PI Asset Framework 2012

Installation Guide

OSIsoft, LLC

777 Davis St., Suite 250
San Leandro, CA 94577 USA

Tel: (01) 510-297-5800
Fax: (01) 510-357-8136
Web: http://www.osisoft.com

OSIsoft Australia • Perth, Australia
OSIsoft Europe GmbH • Frankfurt, Germany
OSIsoft Asia Pte Ltd. • Singapore
OSIsoft Canada ULC • Montreal & Calgary, Canada
OSIsoft, LLC Representative Office • Shanghai, People's Republic of China
OSIsoft Japan KK • Tokyo, Japan
OSIsoft Mexico S. De R.L. De C.V. • Mexico City, Mexico
OSIsoft do Brasil Sistemas Ltda. • Sao Paulo, Brazil
OSIsoft France EURL • Paris, France

PI Asset Framework 2012 Installation Guide

Version: 2.5

Published: 05 November 2012

Table of Contents

Chapter 1

Deployment Scenarios for PI Asset Framework

PI Asset Framework (PI AF) is a key component of the PI System that allows organization of data with context, such as the physical assets such as equipment, devices, processing units that exist in a plant.

The default PI AF installation includes both the PI AF application service and the PI AF SQL database. Together, the application service and database are referred to as the PI AF server. You may install these components on a single computer or on different computers. PI AF supports a variety of installation configurations, including installing the PI AF application service and the PI AF SQL database on different computers, installing the PI AF SQL database on a mirrored SQL Server, or implementing high availability features with PI AF server collectives.

This chapter contains the following topics:

- *PI AF Architecture* (page 1)
- *Simple PI AF Deployment* (page 2)
- *PI AF on a Mirrored SQL Server* (page 3)
- *PI AF Collective* (page 3)
- *PI AF on Microsoft Cluster Services (MSCS)* (page 5)
- *Configuration Options for PI Server, PI AF Server, and SQL Server* (page 6)
- *Frequently Asked Questions about Deployment* (page 8)

PI AF Architecture

PI AF uses a multi-tiered architecture. A minimal system consists of a client application or the PI AF SDK, the PI AF server application service, and the PI AF SQL database.

In terms of physical topology, any configuration of the three tiers is possible, including running all tiers on the same system or on separate systems.

- Clients can communicate with multiple PI AF servers and multiple PI Servers.
- A single PI AF server can service multiple clients.
- A single PI AF SQL database can host multiple PI AF servers.
- High availability features can be configured many ways, including load-balanced PI AF servers, SQL Server mirroring, SQL Server replication, Microsoft Cluster Service (MSCS), or combinations of these methods.

Simple PI AF Deployment

The most common production deployment of a PI AF implementation has the PI AF server deployed on one computer consisting of both the PI AF application service and PI AF SQL database.

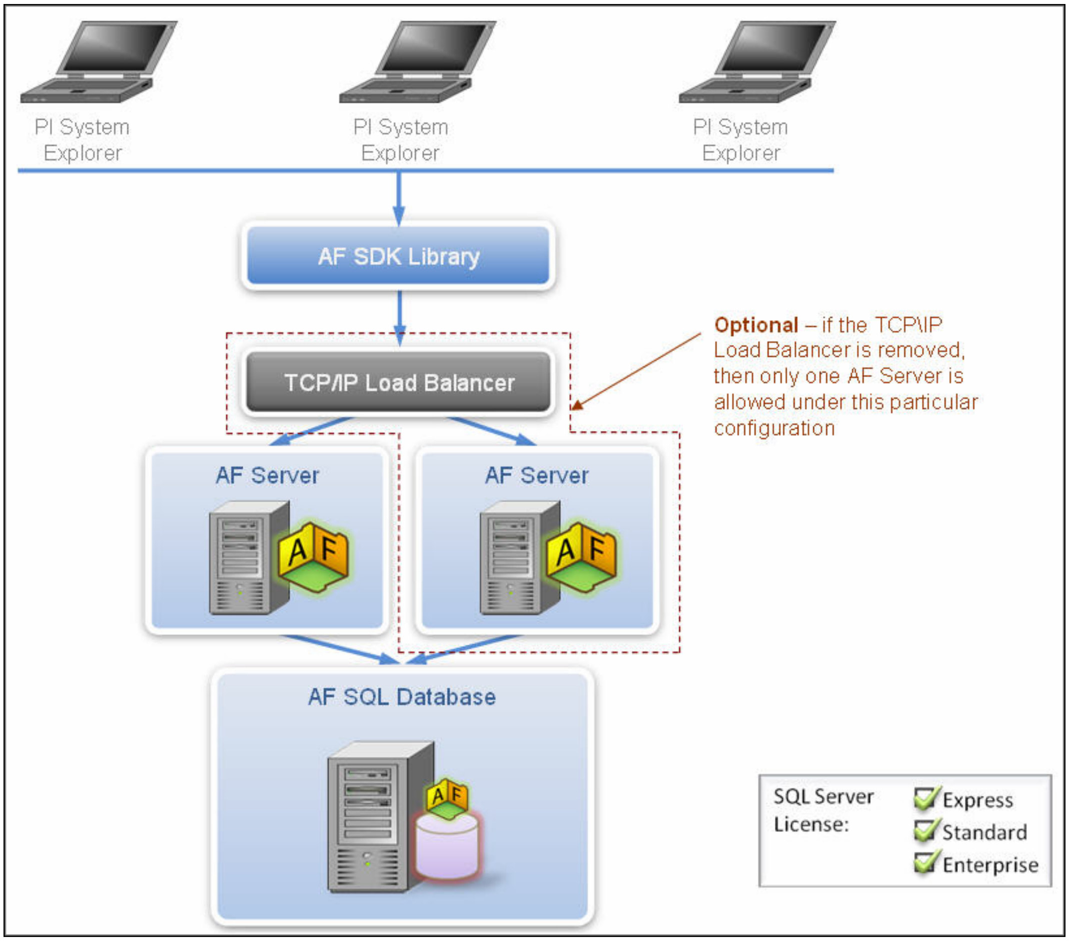
For systems with few assets (10,000 or less) and low to moderate workloads (25,000 PI points or fewer), OSIsoft recommends that you:

- Install PI Server, PI AF server, and SQL Server on the same computer.
- Use SQL Server Express edition or higher, SQL Server version 2005, or later. See *SQL Server Requirements* (page 17).
- Consider installing SQL Server on a different computer from the PI Server. Installing SQL Server Standard or Enterprise edition on the same computer as the PI Server can significantly degrade PI Server performance.

Possible deployment scenarios include:

- Deploy the PI AF application service and PI AF SQL database on the same computer, and deploy a PI AF client on the same computer or on a different computer.
- Deploy the PI AF application service and PI AF SQL database on separate computers, and deploy a PI AF client on one of these computers or on a different computer.
- Deploy the PI AF application service on multiple computers pointing to a single PI AF SQL database, and deploy a network load balancer between the PI AF client and the AF application services.

For example:



PI AF on a Mirrored SQL Server

Deploy PI AF on a mirrored SQL Server for a highly available system. Possible scenarios include:

- Deploy the PI AF application service and PI AF SQL database on separate computers, with the PI AF SQL database on a mirrored SQL Server, and deploy the PI AF client on a different computer.
- Deploy the PI AF application service on multiple computers pointing to a PI AF SQL database that is installed on a mirrored SQL Server, and deploy a network load balancer between the PI AF client and the PI AF application services.

PI AF Collective

A PI AF collective is a set of PI AF servers that acts as the logical PI AF server in a PI System to provide high availability (HA), disaster recovery, load distribution, and increased scalability.

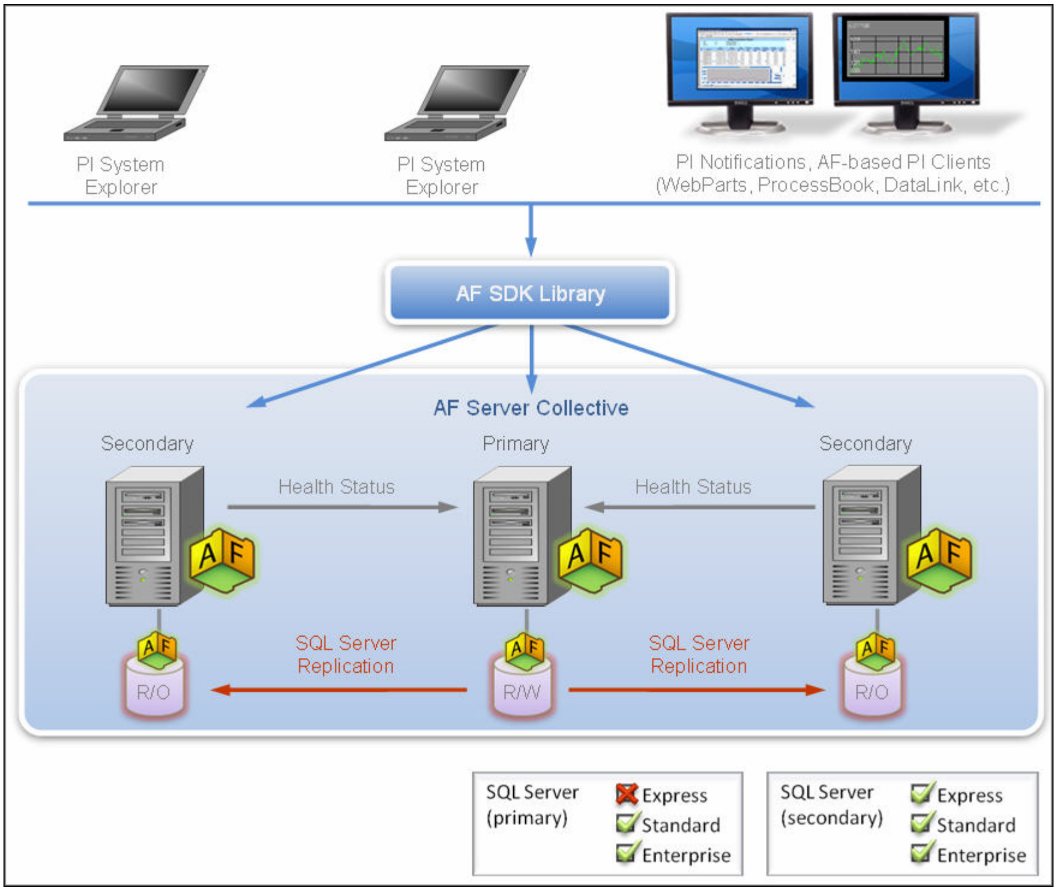
Deployment scenarios for a PI AF collective include:

- Multiple pairs of a PI AF application service and a PI AF SQL database (the PI AF application service and PI AF SQL database pair can be on the same computer or different computers) configured into an PI AF collective, with a PI AF client on the same computer or on a different computer.
- Multiple pairs of a PI AF application service and a PI AF SQL database configured into a PI AF collective, with each pair configured as a SQL Server cluster or mirrored SQL Server.

Sample PI AF Collective Configuration

The high availability (HA) feature, implemented with PI AF, uses a PI AF collective. Since the failover and load balancing logic is implemented at the level of the PI AF SDK, each PI AF SDK instance must know the address of at least one of the PI AF servers in a PI AF collective. After the PI AF SDK connects to the PI AF server, the PI AF SDK is updated with the information about the other members of the PI AF collective. The PI AF SDK will select the appropriate PI AF server, detect failure, and switch to the next appropriate PI AF server.

Each PI AF server / PI AF SQL database pair can be on the same computer or on different computers. Each PI AF server must know its server role (primary or secondary), each primary server must know where the secondary servers are located to allow for replication, and each secondary server must know where the primary server is located in order to send its status to the primary. SQL Server replication enables the secondary database server(s) to contact the primary database server and replicate metadata and data.



In the figure, R/W indicates that the primary server supports reading and writing of data by PI AF clients. R/O indicates the secondary servers only support reading of data by PI AF clients.

The primary server could be located at headquarters and each plant could have a secondary server. Data writers always connect to the primary server to make changes. Users at each plant connect to their local secondary server, except to write, in which case they connect to the primary server. The primary server and all secondary servers will contain the same exact data.

For detailed information about using PI AF collectives, see *Manage PI AF Collectives* (page 65).

Note: Back up your data even if you use SQL Server replication. For example, if you mistakenly delete the PI AF SQL database from the primary server, SQL Server will replicate this deletion to the secondary servers, and all your PI AF data would be lost.

PI AF on Microsoft Cluster Services (MSCS)

Here are a couple of high availability deployment scenarios for PI AF on a SQL Server cluster:

- Deploy PI AF application service and PI AF SQL database on separate computers. Install the PI AF SQL database on a SQL Server that resides on a MSCS cluster. Install the PI AF client on a different computer.
- Deploy PI AF application service on multiple computers pointing to a PI AF SQL database that installed on a SQL Server cluster. Deploy a network load balancer between the PI AF client and the PI AF application services.

Configuration Options for PI Server, PI AF Server, and SQL Server

For PI Server, PI AF server, and Microsoft SQL Server, you need one or more Microsoft Windows compatible computers, preferably 64-bit operating system. It is possible to install a 32-bit version of Windows on a 64-bit computer. However, the computer would not have the benefits of 64-bit Windows operating systems, such as more than 2GB of RAM per process.

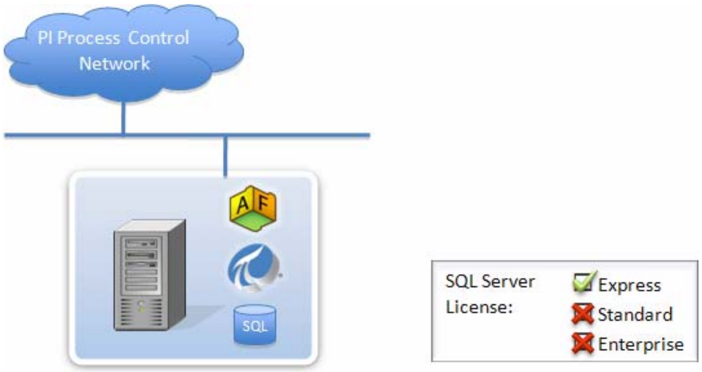
For best performance and improved security, OSIsoft recommends that you install SQL Server on a different computer from PI Server. OSIsoft also recommends at least two physical drives on the PI Server computer.

You must install PI AF server and PI Server on different computers if:

- PI AF server will use time-series data from multiple PI Servers or PI AF collectives.
- PI AF server is configured for high availability (such as a PI AF collective, load balanced PI AF servers, PI AF servers connected to a mirrored SQL Server, or PI AF servers connected to clustered SQL Servers).

The number of required computers depends on the size and complexity of your PI System.

Small System, Single PI Server

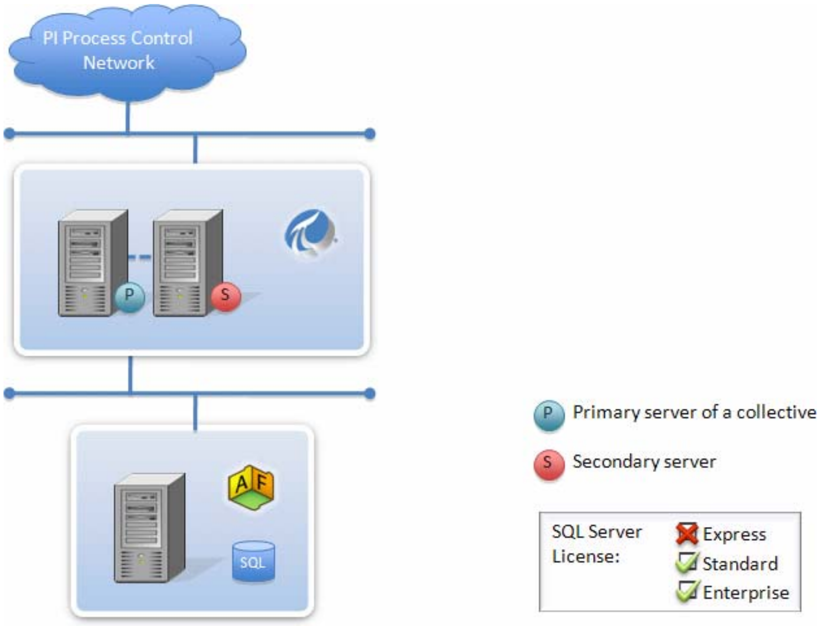


For systems with few assets (10,000 or less) and low-to-moderate workloads (25,000 PI points or fewer), OSIsoft recommends that you:

- Install PI Server, PI AF server, and SQL Server on the same computer.
- Use SQL Server Express edition. (In general, OSIsoft recommends that you use SQL Server 2008 R2 Enterprise edition, except for the case of a small PI AF SQL database with few users and low usage.)

- Consider installing SQL Server on a different computer from PI Server, or use a shared SQL Server that supports many applications in addition to PI AF.

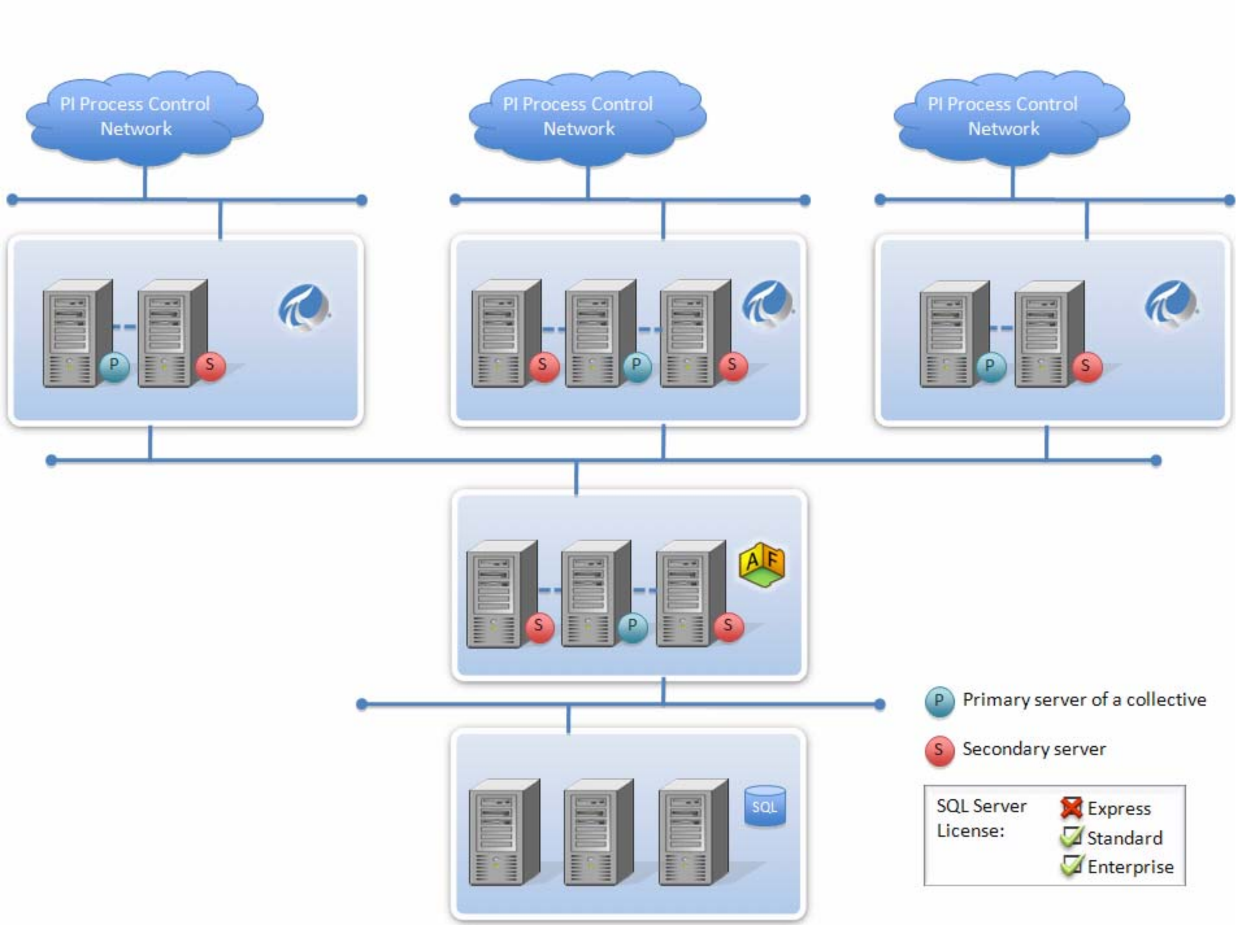
Larger, Higher Performance PI System



For systems with more than 10,000 assets, and moderate-to-high workloads and point counts, OSIsoft recommends that you:

- Install Microsoft SQL Server on a separate computer from PI Server.
- Install PI AF server on either the PI Server or SQL Server computer.
- Use Microsoft SQL Server Standard or Enterprise edition instead of Express edition.
- Consider using PI Server collectives and PI AF collectives for higher performance and scalability.

Distributed, Highly Available PI System


PI Process Control Network
PI Process Control Network
PI Process Control Network
P
S
S
P
S
P
S
S
P
S
A F
SQL
P Primary server of a collective
S Secondary server
SQL Server License:
☒ Express
☑ Standard
☑ Enterprise

For distributed systems with large workloads and point counts, and with multiple PI Servers or PI Server collectives that link to a central AF database, OSIsoft recommends that you:

- Install PI Server collectives, PI AF collectives, and Microsoft SQL Server on separate, redundant computers to achieve the best level of performance and scalability.

Frequently Asked Questions about Deployment

Question	Answer	Explanation
Can the PI AF application service run on the database server system?	Yes	
Can the PI AF application service run on a different system from the database server?	Yes	
Can the PI AF application service run on a system in a domain that is not trusted by the domain of the database server system?	Yes	Configure the PI AF application service to use a SQL Server login, instead of Windows Authentication when connecting to the SQL Server.
Can the database server use the default instance?	Yes	Modify the PI AF application service connection string to use the default instance or an appropriate alias.

Question	Answer	Explanation
Can the database server use a named instance?	Yes	Modify the PI AF application service connection string to use the named instance or an appropriate alias.
If the PI AF application service is not installed on the database server system, what software, other than the SQL Server components, gets installed on the database server system?	None	
Will PI AF server operate correctly when the database is installed on a shared SQL Server instance?	Yes	
How many SQL Server databases does the application require?	1 or 2	The setup program creates a single PI AF SQL database named '`PIFD`'. PI AF creates a second user database named '`PIFD_Distribution'` on the primary for SQL Server replication.
Is any specific collation required?	Yes, case insensitive.	Although the installation procedure does not specify any particular collation, `SQL_Latin1_General_CP1_CI_AS` has had the most testing.
Does PI AF expect SQL Server to listen on a specific port?	No	
Does the database run in MULTI_USER mode?	Yes	
Are any additional SQL Server features required?	Yes	SQL Server Agent service is required for automated backup or if PI AF is configured for high availability. PI AF high availability requires the replication feature of SQL Server.
Is IIS required on the database server system?	No	
Is .NET Framework required on the database server system?	Yes	Unless the DBA manually installs the PI AF database objects, the setup program requires .NET Framework version 4.0. However, this can be removed after the installation.
Is MS-DTC required?	No	
Is it necessary to enable remote database connections?	Yes	Yes, if the PI AF application service is not installed on the database server system.

PI AF High Availability Options

There are a number of high availability (HA) options for PI AF, both for the MS SQL Server that hosts the PI AF SQL database (PIFD) and for the PI AF application service.

MS SQL Server HA options	PI AF server HA options
Clustered	Clustered
Mirrored	Load balancing

MS SQL Server HA options	PI AF server HA options
Transactional replication (with PI AF collective)	PI AF collective

MS SQL Server HA with PI AF

See Microsoft's technical support website for high availability solutions for MS SQL Server

There are advantages and disadvantages for using MS SQL Server with PI AF:

MS SQL Server HA	Advantages	Disadvantages
Clustered	▪ Allows for full-time R/W access to PI AF database. ▪ No resynchronization required. Cluster members always use latest shared copy of PI AF database.	▪ Requires significant initial investment in cluster hardware ▪ May be slow to failover between cluster members (compared to mirroring) ▪ Only one copy of the database. ▪ Distance between nodes is limited to a few meters because of physical shared drive.
Mirrored	▪ Allows for full-time R/W access to AF database. ▪ Fast failover time (compared to SQL clustering). ▪ Two copies of the database on independent hardware. ▪ The members can physically be separated by a long distance.	▪ Requires 3rd witness server for hot failover. ▪ If run in asynchronous mode, the mirror database may not always be up-to-date with changes.
Transactional replication (with PI AF collective)	▪ Low cost entry into HA (reuse existing hardware, easy to implement, can use SQL express for secondary servers). ▪ Can scale out PI AF reads across API F/SQL servers with AF collective static load balancing. ▪ Two or more copies of the database on independent hardware. ▪ The members can physically be separated by a long distance.	▪ Allows only R/W access to PI AF database on collective Primary, Read access only on secondary members ▪ Not appropriate if PI AF metadata writes are required around-the-clock. ▪ SQL express members will scale poorly for heavily used PI AF databases ▪ Unless clustering or mirroring is used on the primary SQL Server, writing will not be possible if the Primary SQL Server is not available. ▪ Renaming the PIFD database is not supported.

PI AF High Availability Solution Comparison

Here is a High Availability (HA) solution comparison for PI AF application server.

PI AF Server HA Type	Pros	Cons
Clustered	No real advantages, other than it can help restart the service if it fails.	▪ Requires significant initial investment in cluster hardware. ▪ PI AF server unavailable during cluster failover period. ▪ No real advantage over having single server service restart itself on failure.
Network Load Balancing	Allows for load balancing across multiple servers using Network Load Balancing (NLB) clusters or round-robin DNS.	Network Load Balancing may be single point of failure if unavailable.
PI AF Collective (with Static load balancing)	Low-cost entry into HA.	▪ Static load balancing across PI AF collective members requires per-client PI AF SDK configuration. ▪ As of Feb 2012, there is no dynamic load balancing available.

Chapter 2

PI AF Pre-installation Tasks

Before you install PI AF:

1. See *PI System Installation Order* (page 13).
2. Log on to your Windows system using an account with administrator privileges.
3. Close OSIsoft applications that are currently running.
4. Verify system requirements. Refer to the *PI AF 2010 R2 Release Notes* for the latest system requirements.
5. *Determine Roles and Permissions* (page 15).
6. *Synchronize Time Settings on PI System Computers* (page 15).
7. *Install or Enable OSIsoft Prerequisites* (page 16).
8. *Download the PI AF Install* (page 16).
9. *Install Microsoft SQL Server* (page 17).

PI System Installation Order

When installing or upgrading the PI System, including PI Server, PI AF server, PI AF client, and PI AF-dependent applications, such as PI Notifications, follow this order:

1. Perform the PI AF Server Pre-installation Tasks.
2. Install Microsoft SQL Server.
3. Install the PI AF server.

   You are not required to install the PI AF application service on the same computer as SQL Server.

   If installing SQL Server separately:

   a. On the SQL Server computer, run the PI AF Server setup program and install the PI AF SQL database feature.

   b. If you are installing the SQL scripts without executing them, follow the steps in "Manually Creating the PI AF SQL Database" in the *PI AF Installation and Maintenance Guide*.

   c. On the PI AF application service computer, run the PI AF Server setup program and install the PI AF application service feature.

4. Perform the PI Server Pre-installation Tasks.

5. Install any PI Servers that will be using the PI AF server for storing the PI Module Database or notification histories. This installation must precede the PI AF client installation on PI Server computers.
6. Install the PI AF SDK and, optionally, PI System Explorer. The PI AF SDK and PI System Explorer do not need to be on the same computer as the PI AF server. For PI Server computers, the PI AF SDK and PI System Explorer are installed during PI Server installation.
7. Install any PI AF-dependent applications, such as PI Notifications or PI AF Compatibility Layer, on the same computer where the PI AF Client is installed.

Refer to each PI System product user manual for detailed installation procedures.

System Requirements

This release supports Windows XP (SP2 or later), Windows Server 2003 (SP1 or later), Windows Vista, Windows Server 2008, Windows Server 2008 R2, Windows Server 2008 R2 Server Core, and Windows 7. Both 32-bit and 64-bit versions of the applicable operating systems are supported.

Refer to the *PI AF Release Notes* for detailed system requirements.

Hardware Requirements

PI AF is extremely flexible and supports the storage of many different kinds of objects. For example: a PI AF object can be as simple as a static numeric value or string of text, or it can be a much more complicated object such as PI Event Frames, custom data references, or even binary objects. As such, it is not possible to definitely correlate the number of PI AF objects to hardware requirements. However, there are some general guidelines.

Your hardware sizing should be based upon workload, not PI AF object count, because they do not correlate. As input and output (I/O) workload increases, it is important to ensure the disk subsystem can handle the I/O count as well as the storage requirements. Adding memory (RAM) improves SQL Server read and write performance. Increasing the number or performance of the CPU is helpful for concurrent users.

Windows Operating System Requirements

The following Windows operating systems are supported:

- Windows XP (SP2 or later)
- Windows Server 2003 (SP1 or later)
- Windows Vista
- Windows Server 2008
- Windows Server 2008 R2
- Windows 7

PI AF supports 32-bit and 64-bit versions of these operating systems.

Determine Roles and Permissions

This topic can help you determine your roles and permissions for PI AF.

Question	Answer
Does PI AF require the `SysAdmin` role?	No.
Does PI AF require a login through the "`sa`" account?	No.
Does PI AF require `db_owner` role?	No.
How many logins are required?	1 or 2. Low privileged login for account that runs the PI AF server needs `db_afserver` role. Should not be granted higher privilege. Never allow the PI AF server to connect to SQL Server with SysAdmin privileges. For PI AF with high availability, SQL Server replication is used and the PIAdmin user requires the db_owner role during setup or during changes to the SQL Server replication.
What roles / permissions does the PI AF server need during runtime?	Account that runs the PI AF application service must be a member of `db_AFServer` application role.
Does PI AF use extended stored procedures, such as `XP_cmdshell`?	No. OSIsoft recommends that the DBA disable `XP_cmdshell`.
Does PI AF use .NET CLR embedded in SQL?	No. Beginning in PI AF 2.4, the PI AF server no longer uses or enables .NET CLR in SQL.

Synchronize Time Settings on PI System Computers

For all computers that are part of the PI System, you must ensure that the time is set correctly and synchronized to PI Server. In addition, make sure that all Windows computers have the proper time-zone settings and that they are set to automatically adjust for daylight-saving changes

OSIsoft recommends that you synchronize the PI Server clock with a network time protocol (NTP) server.

For details, see the OSIsoft Technical Support Web page about daylight saving time at: http://techsupport.osisoft.com/Knowledge+Center/System+Manager+Resources/Daylight+Saving+Time/Daylight+Saving+Time+Home.htm.

Install or Enable OSIsoft Prerequisites

Installation of OSIsoft products depends on the presence of operating system components such as the Microsoft .NET Framework. The OSIsoft Prerequisites Kit checks for the presence of these prerequisites and installs them if necessary.

Note: Before you install the OSIsoft Prerequisites kit on Windows 2008 Server, make sure that the Microsoft .NET Framework 3.5 SP1 feature is enabled.

To enable OSIsoft Prerequisites on Server Core installations of Windows Server 2008 R2:

1. Open a command prompt window.
2. Go to the directory where you extracted the files from the setup kit.
3. At the command prompt, type:

   ```
   silent -enabledotnet
   ```

To enable OSIsoft Prerequisites for Full Installations of Windows Server 2008 R2:

1. Click **Start** > **Administrative Tools** > **Server Manager**.
2. Right-click **Features** on the tree view and select **Add Features**. The **Select Features** dialog box appears.
3. Double-click **.NET Framework 3.5.1 Features**. The **.NET Framework 3.5.1** and **WCF Activation** check boxes appear.
4. Select the **.NET Framework 3.5.1** check box.
5. Click **Next**. The **Confirm Installation Selections** dialog box appears.
6. Click **Install**.

To Install OSIsoft Prerequisites for Windows Server 2003 and 2008:

1. Double-click the self-extracting executable for the OSIsoft Prerequisites Kit.
2. Click **Unzip** to extract the files and start the Setup program.
3. Follow the prompts of the Setup program to install the prerequisites.

Download the PI AF Install Kit

1. From the OSIsoft Technical Support Web site, click **My Support** > **My Products**.
2. Find the PI AF software that you want to install.

   The **Download** page displays a table of all the install kits available to you.
3. Select the install kit and click **Download Now**.
4. Read the OSIsoft, LLC. ("OSIsoft") Software License and Services Agreement and click **I Agree.**
5. When prompted to run or save the executable (`.exe`) file, click **Save** and click **OK**.

Install Microsoft SQL Server

This section contains these topics:

- *SQL Server Requirements* (page 17)
- *SQL Server Considerations* (page 18)
- *SQL Server Installation Guidelines* (page 18)

Related topics:

- *Security Overview for PI AF* (page 83)
- *PI AF Collective SQL Server Installation Requirements* (page 67)

SQL Server Requirements

General	Details
Supported SQL Server editions	Express Standard Enterprise Datacenter
Supported SQL Server versions	SQL Server 2005 32 bit x86 SQL Server 2005 64 bit x64 SQL Server 2008 32 bit x86 SQL Server 2008 64 bit x64 There is no support for the Itanium CPU. The 32-bit PI AF server works with 32-bit or 64-bit SQL Server. The 64-bit PI AF server works with 32-bit or 64-bit SQL Server
Required SQL Server components	Database engine, SQL Agent (backup and replication)

In general, OSIsoft recommends that you use SQL Server 2008 R2 Enterprise edition, except for the case of a small PI AF SQL database with few users and low usage. Although supported by PI AF, SQL Server 2008 R2 Express has a 1 GB memory limitation and 10 GB database size limitation. In addition, SQL Server 2008 R2 Express does not support Microsoft Business Intelligence (BI) tools such as SQL Reporting Services and SQL Analysis Services. PI AF high availability features are not supported with SQL Server 2008 R2 Express.

When estimating the SQL Server disk space required for the PI AF SQL database (PIFD), consider the type and quantity of your PI AF objects. As a first order estimate, a PI AF SQL database with 50,000 elements each with 20 attributes of double data type would consume approximately 3 GB of disk space. If you use PI AF objects such as PI Event Frames, PI Notifications, or other data types, your disk space requirements will increase. In the case of custom PI AF data references, it is prudent to test size-implications in a test environment.

See also *PI AF Collective MS SQL Server Installation Requirements* (page 67).

SQL Server Considerations

Question	Answer
Do end users connect to SQL Server?	No. OSIsoft recommends that end users not be granted privileges on the SQL Server instance
Must end users be granted access to SQL Server objects?	No.
Does the PI AF server control user access to data stored in the SQL Server database?	Yes. Users do not connect to the SQL Server database. The PI AF server uses Windows authentication to identify users and performs AccessCheck on Windows security descriptors stored in the SQL Server tables to control user access to application data.
Does each user require a login to SQL Server?	No. Users do not connect to SQL Server.
Does the DBA have to manage user permissions to SQL Server objects?	No. Users do not connect to SQL Server.
Does the remote application require any Windows permissions on the SQL Server computer?	Yes. Except for managing PI AF collectives (SQL Server replication), the PI AF SDK never connects to SQL Server and therefore the user does not need any permission on SQL Server. For PI AF high-availability management, the user running PI AF SDK must have the SysAdmin role on the SQL Server instance, but no Windows O/S level privileges are required.
Is PI AF compatible with SQL Server clustering, mirroring, and replication?	Yes.

SQL Server Installation Guidelines

Question	Answer
Does the PI AF installation program install SQL Server?	No.
What Windows privileges are required on the database server for the database installation program?	Optionally, none. The installation of the SQL scripts, as well as verification of the SQL connection, can be optionally deselected.
Is it possible for the DBA to manually install the SQL objects without help from the installation program?	Yes.

Question	**Answer**
Are SQL Server scripts available for review by the DBA prior to running?	Yes. The setup kit installs the SQL scripts to the `PIPC\AF\SQL` directory and can optionally be instructed not to execute them as part of the installation. These scripts can be run manually after the installation is complete. Alternately, install on a test system or virtual server image. Capture the SQL scripts or back up or detach the PIFD database and restore it on the production database server.
What SQL Server privileges are required on the database server for the database installation program?	SysAdmin privilege is required if opting for the installation program to create the database. If opting for manual installation, no privileges are necessary. See *Manually Create or Upgrade the PI AF SQL Database* (page 37).
In a database-only installation, what configuration changes are made to the Windows operating system?	None. No files are installed on the database server, other than database files. No registry keys are modified.
Are any objects created in the master database?	No.
Are any objects created in the MSDB database?	No.
Are any objects created in the model database?	No.
Can the DBA control where the database data and log files are created?	Yes. Prior to running the installation program, set the paths in the 'database settings' for the SQL Server instance. If manually installing, modify schema1.sql to explicitly set the paths.
Can the DBA create the database manually?	Yes. `CREATE DATABASE PIFD;` The DBA can specify any paths and database options. Then, either run the installation program or run the SQL Server scripts manually. See *Manually Create or Upgrade the PI AF SQL Database* (page 37).

Chapter 3

PI Asset Framework Installation and Upgrade Tasks

PI AF can be installed in a number of ways. The easiest way to install PI AF is on a single computer. However, you can choose to install the PI AF application service and PI AF SQL database on separate computers. Additionally, you can install PI AF in a mirrored SQL Server environment.

This section contains the following topics:

- *Install or Upgrade PI AF Server on a Single Computer* (page 21)
- *Install or Upgrade PI AF Server Components on Separate Computers* (page 23)
- *Install or Upgrade PI AF Client* (page 24)
- *Install or Upgrade PI AF SQL Database on a Mirrored SQL Server* (page 25)
- *Install PI AF Server when SQL Server has been Uninstalled and Reinstalled* (page 33)
- *Install PI AF Server on a Windows 2003 Server Domain Controller* (page 34)

Install or Upgrade PI AF Server on a Single Computer

To install PI AF server on a single computer:

1. *Download the PI AF Install Kit* (page 16).
2. Do one of the following:
    - o *Run the PI AF Server Setup Program for New Installation.* (page 21)
    - o *Run the PI AF Server Setup Program for Upgrade* (page 22).

Run the PI AF Server Setup Program for New Installation

Use this procedure when you install PI AF Server on a new computer.

1. Go to the directory where you downloaded the PI AF install kit.
2. Double-click the executable (`.exe`) file.
3. On the **Self-Extracting Executable** dialog box, click **Browse**, select the directory where you want to extract the files, and click **OK**.
4. When the installation files have been extracted, click **OK**.

   The **Welcome** page appears.

5. Click **OK**.
6. Click **Next**.
7. In the **User Information** dialog box, enter **Full Name** and **Organization** values, or accept the default values. Click **Next.**
8. Click **Browse** to select a **Destination Folder**, or accept the default folder.

   If this is an upgrade, the destination folder must be the same as the original installation.
9. Click **OK.**

   The **Select Features** dialog box appears.

   If this is an upgrade, only those features selected during the initial install are selected. Since this is an upgrade of a single computer PI AF Server installation, all options should be selected, unless the original installation did not automatically execute the SQL scripts.
10. Accept the selected features and click **Next**.

    The **Local SQL Server Connection** dialog box appears with the default SQL Server instance name, `sqlexpress`.
11. Enter the local SQL Server instance name. If the SQL Server is the default instance, you may leave the field blank.
12. Click **Next**.

    The **Ready to Install the Application** dialog box displays the features that will be installed.
13. Click **Install**.

    The **Updating System** dialog box appears.

    To cancel the installation, click **Cancel**. Depending on the state of the installation process when you cancel, the PI AF SQL database might have already been created and you will need to remove the database manually. Otherwise, allow the installation to continue.
14. If this is an upgrade, and the SQL scripts were manually executed in the original installation:

    a. *Manually Create or Upgrade the PI AF SQL Database* (page 37).

    b. Verify that the PI AF application service is running under the correct account.
15. Click **Finish**.
16. Click **Close**.

Run the PI AF Setup Program for Upgrade

Use this procedure to upgrade an existing installation of PI AF server.

1. Back up the PIFD SQL database.

   When upgrading, the setup program may make update changes to the existing PIFD database. After these changes are complete, a downgrade of the PIFD database will not be possible.

2. Go to the directory where you downloaded the PI AF install kit.
3. Double-click the executable (`.exe`) file.
4. On the **Self-Extracting Executable** dialog box, click **Browse**, select the directory where you want to extract the files, and click **OK**.
5. When the installation files have been extracted, click **OK**.

   The **Welcome** page appears.
6. Click **Next**.
7. In the **User Information** dialog box, enter **Full Name** and **Organization** values, or accept the default values. Click **Next.**
8. On the **Destination Folder** dialog box, click **Next** to accept the default folder.
9. On the **PIFD SQL Database Warning** dialog box, click the **Warning Acknowledged** check box and click **Next**.

   The **Ready to Install the Application** dialog box appears. If the SQL Scripts were manually executed at the original installation, this will be noted on the dialog box.
10. Click **Next**.

    The **Updating System** dialog box appears.

    To cancel the installation, click **Cancel**. Depending on the state of the installation process when you cancel, the PI AF SQL database might have already been created and you will need to remove the database manually. Otherwise, allow the installation to continue.
11. If the **Files in Use** dialog box appears, select whether to automatically close the applications and click **Next**.
12. Click **Close**.
13. If the SQL scripts were manually executed in the original installation:
    a. *Manually Create or Upgrade the PI AF SQL Database* (page 37).
    b. Verify that the PI AF application service is running under the correct account.

Install or Upgrade PI AF Server Components on Separate Computers

You are not required to install all components of PI AF server on the same computer as SQL Server. For example, you might install the PI AF SQL database on your SQL Server computer, but the PI AF application service on a different computer.

When you run the setup program, the **Select Features** dialog box lets you select the features to install. By default, both the PI AF application service and the PI AF SQL database features are selected for installation.

Select Features for Installation

To install the PI AF application service and the PI AF SQL database on separate computers:

1. If this is an upgrade, stop any PI AF application services.
2. On the SQL Server computer, run the setup program, clear the **AF Application Service** feature, and select only the **AF SQL Database** feature.

   Note: If you are installing the SQL scripts without executing them, disable **AF SQL Script Execution** under the **AF SQL Database** feature.

   During the installation, you will be prompted to provide the domain and name of the system where the remote application server can be found so that the proper authentication can be granted to the PI AF application service.
3. On the PI AF application service computer, run the setup program, deselect the **AF SQL Database** feature, and select only the **AF Application Service** feature. During the installation, you will be prompted to provide the name of a remote SQL Server.
4. If you disabled **AF SQL Script Execution** in Step 2, see *Manually Create or Upgrade the PI AF SQL Database* (page 37) .

Install or Upgrade PI AF SDK and PI System Explorer

The PI AF Client consists of the PI AF SDK, PI System Explorer, PI AF Builder, and user documentation. The PI AF Client install kit contains the PI SDK and the PI AF Client.

If you are running the PI AF Client setup program on the same computer as the PI AF server, OSIsoft recommends installing PI AF server first.

PI System Explorer supports multiple languages. Install the PI System Explorer MUI Language Pack to enable multi-language access. If PI System Explorer does not support a particular language, the user interface appears in English. See *Enable Multiple Languages for PI System Explorer* (page 25).

If you intend to use AF Builder on this computer, you must install Microsoft Excel first.

To install the PI AF Client:

1. Verify that you are logged in with administrative rights.
2. Go to the directory where you downloaded the PI AF install kit.
3. Double-click the executable (`.exe`) file.
4. On the **Self-Extracting Executable** dialog box, click **Browse**, select the directory where you want to extract the files, and click **OK**.
5. When the installation files have been extracted, click **OK**.

   The **Welcome** page appears.
6. Enter your user information and click **Next**.
7. Click **Start**.

The PI SDK is installed.

8. Click **Finish**.

   The PI AF Client installation Welcome page appears.

9. Click **Next**.
10. Enter your user information and click **Next**.
11. Optionally, define a network connection to the PI AF server.
12. Click **Next**.
13. Select **Typical** or **Custom** installation type.
14. Click **Next**. The **Installation Complete** dialog appears.
15. Click **Close**.

Enable Multiple Languages for PI System Explorer

PI System Explorer supports multiple languages. Install the PI System Explorer MUI Language Pack to enable multi-language access. If PI System Explorer does not support a particular language, the user interface appears in English.

Procedure

1. Download the PI System Explorer MUI Language Pack from http://techsupport.osisoft.com.
2. Install the PI System Explorer MUI Language Pack.

Install or Upgrade PI AF SQL Database on a Mirrored SQL Server

You can run PI AF SQL database on a mirrored SQL Server. A mirrored SQL Server session can be implemented in various manners. The instructions provided in this section address a single approach, and assume the following:

- The mirrored SQL Server session includes three computers: a principal server; a mirror server; and a witness server.
- Identical SQL Server editions are installed on the principal and mirror SQL Server computers (SQL Server 2008 Standard) using an instance name, while SQL Server 2008 Express edition is installed on the witness computer.
- PI AF Server is installed on a separate computer from those used in the mirrored SQL Server session.
- The PI AF client is installed on a computer that does not include the PI AF application service or the PI AF SQL database.

Set Up PI AF Server on a Mirrored SQL Server System Task Overview

To set up PI AF server on a mirrored SQL Server system, perform the following tasks:

1. *Run the Setup Program on the Principal and Mirror Server Computers* (page 26). Select only the PI AF SQL database feature during setup on both computers.
2. *Install the PI AF Application Service on the PI AF Server Computer* (page 27).
3. *Install the PI AF Client and Connect to the PI AF Server Computer* (page 28).
4. *Back Up PIFD Database on Principal Server and Restore on the Mirror Server Computer* (page 31).
5. *Create a Mirrored SQL Server Session on the Principal Server Computer* (page 32)

Run the Setup Program on the Principal and Mirror Server Computers

On both the Principal and Mirror server computers:

1. Run the PI AF Server setup program.
2. On the **Select Features** dialog box, cancel the **AF Application Service** feature selection.
3. Click **Next**.

   The **Remote SQL Server Connection** dialog box appears.
4. Enter the SQL Server name and SQL instance (if applicable), in the format: `<SQLServerName>[\<InstanceName>]`.

   If you are installing the SQL scripts manually and cannot validate the SQL Server connection because of security issues, you can skip the validation step by clearing the **Validate connection to the remote SQL Server** check box. Note that the PI AF server will not function until the SQL scripts are run and installed.
5. Click **Next**.

   The **Remote Application Server Connection** dialog box appears.
6. If the PI AF application service is not running under a domain account, enter the domain name and computer of the PI AF application service, in the format: `<DomainName>\<AFApplicationServiceComputerName>`.

   If you are running the PI AF application service under a domain account, you do not need to enter a value.
7. Click **Next** and continue through the rest of the setup program.
8. If you are installing the SQL scripts manually, perform the tasks in *Manually Create or Upgrade the PI AF SQL Database* (page 37).
9. If the PI AF application service is running under the NT AUTHORITY\NetworkService account, skip this step.

   If the PI AF application service is *not* running under the NT AUTHORITY\NetworkService account, add the domain account to the AFServers user group:

a. Click **Start** > **Administrative Tools** > **Computer Management** to open Microsoft Windows Computer Management.

b. Under **Computer Management (Local)**, select **System Tools** > **Local Users and Groups** > **Groups**.

c. Right-click the **AFServers** group and choose **Properties**.

d. Click **Add** and on the **Select Users** dialog box, add the domain account under which the PI AF application service runs.

e. Save the changes to the user group and close Computer Management.

Set the PIFD Database Recovery Mode to Full on the Principal and Mirror Server Computers

1. Open Microsoft SQL Server Management Studio, and connect to the SQL Server instance that stores the PI AF SQL Server database (PIFD).
2. Expand **Databases**, right-click **PIFD**, and choose **Properties**.
3. In the **Database Properties – PIFD** window, select the **Options** page.
4. Set the **Recovery model** to **Full**.
5. Click **OK**.

Install the PI AF Application Service on the PI AF Server Computer

On the PI AF server computer:

1. Run the PI AF Server setup program.
2. On the **Select Features** dialog box, cancel the **AF SQL Database** feature selection.
3. Click **Next**.

   The **Remote SQL Server Connection** dialog box appears.
4. Enter the SQL Server name for the principal database server, and SQL instance name (if applicable), in the format: `<SQLServerName>[\<InstanceName>]`.

   If you are installing the SQL scripts manually, and cannot validate the SQL Server connection because of security issues, you can skip the validation step by clearing the **Validate connection to the remote SQL Server** check box. Note that the PI AF server will not function until you install and run the SQL scripts.
5. Click **Next** and continue through the rest of the setup program.
6. If the PI AF application service needs to run under a domain account, follow the instructions in the section *Change the PA AF Application Service Account* (page 84).

Install the PI AF SDK and PI System Explorer and Connect to the PI AF Server Computer

1. Install or upgrade PI AF Client.
2. Start PI System Explorer and connect to the PI AF application service computer
3. Close PI System Explorer.

Related Topics

- *Install or Upgrade PI AF Client* (page 24)
- *Connect to a PI AF Server* (page 28)

Connect to a PI AF Server

To connect to PI AF server in PI System Explorer, follow these steps:

1. Choose **File** > **Connections**.

   The **Servers** dialog box appears. This dialog box lists all the PI servers and PI AF servers for which a connection is configured. The currently connected PI and PI AF servers are indicated with green circles.

2. To connect to a different PI AF server, right-click on the server name in the list and choose **Connect**.

> **Note:** If the server you need is not displayed, you can add it as described in *Add a PI AF Server to the Connection List* (page 29).

View PI AF Server Database and Object Counts

1. Select **File** > **AF Server Properties**.
2. The **AF Server Properties** dialog box appears.
3. Select the **Counts** tab.

   The **Counts** tab shows object counts for the AF Server to which you are currently connected. Displayed information includes number of databases, number of elements, number of element templates, number of event frames, and so on

View AF Server ID, Port, and Other Properties

1. Select **File** > **AF Server Properties**.
2. The **AF Server Properties** dialog box appears.
3. Select the **General** tab.

   The **General** tab contains information about the AF Server to which you are currently connected. Displayed information includes:

- AF Server Name, Host Name, and ID
- AF Server Account
- AF Server version number
- AF Server Port, Timeout, and Aliases

Note: The **General** tab also includes the **Configure Active Directory** button. See *Configuring an Active Directory* (page 30) for more information.

Add a PI AF Server to the Connection List

To add to the list of PI AF servers that PI System Explorer can connect to, follow these steps:

1. In PI System Explorer, choose **File > Connections**.

   The **Servers** dialog box appears. PI Servers version 3.4.370 and earlier marked with a yellow triangle bitmap. You can connect to these earlier server versions, but you might not have complete functionality.

2. Click **Add AF Server.**

3. Enter the AF Server properties.

   - The **Name** does not have to match the host name.
   - The **Host** name may be the fully qualified domain name, server name, or IP address. IPv6 addresses must be enclosed in brackets [ ].
   - Leave the **Account** field blank.
   - The default **Timeout** value of 300 seconds is acceptable in most cases. If you experience timeout errors as you work in the PI System Explorer, increase the time in the **Timeout** box.
   - **Aliases** are alternate names that can be used for the PI AF server when users look up for the PI AF server. PI AF server aliases are stored only locally on the client where they are configured. (Optional)
   - The **Configure Active Directory** button is for setting up the PI Notifications contacts list. This is a PI AF system administrator function. (Optional)

4. Click **OK**.

Note: If an error message appears saying that you cannot connect to the PI AF server, then you need to fill in the **Account** field (*Fill in the Account Field* (page 29)).

Fill in the Account Field

When you add a new PI AF server connection to PI System Explorer, you initially leave the Account field blank. If an error message appears saying that you cannot connect to the PI AF server, then you need to fill in the **Account** field.

1. Type in the name of the account under which the AF Service runs. For example:

   ```
   company.net\afcollective
   ```

Note: You can modify the account only when disconnected from the server.

2. If you still cannot connect, then the PI AF Service account probably lacks the permissions it needs to generate an SPN. Do one of these two things:
   - Have the domain administrator set the domain manually, using the **SetSpn** utility. **This is the recommended option.** Note that Microsoft has some documentation on the concept and implementation of SPNs, and there is a tool (**SetSpn.exe**) that helps with managing them.
   - Have the PI AF administrator configure the PI AF server to use a User Principal Name (UPN) for authentication instead of an SPN. See the *PI Asset Framework Installation and Maintenance Guide* for more information.

Configure Active Directory Access for PI Notifications Contacts

When using PI Notifications with PI AF server, you may need to specify how to access Microsoft's Active Directory in order to retrieve the users used to populate the PI Notifications' Contacts lists.

Each PI AF server provides the option to specify the Domain and User folder, as well as the user account, to be used to access Active Directory and to retrieve users for the Contacts list. By default, the account under which the PI AF server 2.x application service is running is used to retrieve the user information from Active Directory for the domain in which the AF Server resides. However, if you need to access an Active Directory in a different domain, or if you need to define a specific user account to be used to access Active Directory, you will need to configure the PI AF server's Active Directory Access.

1. Open PI System Explorer and connect to a database belonging to the PI AF server for which you want to configure the Active Directory access.
2. From the **Tools** menu, select **Active Directory Properties**. The Active Directory dialog opens.
3. In the **Full Domain Name** text box, enter the full DNS name of the Active Directory domain from which the user accounts will be retrieved for the PI Notifications Contacts. If this field is left blank, the domain in which the PI AF application service resides will be used.
4. In the **User Folder** text box, enter the path to the user folder where the list of users for this domain resides.

   In larger Active Directory domains, users may be organized within folders. The use of User folders can allow for faster retrieval of a list of Active Directory users.

   Use the following structure for the User folder:

   ```
   DomainUserFolder/SubDomainUserFolder/Sub SubDomainUserFolder
   ```
5. You can define the user account to use to access Active Directory for building the PI Notifications Contact list. Select one of the following options:

   Use AF Server's Account – This is the default selection. Select the User AF server's Account option to access Active Directory using the account under which the PI AF application service runs. By default, the PI AF server is installed using the Network

Service account. However, the PI AF server service account can be changed. If the PI AF server’s service account does not have the necessary permission to read the Active Directory, no users will be retrieved in the Contacts list. If your Active Directory security is configured in a way such that the PI AF server’s service account can read the Active Directory, then this is the simplest option.

Impersonate Client - Select this option to use the credentials of the user account under which the connecting client application is running. If the PI AF server’s service is running under an account (Network Service is the default account) that does not have permission to read the Active Directory, this option can be used. As long as the user account under which the connecting client application is running has permission to read Active Directory, a list of users is returned to the Contacts list. The contents of the Contacts list may vary, depending upon the user account used for connecting, since the security to read the users is determined by Active Directory.

Note: Specifying this option may require Kerberos configuration if an AF SDK application will be using impersonation in a middle tier, such as a Web Service or in IIS.

Specify Account – This option allows you to define a specific user account to be used to read the Active Directory. You might use this option if you need to read the Active Directory from a domain that is different than that under which the PI AF server resides, or if the user account under which the PI AF server’s service runs and the account under which the client application runs has no permission to read the required Active Directory. Specify any other account as your application requires, using the format "`Domain\User`." Ensure that the specified user account has the appropriate permission to read the target Active Directory.

6. Select the **Global Catalog** check box for the Active Directory domain controller searches to use the global catalog if it is available. Otherwise searches must go to the owning domain controller.
7. Clear the **Return All Persons** check box to return only users from the target Active Directory.

   Active Directory objects are derived from one another as follows:

   `Top>Persons>OrganizationalPerson>Contact`

   and

   `Top>Persons>OrganizationalPerson>User`

   When you select this check box, Persons, OrganizationalPersons, Contacts and Users are returned from the target Active Directory. If you clear the check box, it returns only Users.

Back Up PIFD Database on Principal Server and Restore on the Mirror Server Computer

1. On the Principal server computer, make a full backup of the PIFD database.

2. On the mirror server computer, Using the back-up file you created in the previous step, right-click the PIFD database and select **Task | Restore | Database** to open the **Restore Database – PIFD** window.
3. In the **Source for restore** area, select the **From device** option.
4. Click the **From device** button to browse to and select the back-up file. Return to the **Restore Database – PIFD** window.
5. Select the **Restore** check box for the newly added back-up file in the list of back-up sets.
6. In the **Options** page follow these sub-steps:
   a. Select the **Overwrite the existing database (WITH REPLACE)** check box.
   b. Select **Leave the database non-operational and do not roll back uncommitted transactions. Additional transaction logs can be restored (RESTORED WITH NO RECOVERY)**.
   c. Click **OK** to start the restore operation.
   d. When a message appears that indicates the restore operation finished successfully, click **OK** to return to Microsoft SQL Server Management Studio. The PIFD database is shown in the **Restoring** mode.

Create a Mirrored SQL Server Session on the Principal Server Computer

1. On the principal server computer, right-click the PIFD database and select **Task | Mirror**.

   The **Database Properties – PIFD** window appears with the **Mirroring** page selected.
2. Click **Configure Security**.

   The **Configure Database Mirroring Security Wizard** appears.
   a. On the **Include Witness Server** page, select **Yes.**
   b. Click **Next**.
   c. On the **Choose Servers to Configure** page, select the **Witness server instance** check box.
   d. Click **Next**.
   e. On the **Principal Server Instance** page, click **Next**.

      The **Mirror Server Instance** page appears.
   f. Select the mirror server from the **Mirror Server Instance** list.

      The **Connect to Server** dialog box appears with the selected server/instance.
   g. Click **Connect** to verify that you are able to connect to the mirror server.

      This returns you to the **Mirror Server Instance** page.
   h. Click **Next**.

      The **Witness Server Instance** page appears.

3. Select the witness server on the **Witness Server Instance** page.

   The **Connect to Server** dialog box appears with the selected server/instance.

   a. Click **Connect** to verify that you are able to connect to the witness server.

      This returns you to the **Witness Server Instance** page.

   b. Click **Next**.

      The **Service Accounts** page appears.

   c. Leave the **Principal, Witness**, and **Mirror** boxes empty if all instances of SQL Server Database Engine are running under the same domain account.

   d. Click **Next**.

   e. The **Complete Wizard** page appears.

4. Click **Finish**.

   The **Configuring Endpoints** window appears. When the endpoint configuration is complete, the **Status** column displays **Success**.

5. Click **Close**.

   The **Database Properties** window appears.

6. Click **Start Mirroring**.

   The **Database Properties – PIFD** window appears. The **Operating mode** is set to **High safety with automatic failover (synchronous)**.

7. Click **OK**.

Install PI AF Server when SQL Server has been Uninstalled and Reinstalled

The PI AF server installation is supported on a SQL Server computer where SQL Server was once removed, then reinstalled. However, this type of installation requires special considerations.

An error can occur during the installation of the PI AF server if the SQL Server has been uninstalled and reinstalled on a computer where the PIFD database has been created previously. The displayed error messages are:

```
Server: Msg 5170, Level 16, State 1, Line 1
Cannot create file 'C:\Program Files\Microsoft SQL
Server\MSSQL10.KATMAI\MSSQL\DATA\PIFD.mdf' because it already
exists. Change the file path or the file name, and retry the
operation.

Server: Msg 1802, Level 16, State 1, Line 1
CREATE DATABASE failed. Some file names listed could not be
created. Check related errors.
```

The following steps lead to this error:

1. Install PI AF server including the SQL script execution feature that creates the PIFD database.
2. Uninstall PI AF server in its entirety.
3. Uninstall SQL Server 2005 or SQL Server Express 2005 or later version.
4. Install SQL Server 2005 or SQL Server Express 2005 or later version.
5. Install PI AF server including the SQL script execution feature.

SQL Server issues these errors shown when you attempt to create a database that already exists but is not ‘attached’ to SQL Server.

To correct this problem, you must either manually remove the database files found in the folder location given by the error message or manually attach the database files to the newly-installed SQL Server.

Install PI AF Server on a Windows 2003 Server Domain Controller

The PI AF server installation is supported on a Windows 2003 Server domain controller for the purposes of testing and demonstration, but you need to take a few manual steps to enable your PI AF server to connect to the PI AF SQL database, PIFD.

Note: By default, only administrators on the PI AF server have write permission to PI AF SQL database. Those with read-only permission have fewer options displayed in the right-click menus. To enable other users to write to PI AF databases while connected as administrator, set the system-level security for groups or individuals.

Follow these steps:

1. *Run the PI AF Server Setup Program* (page 21).

   Errors, such as the following, will appear:

   ```
   "[Microsoft][ODBC SQL Server Driver][SQL Server]Windows NT
   user or group '[Machine Name]\AFServers' not found. Check
   the name again."
   ```

2. Click **OK** for each error message to complete the installation.
3. In a text editor, open .`Grantbat.sql`, located in the`.\PIPC\AF\SQL` folder.
4. Change the following line:

   ```
   SET @AFSERVERSGROUP = @AFSERVERSGROUP + N'\AFServers';
   ```

   to

   ```
   SET @AFSERVERSGROUP = N'Your Domain Name\AFServers';
   ```

5. Open a command prompt window and navigate to the `..\PIPC\AF\SQL` folder.
6. Execute the following commands:

   ```
   sqlcmd -S .\sqlexpress -d PIFD -i grantbat.sql
   sqlcmd -S .\sqlexpress -d PIFD -i grants.sql
   ```

where `.\sqlexpress` is the SQL Server 2005 instance that hosts the PI AF SQL database (PIFD).

Use `osql` to run these commands if the T-SQL execution command line utility, `sqlcmd`, is not installed on your system.

Chapter 4

Manually Create or Upgrade the PI AF SQL Database

You can choose to manually install or upgrade the PI AF SQL database (PIFD) by disabling the AF SQL Script Execution feature during the PI AF server installation.

When you run the setup program, you can cancel selection of the **AF SQL Script Execution** feature so that the SQL Server scripts are not executed as part of the installation process. The SQL Server scripts and the `GO.bat` file are placed in the `..\PIPC\AF\SQL` folder. The `GO.bat` file contains the commands that execute the deployed SQL Server scripts manually.

Upon execution, the scripts create the PI AF SQL database (PIFD) and populate its tables.

The execution of the scripts must occur from an account with `sysadmin` privileges on the SQL Server instance.

This section contains the following topics:

- *Create the AFServers Local Group on the PI AF Application Service Computer* (page 37)
- *Execute the SQL Scripts to Create and Populate the PI AF SQL Database* (page 38)
- *Modify the PI AF Application Service Connect String* (page 39)
- *Configure PI AF Application Service to Point to a Different PI AF SQL Database* (page 40)

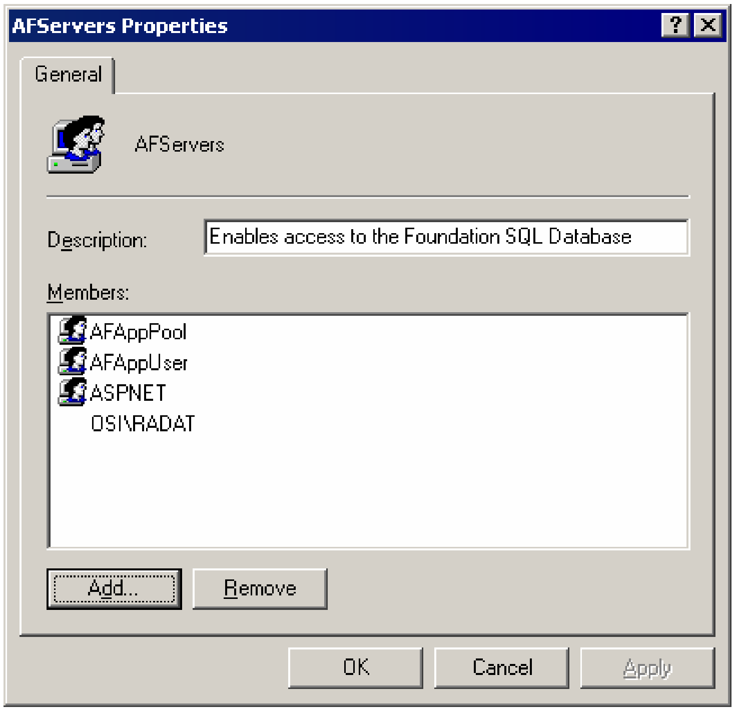
Create the AFServers Local Group on the PI AF Application Service Computer

Before you run the SQL scripts, follow these steps to enable interaction between the PI AF application service and the PI AF SQL database:

1. On the computer where you installed the PI AF SQL database, open Computer Management.
2. Create the AFServers local group if it does not already exist.
3. If the PI AF application service is not running under a domain account, add the PI AF application service computer name to the AFServers group, using this syntax:

   `DOMAIN\ComputerName`

   In this example, the domain is `OSI` and the computer name is `RADAT`.



AFServers

Description: Enables access to the Foundation SQL Database

Members:

AFAppPool
AFAppUser
ASPNET
OSI\RADAT

If the PI AF application service is running under a domain account, add the name of the domain account under which the PI AF application service is running to the AFServers group. Be sure to include domain information for the system using this format:

`DOMAIN\DomainAccount`

4. Create a SQL Server login and map it to the AFServers local user group.

Execute the SQL Scripts to Create and Populate the PI AF SQL Database

To manually create or upgrade the PI AF SQL database after installing the SQL scripts, run the SQL scripts from the SQL folder. Here is some example syntax:

- SQL Server authentication example

  The following command is an example of using SQL Server authentication on a SQL Server that includes an instance name:

  ```
  GO.bat MySQL\MyInstance PIFD MySQLLogin MySQLLoginPwd
  ```

- Windows authentication example

  The following command is an example of using Windows Authentication on a SQL Server that does not include an instance name:

  ```
  GO.bat MySQL PIFD
  ```

To execute the SQL scripts:

1. If this is an upgrade, stop the PI AF server services.

2. Open a command prompt window.

   Use **osql** to run these commands if the T-SQL command-line utility, **sqlcmd**, is not installed on your system.

3. Use the following syntax to execute the SQL scripts found in the SQL folder:

   ```
   GO.bat <SQLName>[\<SQLInstanceName>] PIFD [<SQLUserName>
   <SQLUserPassword>]
   ```

   where:

   `<SQLName>` is the name of the SQL Server into which the PI AF SQL database (PIFD) will be installed.

   `\<SQLInstanceName>` is optional, and should be included if SQL Server was installed with an instance name.

   `PIFD` is the name of the PI AF SQL database.

   `<SQLUserName>` and <`SQLUserPassword`> are optional, and should be used if SQL Server authentication is required to connect to SQL Server . If not provided, the scripts use Windows authentication to connect to SQL Server.

   The process is complete when the command line looks like:

   ```
   c:\..\PIPC\AF\SQL\PISYSOLEDB>_
   ```

Modify the PI AF Application Service Connect String

Modify the PI AF application service connect string to enable communication between the PI AF server and the PI AF SQL database.

On each PI AF application service computer, follow these steps:

1. In Windows Explorer, navigate to the `..\PIPC\AF` folder.

2. Use a text editor to open the PI AF application service configuration file, `AFService.exe.config`.

3. Enter the name of the remote SQL Server, and the named instance if applicable, in the connect string server.

   Refer to the following lines of code:

   ```
   <?xml version="1.0" encoding="utf-8"?>
   <configuration>
     <appSettings>
                   <add key="connectString" value="Persist
   Security Info=False;Integrated
   Security=SSPI;server=<SQLName>[\SQLInstance];database=PIFD;Appl
   ication Name=AF Application Server;"/>
       <add key="streamedPort" value="5459"/>
   ```

   If SQL Server is running on a cluster, it is important to use the clustered resource IP address, instead of a computer name.

   ```
   <?xml version="1.0" encoding="utf-8"?>
   <configuration>
   ```

```
  <appSettings>
                <add key="connectString" value="Persist
Security Info=False;Integrated
Security=SSPI;server=<SQLClusterName>[\SQLInstance];database=PI
FD;Application Name=AF Application Server;"/>
    <add key="streamedPort" value="5459"/>
```

If SQL Server is configured to use SQL Server mirroring, then add `Failover Partner=<SQLServerName>[\<InstanceName>]` after the `server=`, as shown in the following lines of code:

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <appSettings>
                <add key="connectString" value="Persist
Security Info=False;Integrated
Security=SSPI;server=<SQLName>[\SQLInstance];failover
partner=<SQLName>[\SQLInstance];database=PIFD;Application
Name=AF Application Server;"/>
    <add key="streamedPort" value="5459"/>
```

To enable encrypted communication, add `encrypt=Yes;` to the code. See the Microsoft SQL Native Client documentation for other options.

4. If the PI AF application service is running, stop and restart it for your changes to take effect.

Configure PI AF Application Service to Point to a Different PI AF SQL Database

If you need to direct your PI AF application service to a different PI AF SQL database, follow these instructions to specify a new SQL Server instance and to enable communications.

1. On the PI AF application service computer, edit the `AFService.exe.config` file in the `PIPC\AF` folder and replace the server information with the name of the remote SQL Server to be accessed.
2. Restart the PI AF application service computer.
3. If the PI AF application service is using the NetworkService or LocalSystem account, add the Domain\Machine Name for the remote PI AF server to the local AFServers Windows group (on the PI AF SQL database computer.)
4. If the PI AF application service has been modified to use any other account, add the account under which it is running to the local AFServers Windows group (on the PI AF SQL database computer.)
5. Restart the PI AF SQL database computer.

Chapter 5

Install PI AF Server on Microsoft Cluster Service (MSCS)

This chapter describes the special requirements and procedures needed to install or upgrade PI AF server on Microsoft Cluster Service (MSCS).

OSIsoft assumes that you are familiar with the configuration and operation of MSCS, and with the cluster administration tool for your operating system:

- Windows Server 2008: Failover Cluster Manager
- Windows Server 2003: Cluster Administrator

Note: The installation instructions in this chapter demonstrate installing the PI AF SQL database feature on a SQL Server failover cluster and the PI AF application service on a separate Windows failover cluster. As recommended, the PI AF application service is configured to run under a domain account.

This chapter contains the following topics:

- *Pre-installation Tasks for PI AF Server on MSCS* (page 41)
- *Install and Configure PI AF SQL Database on MSCS* (page 43)
- *Install and Configure the PI AF Application Service on MSCS* (page 47)
- *Upgrade PI AF on MSCS* (page 53)

Pre-installation Tasks for PI AF Server on MSCS

1. Perform the tasks in this section before you install PI AF Server for the first time.
2. Review the following Microsoft documents:
   - Windows Server 2003: *Quick Start Guide for Server Clusters* (*http://technet.microsoft.com/en-us/library/cc739757(WS.10).aspx*)
   - Windows Server 2008: *Failover Clusters* (*http://technet.microsoft.com/en-us/library/cc732488(WS.10).aspx*)
3. Install and configure:
   - SQL Server failover cluster (required for the PI AF SQL database only)
   - Microsoft Cluster Services (required for both PI AF SQL database and PI AF application service)
4. Review *Overview of PI AF Security* (page 83).

- Verify that an AFServers domain user group has been created and that it contains the correct members.

  See *Configure the AFServers Domain Group for PI AF on a Cluster* (page 42).

- Review PI AF Link Subsystem user accounts.

  See *Special Security Considerations for PI AF on MSCS* (page 43).

5. On each SQL Server cluster node, verify that the correct ports are open between each computer.

   See *PI AF Security and Firewalls* (page 97).

Configure the AFServers Domain Group for PI AF on MSCS

When you run the PI AF application service or the PI AF SQL database on a Microsoft cluster, OSIsoft recommends that you run the PI AF application service under a domain user account that belongs to the AFServers domain group. This domain user group is used to create a SQL Login account, which allows the appropriate communications between the PI AF servers and the PI AF SQL databases.

Note: You must have appropriate permissions to create or configure a Domain User group. You must be a member of the Account Operators group, the Domain Admins group, or the Enterprise Admins group in Active Directory, or you must have been delegated the appropriate authority. In addition, your computer must be running a Windows Server operating system.

To add a domain user group:

1. Open the Active Directory Users and Computers utility and connect to the domain in which the PI AF Server service account exists:
   a. Open a command window.
   b. Type `dsa.msc`
   c. Click **OK**.
2. Right-click the **Users** node in the left pane, and select **New Group**.
3. In the **Group name** box, enter a name, such as `AFServers`.
4. Set the **Group Scope** to **Global**.
5. Set the **Group Type** to **Security**.
6. Click **OK** to create the domain group.
7. Right-click the newly created group (such as `AFServers`) and select **Properties**.
   a. Select the **Members** tab and click **Add**.
   b. Click **Object Types**.
   c. Select **Computers** and leave the previously selected **Object Types** selected.
   d. Click **OK**.

The **Select Users, Contacts, Computers, or Groups** dialog box appears.

8. In the **Enter the object names to select** text box, enter the name of the domain user under which the `AFServer` service runs.

   If the PI AF SQL database is on a SQL Server in a cluster, enter the computer names of each of the PI AF Servers included in the cluster.

9. Click **OK**.
10. Close the Active Directory Users and Computers utility.
11. On each computer added to the domain group:
    a. Reboot the computer for membership to take immediate effect.
    b. Open a command window.
    c. Verify membership. At the command prompt, type: `gpresult /z /`.

Special Considerations for PI AF Security on MSCS

When the PI AF server is clustered, there are extra steps required to allow AF Link to PI to function correctly.

A domain group must be created and configured.

If the PI AF Link Subsystem service is running under NT AUTHORITY\Network Service, then only the computer names of both nodes of the PI cluster must be added to the new domain group.

If the PI Server and PI AF server are on the same cluster, PI AF Link Subsystem must run under a domain account. When PI AF Link Subsystem runs under a domain account, this domain account must be added to the domain group created to support AF Link to PI. The password on this domain account should be set to NOT expire.

In both cases listed above, you must allow read/write access to the PI Server element under PI AF to the new domain group. Additionally, the AFGroupSID property under MDB->%OSI->MDBAFMigrationData needs to point to the SID of the newly created domain group. You can get the SID of this new domain group by using the Mappings & Trusts tool in PI SMT.

Install and Configure PI AF SQL Database on MSCS

Begin a new installation of PI AF Server on MSCS by installing and configuring the PI AF SQL database.

1. *Install the PI AF SQL Database on Each MSCS Node* (page 44)
2. *Execute the SQL Scripts on MSCS* (page 45)
3. *Configure Logins and User Groups on MSCS* (page 45)
4. *Verify Operation of the SQL Server Service on MSCS* (page 47)

After you complete this procedure, install and configure the PI AF application service on MSCS.

Install the PI AF SQL Database on Each MSCS Node

Begin the process of installing PI AF Server by installing the PI AF SQL database on each node of the cluster.

Before you begin, perform the *Pre-installation Tasks for PI AF Server on MSCS* (page 41).

1. Go to the directory where you downloaded the PI AF install kit.
2. Double-click the executable (`.exe`) file.
3. On the **Self-Extracting Executable** dialog box, click **Browse,** select the directory where you want to extract the files, and click **OK**.
4. When the installation files have been extracted, click **OK**.

   The **Welcome** page appears.
5. Click **Next**.
6. Accept the default **Full Name** and **Organization** values, or change these values. Click **Next**.
7. Accept the default destination folder, or click **Browse** to locate and select a different folder. Click **Next**.

   The **Select Features** dialog box appears.
8. Disable the **AF Application Service** and the **AF SQL Script Execution** features. The PI AF Server installation does not support the AF SQL Script Execution feature when installing to a SQL Server Cluster; the SQL Scripts must be manually executed.
9. Click **Next**.
10. Enter the SQL cluster name, and SQL instance (if applicable), in the following format: `<SQLClusterName>[\<SQLClusterInstanceName>]`.
11. Clear the **Validate connection to the remote SQL Server** check box.

    You do not need to validate the connection to the remote SQL Server at this time because you will be executing the SQL scripts.
12. Click **Next**.

    The **Remote Application Server Connection** dialog box appears.
13. Do not enter a value. Click **Next** and continue through the rest of the installation program.

    Note: For installations prior to PI AF server 2.4, you may see an installation error on the PI SQL for AF Server displayed in the final installation wizard. When installing the AF Server and AF SQL database on separate computers, this is an acceptable error and can be ignored.

14. Open **Computer Management** and delete the AFServers local group. You do not need this local group because you will be using the domain user group that you previously configured.

Execute the SQL Scripts on MSCS

After you have installed PI AF SQL database on each node of the SQL Server cluster, you need to execute the AF SQL scripts that create and populate the tables of the PI AF SQL database (PIFD).

The `GO.bat` file contains the commands that execute the deployed SQL Server scripts. The scripts and the `GO.bat` file are located in the `..\PIPC\AF\SQL` folder.

Note: You must execute the scripts from an account with `sysadmin` privileges on the SQL Server instance.

1. On the active SQL Server node only, open a command prompt window.
2. Change the directory to the `SQL` folder in the `\PIPC\AF` folder (for example: `cd c:\program files(x86)\PIPC\AF\SQL`).
3. Use the following syntax to execute the SQL scripts found in the SQL folder:

   ```
   GO.bat <SQLClusterName>[\<SQLClusterInstanceName>] PIFD
   [<SQLUserName> <SQLUserPassword>]
   ```

   where:

   `<SQLClusterName>` is the name of the SQL Server cluster where the PI AF SQL database (PIFD) will be installed.

   `\<SQLClusterInstanceName>` is optional, and should be included if the SQL Server cluster was installed using a named instance.

   `PIFD` is the name of the PI AF SQL database.

   `<SQLUserName>` and <`SQLUserPassword`> are only needed if mixed mode authentication is required to connect to the SQL Server cluster. To use Windows authentication, omit these to use Windows authentication. Typically, mixed mode authentication is required when the PI AF SQL database and PI AF application service are on different, non-trusted domains.

   When the process is complete, the command line looks like the following:

   ```
   c:\..\PIPC\AF\SQL\PISYSOLEDB>_
   ```

Configure Logins and User Groups

To allow appropriate communication between AF SQL database and the AF application service, you need to create an SQL login that is mapped to the domain user account AFServers and to delete any local logins and users that were created when you installed AF SQL database.

1. *Create and Map the SQL Server Login* (page 46).
2. *Delete Local Logins and Users as Needed* (page 46).

Create and Map the SQL Server Login

An SQL login that is mapped to the domain user account AFServers is required for communication between PI AF SQL database and PI AF application service.

Before starting this procedure, ensure that you have configured the AFServers domain group for PI AF. See *Configure the AFServers domain group for PI AF on MSCS* (page 42).

1. Open Microsoft SQL Server Management Studio, and connect to the SQL Server cluster instance that stores the PI AF SQL database (PIFD).
2. Under the SQL Server cluster instance, expand **Security** > **Logins**.
   a. Right-click the **Logins** folder and select **New Login:**
   b. Enter the domain user group including the domain name (`YourDomain\YourAFDomainGroup`) in the **Login name** box.
3. If it is necessary to manually include the **Groups** object type before your entry is accepted as valid, follow these steps:
   a. To include the groups object type, click **Search**.
   b. In the **Select User Group** dialog box, click **Object Types**.
   c. In the **Object Types** dialog box, select **Groups.**
   d. Click **OK** to return to the **Select User Group** dialog box.
   e. Enter the domain user group, including the domain name (`YourDomain\YourAFDomainGroup`), in the **Enter the object name to select** box.
   f. Click **OK** to return to the **General** page.
4. Select the **Windows authentication** option.
5. In **Default database**, select **PIFD**.
6. Select the **User Mapping** page.
7. Under **Users mapped to this login**, select the **Map** check box for **PIFD** database row.
8. Ensure that the **User** column for the **PIFD** row is set to the domain user group `YourDomain\YourAFDomainGroup.`
9. Under **Database role membership for: PIFD**, select the **db_AFServer** check box.
10. The **public** role should be selected by default; if it is not, select its check box.
11. Click **OK** to save the new SQL Server login.

Delete Local Logins and Users as Needed

1. The SQL scripts that create and populate the PI AF SQL database also create local logins and users. You do not need these local accounts, so you should delete them.
2. Open Microsoft SQL Server Management Studio, and connect to the SQL Server cluster instance that stores the PI AF SQL database (PIFD).
3. Expand **Security** > **Logins**.

4. Check with your SQL Server administrator to ensure that the local `NT AUTHORITY\NetworkService` login is not required for any other reason. If the login is not required, delete it.
5. Delete the following local SQL Server login:
   - *LocalMachineName*`\AFServers`
6. Expand **Databases** > **PIFD** > **Security** > **Users**.
7. Delete the following SQL Server users, if they exist:
   - `PIFD AFServers`
   - `NT AUTHORITY\NetworkService`

   Deleting a user automatically deletes the corresponding schema, if one exists.

Verify Operation of the SQL Server Service

After you have installed and configured the PI AF SQL database on each cluster node, you need to verify that the SQL Server service can run on all nodes of the cluster.

Before you begin, use the cluster administration tool for your operating system to bring the SQL Server service online.

1. Open the **Services** window (**Start > Administrative Tools > Services**) on each node in the cluster.
2. Scroll to the **SQL Server** service.
3. All nodes should show the service's **Startup Type** as **Manual**. Only one node should show the service as **Started**.
4. Use the cluster administration tool for your operating system to move the service to another node:
   - Windows Server 2008: In the Failover Cluster Manager, right-click the service and select **Move this service or application to another node > Move to node** <*name of non-active node in Microsoft Cluster*>.
   - Windows Server 2003: In Microsoft Cluster Administrator, right-click the cluster group for the service, and click **Move Group.**
5. Verify that the service is running on the new owner node and shows the service's **Startup Type** as **Manual**. The service should not be running on the other nodes.
6. Repeat the previous steps until you have verified that all nodes in the cluster can take control of the service.

Install and Configure the PI AF Application Service

After you have installed and verified PI AF SQL database on MSCS, install and configure the PI AF application service.

1. *Install the PI AF Application Service on Each MSCS Node* (page 48).

2. *Configure the PI AF Application Service* (page 49).
3. *Verify Operation of the PI AF Application Service* (page 52).
4. (PI AF collectives only) *Configure Certificates for PI AF High Availability* (page 53).

Install the PI AF Application Service on Each MSCS node

Before you begin, perform the *Pre-installation Tasks for PI AF Server on MSCS* (page 41).

1. Go to the directory where you downloaded the PI AF install kit.
2. Double-click the executable (`.exe`) file.
3. On the **Self-Extracting Executable** dialog box, click **Browse,** select the directory where you want to extract the files, and click **OK**.
4. When the installation files have been extracted, click **OK**.

   The **Welcome** page appears.
5. Click **Next**.
6. Accept the default **Full Name** and **Organization** values, or change these values. Click **Next**.
7. Accept the default destination folder, or click **Browse** to locate and select a different folder. Click **Next**.

   The **Select Features** dialog box appears.
8. Click the **AF SQL Database** feature and choose **Entire feature will be unavailable**. You will only be installing the **AF Application Service** feature.
9. Click **Next**.
10. On the **SQL Server Connection** page, enter the SQL cluster name, and SQL instance (if applicable), in the format:

    ```
    <SQLClusterName>[\<SQLClusterInstanceName>]
    ```

    where:
    `<SQLClusterName>` is the name of the Microsoft SQL Server cluster into which the PI AF SQL database (PIFD) will be installed.

    `[\<SQLClusterInstanceName>]` is optional, and should be included if the Microsoft SQL cluster was installed with an instance name.

    If you cannot validate the SQL Server connection, you can skip the validation step by clearing the **Validate connection to the SQL Server** check box.
11. **Click Next**.
12. Click **Install** and continue through the rest of the installation kit. Click **Finish** when PI AF server has been successfully installed.
13. Click **Close**.
14. Complete the procedure in *Remove the NetworkService Account's Access to the PI AF SQL Database* (page 86).

The PI AF application service is installed using the local NetworkService account, but needs to be run under a domain account to provide the most secure method for protecting your PI AF server.

15. Ensure the PI AF application service is shut down.

Configure the PI AF Application Service

After you have installed the PI AF application service on all cluster nodes, you need to add the service as a cluster resource, create dependencies, and bring the service online. Use the appropriate procedure for your operating system.

- *Configure the PI AF application service on Windows Server 2008* (page 49).
- *Configure the PI AF application service on Windows Server 2003* (page 50).

Configure the PI AF Application Service on Windows Server 2008

After you install the PI AF application service on each node of the cluster, you need to configure the service and bring it online.

Begin with the PI AF application service installed on each node of the cluster.

1. Using Failover Cluster Manager:
   a. Right-click **Services and applications.**
   b. Select **More Actions.**
   c. Select **Create Empty Service or Application**.

      A new entry is added with the name of **New service or application**.
   d. Right-click the newly created **New service or application** and select **Rename**.
   e. Enter a name for your PI AF application service cluster, such as AF SERVER.
   f. Right-click the newly renamed AF SERVER.
   g. Select **Add a resource.**
   h. Select **Client Access Point**.
2. In the **New Resource Wizard**:
   a. Specify the name and IP address of the PI AF application service cluster.

      A new DNS entry will be created using the Name and IP Address. The Name and/or IP address will be used by PI AF clients to connect to the PI AF application service cluster.
   b. Enter the **Network Name** of the PI AF application service cluster in the **Name** box, such as AFServerCluster.
   c. Enter the appropriate static IP address in the row that represents the Public network connection in the cluster.
   d. Remove the check mark for any other networks listed in the box. Ensure you do not already have an Active Directory entry for the Network Name you entered.

e. Click **Next**. The **Confirmation** page appears.

f. If the **Network Name** and/or **IP Address** are not correct, click **Previous** and make the required corrections. Otherwise, click **Next** to create the new DNS entry.

The **Summary** page displays the creation and configuration results for the new resource.

g. If there are errors displayed, click **View Report** to review the results and troubleshoot the errors. Otherwise, click **Finish**.

3. Right-click the new AF SERVER.

a. Select **Add a resource.**

b. Select **Generic Service**. The **New Resource Wizard** dialog appears.

4. In the **New Resource Wizard:**

a. Select the PI AF application service to be added to the AF SERVER cluster.

b. Scroll through the list of services and select **PI AF Server 2.x.**

c. Click **Next**. The **Confirmation** page appears.

d. If the **Service** and/or **Parameters** are not correct, click **Previous** and make the required corrections. Otherwise, click **Next**.

The **Summary** page displays the creation and configuration results for the new resource.

e. If errors appear, click **View Report** to review the results and troubleshoot the errors. Otherwise, click **Finish**.

5. With the new AF SERVER selected:

a. Right-click the newly created resource **PI AF Server 2.x**.

b. Select **Properties**.

6. In the **PI AF Server 2.x Properties** dialog:

a. Click the **Dependencies** tab.

b. In the **Resource** column, click the **Click here** button to add a dependency.

c. From the drop-down list, select the **Name** of the PI AF application service cluster previously defined.

d. Click **OK**.

7. If the AF SERVER is not online, right-click it and select **Bring this service or application online**.

The status of each of the AF SERVER’s resources changes from **Offline** to **Online**.

8. *Verify operation of the PI AF application service* (page 52).

Configure the PI AF Application Service on Windows Server 2003

After you install the PI AF application service on each node of the cluster, you need to configure the service and bring it online.

Begin with the PI AF application service installed on each node of the cluster.

1. Using the Cluster Administrator, right-click **Groups** and select **Configure Application**.
2. In the **Cluster Application Wizard:**
    a. Click **Next**.
    b. On the **Select or Create a Virtual Server** page select the **Create a new virtual server** option and click **Next**.
    c. On the **Resource Group for the Virtual Server** page, select the **Create a new resource group** option and click **Next**.
    d. On the **Resource Group Name** page, enter a **Name** for the Resource Group, such as AFCluster Group.
    e. Optionally, enter a **Description**. Click **Next**.
    f. On the **Virtual Server Access Information** page, In the **Network name** box, the **Resource Group** name is displayed by default (any spaces have been removed). A new DNS entry will be created using the **Network name** and **IP address values**. The Network name and/or IP address will be used by AF clients to connect to the PI AF application service cluster. You can leave the default **Network name** or enter a different value. Enter the **IP address** to be associated with the **Network name**.
    g. Click **Next**.
3. The **Advanced Properties for the New Virtual Server** page appears:

    It is not necessary to configure advanced properties for any of the **Categories** provided. However, if you know you need to change the default properties for any of the listed categories:

    a. Select an item in the **Categories** list and click **Advanced Properties**.
    b. Make any changes and click **OK.**
    c. Click **Next**.
4. On the **Create Application Cluster Resource** page, keep the default option **Yes, create a cluster resource for my application now** selected, and click **Next**.
5. On the **Application Resource Type** page:
    a. Select **Generic Service** in the **Resource type** list.
    b. Click **Next**.
6. On the **Application Resource Name and Description** page:
    a. Enter a **Name** for your AF Service resource, such as `AF SERVER`.
    b. Optionally. enter a **Description**.
    c. It is not necessary to configure **Advanced Properties.** However, if you know you need to change the default properties, click **Advanced Properties**.
    d. Make any changes and click **OK.**
    e. On the **Application Resource Name and Description** page, click **Next**.
7. On the **Generic Service Parameters** page:

   a. Enter `AFService` in the **Service name** box. Start parameters are not required.

   b. Click **Next**.

8. On the **Registry Replication** page, click **Next**.

   It is not necessary to replicate these registry keys.

9. On the **Completing the Cluster Application Wizard** page, click **Finish** to return to the Cluster Administrator.

10. Select your new AFCluster group in the **Groups** folder.

    Three resources are included: IP Address, Network Name, and Generic Service.

11. Right-click the new AFCluster group and select **Bring Online**.

    The **State** of the AFCluster group members changes from **Offline** to **Online Pending** to **Online**.

12. *Verify operation of the PI AF application service* (page 52).

Verify Operation of the PI AF Application Service After Installation

After you have installed and configured the PI AF application service, you need to verify that the service can run on all nodes of the cluster.

Before you begin, use the cluster administration tool for your operating system to bring the AF Server service online.

1. Open the **Services** window (**Start > Administrative Tools > Services**) on each node in the cluster.

2. Scroll to the **AF Server** service.

3. All nodes should show the service's **Startup Type** as **Manual**. Only one node should show the service as **Started**.

4. Use the cluster administration tool for your operating system to move the service to another node:

   - Windows Server 2008: In the Failover Cluster Manager, right-click the service and select **Move this service or application to another node > Move to node** <*name of non-active node in Microsoft Cluster*>.
   - Windows Server 2003: In Microsoft Cluster Administrator, right-click the cluster group for the service, and click **Move Group.**

5. Verify that the service is running on the new owner node and shows the service's **Startup Type** as **Manual**. The service should not be running on the other nodes.

6. Repeat the previous steps until you have verified that all nodes in the cluster can take control of the service.

7. If the clustered PI AF application service will be part of a PI AF collective, see *Configure Certificates for PI AF High Availability* (page 53).

8. For MSCS clusters on Windows Server 2008, you might want to change the default number of failovers. See *Modify the Default Number of Failovers on Windows Server 2008.* (page 53)

Configure Certificates for PI AF High Availability

If this AF Server will be a member in an AF collective, each computer in the Microsoft cluster must use the same Windows certificate that supports communication with the clustered PI AF server service.

Before you begin, ensure that the PI AF application service has been installed and verified on each cluster that you want to include in the collective.

1. Copy the AF Server certificate, named `AFServer.pfx` and located in the Documents and `Settings\All Users\Application Data\OSIsoft\AF` directory, from the active node in the cluster to the same location on other node(s) in the cluster.
2. Use the cluster administration tool for your operating system to restart the PI AF application service on each node of the cluster.
   - Windows Server 2008: In the Failover Cluster Manager, right-click the service and select **Move this service or application to another node > Move to node** *<name of non-active node in Microsoft Cluster>.*
   - Windows Server 2003: In Microsoft Cluster Administrator, right-click the cluster group for the service, and click **Move Group.**

Modify the Default Number of Failovers on Windows Server 2008

In Windows Server 2008, the default number of times a group in a two-node cluster is allowed to fail over set to one time in a period of six hours. You may want to change this default. (In Windows 2000 and Windows 2003, the default was ten times in six hours.)

1. In Failover Cluster Manager, right-click the service and select **Properties**.
2. Select the **Failover** tab and modify the number.

Upgrade PI AF on MSCS

This section describes the special requirements and procedures needed to upgrade PI AF SQL database and PI AF application service on Microsoft Cluster Service (MSCS).

Note: These instructions demonstrate upgrading the PI AF SQL Database feature on a SQL Server cluster and the PI AF application service on a separate cluster. As recommended, the PI AF application service is configured to run under a domain account.

- *Upgrade the PI AF SQL Database on MSCS* (page 54).
- *Upgrade the PI AF Application Service on MSCS* (page 56).

Upgrade the PI AF SQL Database on MSCS

Begin the upgrade of PI AF Server on MSCS by upgrading the PI AF SQL database.

- *Take the PI AF Application Service Resource Offline on the Active Cluster Node* (page 54).
- *Run the PI AF Setup program on the Non-Active SQL Server Cluster Node* (page 54).
- *Run the PI AF Setup program on the Active Node of the SQL Server Cluster* (page 55).

Take the PI AF Application Service Resource Offline on the Active Cluster Node

To upgrade PI AF SQL database on MSCS, you must shut down the PI AF application service to prevent any changes to the database during upgrade.

1. Start the cluster administration tool for your operating system:
   - Windows 2008: Failover Cluster Manager.
   - Windows 2003: Cluster Administrator.
2. Pause the non-active nodes in the cluster.
3. Take the PI AF Server resource offline.

Upgrade PI AF SQL Database on the Non-active Nodes of the SQL Server Cluster

To upgrade PI AF SQL database on MSCS, you begin by running the setup program on the non-active nodes of the SQL Server cluster.

Before you begin, ensure that the PI AF application service resource is offline.

1. Go to the directory where you downloaded the PI AF install kit.
2. Double-click the executable (`.exe`) file.
3. On the **Self-Extracting Executable** dialog box, click **Browse,** select the directory where you want to extract the files, and click **OK**.
4. When the installation files have been extracted, click **OK**.

   The **Welcome** page appears.
5. Click **OK** and click **Next** to continue with the installation.
6. Accept the default **Full Name** and **Organization** values, or change these values to meet your needs. Click **Next.**

   The **Destination Folder** dialog appears.
7. Accept the default **Destination Folder**. Click **Next**.

   The **PI AF Server 2010 Setup** dialog box appears.
8. Click **Install** to continue through the upgrade installation.

You are now ready to *upgrade the PI AF application service on the active cluster node* (page 55).

Upgrade PI AF SQL Database on the Active Node of the SQL Server Cluster

Upgrade PI AF SQL database on the active node of the SQL Server cluster on MSCS.

Before you begin, ensure that the PI AF SQL database has been upgraded on all non-active cluster nodes and that the PI AF application service resource is offline.

1. Go to the directory where you downloaded the PI AF install kit.
2. Double-click the executable (`.exe`) file.
3. On the **Self-Extracting Executable** dialog box, click **Browse,** select the directory where you want to extract the files, and click **OK**.
4. When the installation files have been extracted, click **OK**.
5. Click **Next** on the **Welcome to the AF Server Installation** dialog box, and complete the remaining tasks of the setup program as follows:
   a. Accept the default **Full Name** and **Organization** values, or change these values to meet your needs. Click **Next**.
   b. Accept the default **Destination Folder**. Click **Next**.
   c. Review the **Remote PIFD SQL Database Warning** and select the **Warning Acknowledged** check box. Click **Next**.

      The **PI AF Server 2010 Setup** dialog box appears.
   d. Click **Install** and continue through the upgrade installation.
6. Open **Computer Management** and delete the AFServers local group, if it exists.
7. Complete the following steps to execute the SQL scripts:
   a. Open a DOS Command window.
   b. In the DOS command window, navigate to the folder where the `GO.bat` file is located:

      ```
      ..\PIPC\AF\SQL
      ```
   c. Use the following syntax to execute the SQL scripts found in the SQL folder:

      ```
      GO.bat <SQLClusterName>[\<SQLClusterInstanceName>] PIFD
      [<SQLUserName> <SQLUserPassword>]
      ```

      where:

      `<SQLClusterName>` is the name of the Microsoft SQL Server Cluster where the PI AF SQL database (PIFD) will be installed.

      `\<SQLClusterInstanceName>` is optional, and should be included if the Microsoft SQL Cluster was installed with an instance name.

      `PIFD` is the name of the AF SQL Database.

The `<SQLUserName>` and `<SQLUserPassword>` are optional, and should be used solely if SQL Server Authentication is required to connect to the SQL Server cluster. When you omit these parameters, the scripts will use Windows Authentication to connect to the SQL Server Cluster.

The process is complete when the command line looks like the following:

```
c:\..\PIPC\AF\SQL\PISYSOLEDB>_
```

8. Check with your SQL Server administrator to ensure that the local `NT AUTHORITY\NetworkService` login is not required for any other reason. If the login is not required, delete it.
9. Delete the following local SQL Server login:
   - *LocalMachineName*`\AFServers`
10. In Microsoft SQL Server Management Studio, expand **Databases** > **PIFD** > **Security** > **Users**.
11. Delete the following SQL Server users, if they exist:
    - `PIFD AFServers`
    - `NT AUTHORITY\NetworkService`
12. In Microsoft SQL Server Management Studio, Select **SQLClusterInstance** > **Databases** > **PIFD** > **Security** > **Users**.
13. Delete the `PIFD AFServers` and `NT AUTHORITY\Network Service` users.

    Deleting the user should automatically delete the corresponding schema, if one exists.

After upgrading the PI AF SQL database on all cluster nodes, you are ready to *upgrade the PI Application service* (page 56).

Upgrade the PI AF Application Service on MSCS

After you have upgraded the PI AF SQL database, upgrade the PI AF application service.

- *Upgrade the PI AF Application Service on the Active Node of the Cluster* (page 56).
- *Upgrade the PI AF Application Service on the Non-active Nodes of the Cluster* (page 57).
- *Verify Operation of the PI AF Application Service After Upgrade* (page 58).

Upgrade the PI AF Application Service on the Active Node of the Cluster

To upgrade PI AF application service on MSCS, begin by running the setup program on the active node of the cluster where the service is located.

Before you begin, ensure that the PI AF SQL database has been upgraded on all cluster nodes and that the PI AF application service resource is offline.

1. Log on to the active node of the cluster where the PI AF application service is installed.
2. Go to the directory where you downloaded the PI AF install kit.
3. Double-click the executable (`.exe`) file.

4. On the **Self-Extracting Executable** dialog box, click **Browse,** select the directory where you want to extract the files, and click **OK**.
5. When the installation files have been extracted, click **OK**.

   The **Welcome** page appears.
6. Click **OK**.
7. Click **Next**.
8. Accept the default **Full Name** and **Organization** values, or change these values to meet your needs. Click **Next.**
9. Accept the default **Destination Folder** and click **Next**.
10. Click **Install** and continue through the rest of the setup program.
11. Click **Finish**.
12. Click **Close**.
13. Ensure the **PI AF Server 2.x Service** is still configured to run under the correct domain account.

Upgrade the PI AF Application Service on the Non-active Nodes of the Cluster

After you have upgraded the PI AF application service on the active cluster node, upgrade it on the non-active cluster nodes.

Before you begin, ensure that the PI AF application service resource is offline.

1. Log onto the non-active PI AF application service cluster node.
2. Go to the directory where you downloaded the PI AF install kit.
3. Double-click the executable (`.exe`) file.
4. On the **Self-Extracting Executable** dialog box, click **Browse,** select the directory where you want to extract the files, and click **OK**.
5. When the installation files have been extracted, click **OK**.

   The **Welcome** page appears.
6. Click **OK**.
7. Click **Next** and complete the remaining tasks of the setup program as follows:
   a. Accept the default **Full Name** and **Organization** values, or change these values to meet your needs. Click **Next.**
   b. Accept the default **Destination Folder.** Click **Next**.
   c. Click **Install** and continue through the rest of the setup program.
   d. Click **Finish.**
   e. Click **Close**.
8. Ensure the **PI AF Server 2.x** service is still configured to run under the correct domain account.

9. For MSCS clusters on Windows Server 2008, you might want to change the default number of failovers. See *Modify the Default Number of Failovers on Windows Server 2008.* (page 53)

Verify Operation of the PI AF Application Service After Upgrade

After you have upgraded the PI AF application service, you need to start the service, verify that the service can run on all nodes of the cluster, and verify that client applications can connect.

1. Log on to the active node of the cluster on which the PI AF application service is installed.
2. Resume the non-active node(s) in the cluster.
3. Bring the PI AF Server resource online.
4. Open the **Services** window (**Start > Administrative Tools > Services**) on each node in the cluster and ensure that the **Startup Type** is **Manual** for the **PI AF Server** service. Only one node should show the service as **Started**.
5. Use the cluster administration tool for your operating system to move the service to another node:
   - Windows Server 2008: In the Failover Cluster Manager, right-click the service and select **Move this service or application to another node > Move to node** <*name of non-active node in Microsoft Cluster*>.
   - Windows Server 2003: In Microsoft Cluster Administrator, right-click the cluster group for the service, and click **Move Group.**
6. Verify that the PI AF Server service is running on the new owner node and is *not* running on the other node(s).
7. Verify a client application can connect using the AF Cluster’s assigned **Network Name**.
8. Repeat the previous three steps until you have verified that all nodes in the cluster can take control of the PI AF Server service and verified that a client application can connect.

The upgrade of PI AF Server on MSCS is now complete.

Chapter 6

Configure Silent PI AF Installations

The bundled PI AF server installations extract several installation modules. The `setup.ini` configuration file specifies the components of the installation process, their order, and the arguments used to launch them. Modify this file to specify different command-line arguments to different stages of the setup. This may be useful for situations where the environment is well controlled and the options are known in advance, such as an embedded installation.

The PI AF Server bundle also includes a `silent.ini` file that contains modifications to `setup.ini` that are typically needed to run a silent installation. You can augment these arguments by adding any of the options described below.

For PI SDK installation and arguments, see the PI SDK user's manual.

Note: You must run command-line examples from an Administrator command prompt when running on Windows 7 or other recent operating systems when running as a normal user.

This chapter contains the following topics:

- *Configure Silent Installation for PI AF Server* (page 59)
- *Configure Silent Installation for PI AF SDK and PI System Explorer* (page 62)

Configure Silent Installation for PI AF Server

This section contains the following topics:

- *Command Line Arguments for PI AF Server Installation* (page 59)
- *Features Specified by ADDLOCAL Argument for PI AF Server Installation* (page 60)
- *Install PI AF Server Syntax Examples* (page 60)

Command Line Arguments for PI AF Server Installation

Argument	Description
`ADDLOCAL`	Specifies features to install. See *Features Specified by ADDLOCAL Argument for PI AF Server Installation* (page 60).
`ALLUSERS`	Specifies the per-computer or per-user installation context. Use a value of `1` for silent installations.

Argument	Description
`REBOOT`	Restarts the computer. Use a value of `Suppress` for silent installations.
`FDSQLDBSERVER`	Specifies the SQL Server instance.
`FDSQLDBNAME`	Specifies the SQL Server database.
`FDSQLDBVALIDATE`	Specifies that the SQL Server connection is validated if the SQL Server Script Execution feature is not selected. A value of “`0`” will bypass the connection validation. If not specified, then the SQL Server connection will be validated.
`FD_REMOTEAPPS`	Specifies the domain\machine name or domain\account name of a remote PI AF application service. This option is only used for initial SQL Server-only installations

Features Specified by ADDLOCAL Argument for PI AF Server Installation

This table lists the features specified by the `ADDLOCAL` argument. Feature names are case-sensitive. `ADDLOCAL` values consist of a comma-separated list and cannot contain any spaces. To install all features, use `ADDLOCAL=ALL`.

Internal Feature Name / Name Used in Command Line	User-Friendly Feature Name	Description
`ALL`	N/A	All features are installed
`FD_AppsServer`	PI AF Application Service	This feature installs the PI AF Server 2.x application service.
`FD_SQLServer`	PI AF SQL Database	This feature installs the PI AF SQL Server scripts to the `AF\SQL` folder.
`FD_SQLScriptExecution`	PI AF SQL Script Execution	This feature handles the execution of the PI AF SQL Server scripts during the installation process. If this feature is included for installation, the SQL Server scripts are executed. If it is not included, the scripts are not executed. If you include this feature in a silent installation, you must also use the `FD_SQLServer` feature.

Install PI AF Server Syntax Examples

For a silent PI AF Server installation use the syntax shown in one of the following examples. Note that the `/i` argument specifies an installation, and the `/qn` argument specifies "quiet mode" and suppresses dialog boxes and prompts.

This section contains the following topics:

- *Install All PI AF Server Features* (page 61)
- *Install the PI AF Application Service* (page 61)
- *Install PI AF SQL Database Scripts Without Executing the Scripts* (page 61)

- *Install and Execute PI AF SQL Database Scripts* (page 61)
- *Upgrade a Previous PI AF Server Installation* (page 62)
- *Install and Execute PI SQL for AF* (page 62)

Install All PI AF Server Features

Either of these commands install all PI AF server features:

```
msiexec.exe /i AFServer_<Version #>.msi REBOOT=Suppress
ADDLOCAL=ALL FDSQLDBSERVER=.\sqlexpress FDSQLDBNAME=PIFD
ALLUSERS=1 /qn

msiexec.exe /i AFServer_<Version #>.msi REBOOT=Suppress
FDSQLDBSERVER=.\sqlexpress FDSQLDBNAME=PIFD ALLUSERS=1 /qn
```

Note: If the `ADDLOCAL` property is not defined on the command line as shown above, the default is the value of `ALL`.

Install the PI AF Application Service

To install only the PI AF application service, use this command:

```
msiexec.exe /i AFServer_<Version #>.msi REBOOT=Suppress ADDLOCAL=
FD_AppsServer FDSQLDBSERVER=machine.\sqlexpress FDSQLDBNAME=PIFD
ALLUSERS=1 /qn
```

Install PI AF SQL Database Scripts Without Executing the Scripts

To install only the PI AF SQL database scripts (without executing):

```
msiexec.exe /i AFServer_<Version #>.msi REBOOT=Suppress ADDLOCAL=
FD_SQLServer FDSQLDBSERVER=.\sqlexpress FDSQLDBNAME=PIFD
FD_REMOTEAPPS=domain\machine ALLUSERS=1 /qn
```

Note: The scripts will need to be manually executed after installation.

Install and Execute PI AF SQL Database Scripts

To install only the PI AF SQL database and execute the SQL scripts, run this command:

```
msiexec.exe /i AFServer_<Version #>.msi REBOOT=Suppress ADDLOCAL=
FD_SQLServer, FD_SQLScriptExecution FDSQLDBSERVER=.\sqlexpress
FDSQLDBNAME=PIFD FD_REMOTEAPPS=domain\machine ALLUSERS=1 /qn
```

Note: To include the `FD_SQLScriptExecution` feature the `FD_SQLServer` feature must also be included.

Upgrade a Previous PI AF Server Installation

When upgrading PI AF server, it is not necessary to specify the arguments or features.

To upgrade any previously installation of PI AF server, run this command:

```
msiexec.exe /i AFServer_<Version #>.msi REBOOT=Suppress ALLUSERS=1
/qn
```

Install and Execute PI SQL for AF

Run the following command. Specify the appropriate msi (either x64 or x86).

```
msiexec.exe /i afsqlservice-x(64/86).msi /qn
```

Configure Silent Installation for PI AF Client

This section contains the following topics:

- *Command Line Arguments for PI AF Client Installation* (page 62)
- *Features Specified by ADDLOCAL Argument for PI AF Client Installation* (page 63)
- *Install PI AF Client Syntax Examples* (page 63)

Command Line Arguments for Installation of PI AF Client

Argument	Description
`ADDLOCAL`	Specifies features to install. See *Features Specified by ADDLOCAL Argument for PI AF Client Installation* (page 63).
`ALLUSERS`	Specifies the per-computer or per-user installation context. Use a value of `1` for silent installations.
`REBOOT`	Restarts the computer. Use a value of `Suppress` for silent installations.
`AF_SERVER`	Specifies the default PI AF server name (the computer where the PI AF application service resides) for the client. If a value is not defined by the user and the PI AF application service is not resident on the target installation computer, the default PI AF server name is not set during the installation. If not set, the default PI AF server name can be set manually after the installation has completed. If a value is not defined and the PI AF application service has already been installed on the same computer, then the current computer will be set as the default PI AF server. The AF_SERVER argument is not used during an upgrade.
`ONLYSHOWSERVER`	0: Default. No change to the install. 1: Only displays the dialog to enter the Server Name for AF Client and the progress dialog.
`AFSDKONLY`	0: Default. No change to the install. 1: On a clean install, installs AFSDK only. If it is an upgrade, it will upgrade normally.

Features Specified by ADDLOCAL Argument for PI AF Client Installation

This table lists the features specified by the `ADDLOCAL` argument. Feature names used with the `ADDLOCAL` argument are case-sensitive. `ADDLOCAL` values consist of a comma-separated list and cannot contain any spaces. To install all features, use `ADDLOCAL=ALL`.

Internal Name / Name Used in Command Line	External Feature Name	Description
`ALL`	N/A	All features are installed.
`FD_AFSDK`	PI AF SDK	This feature installs PI AF Client core files: the PI AF SDK and the AF Common Controls. This is a required feature.
`FD_AFExplorer`	PI System Explorer	This feature installs PI System Explorer, which provides a user interface for displaying the hierarchical structure of the PI AF servers and other PI AF entities. The AFImport, AFExport, and RegPlugIn utilities are also included.
`FD_AFBuilder`	PI AF Builder	The PI AF Builder add-in to Excel.
`FD_AFDocs`	Documentation	This feature installs the documentation, which is a set of PI AF `.CHM` help files.

Note: PI AF SDK is a required feature. It must be specified if individual features are to be included.

Install PI AF Client Syntax Examples

To install PI AF SDK or PI System Explorer silently, use the syntax shown in one of the following examples. Note that the `/i` argument specifies an installation, and the `/qn` argument specifies "quiet mode" and suppresses dialog boxes and prompts.

This topic contains the following topics:

- *Install PI AF Client on PI AF Application Service Computer* (page 63)
- *Specify Default PI AF Server when Installing PI AF SDK and PI System Explorer* (page 64)
- *Install Specific Features of PI AF Client* (page 64)
- *Upgrade a Previous PI AF Client Installation* (page 64)

Install PI AF Client on PI AF Application Service Computer

When installing the PI AF SDK and/or PI System Explorer after the PI AF server installation, it is not necessary to specify the default PI AF server, as the setup program will have already done so:

```
msiexec.exe /i AFClient_<Version #>.msi REBOOT=Suppress ALLUSERS=1
/qn
```

Specify Default PI AF Server when Installing PI AF Client

The default PI AF Server is specified using the AF_SERVER argument:

```
msiexec.exe /i AFClient_<Version #>.msi REBOOT=Suppress ALLUSERS=1
AF_SERVER=<User-designated PI AF server name> /qn
```

Install Specific Features of PI AF Client

The PI AF SDK feature must always be installed when selecting individual features:

- Install the PI AF SDK, Common files and documentation without PI System Explorer:

  ```
  msiexec.exe /i AFClient_<Version #>.msi REBOOT=Suppress
  ADDLOCAL=FDClientCommonFiles,FD_AFSDK,FD_AFDocs ALLUSERS=1 /qn
  ```

- Install the PI AF SDK, PI System Explorer, and Common files without the documentation:

  ```
  msiexec.exe /i AFClient_<Version #>.msi REBOOT=Suppress
  ADDLOCAL=FDClientCommonFiles,FD_AFSDK,FD_AFExplorer ALLUSERS=1 /qn
  ```

Upgrade a Previous Installation of PI AF Client

When upgrading a previous client installation, it is not necessary to re-specify the PI AF arguments or features:

```
msiexec.exe /i AFClient_<Version #>.msi REBOOT=Suppress ALLUSERS=1
/qn
```

Chapter 7

Manage PI AF Collectives

About PI AF Collectives

PI Server collectives and PI AF collectives are mutually exclusive; you do not need a PI Server collective to create a PI AF collective or vice-versa. Neither the primary nor the secondary PI AF server need a PI Server installed.

A PI AF collective uses SQL Server replication to copy data from the primary PI AF SQL database computer (publisher) to each of the secondary PI AF SQL database computers.

Each secondary server communicates with the primary server through a Windows Communication Foundation (WCF) connection and reports its status information. The server authenticates the WCF connection using a Windows certificate that the PI AF server generates when it is started.

SQL Server replication transmits the primary PI AF server's certificate to each secondary server. After the secondary server receives the primary server's certificate, it can communicate its status to the primary server.

When PI AF data is changed on the primary PI AF server:

- The log reader agent sends any changes from PIFD to the PIFD_distribution database.

- For each secondary server, its agent pushes changes to the SQL Server instance on the secondary server.

  If the secondary server is not reachable (if there is a network problem or the computer is offline), the agent retries later.

PI AF Collective Security Requirements

To create a PI AF collective, you must meet the following security requirements:

- Windows credentials are used to run the PI System Explorer (PSE) to create the PI AF collective. These credentials are authenticated by PI AF, Windows, and SQL Server. The credentials used to create the PI AF collective are not used in the PI AF collective or SQL Server replication operation. The credentials are used one time and one time only: to create the PIAF collective.
- It is crucial that you use a low-privileged domain account for the SQL Agent Service and the PI AF application service. Do not use the Network Service account.
  - Do not grant the SysAdmin role in SQL Server to the NT Authority\Network Service account.
- The account that runs the SQL Agent Service on the primary SQL Server computer should have the db_owner role on the primary and secondary `PIFD` databases.
  - If you grant the sysadmin role instead of db_owner, the SQL Agent credentials must not be Local System, Network Service, or Local Service. OSIsoft recommends using db_owner.
  - Do not use Local System as the PI AF application service account. By default, the PI AF application service account is run under the Network Service account. However, a Network Service account is not required for the PI AF application service.
- Add the user account that performs the PI AF collective installation:
  - to the Windows Users and Groups as a local admin on all computers in the collective.
  - to SQL Server with the SysAdmin and Public roles on all computers in the collective.
- The PI System Explorer (PSE) user account must have administrator privileges within PI AF and must have the db_owner role on each SQL Server computer.
- On any SQL Server:
  - Do not grant the AF Server account the SysAdmin role or db_owner role.
  - Do not grant the AFServers local Windows account the SysAdmin role or db_owner role.
  - Do not run the SQL Server engine as an account with local or domain admin privileges. Least privilege is best.
- The only account that should exist in the AFServers group is the account under which the PI AF application service computer runs.
- The SQL Agent Service account must have write access to the primary SQL server’s `\repldata` folder.
- The PI AF application service computers must be in a domain; workgroups are not allowed.

- The PI AF SQL database computers can be in a workgroup or a domain.

  If the PI AF SQL database computers are in a workgroup, you must use a local Windows account that exists on the computer where PSE is run to create the collective and on the SQL Server computer. The accounts must have matching passwords, be in the local Windows administrators group on all computers, and be a member of the SQL Server SysAdmin role. This local account will be used to run PSE and create the PI AF Collective.

  If you run PSE as a domain account that is mapped to SysAdmin in SQL Server but your SQL Server is in a workgroup, you will get an error:

  ```
  cannot open service control manager on computer '172.30.86.10'.
  This operation might require other privileges. Do you wish to
  continue?
  ```

- For more information about minimum privilege levels required for replication, see:
  - "Replication Agent Security Model" at http://technet.microsoft.com/en-us/library/ms151868(v=sql.105)
  - "Security Role Requirements for Replication" at http://technet.microsoft.com/en-us/library/ms152528(v=sql.105)

PI AF Collective Creation Requirements

PI AF collectives have the following creation requirements:

- PI AF collectives are supported for PI AF 2.1 or later.
- The PI AF server version must be the same on all PI AF collective computers.
- The PI AF collective consists of at least two working PI AF servers. The PI AF client is not required on either PI AF server, but having it installed makes working with PI AF convenient.
- The PI AF SQL database on the primary and secondary servers must be named `PIFD`. You may not rename the PIFD database in a PI AF collective.
- The Named Pipes and TCP/IP protocols must be enabled for the instances where the PI AF SQL databases are installed.

PI AF Collective MS SQL Server Installation Requirements

PI AF collectives have these SQL Server requirements:

- Two SQL Server instances are required, each on separate physical hardware.
- The primary PI AF server requires SQL Server (SQL Server 2005 or later. Developer, Standard, or Enterprise edition).
- The secondary SQL Server computer can use the SQL Express edition, with limitations (these limits have increased in SQL Server 2008 Express; refer to Microsoft's web site for details.)
- SQL Server Compact edition is not supported.

- It is not necessary to have the same SQL Server edition/version for all members of a collective, but it is recommended.
- SQL Agent Service must be running on primary SQL Server computer.
- SQL Server Replication must be installed on the primary SQL Server computer; it is not required on the secondaries. If replication is subsequently added or installed, you must restart the SQL Server Agent to prevent errors.

See *Install Microsoft SQL Server* (page 17) for requirements for SQL Servers that are not part of a collective.

Before You Begin Creating a PI AF Collective

Perform these steps before you create a PI AF collective:

1. Make sure that you meet all security requirements. See *PI AF Collective Security Requirements* (page 66).
2. Make sure that you meet all collective creation requirements. See: *PI AF Collective Creation Requirements* (page 67).
3. PI AF server must be installed on each member of the collective. See *PI Asset Framework Installation and Upgrade Tasks* (page 21).
4. Make a full backup of the `PIFD` database.

   OSIsoft highly recommends that you make regular backups of SQL Server data, especially on the primary server. The PI AF installation process creates a SQL Server backup job that is scheduled to run by SQL Server Agent. Make sure you copy these backups to media other than the media that contains the data.
5. Login to the workstation from which you will create the collective – do not do this on the SQL Server computer – using the Windows credentials that you will use to create the collective, and make a successful connection to each PI AF server that will be part of the collective. See *Connect to a PI AF Server* (page 28).
6. On the same workstation, verify that you can perform a simple file share access to each SQL Server:
   a. Select **Start** > **Run**.
   b. Enter \\SQL_Server_computer_name for each SQL server.

      This ensures that your credentials authenticate to each SQL Server at the Windows level.
7. Now ensure that your credentials have the necessary SQL permissions:
   a. Establish a connection to each SQL Server via SQL Server Management Studio (SSMS) or `sqlcmd.exe`.
   b. Once connected, run the following query:

      ```
      SELECT IS_SRVROLEMEMBER (‘sysadmin’) "is sysadmin",
      CURRENT_USER "connected as", SYSTEM_USER "login user" ;
      ```

where

"`is sysadmin`" returns `1=true, 0=false`

"`connected as`" returns "`dbo`"

"`login user`" returns the user's Windows user principal

Do not proceed until the connection and query succeeds for each SQL Server that will be part of your PI AF collective.

8. Verify that TCP/IP and Named Pipes are enabled on all SQL Server computers for the correct instance. Run SQL Server Configuration Manager, choose your instance, and verify that the correct protocols are enabled.
9. Make sure the SQL Agent service credentials have `Modify` access to the `REPLDATA` folder on the primary SQL Server computer.
10. Make sure the SQL Agent service is running on the primary SQL Server computer.
11. All computers upon which the PI AF application service runs must be in a domain. Check the domain of each using the computer properties.

Create a PI AF Collective

1. Make sure that you understand and meet the requirements in the following topics:
   - *PI AF Collective Security Requirements* (page 66)
   - *PI AF Collective Creation Requirements* (page 67)

Perform all the preliminary steps listed in *Before You Begin Creating a PI AF Collective* (page 68).

1. Start the SQL Server Agent Service.

   SQL Server replication depends on the SQL Server Agent service. If it is not running, when you attempt to set up a PI AF collective, the setup fails without warning. The only way to recover is to delete the collective, start the SQL Server Agent service, then set up the collective.
2. In PI System Explorer (PSE), select **File > Connections** to open the **Servers** dialog box.
3. Right-click on an AF server that you want in the collective and select **Create Collective** from the resulting menu.

   The **Create New Collective - Verify Backup Completed** dialog box appears.
4. Click to select the **I have verified my backups are valid** check box and click **Next**.

   The **Create New Collective - Select Primary** dialog box appears.
5. Choose your primary server.
6. Click **Next**.

   The **Create New Collective - Select Secondary Servers** dialog box appears.
7. From the **Server** list, select a PI AF server to add to the collective as a secondary server and click **Add**. Repeat to add additional secondary. If you want to create the collective

without adding a secondary, then skip this step. You can add secondary servers after the collective is created. See *Add a Secondary Server to a Collective* (page 73).

8. Click **Next**.

   The **Create New Collective – Verify Selections** dialog box appears.

9. (Optional). Click **Advanced Options**. See *Configure Collective Properties* (page 71) for a description of the advanced option fields.

10. Click **Next.**

    The collective is created and the **Create New Collective – Finishing** dialog box appears.

11. Click **OK**.

    The **Create New Collective – Finishing** dialog box appears and the replication process begins.

    - If you click **Finish** before the secondary servers are listed in the lower area of the dialog box, the replication process stops on any secondary servers in the collective. A message appears that indicates the replication process is not complete. You will need to start the replication process on any secondary servers that currently belong to the collective.
    - If you click **Finish** before the replication is complete, a message appears indicating the replication is not complete, and where to look for the current replication status.

When the replication process is complete, the status for the first row (the snapshot creation) shows **Succeeded**. The status for the second row (the replication process as it relates to the primary server) shows **Idle**. The status for the third row and subsequent rows (the replication process as it relates to the secondary servers) shows **Idle**. For details about the collective status, see *Collective Status Details* (page 72).

Backup PI Collective SQL Server Data

OSIsoft highly recommends that you make regular backups of SQL Server data, especially on the primary server. The PI AF installation process creates a SQL Server backup job that is scheduled to run by SQL Server Agent. Make sure you copy these backups to media other than the media that contains the data.

If you accidentally delete data on the primary, the deletions will be replicated to the secondary. The only way to recover accidentally deleted data is from backup.

Make a full backup of the `PIFD` and `PIFD_Distribution` databases. The `PIFD_Distribution` database is located in the `System Databases` container.

See also *PI AF Backup Considerations* (page 111).

Configure Distributor Database Security

When you create a PI AF collective, a distributor database (`PIFD_distribution`) is created to allow for SQL Server replication. The AFServers group must have the `db_AFServer` role for this database. This role is automatically assigned to the local AFServers group during the PI AF collective creation. However, if you are installing a PI AF collective on a SQL Server cluster, the local AFServers group does not exist; it was replaced with a domain group as part of the process of installing PI AF on a SQL Server cluster. If the AFServers domain group does not have the `db_AFServer` role for the `PIFD_distribution` database, the collective creation will fail with an error message:

```
Waiting on a (Good) SyncStatus .. Current
SyncStatus(Snapshot Not Ready)
```

This error can be corrected during the PI AF collective creation process; it is not necessary to exit the **Create New Collective** dialog. Once the following steps are completed, the PI AF collective creation process will continue normally.

1. Open Microsoft SQL Server Management Studio, and connect to the SQL Server instance for the primary server in the PI AF collective.
2. Under the SQL Server cluster instance, expand **Security** > **Logins**.
3. Right-click the login created for the AFServers domain group and select **Properties**.
4. Select the **User Mapping** page.
5. Under **Users mapped to this login**, select the **Map** check box for **PIFD_distribution** database row.
6. Ensure the **User** column for the **PIFD_distribution** row is set to the domain user group (*YourDomain\YourAFDomainGroup*).
7. With the **PIFD_distribution** row selected, select the **db_AFServer** role check box under **Database role membership for: PIFD_distribution**. The public role should be selected by default; if it is not, select its check box.
8. Click **OK** to save the SQL Server login.

Configure PI AF Collective Properties

1. To configure an existing collective's properties, follow these steps:
2. In PI System Explorer, select **File > Connections**.

   The Servers dialog box appears.
3. Right-click on a member of the collective and then click the **Properties** button.

   The AF Server Properties dialog box appears.
4. Click the **Collective** tab.
5. Select a collective member and edit the settings. Note the following:
   - Timeout: The number of seconds for an operation to finish on the PI AF server.
   - Priority: The priority order for selecting the collective member on the current computer. You can modify this value for each collective member.
   - Period: The frequency, in seconds, in which a collective member checks the status of the remaining collective members.

- Grace: The time, in seconds, that is allowed before the communication status is set to `TimedOutOnPrimary` when there is no communication with the primary server.

  The settings also include some read-only fields. Note the following:

  - Port (read-only): The port through which the PI AF server communicates. This value is set in the AF server's configuration, prior to becoming a collective member.
  - Account (read-only): The account under which the PI AF application service is running. This value is set in the AF server's configuration, prior to becoming a collective member.
  - Role (read-only): The role within the collective of the selected collective member, primary or secondary. This value is set when the AF server is added to the collective.
  - Status (read-only): The status of the selected collective member, including the last time communication was verified with the primary server (not listed for the primary server), the last time the collective member was synchronized, current synchronization status, and current communication status.

6. Click More... to display the **Collective Status Details** dialog box (*Collective Status Details* (page 72)).

Check PI AF Collective Status

1. Click **File > AF Server Properties** to open the **AF Server Properties** dialog box.
2. Click the **Collective** tab to see the collective configuration information as well as information specific to the selected collective member. For a description of these settings, see *Configure Collective Properties* (page 71).

   The status of the selected member is in the **Status** area of the **Collective** tab.
3. Click **More** in the **Status** area.

   The **Collective Status Details** dialog box appears. *Collective Status Details* (page 72) explains how to interpret the data.

Collective Status Details

The **Collective Status Details** dialog box shows the last status messages for the primary and secondary servers:

- The first row shows the status of the snapshot creation process.
- The second row shows the status of the replication process between primary server and secondary server(s).
- The third row and below show the latest replication status messages for the secondary server(s).

Note: If there is no current activity, the **Details** area is empty.

All three dialog boxes have the following columns:

- **Name**: The name of the collective member.
- **Sync Status**: The synchronization status between the server members in the collective.
- **Status**: The status of the replication process from the primary server to the secondary server(s).
- **Comment**: The current stage of the replication process.
- **Commands Delivered**: The number of commands being sent from the primary server to the secondary server.
- **Error Code**: If an error occurs, the associated error code.
- **Error Message**: If an error occurs, the associated error message.

Note: If you click **Exit** prior before the dialog box lists a newly added secondary server, the replication process stops on the secondary server. A message appears that indicates the replication process is not complete. You will need to start the replication process on the newly added secondary server.

Add a Secondary Server to a PI AF Collective

You can add a secondary server to a PI AF collective when you create the collective, or after you create it. When you add a secondary PI AF server to a collective:

- A push subscription is set up in the `PIFD_distribution` database.
- A push subscription agent is started for each secondary server added to the collective.

The push subscription agent pushes the current snapshot to the secondary servers to initialize them. All the tables that are marked for replication are pushed to the secondary server. The existing snapshot data is replicated from the primary server to the newly added secondary server. Any pre-existing data on the secondary server is lost.

To add a secondary server:

1. In PI System Explorer (PSE), select **File** > **Connections** to open the **Servers** dialog box.
2. Right-click on a PI AF server and select **Add AF Server**.

   The **Adding Secondaries – Select Secondary Servers** dialog box appears.
3. From the **Server** list, select the PI AF server to add to the collective as a secondary server.
4. Click **Add** to add the PI AF server to the list.
5. Click **Next**.

   The **Adding Secondaries - Verify Selections** dialog box appears.
6. Click **Next**. The secondary server is added to the collective.

   The Adding Secondaries – Finishing dialog box appears. The process of replicating data to the secondary server begins and the dialog box displays collective status details during the process. When the replication process is complete on the secondary server, the

Status for the third and subsequent rows display **Idle**. For more on status details, see *Collective Status Details* (page 72).

Note: If you click **Exit** before the dialog box lists the newly added secondary server, the replication process stops on that secondary server. A message appears that indicates the replication process is not complete. You will need to start the replication process on any secondary servers that currently belong to the collective.

Connect or Switch to a Specific Member of a PI AF Collective

When you connect to a PI AF HA collective, PI AF automatically connects you to the collective member with the highest priority (lowest number). You can switch to a specific member of the collective.

1. In PI System Explorer, select **Connections**.
2. Right-click the collective and choose **Connect to Collective Member**.

   The **Choose Collective Member** dialog box appears.
3. In the **Collective Member** list, select the collective member to which you want to connect.
4. Click **OK**. You are now connected to the selected collective member.

Remove a Secondary Server from a PI AF Collective

When you remove a secondary server from a collective, the subscription is dropped on both ends (primary server and secondary server), the push agent for the secondary server is stopped, and the secondary server is deleted from the collective.

Caution: If you remove a primary PI AF server from a collective, the entire collective is removed. The subscription is dropped on both ends (primary server and secondary server). All agents are stopped. The PIFD_distribution database is deleted. All replication is halted and cannot be restarted. The primary server is available as a stand-alone PI AF server.

To remove secondary server from a collective:

1. In PI System Explorer (PSE), select **File** > **Connections** to open the **Servers** dialog box.
2. Select the AF server that you want to remove from the collective and click the **Properties** button.
3. Click the **Collective** tab.
4. Right-click the secondary server and select **Delete**.

   The secondary server is removed from the collective and becomes available in the **PI AF Servers** dialog box.

Stop or Start Replication

There is not a pause or resume option for replication; replication is either running or stopped.

When replication is stopped, the subscription is dropped on both ends (primary server and secondary server). The push agent for the secondary server is stopped. All agents are stopped. The PIFD_distribution database is deleted, and all replication is halted.

This section contains the following topics:

- *Stop Replication on a Secondary Server* (page 75)
- *Stop Replication on the Primary Server* (page 75)
- *Start Replication on a Server* (page 76)

Stop Replication on a Secondary Server

1. In PI System Explorer, select **File** > **Connections**.

   The Servers dialog box appears.

2. Right-click on a member of the collective and then click the **Properties** button.

   The AF Server Properties dialog box appears.

3. Click the **Collective** tab.
4. Right-click the secondary server and select **Stop Replication**. Replication is stopped on the secondary server. As long as the server is a member of the collective, you can start replication at a later time.

Stop Replication on the Primary Server

1. In PI System Explorer, select **File** > **Connections**.

   The Servers dialog box appears.

2. Right-click on a member of the collective and then click the **Properties** button.

   The AF Server Properties dialog box appears.

3. Click the **Collective** tab.
4. Right-click the primary server and select **Stop Replication**.

   Replication is stopped on the primary server and all secondary servers. As long as the collective still exists, you can start replication on the primary server at a later time; you will need to start replication on each secondary server, too.

Start Replication on a Server

If you have stopped replication on a collective member, it does not restart automatically. If you want the collective member to be involved in replication, you must start the replication on that member.

1. In PI System Explorer, select **File** > **Connections**.

   The Servers dialog box appears.

2. Right-click on a member of the collective and then click the **Properties** button.

   The AF Server Properties dialog box appears.

3. Click the **Collective** tab.
4. Right-click the server and select **Start Replication**. If this is the primary server, you also need to start replication on each secondary server.

Reinitialize a PI AF Collective Member

You can force a new snapshot of the database on the primary PI AF server to be created and pushed out to a secondary server by reinitializing the secondary server. If you have multiple secondary servers, you must reinitialize each individually.

When a secondary server is reinitialized, a new snapshot is created on the primary server. An agent pushes the snapshot to the secondary servers to initialize them. All the tables that are marked for replication are pushed to the secondary servers. Any pre-existing data on the secondary servers is lost.

1. In PI System Explorer, select **File** > **Connections**.

   The **Servers** dialog box appears.

2. Right-click on a member of the collective and then click the **Properties** button.

   The **AF Server Properties** dialog box appears.

3. Click the **Collective** tab.
4. Right-click the server and select **Reinitialize Replication**.

Configure Permissions on the Replication Data Folder

If the SQL Server Agent service runs under a domain account: on the primary PI AF SQL database computer, configure permissions on SQL Server’s `\repldata` folder to allow the SQL Server Agent service account to have access. Additionally, the account under which the SQL Server Agent service runs requires the `sysadmin` role on all SQL Servers involved in the PI AF collective.

1. On the primary PI AF SQL database computer, open Windows Explorer.
2. Navigate to the `\repldata` folder for the SQL Server instance where the PI AF SQL database is installed.

3. Right-click the `\repldata` folder and select **Properties**.
4. Click the **Security** tab and click **Edit**

   The **Permissions for repldata** dialog box appears.
5. Click **Add**.

   The **Select Users, Computers, or Groups** dialog box appears.
6. Check that the **From this location:** field shows the correct domain. If not, click **Location** button and navigate to and select the correct domain.
7. In the **Enter the object names to select** field, enter the name of the domain account under which the SQL Server Agent service runs.
8. Click **OK**.

   The **Permissions for repldata** dialog box appears.
9. In the **Permissions for [SQL Agent Account Name]** area, select the **Modify** check box, ensuring that all but the **Full control and Special permissions** check boxes are selected.
10. Click **OK**.
11. Click **OK** to return to Windows Explorer.

Upgrade a PI AF Collective

The PI AF upgrade process requires that you run the upgrade's executable file on each computer in the PI AF collective. All of the PI AF servers in a PI AF collective must be the same PI AF version. To minimize the amount of time when your PI AF users cannot write to the PI AF SQL database, and to maximize the availability of the PI AF data as read-only to your PI AF users, upgrade your PI AF collective members in this order:

1. *Upgrade Primary PI AF Server* (page 77).
2. *Upgrade Secondary PI AF Servers* (page 79).

Upgrade Primary PI AF Server

1. *Backup the Primary PI AF SQL Databases* (page 77).
2. *Stop Replication on the Primary AF SQL Database Computer* (page 78).
3. *Shutdown the Primary PI AF Application Service* (page 78).
4. *Run the Setup Executable on the Primary PI AF Server* (page 78).
5. *Restart the Primary PI AF Application Service* (page 78).

Backup the Primary PI AF SQL Databases

Make a full backup of the `PIFD` and `PIFD_Distribution` databases. The `PIFD_Distribution` database is located in the `System Databases` container.

Stop Replication on the Primary PI AF SQL Database Computer

1. Notify users to stop making changes. Make sure replication is completed and all changes are fanned out to secondary servers.

   Caution: Any updates that are in process are likely to be lost. It is recommended that you notify your users ahead of time that they should not attempt to make any changes to the PI AF SQL data during the brief period of time it takes to install the PI AF upgrade.

2. On the primary PI AF SQL database computer, verify that replication is complete:
   a. Check the synchronization status of each secondary PI AF server under **Replication > Local Publications > [PIFD]: PIAF >[Secondary Database Server Name].[PIFD].**
   b. Right-click and select **View Synchronization Status**.
3. In PI System Explorer, select **File > Connections**.

   The Servers dialog box appears.
4. Right-click on a member of the collective and then click the **Properties** button.

   The AF Server Properties dialog box appears.
5. Click the **Collective** tab.
6. Right-click the primary server and select **Stop Replication**.

   Replication is stopped on the primary server and all secondary servers. As long as the collective still exists, you can start replication on the primary server at a later time; you will need to start replication on each secondary server, too.

Shut Down the Primary PI AF Application Service

Disable and shut down the PI AF application service.

Run the Setup Executable on the Primary PI AF Server

If your PI AF application service and PI AF SQL database are on a single computer, see *Install or Upgrade PI AF Server on a Single Computer* (page 21)

If your PI AF application service and PI AF SQL database are on separate computers, see *Install or Upgrade PI AF Server Components on Separate Computers* (page 23).

Reassign the Domain Account to the Primary PI AF Application Service

The primary PI AF application service is automatically enabled and restarted on Primary after upgrade. If the domain account was assigned to the service, it will need to be reassigned.

Upgrade Secondary PI AF Servers

On each secondary collective member:

1. Disable and shut down the PI AF application service.
2. For each of your secondary PI AF servers:

   If your PI AF application service and PI AF SQL database are on a single computer, see *Install or Upgrade PI AF Server on a Single Computer* (page 21)

   If your PI AF application service and PI AF SQL database are on separate computers, see *Install or Upgrade PI AF Server Components on Separate Computers* (page 23).

   You do not need to leave the PI AF application service disabled unless you are doing a manual PI AF SQL database installation.

Start Replication

Restart replication on the primary PI AF server computer and all collective members that have been upgraded.

If you have stopped replication on a collective member, it does not restart automatically. If you want the collective member to be involved in replication, you must start the replication on that member.

1. In PI System Explorer, select **File > Connections**.

   The Servers dialog box appears.

2. Right-click on a member of the collective and then click the **Properties** button.

   The AF Server Properties dialog box appears.

3. Click the **Collective** tab.

Right-click the server and select **Start Replication**. If this is the primary server, you also need to start replication on each secondary server. The PI AF collective upgrade process is complete.

Troubleshoot PI AF Collective Issues

Status Details Indicates No Configured Subscriber

This message indicates no secondary server has been configured for replication. If a secondary server has already been added to the collective, the error could indicate there is a communication problem between the primary PI AF server and secondary server, or between the secondary PI AF server and the secondary PI AF SQL database.

If the failure was due to a problem between the primary and secondary PI AF server, review the PI AF event log on the secondary server for possible causes of the error. Verify the user account used in PI System Explorer has the proper access to the PI AF server.

If the failure was due to a problem between the secondary PI AF server and the secondary PI AF SQL database, review the PI AF event log on the secondary PI AF SQL database for possible causes of the error. Verify the user account used in the PI System Explorer has the proper access to the PI AF SQL database.

Collective Creation Fails Due to Login Failure

When creating a collective, the **Create New Collective – Finishing** dialog box displays the following message in top section: `“Login failed for user ‘[DOMAIN]\[UserName]’.”`

This message indicates that the logged-on user is unable to access one of the servers included in the collective. The error is most likely related to the fact that the logged-on user does not have the correct permissions on the primary PI AF SQL database computer. Review the Application event logs on the PI AF server and PI AF SQL database computers, beginning with the primary PI AF server, to determine which computer is receiving the connection error.

Be sure that the login account is given `sysadmin` privileges to SQL Server on the AF SQL database computer.

Snapshot Creation Fails Due to Access Error

During creation of a collective, the **Create New Collective – Finishing** dialog box displays the following message in the middle section: `“Current SyncStatus(Snapshot not ready).”` In the SnapShot status row (the first row in the bottom section), the message displays `“Access to the path ‘[..\repldata\...] is denied.”`

This message indicates that the SQL Server Agent service account does not have Write access to the `\repldata` folder for the SQL Server instance into which the Primary PI AF SQL database was installed. See *Configure Permissions on the Replication Data Folder* (page 76)). After setting the proper security permissions on the `\repldata` folder, exit the **Create New Collective – Finishing** dialog box. A message appears, indicating the primary server’s replication has not finished. Click **OK** and return to the **Collective** tab in the **AF Server Properties** dialog box. Delete the collective, then recreate the collective, and the snapshot is created correctly.

PI AF Collective Cannot be Created When SQL Server Agent is not Running

You attempt to create a collective by right-clicking a PI AF server in the **AF Servers** dialog box, and select **Create Collective.**

If the SQL Server Agent service for the selected PI AF server is not running, a message appears indicating the SQL Server Agent is not running on the PI AF SQL database computer. Click **OK** to return to the **AF Servers** dialog box. Start the SQL Server Agent service on the primary server, then create the new collective.

You attempt to create a collective by right-clicking in the white area of the **AF Servers** dialog box, and an error dialog box appears, along with the **Create New Collective –**

Finishing dialog box, indicating: `"SQL Server Agent is not running."` Click **OK** to exit the error dialog box. In the **Create New Collective – Finishing** dialog box the same message appears. Click **Cancel** to exit the dialog box. The collective was not created. Start the SQL Server Agent service on the primary server, then create the new collective.

PI AF Collective Administration Frequently Asked Questions

This topic contains frequently asked questions about PI AF collectives.

Question	Answer
What if the primary SQL Server computer has a catastrophic failure?	Set up a new primary SQL Server and restore from a backup (PIFD, PIFD_DISTRIBUTION, master, msdb). If this is not possible, create a new collective.
What if a secondary SQL Server computer has a catastrophic failure?	▪ On the primary server, stop replication to the missing secondary server. ▪ On the primary server, add a new secondary server and start replication to the new secondary server.
How to apply windows or SQL Server patches to a running PI AF collective	▪ Apply Windows patch(es). ▪ Reboot the computer, if necessary.

Chapter 8

Security Overview for PI AF

Related Topics

- *PI AF Collective Security Requirements* (page 66)
- *Special Considerations for PI AF Security on MSCS* (page 43)

General PI AF Security Recommendations

This topic contains general recommendations for securing PI AF:

- The SQL Server database engine should run as a low-privilege account. Some versions of SQL Server will by default run this service with the Local System identity, but Network Service or Local Service is a better choice, and a specifically created account with limited privileges is better still
- Do not grant administrator privilege to the identity under which the PI AF application service runs on any SQL Server instance.

  Note: By default, the PI AF installation configures the PI AF application service account to run as Network Service and configures SQL Server to grant minimal privileges to this login.

- Do not run the PI AF application service under the Local System account, as that will typically grant it SysAdmin privilege on any local SQL Server instances.

  Note: The PI AF application service logs a warning message to the Windows AF Event log if the service is running under an account or with a SQL login with unnecessarily high privileges.

- Limit access to the `AFService.exe.config` file to authorized users (including the account under which the PI AF application service runs). Do this either by limiting access to log on to the PI AF server, or by setting a security descriptor on the `AFService.exe.config` file or its directory.

- Disable Xp_cmdshell and OLE Automation in SQL Server. Be aware that an attacker with SysAdmin privileges can re-enable these features.
- Make sure that the account that runs the SQL Server database engine does not have access to any Windows objects that it does not need to access (files, registry keys, other services, and so on).
- Disable SQL Server's network listener and browser service if these are not needed. If the PI AF application service is not installed on the SQL Server computer, then the network listener is required. If the SQL Server instance that PI AF is using is a "named" instance, then, generally the SQL Browser service must be running.
- Do not grant non-admin PI AF users any SQL Server access privileges on a PI AF SQL database, except for PI AF collective administrators, who must have SysAdmin privilege for their Windows account.
- See these Microsoft SQL Server Security documents for further information:
  - *Security Considerations for a SQL Server Installation* (http://msdn.microsoft.com/en-us/library/ms144228.aspx)
  - *Securing SQL Server* (http://msdn.microsoft.com/en-us/library/bb283235.aspx)

Securing the PI AF Application Service Account Configuration

The PI AF server installation program sets up a default access configuration by which the PI AF application service gets the permissions it needs on the PI AF SQL database server. As part of this default configuration, the installation program configures the application service to run under the NetworkService account on the PI AF server computer.

For security reasons, we recommend that you change the PI AF application service to run under a domain account (*Run the Application Service Under a Domain Account* (page 84)).

Note: If PI AF application service and PI AF SQL database computers are located in different domains, and a trust does not exist between those domains, then the default configuration will not work. You must use SQL Server authentication to enable communication between the computers (*Configure PI AF to Use SQL Server Security* (page 90)).

Run the Application Service Under a Domain Account

The PI AF Server installation program configures the PI AF application service to run under the NetworkService account. It also configures access for the NetworkService account to the PIFD database on the PI AF SQL database server. This means that any local process running under the NetworkService account will have the same privileges to the PIFD database on the PI AF SQL database server.

For security reasons, we recommend that you change the PI AF application service to run under a domain account, and then remove the privileges for the NetworkService account on the SQL server (*Run the Application Service Under a Domain Account* (page 84)). This provides you with the most secure method for protecting your PI AF and SQL servers.

1. Identify the domain account that you want to use for the PI AF Server application service. That domain account requires privileges to *set the Service Principal Name* (page 85) (SPN). If you cannot get the required access permissions, but still need to use the domain account, then you can *configure the AF Server to use a User Principal Name (UPN* (page 86)).
2. *Add the domain account to the AFServers local user group* (page 88). The application service gets the required access to the PI AF SQL database through this local group on the SQL database computer.
3. Open the Services administrative tool on the PI AF server computer.
4. Right-click the **PI AF Application Service** and select **Properties**.
5. Click the **Log On** tab and change the account to a domain account, using the "`domain\account`" format, or click the **Browse** button to search for and select the domain account to use.
6. Click **OK**.
7. Right-click the **PI AF Application Service** and select **Restart**.

   A message appears indicating the service is being stopped, and then started. The service is now running under the new account.
8. Remove the previous account's access to the PIFD database. . Most often, the previous account was the default account, NetworkService. For example, see *Remove the NetworkService Account's Access to the PI AF SQL Database* (page 86).

   Note: After you remove the NetworkService account from the PIFD database, any time you run the setup program (repair or upgrade), you may have to repeat this step.
9. Reconfigure your PI AF server's properties to reference the new PI AF application service account.
   a. In PI System Explorer, select **File** > **Connections**.
   b. Select the AF Server in the list and click **Properties**.
   c. If you are using a UPN for the connection, then type in the Account name, otherwise ensure that the Account field is clear; and then click Connect.
   d. Click **OK**.
   e. Click **Close**.

Check SPN Creation Permissions

If you configure the PI AF application service to run under a domain account, then you need to check that the domain account has privileges to set the Service Principal Name (SPN) for the service. By default, for PI AF Server 2010 and later, a PI AF server registers an SPN for the PI AF application service upon startup. PI AF clients, such as PI System Explorer, will use this SPN to authenticate the connected server's identity.

An SPN is a domain-wide directory for services on the domain. Microsoft introduced SPNs to make communicating with specific servers more secure and manageable. By default, PI System Explorer and other PI AF clients use the PI AF application service's SPN to connect to PI AF servers.

Local computer accounts, such as NetworkService, typically have permission to set an SPN. However, domain accounts often do not. If the PI AF application service is running under a domain account that does not have the privileges to set the SPN for the service, then extra configuration is needed for a client such as PI System Explorer to connect to that PI AF server.

There are two configuration options:

- Have the domain administrator set the domain manually, using the Microsoft's **SetSpn** utility. This is the recommended option. Note that Microsoft has some documentation on the concept and implementation of SPNs, and there is a tool (**SetSpn.exe**) that helps with managing them.
- Have the PI AF server administrator configure the PI AF server to use a User Principal Name (UPN) for authentication instead of an SPN (*Configure the AF Server to use a UPN* (page 86)).

In either case, to add the PI AF server connection to an instance of PI System Explorer, you will need to type in the SPN or UPN account name. See the section on adding a PI AF server in the *PI System Explorer User Guide* for more information.

Configure PI AF Server to use a UPN

To configure PI AF server to use a user principal name (UPN), edit the **AFServer.exe.config** file. The file contains the following element in a default installation:

```
<identity>
   <servicePrincipalName value="AFServer" />
   <!-- <userPrincipalName value="username@domain"/> -->
</identity>
```

Note that the UPN setting (`userPrincipalName`) is commented out and the SPN (`servicePrincipalName`) setting is enabled.

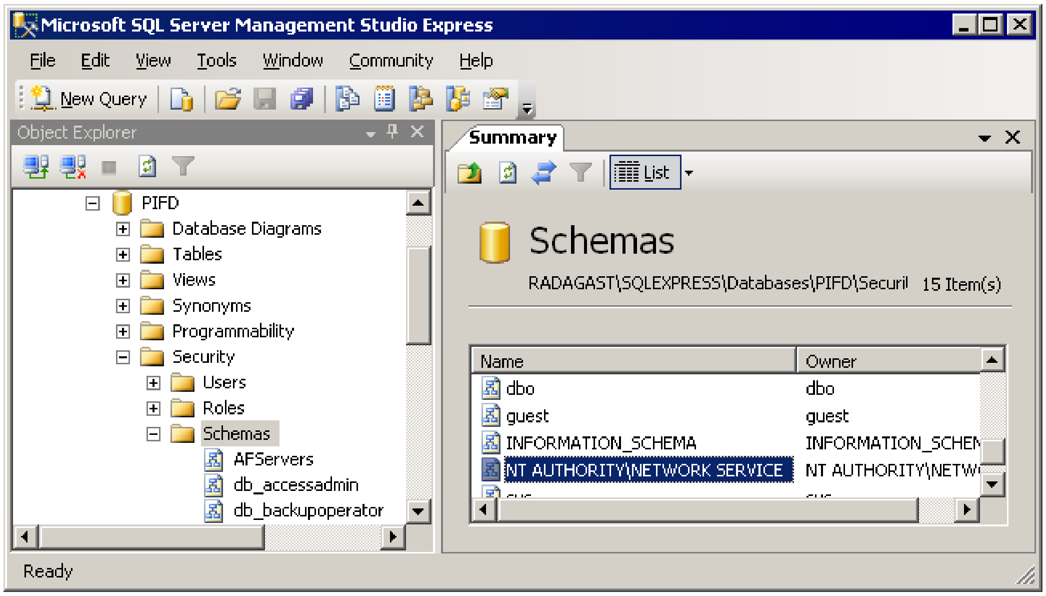
To configure the PI AF server to use a UPN instead of an SPN, comment out the `servicePrincipalName` element and uncomment the `userPrincipalName` element. The value of the `userPrincipalName` would be the domain credentials under which the PI AF server is running. For example:

```
<identity>
   <!--<servicePrincipalName value="AFServer" />-->
   <userPrincipalName value="username@domain"/>
</identity>
```

Remove the NetworkService Account’s Access to the SQL Database

If you change the PI AF application service so that it does not run under the NetworkService account, you must remove the NetworkService account’s access to the PI AF SQL database (PIFD). After you remove the NetworkService account from the PIFD database, any time you run the setup program (repair or upgrade), you may have to repeat this procedure.

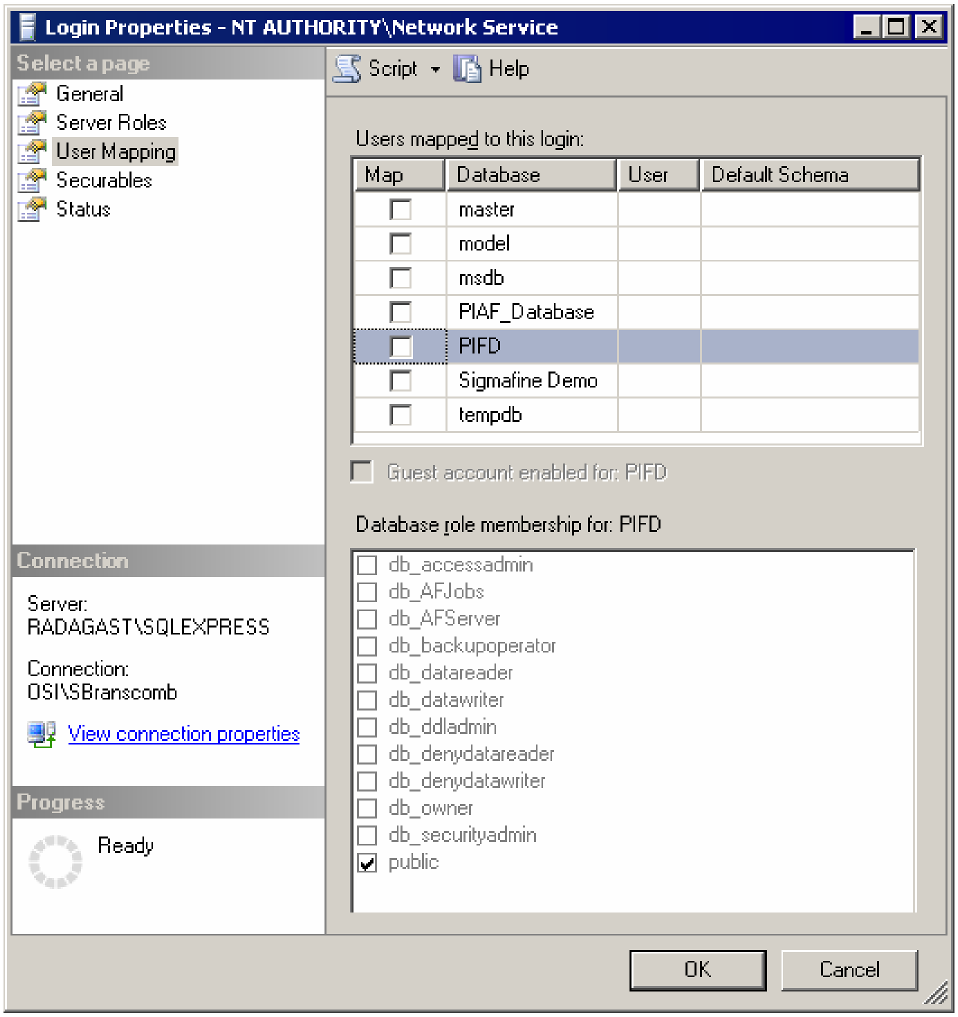
1. On the PI AF SQL database computer, click **Start** > **Administrative Tools** > **Computer Management**.
2. Under **Computer Management (Local)**, expand **System Tools** > **Local Users and Groups** > **Groups**.
3. In the list of groups, double-click **AFServers**.
4. Select the NetworkService account and click **Remove**.
5. Click **OK** and click **Close**.
6. Open SQL Server Management Studio and connect to the SQL Server instance in which the PIFD database resides.
7. Expand the **PIFD** database and navigate to the **Security > Schemas** folder.



RADAGAST\SQLEXPRESS\Databases\PIFD\Securi 15 Item(s)

Name	Owner
dbo	dbo
guest	guest
INFORMATION_SCHEMA	INFORMATION_SCHEN
NT AUTHORITY\NETWORK SERVICE	NT AUTHORITY\NETW

8. Right-click the **NT AUTHORITY\NetworkService** schema and select **Delete**.
9. Click **OK** to remove the schema.
10. Under the SQL Server instance, expand the **Security** folder; then expand the **Logins** folder.
11. Right-click **NT AUTHORITY\NetworkService** and select **Properties**.
12. Select the **User Mapping** page.
13. Select the row for the **PIFD** database.
14. Clear the check box under **Map** for the PIFD database.



Users mapped to this login:

Map	Database	User	Default Schema
□	master		
□	model		
□	msdb		
□	PIAF_Database		
□	PIFD		
□	Sigmafine Demo		
□	tempdb		

□ Guest account enabled for: PIFD

Database role membership for: PIFD

- □ db_accessadmin
- □ db_AFJobs
- □ db_AFServer
- □ db_backupoperator
- □ db_datareader
- □ db_datawriter
- □ db_ddladmin
- □ db_denydatareader
- □ db_denydatawriter
- □ db_owner
- □ db_securityadmin
- ☑ public

Server:
RADAGAST\SQLEXPRESS

Connection:
OSI\SBranscomb

Ready

15. Click **OK**.

    The “`NT AUTHORITY\NetworkService`” user in the PIFD database is removed, and the “`NT AUTHORITY\NetworkService`” login no longer has access to the PIFD database.

Add a Domain User to the AFServers Local User Group

When the PI AF application service is run under a domain account, you need to add that domain account to the AFServers local user group on the PI AF SQL database computer.

To add a domain user to the AFServers local user group:

1. On the PI AF SQL database computer, click **Start** > **Administrative Tools** > **Computer Management**.
2. Under **Computer Management (Local)**, expand **System Tools** > **Local Users and Groups** > **Groups**.
3. In the list of groups, double-click **AFServers**.

4. Add the domain account under which the PI AF application service is running to the AFServers group. If it is running under the NT AUTHORITY\NetworkService account, add the PI AF server's system account to this group.

   Note: If the PI AF application service is running as the LocalService account, then you will likely need to use SQL Server security, instead of integrated security.

5. Close Computer Management.

PI AF Application Service and PI AF SQL Database Considerations

By default, the PI AF application service runs under the NT AUTHORITY\NetworkService user account on the PI AF server computer. That user account is a member of a local group, called the AFServers user group, on the PI AF SQL database computer. The AFServers user group provides the required access on the SQL database computer through a SQL Server login that is mapped to the AFServers group.

Here is how the installation applications create the default configuration:

- The PI AF server installation application creates the PI AF application service on the PI AF server computer. It configures this application service to run under the NT AUTHORITY\NetworkService user account on that computer.
- The PI AF SQL database installation application:
  - Creates a local user group, AFServers, on the PI AF SQL database computer. This process will fail if SQL Server is on a domain controller or on a cluster.
  - Adds the application service account (NT AUTHORITY\NetworkService) to the local AFServers group on the PI AF SQL database computer.

  Note: If you install the PI AF SQL database separately from the PI AF server installation, then the installation application prompts for the domain and computer name of the PI AF server. It then adds the PI AF server's computer account to the local AFServers group on the PI AF SQL database computer.

  - Creates a SQL Server login that is mapped to the AFServers local user group. The SQL Server login has the necessary access required for the PI AF application service.

Configure PI AF and SQL Database on Untrusted Domains

When the PI AF application service and PI AF SQL database are in different domains that are not trusted, or if they are in workgroups, you need to configure the two to allow for communication.

1. Configure SQL Server to allow remote connections. See *Enable SQL Server's Remote Connections* (page 112).
2. Configure PI AF to use SQL server security. See *Configure PI AF to Use SQL Server Security* (page 90).

3. If you are using a "named instance" of SQL Server and have not specified a port in the connect string, then make sure the SQL Server Browser service is running on the SQL Server computer. To promote the most secure environment, you should specify the port in the connection string.
4. Ensure that your system security is configured as described in *PI AF Security and Firewalls* (page 97).

Configure PI AF to Use SQL Server Security

By default, PI AF uses Windows authentication to connect to the PI AF SQL database. However, when The PI AF server and SQL server are on different non-trusted domains, you need to configure PI AF to use SQL Server authentication instead. Follow these steps:

1. *Configure SQL Server to Use Mixed Mode Authentication* (page 90)
2. *Create and Configure SQL Server User* (page 90)
3. *Specify SQL Server Security Mode and Add User* (page 93)
4. *Specify a PI AF SQL Database in the Connect String* (page 93)

Configure SQL Server to Use Mixed Mode Authentication

To use mixed mode authentication:

1. Open Microsoft SQL Server Management Studio, and connect to the SQL Server instance that stores the PI AF SQL database (PIFD).
2. Right-click the SQL Server instance and select **Properties**.

   The **Server Properties** dialog box appears.
3. Select the **Security** page.
4. Select the **SQL Server and Windows Authentication mode** option.
5. Click **OK** to return to Microsoft SQL Server Management Studio.

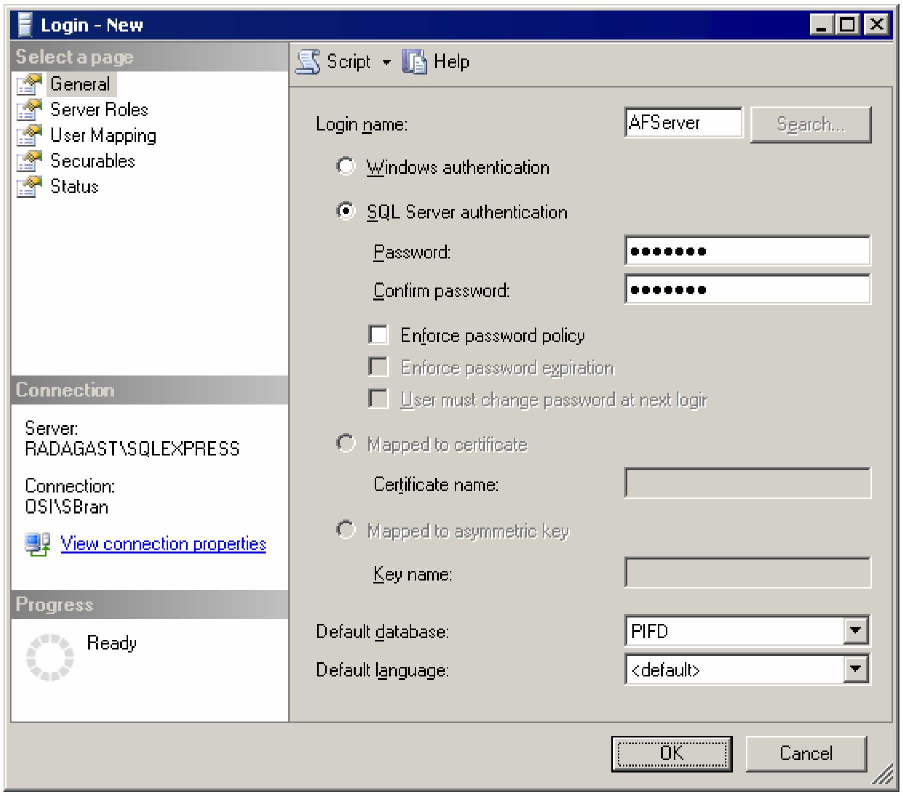
   If the SQL Server service has not been restarted since mixed mode authentication was selected, then mixed mode authentication will not be available until the SQL Server database engine service is restarted.

Create and Configure SQL Server User

Follow the steps below to: create a SQL Server login, grant the SQL Server login account access to the PI AF SQL database (PIFD), and grant the SQL Server user the `db_AFServer` database role.

1. In the Microsoft SQL Server Management Studio, connect to the SQL Server instance that stores the PI AF SQL database (PIFD).
2. Under the SQL Server instance, expand **Security** > **Logins**.
3. Create a new login and enter a name in the **Login name** box.

4. Select the **SQL Server authentication** option.
5. Enter the password in the **Password** and **Confirm password** boxes.
6. In **Default database**, select **PIFD**.



Login - New

Select a page: General, Server Roles, User Mapping, Securables, Status

Login name: AFServer

○ Windows authentication

● SQL Server authentication

Password: •••••••

Confirm password: •••••••

□ Enforce password policy

□ Enforce password expiration

□ User must change password at next login

○ Mapped to certificate

Certificate name:

○ Mapped to asymmetric key

Key name:

Default database: PIFD

Default language: <default>

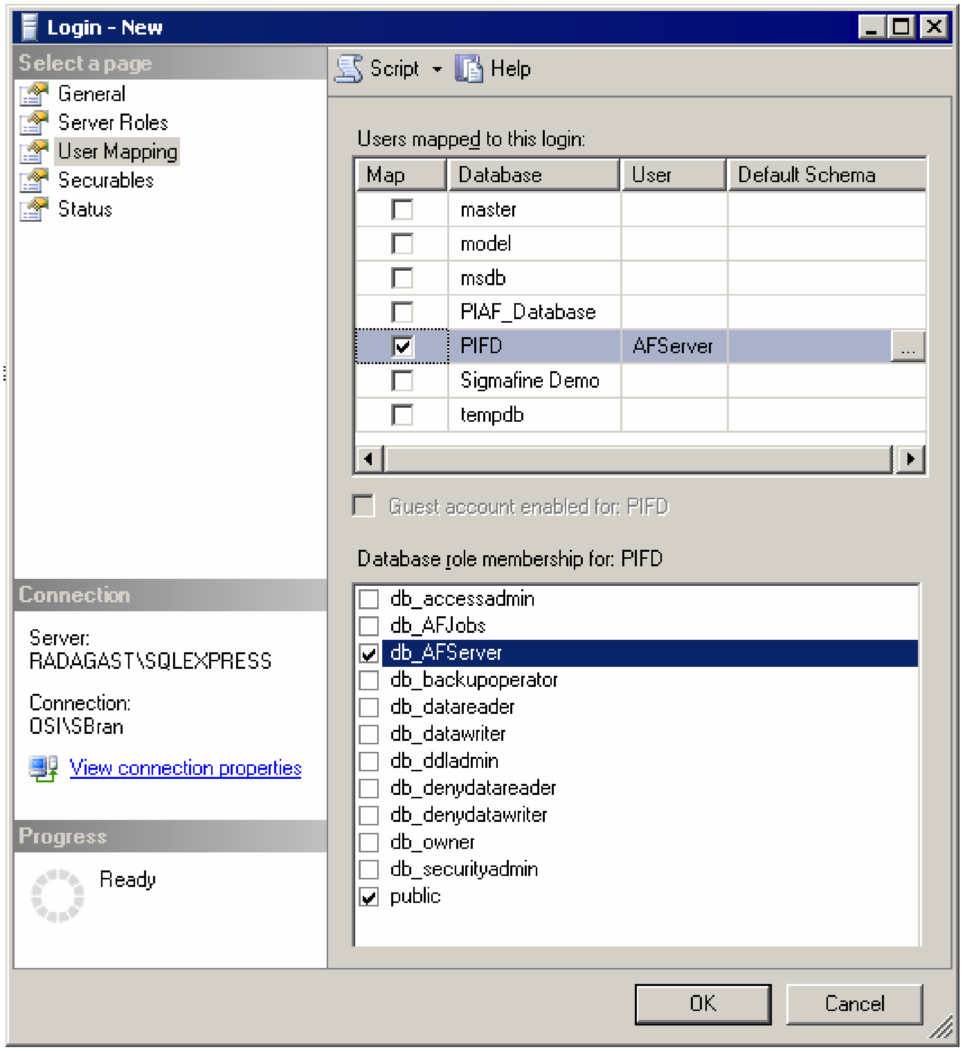
Connection

Server: RADAGAST\SQLEXPRESS

Connection: OSI\SBran

Progress: Ready

7. Select the **User Mapping** page.
8. Select the row for the PIFD database.
9. Select the **Map** check box for the PIFD database.



Users mapped to this login:

Map	Database	User	Default Schema
□	master		
□	model		
□	msdb		
□	PIAF_Database		
☑	PIFD	AFServer	...
□	Sigmafine Demo		
□	tempdb		

□ Guest account enabled for: PIFD

Database role membership for: PIFD

- □ db_accessadmin
- □ db_AFJobs
- ☑ db_AFServer
- □ db_backupoperator
- □ db_datareader
- □ db_datawriter
- □ db_ddladmin
- □ db_denydatareader
- □ db_denydatawriter
- □ db_owner
- □ db_securityadmin
- ☑ public

Server:
RADAGAST\SQLEXPRESS

Connection:
OSI\SBran

Ready

10. Under **Database role membership for: PIFD**, select the **db_AFServer** check box.
11. Click **OK**.

About the PI AF Server Connect String

The connect string defines the location of the PI AF SQL database and the security mode used to connect to the database. This is a standard ADO.NET connection string. The connect string is defined in the `AFService.exe.config` file. You can modify the connect string to indicate that the new authentication mode is being used, and to provide the credentials for connecting.

Some of the changes you may need to make to the connect string are:

- Specify the SQL Server security mode.
- Add the SQL Server user and password.
- Specify the PI AF SQL database.

Note: OSIsoft recommends that you limit access to the `AFService.exe.config` file to authorized users (including the account under which the PI AF application service runs). Do this either by limiting access to log on to the PI AF Server, or by setting a security descriptor on the `AFService.exe.config` file or its directory.

Connect String Examples

Integrated Security:

```
<add key="connectString" value="Persist Security
Info=False;Integrated
Security=SSPI;server=AFSQLDB\SQLEXPRESS;database=PIFD;Application
Name=AF Application Server;"/>
```

SQL Server Security:

```
<add key="connectString" value="Persist Security
Info=False;Trusted_Connection=no;server=AFSQLDB\SQLEXPRESS;databas
e=PIFD;Application Name=AF Application
Server;uid=af_sql_user;pwd=af_sql_password;"/>
```

Specify SQL Server Security Mode and Add User

If you want to use SQL Server security, you need to change the connect string to reference the correct security mode and add a SQL Server user and password.

1. Open the `AFService.exe.config` file with a text editor, such as Notepad.
2. Locate the connect-string key. It has the following format:

   ```
   <add key="connectString" value="Persist Security
   Info=False;Integrated
   Security=SSPI;server=.\phxtest;database=PIFD;Application
   Name=AF Application Server;"/>
   ```

3. Modify the connect string by replacing `Integrated Security=SSPI` with `Trusted_Connection=no`.
4. Add the SQL Server user ID (`uid`) and password (`pwd`) at the end of the connect string:

   After your changes, the connect string should resemble this example:

   ```
   <add key="connectString" value="Persist Security
   Info=False;Trusted_Connection=no;server=AFSQLDB\SQLEXPRESS;databas
   e=PIFD;Application Name=AF Application
   Server;uid=af_sql_user;pwd=af_sql_password;"/>
   ```

5. Save and close the file.
6. Restart the PI AF application service.

Specify a PI AF SQL Database in the Connect String

If your PI AF SQL database is moved to a new server, or you need to work with a different PI AF SQL database, you can specify the change within the connect string. Follow these steps:

1. On the PI AF server computer, open the `AFService.exe.config` file with a text editor, such as Notepad.
2. Locate the connect-string key. It has the following format:
   - Integrated Security
     ```
     <add key="connectString" value="Persist Security
     Info=False;Integrated
     Security=SSPI;server=.\phxtest;database=PIFD;Application
     Name=AF Application Server;"/>
     ```
   - SQL Server Security
     ```
     <add key="connectString" value="Persist Security
     Info=False;Trusted_Connection=no;server=.\phxtest;database=PIFD
     ;Application Name=AF Application
     Server;uid=af_sql_user;pwd=af_sql_password;"/>
     ```
3. Modify the connect string, specifying the new location of the server. You can use a computer name or an IP address, and can include the SQL Server instance name.
   - Integrated Security
     ```
     <add key="connectString" value="Persist Security
     Info=False;Integrated
     Security=SSPI;server=AFSQLDB\SQLEXPRESS;database=PIFD;Applicati
     on Name=AF Application Server;"/>
     ```
   - SQL Server Security
     ```
     <add key="connectString" value="Persist Security
     Info=False;Trusted_Connection=no;server=AFSQLDB\SQLEXPRESS;data
     base=PIFD;Application Name=AF Application
     Server;uid=af_sql_user;pwd=af_sql_password;"/>
     ```
4. Save and close the file.
5. Restart the PI AF application service.

Connect PI System Explorer and PI AF Server

To ensure a successful connection between your PI System Explorer and PI AF server:

1. Make sure that the PI AF server is version 2.0.4 or later. If the version is older, upgrade it first.
2. Create the same local account on both computers. Use the same password, too.
3. Set the firewalls to open the incoming connections on PI AF Server. See *PI System Firewall and Port Considerations* (page 101) for which ports need to be open.
4. Log on to the PI System Explorer client computer using the new local account.
5. Open PI System Explorer and try to connect to the target PI AF server.
6. In PI System Explorer, on either the **Database Properties** dialog box or the **Select Database** dialog box, click ▦ to open the **System Properties** dialog box.
7. Set **Name** and **Host** to the actual settings of your PI AF server. **Account** remains empty.
8. Click **OK**.

9. Click **Connect** to initiate a connection.
10. If you have a connection problem, see *Set Audit Policy* (page 95) and *Set Sharing and Security Model for Local Account* (page 95).

Set Audit Policy

The best way to understand the root cause of the connection problem is to turn auditing on, and to check the security-related events in Windows Event Viewer.

1. Click **Start** > **Administrative Tools** > **Local Security Policy**.
2. Under **Security Settings**, select **Local Policies** > **Audit Policy**.
3. Set the security setting to **Success, Failure** for the following policies:
   - **Audit account logon events**
   - **Audit logon events**
   - **Audit object access**
   - **Audit privilege use**

   To do so:

   a. Right-click each policy and choose **Properties**.

   b. Select the **Success** and **Failure** check boxes.

   c. Click **OK**.

Set Sharing and Security Model for Local Account

A probable cause of a connection problem is that the PI AF node did not authenticate the client user as a local user, but used the Guest account instead.

To allow the local computer to authenticate local users as themselves instead of Guest:

1. On the PI AF server computer, click **Start** > **Administrative Tools** > **Local Security Policy**.
2. Under **Security Settings**, select **Local Policies** > **Security Options**.
3. Right-click **Network access: Sharing and security model for local account** and choose **Properties**.
4. Set the security setting to **Classic - local users authenticate as themselves**.
5. Click **OK** to save your change.

Configure Active Directory Access for PI Notifications Contacts

When using PI Notifications with PI AF server, you may need to specify how to access Microsoft's Active Directory in order to retrieve the users used to populate the PI Notifications' Contacts lists.

Each PI AF server provides the option to specify the Domain and User folder, as well as the user account, to be used to access Active Directory and to retrieve users for the Contacts list.

By default, the account under which the PI AF server 2.x application service is running is used to retrieve the user information from Active Directory for the domain in which the AF Server resides. However, if you need to access an Active Directory in a different domain, or if you need to define a specific user account to be used to access Active Directory, you will need to configure the PI AF server's Active Directory Access.

1. Open PI System Explorer and connect to a database belonging to the PI AF server for which you want to configure the Active Directory access.
2. From the **Tools** menu, select **Active Directory Properties**. The Active Directory dialog opens.
3. In the **Full Domain Name** text box, enter the full DNS name of the Active Directory domain from which the user accounts will be retrieved for the PI Notifications Contacts. If this field is left blank, the domain in which the PI AF application service resides will be used.
4. In the **User Folder** text box, enter the path to the user folder where the list of users for this domain resides.

   In larger Active Directory domains, users may be organized within folders. The use of User folders can allow for faster retrieval of a list of Active Directory users.

   Use the following structure for the User folder:

   ```
   DomainUserFolder/SubDomainUserFolder/Sub SubDomainUserFolder
   ```

5. You can define the user account to use to access Active Directory for building the PI Notifications Contact list. Select one of the following options:

   Use AF Server's Account – This is the default selection. Select the User AF server's Account option to access Active Directory using the account under which the PI AF application service runs. By default, the PI AF server is installed using the Network Service account. However, the PI AF server service account can be changed. If the PI AF server's service account does not have the necessary permission to read the Active Directory, no users will be retrieved in the Contacts list. If your Active Directory security is configured in a way such that the PI AF server's service account can read the Active Directory, then this is the simplest option.

   Impersonate Client - Select this option to use the credentials of the user account under which the connecting client application is running. If the PI AF server's service is running under an account (Network Service is the default account) that does not have permission to read the Active Directory, this option can be used. As long as the user account under which the connecting client application is running has permission to read Active Directory, a list of users is returned to the Contacts list. The contents of the Contacts list may vary, depending upon the user account used for connecting, since the security to read the users is determined by Active Directory.

   Note: Specifying this option may require Kerberos configuration if an AF SDK application will be using impersonation in a middle tier, such as a Web Service or in IIS.

   Specify Account – This option allows you to define a specific user account to be used to read the Active Directory. You might use this option if you need to read the Active Directory from a domain that is different than that under which the PI AF server resides, or if the user account under which the PI AF server's service runs and the account under which the client application runs has no permission to read the required Active Directory. Specify any other account as your application requires, using the format "`Domain\User`." Ensure that the specified user account has the appropriate permission to read the target Active Directory.

6. Select the **Global Catalog** check box for the Active Directory domain controller searches to use the global catalog if it is available. Otherwise searches must go to the owning domain controller.

7. Clear the **Return All Persons** check box to return only users from the target Active Directory.

   Active Directory objects are derived from one another as follows:

   `Top>Persons>OrganizationalPerson>Contact`

   and

   `Top>Persons>OrganizationalPerson>User`

   When you select this check box, Persons, OrganizationalPersons, Contacts and Users are returned from the target Active Directory. If you clear the check box, it returns only Users.

Firewalls and PI AF Security

Customers are often required to isolate the process control part of their network from the rest of their network. They might also configure a buffer zone, or demilitarized zone (DMZ), to install servers and software that needs to transfer data between the process control network and the local area network. The DMZ is usually isolated between firewalls.

There are three server components in a PI System:

- PI Server
- PI AF server
- Microsoft SQL Server that hosts the PI AF SQL database.

While these components could be installed on a single computer, this section assumes that each component is installed on a separate computer in order to illustrate the complexity of connectivity and security configuration. In addition to this being a more interesting topology to discuss, it also distributes the processor load across several computers, which can increase system performance.

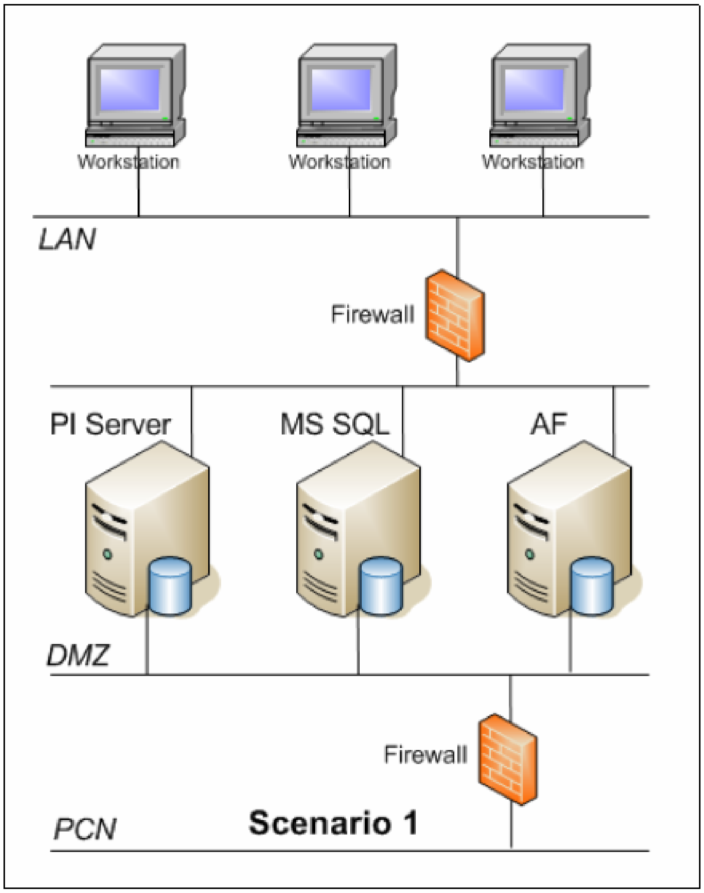
⚠ **Caution**: Opening ports in your firewall can leave your server exposed to malicious attacks. Make sure that you understand firewall systems before you open ports. For more information, see *Security Considerations for a SQL Server Installation* (*http://msdn2.microsoft.com/en-us/library/ms144228.aspx*).

Firewall Topology Examples

This section presents three scenarios that illustrate possible locations for a firewall.

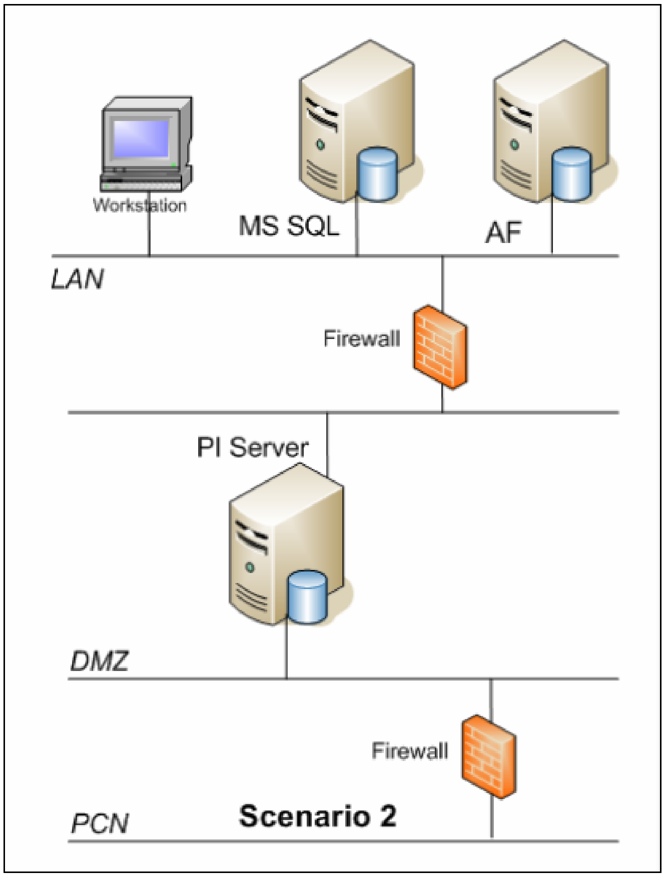
Firewall with All Servers Installed Within the DMZ

In this example, all the servers are installed in the DMZ. This simplifies the security settings between the servers because they all reside within the firewalls.



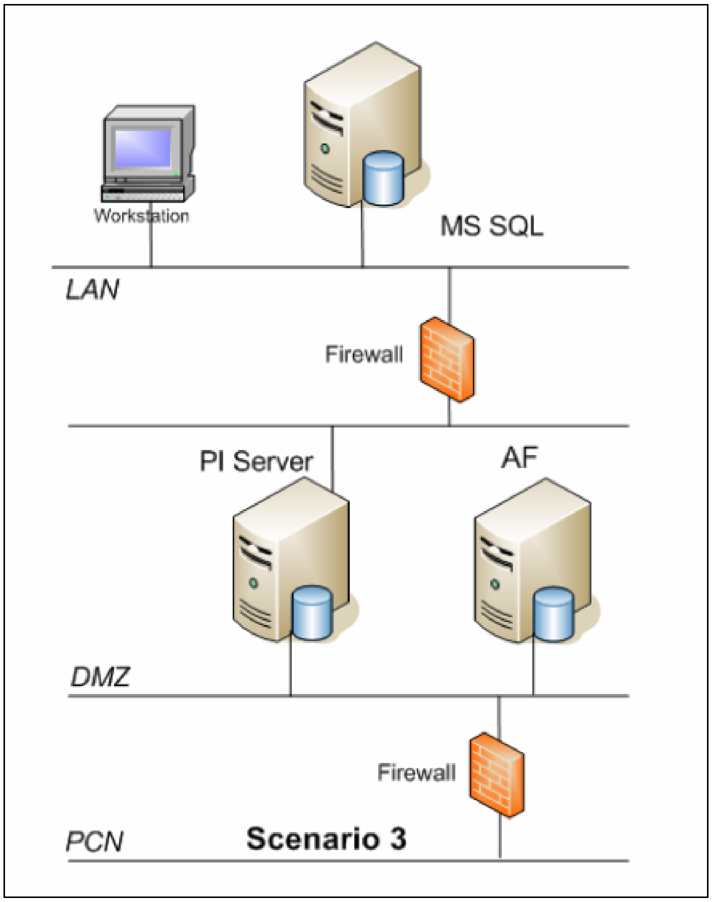
Firewall with PI Server in the DMZ and PI AF and SQL Server on the LAN

In this scenario, only the PI Server resides in the DMZ. The SQL Server and PI AF server are connected to the LAN. This scenario might occur when customers want to access data from foreign databases or synchronize PI AF assets with an ERP or maintenance system.



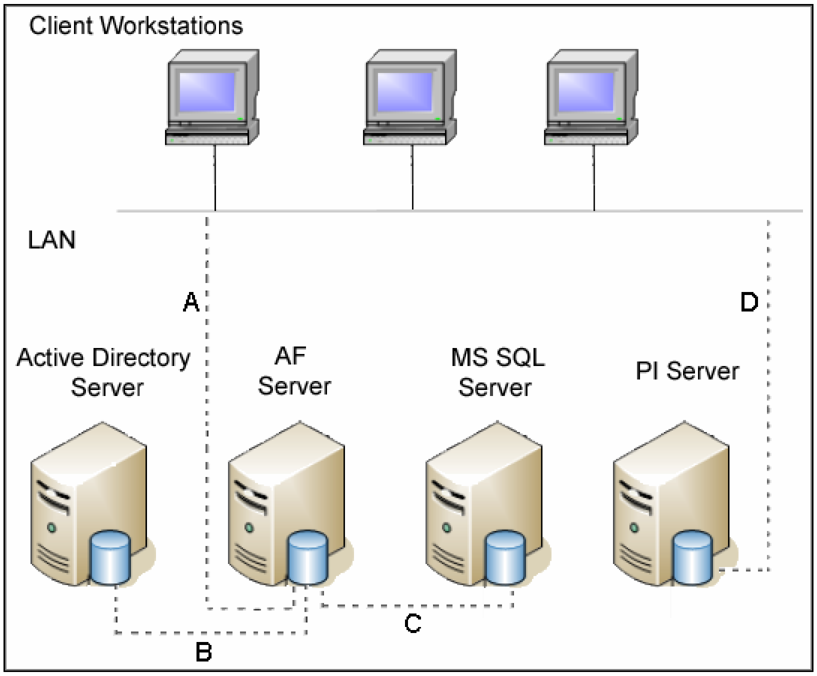
Firewall with SQL Server Outside of the DMZ

In this scenario, only the SQL Server resides outside of the DMZ. This may happen when customers want to use an existing SQL Server to host the PI AF SQL database.



PI AF Network Connection Types

A PI AF system includes multiple network connections.



Connection Type	Description
A	The connection between the PI AF server and any PI AF SDK client, including PI System Explorer, allows the client to read and write structure information such as elements and models between the PI AF SDK and the PI AF server.
B	The connection between PI AF server and Active Directory allows the PI AF server to read a list of Active Directory users, which are in turn exposed through PI AF as contacts.
C	The connection between PI AF server and SQL Server allows the PI AF server to reads and write structure information, such as elements and models, to a SQL Server database.
D	The connection between a PI AF client and a PI Server allows a PI AF client to read and write PI data and populates attribute values within the PI AF SDK.

PI System Firewall and Port Considerations

This section presents port considerations for the following firewall configurations:

- *Firewall between PI AF Server and PI AF Client* (page 102)
- *Firewall between PI AF Server and SQL Server* (page 102)
- *Firewall between PI AF Client and PI Server* (page 104)
- *Firewall between PI AF Server and Domain Controller* (page 105)

Firewall between PI AF Server and PI AF Client

All connectivity between a PI AF client and a PI AF server occurs through PI AF SDK. The appropriate port must be open. The PI AF server connection must use the IP address or DNS name of the PI AF server, not the computer name.

By default, PI AF SDK communicates with PI AF server through port 5457 and port 5459.

- Port 5457 is the primary port that PI AF SDK uses to communicate with PI AF server from the client.
- Port 5459 is used by some client products, such as PI OLEDB Enterprise and PI WebParts to communicate with PI AF server.

Depending on how connections are defined, PI AF server may perform a reverse-name lookup of the connecting client IP address as part of the authentication process. The method chosen for name resolution may require that PI AF server be able to open outbound connections on some ports:

- Resolution by way of entries in the HOSTS file (no port requirement, but clients must have fixed IP addresses).
- Resolution by way of DNS (usually port 53).
- Resolution by way of NETBIOS name services (port 137).

Firewall between PI AF Server and SQL Server

This section contains the following topics:

- *About SQL Server Access* (page 102)
- *Configure SQL Server Access* (page 102)
- *Open a Port in Windows Firewall for TCP Access* (page 103)
- *SQL Server Browser Service* (page 104)
- *List the SQL Server Executable File as an Exception to the Blocked Programs* (page 104)
- *Connect to a Named Instance on a MSCS Cluster* (page 104)

About SQL Server Access

By default, for an unnamed SQL Server instance, communication to the SQL Server database engine requires port 1433 to be open; however, the port used can be changed. For detailed information, review *How to Configure a Windows Firewall for Database Engine Access* (*http://msdn2.microsoft.com/en-us/library/ms175043.aspx*).

By default, Microsoft Windows XP Service Pack 2 enables Windows Firewall, which closes port 1433 to prevent Internet computers from connecting to a default instance of SQL Server on your computer. Connections to the default instance using TCP/IP are not possible unless you reopen port 1433. For more information, see the Windows documentation.

Configure SQL Server Access

To access an instance of the SQL Server database engine through a firewall, you must configure the firewall on the computer running SQL Server to allow access.

For general information about how SQL Server works with firewall systems, see *Connecting to SQL Server over the Internet* (*http://msdn2.microsoft.com/en-us/library/ms175483.aspx*).

You can use SQL Server Management Studio to configure a static port, open the firewall, and connect to the database engine. See *Getting Started with the Database Engine* (*http://msdn2.microsoft.com/en-us/library/ms345318.aspx*).

To allow SQL Server access:

- Configure the SQL Server database engine to use a specific TCP/IP port.

  The default instance of the database engine uses port 1433.

- Configure instances of SQL Server 2005 Express Edition, SQL Server Mobile, and named instances of the Database Engine use specific ports, rather than dynamic ports.

  See *Configure a Server to Listen on a Specific TCP Port (SQL Server Configuration Manager)* (*http://msdn2.microsoft.com/en-us/library/ms177440.aspx*).

- Configure the firewall to allow access to that port for authorized users or computers.

OPEN A PORT IN WINDOWS FIREWALL

(This procedure assumes you are using Windows XP. Please check the Windows Firewall documentation for your operating system.)

1. In Control Panel, open **Network Connections**.
   a. Right-click the active connection and select **Properties**.
   b. Click the **Advanced** tab.
   c. Click **Windows Firewall Settings** to open the **Windows Firewall** dialog box.
2. Click the **Exceptions** tab.
   a. Click **Add Port**.
   b. In the **Name** box, type `SQL Server <instance name>`.
   c. In the **Port number** box, type the port number of the instance of the database engine, such as 1433 for the default instance.
   d. Verify that **TCP** is selected and click **OK**.
3. To open the port to expose the SQL Server Browser service, click **Add Port**, type `SQL Server Browser` in the **Name** box, type `1434` in the **Port Number** box, select **UDP**, and then click **OK**.

   See also *Stop SQL Server Browser Service* (page 104).
4. Click **Add Program** in the **Windows Firewall** dialog box for additional options, such as granting access to specific programs and restricting access to certain IP addresses or network subnets.

   Note: To allow named pipes access through the firewall, you must also enable File and Printer Sharing through the firewall.
5. Close the **Windows Firewall** and the **Properties** dialog boxes.

Stop SQL Server Browser Service

The SQL Server Browser service allows users to connect to instances of the SQL Server database engine that are not listening on port 1433, without knowing the port number. To use the SQL Server Browser service, you must open UDP port 1434.

To promote the most secure environment:

1. Leave the SQL Server Browser service stopped.
2. Configure clients to connect using the port number.

List the SQL Server Executable File as an Exception to the Blocked Programs

As an alternative to configuring SQL Server to listen on a fixed port and opening the port, you can list the SQL Server executable file (`Sqlservr.exe`) as an exception to the blocked programs. Use this method when you want to continue to use dynamic ports. Only one instance of SQL Server can be accessed in this way.

1. In the **Windows Firewall** dialog box, on the **Exceptions** tab, click **Add Program**.
2. Click **Browse**, and navigate to the instance of SQL Server that you want to access through the firewall, and then click **Open**.

   By default SQL Server is in this folder: `C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Bin\Sqlservr.exe`.
3. Click **OK** twice to close the **Windows Firewall** dialog box.

Connect to a Named Instance on a MSCS Cluster

When the PI AF SQL database is installed on a named instance on a SQL Server cluster, there are special firewall settings required.

Alternatively, you can open the firewall on computers that need to connect to the named instance on the SQL Server cluster, by creating an inbound rule that is open for all local and remote ports, but only from the IP addresses of each node of the SQL Server cluster. However, be sure you understand the implications behind opening ports before you attempt this alternative approach.

Firewall between PI AF Client and PI Server

PI AF clients need to connect to the PI AF application service to access the PI AF SQL database. They may also need to connect directly to PI Server if PI AF elements have been configured with PI point data references. The connection to PI Server is established directly from the PI AF client. No direct connection or authentication is needed against the SQL Server or PI AF server.

By default, communication to the PI Server requires port 5450 to be open; however, you can change this. For detailed information, review *Which Ports need to remain open on a firewall for a PI3 Server and clients to communicate?* (*http://techsupport.osisoft.com/Support+Solution/7/7A928A04585C47D6A3562B7E8F630FA5.htm*) from techsupport.osisoft.com.

Firewall between PI AF Server and Domain Controller

In many cases, you have your servers on one side of a firewall and the domain controllers that the users need to authenticate on the other side of the firewall. If this is the case, you need to open the following ports between your servers and the domain controllers:

- TCP ports 137, 138, 139 — These are the standard ports used for both authentication and NetBIOS services browsing for a Windows NT 4.0 domain controller and are fully supported for backward compatibility by Windows 2000 domain controllers. If you are using any version of Terminal Server or Citrix MetaFrame and the users of the server need to authenticate with a domain controller, you need to open these ports up both ways between the domain controllers and the servers.
- TCP port 88 (Kerberos authentication) — Windows 2000 offers an alternative and more secure method of authentication called Kerberos. If you have Windows 2000 Terminal Servers and they are authenticating with a Windows 2000 domain controller, they will use Kerberos authentication by default. If you need for users of these Windows 2000 Terminal Servers to authenticate with a Windows 2000 domain across a firewall, you will need to open up this port.
- If you need to open communication between two domain controllers across a firewall for either trust relationship traffic or Active Directory traffic, see How to configure a firewall for domains and trusts (http://support.microsoft.com/kb/179442).
- You can find more detailed coverage of Microsoft port usage in the following technical articles:
  - Windows NT, Terminal Server, and Microsoft Exchange Services Use TCP/IP Ports (http://support.microsoft.com/kb/150543)
  - Information about TCP/IP port assignments (http://support.microsoft.com/kb/174904)
  - TCP ports and Microsoft Exchange: In-depth discussion (http://support.microsoft.com/kb/176466)

PI AF Port Summary

The following ports may need to be open on a firewall to allow access to PI AF server or other associated services:

- 44 WINS - Windows Internet Name Service (name resolution).
- 53 DNS - Domain Name Service (name resolution).
- 88 Kerberos - Windows 2000, XP authentication.
- 123 NTP Network - Time protocol, for clock synchronization.
- 135 DCOM port mapper - Windows authentication, DCOM applications including OPC, SMT 3.
- 137 NETBIOS Name Service - NetBIOS name resolution.
- 138 NETBIOS Datagram Service.
- 139 NETBIOS Session Service.

Note: Ports 135, 137, and 139 are considered high-risk and are usually blocked.

- 389 LDAP.
- 445 SMB
- 636 LDAP SSL
- 1433, 1434. See: *Connection to SQL Server over the Internet* (*http://technet.microsoft.com/en-us/library/ms175483.aspx*) and *Configuring the Windows Firewall to Allow SQL Server Access* (*http://msdn.microsoft.com/en-us/library/cc646023.aspx*).
- 3268 LDAP GC
- 3268 LDAP GC SSL
- 3389 Windows Remote desktop - Remote desktop for PI Server administration.
- 5450 PI Network Manager.
- 5454:5455 PI Analysis Framework 1.x.
- 5456 PI ACE - Used by PI ACE 2 scheduler.
- 5457 AF Server.
- 5458 PI Notifications.
- 5459 AF Server (used by PI OLEDB Enterprise and PI WebParts)

PI AF Clients and Windows Authentication

The PI AF Client setup program consists of the PI AF SDK, PI System Explorer, and user documentation.

PI System Explorer and other PI AF SDK clients communicate with PI AF server using Windows authentication. Except for configuration of a PI AF collective, the PI AF SDK never connects directly to the PI AF SQL Server. When you attempt to connect to a PI AF server through PI System Explorer, your login credentials are used. If you have permission to access the PI AF server, the connection is made.

If you do not have the appropriate rights (for example, if you are logged in as a local user, not a domain user, or the client computer is in a domain other than that of the PI AF server), a login dialog box appears where you can enter credentials.

Run PI System Explorer with Elevated Permissions

If you run PI System Explorer directly on the PI AF server computer and the operating system has user-account control enabled, then using a local administrative account will not elevate the account: You will be prompted to restart with elevated permissions. To avoid this prompt, choose one of these options:

Run PI System Explorer as Administrator:

1. On the **Start** menu, right-click **PI System Explorer** (or other PI AF client).
2. Select **Run as Administrator**.

Set PI System Explorer always to run as Administrator:

1. On the **Start** menu, right-click **PI System Explorer** (or other PI AF client).
2. Select **Properties**.
3. On the **Compatibility** tab, select the **Run this program as an administrator** check box.

Modify the PI AF security settings so that the user or a group containing the user (other than local Administrators) has appropriate privileges.

Configuring Security for External Tables

A PI AF table can be linked to data from external data sources such as Excel, Access, SQL Server, or other OLEDB/ODBC data sources. A PI AF table linked to an external data source is called a linked table or an external table. There are potential security risks for external tables in general. Risks vary depending on how an external table connects to the foreign data source.

You can restrict the use of certain connection types. You can also disable external tables altogether. The following sections explain how external tables get their data and what the security options for external tables on a PI AF server.

How Linked Tables Access Data

When a client application requests the external data, the PI AF server queries the external data source and returns the data to the client as a read-only PI AF table.

Note: When using PI System Explorer to configure linked PI AF tables with a 64-bit version of the PI AF server, only 64-bit OLE DB providers may be used. Furthermore, the Data Link Properties dialog that is invoked with the Build button when linking a table cannot be used to configure the linked table, because it only lists 32-bit providers.

When you configure the linked table, you are required to specify the credentials that the AF Server uses to connect to the database. The authentication options are:

- **Windows impersonated.** If the source database supports Windows authentication, then use the Windows identity of the client that is requesting the data. This is an *impersonated* connection. This is the most secure method of authentication; use it wherever possible.
- **Windows non-impersonated.** If the source database does not support Windows authentication, or if the database and PI AF Server are on different, non-trusted domains, then specify a user name and password with the necessary access on the source database. PI AF uses this hard-coded account to read the data in the external data source. For example, MySQL database does not support Windows authentication, so you would use the user name and password of an account on the MySQL database.

- **SQL Server Security.** When linking to SQL Server data, you might need to use SQL Server Security.

Note: When using PI System Explorer to configure linked AF Tables with a 64-bit version of the AF Server, only 64-bit OLE DB providers may be used (). Furthermore, the Data Link Properties dialog that is invoked with the Build button when linking a table cannot be used to configure the linked table, because it only lists 32-bit providers.

Risk of Using Non-impersonated Connections

Depending on the configuration of the SQL Server, a user with PI AF administrator privileges could create attacks on the SQL Server and take full control of the system if the following conditions all exist:

- A PI AF table is configured to use the AF server identity for linking to an external database.
- Non-impersonated linked (external) tables are enabled on the AF server.

  Note: By default, non-impersonated linked tables are disabled on the AF server. In order for a user to execute an attack, that user would need to enable non-impersonated external tables.

- The PI AF Server account has administrative rights on a SQL Server.

  Note: By default, the AF Server runs under the NetworkService account and does not have administrative rights to the locally-configured SQL Server or access to remote computer databases. Without administrator rights to the remote database, the possibility for elevation of privilege attacks is limited.

Caution: For security reasons, do not grant the PI AF server administrative privileges on the computer or SQL Server when running with non-impersonated queries.

Linked Table Access on PI System Explorer 2.0.x

For security reasons, AF Server versions 2.1 and later do not by default allow access to linked tables from the following versions of PI System Explorer:

- 2.0.3.2019
- 2.0.4.2025

Linked Table Data Access Recommendations

- Leave access from PI System Explorer versions 2.x disabled. See *Changing Security Settings for Linked Tables* (page 109) for instructions.

- If access to external tables is not needed, disable it altogether. See *Changing Security Settings for Linked Tables* (page 109) for instructions.
- Do not grant the PI AF application service account administrative privileges on the PI AF server or SQL Server when running with non-impersonated queries.
- By default, you must have administrative privileges on the PI AF server to configure an external table that runs non-impersonated queries. Leave this default setting.

Changing Security Settings for Linked Tables

Use the AF Diagnostics utility to adjust security settings for external tables. The AF Diagnostics utility is a command-line utility that you can use to enable or disable PI AF server features and perform other administrative functions. The utility makes a direct connection with the associated SQL Server database and requires the SQL Server sysadmin or db_afadmin role.

The utility name is **afdiag** and it is located in the `\PIPC\AF` folder.

Task	Command	Default Setting
Enable support for external PI AF tables	`afdiag /DTImp`	enabled
Disable support for external PI AF tables	`afdiag /DTImp-`	enabled
Enable support for external PI AF tables from PSE 2.0	`afdiag /DT20`	disabled
Disable support for external PI AF tables from PSE 2.0	`afdiag /DT20-`	disabled
Enable support for external PI AF tables for non-impersonated users	`afdiag /DTImp`	enabled
Disable support for external PI AF tables for non-impersonated users	`afdiag /DTImp-`	enabled
Change security settings for a specific PI AF table	In PI System Explorer, right-click on the table in the Browser and choose **Security** from the resulting menu.	By default, table configuration requires administrative privileges on the PI AF server.
Change security settings for all tables.	In PI System Explorer, right-click on **Tables** in the Browser and choose **Security** from the resulting menu.	By default, table configuration requires administrative privileges on the PI AF server.

Chapter 9

PI AF Configuration and Maintenance

This section contains the following topics:

PI AF Backup Considerations

OSIsoft highly recommends that you back up your database on a regular basis. Use Microsoft SQL Server Management Studio or the **sqlcmd** command utility.

Consider these points as you design a backup strategy:

- Standard maintenance best practices call for log backup, daily data backup, and periodic re-index on all databases.
- When the SQL Server Agent is available (all editions of SQL Server except Express), PI AF will automatically install and schedule a nightly SQL Server backup. Examples of SQL Server versions are: SQL Server 2000, SQL Server 2005, SQL Server 2008, SQL Server 2008 R2. Refer to the `Maintenance.sql` file located in the `PIPC\AF\SQL` directory.
- Releases beginning with PI AF 2.1 schedule a SQL Server Agent job to back up data and logs. SQL Server replication requires the SQL Server Agent on the publisher (primary) instance.
- Frequency of backup depends on your application; nightly backups may be best. The default backup does a complete backup every night at 0315, local time. However, you can change the time and can change the frequency and whether full or differential backups are done.
- Place the back-up file on a different physical disk from where the SQL Server data is located. You may not be able to write to the root folder of `C:\` Use another drive, such as a network drive, or a subfolder.
- SQL Express 2005 and SQL Express 2008 do not include a job scheduler, so you need to use a Windows utility to schedule the backup. You can use the following command to run the backup:

  ```
  sqlcmd -S <SQLINSTANCE> -d PIFD -Q "EXEC dbo.usp_backup
  @outpath = N'', @allwaysfullbackup = 1;" -E
  ```

You will need `sysadmin`, `db_owner`, or `db_backupoperator` role. The least privilege is the best security practice.

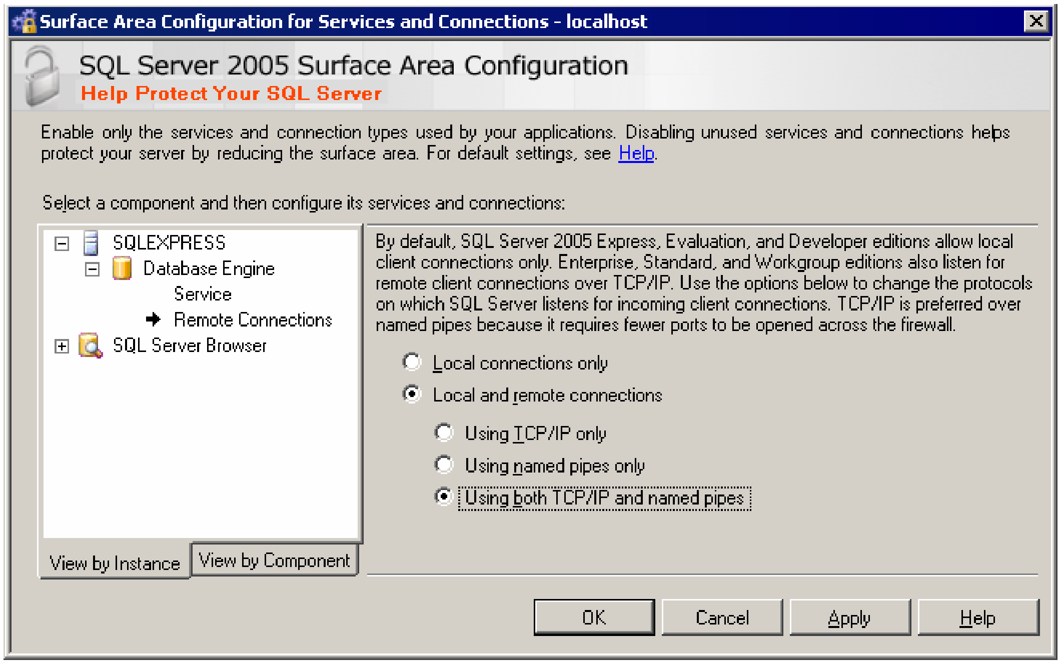
- The Master database should also be backed up at some frequency. This database contains the metadata for the PIFD database, such as the database properties, table definitions, and so forth. The PI AF scheduled backup will back up the PIFD, master, msdb, and PIFD_distribution.
- The PI AF Server installation kit configures the PIFD database with a simple recovery model by default. This means that transaction logs cannot be backed up and "point-of-failure" recovery is not possible. If the PIFD database is set to the full recovery model, then the PIFD transaction logs should also be backed up. This will truncate the transaction logs so they do not grow without bounds and also allow either point-in-time or point-of-failure recovery. The PI AF scheduled backup will back up the transaction log if the database is configured with the full recovery model. OSIsoft recommends that you change your PIFD database from the simple recovery model to the full recovery model to allow point-in-time recovery.

Enable SQL Server (2005) Remote Connections

If your PI AF application service and PI AF SQL database are installed on different systems, you need to ensure that SQL Server is able to accept remote connections. Check with your SQL Server Database Administrator and/or your Network Administrator to determine the network protocols to enable. (This procedure assumes that you are running SQL Server 2005.)

To enable remote connections:

1. Click **Start** > **All Programs** > **Microsoft SQL Server 2005** > **Configuration Tools** > **SQL Server Surface Area Configuration** to open the **SQL Server Surface Area Configuration** window.
2. Click the **Surface Area Configuration for Services and Connections** link to open the **Surface Area Configuration for Services and Connections – localhost** dialog box.



Surface Area Configuration for Services and Connections - localhost

SQL Server 2005 Surface Area Configuration

Help Protect Your SQL Server

Enable only the services and connection types used by your applications. Disabling unused services and connections helps protect your server by reducing the surface area. For default settings, see Help.

Select a component and then configure its services and connections:

- SQLEXPRESS
  - Database Engine
    - Service
    - Remote Connections
  - SQL Server Browser

By default, SQL Server 2005 Express, Evaluation, and Developer editions allow local client connections only. Enterprise, Standard, and Workgroup editions also listen for remote client connections over TCP/IP. Use the options below to change the protocols on which SQL Server listens for incoming client connections. TCP/IP is preferred over named pipes because it requires fewer ports to be opened across the firewall.

○ Local connections only

● Local and remote connections

○ Using TCP/IP only

○ Using named pipes only

● Using both TCP/IP and named pipes

3. Select **Remote Connections** for the SQL Server instance that stores the PIFD database.

4. Select **Local and remote connections**, then select the appropriate option for your environment:

   o Using TCP/IP only

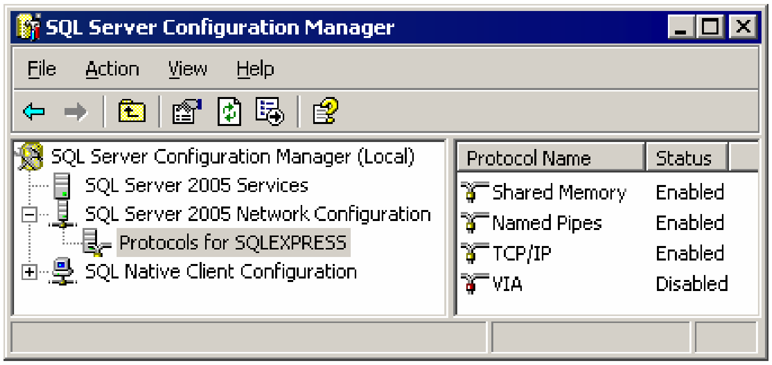
   o Using named pipes only

   o Using both TCP/IP and named pipes

5. Click **OK**. A message appears indicating the change does not take effect until the Database Engine restarts. Click **OK** to return to the **SQL Server Surface Area Configuration** dialog box.

6. Close the **SQL Server Surface Area Configuration** dialog box.

7. Click **Start** > **All Programs** > **Microsoft SQL Server 2005** > **Configuration Tools** > **SQL Server Configuration Manager** to open the **SQL Server Configuration Manager** dialog box.



SQL Server Configuration Manager

- SQL Server Configuration Manager (Local)
  - SQL Server 2005 Services
  - SQL Server 2005 Network Configuration
    - Protocols for SQLEXPRESS
  - SQL Native Client Configuration

Protocol Name	Status
Shared Memory	Enabled
Named Pipes	Enabled
TCP/IP	Enabled
VIA	Disabled

8. Expand **SQL Server 2005 Network Configuration** and select the protocols for the SQL Server instance that stores the PIFD database.
9. Right-click the protocol you want to enable and select **Enable**. A message appears indicating the change does not take effect until the service is restarted. Repeat this for each network protocol that needs to be enabled. Click **OK**.
10. Select **SQL Server 2005 Services** in the left pane. In the right pane, right-click the SQL Server instance and select **Restart**. The SQL Server service is restarted and your changes now take effect.

Monitor PI AF Server and SQL Server Communication

You can monitor the overall readiness of PI AF server with PI AF Server Health counter in the Windows Performance Monitor.

To view the **Health** counter in Performance Monitor:

1. On the PI AF server computer, select **Control Panel > Administrative Tools > Performance Monitor**.
2. In the **Performance Monitor** window, under **Monitoring Tools**, select **Performance Monitor**.
3. In the right-hand pane, click the green plus sign.
4. In the **Add Counters** dialog box, scroll down to and expand **PI AF Server** to show the **Health** counter.
5. Select the **Health** counter and click **OK**.

   The **Performance Monitor** now displays the **PI AF Server Health** counter in the chart. The performance counter can have two values:

   - **0** — PI AF server is not running or cannot establish a success connection with SQL Server.
   - **1** — PI AF server is running and communicating successfully with SQL Server.

Troubleshooting Connection Problems

This section presents some connection errors that you might encounter, and provides some possible solutions.

Cannot Connect to SQL Database

Try the following:

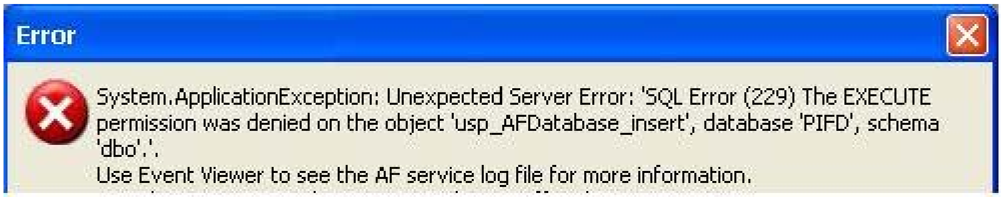
- Check the PI AF server's connect string for correct server\instance and database name. See *Modify the PI AF Application Service Connect String* (page 39).
- Check SQL Server, to verify the PIFD database is not offline.

Cannot Connect to PIFD Database

Try the following:

The account under which the PI AF application service is running does not have permission to connect to the `PIFD` database. Assign this account the appropriate permission.

SQL Error 229



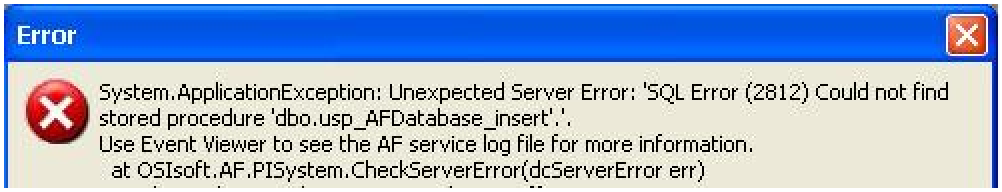
System.ApplicationException: Unexpected Server Error: 'SQL Error (229) The EXECUTE permission was denied on the object 'usp_AFDatabase_insert', database 'PIFD', schema 'dbo'.'.
Use Event Viewer to see the AF service log file for more information.

```
System.Data.SqlClient.SqlException: The EXECUTE permission was
denied on the object 'usp_GetCollection', database 'PIFD', schema
'dbo'.
Database role db_afserver has not been granted permission to
execute this stored procedure.
```

Try the following:

Assign this account the appropriate permission.

SQL Error 2812

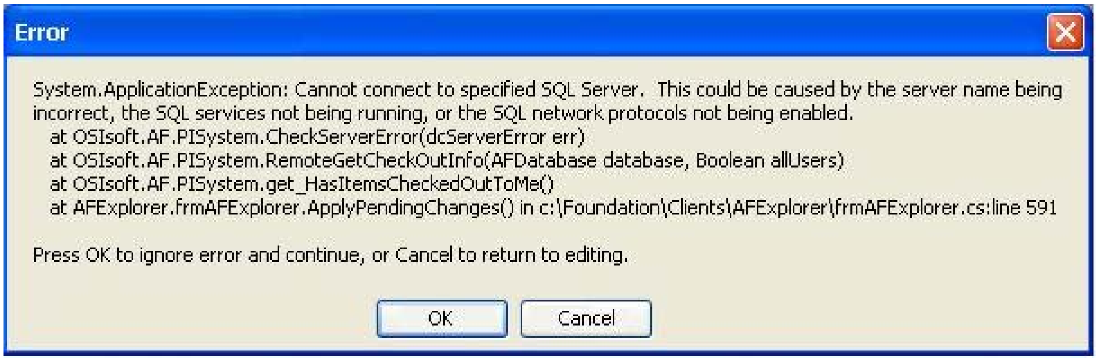


System.ApplicationException: Unexpected Server Error: 'SQL Error (2812) Could not find stored procedure 'dbo.usp_AFDatabase_insert'.'.
Use Event Viewer to see the AF service log file for more information.
 at OSIsoft.AF.PISystem.CheckServerError(dcServerError err)

Try the following:

A stored procedure is missing from the PI AF SQL database. Run `GO.BAT` to rerun the SQL scripts. See *Execute the SQL Scripts to Create and Populate the PI AF SQL database* (page 38).

Cannot Connect to Specified SQL Server



Error

```
System.ApplicationException: Cannot connect to specified SQL Server.  This could be caused by the server name being
incorrect, the SQL services not being running, or the SQL network protocols not being enabled.
   at OSIsoft.AF.PISystem.CheckServerError(dcServerError err)
   at OSIsoft.AF.PISystem.RemoteGetCheckOutInfo(AFDatabase database, Boolean allUsers)
   at OSIsoft.AF.PISystem.get_HasItemsCheckedOutToMe()
   at AFExplorer.frmAFExplorer.ApplyPendingChanges() in c:\Foundation\Clients\AFExplorer\frmAFExplorer.cs:line 591

Press OK to ignore error and continue, or Cancel to return to editing.
```

```
System.Data.SqlClient.SqlException: An error has occurred while
establishing a connection to the server. When connecting to SQL
Server 2005, this failure may be caused by the fact that under the
default settings SQL Server does not allow remote connections.
(provider: Named Pipes Provider, error: 40 - Could not open a
connection to SQL Server).
```

Try the following:

- Verify that the SQL Server database engine service is running.
- Verify that remote communication is enabled.
- Verify that the protocol is enabled.

Replication Won’t Complete Waiting on a (Good) SyncStatus

If you install a PI AF collective on a SQL Server cluster, you must give the SQL Server login created for the AFServers domain group access to the PIFD_distribution database created during PI AF collective creation. See *Configure Distributor Database Security* (page 70) for details.

If the AFServers domain group does not have the db_AFServer role for the PIFD_distribution database, the collective creation will fail and display the following messages continuously in the PI AF Creation wizard:

```
The collective <name of collective> was created successfully.
The replication has started on the collective member <name of
member>. This action can take some time to complete. Waiting on a
(Good) SyncStatus .. Current SyncStatus(Snapshot Not Ready).
```

Index