

WEDNESDAY, OCTOBER 25, 2023

Best practices for security in AVEVA™ PI System™

Presented By:

Ryan Biggins - AVEVA

Roger Ward - AVEVA

AVEVA



Ryan Biggins

Senior Technical Support Engineer I

- AVEVA
- ryan.biggins@aveva.com



Agenda

AVEVA PI System security
best practices

- Firewall
- Windows OS & security applications
- AVEVA™ PI Server versioning
- Authentication
- Authorization
- Security recommendations
- AVEVA PI System backups
- Questions

Lines of defense

Outermost

Innermost

Firewall

Configure server specific firewall rules to secure network traffic

AVEVA PI™ System™ data archive

Connecting to the data archive: Required firewall ports

Directions are in relation to the machine running the data archive

| Functionality | Remote Application | Protocol | Port | Direction |
|--|-------------------------|----------|---------|-----------|
| Client connections to data archive | All client applications | TCP | 5450 | Inbound |
| SPN registration (PI Mappings) | Domain controller | TCP/UDP | 135 | Outbound |
| Kerberos (PI Mappings) | Key distribution center | TCP/UDP | 88 | Outbound |
| NTLM (PI Mappings) | Domain controller | TCP/UDP | Dynamic | Outbound |
| IP/Host lookup (PI Trust) | DNS | UDP | 53 | Outbound |
| Domain/OS user lookup (PI Trust) | Domain controller | TCP/UDP | Dynamic | Outbound |
| MDB to asset framework synchronization | Asset framework server | TCP | 5457 | Outbound |

Full List: [Port requirements for PI Data Archive](#)

Asset framework server

Asset framework server: Required inbound firewall ports

Directions are in relation to the machine running the asset framework server

| Functionality | Remote Application | Protocol | Port | Direction | Service |
|---|--|----------|------|-----------|-----------------------------|
| PI AF SDK client connections to asset framework server | PI AF SDK clients (PI System Explorer, etc.) | TCP | 5457 | Inbound | Asset framework app service |
| PI SQL for asset framework client connections to PI AF Server | PI SQL for asset framework clients (PI OLEDB Enterprise, etc.) | TCP | 5459 | Inbound | Asset framework app service |
| Client connections to PI Analysis Service | PI AF SDK clients (PI System Explorer, etc.) | TCP | 5463 | Inbound | PI analysis service |
| Client connections to PI Notifications Service | PI AF SDK clients (PI System Explorer, etc.) | TCP | 5468 | Inbound | PI Notifications service |

Full List: [Port requirements for PI AF Server](#); [Port requirements for PI Analysis Service](#); [Port requirements for PI Notifications Service](#)

AVEVA™ PI Server: Windows OS & security applications

Maximize security utilizing Windows available features and security applications



AVEVA™ PI Server: Anti-virus exclusion rules

File-class and folder-level filtering

Anti-virus software are complementary security solutions to block and remove known threats

However, they can impact AVEVA PI System performance or lead to data loss if configured improperly

- File-class filtering: Include/exclude files from scans based on file type
- Folder-level filtering: Include/exclude files from scans based on location within file directory

Recommendations:

- Leverage both file-class and folder-level filtering:
 - Use file-class filtering for each of the specified file types (archives, queues, and logs)
 - Apply this exclusion only to specific folders
- Routinely review/update exclusion rules
- Keep anti-virus up-to-date

AVEVA™ PI Server: Windows Server Core OS

Security on the server

Install data archive on Windows Server 2016 – 2022 Core OS

Benefits:

- Enhanced security: fewer components installed and running reduces cyber attack surface
- No memory-mapped GUI
- Minimize patch maintenance & reboots
- Lower resource usage: less disk, smaller memory/resource requirements, and lower total cost of ownership

Drawbacks:

- More difficult user experience: requires a certain level of command-line knowledge

The data archive security relies on enforcement by the Windows OS; it is important to keep Windows up-to-date

AVEVA™ PI Server: Windows security applications

Windows Defender Application Control (WDAC)

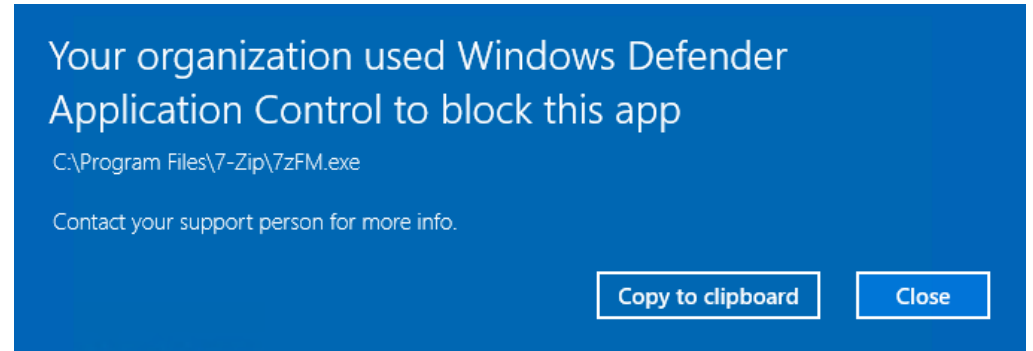
Secures server against unknown malware and other unauthorized code

Features:

- Kernel-level protection: Uses whitelisting and code integrity (CI) policies
- Ease of deployment: Managed by group policy or enterprise solutions for large-scale environments

Recommended for Windows Server 2016 - 2022 Core OS

Review hardware requirements and compatibility before implementation



AVEVA™ PI Server: Windows security applications

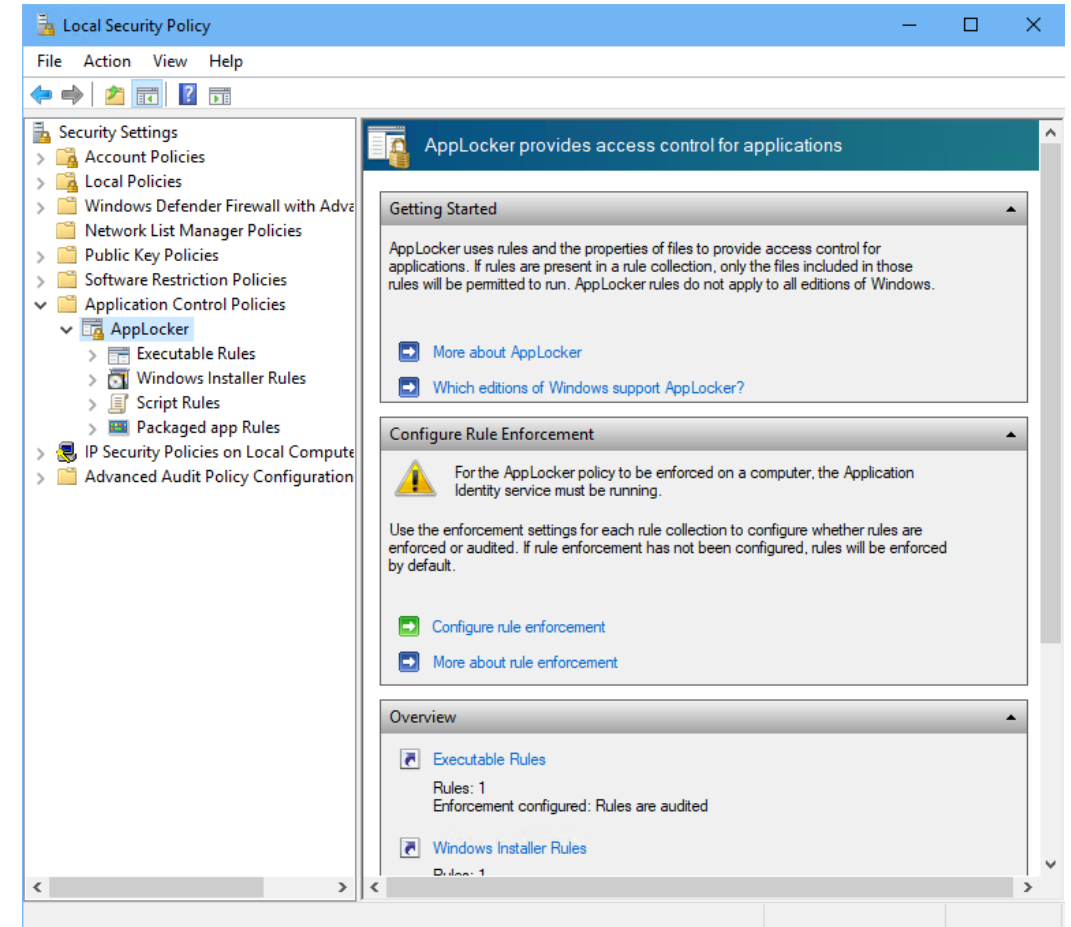
AppLocker

Gives granular control over who can execute which applications

Features:

- Whitelisting: allow specific applications
- Manage “least privileges” access to important files and applications
- **Audit-only mode (optional mode):** Violation of the configured enforcement policy is logged in event viewer, but policy itself is not enforced; ideal for testing policies before implementing

Recommended for OS earlier than Windows Server 2016 and non-Server Core OS



AVEVA™ PI Server versioning

Upgrade to the latest data archive and asset framework for new features, fixes, and enhancements



AVEVA™ PI Server

Branching releases

AVEVA PI Server 2018 SP3 Patch X (Feature-Stable)

Current release: 2018 SP3 Patch 5

AVEVA is committed to maintaining AVEVA PI Server 2018 SP3 branch which will continue to receive bug and security fixes delivered as patches

AVEVA PI Server 2023 (Fully-Featured)

First hybrid AVEVA PI Server release offering which has included integration with AVEVA™ Data Hub (cloud-based data historian)

Available for AVEVA Flex Customers

AVEVA™ PI Server 2023

New security features: high-level overview

Secure communication via TLS/SSL certificates

- Optional feature; required for OIDC Authentication and AIM
- Communication between PI Client and AVEVA PI Server natively secure for all authentication methods

OpenID Connect (OIDC) authentication via AVEVA Identity Manager (AIM)

- OIDC is an authentication protocol that uses an external identity provider to verify a user's identity and grant access to resources via access tokens
- AIM offers user authentication as a service; handles OIDC authentication in AVEVA PI System
- Single Sign-On capability

AVEVA PI Server 2023 is still backward compatible with the traditional AVEVA PI Server authentication methods

Authentication

Limit users and applications that can connect to AVEVA PI Server using the most secure authentication method



Authentication

is the process by which a user or application proves its identity to a server and forms an initial connection.

Authentication is possible through a variety of different methods in AVEVA™ PI System™.

Authentication

- Authentication methods (preference order)
 1. OpenID Connect (OIDC) (**PI Server 2023+ only**)
 2. Windows Integrated Security (WIS)
 - a. Kerberos
 - b. NTLM
 3. PI Trusts
 4. Explicit Logins (PI Users)

Most secure

Secure

Less secure

Least secure

Authentication

Windows authentication & Windows Integrated Security (WIS)

- Universal credentials: Users login/authenticate with their existing Windows accounts
- Simplifies server administration: only need to modify the Windows security configuration; data archive security can automatically reflect changes; PI Audit records can trace changes made by specific Windows users
- Secure authentication: connections are authenticated through Microsoft's Security Support Provider Interface (SSPI)
- Granular control over access permissions: data archive can have read and/or write permissions defined for any number of PI Identities for different objects within

If using OIDC authentication is not possible, Windows authentication is recommended

Authentication

Windows authentication & Windows Integrated Security (WIS)

Microsoft Security Support Provider Interface (SSPI):

- Supports two different Windows authentication protocols:
- Kerberos (**Recommended**)
 - Ticket-based authentication protocol
 - Involves server, client, and key distribution center (KDC) (on domain controller)
- NT LAN Manager (NTLM) (**Less Recommended**)
 - Challenge-response-based authentication protocol
 - Involves server and client only

For more information on Kerberos, stay tuned for the next presentation

NTLM is still more secure than authenticating through PI Trust or explicit login (PI User accounts)

Authentication

PI Trusts

Allow client applications to authenticate without a username or password

Connection information of the client application is compared against records in the PI Trust table, including:

- Application name
- IP address and netmask of the client
- Fully qualified hostname of client (such as apollo.aveva.com)
- Short hostname of client (such as apollo)

Each PI Trust is defined against a single PI Identity

When an interface successfully authenticates through a PI Trust, it gets the access permissions defined for the associated identity, group, or user

Not recommended and reserved for cases where Windows authentication cannot be used

Recommend upgrading authentication model to Windows authentication (from PI Trusts or explicit login)

Authentication

PI Trusts

Recommendations:

- Avoid “open” PI Trusts
 - PI Trusts which only specify the server name (any variety) as an identifying parameter are considered “open” PI Trusts
 - Open PI Trusts are a major security vulnerability
- If using PI Trusts is necessary, follow the 2+ Rule
 - **2+ Rule:** Include at least 2 identifying parameters for PI Trust selection:
 - Application Name + IP Address
 - Application Name + Host Name
 - Application Name + Fully Qualified Domain Name (FQDN)

Authentication

Explicit logins (PI Users)

Long ago, users connecting to the data archive were typically authenticated through explicit logins, which means the user signs on to the data archive by typing in a username and password.

By default, explicit logins are disabled, and not recommended:

- Users must sign on separately to Windows and data archive
- System managers must maintain separate user accounts for every user on data archive
- Explicit logins are the least secure way to authenticate

Recommend upgrading the authentication model to Windows authentication (from PI Trusts or explicit login)

Authorization

Set minimum access/privileges required for authenticated users and applications



Authorization

is the process by which an authenticated user is granted a set of actionable permissions within a server.

PI Identities are assigned to connecting Windows users (via PI Mappings) or to applications (via PI Trusts).

Authorization

- Security best practice: principle of least privilege
- PI Identities & PI Mappings
- PI Users & PI Groups
- PI access levels
- Point versus data security
- PI Buffer & Interface

Security best practice

Apply principle of least privilege (POLP) to the data archive

Guidelines:

- Limit user/application access to **only what is essential** for that user/application
- Restrict the number of users granted administrative privileges
- Assign permissions to user groups rather than individual users

Reduces risk for:

- Security breaches: unauthorized access to critical systems or sensitive data
- Further spread of compromises
- Misuse of privileges

PI Identities and PI Mappings

Accessing the data archive

Together, PI Identities and PI Mappings determine which Windows users or groups are authenticated on the data archive server and what authorization (access permissions) those users or groups have

Configuring Windows authentication in PI Security

- I. **PI Identity:** User category; represents a set of access permissions on the data archive server
- II. **PI Mapping:** Mechanism for associating Windows user or group to a PI Identity (or a PI User or PI Group)

Although the data archive server can use Windows security for authentication, access permission levels still need to be defined explicitly on the data archive server

PI Users and PI Groups

Related to explicit logins

- Previous versions of the data archive relied on individual user accounts (PI Users) that could be included in groups (PI Groups)
- Replaced by PI Identities & Mappings
- PI Users and PI Groups still exist for backward compatibility
- PI Users and PI Groups are not recommended

AVEVA™ PI System™ access levels

Where to configure and set permissions?

Administrative applications to modify permissions:

| Permissions | Client Tools |
|------------------|------------------------------------|
| Top-level access | PI SMT database security tool |
| PI Points | PI SMT Point Builder or PI Builder |
| PI Modules | Module database builder |

Data archive provides these standard levels of access permissions:

- *Read-only access*: Users can view the item, but they cannot edit it.
- *Write-only access*: Users can edit the item, but they cannot view it. (Special cases)
- *Read-write access*: Users can view and edit the item.
- *No access*: Users cannot view or edit the item.

Point versus data security

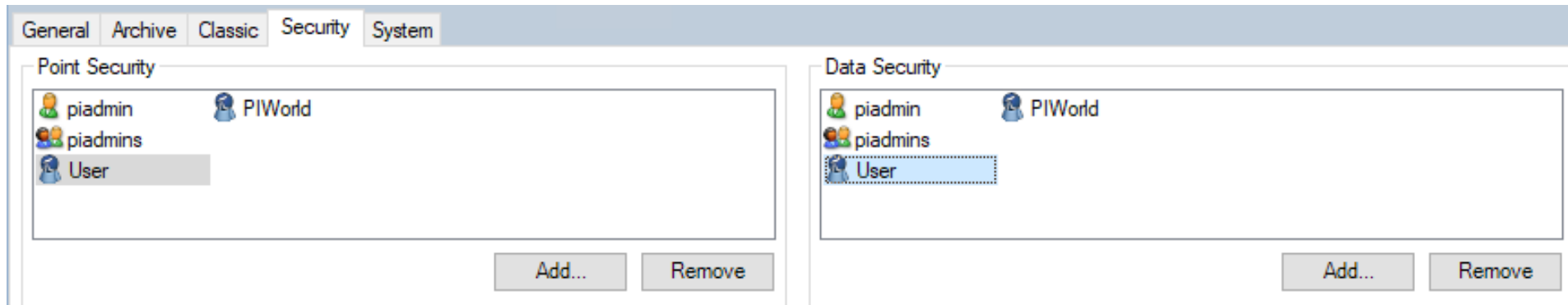
What is the difference?

Point security (PtSecurity):

Permissions to view or edit PI Point configuration parameters

Data security:

Permissions to view, edit, or write events (values and timestamps) to the PI Point



PI Buffer & AVEVA™ PI Interface

Recommended scenario: AVEVA PI Interface with PI Buffer enabled

Configure AVEVA PI Interfaces and PI Buffers to have their own PI Identities and grant the minimum permissions required to each

AVEVA PI Interface requires permission to **Read** the configuration of all their PI Points

PI Buffer requires permission to **Write** data to the PI Points

Minimum data archive permissions for AVEVA PI Interfaces with PI Buffering, no output points

| Process | Read permissions | Write permissions |
|--------------------------------|--|-------------------|
| AVEVA PI Interface | PIPoint, DBSecurity, PtSecurity & DataSecurity | None |
| PI Buffer (PIBufSS or BufServ) | None | DataSecurity |

PI Buffer & AVEVA™ PI Interface

Upgrade to the latest for Windows Integrated Security (WIS)

PI Mappings with Windows Integrated Security should be used whenever possible

- Use Windows Credential Manager if service account credentials are invalid for a PI Mapping (i.e. AVEVA PI Interface server is in a workgroup or untrusted domain)

PI Buffer Subsystem:

- PI Buffer Subsystem can natively use Windows authentication (Version 3.4.380.79+)

AVEVA PI Interface:

- With PI API for WIS (Version 2.0.1.35+), Windows authentication support is extended to the AVEVA PI Interface, or any other PI API-based application
- Before upgrading to PI API for WIS, configure PI Mappings to replace any existing PI Trusts used by AVEVA PI Interfaces
- PI Trust authentication is disabled by default on a PI client upon upgrading to PI API for WIS

Security recommendations

Simple steps to improve AVEVA PI System security



Security recommendations

Simple steps to improve AVEVA PI System security

Protect the piadmin account:

- Default administrator AVEVA PI System user account called piadmin; full permission
- For a secure environment, do not use **piadmin**; check to make sure the account has a password; use the group **piadmins** as an alternative

Require passwords on all user accounts

- Disable user accounts that do not have a password

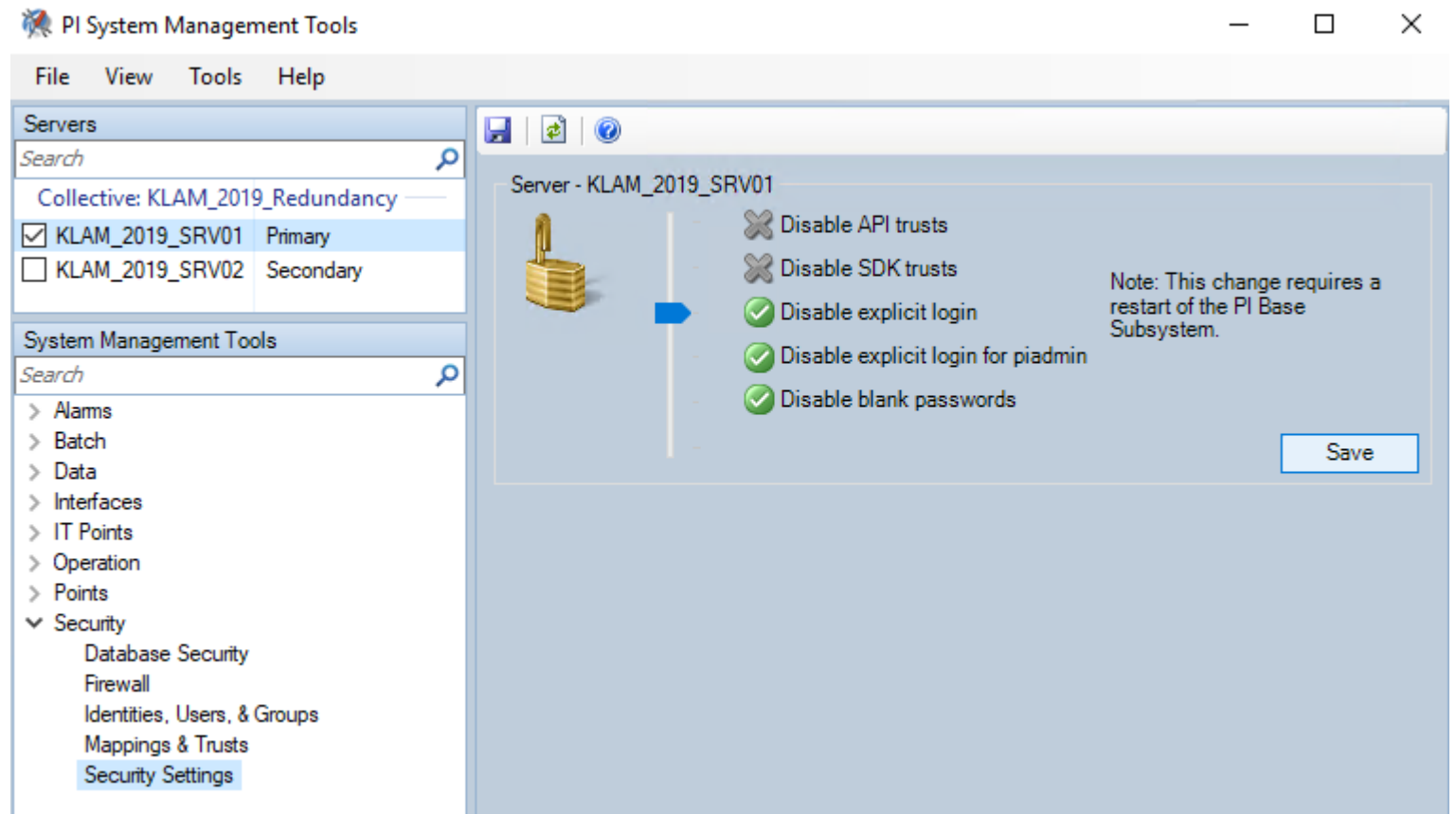
Disable all explicit logins for individual user accounts

- Disable explicit logins after configuring mappings to replace user logins

AVEVA™ PI System™ management tools: security settings

To apply the changes; set the slider to the desired security level, click “**Save**” and restart the PI Base Subsystem service.

- **Disable** explicit login
- **Disable** explicit login for piadmin
- **Disable** blank passwords



AVEVA™ PI System™ backups

Backup your data archive files



AVEVA™ PI Server backups

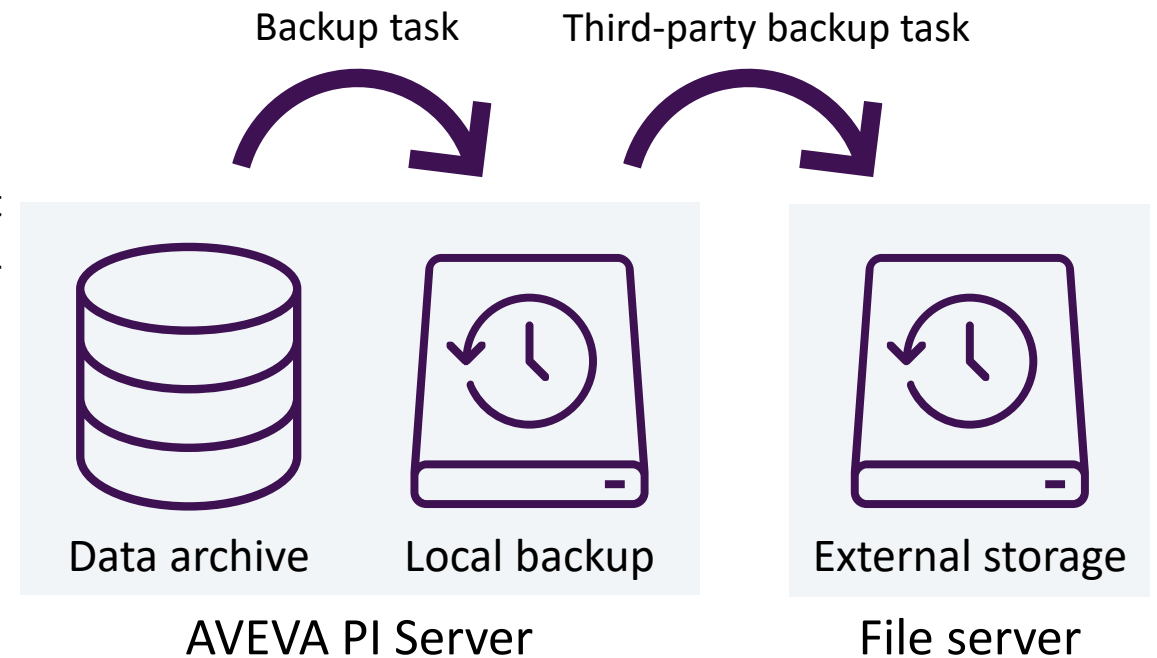
Configure daily AVEVA PI Server backups

- Schedule backups daily (off-peak hours) with Windows Task Scheduler
- Perform “incremental” backups to reduce downtime and impact
- Disaster recovery: protection against threats like ransomware or power outages and corruption; able to restore the data archive to a previous state

Two-phase backup strategy:

- I. Perform initial backup locally on the data archive
- II. Use a third-party application to copy backup files to a different server or network drive

Article: [Data archive backup best practices](#)





Resources

AVEVA PI System tech support knowledge articles:

- [Seven best practices for securing your AVEVA PI Server](#)
- [Data archive backup best practices](#)
- [Firewall port requirements](#)
- [What is the difference between point security and data security for PI Points?](#)
- [Whitelisting with Windows Defender Application Control \(WDAC\)](#)
- [Whitelisting with AppLocker](#)
- [Anti-virus Software and AVEVA PI System](#)

Kerberos



Roger Ward

Tech Support Senior Engineer

- AVEVA
- roger.ward@aveva.com



Goals

- Explain why Kerberos Authentication is best practice
- Explain what Kerberos is and how it works
- Summarize how to implement Kerberos

Agenda

Background

Kerberos 101

Configuration Checklists

Signs of a Kerberos Problem

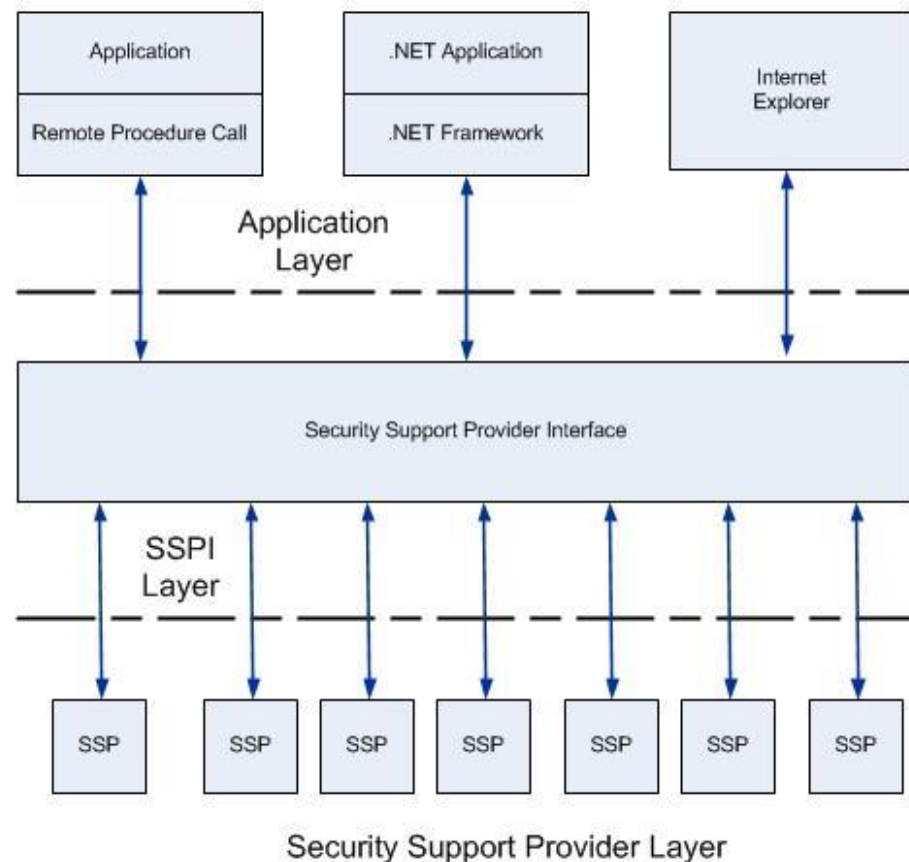
4 Troubleshooting tips

Background

SSPI & Kerberos

- When Windows authentication is required, PI applications call the Microsoft **SSPI** function.
- SSPI is an abstraction layer that allows applications to interact with various security protocols and mechanisms without needing to understand the underlying details.
- Common Windows Auth. Security Support Providers:
 - NTLM
 - Kerberos ← AVEVA best practice
 - Negotiate

Security Support Provider Interface Architecture



Alternatives to Kerberos

| Kerberos Alternative | PI Data Archive | PI Asset Framework | Drawbacks |
|----------------------|-----------------|--------------------|---|
| PI Trust | ✓ | ✗ | <ul style="list-style-type: none">• All users from the trusted client are granted the same permissions.• Spoofable |
| Basic (WIS) | ✓ | ✓ | <ul style="list-style-type: none">• Users must manually enter their creds each time they connect.• Credentials are passed across the network and are at risk of interception |
| NTLM (WIS) | ✓ | ✓ | <ul style="list-style-type: none">• Weaker encryption algos• Sometimes susceptible to Pass-the-Hash attacks |
| Negotiate (WIS) | ✓ | ✓ | <ul style="list-style-type: none">• Can fall back to NTLM if Kerb. fails |

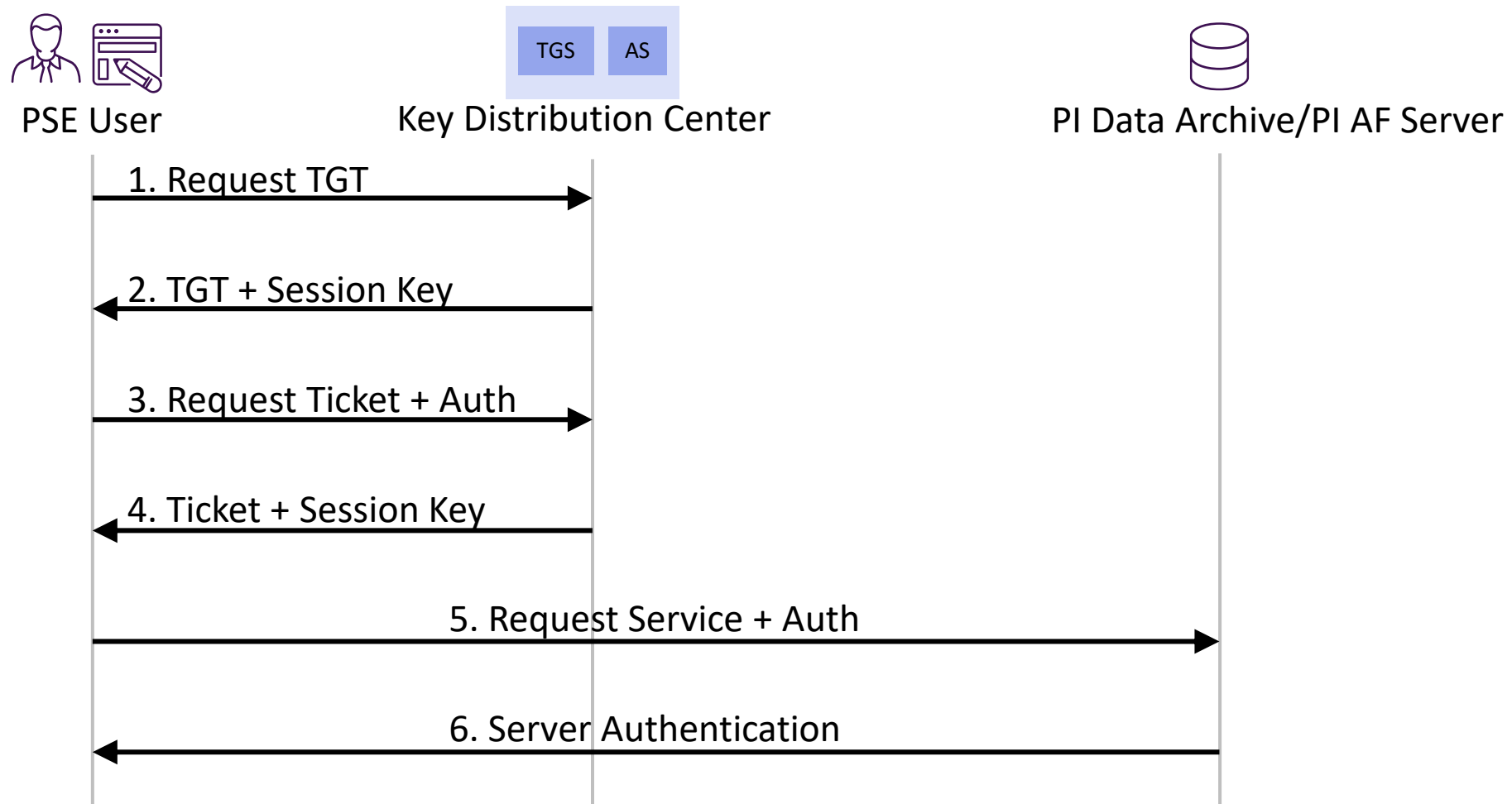
Kerberos 101

Kerberos

- Open, centralized, ticket-based authentication protocol developed by MIT in 1988
- Default authentication protocol for Windows 2000 or later when joined to Windows AD environments
- Name is derived from the three-headed dog creature from Greek mythology known as 'Kerberos'
- The three heads of the dog represent the three parties involved in the Kerberos authentication process:
 - Client
 - Server
 - Key Distribution Center (KDC)

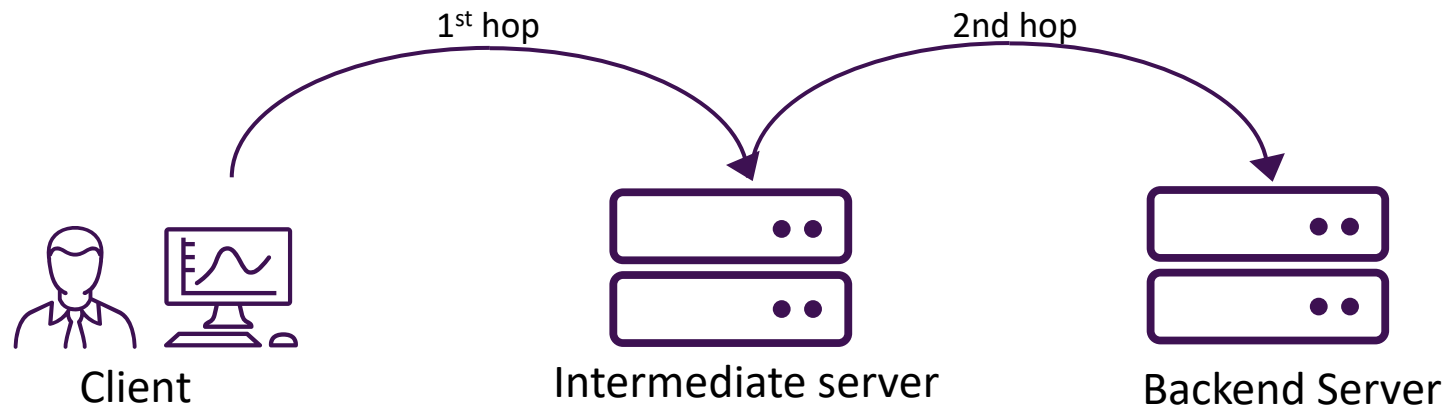


How Kerberos works



Kerberos Delegation

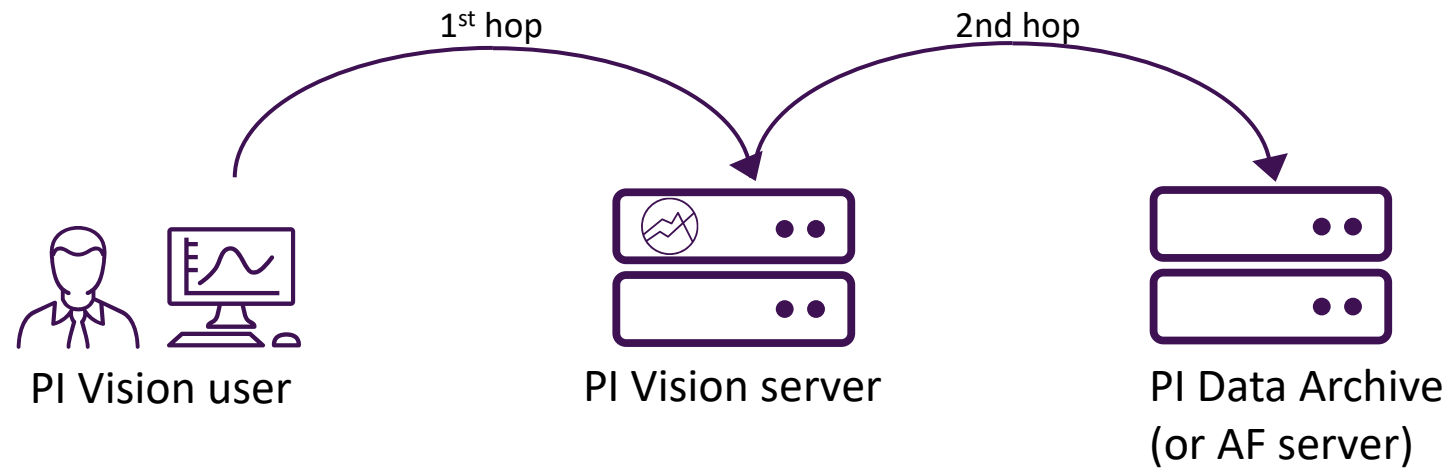
- Extra step required when authentication request is routed through an intermediary server during a 'double-hop'
- Intermediary 'impersonates' end-user to the backend server.



Kerberos Delegation

Double-hop scenarios

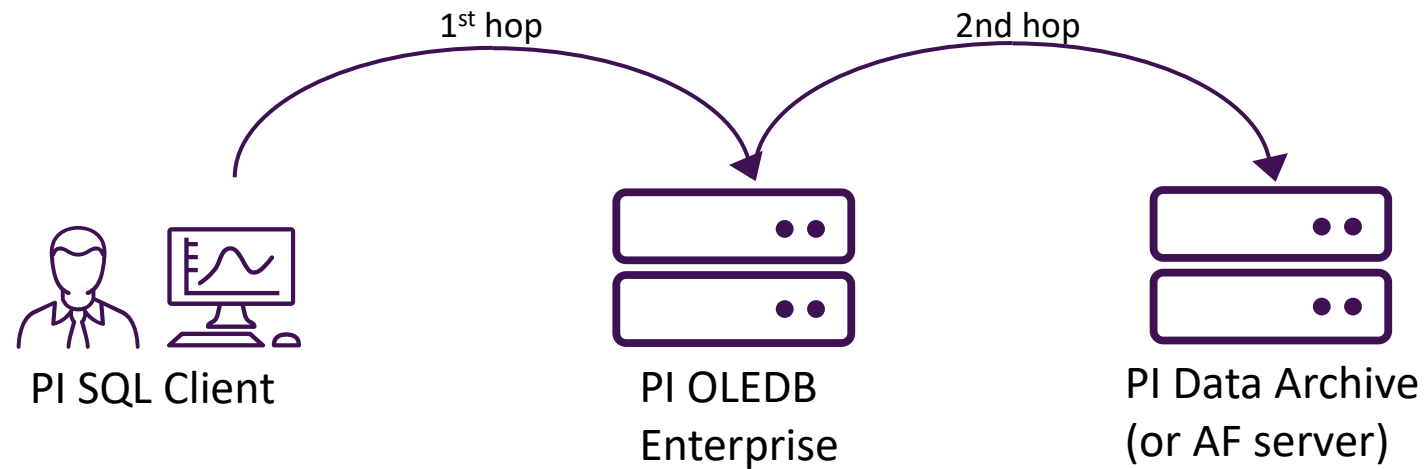
- PI Vision + remote client



Kerberos Delegation

Double-hop scenarios

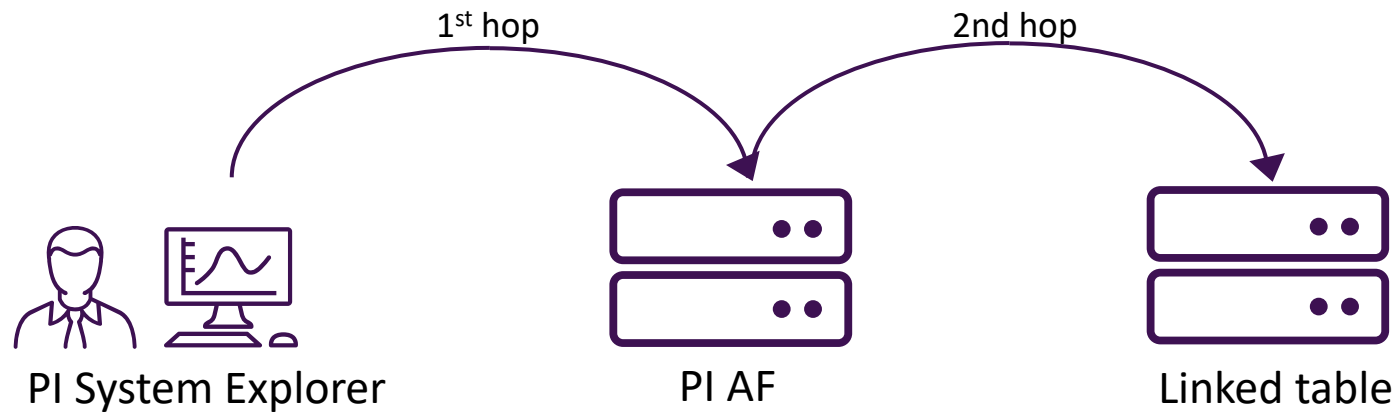
- PI Vision + remote client
- PI OLEDB Provider/Enterprise + PI SQL Client



Kerberos Delegation

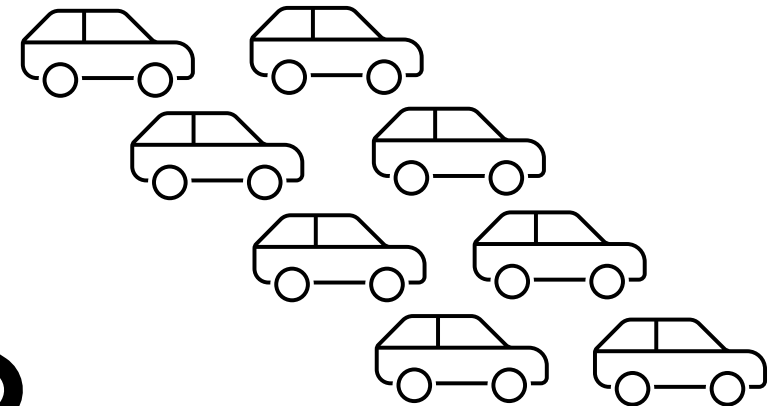
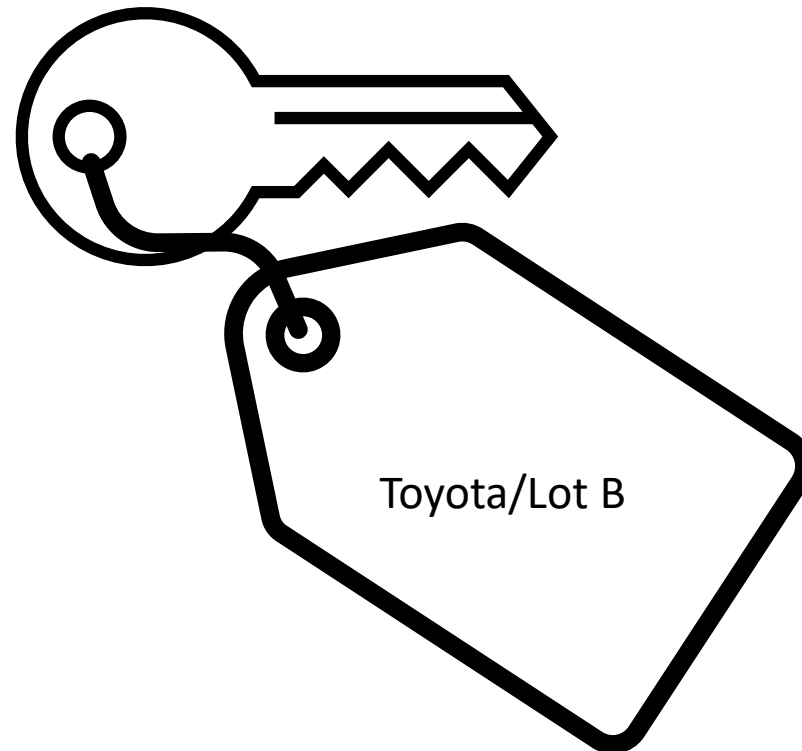
Double-hop scenarios

- PI Vision + remote client
- PI OLEDB Provider/Enterprise + PI SQL Client
- PI System Explorer + AF Linked Table



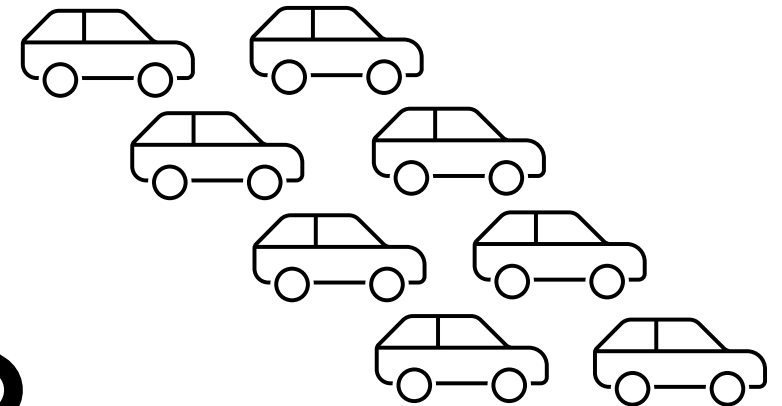
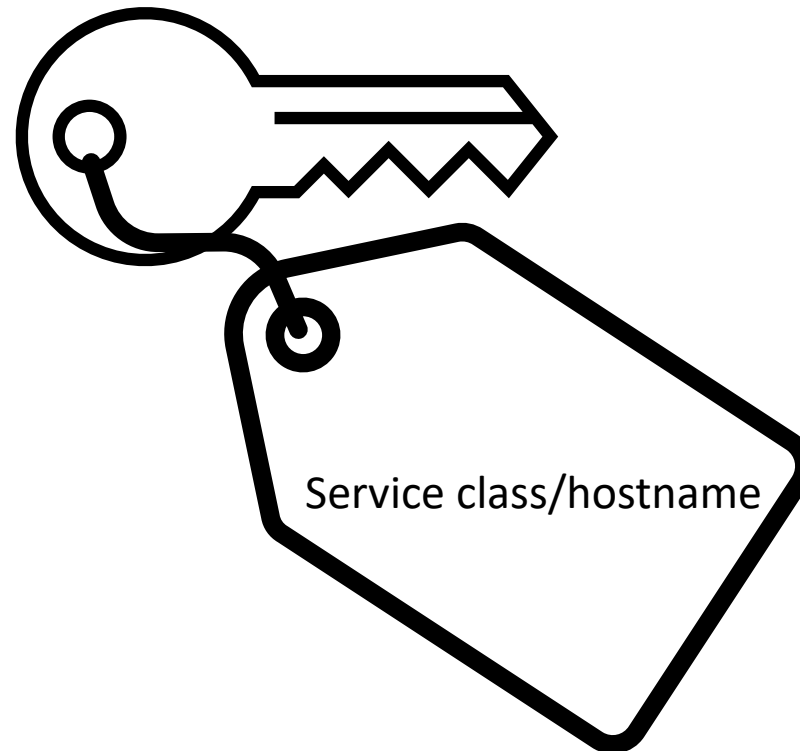
Service Principal Names (SPNs)

- SPNs are little notes that relate an account to a service being offered on a server
- Used by clients to tell the KDC which ticket it needs to access a service on the server.
- Analogy: Car rental
 - 'Service' = rental car
 - 'Ticket' = car key
 - 'SPN' = label on the key



Service Principal Names (SPNs)

- SPNs are little notes that relate an account to a service being offered on a server
- Used by clients to tell the KDC which ticket it needs to access a service on the server.
- Analogy: Car rental
 - 'Service' = rental car
 - 'Ticket' = car key
 - 'SPN' = label on the key

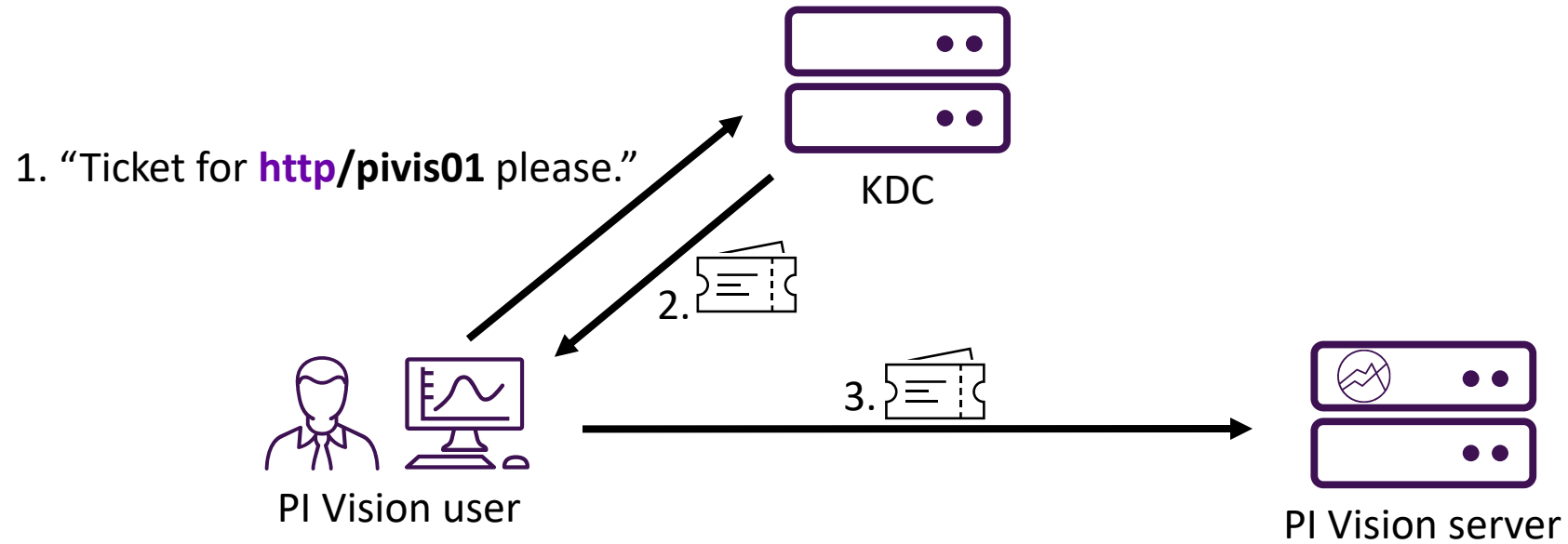


Service Principal Names (SPNs)

- SPNs are little notes that relate an account to a service being offered on a server
- Used by clients to tell the KDC which kind of ticket it need to access a service on the server.
- Analogy: Car rental
 - 'Service' = car
 - 'Ticket' = key
 - 'SPN' = label on the key

| Service class | Hostname |
|---------------------------|----------|
| ↓ | ↓ |
| HTTP/pivision.aveva.int | |
| PISERVER/pida01.aveva.int | |
| AFSERVER/piaf01.aveva.int | |

Using an SPN to request a ticket



Configuration Checklists

Configuration Checklist (PI Data Archive)

- Windows Integrated Security (WIS) will accept SSPI defaults

Configuration Checklist (PI AF)

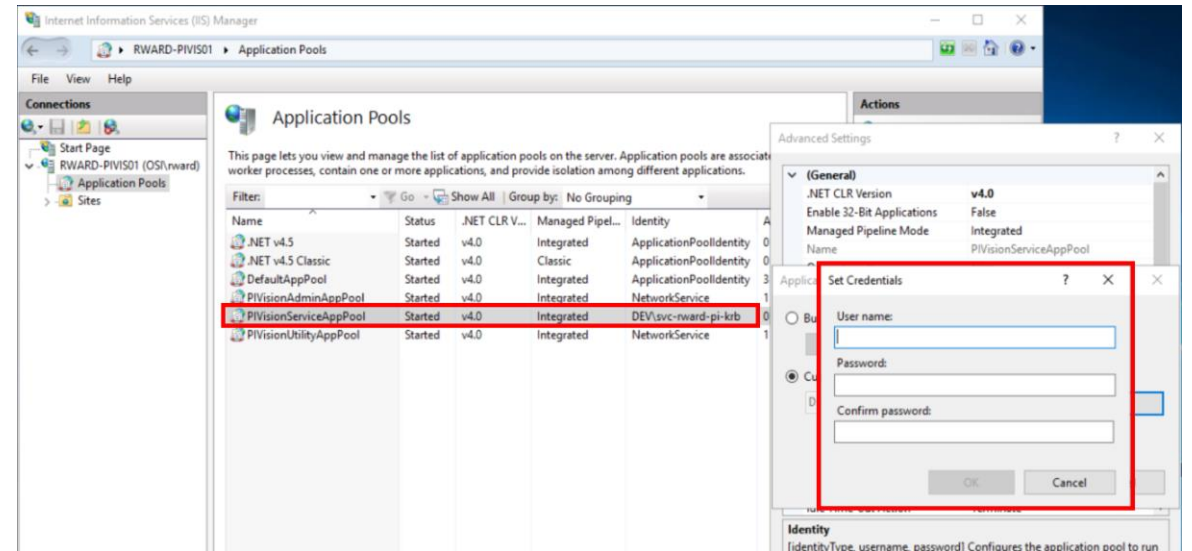
- By default, PI System Explorer and other PI AF clients attempt to connect to the PI AF server (machine hosting PI AF Application Service) using Kerberos authentication.

Configuration Checklist (PI Vision)

1. Create a custom service account for the PI Vision web server

Configuration Checklist (PI Vision)

1. Create a custom service account for the PI Vision web server
2. Run PI Vision as the new service account.

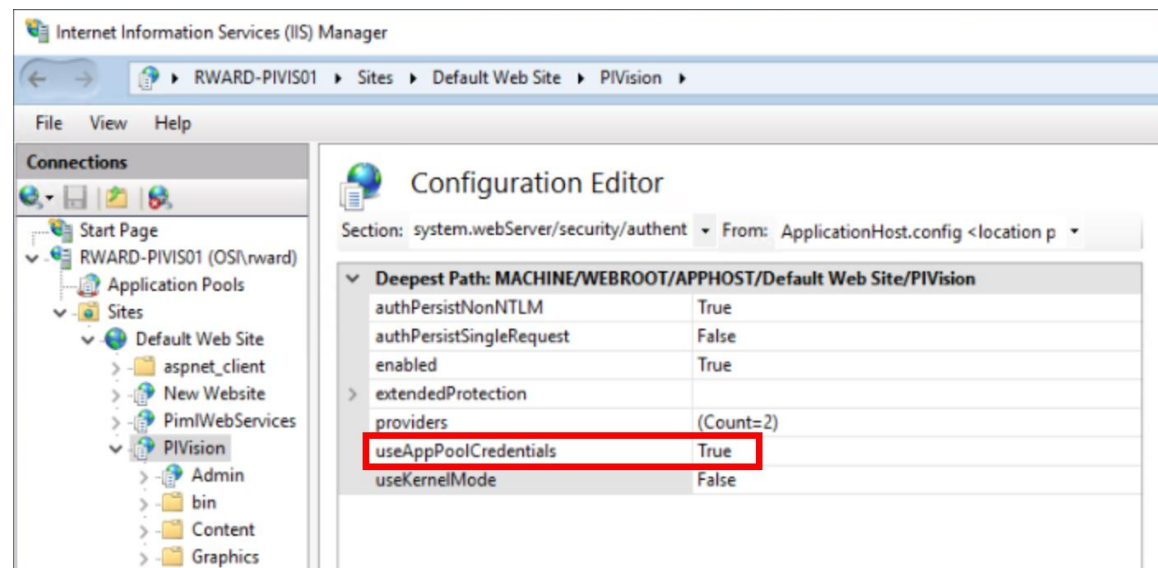


Configuration Checklist (PI Vision)

1. Create a custom service account for the PI Vision web server
2. Run PI Vision as the new service account.
3. Configure the AVEVA PI Vision website to use the application-pool credentials

Path:

system.webServer/security/authentication/windowsAuthentication



Configuration Checklist (PI Vision)

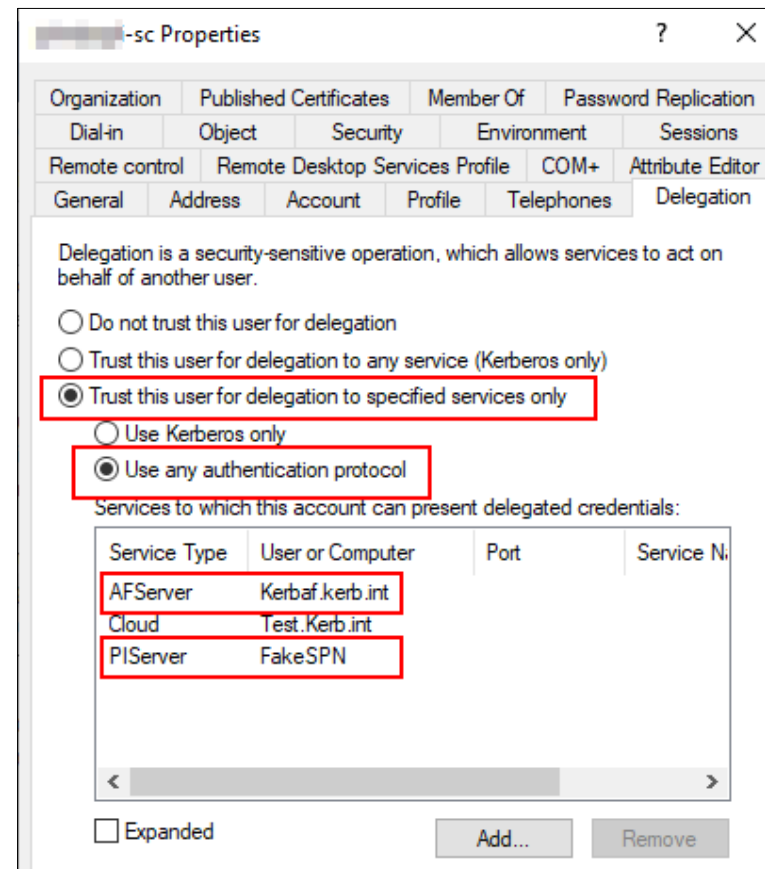
4. Create two Active Directory service principal names (SPNs) for the AVEVA PI Vision server

```
setspn -U -S http/hostname domain\service-account
```

```
setspn -U -S http/fully-qualified-DNS-name domain\service-account
```

Configuration Checklist (PI Vision)

1. Create a custom service account for the PI Vision web server
2. Run PI Vision as the new service account
3. Configure the AVEVA PI Vision website to use the application-pool credentials
4. Create two Active Directory service principal names (SPNs) for the AVEVA PI Vision server
5. Configure the PI Vision service account to delegate to the PISERVER and AFSERVER services



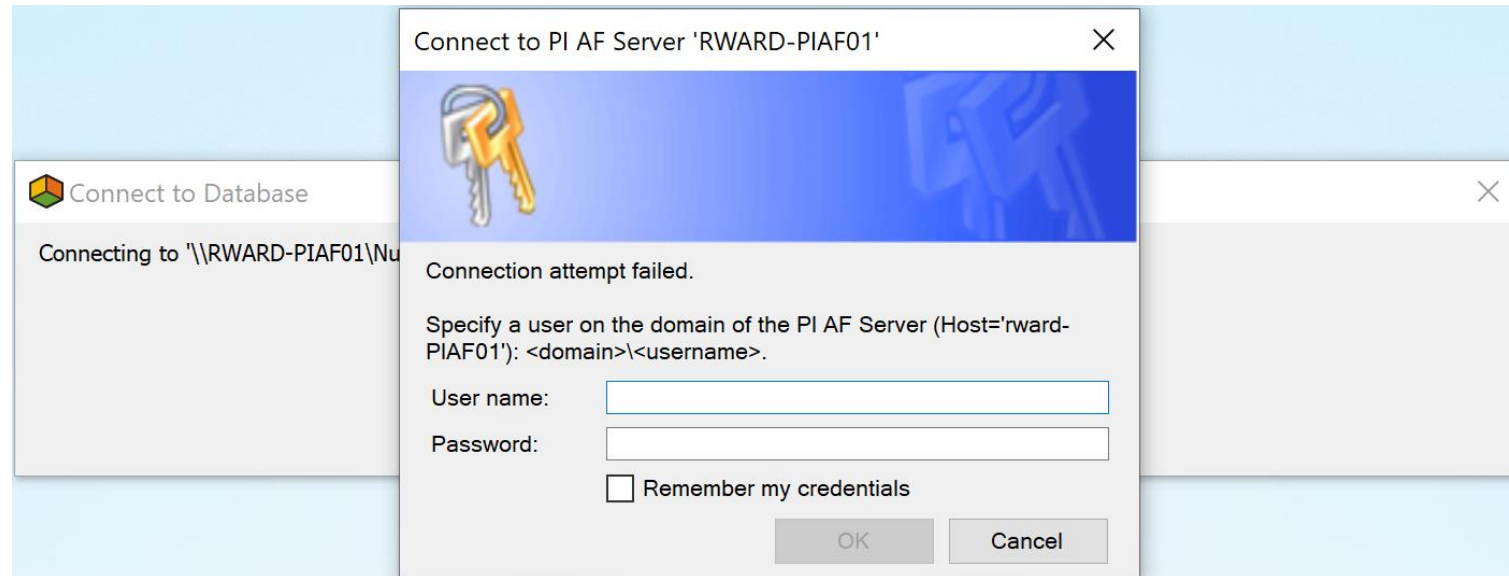
Configuration Checklist (PI Vision)

- Edge cases
 - using resource-based constrained delegation
 - PI Vision in a separate domain from PI Data Archive
 - using an ANAME alias

Signs of a Kerberos Problem

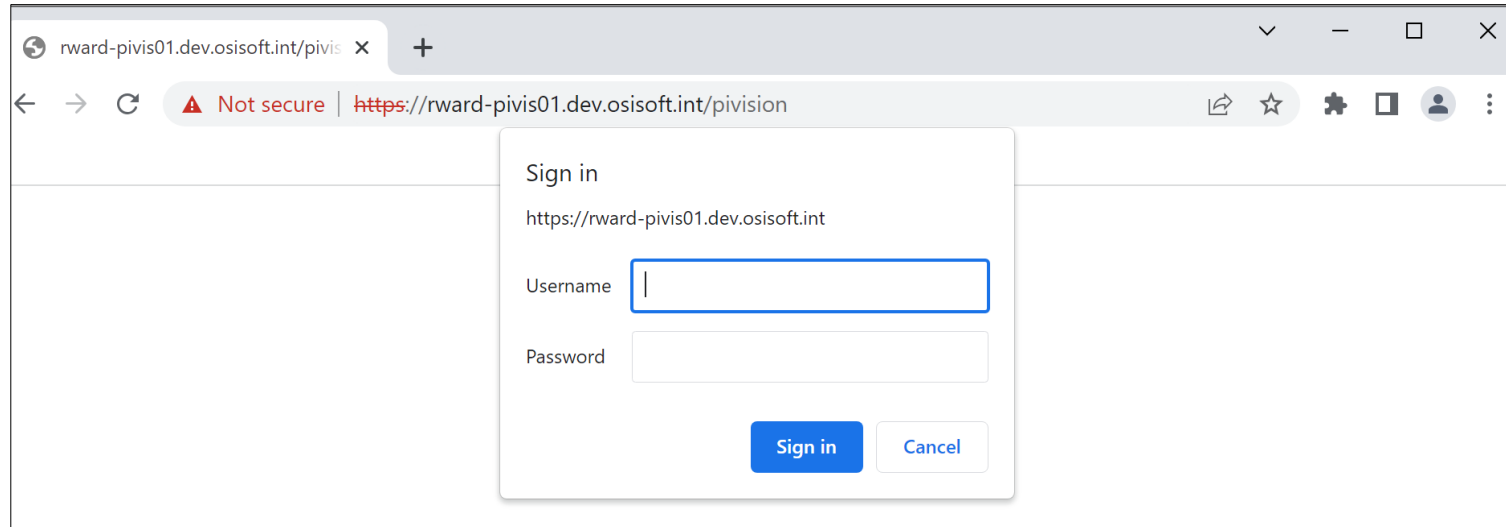
Common signs of a Kerberos problem

PI System Explorer



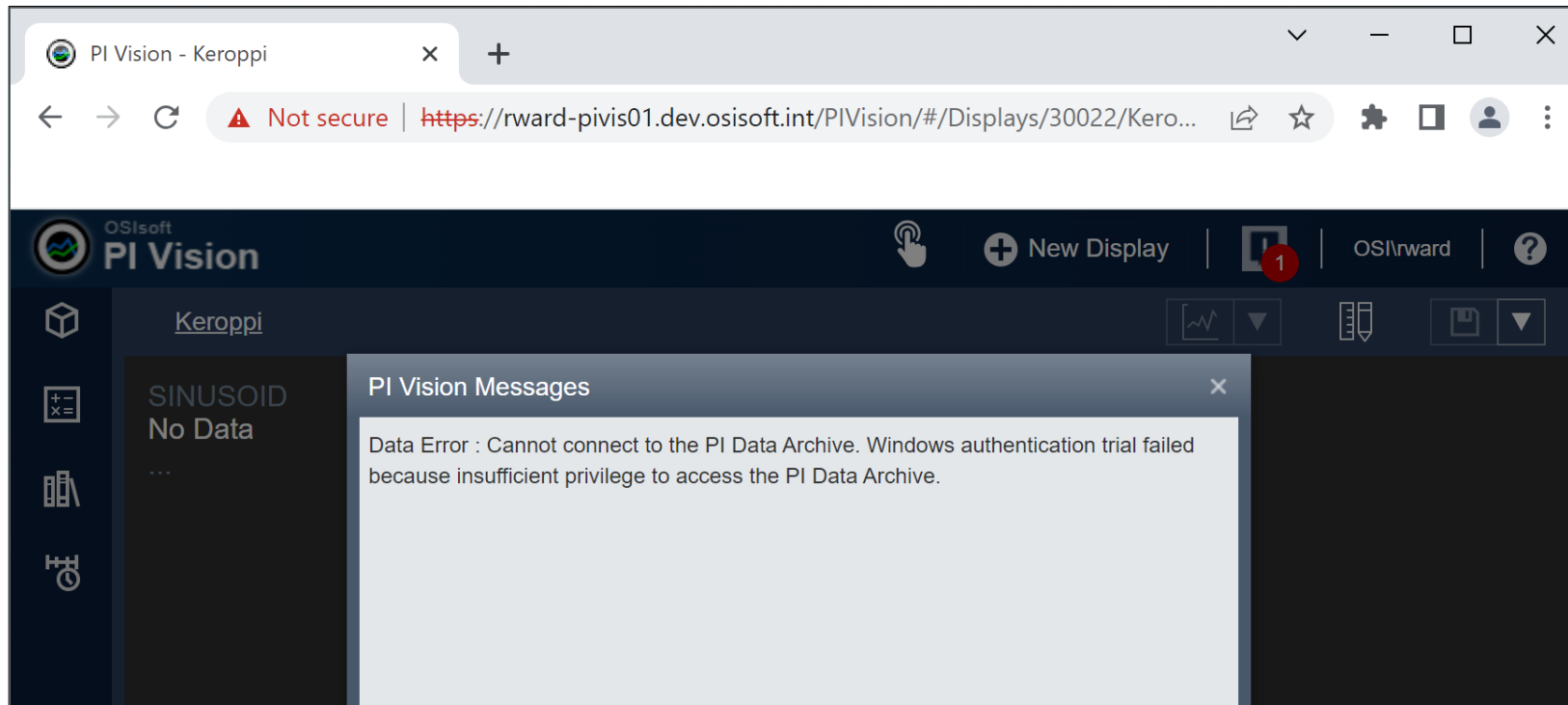
Common signs of a Kerberos problem

PI Vision



Common signs of a Kerberos delegation problem

PI Vision



4 Troubleshooting Tips

Troubleshooting Kerberos Tip #1

Check the PI Data Archive message logs!

D 15-Sep-15 11:00:48 pinetmgr (7082)

Unsuccessful login ID: <PID>. Address: <IP address>. Name: w3wp.exe Credentials used: NT
AUTHORITY\ANONYMOUS LOGON. Method: Windows Login (SSPI,NTLM,HMAC-MD5,RSADSI RC4,128). Error: [-
10433] No identity mapping for this request

D 15-Sep-15 11:00:48 pinetmgr (7082)

>> Successful login ID: 91. Address: 10.0.0.2. Name: piartool(12488):remote. Identity List: PIOperators | PIWorld.
Environment Username : DOMAIN\PIGuy. Method: Windows Login (SSPI,NTLM)

D 15-Sep-15 11:00:48 pinetmgr (7082)

>> Successful login ID: 91. Address: 10.0.0.2. Name: piartool(12488):remote. Identity List: PIOperators | PIWorld.
Environment Username : DOMAIN\PIGuy. Method: Windows Login (SSPI,Kerberos)

Troubleshooting Kerberos Tip #2

Enable Kerberos Logging!

1. Navigate to client machine (or Vision server if using delegation)

2. Navigate to the following registry key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters

3. Create the following new registry key:

Registry Value: **LogLevel**

Value Type: **REG_DWORD**

Value Data: **1**

4. In an administrator command prompt, run **klist purge**

5. Open Event Viewer > Windows Logs > System to review the Kerberos Logs

Troubleshooting Kerberos Tip #3

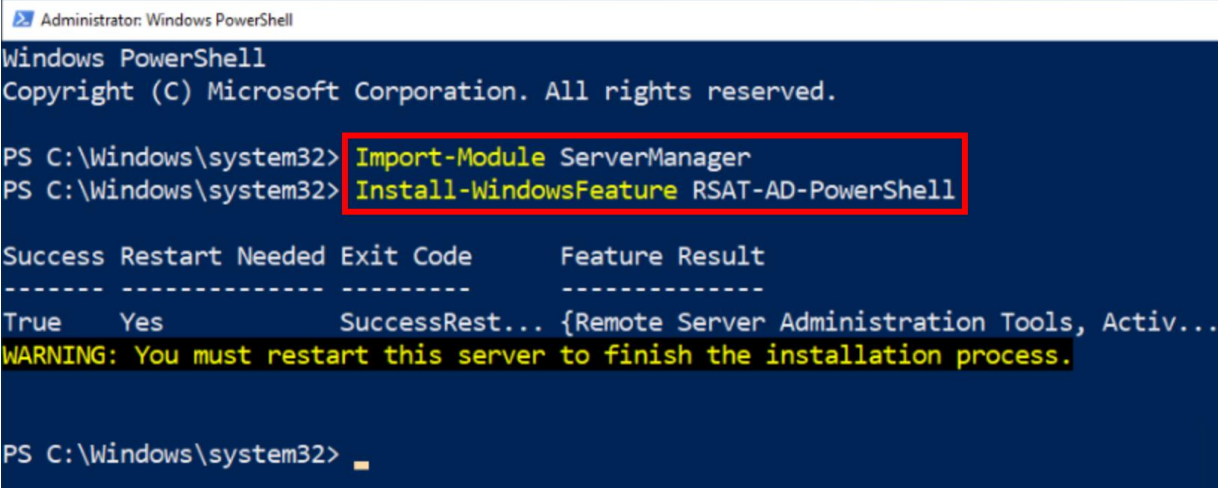
Check your SPNs!

| Account type | Vision Svc Account | PI DA Account | PI AF Account |
|---|--------------------------------------|-------------------------------|----------------------------------|
| Custom account | setspn -l <domain\VisionSvcAcctName> | setspn -q PIServer/<hostname> | setspn -l <domain\AFSvcAcctName> |
| Machine account (e.g. NT Service\PIVision) | setspn -l <VisionServerHostname>\$ | setspn -q PIServer/<hostname> | setspn -l <domain\hostname>\$ |

Troubleshooting Kerberos Tip #4

Check your delegation settings!

1. Open Powershell (from anywhere)
2. Run the following scripts to import and install ServerManager and RSAT-AD-Powershell Module:



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> Import-Module ServerManager
PS C:\Windows\system32> Install-WindowsFeature RSAT-AD-PowerShell

Success Restart Needed Exit Code      Feature Result
-----
True      Yes           SuccessRest... {Remote Server Administration Tools, Activ...}
WARNING: You must restart this server to finish the installation process.

PS C:\Windows\system32>
```

3. Run the following PowerShell command:

```
Get-ADUser '<VisionServiceAcctName>' -Properties msDS-AllowedToDelegateTo,Displayname | select Displayname -ExpandProperty msDS-AllowedToDelegateTo | format-list
```

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