



# PI Connector for MQTT Sparkplug

1.0.0.6

© 2015-2024 AVEVA Group Limited and its subsidiaries. All rights reserved.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, mechanical, photocopying, recording, or otherwise, without the prior written permission of AVEVA Group Limited. No liability is assumed with respect to the use of the information contained herein.

Although precaution has been taken in the preparation of this documentation, AVEVA assumes no responsibility for errors or omissions. The information in this documentation is subject to change without notice and does not represent a commitment on the part of AVEVA. The software described in this documentation is furnished under a license agreement. This software may be used or copied only in accordance with the terms of such license agreement. AVEVA, the AVEVA logo and logotype, OSIsoft, the OSIsoft logo and logotype, Archedra, Avantis, Citect, DYNsIM, eDNA, EYESIM, InBatch, InduSoft, InStep, IntelaTrac, InTouch, Managed PI, OASyS, OSIsoft Advanced Services, OSIsoft Cloud Services, OSIsoft Connected Services, OSIsoft EDS, PIPEPHASE, PI ACE, PI Advanced Computing Engine, PI AF SDK, PI API, PI Asset Framework, PI Audit Viewer, PI Builder, PI Cloud Connect, PI Connectors, PI Data Archive, PI DataLink, PI DataLink Server, PI Developers Club, PI Integrator for Business Analytics, PI Interfaces, PI JDBC Driver, PI Manual Logger, PI Notifications, PI ODBC Driver, PI OLEDB Enterprise, PI OLEDB Provider, PI OPC DA Server, PI OPC HDA Server, PI ProcessBook, PI SDK, PI Server, PI Square, PI System, PI System Access, PI Vision, PI Visualization Suite, PI Web API, PI WebParts, PI Web Services, PRISM, PRO/II, PROVISION, ROMEo, RLINK, RtReports, SIM4ME, SimCentral, SimSci, Skelta, SmartGlance, Spiral Software, WindowMaker, WindowViewer, and Wonderware are trademarks of AVEVA and/or its subsidiaries. All other brands may be trademarks of their respective owners.

#### U.S. GOVERNMENT RIGHTS

Use, duplication or disclosure by the U.S. Government is subject to restrictions set forth in the license agreement with AVEVA Group Limited or its subsidiaries and as provided in DFARS 227.7202, DFARS 252.227-7013, FAR 12-212, FAR 52.227-19, or their successors, as applicable.

AVEVA Legal Resources: <https://www.aveva.com/en/legal/>

AVEVA Third Party Software Notices and Licenses: <https://www.aveva.com/en/legal/third-party-software-license/>

# Contents

<b>PI Connector for MQTT Sparkplug 1.0</b>	<b>5</b>
<b>Introduction to PI Connector for MQTT Sparkplug</b>	<b>6</b>
PI Connector for MQTT Sparkplug operational overview	6
PI Point Naming for PI Connector for MQTT Sparkplug	7
Connector generated quality events	8
Quality of Service (QoS) levels	8
PI AF structure for PI Connector for MQTT Sparkplug	9
MQTT server level redundancy	10
MQTT server disconnection	10
Properties	10
Node and device status	11
<b>Prepare for connector installation</b>	<b>12</b>
Software and hardware requirements for connectors	12
Upgrades of connectors	13
Connector security	13
Security best practices for PI Connector for MQTT Sparkplug	13
Sensitive data security	13
Firewall configuration	14
Create the Windows account for the connector	15
Identify the administration port number	16
Identify administration group users	16
<b>Install the connector</b>	<b>18</b>
Configure silent installation for connectors	19
Change connector installation settings	19
Uninstall the connector	20
Uninstall the connector in silent mode	20
Troubleshoot installation	21
<b>Connector configuration</b>	<b>22</b>
Open the administration website of the connector	22
Register the connector	22
Add a data source	23
Data source configuration settings for MQTT Sparkplug	23
Data source configuration reference for MQTT Sparkplug	24
Modify data sources	25
Discover data source contents and select assets and PI points for data collection	25
Start and stop data collection	28

**Verify connection from data source to the connector ..... 29**

**Verify data collection ..... 29**

    Message logs ..... 29

    Advanced diagnostics ..... 30

    PI Connector Relays ..... 31

**Interactions with Data Archive and AF ..... 31**

**Release notes ..... 32**

**Technical support and other resources ..... 34**

# PI Connector for MQTT Sparkplug 1.0

PI Connector for MQTT Sparkplug retrieves data from MQTT servers to the PI Server. MQTT is a messaging protocol that was created for Machine-to-Machine (M2M)/Internet of Things (IOT) communication.

For details about this release, see the [Release notes](#).

# Introduction to PI Connector for MQTT Sparkplug

PI Connector for MQTT Sparkplug is an MQTT client that retrieves data from MQTT servers with service nodes and devices adhering to the Sparkplug specification. The Sparkplug specification, created for Machine-to-Machine (M2M)/Internet of Things (IOT) communications, allows communication between MQTT clients through an MQTT server (broker). It uses the lightweight MQTT publish/subscribe messaging protocol to define an MQTT topic namespace, an MQTT message payload format, and a method for performing MQTT state management.

Clients subscribe to topics to publish and receive messages. Servers manage the communication between clients by keeping track of client subscriptions to topics, and by forwarding published messages to the appropriate clients.

PI Connector for MQTT Sparkplug collects data when new data is published to subscribed topics. The connector is notified, through a process called report-by-exception, and the new data is processed.

PI Connector for MQTT Sparkplug can connect to multiple MQTT servers and can be configured to specific topics using standard MQTT topic filtering. The publish/subscribe infrastructure effectively standardizes SCADA/IIoT communications.

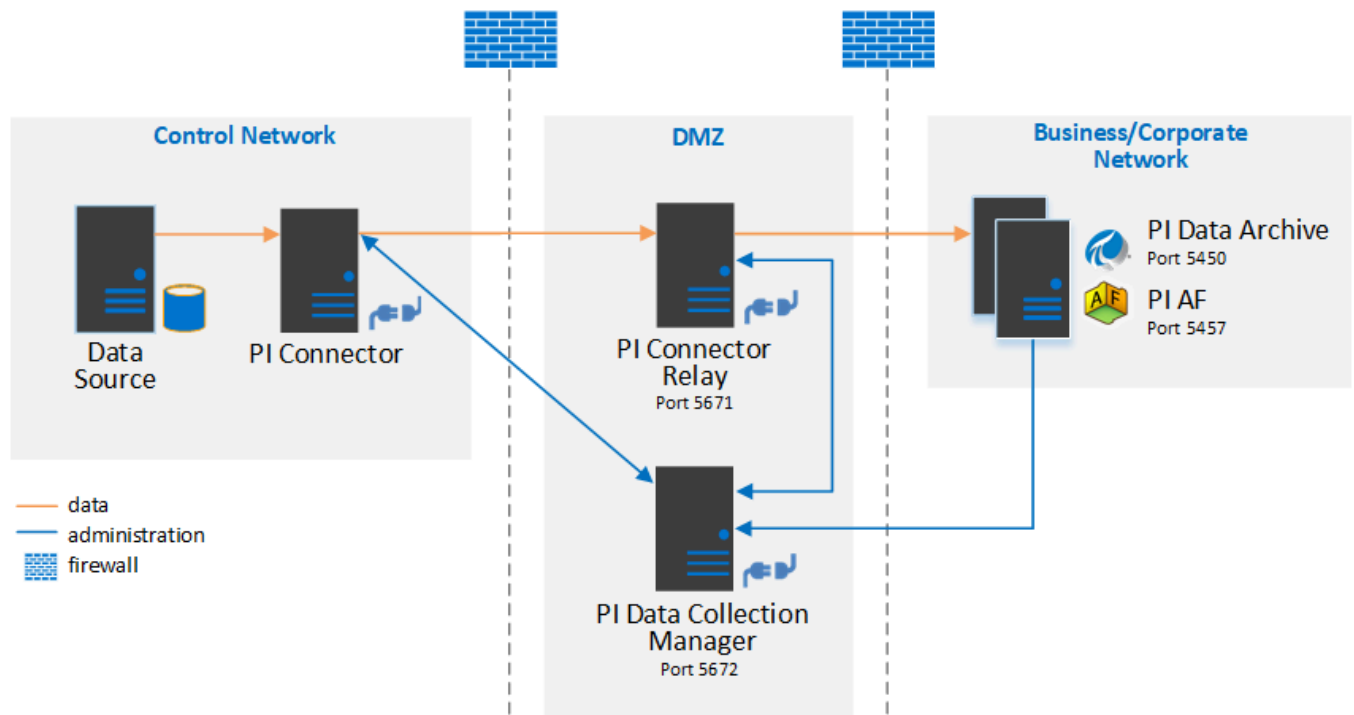
## PI Connector for MQTT Sparkplug operational overview

Each PI connector is designed for a specific data source. PI Connector for MQTT Sparkplug queries the data source to discover assets, relations between assets, time-series measurements, and relations between assets and time-series measurements that the data source contains. The connector creates generalized streams to convey the assets, relationships, and time-series measurements to one or more PI Connector Relay hosts.

The connector output streams are generalized in the sense that they are independent of the databases or historians that store data from the streams. For more information about connectors in general, refer to the Overview of PI Connectors user guide.

The following figure shows the data flow from a data source to the PI System.

**PI connector architecture diagram**



In this figure, the connector communicates with PI Connector Relay over an encrypted TCP connection, which allows it to be on a different computer.

Although the figure shows only one PI Connector Relay host, a connector can replicate its output streams to multiple PI AF hosts. Similarly, a PI Connector Relay can support multiple PI AF servers and Data Archive servers, including collectives.

The connector does not communicate directly to any type of historian or database. Streams from the connector are strictly one-way to the PI Connector Relay host, which means that it cannot obtain any information from either PI AF or Data Archive.

Both the connector and PI Connector Relay communicate with PI Data Collection Manager, which is used to specify all settings for the configuration. For additional information about PI Connector Relay and PI Data Collection Manager, refer to PI Connector Administration user guide.

## Asset creation and data collection

From the response, the connector creates the PI AF element hierarchy and PI points in Data Archive. Each device is represented as an element in PI AF. Therefore, an AF data reference attribute is created for each measurement under the corresponding device.

The PI points' time stamps are based on the "timestamp" field in the metric. If there is no "timestamp" field, then it uses the "timestamp" field of the message. If there is no "timestamp" field on the message, the current time of the machine that the connector is running on is used. Aliasing of metric names is supported.

**Note:** For more information on the point source of the PI points created, see [Data source configuration settings for MQTT Sparkplug](#).

## PI Point Naming for PI Connector for MQTT Sparkplug

The Sparkplug specification requires the following topic structure:

namespace/group\_id/message\_type/node\_id/[device\_id] where the device\_id is optional.

The connector creates PI points using the Sparkplug topic namespace. The PI points are named as follows:

*Prefix Point.Connector Name.Data source name/namespace/group\_id/node\_id/[device\_id]/name*

For example, if a message is published to the topic:

**spBv1.0/Edge Group/DDATA/Edge Node 1/Edge Device 1** for a tag with the name *Test/Test Tag*, a point is then created with the following name:

*Prefix Point.Connector name.Data source name/spBV1.0/Edge Group/Edge Node 1/Edge Device 1/Test/Test Tag*

**Note:** The Prefix Point can be customized using the PI Data Collection Manager

## Connector generated quality events

The connector generates quality events in each value stream to mark exceptional conditions. The connector-generated quality events are recorded in the archives of historians in the same manner as measurement values from the data source. Connector-generated events occur under the following conditions:

- Start and stop data collection (optional).
- Addition or deletion of a measurement (optional).

PI Connectors use the OPC quality codes in section 6.8 of the *OPC Data Access Custom Interface Specification (version 3.0)*. Additionally, PI Connector for MQTT Sparkplug uses the following quality codes for connector generated quality events:

Code	Description	Cause
32 (decimal) 00 1000 00 (binary)	Waiting for initial data	Initial quality event for all data collection starts. Initial quality event when a PI point is added or selected.
8 (decimal) 00 0010 00 (binary)	Not connected	Stopped quality event for all streams when data collection stops. Quality event when a PI point is deselected.

## SYSTEM digital states

In order to know when there is an event, the connector writes the appropriate SYSTEM digital state to the tags. SYSTEM digital states are, for example, Shutdown or IO Timeout.

## Quality of Service (QoS) levels

The connector uses these QoS levels for the topics it will send to and request from:

- Sending an NCMD message for rebirths: QoS 2.



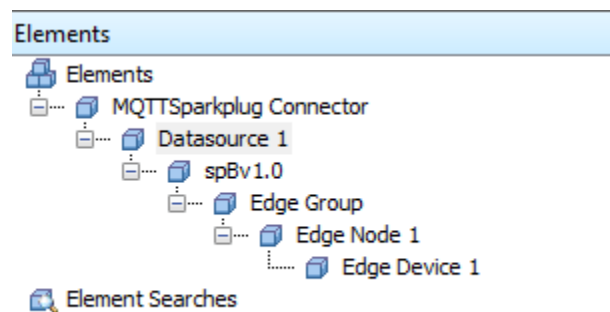
- Subscribing to a topic: The default is QoS 2, but you can set a custom QoS in the **Topics** file.

See [Data source configuration settings for MQTT Sparkplug](#) and [Data source configuration reference for MQTT Sparkplug](#).

## PI AF structure for PI Connector for MQTT Sparkplug

As stated previously, the Sparkplug specification requires the following topic structure: namespace/group\_id/message\_type/node\_id/[device\_id] where the device\_id is optional.

The connector builds an asset hierarchy using the Sparkplug topic namespace. The asset structure is as follows: group\_id->node\_id->device\_id. For example, if a message is published to the topic *spBv1.0/Edge Group/DDATA/Edge Node 1/Edge Device 1*, the following PI AF structure is created:



An asset is created for each "folder", with the asset containing PI tags for that folder. For example, a metric named Edge Node 1/Edge Device 1/Analog Input 1 and published to topic *spBv1.0/Complex/DDATA/Set 1/Edge Group* may have an asset created like this:

Name	Value	Time Stamp
Template: MQTT Sparkplug Connector.2E88D2F3		
Analog Input 1	0	3/20/2019 3:52:40.509 PM
Analog Input 2	10100	3/20/2019 3:52:40.509 PM

If the metric property contains a property named *engUnit*, the connector will attempt to use that property as the PI point's unit of measure.

The screenshot shows the AVEVA PI Connector for MQTT Sparkplug interface. On the left, a tree view displays the hierarchy of elements, including 'Elements', 'Untitled Connector 1', 'Datasource 1', 'spBv1.0', 'Complex', 'Set 1', 'Edge Group', 'Device Control', 'Edge Node 1', 'Edge Device 1', 'Test', 'Node Control', 'Node Info', 'Sparkplug B Devices', 'llgsdsf', 'spBv1.0', 'mos', and 'Element Searches'. On the right, the 'Edge Node 1' tab is active, showing a table of data points. The table has columns for Name, Value, and Time Stamp. The data points are as follows:

Name	Value	Time Stamp
1 SByte Int1Tag	55 rpm	3/20/2019 3:52:40.1
2 Short Int2 Tag	8	3/20/2019 3:52:40.1
3 Integer Int4 Tag	19 m	3/20/2019 3:52:40.1
4 Long Int8 Tag	100	3/20/2019 3:52:40.1
9 Float Float4 Tag	7	3/20/2019 3:52:40.1
10 Double Float8 Tag	12.5	3/20/2019 3:52:40.1
11 Boolean Tag	0	3/20/2019 3:52:40.1
12 String Tag	test	3/20/2019 3:52:40.1
13 DateTime Tag	10/7/2017 4:00:00 PM	3/20/2019 3:52:40.1

## MQTT server level redundancy

The connector allows a maximum of three server connections per data source. An additional IP, Port, User name, Password, and CA Certificate may be needed for each additional MQTT Server.

## MQTT server disconnection

The connector checks every 30 seconds to see if it has lost connection to a server. If it has been disconnected, the connector will attempt to reconnect every 30 seconds until successful.

If you complete the primary **host id** field in the data source, the connector will set its *STATE* to ONLINE when it connects, and in its death certificate, will set its *STATE* to OFFLINE.

For reference information, see section 8 *Sparkplug MQTT Session Management and Message Flow* in the Sparkplug Specification [Sparkplug MQTT Topic & Payload Definition Version 2.1](#).

## Properties

Properties of metrics are not created. The only property that is read is the unit of measure (UOM). The UOM is included in the PI tag. For further information, see [PI AF structure for PI Connector for MQTT Sparkplug](#).

Additional device information, such as Manufacturer, Device Type, and Serial Number are received as metrics, and therefore create a PI point for each of them.

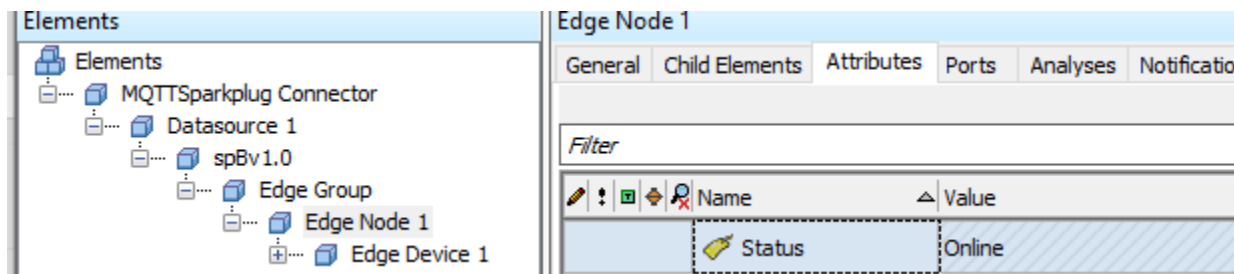
### Example: Additional device information

The screenshot shows the AVEVA PI Connector for MQTT Sparkplug interface. On the left, a tree view displays the hierarchy of elements, including 'local', 'spBv1.0', 'opto', 'spBv1.0', 'DemoCenters', 'EPIC-DC013', 'Node Control', 'Node Properties', and 'EPIC-DC131'. On the right, the 'Edge Node 1' tab is active, showing a table of device information. The table has columns for Name, Value, and Time Stamp. The data points are as follows:

Name	Value	Time Stamp
Device Type	Opto 22 Sparkplug Client (s...	3/19/2019 11:24:30.85 AM
Hardware Make	Opto 22	3/19/2019 11:24:30.85 AM
Software Version	1.1.2-08172018-1241	3/19/2019 11:24:30.85 AM

## Node and device status

A status tag (PI point) is created for each device and node representing the current status of the node or device. The status tag is a PI Digital State point. The PI point will be set to Online on receiving a BIRTH status from MQTT, and will set to Node Death or Device Death on receiving a DEATH message. The PI point will be set to Server Disconnect if the connector cannot connect to any of the data source's servers. A System digital state of Not Connect will be written when the Connector is stopped (optional).



**Digital states that can be written to the status tag (subject to change)**

	Value	Name
▶	0	Online
	1	Node_Death
	2	Device_Death
	3	Lost_Server_Connection
*		

# Prepare for connector installation

Before installing the connector, complete the following tasks.

1. Verify the host meets the software requirements for the connector.  
For more information, see [Software and hardware requirements for connectors](#).
2. If you are upgrading to a new version of the connector, review [Upgrades of connectors](#).
3. If the data source has additional requirements for installation, complete those tasks.
4. Configure security for the connector and your network.  
For more information, see [Connector security](#).
5. [Identify the administration port number](#).
6. [Identify administration group users](#).

## Software and hardware requirements for connectors

### Software requirements

The following software is required on the host where the connector is installed:

- Microsoft Windows
  - 64-bit system
  - Server class: Windows Server 2008 R2 SP1 or later
  - Client class: Windows 7 SP1, 8.1, 10
- Web browser: An HTML5-compliant web browser for access to the administration website of the connector.  
The following browsers are supported in desktop mode only:
  - Microsoft Edge version 40
  - Google Chrome version 44 or later

The following software is also required, but can be installed on other hosts:

- PI System
  - Data Archive version 3.4.380 or later
  - PI AF server 2015 (version 2.7.0) or later
- PI Connector Relay version 2.4.44 or later
- PI Data Collection Manager version 2.4.44 or later

### Hardware requirements

The following hardware is required or recommended:

- RAM: 4 GB minimum, 8 GB or more recommended
- Hard drive space: 25 GB or more
- Processor: Dual-core minimum, quad-core or greater recommended

## Upgrades of connectors

If you are upgrading your connector, you need to follow the installation procedure as described in [Install the connector](#) and be aware of the following:

- If your current connector uses PI Data Collection Manager version 2.2 or earlier, you must install PI Data Collection Manager version 2.3 *before* upgrading to a new version of the connector. For information on installation of PI Data Collection Manager version 2.3 or later, see the [PI Connector Administration 2.3 or later user guides](#).
- When specifying the user name in the Windows Service Configuration window during installation, it allows you to specify a log on user different than the user already configured to run the connector service.

---

**Caution:** If you change the log on user and the connector already has data sources configured, the connector might not be able to communicate with the server after the upgrade.

---

## Connector security

The following topics describe security procedures to ensure the integrity of your data; however, some data source protocols are inherently insecure. OSIsoft recommends you review the security standards for your data source to determine the appropriate security measures necessary to secure your system.

## Security best practices for PI Connector for MQTT Sparkplug

The connector currently supports TLS v1.2. You must upload a CA certificate in the data source configuration in order to use a secure connection. The certificate received from the server must be valid and either the root certificate must be in the Windows Certificate Store (Local Machine -> Trusted Root Certification Authorities), or match the uploaded certificate. You can provide any certificate in the data source configuration if the valid certificate exists in the Windows Certificate Store.

- To do server validation, you must upload a certificate in the data source configuration even if the valid certificate already exists in the Windows Certificate Store.
- OSIsoft recommends using an *insecure connection* to test for dataflow before using TLS and certificates.

## Sensitive data security

### Passwords

Passwords may be used by connectors to access data sources. These passwords are located in the data source configuration files on the connector and PI Data Collection Manager hosts.

- On the connector host, the data source configuration file **Datasource.config.json** is stored in the **%PIHOME64%\Connectors\ConnectorName\Configuration** folder.
- On the PI Data Collection Manager host, the data source configuration information is stored in the **NodeMap.config.json** file in the **%PIHOME64%\Data Collection Manager\DataCollectionManager\Configuration** folder.

---

**Note:** The Microsoft Data Protection API (DPAPI) is used to perform encryption for connectors that encrypt confidential information such as passwords.

---

## Cryptographic keys

Connectors create two X.509 certificates at installation time for each connector application (connector, PI Connector Relay, and PI Data Collection Manager). The first X.509 certificate is used to secure an HTTPS connection used for application administration. The second X.509 certificate is used to secure AMQPS communication. The private keys for these certificates are stored in the Windows Certificate Store.

## Firewall configuration

You must properly configure firewalls to support the connector.

## Remote administration

The connector process hosts a web service for connector administration. To access the connector administration pages from a remote host, all firewalls between the remote host (running a compatible browser) and the connector host must allow the browser to open a connection to the administration port that is assigned to the connector during installation. For example, if Windows firewall is enabled on the connector host, Windows firewall needs to allow incoming connections to the connector administration port from remote hosts that are permitted to administer the connector.

Access to the connector's web page can be restricted to the local host alone. The firewall for listening on that port does not have to be open to remote machines. For administering the connector using PI Data Collection Manager, no listening ports on the connector are required. This is a more secure way to administer the connector remotely. This is possible because the connector initiates the connection to PI Data Collection Manager. The connection is required for users to perform administrative tasks, such as configuring which relay to send data and data selection.

## PI Connector to PI Data Collection Manager Security

Communication between the connector and PI Data Collection Manager occurs using Advanced Message Queuing Protocol (AMQP) over TCP on port 5672. This port is not configurable. The channel communication is secured by self-signed certificates that are created during installation. These same certificates are also used for authentication. If any firewalls are in the network route from the connector to PI Data Collection Manager, all firewalls must be configured to permit the connector to open connections to TCP port 5672 on the PI Data Collection Manager host.

---

**Note:** The firewalls can be physical network devices or the Windows firewall on the PI Data Collection Manager or connector hosts.

---

When a registration request is submitted from a connector to PI Data Collection Manager, the connector initiates

a security handshake outbound to the PI Data Collection Manager administration port. (The administration port is selected during installation of PI Data Collection Manager; the default port is 5460.) During the security handshake, the connector and PI Data Collection Manager exchange certificates to use for authenticating and encrypting communication. The security handshake will complete and communication between the connector and PI Data Collection Manager will occur only if the administrator approves the registration request in PI Data Collection Manager. Once the request is approved, the connector can be administered using PI Data Collection Manager. Communication between the connector and PI Data Collection Manager will now occur exclusively using AMQP over port 5672.

---

**Note:** The administration port (default 5460) on PI Data Collection Manager must remain open to the connector machine during the security handshake. After the security handshake is complete, the PI Data Collection Manager administration port can be closed to the connector. However, the 5672 communication port (AMQP), outbound from the connector to PI Data Collection Manager, must remain open between the connector and PI Data Collection Manager to allow them to communicate with each other.

---

## PI Connector to PI Connector Relay security

Communication between a connector and PI Connector Relay occurs using Advanced Message Queuing Protocol (AMQP) over TCP on port 5671. This port is not configurable. The channel is secured by self-signed certificates that are created during installation. The same certificates are also used for authentication. If any firewalls are in the network route from the connector to the relay, all firewalls must be configured to permit the connector to open connection to TCP port 5671 on the relay host.

---

**Note:** The firewalls can be physical network devices or the Windows firewall on relay or connector hosts.

---

When configuring data flow from connector to relay, PI Data Collection Manager initiates a security handshake between the connector and the relay. During the security handshake, the connector and relay exchange certificates for authenticating and encrypting that allow data communication. PI Data Collection Manager exchanges a certificate between the connector and the relay, and then the relay returns the certificate. Secure data communication between the connector and relay will then occur using AMQP over port 5671.

## Create the Windows account for the connector

You must create a Windows account to host the connector. There are two types of accounts:

- Windows domain accounts are the more secure option for hosting the connector. In a domain environment, a domain controller performs authentication for centralized control.
- Windows workgroups are the less secure option for hosting the connector. In a workgroup environment, all computers are peers and authentication is performed locally.

Determine whether the connector host is part of a Windows domain or workgroup. Computer domain information can be found in the Control Panel system information, in the **Computer name, domain, and workgroup settings** area.

Create either a dedicated domain account, or local account for the connector.

---

**Note:** The account should not be a member of the host's local administrators group. You may need to contact your IT department to create accounts.

---

- If the computer is part of a domain, create a dedicated domain account for the connector.  
You must have domain administrator privileges to create domain accounts.

- If the computer is part of a workgroup, create a local account for the connector.  
You must have local administrator privileges to create local accounts.

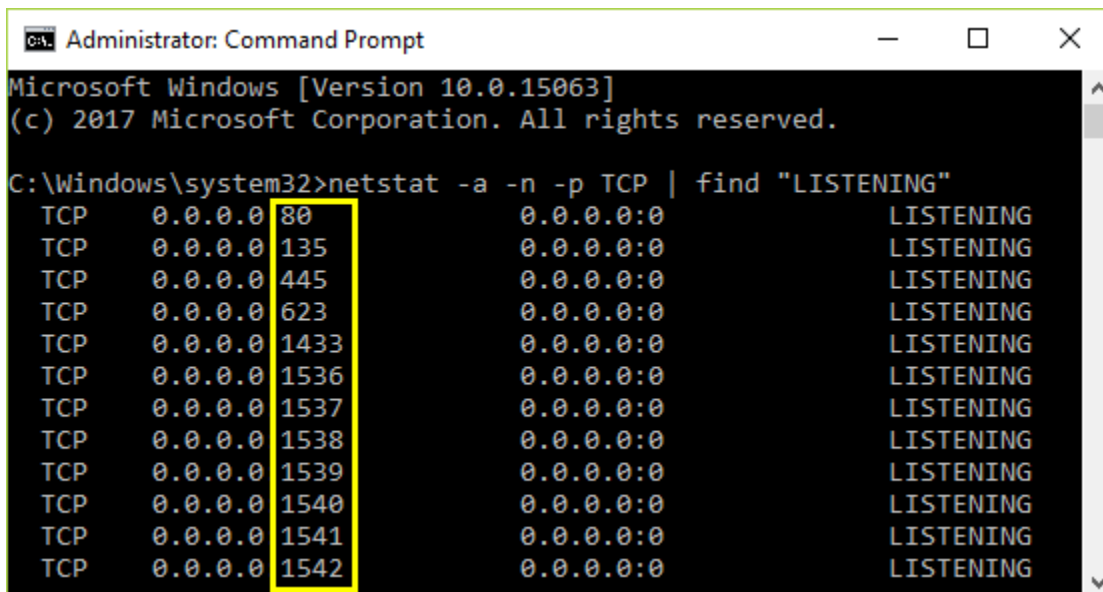
## Identify the administration port number

The connector service uses a TCP port to host the administration web service. If you intend to access the web service from a remote host, all firewalls between the remote host and connector host must permit a browser on the remote host to open a connection to the web service. For example, if Windows firewall is enabled on the connector host, configure Windows firewall to allow access to the configured web service port from approved remote hosts.

Determine an unused TCP port for the web service before installing the connector software. You are prompted to enter this port number during installation.

1. Open a command prompt and enter: `netstat -a -n -p TCP | find "LISTENING"`

The tool displays only TCP ports that are currently in use.



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Windows\system32>netstat -a -n -p TCP | find "LISTENING"
TCP    0.0.0.0:80          0.0.0.0:*        LISTENING
TCP    0.0.0.0:135        0.0.0.0:*        LISTENING
TCP    0.0.0.0:445        0.0.0.0:*        LISTENING
TCP    0.0.0.0:623        0.0.0.0:*        LISTENING
TCP    0.0.0.0:1433       0.0.0.0:*        LISTENING
TCP    0.0.0.0:1536       0.0.0.0:*        LISTENING
TCP    0.0.0.0:1537       0.0.0.0:*        LISTENING
TCP    0.0.0.0:1538       0.0.0.0:*        LISTENING
TCP    0.0.0.0:1539       0.0.0.0:*        LISTENING
TCP    0.0.0.0:1540       0.0.0.0:*        LISTENING
TCP    0.0.0.0:1541       0.0.0.0:*        LISTENING
TCP    0.0.0.0:1542       0.0.0.0:*        LISTENING
```

2. View the last set of numbers in the second column to determine ports that are in use.  
For example, the preceding figure shows that ports 80, 135, 445, and so on are in use. The default port 5460 is available, or you can choose another unused port. Since default and other well-known ports can be the targets of cyber attacks, choosing a non-default port can provide an additional defense.

## Identify administration group users

To configure and administer the connector, users must belong to the local Windows PI Connector Administrators group on the computer where the connector is installed.

1. Identify all local or domain users that require administrative privileges for the connector.
2. Use Windows tools to add and remove appropriate users.

During installation, you are prompted to add these users. After installation, you can use Windows



administration tools to add or remove users from the PI Connector Administrators group at any time.

---

**Note:** When selecting users for the PI Connector Administrators group, be aware that users in this group can locally or remotely stop and start connectors and modify configurations.

---

# Install the connector

## Before you start

Ensure all connector-specific installation requirements are met to successfully install the connector. See [Prepare for connector installation](#).

If you are installing an upgraded connector, see [Upgrades of connectors](#) for important information before installing the connector.

---

**Note:** You must be logged in to a Windows account with administrator privileges.

---

## Procedure

1. Start the connector installation kit.
2. Set the extraction path for the installation files and click **OK**.  
The connector setup wizard opens.
3. Install and configure all required software using the installation wizard.  
The setup program installs the prerequisite software and opens the connector installation wizard to guide you through connector configuration choices.
4. Configure the following items:
  - Administration port number for hosting the administration web service.
  - Windows service account information. The installation wizard automatically adds the connector service account to the PI Connector Administrators group.
  - Optional: Alternate file path for buffer and other local files.
5. Click **Install**.
6. Add all local or domain users that require administrative privileges to the PI Connector Administrators group, and then click **Next**.  
Users must belong to this group to configure and perform administrative tasks for the connector.
7. Click **Finish** to exit the installer.

If connector installation is not successful, see [Troubleshoot installation](#).

---

**Note:** Catalog files are separate downloadable files, and are used for application whitelisting. If you use whitelisting, install the catalog files associated with your OSIsoft products to ensure that those products function as intended. Windows catalog files that have been digitally signed by OSIsoft can be used as a digital signature for 3rd party and other unsigned components installed by OSIsoft setup kits. This facilitates a trusted way to verify these components and may be used for whitelisting purposes. For information on how to use catalog files for whitelisting, refer to the OSIsoft Knowledge Base article: [Whitelisting PI applications based on catalog files](#).

---

## Configure silent installation for connectors

You can install this software with the Windows silent installation feature. Sometimes called an unattended installation, silent installation requires no user interaction during the setup process. System administrators with an automated software distribution application can use silent installation to deploy software automatically to large numbers of corporate computers.

Modify the **silent.ini** file to configure silent installation. Configuring the **silent.ini** file determines items that you would have selected during a normal installation with the connector installation wizard.

### Before you start

See [Prepare for connector installation](#).

### Procedure

1. Prepare the silent installation file path and identify the status of supporting software.
  - a. Run the connector setup kit self-extracting executable file.

The self-extracting window opens. You will only complete the step to extract the installation files, not actually proceed to install the connector or prerequisites.

- a. Enter an extraction path and click **OK**.

The installation files are extracted and the setup program opens.

- a. Cancel the installation.

2. Go to the extraction folder, and open the **silent.ini** file in a text editor.
3. Modify the *COMMANDLINE* section for the module for the connector.

See the **silent.ini** file included in the setup kit for more details about each of the configurable settings:

- Required: *SERVICE\_ACCOUNT*. Set this property to the domain and name of the Windows account for the connector service.
- Required: *SERVICE\_ACCOUNT\_PASSWORD*. Set this property to the password for the Windows account for the connector service.

---

**Note:** The password in the **silent.ini** file is visible to any user who has read access to the file. Protect all copies of the file with an access control list that allows read access to only a white list of users who know the password and denies read access to all other users. Preferably, remove the file immediately after installation. If long-term retention is necessary, keep the file on removable media that is stored offline in a physically secure location.

---

- Optional: *USERPORT*
  - Optional: *ALTERNATEFILEPATH*
4. To run the silent installation, open a command prompt window, change the working directory to the extraction path, and enter `setup.exe -f silent.ini`.

## Change connector installation settings

---

**Caution:** Before changing installation settings, backup or save configuration so that those settings can be

---

---

referenced later if necessary.

---

The following installation settings can be changed from the connector installation wizard accessed from the Windows Control Panel. Change installation settings for the connector when:

- Reinstalling the connector software
- Replacing missing files from the installation
- Changing the administration port number
- Changing the location of the buffer and data files
- Changing the Windows account for the connector service

---

**Note:** To remove users from the PI Connector Administrators Group, modify the Windows User Accounts configuration through the Windows Control Panel.

---

## Procedure

1. Open Programs and Features as an administrator from the Windows Control Panel.
2. Select the connector program, and then click **Change**.

---

**Note:** Changing installation settings stops the connector service.

---

The connector installation wizard opens.

3. Click **Next**.  
The installation and change options are shown.
4. Click **Change** to modify the settings.
5. Change installation configurations using the wizard.

## Uninstall the connector

You can uninstall the connector with Control Panel or with the **.msi** file extracted from the setup kit.

---

**Caution:** Before uninstalling the connector, backup or save configuration so that those settings can be referenced if reinstalling later. Uninstalling the connector will remove all configuration files in the directory.

---

Uninstall the connector with one of the following methods:

- From the Windows Control Panel, open **Programs and Features**, then select the connector and click **Uninstall**.
- In the extraction folder created by the setup kit, right-click the **ConnectorName.msi** file and then click **Uninstall**.

---

**Note:** The version of the **ConnectorName.msi** file must be the same as the installed connector.

---

## Uninstall the connector in silent mode

Use silent mode to uninstall the connector from the command line.

---

**Note:** The original **ConnectorName.msi** file or a copy of the same version must be used for silent uninstall.

---

1. Open a command prompt window.
2. Change the working directory to the folder containing the **ConnectorName.msi** file.
3. Enter `msiexec -x ConnectorName.msi -qn`.

## Troubleshoot installation

If installation of the connector is not successful, you can troubleshoot installation problems by viewing the connector setup log for detailed information.

- Locate the connector setup log in **%PIHOME%\dat**.  
The connector setup log file is named **SetupConnectorName.log** where *ConnectorName* is the product name of the connector.

# Connector configuration

You can access the administration website of the connector to register the connector, add data sources, start and stop collecting data, and verify connection and data collection.

## Open the administration website of the connector

Configure and perform configuration tasks for the connector from the administration website of your PI connector using a supported browser.

See [Software and hardware requirements for connectors](#).

### Before you start

The connector service must be running. From the Windows menu, run `services.msc` to open the Services window, and then locate and start the connector service.

To access the administration website of the connector from remote computers, configure Windows firewalls and any other firewalls in the network to permit remote access to the service port.

### Procedure

1. On the computer where the connector is installed, from the Windows menu, click **All Programs > PI System > PI Connector for connector\_name Administration**.

**Note:** If you are using a remote computer, enter the following URL into the browser's address bar, using the connector's IP or hostname and port:

---

`https://IP_or_hostname:port/ui`

---

2. If your browser does not recognize the security certificate, allow your browser to access the site.
3. Log in using the account credentials using `domain\user_name` format.

The account that you log in with must belong to the local Windows PI Connector Administrators security group.

The administration website of the connector opens to the Overview page.

## Register the connector

You must register the connector from the administration website of the connector. Later, an administrator authorizes the connector using PI Data Collection Manager.

1. In the administration website of the connector, click **Set Up Connector**.
2. Enter the following settings:
  - **Registration Server Address:** The address and port number of the PI Data Collection Manager administration web service, in the format:

**https://IP\_or\_hostname:port**

The PI Data Collection Manager administrator can provide this address.

- **Registration Server User Name** and **Registration Server Password**: The user name (in the format *domain\user\_name*) and password for a user who belongs to the PI Trusted Installers Windows group on the PI Data Collection Manager host.
- **Description**: A description of the connector. This field is optional.

3. Click **Request Registration**.

The connector is authorized for data flow using PI Data Collection Manager, which is often installed on a separate host. A separate user, such as a PI System administrator, typically authorizes the connector. For more information about PI Data Collection Manager, see the PI Connector Administration user guide.

---

**Note:** The connector requires PI Data Collection Manager version 2.5 or later. If version 2.4 or earlier is installed, an error message for registration with PI Data Collection Manager will appear: PI Data Collection Manager version 2.5 or later is required (current version <version # of PI Data Collection Manager>). or, PI Data Collection Manager version 2.5 or later is required (current version cannot be determined).

---

## Add a data source

Add a data source and configure it for data collection using the administration website of the connector or the Data Collection Manager. For additional details, see the [Data collection configuration section](#) of the PI Connector Administration user guide.

1. In the Overview pane, expand **Data Sources**, and then click **Add data source**.
2. In the Data Source Details pane, expand **Data Source Settings**, and then enter the [Data source configuration settings for MQTT Sparkplug](#).
  - All data source name values for the connector must be unique.
  - Data source names are not case sensitive. For example, DataSource1 and DATASOURCE1 are treated as the same name.
3. Click **Save**.

## Data source configuration settings for MQTT Sparkplug

Each data source can be added to the connector by providing the following parameters.

- **Name**

[Required]. The name of the data source.

- Data source name values for a given connector must be unique.
- Data source names are not case sensitive. For example, DataSource1 and DATASOURCE1 are considered the same.

---

**Tip:** The data source name can be used as the point source for the PI points created. To enable this feature, update the PI Connector Relay to version 2.4 or later. If you do not upgrade to a compatible PI Connector Relay, the data flow will not be interrupted, however, you might see some errors under Relay diagnostics and the point source will display the point name.

---

- **Description**

[Optional]. The description of the data source configuration.

- **Host name or IP address**

[Required]. The name or IP address of the MQTT server.

- **Port**

[Required]. The port of the MQTT server.

- **User**

[Optional]. The user for authentication on the MQTT server.

- **Password**

[Optional]. The password for the user specified in the *User* field.

- **TLS only: CA Certificate File**

[Optional]. The server's CA Certificate file. Required to use a secure connection.

---

**Note:** This feature and its documentation content have not yet been fully implemented. Implementation is currently in the research and development stage. This placeholder has been added to indicate that the feature documentation may appear in this location in the future.

---

- **Primary Host ID**

[Required]. The ID of the Primary Host. The connector is considered the Primary Application. See *SparkplugMQTTTopic &PayloadSpecification Section 8*, posted online by Cirrus Link Solutions for details.

- **Topics**

[Required]. The CSV file containing the topic(s) filters that you want to subscribe to on the MQTT server. You may put an optional QoS after the topics. The default QoS is 2. For more information about topic rules, see [Data source configuration reference for MQTT Sparkplug](#).

## Data source configuration reference for MQTT Sparkplug

This section contains information regarding additional data source configuration information for the connector. Topics adhere to the MQTT and Sparkplug specification and must follow these rules:

- Topic names and topic filters are divided into topic levels using the / character.
- # is the multi-level wildcard and must be specified on its own or following the / character. # must be the last character.
- + is the single-level wildcard and can be used at any level. + must occupy an entire level. + can occur multiple times within a topic filter and can be used in conjunction with the # wildcard.

---

**Note:** Topic names are case sensitive and must follow the Sparkplug format of *namespace/group\_id/message\_type/node\_id/[device\_id]*.

---

- For a more detailed description on topics please refer to the MQTT specification and the Sparkplug specification.

Here are three examples of Topics CSV files you may find useful:

1. Example1.csv

```
#
```

Subscribe to all available topics.



## 2. Example2.csv

```
spBv1.0/Sparkplug B Devices/DDATA/Edge Node 1/#, 0
spBv1.0/Sparkplug B Devices/DDATA/Edge Node 2/#, 1
spBv1.0/Sparkplug B Devices/DDATA/Edge Node 3/#, 2
spBv1.0/Sparkplug B Devices/NBIRTH/Edge Node 1, 0
spBv1.0/Sparkplug B Devices/NBIRTH/Edge Node 2, 0
spBv1.0/Sparkplug B Devices/NBIRTH/Edge Node 3, 0
spBv1.0/Sparkplug B Devices/DBIRTH/EdgeNode 1/+, 0
spBv1.0/Sparkplug B Devices/DBIRTH/EdgeNode 2/+, 0
spBv1.0/Sparkplug B Devices/DBIRTH/EdgeNode 3/+, 0
```

Subscribe to topic Edge Node1 and its child topics with QoS 0, topic Edge Node 2 and its child topics with QoS 1, and topic Edge Node 3 and its child topics with QoS 2. It is required to also capture NBIRTH and DBIRTH, which are required for birth certificates and populating the data selection. You can use a generic wild card to capture NBIRTHs and DBIRTHs for simplicity, that is:

```
spBv1.0/SparkplugB Devices/NBIRTH/#, 0
spBv1.0/SparkplugB Devices/DBIRTH/#, 0)
```

You may see extraneous elements and PI tags in data selection which will never be updated (for example Edge Node 4, Edge Node 5, etc.).

## 3. Example3.csv

```
+ /MyGroup/#
```

Subscribe to any topics that have MyGroup as the second level. For example,

- *spAv1.0/MyGroup/*
- *spAv1.0/MyGroup/DDATA/*
- *spAv1.0/MyGroup/NBIRTH/Edge Node 6/*

## Modify data sources

Use the administration website of the connector to modify data sources.

1. In the Data Sources section, click the data source status box.
2. In the Data Source Settings pane, click **Edit**.
3. Edit the data source settings and click **Save**.

## Discover data source contents and select assets and PI points for data collection

The connector subscribes to the MQTT broker with the topics inside the Topics CSV file, and then automatically create PI Tags and the assets based on the data selected after performing a Discovery. Perform the steps in the procedure below to instruct the connector to automatically discover available data source contents. After the discovery process completes, you can select among available assets and value streams for data collection using PI Data Collection Manager.

## Before you begin

Make certain that the connector is running.

## Procedure

1. Select the Data Sources node and then **Discover Data Source Contents** in the *DataSourceName* Data Source Details pane.

The screenshot shows the 'Routing' configuration window. In the 'Data Sources' pane, the 'opto' data source is selected and highlighted with a red box. The 'Connectors' pane shows the 'MQTT MQTT Sparkplug' connector. The 'Relays' pane shows a 'relay' with a green checkmark. The 'Destinations' pane shows a 'ds' with a green checkmark. On the right, the 'opto Data Source Details' pane is open, showing the 'Discover Data Source Contents' button highlighted with a red box.

You can now proceed to discover the contents of the selected data source.

**Note:** Discover Data Source Contents should only be used once. If it is triggered again after discovery has been completed, it may stop data collection. As a result, you will need to restart the connector from Windows Services before it can collect data again.

2. Select the Connectors node and then **Select Data** in the *ConnectorName* Connector Details pane.

The screenshot shows the 'Routing' configuration window. In the 'Connectors' pane, the 'MQTT MQTT Sparkplug' connector is selected and highlighted with a blue box. The 'Relays' pane shows a 'relay' with a green checkmark. The 'Destinations' pane shows a 'ds' with a green checkmark. On the right, the 'MQTT Connector Details' pane is open, showing the 'Select Data' button highlighted with a red box.

- Select any data under the data source that you want to collect and then click **Next**.
- Click **Save**.

Example of selecting data for collection

### Selection History

Select objects under common ancestor opto:

IP,  
Port

Query executed successfully. Your selections have been updated.

### Selected Data

☒ Name

☒  opto

☒  IP

☒  Port

The connector discovers the hierarchy associated with the topics inside the Topics CSV file. You can now populate the hierarchy with the assets and PI points in the Topics file.

**Note:** The connector performs a rediscovery every 15 seconds and add any newly discovered assets and PI points to the **Topics** file. You may want to use the PI Data Collection Manager to refresh the hierarchy shown in the UI and to select additional assets and PI points for data collection.

The connector retrieves information about assets and PI points from the **Topics** file and populates the hierarchy in the UI.



















**Note:** If new assets need to be added to the Data Selection, do not click on Discover Data Source Contents again within the PI Data Collection Manager UI. As the connector performs periodic rediscovery, there is no need to trigger data discovery manually again.

3. Click **Select Data** in the right pane under **Select Data for Collection** again after the initial discovery process has completed (~30 seconds).

Any new data that comes in will be updated in the **Select Data** screen on a 30 second interval.

- Click the check box next to the assets and/or PI points to select them for data collection

Example of selected assets and /or PI points

<input checked="" type="checkbox"/>	Name
<input checked="" type="checkbox"/>	▾  Datasource 1
<input checked="" type="checkbox"/>	 IP
<input checked="" type="checkbox"/>	 Port
<input checked="" type="checkbox"/>	▾  spBv1.0
<input checked="" type="checkbox"/>	▾  groovBox
<input checked="" type="checkbox"/>	▾  Selam Cube
<input checked="" type="checkbox"/>	▾  _Fish Tank_
<input checked="" type="checkbox"/>	▸  _Diagnostics_
<input checked="" type="checkbox"/>	▸  Controller:Global
<input checked="" type="checkbox"/>	▸  Device Control
<input checked="" type="checkbox"/>	▸  _Marygroov_
<input checked="" type="checkbox"/>	▾  bdSeq
<input checked="" type="checkbox"/>	 Value
<input checked="" type="checkbox"/>	▸  Node Control
<input checked="" type="checkbox"/>	▸  Node Info
<input checked="" type="checkbox"/>	▸  Node-Red Data
<input checked="" type="checkbox"/>	▸  groovEdgeBox
<input checked="" type="checkbox"/>	▸  Opto22

## Results

You have now discovered the data source contents and selected assets and PI Points for data collection.

**Caution:** We recommend that you do not rediscover data source contents for previously discovered data sources as doing so clears out the data selection for those previously discovered data sources. The connector will stop collecting data if you save the new contents or have the **Use these selections as rules to automatically update destinations** option selected. To resume the data flow, you will need to restart the connector service from the Windows Service Manager (Services.msc).

## Start and stop data collection

Once the connector is configured, you can start or stop data collection from the administration website of your PI connector.

1. Under **Overview** in the **Connector** section, click the connector status.
2. Under **Connector Details** in the **Connection Tools** section, click **Start Connector** or **Stop Connector**.

## Verify connection from data source to the connector

Use the administration website of the connector to verify the connection between the data source and connector.

In the Data Sources section, verify that the status message is *Running*.

## Verify data collection

For each Data Archive server, use PI System Explorer to confirm that the connector is collecting data.

### Before you start

Verify the following items to ensure data collection.

1. Verify the connector service is started.
  - a. From the Windows **Start** menu, run the **services.msc** command.
  - b. In the Services window, verify the connector service status is Started.
2. Verify the connector is running.
  - a. Open the administration website of the connector.
  - b. In the Overview pane, verify that the **Connector Status** box shows the status Running with a green check mark (✓).
  - c. Click the **Connector Status** box and verify the available button is **Stop Connector**.
3. Verify the data source is connected. Under **Data Sources**, verify that each data source shows the status Running with a green check mark (✓).

### Procedure

1. Open PI System Explorer and click **Database**.
2. In the Select Database window, select the AF database that is configured to receive the data.
3. Click **Elements**.
4. Navigate to the AF element of interest.
5. Click the **Attributes** tab.

The AF attributes that are PI data references should have proper time stamps under the **Time Stamp** column.

## Message logs

The Connector Message Logs section on the administration website of the connector contains important status events and errors generated by the connector. The 1,000 most recent messages logged by the current connector service process are available. You can view older messages in the connector host machine's Windows Event Viewer under **Applications and Services Logs > PI Connectors**.

Each message in the log displays its severity level, time stamp, and the message itself. Internally, time stamps are

stored as UTC times but displayed according to the browser's time zone settings.

You can specify the message recording level (that is, what types of messages are captured) as well as which messages appear on the screen.

## Specify which messages to record

By default, connectors record only error and warning messages in the message log. To change the behavior to record more or fewer types of messages, click the **Record message\_level** drop-down and select an option.

If you change the message recording behavior from the administration website of the connector, the change is immediately reflected in the message log for PI Data Collection Manager. Likewise, if an administrator changes the message recording behavior in PI Data Collection Manager, the change is immediately reflected in the administration website of the connector.

## View the message log

To specify which messages display in the message log, click the **Show message\_level** drop-down list and select an option.

Changes to the message display options are not reflected across applications.

---

**Note:** Changing the recording setting affects which messages are recorded, not which messages are displayed. For example, if you specify the recording setting **Record error messages** and the display setting **Show error and warning messages**, the log could contain older warning messages that were recorded prior to the change.

---


You can sort messages by severity level, date (including time stamp), and message text. To sort, click the column you want to sort by. To reverse the order, click the column again.

Messages are limited to 100 messages per page. If more than 100 messages are displayed, use the navigation buttons (**First**, **Previous**, **Next**, and **Last**) to navigate through the pages.

To filter messages by a specific string, type the string in the **Filter Messages** field.

## Advanced diagnostics

The Advanced Diagnostics page contains a list of reports that provide detailed information on the connector. Most reports contain diagnostic information used by OSIsoft Tech Support.

To access the Advanced Diagnostics page on the administration website of the connector, click , then click **Advanced Diagnostics**. To return to the Overview page, click **Cancel**.

The Buffer Disk Usage report contains the following information about data that has been collected but not yet sent to the target destination.

- **Name**  
The name of the buffer disk.
- **CurrentDiskUsage**  
The amount of disk space currently used by a buffer file. The connector allocates buffer files on startup and when it needs additional buffers. The size of the buffer file is not an indication of the amount of buffered data.
- **MaxDiskUsage**

The maximum amount of disk space for buffers.

- **PercentDiskUsed**

The percentage of total disk space being used.

## PI Connector Relays

All PI Connector Relay hosts that are configured with the connector are listed in the Relays column of PI Data Collection Manager.

For information on how to add a PI Connector Relay, see the Add a PI Connector Relay topic in the PI Connector Administration user guide.

## Interactions with Data Archive and AF

Relays have specific behaviors in their interactions with Data Archive and PI AF. Some behaviors are configurable. For more information about the behaviors, see the Supplement for Data Archive and Supplement for PI AF topics in the PI Connector Administration user guide.

# Release notes

PI Connector for MQTT Sparkplug

1.0.0.6

## Overview

PI Connector for MQTT Sparkplug provides unidirectional data transfer from MQTT Servers to the PI System.

## Fixes and Enhancements

### Fixes

There are no fixes with this release.

### Enhancements

There are no enhancements with this release.

### Known Issues

There are no known issues with this release.

## System Requirements

### Operating Systems

This connector is a 64-bit application which runs on 64-bit architecture systems.

Server Class	Client Class
2008 R2 SP1 or later	7 SP1, 8.1, 10 or later

### Distribution Kit Files

Product	Software Version
Microsoft .NET Framework 4.7 Setup	4.7.02053.00
PI Connector for MQTT Sparkplug	1.0.0.6

## Installation and Upgrade

### Installing PI Connector for MQTT Sparkplug

The PI Connector for MQTT Sparkplug can be installed or upgraded using the installation kit. This installation kit can be obtained by using the How to Download Products link listed in the OSIsoft Customer Portal How To's list. This list is located on the [OSIsoft Customer Portal](#) site.



For additional information regarding the PI Connector for MQTT Sparkplug installation, please see the [Install the connector](#) sections of the user guide. The user guide is located in the PI Connectors section of the Doc Library.

### Uninstalling PI Connector for MQTT Sparkplug

The PI Connector for MQTT Sparkplug can be uninstalled using the Programs and Features list accessible from the Windows Control Panel. After accessing the Programs and Features list, select the *PI Connector for MQTT Sparkplug* and then select **Uninstall** to uninstall the interface.

## Security information and guidance

We are [committed to releasing secure products](#). This section is intended to provide relevant security-related information to guide your installation or upgrade decision.

We [proactively disclose](#) aggregate information about the number and severity of security vulnerabilities addressed in each release. The tables below provide an overview of security issues addressed and their relative severity based on [standard scoring](#).

No additional security vulnerabilities are applicable to this release.

### Overview of New Vulnerabilities Found or Fixed

This release of PI Connector for MQTT Sparkplug contains three (3) reported security issues.

This table lists the known vulnerabilities along with their mitigation in this product.

Component	Version	CVE or Reference	CVSS	Mitigation
angular/core	4.4.4	CVE-2021-4231	5.4	This vulnerability does not apply to PI Connectors because they do not implement Server-Side Rendering (SSR).
ag-grid	12.0.1	CVE-2017-16009	6.1	This vulnerability does not apply to PI Connectors because they do not use Angular expressions and AngularJS.
Bouncy Castle	1.8.1	CVE-2020-15522	5.9	This vulnerability does not apply to PI Connectors because they do not use ECDSA Encryption.

# Technical support and other resources

For technical assistance, contact OSIsoft Technical Support at +1 510-297-5828 or through the [OSIsoft Customer Portal Contact Us page](#). The Contact Us page 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](#). 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.



**AVEVA Group plc**

High Cross  
Maddingley Road  
Cambridge  
CB3 0HB  
UK

Tel +44 (0)1223 556655

**[www.aveva.com](http://www.aveva.com)**

To find your local AVEVA office, visit **[www.aveva.com/offices](http://www.aveva.com/offices)**

AVEVA believes the information in this publication is correct as of its publication date. As part of continued product development, such information is subject to change without prior notice and is related to the current software release. AVEVA is not responsible for any inadvertent errors. All product names mentioned are the trademarks of their respective holders.