

Configuring PI System Security

OSIsoft, LLC
1600 Alvarado Street
San Leandro, CA 94577

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, mechanical, photocopying, recording, or otherwise, without the prior written permission of OSIsoft, LLC.

OSIsoft, the OSIsoft logo and logotype, Managed PI, OSIsoft Advanced Services, OSIsoft Cloud Services, OSIsoft Connected Services, OSIsoft EDS, PI ACE, PI Advanced Computing Engine, PI AF SDK, PI API, PI Asset Framework, PI Audit Viewer, PI Builder, PI Cloud Connect, PI Connectors, PI Data Archive, PI DataLink, PI DataLink Server, PI Developers Club, PI Integrator for Business Analytics, PI Interfaces, PI JDBC Driver, PI Manual Logger, PI Notifications, PI ODBC Driver, PI OLEDB Enterprise, PI OLEDB Provider, PI OPC DA Server, PI OPC HDA Server, PI ProcessBook, PI SDK, PI Server, PI Square, PI System, PI System Access, PI Vision, PI Visualization Suite, PI Web API, PI WebParts, PI Web Services, RLINK and RtReports are all trademarks of OSIsoft, LLC.

All other trademarks or trade names used herein are the property of their respective owners.

U.S. GOVERNMENT RIGHTS

Use, duplication or disclosure by the US Government is subject to restrictions set forth in the OSIsoft, LLC license agreement and/or as provided in DFARS 227.7202, DFARS 252.227-7013, FAR 12-212, FAR 52.227-19, or their successors, as applicable.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, mechanical, photocopying, recording or otherwise, without the written permission of OSIsoft, LLC.

Contents

Lesson 1 – Gaining Administrator Access	4
Lesson 2 – Introduction to PI Data Archive.....	4
Video: What are Identities, Mapping & Trusts? (High level PI Server Security Map)	4
Video: Data Archive Security Deep Dive Map – Security Areas, Defaults and Customization	7
Lesson 3: Online Course’s Example Security Model	12
Video: Demo of Custom Data Archive Security Plan in Action	12
Lesson 4: Configuring Security.....	12
Video: Configure Overall PI Data Archive Security for Users and SDK Applications	12
Video: Setup Custom Security on PI Points for Both Users and Applications.....	13
Exercise: Customize User Security (additional practice activity)	13
Video: Configuring Minimum Permissions for PI Interface and Buffering.....	15
Video: Disable the Least Secure Authentication Options on Your Data Archive	17
Video: Configure Windows Credentials for a Workgroup Interface Machine	18
Video: Create, Map, and Grant Permissions to Custom Identities in AF.....	25
Exercise: AF Security.....	28
Exercise: Your Database Security.....	30

Lesson 1 – Gaining Administrator Access

Lesson 2 – Introduction to PI Data Archive

Video: What are Identities, Mapping & Trusts? (High level PI Server Security Map)

Securing a PI System

In the context of the PI System, “Security” has multiple objectives:

- Add to the overall reliability and resiliency of the system
- Protecting PI System data and services from malicious attacks
- Limiting user access based on individual user needs

PI System Security is best implemented in a corporate network-secured computing environment. This usually includes:

- Domain security for users, directories, and applications
- Router security including router-based firewalls
- Antivirus programs and regular operating system patches
- Controlled access by remote parties (VPN)

First and foremost, OSIsoft recommends hardening the platform using the Windows operating system and network environment. Administrators can do so effectively by leveraging industry standard profiles and built-in capabilities (e.g. AppLocker, Windows Advanced Firewall, etc.).

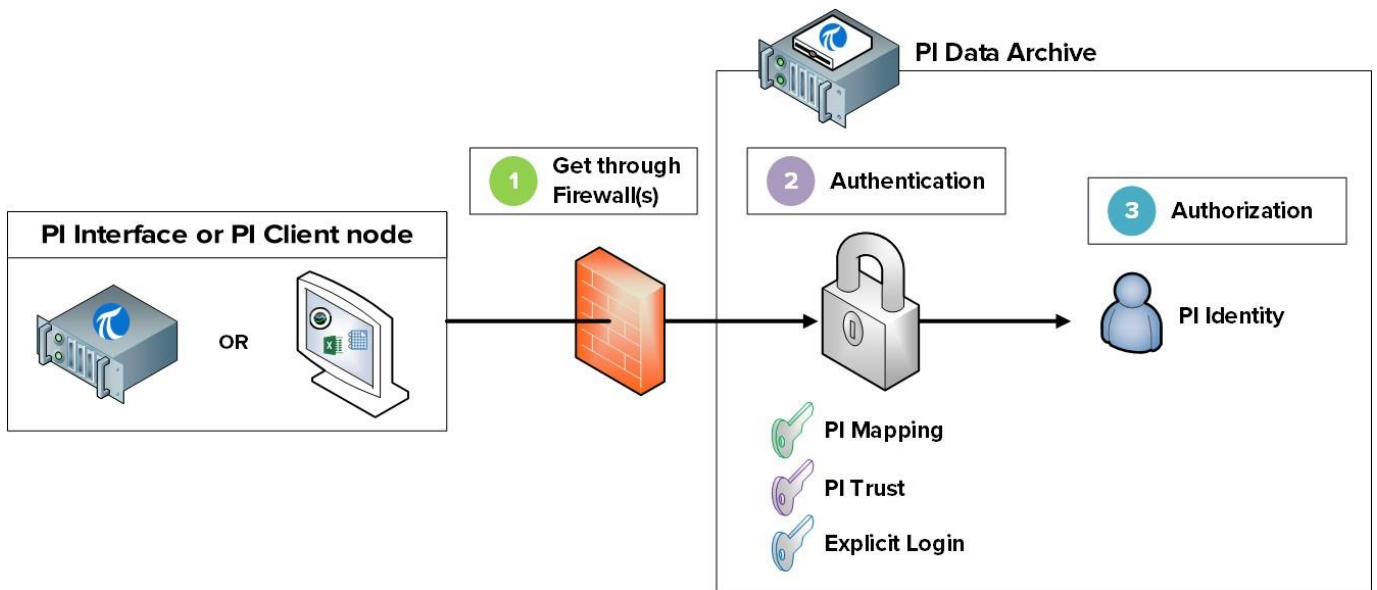
Windows Integrated Security (WIS) brings improvements in authentication and encryption of data throughout the entire PI System. To take advantage of the security features built into the PI System platform, applications must authenticate with WIS. WIS is the strongest authentication mechanism available for the Data Archive. Additionally, transport security is automatically enabled to protect the confidentiality and integrity of data with the latest versions. The ideal Data Archive deployment has all client applications and services authenticating with WIS, so that all other authentication protocols can be disabled.

Antivirus software should be used on the PI System components. However, the archives and data files should be removed from the list of files scanned. Additionally, OSIsoft recommends leveraging application whitelisting as a more effective measure.

Accessing a secured PI System

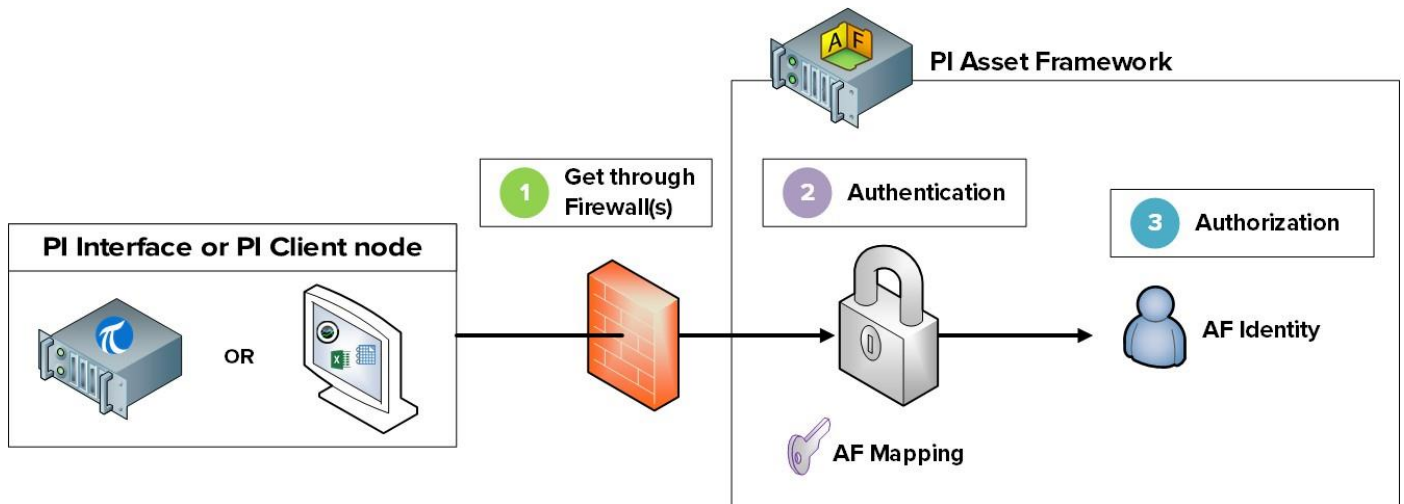
In order to access a secure Data Archive, a connection must:

1. Contact the server over a network. The most common barrier to network communication are the firewalls, which guard the server.
2. Authenticate itself through either a PI Mapping, a PI Trust or Explicit Login
3. Receive the proper authorization through its PI Identity



In order to access a secure Asset Framework, a connection must:

1. Contact the server over a network. The most common barrier to network communication are the firewalls, which guard the server.
2. Authenticate itself through AF Mapping
3. Receive the proper authorization through its AF Identity



Authentication vs. Authorization

We began our discussion of authentication and authorization in chapter 2, when configuring security for our PI Interface instance. Let's review what we know so far. In the context of the PI System:

- Authentication is the process that verifies the identity of a user or process, before allowing it to connect to the Data Archive
- Authorization is the process that determines what an application can do once connected to the Data Archive or the Asset Framework (e.g. create a PI Point, create an asset, run a backup, etc.)

The analogy we made previously was the Data Archive (or the Asset Framework) as a facility. The process of authentication is like the security guard at the entrance of the facility. He decides whether someone should be let in. If he does let them in, he gives them an access card. This access card is their authorization. It will give them access to specific rooms within the facility.

Authentication



Authorization



Video: Data Archive Security Deep Dive Map – Security Areas, Defaults and Customization

Data Archive Security

Authentication

There are three different methods of authentication on the Data Archive:

1. PI Mappings


PI Mappings use *Windows Integrated Security* to authenticate users on the Data Archive. With this method, users and services connect directly to the Data Archive using their Windows account. A PI Mapping grants a Windows user or group specific rights on the Data Archive by assigning a PI Identity.

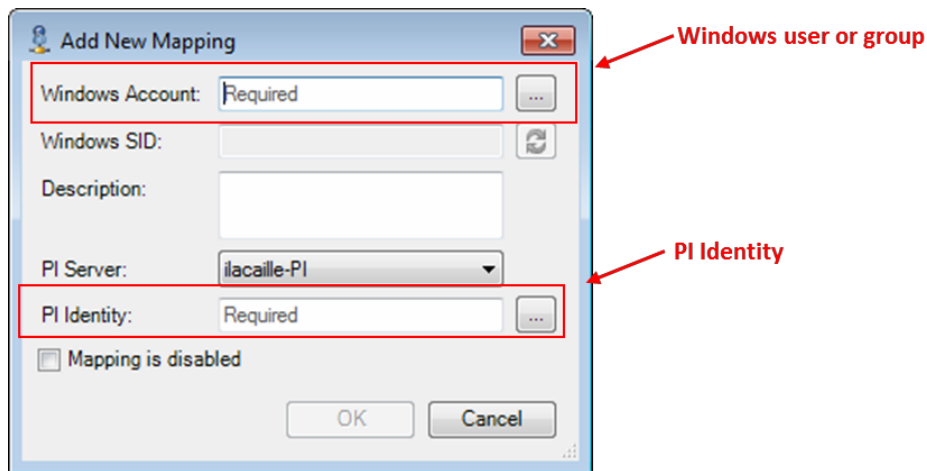
This method of authentication has several advantages:

- It is the most secure
- It enables transport security (encryption in transit) of communications with the Data Archive¹
- It represents the least amount of maintenance for PI System administrators
- It allows users to connect directly with their Windows accounts

The recommended strategy for using PI Mappings is to create a Windows Group for each level of authentication needed on the Data Archive (e.g. one group for Read-Only users, one group for PI System Administrators, etc.), then assign a unique PI Identity to each one of these groups.

PI Mappings are created from System Management Tools, from Security > Mappings &

Trusts > Mappings Tab, by pressing the New button Mapping Window . This will open the Add New



The following conditions must be true in order to use PI Mappings:

- **The application must connect with** PI AFSDK (any version), PI SDK version 1.3.6 or later or the PI API for Windows Integrated Security (version 2.0.1.35 and later, released in 2016)
- The connecting application is running on a Windows operating system

In the event that these conditions cannot be met, a PI Trust should be used for authentication.

2. PI Trusts

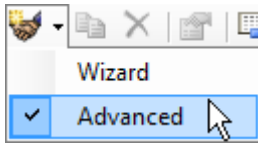
PI Trusts should NOT be used unless it is not possible to authenticate using Windows Integrated Security. The most common scenario is:

- PI Interfaces and other applications running on non-Windows Operating Systems

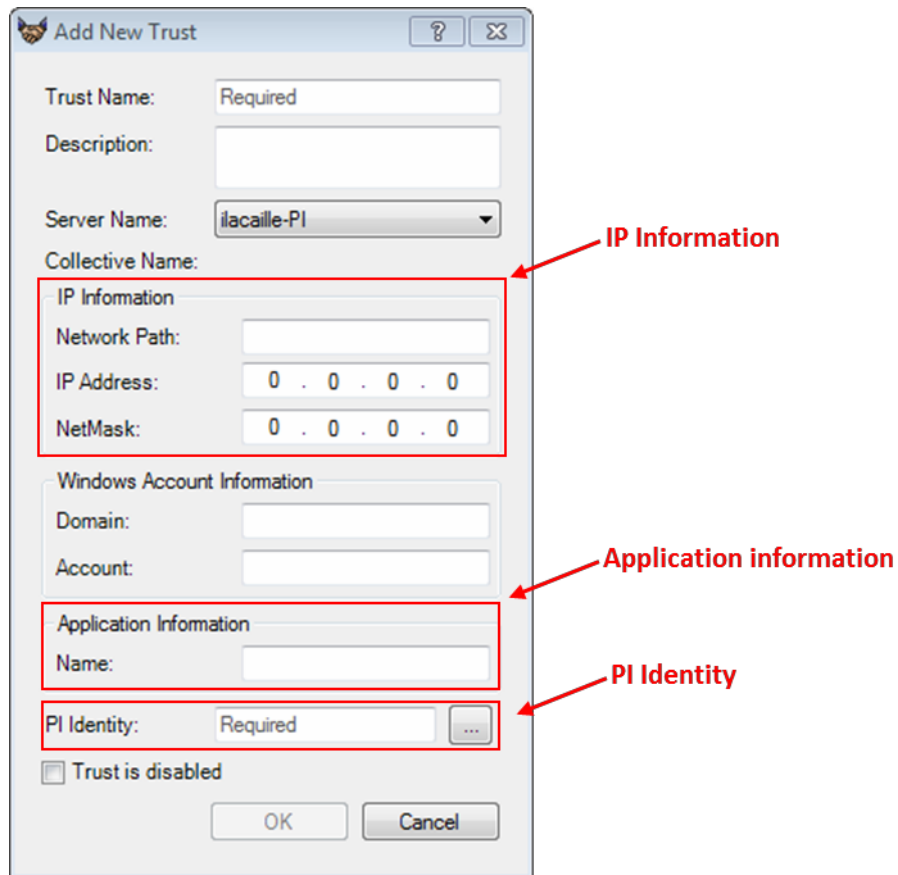
Note: Prior to 2016 release of the PI API for Windows Integrated Security, any applications using the PI API, such as PI Interfaces, could not use PI Mappings. Now, almost all PI Interface nodes can be upgraded to the new security model, regardless domain or workgroup configuration. For more information, see [KB00354 - Supported Windows Security Configurations in Domains and Workgroups for the PI Data Archive](#)

The PI Trust authentication method work by comparing the connection credentials of the connecting application to the credentials saved in PI Trusts. If the credentials match, the connection is allowed. No login is required by the application.

PI Trusts are created from System Management Tools, from Security > Mappings & Trusts > Trusts Tab, by pressing the arrow next to the New... button and selecting the advanced option:



This will open the Add New Trust Window.



It is not necessary to fill in all of the information in this Window. OSISOFT recommends that you fill out PI Trusts using the 2+ Trust convention. This means you need to enter the following:

- The IP Information:

The Network Path (Host name or fully qualified domain name of the computer)

OR

The IP Address and a NetMask of 255.255.255.255.

- The Application Information

The application name. Applications that connect through the PI API send an identifier called an application process name, or procname. This is a four-character string with an E appended. For example, the procname for the PI Perfmon interface is PIPeE.

3. Explicit Login

The final authentication method, Explicit Login, is not recommended in any scenario. It only exists for backwards compatibility purposes. Using this method, users login to the Data Archive directly using a PI User and a password.



Tip

OSIsoft now recommends upgrading from PI trusts and Explicit Login to Windows authentication & PI mappings as the authentication model throughout your PI system. This can be done by upgrading to the PI API for Windows Integrated Security on all PI Interface nodes, and all other custom PI API applications, which run on Windows Operating Systems.

PI trusts and explicit logins are disabled on PI API 2018 for Windows Integrated Security. Therefore, before upgrading to PI API 2018 for Windows Integrated Security, you must configure PI mappings to replace any existing PI trusts used by PI interfaces.

Authorization

There are three types of security objects that grant authorization on the Data Archive: PI Identities, PI Users and PI Groups. All three represent a set of access permissions on the Data Archive.

1. PI Identities

It is recommended to use PI Identities when configuring PI Mappings and PI Trusts. They cannot be used with Explicit Login, since there is no password associated with a PI Identity.

2. PI Users

PI Users can be used when configuring PI Mappings and PI Trusts. Each PI User is associated with a password, and therefore can be used with Explicit Login authentication. PI Users are still supported for backwards compatibility, and the standard built-in accounts, piadmin and pidemo, are still provided.



Tip

Piadmin is the default “god user”, and should not be used in any PI Mapping or PI Trust for security purposes. The only valid use of piadmin is disaster recovery.

3. PI Groups

PI Groups can be used when configuring PI Mappings and PI Trusts. In the past, PI Groups were used for grouping together PI user accounts and providing them with the same access permissions. This can now be accomplished by mapping Windows Groups to PI Identities using PI Mappings. PI Groups are still supported for backwards compatibility, and the standard built-in groups, piadmins and piusers, are still supported.

Note: The PIWorld Identity is a special PI Identity created by default during the Data Archive installation. This identity is granted by default to any user connecting to the Data Archive through PI Mapping. By default, the PIWorld Identity has read access to all PI Points.

In order to limit the read access to all PI Points granted by the PI World Identity, two solutions are available: (1) Disable the PI World Identity or (2) remove the PI World Identity from the database security access control lists.

Access Permissions on the Data Archive

So far, we have seen how a connection can be authenticated (using PI Mappings, PI Trusts or Explicit Login), and what gives them authorization (PI Identities, PI Users or PI Groups). However, what permissions can you get once you obtain authorization?

The Data Archive has a variety of resources to which you can control access. These resources include PI Points, modules, archive configuration, backups, batches, audit trails, and so on. We refer to those PI resources as *secure objects*.

For each secure object, you can define which PI Identities (or PI Users or PI Groups) have read and/or write access. This security setting is stored in an access control list (ACL).

For example, let's say you have the following three PI Identities:



The "Read-only users" PI Identity should view the tuning parameters of the Data Archive, but should not be able to edit them. The "Administrators" and "Power Users" on the other hand, should have write access to the tuning parameters. The ACL for the tuning parameters should therefore be:

```
Administrators:A(r,w) | Power Users:A(r,w) | Read-only users:A(r)
```

There are three places where ACLs can be set:

1. On groups of secure objects in the Database Security table (SMT > Security > Database Security)
2. On individual PI Points (the Point Security and Data Security attributes)
3. On individual modules in the Module Database

Managing PI Identities and Mappings – taken from pdf 7

The **Security → Identities, Users, & Groups** plug-in in PI SMT allow you to create and manage PI Identities, PI Users and PI Groups. Several entries are created by default during installation. When configured, you can use the security entries to specify security settings throughout the PI Data Archive, including PI databases security and PI point security.

Ideally, you will have one PI Identity for each Active Directory Group of users, you will use to access the PI System. And PI Identity for service account of applications requiring same level of access.

About PIWorld Identity

The **PIWorld** identity represents the Everyone concept of Windows; it specifies the rights of non-explicit users or groups. All authenticated PI Server users automatically get the access permissions defined for PIWorld (in addition to any other access permissions they have been granted).

By default, PIWorld is granted read access to most PI Server databases and objects. You can change the access permissions granted PIWorld, but you **cannot delete** this identity. The PIWorld identity cannot be used in a mapping or a PI Trust.

You can **disable** PIWorld. If you do that, then users no longer get PIWorld access along with their explicitly granted access permissions. This is a recommended action for fresh installations of PI System. This can be risky for PI System upgrades. You might be relying on PIWorld access in several places without knowing it.

piadmin vs. piadmins

PI User **piadmin** is a “**GOD**” local user that have unrestricted access to whole PI Data Archive, no matter is it is defined in database or PI point ACL. Avoid mapping piadmin to Windows user or service account.

PI Group **piadmins** is treated as any other PI Identity. If it is removed from PI points or database ACL, it loses access. PI Data Archive administrators should be mapped to it.

Lesson 3: Online Course’s Example Security Model

Video: Demo of Custom Data Archive Security Plan in Action

Lesson 4: Configuring Security

Video: Configure Overall PI Data Archive Security for Users and SDK Applications

Video: Setup Custom Security on PI Points for Both Users and Applications

Exercise: Customize User Security (additional practice activity)

Objectives

- Create PI Identities that will be mapped to Windows Users and Groups
- Configure point security for data access

Problem Description

You have many users requiring access to your PI System, but they all require different levels of access to different PI Points. Therefore, you want to grant access to the Data Archive and its resources based on user roles.

You have three domain groups:

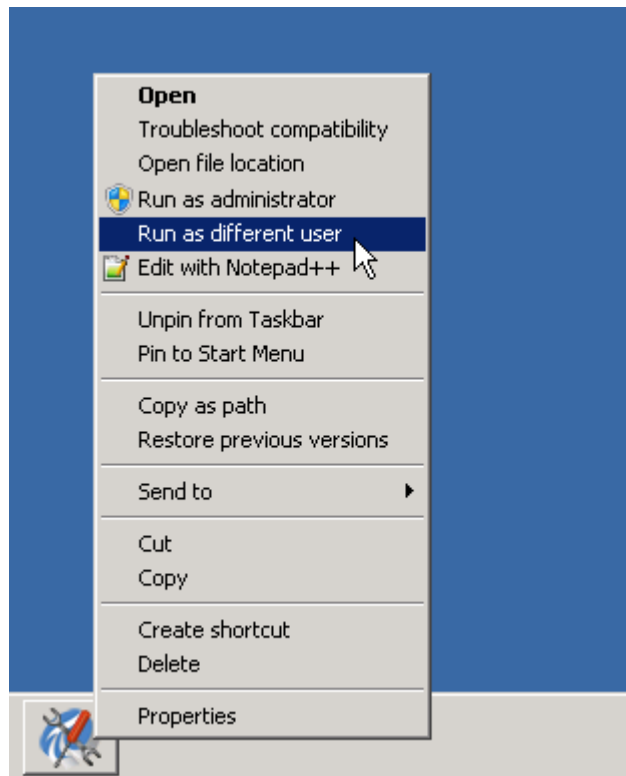
1. Engineers
2. Operators
3. Supervisors

You need to create a security structure that enforces the following business rules:

- The point **OSIsoftPlant.Production** is a sensitive calculation and it should only be visible to the Supervisors group.
- The pressure sensor on Mixing Tank 2 is broken, so the data is being entered manually by the operators. Therefore, the Operators group needs write access to the data for PI Point **VPSD.OSIsoftPlant.PL2.MXTK2.Pressure**. It should be readable by anyone.
- The Engineers group needs to be able to edit the attributes of all of the OSIsoft Plant PI Points (with the exception of **OSIsoftPlant.Production**, which they should not be able to see).

Approach

- Step 1.** Map the three domain groups to the default PI Identities PIEngineers, PIOperators, PISupervisors
- Step 2.** Edit the Database Security and PI Point Security according to the rules above
- Step 3.** Test your security rules. To run SMT as a different user, hold the Shift key, then right-click SMT in the task bar and select “Run as different user”.



You may use the following accounts for your tests:

Domain Account Name	Member Of	Password
Charles	Supervisors	ITPROSpwd01!
Homer	Operators	ITPROSpwd01!
Bertha	Engineers	ITPROSpwd01!

1. Logon as Homer and try to search for the point **OSIssoftPlant.Production**. What result do you get? As Homer, write data to PI Point **OSIssoftPlant.PL2.MXTK2.Pressure** using SMT > Data > Archive Editor. Does it work?
2. Logon as Bertha. Try writing data to PI Point **OSIssoftPlant.PL2.MXTK2.Pressure**. Does it work? Now try turning compression off for **OSIssoftPlant.PL2.MXTK2.Pressure**.

3. Logon as Charles. Can you find and read PI Point **OSIsoftPlant.Production**?

Video: Configuring Minimum Permissions for PI Interface and Buffering

Exercise: Tighten security for the PI Interface for OPC DA

Objectives

- Create a PI Identity for PI Interfaces and for PI Buffers with least privileges.

Problem Description

Previously, we installed and configured a PI Interface for OPC DA. We created a single identity called "PI Interfaces & PI Buffers". Now, we want to tighten our security even further, by creating two PI Identities that gives them the minimum required privileges to the PI Interface and PI Buffer Subsystem on the Data Archive. Our knowledge base article [KB00833 – Seven best practices for securing your PI Server](#), outlines the most secure configuration as follows:

Process	Read Permissions	Write Permissions
Interface	1. Database security > PIPOINT Table 2. Point Security on the PI Points	None
Buffer	None	Data security on the PI Points

You will implement this security configuration

Part 1 – Monitor the data coming from the PI Interface

Step 1. Whenever making changes to a PI Interface, it's important to make sure we don't affect data collection. Open the display "Pump Overview", so you can keep track of data flow.

Part 2 – Create an identity for the PI Interface & PI Buffer Subsystem

Step 2. On PISRV01, run SMT. Navigate to Security > Identities, Users, & Groups.

Step 3. On the PI Identities tab, create a new PI Identity called "PIInterfaces" and another called "PIBuffers"

Part 3 – Edit the Database Security for the new PI

Identity **Step 4.** Navigate to Security > Database

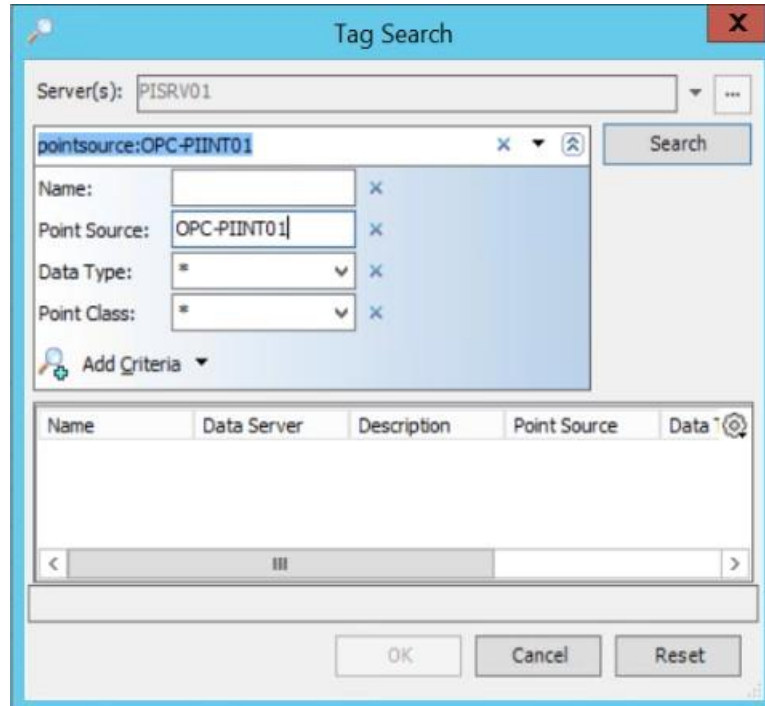
Security **Step 5.** Double click on the "PIPOINT" table.

Step 6. Add the "PIInterfaces" Identity, and give it read

access

Part 4 – Edit the PI Point security for the Pump PI Point

- Step 7.** Load all the PI Points with point source “OPC-PIINT01” in Excel using PI Builder. Make sure to select the security attributes when importing the PI Points.



- Step 8.** Edit the ACL in the datasecurity and ptsecurity column.
- “PIInterfaces” should have read access to ptsecurity
 - “PIBuffers” should have write access to datasecurity

- Step 9.** Publish your changes

Part 6 – Edit the PI Mapping for the PI Interface & Buffer

- Step 10.** Navigate to Security > Mappings & Trusts

- Step 11.** On the Mappings tab, open the PI Mapping you created for the Windows Account “svc-PIInterface”. Assign it to the PI Identity “PIInterfaces”

- Step 12.** Open the PI Mapping you created for the Windows Account “svc-PIBuffer”. Assign it to the PI Identity “PIBuffers”

- Step 13.** Navigate to Security > Identities, Users and Groups

- Step 14.** Delete the PI Identity “PI Interfaces & PI Buffers”

Part 7 – Validate your new security configuration

- Step 15.** On PIINT01, restart the PI Buffer subsystem (this should also restart the PI Interface)

- Step 16.** On PISRV01, in SMT, navigate to Operations > Network Manager Statistics. How are opcpE and pibufss.exe connecting?

- Step 17.** Return to your “Pump Overview” display and validate that you are still receiving pump data from PIINT01



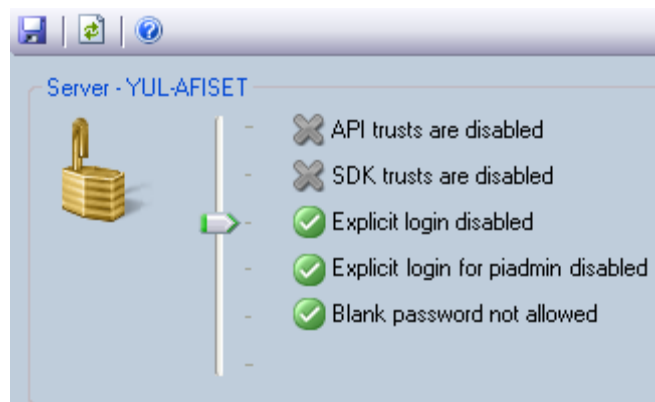
Tip

Always check your data after making changes to security!

Video: Disable the Least Secure Authentication Options on Your Data Archive

The “Security Slider”

You have the ability to disallow specific types of logins to your Data Archive. This is controlled by the **Security Settings** plug-in in SMT (Security > Security Settings).



In a good security environment, you will set the slider to a minimum of explicit logins disabled. This should not impact you at all if you avoid using piusers and pigroups.



Tip

If you want to set the security slider all the way to the top, you need to ensure that none of the active connections to the Data Archive use PI Trusts. A good way of checking is by using Network Manager Statistics in SMT. The connections using PI Trusts will be indicated in the “Trust” column.

Video: Configure Windows Credentials for a Workgroup Interface Machine

Exercise: Upgrading existing PI Interface authentication from PI trusts and to Windows authentication



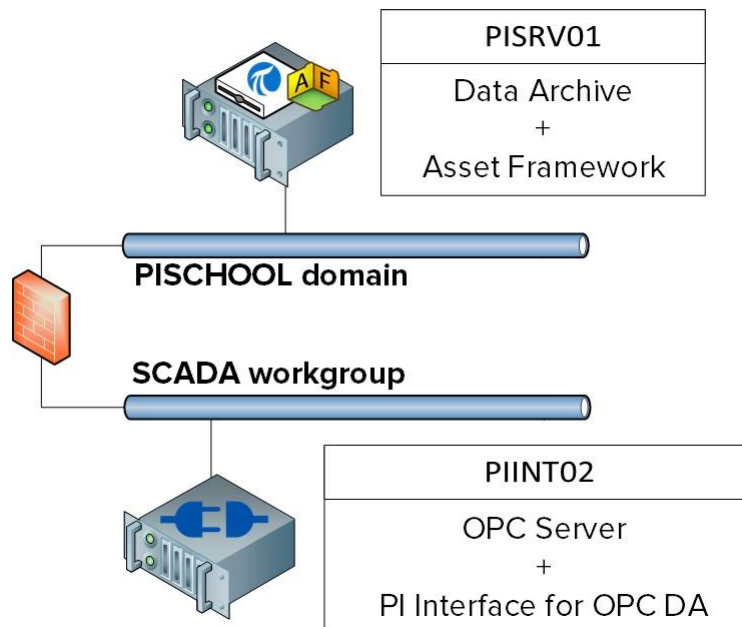
In this part of the class, you will perform a learning activity to explore the different concepts presented in this chapter or section. You may be invited to watch what the instructor is doing or perform the same steps at the same time. You may play a game or hold a quiz. Your instructor will have directions.

Objectives

- Upgrade a PI Interface node to PI API for Windows Integrated Security

Approach Given that the PI API for Windows Integrated Security was only released in 2016, on existing PI Systems, many PI Interface nodes will still be using the old PI Trust authentication model. This is the case in our PI System, which is running a PI Interface for OPC DA on the node PIINT02. OSIsoft recommends upgrading to the PI API for Windows Integrated Security on all PI Interface nodes, and all other custom PI API applications, which run on Windows Operating Systems.

Here is the architecture for PIINT02:



PIINT02 is not a member of the PISCHOOL domain, but rather it resides in the SCADA workgroup. In order to use Windows Integrated Security, we need to make sure the account running the PI Interface for OPC DA can be authenticated on the PI Data Archive. To do this, we will use the Windows Credential Manager, using the solution outlined in [KB01457 – Using the Credential Manager with PI applications](#).

Part 1 – Monitor the data coming from the PI Interface

Step 1. On PISRV01, create a display in PI Vision a trend of the tag Tank1.MixerSpeed

Part 2 – Identify all the connections from the PI Interface node

Step 2. On PIINT02, open the command prompt, and run the command **ipconfig**. What is the IP address of the computer?

192.168.1. _____

Step 3. On PISRV01, in SMT, navigate to Operations > Network Manager Statistics

Step 4. Sort the connections using the column “Peer Address”. Note all of the columns coming from the IP address you identified:

Step 5. Click on the connections in the list. How are these applications currently authenticating?

Step 6. What other PI System applications does an administrator run on a PI Interface node?

Part 3 – Find the accounts which are running the PI Interface and PI Buffer Subsystem

Step 7. Log on to PIINT02

Step 8. Run the services snap-in. Under which accounts are the PI Interface and PI Buffer Subsystem services running?

Note: In our case, the services are already running under local accounts, with the minimum required privileges on the machine PIINT02. However, you might encounter instances where these services are running under the “LocalSystem” account. OSIsoft recommends that you create local accounts with least privileges for your PI System services while upgrading to the latest security model.

Part 4 – Prepare the Data Archive

Step 9. In the last directed activity, you created two PI Identities with the following permissions:

Identity	Read Permissions	Write Permissions
PIInterfaces	1. Database security > PIPOINT Table 2. Point Security on the PI Points with point source OPC-PIINT01	None
PIBuffers	None	Data security on the PI Points with point source OPC-PIINT01

These PI Identities are mapped to the following domain service accounts:

PI Identity	Domain Account
PIInterfaces	PISCHOOL\svc-PIInterface
PIBuffers	PISCHOOL\svc-PIBuffer

These domain accounts are managed service accounts, whose passwords do not expire. In order for the PI Interface and PI Buffer on PIINT02 to leverage these existing PI Identities and PI Mappings, we simply need the following:

- The PI Interface on PIINT02 must authenticate using the domain account PISCHOOL\svc-PIInterface
- The PI Buffer on PIINT02 must authenticate using the domain account PISCHOOL\svc-PIBuffer

Step 10. Load all the PI Points with point source “OPC-PIINT02” in Excel using PI Builder. Make sure to select the security attributes when importing the PI Points.

Step 11. Edit the ACL in the datasecurity and ptsecurity column

- a. Give the “PIInterfaces” identity read access to ptsecurity
- b. Give “PIBuffers” identity write access to datasecurity

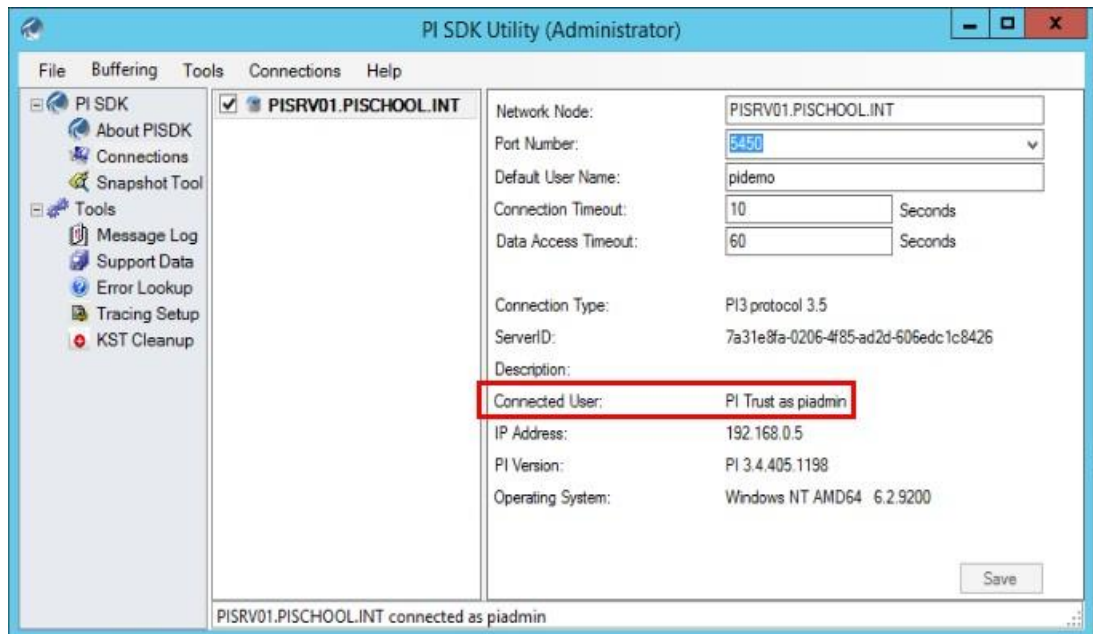
Step 12. Publish your PI Point security changes.

Part 5 – Configure credentials using the Windows Credential Manager

In order to use the proper PI Mappings on the PI Data Archive, we need local users to authenticate on the server PISRV01 using domain accounts. Below is a table showing the credentials used for each local account:

Local account	Domain Account
PIINT02\student01	PISCHOOL\student01
PIINT02\OPCInterface	PISCHOOL\svc-PIInterface
PIINT02\PIBuffer	PISCHOOL\svc-PIBuffer

- Step 13.** We will first configure the credentials for the **local user student01**
- Log on to PIINT02
 - First, test how the local student01 is currently connecting. Run the application “PI SDK Utility”, and connect to the server “PISRV01.PISCHOOL.INT”. You should see this:



The local user .\student01 cannot connect using WIS because it cannot authenticate on the domain PISCHOOL.INT, so the PI Trust is being used.

- Run the snap-in “Credential Manager”. Select “Windows Credentials”
- Click “Add a Windows credential”
- Enter the domain account credentials for PISCHOOL\student01

Type the address of the website or network location and your credentials

Make sure that the user name and password that you type can be used to access the location.

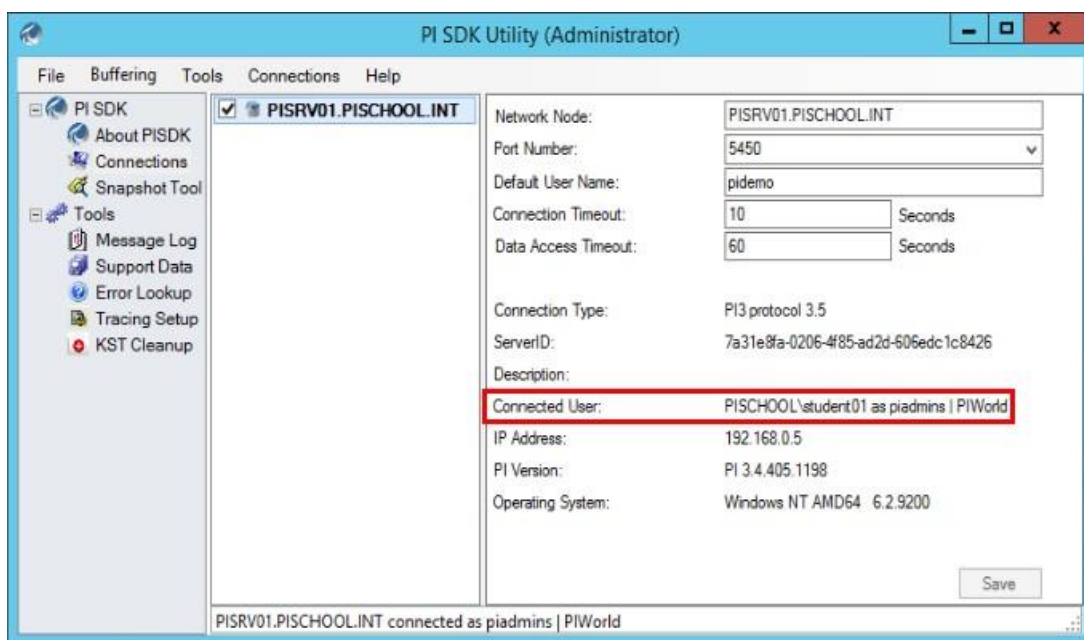
Internet or network address
(e.g. myserver, server.company.com): PISRV01.PISCHOOL.INT

User name: PISCHOOL\student01

Password: ●●●●●●

OK Cancel

- f. Click ok.
- g. Test the new credentials. In the “PI SDK Utility” un-check and re-check the server PISRV01.PISCHOOL.INT. You should now see the following:



- h. The mapping for PISCHOOL\student01 is now being used!

Step 14. We will now repeat the same steps for the **local account PIBuffer**. However, since we are not running as the user `.\PIBuffer`, we will have to use the command prompt to add credentials to the Credentials Manager for the account

- a. Run the command prompt
- b. Enter the following command

runas /user:PIBuffer cmd

This will run a command prompt as the local user PIBuffer. Enter the password “P1school!” when prompted.

- c. A new command prompt should have appeared. Enter the following command:

**CMDKEY /add:PISRV01.PISCHOOL.INT /user:PISCHOOL\svc-PIBuffer
/pass:student**

This will add an entry to the Credentials Manager for the local user PIBuffer

- d. Test the new credentials by restarting the PI Buffer Subsystem.
 - i. On PISRV01, in PI SMT, navigate to Operations > Network Manager Statistics
 - ii. Refresh the page. How is pibufss.exe on computer PIINT02 connecting?

Step 15. We will now repeat the same steps for the **local account OPCInterface**.

- a. Run the command prompt
- b. Enter the following command

runas /user:OPCInterface cmd

This will run a command prompt as the local user PIInterface. Enter the password "P1school!" when prompted.

- c. A new command prompt should have appeared. Enter the following 2-line command:

**CMDKEY /add:PISRV01.PISCHOOL.INT /user:PISCHOOL\svc-PIInterface
/pass:student**

This will add an entry to the Credentials Manager for the local user OPCInterface

- d. Since the PI Interface for OPC DA connects to the PI Data Archive using the PI API, it will NOT be able to connect using WIS. Test this by restarting the PI Interface for OPC DA.
 - i. On PISRV01, in PI SMT, navigate to Operations > Network Manager Statistics
 - ii. Refresh the page. How is OPCpE on PIINT02 connecting?

Part 6 – Upgrade the PI API to the PI API for Windows Integrated Security

Step 16. Log on to PIINT02

Step 17. In the folder C:\Course Folder\Install Kits, run the program "PIAPI-2018-for-Windows-Integrated-Security_x.x.x.xx_". You may be prompted to reboot the computer.

Step 18. When the install finishes and the computer restarts, make sure the PI Buffer Subsystem and PI Interface services are running.

Part 7 – Validate the new authentication model

Step 19. Log on to PISRV01

Step 20. In SMT, navigate to Operations > Network Manager Statistics

Step 21. Confirm that the PI Interface for OPC DA has received the PIInterfaces identity

Step 22. In PI Vision, validate that you are still receiving data for the tag Tank1.MixerSpeed

Video: Create, Map, and Grant Permissions to Custom Identities in AF

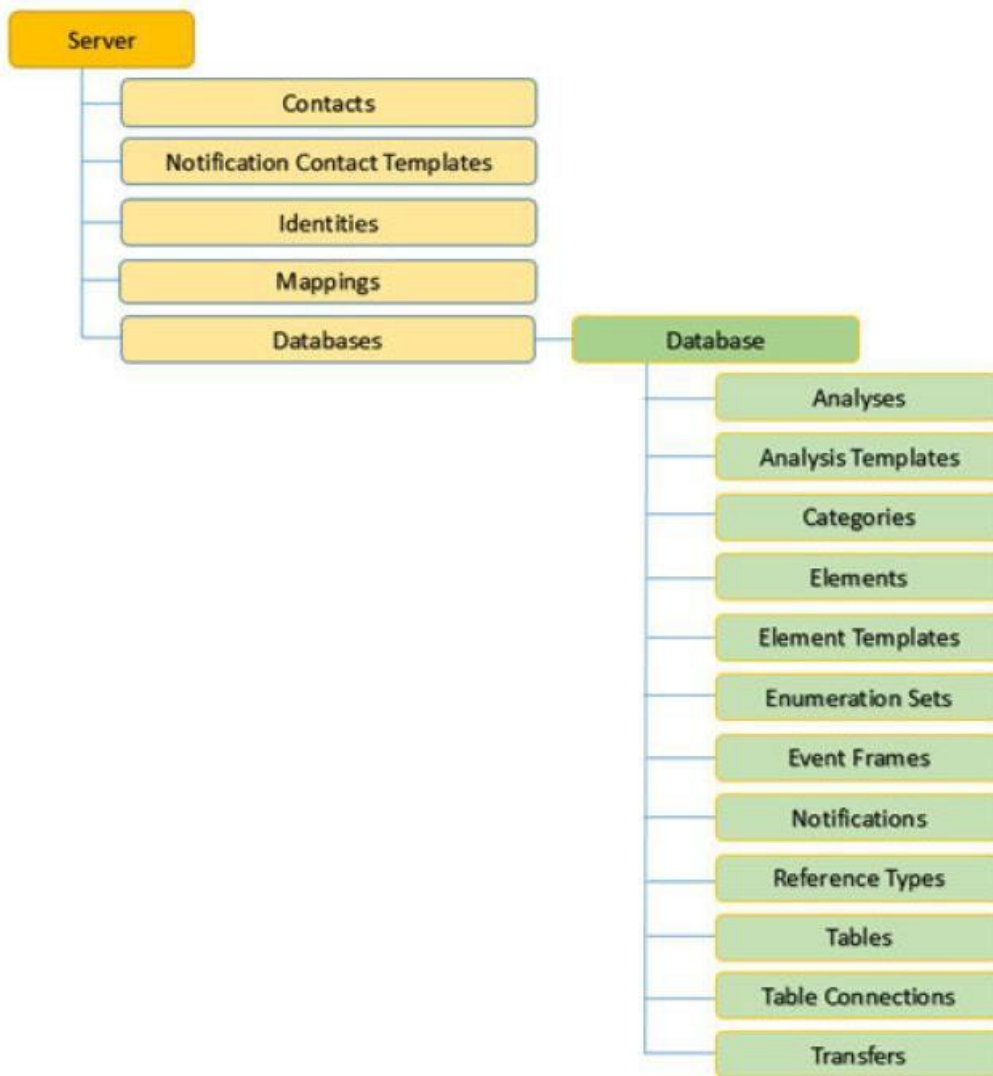
Asset Framework Security

Authentication and Authorization

AF version 2.7 and later uses a security model that is similar to the one used in Data Archive. This model relies on integrated Windows security for authentication, but provides its own authorization to AF objects using AF Identities and mapping.

Security hierarchy

AF identities control read, write, delete and various other permission on AF components. Each AF object (shown in the illustration below) has an associated security descriptor as well as a type (Elements, Notifications, etc.). Each object of the same type belong to a collection. Finally, each collection has an associated security descriptor that contains access permission information.



Security descriptors for some collections are configured for the entire server (Contacts, identities, Mappings, etc.) while others can be configured for specific databases (Elements, Event Frames, Notifications, etc.).

Note: A user **MUST HAVE** read permission on an AF database to be able to read any object within it. Same principle goes for write permission and modifying an object. Note, if you grant access at the database level, that access does not inherit down to the contained objects.

There is one exception: a user with “admin” rights on the “Server” objects will have unlimited access to everything in the server, regardless of the ACLs of the server’s objects.

Permission inheritance

When an AF object or collection is created, a default set of access permission is assigned, based on the access permissions that are set on the parent. However, when you change permission on the parent, the following **Child Permission** settings can be used:

Option	Description
Do not modify child permissions	<p>Prevents access permissions that have been set for the current object or collection from being replicated to child collections and objects in the AF hierarchy.</p> <p>This option is the default when the connected AF server is running 2.5 and earlier versions.</p>
Update child permissions for modified identities	<p>For each selected item on the Items to Configure list in the Security Configuration window, replicates the access permissions for all child collections and objects for each identity on the Identities list whose access permissions have been modified. This option is the default when the connected AF server is running 2.6 and later versions. This option is not available when the connected AF server is running 2.5 and earlier versions.</p>
Replace child permissions for all identities	<p>For each selected item on the Items to Configure list in the Security Configuration window, replaces all child permissions for every identity on the Identities list with the parent access permissions.</p>



For more information on AF security see the "Security configuration in AF" section in *PI System Explorer User Guide*, version 2018 R2.

Exercise: AF Security

Objectives

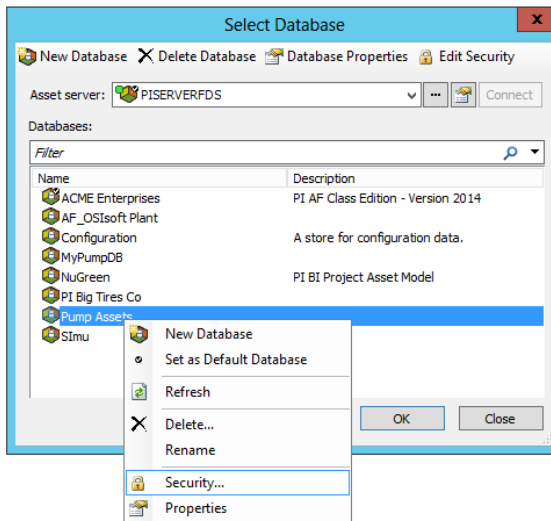
- Familiarize yourself with AF security
- Modify AF security from an existing database

Problem Description

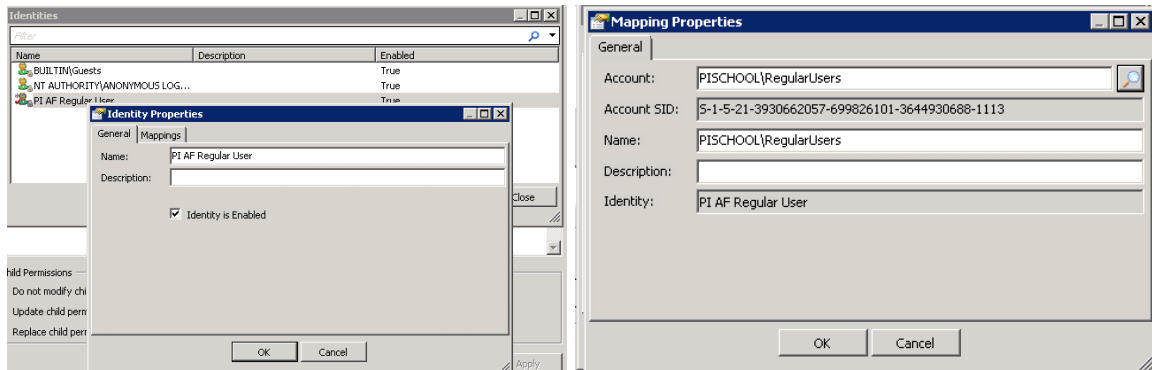
In order to maximize the AF experience, you want to create a AF Identity that will be used by all of your regular users. This identity should have read on the Pump Assets database and should also have the permission to create and modify only elements.

Approach

1. Open PI System explorer and click on the Database icon on top left of your screen.
2. In the select Database section right click on your database name and select security.



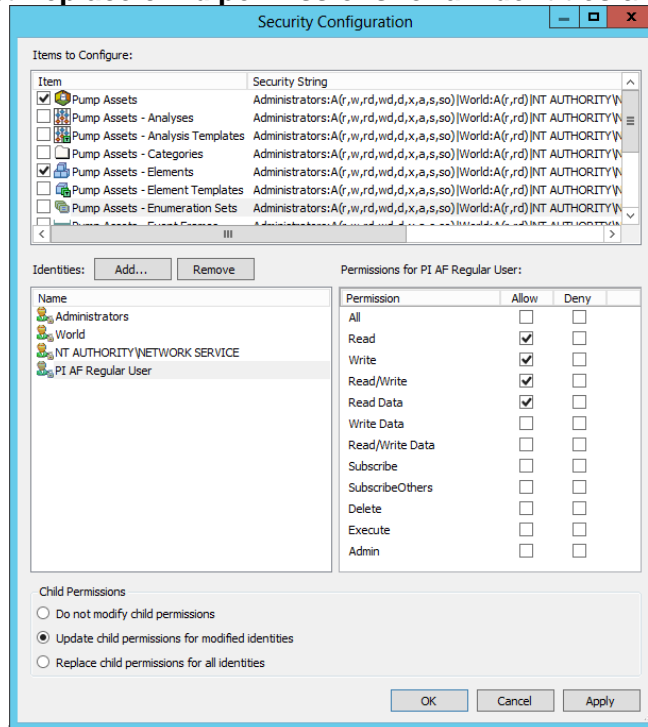
- Step 1.** In the Identities section, Add a new identity named “PI AF Regular Users” and map it to the RegularUsers Windows group



- Step 2.** We can now add the Read permission to the “Regular Users” Identity. With all the items selected under “Items to Configure”, select only **Read** and **Read Data** access for “Regular Users”. Select the child permission **Replace child permissions for all identities** and click on Apply.

- Step 3.** The last step is to add the Write permission to the Element section. In order to have write permission to an object in a database, the AF Identity “Regular Users” needs to have write access to the database.

Step 4. Under “Items to Configure”, uncheck all the items except “Database” and “Elements”. Then, select the identity “Regular Users”, and add Write permission. Finally, select **Replace child permissions for all identities** and click on Apply.



Step 5. Now go ahead and test if your AF security modifications worked by right-clicking the PI System Explorer icon on the task bar and selecting “run as a different user”. Run as the user “pischool\Joe” (password: P1school!) who is a member of the group “RegularUsers” .

Exercise: Your Database Security

Objectives

- Edit the Security for your Pump Asset database

Problem Description

You would like to configure the security of your Pump Asset database. The first thing that should be done is to restrict the access to the database so that only the Windows users you have added can read the database.

The engineers (Engineers Windows group) should have access to create and modify all the elements and analysis of the database but not the templates.

The supervisors (Supervisors Windows group) would like to be informed of any problem with the pumps. In order to do so they would need to be able to create PI Notifications on the Database.

As for the operators (Operators Windows group), they only need to be able to view the elements and attributes already build in the database.

Approach

Step 1. Start by creating the AF Identities needed and mapped those to the corresponding Windows account

Step 2. Next step would be to modify the AF security of your database in order to respect the security definition defined in the Problem Description

Step 3. Test the AF security by right-clicking the PI System Explorer icon and selecting *run as a different user*. For the following user are you able to:

- PISCHOOL\Bertha (password: P1school!)
 - Create a new element in your database: YES NO
 - Create a new analysis in any elements: YES NO
 - Modify the pump template YES NO

- PISCHOOL\Homer (password: P1school!)
 - View elements attribute and values: YES NO
 - Modify an element or template: YES NO

- PISCHOOL\Charles (password: P1school!)
 - Access and create notifications YES NO