PI Integrator for Business Analytics 2018 R2

User Guide

OSIsoft, LLC
1600 Alvarado Street
San Leandro, CA 94577 USA
Tel: (01) 510-297-5800
Fax: (01) 510-357-8136
Web: http://www.osisoft.com

PI Integrator for Business Analytics 2018 R2 User Guide: Patent pending

Version: 2.1

Published: 12 September 2019

Contents

What is PI Integrator for Business Analytics?

PI Integrator for Business Analytics presents PI System data perfectly suited to business intelligence tools including, but not limited to, Tableau, Tibco Spotfire, QlikView, and Microsoft Power BI for reporting and analytics. Business Intelligence (BI) client tools offer the ability to run retrospective analyses on a much larger set of your real-time PI System data. BI helps you learn from operational behaviors and patterns, identifying dependencies and correlations of various factors within your operations.

PI Integrator for Business Analytics Advanced Edition serves real-time packets of PI System data to streaming platforms such as Apache Kafka. Publishing to a streaming platform allows the PI System to transmit pre-defined packets of time-series data to streaming consumers. Streaming platforms assist in operationalizing machine learning models and support Kappa and Lambda architectures for data consumption.

Native time-series data, asset context, and event context are exposed through web-configured views. Data are perfectly dimensionally modeled, cleansed, and presented with appropriate metadata so that BI tools can properly browse, query, and consume PI System data seamlessly. Data can also be directly integrated and loaded into data warehouse platforms. PI Integrator for Business Analytics eliminates the need for programming or SQL expertise and manages the complete data lifecycle, including access, updates, and data provenance.

PI Integrator for Business Analytics requires a PI Asset Framework (PI AF) model to select PI System data to produce decision-ready data. The data can be cleansed using a variety of filters and enhanced with asset, event, and time context from the PI System. The resulting data are immediately usable in BI tools without further modification.

Advantages of PI Integrator for Business Analytics

The advantages of using PI Integrator for Business Analytics are:

- Large data sets can be easily selected and imported. No coding is required to prepare the data and no knowledge of the source data is required.
- The size of the data set can be scaled up without requiring customization of the data importing procedures.
- PI System data can be merged with other data sets for aggregate-level analysis and consumed by a variety of business intelligence tools, data warehouses, and streaming platforms.
- Published data is synchronized with the PI System and automatically updated to reflect changes.
- Data is refreshed on a schedule or in response to changes to key values.
- The web-based user interface is easy to use, requiring no installation by end users.

Caveats to using PI Integrator for Business Analytics

Note the following about PI Integrator for Business Analytics:

- PI Integrator for Business Analytics only supports data with timestamps in the past. Future data is currently not supported.
- PI Integrator for Business Analytics publishes PI System data to a wide variety of targets. However, it does not accept changes to PI System data from external data sources.
- Streaming views can only stream up to 25,000 total matches of the search shapes.

PI Integrator for Business Analytics editions

There are two editions of PI Integrator for Business Analytics:

- **Standard**

  The Standard edition is an enterprise solution for customers who want to publish their PI System data to an external data warehouse. Once exported to these data warehouses, PI System data can be merged with data from other systems. Client applications can access this data natively rather than using the PI ODBC driver.

  The Standard edition also allows you to publish PI System data to the PI View target type. A PI View is a row and column representation of data that can be consumed by a wide range of BI tools through the PI ODBC driver. The data for the PI View is stored in a SQL Server in PI Integrator for Business Analytics. Publishing to the PI View target is suitable for smaller-scale operational reporting and is limited to PI System data.

- **Advanced**

  In addition to publishing data to external data warehouses, the Advanced edition supports streaming data to supported streaming targets. Once published, this data can be used to train machine learning applications to discover patterns and predict future behavior.

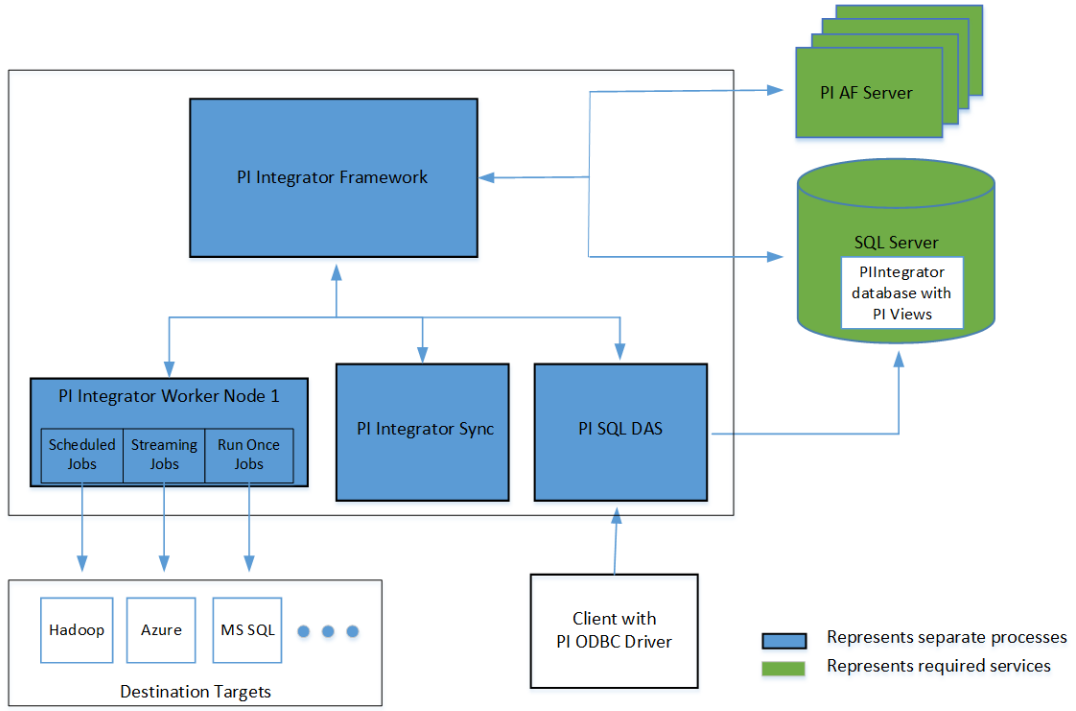
Supported Publish Targets

The following table shows the different publish targets supported with each edition.

Destination Type	Target Destination	Format	Standard Edition	Advanced Edition
General	PI View	row-column	✓	✓
	Text File		✓	✓
Relational Database	Microsoft SQL Server	row-column	✓	✓
	Oracle Database		✓	✓
	Azure SQL Database		✓	✓
Data Warehouse	Apache Hive	row-column	✓	✓
	Azure SQL Data Warehouse		✓	✓
	Amazon Redshift		✓	✓
Data Lake	Hadoop HDFS	row-column	✓	✓
	Azure Data Lake Store		✓	✓
	Amazon S3		✓	✓
Messaging Hub	Apache Kafka	stream		✓
	Azure IoT Hub			✓
	Azure Event Hubs			✓
	Amazon Kinesis Data Streams			✓

System architecture

The following diagram shows a typical architecture of a PI Integrator for Business Analytics system.



PI Integrator for Business Analytics System Architecture

The following describes the components that are required for the data warehouse targets. PI Integrator Framework, PI Integrator Worker Nodes, and PI Integrator Sync processes all reside on the same computer.

- **PI Integrator Framework**

  The PI Integrator Framework performs the following functions:

  - Provides the web application through which views are created, published, and managed.
  - Schedules jobs to be published.
  - Distributes jobs among PI Integrator Worker Nodes to balance the publishing of views amongst the nodes. In this diagram, there is only one worker node.
  - Tracks and manages the output streams used in views.
  - Records view statistics including time to publish the view, number of rows written, number of rows filtered, and error count.

- **PI Integrator Sync**

  PI Integrator Sync ensures that published data is correct by monitoring the following:

  - View shape and data changes of scheduled asset views and scheduled streaming views
  - View shape changes of key-value-triggered streaming views

- **PI Integrator Worker Node**

  PI Integrator Worker Node publishes jobs to its destination targets. Additional worker nodes can be installed to improve performance.

- **PI Asset Framework (PI AF)**

  PI Integrator for Business Analytics retrieves and updates view definitions stored in the PI AF configuration database.

- **SQL Server**

  Metadata tables, logs, and statistics are stored in SQL Server.

PI View architecture

The PI Integrator Framework, PI Integrator Sync, and PI Asset Framework are also components of the PI View architecture. In addition, the following components are required for the PI View architecture.

- **PI ODBC Driver**

  The PI ODBC driver on the client serves as the point of contact for the remote client application, requesting and receiving PI View data on behalf of the client through interaction with PI SQL DAS on the server.

- **PI SQL Data Access Server (PI SQL DAS)**

  PI SQL DAS (PI Integrators) is a Windows service installed as part of PI Integrator for Business Analytics. It acts as the intermediary between PI ODBC Driver and the PI AF and SQL databases. PI SQL DAS retrieves the view definitions from the PI AF configuration database and the materialized data from the SQL database to construct the PI View data to send to the remote client application.

- **SQL Database**

  Data for the PI View target is stored in tables in the SQL database.

System requirements

This section describes the system requirements for a PI Integrator for Business Analytics installation and for each of the supported publish targets.

PI Integrator for Business Analytics requirements

The following are the system requirements for PI Integrator for Business Analytics:

- PI Server 2010 or later
  - PI Asset Framework 2015 or later
  - PI Data Archive 2010 or later

    Note:

    PI Integrator for Business Analytics supports automatic updates of published PI System data on selected targets. To take advantage of this feature, you must be using PI Data Archive 2017 or later. For more information about this feature, see How published data gets updated.
- PI AF SDK 2018 SP1 or later
- PI Integrator for Business Analytics
  - 16GB of memory and two modern CPU cores

    Note:

    This is sufficient for the minimum one worker node process that is installed. For each additional worker node process on the same machine, add an additional 4GB of memory and two modern CPU cores.
  - Microsoft Windows Server 2008 R2 SP1 or later

    Note:

    The Microsoft Windows Server must be part of a domain. PI Integrator for Business Analytics cannot be installed in a Workgroup.
- Microsoft SQL Server 2008 R2 SP2 or later (installed locally or on the network)

  Microsoft SQL Server must be installed with the Full-Text Search component prior to installing PI Integrator for Business Analytics. Supported editions of SQL Server include: SQL Server Standard, SQL Server Enterprise, and SQL Server Express with Advanced Services.

Note:

SQL Server Express with Advanced Services is supported, but it is not recommended with PI Integrator for Business Analytics. SQL Server Express (without Advanced Services) is not supported with PI Integrator for Business Analytics.

Web browser requirements

Use one of the following web browsers:

- Google Chrome version 45.xx or later (recommended)
- Microsoft Edge version 41.16299.x or later

PI View publish target requirements

PI ODBC 2016 R2 or later must be installed on all client machines that make requests to PI Integrator for Business Analytics for PI View data.

Oracle Database publish target requirements

The Oracle Database publish target requires that you install the following software on the machine where PI Integrator for Business Analytics is installed:

- 64-bit Oracle Data Access Components 12c Release 4 (12.1.0.2.4) for Windows x64

PI Integrator for Business Analytics supports the following versions of the Oracle Database:

- Oracle Database 12c Release 1 (12.1.0.2.0) for Microsoft Windows (x64)

Amazon Web Services targets

Current version of the following Amazon Web Services platforms:

- Amazon Kinesis
- Amazon Redshift
- Amazon S3

Amazon Redshift ODBC driver

PI Integrator for Business Analytics has been tested with the following versions of the Amazon Redshift ODBC driver:

- Amazon Redshift (x86) ODBC Driver version 1.4.2.1010
- Amazon Redshift (x64) ODBC Driver version 1.4.2.1010

Apache Hadoop tested versions

PI Integrator for Business Analytics has been tested with the following software versions:

- HortonWorks – HDP 2.5.0.0-1245

  > **Note:**
  >
  > HortonWorks is only supported with the Thrift API. WebHCat is not supported.

  - Apache Hive – 1.2.1000
  - HDFS – 2.7.3
- Cloudera – CDH 5.14.0

PI Integrator for Business Analytics will likely work with other versions as well.

Apache Kafka tested versions

The following versions of Apache Kafka are supported: 0.8x, 0.9x, 0.10x, and 0.11x.

Apache Thrift tested versions

PI Integrator for Business Analytics has been tested with Apache Thrift 0.9.3.0. PI Integrator for Business Analytics will likely work with other versions as well.

Microsoft Azure requirements

Current version of one or more of the following Microsoft Azure platforms:

- Azure Event Hubs
- Azure IoT Hub
- Azure SQL Database
- Azure SQL Data Warehouse
- Azure Data Lake Store (renamed Azure Data Lake Storage Gen 1)

Note:
PI Integrator for Business Analytics only supports Azure Data Lake Storage Gen 1. There is currently no support for Azure Data Lake Storage Gen 2.

Schema Registry tested version

PI Integrator for Business Analytics has been tested with Confluent Schema Registry 4.0.0. PI Integrator for Business Analytics will likely work with other versions as well.

How to install PI Integrator for Business Analytics

PI Integrator for Business Analytics is comprised of the following installation phases:

- **Phase 1: Prepare for installation**

  This phase ensures that you have the appropriate access and permissions to the components that interact with PI Integrator for Business Analytics: PI AF server, PI Data Archive, and Microsoft SQL Server. These prerequisites must be in place before you run the installation kit for PI Integrator for Business Analytics.

- **Phase 2: Install PI Integrator for Business Analytics**

  In this phase, you install PI Integrator for Business Analytics, specifying the PI AF server and Microsoft SQL Server. New PI Integrator databases are created on the Microsoft SQL Server for PI Integrator for Business Analytics.

- **Phase 3: Verify the installation**

  This phase verifies that the PI Integrator for Business Analytics services have started and are running.

The following topics describe the steps for each phase of the installation in more detail:

- Phase 1: Prepare to install PI Integrator for Business Analytics
- Phase 2: Install PI Integrator for Business Analytics
- Phase 3: Verify the installation

Phase 1: Prepare to install PI Integrator for Business Analytics

The following components are required for a successful installation of PI Integrator for Business Analytics: PI Server (which includes the PI Asset Framework server and PI Data Archive), and Microsoft SQL Server (which will include the databases that store the PI View data, metadata for continuous views, and the PI Integrator for Business Analytics logs and statistics databases).

Phase 1 involves obtaining the access and permissions required to install PI Integrator for Business Analytics and ensures that you have the required permissions to access the components. This phase identifies all access and permission requirements in one place, streamlining your requests to your IT department and/or Microsoft SQL Server administrator.

Procedure

1. Ensure that the minimum requirements are met and the required software are installed as described in System requirements.

Note:

SQL Server must have Full-Text Search installed. This optional component in the SQL Server installation must either be explicitly selected during the SQL Server installation or added post-installation. To add full-text search post-installation, modify the SQL Server installation using the Programs and Features option on the Control Panel.

2. Ensure that you are a domain user with local administrator privileges on the Microsoft Windows Server where PI Integrator for Business Analytics will be installed.
3. Obtain a Windows service account username and password for your domain. You may need to contact your IT administrator to create one for you.

   Note:

   OSIsoft recommends using a Managed Service Account to run PI Integrator for Business Analytics, but a standard domain user account dedicated to running the service is also supported. For more information, see Kerberos constrained delegation.

4. Verify that the Windows service account on the machine where PI Integrator for Business Analytics is installed has the following permissions:
   - Read and Read Data access at the AF server level for all PI AF Servers that PI Integrator for Business Analytics needs to access
   - Read and Read Data access on any PI AF databases and any of its child objects that PI Integrator for Business Analytics needs to access
   - Read access to the PIPoint table under Database Security
   - Read access to both point and data security on all PI points that PI Integrator for Business Analytics needs to access
5. Ensure that the user account used to install the software has sysadmin privileges on the SQL Server on which you will be installing the PI Integrator databases. This is required to create the PI Integrator's backend SQL databases.

   Note:
   If the user account cannot be granted the required privileges, then the SQL databases must be manually created by a user, typically a database administrator, who does have sysadmin privileges. In this situation, the SQL databases must be created first, before PI Integrator for Business Analytics is installed.

   Note:

   Go to OSIsoft Tech Support (https://techsupport.osisoft.com) to download the PI Integrator for Business Analytics 2018 R2 SQL Utility which contains the script that creates the databases.

   After you install the SQL databases, add the user account that will install PI Integrator for Business Analytics as a login on SQL Server. The user installing the PI Integrator for Business Analytics must have db_accessadmin database role membership on the PIIntegratorDB, PIIntegratorStats, and PIIntegrator databases. In addition, the user must have db_datareader database role membership on the PIIntegratorStats database.

6. The user account used to install PI Integrator for Business Analytics must be mapped to the Administrators identity in PI AF.

7. Verify that the following ports are available. The following table describes how these ports are used in the PI Integrator for Business Analytics architecture.

Functionality	Remote Application	Protocol	Port	Direction	Configured On
PI Integrator for Business Analytics connection to SQL database	PI Integrator for Business Analytics	TCP	1433[1]	Inbound	SQL Server
Client connections to PI Integrator for Business Analytics user interface	Client web browser	TCP	443[2]	Inbound	PI Integrator for Business Analytics server
PI ODBC connections to PI SQL DAS (required only for the PI View target)	PI ODBC Driver	TCP	5461	Inbound	PI SQL DAS (PI Integrators) server
PI Integrator for Business Analytics outgoing data (required only for Microsoft Azure IoT Hub or Microsoft Azure Event Hub)	Microsoft Azure IoT Hub or Microsoft Azure Event Hubs	TCP	5671	Outbound	PI Integrator for Business Analytics server
PI Integrator for Business Analytics connection to publish target	Check with your IT department to ensure that the inbound port that is required on your publish target is open.				

[1] This connection can be configured to use a dynamic port.

[2] The default port for HTTPS is 443, but an alternate port can be specified during the PI Integrator for Business Analytics installation.

8. (Optional) Contact your IT administrator to request that Kerberos constrained delegation be configured for the service account that runs PI Integrator for Business Analytics to delegate to PI AF in order to restrict access in the PI Integrator for Business Analytics user interface to only the PI AF databases and items permitted by the existing PI AF security. If desired, Service Principal Names (SPNs) can be created for the service account prior to installing PI Integrator for Business Analytics.

   For details on configuring Kerberos delegation, refer to Kerberos constrained delegation.

9. (Optional) If you will be publishing to the PI View target and PI Integrator for Business Analytics, PI AF, and clients are on different servers, contact your IT administrator and request that Kerberos constrained delegation be configured for the account (typically the PI Integrator for Business Analytics machine account) running PI SQL DAS (PI Integrators) to delegate to PI AF to provide clients with PI View data access. For more information, see the *PI SQL Data Access Server (PI Integrators) 2016 R2 Administrator Guide*.

10. (Optional) Contact your IT administrator to request a certificate from a Certificate Authority issued to the server that runs PI Integrator for Business Analytics. The certificate Subject should include the fully-qualified domain name (FQDN) of the server, and the Subject Alternative Name should include both the FQDN and the host name of this server.

11. (Optional) Contact your IT administrator if you are installing PI Integrator for Business Analytics in an environment where there are multiple domain controllers or a read-only domain controller. There may be additional port requirements for these environments. For more information, refer to the Microsoft documentation on Active Directory and Active Directory Domain Services Port Requirements (https://docs.microsoft.com/en-us/

previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/dd772723(v=ws.10)).

Phase 2: Install PI Integrator for Business Analytics

Phase 2 involves installing PI Integrator for Business Analytics and specifying the PI AF server and Microsoft SQL Server.

Before you start

Before you install PI Integrator for Business Analytics:

- Ensure that you have met all of the prerequisites in: Phase 1: Prepare for installation.
- Ensure that you have local-admin privileges on the computer where you are installing PI Integrator for Business Analytics.
- If the user account used to install PI Integrator for Business Analytics does not have the sysadmin privileges required to install the SQL databases, then the databases must be manually created by a user with sysadmin privileges. This must be completed before you install PI Integrator for Business Analytics. Otherwise, the installation will fail.

  Go to OSIsoft Tech Support (https://techsupport.osisoft.com) Downloads page to download the PI Integrator for Business Analytics 2018 R2 SQL Utility which contains the script that creates the databases.

  Note:

  If the SQL databases are manually installed, the user account that is used to install PI Integrator for Business Analytics requires the following privileges:

  - db_accessadmin database role membership on the PIIntegratorDB and PIIntegratorLogs databases
  - db_accessadmin database role membership and SELECT privileges on the PIIntegratorStats database

Note:

Each instance of any PI Integrator product built on the PI Integrator Framework must be installed on its own machine. For example, PI Integrator for Business Analytics and PI Integrator for SAP HANA cannot be installed on the same machine, nor can two instances of PI Integrator for Business Analytics.

Procedure

1. Log on to the computer where you will be installing PI Integrator for Business Analytics.
2. Download the latest version of the PI Integrator for Business Analytics setup kit from the Technical Support (https://techsupport.osisoft.com/Downloads/All-Downloads/) Download Center.
3. Right-click the setup executable and click **Run as Administrator** to run the installation wizard.

   The Self-Extracting Executable window opens.
4. Specify the extraction path for the installer and click **OK.**

The Welcome to the PI Integrator for Business Analytics 2018 R2 Setup window opens, listing the separate modules included with the installation. The installation wizard installs each module or ensures that the module already exists on your system.

5. Click **OK**.
6. If no OSIsoft products have been previously installed on this computer, then complete the following steps. Otherwise, skip to the next step.

   a. In the Default Servers window, specify the PI Data Archive server and, optionally, the PI AF Server, and click **Next**.

   b. In the Installation Directories window, specify the locations for installing OSIsoft products. You can either accept the defaults or specify a different location.

      Note:
      PI Integrator for Business Analytics is installed in %PIHOME64%.

   c. Click **Next**.
7. In the Welcome to the PI Integrator for Business Analytics 2018 R2 Installation window, click **Next**.

   The Customer Experience Improvement window is displayed
8. Select one of the options and click **Next**.
9. In the Logon Information window, specify the **Username** (including domain) and **Password** for the Windows service account that will run the PI Integrator for Business Analytics services.
10. Click **Next**.

    The AF Server Connection window opens.
11. Specify the PI AF server on which PI Integrator for Business Analytics will store the view definitions and other metadata.

    In the **AF Server** field, enter the name or location (IP address) of the PI AF server.

    Note:
    If you encounter an error, ensure that the user account used to install PI Integrator for Business Analytics is mapped to the Administrators AF identity on the PI AF server.
12. Click **Next**.

    The SQL Server window opens.
13. Specify the Microsoft SQL Server on which PI Integrator for Business Analytics will store PI View data, statistical data, and PI Integrator for Business Analytics logs.

    Specify only the host name (or fully-qualified domain name) if you're using the default instance. If you are using a named instance, specify the host name (or fully-qualified domain name) and instance, for example: mySQLserverBA1\PIViewInstance.
14. Specify how PI Integrator for Business Analytics will be authenticated with the specified Microsoft SQL Server database. Choose one of the following:

    - Windows Authentication (Default)

      The Windows service account user is used as the credentials to connect to the Microsoft SQL Server.
    - SQL Server Authentication

> **Note:**
>
> SQL Server authentication is *not* recommended. Create a login specifically for the PI Integrator Framework service.

i. Click **SQL Server Authentication** to use SQL Server authentication to connect to the specified Microsoft SQL Server database.

ii. Enter the user name and password for the dedicated Microsoft SQL Server user that has the required access to the Microsoft SQL Server.

15. Click **Next**.

    The Port and SSL Certificate Configuration window opens.

16. Enter a valid available port number in the **Enter a port number** field and click **Validate Port**.

    This port is used in a web browser to connect to PI Integrator for Business Analytics.

    > **Tip:**
    > If you use the default port, 443, you can omit this port number when you specify the URL for PI Integrator for Business Analytics.

17. Choose an SSL certificate from one of the following sources:

    - (Recommended) SSL certificate from a certificate authority. Choose **Import certificate** and click **Select Certificate** to choose a certificate that has been issued by a certificate authority and imported to the machine where PI Integrator for Business Analytics is being installed.

    - Self-signed certificate that is generated during the installation. This is the default. Choose **Self-signed certificate**.

      > **Note:**
      > If you choose this option, users logging in from remote machines may see a security warning message. To avoid this warning for self-signed certificates, the certificate must be explicitly trusted on the client machine. See the workaround in the OSIsoft Tech Support article KB01415 - Certificate error returned when navigating to a PI Coresight web site using a self-signed certificate (https://techsupport.osisoft.com/Troubleshooting/KB/KB01415/).

18. Click **Next**.

    > **Note:**
    > If you encounter an error, ensure that the port is unused and open.

19. In the PI Integrator Worker Nodes window, click the arrow and select the number of worker nodes you want installed, and then click **Next**.

    The Ready to Install the Application window opens.

    > **Note:**
    >
    > Each worker node requires additional CPU and RAM. For more information on the resources required, see System requirements, and for more information about worker nodes, see PI Integrator for Business Analytics scale architecture.

20. Click **Install**.

The Updating System window opens showing the progress of the installation.

21. When the installation is finished, the Installation Complete window appears. Click **Close.**

Phase 3: Verify the installation

After you complete installing PI Integrator for Business Analytics, verify that its services are running.

Procedure

1. Log on to the machine hosting PI Integrator for Business Analytics.
2. Open **Services**.
3. Verify that the PI Integrator for Business Analytics services are listed and running.

   You should see the following services:

   - PI Integrator Framework
   - PI Integrator Sync
   - PI Integrator Worker Node 1
   - PI Integrator Worker Node *n* (You will see a service for each worker node created.)
4. Open a web browser.
5. Enter the URL for PI Integrator for Business Analytics.

   The URL points to the host machine and port for PI Integrator for Business Analytics. The URL is https://*host name or FQDN*:*port number*, where *FQDN* is the fully-qualified domain name.

   If you installed PI Integrator for Business Analytics on a host named *lab5* in the domain *prod.onet.com* and configured it to use port *7777*, you could enter either of the following:

   - `https://lab5.prod.onet.com:7777`
   - `https://lab5:7777`

Post-installation tasks

After you have completed installing PI Integrator for Business Analytics, navigate to the PI Integrator Framework service URL. For more information, see Start PI Integrator for Business Analytics.

Then complete the following tasks before you start using PI Integrator for Business Analytics:

- Add the PI AF servers and databases from which you will be accessing your PI System data. See Add PI AF servers and databases.
- Add users who will be able to create views. See Add and configure identities.
- Complete any setup tasks required for your publish target. See Set up your publish targets.
- Ensure that the service account that runs the PI Integrator Framework service has read access to any PI AF servers, PI AF databases, PI AF objects (elements, attributes, templates, and so on), and PI points that are used in your views. The service account requires PI Data

Archive permissions because the PI Integrator Framework service queries PI Data Archive directly for PI AF attribute data that are PI point data references.

Add PI AF servers and databases

You can specify additional PI AF servers and databases that contain data that can be used in your asset and event views.

Procedure

1. Click the menu icon ☰ and click **Administration**.
2. On the Administration page, click the **AF Databases** tab.
3. In the **Add a new AF Server** section of the page, enter the name or location (IP address) of the PI AF server in the **AF Server** field.
4. If your PI AF server is not using the default port (5457), specify the port to use in the **Port** field.
5. Click **Add AF Server**.

Add and configure identities

This procedure describes how to create a new identity, add users to the identity, and configure the identity's access to publish targets and views.

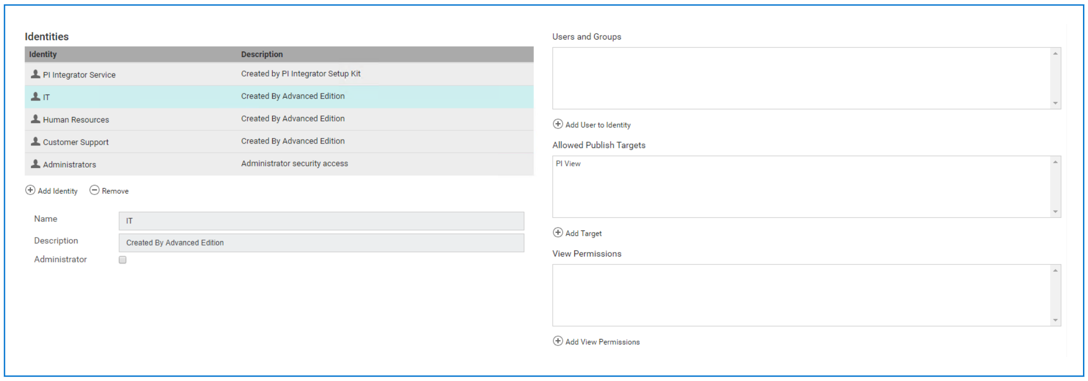
Procedure

1. Click the menu icon ☰ and click **Administration**.
2. On the **Administration** page, click the **Users** tab. The Identities page opens.
3. Click **Add Identity**.

   The Add Identity dialog box opens.

4. Do one of the following:
   - Enter the name of a new identity in the **identity name** field and click **Create.**
   - Select an identity from the list and click **Ok.**

   The list shows all identities that are associated with the PI AF server that hosts the configuration for PI Integrator for Business Analytics. The **Name** field is populated with the identity.



Identities

Identity	Description
PI Integrator Service	Created by PI Integrator Setup Kit
IT	Created By Advanced Edition
Human Resources	Created By Advanced Edition
Customer Support	Created By Advanced Edition
Administrators	Administrator security access

Name: IT

Description: Created By Advanced Edition

Administrator: □

Users and Groups

Allowed Publish Targets: PI View

View Permissions

5. Click **Add User to Identity** to add Windows Active Directory users to the identity.
6. In the Add Users and Groups dialog box, enter the domain and username in the **domain\user** field.

   Use the `domain\user` format. Or you can enter the full name of the user in the **full name** field.
7. Click **Search.**

   A list of Active Directory users appears matching the entered criteria.
8. Select a user from the list and click **Ok.**

   The user appears in the **Users and Groups** list.
9. Click **Add Target** to grant the identity access to publish targets.

   By default, all identities are granted access to the PI View target. Generally, when a new identity is added, this is the only target displayed. If the desired targets do not appear in this list, first create the target, then grant the identity access to it.
10. In the Add Publish Targets dialog box, select the targets you want to grant the identity access to and click **Ok.**

    The targets appear in the **Allowed Publish Targets** list.
11. Click **Add View Permissions** to grant the identity access to any existing views.
12. In the Add View Permissions dialog box, select the views you want to grant the identity access to and click **Ok.**

    The views appear in the **View Permissions** list.
13. Click the arrow and choose one of the following permissions:
    - **Reader** grants access to the view configuration in the PI Integrator for Business Analytics user interface. Reader also grants access to the data published to the PI View target.
    - **Owner** grants the permissions of Reader. In addition, it gives the identity the ability to change the view permissions and grant view permissions to other identities.

Upgrade PI Integrator for Business Analytics

PI Integrator for Business Analytics installs executable files, including upgrading the Microsoft .NET framework files.

If any views are running when the upgrade begins or are scheduled to be run while the upgrade is taking place, PI Integrator for Business Analytics stops or postpones the jobs before it begins upgrading the executable files. Once the upgrade is completed, it restarts the jobs or resumes running the jobs.

If you prefer, you may manually stop any jobs that are running. However, you will have to remember to restart the jobs once the upgrade is completed.

Before you start

- Upgrades from PI Integrator for Business Analytics 2016 R2 SP1 or later to PI Integrator for Business Analytics 2018 R2 are supported. If you have an earlier version, you must first upgrade to 2016 R2 SP1 before you can upgrade to PI Integrator for Business Analytics 2018 R2.
- Upgrades from PI Integrator for Microsoft Azure 2016 R2 to PI Integrator for Business Analytics 2018 R2 are supported.
- Before you upgrade PI Integrator for Business Analytics ensure that you have `local-admin` privileges on the computer where you are installing PI Integrator for Business Analytics.
- If you are upgrading from PI Integrator for Business Analytics 2018, you must have SELECT, ALTER, and UPDATE permissions on the PIIntegratorStats database.

  If you do not have these permissions on the PIIntegratorStats database, then it must be manually updated before you upgrade PI Integrator for Business Analytics

  Download the PI Integrator for Business Analytics 2018 R2 SQL Utility from the Tech Support Download Center. A system administrator or a user with SELECT, ALTER, and UPDATE permissions on the PIIntegratorStats database must run the `UpdateStatsTable.sql` script. Once the database is upgraded, the user running the PI Integrator for Business Analytics install kit only needs SELECT permissions on the PIIntegratorStats database to upgrade PI Integrator for Business Analytics.
- Microsoft SQL Server Full-Text Search component is a requirement of PI Integrator for Business Analytics. Full-Text Search allows PI Integrator Framework service to efficiently index and manage large numbers of PI tags and keep track of changes to the view shapes. Note that Full-Text Search is an optional component of the SQL Server Database Engine and can be added during the Microsoft SQL Server installation or added later by running SQL Server Setup. It must be installed prior to upgrading PI Integrator for Business Analytics.
- If you used SQL Server authentication in the previous installation, the upgrade process assumes you are using the same SQL Server user login. If you change your login or you want to use Windows authentication instead, you must first uninstall PI Integrator for Business Analytics, and then install the latest version of the product.
- If PI Integrator for Business Analytics was running against PI AF Server 2014 or earlier, then you must upgrade to PI AF 2015 or later before upgrading PI Integrator for Business Analytics. Otherwise your existing PI Integrator for Business Analytics users will not be automatically converted to PI AF identities. For more information, see User Permissions.

Note:

During the upgrade, you will not be able to specify a new PI AF Server or SQL Server.

Procedure

1. Download the PI Integrator for Business Analytics setup kit from the Technical Support (https://techsupport.osisoft.com/) Download Center.
2. Right-click the setup executable and click **Run as Administrator** to launch the installation wizard.

   The Self-Extracting Executable window opens.
3. Specify the extraction path for the installer and click **OK**.

   The Welcome to the PI Integrator for Business Analytics 2018 R2 Setup window opens, listing the separate modules included with the installation. The installation wizard upgrades each module or ensures that the correct version of the module already exists on your system.
4. Click **OK**.

   The Welcome to the PI Integrator for Business Analytics 2018 R2 Installation window opens.
5. Click **Next.**

   The Logon Information window opens.
6. Specify the **Password** for the Windows service account that runs the PI Integrator for Business Analytics services.
7. Click **Next**.

   The Port and SSL Certificate Configuration window opens.
8. Enter a valid available port number in the **Enter a port number** field and click **Validate Port**.

   This port is used by the PI Integrator for Business Analytics user interface to connect with the PI Integrator Framework service component.

   Tip:
   If you use port 443, you can omit this port number when you specify the URL for PI Integrator for Business Analytics.
9. Choose an SSL certificate from one of the following sources:

   - (Recommended) SSL certificate from a certificate authority. Choose **Import certificate** and click **Select Certificate** to choose a certificate that has been issued by a certificate authority and imported to the machine where PI Integrator for Business Analytics is being installed.
   - **Self-signed certificate** that is generated during the installation. This is the default.

     Note:
     If you choose this option, users logging in from remote machines may see a security warning message. To avoid this warning for self-signed certificates, the certificate must be explicitly trusted on the client machine. See the workaround in the OSIsoft Tech Support article KB01415 - Certificate error returned when navigating to a PI Vision or PI Web API web site using a self-signed certificate (https://techsupport.osisoft.com/Troubleshooting/KB/KB01415/).

10. In the PI Integrator Worker Nodes window, click the arrow and select the number of worker nodes you want installed, and then click **Next**.

    The Ready to Install the Application window opens.

    > **Note:**
    >
    > Each worker node requires additional CPU and RAM. For more information on the resources required, see System requirements, and for more information about worker nodes, see PI Integrator for Business Analytics scale architecture.

11. Click **Next**.

    The Ready to Install the Application window opens.

    > **Note:**
    > If you encounter an error, ensure that the port is unused and open.

12. Click **Install**.

    The Updating System window opens showing the progress of the installation.

13. When the installation is finished, the Installation Complete window appears. Click **Close.**

Set up your publish targets

Complete the following procedure to set up your publish targets.

Procedure

1. If you are publishing your PI System data to one of the following targets, follow the instructions in the referenced topic to set up the target. For all other targets, skip to the next step.

    - PI View – Install PI ODBC on your client machines. For more information, see Install driver for the PI View target.

    - Azure Data Lake Store – Refer to Set up the Azure Data Lake Store target.

    - Oracle Database – Refer to Set up the Oracle Database publish target.

    - Azure SQL Database or Azure SQL Data Warehouse target – Refer to Set up the Azure SQL Database or Azure SQL Data Warehouse target.

    - Amazon Redshift – Install Amazon Redshift ODBC driver on the machine where PI Integrator for Business Analytics is installed – Refer to Install and configure the Amazon Redshift ODBC driver.

2. Add the publish target to PI Integrator for Business Analytics. See Add a publish target.

3. Configure the publish target. Refer to the topic for configuring your target.

4. Grant users access to the publish target. See Grant access to targets.

Add a publish target

This topic describes how to add publish targets.

> **Note:**
>
> - The available target outputs are determined by the software edition and/or license.
>
> - The PI View target is automatically created when you install PI Integrator for Business Analytics. No additional configuration is required.

Procedure

1. Click the menu icon ☰ and click **Administration.**

2. Click the **Targets** tab.

    The **Publish Target Configuration** page opens.

3. Click **Add Publish Target.** The **Create a New Publish Target** dialog box opens.

4. Enter the name of the publish target in the **Target Name** field. Click **Target Type** and select the output type from the list.

5. Click **Create New Target.**

Configure Amazon Kinesis target

Complete the procedure below to configure the Amazon Kinesis target and verify that you can write to the Amazon Kinesis Data Streams.

Before you start

- Create the Amazon Kinesis target before you configure it. For more information, see Add a publish target.

Procedure

1. On the Administration page, click the **Targets** tab. Then select the target in the **Publish Targets** list.

   Note:
   If you have already selected your target, skip to the next step.

2. Refer to the following table and enter the required information. Click the buttons as they become enabled.

Parameter	Description
AWS Access Key ID	Used in combination with Secret Access Key to authenticate requests to the stream. **Note:** There may be more than one ID, but only one Secret Access Key.
AWS Secret Access Key	Used in combination with AWS Access Key ID to authenticate requests to the stream. **Note:** There may be more than one ID, but only one Secret Access Key.
Kinesis Data Stream	Name of the Amazon Kinesis Data Stream to which data is written.
Region	Geographic area this client communicates with. Default: US East (N. Virginia)
Data Storage Format	(Optional) File format in which data is stored. The default is Parquet.
Compression	(Optional) Compression type on message sets. The default is None.
Allow Nulls	(Optional) When selected, null values are valid.

3. Click **Verify Writer**.
4. Click **Save Changes**.

After you finish

- Give users access to the Amazon Kinesis target. For more information, see Grant access to targets.
- Ensure that the Kinesis Data Streams producer has the following permissions on the Amazon Kinesis target: DescribeStream, PutRecord/PutRecords actions.

Install and configure the Amazon Redshift ODBC driver

You must install and configure the Amazon Redshift ODBC driver on the machine where PI Integrator for Business Analytics is installed before you configure the Amazon Redshift target.

Procedure

1. From the Install and Configure the Amazon Redshift ODBC Driver on Microsoft Windows Operating Systems (https://docs.aws.amazon.com/redshift/latest/mgmt/install-odbc-driver-windows.html) page, download the installer file depending on the system architecture of your SQL client tool or application:
   - 32-bit – Amazon Redshift (x86)
   - 64-bit – Amazon Redshift (x64)
2. Run the file to install the Amazon Redshift ODBC driver.
3. Follow the instructions to configure the driver.

Configure Amazon Redshift target

Complete the procedure below to configure the Amazon Redshift target and verify that you can write to the Amazon Redshift database.

Before you start

- Install and configure the Amazon Redshift ODBC driver. For more information, see Install and configure the Amazon Redshift ODBC driver.
- Create the Amazon Redshift target before you configure it. For more information, see Add a publish target.

Procedure

1. On the Administration page, click the **Targets** tab. Then select the target in the **Publish Targets** list.

   > **Note:**
   > If you have already selected your target, skip to the next step.

2. Refer to the following table and enter the required information. Click the buttons as they become enabled.

Parameter	Description
ODBC Driver	(Optional) ODBC driver that connects to the Amazon cluster. The default is Amazon Redshift (x64).

Parameter	Description
Cluster Name	Amazon cluster node to which data is sent.
Cluster Database Port	(Optional) Port through which to connect to the cluster database. The default is 5439.
Cluster Database Name	Cluster database to which data is written.
Database Username	Database username used to connect to the cluster.
Password	Password for the database username used to connect to the cluster.

3. Click **Verify Writer**.
4. Click **Save Changes**.

After you finish

- Give users access to the Amazon Redshift target. For more information, see Grant access to targets.
- Ensure that PI Integrator for Business Analytics Windows service account has the following minimum permissions on the Amazon Redshift target: SELECT, CREATE, DROP, UPDATE, and INSERT.

Configure Amazon S3 target

Complete the procedure below to configure the Amazon S3 target and verify that you can write to the Amazon S3 database.

Before you start

- Create the Amazon S3 target before you configure it. For more information, see Add a publish target.

Procedure

1. On the Administration page, click the **Targets** tab. Then select the target in the **Publish Targets** list.

   Note:
   If you have already selected your target, skip to the next step.

2. Refer to the following table and enter the required information. Click the buttons as they become enabled.

Parameter	Description
Data Storage Format	File format in which data is stored. The default is Parquet.
Compression	Compression type on message sets. The default is None. **Note:** Choose a compression setting to get better performance.

Parameter	Description
AWS Access Key ID	Used in combination with Secret Access Key to authenticate requests to the stream. **Note:** There may be more than one ID, but only one Secret Access Key.
AWS Secret Access Key	Used in combination with Amazon Access Key ID to authenticate requests to the stream. **Note:** There may be more than one ID, but only one Secret Access Key.
Include Header	When selected, column names are added to the beginning of the file.
Field Delimiter	Character(s) that separate the data fields in the row. By default, a tab (\t), separates the fields.
Row Delimiter	Character(s) that separate the data rows. By default, a new line separates the data rows. The characters that specify a new line are platform-specific. The default automatically provides the correct characters for the environment.
Bucket Name	S3 bucket that data is uploaded to.
Folder Path	(Optional) Specify with key name prefixes and forward slashes (/) to organize views in S3. The key name prefixes must exist in S3 before you configure the target. For more information about creating a logical hierarchy in S3, see Object Key and Metadata (https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingMetadata.html).
Region	Geographic area that this client communicates with. Default: US East (N. Virginia)
Allows Nulls	When selected, null values are valid.
Maximum Rows/Objects	(Optional) Maximum number of objects in a file. Default: 100,000 rows. See the Note below.
Maximum File Size (KB)	(Optional) Maximum file size in kilobytes. Default: 10,000 KB. See the Note below.
Maximum Update Time (sec)	(Optional) Maximum time to update the database, in seconds, before the writer times out. Default: 86,400 seconds (1 day). See the Note below.
Amazon Athena Database	(Optional) Name of the Amazon Athena database that data is written to.

Note:

Specify one of the three optional parameters: **Maximum Rows/Objects**, **Maximum File Size**, or **Maximum Update Time.** If none are specified, then views will always be published to the same file and a new file will never be created.

The three parameters have default values and all defaults are enforced. The first parameter reached will trigger the creation of a new file. To standardize on one parameter for new file creation, enter very large values that are impossible to reach for the remaining parameters.

3. Click **Verify Writer**.
4. Click **Save Changes**.

After you finish

- Give users access to the Amazon S3 target. For more information, see Grant access to targets.
- Ensure that PI Integrator for Business Analytics Windows service account has the following permissions on the Amazon S3 target: List Objects, Write Objects, Read Bucket Permissions, and Write Bucket Permissions.
- If you are using the Amazon Athena database, then ensure PI Integrator for Business Analytics Windows service account has the following permissions on the database: SELECT, CREATE, UPDATE, SHOW DATABASE, SHOW TABLES, and CREATE EXTERNAL TABLE.

Configure Apache Hive targets

Complete the procedure below to configure the Apache Hive target and test your connection to the Hive database.

> **Tip:**
> Enter the information in the fields in order. After the required information has been specified in the fields, the buttons are enabled. Click the button before continuing to the next field.

Before you start

Create the Apache Hive target before you configure it. For more information, see Add a publish target.

Procedure

1. On the Administration page, click the **Targets** tab. Then select the target in the **Publish Targets** list.

   > **Note:**
   > If you have already selected your target, skip to the next step.

2. Refer to the following table and enter the required information. Click the buttons as they become enabled.

Parameter	Description
`HDFS URL`	URL to access HDFS through WebHDFS directly, or through the Apache Knox gateway or HttpFS. Examples: ◦ HDFS – http://host:50070/webhdfs/v1 ◦ HttpFS – http://host:14000/webhdfs/v1 ◦ Apache Knox – https://host:8443/gateway/default/webhdfs/v1
`Verify SSL Certificate`	Select the check box if you are using an SSL certificate.
`Username`	User name used to connect to HDFS. The user must have permissions to read and write to HDFS.

Parameter	Description
`Password`	(Optional) Password to authenticate the user or when connecting to HttpFS. If a password is provided, then Hadoop HTTP authentication is used. If no password is entered, then PI Integrator for Business Analytics uses Hadoop simple authentication.
`Directory`	Directory where the data files are created. Click **Browse** to navigate to the directory where you want the files located. The format for specifying the directory location is: `/rootfolder/folder1/folder2`.
`Hive Hostname`	Host name of the machine on which Thrift is running. This name can be an alias, internal address, or IP address. The default is host name in the HDFS URL.
`Hive Port`	(Optional) Port through which to connect to Thrift.
`Hive Username`	(Optional) Username used to connect to HCatalog.
`Hive Table Format`	Format in which to store tables in Apache Hive. The current supported file formats are text (TEXTFILE) and optimized row columnar (ORC). **Note:** ORC requires Apache Hive 0.11 or later.
`Hive Database`	Name of database in Apache Hive in which the tables are created.

3. Click **Connect to Apache Hive.**

   PI Integrator for Business Analytics connects to Apache Hive, queries the database, and populates the **`Hive Table Format`** and **`Hive Database`** fields with the supported table formats and databases.

4. Click **Verify Apache Hive Writer** to verify that Apache Hive writer can write to the Hive database.

   Note:

   If you are unable to successfully write to the Hive database, refer to Tips for setting up Apache Hive.

5. Click **Save Changes.**

After you finish

Give users access to the Apache Hive target. For more information, see Grant access to targets.

Tips for setting up Apache Hive

In order for Apache Hive to work with PI Integrator for Business Analytics, you must complete the following tasks:

- Create the HDFS user.
- Create the HCat user.
- Create the user directory and grant permissions.
- Disable SASL.

The following procedure describes how to complete these tasks.

Procedure

1. Create the HDFS user.

    a. Create the HDFS user on the node where WebHDFS is installed.

    b. Add the HDFS user to a group.

    Note:

    The HDFS user can be added to any group. However, for the purposes of this example, this group will be referred to as the HDFS group.

2. Create the HCat user.

    (Optional) If HCat is on a different node, then you must add the HCat user.

    a. Create the HCat user on the node where HCat is installed.

    b. Add the HCat user to the HDFS group.

3. Create the user directory and grant permissions.

    In the following procedure, you create a user directory and ensure it is set up correctly so that the HDFS user can write to it.

    a. Create a user directory on HDFS.

    b. Change the owner of this directory to the HDFS user.

    c. Change the group to which this directory belongs to HDFS.

    d. Grant read and write permissions to the owner of the directory (that is, the HDFS user).

    e. Grant read and write permissions to the group to which the directory belongs.

4. Disable SASL.

    Note:

    PI Integrator for Business Analytics only supports Apache Hive targets that are configured with NOSASL authentication. For more information on Apache Hive authentication options, see Setting Up HiveServer2 (https://cwiki.apache.org/confluence/display/Hive/Setting+Up+HiveServer2#SettingUpHiveServer2-Authentication/SecurityConfiguration).

Configure Apache Kafka target

Complete the procedure below to configure the Apache Kafka target and verify that you can write to the Apache Kafka database.

Before you start

- Create the Apache Kafka target before you configure it. For more information, see Add a publish target.
- (Optional) Verify that OpenSSL is installed on the machine where PI Integrator for Business Analytics is installed. This step is only required if you are using TLS to connect to Apache Kafka.

Procedure

1. On the Administration page, click the **Targets** tab. Then select the target in the **Publish Targets** list.

   > **Note:**
   > If you have already selected your target, skip to the next step.

2. Refer to the following table and enter the required information. Click the buttons as they become enabled.

Parameter	Description
`Kafka Brokers`	Comma-separated list of Kafka brokers. Specify using `Host:Port, Host:Port` format.
`Codec`	Compression type on messages sets. The default is None. Valid choices include: gzip, Snappy, and LZ4.
Use TLS	Use TLS (Transport Layer Security) when connecting to Kafka brokers. **Note:** SSL is deprecated and has been replaced with TLS. While TLS is required to connect to Apache Kafka, the two terms are often used interchangeably in Apache Kafka.
Client Certificate	Full path to the client certificate (`.pem` file). Required only if TLS is used. Contact your Apache Kafka administrator for an OpenSSL client certificate for PI Integrator for Business Analytics. For more information on TLS, see Encryption and Authentication with SSL (https://docs.confluent.io/current/kafka/authentication_ssl.html).
Client Key	Full path to the client key file (`.key` file). Required only if TLS is used.
Key Password	Password to the TLS certificate key file. Required only if TLS is used.
CA Root Certificate	Full path to the CA Root certificate used to sign the client certificate. Required only if TLS is used.
SASL Mechanism	SASL mechanism used. Four authentication mechanisms are supported: GSSAPI (also known as Kerberos), PLAIN, SCRAM-SHA-256, and SCRAM-SHA-512. It is a best practice to combine PLAIN, SCRAM-SHA-256, or SCRAM-SHA-512 with TLS encryption so that encrypted passwords are sent over the network.
Username	Kafka username for SASL authentication. Not used with GSSAPI authentication.
Password	Kafka password for SASL authentication. Not used with GSSAPI authentication.

3. Click **Verify Kafka Writer**.
4. Click **Save Changes**.

After you finish

- Give users access to the Apache Kafka target. For more information, see Grant access to targets.
- If you are using TLS to connect to the Apache Kafka brokers, then you must convert the Windows certificates to OpenSSL certificates. See your Apache Kafka administrator if you need help converting these files.

Set up the Azure Data Lake Store target

Complete the following procedure to set up the Azure Data Lake Store target.

Procedure

1. Set up the Data Lake Store environment and install the Data Lake Store. For more information, see Tips to set up the Azure Data Lake environment.
2. Add the publish target to PI Integrator for Business Analytics. See Add a publish target.
3. Configure the Azure Data Lake Store target. For more information, see Configure the Azure Data Lake Store target.
4. Grant users access to the publish target. See Grant access to targets.

Configure the Azure Data Lake Store target

Complete the procedure below to configure the Azure Data Lake Store target.

Before you start

- Complete setting up your Azure Data Lake environment and gathering the information required to configure the target. For more information, see Tips to set up the Azure Data Lake environment.
- Create the Azure Data Lake Store target before you configure it. For more information, see Add a publish target.

Procedure

1. On the Administration page, click the **Targets** tab. Then select the target in the Publish targets list.
2. Configure the Azure Data Lake Store target with the following parameters:

Parameter	Description
Tenant ID	Identifier for your Azure Active directory.
Client ID	Identifier for the Azure Data Lake application that authenticates the PI Integrator for Business Analytics application with the Azure Data Lake Store.
Client Key	Key used to authenticate PI Integrator for Business Analytics.
Subscription ID	Subscription ID for the Azure account.

3. Click **Authenticate** to verify that the provided credentials allow PI Integrator for Business Analytics to connect to the Azure Data Lake Store.

   If authentication is successful, a list of data lakes appears in the **Azure Data Lake Stores** list.

4. Continue configuring the following parameters:

Parameter	Description
Azure Data Lake Stores	Data lake in which your data is stored.
ADL Directory	Browse to navigate to the location or manually enter the location to which the data is written.
Append Timestamp	When selected, a timestamp of when the view is published is appended to the file name and a new file is created each time the view is published. If not selected, then the data is appended to the existing file.
Include Header	When selected, column names are added to the beginning of the table.
Field Delimiter	Character(s) that separate the data values in the Azure Data Lake file. The default is a tabbed space. To choose a tab delimiter, either leave the field blank or enter `\t`. **Note:** Do not use a character that appears in your data, for example, a period.
File Extension	(Optional) The default, if the field is left blank, is `.txt`. **Note:** The file format does not change if you change the extension.

5. Click **Verify ADL Writer** to verify that PI Integrator for Business Analytics can write to the specified Azure Data Lake Store location.

6. Click **Save Changes**.

After you finish

Give users access to the Azure Data Lake Store target. For more information, see Grant access to targets.

Tips to set up the Azure Data Lake environment

Before you can configure the Azure Data Lake Store target, you will need to set up your Azure Data Lake environment. This includes the following:

- Obtain the Tenant ID of the Active Directory
- Create and configure an Azure Data Lake application
- Create an Azure Data Lake Store

To get started with Azure Data Lake Stores, refer to the following Microsoft site: Get started with Azure Data Lake Storage Gen1 using the Azure portal (https://azure.microsoft.com/en-us/documentation/articles/data-lake-store-get-started-portal/).

As you create your Azure Data Lake environment, you will be collecting the following pieces of information:

- Tenant ID — ID that identifies Active Directory
- Client ID — ID that identifies the Azure Data Lake application
- Client Key— Used to authenticate PI Integrator for Business Analytics
- Subscription ID — ID that identifies Azure Data Lake Store

Note:

OSIsoft recommends you copy these values to a text file for reference later.

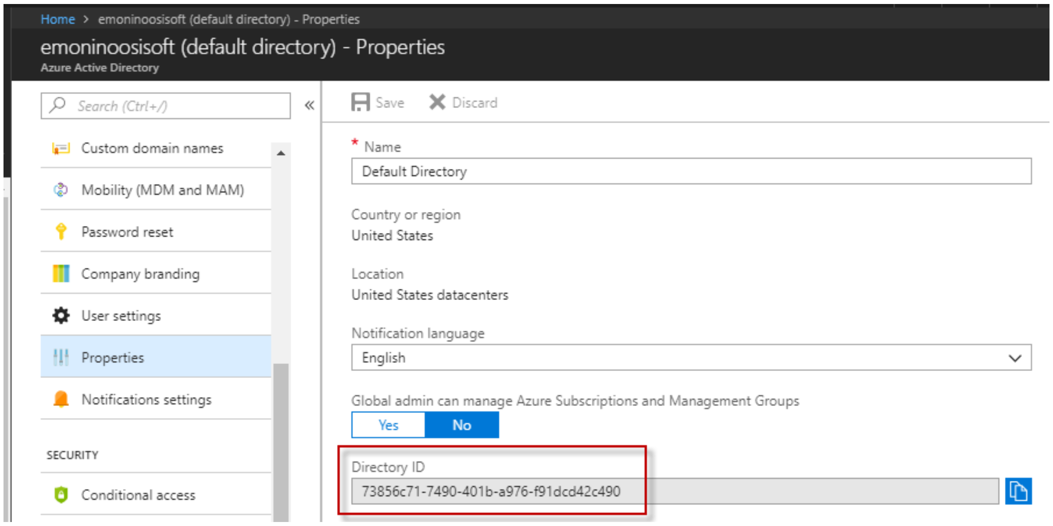
You will need this information when you configure your Microsoft Azure Data Lake Store target. This information is used by PI Integrator for Business Analytics to connect to your Azure Data Lake Store.

Obtain the Tenant ID for Azure Active Directory

Note:
There are many ways to obtain the Tenant ID. Refer to Microsoft documentation for other alternatives.

Procedure

1. From the Microsoft Azure portal (https://portal.azure.com), log into the account to connect to the Azure Data Lake service.
2. Select the Azure Active Directory where the web application is created.
3. Click **Properties**.



Home > emoninoosisoft (default directory) - Properties

emoninoosisoft (default directory) - Properties

Azure Active Directory

* Name
Default Directory

Country or region
United States

Location
United States datacenters

Notification language
English

Global admin can manage Azure Subscriptions and Management Groups
Yes [✓ No]

Directory ID
73856c71-7490-401b-a976-f91dcd42c490

Note:

With subsequent portal updates, the screen may look different and the parameters may be located elsewhere.

The Tenant ID is the value in the **Directory ID** field.

4. Copy this string to a text file.

The Tenant ID is required to configure the Azure Data Lake Store target. See Configure the Azure Data Lake Store target for more information.

Configure the web application to access the web APIs

The web application accepts incoming requests from PI Integrator for Business Analytics and controls access to Azure Data Lake Store.

Procedure

1. Open a web browser and go to the Microsoft Azure portal (https://portal.azure.com) and navigate to Azure Active Directory.
2. Create and configure a web application.

   Tip:
   Be sure to create your web application *within* Active Directory. This application should not be confused with an *Azure web application*.

   Note:
   When you create the web application, a client ID is automatically assigned to the application.

   a. Copy the Client ID to a text file.

      The Client ID is required to configure the Azure Data Lake Store target. See Configure the Azure Data Lake Store target for more information.
3. Configure the client application to access the web APIs.

   You must do the following:

   a. Give your web application permissions to access the "Windows Azure Service Management API."
   b. Assign the Windows Azure Service Management API the delegated permission "Access Azure Service Management as organization users."
   c. Create and configure a key.
   d. Save the application.

   The field is populated with the key's value, a long string of alphanumeric characters. This Client Key is required to configure the Azure Data Lake Store target.
4. Copy the Client Key to a text file.

   Note:

   You must copy the key's value before leaving the page. Once you leave the page, you will not be able to retrieve it.

Create an Azure Data Lake Store

Procedure

1. Open a web browser and navigate to the Microsoft Azure portal (https://portal.azure.com).
2. Create a Data Lake Store.
3. Select the Azure Data Lake Store.

4. Copy the Subscription ID to a text file.

   The Subscription ID is required to configure the Azure Data Lake Store target. See Configure the Azure Data Lake Store target for more information.

5. Add the web application you created in Configure the web application to access the web APIs to the Data Lake Access control (IAM) and configure its permissions to access the Azure Data Lake Store by doing the following:

   a. Assign the Contributor role to the web application.

   b. Give the application Read, Write, and Execute privileges on the root folder of the Azure Data Lake Store.

Configure Azure Event Hubs target

Complete the procedure below to configure the Azure Event Hubs target and test your connection to Azure Event Hubs.

Before you start

Create the Azure Event Hubs. The minimum permissions required is Send.

Procedure

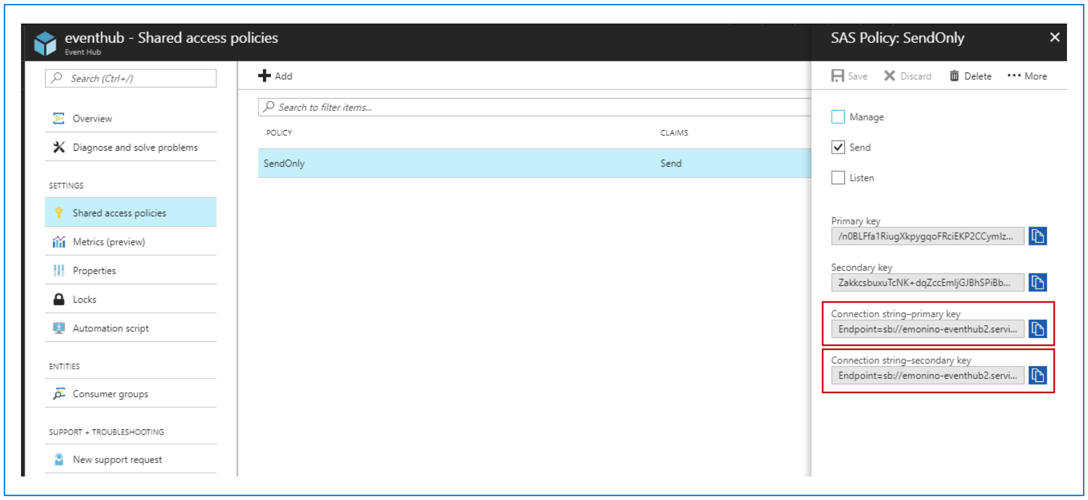
1. On the Administration page, click the **Targets** tab. Then select the target in the **Publish Targets** list.

   > **Note:**
   > If you have already selected your target, skip to the next step.

2. Configure the Azure Event Hubs with the following parameters:

Parameter	Description
`Connection string`	Connection string to the Azure Event Hubs' primary key or secondary key. Note: This connection string is to the Event Hubs, not the Event Hubs' service bus.

The following screen capture shows where to find these parameters in Microsoft Azure Portal.



□ Manage
☑ Send
□ Listen

Primary key: /n0BLFfa1RiugXkpygqoFRciEKP2CCymlz...

Secondary key: ZakkcsbuxuTcNK+dqZccEmljGJBhSPiBb...

Connection string–primary key: Endpoint=sb://emonino-eventhub2.servi...

Connection string–secondary key: Endpoint=sb://emonino-eventhub2.servi...

> **Note:**
>
> An existing Azure shared access policy for the Event Hubs that meets the minimum permissions may be used, or a new shared access policy can be created for this purpose.
>
> With subsequent portal updates, the screen may look different and the parameters may be located elsewhere.

3. Click **Verify Event Hub Writer** to verify that the Event Hubs is valid.
4. Click **Save Changes**.

After you finish

Give users access to the Azure Event Hubs target. For more information, see Grant access to targets.

Configure Azure IoT Hub target

Complete the procedure below to configure the Azure IoT Hub target and test your connection to Azure IoT Hub.

Before you start

Create the Azure IoT Hub. Create or identify the Azure IoT Hub shared access policy that PI Integrator for Business Analytics will use. If you create a device to which all PI Integrator for Business Analytics views are written by specifying the Device ID, then "Registry read" is the minimum required permission. If PI Integrator for Business Analytics automatically creates a device for each view, then "Registry write" is the minimum required permission.

> **Note:**
>
> Symmetric key is the only authentication supported in this release.

Procedure

1. On the Administration page, click the **Targets** tab. Then select the target in the **Publish Targets** list.

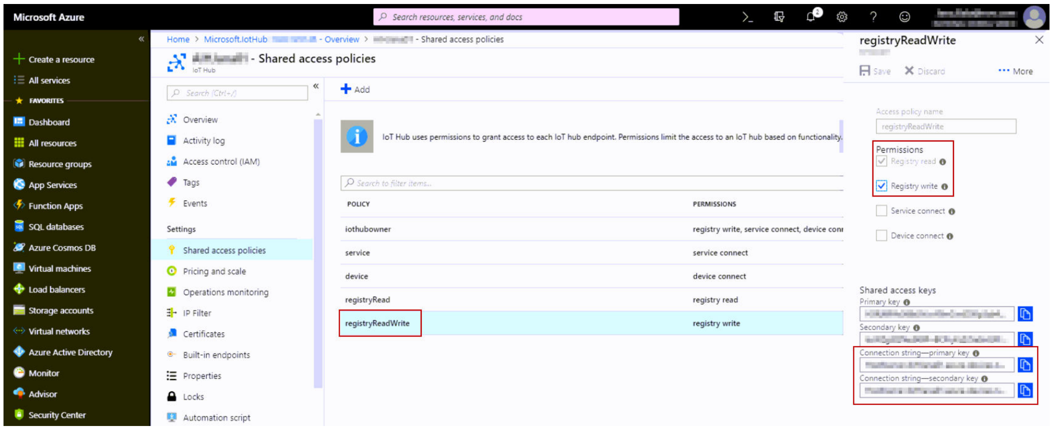
   > **Note:**
   > If you have already selected your target, skip to the next step.

2. Configure the Azure IoT Hub with the following parameters:

Parameter	Description
`Connection string`	Connection string to the IoT Hub's primary key or secondary key. **Note:** This connection string is to the IoT Hub, not to the IoT Device.

Parameter	Description
`Device ID`	(Optional) Device ID of the IoT Device or IoT Edge Device. This is the name assigned to the device. **`Device ID`** is required for IoT Edge Devices. It is optional for IoT Devices. If no name is specified, an IoT Device is created for each view.

The following screen capture shows where to find the connection string for the IoT Hub in Microsoft Azure Portal. Note that PI Integrator for Business Analytics requires the connection string from the IoT Hub **Shared access policies** (not the connection string at the device level). The policy selected on this page determines the permissions for the connection string. Therefore, select or create a policy that provides the permissions required, depending on whether Device ID is selected or not, and provide the selected policy's connection string for the PI Integrator for Business Analytics target.



[redacted] - Shared access policies

IoT Hub uses permissions to grant access to each IoT hub endpoint. Permissions limit the access to an IoT hub based on functionality.

Search to filter items...

POLICY	PERMISSIONS
iothubowner	registry write, service connect, device con
service	service connect
device	device connect
registryRead	registry read
registryReadWrite	registry write

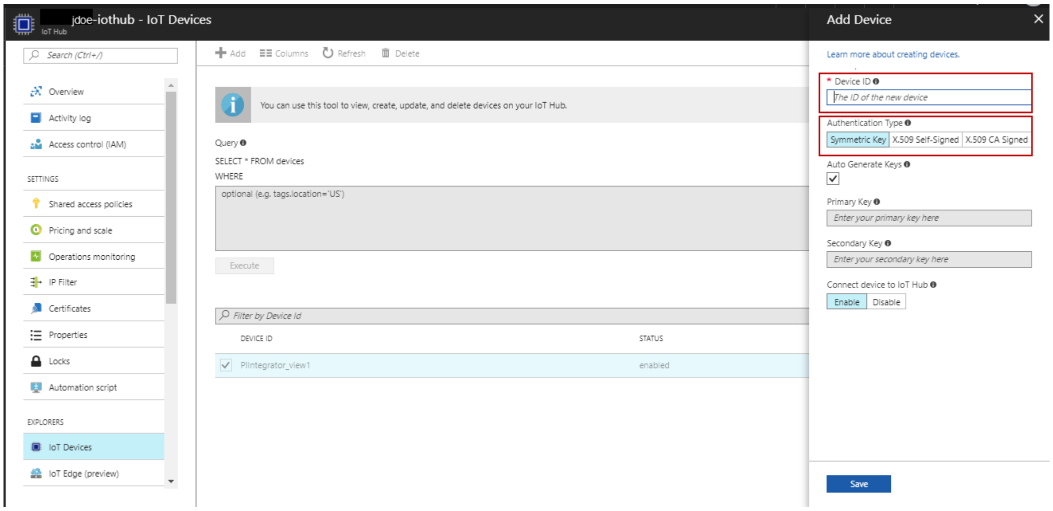
registryReadWrite

Access policy name: registryReadWrite

Permissions
☑ Registry read
☑ Registry write
☐ Service connect
☐ Device connect

Shared access keys
Primary key: [redacted]
Secondary key: [redacted]
Connection string—primary key: [redacted]
Connection string—secondary key: [redacted]

The following screen capture shows where to find the Device ID parameters and where to set the Authentication Type in Microsoft IoT Portal for the IoT Hub device.



[redacted] jdoe-iothub - IoT Devices

IoT Hub

You can use this tool to view, create, update, and delete devices on your IoT Hub.

Query
SELECT * FROM devices
WHERE
optional (e.g. tags.location='US')

Filter by Device Id

DEVICE ID	STATUS
☑ PIIntegrator_view1	enabled

Add Device

Learn more about creating devices.

* Device ID: The ID of the new device

Authentication Type: [✓ Symmetric Key] X.509 Self-Signed X.509 CA Signed

Auto Generate Keys ☑

Primary Key: Enter your primary key here

Secondary Key: Enter your secondary key here

Connect device to IoT Hub: [✓ Enable] Disable

Note:

With subsequent portal updates, the screen may look different and the parameters may be located elsewhere.

3. Click **Verify IoT Hub Writer** to verify that the IoT Hub is valid.

   If a Device ID is specified, PI Integrator for Business Analytics attempts to find the device. If no Device ID is specified, then a device is created and once the verification is completed, it is deleted.

4. Click **Save Changes**.

After you finish

Give users access to the Azure IoT Hub target. For more information, see Grant access to targets.

Set up the Azure SQL Database or Azure SQL Data Warehouse target

Complete the procedure to set up the Azure SQL Database or Azure SQL Data Warehouse target.

Procedure

1. Install the database in Azure and complete the following tasks:

   a. Set a firewall rule within Azure to grant permission to the server (where PI Integrator for Business Analytics is installed) to send requests to these targets. By default, Azure firewalls prevent access to the Azure SQL Database and Azure SQL Data Warehouse database servers. Therefore, you must explicitly grant access to the server.

   > **Tip:**
   >
   > Navigate to the Microsoft Azure portal (https://portal.azure.com) on the machine where PI Integrator for Business Analytics is installed. The client ID field identifying the clients who are being given access to the database servers will be automatically populated with the machine's IP address.

   b. Grant the user who will be connecting to Azure SQL Database or Azure SQL Data Warehouse the following minimum permissions: CONNECT, SELECT, CREATE TABLE, and ALTER.

2. Add the publish target to PI Integrator for Business Analytics. See Add a publish target.

3. Configure the publish target. Click on the appropriate topic below for your target:

   - Configure Azure SQL Database target
   - Configure Azure SQL Data Warehouse target

4. Grant users access to the publish target. See Grant access to targets.

Configure Azure SQL Database target

Complete the procedure below to configure the Azure SQL Database target and test your connection to the Azure SQL Database.

Before you start

- Create the Azure SQL Database.
- Add the Azure SQL Database as a target. For more information, see Add a publish target.

Procedure

1. On the Administration page, click the **Targets** tab. Then select the target in the **Publish Targets** list.

   > **Note:**
   > If you have already selected your target, skip to the next step.

2. Configure the Azure SQL Database target with the following parameters:

Parameter	Description
`Hostname`	Server name that hosts Azure SQL Database. The format is: *server_name*.database.windows.net.
`SQL Authentication Username`	User name used to connect to Azure SQL Database (Only specify if using SQL Server authentication).
`SQL Authentication Password`	Password used to connect to Azure SQL Database (Only specify if using SQL Server authentication).
`Use High Availability`	(Optional) Connect to a SQL server that supports high availability and failover clusters. **`Use High Availability`** turns the **`MultiSubnetFailover`** connection property on in the connection string. For more information on this property, refer to the Microsoft web site (https://msdn.microsoft.com/en-us/library/hh205662(v=vs.110).aspx).
`Database`	Name of database in Azure SQL Server in which tables are located.

3. Click **Connect**.
4. Select the database from the **Database** list.
5. Click **Save Changes**.

After you finish

Give users access to the Azure SQL Database target. For more information, see Grant access to targets.

Configure Azure SQL Data Warehouse target

Complete the procedure below to configure the Azure SQL Data Warehouse target and test your connection to the Azure SQL Data Warehouse.

Before you start

- Create the Azure SQL Data Warehouse.
- Add the Azure SQL Data Warehouse as a target. For more information, see Add a publish target.

Procedure

1. On the Administration page, click the **Targets** tab. Then select the target in the **Publish Targets** list.

   > **Note:**
   > If you have already selected your target, skip to the next step.

2. Configure the Azure SQL Data Warehouse target with the following parameters:

Parameter	Description
`Hostname`	Server name that hosts Azure SQL Database. The format is: *server_name*.database.windows.net.
`SQL Authentication Username`	User name used to connect to Azure SQL Data Warehouse (Only specify if using SQL Server authentication).
`SQL Authentication Password`	Password used to connect to Azure SQL Data Warehouse (Only specify if using SQL Server authentication).
`Use High Availability`	(Optional)Connect to a SQL server that supports high availability and failover clusters. **`Use High Availability`** turns the **`MultiSubnetFailover`** connection property on in the connection string. For more information on this property, refer to the Microsoft web site (https://msdn.microsoft.com/en-us/library/hh205662(v=vs.110).aspx).
`Database`	Name of database in Azure SQL Data Warehouse in which tables are located.

3. Click **Connect**.
4. Select the database from the **Database** list.
5. Click **Save Changes**.

After you finish

Give users access to the Azure SQL Data Warehouse target. For more information, see Grant access to targets.

Configure Hadoop Distributed File System (HDFS) targets

Complete the procedure below to configure the Hadoop Distributed File System target and verify that the HDFS writer is working.

Before you start

Create the Hadoop Distributed File System target before you configure it. For more information, see Add a publish target.

Procedure

1. On the Administration page, click the **Targets** tab. Then select the target in the **Publish Targets** list.

Note:
If you have already selected your target, skip to the next step.

2. Configure the Hadoop Distributed File System target with the following parameters:

Parameter	Description
`HDFS URL`	URL to access HDFS through WebHDFS directly, or through the Apache Knox gateway or HttpFS. Examples: ◦ HDFS – http://host:50070/webhdfs/v1 ◦ HttpFS – http://host:14000/webhdfs/v1 ◦ Apache Knox – https://host:8443/gateway/default/webhdfs/v1
`Verify SSL Certificate`	Select the check box if you are using an SSL certificate. Clear the check box if you are using a self-signed certificate.
`Username`	User name used to connect to HDFS. The user must have permissions to read and write to HDFS.
`Password`	(Optional) Password to authenticate user. It is used when connecting to Apache Knox or when connecting to HttpFS if security is enabled. If a password is provided, then Hadoop HTTP authentication is used. If no password is entered, then PI Integrator for Business Analytics uses Hadoop simple authentication.
`Directory`	Directory where the data files are created. Click **Browse** to navigate to the directory where you want the files located.
`Append Timestamp`	When selected, a time stamp of when the view is published is appended to the file name and a new file is created each time the view is published. If not selected, then the data is appended to the existing file.
`Include Header`	When selected, column names are added to the beginning of the file.

3. Click **Verify HDFS Writer** to verify that the HDFS writer can connect to and write to HDFS.

Note:

If you are unable to successfully write to the HDFS, refer to Tips for setting up Hadoop Distributed File System (HDFS).

4. Click **Save Changes**.

After you finish

Give users access to the Hadoop Distributed File System target. For more information, see Grant access to targets.

Tips for setting up Hadoop Distributed File System (HDFS)

In order for HDFS to work with PI Integrator for Business Analytics, complete the following tasks:

- Create the HDFS user.
- Create the user directory and grant permissions.

The following procedure describes how to complete these tasks.

Procedure

1. Create the HDFS user.
   a. Create the HDFS user on the node where WebHDFS is installed.
   b. Add the HDFS user to a group.

   Note:

   The HDFS user can be added to any group. However, for the purposes of this example, this group will be referred to as the HDFS group.

2. Create the directory and grant permissions.
   a. Create a directory on HDFS.
   b. Change the owner of this directory to the HDFS user.
   c. Change the group to which this directory belongs to HDFS.
   d. Grant Read and Write permissions to the owner of the directory (that is, to the HDFS user).
   e. Grant Read and Write permissions to the group that the directory belongs to.

Configure Microsoft SQL Server targets

Complete the procedure below to configure the Microsoft SQL Server target and test your connection to the SQL database.

Before you start

Create the Microsoft SQL Server target before you configure it. For more information, see Add a publish target.

Note:

Ensure that the service account that runs PI Integrator Framework service (or the SQL user if you are using SQL authentication) has the following permissions on the Microsoft SQL Server:

- Server level – CONNECT SQL, VIEW ANY DATABASE
- Database level – CONNECT, CREATE TABLE
- dbo SCHEMA – SELECT, ALTER, INSERT

Procedure

1. On the Administration page, click the **Targets** tab. Then select the target in the **Publish Targets** list.

Note:
If you have already selected your target, skip to the next step.

2. Configure the Microsoft SQL Server target with the following parameters:

Parameter	Description
`Hostname`	Host name and instance (`Hostname\Instance`) of the machine on which SQL Server is running
`SQL Authentication Username`	User name used to connect to SQL Server (Only specify if using SQL Server authentication. If using Windows integrated security, the PI Integrator for Business Analytics service account is used.)
`SQL Authentication Password`	Password used to connect to SQL Server (Only specify if using SQL Server authentication. If using Windows integrated security, the PI Integrator for Business Analytics service account is used.)
`Use High Availability`	(Optional) Connect to a SQL Server that supports high availability and failover clusters. **Use High Availability** turns on the `MultiSubnetFailover` connection property on in the connection string. For more information on this property, refer to the Microsoft web site (https://msdn.microsoft.com/en-us/library/hh205662(v=vs.110).aspx).
`Database`	Name of database in SQL Server in which tables are located

3. Click **Connect** to verify that you can connect to the SQL database.

4. Click **Save Changes**.

After you finish

Give users access to the Microsoft SQL Server target. For more information, see Grant access to targets.

Install driver for the PI View target

Note:
This is an optional step. The PI ODBC driver is only required if you are publishing to a PI View.

The PI ODBC driver on the client serves as the point of contact, requesting and sending PI Views on behalf of the client through interaction with the PI SQL Data Access Server (PI SQL DAS) on the server. It must be installed on every client machine that makes requests for PI View data.

In this procedure, you install the PI ODBC driver and specify PI Views as the data source.

Procedure

1. Download the PI ODBC driver from the OSIsoft Tech Support Downloads page (https://techsupport.osisoft.com/Downloads/All-Downloads/) and install the PI ODBC driver and tools on the machine.

2. Run the `odbcad32.exe` file.

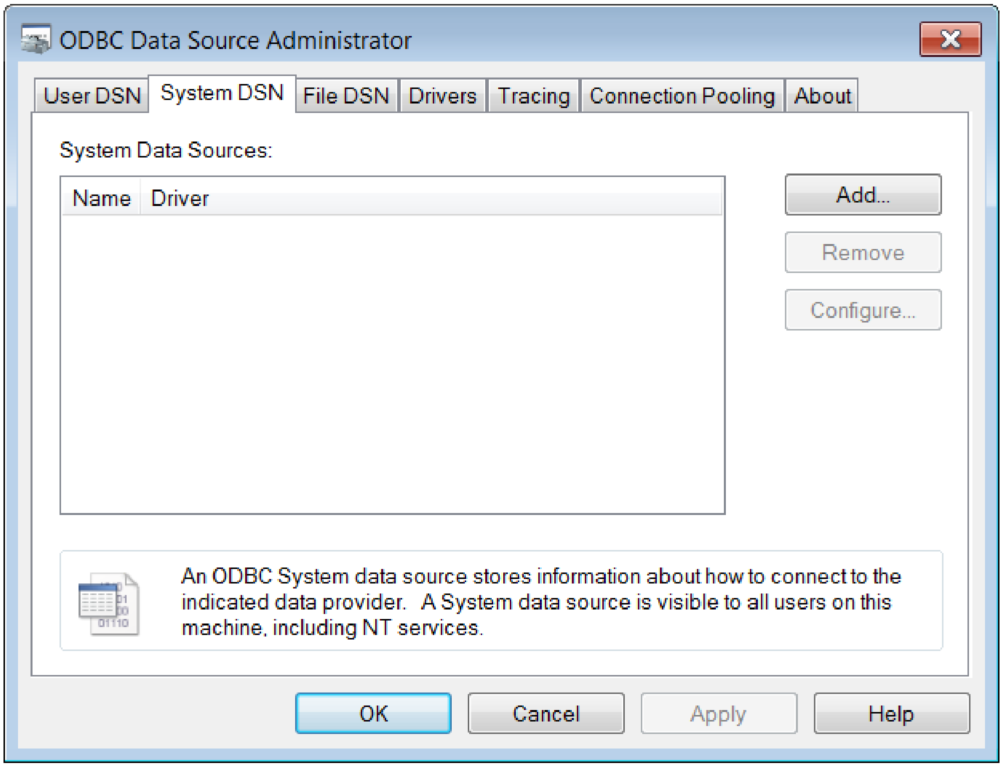
Note:
There two versions of `odbcad32.exe`, one that loads the 32-bit version of the ODBC driver and another that loads the 64-bit version. The files to load the ODBC drivers can be found in the following locations:

- 32-bit version – `windows_directory\SysWOW64\odbcad32.exe`
- 64-bit version – `windows_directory\system32\odbcad32.exe`

Run the file that is compatible with your client application.

The ODBC Data Source Administrator window opens.

3. Click the **System DSN** tab.



ODBC Data Source Administrator

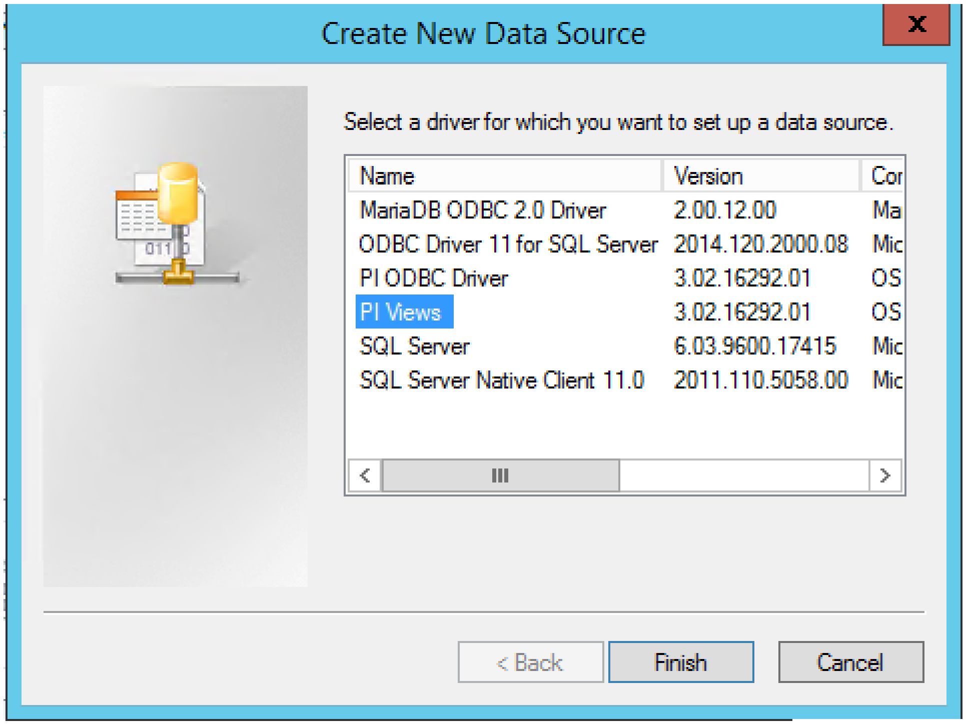
System Data Sources:

Name	Driver

An ODBC System data source stores information about how to connect to the indicated data provider. A System data source is visible to all users on this machine, including NT services.

4. Click **Add** to configure a new data source for the ODBC driver.

The Create New Data Source window opens.

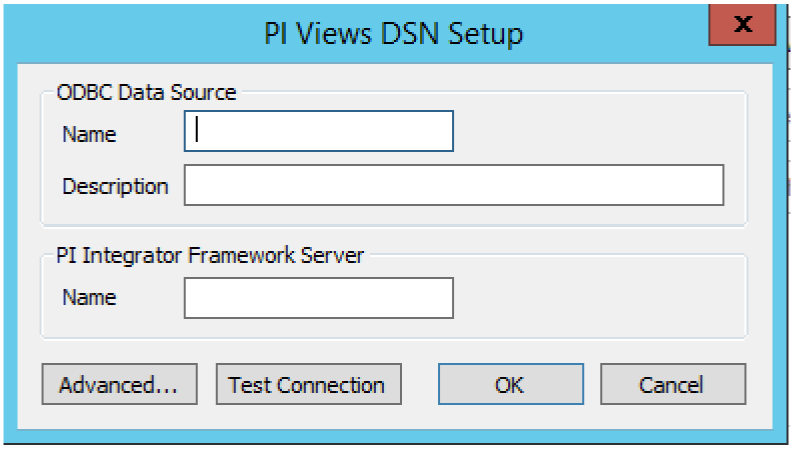


Select a driver for which you want to set up a data source.

Name	Version	Cor
MariaDB ODBC 2.0 Driver	2.00.12.00	Ma
ODBC Driver 11 for SQL Server	2014.120.2000.08	Mic
PI ODBC Driver	3.02.16292.01	OS
PI Views	3.02.16292.01	OS
SQL Server	6.03.9600.17415	Mic
SQL Server Native Client 11.0	2011.110.5058.00	Mic

5. Select **PI Views** as the driver.
6. Click **Finish.**

   The PI Views DSN Setup window opens.



7. In the ODBC Data Source pane, enter a name for the data source in the **Name** field and a brief description in the **Description** field.
8. In the PI Integrator Framework Server pane, enter the name of the machine hosting PI Integrator for Business Analytics in the **Name** field.
9. Click **Test Connection** to validate the host name.
10. Click **OK**.

PI ODBC on the client is ready for PI Integrator for Business Analytics.

11. Validate the successful installation and configuration of the PI ODBC driver by opening **PI SQL Commander Lite** (or another SQL Query application) and verify that the host name appears in the ODBC Data Sources panel.

After you finish

Give users read access to the PI AF configuration database that is specified for PI Integrator for Business Analytics. This is required to enable users to view the PI View data.

Set up the Oracle Database publish target

Complete the procedure to set up the Oracle Database publish target.

Procedure

1. Install the Oracle Database Access Components. For more information, see Install Oracle Database Access Components.
2. Add the publish target to PI Integrator for Business Analytics. See Add a publish target.
3. Configure the Oracle Database publish target. For more information, see Configure Oracle targets.
4. Give the service account running the PI Integrator Framework service the following minimum Oracle permissions:
   - System privileges – CREATE SESSION and CREATE TABLE
   - Tablespace privileges – Sufficient quota to create tables
5. Grant users access to the publish target. See Grant access to targets.

Install Oracle Database Access Components

> **Note:**
> This is an optional step. Oracle Database Access Components (ODAC) is only required if you are publishing to the Oracle Database.

Complete this procedure before you add and configure the Oracle database as a publish target.

Procedure

1. Install the Oracle Database Access Components software on the computer where PI Integrator for Business Analytics is installed.

   > **Note:**
   > Check System requirements for the specific version of the ODAC software to install.

2. Locate the `tnsnames.ora` file in `\`*`ODAC_install_directory`*`\Network\Admin\Sample`.
3. Edit the `tnsnames.ora` file and add an entry for the Oracle database.

   The syntax is as follows:

```
Net_Service_Name =
    (DESCRIPTION=
        (ADDRESS=(PROTOCOL=protocol_name)(HOST=Oracle_database_host_name)
(PORT=port)
        (CONNECT_DATA=
            (SERVER=service_handler_type)
            (SERVICE_NAME=(TNS_listener_service_name)
```

The *Net_Service_Name* is the alias for the SERVICE_NAME. When you configure the Oracle publish target, you can set the **Data Source** parameter to the *Net_Service_Name*. For more information on the tnsnames.ora file, refer to your Oracle documentation.

4. Move the tnsnames.ora file to the \ODAC_install_directory\Network\Admin directory.
5. Add the location of the ODAC software to the **PATH** environment variable.
6. Create the **TNS_ADMIN** system environment variable and point it to the directory where the tnsnames.ora file is located.

After you finish

Continue with adding the Oracle database as a publish target. For more information, see Add a publish target.

Configure Oracle targets

Complete the procedure below to configure the Oracle target and test your connection to the Oracle database.

Before you start

- Install Oracle Database Access Components.

  See Install Oracle Database Access Components.
- Create the Oracle target. For more information, see Add a publish target.

Procedure

1. On the Administration page, click the **Targets** tab. Then select the target in the **Publish Targets** list.

   Note:
   If you have already selected your target, skip to the next step.
2. Configure the Oracle target with the following parameters:

Parameter	Description
Data Source	Oracle Net Services name, connect descriptor, or alias that identifies the Oracle database **Note:** See Install Oracle Database Access Components for information on how the Oracle Net Services name is specified.
Username	User name used to connect to the Oracle database
Password	Password used to connect to the Oracle database

3. Click **Connect** to verify that you can connect to the database.
4. Click **Save Changes**.

After you finish

Give users access to the Oracle target. For more information, see Grant access to targets.

Configure text file targets

Complete the procedure below to configure the text file target.

Before you start

Create the text file target before you configure it. For more information, see Add a publish target.

Procedure

1. On the Administration page, click the **Targets** tab. Then select the target in the **Publish Targets** list.

   Note:
   If you have already selected your target, skip to the next step.

2. Configure the text file target with the following parameters:

Parameter	Description
`Directory`	Directory where the text file is created.
`Append Timestamp`	When selected, a time stamp of when the view is published is appended to the file name and a new file is created each time the view is published. If not selected, then the data is appended to the existing file.
`Include Header`	When selected, column names are added to the beginning of the text file.
`Field Delimiter`	Character(s) that separate the data values in the output file. The default is a tabbed space. To choose a tab delimiter, either leave the field blank or enter `\t`. **Note:** Do not use a character that appears in your data, for example, a period. The period in your data will be removed before being written to the file.
`File Extension`	File extension of output files. The default is `.txt`. **Note:** The file format does not change if you change the extension.

3. Click **Save Changes**.

After you finish

Give users access to the text file target. For more information, see Grant access to targets.

Grant access to targets

The following procedure describes how to give users permission to publish their data to a publish target.

Note:
In addition to granting identities access to publish targets, identities must also be given access to the views to be published. Identities are added on the **Users** tab of the Administration page. For more information, see Add and configure identities.

Procedure

1. Click the menu icon ☰ and click **Administration.**
2. Click the **Targets** tab.
3. Click the target in the **Publish Targets** list.
4. To grant access to the selected publish target, click **Add Identity** in the **Target Access** pane.
5. Select the identity and click **Ok.**
6. Click **Save Changes**.

Start PI Integrator for Business Analytics

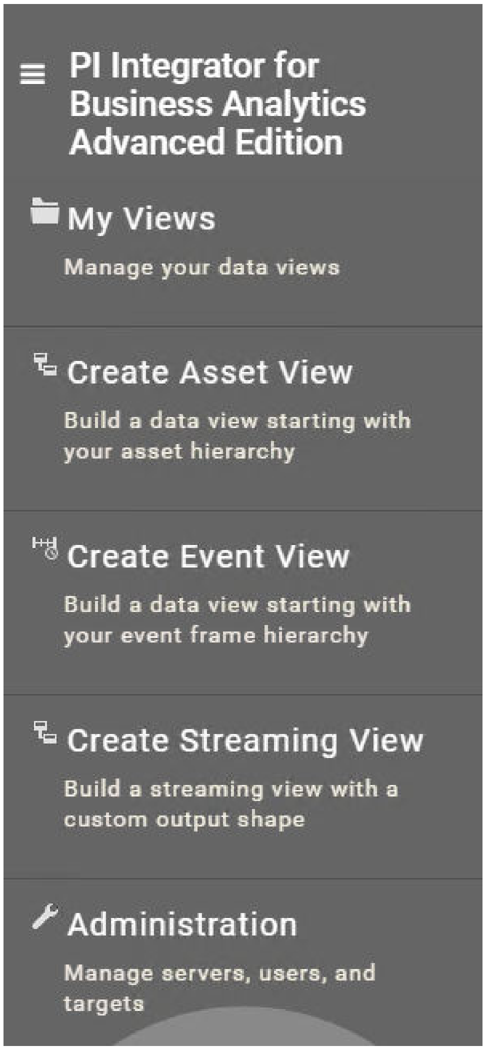
Procedure

1. Open a web browser.
2. Enter the URL for the PI Integrator for Business Analytics application.

   > **Note:**
   > Check with your system administrator for the URL.

   The application opens to the My Views page.
3. Click the menu icon ☰ to open the PI Integrator for Business Analytics menu.

   The following menu opens:

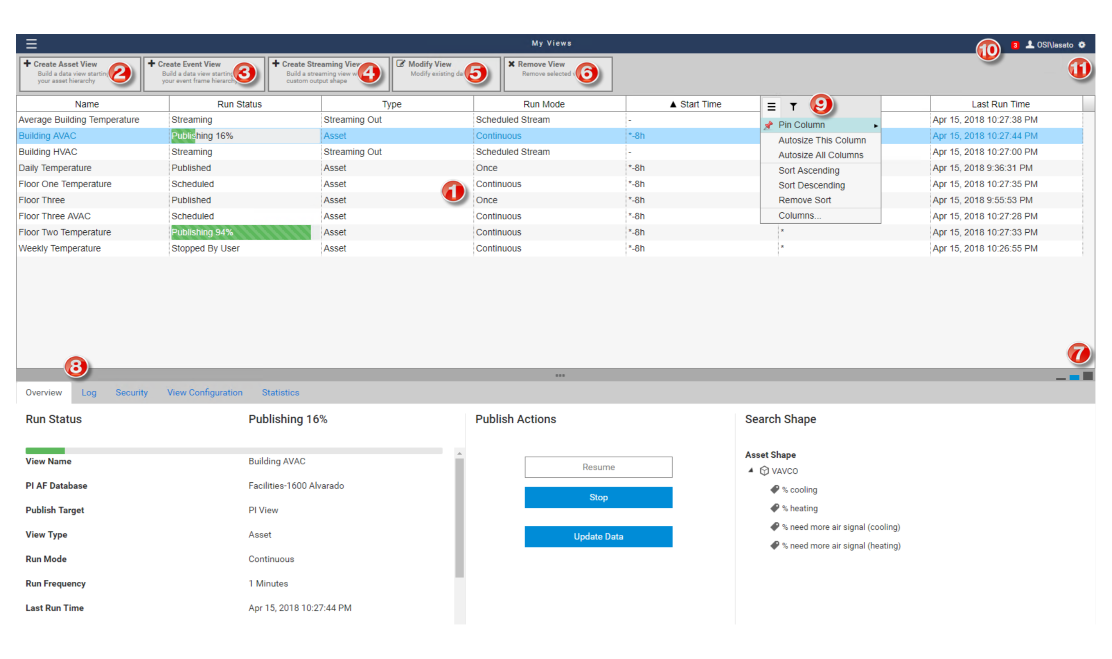

PI Integrator for Business Analytics Advanced Edition
My Views
Manage your data views
Create Asset View
Build a data view starting with your asset hierarchy
Create Event View
Build a data view starting with your event frame hierarchy
Create Streaming View
Build a streaming view with a custom output shape
Administration
Manage servers, users, and targets

You can open this menu from any place in the application and do the following:

- Navigate to the My Views page – For more information about the My Views page, see The My Views page.
- Create an asset view – For more information on creating asset views, see Create an asset view.
- Create an event view – For more information on creating event views, see Create an event view.
- Create a streaming view – For more information on creating streaming views, see Create a streaming view. This feature is available with the PI Integrator for Business Analytics Advanced Edition.
- Navigate to the Administration page – For more information on the tasks you can perform from this page, see Administration tasks.

The My Views page

When you enter the URL for PI Integrator for Business Analytics, the application opens to the My Views page. From this page, you create and edit asset views, event views, and streaming views. This page also displays the list of views to which you have access. The screen shot and table below describe the information available about your view and how to use this page.



Name	Run Status	Type	Run Mode	▲ Start Time		Last Run Time
Average Building Temperature	Streaming	Streaming Out	Scheduled Stream	-		Apr 15, 2018 10:27:38 PM
Building AVAC	Publishing 16%	Asset	Continuous	*-8h		Apr 15, 2018 10:27:44 PM
Building HVAC	Streaming	Streaming Out	Scheduled Stream	-		Apr 15, 2018 10:27:00 PM
Daily Temperature	Published	Asset	Once	*-8h		Apr 15, 2018 9:36:31 PM
Floor One Temperature	Scheduled	Asset	Continuous	*-8h		Apr 15, 2018 10:27:35 PM
Floor Three	Published	Asset	Once	*-8h		Apr 15, 2018 9:55:53 PM
Floor Three AVAC	Scheduled	Asset	Continuous	*-8h		Apr 15, 2018 10:27:28 PM
Floor Two Temperature	Publishing 94%	Asset	Continuous	*-8h	*	Apr 15, 2018 10:27:33 PM
Weekly Temperature	Stopped By User	Asset	Continuous	*-8h	*	Apr 15, 2018 10:26:55 PM

Run Status Publishing 16%

View Name	Building AVAC
PI AF Database	Facilities-1600 Alvarado
Publish Target	PI View
View Type	Asset
Run Mode	Continuous
Run Frequency	1 Minutes
Last Run Time	Apr 15, 2018 10:27:44 PM

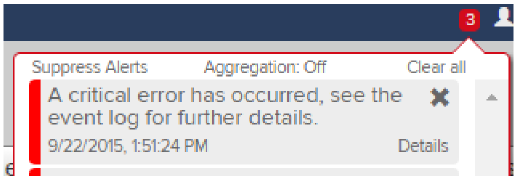
Publish Actions

Search Shape

Asset Shape

- VAVCO
  - % cooling
  - % heating
  - % need more air signal (cooling)
  - % need more air signal (heating)

Number	Description
1	All the views to which you have access are listed in the table. You can only edit views for which you have write access permissions. You can make a copy of a view for which you have read access permissions and then edit the copy.
2	Use **Create Asset View** to create an asset view. For more information, see Create an asset view.
3	Use **Create Event View** to create an event view. For more information, see Create an event view.
4	Use **Create Streaming View** to create a streaming view. For more information, see Create a streaming view. This feature is available with the PI Integrator for Business Analytics Advanced Edition.
5	To modify a view, select the view in the table and click **Modify View**.
6	To delete a view, select the view in the table and click **Remove View**. Deleting a view removes the view's name from the list of reserved view names. Note, deleting a view does not free up the available output streams allowed with your license until 7 days have passed. For more information, see Recovering output streams.
7	Click on the bars to open and close the details panel with the **Overview**, **Log**, **Security**, **View Configuration**, and **Statistics** tabs.

Number	Description
8	For the selected view, the **Overview**, **Log**, **Security**, **View Configuration**, and **Statistics** tabs provide the following details about that view: • **Overview** indicates whether the view has been published. This tab also summarizes information about the view, such the PI AF database it uses, when the view was last run, and the shape that it uses. If the view is currently being published, the run status bar indicates progress and you have the option to stop the publishing process. • **Log** displays information for the selected view. You can adjust the start and end times, and you can filter the messages to display those of a certain severity, for example, critical errors. • **Security** shows who has access to the view, and if you have sufficient privileges, allows you to change the level of access. • **View Configuration** gives you a quick overview of your views, including the elements and attributes in the view, details about the elements and attributes and any row filters. • **Statistics** displays statistics for the selected view. For more information, see View statistics data.
9	Place your cursor in the column heading to enable the menu icon ≡ and click it to open the menu. From this menu, you can resize the columns, sort the data in the column, and add or delete columns from the table.
10	The red message counter icon at the top right displays the number of warning and error messages recorded by PI Integrator for Business Analytics. Click the icon to open the message list. Click the commands at the top of the message list. **Suppress Alerts**/**Unsuppress Alerts** turns alerts off and on. **Aggregation Off**/**Aggregation On** controls how multiple occurrences of a message are reported. **Aggregation Off** reports each occurrence of a message. **Aggregation On** displays the message once and reports the number of occurrences. **Clear all** deletes all messages from the list.  3 Suppress Alerts Aggregation: Off Clear all Details A critical error has occurred, see the event log for further details. 9/22/2015, 1:51:24 PM
11	Click the gear icon ⚙ at the top right to see the version of PI Integrator for Business Analytics and PI AF server and to change the language and locale settings.

How to use PI Integrator for Business Analytics

PI Integrator for Business Analytics provides an easy-to-use, web user interface. The main features include creating asset views, event views and streaming views; and modifying, copying, and securing your views.

PI Integrator for Business Analytics views

A view is a modeled description of the PI System data you want to analyze. There are several types of views: asset views, event views, and streaming views. The question you are addressing will determine which type of view is best suited to address your use case. The following is an example of how you can use each type of view to answer different questions about your organization.

- **Asset views** organize data around your assets and allow you to make comparisons between assets.

  For example, let's say you want to analyze a set of wind turbines by megawatt output and see the results by turbine model and manufacturer. You could create an asset view based on a turbine element template with megawatt output, model, and manufacturer attributes. This would allow you to compare the performance across your fleet of wind turbines.

- **Event views** organize data around event frames and allow you to detect patterns in the event frames.

  > **Note:**
  >
  > PI Integrator for Business Analytics only returns closed event frames (with a valid start and end time). It cannot publish open event frame data.

  Using the same example above, let's say you now want to look at the downtime of the wind turbines. You could create an event view that compares the duration of downtimes and include the model and manufacturer attributes to see if there is a pattern to the downtime event frames.

- **Streaming views** organize data around your assets and allow you to make this data available in near real time for predictive analytics.

  Continuing with the example above, assume you want to predict the power output from each wind turbine for the upcoming hour based on current data. You could create a streaming view that includes wind speed, air density, and current turbine megawatt output and use this data to train an analytics model predicting the power output based on these inputs.

What is a shape?

Views are constructed using a **shape**, a pattern for searching for data within the PI System. The shape definition provides the following information which is critical to creating the view:

- what data to include
- how the data are structured in the view

Shapes provide the unique ability to search for relationships between elements and attributes as well as the elements and attributes themselves. With PI Integrator for Business Analytics you can define parents, children, and their relationship as part of the shape, as well as the more traditional template, name, and category search parameters. You can also extend the shape to find matches for assets or event frames derived from the same template.

Each shape corresponds to a respective view:

- Asset shapes contain the assets, attributes, and their relationships in asset views.
- Streaming and asset shapes are created in the same way. The views differ in the Message Designer: asset views are presented in a tabular format and streaming views are presented in attribute-value pairs format.
- Event shapes contain event frames, event frame attributes, referenced elements, and referenced element attributes in event views.

Overview of how to use PI Integrator for Business Analytics

This outline describes how to use PI Integrator for Business Analytics to produce decision-ready data for your BI tool.

Tip:
If you are using PI Integrator for Business Analytics for the first time, OSIsoft recommends you start by exploring how to create an asset view and then move on to creating streaming or event views.

1. Select the PI System data to include in your analysis.

   Determine whether your analysis requires an asset view, event view, or streaming view. If you want to analyze your data broken down by assets, create an asset view. If you want to analyze your data by event frames, create an event view. If you want to analyze your data broken down by assets and you need values streamed for real-time analytics or some other analysis, create a streaming view.

   - Asset View – Start by creating a simple shape, for example, to find a single asset. The Matches pane is a preview of the elements that are found in the PI AF database that match your shape.
   - Event View – Start by creating a simple event shape, for example, to focus on a single event frame and one element referenced by the event frame. Add element attributes that can provide more context for the event data to the asset shape. The Matches pane keeps track of the assets, attributes, and event frames that match the shape.
   - Streaming View – Start by creating a simple shape, for example, to find a single asset. The Matches pane is a preview of the elements that are found in the PI AF database that match your shape.

2. Preview your data set.

   The preview shows a subset of the information. It is built from the first ten matches and uses the first 100 records for each match. Therefore, you may not see all the data you expect. The purpose of the preview is to give you an idea of what the data looks like so that you can determine what additional data to include to provide context or how to exclude rows and focus on the data you are interested in.

3. (Streaming views only) Specify the schema used to send the messages and how the message is triggered.
4. Refine your data set.

   There is a lot of flexibility in how the final data set can be manipulated to produce the desired results. You can do the following:

   - Modify how the data columns/data fields are displayed
   - Add data columns/data fields
   - Add time columns/time fields
   - Add calculations on a column or field
   - Filter the data to only include the data you are interested in
   - Specify how the data is retrieved (summarized, interpolated, or exact values)

   Note:

   Columns applies to asset and event views and *fields* applies to streaming views.

5. Publish the data to a publish target.

   Data can be published once or published on a schedule.

6. View your data in your preferred BI tool.

For more detailed procedures start with one of the following:

- Create an asset view
- Create an event view
- Create a streaming view

Create an asset view

If you want to analyze your data broken down by assets, create an asset view. If you want to analyze your data by event frames, see Create an event view. If you want to analyze your data broken down by assets and you need values streamed for real-time analytics or some other analysis, see Create a streaming view.

Procedure

1. Click the menu icon ☰ and click **Create Asset View**.
2. Enter a name for the view.

   Note:
   Observe the naming conventions of the target to which this view will be published. For more information, see View names and destination endpoints.

3. If your user account is assigned to multiple PI AF identities with access to PI Integrator for Business Analytics, then click **Access Permissions** and select the identity to which you want to give view access.

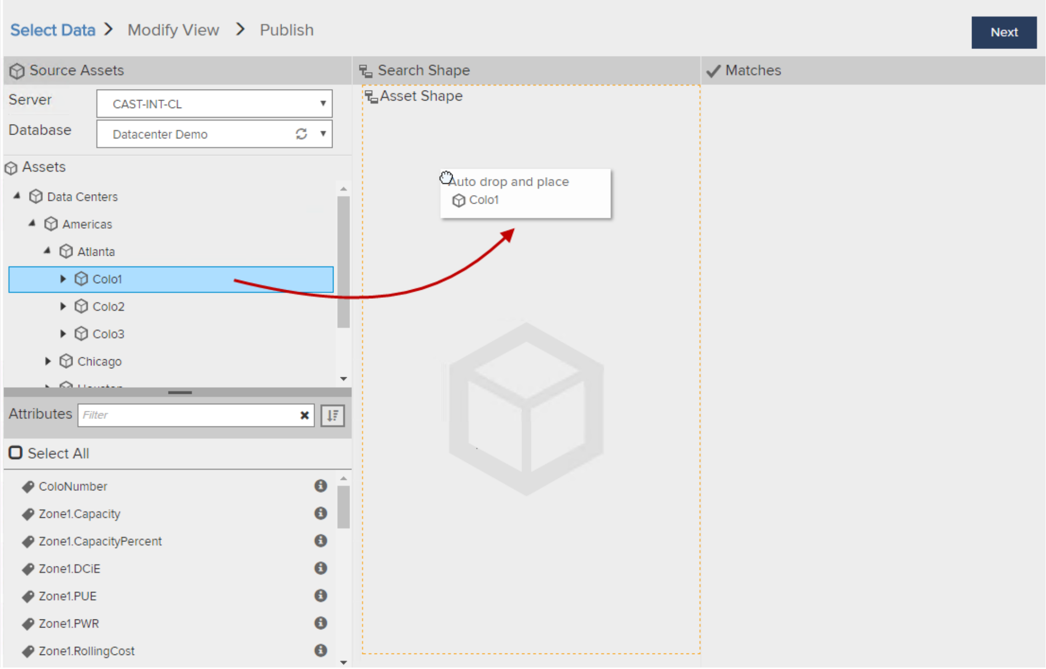
   If only one PI AF identity has been granted access to PI Integrator for Business Analytics, this identity is automatically assigned to the view.

When you first create a view, you can only grant access to one PI AF identity. You can later grant access to additional PI AF identities. For more information, see Secure your views.

4. Click **Create View.**
5. In the Source Assets pane, click **Create a New Shape.**

> **Tip:**
> You can use the shape of an existing view by clicking **Import a Shape from Another View.**

6. Use the **Server** and **Database** fields to browse to the desired PI AF server and database.
7. Drill down the PI AF tree to find the asset you want to analyze.
8. Drag the asset onto the Asset Shape pane.



Server: CAST-INT-CL
Database: Datacenter Demo

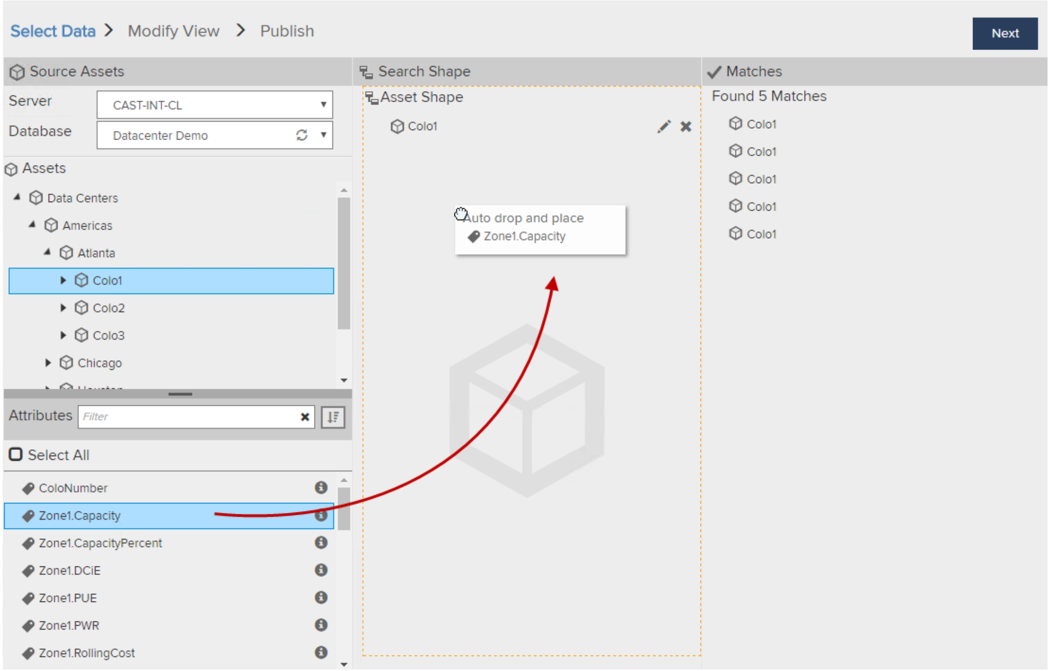
Dragging an asset onto the Asset Shape pane

The asset is added to the Asset Shape tree.

When you select an asset, the Attributes pane opens displaying the selected element's attributes.

9. Drag any attributes to include in your shape.

> **Note:**
> You can sort the attributes, group them by category, or filter which attributes are displayed to more easily find the ones you want.



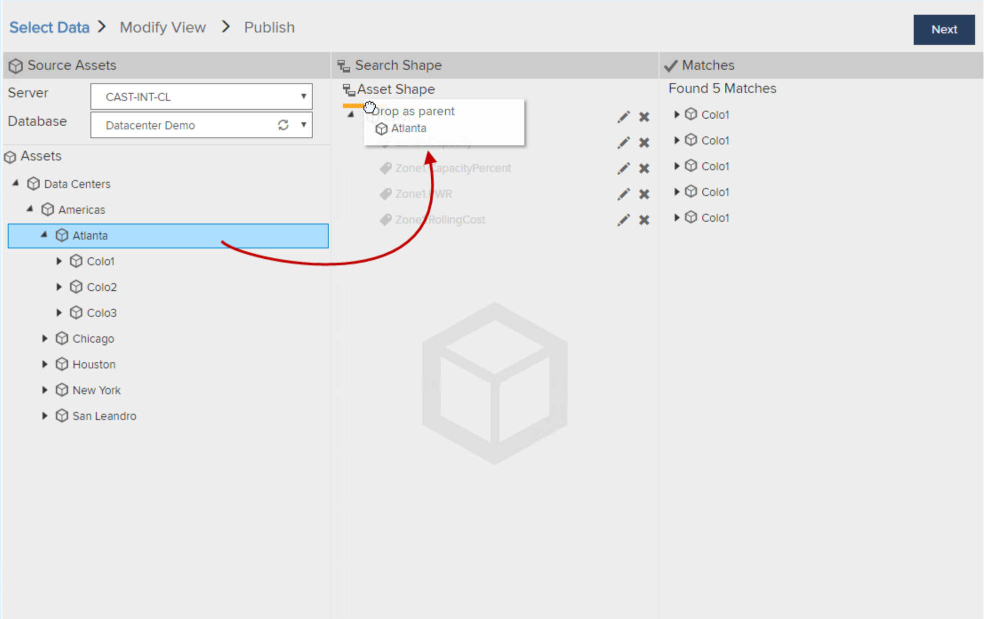
Adding an element using Auto drop and place

Tip:

If you drag an object *outside* the Asset Shape tree, a tool tip is displayed with the text **Auto drop and place.** The element is automatically added to the tree in a logical location. This element maintains the same relationship in the Asset Shape tree that it has in the PI AF tree. If there is no location that makes sense, the drop is rejected.

Tip:

You can also place the object in the Asset Shape tree. A tool tip is displayed that guides you to add the asset as a parent, child, or sibling entity. It will not prevent you from dropping an object in a location that does not match the PI AF hierarchy.



Server CAST-INT-CL

Database Datacenter Demo

Placing an element in the Asset Shape tree

10. Drag any additional assets and attributes onto the Asset Shape pane.

    The Matches pane displays the elements that match the defined shape.

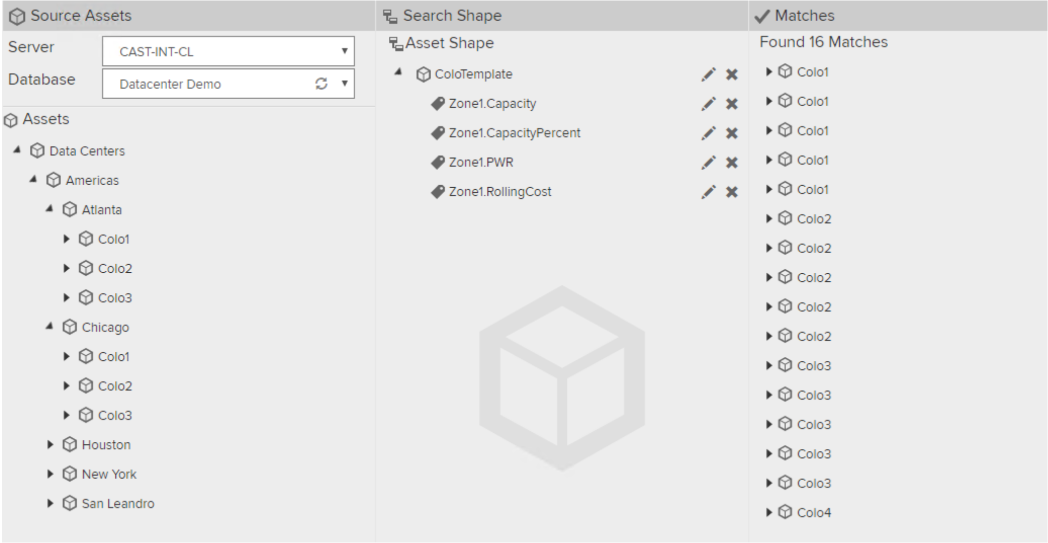
11. To see the data for all assets that share the same PI AF template:

    a. Click the icon ✎ next to the asset to open the Edit Filters dialog box.

    b. Clear the **Asset Name** check box.

    c. Select the **Asset Template** check box and click **Save.**

    The Matches pane displays data from all assets that share this template.



Source Assets

Server: CAST-INT-CL

Database: Datacenter Demo

Assets
- Data Centers
  - Americas
    - Atlanta
      - Colo1
      - Colo2
      - Colo3
    - Chicago
      - Colo1
      - Colo2
      - Colo3
    - Houston
    - New York
    - San Leandro

Search Shape

Asset Shape
- ColoTemplate
  - Zone1.Capacity
  - Zone1.CapacityPercent
  - Zone1.PWR
  - Zone1.RollingCost

Matches

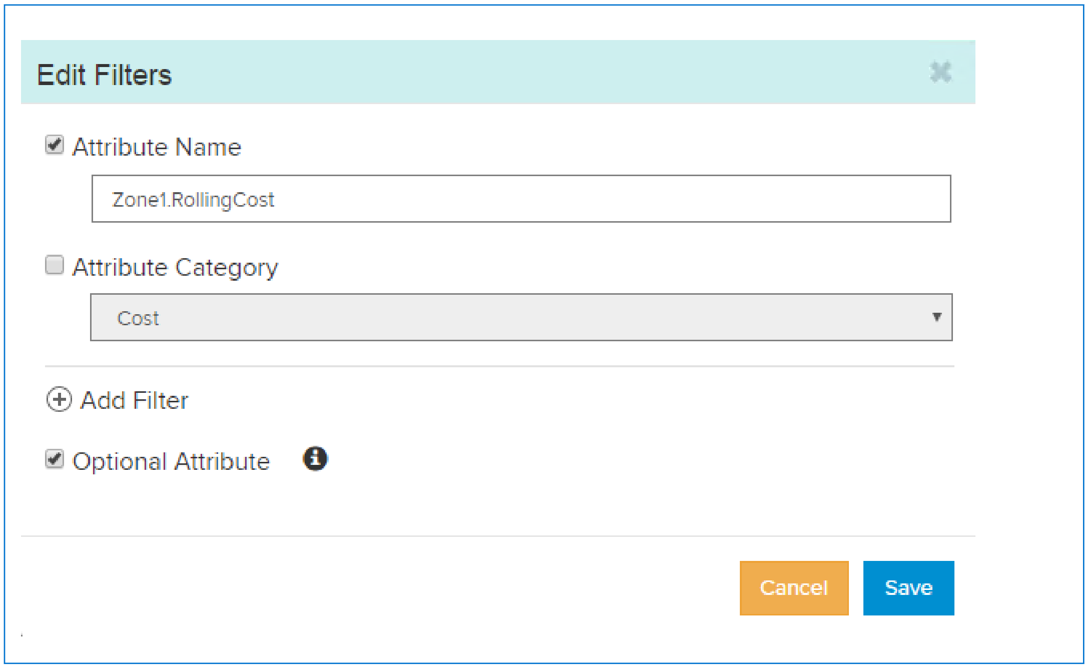
Found 16 Matches
- Colo1
- Colo1
- Colo1
- Colo1
- Colo1
- Colo2
- Colo2
- Colo2
- Colo2
- Colo2
- Colo3
- Colo3
- Colo3
- Colo3
- Colo3
- Colo4

12. To find matches for similar assets that have a different set of attributes:

    a. Click the icon ✏ next to the attribute that is not required.

    b. In the Edit Filters dialog box, select the **Optional Attribute** check box, then click **Save**.

    For example, you might use the **Optional Attribute** option if you acquired equipment over a period of time and some of the attributes differ between the older and newer equipment.



Edit Filters

☑ Attribute Name

Zone1.RollingCost

☐ Attribute Category

Cost

Add Filter

☑ Optional Attribute

13. Click **Next** to preview a subset of your data.

    The first 100 rows for the first 10 matches from the PI AF database are displayed.

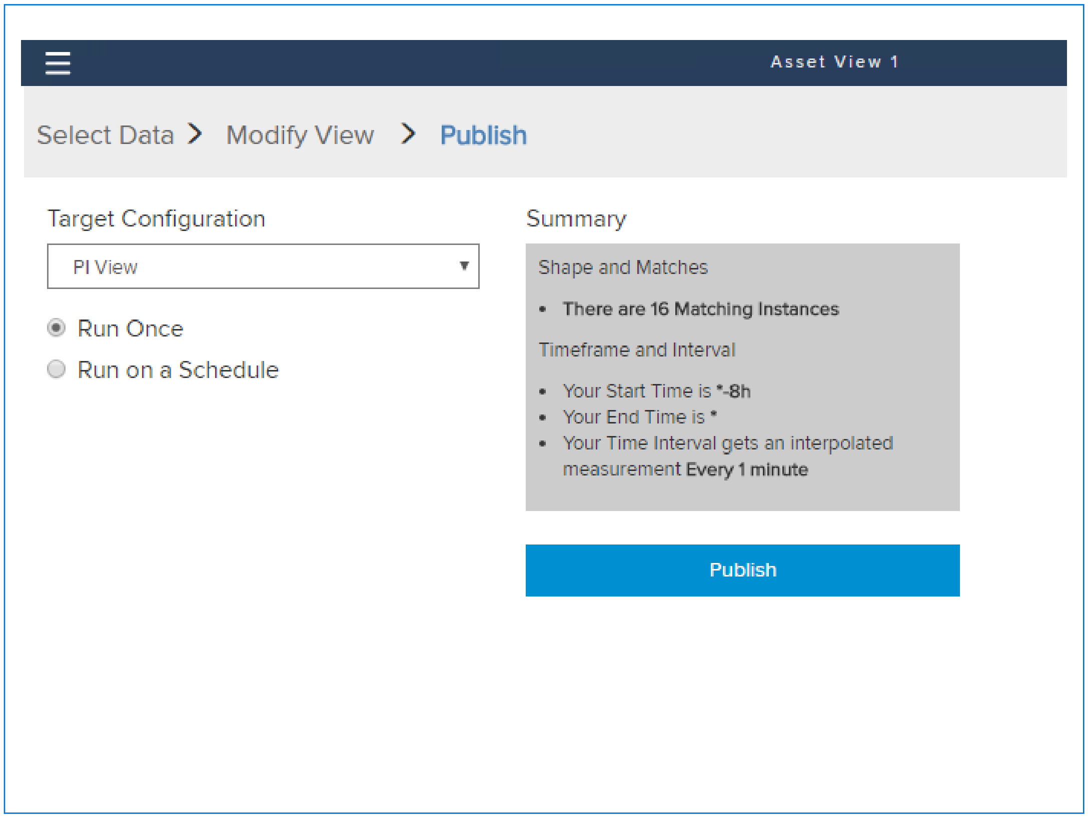
14. To refine the results, you can add more data, modify columns, filter the data, or change how values are retrieved.

    For more information, see Modify the data in your asset and event views.

Note:

Because PI Integrator for Business Analytics only displays the first 100 rows for the first 10 matches of your shape, you could set your filters in a way that excludes this data. In this situation, no data will appear on the page even though your configured view results in matches.

15. Click **Next.**



Summary

Shape and Matches

- There are 16 Matching Instances

Timeframe and Interval

- Your Start Time is *-8h
- Your End Time is *
- Your Time Interval gets an interpolated measurement Every 1 minute

16. From the **Target Configuration** list, select a target.
17. Click **Run Once** to create the view once, or click **Run on a Schedule** to periodically append new data to the view.
18. Click **Publish.**

Create an event view

If you want to analyze your data by event frames, create an event view. If you want to analyze your data broken down by assets, see Create an asset view. If you want to analyze your data broken down by assets and you need values streamed for real-time analytics or some other analysis, see Create a streaming view.

Note:

PI Integrator for Business Analytics only returns closed event frames (with a valid start and end time). It cannot publish open event frame data.

Procedure

1. Click the menu icon ☰ and click **Create Event View.**
2. Enter a name for the view.

   Note:
   Observe the naming conventions of the target to which this view will be published. For more information, see View names and destination endpoints.

3. If your user account is assigned to multiple PI AF identities with access to PI Integrator for Business Analytics, then click **Access Permissions** and select the identity to which you want to give view access.

   If only one PI AF identity has been granted access to PI Integrator for Business Analytics, this identity is automatically assigned to the view.

   When you first create a view, you can only grant access to one PI AF identity. You can later grant access to additional PI AF identities. For more information, see Secure your views.

4. Click **Create View.**
5. In the Source Events pane, click **Create a New Shape.**

   Tip:
   You can use the shape of an existing view by clicking **Import a Shape from Another View.**

6. Use the **Server** and **Database** fields to select the PI AF server and database where the event frames are stored.
7. From the Event Frames pane, drag the event frame and referenced element onto the Event Shape pane.

   Tip:

   Click the icon in the Source Events pane and set filters to display only event frames that are of interest. For example, you can filter by time, assets, events, and asset or event templates.

   On the More Options pane, if **All descendants** is selected, the entire PI AF hierarchy is searched. If this is not selected, only the root-level event frames are searched.

   For tips on creating event shapes, see Tips on building shapes in event views.

8. Click the icon 🔍 next to the element to open the **Assets** tab and go directly to its location in the PI AF hierarchy.
9. Drag any assets and attributes from the PI AF tree on to the **Event Shape** tree.

   For tips on creating asset shapes, see Tips on building shapes in event views.

10. To retrieve data for all event frames that share the same PI AF template:
    a. Click the icon ✎ next to the event frame in the **Event Shape** tree.
    b. Clear the **Event Frame Name** check box.
    c. Select the **Event Frame Template** check box and click **Save.**
11. Click **Next** to preview a subset of your data.

> **Note:**
>
> - The start time displayed is the start time of the first event frame that was added to the shape.
> - PI Integrator for Business Analytics retrieves only closed event frames.

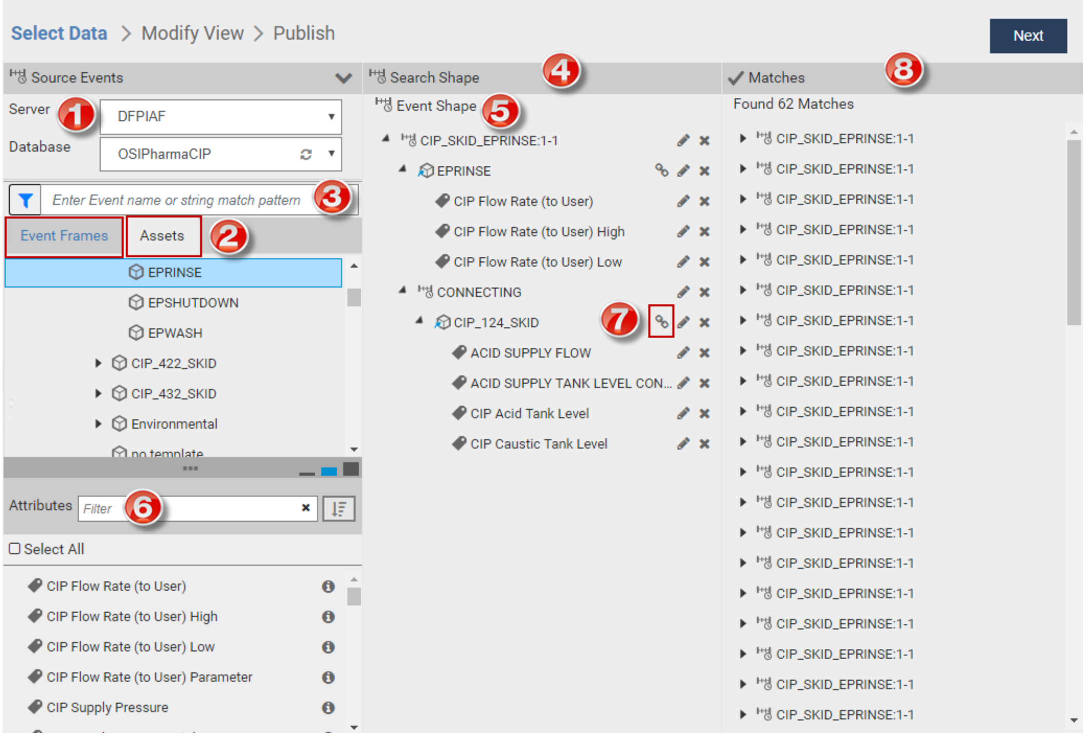
12. To refine the results, you can add more data, modify columns, filter the data, or change how values are retrieved. For more information, see Modify the data in your asset and event views.

    > **Note:**
    >
    > Because PI Integrator for Business Analytics only displays the first 100 rows for the first 10 matches of your shape, you could set your filters in a way that excludes this data. In this situation, no data will appear on the page even though your configured view results in valid matches.

13. Click **Next** to publish your data.
14. From the **Target Configuration** list, select a target.
15. Click **Run Once** to publish the view once, or click **Run on a Schedule** to periodically append new data to the view.
16. Click **Publish.**

Tips on building shapes in event views

You select the event frames to include in your event view on the Select Data page.



Server: DFPIAF

Database: OSIPharmaCIP

Found 62 Matches

The Select Data page

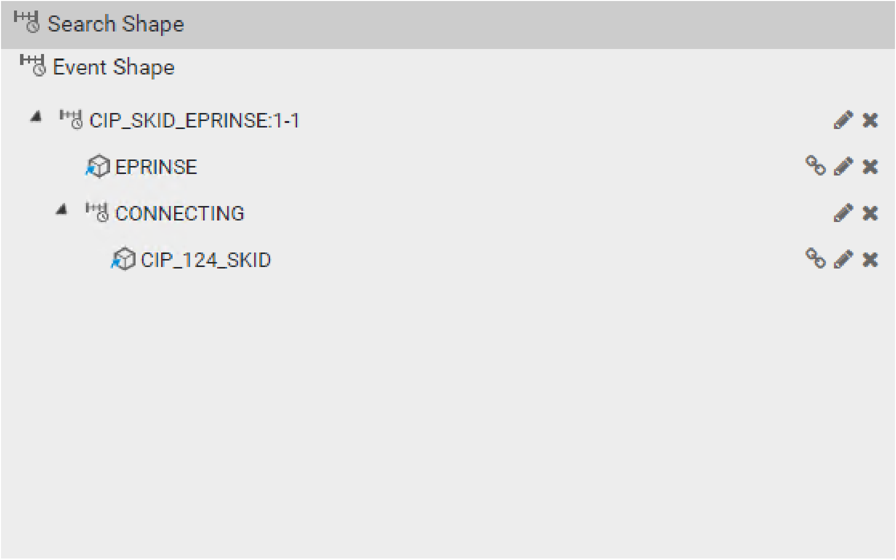
The following table describes the different parts of this page and how you use it to create your event view shape.

Number	Description
1	Specify the server and database on which the PI AF database is located.
2	Click the **Event Frames** tab to display the event frames. Click the **Assets** tab to display the elements.
3	To filter the list of event frames, enter a search string for the event frame name.
4	Search Shape pane where you specify the search pattern for your event view.
5	Event Shape pane where you add event frames and their attributes, and referenced elements and their attributes.
6	Attributes pane displays attributes you can add to the Event Shape pane. **Tip:** Click ℹ next to the attribute to open a window that displays data about the attribute.
7	Link a referenced element to its own separate search shape. Do this only if you want to include parent elements and attributes for the linked element.

Number	Description
8	Matches pane is a preview of the assets and event frames defined in your search shape for which matches are found in the PI AF database.

When working with the event shape:

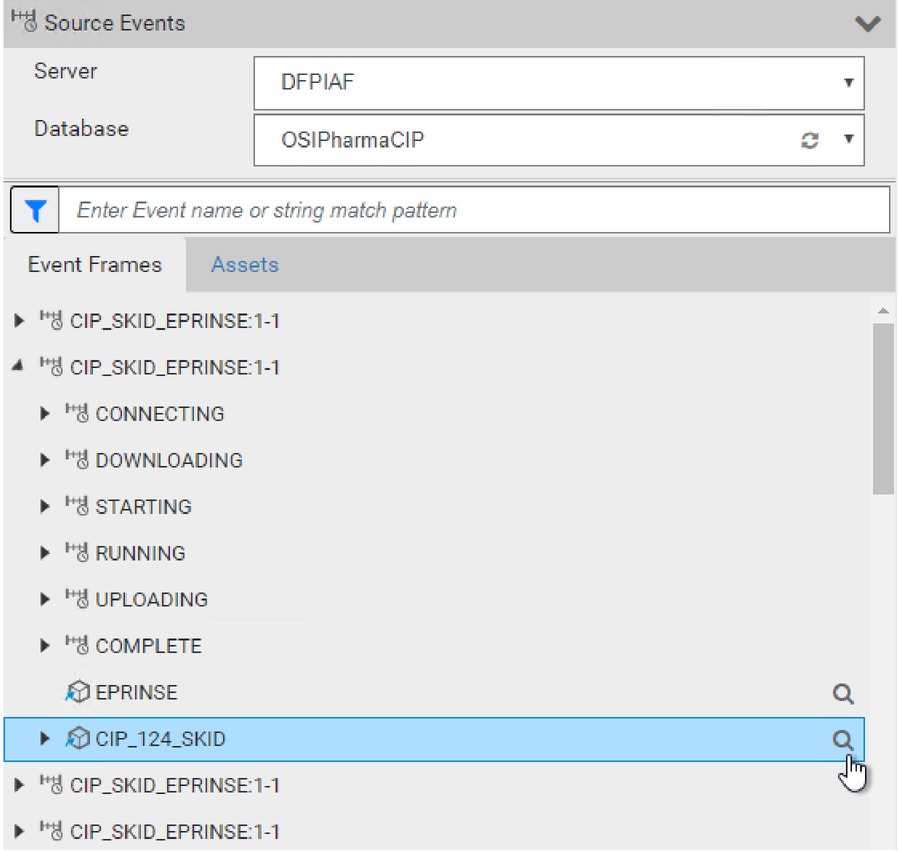
- You can add as many event frames as you like, but there can be only one event frame at each level in the event frame hierarchy as shown below. For example, the event shape node can have only one child event frame. Drag the event frame from the Event Frames pane onto the Event Shape pane.



Event shape: One event shape node with one child event frame

- Each event frame can have only one referenced element. Drag the referenced element from Event Frames pane into the event shape.
- Click on the event frame in the Event Frames pane to display its attributes in the Attributes pane. Drag any of its attributes into the event shape.

- In the Source Events pane, click the **Event Frames** tab, and then click the magnifying glass next to an element to switch to the Assets pane and see the element's location in the PI AF hierarchy.



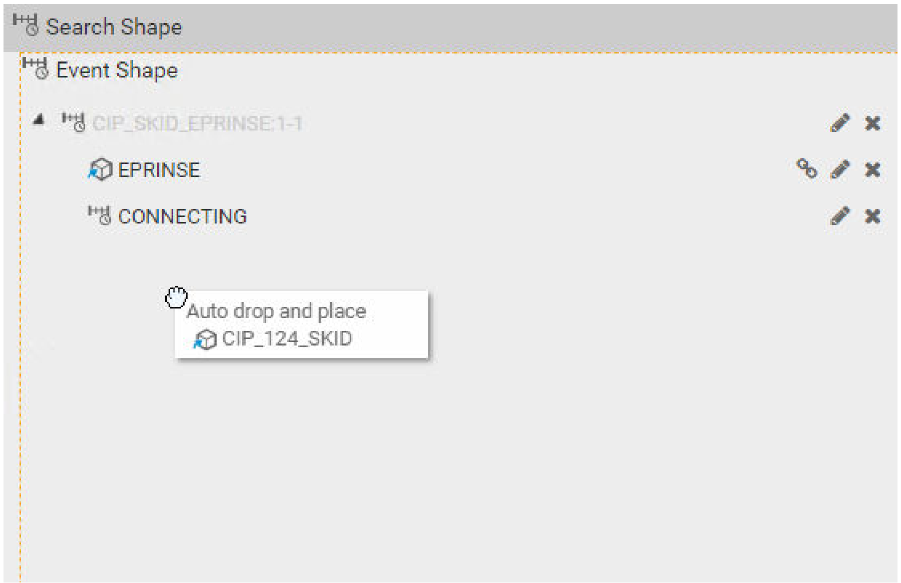
Server: DFPIAF

Database: OSIPharmaCIP

Locate an element in the PI AF hierarchy

The Attributes pane displays the attributes for the selected element. Drag any of its attributes into the event shape.

- Event frames and elements can only be dropped onto the Event Shape tree using **Auto drop and place** if it makes logical sense. If you drag an element to an open area below the event shape, a tool tip is displayed with the text **Auto drop and place.** PI Integrator for Business Analytics takes the object's relationship to other objects in the PI AF hierarchy and attempts to match this relationship in the shape. **Auto drop and place** is only able to add the dragged object to the shape when the object is an immediate parent or child of an object that already appears in your shape.



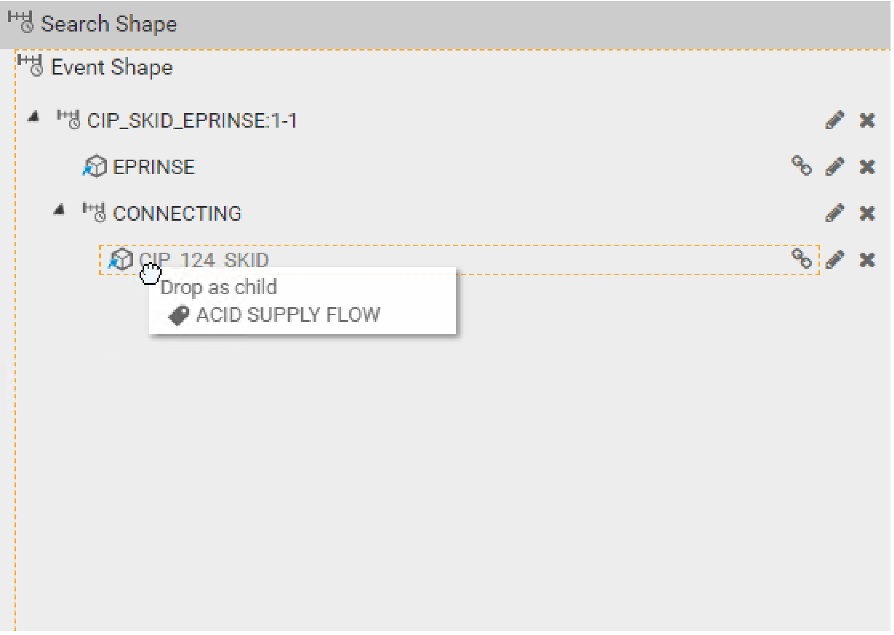
Auto drop and place objects

Tip:
If you are new to PI Integrator for Business Analytics, start by using **Auto drop and place**.

- As you drag an event frame, element, or attribute anywhere in the Event Shape tree, a tool tip guides you to drop the object as a parent, sibling, or child.

Note:

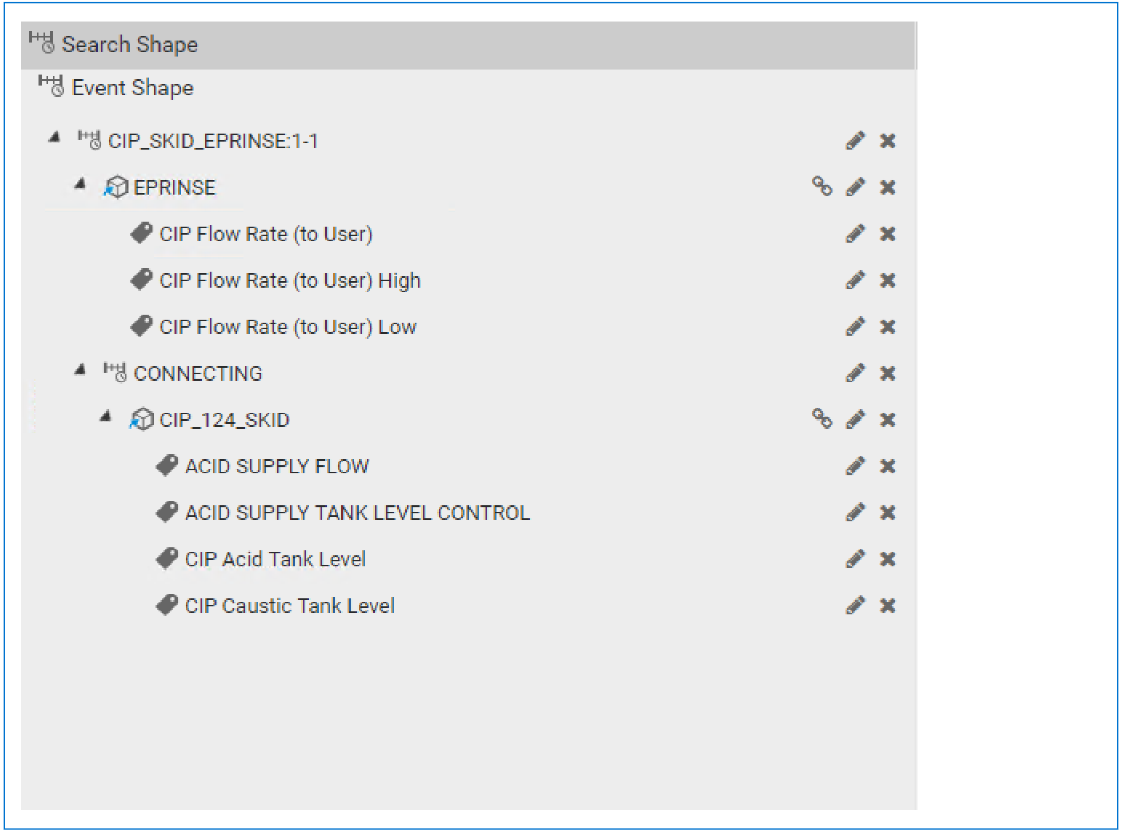
It will not prevent you from dropping an object in a location that does not match the PI AF hierarchy.



Dragging and dropping objects in a shape tree

When and how to use linked assets

In most instances, you will create your shape in the Event Shape pane, adding your event frame, child event frame, and referenced elements along with their attributes as shown in the screen capture below.

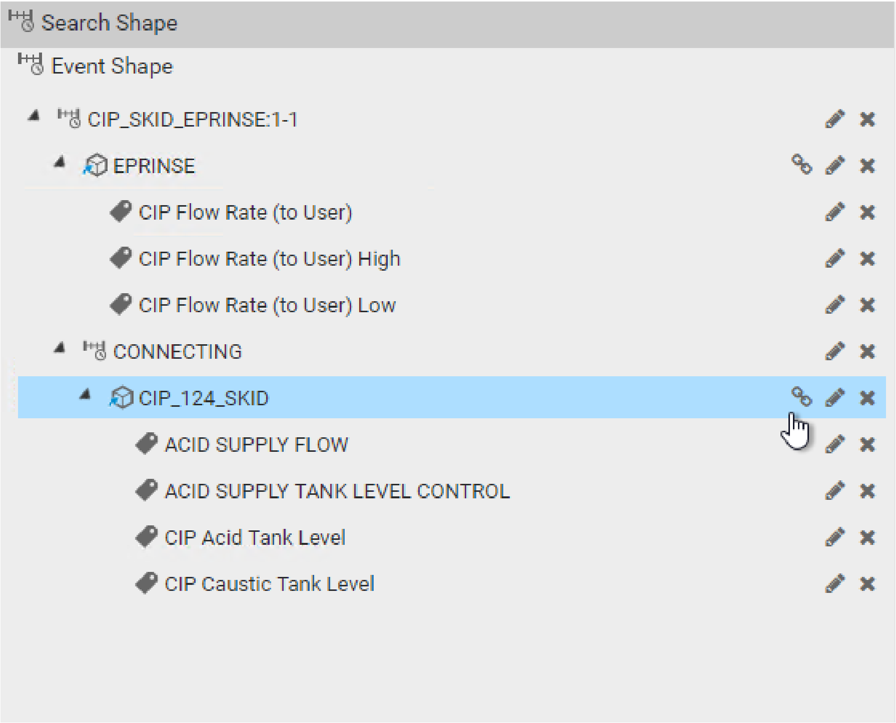


Search Shape

Event Shape

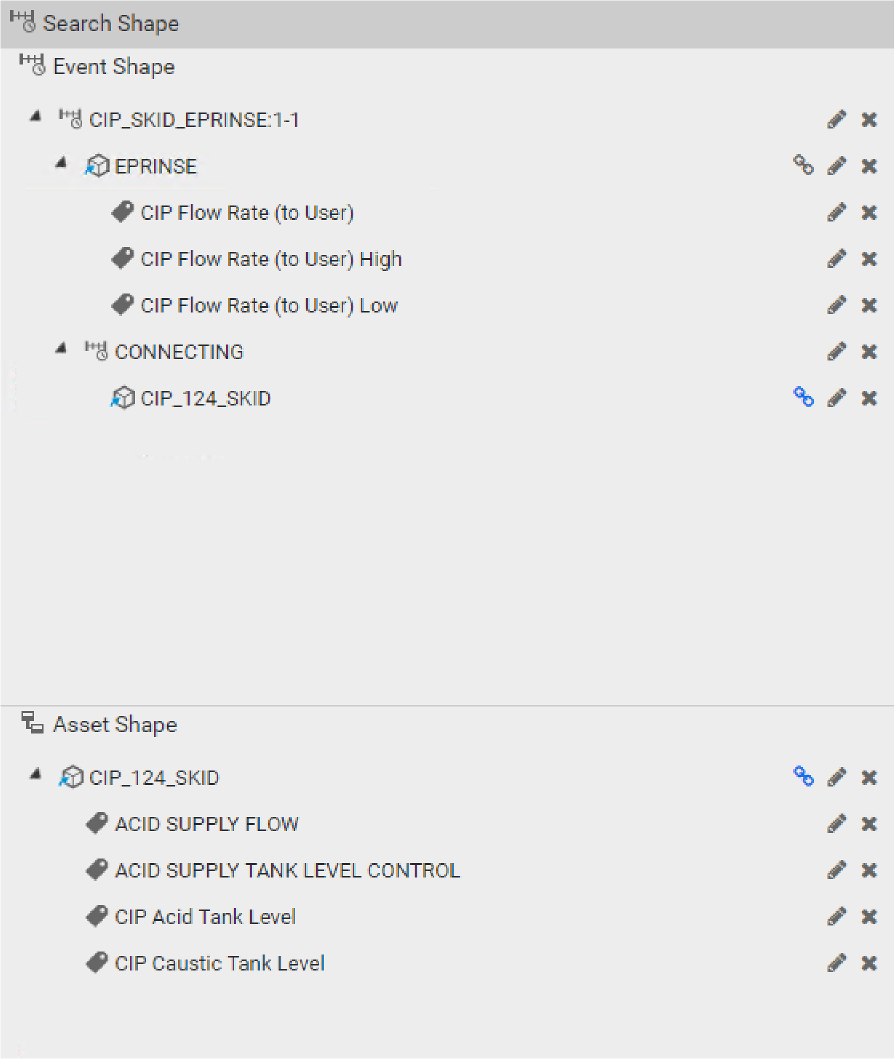
- CIP_SKID_EPRINSE:1-1
  - EPRINSE
    - CIP Flow Rate (to User)
    - CIP Flow Rate (to User) High
    - CIP Flow Rate (to User) Low
  - CONNECTING
    - CIP_124_SKID
      - ACID SUPPLY FLOW
      - ACID SUPPLY TANK LEVEL CONTROL
      - CIP Acid Tank Level
      - CIP Caustic Tank Level

In the event shape, you can only add elements below the element that is referenced by the top most event frame. In the example above, you cannot add parent elements that are above the CIP_124_SKID element in the PI AF hierarchy. If you need attributes or elements from a parent or a referenced element, then click the **Linked Assets** link to open the Asset Shape pane. (See the screen capture below.)



Linked assets link

When you click the Linked Assets icon, it displays a second pane, the Asset Shape pane. The linked element, its attributes, and any elements and attributes that are descended from it are moved to the Asset Shape pane. In this example, the CIP_124_SKID element is copied to the Asset Shape pane along with the four attributes. The screen capture below illustrates this.



Search Shape

Event Shape

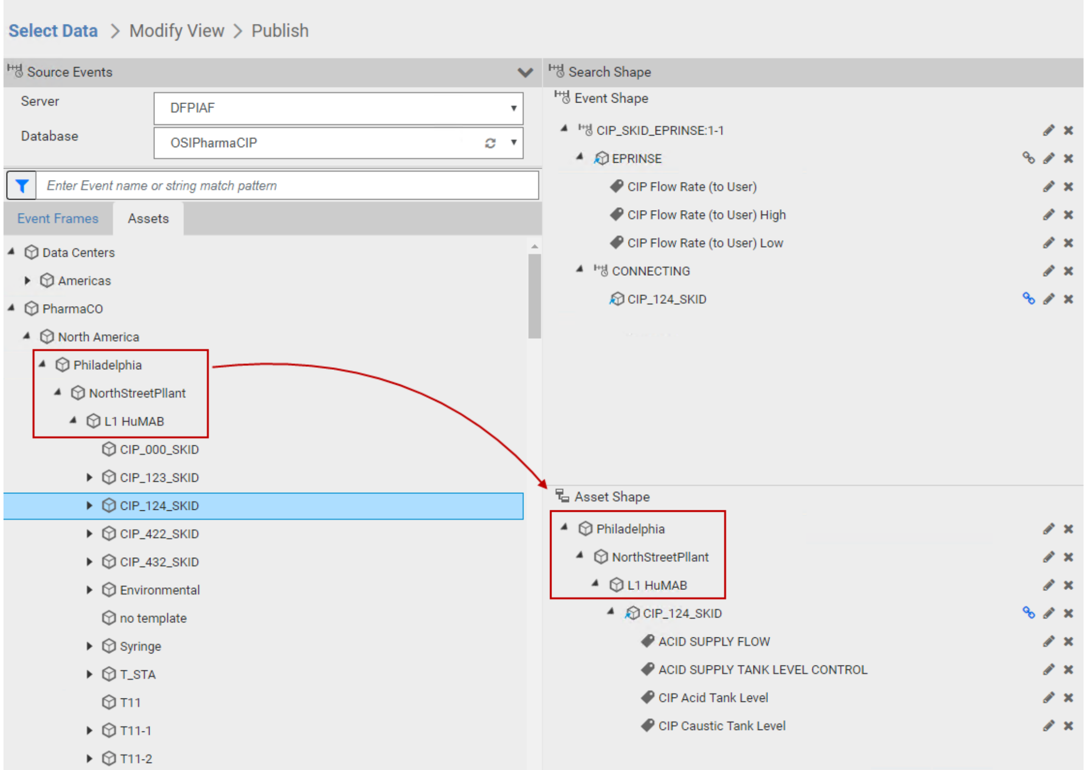
- CIP_SKID_EPRINSE:1-1
  - EPRINSE
    - CIP Flow Rate (to User)
    - CIP Flow Rate (to User) High
    - CIP Flow Rate (to User) Low
  - CONNECTING
    - CIP_124_SKID

Asset Shape

- CIP_124_SKID
  - ACID SUPPLY FLOW
  - ACID SUPPLY TANK LEVEL CONTROL
  - CIP Acid Tank Level
  - CIP Caustic Tank Level

Asset shape added to the search shape

In the Asset Shape pane, you can add any elements and their attributes regardless of where they appear in the PI AF hierarchy. In this example, the L1 HuMAB, NorthStreetPllant, and Philadelphia elements are added to the asset shape.



Server: DFPIAF

Database: OSIPharmaCIP

Elements added to the asset shape

If you click the Linked Assets link in the asset shape, the Asset Shape pane disappears and the linked asset and any of its attributes are returned to the Event Shape pane.

Note:

The only reason to separate an element into the Asset Shape pane is to include elements and attributes that occur above it in the PI AF hierarchy. Depending on the complexity of the shape, this can increase the time it takes to publish the view.

Create a streaming view

Note:

This feature is available in PI Integrator for Business Analytics Advanced Edition.

The following is an overview of the main steps to create a streaming view. Click on the links to get to the specific procedure.

Procedure

1. Define the shape of the streaming view.
2. Choose the schema to use with your view with one of the following:
    - Use a schema imported from a file
    - Use a schema imported from a schema registry
    - Use a generated schema

   For more information about schemas, see About schemas.
3. Configure when messages are sent.

   For more information about message triggers, see About message triggers.
4. (Optional) Backfill data.
5. (Optional) Filter the data.

Define the shape of the streaming view

If you want to analyze your data broken down by assets, see Create an asset view. If you want to analyze your data by event frames, see Create an event view.

Procedure

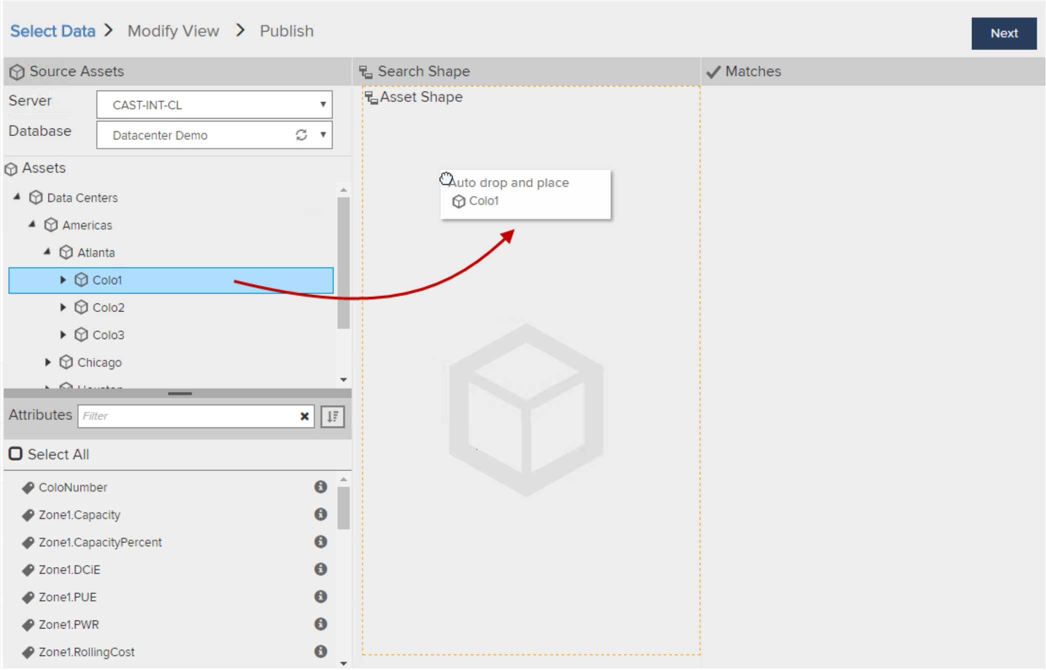
1. Click the menu icon ☰ and click **Create Streaming View**.
2. Enter a name for the view.

   > **Note:**
   > Observe the naming conventions of the target to which this view will be published. For more information, see View names and destination endpoints.
3. If your user account is assigned to multiple PI AF identities with access to PI Integrator for Business Analytics, then click **Access Permissions** and select the identity that will be given access to the view.

   If only one PI AF identity has been granted access to PI Integrator for Business Analytics, this identity is automatically assigned to the view.

   When you first create a view, you can only grant access to one PI AF identity. You can later grant access to additional PI AF identities. For more information, see Secure your views.
4. Click **Create View**.
5. In the Source Assets pane, click **Create a New Shape**.

   > **Tip:**
   > You can use the shape of an existing view by clicking **Import a Shape from Another View**.
6. Use the **Server** and **Database** fields to browse to the desired PI AF server and database.
7. Drill down the PI AF tree to find the asset you want to analyze.
8. Drag the asset onto the Asset Shape pane.



Server: CAST-INT-CL

Database: Datacenter Demo

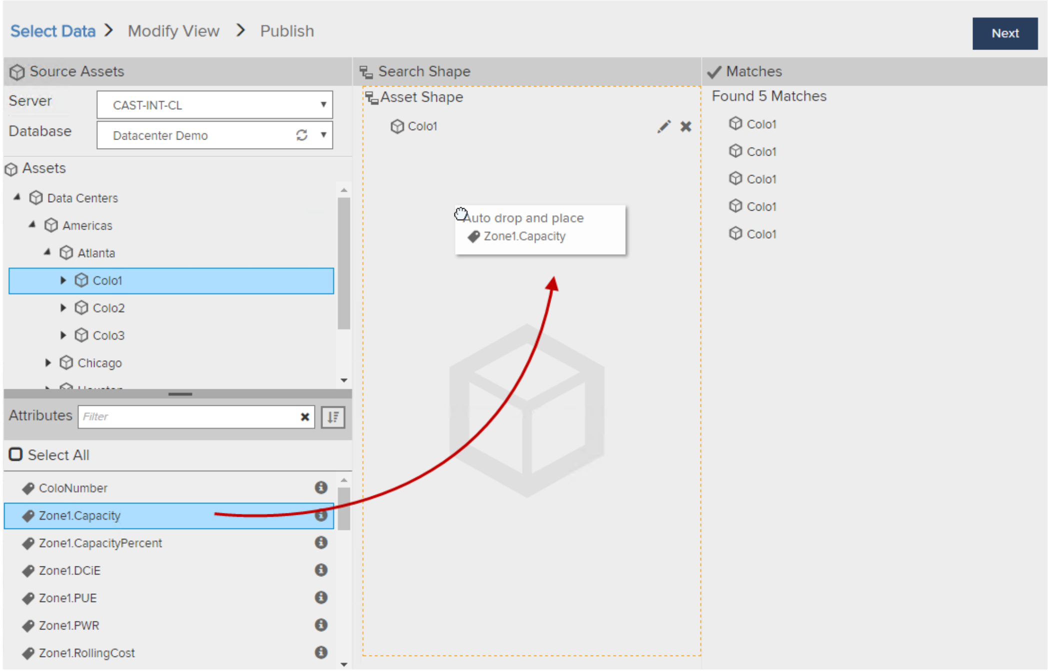
Dragging an asset onto the Asset Shape pane

The asset is added to the Asset Shape tree.

When you select an asset, the Attributes pane opens displaying the selected element's attributes.

9. Drag any attributes to include in your shape.

Note:
You can sort the attributes, group them by category, or filter which attributes are displayed to more easily find the ones you want.



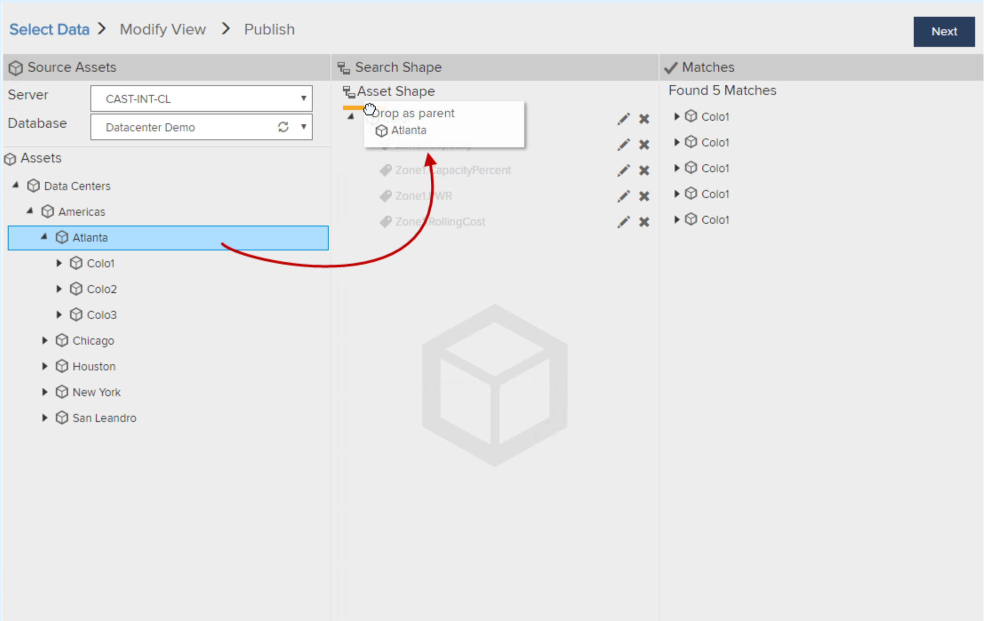
Adding an element using Auto drop and place

Tip:

If you drag an object *outside* the Asset Shape tree, a tool tip is displayed with the text **Auto drop and place.** The element is automatically added to the tree in a logical location. This element maintains the same relationship in the Asset Shape tree that it has in the PI AF tree. If there is no location that makes sense, the drop is rejected.

Tip:

You can also place the object in the Asset Shape tree. A tool tip is displayed that guides you to add the asset as a parent, child, or sibling entity. It will not prevent you from dropping an object in a location that does not match the PI AF hierarchy.



Placing an element in the Asset Shape tree

10. Drag any additional assets and attributes onto the Asset Shape pane.

    The Matches pane displays the elements that match the defined shape.

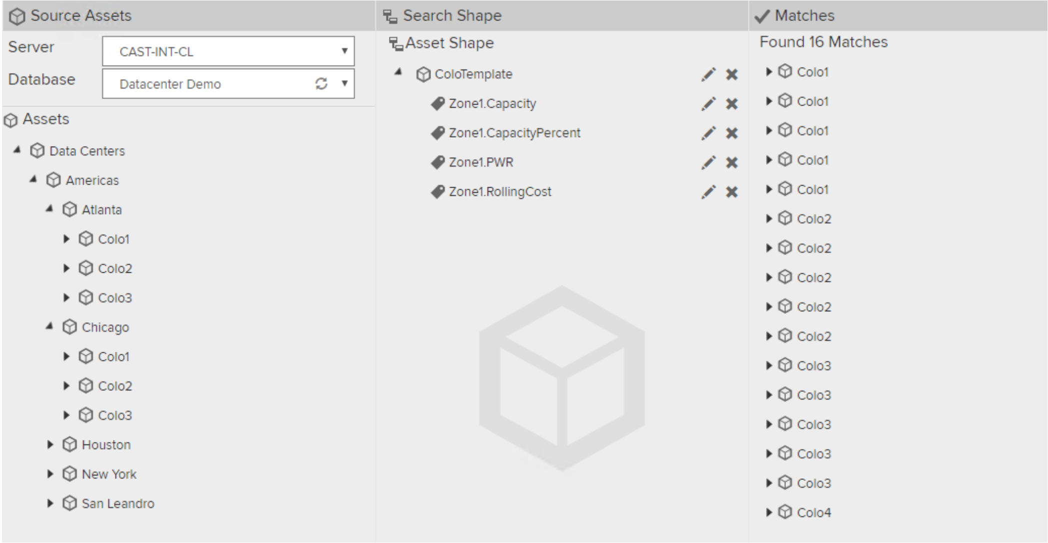
11. To see the data for all assets that share the same PI AF template:

    a. Click the icon ✎ next to the asset to open the Edit Filters window.

    b. Clear the **Asset Name** check box.

    c. Select the **Asset Template** check box and click **Save.**

    The Matches pane displays data from all assets that share this template.



Source Assets

Server: CAST-INT-CL

Database: Datacenter Demo

Assets
- Data Centers
  - Americas
    - Atlanta
      - Colo1
      - Colo2
      - Colo3
    - Chicago
      - Colo1
      - Colo2
      - Colo3
    - Houston
    - New York
    - San Leandro

Search Shape

Asset Shape
- ColoTemplate
  - Zone1.Capacity
  - Zone1.CapacityPercent
  - Zone1.PWR
  - Zone1.RollingCost

Matches

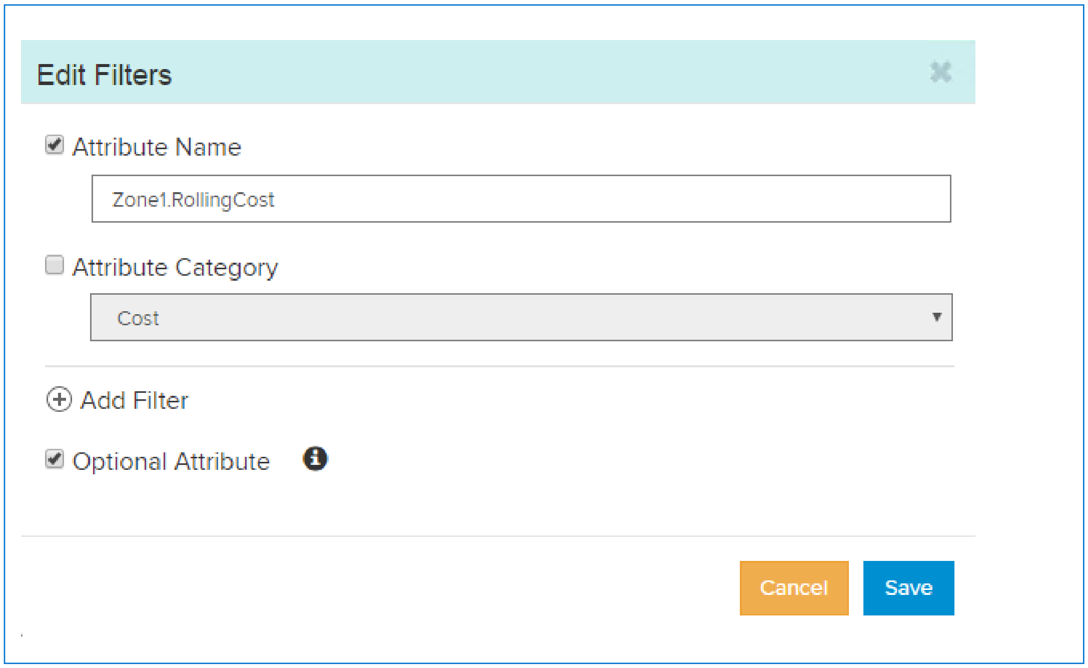
Found 16 Matches
- Colo1
- Colo1
- Colo1
- Colo1
- Colo1
- Colo2
- Colo2
- Colo2
- Colo2
- Colo2
- Colo3
- Colo3
- Colo3
- Colo3
- Colo3
- Colo4

12. To find matches for similar assets that have a different set of attributes:

    a. Click the icon ✎ next to the attribute that is not required.

    b. In the Edit Filters dialog box, select the **Optional Attribute** check box, then click **Save.**

    For example, you might use the **Optional Attribute** option if you acquired equipment over a period of time and some of the attributes differ between the older and newer equipment.



Edit Filters

☑ Attribute Name

Zone1.RollingCost

☐ Attribute Category

Cost

☑ Optional Attribute

13. Click **Next.**

    The Modify View page is displayed. See The Modify View page for an overview of the tasks you will be performing to modify your view.

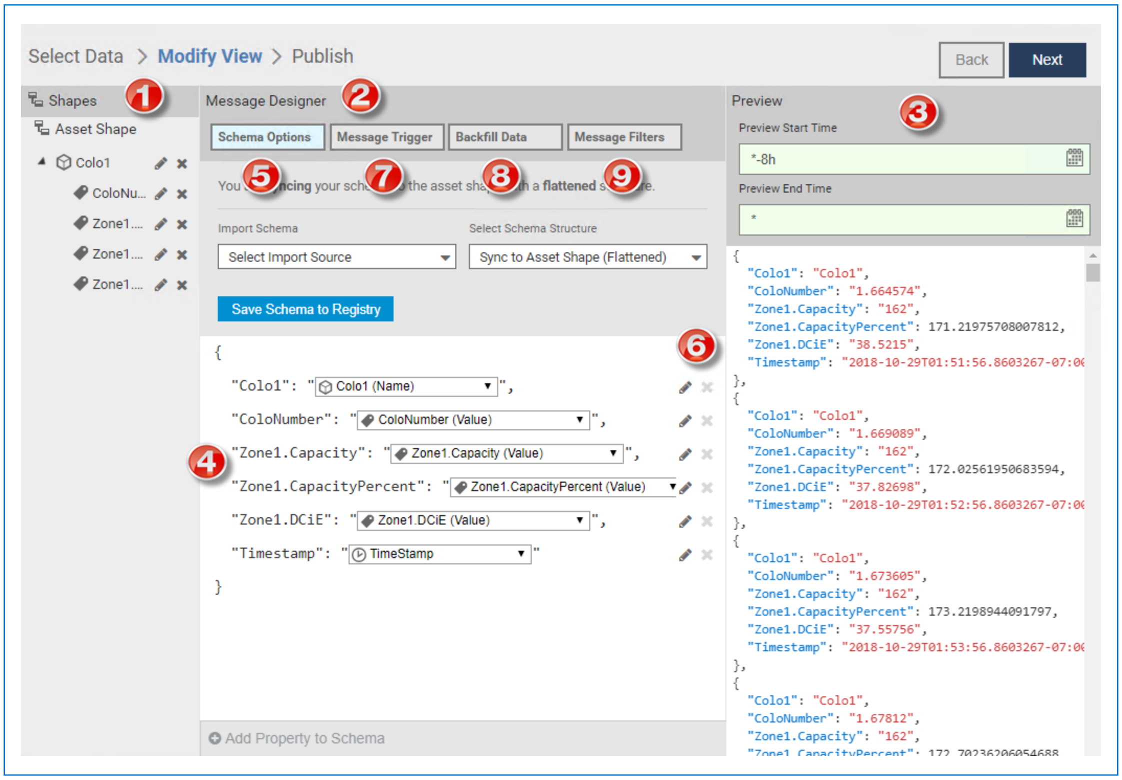
14. Choose the schema for your data by completing one of the following procedures:

- Use a generated schema
- Use a schema imported from a file
- Use a schema imported from a schema registry

Note:
For more information about the schema options, see About schemas.

The Modify View page

From the Modify View page, you specify the schema to use to send messages and specify when messages are sent. Optionally, you can exclude data and backfill data from an earlier period. The following screen shot identifies the different panes and key functions and features.



```
{
  "Colo1": "Colo1 (Name)",
  "ColoNumber": "ColoNumber (Value)",
  "Zone1.Capacity": "Zone1.Capacity (Value)",
  "Zone1.CapacityPercent": "Zone1.CapacityPercent (Value)",
  "Zone1.DCiE": "Zone1.DCiE (Value)",
  "Timestamp": "TimeStamp"
}
```

```
{
  "Colo1": "Colo1",
  "ColoNumber": "1.664574",
  "Zone1.Capacity": "162",
  "Zone1.CapacityPercent": 171.21975708007812,
  "Zone1.DCiE": "38.5215",
  "Timestamp": "2018-10-29T01:51:56.8603267-07:0
},
{
  "Colo1": "Colo1",
  "ColoNumber": "1.669089",
  "Zone1.Capacity": "162",
  "Zone1.CapacityPercent": 172.02561950683594,
  "Zone1.DCiE": "37.82698",
  "Timestamp": "2018-10-29T01:52:56.8603267-07:0
},
{
  "Colo1": "Colo1",
  "ColoNumber": "1.673605",
  "Zone1.Capacity": "162",
  "Zone1.CapacityPercent": 173.2198944091797,
  "Zone1.DCiE": "37.55756",
  "Timestamp": "2018-10-29T01:53:56.8603267-07:0
},
{
  "Colo1": "Colo1",
  "ColoNumber": "1.67812",
  "Zone1.Capacity": "162",
  "Zone1.CapacityPercent": 172.7023620605468
```

Number	Description
1	Asset shape – You can drag and drop elements and attributes from the shape onto the schema properties in the Message Designer pane.
2	Message Designer – In this pane, you select the schema, specify the message trigger, modify schema properties, and backfill data.
3	Preview – Displays the first 100 messages in the schema format displayed in the Message Designer pane.
4	Schema – Displays the schema used to send messages.
5	Schema Options – Selects the schema used to send messages. You can use a schema generated based on the asset shape or import a schema from a file or a registry.
6	Modify the schema properties, change the order of the schema properties, or delete the schema properties. Not all options are available with all schema types.

Number	Description
7	Message Trigger – Specifies the frequency and conditions under which a message is sent to the publish target.
8	Backfill Data – Specifies earlier values to send to the publish target.
9	Message Filters – Specifies data results to exclude.

For information on how to complete the tasks on the Modify View page, see the following:

- Use a schema imported from a file
- Use a schema imported from a schema registry
- Use a generated schema
- Configure when messages are sent
- Backfill data

About schemas

Note:

This feature is available in PI Integrator for Business Analytics Advanced Edition.

By default, the search shape is used to generate the schema for the streaming messages. You can use this generated schema or you can import a schema and the shape's data values are assigned to the schema. Schemas in the following formats are supported:

- JavaScript Object Notation (JSON)
- Comma-separated values (CSV)
- Apache Avro

Imported schemas

Schemas can be imported from a file or from a schema registry.

- Schemas imported from a file – Schemas in the following formats can be imported from a file: JavaScript Object Notation (JSON), Comma-separated values (CSV), and Apache Avro. Once imported, you assign values to the properties and edit the properties.
- Schemas imported from a schema registry – This release supports the Confluent Schema Registry using Apache Avro schemas.

  Avro schemas imported from the schema registry enforce strict rules. Once imported, the property name and data type are set from the Avro field name and type, respectively, and these cannot be changed. If either of the following is true, then the view will not publish

  - A property is not assigned a value
  - A property has a type mismatch and the corresponding Avro field does not support the null type

  If there is a type mismatch and the Avro field supports the null type, the view publishes but the field is omitted.

Generated schemas

The generated schemas are synched to the asset shape in a nested, flattened, or free-form structure. The schema property names match the asset and attribute names in the shape. The property value is populated with the data values of the related asset or attribute from the shape. In Flattened mode, the schema is displayed in a nonhierarchical structure. In Nested mode, the schema hierarchy is preserved. The Flattened and Nested schemas allow you to change property names, the values associated with the properties, and the data types. You can take a nested or flattened schema and turn it into a free-form schema. The Free-form schema gives you the most flexibility with modifying the schema. In addition to being able to do everything you can with a flattened or nested schema, you can also make changes to the properties by adding, deleting, and reordering properties.

Use a schema imported from a file

Before you start

Read About schemas for information on the different ways you can use a schema.

Procedure

1. In the Message Designer pane, click **Schema Options**.
2. Click **Select Schema** and choose **File**.
3. In the Open window, select the schema file and click **Open**.

   Schemas in the following formats are supported: JSON, CSV, and Apache Avro. Files must have a `.json`, `.csv`, or `.avsc` extension to be displayed in the Message Designer.
4. Assign the value to the schema properties using one of the following methods:
   - Drag an asset or attribute from the asset shape on to the schema.
   - Click the pencil icon to open the Edit Property window. Select an asset or attribute from the shape and then pick a value from the **Property Data Content** list. Click **Update Property**.
5. Drag and drop a schema property to move it to a different location.
6. Click the *x* to delete the schema property.
7. Click **Add Property to Schema** in the lower left corner to add a schema property.
   a. Enter the name of the property and click **Confirm**.
   b. Assign a value to the property by dragging an attribute from the asset shape or clicking on the ✎ icon.
8. Continue with the next procedure Configure when messages are sent.

Use a schema imported from a schema registry

Before you start

Read About schemas for information on the different ways you can use a schema.

Procedure

1. In the Message Designer pane, click **Schema Options**.
2. Click **Select Import Schema** and choose **Schema Registry**.
3. Select the schema from the Schema Registry Browser and click **Use Selected Schema**.
4. Assign the value to the schema properties using one of the following methods:
    - Drag an asset or attribute from the asset shape on to the schema.
    - Click the pencil icon to open the Edit Property window, and pick an asset or attribute from the shape and then pick a value from the **Property Data Content** list. Click **Update Property**.

    Before you can continue and publish your view, you must provide valid values for all properties in your schema. Avro schemas imported from the schema registry enforce strict rules. The name and data type cannot be changed. If there is a data type mismatch between the schema and the selected value, PI Integrator for Business Analytics will attempt a data type conversion. If it cannot convert the data type, then null values appear for that property. Check the Preview pane for null values. You must resolve all mistyped values. If there are unresolved values, the view will not publish. The exception to this is if the schema allows nulls; in this instance, unresolved data type mismatches do not have to be resolved and you will be able to publish your view.
5. Continue with the next procedure Configure when messages are sent.

Use a generated schema

Before you start

Read About schemas for information on the different ways you can use a schema.

Procedure

1. In the Message Designer pane, click **Schema Options**.

    By default, the schema that appears is synched with the asset shape and displayed in a flattened structure.
2. Click **Select Schema Structure** and pick one of the choices.
    - Sync to Asset Shape (Flattened) – The schema is displayed in a nonhierarchical structure.
    - Sync to Asset Shape (Nested) – The schema hierarchy is preserved.
    - Free-form – Free-form is applied to whatever hierarchy is displayed (Nested or Flattened) at the time.

    The schema displays the properties with the data values of the shape assets and attributes assigned. You can choose a different property value from a list of all available properties for the PI AF element or attribute.
3. To assign a different value to the schema property, click the arrow and select a property from the list.
4. To make other changes to the schema property, click the pencil icon to open the Edit Property window.

> **Tip:**
> You can, for example, make changes to the schema property name or the default data type of the property.

5. (Free-form schema only) Drag and drop the schema property to move it to a different location.

   > **Tip:**
   > - Properties at the same level in the hierarchy cannot be reordered. A property can only be moved to be the child of a different parent.
   > - All child properties of a given parent must have unique names. A drop is rejected if it violates this rule.

6. (Free-form schema only) Click the *x* to delete the schema property.
7. (Free-form schema only) Click **Add Property to Schema** in the lower-left corner to add a schema property.
8. Continue with the next procedure Configure when messages are sent.

Save a schema to the schema registry

Any schema imported from a file or any generated schema can be saved to the schema registry. All schemas, regardless of their source, are saved as Avro schemas. Once the schema is saved, then the schema in the Message Designer pane will be bound by the rules enforced by the schema registry. Therefore, you want to make any changes before you save the schema to the registry.

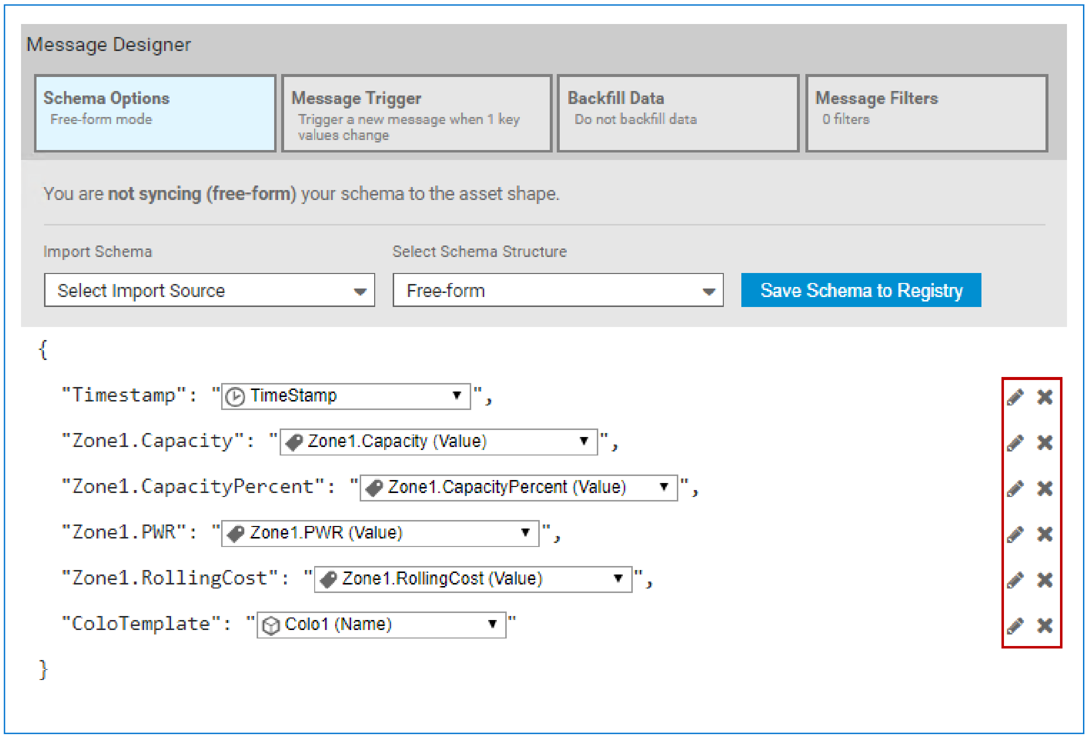
> **Note:**
> - You can always remove the connection of your schema in the Message Designer pane from the schema registry by clicking **Stop Using Registry**.
> - In this release, schemas can only be saved to a schema registry. They cannot be saved to a file.

Procedure

1. From the Modify View page, click **Save Schema to Registry**.

   > **Note:**
   >
   > **Schema Options** must be selected for this button to appear.

   Before you save the schema to the registry, you can edit and delete the schema properties. You can also reorder the properties if the schema is not synchronized with the asset shape, that is, if it is set to free-form. Drag and drop the properties to change their order.



Message Designer

You are **not syncing (free-form)** your schema to the asset shape.

Import Schema: Select Import Source

Select Schema Structure: Free-form

```
{
  "Timestamp": "TimeStamp",
  "Zone1.Capacity": "Zone1.Capacity (Value)",
  "Zone1.CapacityPercent": "Zone1.CapacityPercent (Value)",
  "Zone1.PWR": "Zone1.PWR (Value)",
  "Zone1.RollingCost": "Zone1.RollingCost (Value)",
  "ColoTemplate": "Colo1 (Name)"
}
```

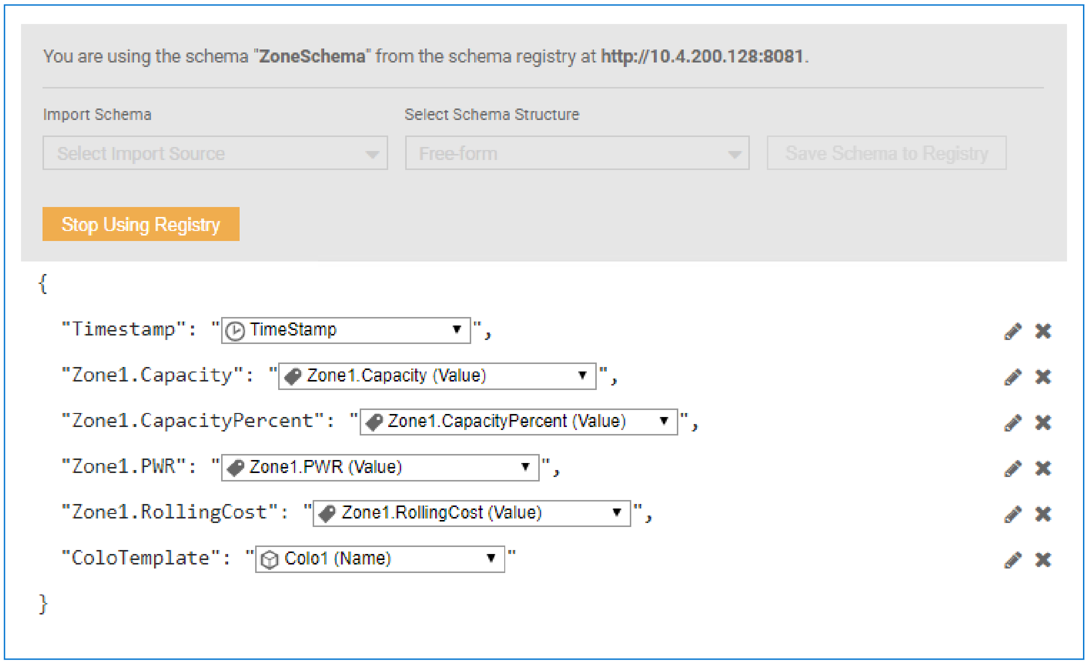
2. In the Save Schema to Registry window, specify the location of the schema registry in the **Schema Registry URL** field.

   Tip:

   Start typing in the field and a list of available schema registries appears.

3. Enter a name for your schema in the **Schema Subject** field and click **Save.**

   You can still edit some of the properties of the schema properties. However, you can no longer reorder or delete schema properties.



You are using the schema "**ZoneSchema**" from the schema registry at **http://10.4.200.128:8081**.

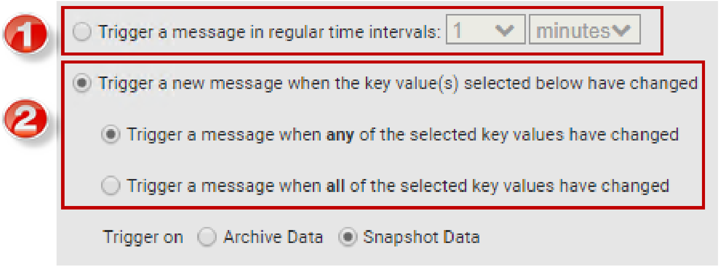
```
{
  "Timestamp": "TimeStamp",
  "Zone1.Capacity": "Zone1.Capacity (Value)",
  "Zone1.CapacityPercent": "Zone1.CapacityPercent (Value)",
  "Zone1.PWR": "Zone1.PWR (Value)",
  "Zone1.RollingCost": "Zone1.RollingCost (Value)",
  "ColoTemplate": "Colo1 (Name)"
}
```

Tip:

You can click **Stop Using Registry** to remove the connection of this schema to the schema registry. Once you do this, you can return to making any changes you could before you saved the schema.

About message triggers

The message trigger determines the frequency and conditions under which a message is sent to the publish target. There are two types of triggers, one based on a time interval and the other based on changes to the key values. All key values must be PI point attributes. These options are displayed in the screen shot below.



○ Trigger a message in regular time intervals: 1 minutes

● Trigger a new message when the key value(s) selected below have changed

● Trigger a message when **any** of the selected key values have changed

○ Trigger a message when **all** of the selected key values have changed

Trigger on ○ Archive Data ● Snapshot Data

1. Message trigger based on time
2. Message trigger based on a change in the data values

The sections below describe how to use these options.

Trigger a message at regular time intervals

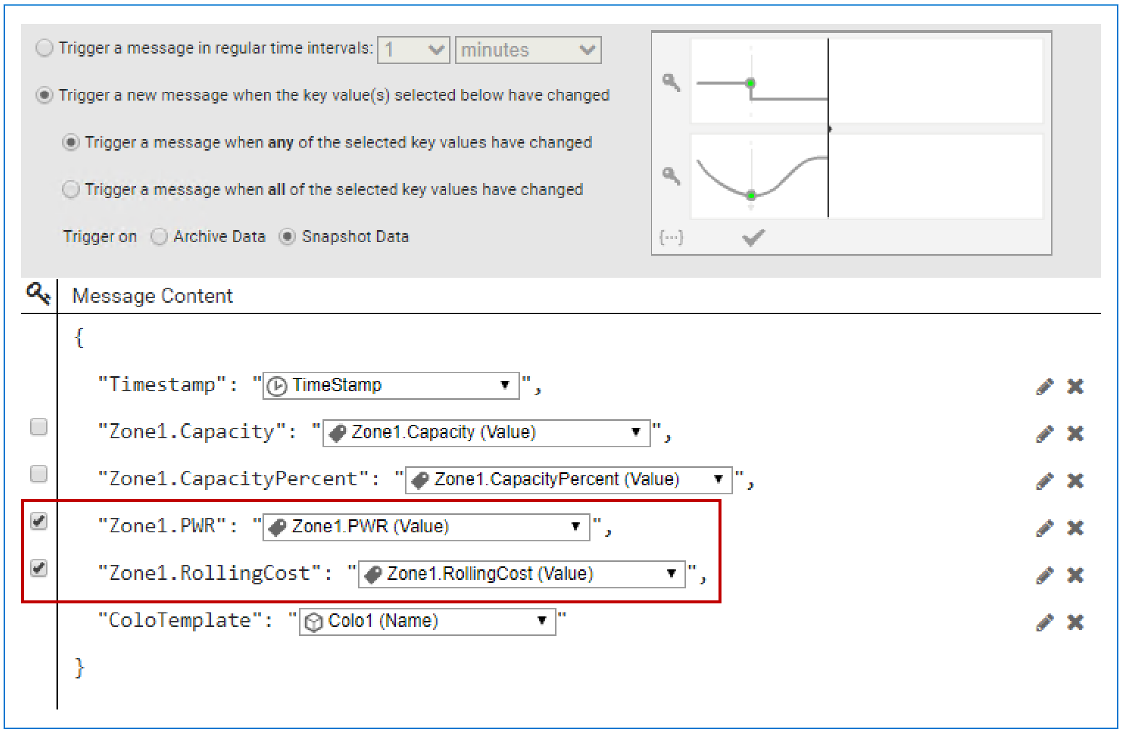
You can set a time interval between 30 seconds and up to 12 months. A message is sent at the time interval specified, independent of whether there are any changes to the data. Views with this type of message trigger are called scheduled streaming views.

Note:

Depending on message size and buffers, there can be a delay in when the data is received in the target. Edge-to-edge latency, the interval between when a value arrives in the PI System and when it arrives in the target system, can be greater than the interval between message triggers.

Identify the keys that trigger the message

You can decide which key changes will trigger a message. Views with this type of message trigger are called key-value-triggered streaming views. In the screen shot below, two keys which correspond to PI tags, Zone1.PWR and Zone1.RollingCost, are selected.



○ Trigger a message in regular time intervals: 1 minutes

● Trigger a new message when the key value(s) selected below have changed

● Trigger a message when **any** of the selected key values have changed

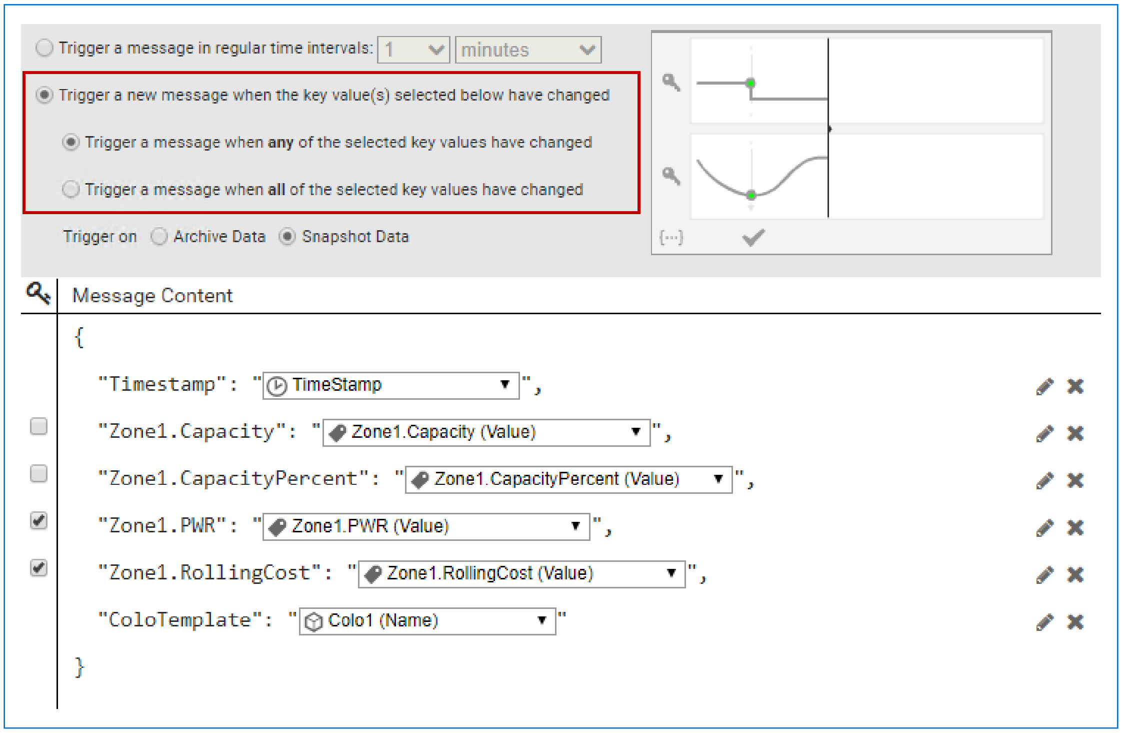
○ Trigger a message when **all** of the selected key values have changed

Trigger on ○ Archive Data ● Snapshot Data

Message Content

```
{
    "Timestamp": "TimeStamp",
□   "Zone1.Capacity": "Zone1.Capacity (Value)",
□   "Zone1.CapacityPercent": "Zone1.CapacityPercent (Value)",
☑   "Zone1.PWR": "Zone1.PWR (Value)",
☑   "Zone1.RollingCost": "Zone1.RollingCost (Value)",
    "ColoTemplate": "Colo1 (Name)"
}
```

Once you identify the keys, you can further customize the conditions under which a message is triggered.



○ Trigger a message in regular time intervals: 1 minutes

● Trigger a new message when the key value(s) selected below have changed

● Trigger a message when **any** of the selected key values have changed

○ Trigger a message when **all** of the selected key values have changed

Trigger on ○ Archive Data ● Snapshot Data

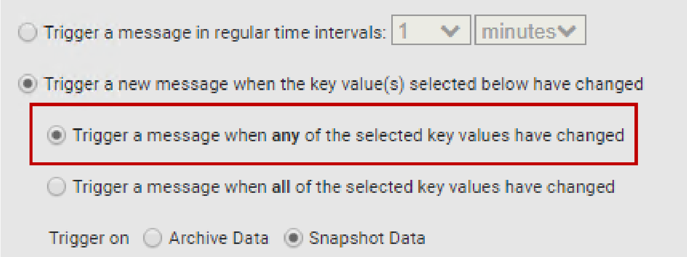
Message Content

```
{
    "Timestamp": "TimeStamp",
□   "Zone1.Capacity": "Zone1.Capacity (Value)",
□   "Zone1.CapacityPercent": "Zone1.CapacityPercent (Value)",
☑   "Zone1.PWR": "Zone1.PWR (Value)",
☑   "Zone1.RollingCost": "Zone1.RollingCost (Value)",
    "ColoTemplate": "Colo1 (Name)"
}
```

These choices are described below.

Trigger a message when any key value changes

The first option is to trigger a message whenever the data for any of the selected keys changes.



○ Trigger a message in regular time intervals: 1 minutes

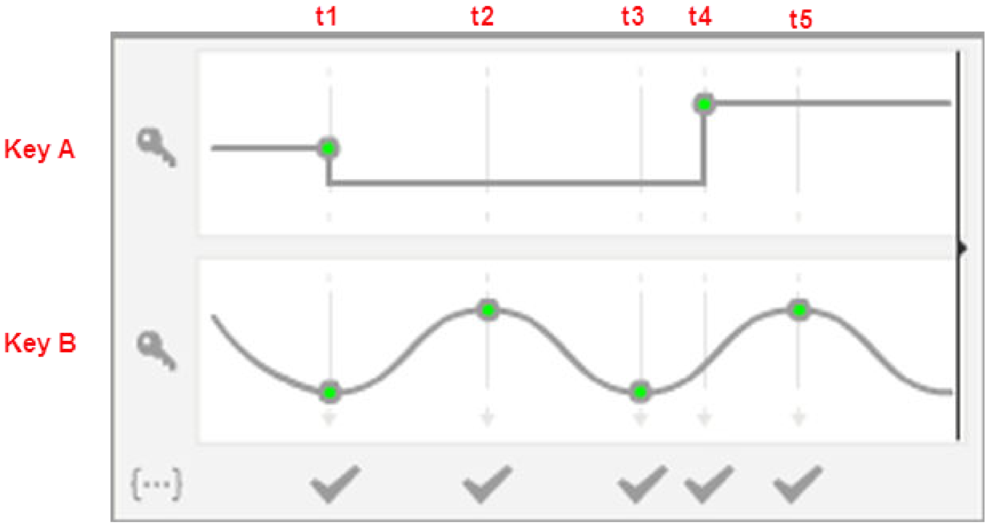
● Trigger a new message when the key value(s) selected below have changed

● Trigger a message when **any** of the selected key values have changed

○ Trigger a message when **all** of the selected key values have changed

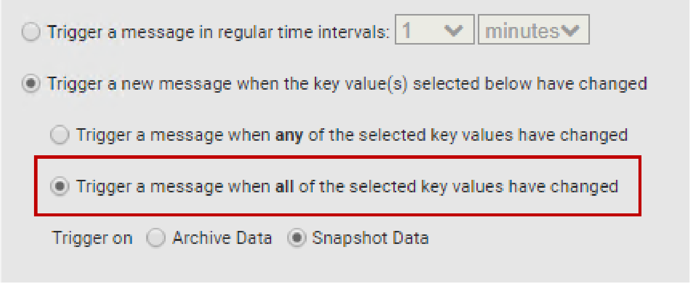
Trigger on ○ Archive Data ● Snapshot Data

The following is a graphical representation of this option. It displays two keys, Key A and Key B. Messages are triggered whenever there is a change to any one of the keys, indicated by the dots. Messages are sent at t1, t2, t3, t4, and t5, as indicated by the check marks.



Trigger a message only when all key values change

The second option is to have a message sent only when the values of all keys have changed.



○ Trigger a message in regular time intervals: 1 minutes

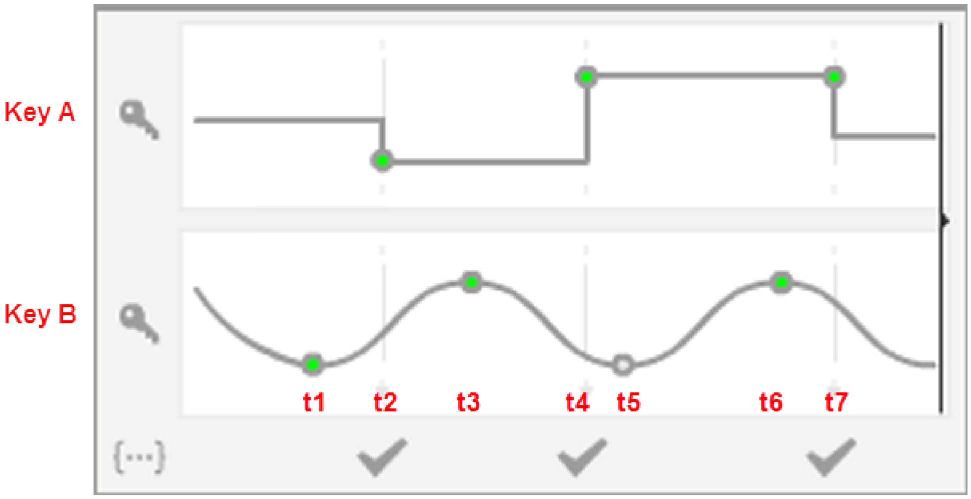
● Trigger a new message when the key value(s) selected below have changed

○ Trigger a message when **any** of the selected key values have changed

● Trigger a message when **all** of the selected key values have changed

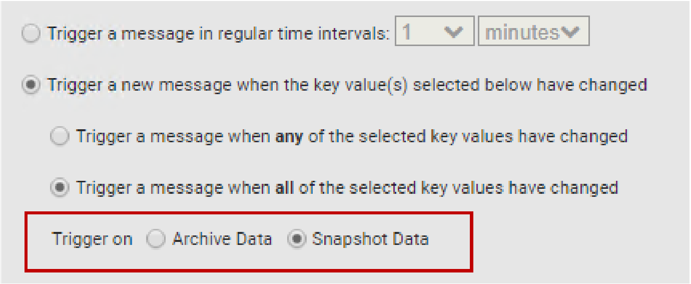
Trigger on ○ Archive Data ● Snapshot Data

The following graph illustrates this. Three messages are sent at t2, t4, and t7. The green dots indicate which changed values are recorded. The value at t5 is not sent, as indicated by the empty dot.



Type of data that triggers the message

In addition to identifying the most critical data to focus on, you can also specify if you want to use archive or snapshot values to trigger the message.



○ Trigger a message in regular time intervals: 1 minutes

● Trigger a new message when the key value(s) selected below have changed

○ Trigger a message when **any** of the selected key values have changed

● Trigger a message when **all** of the selected key values have changed

Trigger on ○ Archive Data ● Snapshot Data

Configure when messages are sent

Before you start

Read the About message triggers topic. It provides the background you need to set the message trigger.

You must generate your schema before you set the message trigger.

Procedure

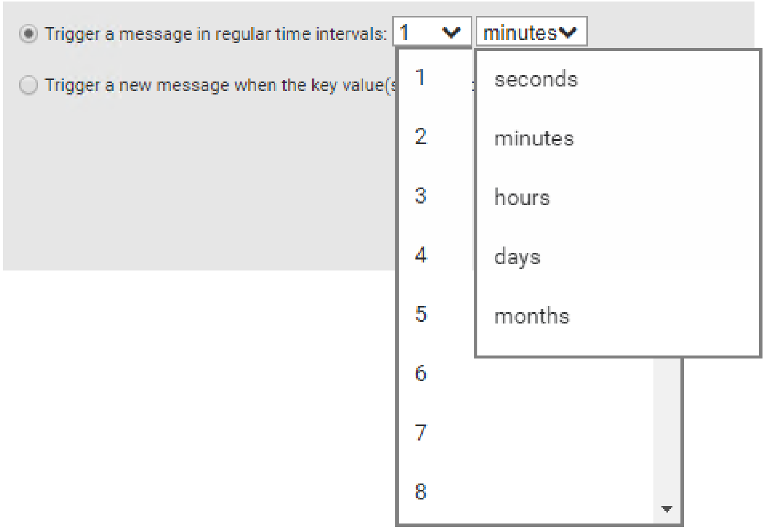
1. On the Modify View page, click **Message Trigger**.
2. Choose one of the following options:

	Option	Description
A	**Trigger a message in regular time intervals**	Messages are sent at the interval specified regardless of whether there is a change to the key value.
B	**Trigger a new message when the key value(s) selected below have changed**	Messages are sent based on changes to the key values.

- ◦ If you selected A, continue to step 3.
- ◦ If you selected B, continue to step 4.

3. (A only) Click on the lists to specify the time interval between messages.

   You can specify intervals between 30 seconds and 12 months.



● Trigger a message in regular time intervals: 1 minutes

○ Trigger a new message when the key value(s

Message time interval

4. (B only) Complete the following steps:

   a. Select the keys whose values will trigger the message.

   b. Choose one of the following options:

Option	Description
Trigger a message when any of the selected key values have changed	Only one key value needs to change to trigger a message
Trigger a message when all of the selected key values have changed	All key values must change to trigger a message

   c. Choose whether the message is triggered off of changes to the snapshot value or the archive value of the selected keys.

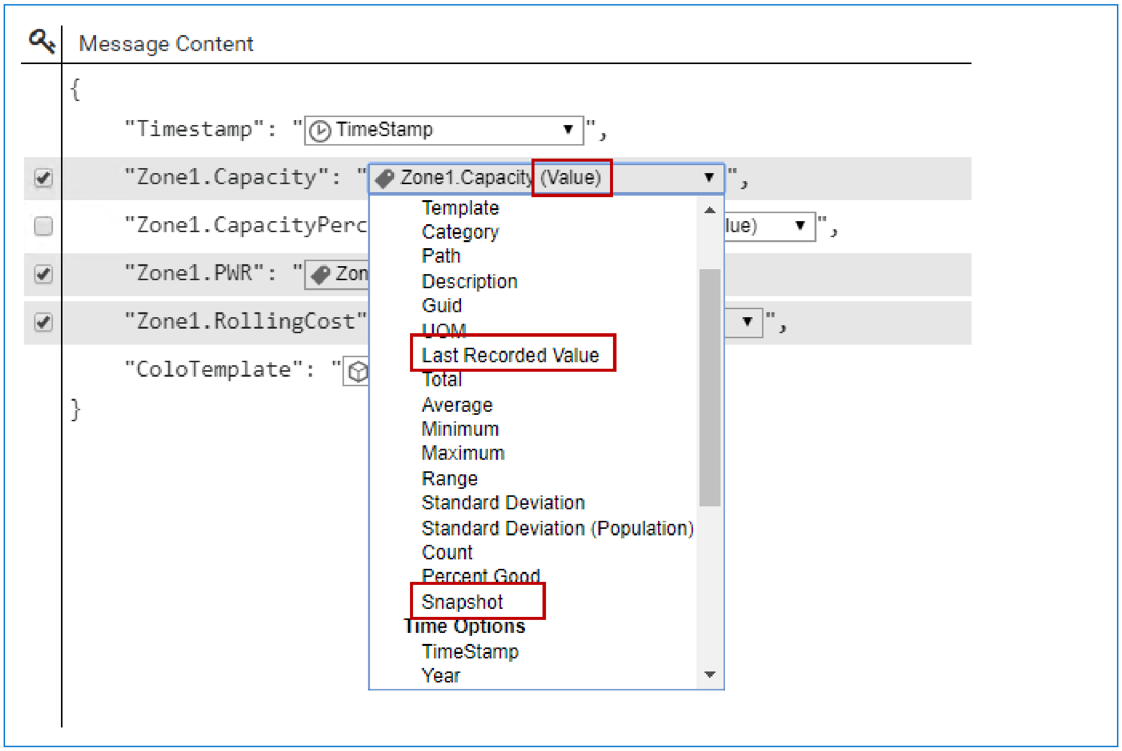
   For more information on how these choices affect what data is sent, see About message triggers.

What data is sent to the target?

After you configure when a message is sent, then specify what type of data is sent. For each property, you can select from a list of Value Options.

Note:

For the key-based scenarios, the type of data that triggers the message (archive or snapshot) is separate from the data that actually gets sent to the target. For example, you can specify that a change to the snapshot data of a key triggers the message. However, you can specify that the archive value of the key (not the snapshot value) is sent to the target. In the screen shot below, Value is selected for the Zone1.Capacity property.



Message Content

```
  {
      "Timestamp": "TimeStamp ▾",
☑     "Zone1.Capacity": "Zone1.Capacity (Value) ▾",
□     "Zone1.CapacityPerc                        lue) ▾",
☑     "Zone1.PWR": "Zon
☑     "Zone1.RollingCost"                        ▾",
      "ColoTemplate": "
  }
```

The following scenarios describe the conditions under which a message is triggered.

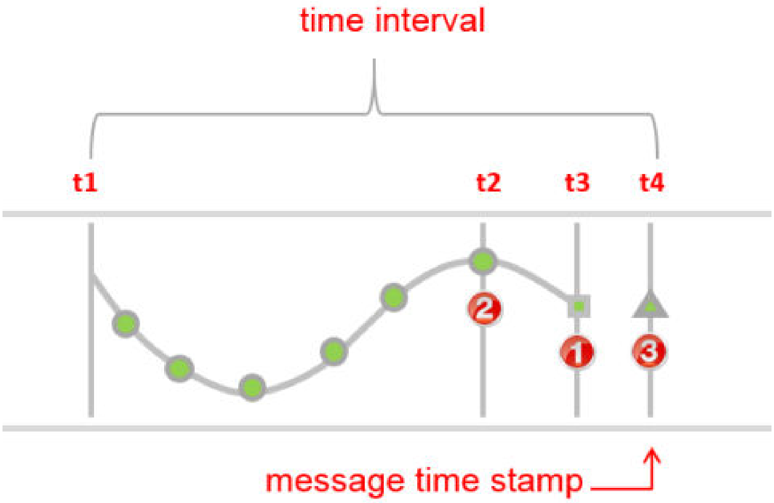
- Scenario 1: Interval data
- Scenario 2: Any key change of archive data triggers a message
- Scenario 3: Any key change of snapshot data triggers a message

In each situation, the properties can be configured with a different value choice. The scenarios describe the effect of configuring the properties with the Value, Last Recorded Value, and Snapshot choices.

Scenario 1: Interval data

Interval data is sent at specified intervals. In the following example, t1 and t4 mark the beginning and end of the time interval. The message time stamp is the time at t4. The data that is sent depends on the value choice selected for the property:

- If the property is configured for Snapshot Value, then the snapshot value at t3 is sent with the t4 time stamp. (1)
- If the property is configured for Last Recorded Value, then the last recorded value before the message time stamp is sent, in this example, the archive value at t2 is sent with the t4 message time stamp. (2)
- If the property is configured for Value, then the archive and snapshot values in the time interval are used to calculate the interpolated value at t4. (3)



Key	
●	Archive value
■	Snapshot value
▲	Interpolated value

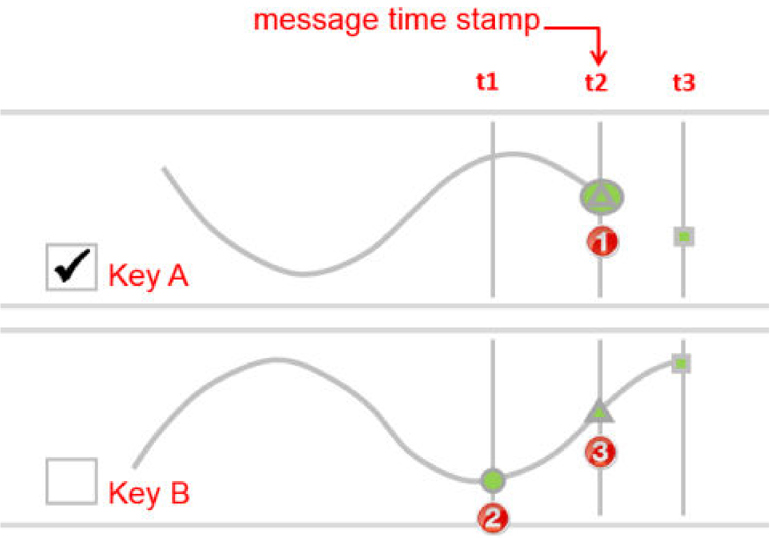
Scenario 2: Any key change of archive data triggers a message

When a snapshot value comes in at t3, it triggers the snapshot value at t2 to be archived (at t2). The archive value at t2 triggers the message and the time stamp is t2. The following illustration shows what data is sent to the target depending on the value choice selected:

- If A is configured for Last Recorded Value data, then the archive value at t2 is sent (1).
- If A is configured for Value data, then the interpolated value at t2 is sent (1).

Similarly, the data that is sent for property B depends on how it is configured:

- The Last Recorded Value is the first value in the PI Data Archive prior to or at the message time stamp (t2). In this example, if B is configured for Last Recorded Value, then the archive value which is the first value prior to t2 is sent (2).
- If B is configured for Value data, then the data is interpolated at t2 using the archive value at t1 and the snapshot value at t3 (3).



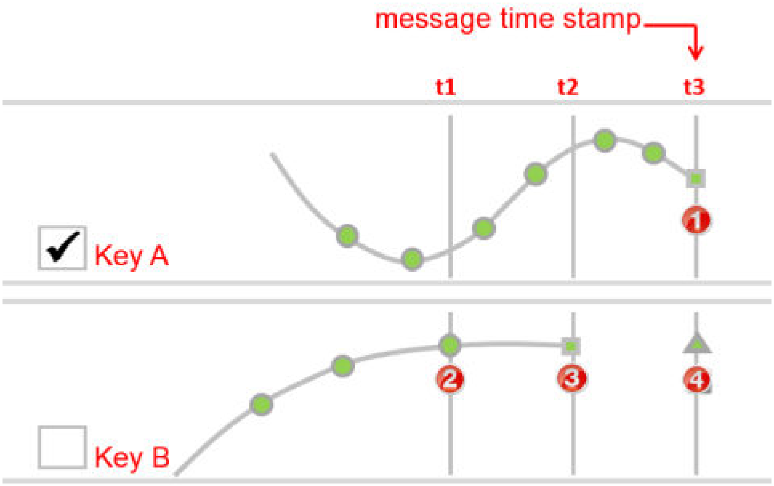
Key	
●	Archive value
■	Snapshot value
▲	Interpolated value

Scenario 3: Any key change of snapshot data triggers a message

A change to the snapshot value of any of the keys triggers a message. In this example, the message is triggered off of Key A. Snapshot data for Key A triggers a message at t3 and the message time stamp is t3. The snapshot value at t3 is returned for Key A (1).

Key B is not selected as a triggering key. The values for a second key, Key B, are determined by its configuration:

- If Key B is configured for Last recorded value, then the archive value at t1 with the t3 message time stamp is sent. (2)
- If Key B is configured for Snapshot value, then the snapshot value at t2 is sent with the t3 message time stamp. (3)
- If Key B is configured for Value, then the interpolated value at t3 is sent with the t3 timestamp. (4)



Key	
●	Archive value
■	Snapshot value
▲	Interpolated value

If you select the option, **Trigger a message when all of the selected key values have changed**, then there must be a change to all keys before a message is triggered. Snapshot values are returned for all selected keys, and the time stamp of the last key to return a snapshot value is the message time stamp.

Previews of streaming view data

Previews of the data always show archive values. Therefore, if the result of the message trigger settings is that snapshot data is sent to the target, this snapshot data does not appear in the preview. You will see archive values.

Out-of-order data

Key-triggered streaming views will not trigger a message on an event that has a time stamp prior to the last event's time stamp.

Backfill data

When you publish your data, the current values for your shape are sent to the target. You can get earlier values by backfilling your data.

> **Note:**
>
> Backfilling data is supported with scheduled streaming views. It is not supported with key-value-triggered streaming views.

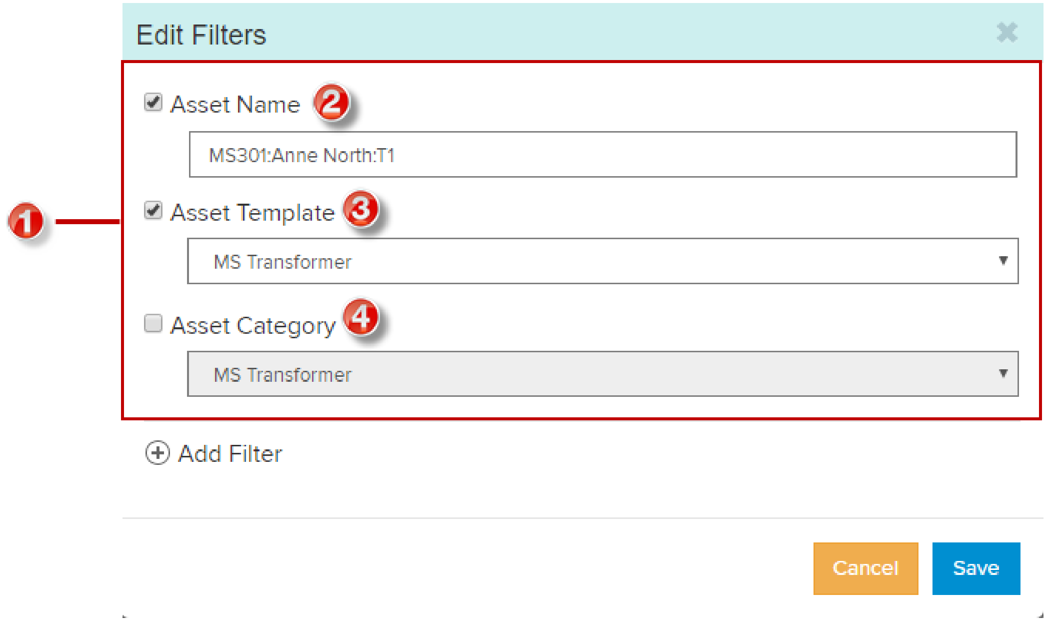
Procedure

1. From the Modify View page, click **Backfill Data**.
2. Click **Backfill data starting from**.
3. Click on the calendar icon in the text box to open the calendar.
4. Scroll through the calendar and click on the start date.

Use filters to refine the view shape

On the Select Data page, you often start by adding a single asset or event frame to the search shape. You can then use filters to extend that shape to other assets or event frames. You click the ✎ icon to open the Edit Filters dialog box. The following screen shot is the Edit Filters dialog for an asset view shape.

> **Note:**
>
> The example in this section discusses the edit filters for an asset view shape. Event frame filters have conditions with similar names and the behavior of the filters is the same as asset view filters.



☑ Asset Name

MS301:Anne North:T1

☑ Asset Template

MS Transformer

□ Asset Category

MS Transformer

Edit Filters dialog for an asset view shape

The screen shot identifies the filter and the conditions that comprise it.

Number	Description
1	Example of an asset view filter
2	Asset Name condition
3	Asset Template condition
4	Asset Category condition

You may search based on one or more of these conditions. All selected conditions must be met in order to qualify as a match. For example, in the screen shot, the **Asset Name** and **Asset Template** are both selected and both conditions must be met to find a match. Only assets whose name is *MS301:Anne North:T1* and are based on the MS Transformer template will appear in the **Matches** pane.

For event views, the filter conditions are named **Event Name**, **Event Template**, and **Event Category**. However, the behavior of the filters is the same as it is for asset view filters.

You can expand your search to include more possible matches by adding filters. You click the plus (+) sign to add another set of filters.

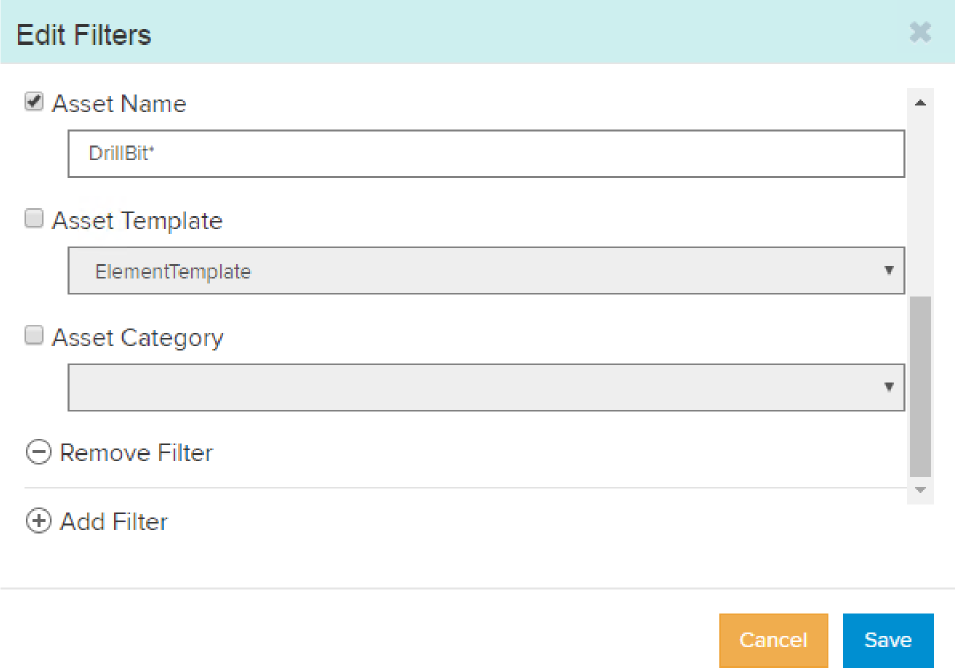
Note:

Use the scroll bar to scroll down and see any additional filters.

Each filter consists of a set of Asset Name, Asset Template, Asset Category conditions that function as AND conditions. Each selected condition in the filter must match to qualify an asset as a match.

If there are two or more filters, then the conditions of either filter need to be met to qualify an asset as a match.

Returning back to the example, a second set of filters is added and the Asset Name condition is set to DrillBit*.



Edit Filters

☑ Asset Name

DrillBit*

□ Asset Template

ElementTemplate

□ Asset Category

Second filter in asset view

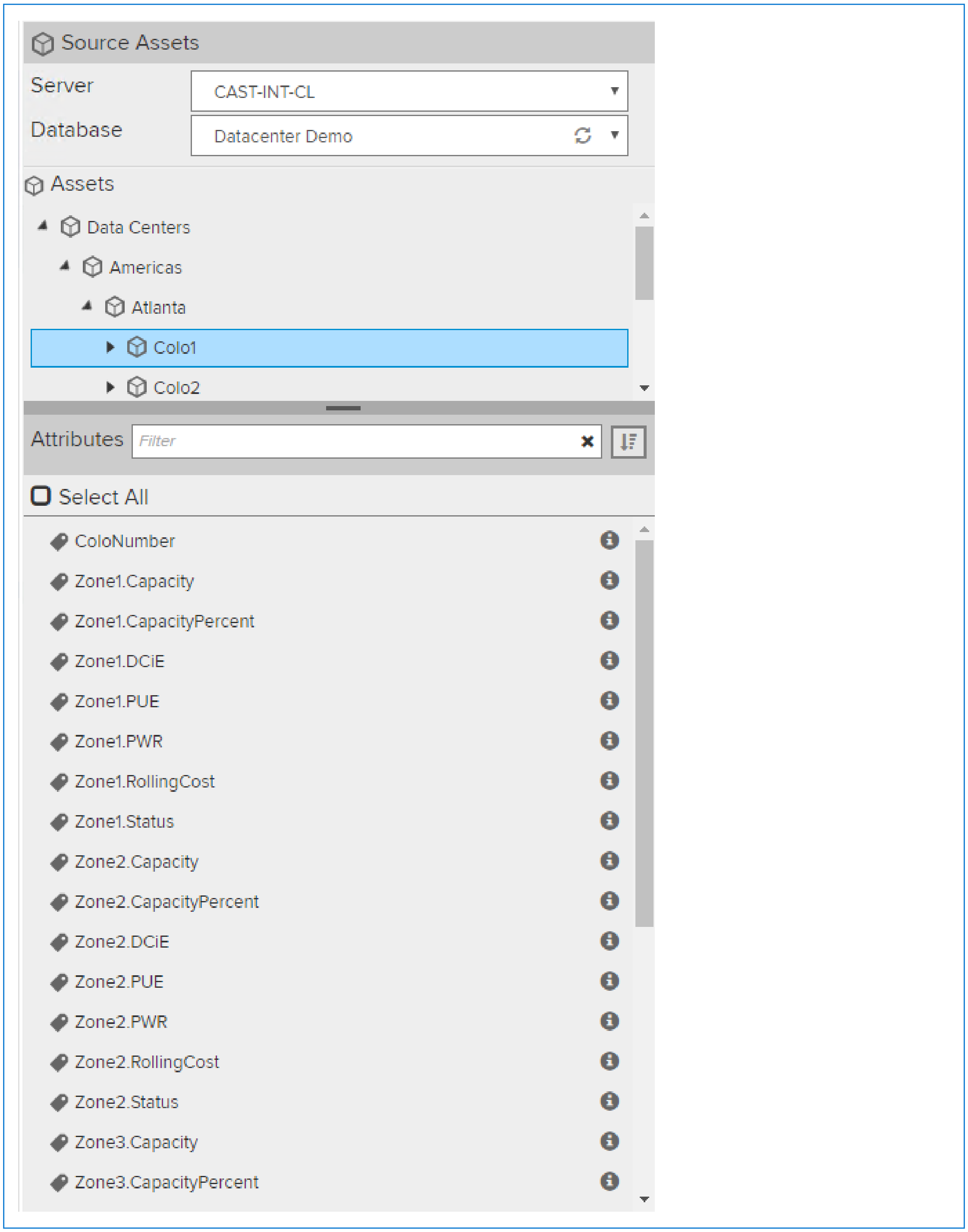
The PI Integrator Framework service searches the PI AF server:

- Using the first filter, it looks for any asset whose name is *MS301:Anne North:T1* and is based on the MS Transformer template.
- Using the second filter, it looks for any asset whose name begins with *DrillBit.*

The search returns any assets that meet *either* of these conditions. Therefore, multiple filters function as an OR filter.

Group results using wildcard groups

There are situations where grouping shape elements or attributes may be desirable, for example, there is a pattern to the Name attribute of several attributes and you want to produce a table with one column for each attribute type in the output table. In the following example, there are three Zone1 attributes: Zone1.Capacity, Zone1.PWR (Power), and Zone1.RollingCost. These attributes (Capacity, PWR, and RollingCost) are also shared by Zone2, Zone3, and Zone4. (For example, the Zone2 attributes are Zone2.Capacity, Zone2.PWR, and Zone2.RollingCost.) You want to compare these attributes by zones. The following screen shot is a partial view of this PI AF structure.



Source Assets

Server: CAST-INT-CL

Database: Datacenter Demo

Assets

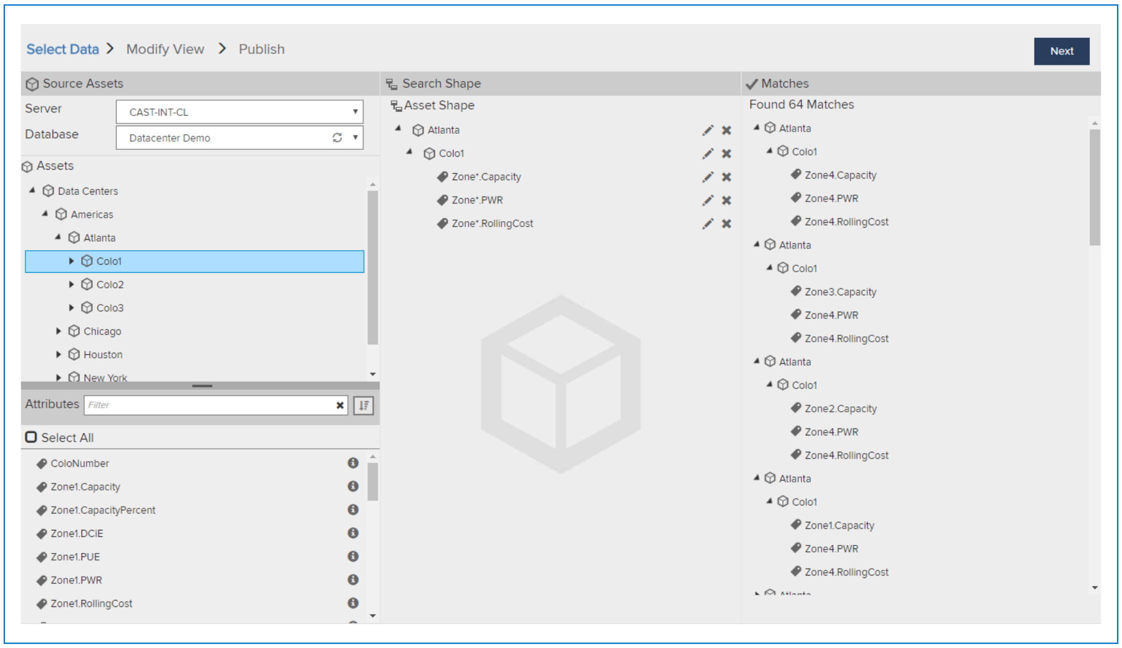
- Data Centers
  - Americas
    - Atlanta
      - Colo1
      - Colo2

Attributes: Filter

□ Select All

- ColoNumber
- Zone1.Capacity
- Zone1.CapacityPercent
- Zone1.DCiE
- Zone1.PUE
- Zone1.PWR
- Zone1.RollingCost
- Zone1.Status
- Zone2.Capacity
- Zone2.CapacityPercent
- Zone2.DCiE
- Zone2.PUE
- Zone2.PWR
- Zone2.RollingCost
- Zone2.Status
- Zone3.Capacity
- Zone3.CapacityPercent

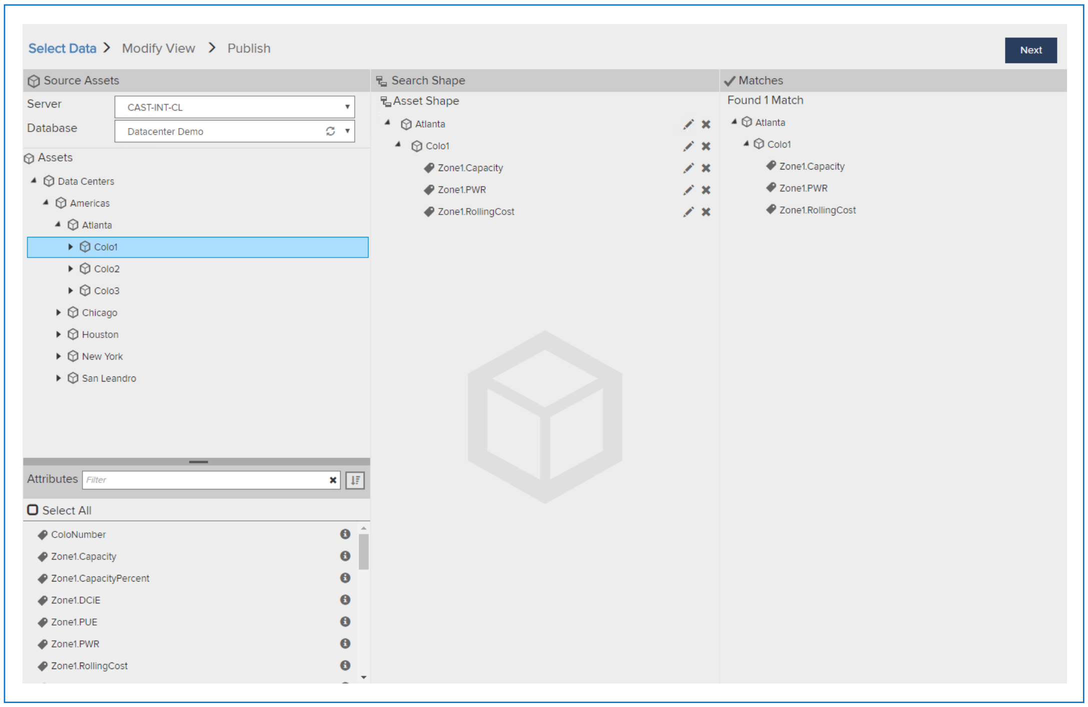
If you used a simple wildcard, you would get the following result with 64 matches. While some combinations are logical (for example, the Zone4 attributes grouped together, there are other combinations with a mix of different zones which is not the desired result.



In this instance, you want to generate a data set with one column for each attribute rather than 12 columns (three for each of the four zones). You can add wildcard groups to the attributes in the Asset Shape tree to get the desired results. The following procedure and example illustrate the concept of a wildcard group and how it can be used.

Procedure

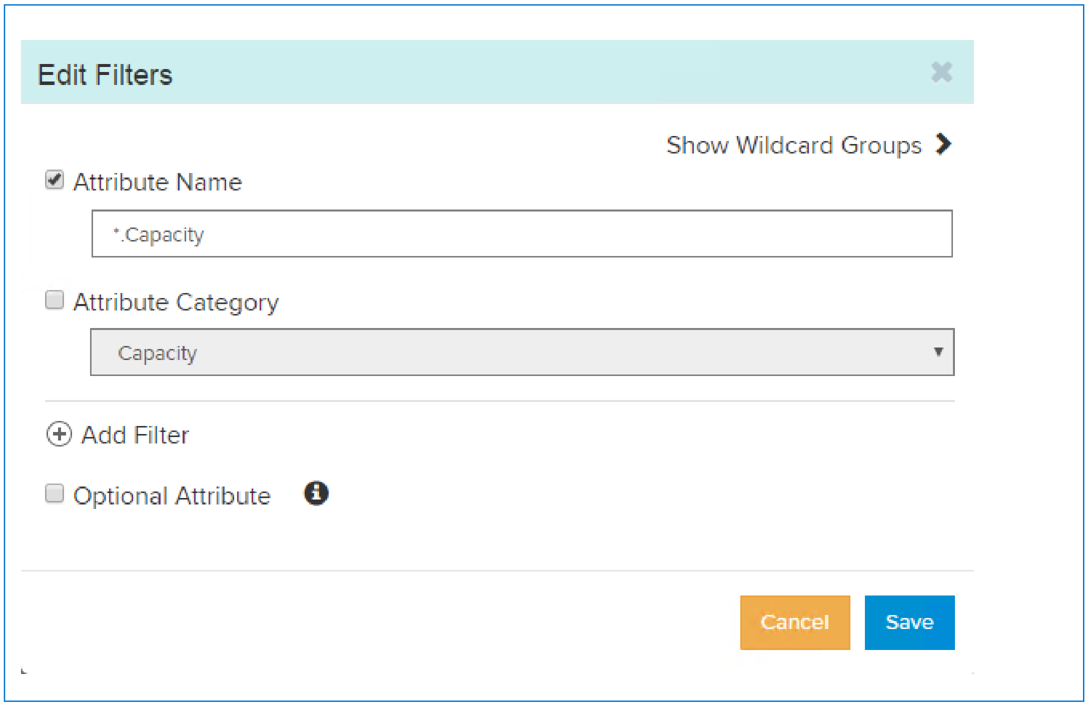
1. Create a shape with the asset and one set of the attributes you are interested in.



2. Click ✏ next to the first attribute (`Zone1.Capacity`).

3. In the Edit Filters dialog box, replace the string on which you are grouping the results with an asterisk.

   In this example, you would replace *Zone 1* with an asterisk (*).

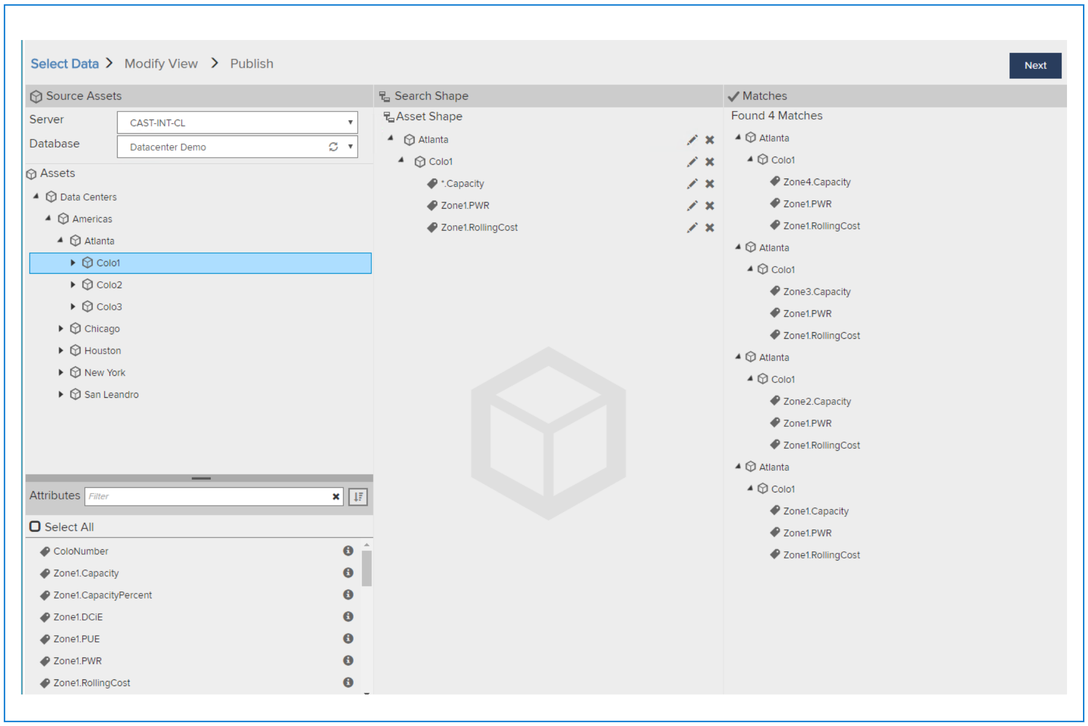


☑ Attribute Name: *.Capacity

☐ Attribute Category: Capacity

☐ Optional Attribute

4. Click **Save**. This produces the following matches. One match groups the attributes of the same zone (Zone1), but the remaining three matches group attributes for different zones.



Server: CAST-INT-CL

Database: Datacenter Demo

Assets
- Data Centers
  - Americas
    - Atlanta
      - Colo1
      - Colo2
      - Colo3
    - Chicago
    - Houston
    - New York
    - San Leandro

Attributes
- ColoNumber
- Zone1.Capacity
- Zone1.CapacityPercent
- Zone1.DCiE
- Zone1.PUE
- Zone1.PWR
- Zone1.RollingCost

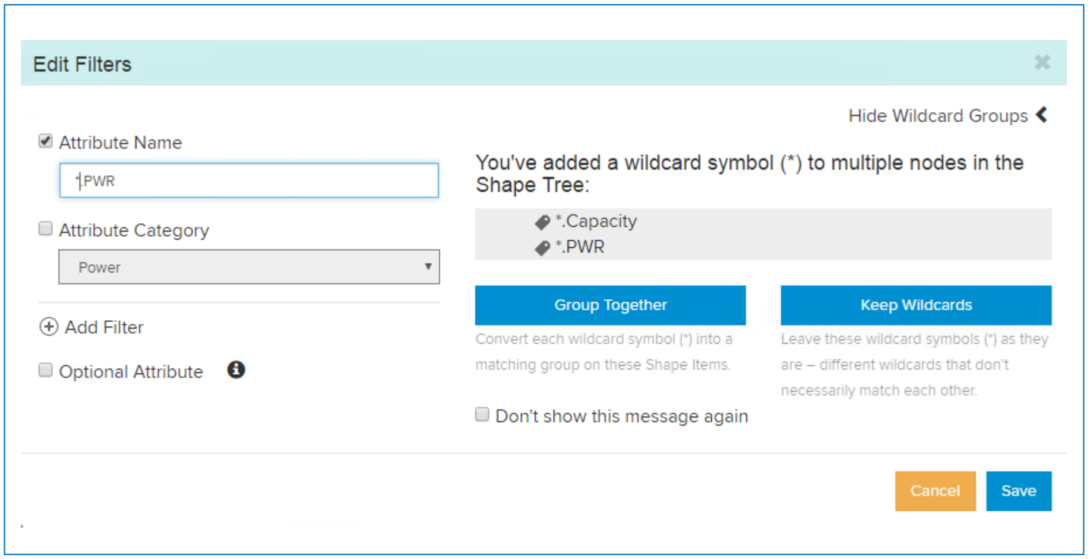
Asset Shape
- Atlanta
  - Colo1
    - *.Capacity
    - Zone1.PWR
    - Zone1.RollingCost

Found 4 Matches
- Atlanta
  - Colo1
    - Zone4.Capacity
    - Zone1.PWR
    - Zone1.RollingCost
- Atlanta
  - Colo1
    - Zone3.Capacity
    - Zone1.PWR
    - Zone1.RollingCost
- Atlanta
  - Colo1
    - Zone2.Capacity
    - Zone1.PWR
    - Zone1.RollingCost
- Atlanta
  - Colo1
    - Zone1.Capacity
    - Zone1.PWR
    - Zone1.RollingCost

5. Click ✎ next to the second attribute (`Zone1.PWR`).

6. In the Edit Filters dialog box, replace the same string (*Zone1*) with an asterisk.

   The Edit Filters dialog box displays the following:



Edit Filters

Hide Wildcard Groups

☑ Attribute Name

*PWR

□ Attribute Category

Power

You've added a wildcard symbol (*) to multiple nodes in the Shape Tree:

*.Capacity
*.PWR

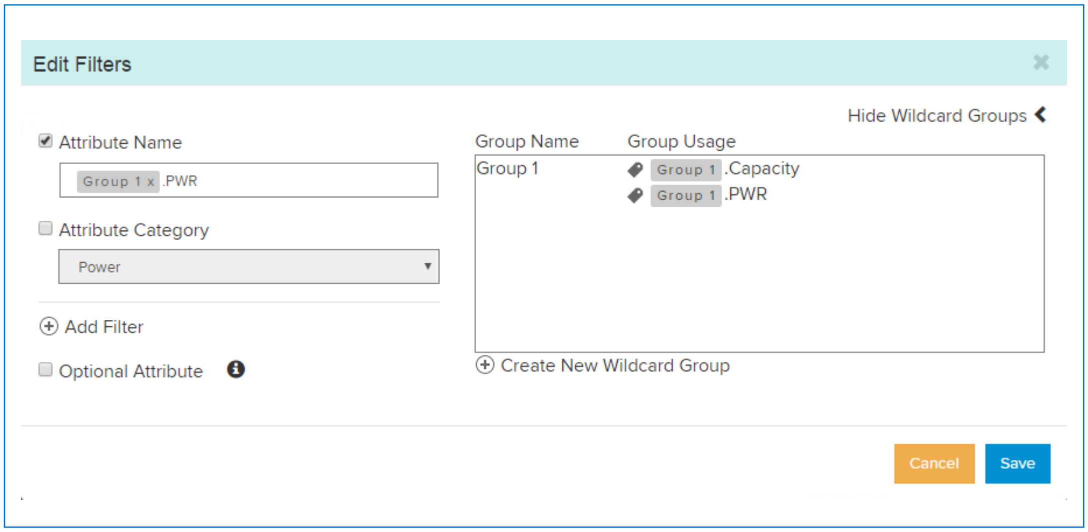
Convert each wildcard symbol (*) into a matching group on these Shape Items.

Leave these wildcard symbols (*) as they are – different wildcards that don't necessarily match each other.

□ Don't show this message again

7. Click **Group Together.**

   In the Edit Filters dialog box, the asterisk is replaced with *Group 1*. The right pane shows the attributes included in Group 1 (`Group1.Capacity` and `Group1.PWR`).



Edit Filters

Hide Wildcard Groups

☑ Attribute Name

Group 1 x .PWR

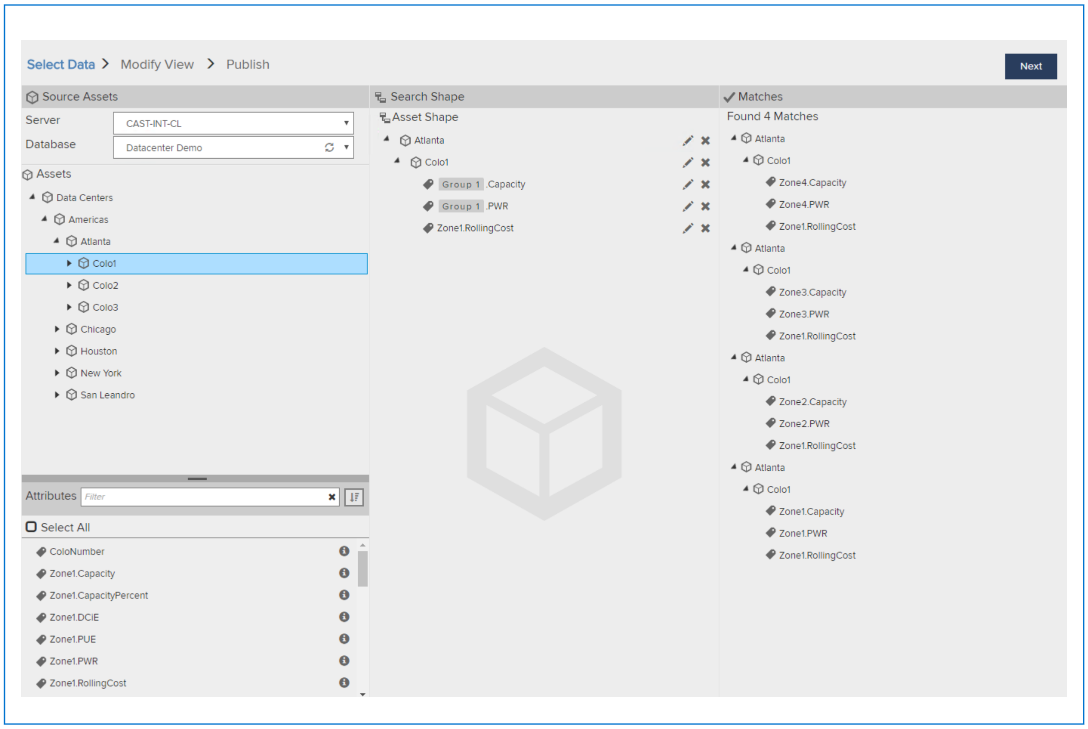
□ Attribute Category

Power

Group Name	Group Usage
Group 1	Group 1 .Capacity Group 1 .PWR

8. Click **Save.**

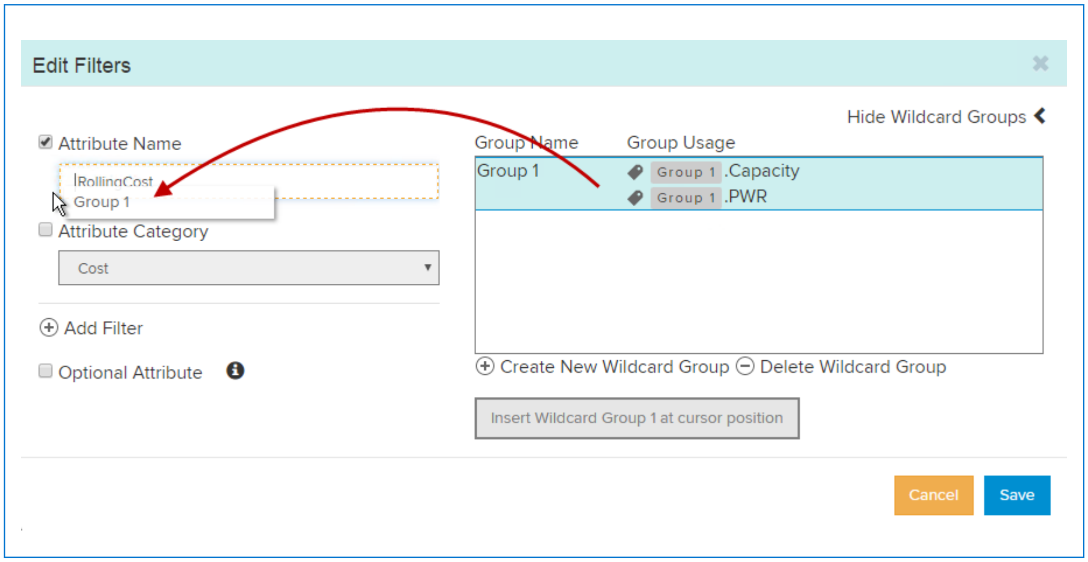
   Both attributes in the asset shape are displayed with the Group 1 wildcard.



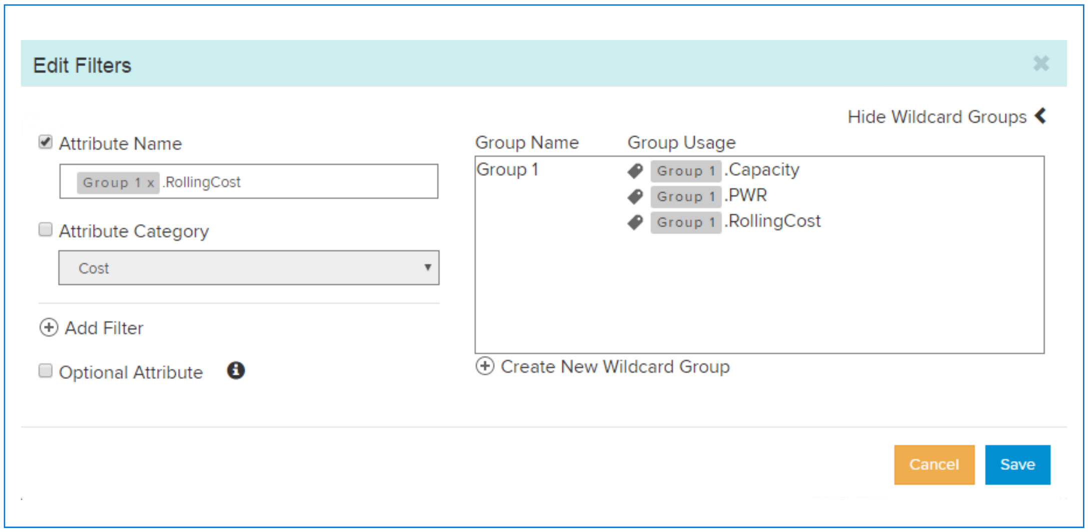
9. Click ✎ next to the third attribute (`Zone1.RollingCost`).

10. Delete the shared string (*Zone1*).

11. Click on **Group 1** in the right pane, drag it into the **Attribute Name** field.



The following screen shot shows the three attributes with the Group 1 wildcard.



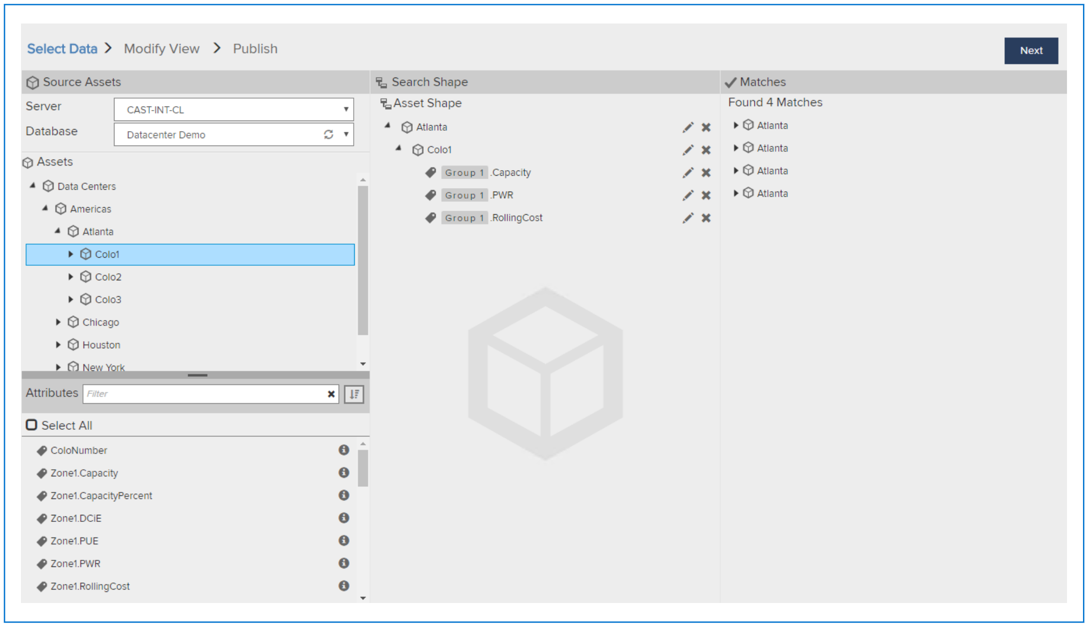
☑ Attribute Name: Group 1 x .RollingCost

☐ Attribute Category: Cost

☐ Optional Attribute

Group Name	Group Usage
Group 1	Group 1 .Capacity Group 1 .PWR Group 1 .RollingCost

12. Click **Save.**



Server: CAST-INT-CL

Database: Datacenter Demo

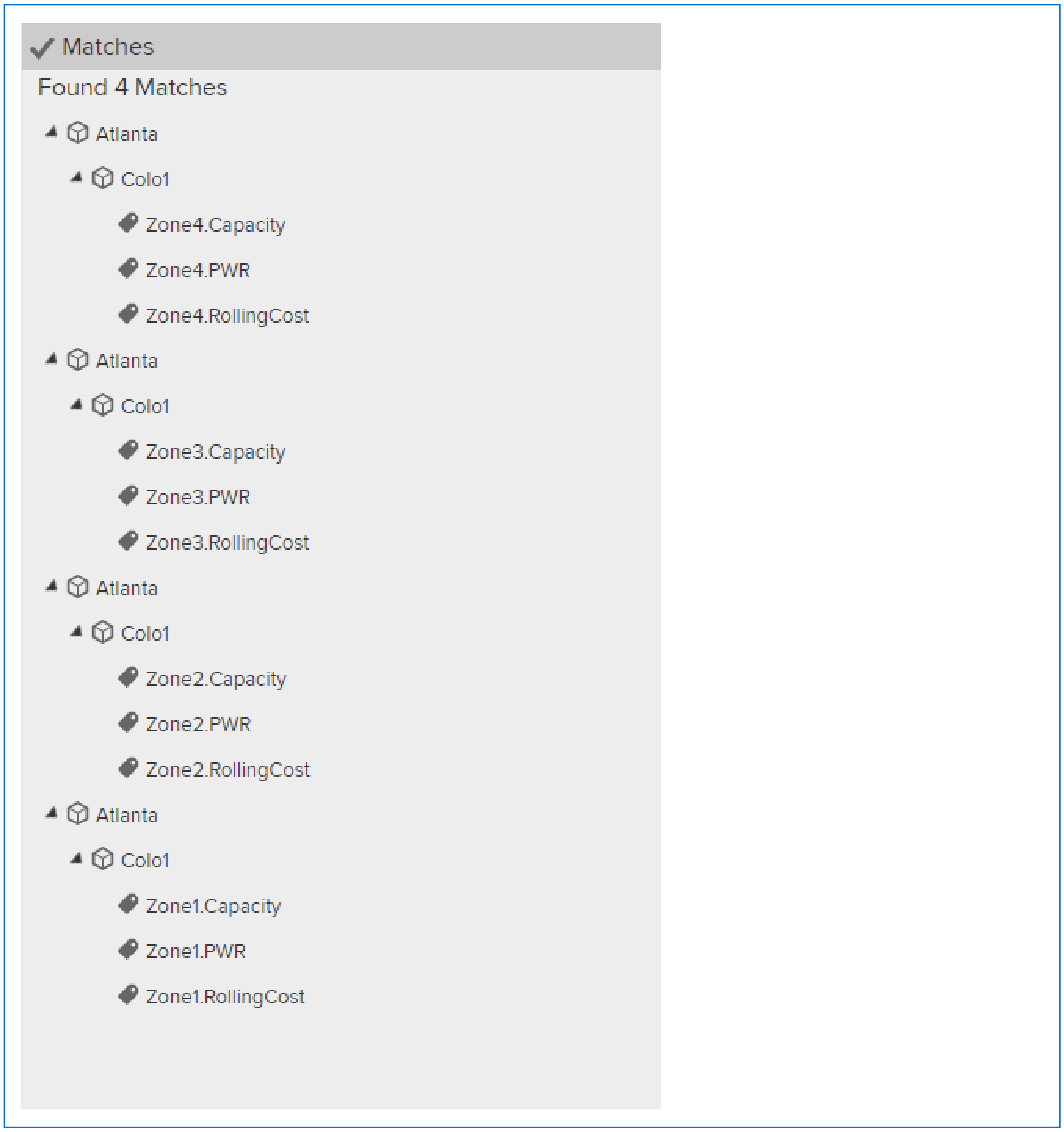
Assets: Data Centers > Americas > Atlanta > Colo1, Colo2, Colo3; Chicago; Houston; New York

Attributes: ColoNumber, Zone1.Capacity, Zone1.CapacityPercent, Zone1.DCiE, Zone1.PUE, Zone1.PWR, Zone1.RollingCost

Asset Shape: Atlanta > Colo1 > Group 1 .Capacity, Group 1 .PWR, Group 1 .RollingCost

Found 4 Matches: Atlanta, Atlanta, Atlanta, Atlanta

Using the group wildcard, the four matches show the Zone1, Zone2, Zone3, and Zone4 attributes grouped together.



✓ Matches

Found 4 Matches

- Atlanta
  - Colo1
    - Zone4.Capacity
    - Zone4.PWR
    - Zone4.RollingCost
- Atlanta
  - Colo1
    - Zone3.Capacity
    - Zone3.PWR
    - Zone3.RollingCost
- Atlanta
  - Colo1
    - Zone2.Capacity
    - Zone2.PWR
    - Zone2.RollingCost
- Atlanta
  - Colo1
    - Zone1.Capacity
    - Zone1.PWR
    - Zone1.RollingCost

Modify the data in your asset and event views

> **Note:**
> You can make changes to a published view. For more information on modifying a published view, see Modify a view

Before publishing a view, you can refine your data results, including:

- Changing how your data is retrieved

  You can adjust the sampling interval or you can choose to use a key column to organize the data in the view. See Data retrieval options for information about the different ways data can be retrieved and which options will produce the data representations you want. For more information on how to specify the data retrieval method in your views, see Adjust how values are retrieved.

- Adding data columns that display attribute information

For more information, see Add a data column.

- Adding a time column that displays your time data in a different format

  For more information, see Add a time column.

- Modifying a column

  For more information, see Modify a column.

- Filtering the data in a view

  For more information, see Filter the data.

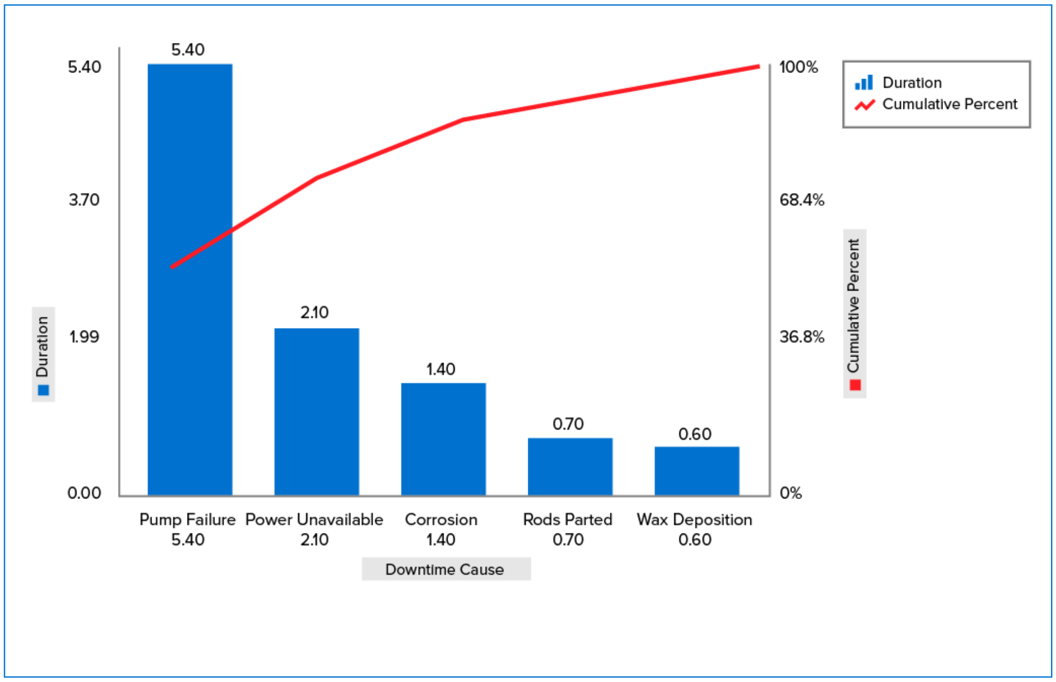
Data retrieval options

You can control how data is retrieved within your view by adjusting the sampling interval or organizing the data based on an attribute as a key column.

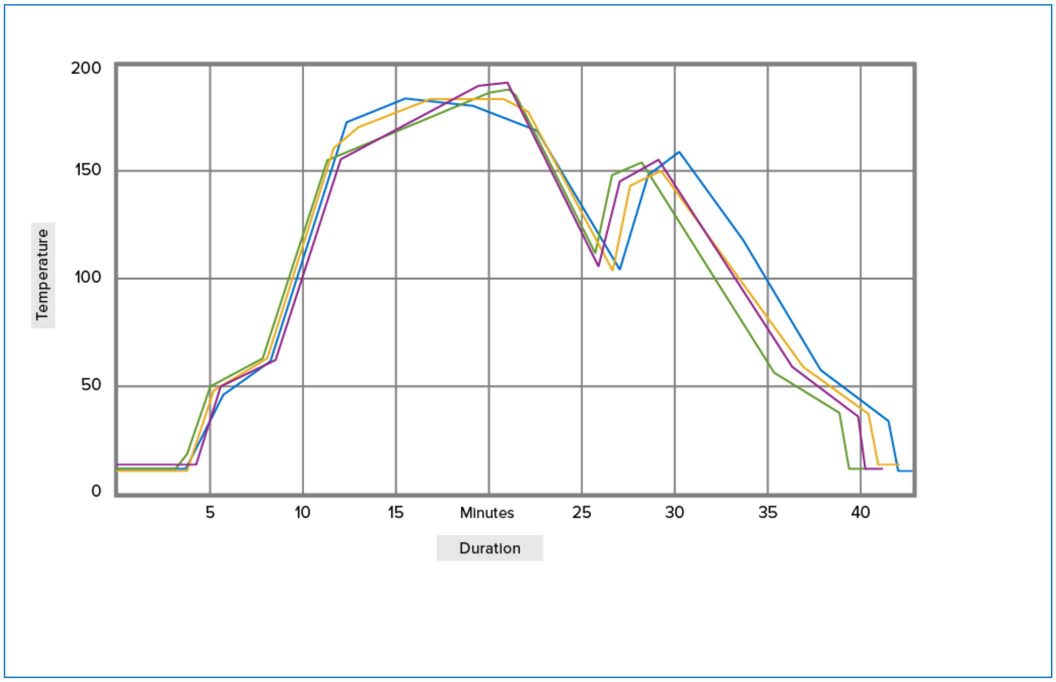
- In an asset view, data is retrieved in one of the following ways:
  - Evenly spaced in time (also known as interpolated)
  - Based on a reference attribute time (also known as compressed)

    Time stamps are taken from the reference attribute; depending on the option you choose, all others are either interpolated or given a null value if there is no value for that attribute at the exact timestamp.
- In an event view, data is aligned by event frames and is formatted in one of the following ways:
  - One summary record for each event. This is ideal for Pareto charts.

    A Pareto chart shows both bars and a line. Individual values are represented by bars, with longest bars on the left. The running total is represented by the line.



- Evenly spaced or based on a key column in time within event frames. This is useful for golden batch analysis.



Adjust how values are retrieved

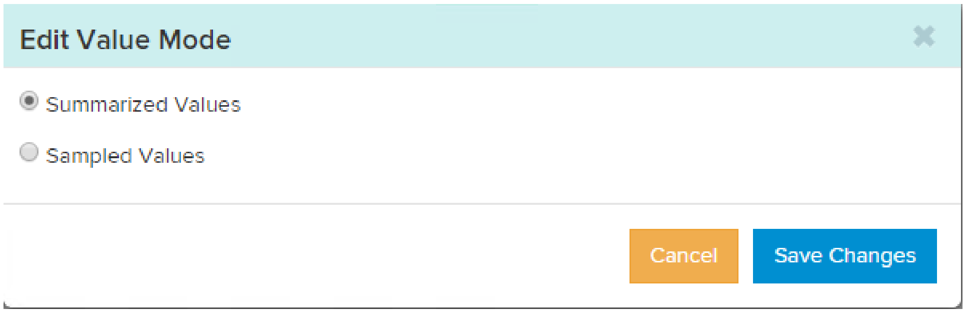
Procedure

1. On the My Views page, select the view you want to modify and click **Modify View.** Then click **Next** to open the Modify View page.

Note:
If you are already on the Modify View page, skip to the next step.

2. Click **Edit Value Mode** and choose how you want your data reported:

   - (Event views only) **Summarized Values** returns one row per event frame within the overall time frame specified for the event view. Use this option to generate results that can be displayed in a Pareto chart. The **Summarized Values** option only appears if you are modifying an event view.



Edit Value Mode

● Summarized Values

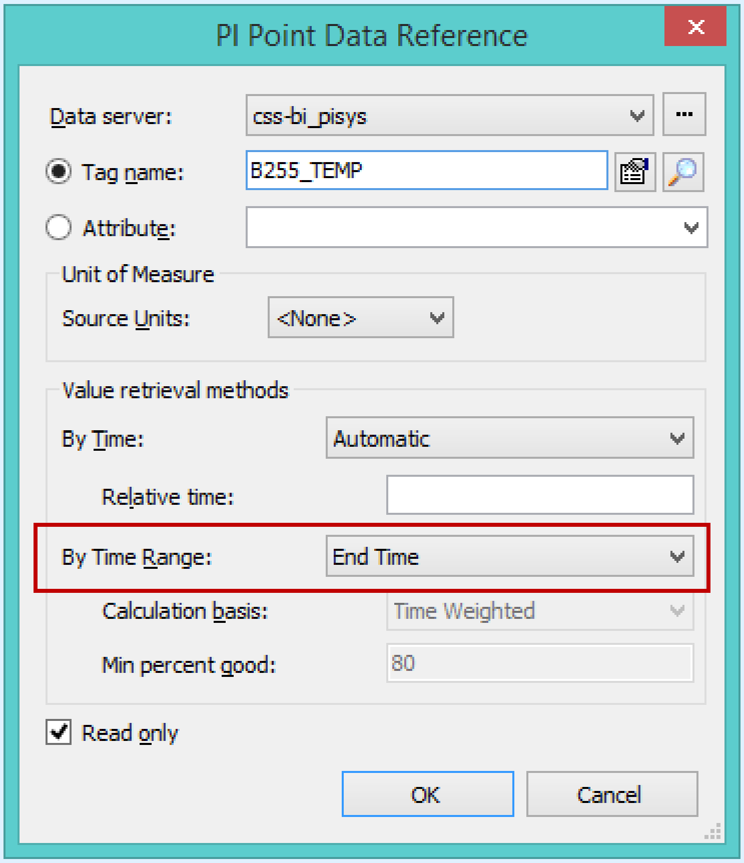
○ Sampled Values

Summarized Values

The summarized values are the event frame values you see in PI System Explorer. By default, this is the PI point value at the end of the event frame.

Note:

The event frame value is configured in PI System Explorer at the attribute level. The **By Time Range** parameter in the PI Point Data Reference dialog box, shown below, is where the value retrieval method is configured.



PI Point Data Reference

Data server: css-bi_pisys

● Tag name: B255_TEMP

○ Attribute:

Unit of Measure

Source Units: <None>

Value retrieval methods

By Time: Automatic

Relative time:

By Time Range: End Time

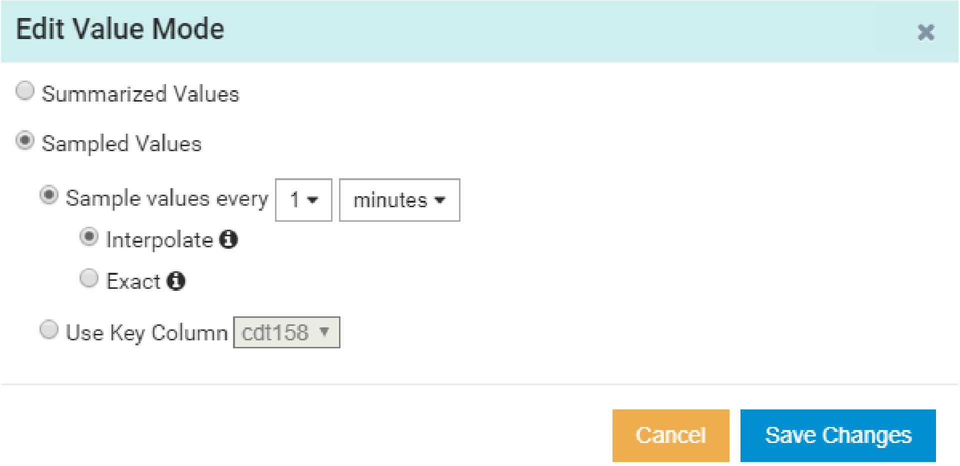
Calculation basis: Time Weighted

Min percent good: 80

☑ Read only

Note:
PI Integrator for Business Analytics does not support the **By Time** value retrieval method set to **Not Supported.** For more information, see the OSIsoft Tech Support article KB01937 - Integrator Event Frames summary calculation values are blank (https://techsupport.osisoft.com/Troubleshooting/KB/KB01937/)

- **Sample values every** changes the sampling interval so that a value is interpolated at the specified time interval, for example every 15 minutes.



Edit Value Mode

○ Summarized Values

● Sampled Values

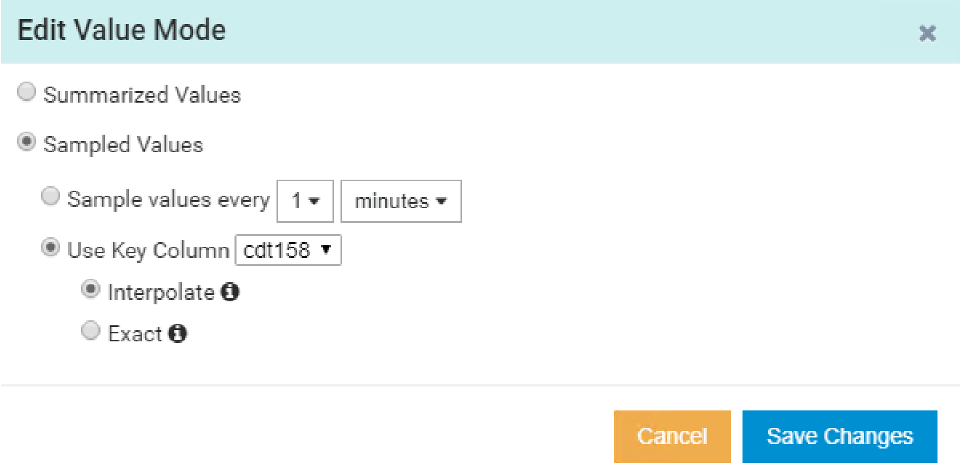
- ● Sample values every 1 minutes
  - ● Interpolate
  - ○ Exact
- ○ Use Key Column cdt158

Sample values every

Click **Sample values every** and set the time interval:

- **Interpolate** always returns a value at the specified time interval, interpolating values as needed.
- **Exact** returns values, if they exist, at the specified time interval. If no values exist, it returns a null.

◦ **Use Key Column** uses an attribute to organize how data is interpolated.



Edit Value Mode

○ Summarized Values

● Sampled Values

- ○ Sample values every 1 minutes
- ● Use Key Column cdt158
  - ● Interpolate
  - ○ Exact

Use Key Column

Choose the attribute, then choose one of the following options:

  - **Interpolate** finds the values of the key column and their recorded time stamps. The values for the other columns are interpolated at the same time stamps as the key column's time stamps.
  - **Exact** finds the values of the key column and their recorded time stamps. If a value does not exist at these recorded time stamps for the other columns, then a null value is returned.

3. Click **Save Changes**.

How summary data is calculated

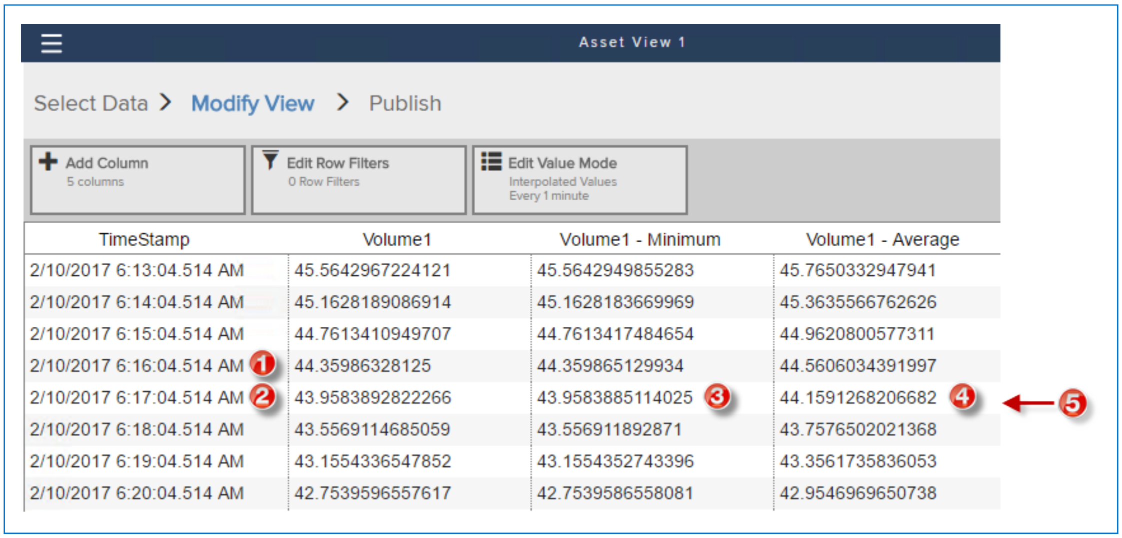
On the Modify View page, you can add a column with summary data for any numeric column in your view. The following are examples of the calculated values you can specify:

- Total – total of all values for the interval
- Average – average of all values for the interval
- Minimum – minimum value in the interval
- Maximum – maximum value in the interval
- Range – maximum value in the interval minus the minimum value in the interval

The interval is determined using time stamps in the view:

- Start time is the time stamp of the previous row
- End time is the time stamp of the current row

The screen shot and table below illustrate the relationship between the time stamps and the calculated values. In this example, two columns were added, **Volume 1 - Minimum** and **Volume 1 - Average.** Both are based on the **Volume 1** column. The current row is the row whose time stamp marks the end of the time interval. The time stamp of the previous row marks the beginning of the time interval. **Volume 1 - Minimum** takes all the data values between these two times, finds the minimum value, and populates the **Volume 1 - Minimum** column for the current row (that is, the row of the end time). Similarly, it calculates the value for **Volume 1 - Average** column by averaging the Volume 1 values between the start time and end time and populates the **Volume 1 - Average** column for the current row.



TimeStamp	Volume1	Volume1 - Minimum	Volume1 - Average
2/10/2017 6:13:04.514 AM	45.5642967224121	45.5642949855283	45.7650332947941
2/10/2017 6:14:04.514 AM	45.1628189086914	45.1628183669969	45.3635566762626
2/10/2017 6:15:04.514 AM	44.7613410949707	44.7613417484654	44.9620800577311
2/10/2017 6:16:04.514 AM	44.35986328125	44.359865129934	44.5606034391997
2/10/2017 6:17:04.514 AM	43.9583892822266	43.9583885114025	44.1591268206682
2/10/2017 6:18:04.514 AM	43.5569114685059	43.556911892871	43.7576502021368
2/10/2017 6:19:04.514 AM	43.1554336547852	43.1554352743396	43.3561735836053
2/10/2017 6:20:04.514 AM	42.7539596557617	42.7539586558081	42.9546969650738

Number	Description
1	Start time of the interval
2	End time of the interval
3	Minimum volume in the interval between the start and end times
4	Average of the volumes in the interval between the start and end times
5	Current row

For information on how to add a column of summary data, see Add a data column.

Add a data column

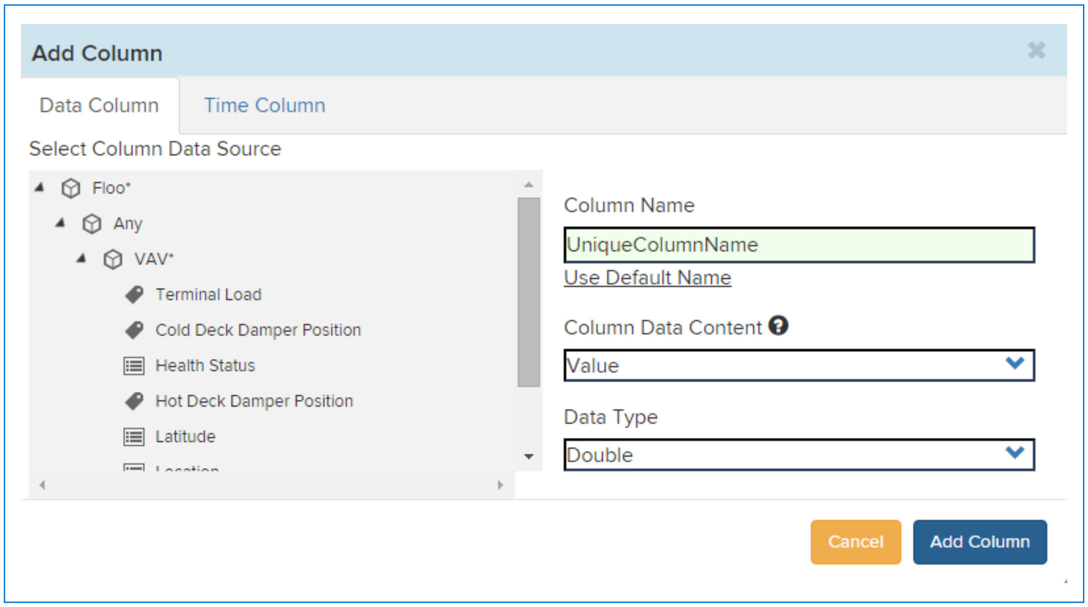
You can add data columns with attribute information.

Procedure

1. On the My Views page, select the view you want to modify and click **Modify View**. Then click **Next** to open the Modify View page.

   > **Note:**
   > If you are already on the Modify View page, skip to the next step.

2. Click **Add Column**.
3. Click the **Data Column** tab and select the attribute that is the data source.



Column Name: UniqueColumnName

Column Data Content: Value

Data Type: Double

4. Give the column a unique name.
5. Set a calculation (for example, an average) on the attributes in the **Column Data Content** field.

   > **Note:**
   > The `Last Recorded Value` function is used with data that should not be interpolated, for example, a status attribute that is either on or off. `Last Recorded Value` looks back in time and returns the most recent value of the change in the status attribute.

6. (Optional) Change the data type in the **Data Type** field.
7. Click **Add Column.**

Add a time column

Use **Time Column** to display additional time information to your views.

> **Note:**
> Some steps vary depending on whether you are creating an asset view or an event view. Where the procedure varies, the step is noted with the type of view to which it applies.

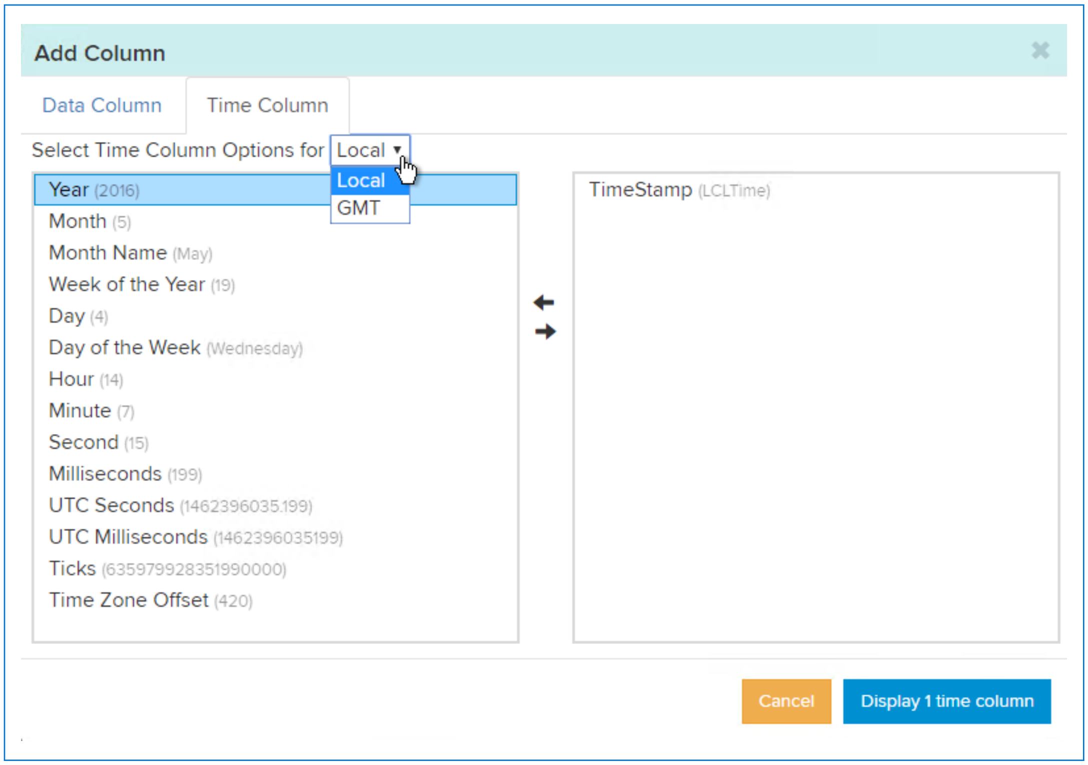
Procedure

1. On the My Views page, select the view you want to modify and click **Modify View.** Then click **Next** to open the Modify View page.

   > **Note:**
   > If you are already on the Modify View page, skip to the next step.

2. Click **Add Column.**
3. (Asset Views) Click the **Time Column** tab.

   Use **Time Column** to add columns that display your time stamp data in a different format.



a. From the **Select Time Column Options for** list, select either local time or Greenwich Mean Time (GMT).

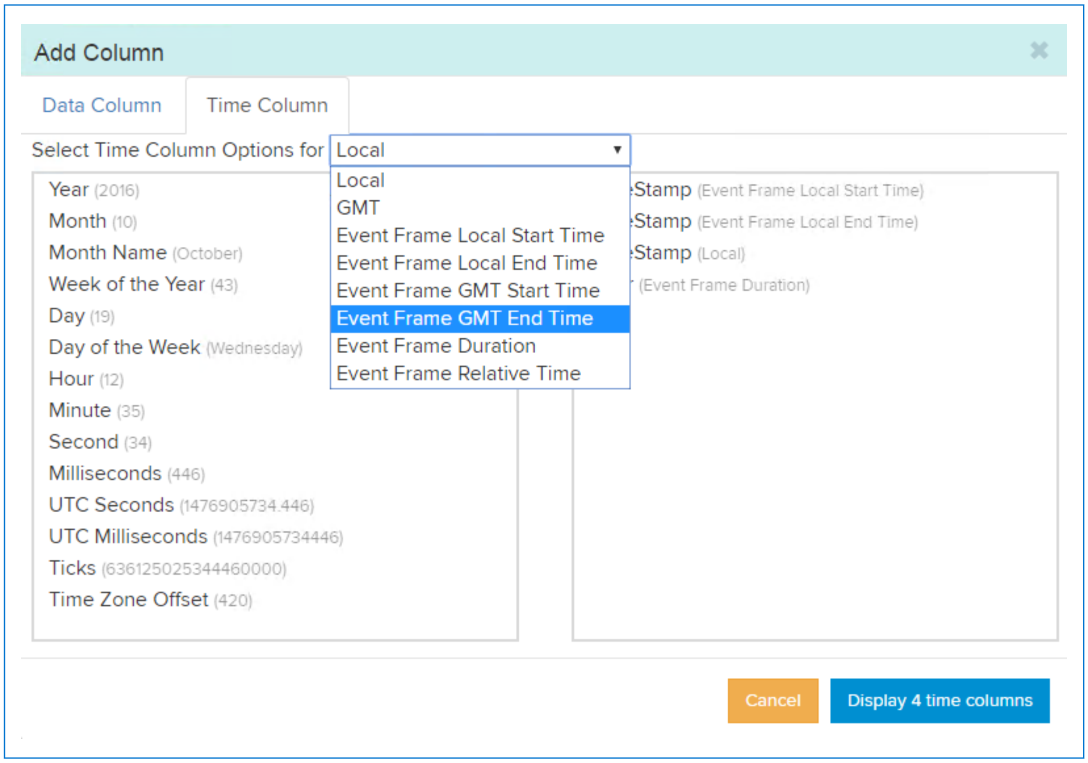
   For example, if you choose **Hour** and **GMT**, this adds a column to your view that displays only the hour of your PI point in GMT time.

b. Select a unit of time in the left column and click the right arrow.

c. When you are finished, click the **Display time column** button.

4. (Event Views) Click the **Time Column** tab.

   The **Select Time Column Options for** list displays the different time-related data that you can display in the event view, including the event frame start time and end time. You can display this time in either local time of the computer running the PI Integrator Framework service or Greenwich Mean Time (GMT).


Add Column
Data Column
Time Column
Select Time Column Options for
Local
Local
GMT
Event Frame Local Start Time
Event Frame Local End Time
Event Frame GMT Start Time
Event Frame GMT End Time
Event Frame Duration
Event Frame Relative Time
Year (2016)
Month (10)
Month Name (October)
Week of the Year (43)
Day (19)
Day of the Week (Wednesday)
Hour (12)
Minute (35)
Second (34)
Milliseconds (446)
UTC Seconds (1476905734.446)
UTC Milliseconds (1476905734446)
Ticks (636125025344460000)
Time Zone Offset (420)
Stamp (Event Frame Local Start Time)
Stamp (Event Frame Local End Time)
Stamp (Local)
(Event Frame Duration)
Cancel
Display 4 time columns

a. From the **Select Time Column Options for** list, select the data you want displayed in your view.

The following table describes the different times that can be displayed in your view.

List Options	Description
Local	When you use sampled values, time stamp of the data in local time. When you use summarized values, this time is Event Frame Local End Time.
GMT	When you use sampled values, time stamp of the data in GMT time. When you use summarized values, this time is Event Frame GMT End Time.
Event Frame Local Start Time	Start time of the event frame in local time.
Event Frame Local End Time	End time of the event frame in local time.
Event Frame GMT Start Time	Start time of the event frame in GMT time.
Event Frame GMT End Time	End time of the event frame in GMT time
Event Frame Duration	Event frame end time – (minus) event frame start time.
Event Frame Relative Time	Row time – (minus) event frame start time.

b. Select the unit of time in the left column and click the right arrow.

For example, if you select **Event Frame Local Start Time** and **Hour**, this adds a column with only the hour of the event frame start time in local time format.

c. When you are finished, click the **Display time column** button.

Modify a column

You can rename a column, set a calculation such as an average on the values in the column, change the data type, change the unit of measure, or remove the column.

Procedure

1. Click on the column to open the **Column Details** panel.

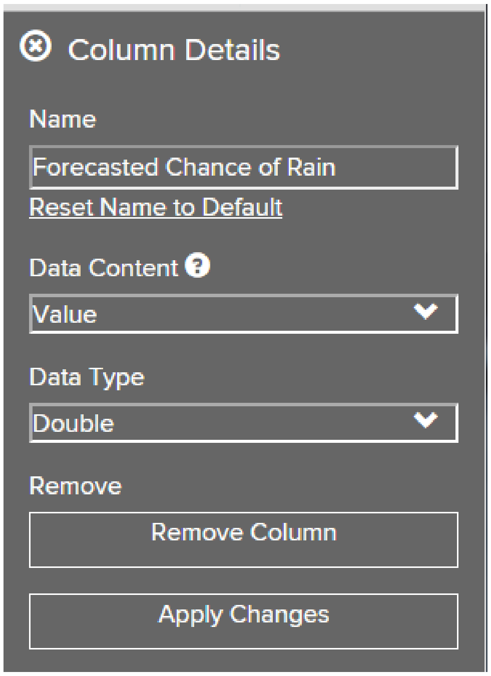
Note:

- The PI Integrator Framework reserves the case-insensitive strings, *ID*, *PIIntTSTicks*, and *PIIntShapeId*, as column names. You may use these strings to name columns in your asset and event views. However, if you do, an underscore (_) is appended to the column name in your target data, for example, *ID_* or *Id_*.

  Note:

  This restriction does not apply to the streaming publish targets: Apache Kafka, Azure Event Hubs, and Azure IoT Hub.

- Column names are reformatted based on the limitations of each target store. For example, Oracle column names are limited to 30 characters and column names longer than 30 characters are truncated.
- The Oracle database targets have reserved strings; if these strings appear in the column names, an underscore (_) is appended to the string. For a list of the reserved strings, see Reserved strings.
- Column names must be unique.
- The `Last Recorded Value` function in the **Data Content** field is used with data that should not be interpolated, for example, a status attribute that is either on or off. `Last Recorded Value` looks back in time and returns the most recent value of the change in the status attribute.



Name: Forecasted Chance of Rain

Data Content: Value

Data Type: Double

2. Make any changes to the column.
3. When you are done, click **Apply Changes**.

Filter the data

You can filter the data in a view using various parameters. For example, you can specify that you want to include rows if the column contents contain a particular numeric value or match a string pattern.

When you apply a filter, PI Integrator for Business Analytics takes the data set that matches your asset shape, joins it to the data set that matches your filter, and produces the subset of data that satisfies both criteria.

Procedure

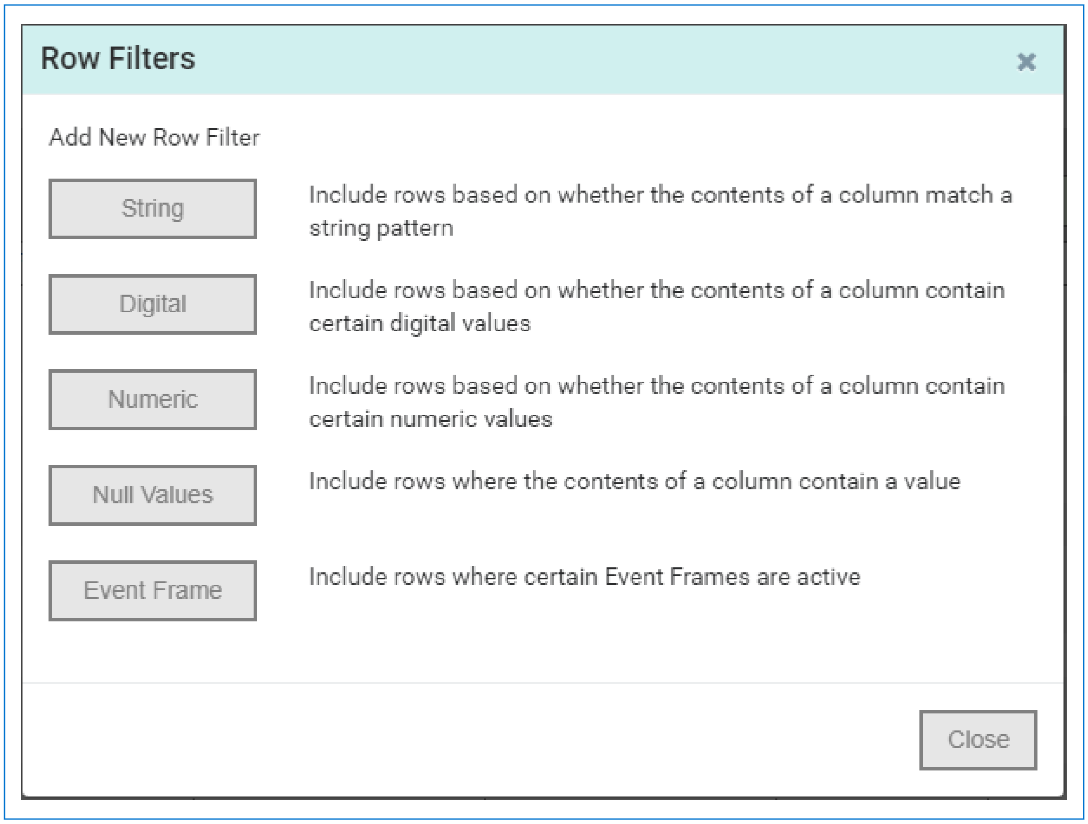
1. On the My Views page, select the view that you want to modify and click **Modify View.** Then click **Next** to open the Modify View page.

   Note:
   If you are already on the Modify View page, skip to the next step.

2. Click **Edit Row Filters** and choose the type of filter you want.

   Note:

   - The filters most often used are numeric and string filters.
   - Event frame filters only apply to asset views. Therefore, if you are creating an event view, this filter type will not appear as an option.



Row Filters

Add New Row Filter

String — Include rows based on whether the contents of a column match a string pattern

Digital — Include rows based on whether the contents of a column contain certain digital values

Numeric — Include rows based on whether the contents of a column contain certain numeric values

Null Values — Include rows where the contents of a column contain a value

Event Frame — Include rows where certain Event Frames are active

For information about applying an **Event Frame** filter, see Filter by event frames.

3. When you have finished defining the filter, click the **Save** button.
4. In the Row Filters dialog box, click **Close.**

Filter by event frames

The following procedure shows how to apply an event frame row filter to an asset view.

Note:
Filtering by event frames applies only to asset views.

When you define an asset shape, you create a collection of matches that meet the same criteria. When you apply an event frame filter to this view, you define an event shape that creates a collection of matches for a set of event frames. PI Integrator for Business Analytics then joins these two collections based on a common asset to obtain the subset of data that matches both.

For example, assume you have a number of wells where a certain piece of equipment is run one at a time at each well, and event frames are used to record the data collected by this equipment. Each event frame has a different start and end time and applies to a different well. You can use the event frame row filter to include asset view data for the well only for the period that the equipment was running on that well.

Procedure

1. On the My Views page, select the view that you want to modify and click **Modify View.** Then click **Next** to open the Modify View page.

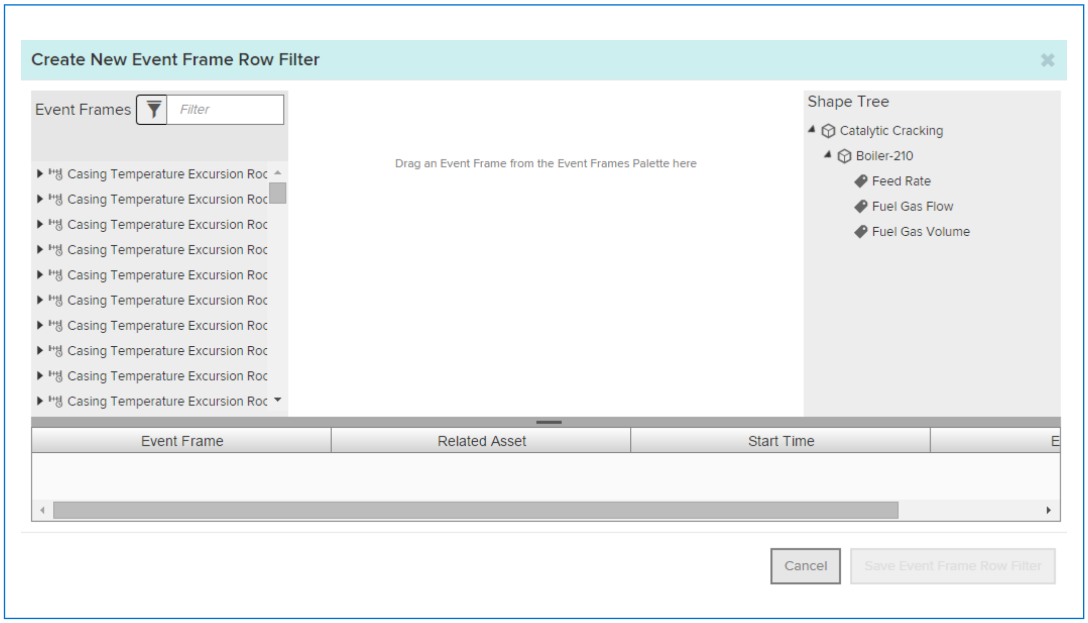
> **Note:**
> If you are already on the Modify View page, skip to the next step.

2. Use the **Start Time** and **End Time** fields to adjust the time range to include the times when the event frames of interest were recorded.

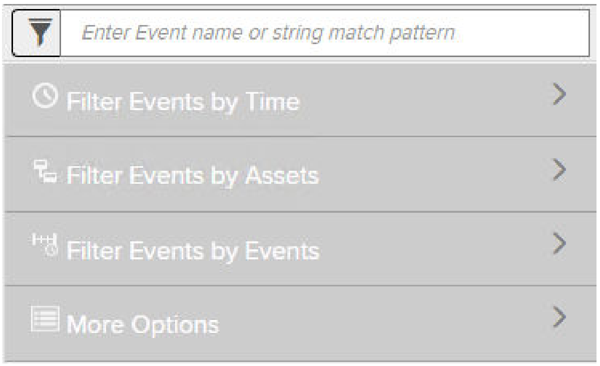
> **Note:**
> If the start and end times are outside the event frame time range, no event frames will be found.

3. Click **Edit Row Filters** and choose **Event Frame** for the type of filter.

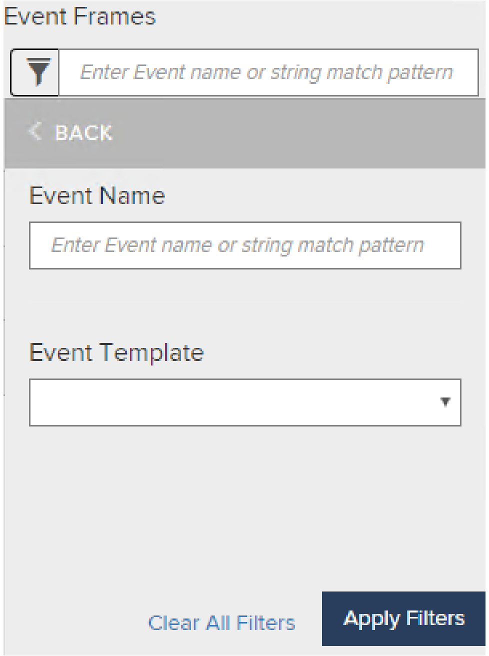
   PI Integrator for Business Analytics now searches for event frames on your PI AF database for this view and displays a subset of the ones it finds.


Create New Event Frame Row Filter
Event Frames
Filter
Casing Temperature Excursion Roc
Casing Temperature Excursion Roc
Casing Temperature Excursion Roc
Casing Temperature Excursion Roc
Casing Temperature Excursion Roc
Casing Temperature Excursion Roc
Casing Temperature Excursion Roc
Casing Temperature Excursion Roc
Casing Temperature Excursion Roc
Casing Temperature Excursion Roc
Drag an Event Frame from the Event Frames Palette here
Shape Tree
Catalytic Cracking
Boiler-210
Feed Rate
Fuel Gas Flow
Fuel Gas Volume
Event Frame
Related Asset
Start Time
E
Cancel
Save Event Frame Row Filter

4. Click the ▼ icon to open the menu. Click the right-angle bracket (>) on one of the filtering categories to open the related panel.

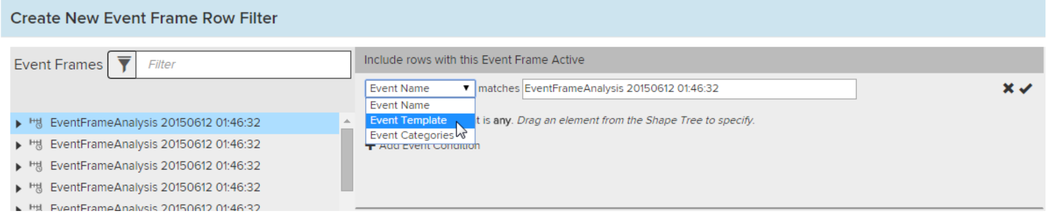


   In the filtering fields, specify parameters to narrow down the event frames to find the ones you are looking for. For example, enter a pattern-matching string in the **Event Name** field or select a template in **Event Template.**


Event Frames
Enter Event name or string match pattern
BACK
Event Name
Enter Event name or string match pattern
Event Template
Clear All Filters
Apply Filters

5. Click **Apply Filters**.
6. From the event frames found, drag an event frame to the center pane.

   The filter now includes rows for which this event frame is active.
7. Optionally, you can broaden the row filter search criteria to include all event frames with the same template or category. To do this, use the drop-down list to change the search from **Event Name** to **Event Template** or **Event Categories**.


Create New Event Frame Row Filter

Include rows with this Event Frame Active

Event Name matches EventFrameAnalysis 20150612 01:46:32

t is any. *Drag an element from the Shape Tree to specify.*

EventFrameAnalysis 20150612 01:46:32
EventFrameAnalysis 20150612 01:46:32
EventFrameAnalysis 20150612 01:46:32
EventFrameAnalysis 20150612 01:46:32
EventFrameAnalysis 20150612 01:46:32

8. Click the icon ✔ next to the event condition.

   PI Integrator for Business Analytics fetches matching event frames and shows them in the preview pane at the bottom of the window.
9. To align the event frames with the correct asset, drag the asset or attribute from the **Shape Tree** onto the filter criteria.

   This step defines the relationship between the two data sets (the event frame data set and the asset and attributes data set). This is similar to the clause in a relational table join that equates an attribute in one table (or dataset) to an attribute in the other table (dataset). Here, we are equating the asset "owning" the event frame to the asset from your **Shape Tree.**

   PI Integrator for Business Analytics updates the display of matching event frames in the preview.
10. When you have finished defining the filter, click **Save Event Frame Row Filter**.

About publishing large views

Large views with 100 or more combined elements and attributes are likely to encounter a limit with the Web Sockets transport protocol which has a maximum data packet size of 64K. Before you publish any large views, you may need to change the transport type to Server Sent Events to accommodate the larger packet sizes. This should only be required for users using the Microsoft Edge web browser.

From any page, click the gear icon ⚙ in the upper right corner and set **Transport Type** to **Server Sent Events**.

About continuously published views

Views can be published continuously on a schedule. You can republish a view in intervals as short as one minute and up to 12 months. For example, you can set up your view to republish at 12:00 am each day.

> **Note:**
>
> Continuous views run in the local time where the PI Integrator Framework service is running. Therefore, users who are in a different time zone must take this into account when scheduling their runs.

Each time the view is published, the new data is appended to the existing data. Therefore, the target table or file keeps growing each time the view is republished. There is currently no option to overwrite the data. Therefore, you must manually delete data you no longer need.

You specify the time range for the period you want updated. If there is concern about consuming too many resources, you can specify shorter time intervals and update the data by publishing multiple times.

You specify that you want your view published on a schedule on the Publish page. For more information, see Publish a view on a schedule.

On the My Views page, continuously published views have a **Run Mode** of Continuous.

PI Integrator for Business Analytics supports automatic updates of published PI System data for selected targets. For more information about this feature, see How published data gets updated.

View names and destination endpoints

When PI Integrator for Business Analytics publishes a view, the view name is used to create the name of the destination point. Each target has its own naming conventions and rules for what is an acceptable name. If a view name contains a character that is not allowed by the target, PI Integrator for Business Analytics either removes the character or replaces it with an underscore character (_).

Targets also have rules about the length of names. If the endpoint name exceeds these limits, then PI Integrator for Business Analytics displays a warning or error message.

Check the documentation for your specific target for the applicable naming conventions and length limits.

Publish a view on a schedule

You can publish a view on an ongoing schedule. On the Publish page, you can specify the frequency with which you want to publish the view. Results from each run are appended to the previous results. For more information about continuously published views, see About continuously published views.

Procedure

1. On the Publish page, select the target from the **Target Configuration** list.
2. Click **Run on a schedule.**
3. Specify the date and time of the first run.

   Note:

   Scheduled views are run in the local time of the computer running the PI Integrator Framework service. If you are in a different time zone, you may need to convert your local scheduled time to the PI Integrator Framework service time zone to get the desired result.
4. Specify the frequency of the subsequent runs.

   Note:

   You can specify a frequency as short as one minute and up to 12 months.
5. Click **Publish.**

Publish a streaming view

Before you start

Large views with 100 or more combined elements and attributes are likely to encounter a limit with the Web Sockets transport protocol which has a maximum data packet size of 64K. Before you publish any large views, change the transport type to Server Sent Events to accommodate the larger packet sizes.

On the My Views page, click the gear icon ⚙ in the upper right corner and set **Transport Type** to **Server Sent Events.**

Note:

Streaming targets can only stream 25,000 matches of the search shape. Once this limit is reached, no other matches are streamed and an error message is written to the view log file.

Procedure

1. On the Publish page, select a target from the Target Configuration list.
2. (Apache Kafka only) Select a topic to which the message is sent.

   By default, messages are sent to a topic that has the same name as the view.

   You can also choose to send messages to existing topics.

a. Click **Get Topics** to populate the list of available topics you can select from.

b. Click the arrow to display the list of topics.

3. Specify the start time for the first publishing of the view.

4. Click **Publish.**

View statistics data

The **Statistics** tab displays information about the process of publishing views. This is helpful for troubleshooting bottlenecks during the reading of data from the PI System through to the writing of the data to the target. The statistics include the time of each published run; this can be helpful with scheduling when downstream applications read the data from the target.

If you do not see the statistics for an earlier time period, PI Integrator for Business Analytics may have purged these records from the SQL Server where they are stored in order to prevent excessive disk consumption. See Set your record retention policies for more information on when these records are deleted. Use the procedure below to familiarize yourself with the information on the statistics tab.

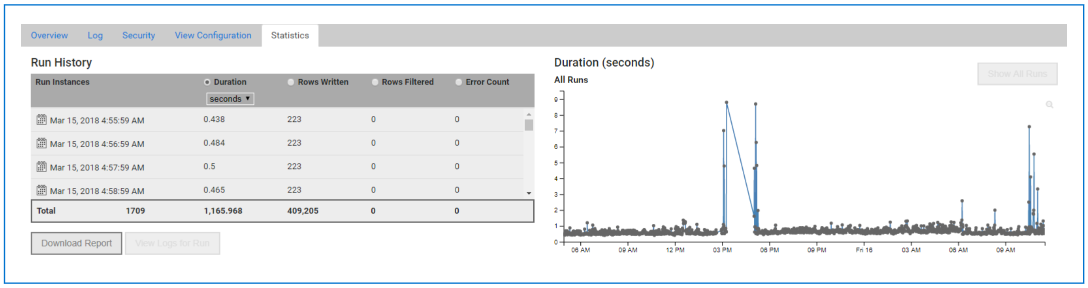
Note:

OSIsoft Technical Support uses **Enable Full Reporting** to collect extensive statistics that help troubleshoot problems with publishing views. Do not turn this feature on unless you are directed to by Technical Support. With full reporting enabled, your available disk space may be rapidly filled.

Procedure

1. In the My Views page, select the view you are interested in.

2. If the View Details pane is not open, click the button in the lower right corner to open it. Then click the **Statistics** tab. The statistics for the selected view are displayed.



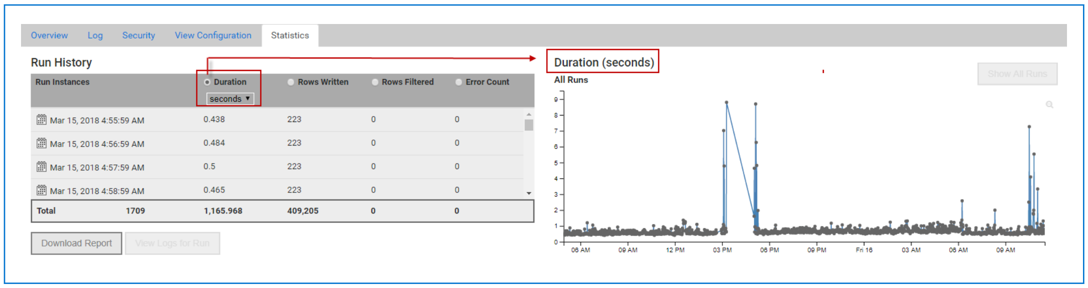
Run History

Run Instances		● Duration seconds ▾	○ Rows Written	○ Rows Filtered	○ Error Count
Mar 15, 2018 4:55:59 AM		0.438	223	0	0
Mar 15, 2018 4:56:59 AM		0.484	223	0	0
Mar 15, 2018 4:57:59 AM		0.5	223	0	0
Mar 15, 2018 4:58:59 AM		0.465	223	0	0
Total	1709	1,165.968	409,205	0	0

Duration (seconds)

All Runs

3. Click and choose one of the statistics in the table header to view the trend data.



Run History

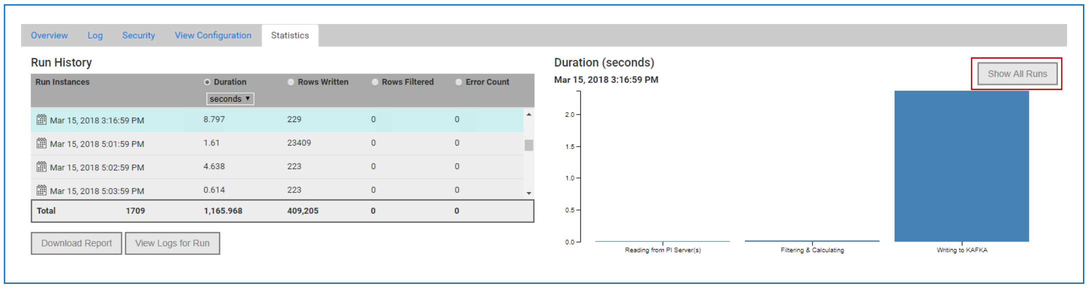
Run Instances		● Duration seconds ▾	○ Rows Written	○ Rows Filtered	○ Error Count
Mar 15, 2018 4:55:59 AM		0.438	223	0	0
Mar 15, 2018 4:56:59 AM		0.484	223	0	0
Mar 15, 2018 4:57:59 AM		0.5	223	0	0
Mar 15, 2018 4:58:59 AM		0.465	223	0	0
Total	1709	1,165.968	409,205	0	0

Duration (seconds)

All Runs

4. Click on a row in the table to view additional statistics for the selected run in the right pane.

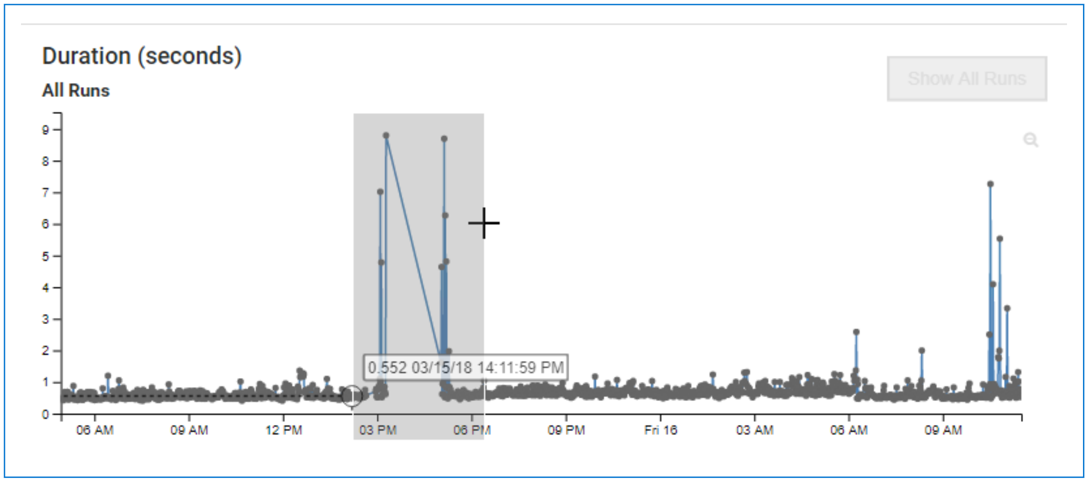
5. Click **Show All Runs** to return to the trend view.



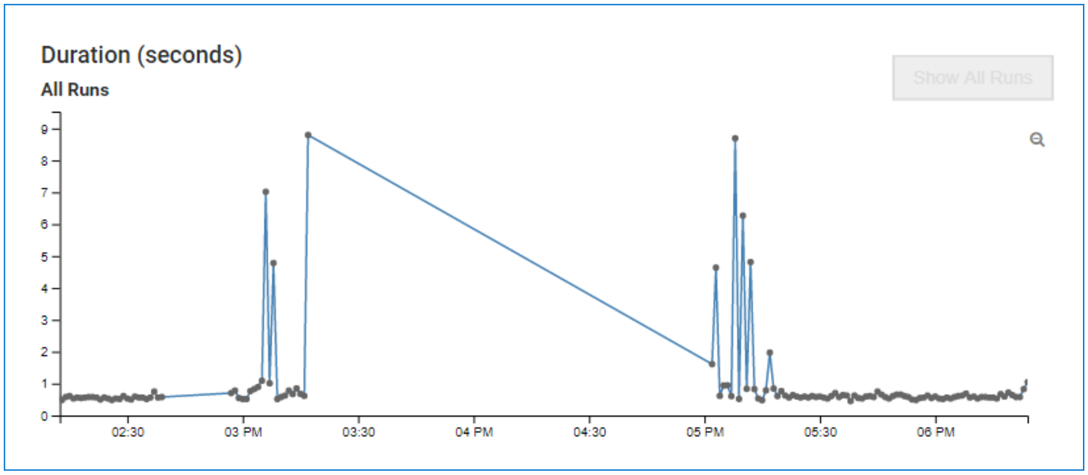
Run History

Run Instances	○ Duration (seconds ▾)	○ Rows Written	○ Rows Filtered	○ Error Count
Mar 15, 2018 3:16:59 PM	8.797	229	0	0
Mar 15, 2018 5:01:59 PM	1.61	23409	0	0
Mar 15, 2018 5:02:59 PM	4.638	223	0	0
Mar 15, 2018 5:03:59 PM	0.614	223	0	0
Total 1709	**1,165.968**	**409,205**	**0**	**0**

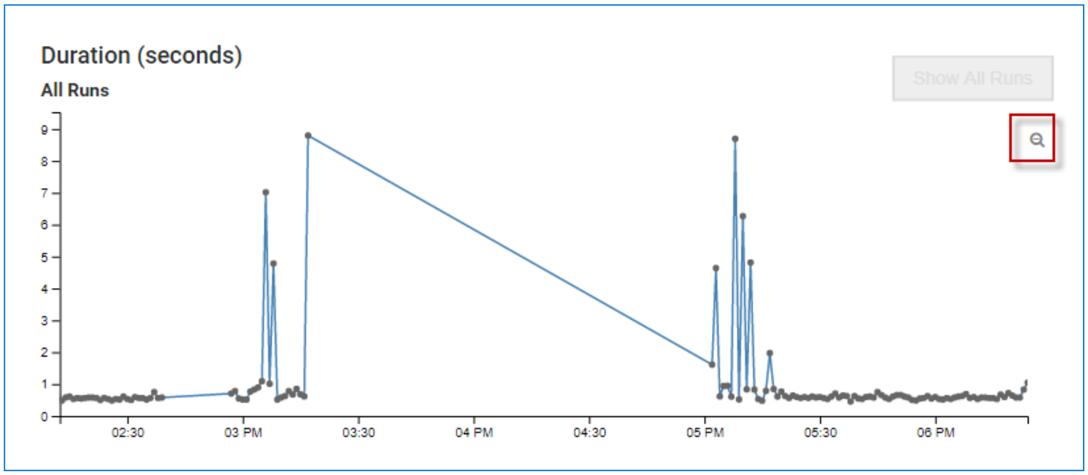
6. Select a portion of the trend graph to zoom in.



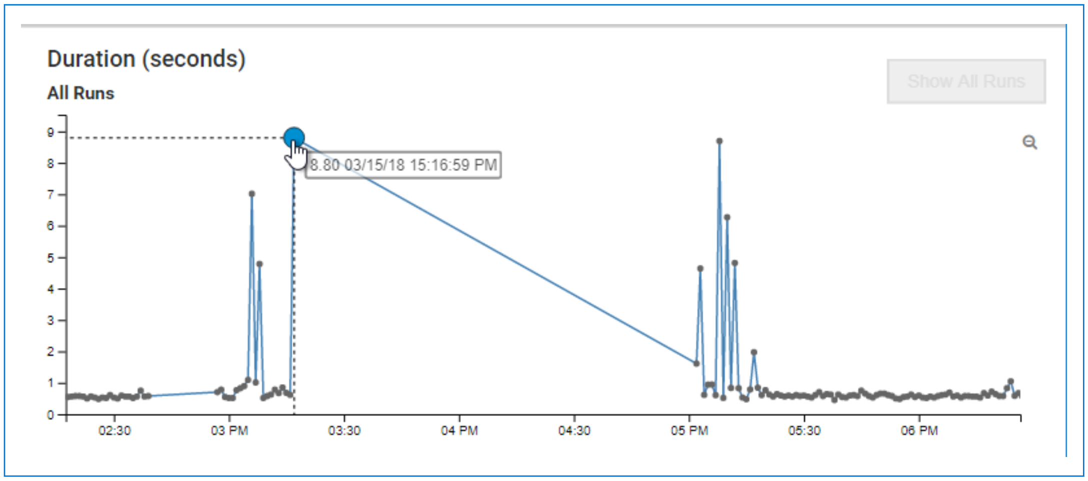
The selected area expands to fill the X-axis of the graph.



7. Click the magnifying glass to zoom out.



8. Click a node in the trend graph to see details for that run.



9. Click **View Logs for Run** to see the log records for the run. PI Integrator for Business Analytics takes you to the **Log** tab for the selected run.

How published data gets updated

PI Integrator Sync monitors assets in the PI System for asset views, scheduled streaming views, and key-value-triggered streaming views. It keeps your published data current in the following ways:

- PI Integrator Sync monitors your view shape and tracks changes to PI AF that affect the matches in your view. For example, assume you have a view of pumps and there are 10 matches. A new pump is added to PI AF that results in 11 matches of your view shape. PI Integrator Sync publishes data for the 11 matches going forward, and for asset views and scheduled streaming views, it will backfill the data for the new pump.
- PI Integrator Sync monitors changes to data in PI Data Archive and updates any published data. For example, when a data value in PI Data Archive is updated with a new value, PI Integrator Sync publishes the new value to the target.

Note:

For a definition of the different types of streaming views, see About message triggers.

PI Integrator Sync monitors and updates previously published data once every 30 minutes. Therefore, once a change occurs in PI AF or PI Data Archive, it may take up to 30 minutes for this change to be reflected in your data.

To take advantage of the PI Integrator Sync synchronization features, you must be using PI Data Archive 2017 or later.

Note:

For HDFS and file targets, PI Integrator Sync monitors changes to the shape of asset views and publishes the data for the matches going forward. However, PI Data Archive changes are not supported. Therefore, PI Integrator Sync does not backfill data for these targets or update changes to published data.

How published data is synchronized with PI AF

The following describes how published data is synchronized with PI AF when the following occurs:

- Element is added to PI AF
  - Asset views and scheduled streaming views – If an element or combination of elements and attributes is added to PI AF that results in a new match in your view, data for the new element is published going forward and data is backfilled to the original view start time.
  - Key-value-triggered streaming views – If an element or combination of elements and attributes is added to PI AF that results in a new match in your view, the data for the new element is only added going forward. Previously published data is not backfilled.
- Element is deleted from PI AF – If an element is deleted from PI AF that changes the number of matches in your view, the data for the element is not published going forward. However, previously published data is retained.
- Element is renamed in PI AF – If an element is renamed in PI AF, then the element is automatically renamed in the view. The new name appears in published data going forward, but previously published data retains the old element name.

How published data is synchronized with PI Data Archive

The following describes how published data is synchronized with PI Data Archive for each type of view:

- Asset views – When there are changes to the PI Data Archive data, the target data is updated automatically. PI Integrator Sync overwrites the data in the target.
- Scheduled streaming views – If there is a change to a data value, the new value is published to the target. However, the previously published value is not deleted.
- Key-value-triggered streaming views – Updating data is not supported for key-value-triggered streaming views.

Manual updating

If you are using PI Data Archive 2016 R2 or earlier, you can manually update data previously published to a target.

Note:

You can only manually update data in asset views and scheduled streaming view for supported targets. You cannot update data in views that are published only once or published to a file or HDFS target, and you cannot update key-value-triggered streaming views.

You only need to manually update if the data has changed since it was last published to the target data store. Any changes to the data that occur before a scheduled publish are written to the data store with the latest values.

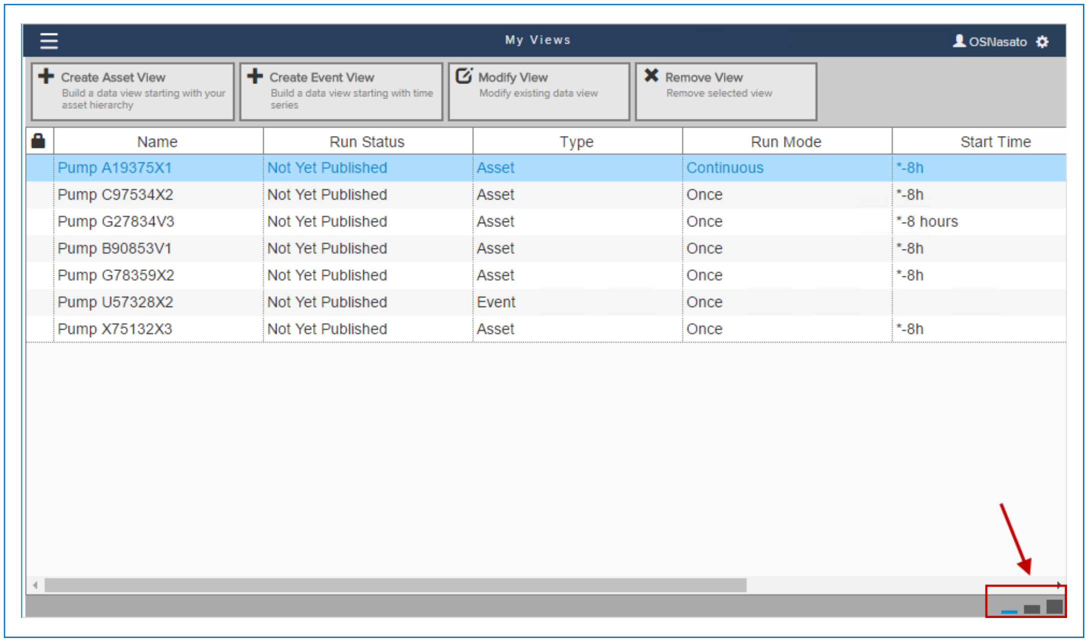
These are some circumstances that might cause the data to change:

- Data was being buffered on an interface node at the time the view was published.
- Data is backfilled or recalculated. This often occurs with PI AF Analytics tags.
- Data is manually entered after the view was published.

Update data manually

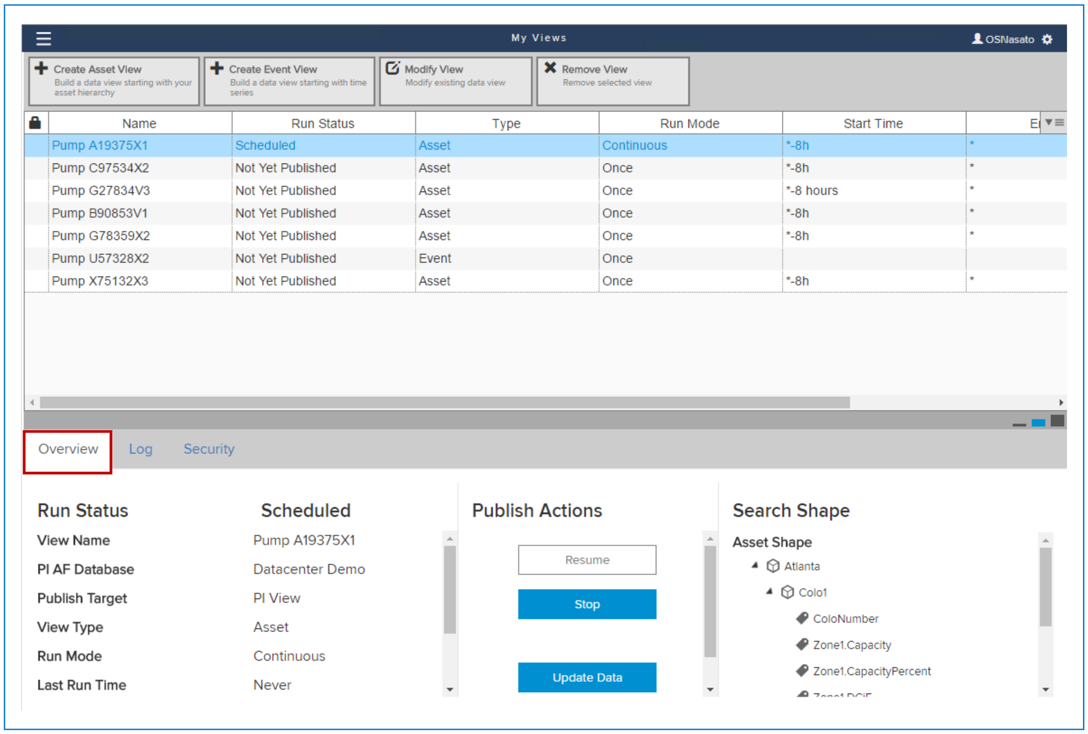
Procedure

1. Select a view in the My Views page whose **Run Mode** status is **Continuous** or **Scheduled Stream**.
2. Click the horizontal bar in the lower right corner of the My Views page to open the details panel.


My Views
OSNasato
Create Asset View
Build a data view starting with your asset hierarchy
Create Event View
Build a data view starting with time series
Modify View
Modify existing data view
Remove View
Remove selected view

Name	Run Status	Type	Run Mode	Start Time
Pump A19375X1	Not Yet Published	Asset	Continuous	*-8h
Pump C97534X2	Not Yet Published	Asset	Once	*-8h
Pump G27834V3	Not Yet Published	Asset	Once	*-8 hours
Pump B90853V1	Not Yet Published	Asset	Once	*-8h
Pump G78359X2	Not Yet Published	Asset	Once	*-8h
Pump U57328X2	Not Yet Published	Event	Once	
Pump X75132X3	Not Yet Published	Asset	Once	*-8h

3. Click the **Overview** tab.



Name	Run Status	Type	Run Mode	Start Time	E
Pump A19375X1	Scheduled	Asset	Continuous	*-8h	*
Pump C97534X2	Not Yet Published	Asset	Once	*-8h	*
Pump G27834V3	Not Yet Published	Asset	Once	*-8 hours	*
Pump B90853V1	Not Yet Published	Asset	Once	*-8h	*
Pump G78359X2	Not Yet Published	Asset	Once	*-8h	*
Pump U57328X2	Not Yet Published	Event	Once		
Pump X75132X3	Not Yet Published	Asset	Once	*-8h	*

Run Status	Scheduled
View Name	Pump A19375X1
PI AF Database	Datacenter Demo
Publish Target	PI View
View Type	Asset
Run Mode	Continuous
Last Run Time	Never

4. In the Publish Actions pane, click **Update Data**.

    Note:

    If the **Update Data** button does not appear, this means update is not supported for this type of view. For information on which views can be updated, see How published data gets updated.

5. Specify the time period of the data you want to update.

    Note:
    You can only update data for a time period in the past.

6. Click **Confirm**.

Modify a view

When a view is modified, there are implications for how existing data is handled:

- When an asset or event view is modified and published, the existing data is overwritten. Previously published data is not preserved. The modified asset or event view uses the start time of the first publishing as its start time.
- Any data that is read from a streaming target into another system is not modified. You will have to reconcile any differences in the data that is sent for the original view and the modified view. In most instances, you will probably delete the existing stored data before publishing the modified view.

Alternatively, you can make a copy of a view and edit the copy; this view is treated as a new view.

Procedure

1. From the My Views page, select the view you want to modify and click **Modify View**.
2. In the Modify View dialog box, do one of the following:
   - To edit the view – Click **Edit this view.**
   - To edit a copy of the view – Select **Edit a copy of this view**, enter a unique name for the view, and click **Edit View.**

   The selected view is displayed in the Select Data page. You can continue with making changes to the data shape, modifying the view, and publishing the data.

   For more information on how to edit a view, refer to Create an asset view, Create an event view, and Create a streaming view.

Copy a view

You can create a copy of any view by selecting it on the My Views page and clicking **Modify View**. For more information, see Modify a view.

Rename a view

You can rename a view from the My Views page.

Procedure

1. On the My Views page, click one of the bars in the lower right corner of the page to open the details panel.

   The panel opens with the **Overview** tab selected.
2. Click the ✎ next to the view name.

   > **Note:**
   > Renaming views is not supported for Text File, HDFS, Apache Kafka, Azure Event Hubs, Azure IoT Hub, Amazon Kinesis, and Amazon S3 targets.
3. Edit the view name and click **Rename**.

Secure your views

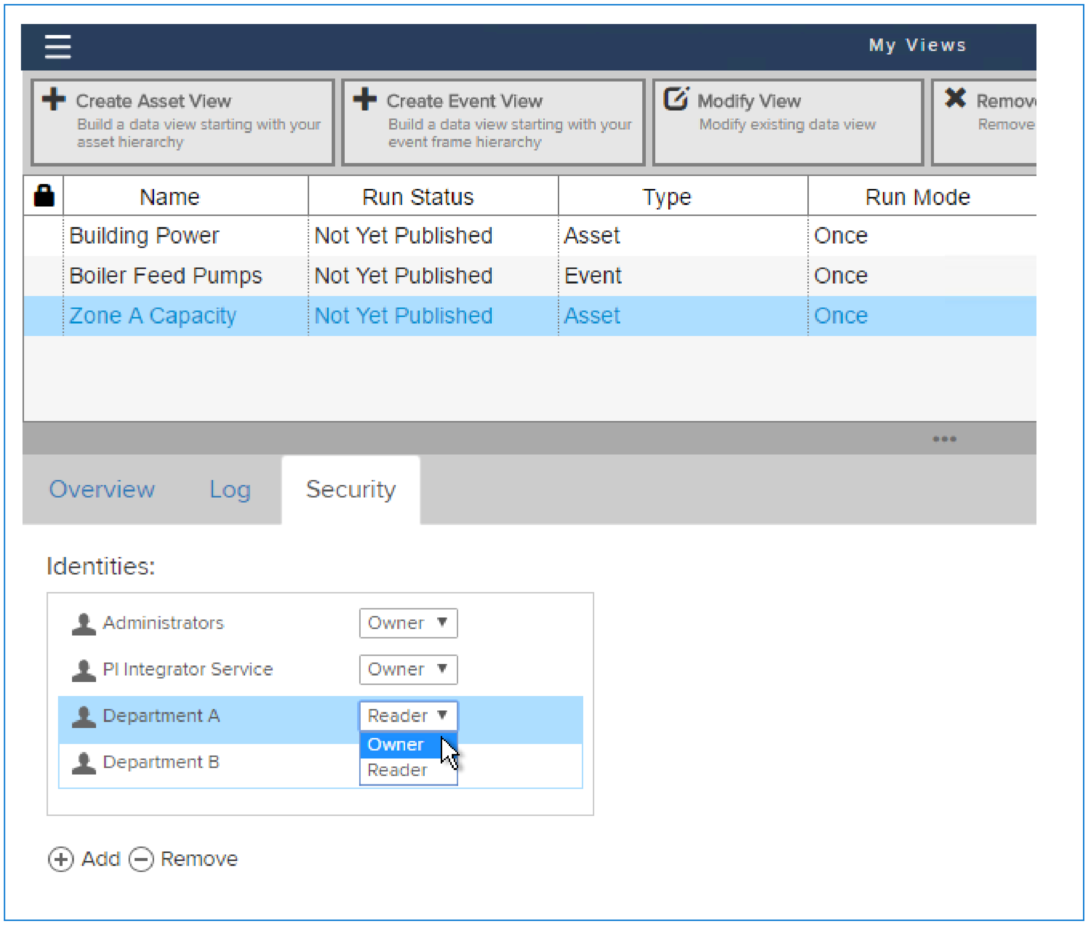
You can control access to any views for which you have Owner permissions. The following permissions can be granted to a view:

- **Owner** grants write access to the view configuration, and it gives the identity the ability to change permissions on the view and grant access to the view. Owner also grants access to the PI View target data.
- **Reader** grants read access to the view configuration and to the PI View target data.

Procedure

1. Click the menu icon ☰ and click **My Views**.
2. On the My Views page, select a view from the list.

   The details for the view appear below the list in the **Details** pane.
3. Click the **Security** tab.


My Views
Create Asset View
Build a data view starting with your asset hierarchy
Create Event View
Build a data view starting with your event frame hierarchy
Modify View
Modify existing data view
Remov
Remove
Overview
Log
Security
Add
Remove

	Name	Run Status	Type	Run Mode
	Building Power	Not Yet Published	Asset	Once
	Boiler Feed Pumps	Not Yet Published	Event	Once
	Zone A Capacity	Not Yet Published	Asset	Once

Identities:

Administrators	Owner
PI Integrator Service	Owner
Department A	Reader Owner Reader
Department B	

4. You can perform the following actions on a view.
   - Change the permissions on a view
   - Add a new identity and grant permission to the view
   - Remove access to a view

PI Integrator Framework Security

There are two general areas to consider when planning security for PI Integrator for Business Analytics:

- Data security — Determines which users are granted access to data in PI AF and how that security is managed.

  Users on the client machines make their requests to PI AF through PI Integrator Framework service and, by default, the user inherits whatever permissions have been granted to the account that the service uses.

  You can have greater control over users' access to data using delegated credentials. The user's credentials are passed to the PI AF service through the PI Integrator Framework service. In this instance, the user's access to PI AF is determined by the permissions that are defined for that particular user. Kerberos allows you to delegate credentials and to further define access to resources on the machine. You can only use constrained delegation which limits users' access to specific resources on the machine. Unconstrained delegation is not supported. For more information, see Kerberos constrained delegation.

  There is another type of data security to be considered, that is, the security of the published data that resides on the designated target. This security is handled and managed by the target. The exception to this is the PI View target whose data security is managed by PI Integrator for Business Analytics. For more information on managing access to PI View target data, see Secure the views for an identity.

  Note:

  Data security only defines which data on PI AF the user can access. This is different from the views they have access to which is addressed with application security.

- Application security — Defines users' access to views and publish targets.

  In PI Integrator for Business Analytics, the PI Integrator Framework service administrator maps users to PI AF identities. All users mapped to a PI AF identity share the same permissions; they acquire all permissions granted to the PI AF identity. Users have owner permissions on any views created by an identity to which they are mapped. Users with owner permissions on a view can see the data and grant access to their views to other users. In turn, they can see any views to which an identity to which they are mapped has been granted read access.

  By default, all users can publish their views to the PI View target. For all other publish targets, they must be granted permission by the administrator.

  Administrators can grant users access to any views or publish targets.

User Permissions

Prior to PI Integrator for Business Analytics 2018, users were added individually. Beginning with PI Integrator for Business Analytics 2018, PI AF identities are supported.

Users that were created in earlier versions of PI Integrator for Business Analytics are converted to PI AF identities in the following way:

- If PI Integrator for Business Analytics was running against PI AF 2015 server or later, users are automatically converted to PI AF identities.
- If PI Integrator for Business Analytics was running against PI AF 2014 server or earlier, then you must upgrade to PI AF 2015 or later before upgrading PI Integrator for Business Analytics. Your users will then be automatically converted to PI AF identities.

View Permissions

When a view is created, it is assigned the PI AF identity of the user creating the view. Only PI AF identities that have been granted access to PI Integrator for Business Analytics are available. If the user belongs to more than one identity, then you choose which identity to assign to the view at the time the view is created. If you do not choose an identity, then a PI identity is assigned, by default, in the following order:

- If the user is mapped to only one PI AF identity, this identity is used.
- If the user is mapped to multiple identities, then the identity with the fewest mappings is assigned. Single-user identities and group identities are treated the same. If multiple identities have the same number of mappings, then the first in an alphabetical sort of the identity name is assigned.

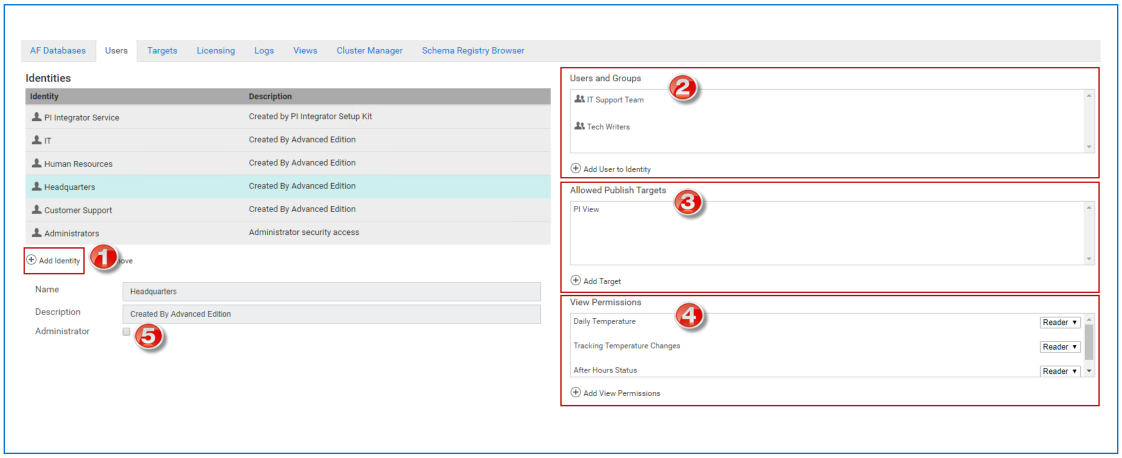
After a view is created, you can assign additional PI AF identities to the view. For more information, see Secure your views.

Users can be given the following permissions on a view:

- **Owner** grants write access to the view configuration, and it gives the identity the ability to change permissions on the view and grant access to the view. Owner also grants access to the PI View target data.
- **Reader** grants read access to the view configuration and to the PI View target data.

Where application security is managed

From the Identities page, you can manage all users and their access to any views and publish targets. You must be a PI Integrator Framework service administrator to access this page.



Identities

Identity	Description
PI Integrator Service	Created by PI Integrator Setup Kit
IT	Created By Advanced Edition
Human Resources	Created By Advanced Edition
Headquarters	Created By Advanced Edition
Customer Support	Created By Advanced Edition
Administrators	Administrator security access

Name: Headquarters
Description: Created By Advanced Edition
Administrator: □

Users and Groups
IT Support Team
Tech Writers

Allowed Publish Targets
PI View

View Permissions

Daily Temperature	Reader ▾
Tracking Temperature Changes	Reader ▾
After Hours Status	Reader ▾

The table describes the tasks you can perform. The numbers correspond to the numbers in the screen shot and identify where on the page the task is accomplished.

Number	Security task
1	Create PI AF identities
2	Assign users and groups to the identities
3	Specify to which targets PI AF identities can publish data
4	Specify which views the PI AF identities have permissions to access and the level of their access
5	Grant the PI identity administrator privileges

For more information on how to complete these tasks, see Add and configure identities.

How to secure views

Ensuring that only the appropriate users are able to access a view is important for maintaining proper oversight and security of your data.

There are two ways to secure views:

- You can configure access to any views for which you are the owner on the My Views page.

  For more information, see Secure your views.

- If you are a PI Integrator Framework service administrator, you can configure access by identity or by views on the Administration page:

  - If you want to configure what views an identity has access to, see Secure the views for an identity.

  - If you want to configure the identities for a single view, see Manage access to a single view.

  - If you want to configure the identities for multiple views at one time, see Manage access to multiple views.

Secure the views for an identity

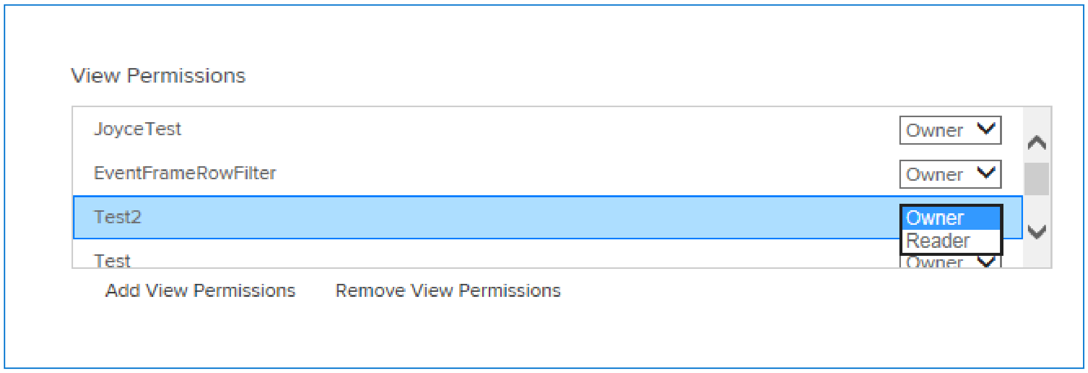
PI Integrator Framework service administrators can assign access to views for all identities from the Administration page.

Procedure

1. Click the menu icon ☰ and click **Administration**.

2. On the Administration page, click the **Users** tab. The **Identities** list displays a list of the PI AF identities.

3. Select the identity whose permissions you want to configure.



View Permissions

JoyceTest	Owner
EventFrameRowFilter	Owner
Test2	Owner
Test	Owner

The **View Permissions** list displays the views for the selected identity and the current permissions for those views.

4. Select the view you want to configure.
5. Select either **Owner** or **Reader** permission from the list.
   - **Owner** grants write access to the view configuration, and it gives the identity the ability to change permissions on the view and grant access to the view. Owner also grants access to the PI View target data.
   - **Reader** grants read access to the view configuration and to the PI View target data.

Kerberos constrained delegation

Note:

Kerberos *authentication* for users logging into the PI Integrator for Business Analytics user interface is not supported. This section, instead, describes Kerberos *delegation* which comes into play when the user is already authenticated with PI Integrator for Business Analytics, and the user is attempting to access PI AF resources from the PI Integrator for Business Analytics user interface.

Kerberos delegation enables users to access remote data sources through Windows authentication. Kerberos is the recommended solution to manage user access among different servers. With Kerberos, PI Integrator for Business Analytics accepts and relays user login credentials to PI AF server. Delegation to PI Data Archive is not supported.

It is recommended that you enable and configure Kerberos constrained delegation for the service account that runs the PI Integrator for Business Analytics services so that only the appropriate resources within the PI System are available to the end user through the PI Integrator for Business Analytics user interface. The user can only publish data they have access to in PI AF server. If Kerberos is not enabled, the user will be granted the same permissions as the PI Integrator Framework service account when it accesses PI AF assets and data.

Note:
PI Integrator for Business Analytics supports constrained delegation only. Unconstrained delegation is not supported.

Before you can enable and configure Kerberos constrained delegation, you must have the following:

- The PI Integrator Framework service running under a managed service account.

A managed service account is recommended because it provides applications such as SQL Server or Exchange with automatic password management and support for simplified service provider names.

For detailed information about managed service accounts, see Introducing Managed Service Accounts (https://technet.microsoft.com/en-us/library/dd560633(v=ws.10).aspx) on the Microsoft web site.

- The machine name where the PI Integrator Framework service is installed.
- The name of the service account that runs the PI Integrator Framework service.
- Access to the domain controller and domain admin rights.

Complete the following tasks to configure Kerberos constrained delegation:

Task 1: Configure service principal names (SPN) for the domain

Task 2: Enable service account for Kerberos constrained delegation

Task 3: Add PI Asset Framework servers with the AF server service type

Note:
This user guide only details the steps to enable Kerberos delegation for the PI Integrator Framework service to restrict the PI AF server objects that users see in the PI Integrator for Business Analytics user interface. It does not include how to set up Kerberos delegation for PI SQL Data Access Server.

With some architectures, you may need to configure PI SQL Data Access Server for Kerberos constrained delegation in order for end users to access data published by the PI View target. For information on this topic, see *PI SQL Data Access Server (PI Integrators) Administrator's Guide*, available on the Technical Support Download site (https://techsupport.osisoft.com/Downloads/All-Downloads/)

Task 1: Configure service principal names (SPN)

To configure constrained delegation for the PI Integrator Framework service account, service principal names (SPNs) must exist for the following:

- All PI AF servers that PI Integrator for Business Analytics needs to access
- The machine on which the PI Integrator Framework service is installed
- PI Integrator Framework service account

Follow the procedure below to verify that these SPNs exist or create the required SPNs.

Procedure

1. Open a console window as a domain administrator.
2. Verify that SPNs exist for all machines on which the PI AF server is installed.

   See the Check and set permissions for SPN creation topic "Check and set permissions for SPN creation" in Live Library (https://livelibrary.osisoft.com) for more information.

Note:
The PI AF server should automatically create the required SPNs. If these PI AF Server SPNs do not exist, contact OSIsoft Technical Support.

3. Create an SPN for the PI Integrator Framework service account. Enter the following commands to specify both the fully-qualified and non-qualified PI Integrator for Business Analytics machine name:

   a. `setspn -S http/`*`hostname domain`*`\`*`service_account`*

   b. `setspn -S http/`*`fully-qualified_domain_name domain`*`\`*`service_account`*

Example SPN configuration

For example, assume that PI Integrator for Business Analytics is running on the `lab1.prod.opsmain.com` and the PI Integrator Framework service is running as service account `prod\piintegratorservice`. The domain is `prod`. Enter the following to configure the SPNs, one for the host name and one for the fully qualified domain name:

```
setspn -S http/lab1 prod\piintegratorservice
```

```
setspn -S http/lab1.prod.opsmain.com prod\piintegratorservice
```

Task 2: Enable service account for Kerberos constrained delegation

This procedure describes how to enable your PI Integrator Framework Windows service account for Kerberos constrained delegation.

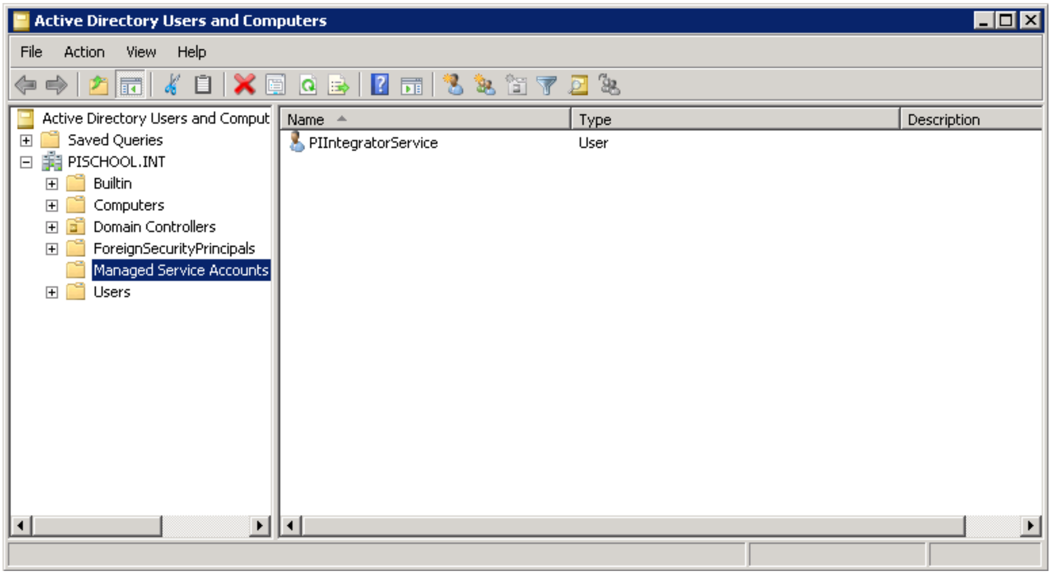
Procedure

1. Log on to the machine hosting the PI Integrator Framework service.
2. Stop the PI Integrator Framework service.
3. Locate the PI Integrator for Business Analytics configuration file: *`%pihome64%`*`\Integrators\BA\CAST.UI.WindowsService.exe.config`.
4. Open the configuration file with a text editor and locate the following configuration:

   ```
   <add key="Impersonate" value="false" />
   ```

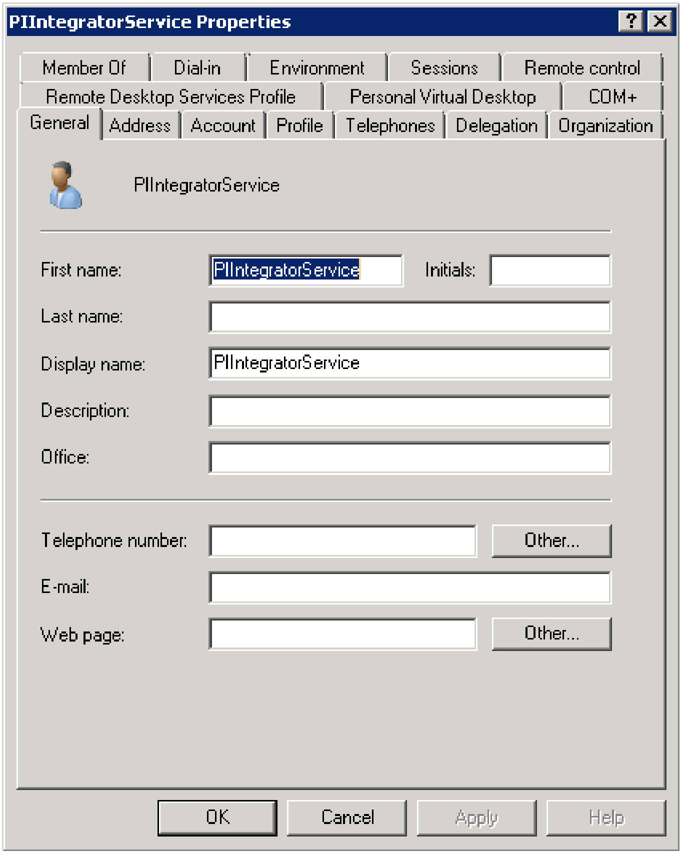
5. Change `"false"` to `"true"`, as follows: `<add key="Impersonate" value="true" />` and save the changes to the file.
6. Log on to the domain controller as a domain administrator (or any computer with Active Directory Users and Computers installed).
7. Open the Active Directory Users and Computers window.
8. In the navigation panel, select **Managed Service Accounts**, or if a standard user account dedicated to running the service is used, then select **Users**.

   A list of service accounts is displayed.



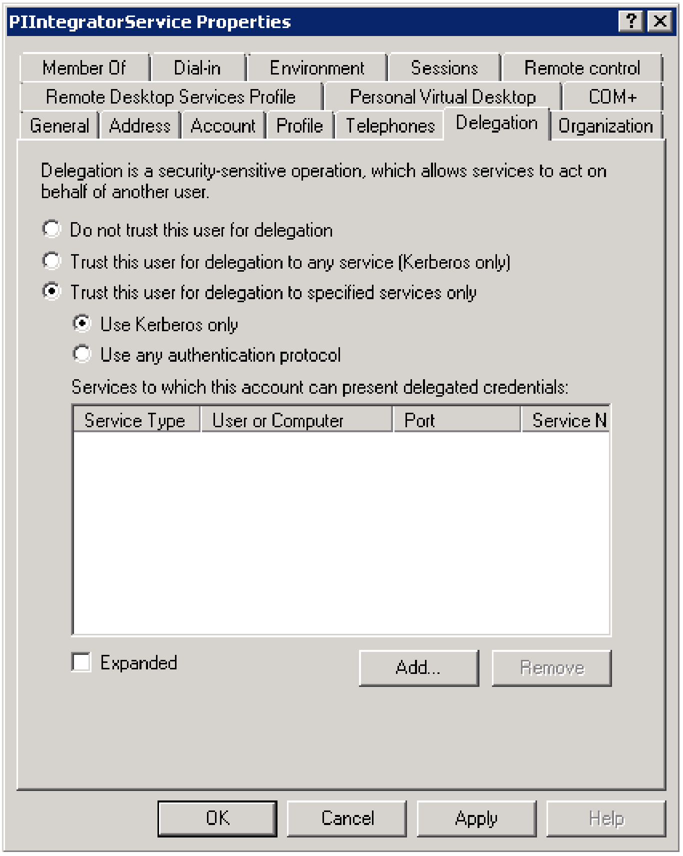
Name	Type	Description
PIIntegratorService	User	

9. Find and double-click the service account for PI Integrator Framework service. The service Properties dialog box opens.



First name: PIIntegratorService
Initials:
Last name:
Display name: PIIntegratorService
Description:
Office:
Telephone number:
E-mail:
Web page:

10. Click the **Delegation** tab.



Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

○ Do not trust this user for delegation

○ Trust this user for delegation to any service (Kerberos only)

● Trust this user for delegation to specified services only

● Use Kerberos only

○ Use any authentication protocol

Services to which this account can present delegated credentials:

Service Type	User or Computer	Port	Service N

□ Expanded

11. Select **Trust this user for delegation to specified services only** to enable constrained delegation.

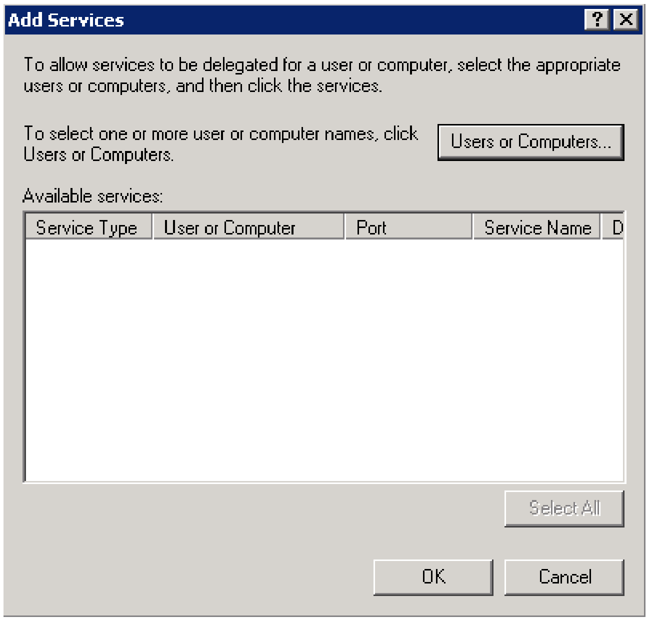
    Note:

    Ensure you do not select **Trust this user for delegation to any service (Kerberos only)**. This selection enables unconstrained delegation which is not supported with PI Integrator for Business Analytics.

    In subsequent tasks, you will add the PI Asset Framework server SPNs that the PI Integrator Framework service can delegate to.

12. Click **Add** to enable constrained delegation.

    The Add Services dialog box appears.



Add Services

To allow services to be delegated for a user or computer, select the appropriate users or computers, and then click the services.

To select one or more user or computer names, click Users or Computers.

Available services:

Service Type	User or Computer	Port	Service Name	D

13. Click OK.

    Your service account is enabled for Kerberos constrained delegation.

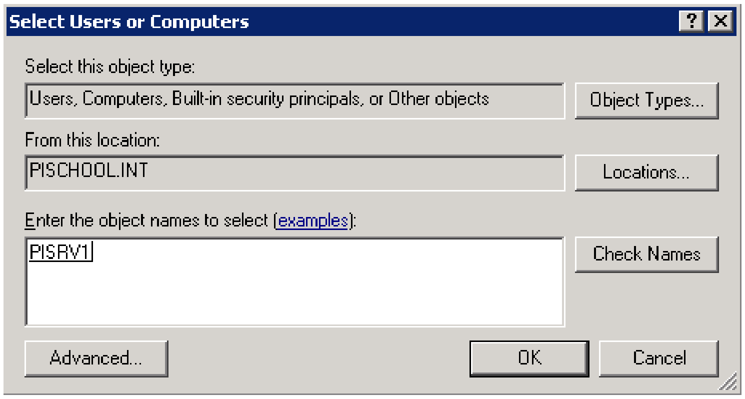
Task 3: Add PI Asset Framework servers with the AF server service type

This procedure describes how to specify the PI AF server for Kerberos constrained delegation for PI Integrator for Business Analytics.

Procedure

1. With the Add Services dialog box still open from Task 2: Enable Service account for Kerberos Constrained Delegation, click **Users or Computers.**

   The Select Users or Computers dialog box opens.



Select Users or Computers

Select this object type:
Users, Computers, Built-in security principals, or Other objects

From this location:
PISCHOOL.INT

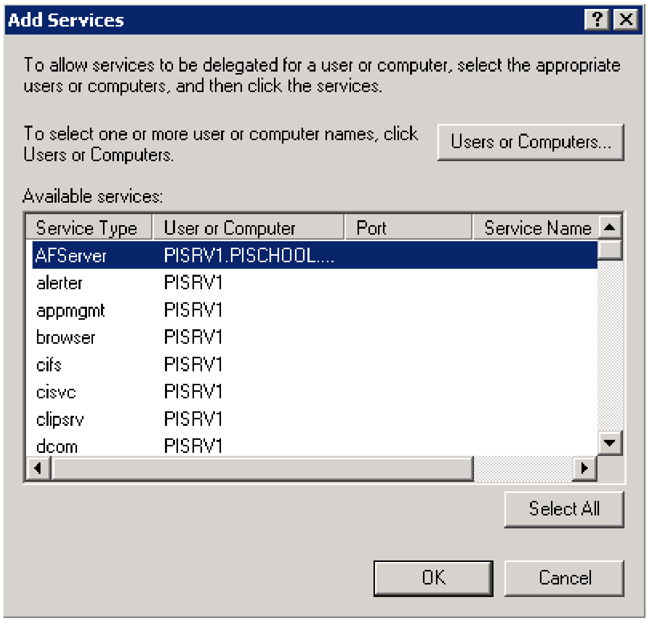
Enter the object names to select (examples):
PISRV1

2. Enter the name of the server on which PI AF is installed.

> **Note:**
>
> If the PI AF server is running as a custom service account, then search for the PI AF server SPN using the service account rather than the machine name.

3. Click **Check Names** to verify the server name. The server name appears verified.
4. Click **OK.**

   The Add Services dialog box opens.



Add Services

To allow services to be delegated for a user or computer, select the appropriate users or computers, and then click the services.

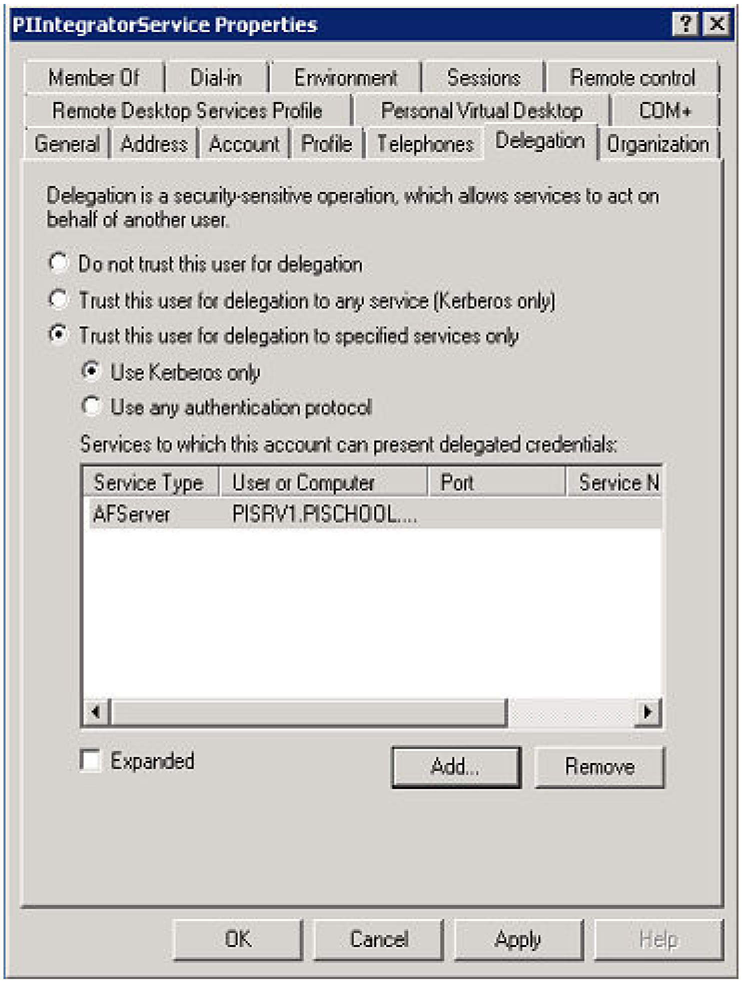
To select one or more user or computer names, click Users or Computers.

Available services:

Service Type	User or Computer	Port	Service Name
AFServer	PISRV1.PISCHOOL....		
alerter	PISRV1		
appmgmt	PISRV1		
browser	PISRV1		
cifs	PISRV1		
cisvc	PISRV1		
clipsrv	PISRV1		
dcom	PISRV1		

5. Select the **AFServer** service type in the Available services list.
6. Click **OK.**

   The selected PI AF server is assigned the `AFServer` service type.
7. Click the **Delegation** tab of the service Properties dialog box.
8. In the **Services to which this account can present delegated credentials** list, verify that the `AFServer` service type has been assigned to the PI AF server.



Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

○ Do not trust this user for delegation

○ Trust this user for delegation to any service (Kerberos only)

● Trust this user for delegation to specified services only

- ● Use Kerberos only
- ○ Use any authentication protocol

Services to which this account can present delegated credentials:

Service Type	User or Computer	Port	Service N
AFServer	PISRV1.PISCHOOL....		

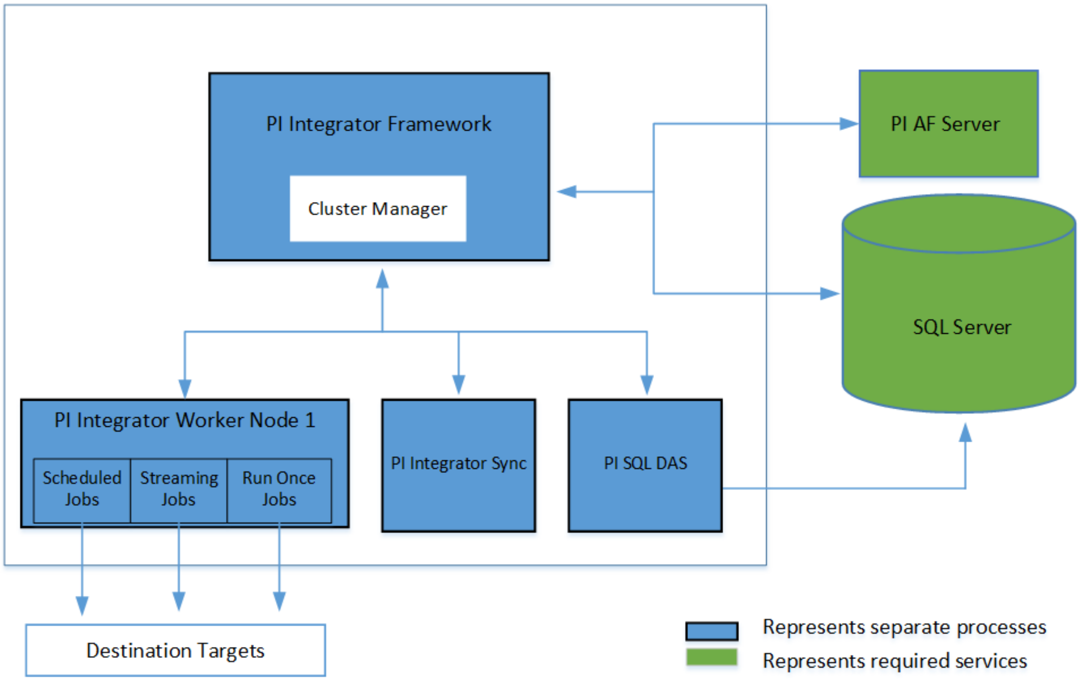
□ Expanded

For more information about navigating to the service Properties dialog box, see Task 2: Enable Service account for Kerberos Constrained Delegation.

9. Repeat this procedure for any PI AF servers from which PI Integrator for Business Analytics will be accessing data.

PI Integrator for Business Analytics scale architecture

The following diagram shows the PI Integrator for Business Analytics architecture.



PI Integrator for Business Analytics with one PI Integrator Worker Node

The PI Integrator Framework, PI Integrator Worker Node, and PI Integrator Sync processes all reside on the same computer.

Each PI Integrator for Business Analytics instance has a minimum of one worker node process that manages the publishing of views including scheduled jobs, streaming jobs, and run once jobs. You can add additional worker nodes to improve the publishing performance. This can be done during installation of PI Integrator for Business Analytics. After installation, you can add more nodes using the Add Remove Programs option in the Microsoft Windows Control Panel. Note that each additional worker node has additional RAM and CPU requirements. For more information, see System requirements. You will not be able to add nodes from the PI Integrator for Business Analytics web application.

The PI Integrator Worker Node publishes jobs to the destination targets. The Cluster Manager automatically distributes jobs, in turn, among the available nodes. For example, assume there are two worker nodes and five jobs. The first job is assigned to the first worker node, the second job is assigned to the second worker node, the third job is assigned to the first worker node, and so on. When a worker node is added to the cluster, all PI Integrator for Business Analytics services are restarted and the Cluster Manager balances the jobs across all available nodes, including the newly added node.

Note:

Jobs are not assigned to the nodes in alphabetical order.

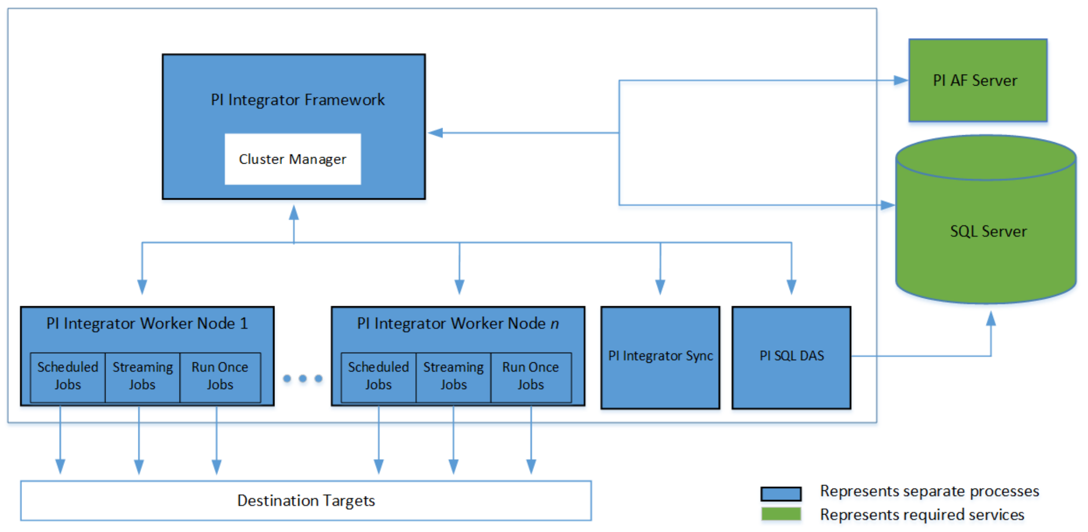
If a node goes down, the Cluster Manager reassigns any jobs that were assigned to it to the remaining worker nodes. The offline worker node is automatically restarted by the PI Integrator Framework service. Once restarted, existing jobs are not rebalanced to include the restarted worker node. However, new jobs are balanced across all working nodes. If this results in an unbalanced distribution of jobs, you can manually rebalance the jobs.

Optimizing the worker node processes

Follow these guidelines to optimize the performance of your worker nodes:

- Install a minimum of two PI Integrator Worker Nodes, ensuring that you have the required RAM and CPU to support additional worker nodes. Then, if one of the nodes fails, the other will be able to pick up the jobs from the failed node and view data will still get published.
- Review your view statistics and identify which views are taking so long to publish that the next scan is missed. Break up problematic views into multiple smaller views. If the problem persists, then consider adding another node.
- Check that your views are efficiently structured. Use PI AF templates whenever possible, but do not create shapes that return bloated results. The number of shape matches has a direct impact on performance. Therefore, if possible, design your search shape on the Select Data page of creating a view to specify only those elements you need and filter out unnecessary elements. (This is before any row filters are applied.)
- Schedule your views so that they are not all publishing at the same time. Offset the jobs from one another.

If, after optimizing your views, you still need to improve the performance, then add a worker node to the cluster. See System requirements for the memory and hardware requirements. You can have up to five PI Integrator Worker nodes. All worker nodes must reside on the same computer on which the PI Integrator for Business Analytics is installed.



PI Integrator for Business Analytics with multiple PI Integrator Worker nodes

Manage the PI Integrator Worker Nodes

PI Integrator for Business Analytics provides a Cluster Manager which you can use to view the status of the cluster and to manage the worker nodes. For each node, it displays the following:

- Service Name – Name of the worker node service. The default worker node is named PI Integrator Worker Node 1. Each subsequent worker node is identified with a number, for example, PI Integrator Worker Node 2, PI Integrator Worker Node 3, and so on.

> **Note:**
> The PI Integrator Worker Node services are installed with Startup Type set to Manual. The PI Integrator Framework service automatically restarts the service as needed; therefore, it's not necessary for users to restart the service.

- Status – Shows whether the node is up or down. The PI Integrator Framework service will restart the worker node service within one minute.
- Address – A unique identifier used internally that indicates the TCP location for the process. This identifier changes each time the worker node service starts up.

The jobs running on each node are displayed with the following information:

- Job ID – GUID that is assigned to the job
- Job Name – Name of the view
- Job Status – Displays the status of the job, for example, Scheduled, Publishing, Streaming
- Last run time – Timestamp of the last publishing of the view

You can perform the following management tasks:

- As necessary, you can redistribute jobs more evenly across worker nodes by clicking **Rebalance Nodes.**
- Click on a job to go to the My Views page where you can get more details about the view, including log messages and run statistics.

Administration tasks

There are a number of administration tasks that you can perform on your PI Integrator for Business Analytics system including securing views for specific users, securing access to PI Integrator for Business Analytics using Kerberos constrained delegation, and recovering output streams.

Topics in this section

- About PI Integrators Service Group
- Remove PI AF servers and databases
- Edit a publish target
- Remove a publish target
- Add a schema registry
- Manage views
- Review log records
- Set your record retention policies
- Licensing and output streams
- Change the Windows service account
- Change the PI Integrator port
- Change the SSL certificate configuration

About PI Integrators Service Group

When you install PI Integrator for Business Analytics, the PI Integrators Service Group Windows group is created, and the Windows service account specified to run the PI Integrator Framework service is added to this group. The PI Integrators Service Group assigns the Windows service account the minimum privileges required to run the PI Integrator Framework service. Therefore, it is recommended that you do not add the Windows service account to the local administrators group on the machine where PI Integrator for Business Analytics is installed.

Remove PI AF servers and databases

You can remove PI AF servers that you no longer want to use in your views.

Procedure

1. Click the menu icon ☰ and click **Administration**.
2. On the Administration page, click the **AF Databases** tab.
3. Select the PI AF server you want to remove from the **AF Servers** list.

> **Note:**
> The databases on the selected server are displayed next to **AF Servers** list in the **AF Databases** list.

4. Click **Remove AF Server** to remove the selected PI AF server and its databases from the list of available servers and databases.

   The PI AF server no longer appears in the **AF Servers** list.

Edit a publish target

The following section describes how to edit the configuration parameters for the publish target.

> **Note:**
>
> When you edit the configuration for a target, the changes are propagated to all views that are subsequently published to that target. Going forward, scheduled views and streaming views already in progress will pick up the new target configuration.

Procedure

1. Click the menu icon ☰ and click **Administration.**
2. On the Administration page, click the **Targets** tab.

   The Publish Target Configuration page opens.
3. Select a publish target from the **Publish Targets** list.

   The Target Configuration panel opens.

   > **Note:**
   > Each type of publish target has a unique set of configuration parameters.
4. Edit the parameters in the Target Configuration panel.

   Click on the link for your publish target for a description of the configuration parameters:

   - Configure Amazon Kinesis target
   - Configure Amazon Redshift target
   - Configure Amazon S3 target
   - Configure Apache Hive targets
   - Configure Apache Kafka target
   - Configure the Azure Data Lake Store target
   - Configure Azure Event Hubs target
   - Configure Azure IoT Hub target
   - Configure Azure SQL Database target
   - Configure Azure SQL Data Warehouse target
   - Configure Hadoop Distributed File System (HDFS) targets
   - Configure Microsoft SQL Server targets

  - Configure Oracle targets
  - Configure text file targets

5. Click **Save Changes**.

Remove a publish target

Note:

A PI View target cannot be removed.

Procedure

1. Click the menu icon ☰ and click **Administration**.
2. On the Administration page, click the **Targets** tab.

   The Publish Target Configuration page opens.
3. Select the publish target you want to remove from the **Publish Targets** list.
4. Click **Remove Publish Target**.
5. Verify that the selected publish target no longer appears in the **Publish Targets** list.

Add a schema registry

Note:

This feature is available in PI Integrator for Business Analytics Advanced Edition.

This release supports the Confluent Schema Registry. Only Avro schemas are supported.

Procedure

1. Click the menu icon ☰ and click **Administration**.
2. Click the **Schema Registry Browser** tab.
3. In the Add Schema Registry pane, enter a name and the URL for the registry. The URL must be prefaced with `http://` or `https://`.
4. Click **Add Schema Registry**.

   The Available Schemas pane is populated with any schemas in the registry. The Schema Preview pane displays the name value pairs for the selected schema.

Add a schema to the schema registry

Procedure

1. Click the menu icon ☰ and click **Administration**.
2. Click the **Schema Registry Browser** tab.
3. Select the registry in the Schema Registries pane.

4. In the Add or Update Schema section, click **Select Schema File**.
5. In the Open window, browse to the schema file, select the file, and click **Open**.

   Note:

   Only Avro schema files are supported.

   The schema name appears in the Available Schemas pane and the schema structure appears in the Schema Preview pane.

Manage views

As an Administrator, you can perform the following actions on views:

- Import and export views
- Delete views
- Add users to views
- Remove users from views

Manage access to a single view

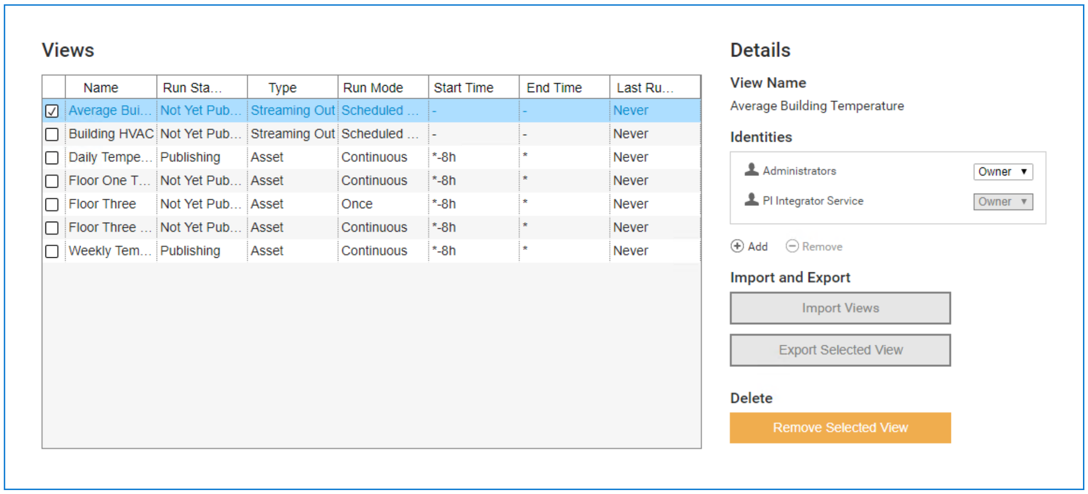
You can manage access to a single view:

- You can add identities to or remove identities from a single view.
- You can change permissions for an identity.

For information on managing access to more than one view at one time, see Manage access to multiple views.

Procedure

1. Click the menu icon ☰ and click **Administration**.
2. Click the **Views** tab.
3. Click the check box to select a view. The Details pane displays the current identities with access to the view.



	Name	Run Sta...	Type	Run Mode	Start Time	End Time	Last Ru...
☑	Average Bui...	Not Yet Pub...	Streaming Out	Scheduled ...	-	-	Never
□	Building HVAC	Not Yet Pub...	Streaming Out	Scheduled ...	-	-	Never
□	Daily Tempe...	Publishing	Asset	Continuous	*-8h	*	Never
□	Floor One T...	Not Yet Pub...	Asset	Continuous	*-8h	*	Never
□	Floor Three	Not Yet Pub...	Asset	Once	*-8h	*	Never
□	Floor Three ...	Not Yet Pub...	Asset	Continuous	*-8h	*	Never
□	Weekly Tem...	Publishing	Asset	Continuous	*-8h	*	Never

View Name
Average Building Temperature

Identities

Administrators	Owner ▾
PI Integrator Service	Owner ▾

4. Do any of the following:

   a. Click the arrow next to the permissions and select from the list to change the permissions for the identity.

   b. Click **Add** and follow the prompts to give the specified identity access to the view.

   c. Select an identity and click **Remove** to remove the identity's access to the view.

Manage access to multiple views

You can select multiple views at one time and add identities to them.

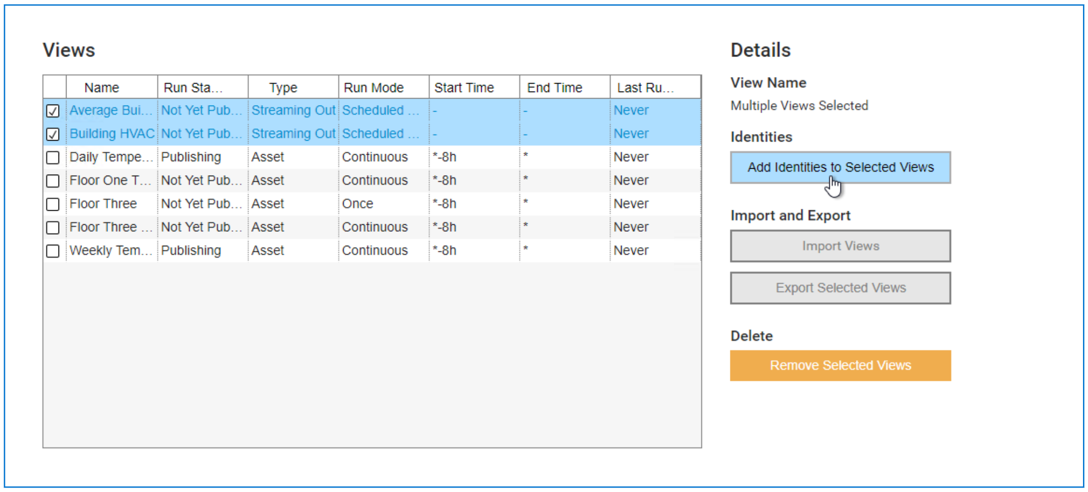
> **Note:**
> You cannot remove identities from multiple views. You can only remove identities from one view at a time.

Identities that are added to views are given Owner permission by default.

The exception to this is if an identity is already assigned to a view. If the view is one amongst other views that are selected and the same identity is assigned to it, it retains whatever permissions were previously set. For example, the Engineers identity is assigned to View ABC and is given Reader permission to the view. Then View ABC is selected along with other views and the Engineers identity is assigned to all the views. In this case, the Engineers identity for View ABC retains its existing permissions setting, that is Reader. All other views are assigned the default Owner permission for the Engineers identity.

Procedure

1. Click the menu icon ☰, and click **Administration**.
2. Click the **Views** tab.
3. Click in the left column of the views you want to select.



Views

	Name	Run Sta...	Type	Run Mode	Start Time	End Time	Last Ru...
☑	Average Bui...	Not Yet Pub...	Streaming Out	Scheduled ...	-	-	Never
☑	Building HVAC	Not Yet Pub...	Streaming Out	Scheduled ...	-	-	Never
☐	Daily Tempe...	Publishing	Asset	Continuous	*-8h	*	Never
☐	Floor One T...	Not Yet Pub...	Asset	Continuous	*-8h	*	Never
☐	Floor Three	Not Yet Pub...	Asset	Once	*-8h	*	Never
☐	Floor Three ...	Not Yet Pub...	Asset	Continuous	*-8h	*	Never
☐	Weekly Tem...	Publishing	Asset	Continuous	*-8h	*	Never

Details

View Name

Multiple Views Selected

Identities

Import and Export

Delete

4. Click **Add Identities to Selected Views.**
5. In the Add Identity window, select the identities you want to add and click **Ok.**

Moving views between environments

As you work on developing your views, you are likely to create them in a development environment, then verify that they generate the results you want in a test environment, before finally moving them into your production system. Use PI Integrator for Business Analytics to move the views between these environments, exporting them from one system and importing them into the other system. You can export views individually or you can export them in bulk to a views configuration file.

The following procedure assumes that you are exporting views from the first system and importing them into the second.

Before you start

On some browsers the default protocol used is Web Sockets which has a 64K limit on the data packet size. You must change the transport type to Server Sent Events to accommodate the larger data packets that are sent when importing and exporting views. On the My Views page, click the gear icon ⚙ in the upper right corner and set **Transport Type** to **Server Sent Events.**

This should only apply to Microsoft Edge browsers.

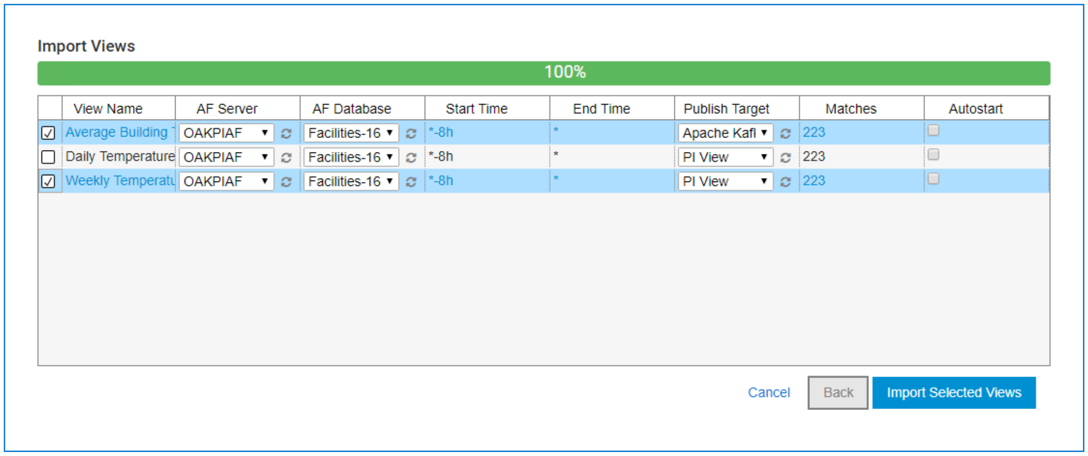
Procedure

1. Click the menu icon ☰ and click **Administration.**
2. On the Administration page, click the **Views** tab. The Views page displays a list of all the views in your PI Integrator for Business Analytics instance.
3. Select the views you want to export and click **Export Selected Views.**

   Files are exported to the `Downloads` directory. Single views are exported to a file with the name of the view, for example, `My Asset View.json`. Multiple views are exported to a file named `exportViews.json` file.
4. Move the exported file to a location that can be accessed from your second system, that is, the system you want to import the views into.

5. On the second system, from PI Integrator for Business Analytics, click the menu icon and click **Administration**.
6. On the Administration page, click the **Views** tab.
7. Click **Import Views**.
8. In the Open window, select the file you exported and click **Open**.

   The Import Views page displays the view. If you import an exported views file, the views contained in the file are extracted.

   Import Views

   100%

	View Name	AF Server	AF Database	Start Time	End Time	Publish Target	Matches	Autostart
☑	Average Building ⁻	OAKPIAF ▾	Facilities-16 ▾	*-8h	*	Apache Kafl ▾	223	□
□	Daily Temperature	OAKPIAF ▾	Facilities-16 ▾	*-8h	*	PI View ▾	223	□
☑	Weekly Temperatu	OAKPIAF ▾	Facilities-16 ▾	*-8h	*	PI View ▾	223	□

   PI Integrator for Business Analytics will attempt to locate the PI AF server and database used to create the view in the first system. If it cannot find the server or the database, these fields will be blank.
9. Select the PI AF server, PI AF database, and the publish target.

   The Matches column tells you the number of matches it finds for the shape with the specified PI AF server and database.
10. (Optional) Click in the View Name, Start Time, and End Time field to change the values.
11. (Optional) Click **Autostart** to automatically start publishing the view once it is imported.

    Note:

    - You cannot autostart a view that has never been published.
    - Exercise caution when importing multiple views. Once imported, they will start running immediately and may overload the computer resources. OSIsoft recommends that you manually set the publishing schedule if you are importing more than a few views.
12. Select the views you want to import and click **Import Selected Views**.

    The views are appended to the end of the list of views. Once imported, if **Autostart** is enabled they will start running immediately and may overload the computer resources. OSIsoft recommends that you manually schedule the views.

After you finish

Return **Transport Type** to its previous setting. In most instances, this is **Auto**.

Review log records

You can review the log records for any view from the **Logs** tab of the Administration page.

You can filter the logs by

- Specifying a time range using the **Start Time** and **End Time** fields
- Selecting a view with the **View Name** list
- Specifying the type of errors (Debug, Info, Warn, Error)

You can copy the displayed logs to the clipboard or download them to a file.

Set your record retention policies

Each time a view is published, log and statistics data are collected and stored in the following databases:

- Log data is stored in the PIIntegratorLogs SQL database.

  Note:

  If you are querying the database directly, time stamps are in GMT format.

- Statistics data is stored in the PIIntegratorStats SQL database.

Over time, these records can take up a lot of space on your server and, therefore, PI Integrator for Business Analytics periodically deletes the log and statistics records. The settings for the tasks are configured in the `%PIHOME64%\Integrators\BA\CAST.UI.WindowsService.exe.config` file.

The configuration file has the following separate sections for setting the policies for log records and for statistics records:

- `<maintenanceTasks>` section which determines when the records are deleted. There are two tasks, logRetentionPolicies and statRetentionPolicies.
- `<logRetentionPolicies>` and `<statsRetentionPolicies>` sections which determines which records are deleted

Log retention policy

For general information about records retention policies, see Set your record retention policies.

The logRetentionPolicies task in the maintenanceTasks section of the application configuration file determines when log records are deleted. By default, the log records are deleted every 24 hours at 7:00 a.m.

The following table describes the task parameters.

logRetentionPolicies task parameters

Parameters	Description of Parameter	Default value
`taskName`	Name of the log records retention task. Do not change this value.	`add taskName="logRetentionPolicies"`

Parameters	Description of Parameter	Default value
runFrequency	Frequency with which the logRetentionPolicies task is run. Use PI Time to specify units of time. runFrequency and timeOfDay together determine when the task is done.	runFrequency="24hours"
timeOfDay	Time that logRetentionPolicies task is run. Use PI Time to specify units of time. runFrequency and timeOfDay together determine when the task is done.	timeOfDay="7:00"

Log retention policy

The policy in the logRetentionPolicies section determines which log records are deleted. The oldest records are deleted first.

Note:

If the policy is deleted, then the log records are kept indefinitely.

You can delete log records based on any combination of the following:

- The age of the records
- The number of records
- The total size of all records

The default policy deletes log records older than two months, keeps the number of records to 100,000 or less, and keeps the maximum size of the log records to 1000 MB or less.

logRetentionPolicies policy parameters

Parameter	Description of Parameter	Default value
uniquePolicyName	Name of the policy.	uniquePolicyName="LogsPolicy1"
maximumTableRecordAge	Maximum age of log records specified in months. Used with maximumTableRowCount and maximumTableSizeOnDisk to determine which log records are deleted.	maximumTableRecordAge="2months"
maximumTableRowCount	Maximum number of rows of log data. Used with maximumTableRecordAge and maximumTableSizeOnDisk to determine which log records are deleted.	maximumTableRowCount="100000"

Parameter	Description of Parameter	Default value
`maximumTableSizeOnDisk`	Maximum size of all log records, specified in megabytes (MB). Used with `maximumTableRecordAge` and `maximumTableRowCount` to determine which log records are deleted.	`maximumTableSizeOnDisk="1000"`

Statistics retention policy

The statistics for each view are stored as a separate table in the PIIntegratorStats SQL database. The table name is the view ID.

Statistics retention policy task

The statRetentionPolicies task in the maintenanceTasks section of the application configuration file determines when the statistics records are deleted. The following table describes the statRetentionPolicies task parameters.

statRetentionPolicies task parameters

Parameter	Description of parameter	Default value
`taskName`	Identifies the name of the statistics retention task. Do not change this value.	`taskName="statRetentionPolicies"`
`runFrequency`	Frequency with which the statRetentionPolicies task is run. Use PI Time to specify units of time. `runFrequency` and `timeOfDay` together determine when the task is run.	`runFrequency="24hours"`
`timeOfDay`	Time that the statRetentionPolicies task is run. Use PI Time to specify units of time. `runFrequency` and `timeOfDay` together determine when the task is run.	`timeOfDay="7:00"`

By default, the statistics records are deleted every 24 hours at 7:00 a.m.

Statistics retention policies

The policies in the statRetentionPolicies section determine which statistics records are deleted. The statistics retention policies assume that views are published at scheduled intervals and the publishing frequency determines which records are deleted. Generally, the more frequently a view is published, more statistics are generated, and you want to delete records more often. This is true for asset views, event views, and scheduled streaming views.

Streaming views that are published in response to changes to key values are not published at regular intervals. Therefore, to effectively manage the amount of statistics data in the database, PI Integrator for Business Analytics makes the assumption that data streaming for these views occurs at the highest possible frequency, that is, at 30-second intervals. Therefore, the policy that includes the publish frequency of 30 seconds is applied to all key-value-triggered streaming views.

> **Note:**
>
> The statistics for views that are only published once are kept indefinitely until the view is removed.

The following policies are defined by default:

- `StatsPolicy1` – Defines a policy for views published at a frequency between 1 second and 5 minutes
- `StatsPolicy2` – Defines a policy for views published at a frequency between 5+ minutes and up to 1 hour
- `StatsPolicy3` – Defines a policy for views published at a frequency of 1+ hours

You can edit the default policies or create additional policies and specify whatever level of granularity you require. Check to see that your policies cover all possible time intervals. If a time interval is not included, then the statistics records for views published at the missing interval will be kept indefinitely.

For each policy, you can delete the records for a view based on any combination of the following:

- The age of the records in the table
- The total number of records in the table
- The total size of the table

The following describes the statRetentionPolicies policy parameters and lists the default values for one of the policies, StatsPolicy1.

statRetentionPolicies policy parameters

Parameter	Description of parameter	Default values for StatsPolicy1
`uniquePolicyName`	Name of the policy. Policy names must be unique. If there are multiple policies with the same name, then the configuration file will not run and an error is thrown.	`uniquePolicyName="StatsPolicy1"`
`filterMinimumRunFrequency`	The lower limit of the frequency of the view publishing. Used with `filterMaximumRunFrequency` to determine which views this policy applies to.	`filterMinimumRunFrequency="1second"`
`filterMaximumRunFrequency`	The upper limit of the frequency of the view publishing. Used with `filterMinimumRunFrequency` to determine which views this policy applies to.	`filterMaximumRunFrequency="5minutes"`

Parameter	Description of parameter	Default values for StatsPolicy1
`maximumTableRecordAge`	The age of the oldest records that are retained. Used with `maximumTableRowCount` and `maximumTableSizeOnDisk` to specify the records that are deleted.	`maximumTableRecordAge="24hrs"`
`maximumTableRowCount`	The maximum number of rows that are retained in the table. If the number of rows exceeds this number, the oldest records are deleted first. Used with `maximumTableRecordAge` and `maximumTableSizeOnDisk` to specify the records that are deleted.	`maximumTableRowCount="100000"`
`maximumTableSizeOnDisk`	The maximum size of the table in megabytes (MB). The oldest records are deleted first. Used with `maximumTableRecordAgemaximumTableRecordAge` and `maximumTableRowCount` to specify the records that are deleted.	`maximumTableSizeOnDisk="200"`

The following describes the StatsPolicy1 with its default values. The StatsPolicy1 policy applies to views that are published at a frequency between 1 second and up to 5 minutes. For each view, statistics records up to 24 hours old are kept, the number of rows in the view's table does not exceed 100,000, and the total size of the table does not exceed 200 MB. Records that do not meet all three conditions are deleted. With all retention policies, the oldest records are deleted first.

Licensing and output streams

The **Licensing** tab on the Administration page provides information about the number of output streams used and which views use the output streams.

An output stream is a PI tag (data point) that is published to a target or only referenced in a view. A unique output stream is a distinct PI tag published in one or more views.

Your specific software package and licensing agreement determines the maximum number of unique output streams you can have at one time.

For example, assume that PI Integrator for Business Analytics is configured with three views: `ProcLab1`, `TestPrd`, and `Fieldoutput`. `ProcLab1` uses 20 output streams (15 unique output streams, 5 non-unique output streams), `TestPrd` uses two unique output streams, and `Fieldoutput` uses 22 output streams (2 unique output streams, 20 non-unique output streams). **Output Streams by View** list displays the three views with the total output streams used in each view. The following totals are displayed:

- **Unique Output Streams Consumed** displays 19 output streams.
- **Remaining Output Streams** displays the balance of the available output streams. The total available streams depend on the maximum allowed with your license.

Increase available output streams

If the number of output streams is insufficient to meet your needs, you can upgrade to a version with a higher maximum. For more information on the available maximum output stream counts, speak with your OSIsoft account manager.

Recovering output streams

Recovering output streams from deleted views frees up the number of unique output streams available for new views. Output streams are automatically recovered internally and their recovery does not require user interaction.

Note:

It is important to understand that removing a view from the My Views page does *not* immediately change the number of unique output streams used in reference to your licensing limit. Output streams are not immediately recovered when a view is removed; they are automatically recovered after 7 days.

Change the Windows service account

PI Integrator for Business Analytics uses Windows Credential Manager to manage service account credentials and target credentials. Use the Change Service Account utility to change the service account that runs PI Integrator for Business Analytics. Note that the utility will pass all currently saved target credentials from the old service account to the new service account.

Before you start

Verify that you have the following permissions:

- Local Administrator privileges on the Microsoft Windows Server where PI Integrator for Business Analytics is installed
- Administrator privileges on the PI AF Server where the PI Integrator for Business Analytics Configuration database is installed

  Note:

  The PI AF Server is identified in the `%PIHOME64%\Integrators\BA\CAST.UI.WindowsService.exe` file in the `<appSettings>` section with the `InstancePath` key.

The following permissions are also required:

- ALTER ANY LOGIN permission on SQL Server
- db_owner database role membership for the PIIntegratorDB, PIIntegratorLogs, and PIIntegratorStats databases

> **Note:**
>
> - The only exception to this is if you are using SQL authentication and you do *not* want to change the SQL account; then these additional permissions are not required.
> - If the installing user does not have the required permissions on the SQL databases, then a user with sysadmin privileges must first run the following files which can be found in `%PIHOME64%\Integrators\BA\SQL`: PI Integrator for Business Analytics 2018 R2 SQL Utility (`Go.Bat` file).
>
>   > **Note:**
>   > If you are using SQL authentication and you do *not* want to change the SQL account, then you do not need to run these files.

Once this is done, then proceed with the procedure below.

Procedure

1. From the OSIsoft Tech Support (https://techsupport.osisoft.com/) Downloads page, download the PI Integrator for Business Analytics 2018 R2 Change Service Account Utility.
2. Extract the `ChangeIntegratorServiceAccount.exe` file into the `%PIHOME64%\Integrators\BA` directory.
3. From the directory, open a command prompt as administrator and run the file.
4. Follow the prompts and provide the password for the account that currently runs the PI Integrator Framework service.

   > **Note:**
   >
   > You must first provide the password for the service account that is currently running the PI Integrator Framework service before you can change the service account.

5. Follow the prompts and provide the service account and password for the new service account that will run the PI Integrator for Business Analytics services. The Change Service Account utility adds the new account and its permissions to PI AF and SQL Server.
6. Press **Enter** to exit the utility.

Change the PI Integrator port

When you change the PI Integrator port, any users who are logged into the PI Integrator for Business Analytics web application will need to reenter the URL with the new port. Any views that are running at the time the port is changed will complete successfully.

Procedure

1. In the Microsoft Control Panel, navigate to Programs and Features.
2. Right-click **PI Integrator for Business Analytics** in the list and click **Change** in the menu.

   The PI Integrator for Business Analytics 2018 Setup window opens.
3. Click **Modify** and click **Next.**
4. In the Logon Information window, enter the username and password for the Windows service account that runs the PI Integrator Framework service. Click **Next**.

5. In the Port and SSL Certificate Configuration window, enter a different port number and click **Validate Port** to verify the availability of the port.
6. Click **Next.**
7. In the Ready to Modify the Application window, click **Install.**

   Once the installation is completed, the application uses the new port.

Change the SSL certificate configuration

Procedure

1. In the Microsoft Control Panel, navigate to Programs and Features.
2. Right-click **PI Integrator for Business Analytics** in the list and click **Change** in the menu.

   The PI Integrator for Business Analytics Setup window opens.
3. Click **Modify** and click **Next.**
4. In the Logon Information window, enter the username and password for the Windows service account that runs the PI Integrator Framework service. Click **Next.**
5. In the Port and SSL Certificate Configuration window, choose an SSL certificate from one of the following sources:
   - Self-signed certificate that is generated during the installation – This is the default. Choose **Self-signed certificate.**

     Note:
     If you choose this option, users logging in from remote machines may see a security warning message. To avoid this warning for self-signed certificates, the certificate must be explicitly trusted on the client machine. See the workaround in the OSIsoft Tech Support article KB01415 - Certificate error returned when navigating to a PI Vision or PI Web API web site using a self-signed certificate (https://techsupport.osisoft.com/Troubleshooting/KB/KB01415/).
   - (Recommended) SSL certificate from a certificate authority – Choose **Import certificate** and click **Select Certificate** to choose a certificate that has been issued by a certificate authority and imported to the machine where PI Integrator for Business Analytics is being installed.
6. Click **Next.**
7. In the Ready to Modify the Application window, click **Install.**

   Once the installation is completed, the application uses the new SSL certificate.

Unsupported data types

Int16

PI Integrator for Business Analytics does not support the `Int16` data type in these situations:

- Data written to AWS S3 targets using the Parquet format cannot be published as `Int16` data.
- Avro serialized data published to any streaming target cannot be published as `Int16` data.

In these situations, PI Integrator for Business Analytics automatically converts the `Int16` data to `Integer` data type.

Reserved strings

Oracle Targets

PI Integrator for Business Analytics reserves the case-insensitive strings *ID*, *PIIntTSTicks*, and *PIIntShapeID*. If any columns are named with these reserved strings, an underscore (_) is appended to the string, for example, *ID_* or *Id_*.

The Oracle Database reserves an additional list of words. If these words appear in a view column name, an underscore (_) is appended to them. For example, *ACCESS* would be changed to *ACCESS_*. Refer to Oracle documentation for more information on Oracle reserved words.

The list of Oracle Database reserved words follows:

```
ACCESS

ADD

ALL

ALTER

AND

ANY

AS

ASC

AUDIT

BETWEEN

BY

CHAR

CHECK

CLUSTER

COLUMN

COMMENT

COMPRESS

CONNECT

CREATE

CURRENT

DATE

DECIMAL

DEFAULT

DELETE

DESC

DISTINCT
```

```
DROP

ELSE

EXCLUSIVE

EXISTS

FILE

FLOAT

FOR

FROM

GRANT

GROUP

HAVING

IDENTIFIED

IMMEDIATE

IN

INCREMENT

INDEX

INITIAL

INSERT

INTEGER

INTERSECT

INTO

IS

LEVEL

LIKE

LOCK

LONG

MAXEXTENTS

MINUS

MLSLABEL

MODE

MODIFY

NOAUDIT

NOCOMPRESS

NOT

NOWAIT
```

```
NULL

NUMBER

OF

OFFLINE

ON

ONLINE

OPTION

OR

ORDER

PCTFREE

PRIOR

PRIVILEGES

PUBLIC

RAW

RENAME

RESOURCE

REVOKE

ROW

ROWID

ROWNUM

ROWS

SELECT

SESSION

SET

SHARE

SIZE

SMALLINT

START

SUCCESSFUL

SYNONYM

SYSDATE

TABLE

THEN

TO

TRIGGER
```

```
UID
UNION
UNIQUE
UPDATE
USER
VALIDATE
VALUES
VARCHAR
VARCHAR2
VIEW
WHENEVER
WHERE
WITH
```

Supported SQL query parameters

The data in PI Views can be consumed by any Business Intelligence tool that is compatible with PI ODBC. A subset of SQL data types, statements, operators and functions supported by PI ODBC can be used with PI Views. The following sections describe this support:

- Supported SQL data types
- Supported SELECT statement syntax
- Supported operators and functions

Supported SQL data types

PI Integrator for Business Analytics supports the following PI AF data types:

- Boolean
- Byte
- DateTime
- Double
- Guid
- Int16
- Int32
- Int64
- Single
- String

Supported SELECT statement syntax

PI Integrator for Business Analytics supports the following SELECT statement syntax:

Note:
In general, ensure proper consideration for sizing of the data sets involved, and be sure to have these sizing considerations for your data set requirements match your system resources.

```
<select_statement> ::=
<query>
[UNION ALL <query> [UNION ALL… ]]
[ORDER BY <expression> [ASC | DESC] [, …]]
```

```
<query> ::=
SELECT [ALL | DISTINCT] [TOP integer_value] <select_list>
[FROM table_source [, …]
[WHERE <condition>]
[GROUP BY [ALL] <expression> [, …]]
```

```
<select_list> ::=
{* |
{table_name | view_name | table_alias} .* |
<expression> [[AS] column_alias] |
column_alias = <expression>}
[, …]
```

```
<table_source> ::=
table_name [[AS] table_alias] |
view_name [[AS] table_alias] |
<select_statement> [[AS] table_alias] |
<joined_table> [[AS] table_alias]
```

```
<joined_table> ::=
<table_source> [INNER | LEFT [OUTER] | RIGHT [OUTER] | FULL [OUTER]] JOIN
<table_source> ON <condition>
```

```
<condition> ::=
{[NOT] <predicate> | (<condition>)}
[{AND | OR} <condition>]
[, …]
```

```
<predicate> ::=
<expression> {= | > | < | >= | <= | <> | !=} <expression> |
<expression> [NOT] IN ({<expression> [, …]) |
<expression> [NOT] BETWEEN <expression> AND <expression> |
<expression> [NOT] LIKE <expression> [ESCAPE <expression>] |
<expression> IS [NOT] NULL
```

```
<expression> ::=
<expression_factor> |
<expression > {+ | - | * | / | %} <expression>
```

```
<expression_factor> ::=
integer_value | float_value | string_value |
True | False |
NULL | ? | column_name |
CAST (<expression> AS data_type_name) |
COUNT (*) |
aggr_function_name ([ALL | DISTINCT] <expression>) |
nonaggr_function_name ([<expression> [, …]]) |
[+ | -] <expression_factor> |
(<expression>) |
NULLIF (<expression>, <expression>) |
COALESCE (<expression>, …) |
CASE <expression> WHEN <expression> THEN <expression> [WHEN …] [ELSE
<expression>] END |
CASE WHEN <condition> THEN <expression> [WHEN …] [ELSE <expression>] END
```

Note:
Brackets ([ ]) denote optional parts of the statement, braces ({ }) with vertical bars (|) denote mutually exclusive parts.

Supported operators and functions

Arithmetic operators

PI Integrator for Business Analytics supports the following arithmetic operators: +, -,*,/, and %.

PI Integrator for Business Analytics supports arithmetic operators for all numeric data types. In addition, it supports the following operator overloads:

- `AnsiString Operator+(x AnsiString, y AnsiString)`
- `String Operator+(x String, y String)`

Mathematical Functions

PI Integrator for Business Analytics supports the following mathematical functions:

Function	Syntax

ABS	`Int32 ABS(x Int32)`
	`Int64 ABS(x Int64)`
	`Single ABS(x Single)`
	`Double ABS(x Double)`

ACOS	`Single ACOS(x Single)`
	`Double ACOS(x Double)`

ASIN	`Single ASIN(x Single)`
	`Double ASIN(x Double)`

ATAN	`Single ATAN(x Single)`
	`Double ATAN(x Double)`

ATN2	`Single ATN2(x Single, y Single)`
	`Double ATN2(x Double, y Single)`

CEILING	`Single CEILING(x Single)`
	`Double CEILING(x Double)`

COS	`Single COS(x Single)`
	`Double COS(x Double)`

EXP	`Single EXP(x Single)`
	`Double EXP(x Double)`

FLOOR	`Single FLOOR(x Single)`
	`Double FLOOR(x Double)`

LOG	`Single LOG(x Single)`
	`Double LOG(x Double)`

LOG10	`Single LOG10(x Single)`
	`Double LOG10(x Double)`

PI	`Double PI()`

POWER	`Single POWER(x Single, y Single)`
	`Double POWER(x Double, y Double)`

Function	Syntax

ROUND	`Single ROUND(x Single)`
	`Single ROUND(x Single, y Int32)`
	`Double ROUND(x Double)`
	`Double ROUND(x Double, y Int32)`

SIN	`Single SIN(x Single)`
	`Double SIN(x Double)`

SQRT	`Single SQRT(x Single)`
	`Double SQRT(x Double)`

TAN	`Single TAN(x Single)`
	`Double TAN(x Double)`

String Functions

PI Integrator for Business Analytics supports the following string functions:

Function	Syntax

CHARINDEX	`Int32 CHARINDEX(toFind AnsiString, s AnsiString)`
	`Int32 CHARINDEX(toFind AnsiString, s AnsiString, start Int32)`
	`Int32 CHARINDEX(toFind String, s String)`
	`Int32 CHARINDEX(toFind String, s String, start Int32)`

LEFT	`AnsiString LEFT(s AnsiString, n Int32)`
	`String LEFT(s String, n Int32)`

LEN	`Int32 LEN(s AnsiString)`
	`Int32 LEN(s String)`

LOWER	`AnsiString LOWER(s AnsiString)`
	`String LOWER(s String)`

LTRIM	`AnsiString LTRIM(s AnsiString)`
	`String LTRIM(s String)`

REPLACE	`AnsiString REPLACE(`
	`s AnsiString, findWhat AnsiString, replaceWith AnsiString)`
	`String REPLACE(s String, findWhat String, replaceWith String)`

REVERSE	`AnsiString REVERSE(s AnsiString)`
	`String REVERSE(s String)`

RIGHT	`AnsiString RIGHT(s AnsiString, n Int32)`
	`String RIGHT(s String, n Int32)`

Function	Syntax

RTRIM	`AnsiString RTRIM(s AnsiString)`
	`String RTRIM(s String)`

SUBSTRING	`AnsiString SUBSTRING(s AnsiString, start Int32, count Int32)`
	`String SUBSTR(s String, start Int32, count Int32)`

UPPER	`AnsiString UPPER(s AnsiString)`
	`String UPPER(s String)`

Aggregate Functions

PI Integrator for Business Analytics supports the following aggregate functions: AVG, COUNT, MAX, MIN, and SUM.

Aggregate functions are implemented in compliance with ANSI SQL. PI Integrator for Business Analytics supports all ODBC-defined scalar functions except: **Char_Length**, **Character_Length**, **Database**, **Difference**, **SoundEx**, and **User.**

Refer to the following link for detailed description of scalar functions (https://msdn.microsoft.com/en-us/library/ms711813(v=vs.85).aspx) on the Microsoft web site.

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.