

PI WebParts 2013

Administrator 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

PI WebParts 2013 Administrator Guide

© 2006-2015 by OSIsoft, LLC. All rights reserved.

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

OSIsoft, the OSIsoft logo and logotype, PI Analytics, PI ProcessBook, PI DataLink, ProcessPoint, PI Asset Framework (PI AF), IT Monitor, MCN Health Monitor, PI System, PI ActiveView, PI ACE, PI AlarmView, PI BatchView, PI Coresight, PI Data Services, PI Event Frames, PI Manual Logger, PI ProfileView, PI Web API, PI WebParts, ProTRAQ, RLINK, RtAnalytics, RtBaseline, RtPortal, RtPM, RtReports and RtWebParts are all trademarks of OSIsoft, LLC. All other trademarks or trade names used herein are the property of their respective owners.

U.S. GOVERNMENT RIGHTS

Use, duplication or disclosure by the U.S. Government is subject to restrictions set forth in the OSIsoft, LLC license agreement and as provided in DFARS 227.7202, DFARS 252.227-7013, FAR 12.212, FAR 52.227, as applicable. OSIsoft, LLC.

Version: 4.0.3

Published: 11 August 2015

Contents

Introduction 1
About this guide 1
Roles of PI WebParts administrators 1
PI WebParts 2013 release 2
PI WebParts 2013 architecture 3
System requirements 5
SharePoint server requirements 5
PI WebParts Services requirements 5
Client requirements 6

PI WebParts installation 9
Preinstallation checklist 9
SharePoint upgrade 11
Verify that SharePoint is running 11
SQL Server permissions for SharePoint 11
PI Server and PI AF data access 11
Configure application-pool identity for PI WebParts Services 12
Requirements for identity authentication in a PI WebParts installation 14
Start the Windows service for claims on the SharePoint server 15
Install PI WebParts 16
Install PI WebParts solution 16
Deploy PI WebParts solution to SharePoint web applications 19
Activate the PI WebParts Configuration feature for desired SharePoint web applications 20
Install PI WebParts Services 20
Configure SharePoint web applications for PI WebParts 22
Activate PI WebParts as a site-collection feature 25
Postinstallation checklist 25
Test the PI WebParts installation 26
PI WebParts Administration website access 27
Set PI WebParts user-interface language 27
Install PI WebParts service pack 28
Update PI WebParts solution 28
Upgrade PI WebParts Services 30

Security 33
Secure PI Server access 33
PI trusts 34
Windows-integrated security requirements 34
Required access permissions 35
Enable access to remote data files 35
Firewall security 36
IIS security 36
SharePoint security 37
Secure Sockets Layer (SSL) 37

Maintenance 39
Performance tuning 39
Custom performance counters 40

Sample counters....41
Windows performance counters....41
PI point performance monitors....41
HTTP compression....41
Log files....42
Version information....42
Troubleshooting....43
Upgrades of PI WebParts....43
Repairs of PI WebParts....43
Enable PI WebParts in a new SharePoint web application....43
Backups and restoration....44
SharePoint content and configuration databases....44
PI WebParts configuration data....45
Migrate PI WebParts configuration data....46
Point PI WebParts to an existing Module Database....47
Backups and restoration of SharePoint servers....48
Removal of PI WebParts....48
Deactivate PI WebParts as a SharePoint site-collection feature....48
Retract and remove the PI WebParts solution from SharePoint....48
Uninstall PI WebParts Services....49

PI WebParts Administration website....51
Presentation configurations....51
Manage table configurations....52
Manage PI Trend and PI XYPlot configurations....61
Manage PI Messenger contacts configurations....63
Remove a PI WebParts configuration....66
Data sources....66
PI Server data sources....67
Relational data sources....69
Web-service data sources....81
PI Asset Framework support....86
Data sets....86
PI calculation data sets....87
Relational data sets....92
Web-service data sets....97
Delete a data set....106

Advanced topics....107
MDB to PI AF migration....107
Network load-balanced web servers....107
Windows Network Load Balancing (NLB)....108
Network interface card (NIC) configuration for NLB....108
Affinity filtering mode setting....108
URL conversion....108
Exceptions to URL conversion....110
Trusts for internal URLs....110

Configuration of Kerberos delegation....111
Prerequisites for Kerberos delegation....111
Verify that user accounts can use Kerberos delegation....112
Configure Kerberos delegation for SharePoint server....112
Configure a domain account to delegate to PI WebParts Services....113

Configure a local account to delegate to PI WebParts Services.... 113
Configure Kerberos delegation for PI WebParts Services 114
Configure a domain account to delegate to PI Server.... 114
Configure a local account to delegate to PI Server.... 115
Data-source configuration for Kerberos.... 115
Establish service principal names (SPNs) for application-pool accounts.... 116
Websites accessed with host headers 117
Remote-file access with Kerberos delegation.... 118
Troubleshooting.... 118
Verify Kerberos configuration on client computer.... 118
Verify Kerberos configuration on web server.... 118

Configuration of certificates.... 121
Configure certificates for claims-mode sites.... 121
Make PI WebParts Services aware of the SharePoint certificate.... 121
Prepare the PI WebParts Services certificate.... 122
Update the PI WebParts Services configuration file to support certificates.... 122
Make SharePoint aware of the PI WebParts Services certificate.... 123

PI WebParts custom performance counters.... 125

Technical support and other resources.... 133

Introduction

PI WebParts is a web-based application that allows users to build and share views of data for reporting and analysis. With PI WebParts, users with no HTML development skills can build web pages that contain dynamic data. PI WebParts can access both PI System and non-PI System data through configurable data-source connections.

PI WebParts uses Microsoft's SharePoint(R) technology, a centralized portal environment, to store customized views and provide administrative functionality for web-part sites and pages. Administrators can use SharePoint tools to manage site settings, grant user privileges, and secure content within sites.

Topics in this section

- About this guide
  This guide contains administrative information for PI WebParts.
- Roles of PI WebParts administrators
  PI WebParts administrators plan, install, configure, maintain, and monitor the application.
- PI WebParts 2013 release
  PI WebParts 2013 introduces some key changes.
- PI WebParts 2013 architecture
  PI WebParts 2013 requires a SharePoint server and the PI WebParts Services application server.
- System requirements
  PI WebParts requires specific software on one or more computers.

About this guide

This guide describes the administrative tasks to build and maintain a PI WebParts installation, including installation of PI WebParts Services and the PI WebParts solution, configuration, security models, management procedures, and basic troubleshooting techniques.

PI WebParts requires installation and management of a Microsoft IIS web server and SharePoint. This guide discusses these applications with regard to PI WebParts and PI WebParts Services, but this guide does not include comprehensive information about Microsoft applications. Consult your SharePoint and IIS documentation for further information.

Roles of PI WebParts administrators

PI WebParts administrators install the application and complete the following tasks:

- Planning
  - Determine system requirements for directory entries and volume space
  - Plan for future requirements, integration, upgrades, and system build-outs
- Configuration

    - Implement directories and security
    - Set up access to PI Servers and other data sources
    - Customize the application (with the company logo, custom style sheets, and custom icons)
- Maintenance
    - Remove unused and outdated files
    - Update the user list
    - Plan and coordinate server maintenance
    - Install and upgrade server software
    - Manage day-to-day operations and availability of the application
- Monitoring
    - Track network performance and resource consumption
    - Allocate user registration and usage (observing software licensing terms)
    - Provide management reports on application usage

PI WebParts 2013 release

Key changes introduced in PI WebParts 2013 include:

- Support for SharePoint 2013 in addition to SharePoint 2010; this includes support for claims-based authentication.
- New architecture for SharePoint deployment. By using a SharePoint solution package, PI WebParts follows a standardized installation approach, which supports large and small SharePoint web farms.
- Independent application server, called PI WebParts Services. PI WebParts Services manages connections with any PI Server and PI AF server to provide data access. You can install PI WebParts Services on the same SharePoint server as PI WebParts or on a different server computer. The installation flexibility lets you satisfy security requirements at your organization and lets you use a scalable and sustainable infrastructure.
- Support for additional browsers. You can view PI WebParts pages in Internet Explorer and Mozilla Firefox. If using SharePoint 2013, you can also view PI WebParts pages in Google Chrome.
- Support for native SVG rendering. If you use a browser that provides native support to render SVG, certain configurations do not require the Adobe SVG Viewer plug-in.
- New search-based user interface to locate and select PI points, PI AF elements, and PI AF attributes when configuring web parts.
- New page feature in the PI TreeView web part that supports large PI AF structures.

PI WebParts 2013 architecture

PI WebParts 2013 requires a SharePoint server, where you deploy the PI WebParts solution, and an application server, called PI WebParts Services, which manages all communication with the PI System.

To install PI WebParts, you must install two features:

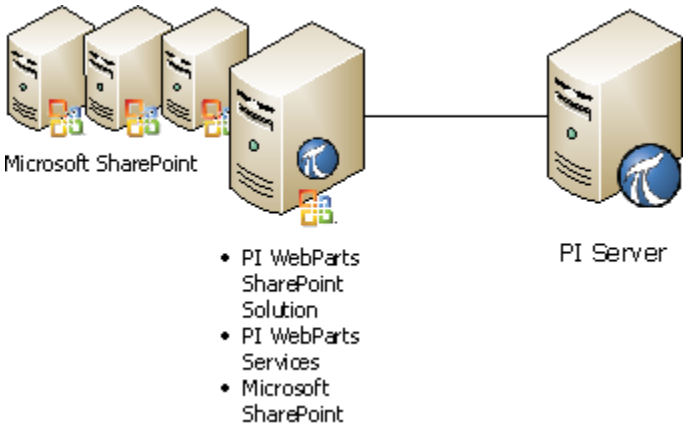
- **PI WebParts SharePoint solution**

  You must add the PI WebParts SharePoint solution to your SharePoint server. After you add the solution, you must deploy the solution through SharePoint Central Administration. If the SharePoint server is part of a farm, you can deploy the solution throughout the farm.

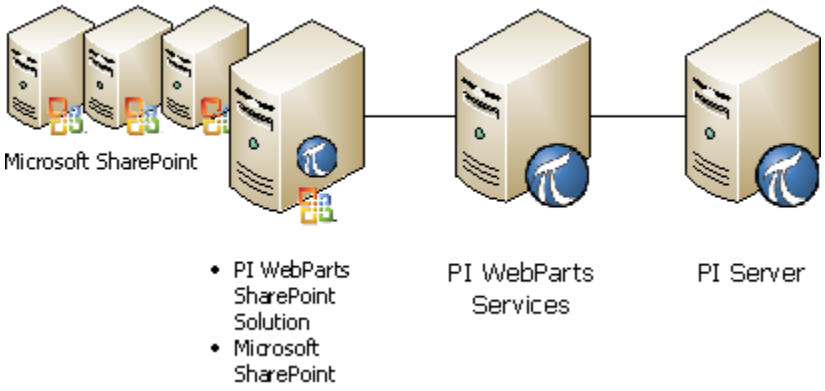
- **PI WebParts Services**

  PI WebParts Services is a single, dedicated application server that supports all the SharePoint servers in a farm. PI WebParts Services requires a non-SharePoint website. PI WebParts Services contains the data-access components needed to connect and retrieve data from your PI Server and PI AF server. These components include PI SDK, PI AF SDK, and PI OLEDB Enterprise.

You can install PI WebParts Services on the same computer as the SharePoint server or on a different computer. You might install on a different computer due to security requirements or to support scalability. PI WebParts Services can support a single independent SharePoint server or a single SharePoint farm. If you have a SharePoint farm, a single application server can provide data access for multiple websites in that farm. PI WebParts Services uses a centrally located data cache for all web servers, preventing frequent calls to PI Server.



Installation of PI WebParts Services on same computer as SharePoint



Installation of PI WebParts Services on a different computer from SharePoint

PI WebParts 2013 supports SharePoint claims-based authentication. In SharePoint 2010, sites can use either classic mode or claims mode. In SharePoint 2013, sites must use claims mode. In classic mode, SharePoint uses Windows authentication to convey identity information when communicating with PI WebParts Services; in claims mode, SharePoint uses certificates to convey identity information. You can choose not to use certificates with claims-mode sites, but this is less secure and is not recommended. PI WebParts installation requirements and procedures differ for claims-mode and classic-mode sites.

PI WebParts Services requires an application-pool identity that has read privileges to any data that users might access. SharePoint application-pool identities do not require that access.

PI Server or PI AF must authenticate the users who make data requests. In most configurations, PI WebParts tracks individual identities and provides access to appropriate data and files. For an initial request from a user, PI WebParts passes the user's Windows login account information to PI WebParts Services, which impersonates that user. PI WebParts Services passes that user's account information to PI Server or PI AF. PI Server invokes the appropriate PI mapping or PI trust for that account, and provides PI WebParts Services with the appropriate data access for that user. Similarly, PI AF provides the appropriate data access for the user account. For subsequent data requests, PI WebParts Services passes the application-pool identity to PI Server or PI AF for authentication. PI WebParts Services keeps track of which users can see which data.

With some configurations, however, PI WebParts does not track individual identities. In these configurations, PI WebParts provides all users access to the PI System data, the SharePoint files, or both based on the privileges of the application-pool identity.

PI WebParts and PI WebParts Services store configuration information in PI Module Database. During installation, you designate the PI Server that stores the PI Module Database for this configuration data. PI WebParts stores configuration data in the RtWebParts module, and PI WebParts Services stores configuration data in the RtBaseline module.

System requirements

PI WebParts requires software installation on one or more computers, and potentially on web client workstations, depending on the planned implementation.

Topics in this section

- SharePoint server requirements
  Before installation, PI WebParts requires specific software on the SharePoint server.
- PI WebParts Services requirements
  Before you install PI WebParts Services, the computer requires specific software.
- Client requirements
  Before using PI WebParts or features of some web parts, client workstations require specific software.

SharePoint server requirements

The Microsoft SharePoint server computer where you install the PI WebParts solution requires:

- 64-bit version of Microsoft Windows Server 2008 SP2, Windows Server 2008 R2, or Windows Server 2012
- Microsoft Internet Information Server (IIS) 6.0 or higher
- Microsoft SharePoint Foundation 2010, Microsoft SharePoint Server 2010, Microsoft SharePoint Foundation 2013, or Microsoft SharePoint Server 2013
- Microsoft .NET Framework (version 3.5 for SharePoint 2010 or version 4.5 for SharePoint 2013)
- A SharePoint web application containing at least one site collection

PI WebParts Services requirements

The computer where you install PI WebParts Services requires:

- 64-bit version of Microsoft Windows Server 2008 SP2, Windows Server 2008 R2, or Windows Server 2012
- Windows Communications Foundation
- Microsoft .NET Framework version 4.5
- Non-HTTP Activation feature (a .NET Framework 3.5.1 feature)

- Windows Identity Foundation (WIF) feature
- TCP Activation feature
- Microsoft Internet Information Server (IIS) 7.0 or higher
- Non-SharePoint website with a unique port number
- Access to PI Server version 3.4.380 or later

In addition, the following services must be started:

- Net.Tcp Listener Adapter
- Net.Tcp Port Sharing

Client requirements

Computers where users run PI WebParts require a supported browser:

- **Microsoft Internet Explorer 8 or later (32-bit versions only)**

  If you use SharePoint 2010 with any version of Internet Explorer or SharePoint 2013 with Internet Explorer 8, then you must install Adobe SVG Viewer to render graphics in the PI Graphic, PI Gauge, PI XYPlot, and PI Trend web parts. You can download this application from the Adobe SVG Viewer download area (http://www.adobe.com/devnet/svg/adobe-svg-viewer-download-area.edu.html). If you use SharePoint 2013 with Internet Explorer 9 or later, then you do not need Adobe SVG Viewer.

- **Firefox 16 or later**

  If you use Firefox, you cannot render web parts or features that rely on ActiveX controls: PI Messenger web part, PI ActiveView web part, the **Launch in PI ProcessBook** command of the PI Graphic web part, or the **Export to Excel** > **Open** command in any web part (though you can still save data to Excel file).

- **Google Chrome 24 or later**

  If you use Chrome, you cannot render web parts or features that rely on ActiveX controls: PI Messenger web part, PI ActiveView web part, the **Launch in PI ProcessBook** command of the PI Graphic web part, or the **Export to Excel** > **Open** command in any web part (though you can still save data to Excel file).

To support the features of some web parts, client workstations may require additional software:

- **PI ActiveView**

  To use the PI ActiveView web part, PI ActiveView 2.2 or higher must be installed on the client workstation. To view ERD displays created in PI ProcessBook 3.2, PI ActiveView 3.2 or higher is required. The PI ActiveView web part does not work in Firefox or Chrome.

- **PI ProcessBook**

  To use the **Launch in PI ProcessBook** command in the PI ActiveView or PI Graphic web parts, PI ProcessBook 3.0 or higher must be installed on the client workstation. This command does not work in Firefox or Chrome.

- **Microsoft Office and instant messaging software**

  To use the PI Messenger web part, Microsoft Office 2003 or higher and either Microsoft Lync, Microsoft Windows Messenger, Windows Live Messenger, Microsoft Office Communicator, or MSN Messenger must be installed on the client workstation. If either Microsoft Outlook XP or the separately-installed Outlook 2003 Address Book control is present, users can import IM contacts directly from the Outlook address book. The PI Messenger web part does not work in Firefox or Chrome.

- **Microsoft Excel**

  To use the **Export to Excel** > **Open** command in the PI BatchTable, PI Table, PI TimeSeries, PI Trend, or PI Values web parts, Microsoft Excel XP or higher must be installed on the client workstation. Remember that the Firefox and Chrome browsers do not support this command.



Note:
You must be an administrator on the client workstation to install the Adobe SVG Viewer or PI ActiveView.

PI WebParts installation

Use the PI WebParts setup program to install the PI WebParts SharePoint solution and PI WebParts Services. You must install the PI WebParts SharePoint solution on the computer where SharePoint is installed. You can install PI WebParts Services on the same computer as the PI WebParts solution or you can install PI WebParts Services on a separate computer.

PI WebParts 2013 cannot coexist with earlier versions of RtWebParts and PI WebParts. However, PI WebParts 2013 can coexist with earlier versions of RtBaselineServices and PI Data Services. Therefore, you can install PI WebParts 2013 with other PI System applications that require those components, such as PI Web Services.

After you install the PI WebParts solution, you must prepare your SharePoint web applications for PI WebParts. For each SharePoint web application from which you want to use PI WebParts, deploy the PI WebParts solution to the application and activate the PI WebParts Configuration feature for the application. After you install PI WebParts Services, you must configure SharePoint to use PI WebParts Services. To uninstall PI WebParts, see Removal of PI WebParts.

If you already have PI WebParts 2013 installed and you want to upgrade to the latest service pack, then follow the procedure to install the PI WebParts service pack. You must update the PI WebParts solution, upgrade PI WebParts Services, and activate the PI WebParts Configuration feature for any SharePoint web applications from which you want to use PI WebParts.

For an overview of installation choices, see PI WebParts 2013 architecture.

Topics in this section

- Preinstallation checklist
  Before you run the PI WebParts setup program, you must verify that your system is ready.
- Install PI WebParts
  Run the PI WebParts setup program and then configure SharePoint.
- Postinstallation checklist
  After you install PI WebParts, you should test the installation, limit administration access, prepare client workstations, and install the language pack.
- Install PI WebParts service pack
  If you previously installed PI WebParts 2013, upgrade to the latest service pack by updating the PI WebParts SharePoint solution and upgrading PI WebParts Services.

Preinstallation checklist

Before you install PI WebParts, verify the following:

- The computer where you will install the PI WebParts SharePoint solution meets the SharePoint server requirements (see SharePoint server requirements).
- Any upgrades to SharePoint are installed and a SharePoint web application with at least one site collection is running.
- You are logged in through a Windows domain user account with Administrator privileges on the SharePoint server.

- The computer where you will install PI WebParts Services meets the PI WebParts Services server requirements (see PI WebParts Services requirements).
- A non-SharePoint website with a unique port number is available for PI WebParts Services. This website must be available and running on the computer where you install PI WebParts Services. Though you can use the default website available with IIS, you might find a site with a more meaningful name helpful. You can create a site with Internet Information Services (IIS) Manager.

  When installing PI WebParts Services, the setup program enables the net.tcp protocol for this website with a binding to TCP port 808. The website requires a unique binding. To use a different binding for this website, enable the net.tcp protocol with your preferred binding before running the setup program. You need to know the binding port when you configure SharePoint to use PI WebParts Services.
- A PI Module Database is available to store configuration information for PI WebParts Services and PI WebParts. If you are upgrading from a previous version, you can use the same PI Module Database to store this information.
- The PI WebParts Services application-pool identity has read access to the RtWebParts module in the PI Module Database, which stores the PI WebParts configuration data for PI WebParts.

  Use PI System Management Tools (PI SMT) to grant permissions.
- All PI WebParts users, including the application-pool identity for PI WebParts Services, have read access to PI points and attributes in PI Server and to PI AF elements and attributes.
- The SharePoint server and PI WebParts Services are configured to support authentication, as necessary. This might include configuration of certificates and configuration of Kerberos delegation. See Requirements for identity authentication in a PI WebParts installation.
- The Windows service for claims is running and set to start automatically if you use claims-mode sites (the default mode in SharePoint 2013). See Start the Windows service for claims on the SharePoint server.

Topics in this section

- SharePoint upgrade
  Follow Microsoft instructions to upgrade SharePoint.
- Verify that SharePoint is running
  Connect to a SharePoint site to verify that SharePoint is running.
- SQL Server permissions for SharePoint
  See Microsoft documentation for information on SQL Server permissions required for SharePoint.
- PI Server and PI AF data access
  PI WebParts users require access to specific data in PI Server and PI AF.
- Configure application-pool identity for PI WebParts Services
  Find and set the application-pool identity and then create a PI mapping or PI trust for that identity.

- Requirements for identity authentication in a PI WebParts installation
  To authenticate identities and ensure secure access between SharePoint and PI System, a PI WebParts installation might require you to enable Kerberos delegation and to install and properly reference certificates.
- Start the Windows service for claims on the SharePoint server
  On the SharePoint server, set the Windows service, Claims to Windows Token Service, to start automatically.

SharePoint upgrade

If you are upgrading your SharePoint platform, follow the instructions from Microsoft to do so. Upgrade SharePoint first, and then install PI WebParts.

Verify that SharePoint is running

Before you install PI WebParts, you must verify that a SharePoint web application containing at least one site collection is running.

Procedure

1. Connect to the SharePoint site by the machine or site name.

   For example, you might connect using the host name: `http://ServerName/`.

2. If the SharePoint site does not load, check that there is a working SharePoint site for the desired URL.

   If necessary, verify that the SharePoint site has been extended to add SharePoint functionality to a particular website.

SQL Server permissions for SharePoint

Refer to Microsoft documentation regarding SQL Server permissions required for SharePoint:

- Plan for administrative and service accounts (SharePoint Foundation 2010) (http://technet.microsoft.com/en-us/library/cc288210.aspx)
- Account permissions and security settings (SharePoint Server 2010) (http://technet.microsoft.com/en-us/library/cc678863(v=office.14).aspx)
- Account permissions and security settings in SharePoint 2013 (http://technet.microsoft.com/en-us/library/cc678863.aspx)

PI Server and PI AF data access

PI WebParts users require access to specific data in PI Server and PI AF. To grant PI Server access, use PI System Management Tools (SMT). For example, you might create a PI mapping that links one or more Windows accounts to a PI identity, which you give the necessary access.

You must grant PI WebParts users, including the application-pool identity for PI WebParts Services, the following access:

- Read access to the configuration modules in PI Module Database (by default, RtWebParts and RtBaseline). The RtWebParts module stores configuration data for PI WebParts, and the

RtBaseline module stores configuration data for PI WebParts Services. Read access allows users to connect to data sources, access data sets, and configure web-part displays.

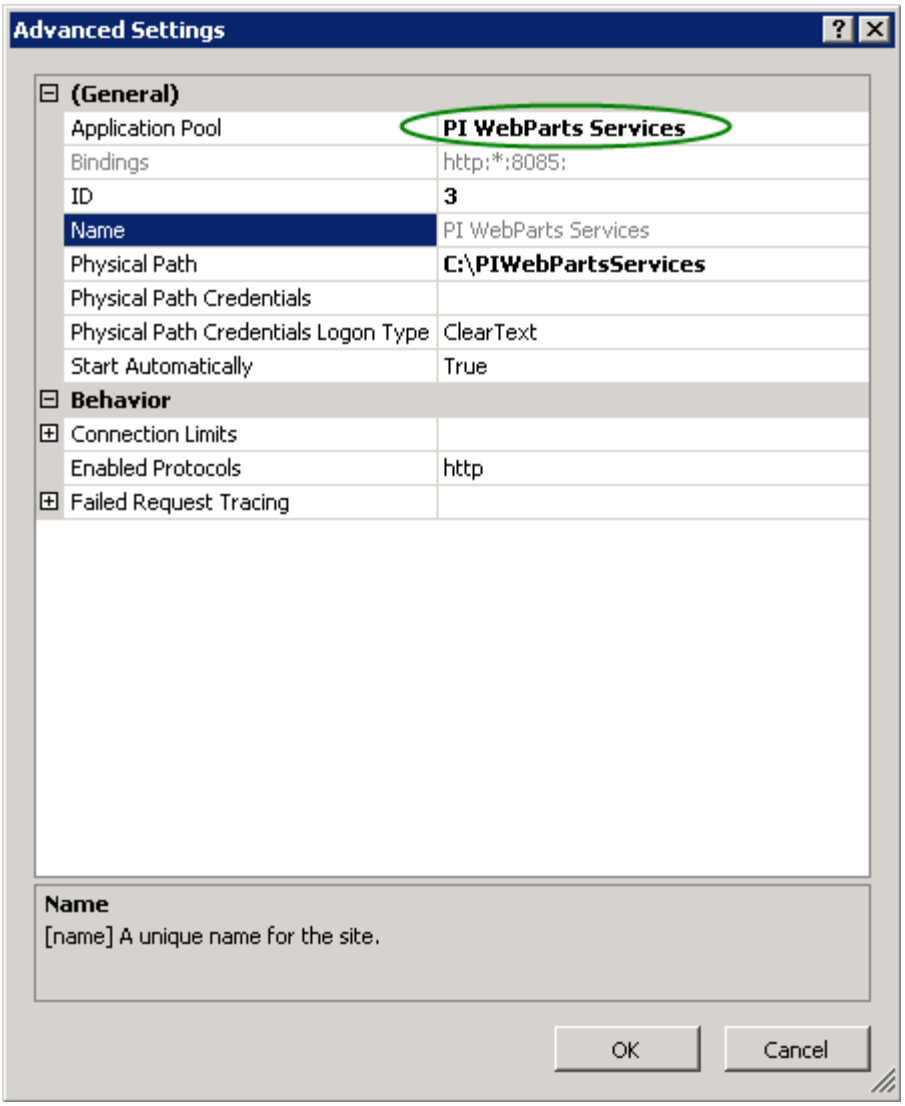
- Read access to any PI AF servers that PI WebParts uses to search for and display PI AF attribute data and that the PI TreeView web part uses.
- Read access to point security and data security for any PI points that PI WebParts accesses.

Configure application-pool identity for PI WebParts Services

Use Internet Information Services (IIS) Manager on the PI WebParts Services computer to set the application-pool identity that PI WebParts Services uses to authenticate with PI Server and PI AF. You can use a built-in or a custom account. OSIsoft recommends that you use a custom account and create a Windows Active Directory (AD) user configured as a service account to serve as a secure account for the application pool.

Procedure

1. Find the application pool for the PI WebParts Services website:
   a. Click **Start** > **Administrative Tools** > **Internet Information Services (IIS) Manager**.
   b. In the **Connections** pane, expand the server that contains the site, and then expand **Sites** to list the configured sites.
   c. Right-click the PI WebParts Services site, and then click **Manage Web Site** > **Advanced Settings**.
   d. Note the application pool configured to run the site's application.



e. Click **Cancel**.

2. Set the application-pool identity:

   a. In the **Connections** pane, under the website server, click **Application Pools**.

   b. From the **Application Pools** list, right-click the application pool of the PI WebParts Services site, and then click **Advanced Settings**.

   c. In the Advanced Settings window, under **Process Model**, click the **Identity** field, and then click the browse button ... to open the Application Pool Identity window, which shows the account.

   d. Specify the desired account for the PI WebParts Services application pool:

- To use a system account, select **Built-in account**, and then select the account.
- To use a custom account, select **Custom account**, and then click **Set** to enter the account credentials.

e. Click **OK**.

3. Create a PI mapping that gives this application-pool identity read access to all PI points and PI point attributes and to any configuration paths that PI WebParts might request. Alternatively, you might create a PI trust, though this less secure method is not recommended.

Application-pool identity	PI Server security options
Built-in account	◦ PI mapping (recommended) for the predefined security principal ◦ PI trust (not recommended) for the w3wp.exe application running from the IP address of the PI WebParts Services computer
Custom account with a specified user name and password	◦ PI mapping (recommended) for the AD user or a PI trust for that user name ◦ PI trust (not recommended) for the w3wp.exe application running from the IP address of the PI WebParts Services computer

For additional information, see the Microsoft SharePoint documentation regarding the administrative and service accounts required for an initial SharePoint deployment (http://technet.microsoft.com/en-us/library/ee662513.aspx).

Requirements for identity authentication in a PI WebParts installation

Certificates and Kerberos let software components authenticate identities. To ensure secure access between SharePoint and PI System, you might need to configure certificates or configure Kerberos delegation on one or more servers in your PI WebParts installation.

The following table shows where you must configure certificates or configure Kerberos delegation. The requirement depends on the installation architecture, the method PI Server uses to authenticate PI WebParts Services, and the type of SharePoint site.

Kerberos and certificate requirements for various installation architectures

Architecture	PI Server authentication method	Type of SharePoint site	Configuration requirement
PI WebParts Services and SharePoint server on same computer	Windows integrated security (recommended)	Classic mode	• Kerberos delegation for PI WebParts Services
		Claims mode	• Kerberos delegation for PI WebParts Services
	PI trusts (not recommended)	Classic mode	None
		Claims mode	None

Architecture	PI Server authentication method	Type of SharePoint site	Configuration requirement
PI WebParts Services and SharePoint server on different computers	Windows integrated security (recommended)	Classic mode	• Kerberos delegation for SharePoint server • Kerberos delegation for PI WebParts Services
		Claims mode	Option 1 (Kerberos): • Kerberos delegation for SharePoint server • Kerberos delegation for PI WebParts Services Option 2 (certificates): • Kerberos delegation for PI WebParts Services • Certificates on SharePoint server and PI WebParts Services
	PI trusts (not recommended)	Classic mode	• Kerberos delegation for SharePoint server
		Claims mode	Option 1 (Kerberos): • Kerberos delegation for SharePoint server Option 2 (certificates): • Certificates on SharePoint server and PI WebParts Services

For information about how to configure Kerberos delegation, see Configuration of Kerberos delegation.

For information about how to configure certificates, see Configuration of certificates.

Start the Windows service for claims on the SharePoint server

To support claims-mode sites, the Windows service, Claims to Windows Token Service, must be running. On the SharePoint server, set this service to start automatically.

Procedure

1. Use the Services administrative tool to set the service **Startup Type** property to **Automatic**.
2. Use the Services on Server page of SharePoint Central Administration to verify that the service has started.

Install PI WebParts

To install PI WebParts, you need to install the PI WebParts SharePoint solution and PI WebParts Services, and then configure SharePoint.

Before you start

Determine the architecture for your deployment and verify the preinstallation checklist.

Procedure

1. Install PI WebParts solution.

   Run the setup program to install the PI WebParts SharePoint solution on a computer with SharePoint installed. You can install PI WebParts Services, too.

2. Deploy PI WebParts solution to SharePoint web applications.

   Use SharePoint Central Administration to deploy the installed PI WebParts SharePoint solution to SharePoint web applications.

3. Activate the PI WebParts Configuration feature for desired SharePoint web applications

   Use SharePoint Central Administration to activate the PI WebParts Configuration feature for any SharePoint web application from which you want to use PI WebParts.

4. Install PI WebParts Services.

   Run the setup program to install PI WebParts Services, if not yet installed.

5. Configure SharePoint web applications for PI WebParts.

   Use SharePoint Central Administration to activate the configuration feature for the administration application and to enter the settings SharePoint needs to integrate PI WebParts.

6. Activate PI WebParts as a site-collection feature.

   After you activate PI WebParts as a SharePoint site-collection feature, PI WebParts appears in the web-part gallery and users can place them on pages.

Install PI WebParts solution

Run the PI WebParts setup program to install the PI WebParts SharePoint solution on a computer with SharePoint installed. During setup, you can install PI WebParts Services on the same computer. Alternatively, you can run the PI WebParts setup program separately to install PI WebParts Services on this computer or another computer.



Tip:
To install the PI WebParts SharePoint solution, the setup program must restart IIS. Therefore, run the setup program at a convenient time to restart IIS.

Before you start

See Preinstallation checklist.

Procedure

1. Start the setup program:

- Start the setup program automatically from the self-extraction program.
- Download the files from the self-extraction program to a particular directory and then run the `SetupDispatcher.exe` file to start the setup program.

The setup program searches the computer for SharePoint and for any earlier versions of PI WebParts, and then opens the appropriate window.

2. If the setup program detects versions of PI WebParts earlier than PI WebParts 2013, uninstall the associated items:

To:	Complete these steps:
Uninstall automatically	a. Click **Uninstall**. The setup program removes the detected items and writes messages that show its progress. A message indicates when the process is complete. b. Click **Continue**.
Uninstall manually	a. Click **Cancel** to close the setup program. b. Manually remove the detected items. You can use the `Cleanup_Actions.txt` file that the setup program writes in the directory that contains the extracted setup kit. This file contains commands needed to remove the detected items. c. Restart the setup program after you remove the detected items.

3. At the prompt, select the features to install:
   - Select the **PI WebParts SharePoint solution** check box to add the PI WebParts solution to SharePoint on this computer.

     This check box is disabled if the PI WebParts SharePoint solution was already installed on this computer.
   - Select the **PI WebParts Services** check box to install PI WebParts Services on this computer.

     The requirements for certificates and Kerberos delegation differ if you install PI WebParts Services on the same computer where you deploy the PI WebParts SharePoint solution or a different computer. See Requirements for identity authentication in a PI WebParts installation for more information.
4. Click **Continue**.
5. At the prompt, click **Restart IIS Now** to have the setup program restart IIS.

   You must restart IIS when installing the PI WebParts solution. If necessary, postpone the installation until you can restart IIS.
6. Select a method to deploy the PI WebParts solution in SharePoint.

   The setup program can automatically deploy the PI WebParts solution to the default content web application (SharePoint - 80) and configure SharePoint to use PI WebParts Services. Alternatively, you can deploy the solution with SharePoint Central Administration.
   - Click **Automatic configuration** to have the setup program deploy the solution to SharePoint - 80.

The setup program will attempt to schedule a timer job to deploy the solution.

- Click **Manual configuration** to configure with SharePoint Central Administration later.

7. Click **Next** to install the selected features.
8. If you chose to install PI WebParts Services, follow the prompts to install the necessary components.
   a. Follow the prompts to install the components required on your computer to support PI WebParts Services.

      Required components that might be installed prior to PI WebParts Services include:

      - OSIsoft MS Runtime Redistributables
      - PI Software Development Kit (PI SDK)
      - PI Software Development Kit 64-bit (PI SDK)
      - PI Buffer Subsystem
      - PI AF Client 2014
      - PI OLEDB Enterprise
      - PI OLEDB Enterprise x86
      - PI OLEDB 2013 R3

      At any prompts regarding files in use, click **Retry** or **Ignore**.

   b. Follow the prompts to install PI WebParts Services. In particular note:

      - On the IIS Web Site page, select a *non-SharePoint website* for PI WebParts Services.

        If the website has no net.tcp binding defined, the setup program enables the net.tcp protocol for the website with a binding to TCP port 808. You need to know the binding port when you configure SharePoint to use PI WebParts Services.

      - On the PI Data Archive for Module Database page, identify which PI Data Archive (that is, PI Server) stores the PI Module Database to use for PI WebParts and PI WebParts Services configuration. Enter the computer that hosts this PI Data Archive (PI Server).
      - On the SharePoint Server or Farm page, enter information about the SharePoint server or farm that this instance of PI WebParts Services supports. Specifically, select the protocol for the URL to the SharePoint security token service, the host name of the independent SharePoint server or the name of the SharePoint farm, and the port used to access the security token service.

      Note:
      If you must restart your server during installation of PI WebParts Services, then you need to rerun the `SetupDispatcher.exe` file after restarting the server to complete the installation. In this case, the setup program cannot automatically deploy the PI WebParts solution to the default content web application. Regardless of your original selection, you must follow the steps to manually deploy the PI WebParts solution, activate the PI WebParts Configuration feature for desired SharePoint web applications, configure SharePoint web applications for PI WebParts, and activate PI WebParts as a SharePoint site-collection feature.

9. When the setup progress shows that PI WebParts setup is done, click **Continue**.

Deploy PI WebParts solution to SharePoint web applications

After you install the PI WebParts SharePoint solution, you must deploy the solution to the SharePoint web applications in which you want to use PI WebParts. If the setup program successfully deployed the solution to SharePoint - 80 and that is the only application in which you want to use PI WebParts, then you can skip this procedure. If the setup program created a timer job to deploy the solution but your server does not have the timer service enabled, you must manually run the timer jobs (see Run SharePoint timer jobs).

Procedure

1. Open the Solution Management page in the SharePoint Central Administration site.

To open from:	Then:
PI WebParts setup program	Click **Continue to SharePoint** from the last page in the PI WebParts setup program.
SharePoint Central Administration site	a. On the **Central Administration** navigation pane, click **System Settings**. b. Under **Farm Management**, click **Manage farm solutions**.

2. On the Solution Management page, click **pi webparts_2013.wsp**.
3. On the Solution Properties page, click **Deploy Solution**.
4. On the Deploy Solution page, from the **Choose a Web application to deploy this solution** list, select the application in which you want to use PI WebParts.

   You can select **All content Web applications** to deploy the solution to all currently installed applications.
5. Click **OK** to deploy the solution to the selected application.

   After you deploy the solution to an application, you must activate the PI WebParts Configuration feature for the application before you can use PI WebParts in that application.
6. Repeat steps 2 through 5 for each application in which you want to use PI WebParts.

After you finish

Activate the PI WebParts Configuration feature for desired SharePoint web applications.

Run SharePoint timer jobs

If the setup program created a timer job to deploy the PI WebParts solution to SharePoint, your SharePoint server must have the timer service enabled to run that timer job. If the service is not enabled, you can use the **`stsadm.exe`** command to run the timer jobs manually.

Procedure

1. At a command prompt, go to the directory that stores the executable:

- In SharePoint 2010, `Program Files\Common Files\Microsoft Shared\web server extensions\14\bin`
- In SharePoint 2013, `Program Files\Common Files\Microsoft Shared\web server extensions\15\bin`

2. Type the following command: `stsadm.exe -o execadmsvcjobs`.

   SharePoint runs the timer job that the setup program created to deploy the PI WebParts solution.

Activate the PI WebParts Configuration feature for desired SharePoint web applications

To use PI WebParts in a SharePoint web application, you must first activate the PI WebParts Configuration feature for that application.

Procedure

1. In the **Central Administration** navigation pane of SharePoint Central Administration, click **Application Management**.
2. On the Application Management page, under **Web Applications**, click **Manage web applications**.
3. For each application from which you want to use PI WebParts, activate the PI WebParts Configuration feature:
   a. From the list of applications, select the SharePoint web application from which you want to use PI WebParts.
   b. On the **Web Applications** tab, in the **Manage** group, click **Manage Features**.
   c. In the Manage Web Application Features window, in the **PI WebParts Configuration** row, click **Activate**. If the feature is already active, then you must deactivate the feature and then activate the feature.
   d. When the **Status** column shows **Active** in the **PI WebParts Configuration** row, click **OK** to close the window.

Install PI WebParts Services

Run the PI WebParts setup program to install PI WebParts Services. You can install PI WebParts Services on the same computer with SharePoint server or on a different computer. If you installed PI WebParts Services at the same time that you installed the PI WebParts solution on SharePoint, you can skip this procedure.

Before you start

Check PI WebParts Services requirements.

Procedure

1. Start the setup program:
   - Start the setup program automatically from the self-extraction program.
   - Download the files from the self-extraction program to a particular directory and then run the `SetupDispatcher.exe` file to start the setup program.

The setup program searches the computer for SharePoint and for any earlier versions of PI WebParts, and then opens the appropriate window.

2. If the setup program detects versions of PI WebParts earlier than PI WebParts 2013, uninstall the associated items:

To:	Complete these steps:
Uninstall automatically	a. Click **Uninstall**. The setup program removes the detected items and writes messages that show its progress. A message indicates when the process is complete. b. Click **Continue**.
Uninstall manually	a. Click **Cancel** to close the setup program. b. Manually remove the detected items. You can use the `Cleanup_Actions.txt` file that the setup program writes in the directory that contains the extracted setup kit. This file contains commands needed to remove the detected items. c. Restart the setup program after you remove the detected items.

3. If SharePoint is installed on your computer, select the PI WebParts feature to install:
   a. Select the **PI WebParts Services** check box to install PI WebParts Services on this computer.
   b. Click **Continue** to launch the PI WebParts Services setup program.
4. Follow the prompts to install the components required on your computer to support PI WebParts Services.

   Required components that might be installed prior to PI WebParts Services include:

   - OSIsoft MS Runtime Redistributables
   - PI Software Development Kit (PI SDK)
   - PI Software Development Kit 64-bit (PI SDK)
   - PI Buffer Subsystem
   - PI AF Client 2014
   - PI OLEDB Enterprise
   - PI OLEDB Enterprise x86
   - PI OLEDB 2013 R3

   At any prompts regarding files in use, click **Retry** or **Ignore**.
5. Follow the prompts to install PI WebParts Services. In particular note:
   - On the IIS Web Site page, select a *non-SharePoint website* for PI WebParts Services.

If the website has no net.tcp binding defined, the setup program enables the net.tcp protocol for the website with a binding to TCP port 808. You need to know the binding port when you configure SharePoint to use PI WebParts Services.

- On the PI Data Archive for Module Database page, identify which PI Data Archive (that is, PI Server) stores the PI Module Database to use for PI WebParts and PI WebParts Services configuration. Enter the computer that hosts this PI Data Archive (PI Server).
- On the SharePoint Server or Farm page, enter information about the SharePoint server or farm that this instance of PI WebParts Services supports. Specifically, select the protocol for the URL to the SharePoint security token service, the host name of the independent SharePoint server or the name of the SharePoint farm, and the port used to access the security token service.

6. When the setup progress shows that the PI WebParts Services setup is done, click **Continue**.
7. After PI WebParts Services successfully installed, click **Continue to SharePoint** to configure SharePoint to use PI WebParts Services.

Configure SharePoint web applications for PI WebParts

Use SharePoint Central Administration to configure SharePoint web applications for PI WebParts. You can skip this procedure if all of the following conditions are true:

- You installed the PI WebParts solution and PI WebParts Services on the same computer at the same time.
- You used automatic configuration and the setup program successfully deployed the solution to SharePoint - 80.
- You will only use PI WebParts in the SharePoint - 80 application.
- The PI WebParts Services application-pool identity is not a domain user name.

Before you start

- Install PI WebParts Services.
- Deploy PI WebParts solution to SharePoint web applications.

Procedure

1. Activate the PI WebParts Configuration feature for the SharePoint administration application.

   Use SharePoint Central Administration to activate the PI WebParts Configuration feature for the SharePoint administration application.

2. Enter settings that each SharePoint web application needs for PI WebParts.

   For each SharePoint web application that will use PI WebParts, use the PI WebParts Configuration page in SharePoint to enter settings that the application needs to integrate PI WebParts.

After you finish

Activate PI WebParts as a site-collection feature.

Activate the PI WebParts Configuration feature for the SharePoint administration application

To configure SharePoint to use PI WebParts Services, you must first activate the PI WebParts Configuration feature for the SharePoint administration application. You only need to activate this feature once for the SharePoint administration application.

Procedure

1. In the **Central Administration** navigation pane of SharePoint Central Administration, click **Application Management**.
2. On the Application Management page, under **Web Applications**, click **Manage web applications**.
3. From the list of applications, select **SharePoint Central Administration v4**.
4. On the **Web Applications** tab, in the **Manage** group, click **Manage Features**.
5. In the Manage Web Application Features window, in the **PI WebParts Configuration** row, click **Activate**.
6. When the **Status** column shows **Active** in the **PI WebParts Configuration** row, click **OK** to close the window.

After you finish

Enter settings that each SharePoint web application needs for PI WebParts.

Enter settings that each SharePoint web application needs for PI WebParts

For each SharePoint web application that will use PI WebParts, enter the settings that the application needs to integrate PI WebParts. These settings control access to PI WebParts Services, authentication of PI WebParts Services, and the identities used for file access on the PI WebParts site and PI System data access. Enter these settings on the PI WebParts Configuration page in SharePoint.

Before you start

- Activate the PI WebParts Configuration feature for the SharePoint administration application.
- Configure certificates or Kerberos delegation, as required. See Requirements for identity authentication in a PI WebParts installation.
- Activate the PI WebParts Configuration feature for desired SharePoint web applications.

Procedure

1. Open the PI WebParts Configuration page in SharePoint:

a. In the **Central Administration** navigation pane, click **Configuration Wizards**.

b. On the Configuration Wizards page, click **PI WebParts Configuration**.

2. From the **Web application that hosts PI WebParts** list, select the SharePoint web application that you want to configure for PI WebParts.

   The list contains SharePoint web applications for which you have activated the PI WebParts Configuration feature. The configuration on this page controls how the selected SharePoint web application accesses PI WebParts Services.

3. Set the URL that the SharePoint web application uses to contact PI WebParts Services:

   a. In the **PI WebParts Services URL** field, type the URL for the PI WebParts Services website that you specified during installation. Specify the URL using the net.tcp protocol.

      For example, you might specify `net.tcp://ServerName:NNN` where *ServerName* is the fully qualified domain name and *NNN* is the net.tcp site binding configured for the website (808 by default).

   b. Click **Test** to verify. A green check mark indicates that the URL is valid.

4. If you specified a claims-mode SharePoint web application, then configure how the application uses identities for file access and for authentication with PI WebParts Services:

   a. If you installed PI WebParts Services and the SharePoint server on different computers, select the **Use certificates for claims-mode sites** check box to use certificates.

      With this configuration, the SharePoint server can impersonate users during the authentication process with PI WebParts Services. With impersonation, returned PI System data is based on the privileges of the impersonated logged-on user. This is the most secure mode of operation. Remember that you must also configure the certificates. Without this configuration, all users will have access to the same data.

   b. Select the **Impersonate users on a SharePoint server for claims-mode sites** check box to have PI WebParts impersonate users.

      With this configuration, any PI WebParts website grants access to files based on the privileges of the impersonated logged-on user. In addition, if you installed PI WebParts Services and the SharePoint server on the same server, this configuration lets the SharePoint server impersonate users during authentication with PI WebParts Services. Without this configuration, the PI WebParts website grants access to files based on the privileges of the SharePoint application-pool identity.

5. Specify the identity that the SharePoint web application uses to authenticate PI WebParts Services:

   a. From the **Identity type** list, select the type of identity that PI WebParts Services uses to communicate with SharePoint.

   b. In the **Valid identity** field, enter the name of the valid identity.

   c. If the identity is a domain name, click **Test** to verify that the entered identity is valid. A green check mark indicates a valid identity; a red X indicates an invalid identity.

   To verify communication from PI WebParts Services, SharePoint will authenticate the specified identity.

   For example, from the **Identity type** list, select **Service Principal Name**, and then set **Valid identity** to a valid service principal name for the PI WebParts Services application-pool account, such as `HTTP/appserver` where *appsever* is the PI WebParts Services computer.

6. In the **Domain name** field, enter the SharePoint farm member that PI WebParts Services should use to access the SharePoint security token service.

   The deployment process for the PI WebParts solution sets this field to an available SharePoint server. You can designate a different server that hosts the security token service.

7. Click **Done**.

Activate PI WebParts as a site-collection feature

From each SharePoint web application, you must activate PI WebParts as a SharePoint site-collection feature to show PI WebParts in the web-part gallery and place them on new web-part pages.

Procedure

1. Log on as an administrator to the SharePoint site.
2. From the Home page for the site collection (the parent site), go to the Site Settings page:
   - In SharePoint 2010, click **Site Actions** > **Site Settings**.
   - In SharePoint 2013, click **Settings** and then click **Site settings**.
3. Under **Site Collection Administration**, click **Site collection features**.
4. On the Features page, in the **OSIsoft PI WebParts** row, click **Activate**.

PI WebParts as a SharePoint site-collection feature

Administrators can regulate access to SharePoint web applications and components configured as site-collection features. Activated features are available to users with matching permissions. Deactivated features are effectively switched off until they are re-activated.

When the PI WebParts site-collection feature is activated, the web parts are added to the Team Site gallery. When the PI WebParts site-collection feature is deactivated, the web parts no longer appear in the web-part gallery and cannot be placed on new web part pages. Pages that use PI WebParts and that are created before the feature is deactivated continue to function properly.

The setup program does not activate PI WebParts as a site-collection feature. If you add additional site collections to the web application to which PI WebParts was installed, you need to explicitly activate the PI WebParts site-collection feature before it is available for use within the new site collection. If you do not see PI WebParts in the list of web parts available to a page, it is possible that the PI WebParts site-collection feature has been deactivated.

Postinstallation checklist

After you install PI WebParts:

- Test the PI WebParts installation.
- Limit access to the PI WebParts Administration website.

- Install appropriate software and reasonable browser security levels on client workstations.
- Install the MUI (multilingual user interface) language pack to view the PI WebParts interface in alternate languages.

Topics in this section

- Test the PI WebParts installation
  On the SharePoint site, add a PI Trend web part to verify that PI WebParts works properly.
- PI WebParts Administration website access
  You can limit the default access everyone gets to the PI WebParts Administration pages.
- Set PI WebParts user-interface language
  To view the PI WebParts user interface in alternate languages, install the PI WebParts MUI and configure the site or browser.

Test the PI WebParts installation

After you install PI WebParts and PI WebParts Services, you can verify that your PI WebParts installation is operational.

Procedure

1. In your browser, go to the SharePoint site on the computer where you installed PI WebParts.
2. Enable the editing tools:
   - In SharePoint 2010, click **Site Actions** > **Edit Page**
   - In SharePoint 2013, click **Settings** and then click **Edit page**
3. On the **Insert** tab, click the **Web Part** button.
4. Add a PI Trend web part to the page:
   a. Under **Categories**, click **PI WebParts**.
   b. Under **Web Parts** (SharePoint 2010) or **Parts** (SharePoint 2013), click **PI Trend**.
   c. Click **Add.**

   If necessary, a prompt will ask you to download Adobe SVG Viewer.
5. Click the **PI Trend Web Part Menu** arrow at the top right corner of the web part and then click **Edit Web Part**.

   The page adds the **PI Trend** tool pane on the far right side of the page (you might need to scroll).
6. Specify the data to show in the trend:
   a. Under **Selected Data**, click **Select PI Data** to open the Select PI Data window.
   b. In the path at the top of the window, set the search scope to your PI Server.
   c. In the **Search text** field, type text to identify a PI point, and then click **Search** .

      For example, you might type `sinusoid`. You can include an asterisk (*) as a wildcard for multiple characters but you must enter at least one non-wildcard character.

The Search Results pane shows the PI points that match the entered search criteria.

If you receive an error message, check the PI mapping or the PI trust on the PI Server to ensure that proper access privileges are configured. You can also check the PI Data Sources page in the PI WebParts Administration website to ensure that the PI Server is accessible, or verify your search criteria.

d. Click a point in the Search Results pane and click **Add Selected** to add to the Selected Items pane.

e. In the path at the top of the window, set the search scope to a PI AF server and database.

f. In the **Search text** field, type text to identify a PI AF attribute, and then click **Search** .

g. Click an attribute in the Search Results pane and click **Add Selected** to add to the Selected Items pane.

h. Click **OK** to use the selected data items in your trend.

7. In the PI Trend tool pane, click **Apply** to show the configured trend data in the web part.

PI WebParts Administration website access

The default configuration gives everyone access to the PI WebParts Administration pages. You can restrict access by creating a Windows group, named RtWebPartsAdmin. If this group exists, only users in this group can access the PI WebParts Administration pages.

Any user with access to the PI WebParts Administration pages still requires appropriate privileges to edit the configuration database, such as to create data sources, data sets, table formats, or configuration settings. Therefore, these users require read and write access to the RtWebParts and RtBaseline modules in PI Module Database.

Installation type	URL to PI WebParts Administration website
Non-farm, on SharePoint - 80	`http://server/_layouts/PI_WebParts/admin.aspx`
SharePoint farm	`http://loadbalancer/_layouts/PI_WebParts/admin.aspx` where *loadbalancer* is the name of the computer that runs the load balancer for the SharePoint farm

Set PI WebParts user-interface language

To enable users to view the PI WebParts interface in any of the supported languages, you must install the PI WebParts MUI (multilingual user interface) language pack and then set the language. Depending on the version of SharePoint, you either set the language when creating the site or by changing the browser's language.

Procedure

1. Download the PI WebParts MUI language pack from the OSIsoft Tech Support Downloads page (https://techsupport.osisoft.com/Downloads/All-Downloads/).
2. Install the PI WebParts MUI language pack.
3. Set the language for the PI WebParts user interface:

- In SharePoint 2010, set the site language when creating the site.
- In SharePoint 2013, set the browser language in each client browser before loading the site.

Supported languages

With the PI WebParts MUI language pack installed, you can view the PI WebParts user interface in the following languages:

- French
- German
- Japanese
- Korean
- Portuguese
- Russian
- Simplified Chinese
- Spanish

Install PI WebParts service pack

Follow this procedure if you previously installed PI WebParts 2013 and you want to upgrade to the latest service pack of PI WebParts 2013.

Before you start

Review your PI WebParts deployment. You must know where you installed the PI WebParts solution and where you installed PI WebParts Services.

Procedure

1. Update PI WebParts solution.
   Run the setup program to install the service pack that updates the PI WebParts SharePoint solution.
2. Upgrade PI WebParts Services.
   Run the setup program to install the service pack for PI WebParts Services, if not yet installed.

Update PI WebParts solution

To migrate from an earlier version of PI WebParts 2013 to the latest service pack, run the PI WebParts setup program to install the service pack on the computer with the PI WebParts 2013 SharePoint solution installed. If PI WebParts Services is installed on the same computer, the setup program can install the service pack for PI WebParts Services during the same session. Alternatively, you can run the PI WebParts setup program separately to install the service pack for PI WebParts Services.



Tip:
To update the PI WebParts SharePoint solution, the setup program must restart IIS. Therefore, run the setup program at a convenient time to restart IIS.

Procedure

1. Start the setup program:
   - Start the setup program automatically from the self-extraction program.
   - Download the files from the self-extraction program to a particular directory and then run the `SetupDispatcher.exe` file to start the setup program.

   The setup program searches the computer for SharePoint and for any earlier versions of PI WebParts, and then opens the appropriate window.
2. At the prompt, select the features to install:
   - Select the **PI WebParts SharePoint solution** check box to update the PI WebParts solution in SharePoint on this computer.

     This check box is disabled if the PI WebParts SharePoint solution was already updated on this computer.
   - Select the **PI WebParts Services** check box to upgrade PI WebParts Services on this computer.

     If you update a PI WebParts SharePoint solution to the latest service pack, then you must also upgrade the PI WebParts Services instance that this solution uses.
3. Click **Continue**.
4. At the prompt, click **Restart IIS Now** to have the setup program restart IIS.

   You must restart IIS when upgrading the PI WebParts solution. If necessary, postpone the upgrade until you can restart IIS.
5. If you chose to upgrade PI WebParts Services, follow the prompts to install the necessary components.
   a. Follow the prompts to install the components required on your computer to support PI WebParts Services.

      Required components that might be installed prior to PI WebParts Services include:
      - OSIsoft MS Runtime Redistributables
      - PI Software Development Kit (PI SDK)
      - PI Software Development Kit 64-bit (PI SDK)
      - PI Buffer Subsystem
      - PI AF Client 2014
      - PI OLEDB Enterprise
      - PI OLEDB Enterprise x86
      - PI OLEDB 2013 R3

      At any prompts regarding files in use, click **Retry** or **Ignore**.

   b. Follow the prompts to install PI WebParts Services. In particular note:

- On the IIS Web Site page, select a *non-SharePoint website* for PI WebParts Services.

  If the website has no net.tcp binding defined, the setup program enables the net.tcp protocol for the website with a binding to TCP port 808. You need to know the binding port when you configure SharePoint to use PI WebParts Services.
- On the PI Data Archive for Module Database page, identify which PI Data Archive (that is, PI Server) stores the PI Module Database to use for PI WebParts and PI WebParts Services configuration. Enter the computer that hosts this PI Data Archive (PI Server).
- On the SharePoint Server or Farm page, enter information about the SharePoint server or farm that this instance of PI WebParts Services supports. Specifically, select the protocol for the URL to the SharePoint security token service, the host name of the independent SharePoint server or the name of the SharePoint farm, and the port used to access the security token service.



Note:
If you must restart your server during installation of PI WebParts Services, then you need to rerun the `SetupDispatcher.exe` file after restarting the server to complete the installation. In this case, the setup program cannot automatically deploy the PI WebParts solution to the default content web application. Regardless of your original selection, you must follow the steps to manually deploy the PI WebParts solution, configure SharePoint to use PI WebParts Services, and activate PI WebParts as a SharePoint site-collection feature.

6. When the setup progress shows that PI WebParts setup is done, click **Continue**.

Upgrade PI WebParts Services

To migrate from an earlier version of PI WebParts 2013 to the latest service pack, run the PI WebParts setup program to install the service pack for PI WebParts Services. If you installed the service pack for PI WebParts Services when you installed the service pack for the PI WebParts solution on SharePoint, then you can skip this procedure.

Procedure

1. Start the setup program:
   - Start the setup program automatically from the self-extraction program.
   - Download the files from the self-extraction program to a particular directory and then run the `SetupDispatcher.exe` file to start the setup program.

   The setup program searches the computer for SharePoint and for any earlier versions of PI WebParts, and then opens the appropriate window.
2. If SharePoint is installed on your computer, select the PI WebParts feature to install:
   a. Select the **PI WebParts Services** check box to upgrade PI WebParts Services on this computer.
   b. Click **Continue** to launch the PI WebParts Services setup program.
3. Follow the prompts to install the components required on your computer to support PI WebParts Services.

   Required components that might be installed prior to PI WebParts Services include:

- OSIsoft MS Runtime Redistributables
- PI Software Development Kit (PI SDK)
- PI Software Development Kit 64-bit (PI SDK)
- PI Buffer Subsystem
- PI AF Client 2014
- PI OLEDB Enterprise
- PI OLEDB Enterprise x86
- PI OLEDB 2013 R3

At any prompts regarding files in use, click **Retry** or **Ignore**.

4. Follow the prompts to install PI WebParts Services. In particular note:
   - On the IIS Web Site page, select a *non-SharePoint website* for PI WebParts Services.

     If the website has no net.tcp binding defined, the setup program enables the net.tcp protocol for the website with a binding to TCP port 808. You need to know the binding port when you configure SharePoint to use PI WebParts Services.
   - On the PI Data Archive for Module Database page, identify which PI Data Archive (that is, PI Server) stores the PI Module Database to use for PI WebParts and PI WebParts Services configuration. Enter the computer that hosts this PI Data Archive (PI Server).
   - On the SharePoint Server or Farm page, enter information about the SharePoint server or farm that this instance of PI WebParts Services supports. Specifically, select the protocol for the URL to the SharePoint security token service, the host name of the independent SharePoint server or the name of the SharePoint farm, and the port used to access the security token service.
5. When the setup progress shows that the PI WebParts Services setup is done, click **Continue**.
6. After the PI WebParts Services service pack successfully installed, click **Continue to SharePoint** to activate the PI WebParts Configuration feature for desired SharePoint web applications.

Security

Because PI WebParts is a web application, you can easily share information through a browser to distributed consumers. However, large numbers of users and access outside your organization increase the risk of unauthorized access to tools and data, and threatens the integrity of your PI System and networks.

Given the different application layers and technologies involved, you can provide security for your PI WebParts installation at more than one level:

- PI Server security governs access to PI Server data; PI AF server security governs access to PI AF data.
- Network security defends against unauthorized access from outside and to non-PI System data sources. Access to relational and web-service data is managed by data sources.
- IIS and SharePoint security, in combination with Windows network IDs provide user authentication and access to web-part pages.

This section provides security recommendations for typical PI WebParts deployments. While higher levels of security are possible, the measures suggested here provide data confidentiality, data integrity, and protection against unauthorized access without compromising the benefits of distributed access to PI WebParts.

Topics in this section

- Secure PI Server access
  To ensure secure access to PI Server, use Windows integrated security, introduced with PI Server 3.4.380.
- Required access permissions
  Set appropriate permissions to enable PI WebParts to access needed data.
- Firewall security
  Configure your firewalls to restrict external access to PI WebParts.
- IIS security
  OSIsoft recommends using integrated Windows authentication for SharePoint installations. The RtWebPartsAdmin group controls access to the PI WebParts Administration website.
- SharePoint security
  SharePoint has a role-based security model.

Secure PI Server access

PI Server 3.4.380 introduced a Windows integrated security model that allows you to manage your PI Server authentication through Windows and Microsoft Active Directory (AD). This model improves PI Server security, reduces your management workload, and provides users a single sign-on experience. On PI Server, Windows integrated security gives you more control over authentication policies and access permissions, and provides Windows account traceability in logs and audit-trail records.

Earlier versions of PI Server only allowed you to set access permissions on an object for a specified owner and group. PI Server 3.4.380 and later allow you to set access permissions for any PI identity, PI user, or PI group.

OSIsoft recommends that you use Windows integrated security.

Use the PI SMT Mappings & Trusts tool to create and edit PI trusts and PI mappings on your PI Server. Typically, you create trusts to authenticate PI interfaces, and you create mappings to enable single sign-on for Windows users on your PI Server.

PI SMT includes tools to help you manage PI Server security. You can download PI SMT from the OSIsoft Technical Support website (http://techsupport.osisoft.com/).

See the *Configuring PI Server Security* guide for more information.

Topics in this section

- PI trusts
  Use PI trusts to access versions of PI Server prior to 3.4.380.
- Windows-integrated security requirements
  Windows integrated security provides secure access to PI Server but requires specific configuration.

PI trusts

PI clients that access older versions of PI Server (versions prior to 3.4.380) must use PI trusts to provide access to pre-approved network entities. To access any PI Server version 3.4.380 or later, OSIsoft recommends that you use PI mappings, rather than PI trusts.

To use PI trusts with PI WebParts, you must establish PI trusts that grant:

- Users read access to any PI Server data displayed in web-part pages
- Administrators (who will create, update, and delete configuration data) write access to the configuration module database, that is the `%OSI` module in the MDB .

For PI WebParts, trusts allow a PI Server to store configuration information and support data flow between clients and server. With a trust, users can access PI System resources based on their IP address, Windows login account, or application; they do not need to enter a user name and password each time they connect. All requests from your SharePoint server come from the same computer and application. This means that all requests have the same IP information and application information. If you need permissions to vary by user, you must create trusts that include Windows account information.

You do not need to fill in every property field. Trust properties are additive, and the more detail you provide, the more restrictive the trust becomes. When applying trusts, the PI Server will always apply the most restrictive trust that is applicable.

To create and configure PI trusts, use the Mappings & Trusts tool in PI SMT. In versions of PI SMT before 3.2.1.3, this tool was called the Trusts tool. You can download the latest version of PI SMT from the OSIsoft Technical Support website (http://techsupport.osisoft.com).

Windows-integrated security requirements

To use Windows integrated security to provide secure access between PI WebParts and PI Server:

- All user IDs and the PI WebParts Services application-pool identity must be valid Active Directory IDs.
- Each Active Directory ID must have a PI mapping that links the Active Directory ID to the appropriate PI identity. The assigned mapping must grant:
  - PI WebParts Services read access to all data that will be displayed with PI WebParts and to the PI Module Database that contains configuration data.
  - End users read access to all the data displayed in the web-part pages that they will view, and write access to the PI Module Database that contains configuration data. Write access lets users create, modify, and delete data sources, data sets, and PI WebParts configurations.
  - Administrative users write access to configuration data (in the PI Module Database) that they will want to create or update.

  You can create PI mappings with PI System Management Tools (PI SMT) 3.3.1.3 or higher. OSIsoft recommends that you map the Active Directory IDs to different PI identities.

  You can set Module Database permissions in the PIModules table with the PI SMT Database Security tool.
- Kerberos delegation must be configured between PI WebParts Services and PI Server.

Required access permissions

You must set appropriate permissions to enable PI WebParts Services to access appropriate data and files.

PI AF server permissions

See the *PI System Explorer 2012 User Guide* for information on managing access to PI AF elements and attributes.

PI Server and PI Module Database permissions

See the *Configuring PI Server Security* guide for information about accessing data in any PI Server.

Folder and registry permissions

The `PIPC\PIWebPartServices\PI Data Services\Temp` directory requires full control for end users and the application-pool identity.

For additional information, see Microsoft's documentation about SharePoint files and permissions.

Remote data files

Configure anonymous access for remote shares to enable users to enter file paths directly in web-part tool panes.

Enable access to remote data files

Users may access data sources stored on other computers, such as Microsoft Excel or Access files, provided these data sources are set up in PI WebParts. With anonymous access

configured for remote shares, users may enter a file path directly in the web-part tool pane. Users can also pass a file path as a parameter through a web-part connection.

Use the Local Security Policy administrative tool to enable access to remote data files. With this access, users can enter file paths to remote computers in web-part tool panes and pass a file path as a parameter in a web-part connection.

Procedure

1. On the PI WebParts Services computer, click **Start** > **Administrative Tools** > **Local Security Policy** to open the Local Security Policy window.
2. Under **Security Settings**, expand **Local Policies**.
3. Click **Security Options**.
4. From the list of policies, double-click **Network access: Let Everyone permissions apply to anonymous users**.
5. Click **Enabled**.

Firewall security

Firewalls protect a network from invasion by unauthorized users outside the LAN. Configure your firewalls to restrict external access to PI WebParts:

- Permit the passage of data on the port used for your SharePoint web application (typically port 80) and any other ports used for HTTP or HTTPS by your website. HTTPS and SSL are normally configured to use TCP port 443.
- Permit internal access from the SharePoint server to any data sources, such as to ports 1433 (the default for Microsoft SQL Server), 5450 (PI Server 3.x), and 1521 (Oracle SQL*Net).
- Permit internal access from the PI WebParts Services computer to ports 5457 and 5459 (PI AF server), 5450 (PI Server 3.x), and 1521 (Oracle SQL*Net). Clients initiate these connections; therefore, these ports must be open on the firewall to allow incoming TCP connections.

IIS security

IIS provides several types of user authentication, including anonymous, basic, integrated Windows, and .NET Passport. OSIsoft highly recommends integrated Windows authentication for SharePoint installations.

In the integrated mode, all website users have a Windows operating system account, and Windows integrated authentication identifies and authorizes users for login. The Windows group, RtWebPartsAdmin, controls access to pages on the PI WebParts Administration website. For new installations, you must create this group on the PI WebParts Services computer; for upgrades, this group already exists.

SharePoint security

SharePoint has its own role-based security model. This model offers user permissions and privileges that can be used to restrict access to web-part pages and the web parts on them.

SharePoint security provides a collection of four standard roles, which offer a reasonable trade-off between individual access rights and ease of management. If you have unique needs, SharePoint permits the creation and customization of user roles.

SharePoint 2010 introduced a claims-based authentication (CBA) option for creating new web applications. In SharePoint 2013, web applications use CBA by default. The PI System is not aware of claims. Therefore, on a CBA site, PI WebParts accesses PI System resources (and external resources) with the same level of privileges (those of the specified application-pool identity). However, on CBA sites with Windows authentication enabled, users can log in to the site with a Windows account, which gives each user a unique privilege level to access resources.

See the Microsoft SharePoint documentation for more information.

Secure Sockets Layer (SSL)

A SharePoint installation does not establish point-to-point transport-layer security by default. Most sites do not require it. You can, however, configure SSL to secure client-to-server communication.



Note:
SSL is especially recommended for web applications that use basic authentication.

Maintenance

Over time, you need to maintain your PI WebParts application. Maintenance tasks include upgrading hardware or software, monitoring performance, managing security, backing up the system, and removing unused websites and files to minimize disk usage.

This section describes common maintenance tasks for PI WebParts.

Topics in this section

- Performance tuning
  Analyze performance parameters to determine the performance of your PI WebParts application.
- Log files
  PI WebParts Services generates two installation log files useful for diagnosing problems.
- Version information
  Two administration web pages list the version information for all installed PI WebParts components.
- Troubleshooting
  To troubleshoot development environments, edit the `web.config` file to produce error messages with trace information.
- Upgrades of PI WebParts
  The PI WebParts setup program automatically detects prior versions of PI WebParts or RtWebParts, which must be removed.
- Repairs of PI WebParts
  The PI WebParts setup kit cannot repair a PI WebParts installation.
- Enable PI WebParts in a new SharePoint web application
  Complete necessary installation procedures to use PI WebParts in a SharePoint web application created after you installed PI WebParts.
- Backups and restoration
  Follow specific procedures to back up, restore, or migrate PI WebParts and Microsoft SharePoint sites.
- Removal of PI WebParts
  To remove PI WebParts, you must remove the PI WebParts solution and uninstall PI WebParts Services.

Performance tuning

You can analyze key performance parameters and identify the interrelationships among them to answer important performance questions about your PI WebParts application, such as:

- Is the server load increasing?
- Are unusual peaks in utilization occurring?

Topics in this section

- Custom performance counters
  Each web part has a set of common performance counters, which you can see in Performance Monitor under **RtWebParts**.
- Sample counters
  PI WebParts Services includes a set of sample performance counters, which you can see in Performance Monitor under **PI Data Services**.
- Windows performance counters
  Standard Windows Performance Monitor counters can provide insight into performance issues.
- PI point performance monitors
  You can use the Performance Counters tool in PI SMT to build PI points from Windows performance counters.
- HTTP compression
  IIS can compress information to reduce network traffic, but this places additional work on the server.

Custom performance counters

PI WebParts has a set of customer performance counters. You install these performance counters separately; the PI WebParts Services installation does not install these performance counters.

The custom performance counters include a set of common performance counters, such as "Update Last Call Secs" and "WebPart Last Call Usecs." A set exists for each web part. You can find these counters in Performance Monitor under **RtWebParts**. For a complete list, see PI WebParts custom performance counters.

If you uninstall PI WebParts Services, you remove the custom counters. If you created PI points to monitor the custom counters, you must manually remove these points from your PI Server.

Install PI WebParts custom performance counters

PI WebParts has a set of customer performance counters that you can install separately. The PI WebParts Services installation does not install these performance counters.

Before you start

Install PI WebParts Services.

Procedure

1. At a command prompt on the computer where you installed PI WebParts Services, type the following command:

   ```
   %windir%\Microsoft.NET\Framework64\v2.0.50727\installutil /AssemblyName
   "OSIsoft.PresentationServices.Instrumentation, Culture=neutral,
   PublicKeyToken=9312a10cb4e30d00, Version=4.0.0.0"
   ```

Sample counters

PI WebParts Services includes a set of sample performance counters, which sample the execution frequency of individual instructions. They store the number of sampling interrupts taken and are used as a denomination in the sampling fraction. For example, PI WebParts Services monitors Percent Cache Hit using a sample counter. You can find these counters in Performance Monitor under **PI Data Services**.

If you uninstall PI WebParts Services, you remove the sample counters.

Windows performance counters

Standard Windows Performance Monitor counters can also help provide insight into performance issues. These counters assist with routine monitoring of the web server and the associated software environment, and are organized by performance object. They should be used in conjunction with the custom performance counters. OSIsoft recommends that you monitor:

- General system performance to track the general health of the physical server computer during routine operation. For more information on general system performance counters, see the Microsoft TechNet article Windows Performance Counters (http://technet.microsoft.com/en-us/library/cc774901(WS.10).aspx).
- ASP.NET and the .NET platform performance counters to track the health of these systems upon which PI WebParts is built. For more information, see the Microsoft Developer Network article ASP.NET Performance Monitoring (http://msdn.microsoft.com/en-us/library/ms972959.aspx).
- PI System performance counters. For more information, see your PI Server documentation.

PI point performance monitors

You can view PI WebParts and standard Windows performance counters graphically by adding counters to the Windows Performance Monitor application. You can also use Performance Monitor to generate log files.

If you prefer to monitor performance counters along with other PI System data, you can use the PI SMT Performance Counters tool to build PI points from Windows performance counters. After you create PI points for desired counters, you can monitor the points continuously with web parts, such as PI Trend.

HTTP compression

Internet Information Server (IIS) can compress the information sent to web browsers. For certain web parts that make extensive use of `.svg` documents, such as PI Graphic and PI Trend, compression can reduce network traffic by over 80%.

Compression places additional load on the server, and is most appropriate for situations where high network latency or limited throughput are concerns, such as over a WAN. For more information, see the IIS article, IIS 7 Configuration Reference (http://www.iis.net/ConfigReference). For the configuration procedures, see the Microsoft article, Configuring

HTTP Compression in IIS 7 (http://technet.microsoft.com/en-us/library/cc771003(v=ws.10).aspx).

Log files

Use the installation log files to diagnose problems that occur immediately following installation. The PI WebParts Services installation generates two log files:

- **`OSIsoft PI WebParts ServicesMaster.log`**

  Contains information from the PI WebParts Services setup program, `setup.exe`. This file lists the status of each step of the installation process. After a successful installation, you can find this master log file in the `\PIPC\DAT` directory; otherwise, you can find the file in the root directory of the web server machine.

- **`SetupPIWPServicesInstaller.log`**

  Contains information from the PI WebParts Services installer, `PIWPServicesInstaller.msi`. You can find this file in the `\PIPC\DAT` directory.

When contacting OSIsoft technical support about an installation issue, zip and send these log files.

Version information

Two different web pages list the versions of software components installed to support PI WebParts:

- PI WebParts Version page lists:
  - Product release and version for all installed PI WebParts components
  - Supporting applications and versions installed

  You can access the PI WebParts Version page from the PI WebParts Administration website.

Installation type	URL to PI WebParts Administration website
Non-farm, on SharePoint - 80	`http://`*`server`*`/_layouts/PI_WebParts/admin.aspx`
SharePoint farm	`http://`*`loadbalancer`*`/_layouts/PI_WebParts/admin.aspx` where *loadbalancer* is the name of the computer that runs the load balancer for the SharePoint farm

- PI WebParts Services Version Information page lists the components and executables installed specifically to support PI WebParts Services.

  You can access this page from the website where you installed PI WebParts Services:

  `http://`*`server`*`:`*`NNNN`*`/PIWebPartsServices/AdminVersionInfo.aspx`

  where *server* is the server name and *NNNN* is the unique port number.

Troubleshooting

To debug errors, you might make the following changes to your SharePoint `web.config` file (typically located in the `\inetpub\wwwroot\wss\VirtualDirectories\`*`port_number`* subdirectory of your SharePoint installation directory):

- In the <system.web> tag, locate the <customErrors mode="On"> tag and change it to <customErrors mode="Off" />. This produces the ASP.NET exception when an error occurs rather than redirecting you to the error page, which provides less information.
- In the <SharePoint> tag, locate the <SafeMode MaxControls="50" CallStack="false"/> tag and change it to <SafeMode MaxControls="50" CallStack="true"/>. This causes the ASP.NET error message to list the stack trace information.

Note:
For security reasons, OSIsoft recommends these changes in development environments only. This information can contain sensitive data that is not suitable for a production environment.

Upgrades of PI WebParts

If you are upgrading an existing PI WebParts installation, the PI WebParts setup program automatically detects prior versions of PI WebParts or RtWebParts installed on your computer. Any versions other than PI WebParts 2013 must be removed before the installation can proceed. The setup program can do this automatically or you can do it manually. To upgrade from PI WebParts 2013, you must install the service pack. See Install PI WebParts service pack.

Note:
Before you upgrade to PI WebParts 2013, you must upgrade to SharePoint 2010 or SharePoint 2013.

Repairs of PI WebParts

The PI WebParts setup kit cannot repair a PI WebParts installation.

Enable PI WebParts in a new SharePoint web application

To use PI WebParts in a SharePoint web application that you created after you installed PI WebParts, you must complete some installation steps for the new application.

Procedure

1. Deploy the PI WebParts solution to the new SharePoint web application.

   Use SharePoint Central Administration to deploy the installed PI WebParts SharePoint solution to SharePoint web applications. See Deploy PI WebParts solution to SharePoint web applications.

2. Activate the PI WebParts Configuration feature for the new SharePoint web application.

Use SharePoint Central Administration to activate the PI WebParts Configuration feature for any SharePoint web application from which you want to use PI WebParts. See Activate the PI WebParts Configuration feature for desired SharePoint web applications.

3. Configure the new SharePoint web application for PI WebParts. Use SharePoint Central Administration to configure SharePoint web applications for PI WebParts. See Configure SharePoint web applications for PI WebParts.
4. Activate PI WebParts as a SharePoint site-collection feature in the new SharePoint web application.

   From the SharePoint site, activate PI WebParts as a SharePoint site-collection feature to show PI WebParts in the web-part gallery and place PI WebParts on site pages. See Activate PI WebParts as a site-collection feature

Backups and restoration

You must follow special procedures to back up, restore, or migrate SharePoint sites. The procedures differ slightly depending on whether you are working with an individual site or with an entire SharePoint portal that contains multiple sites. In either case, you must address two primary sources of application information when you complete backup, restore and/or migration procedures on a PI WebParts installation.



Note:
Comprehensive documentation on backing up SharePoint sites and databases is available from Microsoft. Please review this documentation thoroughly before developing and implementing your migration or backup strategy.

Topics in this section

- SharePoint content and configuration databases
  To preserve your website, back up the SQL Server databases that your SharePoint installation uses.
- PI WebParts configuration data
  PI WebParts stores configuration data in PI Module Database. You can back up and restore this data with PI Module Database Builder.
- Migrate PI WebParts configuration data
  Copy the branch of the Module Database to migrate PI WebParts configuration data from one PI Server to another PI Server.
- Point PI WebParts to an existing Module Database
  Modify the PI WebParts Services configuration file to change the Module Database that PI WebParts retrieves configuration data from.
- Backups and restoration of SharePoint servers
  Refer to Microsoft instructions to back up and restore your SharePoint data.

SharePoint content and configuration databases

To preserve the website structure and web-part pages created in SharePoint, you must back up the SQL Server databases used by your SharePoint installation. A Microsoft SQL Server database stores SharePoint page content and configuration information. Refer to Microsoft instructions for backing up your SharePoint data.

PI WebParts configuration data

PI WebParts stores configuration data in the PI Module Database specified during installation. Use PI Module Database Builder, a Microsoft Excel add-in distributed with PI SMT, to back up and restore configuration data for PI WebParts.

Topics in this section

- Back up configuration data
  Use PI Module Database Builder to back up the PI WebParts configuration data to an Excel worksheet.
- Restore configuration data
  Restore data from an Excel worksheet to your PI Module Database.

Back up configuration data

Use PI Module Database Builder to export PI WebParts Services configuration data and PI WebParts visual configuration data to an Excel worksheet, which you save for backup purposes.

Procedure

1. Open Microsoft Excel and install the PI Module Database Builder add-in, if necessary.

   You can find the add-in (`MDBBuilder.xla`) distributed with PI SMT in the `\PIPC \MDBBuilder` directory.
2. On the **Add-Ins** tab, click **PI-SMT** > **Module Database Builder** > **Connections** to open PI Connection Manager.
3. Select the check box next to the PI Server that stores the PI Module Database with the PI WebParts configuration information, and click **Close**.
4. Import the PI WebParts Services configuration data to the worksheet:
   a. On the **Add-Ins** tab, click **PI-SMT** > **Module Database Builder** > **Import Items** to open the Import Module Database Items window.
   b. Expand the module tree and select the **RtBaseline** module (***Server*** > **Modules** > **%OSI** > **ClientApps** > **RtBaseline**).
   c. Set the import settings to import the relevant data from the PI Module Database:
      - Select **Items From Selected Module**.
      - Select the **Include Sub Items** check box.
      - Select the **Modules**, **Properties**, and **Include Full Module Path** check boxes.
   d. If desired, select the **Import Directly To a File** check box and specify a file.
   e. Click **OK** to import the configuration data.
5. Save the Excel file as a backup file for PI WebParts Services data configuration.
6. Import the PI WebParts visual configuration data to the worksheet:

a. On the **Add-Ins** tab, click **PI-SMT** > **Module Database Builder** > **Import Items** to open the Import Module Database Items window.

b. Expand the module tree and select the **RtWebParts** module (***Server*** > **Modules** > **%OSI** > **ClientApps** > **RtWebParts**).

c. Set the import settings to import the relevant data from the PI Module Database:

- Select **Items From Selected Module**.
- Select the **Include Sub Items** check box.
- Select the **Modules**, **Properties**, and **Include Full Module Path** check boxes.

d. If desired, select the **Import Directly To a File** check box and specify a file.

e. Click **OK** to import the configuration data.

7. Save the Excel file as a backup file for PI WebParts visual configuration.

Restore configuration data

Use PI Module Database Builder to restore PI WebParts Services configuration data or PI WebParts visual configuration data from an Excel worksheet.

Procedure

1. In Excel, open the backup document that contains the configuration information you want to restore.
2. Select the rows in the document that you want to restore.
3. On the **Add-Ins** tab, click **PI-SMT** > **Module Database Builder** > **Export Items** to open the Export Module Database Items window.
4. From the list at the top of the window, select the PI Server that stores the PI Module Database.
5. From the **Mode** list, select the export mode, depending on whether you are editing an existing configuration or creating a new configuration.
6. Click **OK** to export to the Module Database.

Migrate PI WebParts configuration data

PI WebParts stores configuration data, including table and trend formats, data sources, and data sets, in a PI Module Database. Use this procedure to copy the configuration data from the PI Module Database of an existing PI Server to the PI Module Database of a new PI Server, and then set PI WebParts to use the copied data.



Note:
This procedure does not affect:

- PI Server connections available to PI WebParts. Refer to the Known Servers Table topic in the PI SDK manual for more information on migrating the list of PI Servers.
- PI Servers referenced in data sources or data sets.

Procedure

1. Open PI System Management Tools (SMT), version 3.1.2.1 or higher.
2. In the Collectives and Servers pane, select the check boxes next to the existing PI Server and the new PI Server.
3. In the System Management Tools pane, expand **Operation** and click **Module Database** to open the Module Database tool.
4. Copy the PI WebParts Services configuration from the existing PI Server to the new PI Server:
   a. In the Module Database tool, expand the module tree of the existing PI Server (***Existing server*** > **Modules** > **%OSI** > **ClientApps** > **RtBaseline**).
   b. Right-click the **RtBaseline** module and then click **Copy**.
   c. Expand the module tree for the new PI Server (***New server*** > **Modules** > **%OSI** > **ClientApps**).
   d. Right-click **ClientApps** and then click **Paste Hierarchy** to copy the PI WebParts Services configuration data to the new PI Server.
5. Copy the PI WebParts presentation configuration from the existing PI Server to the new PI Server:
   a. In the Module Database tool, expand the module tree of the existing PI Server (***Existing server*** > **Modules** > **%OSI** > **ClientApps** > **RtWebParts**).
   b. Right-click the **RtWebParts** module and then click **Copy**.
   c. Expand the module tree for the new PI Server (***New server*** > **Modules** > **%OSI** > **ClientApps**).
   d. Right-click **ClientApps** and then click **Paste Hierarchy** to copy the PI WebParts presentation configuration to the new PI Server.
6. Configure PI WebParts to use the new PI Server for configuration:
   a. Open the `web.config` configuration file on the PI WebParts Services computer. You can find the file in the `PIWebPartsServices` subdirectory of the installation directory (usually the `Program Files\PIPC` directory).
   b. Locate the `RtBaselineConfigModule` key and change the server name to the new PI Server to reflect the new path of the RtBaseline configuration module.
   c. Locate the `RtWebPartsConfigModule` key and change the server name to the new PI Server to reflect the new path of the RtWebParts configuration module.
   d. Save the `web.config` file.

Point PI WebParts to an existing Module Database

PI WebParts stores configuration data, including table and trend formats, data sources, and data sets, in a PI Module Database. Use this procedure to configure PI WebParts to use the existing configuration data in the PI Module Database of a connected PI Server. By pointing to that PI Server, you can use the configuration data without copying that data.

When installing PI WebParts Services, you can point to the existing Module Database. Otherwise, use the following procedure to point to an existing Module Database.

Procedure

1. Open the `web.config` configuration file on the PI WebParts Services computer. You can find the file in the `PIWebPartsServices` subdirectory of the installation directory (usually the `Program Files\PIPC` directory).
2. Locate the `RtWebPartsConfigModule` and `RtBaselineConfigModule` keys and change the server name portion of the corresponding values to the new PI Server to reflect the new paths of the PI WebParts configuration modules.

Backups and restoration of SharePoint servers

Refer to Microsoft instructions to back up and restore your SharePoint data.

Removal of PI WebParts

To remove PI WebParts, retract and remove the PI WebParts solution from SharePoint and uninstall PI WebParts Services. These procedures do not remove:

- PI WebParts configuration information stored in PI Module Database
- Web part pages, SharePoint document libraries, SharePoint sites created with or for PI WebParts, and PI WebParts log files
- Components that PI WebParts Services installed, such as PI SDK

Deactivate PI WebParts as a SharePoint site-collection feature

You must deactivate PI WebParts as a SharePoint site-collection feature before you retract and remove the PI WebParts solution from SharePoint.

Procedure

1. Log on the SharePoint site as an administrator.
2. On the Home page for the site collection (the parent site), click **Site Actions** > **Site Settings**.
3. Under **Site Collection Administration**, click **Site collection features**.
4. On the Features page, in the **OSIsoft PI WebParts** row, click **Deactivate**.
5. On the Warning page, click **Deactivate this feature**.

Retract and remove the PI WebParts solution from SharePoint

Use the SharePoint Central Administration site to retract and remove the PI WebParts solution from SharePoint. Any web-part pages, SharePoint document libraries, SharePoint sites created with or for PI WebParts, and log files will remain on the system after you complete this procedure.

Before you start

Deactivate PI WebParts as a SharePoint site-collection feature.

Procedure

1. On the Central Administration navigation pane, click **System Settings**.
2. Under **Farm Management**, click **Manage farm solutions**.
3. On the Solution Management page, click **pi webparts_2013.wsp**.
4. On the Solution Properties page, click **Retract Solution**.
5. On the Retract Solution page, click **OK**.

   SharePoint schedules a timer job to retract the solution.
6. If the timer service is not enabled on your SharePoint server, use the **`stsadm.exe`** command to run the timer job manually:
   a. At a command prompt, go to the directory that stores the executable:
      - In SharePoint 2010, `Program Files\Common Files\Microsoft Shared\web server extensions\14\bin`
      - In SharePoint 2013, `Program Files\Common Files\Microsoft Shared\web server extensions\15\bin`

   b. Type the following command: `stsadm.exe -o execadmsvcjobs`.
7. On the Solution Properties page for the pi webparts_2013.wsp solution, click **Remove Solution** to remove the PI WebParts solution from SharePoint.

Uninstall PI WebParts Services

Use the Program and Features tool in Control Panel to remove PI WebParts Services from a computer. When you remove PI WebParts Services, you do not remove internal components installed with PI WebParts Services, such as PI AF Client, PI OLEDB Enterprise, and PI SDK. You can remove those separately, if desired. Similarly, this procedure does not remove the PI WebParts configuration information stored in PI Module Database.

Procedure

1. In Control Panel, click **Programs and Features**.
2. From the list of installed programs, select **PI WebParts Services**, and click **Uninstall**.
3. At the confirmation prompt, click **Yes**.

Results

Windows uninstalls PI WebParts Services.

PI WebParts Administration website

This section describes the PI WebParts Administration website. Use this website to:

- Create and manage presentation configurations that visualize data in a web part. PI WebParts users can apply these configurations to matching web parts when building a web-part page.
- Configure and connect to available data sources. You can connect to PI Server, PI AF server, relational database, and web-service data sources.
- Create data sets from configured data sources. You can create data sets from PI calculation data, relational queries, and web-service queries.

The URL to access the PI WebParts Administration website depends on your installation type:

Installation type	URL to PI WebParts Administration website
Non-farm, on SharePoint - 80	`http://server/_layouts/PI_WebParts/admin.aspx`
SharePoint farm	`http://loadbalancer/_layouts/PI_WebParts/admin.aspx` where *loadbalancer* is the name of the computer that runs the load balancer for the SharePoint farm



Note:
In some installations, you must be a member of the `RTWebPartsAdmin` group to access the site. To edit the configuration database through the site, users require read and write access to the RtWebParts and RtBaseline modules in PI Module Database.

Topics in this section

- Presentation configurations
  Build template configurations for web parts to standardize their appearance and capabilities.
- Data sources
  Configure connections to data sources available in your PI System environment.
- Data sets
  Create data sets from configured data sources.

Presentation configurations

This section discusses management of web-part presentation configurations with the PI Web Parts Administration website.

You can create configurations for the PI Trend, PI XYPlot, and PI Messenger web parts, as well as any tabular web parts. In a configuration, you can apply custom formatting or create interactive features to visualize data in the web part. After you create a configuration, you can apply that configuration to matching web parts when building a web-part page.

Topics in this section

- Manage table configurations
  Design formatting templates for tabular display web parts.

- Manage PI Trend and PI XYPlot configurations
  Design formatting templates for PI Trend and PI XYPlot web parts.
- Manage PI Messenger contacts configurations
  Design contact templates for PI Messenger web parts.
- Remove a PI WebParts configuration
  Delete obsolete configurations from the administration pages.

Manage table configurations

You can create data set-specific templates to customize the display of columnar data in the PI Table, PI TimeSeries, and PI Values web parts. Configurations created in the PI WebParts Administration website are available to these web parts as behavior settings.

Procedure

1. Go to the PI WebParts Administration website:

Installation type	URL to PI WebParts Administration website
Non-farm, on SharePoint - 80	`http://server/_layouts/PI_WebParts/admin.aspx`
SharePoint farm	`http://loadbalancer/_layouts/PI_WebParts/admin.aspx` where *loadbalancer* is the name of the computer that runs the load balancer for the SharePoint farm

2. Under **PI WebParts Configuration**, click **PI Table Configuration** to open the PI Table Configuration page.

   On the left side of the page, the **Saved Configurations** list shows all table configurations defined for PI WebParts. The right side of the page shows the properties of the selected configuration.

3. Manage the configurations:
   - To add new a table configuration, click **New**.
   - To create a new configuration based on an existing configuration, select the existing configuration, click **Copy**, provide a new name, and change other properties if desired.
   - To view or update properties of a configuration, select the saved configuration.
   - To see how a configuration appears, select the configuration and click **Preview**.
   - To remove a configuration, select a configuration and click **Delete**.

Topics in this section

- Table configuration properties
  Configure properties for one template at a time.
- Available columns
  Formatting properties are associated with columns from the data set.
- Column behavior settings
  Assign one of five behaviors to data-set columns.
- Add a table configuration
  Specify columns and properties, then preview the results.

- Preview table column data
  Show how a configuration appears when applied to a table.

Table configuration properties

After you select a table configuration in the **Saved Configurations** list on the PI Table Configuration page, the fields on the right show the properties for the selected configuration. You can select only one configuration at a time. The following property fields apply to the entire table configuration:



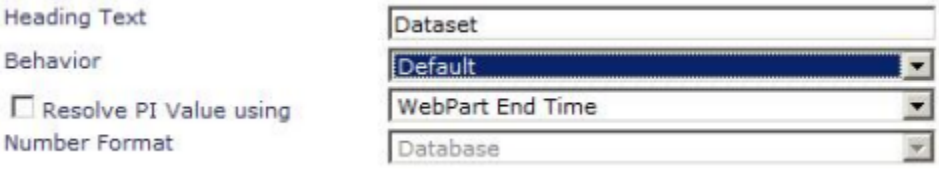
Property	Definition
Name	The name that identifies the configuration in PI WebParts, under **Behavior Settings**. You cannot change the name after you save the configuration.
Description	A description of the configuration.
Dataset	The name of a PI calculation, relational, or web-service data set that uses the configuration.

Available columns

When you select a data set, the **Available Columns** list shows the columns in that data set. Each data-set column has a unique format, which affects appearance, behavior, and resultant actions when a value is clicked in the web part.

Select any column in the list to view or change its properties in the fields on the tabs to the right. You can only select one column from the list. Each column in the data set can have its own unique property settings.

The following column property fields apply to individual columns:



Property	Definition
Heading Text	An optional column heading name substituted for the data-set column name, such as a descriptive term that indicates the source or relevance of the column data. If no heading text is specified, then the column name is used instead.

Property	Definition
Behavior	The column behavior type: • **Default** Displays the column value. • **Ad hoc Trend** Formats column data as a link to an ad hoc trend display. • **Current State** Replaces the column value with a current state bar indicator. • **Hidden** Excludes the column from the default table layout, but makes it available for inclusion by the end user. • **Hyperlink** Formats column data as a hyperlink to a web page, web image (.gif or .jpg), or other file (for example, .svg), and can also send data through a web-part connection. The URL target path is typically data stored in another column.
Resolve PI Value using	The source of a time parameter used to resolve the value of a PI tag in the column. PI tags may be resolved with reference to the web-part end time, or a time column within the data set. This field is only enabled when the check box is selected.
Number Format	The format used to display numbers in the column. Options include **General**, **Database**, **Scientific**, and specific formats (for example, **#,###.##**). The default value is **Database**, which uses the DisplayDigits attribute value for PI tags and the data-source default for non-PI System data. The locale format set in SharePoint regional settings (or the web server for administrative pages) determines group and decimal separators.

Column behavior settings

The following tabs define behavior settings of data-set columns:

- **Formatting**

  Defines the default behavior setting for all column types.

- **Link**

  Defines settings for columns with **Behavior** set to **Hyperlink**.

- **Current State**

  Defines settings for columns with **Behavior** set to **Current State**.

- **Ad hoc Trend**

  Defines settings for columns with **Behavior** set to **Ad hoc Trend**.



Note:
There are no settings to define if you set **Behavior** to **Hidden**.

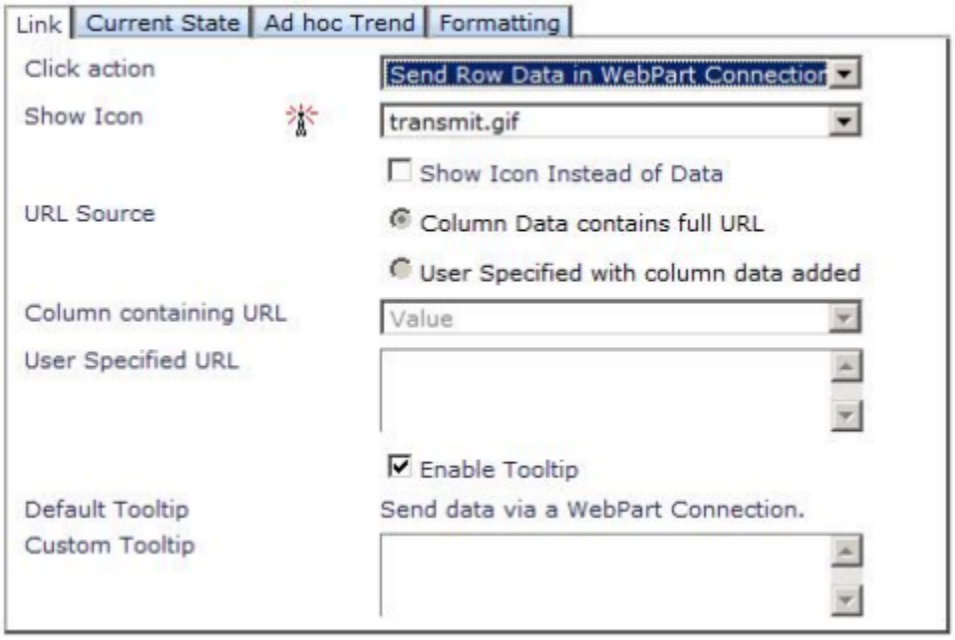
When you select a column in the **Available Columns** list and apply a behavior, the page automatically shows the corresponding configuration tab. You cannot apply more than one behavior to a column, or copy behaviors among columns. Changes to settings on tabs that do not correspond to the selected behavior have no effect on the column.

Topics in this section

- Link behavior options
  Set link behavior to convert column text to a hyperlink.
- Current State behavior options
  Set Current State behavior to convert column text to a state indicator.
- Ad hoc Trend behavior options
  Set Ad hoc Trend behavior to launch a trend from column data.
- Hidden behavior
  Set hidden behavior to hide the column in the web part.
- Text formatting options
  Set formatting behavior to style the appearance of column text.

Link behavior options

Properties on the **Link** tab are enabled when you set the **Behavior** field to **Hyperlink**. The properties that appear depend on the selections that you make.



Property	Definition
Click action	Defines the action taken when a hyperlinked data value in the column is clicked. The settings **New Window**, **Same Window**, and **Modal Window** define where a target URL opens. The setting **Send Row Data in WebPart Connection** sends the selected row to consuming web parts.

Property	Definition
Show Icon	A list of .gif files that can be displayed in the column heading as an indicator.
Show Icon Instead of Data	Specifies display of the file in the **Show Icon** field in each column cell instead of the column heading only.
URL Source	Determines the URL: • Click **Column Data contains full URL** to use the URL in the column data. • Click **User Specified with column data added** to append the column data to the URL specified in the **User Specified Url** field.
Column containing URL	Specifies the data-set column that contains the target URL for the link. The URL can be stored in the configured link column or in a different column. This field appears and applies only when you set **URL Source** to **Column Data contains full URL**.
Column with URL data	Specifies the column that contains content to append to the URL in the **User Specified URL** field to construct the whole URL. This field appears and applies only when you set **URL Source** to **User Specified with column data added**.
User Specified URL	Specifies the base URL to append to the content in the column specified by the **Column with URL data** field. This field appears and applies only when you set **URL Source** to **User Specified with column data added**.
Enable Tooltip	Display tool tips for links in the column.
Default Tooltip	Shows the default action for tool tips. This default action applies when the **Enable Tooltip** check box is selected and no text is specified in the **Custom Tooltip** field. The value of the default is equal to the action defined for the **Click action** field.
Custom Tooltip	Overrides the **Default Tooltip** field if the **Enable Tooltip** check box is selected.

Current State behavior options

Properties on the **Current State** tab are enabled when you set the **Behavior** field to **Current State**. These properties specify the numeric or PI tag columns used to determine the current-state indicator. For example, if the column value exceeds or drops below the minimum or maximum value, the graphic in the column blinks. An error icon is displayed instead of the indicator if a column value is suspect.



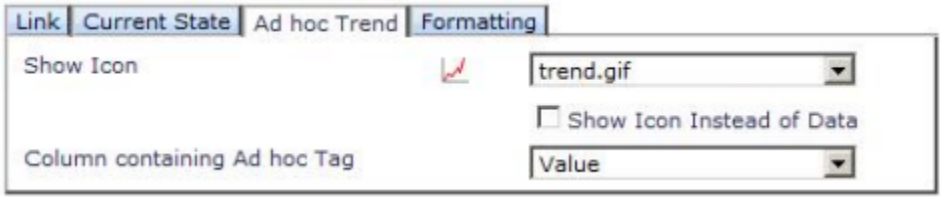
Note:
Current State behavior applies only to numeric data. No value or indicator is shown if a column value with Current State behavior contains non-numeric data.



Property	Definition
Use PI Tag Attributes	Determines parameters for Actual, Typical, Minimum, and Maximum Value using attributes of a single PI tag provided by the Actual Value Column. The resolved tag value is used as the Actual Value, the Typical attribute as the Typical value, the Zero attribute as the Minimum value, and the sum of the Zero and Span tag attributes specifies the Maximum value. Clear the check box to choose different columns to provide each parameter value.
Actual Value Column	A column that supplies the actual data value measured by the current state indicator.
Typical Value Column	A column that supplies the typical data value measured by the current state indicator. Disabled when the **Use PI Tag Attributes** check box is selected.
Minimum Value Column	A column that supplies the lower limit value of the current state indicator. Disabled when the **Use PI Tag Attributes** check box is selected.
Maximum Value Column	A column that supplies the upper limit value of the current state indicator. Disabled when the **Use PI Tag Attributes** check box is selected.

Ad hoc Trend behavior options

Properties on the **Ad hoc Trend** tab are enabled when you set the **Behavior** column to **Ad hoc Trend**.



Property	Definition
Show Icon	A list of .gif and .ico files that can be displayed in the column heading.
Show Icon Instead of Data	Indicates the selected icon should replace the data value in each column cell, instead of appearing in the column header.

Property	Definition
Column containing Ad hoc Tag	The column containing the PI Server tag data used for the trend trace.

Hidden behavior

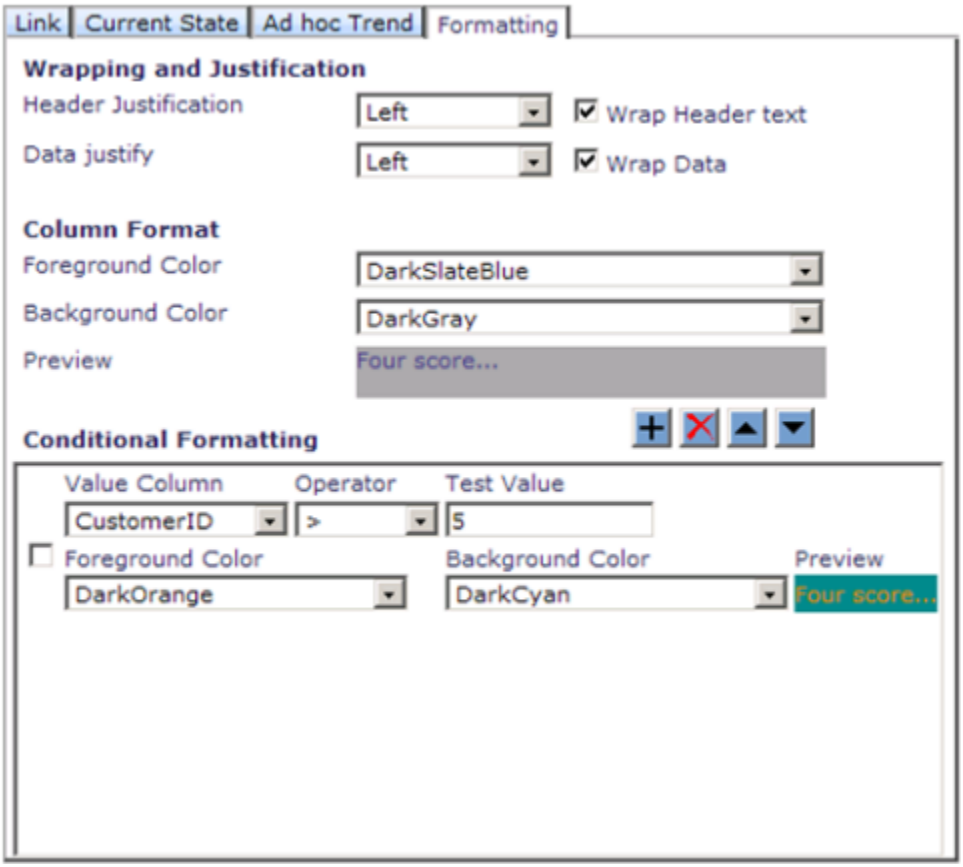
If you set the **Behavior** field to **Hidden**, the data in the column is available to use, but the table does not display the column.

Hidden columns are listed as available during table configuration.

This behavior is useful when a column contains data that supports the behavior of another column but you do not want to display the supporting column on its own.

Text formatting options

Properties on the **Formatting** tab are enabled for all values of the **Behavior** field.



Property	Definition
Header Justification	Determines how heading text should be justified within the column.
Wrap Header text	When this check box is selected, heading text is wrapped using the HTML algorithm for wrapping text in a table.

Property	Definition
Data justify	Determines how data values are justified within the column. By default, non-numeric columns are justified **Left**, numeric columns and columns containing PI System data are justified **Right**, and columns containing current-state images are justified **Center**.
Wrap Data	When this check box is selected, data values are wrapped using the HTML algorithm for wrapping text in a table.
Foreground Color	Determines the color to use for text or data in the column. To use the default style sheet settings for foreground text, set the **Foreground Color** field to **Default Foreground Color**. To specify a color override, select a color from the list. Refer to the text in the **Preview** field to see the effect of the selected foreground and background colors.
Background Color	Determines the color to use for the background cell fill in the column. To use the default style sheet settings for background colors, set the **Background Color** field to **Default Background Color**. To specify a color override, select a color from the list. Refer to the text in the **Preview** field to see the effect of the selected foreground and background colors.
Conditional Formatting	Use these conditional property fields to determine a column's colors when a condition evaluates to true. The value of the **Value Column** field is compared to the value of the **Test Value** field using the logical operator in the **Operator** field. The **Test Value** field can contain a constant value (for example, 50), a string (which uses a case-insensitive comparison), or the name of a column in the same data set, entered as `col(ColumnName)`. For the logical operator **between**, provide two text fields for the comparison. You can add any number of conditional formats for each column. They are evaluated in order from top to bottom for each row in the table, and the first one that is satisfied has its foreground color and background color applied to the cell.

Add a table configuration

You can use the PI Table Configuration page to add a table configuration and make available for use in PI WebParts.

Procedure

1. Go to the PI WebParts Administration website:

Installation type	URL to PI WebParts Administration website
Non-farm, on SharePoint - 80	`http://server/_layouts/PI_WebParts/admin.aspx`
SharePoint farm	`http://loadbalancer/_layouts/PI_WebParts/admin.aspx` where *loadbalancer* is the name of the computer that runs the load balancer for the SharePoint farm

2. Under **PI WebParts Configuration**, click **PI Table Configuration** to open the PI Table Configuration page.

On the left side of the page, the **Saved Configurations** list shows all table configurations defined for PI WebParts. The right side of the page shows the properties of the selected configuration.

3. To create a new table configuration that uses default values, click **New**.

   The fields on the right side of the page are reset to default values.

4. In the **Configuration Name** field, enter a name for the configuration.

   In PI WebParts, this is the **Behavior Settings** name. You cannot change this name after you save the configuration.

5. From the **Dataset** list, select the data set to use for this configuration. The **Available Columns** list shows the columns in the table for the selected data set.

6. For each column in the table, specify a behavior:

   a. From the **Available Columns** list, select a column.

   b. From the **Behavior** list, select a column behavior.

   c. Set the appropriate settings for the selected behavior.

7. Modify any remaining configuration parameters that you want to change.

   PI WebParts assumes default settings for all other parameters.

8. Click **Preview** to preview the table configuration settings that you have entered.

9. Click **Save** to add the new table configuration to the list of saved configurations.

Preview table column data

From the PI Table Configuration page, you can see how a configuration appears when applied to a table.

Procedure

1. Go to the PI WebParts Administration website:

Installation type	URL to PI WebParts Administration website
Non-farm, on SharePoint - 80	`http://server/_layouts/PI_WebParts/admin.aspx`
SharePoint farm	`http://loadbalancer/_layouts/PI_WebParts/admin.aspx` where *loadbalancer* is the name of the computer that runs the load balancer for the SharePoint farm

2. Under **PI WebParts Configuration**, click **PI Table Configuration** to open the PI Table Configuration page.

   On the left side of the page, the **Saved Configurations** list shows all table configurations defined for PI WebParts. The right side of the page shows the properties of the selected configuration.

3. From the **Saved Configuration** list, select a table configuration.

4. Click the **Preview** button.

   A new browser window shows a table that contains all of the columns included in the result set.

The preview table shows up to five rows of returned data for each column; you can use the arrow buttons to scroll through the results.

Note:
The preview table does not use the SharePoint-configured locale setting to format dates and times. Instead, the preview table uses the data-source time zone for time-stamp columns, and displays time stamps in PI time format (dd-mmm-yy HH:mm:ss).

Manage PI Trend and PI XYPlot configurations

PI Trend and PI XYPlot web parts plot data points in configurable formats that update in real-time. With a configuration template, you can preset formatting options, such as multiple-line styles, fonts, color coding, and markers.

Procedure

1. Go to the PI WebParts Administration website:

Installation type	URL to PI WebParts Administration website
Non-farm, on SharePoint - 80	`http://server/_layouts/PI_WebParts/admin.aspx`
SharePoint farm	`http://loadbalancer/_layouts/PI_WebParts/admin.aspx` where *loadbalancer* is the name of the computer that runs the load balancer for the SharePoint farm

2. Under **PI WebParts Configuration**, click **PI Trend Configuration** to open the PI Trend Configuration page.

   On the left side of the page, the **Saved Configurations** list shows all the trend and plot configurations defined for PI WebParts. The right side of the page shows the properties of the selected configuration.

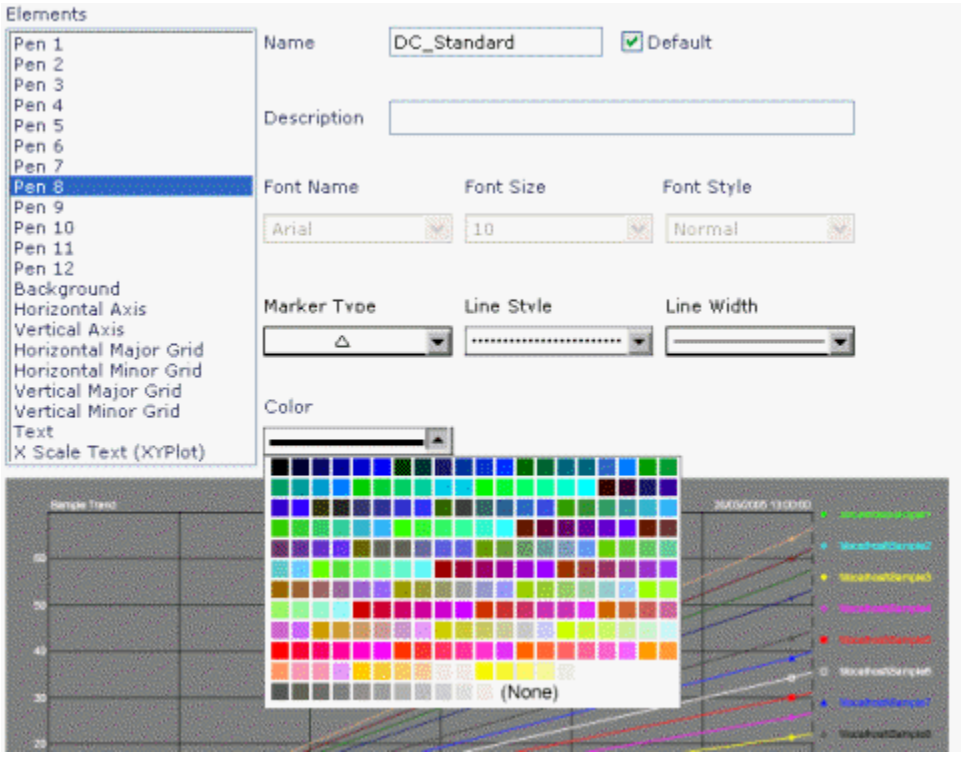
3. Manage the trend and plot configurations: Click or select a saved configuration to view or update properties.
   - To add a configuration, click **New**.
   - To create a new configuration based on an existing configuration, select the existing configuration, click **Copy**, provide a new name, and change other properties if desired.
   - To view or update properties of a configuration, select the saved configuration.
   - To see how a configuration appears, select the configuration and click **Preview**.
   - To remove a configuration, select a configuration and click **Delete**.

Topics in this section

- PI Trend and PI XYPlot configuration properties
  Configure properties for one template at a time.
- Add a Trend or XYPlot configuration
  Specify display properties for each template.

PI Trend and PI XYPlot configuration properties

After you select a trend or plot configuration in the **Saved Configurations** list on the PI Trend Configuration page, the fields on the right show the properties set for the selected configuration. You can select only one configuration at a time. The following property fields apply:



Property	Definition
Name	The name that identifies the configuration in PI WebParts, under **Formatting**. This value cannot be changed after the configuration is saved.
Default	Sets the selected configuration as the default configuration applied to PI WebParts.
Description	A description of the configuration.
Elements	Configurable trace or plot elements. Select an item in the list to format its attributes. Elements include: Pens 1 through 12, Background, Horizontal Axis, Vertical Axis, Horizontal Major Grid, Horizontal Minor Grid, Vertical Major Grid, Vertical Minor Grid, Text, and X Scale Text (for XYPlot only).
Font Name, Font Size, Font Style	Font properties for text associated with a selected element.
Marker Type	A marker shape for a selected pen element.
Line Style	A line style for the selected element. Set Line Style to **(None)** if you prefer not to show a line.
Line Width	A line thickness for the selected element.

Property	Definition
Color	A color for the selected element.

Add a Trend or XYPlot configuration

You can use the PI Trend Configuration page to add a trend or plot configuration and make available for use in PI WebParts.

Procedure

1. Go to the PI WebParts Administration website:

Installation type	URL to PI WebParts Administration website
Non-farm, on SharePoint - 80	`http://server/_layouts/PI_WebParts/admin.aspx`
SharePoint farm	`http://loadbalancer/_layouts/PI_WebParts/admin.aspx` where *loadbalancer* is the name of the computer that runs the load balancer for the SharePoint farm

2. Under **PI WebParts Configuration**, click **PI Trend Configuration** to open the PI Trend Configuration page.

   On the left side of the page, the **Saved Configurations** list shows all the trend and plot configurations defined for PI WebParts. The right side of the page shows the properties of the selected configuration.

3. To create a new trend configuration that uses default values, click **New**.

   The fields on the right side of the page are reset to default values.

4. In the **Name** field, enter a name for the configuration.

   In PI WebParts, this is the **Settings** name under **Trend Formatting**. You cannot change this name after you save the configuration.

5. Modify any remaining trend configuration elements and associated properties that you want to change.

   PI WebParts assumes default settings for all other parameters.

   The pane below the property fields shows a preview of the configuration settings.

6. Click **Save** to add the new trend configuration to the list of saved configurations.

Manage PI Messenger contacts configurations

PI Messenger shows online presence for a list of contacts. Use the PI Messenger Configuration page to configure settings for contacts lists stored in a data set or an LDAP Active Directory location.

Procedure

1. Go to the PI WebParts Administration website:

Installation type	URL to PI WebParts Administration website
Non-farm, on SharePoint - 80	`http://server/_layouts/PI_WebParts/admin.aspx`

Installation type	URL to PI WebParts Administration website
SharePoint farm	`http://loadbalancer/_layouts/PI_WebParts/admin.aspx` where *loadbalancer* is the name of the computer that runs the load balancer for the SharePoint farm

2. Under **PI WebParts Configuration**, click **PI Messenger Configuration** to open the PI Messenger Configuration page.

   On the left side of the page, the **Saved Configurations** list shows all the contacts configurations defined for PI WebParts. The right side of the page shows the properties of the selected configuration.

3. Manage the configurations:
   - To add new a contacts configuration, click **New**.
   - To create a new configuration based on an existing configuration, select the existing configuration, click **Copy**, provide a new name, and change other properties if desired.
   - To view or update properties of a configuration, select the saved configuration.
   - To see how a configuration appears, select the configuration and click **Preview**.
   - To remove a configuration, select a configuration and click **Delete**.

Topics in this section

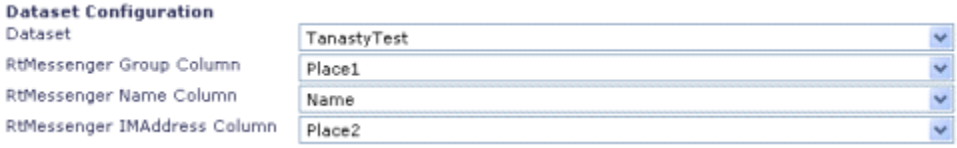
- PI Messenger configuration properties
  Configure properties for one template at a time.
- Add a contacts configuration
  Specify display properties for each template.

PI Messenger configuration properties

After you select a contacts configuration in the **Saved Configurations** list on the PI Messenger Configuration page, the fields on the right show the properties set for the selected configuration. You can select only one configuration at a time. The following property fields apply:



Property	Definition
Name	The name that identifies the contacts configuration in PI WebParts, under **Saved Configurations**. This value cannot be changed after the configuration is saved.
Description	A description of the saved configuration.



Property	Definition
Dataset	The name of a relational or web-service data set that contains the contact information.
PI Messenger Group Column	The column that contains contact group information in the selected data set.
PI Messenger Name Column	The column that contains contact names in the selected data set.
PI Messenger IMAddress Column	The column that contains contact IM addresses in the selected data set.



Property	Definition
Active Directory LDAP Path	The LDAP Path used to search Active Directory locations for organizational units.
IMAddress Field	An Active Directory field that represents user IM addresses. This may be an email address field.
Name Field	An Active Directory field that represents the Full Name attribute of an Active Directory user.

Add a contacts configuration

You can use the PI Messenger Configuration page to add a contacts configuration and make available for use in PI WebParts.

Procedure

1. Go to the PI WebParts Administration website:

Installation type	URL to PI WebParts Administration website
Non-farm, on SharePoint - 80	`http://server/_layouts/PI_WebParts/admin.aspx`
SharePoint farm	`http://loadbalancer/_layouts/PI_WebParts/admin.aspx` where *loadbalancer* is the name of the computer that runs the load balancer for the SharePoint farm

2. Under **PI WebParts Configuration**, click **PI Messenger Configuration** to open the PI Messenger Configuration page.

   On the left side of the page, the **Saved Configurations** list shows all the contacts configurations defined for PI WebParts. The right side of the page shows the properties of the selected configuration.

3. To create a new contacts configuration that uses default values, click **New**.

   The fields on the right side of the page are reset to default values.

4. In the **Name** field, enter a name for the configuration.

   In PI WebParts, this is the **Settings** name under **PI Messenger Formatting**. You cannot change this name after you save the configuration.

5. Modify any remaining PI Messenger configuration parameters that you want to change.
6. Click **Preview** to preview the entered configuration settings.
7. Click **Save** to add the new configuration to the list of saved configurations.

Remove a PI WebParts configuration

You can use the appropriate configuration page to delete configurations. If you remove a configuration, client applications that use the configuration lose their formatting and return an error message. Be sure to update client applications yourself or notify users of the change, and provide information on any new configurations that replace the deleted configuration.

Procedure

1. Go to the PI WebParts Administration website:

Installation type	URL to PI WebParts Administration website
Non-farm, on SharePoint - 80	`http://server/_layouts/PI_WebParts/admin.aspx`
SharePoint farm	`http://loadbalancer/_layouts/PI_WebParts/admin.aspx` where *loadbalancer* is the name of the computer that runs the load balancer for the SharePoint farm

2. Under **PI WebParts Configuration**, click the link for the appropriate configuration page.
3. From the **Saved Configurations** list, select the configuration that you want to delete.
4. Click **Delete** to remove the configuration from the list.

Data sources

This section describes how to use PI Web Parts Administration pages to configure and connect to available data sources.

Once a data source is created and PI WebParts Services can connect to the data provider, you can create data sets that use the data source and that PI WebParts users can search and view.

PI WebParts Services supports PI Server, PI AF server, relational database, and web-service data sources.

Topics in this section

- PI Server data sources
  Configure PI Servers as data sources.
- Relational data sources
  Configure common relational databases as data sources.
- Web-service data sources
  Configure available web services as data sources.
- PI Asset Framework support
  PI WebParts Services connects implicitly through PI System Explorer.

PI Server data sources

You can use the PI Data Sources page on the PI WebParts Administration site to add, view, test, or delete connections to PI Server data sources.

You can also use the PI SDK utility or PI System Management Tools on the PI WebParts Services application server to add a connection to a PI Server data source. The PI Data Sources page will show PI Servers configured through these methods.

Topics in this section

- Add PI Server connections
  Specify connection parameters for a PI Server.
- Edit connections to PI Server data sources
  Provide information to update the connection parameters.
- Delete PI Server connections
  Remove obsolete connections to PI Servers.

Add PI Server connections

You can use the PI Data Sources page to add a connection to a PI Server or a PI Server collective.

Procedure

1. Go to the PI WebParts Administration website:

Installation type	URL to PI WebParts Administration website
Non-farm, on SharePoint - 80	`http://server/_layouts/PI_WebParts/admin.aspx`
SharePoint farm	`http://loadbalancer/_layouts/PI_WebParts/admin.aspx` where *loadbalancer* is the name of the computer that runs the load balancer for the SharePoint farm

2. Under **PI WebParts Configuration**, click **PI Data Sources** to open the PI Data Sources page.

   The **Configured PI Servers** list shows the PI Servers and PI Server collectives currently configured for data exchange.

3. Click **New** to create a new connection to a PI Server.
4. In the **Server Name** field, enter the name clients use to access the PI Server or PI Server collective.

   You cannot change the name after you save the connection.

5. Click **Save** to add the new server to the **Configured PI Servers** list.

   After you add a new PI Server connection, you can edit the properties for that connection.

Edit connections to PI Server data sources

You can use the PI Data Sources page to view and edit connection properties of configured connections to any PI Server or PI Server collective.

Procedure

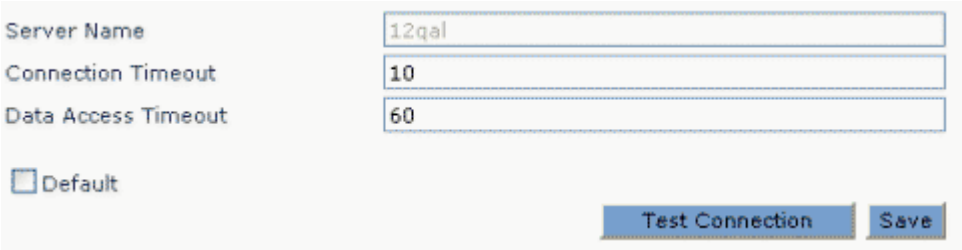
1. Go to the PI WebParts Administration website:

Installation type	URL to PI WebParts Administration website
Non-farm, on SharePoint - 80	`http://server/_layouts/PI_WebParts/admin.aspx`
SharePoint farm	`http://loadbalancer/_layouts/PI_WebParts/admin.aspx` where *loadbalancer* is the name of the computer that runs the load balancer for the SharePoint farm

2. Under **PI WebParts Configuration**, click **PI Data Sources** to open the PI Data Sources page.

   The **Configured PI Servers** list shows the PI Servers and PI Server collectives currently configured for data exchange.

3. Select a configured PI Server or PI Server collective to view current connection properties.



   - **Server Name**

     The name clients use to access the PI Server or PI Server collective. You cannot change the names of already configured connections.

   - **Connection Timeout**

     The number of seconds before an unused connection times out. This value may override the default values configured for the PI SDK on the web server. Set to 0 to use the PI SDK default.

     This value is disabled when creating a new connection, and is not shown for PI Server collectives. Click **Start** > **All Programs** > **PI System** > **About PI-SDK** to update parameters for a collective.

   - **Data Access Timeout**

     The number of seconds before an unresponsive data request times out. This value may override the default values configured for the PI SDK on the web server. Set to 0 to use the PI SDK default.

     This value is disabled when creating a new connection, and is not shown for PI Server collectives. Click **Start** > **All Programs** > **PI System** > **About PI-SDK** to update parameters for a collective.

   - **Default**

     If selected, the PI Server or PI Server collective is the default PI Server data source. The default data source is used to access data when only a tag name is provided (for example, when sending `<tag>` through a PI web-part connection instead of `\\server\<tag>`).

4. Edit property values, if desired.

5. Click **Test Connection** to test the connection to the selected PI Server.

   The connections for both the current Windows user account and the application pool identity are verified. Depending on how the server is configured, the mapped PI trusts or the PI identities associated with each are shown.

   A PI Server must allow access for both the current user and PI WebParts Services to acquire data.

6. Click **Save** to save any changes made.

Delete PI Server connections

You can use the PI Data Sources page to delete a connection to a PI Server or a PI Server collective. When you delete a connection, web parts that use the connection to retrieve data are no longer updated. Be sure to update web part configurations yourself or notify users of the change, and provide information on any new data sources that replace the deleted connection.

Procedure

1. Go to the PI WebParts Administration website:

Installation type	URL to PI WebParts Administration website
Non-farm, on SharePoint - 80	`http://server/_layouts/PI_WebParts/admin.aspx`
SharePoint farm	`http://loadbalancer/_layouts/PI_WebParts/admin.aspx` where *loadbalancer* is the name of the computer that runs the load balancer for the SharePoint farm

2. Under **PI WebParts Configuration**, click **PI Data Sources** to open the PI Data Sources page.

   The **Configured PI Servers** list shows the PI Servers and PI Server collectives currently configured for data exchange.

3. Select the configured PI Server that you want to delete, and click **Delete**.

4. Click **OK** at the confirmation prompt.

   The data source is removed from the list, and web parts can no longer access the data source.

Relational data sources

PI WebParts Services supports a variety of relational databases and connection options. Supported connection options include:

- ODBC
- Microsoft Jet 4.0 OLE DB (Access)
- OLE DB
- Oracle
- PI OLEDB
- SQL Server

PI OLEDB Enterprise is supported by the OLEDB adapter.

Note:
The Oracle and SQL Server .NET data providers do not use OLEDB technology. Rather, they use native technologies that are intended to provide better performance.

You can use the Relational Data Sources page on the Administration site to add, view, test, or delete connections to relational data sources.

Topics in this section

- Add relational connections
  Specify connection parameters for relational databases.
- Edit relational connections
  Provide information to update the connection parameters.
- Delete relational connections
  Remove obsolete connections to relational databases.

Add relational connections

You can use the Relational Data Sources page to add connections to relational data sources.

Procedure

1. Go to the PI WebParts Administration website:

Installation type	URL to PI WebParts Administration website
Non-farm, on SharePoint - 80	`http://server/_layouts/PI_WebParts/admin.aspx`
SharePoint farm	`http://loadbalancer/_layouts/PI_WebParts/admin.aspx` where *loadbalancer* is the name of the computer that runs the load balancer for the SharePoint farm

2. Under **PI WebParts Configuration**, click **Relational Data Sources** to open the Relational Data Sources page.

   The **Configured Data Sources** list shows the relational database servers currently configured for data exchange.

3. Click **New** to create a new connection to a relational database server.

   The connection properties are set to default values.

   Alternatively, you can select an existing relational data source and click **Copy** to use its settings as a starting point for the new configuration.

4. Configure the new connection based on database type:
   - Configure an ODBC connection
   - Configure a Microsoft Access or other OLE DB connection
   - Configure a SQL Server connection
   - Configure an Oracle connection (Microsoft provider)
   - Configure a PI OLEDB connection

5. Click **Test Connection** to verify that you can connect to the data source as specified.
6. Click **Save** to add the new relational database entry to the **Configured Data Sources** list.

Configure an ODBC connection

When you create a new connection to a relational database server, specify the properties to configure an ODBC connection.

Procedure

1. In the **Data Source Name** field, enter a name for the relational database.

   You cannot change this name after you save the data source connection.
2. In the **Description** field, enter a longer text description that helps identify this data source, such as `Server for LIMS data`.
3. From the **Database Type** list, select **ODBC Connection**.
4. Next to the **DSN Name** field, click **Browse** to choose the data source from a list.

   A window opens and lists available system data sources configured on the PI WebParts Services application server. The list contains four columns:

   - The first column contains buttons to select a source.
   - The second column displays the **DSN Name** for each data source.
   - The third column displays the **DSN Type** (for example, SQL Server) for each data source.
   - The fourth column displays the default connection string used to communicate with each data source.
5. Click the button next to the **DSN Name** of the data source that you want to use.

   The selected row is highlighted in purple.
6. Click **OK** to select the data source and close the window.

   The **DSN Name** and **Connection String** fields are populated with the selected DSN information.

   Note:
   Connection strings containing just the DSN, UID and PWD keywords are adequate for Oracle ODBC connections.
7. From the **Source Time Zone** list, select an appropriate time zone for the server.

   This ensures that data from this source can be compared with data from other servers across multiple time zones.
8. If your connection string includes the token `<PASSWORD>`, use the **Password** field to specify a password.

   To prevent the password from being appended to the connection string, select the **No Password** check box.
9. In the **Connection String** field, make any necessary changes to the connection string.

After you finish

Test the connection and save the data-source configuration.

Configure a Microsoft Access or other OLE DB connection

When you create a new connection to a relational database server, specify the properties to configure a Microsoft Access or other OLE DB connection.

Procedure

1. In the **Data Source Name** field, enter a name for the relational database.

   You cannot change this name after you save the data source connection.
2. In the **Description** field, enter a longer text description that helps identify this data source, such as `Server for LIMS data`.
3. From the **Database Type** list, select either **Microsoft Jet 4.0 OLE DB Provider** (for a Microsoft Access database) or **User-specified OLE DB Provider**.

   Note:
   This is how you can configure a connection to the PI OLEDB Enterprise provider.
4. From the **Source Time Zone** list, select an appropriate time zone for the server.

   This ensures that data from this source can be compared with data from other servers across multiple time zones.
5. In the **Connection String** field, enter a connection string.

   Refer to Creating and Configuring Universal Data Link Files (http://msdn.microsoft.com/en-us/library/e38h511e(v=VS.71).aspx) for information on using a UDL file to create and configure a connection string for OLE DB providers.

   Refer to the *PI OLEDB Enterprise User Guide* for more information on the parameters you can use in the connection string to configure a connection to the PI OLEDB Enterprise provider.
6. If your connection string includes the token `<PASSWORD>`, use the **Password** field to specify a password.

   To prevent the password from being appended to the connection string, select the **No Password** check box.

After you finish

Test the connection and save the data-source configuration.

Configure a SQL Server connection

When you create a new connection to a relational database server, specify the properties to configure an SQL Server connection.

Procedure

1. In the **Data Source Name** field, enter a name for the relational database.

   You cannot change this name after you save the data source connection.
2. In the **Description** field, enter a longer text description that helps identify this data source, such as `Server for LIMS data`.
3. From the **Database Type** list, select **SQL Server**.

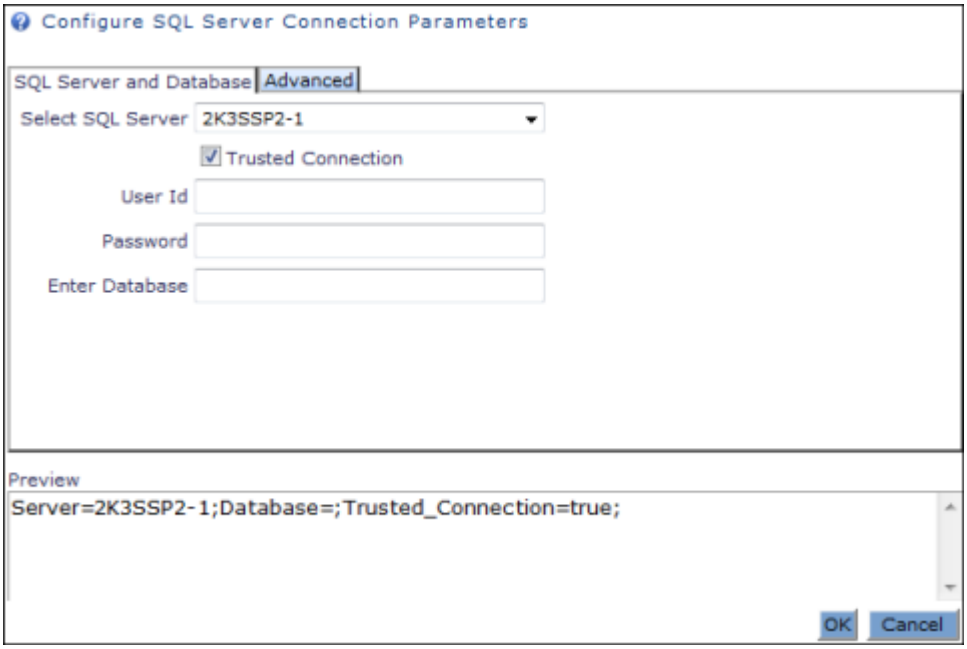
4. From the **Source Time Zone** list, select an appropriate time zone for the server.

   This ensures that data from this source can be compared with data from other servers across multiple time zones.

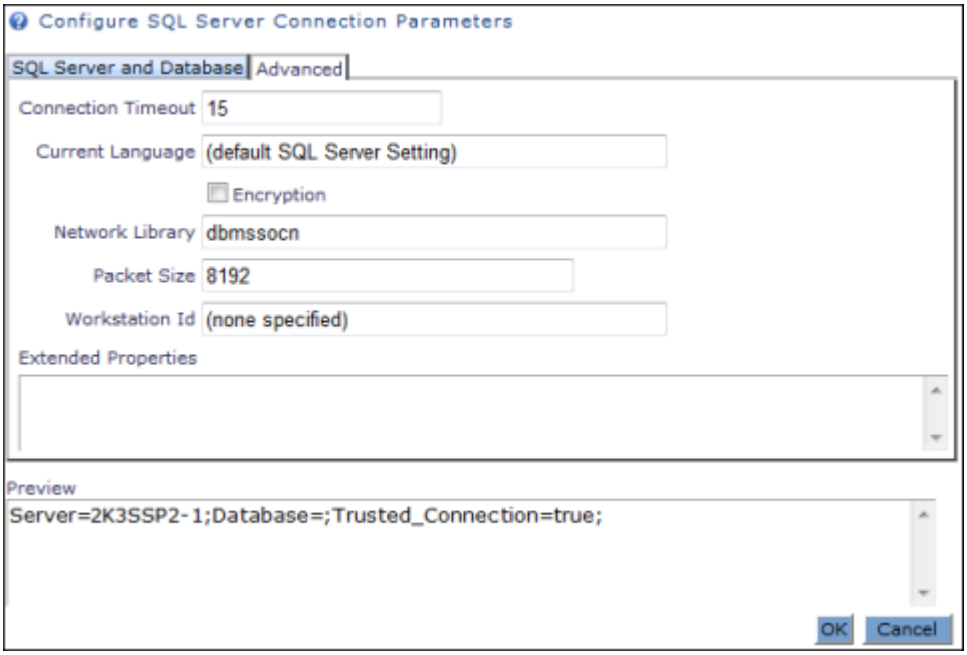
5. Click **Edit Connection String** to generate a connection string.

   The **Edit Data Source** window opens.

6. On the **SQL Server and Database** tab, select an available SQL Server database from a list of known servers and enter login and database information.



7. On the **Advanced** tab, specify additional connection parameters as desired.



As you add parameters, the preview window updates with the correct syntax for the selected parameters.

8. When you are finished, click **OK** to close the window and insert the connection string in the **Connection String** field.

   You can edit this field manually, if desired.

9. If your connection string includes the token `<PASSWORD>`, use the **Password** field to specify a password.

   To prevent the password from being appended to the connection string, select the **No Password** check box.

After you finish

Test the connection and save the data-source configuration.

Configure an Oracle connection (Microsoft provider)

When you create a new connection to a relational database server, specify the properties to configure an Oracle connection using Microsoft Provider.

Procedure

1. In the **Data Source Name** field, enter a name for the relational database.

   You cannot change this name after you save the data source connection.

2. In the **Description** field, enter a longer text description that helps identify this data source, such as `Server for LIMS data`.

3. From the **Database Type** list, select **Oracle (Microsoft Provider)**.

4. From the **Source Time Zone** list, select an appropriate time zone for the server.

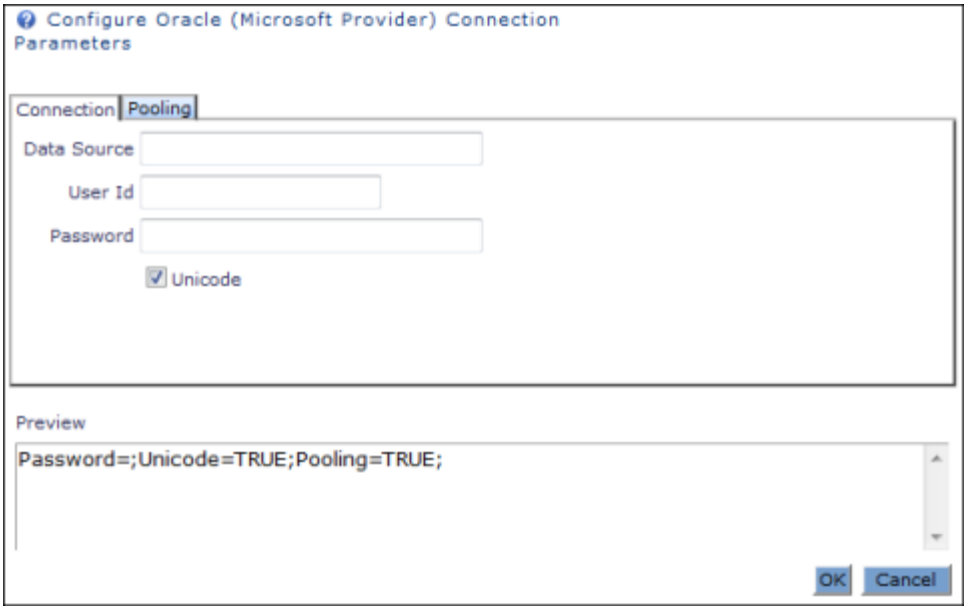
   This ensures that data from this source can be compared with data from other servers across multiple time zones.

5. Click **Edit Connection String** to generate a connection string.

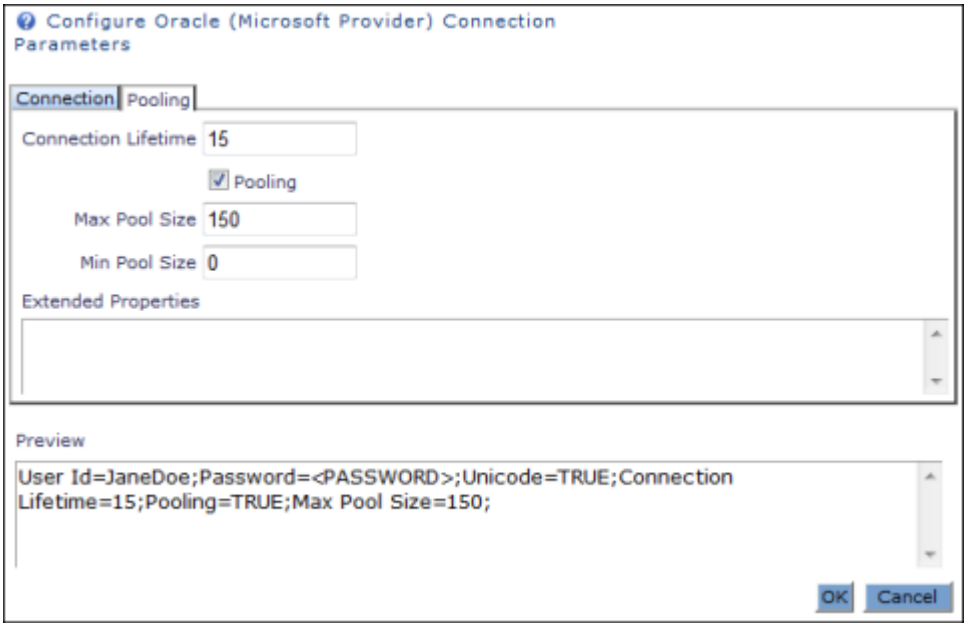
   The Edit Data Source window opens.

6. On the **Connection** tab, enter values in the **Data Source**, **User ID**, and **Password** fields.

   You can also select the **Unicode** check box to require Unicode for the database connection.



7. On the **Pooling** tab, specify additional parameters as desired.



Refer to the Microsoft documentation (http://msdn.microsoft.com/en-us/library/ms254500(v=VS.80).aspx) for information on connection string parameters for the Oracle Data Provider. As you add parameters, the preview window updates with the correct syntax for the selected parameters.

8. Click **OK** to close the window and insert the connection string in the **Connection String** field.

   You can edit this field manually, if desired.

9. If your connection string includes the token `<PASSWORD>`, use the **Password** field to specify a password.

To prevent the password from being appended to the connection string, select the **No Password** check box.

After you finish

Test the connection and save the data-source configuration.

Configure a PI OLEDB connection

When you create a new connection to a relational database server, specify the properties to configure a PI OLEDB connection.

Note:
OSIsoft recommends using PI OLEDB Provider 3.3.0.1 or higher. Set **Session ID =-1** in the PI OLEDB connection string to avoid using the same session ID with two different PI OLEDB processes.

Procedure

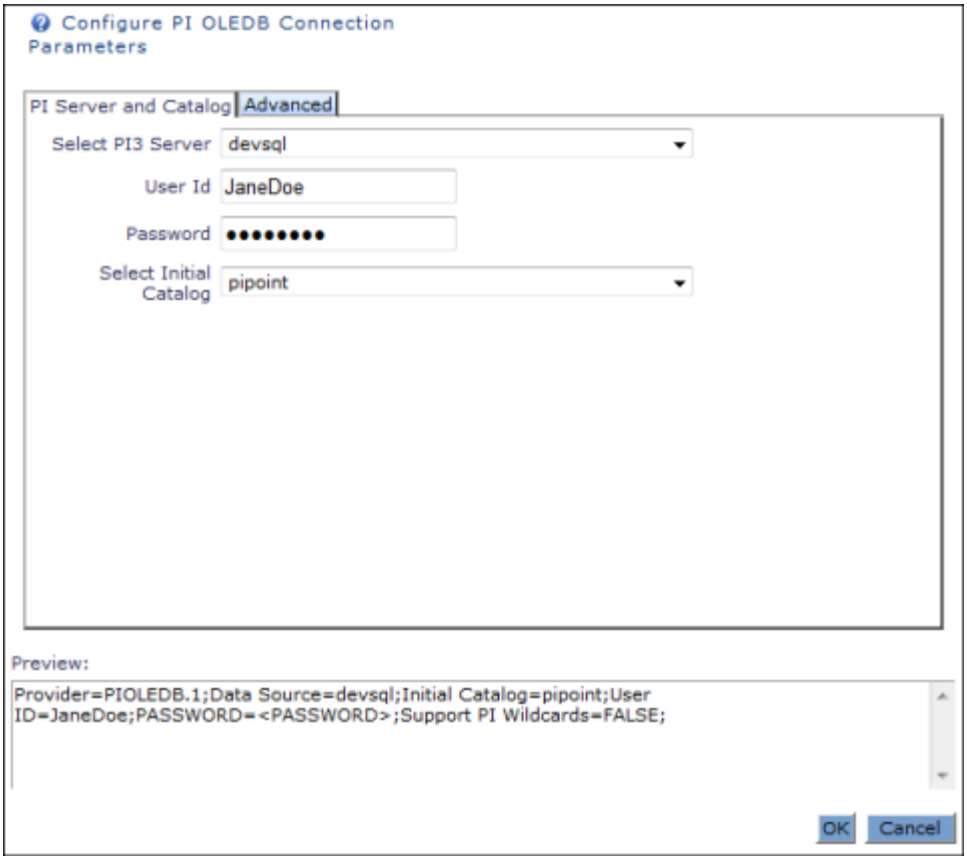
1. In the **Data Source Name** field, enter a name for the relational database.

   You cannot change this name after you save the data source connection.
2. In the **Description** field, enter a longer text description that helps identify this data source, such as `Server for LIMS data`.
3. From the **Database Type** list, select **PI OLEDB**.
4. From the **Source Time Zone** list, select an appropriate time zone for the server.

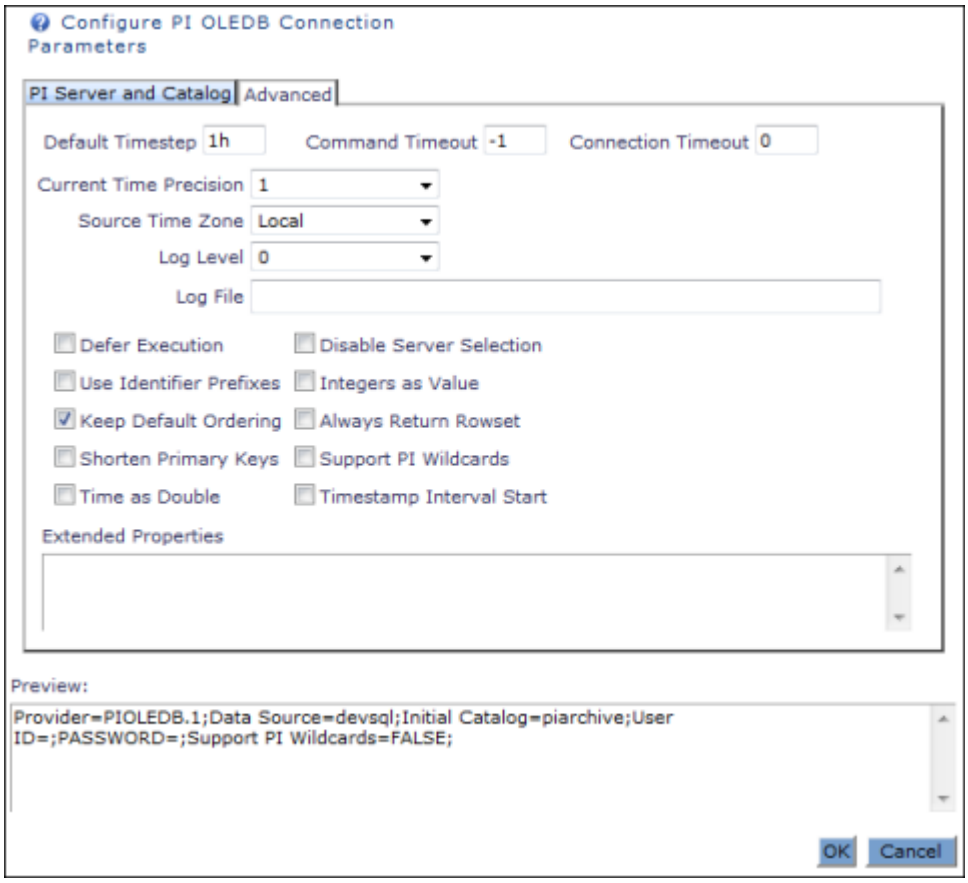
   This ensures that data from this source can be compared with data from other servers across multiple time zones.
5. Click **Edit Connection String** to generate a connection string for this connection.

   The Edit Data Source window opens.
6. On the **PI Server and Catalog** tab, use the **Select PI3 Server** list to choose the PI Server or PI collective name from a list of known servers.

   You can also specify values in the **User ID**, **Password**, and **Select Initial Catalog** fields.



7. On the **Advanced** tab, specify additional connection parameters as necessary.



As you add parameters, the preview window updates with the correct syntax for the selected parameters.

8. Click **OK** to close the window and insert the connection string in the **Connection String** field.

   You can edit this field manually, if desired.

9. If your connection string includes the token `<PASSWORD>`, use the **Password** field to specify a password.

   To prevent the password from being appended to the connection string, select the **No Password** check box.

After you finish

Test the connection and save the data-source configuration.

Microsoft Office compatibility

Microsoft Office 2007 and later saves databases and files in a file format that can be used by ODBC and OLEDB. To download drivers that enable these system data files to be read, see these Microsoft website download pages:

- 2007 Office System Driver: Data Connectivity Components (http://www.microsoft.com/downloads/details.aspx?familyid=7554f536-8c28-4598-9b72-ef94e038c891&displaylang=en)
- Microsoft Access Database Engine 2010 Redistributable (http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=c06b8369-60dd-4b64-a44b-84b371ede16d)

Edit relational connections

You can use the Relational Data Sources page to view and edit connections to relational data sources.

Procedure

1. Go to the PI WebParts Administration website:

Installation type	URL to PI WebParts Administration website
Non-farm, on SharePoint - 80	`http://server/_layouts/PI_WebParts/admin.aspx`
SharePoint farm	`http://loadbalancer/_layouts/PI_WebParts/admin.aspx` where *loadbalancer* is the name of the computer that runs the load balancer for the SharePoint farm

2. Under **PI WebParts Configuration**, click **Relational Data Sources** to open the Relational Data Sources page.

   The **Configured Data Sources** list shows the relational database servers currently configured for data exchange.

3. Select a configured data source to view its connection properties.



   - **Data Source Name**

     A name that data sets use to access the relational database. You cannot change the names of already configured connections.

   - **Description**

     Descriptive text about the relational database connection.

   - **Database Type**

     The type of database specified in the connection string to the data source. Valid types include:

     - **ODBC Connection**
     - **Microsoft Jet 4.0 OLE DB Provider**
     - **User-specified OLE DB Provider**

- **Oracle (Microsoft Provider)**
- **PI OLEDB**
- **SQL Server**

Refer to the Microsoft .NET Framework Data Providers (http://msdn2.microsoft.com/en-us/library/a6cd7c08.aspx) documentation for detailed information on system requirements and supported database versions.

On 64-bit operating systems, some 64-bit providers, such as those for ODBC and Jet are not available. These will generate errors until an appropriate provider is installed.

◦ **DSN Name** (ODBC Connection only)

The name of an imported system DSN, which is accessed through an ODBC connection. Click **Browse** to find and open an ODBC data source that was previously configured and saved in the Web server registry.

◦ **Source Time Zone**

The time zone in which the data source returns date and time information. Used to convert date and time data for presentation. The default value is the time zone of the Web server.

◦ **Password**

The password for the connection string. The entry is masked, and the field is emptied when you save the data source is saved.

◦ **No Password**

When selected, the contents of the **Password** field are ignored. When clear (default), the contents of the **Password** field are added to the connection string.

◦ **Connection String**

Information used to connect to the data source. This field is automatically populated when you select a system DSN for an ODBC connection. You must manually enter a string for any other database type. Click **Edit Connection String** to open a window where you can build the connection string based on parameters for your database type.

To include the contents of the **Password** field in the connection string, use the token `<PASSWORD>` as the value for any `password=` parameter in the connection string. The token is case sensitive.

You may also type the password directly into the connection string, but it is not masked.

4. Edit the properties, as desired.
5. Click **Test Connection** to test the connection to the data source using the **Connection String** value and user credentials.
6. Click **Save** to save your changes.



Delete relational connections

You can use the Relational Data Sources page to delete connections to relational data sources. When you delete a connection, web parts that use the connection to retrieve data are no longer updated. Be sure to update web part configurations yourself or notify users of the change, and provide information on any new data sources that replace the deleted connection.

Procedure

1. Go to the PI WebParts Administration website:

Installation type	URL to PI WebParts Administration website
Non-farm, on SharePoint - 80	`http://`*`server`*`/_layouts/PI_WebParts/admin.aspx`
SharePoint farm	`http://`*`loadbalancer`*`/_layouts/PI_WebParts/admin.aspx` where *loadbalancer* is the name of the computer that runs the load balancer for the SharePoint farm

2. Under **PI WebParts Configuration**, click **PI Data Sources** to open the PI Data Sources page.

   The **Configured PI Servers** list shows the PI Servers and PI Server collectives currently configured for data exchange.

3. Select the configured data source that you want to delete, and click **Delete**.
4. Click **OK** at the confirmation prompt.

   The data source is removed from the list, and client applications can no longer access the data source.

Web-service data sources

PI WebParts supports data provided by web services, including PI ACE 2.*x* calculations and other web data sources. You can use the Web Service Data Sources page on the administration site to add, view, test, or delete connections to web-service data sources.

Topics in this section

- Add web-service connections
  Specify the address and connection parameters for the web service.
- Edit web-service connections
  Provide information to update the connection parameters.
- Delete web-service connections
  Remove connections to obsolete web services.

Add web-service connections

You can use the Web Service Data Sources page to add connections to web-service data sources.

Check your web server settings prior to adding a web-service data source.

Note:
If the web server is installed in a network environment with an IIS proxy server, the `machine.config` file must be edited in order to access web service data sources. Configure the <defaultProxy> element as follows:

```
<defaultProxy>
    <proxy
        usesystemdefault="false"
        proxyaddress="<your-proxy-server-URL>"
        bypassonlocal="true" />
</defaultProxy>
```

Procedure

1. Go to the PI WebParts Administration website:

Installation type	URL to PI WebParts Administration website
Non-farm, on SharePoint - 80	`http://`*`server`*`/_layouts/PI_WebParts/admin.aspx`
SharePoint farm	`http://`*`loadbalancer`*`/_layouts/PI_WebParts/admin.aspx` where *loadbalancer* is the name of the computer that runs the load balancer for the SharePoint farm

2. Under **PI WebParts Configuration**, click **Web Service Data Sources** to open the Web Service Data Sources page.

   The **Configured Web Services** list shows the web services currently configured for data exchange.

3. Click **New** to create a new connection to a web service.

   The connection properties are set to default values.

   Alternatively, you can select an existing web-service data source and click **Copy** to use its settings as a starting point for the new web service.

4. Enter or modify property values to connect to the new web service:
   - **Data Source Name**

     Enter a name for the web service. You cannot change this name after you save the connection to this service.
   - **Description**

     Enter a text description.
   - **Source Time Zone**

     Select the time zone of the data source. This information is used for time conversion calculations.
   - **Web Services URL**

Enter the URL path to the web service file. The file usually has an ASMX, SVC, or WSDL file extension.

- **Username** and **Change Password**

  If the web service requires login information, enter the user name and password.

- **No Password**

  Select this check box to connect without entering a password. Clear this check box if a password is required.

5. If adding an SAP web-service connection, complete any additional steps necessary for SAP. See Add SAP web-service connections.
6. Click **Get Services** to verify that you have selected the correct web service.
7. Click **Get Methods** to review the services and methods available at the web services URL. These services are used during data set configuration.
8. Click **Save** to add the new data source to the **Configured Web Services** list.

Add SAP web-service connections

To configure SAP web-service data sources follow the steps used for typical web services, but include these additional steps.

Procedure

1. Set **Service Type** to **WCF**.
2. Click **Edit Configuration** and specify the appropriate client credential type under <basicHttBinding> section of the configuration data:

```
<security mode="TransportCredentialOnly">
    <transport clientCredentialType="Basic" proxyCredentialType="None"
realm="" />
   <message clientCredentialType="UserName" algorithmSuite="Default" />
</security>
```

3. Edit the end point configuration as instructed by the web-service provider.
4. For SAP services prior to SAP ECC 6.0 release 603:
   a. Click **Edit Metadata**.
   b. In the message part, change the two instances of `parameters` to `parameter`.

Edit web-service connections

You can use the Web Service Data Sources page to view and edit connections to web-service data sources.

Procedure

1. Go to the PI WebParts Administration website:

Installation type	URL to PI WebParts Administration website
Non-farm, on SharePoint - 80	`http://server/_layouts/PI_WebParts/admin.aspx`

Installation type	URL to PI WebParts Administration website
SharePoint farm	`http://loadbalancer/_layouts/PI_WebParts/admin.aspx` where *loadbalancer* is the name of the computer that runs the load balancer for the SharePoint farm

2. Under **PI WebParts Configuration**, click **Web Service Data Sources** to open the Web Service Data Sources page.

   The **Configured Web Services** list shows the web services currently configured for data exchange.

3. Select a configured web service to view or update connection properties.



   - **Data Source Name**

     A name that data sets use to access the web service. This value cannot be changed once a data source has been saved.

   - **Description**

     Text that describes the web service connection.

   - **Source Time Zone**

     The time zone in which date and time information is returned from the data source. Used to convert date and time data for presentation.

   - **Web Services URL**

     The URL path to the web data source, or a file path to a WSDL file. If a server path without attributes is entered, click **Get Services** to populate the **Web Services** list with any services discovered at the entered location. For a saved data source, this field is disabled, but shows the path entered when the data source was saved.

   - **Service Type**

     By default the service type is set to WCF for new data sources. WCF is recommended because it provides more options for customization. ASP.NET is available for legacy configurations or web services.

   - **Username**

     User account to use for discovering Web services provided at the Web Services URL. If the service type is ASP.NET then the username is also used for data access. If the service type is WCF, click **Edit Configuration** to see the user name that is configured for data access. After a WCF type data source is saved, this field is disabled.

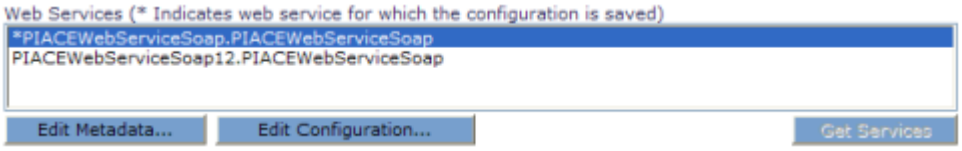
   - **Password**

Password required for the user name account. Passwords are masked, and encrypted. Once saved, the field is disabled and relabeled **Change Password**.

No attempt is made to validate the user/password pair during configuration. Improper credentials will cause data access to fail.

- **Web Services**

  A list of web services (end point names for WCF services) found at the web services URL location. The configured data source uses the selected web service.



  Click **Edit Metadata** to see the metadata associated with the web service. You can edit, copy, or paste this metadata. After you save changes, the list of web services reflects the updated metadata. The button is disabled if metadata is not available.

  Click **Edit Configuration** for WCF-based data sources to see the configuration data associated with the selected end point. You can modify the data by replacing the auto-generated configuration information with the custom data. The button is disabled for ASP.NET web-service data sources.

  Note:
  The configuration is regenerated and all custom changes are lost when the data source configuration is explicitly refreshed when **Get Services** is clicked. Also, since the configuration data is applicable to a single end point only, reconfiguring the data source to use a different end point results in the loss of any custom changes to configuration data.

  Click **Get Services** to search the web services URL to enumerate available web services by identifying WSDL files. Search results appear in the **Web Services** field. The button is disabled after the web-service definition is loaded as part of the metadata and the data source is saved. You must make any subsequent changes to the web service definition directly in the metadata.

- **Web Methods**

  A list of methods available for the selected web service. Use this read-only list to verify that the correct web service has been configured.



Click **Get Methods** to query the web service for available data retrieval methods by using available metadata. The list is informational only, and selection is disabled.

4. Click **Save** to save any changes made.

Delete web-service connections

You can use the Web Service Data Sources page to delete connections to web-service data sources. When you delete a connection, web parts applications that use the connection to retrieve data are no longer updated. Be sure to update web parts configurations yourself or notify users of the change, and provide information on any new data sources that replace the deleted connection.

Procedure

1. Go to the PI WebParts Administration website:

Installation type	URL to PI WebParts Administration website
Non-farm, on SharePoint - 80	`http://server/_layouts/PI_WebParts/admin.aspx`
SharePoint farm	`http://loadbalancer/_layouts/PI_WebParts/admin.aspx` where *loadbalancer* is the name of the computer that runs the load balancer for the SharePoint farm

2. Under **PI WebParts Configuration**, click **Web Service Data Sources** to open the Web Service Data Sources page.

   The **Configured Web Services** list shows the web services currently configured for data exchange.

3. Select the configured data source that you want to delete, and click **Delete**.
4. Click **OK** at the confirmation prompt.

   The data source is removed from the list, and client applications can no longer access the data source.

PI Asset Framework support

PI WebParts Services has built-in support for PI Asset Framework (PI AF) data; you do not need to explicitly configure a PI AF data source or data sets on the administration pages.

To maintain connections to a PI AF server, use PI System Explorer running on the computer where PI WebParts Services is installed. However, you can configure PI AF elements and attributes with PI System Explorer running on any computer.

PI WebParts Services does not support PI AF attributes with data references that return arrays of values.

Data sets

This section describes how to use the PI Web Parts Administration page to create data sets from configured data sources.

Once a data source is created and PI WebParts Services can connect to the data provider, you can define the information provided through a connection by creating a data set that uses the data source.

PI WebParts Services supports PI calculation data, relational queries, and web-service queries as data sets.

Topics in this section

- PI calculation data sets
  PI calculation data sets are based on PI data and associated calculations.
- Relational data sets
  Relational data sets are derived from relational data sources accessible to your PI system.
- Web-service data sets
  Web-service data sets are derived from web-service data sources accessible to your PI system.
- Delete a data set
  Delete obsolete data sets from the administration pages.

PI calculation data sets

PI calculation data sets include both PI summary data computations (for example, averages, minimums, and standard deviations) and PI expression data (such as the result of an evaluated PI performance equation).

You can use the PI Calculation Datasets page to add, view, edit, or delete PI calculation data sets.

Topics in this section

- Add PI calculation data sets
  Specify columns and properties, then preview the results.
- Edit PI calculation data sets
  Provide information to describe the data set, its columns and calculation parameters.
- Properties that define PI calculation data sets
  Calculation parameters are used to compute PI point values and add new data to the data set.
- Some calculations available to PI calculation data sets
  Summary calculations may be used to add additional data columns.

Add PI calculation data sets

Procedure

1. Go to the PI WebParts Administration website:

Installation type	URL to PI WebParts Administration website
Non-farm, on SharePoint - 80	`http://server/_layouts/PI_WebParts/admin.aspx`

Installation type	URL to PI WebParts Administration website
SharePoint farm	`http://loadbalancer/_layouts/PI_WebParts/admin.aspx` where *loadbalancer* is the name of the computer that runs the load balancer for the SharePoint farm

2. Under **PI WebParts Configuration**, click **PI Calculation Datasets** to open the PI Calculation Datasets page.

   The **Configured Datasets** list shows the PI calculation data sets available to the SharePoint Web server.

3. Click **New** to create a new PI calculation data set.

   The property fields reset to default values.

   Alternatively, you can select an existing PI calculation data set and click **Copy**.

4. Enter or modify property values to define the new data set:
   - **Configuration Name**

     Enter a name for the PI calculation data set. You cannot change the name after you save the data set.
   - **Expression**

     Specify a performance equation to evaluate for the data set. For a full list of performance equations and syntax examples, refer to the *PI Server Applications User Guide* or the *PI 3 Performance Equations Help File*.

   Note:
   If the string entered in the **Expression** field is a single PI point with bracketing quotes, such as `'sinusoid'`, the data set is interpreted as a summary data set for that PI point.

   Default values are assumed for any properties that you do not set.

5. Click **Get Columns** to test the expression syntax and data set configuration.

   Available calculations are inserted into the **Columns** table.

   Columns

Name	Description
Average	
Maximum	
Minimum	
PercentGood	

   If an error is returned, verify the syntax and point names in the **Expression** field.

6. In the **Description** fields, enter text descriptions for columns, if desired.
7. Click **Preview** to open a preview window that shows the retrieved data set in columns.

   The window presents data in the time zone of the data source (PI Server) and in PI time format (dd-mmm-yy HH:mm:ss).

8. Click **Save** to add the new data set to the list of PI calculation data sets.

Edit PI calculation data sets

Procedure

1. Go to the PI WebParts Administration website:

Installation type	URL to PI WebParts Administration website
Non-farm, on SharePoint - 80	`http://server/_layouts/PI_WebParts/admin.aspx`
SharePoint farm	`http://loadbalancer/_layouts/PI_WebParts/admin.aspx` where *loadbalancer* is the name of the computer that runs the load balancer for the SharePoint farm

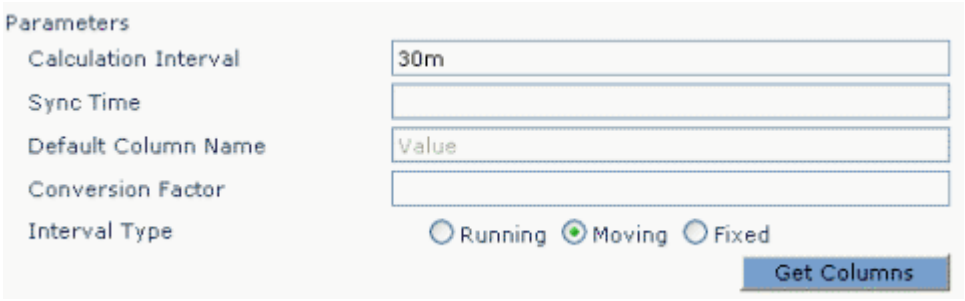
2. Under **PI WebParts Configuration**, click **PI Calculation Datasets** to open the PI Calculation Datasets page.

   The **Configured Datasets** list shows the PI calculation data sets available to the SharePoint Web server.

3. From the **Configured Datasets** list, select a data set to view and change its properties.



   The properties under **Parameters** control how data are calculated on the PI Server.



4. Click **Get Columns** to test the expression syntax and data set configuration.

   The available calculations are inserted into the **Columns** table.



   If an error is returned, verify the syntax and point names in the **Expression** field.

5. In the **Description** fields, enter text descriptions for columns, if desired.
6. Click **Preview** to open a Preview window that shows the retrieved data set in columns.

   The window presents data in the data source (PI Server) time zone and in PI time format (dd-mmm-yy HH:mm:ss).
7. Click **Save** to save changes that you make to property values.

Properties that define PI calculation data sets

The PI Calculation Datasets page lists the properties that define PI calculation data sets. The properties under **Parameters** control how data are calculated on the PI Server.

Property	Definition
Configuration Name	A name that client applications use to access the data set. This value cannot be changed once a data set has been saved.
Description	A description of the current data set.
Data Source	The configured PI Server to use when calculating the data set.
Cache Interval	An integer representing the number of seconds during which the web server caches the results of the query. If **Cache Interval** is `0`, results are not cached and the data source is queried every time an update is requested.
Expression	A PI point name or a PI performance equation to be evaluated.
Stepped Plot	When selected, data are plotted as a staircase trace on trends. When cleared, data are displayed as a curved trace.
Calculation Interval	The span of time over which point values are aggregated to calculate a value. PI time intervals such as `1m` and `1h` are accepted. Very small calculation intervals can negatively affect system performance. Consider increasing calculation or cache intervals if you experience a reduction in performance caused by high loads on CPU and memory.
Sync Time	The clock time to which the calculation interval is synchronized. For example, to calculate an hourly average on the hour for a PI tag, set the **Calculation Interval** to `1h` and **Sync Time** to `00:00:00` (midnight). The default value is 00:00:00. If no value is specified, the current time is used. This field is not used when **Interval Type** is set to **Moving**.
Default Column Name	The column that contains the result of an expression calculation or the current value of a PI tag. In the current version, the **Default Column Name** is always **Value** and cannot be changed.
Conversion Factor	Determines how the Total column is calculated. By default, Total represents the total units over **24h** but can be configured to use a different interval; for example, revolutions per minute. The default interval (a day or 24 hours) is used if the field is left blank. Acceptable values are PI time intervals such as **1m**, for 1-minute increments, and **1h** for 1-hour increments. The raw conversion factor (for example, **24** for an hourly unit conversion) can also be used.

Property	Definition
Interval Type	The calculation method, which can be **Fixed**, **Running**, or **Moving**. Calculations for the **Fixed** and **Running** methods require a value for the **Sync Time** field.

Interval types

The **Interval Type** property specifies how to handle aggregate calculations over time.

- If interval type is **Fixed**, values are calculated for each interval from the **Sync Time** to the end of the most recently completed **Calculation Interval**. Data in an incomplete interval (that is, the very newest data) are ignored so that each calculation represents a full **Calculation Interval** of data.

  For example, if **Sync Time** is **00:00:00** and the **Calculation Interval** is **1h**, a Web client requesting a value at **02:10:00** would receive values from two calculations: one for the interval **[00:00:00, 01:00:00]** and one for **[01:00:00, 02:00:00]**.

- If interval type is **Running**, values are calculated for each interval from the **Sync Time** to the current time. All data are used; however, the most recent calculation may be based on a partial calculation interval of data.

  For example, if Sync Time is **00:00:00** and the **Calculation Interval** is **1h**, a Web client requesting a value at **02:10:00** would receive values from three calculations: one for the interval **[00:00:00, 01:00:00]**, one for **[01:00:00,02:00:00]**, and one for **[02:00:00, 02:10:00]**.

- If interval type is **Moving**, the **Sync Time** is ignored, and values are calculated for full intervals moving backwards from the current time. Each calculation represents a full **Calculation Interval** of data.

  For example, if the **Calculation Interval** is **1h** a Web client requesting a value at **02:10:00** would receive values for the interval **[00:10:00, 01:10:00]**, for **[01:10:00, 02:10:00]**.

Some calculations available to PI calculation data sets

The **Columns** table on the PI Calculation Datasets page shows the calculations that a configured PI calculation data set can retrieve. Available calculations depend on the performance equation.

The following table shows calculations that might be available as data set columns:

Calculation	Description
Average	The average value of the expression for the calculation interval and type.
Maximum	The maximum value of the expression for the calculation interval and type.
Minimum	The minimum value of the expression for the calculation interval and type.
PercentGood	A number between **0** and **100** that represents the percentage of data with good values during the calculation period. For time-weighted calculations, **PercentGood** is based on time.

Calculation	Description
Range	The span of values for the expression for the calculation interval and type.
StdDev	The standard deviation of values for the expression for the calculation interval and type.
Total	The total as calculated over the specified Conversion Factor. If no Conversion Factor is specified, Total is calculated over one day.
Value	The value of the expression for the calculation interval and type as of the time stamp. In the case of summary data sets, this column holds the value of the tag.

Relational data sets

A relational data set retrieves the results from an SQL query of a relational database data source in tabular format. You can also use a stored procedure saved in the data source as the basis for a data set.

You can use the Relational Datasets page on the administration site to add, view, edit, or delete relational data sets.

Topics in this section

- Add relational data sets
  Specify columns and properties, then preview the results.
- Edit relational data sets
  Provide information to describe the data set, its columns and calculation parameters.
- Properties that define relational data sets
  Relational properties are used to manage and resolve queries to relational data sources.

Add relational data sets

Use the Relational Datasets page to create a new relational data set.

Procedure

1. Go to the PI WebParts Administration website:

Installation type	URL to PI WebParts Administration website
Non-farm, on SharePoint - 80	`http://server/_layouts/PI_WebParts/admin.aspx`
SharePoint farm	`http://loadbalancer/_layouts/PI_WebParts/admin.aspx` where *loadbalancer* is the name of the computer that runs the load balancer for the SharePoint farm

2. Under **PI WebParts Configuration**, click **Relational Datasets** to open the Relational Datasets page.

   The **Configured Datasets** list shows the relational data sets available to the web server.

3. Click **New** to create a new relational data set.

   The property fields reset to default values.

Alternatively, you can select an existing relational data set and click **Copy**.

4. Enter or modify property values to define the new data set:
   - **Data Set Name**

     Enter a name for the relational data set. You cannot change the name after you save the data set.
   - **Data Source**

     Select a configured relational data source for the data set.
   - **SQL Statement**

     Enter a SQL statement or stored procedure to retrieve data from the data source. You can:
     - Type or paste a statement as text, or type the name of a stored procedure.
     - Click **Open Query** to import a SQL statement from a file.
     - Click **Clear** to clear the field.

     For example, enter `select * from orders` to retrieve all columns from the Northwind Orders table in SQL Server. Use question marks ('?') to enter placeholders in the select statement.

   Default values are assumed for any properties that you do not set.
5. Click **Verify SQL** to test the SQL statement or stored procedure.

   If the statement or stored procedure is invalid, the data source returns an error string and the **Place Holders** and **Columns** tables are cleared. In this case, correct the syntax of the SQL statement or the stored procedure, and then click **Verify SQL** again.

   If the SQL statement or stored procedure is valid:

   - A row is added to the **Place Holders** table for each placeholder character in the SQL statement or each placeholder character or parameter in the stored procedure.

   - Columns are inserted for the SQL statement or stored procedure to return into the **Columns** table.

6. Configure placeholder information and provide text descriptions for data set columns.
7. Click **Preview** to open a Preview window that shows the retrieved data set in columns.

   The window presents data in the time zone of the data source.
8. Click **Save** to add the new data set to the list of relational data sets.

Edit relational data sets

Procedure

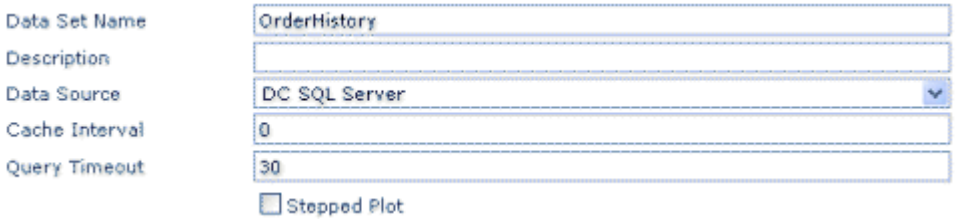
1. Go to the PI WebParts Administration website:

Installation type	URL to PI WebParts Administration website
Non-farm, on SharePoint - 80	`http://server/_layouts/PI_WebParts/admin.aspx`
SharePoint farm	`http://loadbalancer/_layouts/PI_WebParts/admin.aspx` where *loadbalancer* is the name of the computer that runs the load balancer for the SharePoint farm

2. Under **PI WebParts Configuration**, click **Relational Datasets** to open the Relational Datasets page.

   The **Configured Datasets** list shows the relational data sets available to the web server.

3. Select a configured data set to view and update its properties.

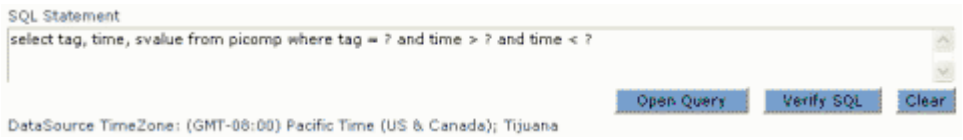


   Default values are assumed for any properties that you do not set.

4. In the **SQL Statement** field, enter a SQL statement or stored procedure that retrieves data from the data source.

   You can:

   - Type or paste a statement as text, or type the name of a stored procedure.
   - Click **Open Query** to import a SQL statement from a file.
   - Click **Clear** to clear the field and the information in the Place Holders and Columns tables.

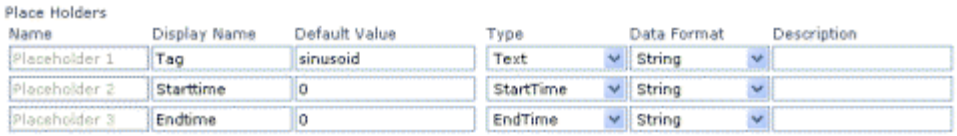


5. Click **Verify SQL** to test the SQL statement or stored procedure.

   If the statement or stored procedure is invalid, the data source returns an error string and the **Place Holders** and **Columns** tables are cleared. In this case, correct the syntax of the SQL statement or the stored procedure, and then click **Verify SQL** again.

   If the SQL statement or stored procedure is valid:

   - A row is added to the **Place Holders** table for each placeholder character in the SQL statement or each placeholder character or parameter in the stored procedure.



- Columns are inserted for the SQL statement or stored procedure to return into the **Columns** table.



6. Configure placeholder information and provide text descriptions for data set columns.
7. Click **Preview** to open a Preview window that shows the retrieved data set in columns.

   The window presents data in the time zone of the data source.
8. Click **Save** to save changes to the properties.

Properties that define relational data sets

The Relational Datasets page lists the properties that define relational data sets:

Property	Definition
Data Set Name	A name used to access the data set. This value cannot be changed once a data set has been saved.
Description	A description of the current data set. This text is shown in the Data sets dialog box.
Data Source	The relational data source for this data set. The query is sent to this data source.
Cache Interval	An integer representing the number of seconds during which the Web server caches the results of the query. If **Cache Interval** is **0**, results are not cached and the data source is queried every time that an update is requested.
Query Timeout	A command execution timeout for relational data sets, specified in seconds. The default value is **30** seconds. A **0** value means a timeout is not enforced. The timeout applies to the full execution of the query; if partial results are returned by the data source, they are discarded and an error is returned if the timeout limit is exceeded. Note that drivers or data sources may not be able to honor the timeout setting.
Stepped Plot	Plot data as a stairstep trace on trends. Clear the check box to display data as a curved trace on trends.
SQL Statement	A SQL statement or stored procedure used to retrieve data from the data source.
Data Source Time Zone	The time zone configured for the selected data source, used to determine the time context for absolute dates in date-time placeholder default values.

Property	Definition
Place Holders	Each row contains fields used to process placeholders in the SQL statement or stored procedure, as well as parameters in the stored procedure. Values in these fields are used to verify SQL when previewing the data, and in client applications using the data set.
Columns	Each row represents a column returned by the SQL statement or stored procedure. You can enter a text description for each column name.

SQL placeholders

A placeholder ('?' character) is a text character used in a SQL statement or stored procedure in place of a PI Server tag or text. When the SQL statement is executed, the '?' character is replaced by a specified value or expression before it is passed to the relational data source. The placeholder acts as a variable, allowing users of the query to supply parameters that produce different data using the same SQL query.

You can use the following types of placeholders in relational data sets:

- Text

  The placeholder character is replaced with a text string.

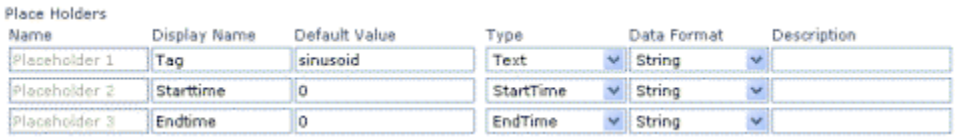
- StartTime or EndTime

  The placeholder character is replaced with the start or end time for a data collection interval.

- ResolveTag

  The placeholder character is replaced with the value of a PI point. The PI Server is queried first for the requested placeholder values. Then the relational data source is queried once for each PI query value, using the PI values as filters.

After you enter a SQL statement with placeholder characters and click **Verify SQL**, a row is added to the Place Holders table for each '?' character in the SQL statement. The first row, named **Placeholder 1**, corresponds to the first '?' character. The second row, named **Placeholder 2**, corresponds to the second '?' character, and so on. Placeholders are evaluated sequentially, from left to right through the SQL statement, and their names cannot be changed.



The following columns are used to expose placeholders as part of a relational data set:

Property	Definition
Display Name	The label used to describe the placeholder on input fields.
Default Value	A default value for the placeholder. This field cannot be empty.
Type	The type of placeholder, indicating how it is resolved by the data source, either Text, StartTime, EndTime, or ResolveTag.

Property	Definition
Data Format	Identifies the data type of the placeholder. Available options are String, Number, DateTime, UTCSeconds or UTCDateTime. Number accepts either a period (.) or a comma (,) as the decimal separator for floating point values, to avoid conflicts with different Locale settings on client and server computers.
Description	A description of the placeholder.

Note:
Oracle (Microsoft Provider) uses different SQL syntax for placeholders. In Oracle a placeholder is denoted by a colon character (:) as a prefix, for example:

```
select * from sinusoid where timestamp > :a and timestamp < :b
```

Web-service data sets

A web-service data set defines a binding to a specific method of a web-service data source. The Web Service Description Language (WSDL) published by the web service is used to identify the web methods and .NET data types, provide corresponding parameter values, and to determine the URL for the target web service.

You can use the Web Service Datasets page to add, edit, or delete a web-service data set.

Topics in this section

- Add a web-service data set
  Specify columns and properties, then preview the results.
- Edit web-service data sets
  Provide information to describe the data set, its columns, and calculation parameters.
- Properties that define web-service data sets
  Web services properties are used to manage and resolve queries to web-service data sets.
- Method Parameters table of web-service data sets
  Specify from available parameters for each selected method.
- Columns table of web-service data sets
  Specify the mapping of data set parameters to columns.
- Rules for complex structures in web-service data sets
  Rules determine how complex web service data sets are derived from entered configuration.

Add a web-service data set

Procedure

1. Go to the PI WebParts Administration website:

Installation type	URL to PI WebParts Administration website
Non-farm, on SharePoint - 80	`http://server/_layouts/PI_WebParts/admin.aspx`

Installation type	URL to PI WebParts Administration website
SharePoint farm	`http://loadbalancer/_layouts/PI_WebParts/admin.aspx` where *loadbalancer* is the name of the computer that runs the load balancer for the SharePoint farm

2. Under **PI WebParts Configuration**, click **Web Service Datasets** to open the Web Service Datasets page.

   The **Configured Datasets** list shows the web service data sets available to the SharePoint web server.

3. Click **New** to create a new web-service data set.

   The property fields reset to default values.

   Alternatively, you can select an existing web-service data set and click **Copy**.

4. Enter or modify property values to define the new data set:
   - **Data Set Name**

     Enter a name for the web-service data set. You cannot change this name after you save the data set.
   - **Data Source**

     Select a configured web-service data source to call the method from.
   - **Service Methods**

     Select a service method to use for the data set. The **Method Parameters** table is populated.

   Default values are assumed for any properties that you do not set.

5. In the **Method Parameters** table, edit input parameters to use when calling the web-service method.

6. Click **Get Columns** to test the specified input parameters.

   The web-service method is executed and verifies that the parameters are valid.

   If errors are returned, refer to the web service to determine appropriate input parameters for the selected method. Correct the input parameters and click **Get Columns** again.

   If the parameters a valid, the **Columns** table is populated with all the parameters that the web-services data set can return.

7. In each row of the table, configure the data column:
   - From the **Behavior** list, select a behavior.
   - In the **Description** field, enter a text description of the column, if desired.

   Note:
   You must set **Behavior** to **DateTime** for the column that contains date and time data. Otherwise, clients will not know which column contains the time stamps for the data set.

8. Click **Preview** to view the data-set columns retrieved.

The preview presents data in the time zone of the web service and in PI time format (`dd-mmm-yy HH:mm:ss`).

9. Click **Save** to add the new data set to the list of web-service data sets.

Edit web-service data sets

You can use the Web Service Datasets page to view and edit configured web-service data sets.

Procedure

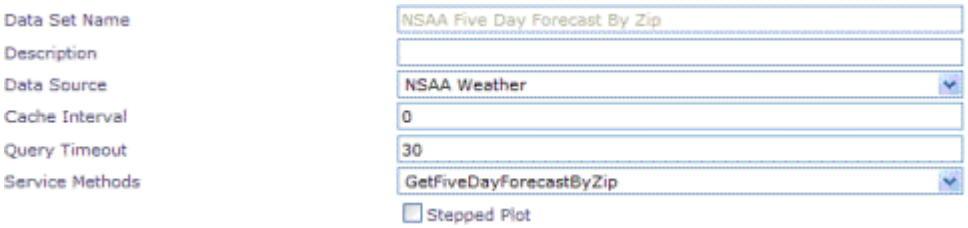
1. Go to the PI WebParts Administration website:

Installation type	URL to PI WebParts Administration website
Non-farm, on SharePoint - 80	`http://server/_layouts/PI_WebParts/admin.aspx`
SharePoint farm	`http://loadbalancer/_layouts/PI_WebParts/admin.aspx` where *loadbalancer* is the name of the computer that runs the load balancer for the SharePoint farm

2. Under **PI WebParts Configuration**, click **Web Service Datasets** to open the Web Service Datasets page.

   The **Configured Datasets** list shows the web service data sets available to the SharePoint web server.

3. Select a configured data set to view and update its properties.



   Default values are assumed for any properties that you do not set.

   After you select a method in **Service Methods**, the **Method Parameters** table is populated.

4. If desired, click **Clear** to clear the fields below the **Service Methods** field, including the **Method Parameters** table and the **Columns** table, and discard any changes.



5. In the **Method Parameters** table, edit input parameters to use when calling the web-service method.

6. Click **Get Columns** to test the specified input parameters.

   The web-service method is executed and verifies that the parameters are valid.

   If errors are returned, refer to the web service to determine appropriate input parameters for the selected method. Correct the input parameters and click **Get Columns** again.

If the parameters a valid, the **Columns** table is populated with all the parameters that the web-services data set can return.

7. In each row of the table, configure the data column:
   - From the **Behavior** list, select a behavior.
   - In the **Description** field, enter a text description of the column, if desired.

   Note:
   You must set **Behavior** to **DateTime** for the column that contains date and time data. Otherwise, clients will not know which column contains the time stamps for the data set.

8. Click **Preview** to view the data-set columns retrieved.

   The preview presents data in the time zone of the web service and in PI time format (`dd-mmm-yy HH:mm:ss`).

9. Click **Save** to save changes you made to the data set.

Properties that define web-service data sets

The Web Service Datasets page lists the properties that define web-service data sets:

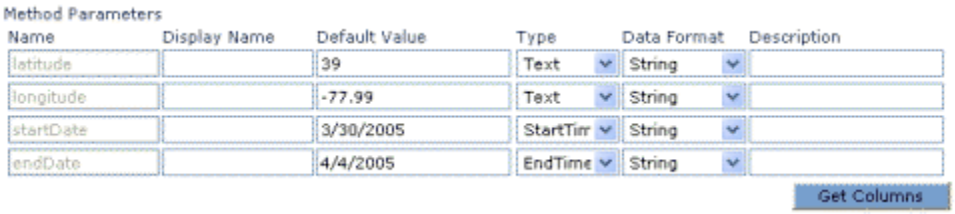
Property	Definition
Data Set Name	A name that clients use to access the data set. This value cannot be changed once a data set has been saved.
Description	A description of the current data set. This text appears on the **Datasets** dialog box.
Data Source	A web-service data-source provider for the data set.
Cache Interval	An integer representing the number of seconds the web server caches the results of the query. If **Cache Interval** is **0**, results are not cached and the data source is queried every time that an update is requested.
Query Timeout	Command execution timeout in seconds (default 30 seconds). A value of zero disables timeout. The data source may return partial results, but these are discarded and an error is returned if the timeout is exceeded.
Stepped Plot	Plot data as a stair-step trace on trend charts. When cleared, data are displayed as a curved trace on trend charts.
Service Methods	The web service method that returns the desired data set columns. Select a method to populate the **Method Parameters** table.
Remove Parameters	A list of semicolon-delimited path names used to hide method parameters and use their default values. Each path name corresponds to a row that is excluded from the list of method parameters returned by the data set. If the prefix of a flattened name matches a listed path name, then the type and all associated sub-types are ignored. XML element attributes are not handled, and a blank value is assumed for data sets created by previous versions.

Property	Definition
Data Path	A flattened path name used to set a single parent element as the root. The **Data Path** denotes a point of interest in the returned type of the web method. Expansion of the return type is governed by specific rules. Only one entry is accepted in this field. XML element attributes are not handled, and a blank value is assumed for data sets created by previous versions. Click **View Data Paths** to open a dialog box that lists possible data paths that you can choose. You can select one path and insert into the **Data Path** field to replace existing contents.
Error Description Path	A list of semicolon-delimited, flattened path names used to indicate errors in the returned data set. The **Error Description Path** denotes a point of interest in the returned data such that if an associated element is not empty, the method fails and an error message is generated. The error message concatenates strings found at each enumerated path element. This field can be empty, in which case it is ignored. If the method call fails (for example, the web service call times out), that error is returned. Click **View Error Paths** to open a dialog box that lists possible error description paths. You can select multiple paths and insert into the **Error Description Path** field to replace existing contents. The dialog box shows a message if the list of paths is too long.

Note:
The **Remove Parameters**, **Data Path**, and **Error Description Path** fields are not exclusive. For example, error messages returned for columns in the **Error Description Path** field are displayed even if they are not included in the data set defined by the **Data Path** field. None of these fields are supported for PI ACE data sets.

Method Parameters table of web-service data sets

The **Method Parameters** table on the Web Service Datasets page shows valid parameters for the method selected in **Service Methods**. These parameters are used to request data from the web-service data source.



After you select the method, the fields in the table are populated with valid parameters for the method:

Property	Definition
Name	The name used by the method. This name cannot be changed.
Display Name	The name used to display this parameter on the Datasets tool part in PI Web Parts.

Property	Definition
Default Value	A default value for the parameter. This field cannot be empty.
Type	The type of placeholder, indicating how it is resolved by the data source, either Text, StartTime, EndTime, or ResolveTag.
Data Format	The format data are returned in (String, UTC Seconds, DateTime, UTC DateTime, or Number).
Description	A description of the parameter.

Columns table of web-service data sets

The **Columns** table on the Web Service Datasets page lists all the web-service parameters that the configured web-services data set can return.



Due to the hierarchical complexity of some web-service data, specific rules and guidelines should be used to map web-service data values into consistent tabular formats. Column names appear in dot notation if the element has a parent, for example `Location.Longitude`, and are flattened one level deep from the Data Path element (if any), unless it is a .NET data set. No filtering is done on the output columns.

The table includes one row for each column that the method returns. The table contains the following properties:

Property	Definition
Name	The name of the column, in dot notation, if it has a parent. This name cannot be changed. The manufactured name of the result (first possible element of the path name) is omitted from the flattened name. The path name is further trimmed using the Data Path configuration setting. A tooltip shows the full name.
Behavior	Either **Default** or **DateTime**. This field indicates the time column returned by the data set. **Note:** You must set **Behavior** to **DateTime** for the column that contains date and time data. Without this specification, client applications will not know which column contains the time stamps for the data set.
Description	A description of the column.

Rules for complex structures in web-service data sets

Web services with complex data structures, including XML element nesting and data arrays, are configurable as data sets. The notion of a flattened hierarchy is central to understanding the handling of parameters and results of web methods in these cases.

Flattened path name syntax is used to identify a specific property within a type (class) hierarchy. The flattened name is used to traverse the type hierarchy, and consists of a succession of property or field names as defined by the type hierarchy, with each name separated by a dot (.).

The following rules summarize how web service data-set columns are generated. They are applicable only to web services implemented using .NET data types:

- Rule 1: If the Data Path configuration points to a .NET data set, the set is returned as-is. Otherwise, .NET data sets are ignored if they appear in the returned data type.
- Rule 2: At the top level (based on Data Path), a simple type (float, integer, enumeration) or an array of simple types is given the column name **`Value`**.
- Rule 3: Column names are based on the flattened path name. Only the path following the Data Path configuration setting is used, and only one level of flattening is attempted. Other complex elements and arrays at deeper levels are ignored and columns are not returned.
- Rule 4: If the Data Path points to an array, the entire array is returned as a table. The number of rows returned equals the number of array elements.
- Rule 5: An array is flattened if it is a member of the structure being flattened, and does not meet the depth criteria described above. Sibling column values are duplicated for each row created for the array. For example, if the return type defines a string **`s`** and an array **`a`** of 3 integers, then a table of 2 columns (one for **`s`** and other for **`a`**) and 3 rows is returned. The string value is duplicated in each of the 3 rows.
- Rule 6: Only the first array encountered is flattened.

Clients can consume simple types or tables, or .NET data sets. The following sections contain use cases that show how to implement complex web-service data sets and describe how to map parameters and results to managed types. These use cases reference managed types and web-method signatures instead of WSDL exposed by the web service, which is assumed to be generated automatically from managed types.

Simple parameters and simple result

This use case shows how to expose a simple web-services data set with basic configuration.

The following web method takes a set of parameters and returns a simple type:

```
[WebMethod]
public string SimpleParams(String prefix, int i, double d) (…)
```

A web-service data set can be defined to access this method by using WSDL published by the web service to determine the necessary parameters and result type. In this case, assuming blank values for Remove Parameters, Data Path, and Error Description Path settings, the following parameters are exposed: **`prefix`**, **`i`**, and **`d`**.

Default parameter values can be specified during configuration, and marked as **Text**, **StartTime**, **EndTime** or **ResolveTag** to indicate how the query is processed using the parameter.

The result is a single row with column name **Value**. If the **Remove Parameters** value is `prefix;i`, then only the **`d`** parameter appears on the data-set configuration page.

Note:
The **Data Path** and **Error Description Path** parameters do not pertain as the example considers only input parameters.

Parameter as child class

This use case occurs when a web-method parameter is a complex type, such as:

```
[WebMethod]
public String MyWebMethod(MyParamClass mpc) {…}
```

The complex type, in which the parameter class contains child classes and peer elements of simple types, is defined as follows:

```
public struct MyChild2Class {
    public int mc2c_i;
}
public struct MyChildClass {
    public String mcc_s;
    public MyChild2Class mcc_mc2c;
    public int mcc_i;
}
public struct MyParamClass {
    public int mpc_i;
    public MyChildClass mpc_mcc1;
    public int[] mpc_ia;
    public String mpc_s;
    public MyChildClass mpc_mcc2;
}
```

The exposed parameters have the following path names:

```
mpc.mpc_i
mpc.mpc_mcc1.mcc_s
mpc.mpc_mcc1.mcc_i;
mpc.mpc_s
mpc.mpc_mcc2.mcc_s
mpc.mpc_mcc2.mcc_i
```

Arrays are ignored and the Data Path is used as a starting point of flattening the returned type. For example, if Remove Parameters is set to `mpc.mpc_s;mpc.mpc_mcc1`, then the only parameters exposed in the configuration pages are:

```
mpc.mpc_i
mpc.mpc_mcc2.mcc_s
mpc.mpc_mcc2.mcc_i
```

Data Path and Error Description Path are not relevant for this use case.

The next four cases are for handling a web-method result with the following method signature:

```
[WebMethod]
public MyResultClass MyWebMethod() {…}
```

The return class is also a complex type:

```
public struct MyResultClass // Result class
{
    public int mrc_i;   // simple integer
    public int[] mrc_ia;    // integer array
    public DataSet mrc_ds;  // .NET DataSet
    public String mrc_s;    // simple string as a peer member
    public MyResultChildClass mrc_mrcc; // Nested child structure
    public String mrc_err;  // An error status
}
public struct MyErrorClass  // Error structure
```

```
{
    public String mec_s;    // Error status embedded in a structure
    public int mec_i;       // Error code
}
public struct MyResultChildClass    // Child class
{
    public String mrcc_s;   // simple string in child class
    public double[] mrcc_da;    // array of doubles in child class
    public MyErrorClass mrcc_mec;   // error info in structure
    public DataSet mrcc_ds; // .NET DataSet
    public MyResultChild2Class mrcc_mrc2c1; // first grandchild instance
    public int mrcc_i;  // simple int as a peer member in child class
    public MyResultChild2Class mrcc_mrc2c2; // second grandchild instance
}
public struct MyResultChild2Class   // Grand-child class
{
    public String mrc2c_s;  // simple string
    public int[] mrc2c_ia;  // array of ints
    public MyErrorClass mrc2c_mec;  // error info
    public double mrc2c_d;  // simple double
}
```

Result as complex type

In this use case, the Data Path and Error Description Path properties are empty. The following result columns are exposed:

```
mrc_i
mrc_ia
mrc_s
mrc_mrcc.mrcc_s
mrc_mrcc.mrcc_i
mrc_err
```

This use case illustrates rule 3, in which column names use the path name following the Data Path setting. One level of flattening is attempted and other complex types (.NET DataSets or deeper classes) are ignored.

According to rule 5, an array is flattened (mrc_ia), and the number of rows is the number of array elements. Sibling column values are duplicated (mrc_i, mrc_s, mrc_mrcc.mrcc_s, mrc_mrcc.mrcc_i). Although this example processes only one array at this level, a second array would be ignored under rule 6.

As a variation of this use case, the Error Description Path could be set to:

`mrc_err;mrc_mrcc.mrcc_mrc2c2.mrc2c_mec`

In this case, any non-empty string value (in the mrc_err member of the result class or in the deeply nested member of the second instance of the child class) would be treated as an error condition.

Result as child class

This use case occurs when the Data Path refers to a nested structure within the returned result. For example, setting Data Path to `mrc_mrcc` returns the following columns:

```
mrcc_s
mrcc_da
mrcc_mec.mec_s
mrcc_mec.mec_i
```

```
mrcc_mrc2c1.mrc2c_s
mrcc_mrc2c1.mrc2c_d
```

The Data Path is used as a starting point of flattening the returned type. Other rules are applied as in the previous use case.

Result as a .NET data set

This use case occurs when the Data Path points to a .NET data-set instance, such as `mrc_ds` or `mrc_mrcc.mrcc_ds`.

In either case, the .NET data set is returned, ignoring all other types in the result. This is an application of rule 1.

Result as an array

This use case occurs when the returned result is an array, or the Data Path points to an array. For example, if the Data Path is `mrc_mrcc.mrcc_da`, then a single column 'Value' is returned, each row containing the value of an array element. This is an application of rules 2 and 4.

A method that returns a complex array, such as

```
[WebMethod]
public MyResultClass[] MyWebMethod(…) {…}
```

returns the following columns:

```
mrc_i
mrc_s
mrc_err
```

The number of rows is the number of elements in the returned array. This is an application of rules #3 and #4. Compare this result with the earlier case when a single instance of the structure was returned by the web method.

Delete a data set

Use the appropriate page on the Administration site to delete a data set. After you delete a data set, client applications that display or process that data can no longer access it. Be sure to update client applications or notify users of the change, and provide information on any new data sets that replace the deleted data set.

Procedure

1. Under **Datasets**, in the Navigation pane of the Administration site, click the type of data set you want to delete:
   - **PI Calculation**
   - **Relational**
   - **Web Service**
2. From the **Configured Datasets** list, select the data set that you want to delete.
3. Click **Delete**, and then click **OK** to confirm that you want to delete the data set.

   The data set is removed from the list and client applications can no longer access the data set.

Advanced topics

Topics in this section discuss advanced configuration issues useful in some installations, such as migration from PI Module Database to PI AF, load balancing, and URL specification.

Topics in this section

- MDB to PI AF migration
  If upgrading from versions earlier than PI WebParts 2010, upgrade your PI Server and migrate your MDB data to PI AF, if your web parts reference modules and aliases.
- Network load-balanced web servers
  Use load balancing to increase availability and improve performance.
- Windows Network Load Balancing (NLB)
  Follow the recommended settings when using PI WebParts on a Windows Network Load Balancing (NLB) cluster.
- URL conversion
  PI WebParts supports the conversion of a URL to a public URL for support of multiple authentication zones.

MDB to PI AF migration

PI WebParts no longer supports the display of enterprise asset data stored in PI Module Database (MDB). If you are upgrading from versions earlier than PI WebParts 2010 and your web parts reference modules and aliases, you must first upgrade your PI Server and migrate the data from MDB to PI AF. Migrating from MDB to PI AF requires no action on your part. PI Server 2010 migrates and synchronizes existing MDB data to PI AF elements.

Starting with PI WebParts 2010, when you open a pre-existing MDB-relative display, PI WebParts converts it to a PI AF element-relative display. The display points to PI AF.

PI WebParts does not verify the PI Server version. PI WebParts can communicate with older versions of PI Server, but cannot communicate with their module databases. If you upgrade a PI WebParts installation that made substantial use of MDB and did not first update PI Server, all of your MDB configuration in PI WebParts would fail with `Element Not Found` or `Attribute Not Found` error messages.

You cannot edit web part pages to fix these errors. Instead, you must upgrade to PI Server 2010.

If you already upgraded PI Server, but the on-the-fly conversion of the MDB configuration in PI WebParts to PI AF fails, you will see `Element Not Found` or `Attribute Not Found` error messages.

Network load-balanced web servers

There are many reasons to use load balancing for SharePoint server farms, including increased availability and improved performance and scalability.

Load balancing may be implemented through dedicated hardware, or services provided from the server operating system. Functional and organizational requirements as well as licensing concerns may also affect how you choose to deploy SharePoint.

PI WebParts is compatible with SharePoint front-end web servers that are load balanced. To determine your optimal SharePoint deployment, consult Microsoft recommendations.

Windows Network Load Balancing (NLB)

Windows Network Load Balancing (NLB) is an operating system approach to load balancing. PI WebParts is compatible with an NLB cluster. Several configuration settings are recommended to use PI WebParts on an NLB cluster.

Refer to the Microsoft Network Load Balancing Deployment Guide for further information on NLB clustering.

Topics in this section

- Network interface card (NIC) configuration for NLB
  To support NLB, install two network interface cards in each front-end web server.
- Affinity filtering mode setting
  Set the port rule **`Affinity`** parameter to `Single server` to force the same web server in the cluster to handle all requests from a particular client.

Network interface card (NIC) configuration for NLB

The recommended configuration for NLB is to install two Network Interface Cards (NICs) in each front-end web server. One NIC is configured for NLB with the public address of the cluster and the other can be used for communications among the servers in the cluster.

If front-end web servers have only one NIC, the NLB cluster should be configured for Multicast operation to allow communications between the nodes, which prevents configuration inconsistencies. Access this setting through the Network Load Balancing Manager, or through Network Connection Properties for each web server.

Affinity filtering mode setting

To optimize the effectiveness of PI WebParts caching, configure the NLB cluster to send all requests from a client to the same web server in the farm. When defining the port rule, set the **`Affinity`** parameter of the Multiple host filtering mode to `Single server` to have all requests from a particular client handled by the same web server in the cluster.

Access this setting through the Network Load Balancing Manager, or through Network Connection Properties for each web server.

URL conversion

PI WebParts works with reverse proxy servers based on Microsoft Internet Security and Acceleration (ISA) Server 2006.

Some PI WebParts features require specification of a URL, such as the selected file for a PI Graphic web part, or a hyperlink behavior in a PI Table web part. If different base URLs are required for multiple authentication zones (for example, a public URL defined for internet zone users and another for intranet users), administrators should specify an internal URL which works for users in zones without alternate access mappings.



Note:
This URL must not be specified as a host header for an extended site to which the ISA server redirects its requests.

PI WebParts supports conversion of URLs, such that when encountered in PI WebParts configurations, they are converted to an appropriate public URL for the current authentication zone, if mappings are available in the SharePoint Web Application's alternate access mappings (see the SharePoint article Plan alternate access mappings (http://technet.microsoft.com/en-us/library/cc261814.aspx)). If a mapping exists for the zone in which the current request originated, PI WebParts converts the specified base internal URL to the public URL.

To convert URLs, you must specify the internal URLs you wish to convert by adding an **InternalURLs** entry in the **AppSettings** section of the root `web.config` file. Multiple URLs can be specified using a semi-colon as the delimiter:

```
<add key="InternalUrls" value ="{first URL to convert};{second URL to convert};…"/>
```

For example, to convert all occurrences of `http://myserver` to an appropriate public URL, you would add the following entry:

```
<add key="InternalUrls" value ="http://myserver"/>
```

Once completed, when specifying a URL in the Selected File property of a PI Graphic web part for example, you would enter a file path using the internal URL `http://myserver/mydisplay.svg`.

- For SharePoint designers browsing from the inside of a firewall, where no alternate access mapping is used, the File Browse/Search dialogs could be used to select a file with an internal URL.
- From outside of a firewall, these dialogs should not be used. Instead, the external user who is designing the web part page should enter a known, internal URL.
- If a public URL is entered, the PI Graphic assembly running on the web server may not be able to load the specified file for users in other authentication zones.

A similar approach should be used when creating hyperlink behaviors in advanced table configurations. If alternate access mappings for the base URL in the link exist, an internal URL should be used. The same practice should be used for button links and linked images inside PI ProcessBook displays used in PI Graphic web parts.

Topics in this section

- Exceptions to URL conversion
  PI WebParts does not attempt to convert internal URLs to public URLs in several cases.
- Trusts for internal URLs
  A new or modified PI trust might be necessary when introducing a new internal URL.

Exceptions to URL conversion

There are several cases where PI WebParts does not attempt to convert internal URLs to public URLs:

- Button or image links inside PI ActiveView displays are resolved by the ActiveView control, which runs on the client machine. This means that instances of PI ActiveView configured with these displays are not fully functional outside of a firewall.
- URL Attributes used for hyperlinks in PI TreeView are not converted to public URLs because the attempt would significantly slow down PI TreeView processing. If possible, enter URL properties such that they work for users on both sides of the firewall.
- If external users running outside of the firewall load pages with PI ActiveView web parts or to run PI ProcessBook to edit display files, all PI Servers referenced in PDI and SVG displays must also reside outside the firewall, so that a direct connection can be established between the client machine and the PI Server.

Trusts for internal URLs

Each time a new internal URL is introduced, it may be necessary to modify or configure additional PI Server trusts. If the trust is based on an IP address and the new URL is an alias that resolves to an IP address that is already trusted, no changes are required.

If the new internal URL is an alias for another URL, but the PI trust is based on the network path, a new PI trust must be established for the new internal URL or the existing trust must be modified to be based on IP address.

If the new internal URL has no corresponding PI trust entry, a new PI trust entry must be created.

Configuration of Kerberos delegation

Kerberos delegation enables users to access remote data sources through Windows authentication. Kerberos is the preferred solution to manage user access among different servers. For example, with Kerberos, the SharePoint server and the PI WebParts Services server can accept and relay user login credentials to the remote server that provides data, such as PI Server or a PI AF server.

This section describes how to configure Kerberos delegation. For information about when PI WebParts requires Kerberos, see Requirements for identity authentication in a PI WebParts installation.



Note:
When you configure Kerberos delegation for a server, that configuration affects any application that runs on the server's website.

Topics in this section

- Prerequisites for Kerberos delegation
  To enable Kerberos delegation, Active Directory must be properly enabled and the installer must be able to select the application pool.
- Configure Kerberos delegation for SharePoint server
  For required PI WebParts configurations, you must delegate client credentials from the SharePoint server to the PI WebParts Services computer.
- Configure Kerberos delegation for PI WebParts Services
  For required PI WebParts configurations, you must delegate client credentials from PI WebParts Services to PI Server.
- Establish service principal names (SPNs) for application-pool accounts
  Kerberos authentication requires a service principal name that associates services with application-pool accounts.
- Remote-file access with Kerberos delegation
  Kerberos delegation enables PI System applications to access remote files secured at the share or file level.
- Troubleshooting
  Refer to these sections to verify or troubleshoot a Kerberos configuration.

Prerequisites for Kerberos delegation

Before you configure Kerberos delegation, verify that:

- All servers run on Windows 2003, Windows 2008, or Windows 2012.
- All user accounts, service accounts, and computers are members of the same Active Directory forest.
- All user accounts and service accounts can use Kerberos delegation.
- The installing user can select the application pool under which the web service will run.

Verify that user accounts can use Kerberos delegation

Use Active Directory Users and Computers to verify that user accounts permit Kerberos delegation.

Procedure

1. In Active Directory Users and Computers, expand your domain and click **Users**.
2. In the account list, right-click the user account and then click **Properties**.
3. On the **Account** tab, verify that the **Account is sensitive and cannot be delegated** check box is not selected.

Configure Kerberos delegation for SharePoint server

If your PI WebParts installation has PI WebParts Services and the SharePoint server on different computers, then you must configure Kerberos delegation to pass client credentials from your SharePoint server to the PI WebParts Services computer, unless you use claims-mode SharePoint sites with PI WebParts and you configure certificates. For more details about enabling Kerberos delegation, consult these Microsoft articles:

- Plan for Kerberos authentication in SharePoint 2013 (http://technet.microsoft.com/en-us/library/ee806870.aspx)
- Plan for Kerberos authentication (SharePoint Foundation 2010) (http://technet.microsoft.com/en-us/library/ff607695.aspx)

Before you start

Verify that your system configuration supports Kerberos delegation. See Prerequisites for Kerberos delegation.

Procedure

1. Establish service principal names (SPNs) for the SharePoint application-pool identity. See Establish service principal names (SPNs) for application-pool accounts.

   Note:
   To use Kerberos delegation with a web farm, configure SharePoint to use the same domain account for the SharePoint - 80 application-pool identity and the farm account.

2. Establish SPNs for the PI WebParts Services application-pool identity. See Establish service principal names (SPNs) for application-pool accounts.
3. Configure the SharePoint application-pool identity to delegate to PI WebParts Services.

If SharePoint application-pool identity uses:	Then:
Domain account	Configure a domain account to delegate to PI WebParts Services
`NetworkService` local account	Configure a local account to delegate to PI WebParts Services

4. Configure each SharePoint web application that uses PI WebParts:
   a. Set the application to authenticate the PI WebParts Services SPN.

See Enter settings that each SharePoint web application needs for PI WebParts. When specifying the identity that the SharePoint application uses to authenticate PI WebParts Services, set the **Identity type** to **Service Principal Name** and set **Valid identity** to `HTTP/appserver` where *appsever* is the PI WebParts Services computer.

b. Select Kerberos in the SharePoint Central Administration options for IIS authentication settings.

Configure a domain account to delegate to PI WebParts Services

If the SharePoint application-pool identity uses a domain account, a domain administrator must use Active Directory to configure the domain account to allow delegation.

Procedure

1. In Active Directory Users and Computers, expand your domain and click **Users**.
2. In the account list, right-click the domain account and then click **Properties**.
3. On the **Account** tab, verify that the **Account is sensitive and cannot be delegated** check box is not selected.
4. On the **Delegation** tab, enable delegation to PI WebParts Services:
   a. Select **Trust this user for delegation to specified services only** and **Use any authentication protocol**.
   b. In the **Services to which the account can present delegated credentials** table, add the `HTTP` service for PI WebParts Services.

      Specify either an account or a computer name, depending on the PI WebParts Services application-pool identity.

PI WebParts Services application-pool identity	Specify
Domain account	Account name
`NetworkService` account	Computer name

5. Click **OK**.

Configure a local account to delegate to PI WebParts Services

If the SharePoint application-pool identity uses the `NetworkServices` local account, a domain administrator must use Active Directory to configure the local account to allow delegation.

Procedure

1. In Active Directory Users and Computers, expand your domain and click **Computers**.
2. In the account list, right-click the computer account and then click **Properties**.
3. On the **Delegation** tab, enable delegation to PI WebParts Services:
   a. Select **Trust this user for delegation to specified services only** and **Use any authentication protocol**.
   b. In the **Services to which the account can present delegated credentials** table, add the `HTTP` service for PI WebParts Services.

Specify either an account or a computer name, depending on the PI WebParts Services application-pool identity.

PI WebParts Services application-pool identity	Specify
Domain account	Account name
`NetworkService` account	Computer name

4. Click **OK**.

Configure Kerberos delegation for PI WebParts Services

If your system uses Windows integrated security for connections to PI Server, you must configure Kerberos delegation from PI WebParts Services to PI Server. With Kerberos delegation, PI WebParts Services can pass user credentials to PI Server.

Before you start

Verify that your system configuration supports Kerberos delegation. See Prerequisites for Kerberos delegation.

Procedure

1. Establish service principal names (SPNs) for the PI WebParts Services application-pool identity. See Establish service principal names (SPNs) for application-pool accounts.

   If you configured Kerberos delegation for SharePoint, then you already established SPNs for the PI WebParts Services application-pool identity.

2. Verify that SPNs have been established for the PI Server service account.

   In most cases, the PI Server service account is the `NetworkService` local account and the SPN is already established.

3. Configure the PI WebParts Services application-pool identity to delegate to PI Server.

If PI WebParts Services application-pool identity uses:	Then:
Domain account	Configure a domain account to delegate to PI Server
`NetworkService` local account	Configure a local account to delegate to PI Server

4. Configure data sources, as necessary.

   To delegate credentials from PI WebParts Services to other data sources, you must complete similar steps as for delegating to PI Server. See Data-source configuration for Kerberos.

Configure a domain account to delegate to PI Server

If the PI WebParts Services application-pool identity uses a domain account, a domain administrator must use Active Directory to configure that domain account to allow delegation.

Procedure

1. In Active Directory Users and Computers, expand your domain and click **Users**.
2. In the account list, right-click the domain account and then click **Properties**.

3. On the **Account** tab, verify that the **Account is sensitive and cannot be delegated** check box is not selected.
4. On the **Delegation** tab, enable delegation to PI Server:
   a. Select **Trust this user for delegation to specified services only** and **Use any authentication protocol**.
   b. In the **Services to which the account can present delegated credentials** table, add the `PI Server` service for the PI Server computer.

      Specify either an account or a computer name, depending on the type of account used by the PI Server service.

If the PI Server service uses:	Then specify:
Domain account	Account name
`NetworkService` account	Computer name

5. Click **OK**.

Configure a local account to delegate to PI Server

If the PI WebParts Services application-pool identity uses the `NetworkServices` local account, a domain administrator must use Active Directory to configure the local account to allow delegation.

Procedure

1. In Active Directory Users and Computers, expand your domain and click **Computers**.
2. In the account list, right-click the computer account and then click **Properties**.
3. On the **Delegation** tab, enable delegation to PI Server:
   a. Select **Trust this user for delegation to specified services only** and **Use any authentication protocol**.
   b. In the **Services to which the account can present delegated credentials** table, add the `PI Server` service for the PI Server computer.

      Specify either an account or a computer name, depending on the type of account used by the PI Server service.

If the PI Server service uses:	Then specify:
Domain account	Account name
`NetworkService` account	Computer name

4. Click **OK**.

Data-source configuration for Kerberos

Different data sources have different configuration requirements to support Kerberos.

SQL Server data sources

Microsoft SQL Server accepts Windows credentials for authentication to the server and for authorization to specific databases. Special configuration is required to allow login through

Kerberos delegation. For specific configuration procedures, consult the appropriate Microsoft article:

- Using Kerberos Authentication with SQL Server (http://msdn.microsoft.com/en-us/library/cc280745.aspx) for SQL Server 2008
- Using Kerberos Integrated Authentication to Connect to SQL Server (http://msdn.microsoft.com/en-us/library/gg558122.aspx) for SQL Server 2012

Note:
The steps required to configure SQL Server to accept Kerberos delegation do not affect and are not related to the security configuration for SharePoint. This is the case even if SharePoint databases and the data-source database are stored on the same computer.

Oracle data sources

Oracle database servers support Windows integrated authentication. You can add domain accounts and assign them to database roles using the Administration Assistant for Windows.

To connect to an Oracle data source, PI WebParts Services requires the Oracle client and an established service name. No additional configuration is required for an Oracle server to enable Kerberos delegation.

Web-service data sources

Web services running on IIS in an intranet environment can be secured to require Windows authentication. You can manage permissions to these services in Internet Information Services Manager when you right-click the hosting site and choose **Permissions**.

The application pool of the website that hosts the web service determines additional requirements:

- If the application pool runs with the NetworkService identity, no additional Kerberos configuration is required.
- If the application pool runs under a domain account, a Kerberos SPN must be established for HTTP.

For example, for a web service that runs under the account `mydomain\mypoolid` and is accessed at the `http://myservice.mydomain.com/ws.asmx:` website, you must establish the following SPN:

```
SETSPN -S HTTP/myservice.mydomain.com mydomain\mypoolid
```

Establish a connection and a data set with the secured web service in PI WebParts Services as you would for any non-secured web services.

Establish service principal names (SPNs) for application-pool accounts

The Kerberos protocol uses service principal names (SPNs) to associate services with application-pool accounts. The application pool can use a local machine (that is, built-in) account or a domain (that is, custom) account, depending on your site's security policies:

- If the application pool uses the `NetworkService` local account, Kerberos can use the default SPN that Windows creates. In this case, you can skip this procedure.
- If the application pool uses a domain account, you must establish SPNs to bind the domain account to the HTTP service. Follow this procedure to use the **SETSPN** command to manage SPNs. For more information about the **SETSPN** command, consult the Microsoft article Setspn (http://technet.microsoft.com/en-us/library/cc731241(WS.10).aspx).

Before you start

Log in as domain administrator.

Procedure

1. Use the **SETSPN** command to establish SPNs for the NetBIOS name and fully qualified domain name of the computer that hosts the service:

   ```
   SETSPN -S HTTP/NETBIOS_name domain\account
   ```

   ```
   SETSPN -S HTTP/FQDN domain\account
   ```

   For example, with a computer named `ComputerX` on domain `DomainY.com` and an application pool that runs under account `AccountZ`, type the following commands:

   ```
   SETSPN -S HTTP/ComputerX DomainY\AccountZ
   ```

   ```
   SETSPN -S HTTP/ComputerX.DomainY.com DomainY\AccountZ
   ```

   Tip:
   If you access the website through headers, include the header in the fully qualified domain name. See Websites accessed with host headers.

Websites accessed with host headers

With Internet Information Services (IIS), you can configure websites that share a single IP address and port number but that users access through different host headers. To enable access through the host header, you must configure a DNS entry to resolve the IP address correctly.

For websites accessed with host headers, the fully qualified domain name uses the header rather than the computer name. In this case, you must specify the fully qualified domain name with the header when establishing the SPN for Kerberos delegation.

For example, suppose you have two websites on DomainY that share a port and IP address.

Site	Port	Header	FQDN
Site1	80	First	First.DomainY.com
Site2	80	Second	Second.DomainY.com

To establish Kerberos delegation through the application pool AccountZ on Site2, type the following **SETSPN** command:

```
SETSPN -S HTTP/Second.DomainY.com DomainY\AccountZ
```

Remote-file access with Kerberos delegation

After you set up the web server for Kerberos delegation, related PI System applications can access remote files that are secured at the share or the file level:

- PI WebParts Services can establish ODBC and OLEDB links to data files.
- PI WebParts can access SVG or PDI files stored in the file system.
- PI DataLink Server can display Excel files with PI DataLink functions.

No additional Kerberos configuration is required for file servers. To confirm security settings, the user should be able to access the file or the file share directly from the client workstation.

Troubleshooting

Establishing Kerberos delegation in an existing distributed environment can be challenging, particularly if service principal names must be established or if the domain policies are restricted. As with other networking tasks, OSIsoft recommends that you confirm one hop at a time to verify the configuration.

Topics in this section

- Verify Kerberos configuration on client computer
  Refer to the security event log on the web server to verify the Kerberos configuration on the client computer.
- Verify Kerberos configuration on web server
  Refer to the security event log to verify that Kerberos delegation is successful.

Verify Kerberos configuration on client computer

Procedure

1. Log out of the client machine and log back in with the appropriate user account, and then browse to the page with double-hop data access.
2. Review the security event log on the web server.

   The security event log records events that reflect the user account activity appear.
3. Determine which protocol is used for authentication.

   If the protocol is NTLM instead of Kerberos, a double hop cannot succeed. This occurs if the web server is not configured to accept Kerberos or the client account cannot use Kerberos.

Verify Kerberos configuration on web server

Procedure

1. Open the security event log on the target machine where the data source resides.

   The data source might reside on the file server, the web service machine, or the database server. The security event log records events that reflect the user account activity.
2. In the event log, examine logon events.

These events list the user name and authentication protocol, and indicate whether logon was successful:

- If the protocol is NTLM and the user name is blank, the web server is not using Kerberos to communicate with the target machine.
- If the client uses Kerberos for a successful connection to the web server, this hop can fail if the target machine is not configured to use Kerberos.

Configuration of certificates

On claims-mode sites, SharePoint can use certificates to exchange identity information with PI WebParts Services. After you install and properly reference certificates, the SharePoint server and PI WebParts Services can accept and relay user login credentials. Alternatively, you can configure Kerberos delegation to relay login credentials between SharePoint server and PI WebParts Services.

This section describes the necessary configuration for IIS self-signed certificates. To use certification authority (CA) certificates, additional configuration might be necessary. Check with the certification authority for details. For information about when PI WebParts requires certificates, see Requirements for identity authentication in a PI WebParts installation.

Configure certificates for claims-mode sites

To use certificates on claims-mode sites to exchange identity information with PI WebParts Services, you must install certificates for SharePoint and PI WebParts Services on the server computers that host these application servers, and you must configure SharePoint and PI WebParts Services to properly reference these certificates.

Procedure

1. Make PI WebParts Services aware of the SharePoint certificate.

   Export the certificate from the SharePoint server, import the certificate to the PI WebParts Services server, and find the certificate's thumbprint.

2. Prepare the PI WebParts Services certificate.

   Create the certificate, give the application-pool identity access to the certificate, and put the certificate in the proper location.

3. Update the PI WebParts Services configuration file to support certificates.

   Enable the certificate-ready configuration file that contains the thumbprint value from the SharePoint certificate and the name of the PI WebParts Services certificate.

4. Make SharePoint aware of the PI WebParts Services certificate.

   Export the certificate from the PI WebParts Services server, import the certificate to the SharePoint server, grant access permissions to the certificate, and configure SharePoint.

Make PI WebParts Services aware of the SharePoint certificate

To support claims-mode sites, PI WebParts Services must be aware of the SharePoint certificate. Use Microsoft Management Console to export the certificate from the SharePoint server, import the certificate to the PI WebParts Services server, and find the certificate's thumbprint. Consult your Microsoft server administrator for more information.

Procedure

1. On the SharePoint server, export the SharePoint Security Token Service certificate without the key (a `.cer` file).
2. On the PI WebParts Services server, import the SharePoint Security Token Service certificate to the Trusted People certificate node.
3. Find the value in the certificate's **Thumbprint** field and copy for later use.

   You need this value to update the PI WebParts Services configuration file.

Prepare the PI WebParts Services certificate

Claims-mode sites require a server certificate on the PI WebParts Services server. Use IIS Manager on the PI WebParts Services server to create a certificate for PI WebParts services, and then use Microsoft Management Console to provide access to the certificate and properly locate the certificate. Consult your Microsoft server administrator for more information.

Procedure

1. On the PI WebParts Services server, use IIS Manager to create a self-signed certificate.

   IIS Manager adds the certificate, named in the format `host.domain`, to the Personal certificate store.

   Note:
   The certificate store might contain an existing server certificate with the same name. PI WebParts Services cannot use all existing server certificates. Use a self-signed certificate created with IIS Manager for PI WebParts Services.
2. Give the PI WebParts Services application-pool identity access to the PI WebParts Services certificate.
3. Add the PI WebParts Services certificate to the Trusted People certificate store.

Update the PI WebParts Services configuration file to support certificates

Before PI WebParts Services can use certificates to support claims-mode sites, you must enable the certificate-ready configuration file, and enter the thumbprint value from the SharePoint certificate and the name of the PI WebParts Services certificate.

Before you start

You must know:

- Value of **Thumbprint** field in the SharePoint Security Token Service certificate
- Name of PI WebParts Services server certificate

Procedure

1. Go to the`\program files\pipc\PIWebPartsServices` directory.
2. Set PI WebParts Services configuration file (the `web.config` file) to use the file designed for certificate usage.

   The setup program installs two files but initiates the file to the non-certificate version.

a. Rename the `web.config` file to `NoCertificateWeb.config` or some similar name.

   PI WebParts Services cannot use this configuration file when using certificates for authentication.

b. Rename the `CertificateEnabledWeb.Config` file to `web.config`.

   PI WebParts Services must use this configuration file when using certificates for authentication.

3. Open the `web.config` file in a text editor.
4. Edit the configuration file to recognize the installed SharePoint certificate:
   a. Search the file for `thumbprint`.

```
<trustedIssuers>
          <add thumbprint="ThumbprintFromSpServer" name="SharePoint
           Security Token Service" />
 </trustedIssuers>
```

   b. Change the value from `ThumbprintFromSpServer` to the thumbprint value you found in the SharePoint Security Token Service certificate.
   c. Remove any spaces from the value of the thumbprint.

```
<trustedIssuers>
          <add thumbprint="f17d7d41838a1b168e6e8b6810294f0961bd5b24"
           name="SharePoint Security Token Service" />
 </trustedIssuers>
```

5. Edit the configuration file to recognize the PI WebParts Services certificate:
   a. Search the file for `serviceCertificate`.

```
<serviceCredentials>
            <serviceCertificate findValue="MyHost.domain.com"
             storeLocation="LocalMachine" storeName="My"
             x509FindType="FindByIssuerName" />
</serviceCredentials>
```

   b. Set the **`findValue`** attribute to the name of the PI WebParts Services server certificate.

      The value entered by the setup program might be correct.

   c. Set the **`x509FindType`** attribute to a method that will find the certificate among available certificates.

      The best method might vary depending on the certificates installed. See the MSDN article X590FindType Enumeration (http://msdn.microsoft.com/en-us/library/system.security.cryptography.x509certificates.x509findtype.aspx) for more information.

6. Save the file.

Make SharePoint aware of the PI WebParts Services certificate

To enable SharePoint to accept the certificate from PI WebParts Services for claims-mode sites, you must import that certificate into the SharePoint server, grant appropriate access, move to the correct location, and then enable SharePoint to trust the certificate. Use Microsoft Management Console and SharePoint Central Administration. Consult your Microsoft server administrator for more information.

Before you start

Prepare the PI WebParts Services certificate.

Procedure

1. On the PI WebParts Services server, export the PI WebParts Services certificate with key (a `.pfx` file).
2. On the SharePoint server, import the PI WebParts Services certificate to the Personal certificate store.
3. Give the SharePoint application-pool identity access to the PI WebParts Services certificate.
4. Add the PI WebParts Services certificate to the Trusted People certificate store.
5. Export the PI WebParts Services certificate without key (a `.cer` file).
6. Add the PI WebParts Services certificate without key to SharePoint through SharePoint Central Administration.
   a. In the **Central Administration** navigation pane of SharePoint Central Administration, click **Security**.
   b. On the Security page, under **General Security**, click **Manage trust**.
   c. On the **Trust Relationships** tab, in the **Manage** group, click **New**.
   d. In the Establish Trust Relationship window, enter the information to identify the trusted certificate:
      - In the **Name** field, enter a name to identify this relationship.
      - In the **Root Authority Certificate** field, add the PI WebParts Services certificate without key (the `.cer` file).
   e. Click **OK**.

PI WebParts custom performance counters

The following table lists the custom performance counters that you can install on the computer that runs PI WebParts Services. See Install PI WebParts custom performance counters.

Note:
You can select these counters across all application domains. However, some counters are not updated at runtime in a given domain. Therefore it is necessary to have some knowledge of the web application and PI WebParts Services architecture to gather meaningful data for analysis.

Object name	Counter name	Counter description
RtWebParts	Update Average Call Secs	Average execution time, in seconds, of calls to RtWebPart Update web service.
RtWebParts	Update Calls/Sec	Rate per second of calls to RtWebPart Update web service.
RtWebParts	Update Last Call USecs	Execution time, in micro-seconds, of last call to RtWebPart Update web service.
RtWebParts	Update Total Calls	Total count of calls to RtWebPart Update web service.
RtWebParts	WebPart Average Call Secs	Average execution time, in seconds, of last call to the RtWebPart base class.
RtWebParts	WebPart Calls/Sec	Rate per second of calls to the RtWebPart base class.
RtWebParts	WebPart Last Call USecs	Execution time, in micro-seconds, of last call to the RtWebPart base class.
RtWebParts	WebPart Total Calls	Total count of calls to the RtWebPart base class.
RtWebParts: *WebPartName*[1]	Update Average Call Secs	Average execution time, in seconds, of calls to update web part.
RtWebParts: *WebPartName* [1]	Update Calls/Sec	Rate per second of calls to update web part.
RtWebParts: *WebPartName* [1]	Update Last Call USecs	Last execution time, in microseconds, of call to update web part.
RtWebParts: *WebPartName* [1]	Update Total Calls	Total count of calls to update web part.
RtWebParts: *WebPartName* [1, 2]	WebPart Average Call Secs	Average execution time, in seconds, of last calls to the web part.
RtWebParts: *WebPartName* [1, 2]	WebPart Calls/Sec	Rate per second of calls to the web part.
RtWebParts: *WebPartName* [1, 2]	WebPart Last Call USecs	Execution time, in microseconds, of last call to the web part.
RtWebParts: *WebPartName* [1, 2]	WebPart Total Calls	Total count of calls to the web part.

Object name	Counter name	Counter description
RtWebParts: *WebPartName*[3, 4]	DeSer. Table Average Call Secs	Average execution time, in seconds, to deserialize.
RtWebParts: *WebPartName*[3, 4]	DeSer. Table Calls/Sec	Rate per second of calls to deserialize.
RtWebParts: *WebPartName*[3, 4]	DeSer. Table Last Call USecs	Last execution time, in microseconds, to deserialize.
RtWebParts: *WebPartName*[3, 4]	DeSer. Table Total Calls	Total count of calls to deserialize.
RtWebParts: *WebPartName*[3]	Non-Agg. Query No Cfg Average Call Secs	Average execution time, in seconds, to process an update for a non-aggregated query without an Rt Advanced Configuration.
RtWebParts: *WebPartName*[3]	Non-Agg. Query No Cfg Calls/Sec	Rate per second of calls to process an update for a non-aggregated query without an Rt Advanced Configuration.
RtWebParts: *WebPartName*[3]	Non-Agg. Query No Cfg Last Call USecs	Last execution time, in microseconds, to process an update for a non-aggregated query without an Rt Advanced Configuration.
RtWebParts: *WebPartName*[3]	Non-Agg. Query No Cfg Total Calls	Total count of calls to process an update for a non-aggregated query without an Rt Advanced Configuration.
RtWebParts: *WebPartName*[3]	Non-Agg. Query w/Cfg Average Call Secs	Average execution time, in seconds, to process an update for a non-aggregated query using an Rt Advanced Configuration.
RtWebParts: *WebPartName*[3]	Non-Agg. Query w/Cfg Calls/Sec	Rate per second of calls to process an update for a non-aggregated query using an Rt Advanced Configuration.
RtWebParts: *WebPartName*[3]	Non-Agg. Query w/Cfg Last Call USecs	Last execution time, in microseconds, to process an update for a non-aggregated query using an Rt Advanced Configuration.
RtWebParts: *WebPartName*[3]	Non-Agg. Query w/Cfg Total Calls	Total count of calls to process an update for a non-aggregated query using an Rt Advanced Configuration.
RtWebParts: *WebPartName*[3, 4]	Ser. Data Query Average Call Secs	Average execution time, in seconds, to serialize a data query.
RtWebParts: *WebPartName*[3, 4]	Ser. Data Query Calls/Sec	Rate per second of calls to serialize a data query.
RtWebParts: *WebPartName*[3, 4]	Ser. Data Query Last Call USecs	Last execution time, in micro-seconds, to serialize a data query.
RtWebParts: *WebPartName*[3, 4]	Ser. Data Query Total Calls	Total count of calls to serialize a data query.
RtWebParts: *WebPartName*[3, 4]	Ser. Table State Average Call Secs	Average execution time, in seconds, to serialize table state.
RtWebParts: *WebPartName*[3, 4]	Ser. Table State Calls/Sec	Rate per second of calls to serialize table state.
RtWebParts: *WebPartName*[3, 4]	Ser. Table State Last Call USecs	Last execution time, in microseconds, to serialize table state.

Object name	Counter name	Counter description
RtWebParts: *WebPartName*[3, 4]	Ser. Table State Total Calls	Total count of calls to serialize table state.
RtWebParts: *WebPartName*[3, 4]	Table Render Init. Average Call Secs	Average execution time, in seconds, to perform initialization to render a web part.
RtWebParts: *WebPartName*[3, 4]	Table Render Init. Calls/Sec	Rate per second of calls to perform initialization to render a web part.
RtWebParts: *WebPartName*[3, 4]	Table Render Init. Last Call USecs	Last execution time, in microseconds, to perform initialization to render a web part.
RtWebParts: *WebPartName*[3, 4]	Table Render Init. Total Calls	Total count of calls to perform initialization to render a web part.
RtWebParts: *WebPartName*[3, 4]	Table Render Main Average Call Secs	Average execution time, in seconds, to perform main routine to render a web part.
RtWebParts: *WebPartName*[3, 4]	Table Render Main Calls/Sec	Rate per second of calls to perform main routine to render a web part.
RtWebParts: *WebPartName*[3, 4]	Table Render Main Last Call USecs	Last execution time, in micro-seconds, to perform main routine to render a web part.
RtWebParts:*WebPartName*[3, 4]	Table Render Main Total Calls	Total count of calls to perform main routine to render a web part.
RtWebParts: RtGraphic	Bar Symbol Average Call Secs	Average execution time, in seconds, to process a bar symbol.
RtWebParts: RtGraphic	Bar Symbol Calls/Sec	Rate per second of calls to process a bar symbol.
RtWebParts: RtGraphic	Bar Symbol Last Call USecs	Last execution time, in microseconds, to process a bar symbol.
RtWebParts: RtGraphic	Bar Symbol Total Calls	Total count of calls to process a bar symbol.
RtWebParts: RtGraphic	MultiState Symbol Average Call Secs	Average execution time, in seconds, to process a multistate symbol.
RtWebParts: RtGraphic	MultiState Symbol Calls/Sec	Rate per second of calls to process a multistate symbol.
RtWebParts: RtGraphic	MultiState Symbol Last Call USecs	Last execution time, in microseconds, to process a multistate symbol.
RtWebParts: RtGraphic	MultiState Symbol Total Calls	Total count of calls to process a multistate symbol.
RtWebParts: RtGraphic	ODBC Query Average Call Secs	Average execution time, in seconds, to process an ODBC query.

Object name	Counter name	Counter description
RtWebParts: RtGraphic	ODBC Query Calls/Sec	Rate per second of calls to process an ODBC query.
RtWebParts: RtGraphic	ODBC Query Last Call USecs	Last execution time, in microseconds, to process an ODBC query.
RtWebParts: RtGraphic	ODBC Query Total Calls	Total count of calls to process a ODBC query.
RtWebParts: RtGraphic	PI Dataset Query Average Call Secs	Average execution time, in seconds, to process a PI data-set query.
RtWebParts: RtGraphic	PI Dataset Query Calls/Sec	Rate per second of calls to process a PI data-set query.
RtWebParts: RtGraphic	PI Dataset Query Last Call USecs	Last execution time, in microseconds, to process a PI data-set query.
RtWebParts: RtGraphic	PI Dataset Query Total Calls	Total count of calls to process a PI data-set query.
RtWebParts: RtGraphic	PI Query Average Call Secs	Average execution time, in seconds, to process a PI point query.
RtWebParts: RtGraphic	PI Query Calls/Sec	Rate per second of calls of calls to process a PI point query.
RtWebParts: RtGraphic	PI Query Last Call USecs	Last execution time, in microseconds, to process a PI point query.
RtWebParts: RtGraphic	PI Query Total Calls	Total count of calls to process a PI point query.
RtWebParts: RtGraphic	SVG Transform Average Call Secs	Average execution time, in seconds, to process an SVG transform.
RtWebParts: RtGraphic	SVG Transform Calls/Sec	Rate per second of calls to process an SVG transform.
RtWebParts: RtGraphic	SVG Transform Last Call USecs	Last execution time, in micro-seconds, to process an SVG transform.
RtWebParts: RtGraphic	SVG Transform Total Calls	Total count of calls to process an SVG transform.
RtWebParts: RtGraphic	Trend Symbol Average Call Secs	Average execution time, in seconds, to process a trend symbol.
RtWebParts: RtGraphic	Trend Symbol Calls/Sec	Rate per second of calls to process a trend symbol.
RtWebParts: RtGraphic	Trend Symbol Last Call USecs	Last execution time, in microseconds, to process a trend symbol.
RtWebParts: RtGraphic	Trend Symbol Total Calls	Total count of calls to process a trend symbol.
RtWebParts: RtGraphic	Value Symbol Average Call Secs	Average execution time, in seconds, to process a value symbol.

Object name	Counter name	Counter description
RtWebParts: RtGraphic	Value Symbol Calls/Sec	Rate per second of calls to process a value symbol.
RtWebParts: RtGraphic	Value Symbol Last Call USecs	Last execution time, in microseconds, to process a value symbol.
RtWebParts: RtGraphic	Value Symbol Total Calls	Total count of calls to process a value symbol.
RtWebParts: RtTreeView	Build Comm Data Average Call Secs	Average execution time, in seconds, of last call to get web part communication data.
RtWebParts: RtTreeView	Build Comm Data Calls/Sec	Rate per second of calls to get web part communication data.
RtWebParts: RtTreeView	Build Comm Data Last Call USecs	Execution time, in microseconds, of last call to get web part communication data.
RtWebParts: RtTreeView	Build Comm Data Total Calls	Total count of calls to get web part communication data.
RtWebParts: RtTreeView	Load Tree Average Call Secs	Average execution time, in seconds, of last call to load the tree control.
RtWebParts: RtTreeView	Load Tree Calls/Sec	Rate per second of calls to load the tree control.
RtWebParts: RtTreeView	Load Tree Last Call USecs	Execution time, in microseconds, of last call to load the tree control.
RtWebParts: RtTreeView	Load Tree Total Calls	Total count of calls to load the tree control.
RtWebParts: RtTreeView	Node Expand Average Call Secs	Average execution time, in seconds, of last call to expand a single node.
RtWebParts: RtTreeView	Node Expand Calls/Sec	Rate per second of calls to expand a single node.
RtWebParts: RtTreeView	Node Expand Last Call USecs	Execution time, in microseconds, of last call to expand a single node.
RtWebParts: RtTreeView	Node Expand Total Calls	Total count of calls to expand a single node.
RtWebParts: RtTreeView	Number Of PI Aliases Read	Total number of PI aliases read by the RtTreeView web part and any tree control in the RtBaseline administrative web pages.
RtWebParts: RtTreeView	Number Of PI Modules Read	Total number of PI modules read by the RtTreeView web part and any tree control in the PI WebParts administrative web pages.
RtWebParts: RtTreeView	Number Of PI Properties Read	Total number of PI properties read by the RtTreeView web part and any tree control in the RtBaseline administrative web pages.
RtWebParts: RtTrend	Calculate Scales Average Call Secs	Average execution time, in seconds, of calls to calculate scales for a trend.
RtWebParts: RtTrend	Calculate Scales Calls/Sec	Rate per second of calls to calculate scales for a trend.

Object name	Counter name	Counter description
RtWebParts: RtTrend	Calculate Scales Last Call USecs	Execution time, in microseconds, of last call to calculate scales for a trend.
RtWebParts: RtTrend	Calculate Scales Total Calls	Total count of calls to calculate scales for a trend.
RtWebParts: RtTrend, RtXYPlot	Render SVG Average Call Secs	Average execution time, in seconds, of calls to render SVG for web part.
RtWebParts: RtTrend, RtXYPlot	Render SVG Calls/Sec	Rate per second of calls to render SVG for web part.
RtWebParts: RtTrend, RtXYPlot	Render SVG Last Call USecs	Execution time, in microseconds, of last call to render SVG for web part.
RtWebParts: RtTrend, RtXYPlot	Render SVG Total Calls	Total count of calls to render SVG for web part.
RtWebParts: RtValues	Agg. Query No Cfg Average Call Secs	Average execution time, in seconds, to process an update for an aggregated query without an Rt advanced configuration.
RtWebParts: RtValues	Agg. Query No Cfg Calls/Sec	Rate per second of calls to process an update for an aggregated query without an Rt advanced configuration.
RtWebParts: RtValues	Agg. Query No Cfg Last Call USecs	Last execution time, in microseconds, to process an update for an aggregated query without an Rt advanced configuration.
RtWebParts: RtValues	Agg. Query No Cfg Total Calls	Total count of calls to process an update for an aggregated query without an Rt advanced configuration.
RtWebParts: RtValues	Agg. Query w/Cfg Average Call Secs	Average execution time, in seconds, to process an initial aggregated query using an Rt advanced configuration.
RtWebParts: RtValues	Agg. Query w/Cfg Calls/Sec	Rate per second of calls to process an initial aggregated query using an Rt advanced configuration.
RtWebParts: RtValues	Agg. Query w/Cfg Last Call USecs	Last execution time, in microseconds, to process an initial aggregated query using an Rt advanced configuration.
RtWebParts: RtValues	Agg. Query w/Cfg Total Calls	Total count of calls to process an initial aggregated query using an Rt advanced configuration.
RtWebParts: RtXYPlot	Execute Initial Queries Average Call Secs	Average execution time, in seconds, to execute initial RtBaseline queries.
RtWebParts: RtXYPlot	Execute Initial Queries Calls/Sec	Rate per second of calls to execute initial RtBaseline queries.
RtWebParts: RtXYPlot	Execute Initial Queries Last Call USecs	Execution time, in microseconds, to execute initial RtBaseline queries.

Object name	Counter name	Counter description
RtWebParts: RtXYPlot	Execute Initial Queries Total Calls	Total count of calls to execute initial RtBaseline queries.
RtWebParts: RtXYPlot	Execute Update Queries Average Call Secs	Average execution time, in seconds, to execute RtBaseline queries for updates.
RtWebParts: RtXYPlot	Execute Update Queries Calls/Sec	Rate per second of calls to execute RtBaseline queries for updates.
RtWebParts: RtXYPlot	Execute Update Queries Last Call USecs	Execution time, in microseconds, of last call to execute RtBaseline queries for updates.
RtWebParts: RtXYPlot	Execute Update Queries Total Calls	Total count of calls to execute RtBaseline queries for updates.

[1]RtActiveView, RtBatchTable, RtGauge, RtGraphic, RtTable, RtTimeSeries, RtTrend, RtValues, RtXYPlot

[2]RtMessenger, RtTimeRange, RtTreeView

[3]RtBatchTable, RtTable, RtTimeSeries

[4]RtValues

Technical support and other resources

For technical assistance, contact OSIsoft Technical Support at +1 510-297-5828 or through the OSIsoft Tech Support Contact Us page (https://techsupport.osisoft.com/Contact-Us/). The website offers additional contact options for customers outside of the United States.

When you contact OSIsoft Technical Support, be prepared to provide this information:

- Product name, version, and build numbers
- Details about your computer platform (CPU type, operating system, and version number)
- Time that the difficulty started
- Log files at that time
- Details of any environment changes prior to the start of the issue
- Summary of the issue, including any relevant log files during the time the issue occurred

To ask questions of others who use OSIsoft software, join the OSIsoft user community, PI Square (https://pisquare.osisoft.com). Members of the community can request advice and share ideas about the PI System. The PI Developers Club space within PI Square offers resources to help you with the programming and integration of OSIsoft products.

Index

C

column behaviors 54
contact configurations 63

D

data sets 86
data sources 66

M

Microsoft Access 72
Microsoft Office 78

O

ODBC 71
Oracle 74

P

PI AF support 86
PI calculation data sets 87
PI OLEDB 76
PI Server data sources 67
placeholders, SQL 96

R

relational data sets 92
relational data sources 69

S

SAP web services 83
SQL Server 72

T

table configurations 52
trend configurations 61

W

web part presentation 51
web service data sets 97
web service data sources 81