentication is the process by which a user or application proves its identity to a server and forms an initial connection
- Claims authentication is based on the premise that an external identity provider (IdP) is trusted to make claims about the identity of a user
- OpenID Connect (OIDC) is a form of claims authentication
 - Built on the OAuth 2.0 Framework
 - Makes Single Sign On (SSO) possible
 - Involves tokens (Access, Refresh, etc.)
- AVEVA Identity Manager (AIM) is the identity service that handles OIDC authentication in AVEVA PI System

For a full discussion of technical details, benefits, and reasons behind the feature introduction, see the presentation **Introduction to claims authentication**

AVEVA[™] Identity Manager (AIM)

- "Identity service;" runs as a Windows service
- Part of the AVEVA Platform Common Services (PCS)
 - Obtainable via Platform Common Services (PCS) for AVEVA PI System install kit
- Manage AIM using the Configurator application
- If available, AIM registers with default IdP:
 - Windows Active Directory (AD)
- Connect AIM to one additional IdP:
 - AVEVA Connect (recommended)
 - Azure Active Directory (AAD)
- Register individual AVEVA PI Server components with AIM

A AVEVA TM Identity Manager × +	~	-		×
← → C ∩ → /identitymanager/	Ŀ	☆		:
AVEVA™ Identity Manager			θ	
Welcome to Identity Manager				
AVEVA [™] Identity Manager publishes a discovery document where you can find metadata and links to all the endpoints, key material, etc.				

Accessing AIM endpoint via browser

Services			- 0	×	
File Action View	Help				
⊨ → 🗖 🛱 🤇	à 🗟 🛛 🖬 🕨 🔲 II 🕩				
🐊 Services (Local)	Services (Local)				
	AVEVA Identity Manager	Name	Description	St ^	
		🎑 AVEVA Certificate Renewal	Automatically renews certificates for AVEVA		
	Stop the service	🎑 AVEVA Data Store	Provides a lightweight data vault for AVEVA a	Ri	
	restart the service	🔍 AVEVA Identity Manager	Provides Single Sign On (SSO) for AVEVA app		
		🎑 AVEVA Service Manager	Facilitates launching of services relating to A	Ri	
	Description:	🍓 AVEVA Watchdog	Manages the lifetime of services relating to	Ri	
	AVEVA applications	🎑 Azure Hybrid Instance Metadata Service	Azure Hybrid Instance Metadata Service	Ri	
		EVA applications. Transfer Service Transfers files in the background using idle i			

Configurator application



AVEVA[™] Identity Manager (AIM)

- "Identity service;" runs as a Windows service
- Part of the AVEVA Platform Common Services (PCS)
 - Obtainable via Platform Common Services (PCS) for AVEVA PI System install kit
- Manage AIM using the Configurator application
- If available, AIM registers with default IdP:
 - Windows Active Directory (AD)
- Connect AIM to one additional IdP:
 - AVEVA Connect (recommended)
 - Azure Active Directory (AAD)
- Register individual AVEVA PI Server components with AIM

Configurator	x
File Help	
Common Platform	Machines running AVEVA software must be configured to trust each other so that encrypted communications can be utilized. This is done by connecting them to a System Management Server.
	 This machine is the System Management Server. There should only be one System Management Server in your topology for all AVEVA products. All other machines should be configured to connect to this System Management Server.
	 No System Management Server configured. (NOT RECOMMENDED) This option also allows you to remove any existing certificates that were managed by the System Management Server.
	You can connect to an existing System Management Server or configure a new System Management Server by selecting one of the first two options, respectively. When you click Configure, a certificate and the web ports to use for communication are configured. To modify these configurations, click Advanced. Advanced
	onfiguration Messages
< >	
Refresh All Me	ssages Configure Close

Configurator application

Authentication flow



Authentication flow (with federation)



Supported products

Where can I use OIDC in AVEVA PI System?

Supported:

- Data archive
- Asset framework
- PI Notifications
- AVEVA PI Vision
- PI Web API
- AVEVA Adapters*
- PI AF SDK-based PI Clients (PI System Explorer, AVEVA[™] PI DataLink[™])
- Custom PI AF SDK applications*

Not Supported:

- AVEVA PI Interfaces
- AVEVA PI Connectors
- PI Buffer Subsystem
- AVEVA PI System Management Tools (SMT)**



Installation/upgrade considerations



Installation/upgrade path

- 1. Decide upon AVEVA PI System architecture; Which server will host AIM service?
- 2. Prepare and import server certificates for AIM and AVEVA PI Server components
 - Third-party CA certs or Enterprise CA certs preferred
- 3. Prepare service accounts and administrative accounts (Windows)
- 4. Install Platform Common Services (PCS) for AVEVA PI System; Contains AIM service
- 5. Add administrative accounts to aaAdministrators local group (Windows)
- 6. Perform initial AIM setup in Configurator application; Change AIM certificate
- 7. Connect AIM to an (additional) identity provider (IdP)
 - Steps will differ depending on IdP (AVEVA Connect or Azure Active Directory (AAD))
 - If needed, federate to an IdP, using AVEVA Connect, common cloud platform, as an identity service
- 8. Install or upgrade AVEVA PI Server components
 - Check the option to enable TLS/SSL
- 9. Manage certificates for AVEVA PI Server components
- 10. Register AVEVA PI Server components with AIM using OIDC Configuration Tool

Federating to other Identity Providers (IdPs)

What if I have an existing IdP that I want to use?

- AVEVA Connect supports federation to your existing IdP
- Examples of other common IdPs:
 - OIDC-compliant IdPs
 - Google, PingID, ADFS, Okta, etc.
 - SAML-compliant IdPs
 - Azure AD (AAD)
 - While AIM can connect directly to AAD, it can also federate to AAD via AVEVA Connect
 - It is recommended to federate to AAD rather than connect directly to AAD
 - Federation to AAD allows you to take advantage of all the subscription services available on AVEVA Connect, common cloud platform

Federating to other Identity Providers (IdPs)

How do I federate to my existing IdP?

- **1**. Determine the type of IdP that you have: (OIDC-compliant, SAML-compliant, Azure AD (AAD))
- 2. Set up AIM to connect to AVEVA Connect, common cloud platform as the IdP
- 3. Contact <u>connect.support@aveva.com</u> about federation
- 4. Support group will verify that requester has the right to set up federation for the respective domain
- 5. Support group will request for information related to your IdP
- 6. (If federating to Azure AD (AAD)) Support group will provide required preparation tasks to complete and wait for confirmation
- 7. Support group will set up federation

Registering AVEVA[™] PI Server components with AIM

AVEVA.PI.OIDCConfigurationTool.exe

- Perform this task locally on each server where an AVEVA PI Server component resides
 - i.e. Register the asset framework server with AIM from the asset framework server; register the data archive server with AIM from the data archive server

Use AVEVA.PI.OIDCConfigurationTool.exe

- Can be run interactively or with supplied parameters
- Supports registration and unregistration of components
- Supports silent mode
- Located in:
 - %PISERVER%\ADM on data archive servers
 - %PIHOME64%\AF on asset framework servers

Registering AVEVA[™] PI Server components with AIM

AVEVA.PI.OIDCConfigurationTool.exe

📕 Identity Ser	ver Registration		-		×
Machines runni other so that en connecting ther	ng AVEVA software mu crypted communication n to a System Manage	ust be confi ns can be u ment Serve	gured to ıtilized. 1 ər.	trust eac This is dor	h ne by
AVEVA Identity https://	Manager URL:	lentitymana	iger		
Components:	PI Data Archive	PI No	tification	IS	
		Oł	<	Cano	cel

Interactive registration

Close	
	Close

Check registration status from Command Prompt with **/DIAGNOSTICS** parameter



Registering AVEVA[™] PI Server components with AIM

AVEVA.PI.OIDCConfigurationTool.exe



Registration through Command Prompt /RIS:<AIMServer> and /PIDATAARCHIVE parameters

Aveva Obe Conliguiation Tool Help			
Register or unregister AF, PI DataArchive, or PI Notifications with the AIM Server.			
Examples:			
- To register AF, PI DataArchive, and PI Notifications with https://my-aimserver, run:			
Aveva.PI.OIDCConfiguration Tool.exe /RIS:https://my-aimserver /AFSERVER /PIDATAARCHIVE /PINOT	IFICATION	IS	
 To register AF, PI DataArchive, and PI Notifications in silent mode, run: Avera PI OIDCConfiguration Teal aver (PIS https://my.simeap.or/AESED/ED /PIDATAAPCHIVE /PINOT 			
To unregister all previously registered components, pup:	FICATION	1370	
Aveva PLOIDConfiguration Tool exe / INBEGISTER			
- To unregister only AF Server, run:			
Aveva.PI.OIDCConfiguration Tool.exe /UNREGISTER /AFSERVER			
- To register only AF Server, run:			
Aveva.PI.OIDCConfigurationTool.exe /RIS:https://my-aimserver /AFSERVER			
Supported Parameters:			
 /RIS: URL to the AIM Server endpoint (required for silent registration). 			
Usage: /KIS:https://my-aimserver (AESED)/ED: Desister level AE with the AIM Server (required for silent existention)			
- /AFSERVER, Register local Ar with the AllM Server (required for silent registration).			
- /PIDATAARCHIVE: Register local PI DataArchive with the AIM Server (required for silent registration)			
Usage: Aveva.PI.OIDCConfiguration Tool.exe /PIDATAARCHIVE			
 /PINOTIFICATIONS: Required to register local PI Notifications with the AIM Server. 			
Usage: Aveva.PI.OIDCConfiguration Tool.exe /PINOTIFICATIONS			
 /ClientRegID: Alternate client credentials when windows authentication is not available. 			
Expected format: clientid redirect Union clientid client Secret (redirect Unional Secret (Redire		mor /AES	
 ClientRegToken: Atemate credentials (access token) when windows authentication is not available 	//my-dimst	aver /Arg	LIVE
Usage: Aveva PI OIDCConfiguration Tool exe /Client Reg Token validAccess Token /BIS https://mv-aimser	/er /AFSE	RVER	
- /UNREGISTER: Required to unregister components.			
Usage: Aveva.PI.OIDCConfigurationTool.exe /UNREGISTER			
- /Q: Suppresses all UI output for silent mode.			
Usage: Aveva.PI.OIDCConfiguration Lool.exe /RIS:https://my-aimserver /AFSERVER /PIDATAARCHIVE /DIAGNOSTICS: Disclay approaching (maintaching at the second	/Q		
Usage: Aveva.PI.OIDCConfigurationTool.exe /DIAGNOSTICS			
Notes:			
- To create a new registration via interactive mode, simply click on the executable or provide command line pa	rameters v	vithout /Q.	
- Unregister is only supported via command line.			
 It no additional parameters are provided for unregister, the tool will unregister all components that were previous fithers is an existing registration on the machine, the tool will not error a new provided for the previous section. 	usly regist	ered.	
 Increase an existing registration on the machine, the tool will not create a new registration. Atleast one component is required to register via silent mode 			
		Clear	
		CIOSE	,

from Command Prompt with **/HELP** parameter



Registering PI Web API/AVEVA™ PI Vision™ with AIM

- Pre-requisite: Register the asset framework with AIM first
- PI Web API
 - o Use PI Web API Admin Utility
- AVEVA PI Vision
 - Use AVEVA PI Vision admin site and registration utility

Registering PI Web API with AIM



Registering AVEVA[™] PI Vision[™] with AIM

Save

Security X	+	×
→ C • • • • • • • • • • • • • • • • • •	/PIVision/Admin/Security	• :
VEVA [™] PI Vision [™] Adn	ninistration	000
Dverview Configuration	Security	
Security Display Defaults Jser Settings	Identity User Access Levels	
Jisplay Management Reports	Identity AF Server: Authentication Mode: Windows OpenID Connect Prompt for Windows username and password when required Identity Management Server Client registration for this PI Vision server is not found. Create a new registration Use an existing registration Add PI Vision URL Copy this command and run in command prompt on the PI Vision server machine. "%PIHOME64%PIVisionUtilities\RegisterPIVisionIdentityClient. copy exe" \ /IdentityServerURL: "https:// /AppPoolIdentity: "NT AUTHORITY\NETWORK SERVICE" \ /PIVision/"	4

←

Managing security access



OIDC mapping types

- AVEVA PI System and asset framework mapping via OIDC role
 - Appropriate for applications with a human user
 - OIDC roles are the user groups on the IdP
 - Will prompt for credentials upon initial connection
 - Session can persist as long as access token and refresh tokens allow (Single Sign On [SSO])
- AVEVA PI System and asset framework mapping via OIDC client ID
 - Appropriate for automated applications (PI Adapters, PI AF SDK applications, etc.)
 - Client ID and Secret (essentially the client password) are used to authenticate
 - Built into the automated application itself
 - Client ID and Secret need to be made known to AIM; Register the client details with AIM via PowerShell

Creating client IDs

- 1. Open PowerShell ISE on the AIM server
- 2. Enter Add-IdentityManagerClient, then enter the required parameters for this command (the required parameters have a '*' next to them in the module window of PowerShell ISE)
 - 1. HostBase The name of the AIM server; Formatted like "https://<AIMServerHostname>"
 - 2. Id As in Client ID; The unique identifier of the client
 - (Optional; Recommended) Secret Essentially the password for the client; Known only to the client and the identity service
- 3. The client is registered with AIM and the supplied ID and secret can be used

PCS for AVEVA PI System comes packaged with a set of PowerShell commandlets that allow you to interact with PCS and make configuration changes programmatically. **Add-IdentityManagerClient** is one such example.





Changes to the security page in AVEVA[™] PI System[™] system management tools (SMT)



💈 Add New Mappir	ng	×
Server:	~	
Authentication:	O Windows Open ID Connect	
Role:	Required	***
Role ID:		20
Description:		
PI Identity:	Required	
Mapping is disable	ed	
	Create Cancel	

A AVEVA [™] Identity Manager ×	+	~	-	×
\leftrightarrow \rightarrow C \bullet	/identitymanager/account/login?ReturnUrl=%2Fide	Ŀ	☆	3 :
AVEVA™ Identity Mar	nager			
	AV=VA			
	User name Diagos typo your usernamo or amail			
	riease type your useritarile of eritai			
	Password Please type your password			
	Sign In			
	Windows integrated login			

💈 Add New Mappi	ng		×
Server:	-		\sim
Authentication:	◯ Windows	Open ID Connect	
Role:	Required		***
Role ID:			2
Description:			
PI Identity:	Required		
Mapping is disable	ed		
		Create	Cancel

PI OIDC Redirect Response × +	\sim	_		
← → C ① localhost:55457/?code=2E2C563A2DE7A7495A3180E2770166097559146B4	Ė	\$		3
Successfully logged in and redirected to the PI OpenId Connect application. You may close this application to continue.	page	and re	turn to	the
appreation to continue.				

🤱 Add New Mappi	ng		×
Server:	-		\sim
Authentication:	◯ Windows	Open ID Connect	
Role:	Required		
Role ID:			R
Description:			
PI Identity:	Required		
Mapping is disable	ed		
		Create	Cancel:

ter:				
Roles	Provider	Description	Provider Type	
and the second se	Windows Active Directory	the second s	Windows Active Directory	
No. No.	Windows Active Directory	Stations.	Windows Active Directory	
a line have from	AVEVA Connect		AVEVA Connect	
Contraction of the second	Windows Active Directory	Contraction for the	Windows Active Directory	
	Windows Active Directory		Windows Active Directory	
and the second se	Windows Active Directory		Windows Active Directory	
Contraction of Contract	Windows Active Directory		Windows Active Directory	
and the state of the	Windows Active Directory	AND ADDRESS	Windows Active Directory	
and the second se	Windows Active Directory		Windows Active Directory	
terra laterative	Windows Active Directory	August hit shallow	Windows Active Directory	- I
contractor in the second	Windows Active Directory	And an	Windows Active Directory	- I
contents from	Windows Active Directory	Australia Team	Windows Active Directory	- I
Construction of Second	Windows Active Directory		Windows Active Directory	
and the second second	Windows Active Directory		Windows Active Directory	
and the second second	Windows Active Directory		Windows Active Directory	
and the second se	Windows Active Directory	the second s	Windows Active Directory	
and the second se	Windows Active Directory	Anna Anna	Windows Active Directory	_ I



🔱 Add New Mappi	ng	×
Server:	No. of Concession, Name	~
Authentication:	⊖ Windows	ID Connect
Role:	Required	
Role ID:		(A)
Description:		
PI Identity:	Required	
Mapping is disable	ed	
	Crea	te Cancel

A Select an OIDC Mapping				×
Select a role or client id available from Click OK to map the role or client id to	the AIM server below. he selected PI Identity. O Roles			
<u>F</u> ilter:				
Client Name	Client Id			
With Date Management Dark	tot. belaiting provided			
All and a second second second	Margaret Party State State State			
the first sector and the sector of the secto	the state of the s			
Contract of the second second second	The second			
Witness of the Physics of Contraction	FOre ID RECEIPT			
The second se	NUMBER OF STREET, STRE			
Contract of the second state	Parlament, Ch., and California Stud			
CARLEY COLUMN	NOVEMBER 201, NOVEMBER 1011			
IN MUSIC INC.	N. N.N. N.			
TESTCLIENT	TESTCLIENT			
		ОК	Cano	:el



🏂 🗙 🕋 🖳 🚚 🛃 🔜 -	0					
Mappings Trusts						
Mapping	Server	Collective	Description	PI Identity	Enabled	Туре
AvevaConnect	And the second second		 Tests (Support) 	piusers	True	Role
🙎 AvevaConnect	NAME AND ADDRESS		Contraction of the local distance of the loc	piadmins	True	Role
3	And the Article		1 Discharting Services	piadmin	True	Windows
2.000 mm	States and the second			piadmins	True	Windows
STESTCLIENT	And in the local division of			piusers	True	ClientCredential
👰 Windows	And a second second		C POR AGON	piadmins	True	Role

AVEVA PI System Explorer (PSE)

😭 Security N	Napping Properties — [×
General		
Role (A):	Enter or Select a Role	 \mathbf{P}
Role ID:		
Name:		
Description:		
Identity:	Select an Identity	~
	O Windows OpenID Connect	
	OK Cancel	



User name
Please type your username or email
Password Please type your password

AVEVA PI System Explorer (PSE)

😭 Security N	Mapping Properties	- 🗆	×	PI OIDC Redirect Response × +	× .	_	
General				\leftrightarrow \rightarrow C (i) localhost:55457/?code=8D1ACEE1CBA1827845341D39E3D0C592EAE6ADB8D57	€ ☆) I	ł
Role (A): Role ID:	Enter or Select a Role			AVEVA			
Name: Description:				Successfully logged in and redirected to the PI OpenId Connect application. You may close this page application to continue.	and reti	ırn to	0
Identity:	Select an Identity		~				
	O Windows OpenID Connect						
	OK Cancel		.:				

AVEVA PI System Explorer (PSE)

😭 Security N	1apping Properties	—	\times
General			
Role (A):	Enter or Select a Role		\mathbf{P}
Role ID:			
Name:			
Description:			
Identity:	Select an Identity		\sim
	○ Windows		
	OK Cancel		

A Select an OIDC Mapping						×
Select a role or client id available from the Click OK to map the role or client id to the s	AIM server b elected PI I	oelow. dentity.	Client ID			
Filter:						
Roles	Provider	Description	Provider Type	Directory		^
Contractory Contractory	Windows Windows	No. in case	Windows Active Directory Windows Active Directory AVEVA Connect			
20Publication argan automatication 2/20 antiphilipmede	Windows Windows Windows	ST-NatiOnatory Rela	Windows Active Directory Windows Active Directory Windows Active Directory		ery.	
Addressing of the second secon	Windows Windows Windows	and particular	Windows Active Directory Windows Active Directory Windows Active Directory			
Nation National Instanto Compute Service National Type	Windows Windows Windows	Namus Baltriation Analysis (San-	Windows Active Directory Windows Active Directory Windows Active Directory			
Second Calific Antibiotics Spectrum Proceeding and the	Windows Windows		Windows Active Directory Windows Active Directory			
Annual State	Windows Windows Windows	here any here a	Windows Active Directory Windows Active Directory Windows Active Directory			
			(ОК	Cancel	Y

AVEVA PI System Explorer (PSE)

😭 Security N	Napping Properties — 🗆 🗙
General	
Role (A):	Enter or Select a Role
Role ID:	
Name:	
Description:	
Identity:	Select an Identity ~
	O Windows OpenID Connect
	OK Cancel

A Select an OIDC Mapping						×
Select a role or client id available from the AIM server below. Click OK to map the role or client id to the selected PI Identity.	O Roles	Client ID				
Filter:						
Client Name Client Id						
An interference in the interference	in a					
Manufacture and the second sec						
No Roman Record Party Address Party House						
NUMBER OF REAL AND A DESCRIPTION OF REAL						
Allow the second s						
The Incompany of the Incompany						
Portugal ID, MICH Row TO, MICH 10, MICH	diam'r.					
Partners of Charles and Address of States						
The second secon	0.00					
10.407.00 E.807.00		_				
TESTCLIENT TESTCLIENT						
			0	K	Cano	el
					Gano	.:

Set preference for PI AF SDK clients

- No popup if the certificate isn't present
- preferOIDCAuth setting in
 %ProgramData%\OSIsoft\AF\AFSDK.config
 - Client-wide setting
 - Valid settings:
 - Prompt
 - Never
 - Always





Troubleshooting



Troubleshooting tips

- Check that managing user is in the aaAdministrators group on AIM server
- Validate general network connectivity between PI Client & AIM and between PI Client & AVEVA PI Server component
- Review AVEVA PI Server component logs and AIM logs (PCS logs)
- Check that certificates are valid (for AIM and AVEVA PI Server components)
- Check that the PI Client trusts certificates (for AIM and AVEVA PI Server components)
- Check registration of AVEVA PI Server components with AIM (Locally, using AVEVA.PI.OIDCConfigurationTool.exe)
- Review configuration between AIM and IdP (Refer to relevant setup guide)

Logs

Authentication troubleshooting

- Check relevant AVEVA PI System application logs for OIDC authentication attempt messages
 - Asset framework (AF): Event viewer > Applications and services logs > AF
 - AVEVA PI System data archive: PIPC logs (PI SMT, PI AF SDK Utility, pigetmsg)
- Check AIM logs (PCS logs)
 - Use ArchestrA log viewer (aaLogViewer)
 - Local to AIM server
 - Can increase logging level to get more information

File	Action View	v Help					
(= =)	2 🖬	0 7	🦹 🛊 🏘	🖗 🖗 🛛	Þ ቆ Q		
🔲 Sta	art Time: 12/31/	1900 11:59:59	9 PM	End Time	e: 12/31/2100	11:59:59 PM	
No:	Date	Time	Process ID	Thread ID	Log Flag	Component	Message
332	8/21/2023	9:52:30 PM	2596	736	Info	ArchestrA.DataSt	. ArchestrA Data Store service starting
333	8/21/2023	9:52:30 PM	2596	736	Info	ArchestrA.DataSt	. ArchestrA Data Store service is preparing to accept connections.
334	8/21/2023	9:52:30 PM	2596	736	Info	ArchestrA.DataSt	. ArchestrA Data Store service started
335	8/21/2023	9:52:34 PM	1968	608	Info	Asb.Watchdog	PCS runtime webservice hosted successfully
336	8/21/2023	9:52:35 PM	1968	608	Info	Asb.Watchdog	NetTcpPortSharing windows service is running.
337	8/21/2023	9:52:35 PM	1492	1504	Info	ArchestrA.Identit	. Service is starting.
338	8/21/2023	9:52:37 PM	1968	608	Info	Asb.Watchdog	Starting 'WcfDiscovery \Asb.Discovery.exe' with parameters: ' /G
339	8/21/2023	9:52:37 PM	1492	2668	Info	ArchestrA.Identit	 Announcing SMS endpoint via SSDP.
340	8/21/2023	9:52:38 PM	1968	1996	Info	Asb.Watchdog	Starting detached process C:\Program Files (x86)\AVEVA\Platform
341	8/21/2023	9:52:39 PM	1968	680	Info	Asb.Watchdog	Starting 'Discovery Pcs. Discovery.exe' with parameters: ' /G=500
342	8/21/2023	9:52:40 PM	1968	2768	Info	Asb.Watchdog	Starting detached process C:\Program Files (x86)\AVEVA\Platform
343	8/21/2023	9:52:43 PM	1968	680	Info	Asb.Watchdog	Starting 'WcfProxy\PCS.Proxy.Wcf.exe' with parameters: ' /G=50
344	8/21/2023	9:52:43 PM	1968	680	Info	Asb.Watchdog	Starting 'WcfDeployment\Asb.DeployService.exe' with parameter
345	8/21/2023	9:52:44 PM	1968	1996	Info	Asb.Watchdog	Starting detached process C:\Program Files (x86)\AVEVA\Platform
346	8/21/2023	9:52:44 PM	1968	1996	Info	Asb.Watchdog	Starting detached process C:\Program Files (x86)\AVEVA\Platform
347	8/21/2023	9:52:47 PM	4408	4140	Info	Asb.DeployService	Opening endpoints.
348	8/21/2023	9:52:47 PM	4760	4176	Info	PCS.Discovery	DiscoveryWebService started.
349	8/21/2023	9:52:50 PM	1968	680	Info	Asb.Watchdog	Starting Windows service AsbServiceManager
350	8/21/2023	9:52:54 PM	3964	4500	Info	Asb.Discovery	Local discovery configuration changed
51	8/21/2023	9:52:54 PM	3964	4500	Info	Asb.Discovery	Starting Local discovery service in 500ms
352	8/21/2023	9:52:54 PM	3964	4500	Info	Asb.Discovery	Legacy discovery web service starting.
353	8/21/2023	9:52:55 PM	3964	4500	Info	Asb.Discovery	DiscoveryService started.
354	8/21/2023	9:52:58 PM	4408	4140	Info	Asb.DeployService	DeployService starting
355	8/21/2023	9:53:03 PM	3964	3920	Info	Asb.Discovery	Opened endpoint: net.tcp://rbiggins-pitest/LDS
356	8/21/2023	9:53:03 PM	4408	4140	Info	Asb.DeployService	DeployService started.
357	8/21/2023	9:53:07 PM	3860	5508	Info	PCS.Proxy.Wcf	WcfProxyService started.
358	8/25/2023	1:07:20 PM	6284	6620	Info	ArchestrA.Identit	. Service is starting.
359	8/25/2023	1:07:22 PM	6284	9936	Info	ArchestrA.Identit	. Announcing SMS endpoint via SSDP.
•							

aaLogViewer application



Increase logging level for PCS logs

AIM troubleshooting

- 1. Open the appsettings.json file
 - Located at C:\Program Files (x86)\AVEVA\Platform Common Services\Management Server\appsettings.json
- 2. Take a copy of the appsettings.json file
- 3. Locate and change the LogLevel of Logging section to "Trace"
- 4. Open the ArchestrA Log Viewer
 - Located at C:\Program Files (x86)\Common Files\ArchestrA\aaLogViewer.exe
- 5. Go to Actions > Log Flags and enable all log flags for ArchestrA.IdentityManager component
- 6. Perform your test and export the log as an ***.aaLGX** file
- 7. Revert the logging level back to default settings when finished



aaLogViewer application



Full steps in How to enable SMS tracing

Questions?

Please wait for the microphone. State your name and company.



Please remember to...

Navigate to this session in the mobile app to complete the survey.

Thank you!

This presentation may include predictions, estimates, intentions, beliefs and other statements that are or may be construed as being forward-looking. While these forward-looking statements represent our current judgment on what the future holds, they are subject to risks and uncertainties that could result in actual outcomes differing materially from those projected in these statements. No statement contained herein constitutes a commitment by AVEVA to perform any particular action or to deliver any particular product or product features. Readers are cautioned not to place undue reliance on these forward-looking statements, which reflect our opinions only as of the date of this presentation.

The Company shall not be obliged to disclose any revision to these forward-looking statements to reflect events or circumstances occurring after the date on which they are made or to reflect the occurrence of future events.



ABOUT AVEVA

AVEVA is a world leader in industrial software, providing engineering and operational solutions across multiple industries, including oil and gas, chemical, pharmaceutical, power and utilities, marine, renewables, and food and beverage. Our agnostic and open architecture helps organizations design, build, operate, maintain and optimize the complete lifecycle of complex industrial assets, from production plants and offshore platforms to manufactured consumer goods.

Over 20,000 enterprises in over 100 countries rely on AVEVA to help them deliver life's essentials: safe and reliable energy, food, medicines, infrastructure and more. By connecting people with trusted information and AI-enriched insights, AVEVA enables teams to engineer efficiently and optimize operations, driving growth and sustainability.

Named as one of the world's most innovative companies, AVEVA supports customers with open solutions and the expertise of more than 6,400 employees, 5,000 partners and 5,700 certified developers. The company is headquartered in Cambridge, UK.

Learn more at www.aveva.com