

WEDNESDAY, OCTOBER 25, 2023

---

# Implementing claims authentication in AVEVA™ PI System™

Presented By: Ryan Biggins

AVEVA



---

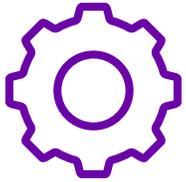
# Ryan Biggins

Senior Technical Support Engineer I

- AVEVA
- [ryan.biggins@aveva.com](mailto:ryan.biggins@aveva.com)



# Improving security with OpenID Connect (OIDC)



## Challenge

Security in my AVEVA PI System is unnecessarily complicated

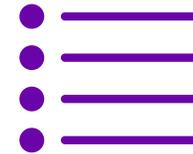
- Servers distributed across workgroups, isolated domains, untrusted domains
- Heavy use of Windows Credential Manager
- Use of PI Trusts (Not recommended)



## 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

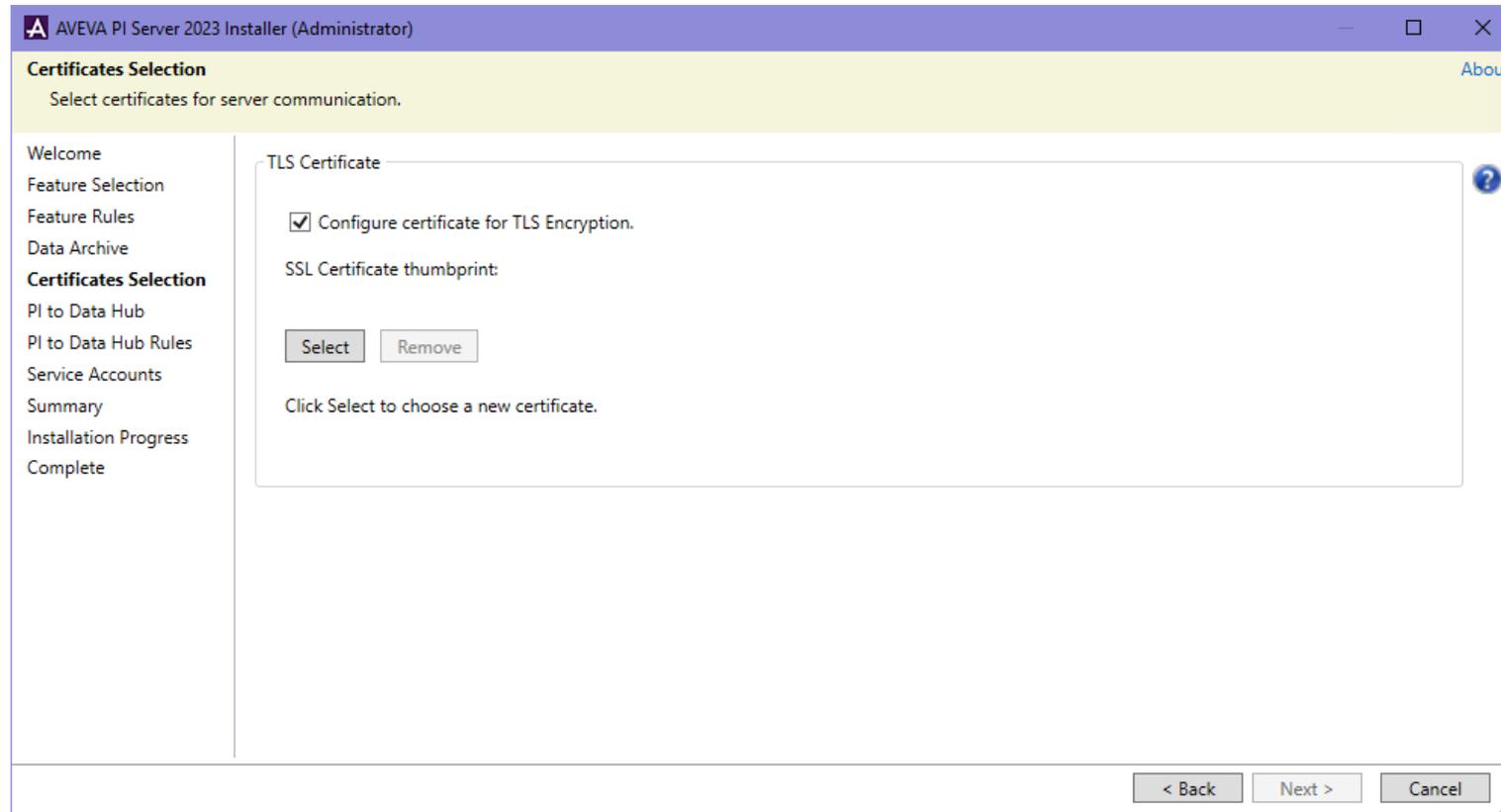
1. Third-party CA (Issued by GlobalSign, DigiCert, GoDaddy, etc.)
  - Preferred if users and applications are spread across multiple untrusted domains
  - Preferred if accessing the application from outside the corporate network
  - Most servers/computers will trust these certs automatically
  - Incur 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**

# Applying and checking certificates

## AVEVA PI System Data Archive or Asset Framework (AF)

### Select certificate during installation

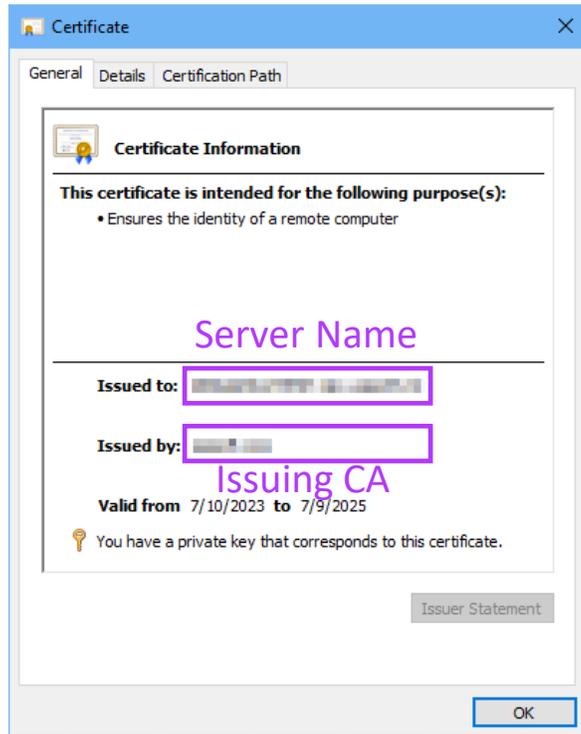


# Applying and checking certificates

## AVEVA PI System Data Archive

Change certificate at a later time (Using **pidiag**)

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

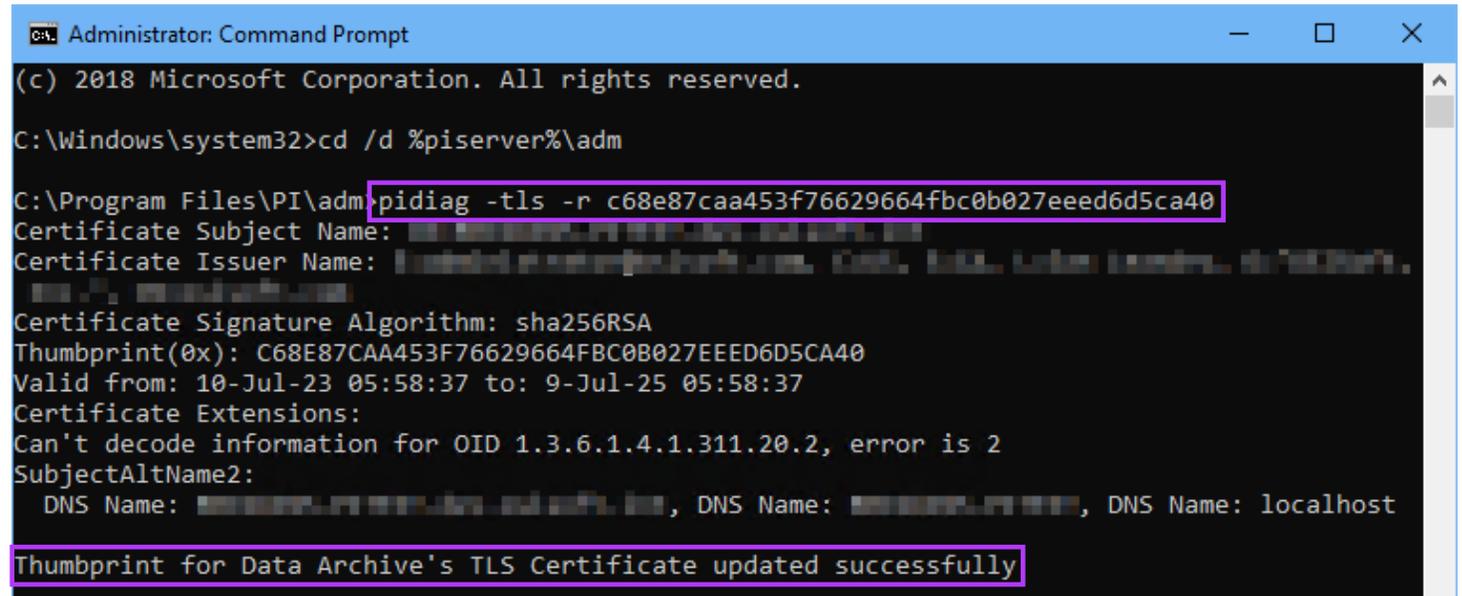
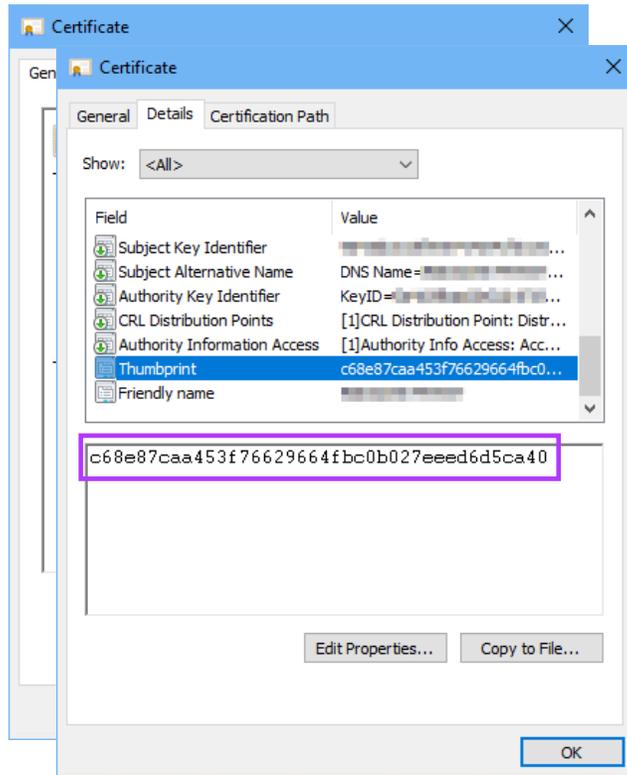


# Applying and checking certificates

## AVEVA PI System Data Archive

Change certificate at a later time (Using **pidiag**)

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

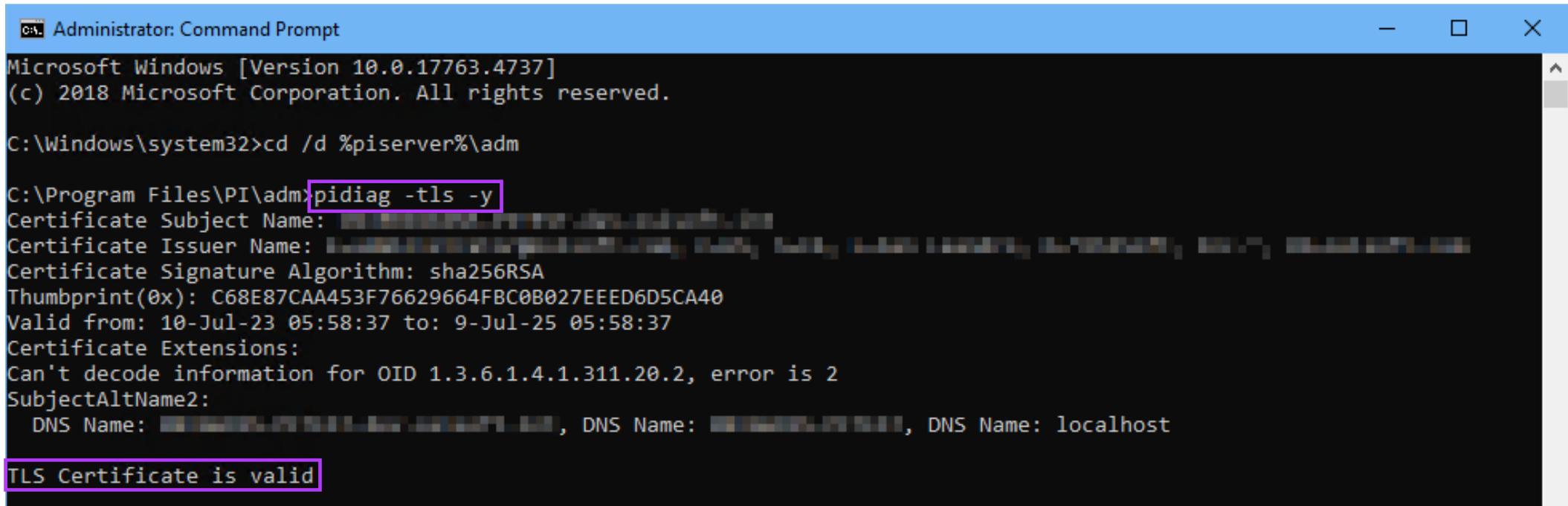


# Applying and checking certificates

## AVEVA PI System Data Archive

Verify current certificate (Using **pidiag**)

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



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.4737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd /d %piserver%\adm

C:\Program Files\PI\adm>pidiag -tls -y
Certificate Subject Name: [redacted]
Certificate Issuer Name: [redacted]
Certificate Signature Algorithm: sha256RSA
Thumbprint(0x): C68E87CAA453F76629664FBC0B027EEED6D5CA40
Valid from: 10-Jul-23 05:58:37 to: 9-Jul-25 05:58:37
Certificate Extensions:
Can't decode information for OID 1.3.6.1.4.1.311.20.2, error is 2
SubjectAltName2:
  DNS Name: [redacted], DNS Name: [redacted], DNS Name: localhost

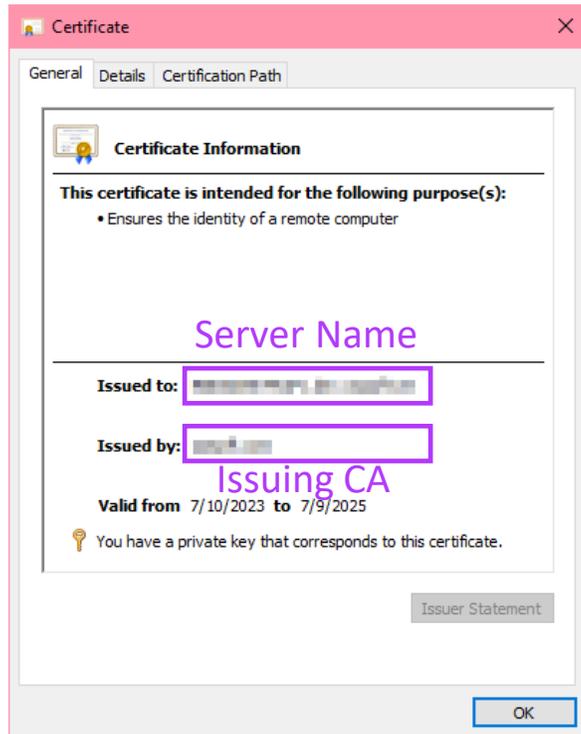
TLS Certificate is valid
```

# Applying and checking certificates

## AVEVA PI System Asset Framework (AF)

Change certificate at a later time (Using **AFDiag**)

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

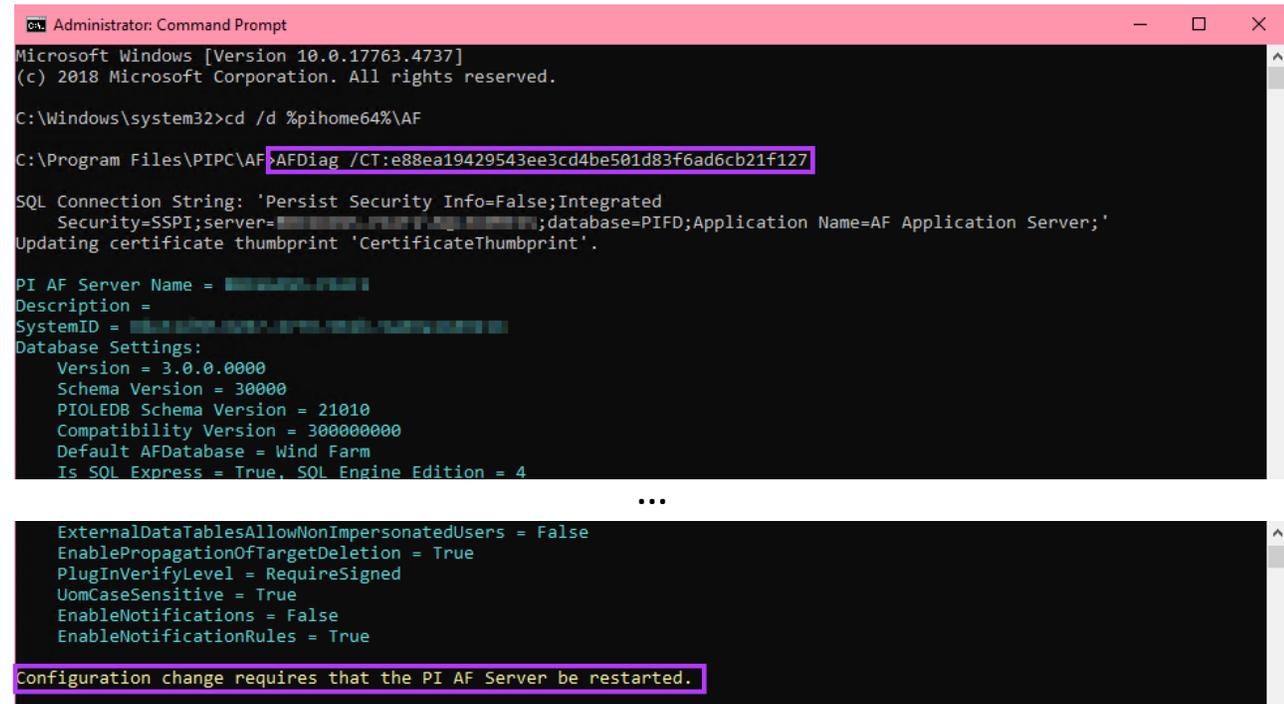
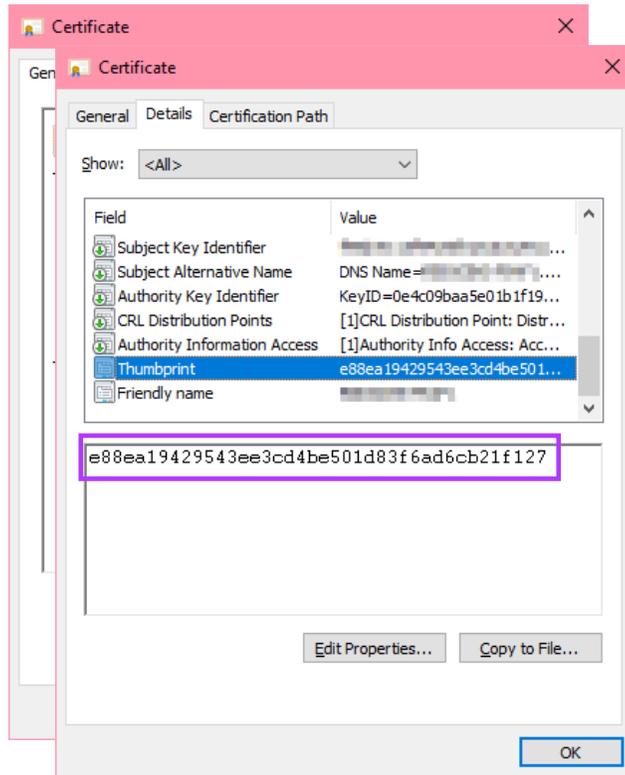


# Applying and checking certificates

## AVEVA PI System Asset Framework (AF)

Change certificate at a later time (Using **AFDiag**)

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

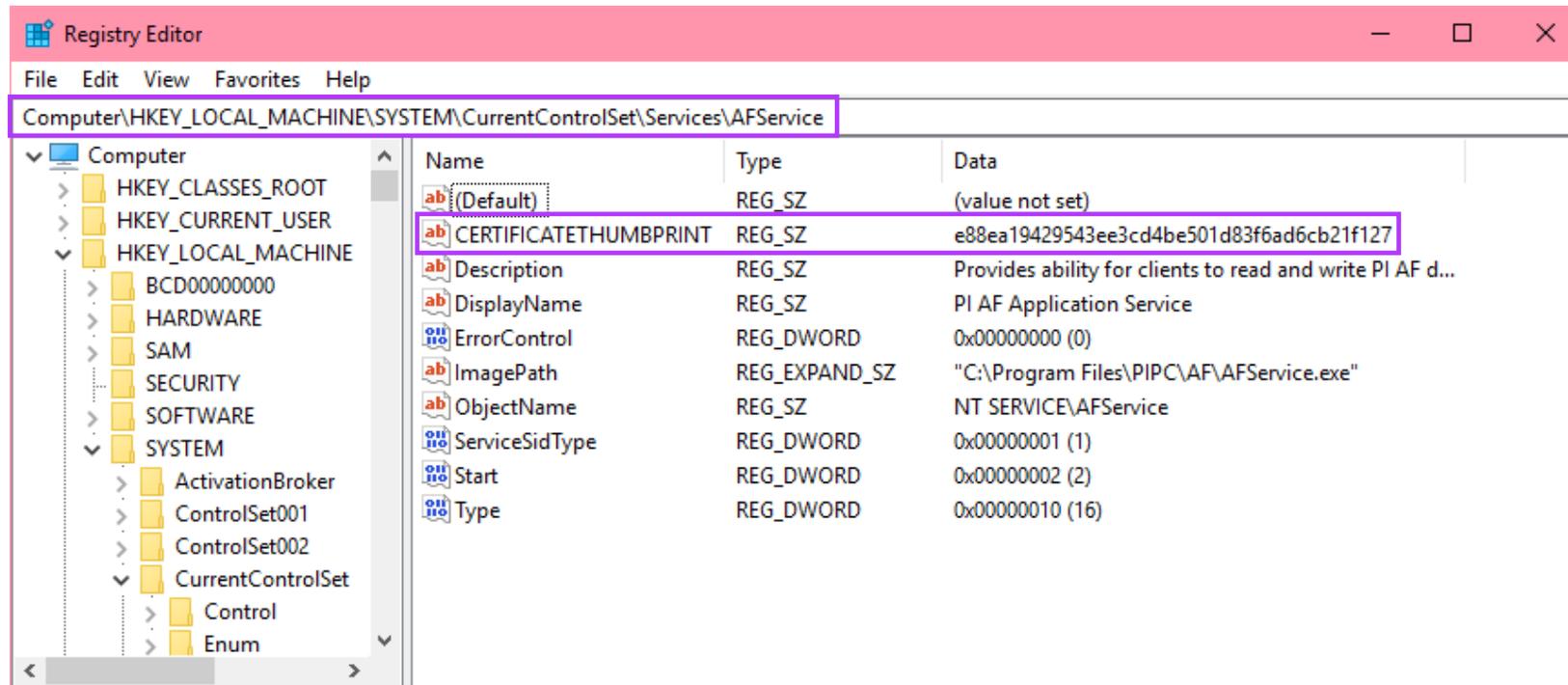


# Applying and checking certificates

## AVEVA PI System Asset Framework (AF)

Verify current certificate (Using registry)

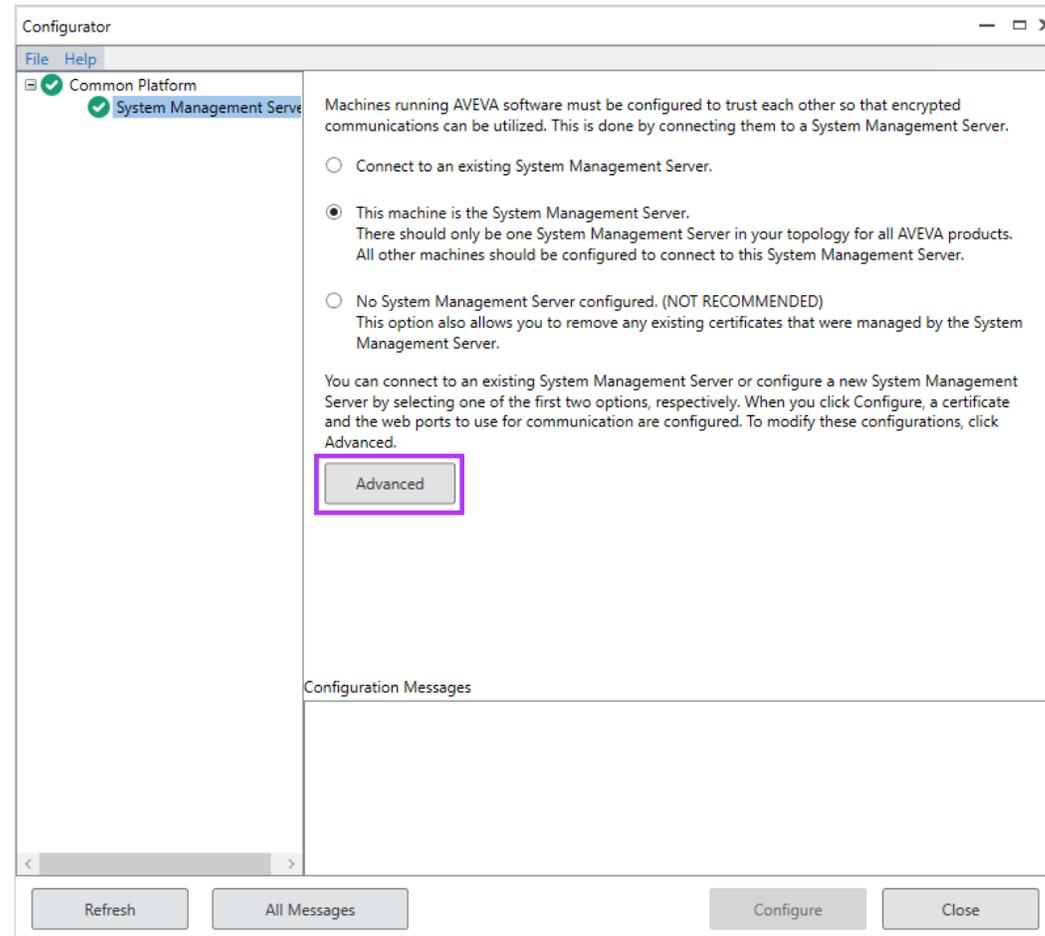
- Computer\HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\AFService
- CERTIFICATETHUMBPRINT



# Applying and checking certificates

## AVEVA Identity Manager (AIM)

Select certificate through configurator



# Applying and checking certificates

## AVEVA Identity Manager (AIM)

Select certificate through configurator

Advanced Configuration

Certificates Ports

In order to enable communications via encrypted channels (e.g. HTTPS), certificates are required to be configured.

Certificates can either be provided by your IT department or automatically generated.

Configuration

Please select the appropriate options below.

Certificate Source: Provided by IT (import / select) Import

Certificate: RBIGGINS-PITEST Details

- RBIGGINS-PITEST
- RBIGGINS-PITEST ASB OPC UA Server
- WMSVC-SHA2

OK Cancel

---

# OpenID Connect (OIDC) authentication

Claims in AVEVA PI System

**AVEVA**

---

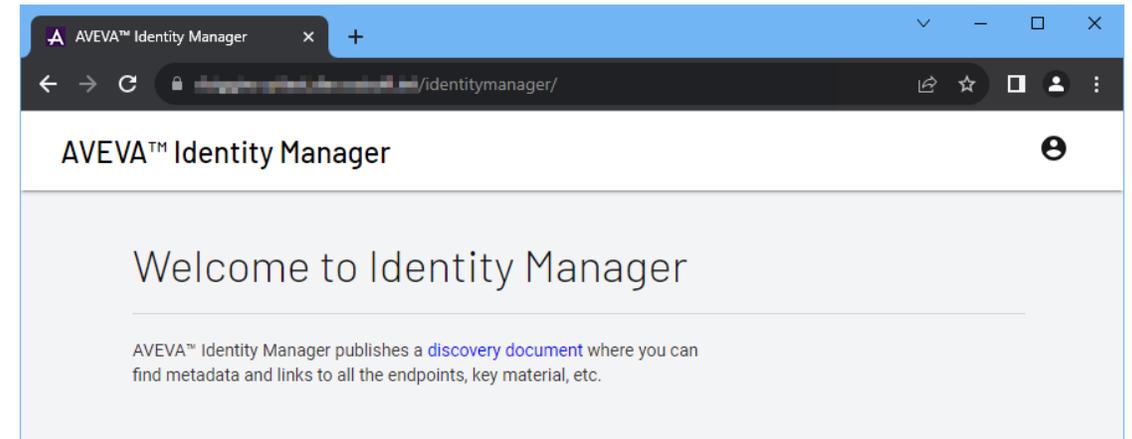
# OpenID Connect (OIDC) authentication

- 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

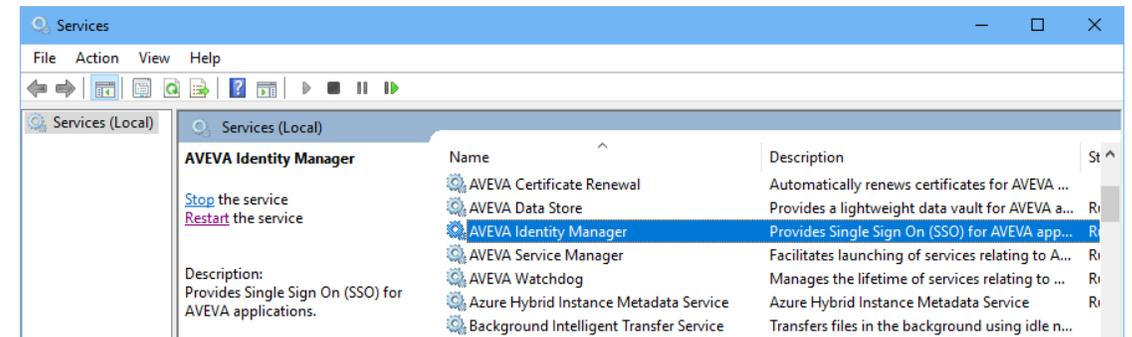
For a full discussion of technical details, benefits, and reasons behind the feature introduction, see the presentation [Introduction to claims authentication](#)

# 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



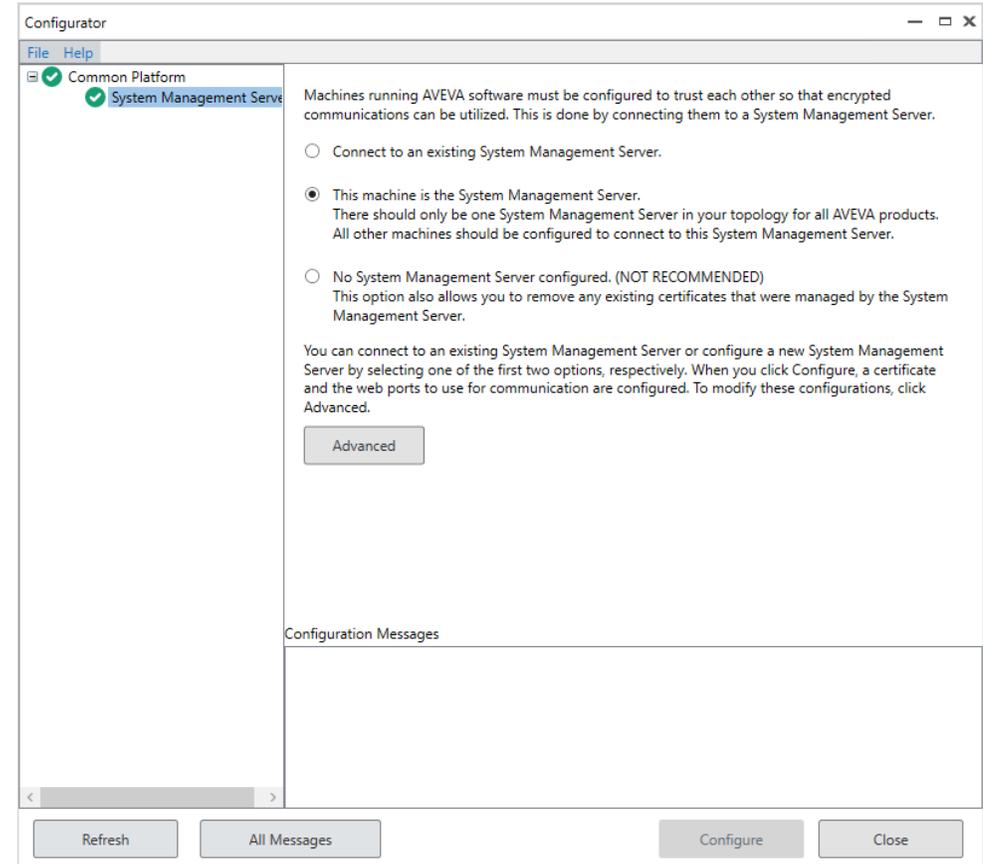
Accessing AIM endpoint via browser



Configurator application

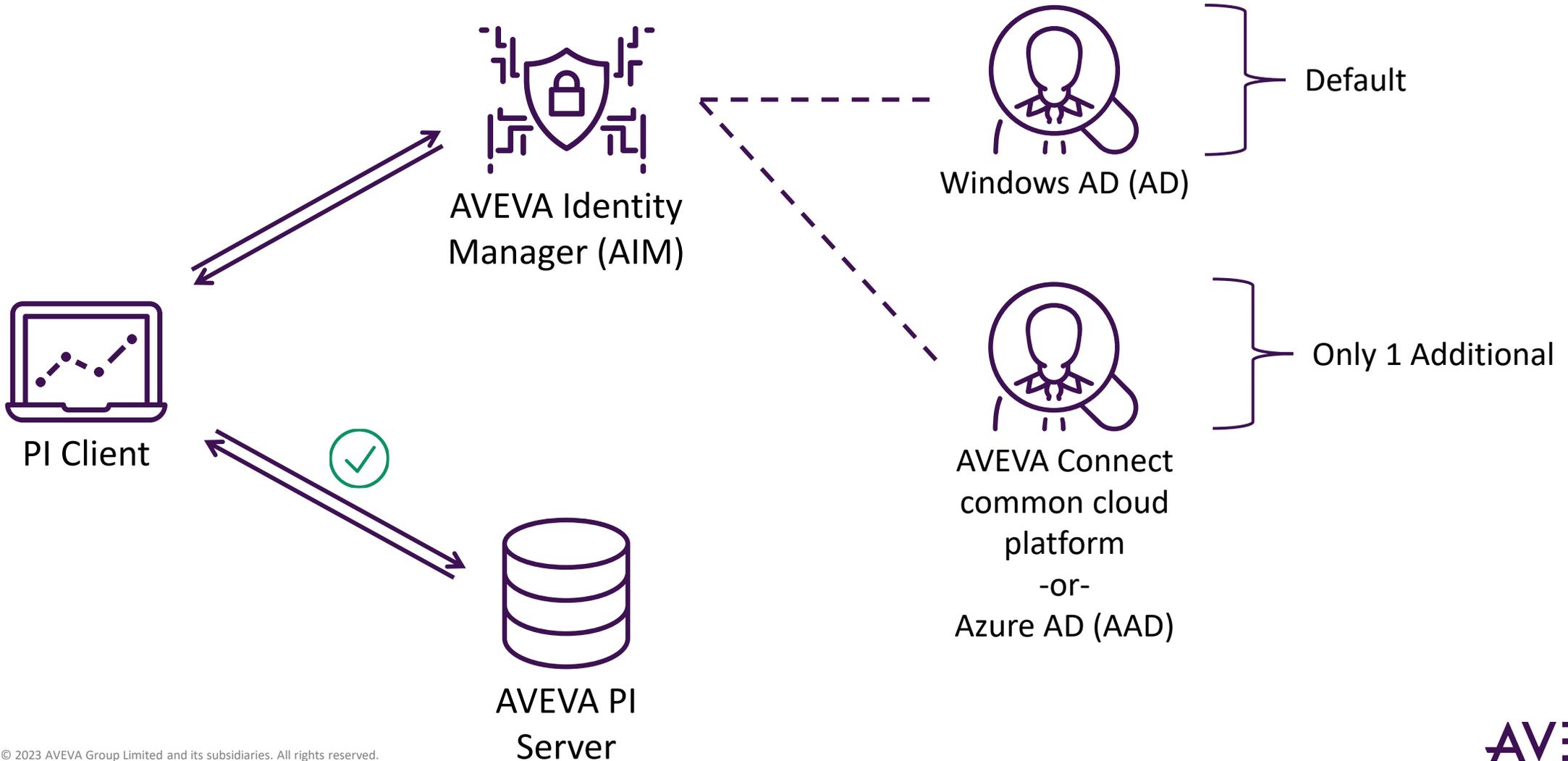
# AVEVA™ Identity Manager (AIM)

- “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

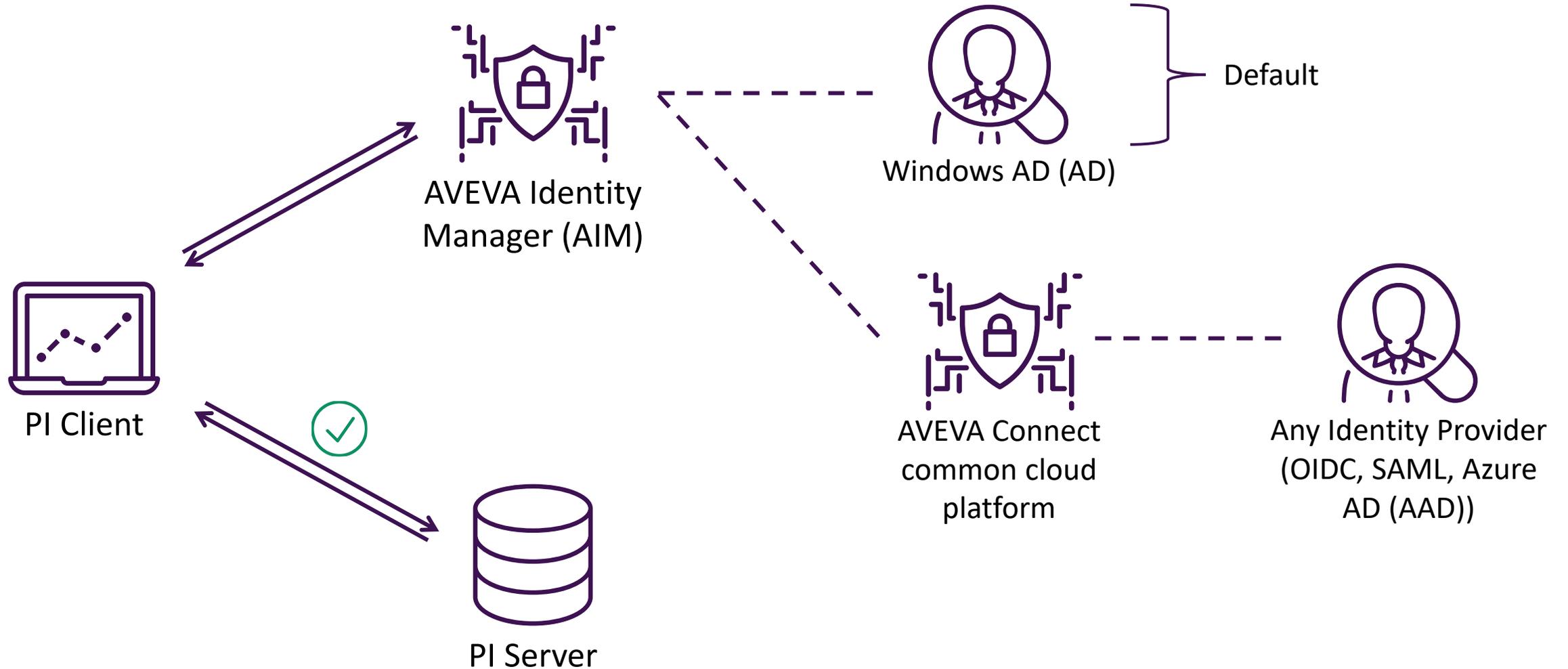


Configurator application

# 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 [connect.support@aveva.com](mailto:connect.support@aveva.com) 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

---

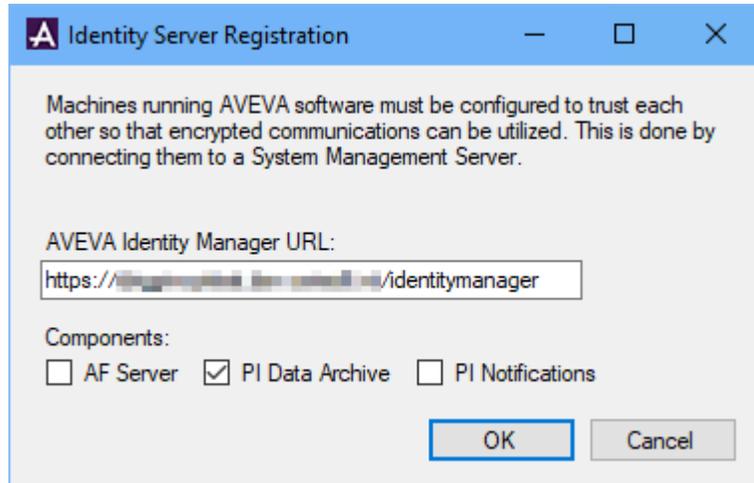
# Registering AVEVA™ PI Server components with AIM

## AVEVA.PI.OIDCConfigurationTool.exe

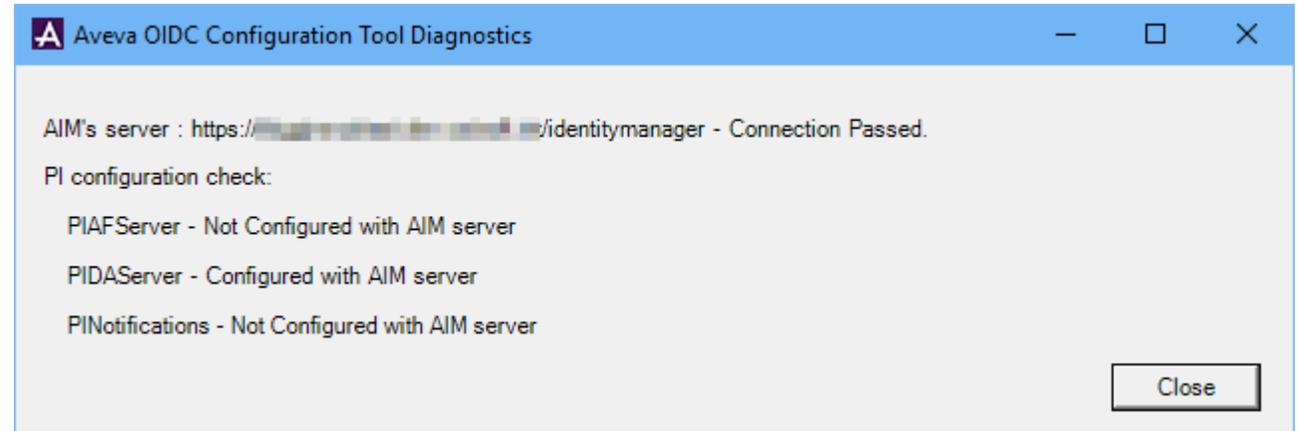
- Perform this task locally on each server where an AVEVA PI Server component resides
  - i.e. Register the asset framework server with AIM from the asset framework server; register the data archive server with AIM from the data archive server
- Use **AVEVA.PI.OIDCConfigurationTool.exe**
  - Can be run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



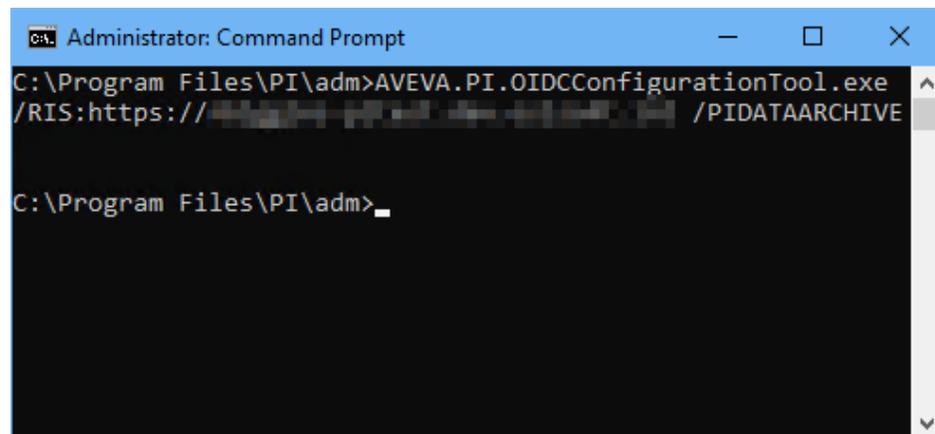
Interactive registration



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

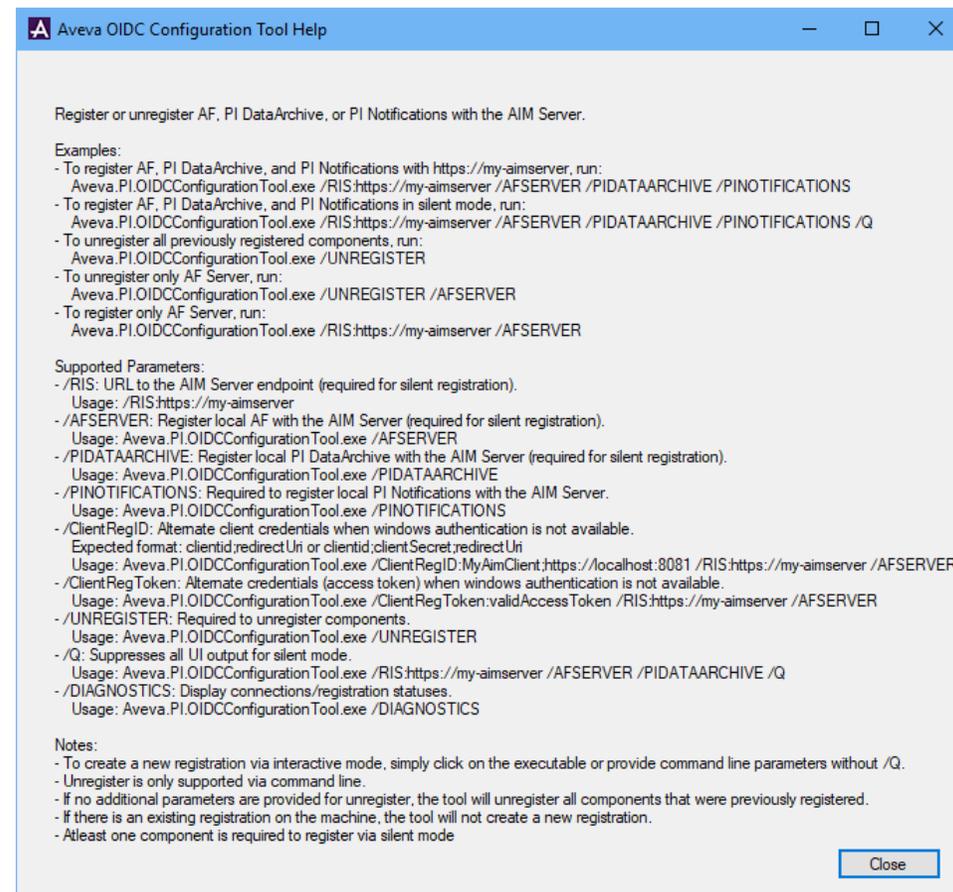
# Registering AVEVA™ PI Server components with AIM

## AVEVA.PI.OIDCConfigurationTool.exe



```
C:\Program Files\PI\adm>AVEVA.PI.OIDCConfigurationTool.exe /RIS:https:// /PIDATAARCHIVE  
C:\Program Files\PI\adm>
```

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



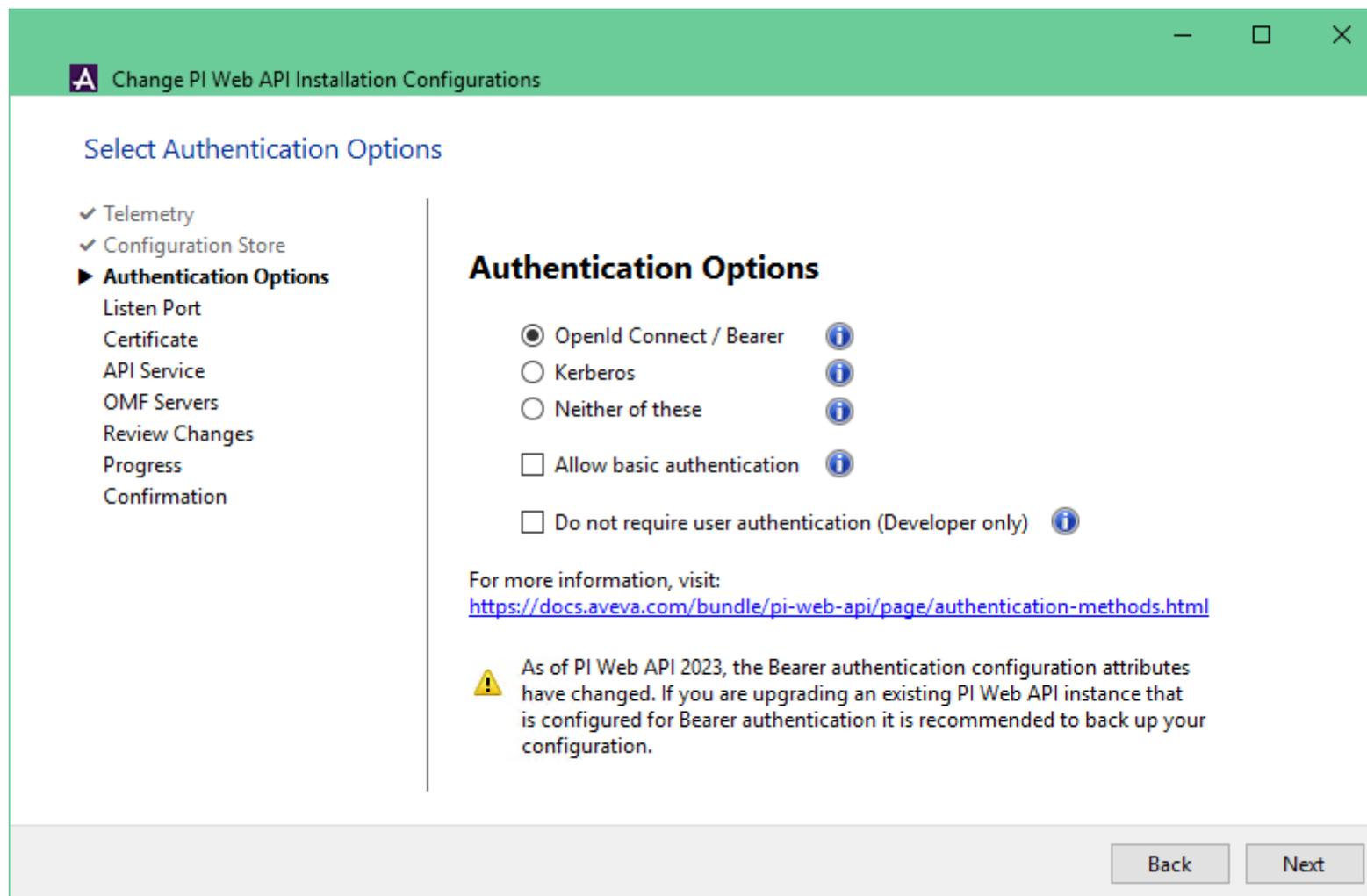
List options and examples  
from Command Prompt with **/HELP** parameter

---

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

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

# Registering PI Web API with AIM



The screenshot shows a window titled "Change PI Web API Installation Configurations" with a green header bar. The main content area is titled "Select Authentication Options". On the left, there is a navigation menu with the following items: "Telemetry" (checked), "Configuration Store" (checked), "Authentication Options" (expanded), "Listen Port", "Certificate", "API Service", "OMF Servers", "Review Changes", "Progress", and "Confirmation". The "Authentication Options" section contains the following settings:

- OpenId Connect / Bearer ⓘ
- Kerberos ⓘ
- Neither of these ⓘ
- Allow basic authentication ⓘ
- Do not require user authentication (Developer only) ⓘ

Below the options, there is a link for more information: <https://docs.aveva.com/bundle/pi-web-api/page/authentication-methods.html>. A warning icon and text state: "As of PI Web API 2023, the Bearer authentication configuration attributes have changed. If you are upgrading an existing PI Web API instance that is configured for Bearer authentication it is recommended to back up your configuration." At the bottom right, there are "Back" and "Next" buttons.

# Registering AVEVA™ PI Vision™ with AIM

The screenshot shows the 'Security' configuration page in the AVEVA PI Vision Administration interface. The page is titled 'Security' and has two tabs: 'Identity' (selected) and 'User Access Levels'. The 'Identity' tab contains the following settings:

- Identity AF Server:** A dropdown menu with a redacted value.
- Authentication Mode:** Radio buttons for 'Windows' and 'OpenID Connect' (selected).
- 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:** A button that triggers a text input field containing 'https://[redacted]/PIVision/'.
- Copy this command and run in command prompt on the PI Vision server machine.** A text area containing the following command:

```
"%PIHOME64%PIVisionUtilities\RegisterPIVisionIdentityClient.exe" \  
/IdentityServerURL:"https://[redacted]/identitymanager" \  
/AppPoolIdentity:"NT AUTHORITY\NETWORK SERVICE" \  
/PIVisionUrl:"https://[redacted]/PIVision/"
```

A 'Copy' button is located to the right of the command text.
- Save:** A button at the bottom left of the configuration area.

---

# 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
  3. (**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.

```
Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Create-ClientID-and-Secret.ps1 X
1 Add-IdentityManagerClient -HostBase https://[redacted] -Id TESTCLIENT -Secret SWORDFISH

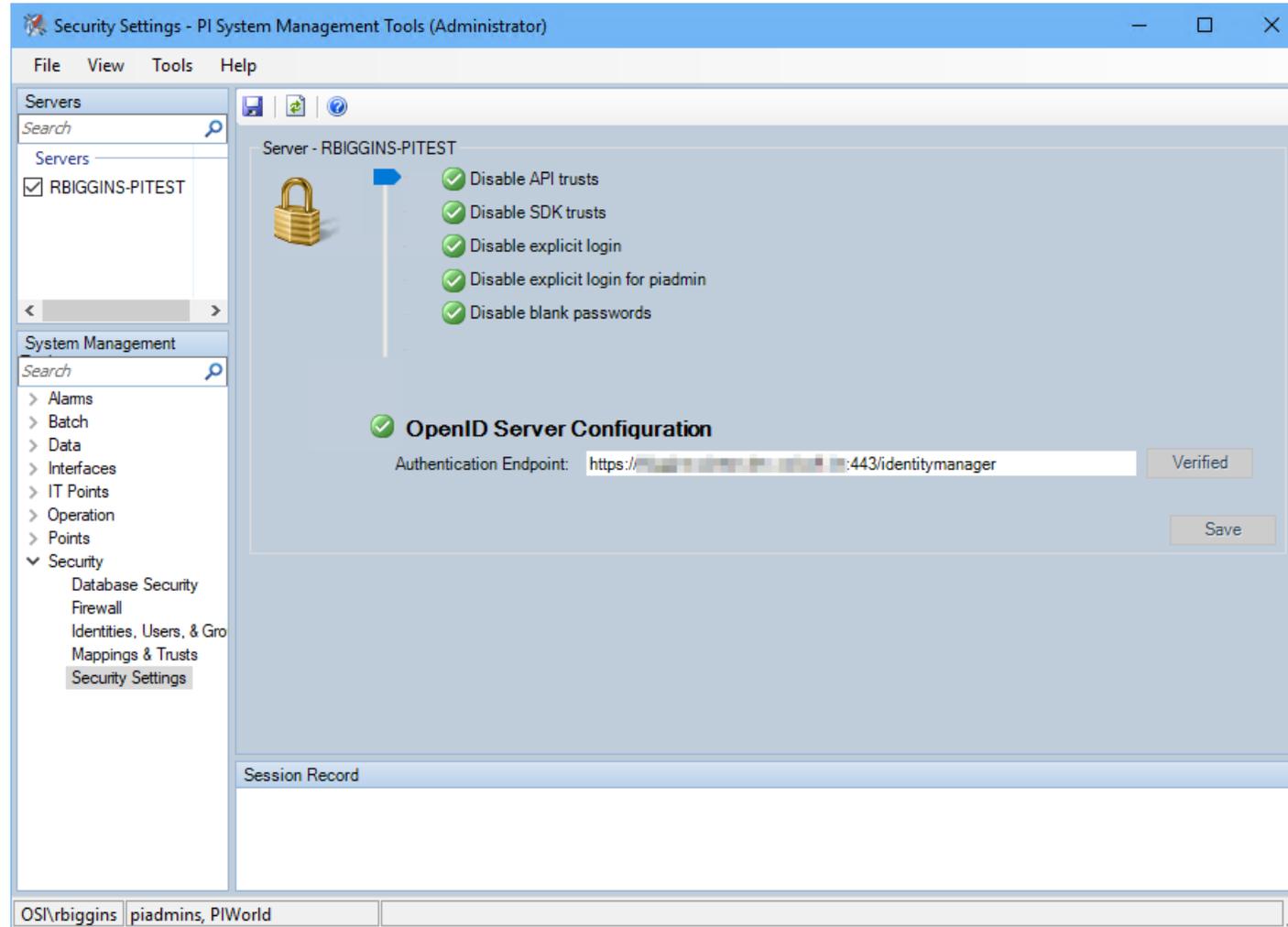
PS C:\Windows\system32> [redacted] Create-ClientID-and-Secret.ps1

ClientId                : TESTCLIENT
ClientName              :
ClientSecret            : SWORDFISH
ClientSecretHashed     :
ClientUri               :
LogoUri                :
AccessTokenType         : Jwt
AllowedGrantTypes       : {}
AllowedCorsOrigins     : {}
Enabled                 : True
PostLogoutRedirectUri  : {}
RedirectUri             : {}
ScopeRestrictions      : {}
AccessTokenLifetime    : 01:00:00
AuthorizationCodeLifetime : 00:05:00
SlidingRefreshTokenLifetime : 15.00:00:00
IdentityTokenLifetime  : 00:05:00
AllowRememberConsent   : True
RequireClientSecret    : True
RequireConsent         : True
RequirePkce            : False
AlwaysIncludeUserClaimsInIdToken : False
AlwaysSendClientClaims : False
AllowOfflineAccess     : False
RefreshTokenExpiration : Absolute
RefreshTokenUsage      : OneTimeOnly
UpdateAccessTokenClaimsOnRefresh : False
AbsoluteRefreshTokenLifetime : 30.00:00:00
AllowXFrameCrossOrigin : False
SkipLoggedOutPage     : False
ExcludeRoleClaims     : False
UseLegacyJwtTokenType  : False

PS C:\Windows\system32>

Completed | Ln 40 Col 25 | 100%
```

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



# Creating AVEVA™ PI Data Archive mappings for OIDC

## AVEVA PI System Management Tools (SMT)

**Add New Mapping**

Server: [Dropdown]

Authentication:  Windows  Open ID Connect

Role: Required [Dropdown]

Role ID: [Text]

Description: [Text Area]

PI Identity: Required [Dropdown]

Mapping is disabled

Buttons: Create, Cancel

AVEVA™ Identity Manager

AVEVA

User name  
Please type your username or email

Password  
Please type your password

Sign In

Windows integrated login

# Creating AVEVA™ PI Data Archive mappings for OIDC

## AVEVA PI System Management Tools (SMT)

**Add New Mapping**

Server: [Dropdown]

Authentication:  Windows  Open ID Connect

Role: [Text Box: Required] ...

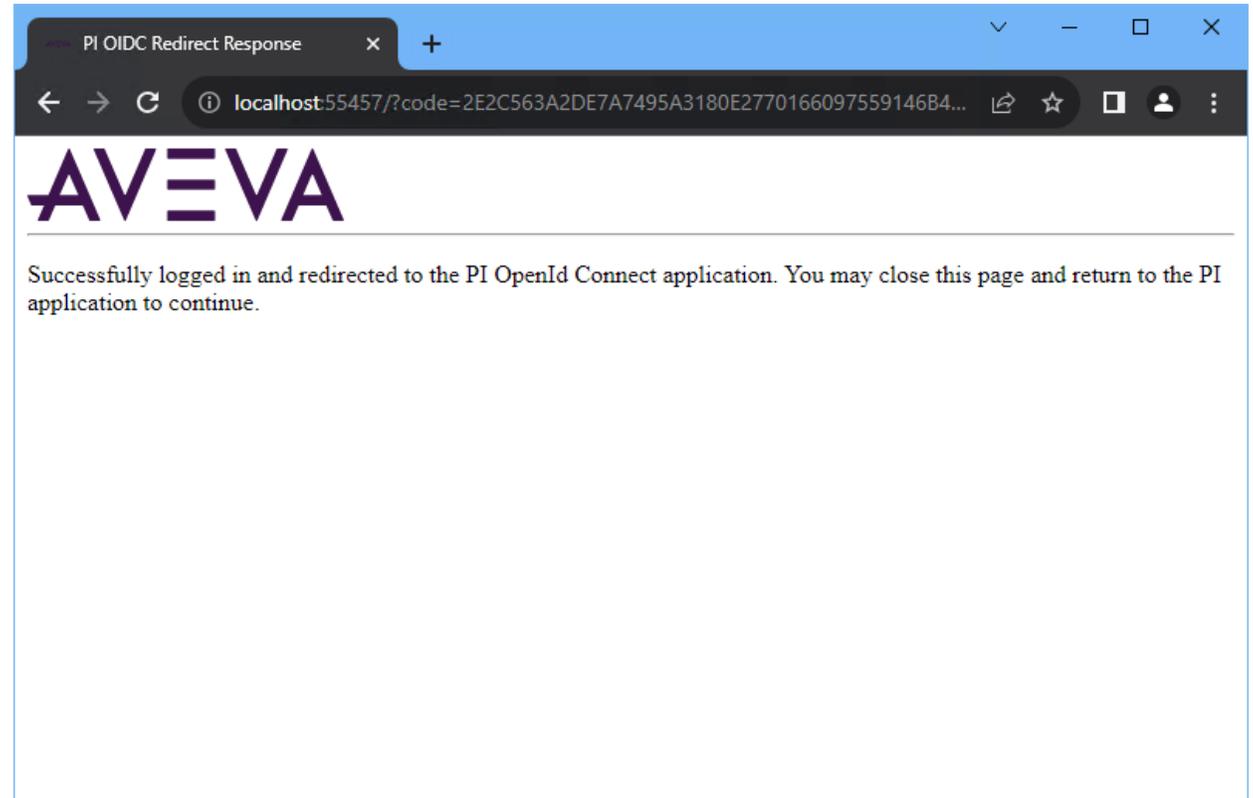
Role ID: [Text Box] ↻

Description: [Text Area]

PI Identity: [Text Box: Required] ...

Mapping is disabled

Create Cancel

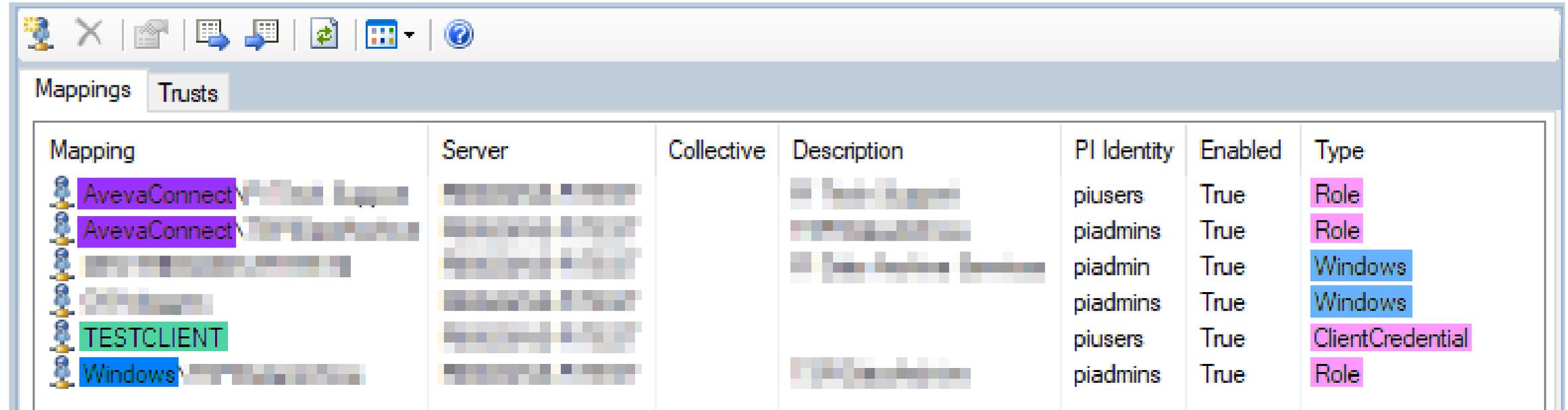






# Creating AVEVA™ PI Data Archive mappings for OIDC

## AVEVA PI System Management Tools (SMT)



The screenshot shows the 'Trusts' tab in the AVEVA PI System Management Tools (SMT) interface. The interface includes a toolbar at the top with various icons for navigation and actions. Below the toolbar, there are two tabs: 'Mappings' and 'Trusts', with 'Trusts' currently selected. The main area displays a table with the following columns: Mapping, Server, Collective, Description, PI Identity, Enabled, and Type. The table contains six rows of data, with some cells highlighted in color.

Mapping	Server	Collective	Description	PI Identity	Enabled	Type
AvevaConnect				piusers	True	Role
AvevaConnect				piadmins	True	Role
				piadmin	True	Windows
				piadmins	True	Windows
TESTCLIENT				piusers	True	ClientCredential
Windows				piadmins	True	Role

# Creating asset framework mappings for OIDC

## AVEVA PI System Explorer (PSE)

Security Mapping Properties

General

Role (A): *Enter or Select a Role*

Role ID:

Name:

Description:

Identity: *Select an Identity*

Windows  OpenID Connect

OK Cancel

AVEVA™ Identity Manager

AVEVA

User name  
Please type your username or email

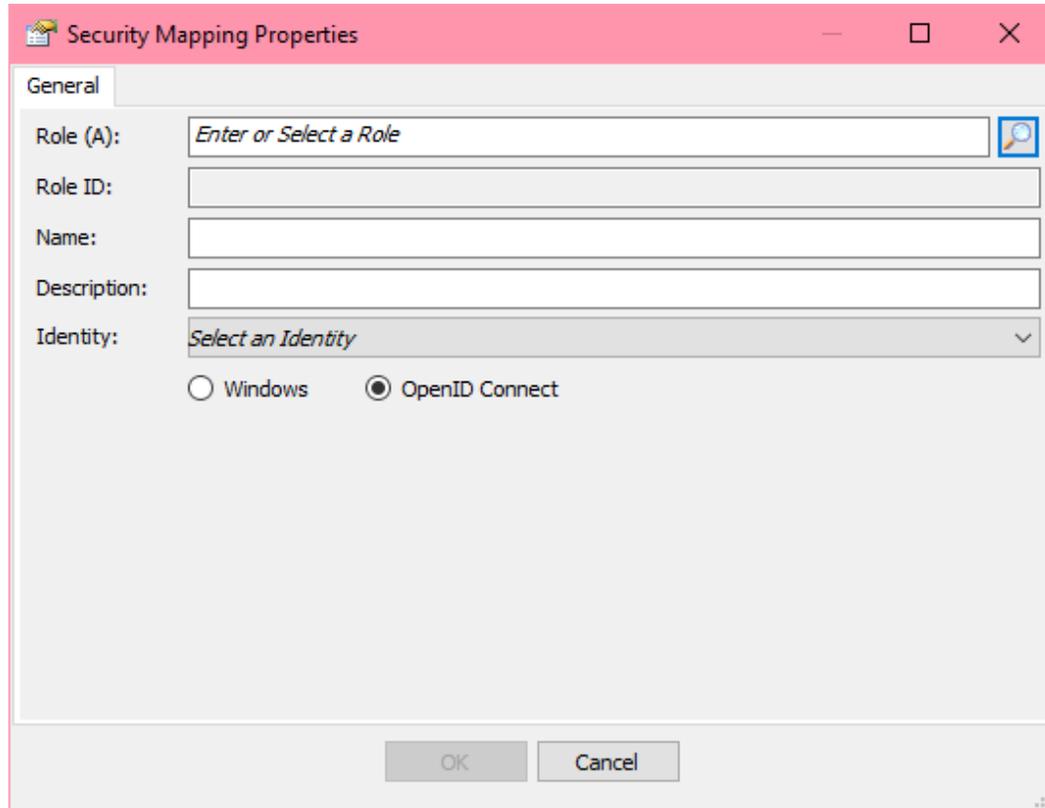
Password  
Please type your password

Sign In

Windows integrated login

# Creating asset framework mappings for OIDC

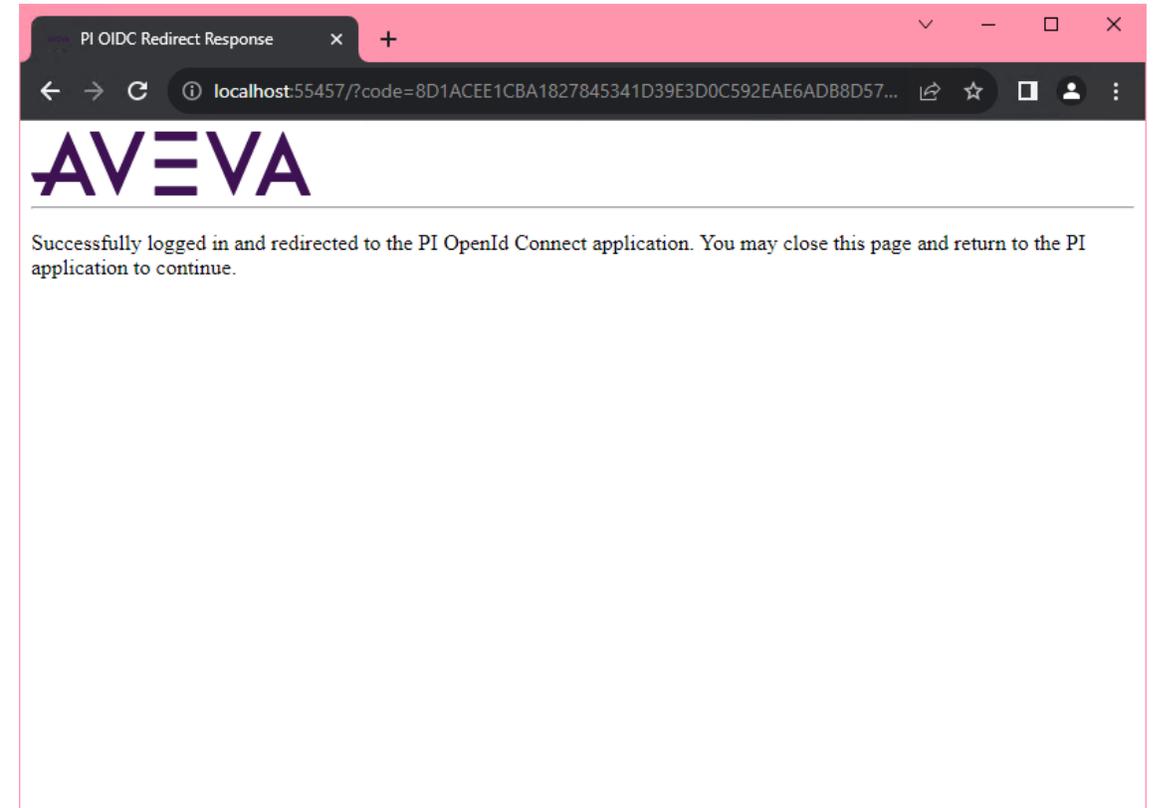
## AVEVA PI System Explorer (PSE)



The screenshot shows the 'Security Mapping Properties' dialog box with the 'General' tab selected. The fields are as follows:

- Role (A):
- Role ID:
- Name:
- Description:
- Identity:
- Authentication:  Windows  OpenID Connect

Buttons: OK, Cancel

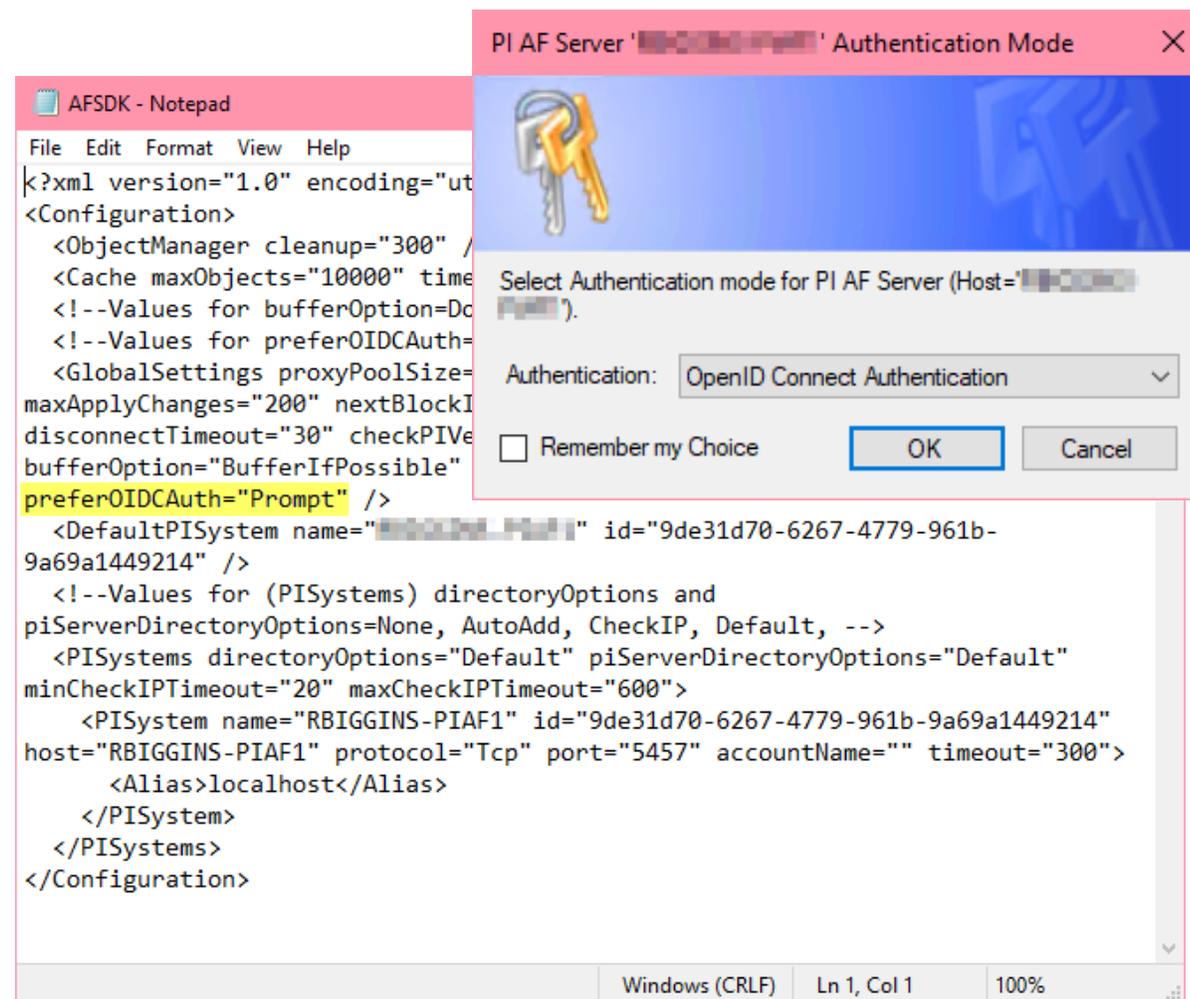






# Set preference for PI AF SDK clients

- 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

---

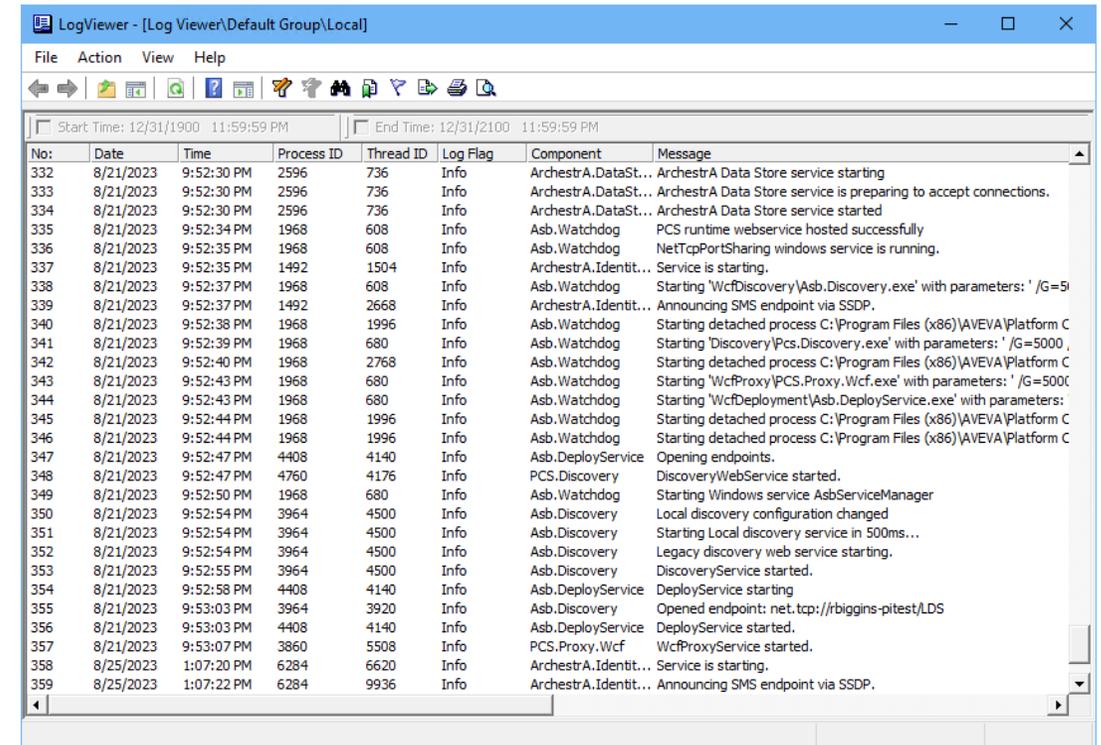
# Troubleshooting tips

- 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

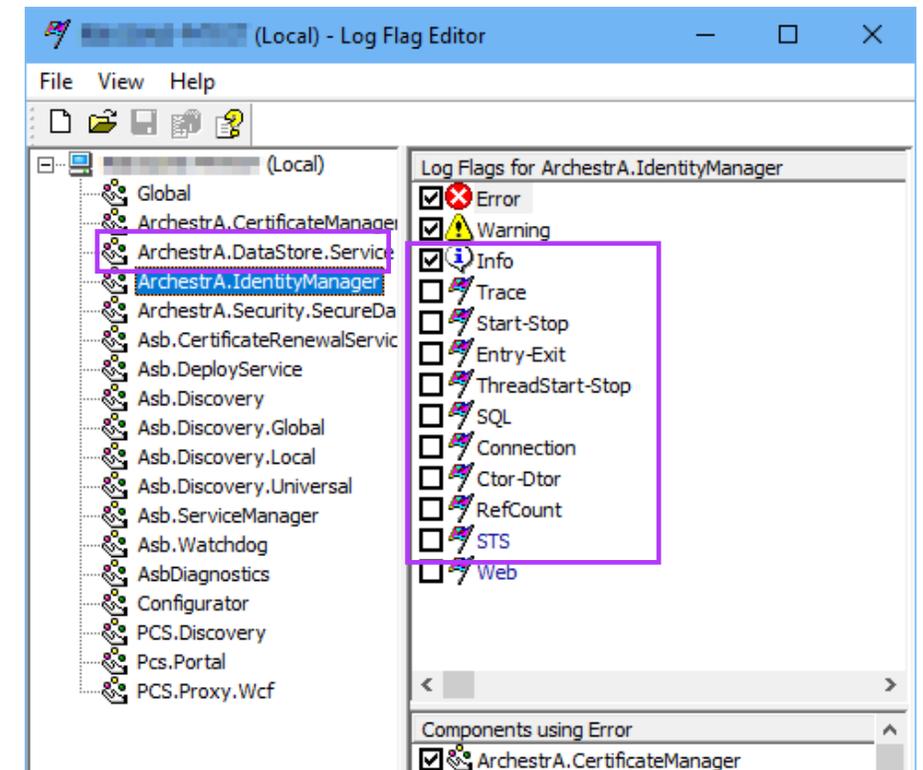


aaLogViewer application

# 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 ArcestrA Log Viewer
  - Located at **C:\Program Files (x86)\Common Files\ArcestrA\aaLogViewer.exe**
5. Go to **Actions > Log Flags** and enable all log flags for **ArcestrA.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.

 [linkedin.com/company/aveva](https://www.linkedin.com/company/aveva)

 [@avevagroup](https://twitter.com/avevagroup)

#### 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](https://www.aveva.com)