



CONNECT data services

© 2015-2025 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, ArchestrA, Avantis, Citect, DYNSIM, eDNA, EYESIM, InBatch, InduSoft, InStep, IntelTrac, 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>CONNECT data services .....</b>	<b>10</b>
Core functionality .....	10
Platform uses .....	12
Security and reliability .....	14
<b>Take a tour of the portal .....</b>	<b>16</b>
View and edit your user profile .....	19
View tenant details .....	20
View resource usage .....	20
View system health .....	23
Search queries .....	24
<b>Get started .....</b>	<b>29</b>
Set up CONNECT for CONNECT data services .....	29
Log into CONNECT .....	30
Subscribe to CONNECT data services .....	31
Create a folder and enable CONNECT data services .....	32
Folders and namespaces .....	34
Set up CONNECT users and groups .....	35
Add users in CONNECT .....	35
Add groups in CONNECT .....	36
Add users to a group in CONNECT .....	36
Assign the Data services Viewer role to a group in CONNECT .....	37
Set up CONNECT data services groups, roles, and permissions .....	37
Log into CONNECT data services .....	37
Add groups and assign roles in CONNECT data services .....	38
Manage permissions for namespaces .....	39
Permissions management .....	39
Cross-region data sharing .....	42
Ingress data .....	44
Manage your data .....	44
Get started with streams .....	45
Get started with assets .....	46
Get started with communities .....	47
Egress data .....	47
<b>Data management .....</b>	<b>49</b>
Sequential Data Store .....	49
Streams .....	49
Manage streams .....	50
Add tags or metadata .....	51

Share streams .....	51
View in trend .....	52
View stream data .....	52
Add event .....	53
Edit event .....	54
Remove event .....	55
Manage permissions for streams .....	55
Download stream data .....	59
Types .....	59
Types best practices .....	60
Add a type .....	61
Manage permissions for types .....	63
Stream views .....	64
<b>Communities .....</b>	<b>65</b>
Communities page .....	67
Community setup .....	70
Understand community roles .....	72
Workflow: Create a community .....	74
Create a community .....	74
Invite a tenant to a community .....	75
Enable stream sharing permissions .....	77
Workflow: Join a community .....	79
Accept community invitation .....	80
Enable stream sharing permissions .....	82
Community administration .....	84
Invite a tenant .....	85
Resend an email invitation .....	86
Remove a tenant from a community .....	87
Edit a community .....	87
Delete a community .....	88
Manage preferred region .....	88
Community tenant administration .....	89
View pending community invitations .....	90
Remove your own tenant from a community .....	90
Pause sharing a community .....	91
Manage users in a community .....	92
Manage groups in a community .....	93
Manage clients in a community .....	94
Configure contact email .....	95
Manage community administrators .....	96
Manage default community administrators .....	97
Community data sharing and viewing .....	97
Enable stream sharing permissions .....	98
Manage shared streams .....	100
View shared streams .....	102
View shared data in a trend session .....	103
View community usage .....	104
<b>Stream metadata rules .....</b>	<b>105</b>
Create a metadata rule .....	108

Maintain a metadata rule .....	110
<b>Asset rules .....</b>	<b>111</b>
Create an asset rule .....	111
How tokens are used to generate assets .....	118
Use multiple asset rules to create assets .....	120
Manage permissions for asset rules .....	122
<b>Change broker .....</b>	<b>123</b>
Change broker best practices .....	124
Manage change broker stream data updates .....	125
<b>Events .....</b>	<b>128</b>
Model events and reference data .....	129
Manage permissions for events and reference data .....	130
Prepare CONNECT data services to use events .....	131
Integrate events with AVEVA Advanced Analytics .....	131
 <b>Data collection .....</b>	<b>132</b>
<b>Data ingress sources .....</b>	<b>132</b>
<b>Edge Data Store &amp; Adapters .....</b>	<b>133</b>
View and monitor a system .....	134
System status definitions .....	136
Add and edit configuration templates .....	136
Deploy a system configuration .....	140
Deploy a system module .....	141
Manage system configurations .....	141
<b>PI agents .....</b>	<b>143</b>
PI to CONNECT Agents .....	144
Set up PI to CONNECT Agent .....	145
PI to CONNECT minimum system requirements .....	145
Disable IE enhanced security .....	148
Install the PI to CONNECT Agent .....	148
Run the PI to CONNECT Agent Configuration Utility .....	152
Support for slow moving data .....	159
Transfer PI System data to CONNECT data services .....	159
Create a PI to CONNECT data transfer .....	160
Start a PI to CONNECT data transfer .....	175
PI to CONNECT data transfer status .....	179
Confirm data retrieval from a PI Server .....	180
Edit a PI to CONNECT transfer .....	180
Download transfer details .....	181
Download a list of missing PI points .....	182
AF data that can be transferred .....	182
PI to CONNECT change synchronization .....	184
PI to CONNECT Agent maintenance .....	188
View PI to CONNECT Agent metrics .....	188
Repair a PI to CONNECT Agent .....	189
Search for a PI to CONNECT Agent .....	190
Remove a PI to CONNECT Agent .....	190
Manage permissions for agents .....	191

PI to CONNECT logs .....	191
View PI to CONNECT Agent logs in the Windows Event Viewer .....	191
View PI to Data Hub Agent Configuration Utility logs .....	192
Common Event Viewer log messages .....	192
Enable verbose logging for PI to CONNECT .....	194
Troubleshoot PI to CONNECT .....	195
Verify the PI to CONNECT Agent is running and registered .....	195
Troubleshoot client Id and secret .....	196
Troubleshoot failed AF indexing .....	197
Troubleshoot a failed PI mapping .....	198
Troubleshoot missing Data Archive configuration .....	198
Troubleshoot common PI point errors .....	199
Troubleshoot insufficient RPC threads for concurrent queries .....	199
Limitations of PI to CONNECT .....	200
PI to CONNECT known issues .....	201
PI to Data Hub 2.2.2174 Release Notes .....	202
PI to CONNECT release history .....	204
CONNECT to PI Agents .....	213
Set up CONNECT to PI Agent .....	215
CONNECT to PI minimum system requirements .....	216
Install the CONNECT to PI Agent .....	216
Run the CONNECT to PI Configuration Utility .....	217
Install and configure a CONNECT to PI Agent silently .....	218
View CONNECT to PI Agent status .....	220
Transfer data to a PI Server .....	220
Create a CONNECT to PI data transfer .....	220
Edit a CONNECT to PI draft transfer .....	221
Start a CONNECT to PI data transfer .....	222
Monitor CONNECT to PI data transfer metrics .....	223
CONNECT to PI Agent maintenance .....	225
View CONNECT to PI Agent metrics .....	225
Repair a CONNECT to PI Agent .....	226
Search for a CONNECT to PI Agent .....	227
Remove a CONNECT to PI Agent .....	227
Health and diagnostics .....	228
Health .....	228
Device Status .....	228
Next health message expected .....	229
Diagnostics .....	229
IO rate .....	230
Error rate .....	230
Stream count .....	230
OMF egress IO rate .....	231
System .....	231
Troubleshoot CONNECT to PI .....	232
Troubleshoot CONNECT to PI connection issues .....	232
CONNECT to PI Agent logs .....	233
CONNECT to PI Agent buffering .....	237
CONNECT to PI 1.0.1523 Release Notes .....	240

<b>OMF connections .....</b>	<b>242</b>
OMF connections best practices .....	242
Configure an OMF connection .....	243
Maintain an OMF connection .....	243
 <b>Visualization .....</b>	 <b>245</b>
Create a trend session .....	245
Download trend data .....	247
Trend visualization .....	248
Trend legend .....	249
Trend URL parameters .....	251
Swap assets in a Trend graph .....	253
Asset explorer .....	255
Assets .....	255
Add an asset .....	256
Add an asset based on an asset type .....	257
Manage permissions for assets .....	258
Remove assets .....	258
Asset types .....	259
Create an asset type .....	260
Convert an asset to an asset type .....	261
Manage permissions for asset types .....	261
Remove asset types .....	262
Remote operations monitoring .....	262
Get started with remote operations monitoring .....	262
Filter and search assets .....	265
Share a view of your fleet .....	266
 <b>Analytics .....</b>	 <b>267</b>
Data views .....	267
Create and configure a data view .....	267
Add a data view .....	269
Add a query .....	269
Select data field sets .....	271
Field set options .....	272
Configure data shape .....	273
Preview and save the data view .....	275
Manage data views .....	277
Manage queries .....	278
Manage data field sets .....	279
Manage data fields .....	279
Edit data field labels .....	280
Edit grouping fields .....	281
Edit identifying fields .....	284
Edit field set order .....	287
Link data fields .....	287
Manage permissions for data views .....	288

Retrieve data for a data view .....	289
Data views and the API Console .....	290
Data view data type conversion .....	292
Parquet data format .....	295
Data view troubleshooting .....	296
<b>Virtual tables (Preview) .....</b>	<b>300</b>
Shares .....	300
Create a share .....	300
Edit a share .....	301
Delete a share .....	301
Create a virtual table .....	301
Edit a virtual table .....	302
Manage permissions for virtual tables .....	302
Delete a virtual table .....	303
<b>Power BI Connector .....</b>	<b>303</b>
Power BI Connector setup .....	304
Retrieve data views with Power BI Connector .....	305
Edit a data view query in Microsoft Power BI .....	308
CONNECT data services Power BI Connector release notes .....	311
 <b>Security .....</b>	<b>315</b>
<b>CONNECT data services groups .....</b>	<b>315</b>
Add a group in CONNECT data services .....	315
Maintain a group in CONNECT data services .....	316
<b>CONNECT data services users .....</b>	<b>317</b>
Add a user in CONNECT data services .....	318
Maintain a user in CONNECT data services .....	319
<b>CONNECT data services roles .....</b>	<b>319</b>
Add a role in CONNECT data services .....	321
Maintain a role in CONNECT data services .....	321
Manage permissions for user roles in CONNECT data services .....	322
<b>CONNECT data services clients .....</b>	<b>323</b>
Add a client-credentials client .....	325
Add a hybrid client .....	326
Add an authorization code client .....	327
Maintain a client .....	328
 <b>Developer tools .....</b>	<b>330</b>
<b>Code samples .....</b>	<b>330</b>
<b>API console .....</b>	<b>330</b>
<b>GraphQL console .....</b>	<b>335</b>
<b>OMF editor .....</b>	<b>337</b>
 <b>Support .....</b>	<b>338</b>
<b>Downloads .....</b>	<b>338</b>
<b>Logs .....</b>	<b>338</b>

<b>Service Blog.....</b>	<b>339</b>
<b>How CONNECT data services charges flex credits.....</b>	<b>339</b>

# CONNECT data services

CONNECT data services is a secure cloud platform for aggregating, storing, enriching, accessing, and analyzing real-time operations data.

CONNECT data services creates a seamless, trustworthy data infrastructure to incorporate information from sensors, plants, enterprises, edge devices, and communities of interested users. This infrastructure enables data sharing and usage within your organization, across locations, and even with external partners.

With CONNECT data services you can use a web-based portal to manage and monitor your tenant, namespace resources, streams, and assets. CONNECT data services can also be accessed and managed via REST APIs.

You can integrate and view CONNECT data services data in the following ways:

- Build applications with client libraries to read and write data to CONNECT data services.
- Use the REST APIs to read and write data to CONNECT data services.
- Retrieve tabular data with Data Views.

You must have a CONNECT account to use CONNECT data services. To request a tenant account, contact [AVEVA](#).

For developer documentation, read the [Developer guide](#).

## Core functionality

CONNECT data services consists of several areas of core functionality.

### Access management

You can customize CONNECT data services access management to meet your organization's requirements and needs. Administrators can:

- Customize authentication (through CONNECT)
- Create and manage users (user accounts must exist first in CONNECT)
- Define and assign roles
- Create and manage clients
- Manage folders/namespaces (through CONNECT)

Administrators can define the permissions to a resource by configuring the access control list (ACL) for that resource. They can also perform tenant management using the CONNECT data services REST API or the CONNECT data services portal.

### Data collection

CONNECT data services provides a variety of methods to collect data. You can ingress data from PI Server and other AVEVA applications or you can develop custom applications using a programmatic interface, Open Message

Format (OMF) or CONNECT data services REST API.

AVEVA products:

- PI to CONNECT Agent: Transfers on-premises PI data and Asset Framework (AF) data into CONNECT data services.
- AVEVA Edge Data Store (EDS): Collects, stores, and provides local access to operational data from edge devices and uploads this data to CONNECT data services.
- AVEVA Adapters: Transfer operational data from a variety of edge and on-premises data sources in real-time into CONNECT data services.
- AVEVA Historian: Replicates historical data from AVEVA Historian into CONNECT data services.

Custom solutions:

- Custom Open Message Format (OMF) applications: A platform-independent format for passing JSON messages to CONNECT data services using an HTTP client. Use OMF to achieve a high-throughput data feed into CONNECT data services.
- REST APIs: Developer-friendly APIs provide programmatic access to read and write sequential data into CONNECT data services.

## Data management

The Sequential Data Store (SDS) is the storage layer of CONNECT data services. It is used to store, retrieve, and organize any type of streaming data. Typically, developers use the SDS as part of their customized applications. It is primarily for time-series data, but also more complex data such as location, time/depth, etc.

The basic features of the SDS include:

- Types: A type defines the structure of data to be collected in CONNECT data services. A type is analogous to a template that defines each instance in a stream of data.
- Streams: A stream is a series of ordered events. Each event is an instance of a type. Collectively, the stream of data forms the structure that the type specifies.
- Stream views: A stream view is a logical overlay for stream data that allows you to create customized views of data streams that meet the needs of multiple users without changing the original data. With a stream view you can do things such as include a subset of the data in a stream, convert units of measure, and change names so terminology is appropriate for a particular audience.

## Community sharing

With Communities you can create a private group where operational data can be shared and viewed by trusted business partners, service providers, and analytics providers. Sharing data with CONNECT data services allows real-time updating of data, full data granularity, and an automated data copy outside your organization. You can share data from a PI server without requiring your partners to have a PI system.

Sharing data streams allows you to:

- Collectively operate more efficiently and reduce waste.
- Detect hidden problems in your equipment and processes, helping to troubleshoot issues.
- Predict future failures before they occur.

- Share data across engineering and operational partners.

## Monitoring and analysis

After defining types, streams, and stream views, use the analytical tools in CONNECT data services to sort and visualize the data. Two analytical tools are available in CONNECT data services:

- Trend: The Trend feature converts stream data to a graphic view, which can reveal trends, high points, or trouble spots. Use Trend to select data streams in a namespace, specify a time range, and then render a graph of those data values. This allows for quick data exploration and troubleshooting within the portal that can be easily shared with colleagues.
- Assets: Assets are a digital twin of physical entities in the real world. An asset can consist of data from one or more streams. Assets are a useful way to organize and contextualize data streams. With PI to CONNECT data transfers, for example, you can organize multiple PI tags under a single asset. You could create an asset with streams measuring data for thermostats, ventilation equipment, lighting systems, and security.

## Data science enablement

You can group and organize operational PI, IoT, and CONNECT data services data. By arranging data into forms that can be consumed by third-party data science applications, data scientists can conduct deep analysis to detect unrealized patterns and insights. Data science enablement efforts allow for better informed planning, predictive maintenance, and operational optimization.

Data views allow you to order, index, and organize data from multiple streams to create curated data subsets. Data views serve as a bridge between raw CONNECT data services data and data science applications. Use an API or the CONNECT data services portal to create data views to arrange data for consumption by third-party data science applications.

The CONNECT data services Power BI Connector retrieves data views from CONNECT data services and makes them available in Microsoft Power BI for advanced data visualization and analysis. You can also use Microsoft Power BI to edit the query generated from the connector to modify the dates, edit the interpolation interval, and enable an incremental refresh of data.

## Platform uses

CONNECT data services extends the data infrastructure seamlessly by integrating existing AVEVA products and third-party vendors from edge to cloud. This extensibility allows data to be shared across the entire infrastructure, reaching new people such as developers creating custom applications, data scientists engaged in data modeling, operations staff who monitor real-time performance, and data analysts using visualized data.

Extending the collection and accessibility of operational data allows new analysis and decision-making processes to benefit your company. Some of the possible uses of this data include:

- Remote operations monitoring
- Aggregating data from multiple PI systems and other sources for monthly or environmental reporting
- Providing real-time troubleshooting data for support personnel
- Data science analysis
- Sharing data with external partners

- Providing data to third party applications like Power BI, Grafana, or custom applications
- Connect manufacturing data streams to an AI analysis application to facilitate process optimization

## Remote monitoring

CONNECT data services provides the ability to integrate data infrastructure from edge to cloud seamlessly. Designed to serve as a "system of systems," CONNECT data services supports data usage across the global enterprise.

In the past, data was often isolated at remote locations due to unreliable network connectivity. For instance, farms need data to answer questions such as how much grain is in a silo or what is the predicted corn harvest this season. Mining companies require data from mining trucks to know when maintenance is necessary. This untapped data can provide valuable insights for an enterprise and its decision making.

Accessing and integrating these "dark" data locations is possible with CONNECT data services. With pervasive data collectors, AVEVA Adapters, Edge Data Store, and custom OMF applications, operational assets that were previously inaccessible are now viable data sources.

The benefits of seamless integration of data infrastructure include:

- Confidence that data across the entire spectrum is authoritative.
- Data is compatible and native to the infrastructure across the spectrum.
- Operational data can be accessed and used anywhere; it is no longer isolated in one facility or system.
- New sources of operational data are available by storing the data in the cloud.
- Existing edge and PI Server data is integrated into CONNECT data services.

## Data science analysis

Data scientists can easily integrate operational data from multiple sources for a variety of applications, such as process optimization and maintenance. Better data modeling enables smart decision-making based on clear answers about what is most relevant to a company's goals. CONNECT data services uses the entire data infrastructure to gather the right type of data for modeling tools that answer business questions such as maintenance and demand forecasting.

CONNECT data services improves business insight by:

- Allowing the operations department and data scientists to share data and collaborate more effectively.
- Providing an environment in which data analysis artifacts are saved, enabling the data scientist to modify their models and workflow more efficiently.
- Ensuring that high-quality data is available for analysis.

Some of the advantages of using CONNECT data services for data science include:

**Data is easier to consume.** Curating and preparing data are the most time-consuming tasks when data scientists create their models. Bad data and data gaps decrease the integrity of results. In contrast, data that is contextualized, structured, filtered for relevancy, and presented in a format that is compatible for modeling tools and applications increases the efficiency of data scientists and the accuracy of their results.

**More data is available.** CONNECT data services removes the challenges of complicated and overbuilt data solutions, such as data lakes and relational databases, and provides a direct option for extending the data infrastructure. Because of the flexibility of the CONNECT data services REST API, data can be consumed by many

software applications that data scientists use to perform their analysis.

**Data is prepared for efficient consumption.** Use data views to organize and configure CONNECT data services data to be compatible with specific tools or applications. Add context to data through data views for easy identification and classification. Organize operational data in tabular form so it can easily be consumed by external tools via the REST API. Use data views to configure data sets for algorithms and modeling tools.

**Data modeling is flexible.** Data scientists need to experiment with and update their models. The REST API gives data scientists freedom to work with many different contemporary data modeling tools and applications. The REST API also provides flexibility as data science technology evolves.

**Data is contextualized.** Data science models are only as good as the data used in those models. Identifying the data that is relevant is as important as the model used. CONNECT data services uses metadata rules to provide the context that makes it easy to search for data. CONNECT data services metadata rules parse and store data that match specific patterns. Additionally, CONNECT data services parses for user-provided context to identify patterns. When it finds a pattern, it attaches metadata.

**APIs integrate operational data with applications.** CONNECT data services supports easy integration with custom applications, extending the enterprise data infrastructure to in-house and partner applications. CONNECT data services offers ease of integration with a modern, secure REST API that is compatible with R and Python applications. Application developers use the REST API to interact with operational data on CONNECT data services.

## Sharing data with business partners

With the Communities feature, industrial companies can share their data streams with external business partners, service providers, and analytics providers. This is done in real-time, on a secure cloud platform. Only the information you specify is shared and no external users log directly into your tenant.

Analysis of aggregated data can bring multiple participants of the supply chain together to drive value, improve efficiency, and support compliance requirements.

To learn more about this feature, see [Communities](#).

## Security and reliability

AVEVA manages, operates, and maintains all aspects of the CONNECT data services platform. CONNECT data services is built and deployed on Microsoft Azure and operates outside the AVEVA corporate firewall. Currently, CONNECT data services runs in three Azure regions: West US, West Europe, and Australia. By housing the platform in multiple regions, CONNECT data services accommodates regulations that mandate where data must be stored.

## Secure and robust data infrastructure

CONNECT data services is built from the ground up to ensure security. The CONNECT data services platform is based on industry standard techniques to ensure the strongest possible data integrity. User authentication is handled through CONNECT. Authenticated users can only perform actions for which their role is authorized. Machine access to CONNECT data services is controlled through a variety of defensive strategies. All data in CONNECT data services is fully encrypted in transit and at rest.

## Elastic resource allocation

Due to its microservice-based architecture, CONNECT data services dynamically adapts to workload changes by automatically provisioning and de-provisioning resources. Each microservice performs a subset of the system's overall capabilities, and when orchestrated together, they function as a complete platform.

When CONNECT data services is turned on in a folder for a tenant in CONNECT, a new set of microservices and all the necessary data storage is provisioned for that folder/namespace. As the tenant's needs for the namespace grow, CONNECT data services automatically provisions additional microservices and storage so the namespace can expand horizontally. Similarly, if requirements shrink, CONNECT data services can reduce the number of required microservices and de-allocate storage.

## Interruption resilience

To prevent data interruptions or loss, CONNECT data services incorporates many safeguards and is designed for high availability. You are not required to perform any specific actions to ensure continuous access to reliable, distributed data storage.

CONNECT data services is continuously tested to ensure the platform is performing reliably. Both the platform and the underlying operating systems are updated regularly. In addition, frequent threat analyses are conducted to thwart potential exploitations. Load balancing precludes distributed denial of service attacks. A gateway prevents unauthorized access to resources.

## Service description

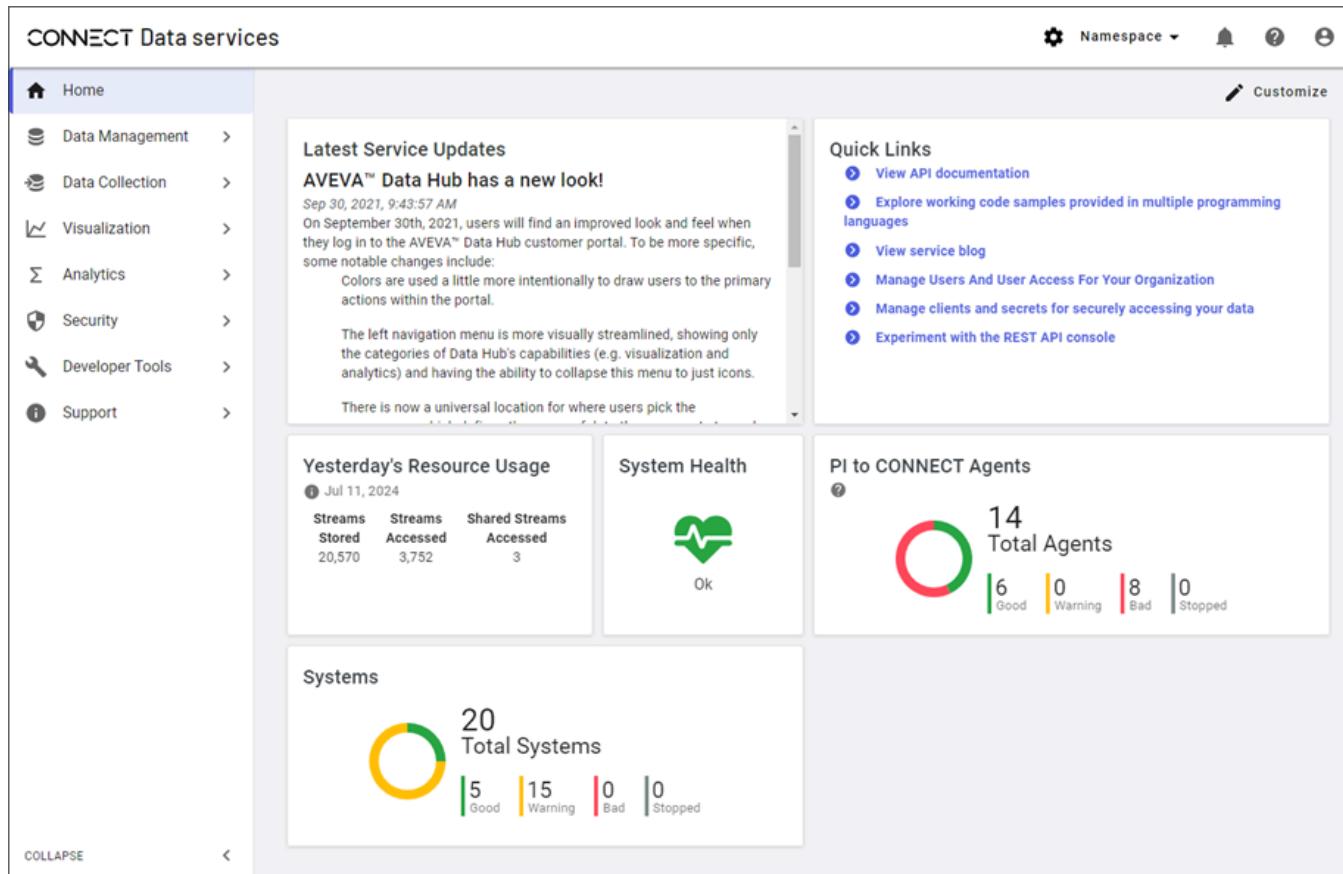
For more information on operational topics relating to CONNECT data services, such as data ownership, data privacy, database backup and redundancy, see the [CONNECT data services Service Description](#).

# Take a tour of the portal

Access and interact with CONNECT data services through the web-based portal.

## CONNECT data services home page

When you first access the portal, the home page provides you with information about the system and other reference materials.



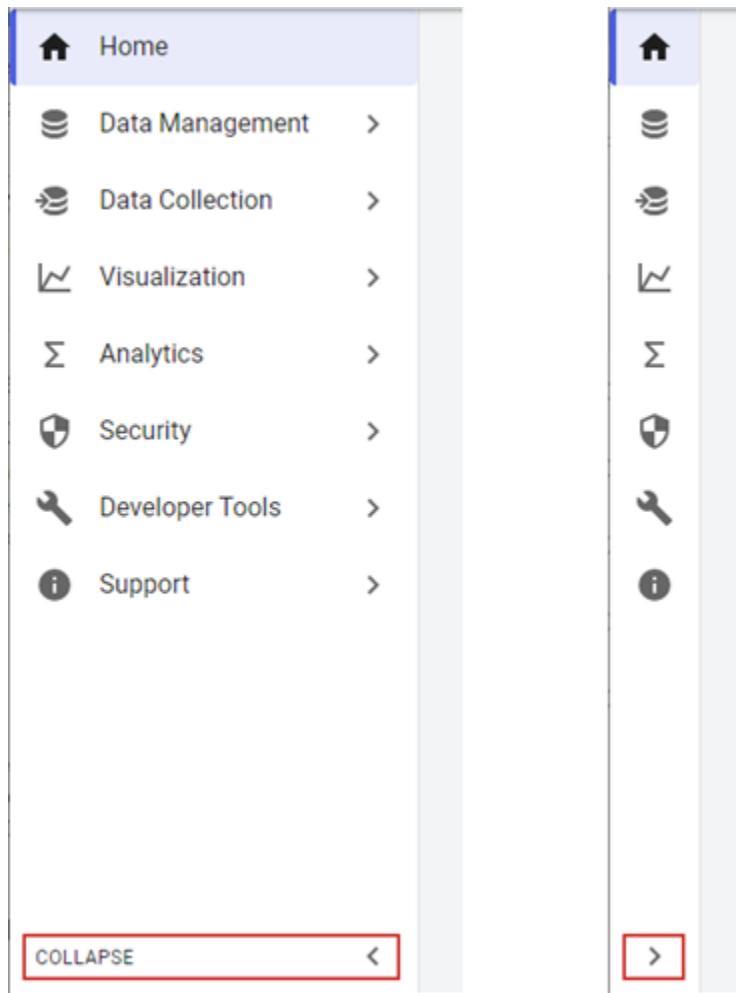
The CONNECT data services home page displays the following:

- Latest Service Updates:** Most recent updates to CONNECT data services such as visual improvements, navigation updates, and new features.
- Quick Links:** Links to important and popular content such as API documentation and commonly used guides.
- Resource Usage:** View resource usage at a glance and select this box to see in-depth information on your [resource usage](#).
- System Health:** Overall system health for CONNECT data services. Select to see a breakdown of [tenant health](#).
- PI to CONNECT Agents:** Health status for each PI to CONNECT agent. Statuses include Good, Warning, Bad, and Stopped. Select to see individual statuses for each agent.

- **Edge Data Store & Adapters:** Health status for each system. Statuses include Good, Warning, Bad, and Stopped. Select to see individual statuses for each system.

## CONNECT data services features

Collapse or expand the left pane to view a menu of features. This pane is always available in the portal, and you can hover over the icons to make selections even while the menu is collapsed.



CONNECT data services includes the following features:

- **Data Management:** Tools for setting up basic capabilities, including tenants, the Sequential Data Store (SDS), and metadata rules for data streams.
- **Data Collection:** Bring data from multiple sources and systems into a namespace.
- **Visualization:** View data trends and use assets to set up digital twins of real-world physical entities.
- **Analytics:** Tools for shaping and querying large datasets.
- **Security:** Add groups, users, roles, and clients to your tenant.
- **Developer Tools:** Code samples, an API console, and an editor for the Open Message Format (OMF).
- **Support:** Documentation, logs, support links, the service blog, and other useful information.

## Feature pages

Select a menu item to take you to that item's feature page.

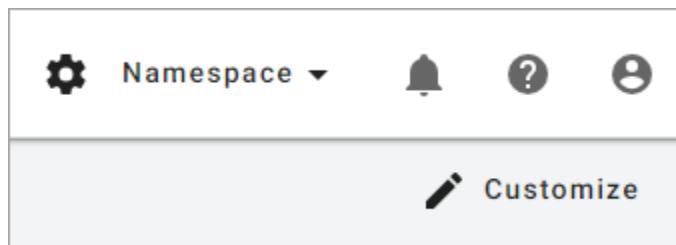
The screenshot shows the 'Groups' feature page. The left pane is a list of groups with columns for Name, Identity Provider, and AVEVA Connect status. The 'Groups' item is selected. The right pane shows detailed information for the selected 'Administration' group, including its ID, name, assigned roles (Tenant Roles: Tenant Administrator, Tenant Member), and community roles.

Most pages consist of two panes:

- The left pane is where you perform the tasks associated with the resource. For example, the left pane is where you add and edit the resource or manage its permissions.
- The right pane may contain a **Details** tab that contains additional information about the selected resource. Some resources also have additional panes for other configuration tasks.

## Portal toolbar

The portal toolbar is located in the upper-right corner of the portal window.



The following table provides a list and descriptions of these toolbar commands.

Item	Function
Manage permissions	Change role-based access to portal resources.
Change namespace	Choose a different namespace.
View notifications	View CONNECT data services-generated notifications.

Item	Function
 Help	Access the online documentation.
 User profile	View a menu of the following commands: current user profile, tenant details, resource usage, feedback page, and sign out of the portal.
 Customize	Customize the layout of the portal dashboard.

## View and edit your user profile

The My Profile window displays your user information and assigned roles.

### Update contact information

To update your contact information:

1. To open your user profile, select the **User Profile** icon  and select your name.
  2. Select **Edit**.
- 
- Note:** If the Identity Provider your organization uses does not allow you to update your contact information, the **Edit** button is disabled.
3. Update your contact information.
  4. Select **Save**.

### Show user-friendly property names

The **Show user friendly property names** option controls the appearance of property names for streams that originate through PI to CONNECT Agents on the Trend and Asset Explorer pages. When this option is turned on, those stream property names mimic PI tag naming and certain stream properties are hidden. For example, say you have the following streams and properties:

- SL-Tank01|Pressure|Value
- SL-Tank01|Pressure|SystemStateCode
- SL-Tank01|Temperature|Value
- SL-Tank01|Temperature|SystemStateCode

With this option turned on, you would see the following on the Trend and Asset Explorer pages:

- SL-Tank01|Pressure
- SL-Tank01|Temperature

The properties that contain values are easier to find and the properties that contain system information are hidden. This setting is specific to your login.

To change your user preferences:

1. To open your user profile, select the **User profile** icon  and select your name.
2. To use friendly property names, turn on the the **Show user friendly property names** toggle under **User Preferences**. The setting saves automatically.

## View tenant details

A tenant grants access for your users, groups, and clients to assets, resources and services associated with the tenant. The Tenant Details page provides the following details about your tenant:

- **Tenant Name:** The full name of the tenant.
- **Company Alias:** The credential name used during the login process.
- **Date Created:** The date the tenant was created.

Only the tenant administrator can make changes to the tenant details.

To view the Tenant Details page:

1. Select the **User profile** icon .
2. Select **Tenant Details**.

## View resource usage

The Resource Usage page displays the streams created and viewed within your tenant or from a community as a bar graph. The graph contains two parameters that you can edit: data source and views.

### To view resource usage

1. Select the **User profile** icon .
2. Select **Resource Usage**.
3. Review License usage.
4. Choose a data source: **Streams Accessed** or **Shared Streams Accessed**. For more information, see Data sources.
5. Choose a time increment: **Monthly View** or **Daily View**. For more information, see View.
6. (Optional) Select **Download Usage** to download the displayed data.

### License usage

Resource usage always displays your license information, regardless of what page parameters you select. This license information lists your total number of licenses available along with the number consumed.

Field	Description
<b>Namespaces</b>	The total number of namespaces the tenant is licensed for and the number of licenses consumed.
<b>Created Streams</b>	The total number of streams the tenant is licensed for and the number of licenses consumed.
<b>Current Month Accessed Streams</b>	The total number of streams the tenant is licensed the access during the month and the number of licenses consumed.

## Data sources

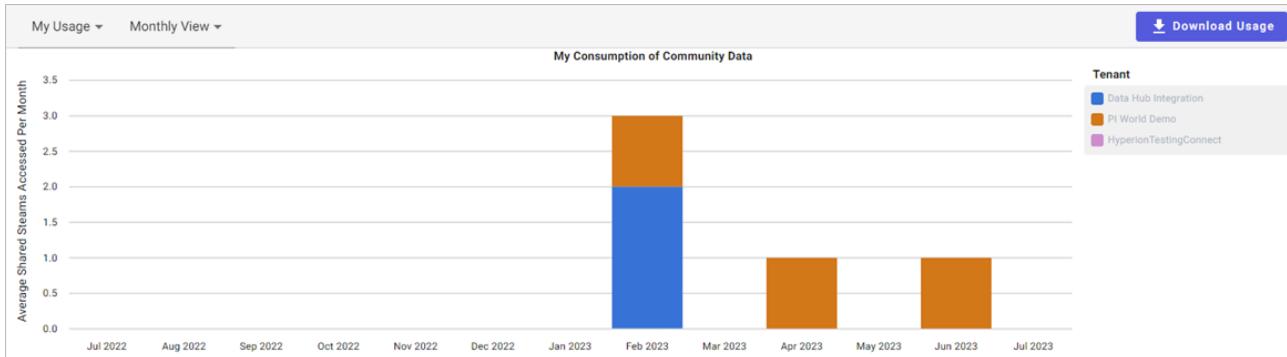
For data source, you can view streams from your native tenant namespaces or from communities you are a member of. Choose between the following options:

- **Streams Accessed:** Displays usage data about streams native to your tenant namespaces.
- **Shared Streams Accessed:** Displays usage data about streams shared into communities that your tenant holds membership in.

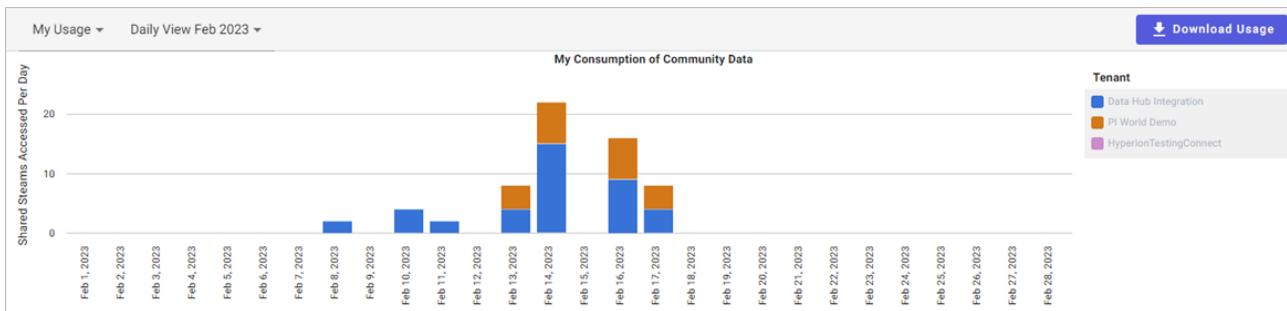
## View

Use the view dropdown to display streams accessed by month or day. Choose between the following options:

- **Monthly:** Displays usage data for the chosen data source for the past seven months, broken down by month.



- **Daily:** Displays usage data for the chosen data source for each day in a chosen month.



## Legend

Regardless of which parameters you choose, resource usage always display a legend that maps the colors of the graph to each data source. The legend also lists whether the data source is a native namespace or a shared community namespace.

### Legend



## Tabular data

Regardless of which parameters you choose, the data displayed in the bar graph is also displayed below it as tabular data. View the Legend to see how the stream data maps to a data source. You can download this data in CSV format by selecting **Download Usage**.

## Video Tutorial: View your CONNECT data services usage

[https://player.vimeo.com/video/848733417?badge=0&autoplay=0&player\\_id=0&app\\_id=58479](https://player.vimeo.com/video/848733417?badge=0&autoplay=0&player_id=0&app_id=58479)

### Video Transcript (Select to expand)

This video shows you how to view your usage in AVEVA Data Hub.

To view your usage in AVEVA Data Hub, select your profile icon, in the top right corner and then select Resource Usage.

Select the dropdown to choose between Streams Accessed and Shared Streams Accessed.

Streams Accessed is a metric that measures how much data you and members of your tenant access in a day, while Shared Streams Accessed is a metric that measures how much Community data you and members of your tenant access in a day.

Use this drop-down to set the timeframe for the data.

You can select between monthly average or daily views.

Changes to either drop-down are reflected in the bar chart and the table below.

Select the Download Usage button to download a local copy of the data to your machine.

## View system health

The Health page displays the health status of each service and namespace in your CONNECT data services tenant. To view your system health status, select **System Health** from the Home page.

### Service Health

**Service Health** includes a health status for each service and namespace included in your CONNECT data services tenant. The namespace region is displayed as well. For more information about each icon, see Statuses.

### Community Health

**Community Health** includes a health status of the [Communities](#) service. A health status is listed for each available region.

- If a region is **Ok** , then the streams shared from that region are accessible to the community as a whole.
- If a region is **Bad** , then the streams shared from that region are not available to the community as a whole.

For more information about each icon, see Statuses.

### Statuses

Icon	Status
	Ok
	Warning
	Bad
	Unknown
N/A	Service not detected

# Search queries

Many pages in CONNECT data services include a search capability, including:

- Sequential Data Store (streams, types, stream views)
- Asset Explorer (assets, asset types)
- Edge Data Store & Adapters (systems, configuration templates)
- Data Views (streams, assets)

This topic describes the available search query options.

## Search operators

You can use search operators to get more refined search results. Use the operators AND, OR, and NOT in all caps.

**Note:** If multiple search terms are used without an operator, OR will be the assumed operator.

Operator	Description
AND	AND operator. The query cat AND dog searches for both "cat" and "dog".
OR	OR operator. The query cat OR dog searches for either "cat" or "dog", or both.
NOT	NOT operator. The query cat NOT dog searches for "cat" or those without "dog".
*	Wildcard operator. Matches 0 or more characters. See Wildcard operator.
:	Field-scoped query. Specifies a field to search. See Field-scoping operator.
" "	Quote operator. Searches on an exact sequence of characters rather than searching on words separated by spaces or punctuation. See Quote operator.
( )	Precedence operator. The query wind AND (speed OR deviation) searches for either "wind" and "speed", or "wind" and "deviation".

## Wildcard (\*) operator

Searching for a value finds only exact, whole-word matches. As an example, searching for "temperature" will not match a field value of "temperatures". You can use the wildcard operator (\*) to match a partial search term. The wildcard can be used in the front (\*perature), middle (tem\*rature), or at the end (temp\*) of each search term. It can only be used once for each search term, except to enclose a term (\*perat\*). CONNECT data services does not

support wildcard operators in the middle and at the front or end of a term (te\*pera\* is invalid).

Query string	Matches field value	Does not match field value
log*	log logger	analog
*log	analog alog	logg
*log*	analog alogger	lop
l*g	log logg	lake swimming (* does not span across tokens)

## Field-scoping (:) operator

The field-scoping operator limits the search to a specific field, such as `id:`, `name:`, `description:`, and `metadatakey:`.

Stream metadata keys are only searchable in association with their values. Without the field-scoping operator, a search is limited to metadata values, along with other searchable fields in the stream. For example, searching streams for "sourcetag" only finds items if they include sourcetag as a value, but searching for "sourcetag:/\*" finds all streams that have a sourcetag metadata key.

## Quote (" ") operator

Search automatically searches on text delimited by white space and punctuation. To search for values that include these delimiters, enclose the value in double quotes.

When using double quotes, the matching text must include the whole value of the field on the object being searched. Partial text will not match unless you use wildcards. For example, if you are searching for a document that has a description of Pump three on unit five, a query of unit five will not match the description, but a query of "unit five" will.

Also, you can use wildcards (the \* asterisk character) on the outside of the quote operators, but if an asterisk is inside of the quotes, it is treated as a string literal rather than a wildcard operator. For example, you can search for "pump three"/\* (asterisk outside the quotes) to find text that starts with "pump three", but if you search for \*"pump three"/\* (asterisk within the quotes), it only matches on a value of "pump three"/\*.

Query string	Matches field value	Does not match field value
"pump pressure"	pump pressure	pressure, pressure pump, pump pressure gauge
"pump pressure"/*	pump pressure, pump pressure gauge	pressure, pressure pump, the pump pressure gauge
*"pump pressure"	pump pressure, the pump pressure	pressure, pressure pump, the pump pressure gauge

Query string	Matches field value	Does not match field value
*"pump pressure"*	pump pressure, the pump pressure, the pump pressure gauge	pressure, pressure pump
"pump*pressure"	pump*pressure	pump pressure, the pump pressure gauge

## Special characters in search queries

Add the backslash escape character (\ ) before any special characters in search queries. The following special characters require an escape character: " | / \* \ () :

The following are examples of using the escape character in query strings.

Example field value	Query string
Austin\Dallas\Fort Worth	Austin\\Dallas\\Fort Worth
1:100	1\:100
http://www.aveva.com	http\:\/www.aveva.com

## Examples of query strings

Query string	Applies to	Description
Id:Id1	assets, streams, stream types, stream views	Returns the item whose Id is <b>Id1</b> .
Id:Id*	assets, streams, stream types, stream views	Returns all items with Ids that begin with <b>Id</b> .
Name:Name1	assets, streams, stream types, stream views	Returns all items with a name equal to <b>Name1</b> .
Id:Id AND Name:Name1	assets, streams, stream types, stream views	Returns the item with an Id equal to <b>Id</b> and a name equal to <b>Name1</b> .
Description:floor1*	assets, streams, stream types, stream views	Returns all items with a description that starts with <b>floor1</b> .
Metadata/Serial Number:M0000*	assets, streams	Return all items that include metadata of the name "Serial Number" that start with <b>M0000</b> (such as M000099 and

Query string	Applies to	Description
		M000001).
Id:X* AND Metadata/ Location:B*	assets, streams	Returns all items that contains: An Id starting with X. A metadata with the name Location that has a value that starts with B (such as "Boston").
Tags:MarkedAsset	assets, streams	Returns all items that have <b>MarkedAsset</b> as a tag.
AssetTypeId:HeaterTypeId	assets	Returns all items with AssetTypeId matching <b>HeaterTypeId</b> .
AssetTypeName:HeaterTypeNa me	assets	Returns all items whose asset type Name field matches <b>HeaterTypeName</b> .
StreamPropertyId:Pressure	assets	Returns all items that have one or more stream references with the stream property ID <b>Pressure</b> . Note: This search only searches non-key Sds stream properties.
StreamReferenceName:Name1	assets	Returns all items whose stream references contain a stream reference name that matches <b>Name1</b> .

## Search result examples

When searching for the following streams:

streamId	Name	Description
stream1	tempA	Temperature from DeviceA
stream2	pressureA	Pressure from DeviceA
stream3	calcA	Calculation from DeviceA values

Entering the following queries returns the following streams:

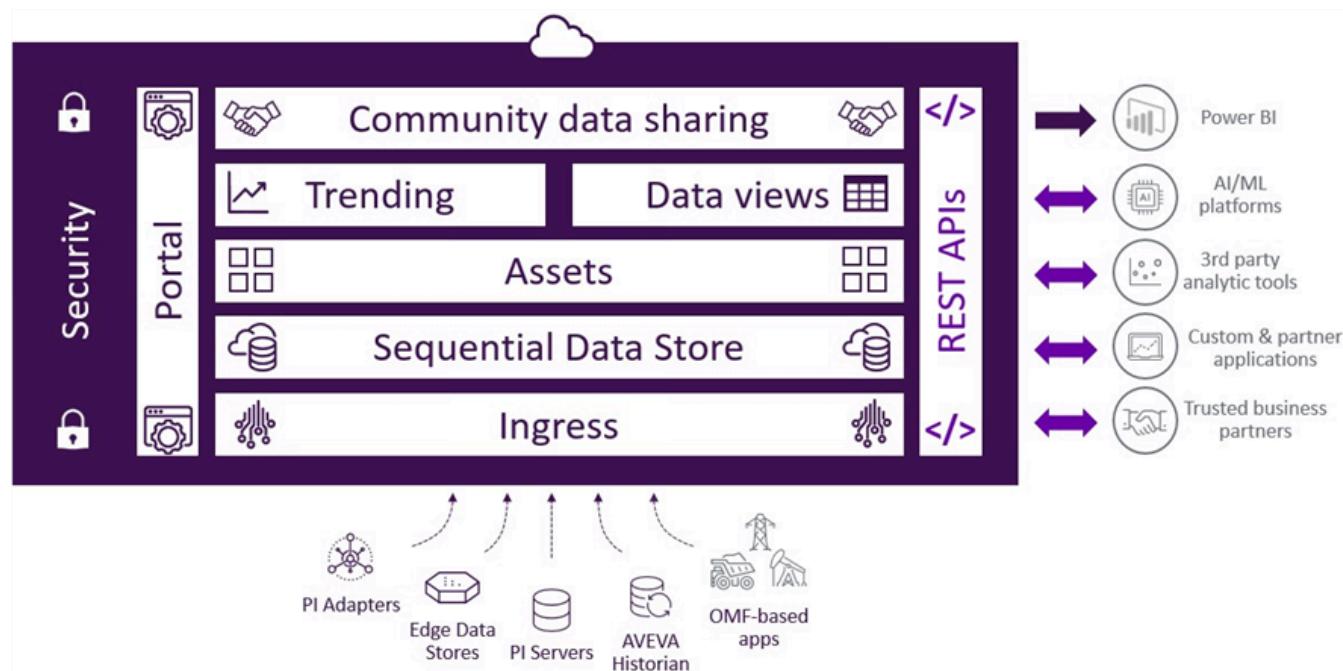
Query string	Returns
temperature	stream1
calc*	stream3
DeviceA*	stream1, stream2, stream3
humidity*	nothing

# Get started

Welcome to CONNECT data services! This Get Started guide walks you through initial setup and configuration of the CONNECT data services platform. Then it provides an overview of some of the major capabilities available for the platform. It is not a comprehensive guide for all available features.

Because CONNECT data services sits on top of the CONNECT platform, setup and configuration of CONNECT data services also requires use of CONNECT. Therefore, this Get Started guide refers to various help topics in both the CONNECT data services and CONNECT documentation.

The following image displays each feature available in CONNECT data services. The topics listed below describe the features, functionality, and implementation of the features depicted in the image.



Complete the following major steps to get up and running in CONNECT data services.

- Set up CONNECT for CONNECT data services
- Set up CONNECT users and groups
- Set up CONNECT data services groups, roles, and permissions
- Ingress data
- Manage your data
- Egress data

## Set up CONNECT for CONNECT data services

To use CONNECT data services, you need to log in to CONNECT and subscribe to CONNECT data services.

### Step 1A: Log in to CONNECT

Sign in to CONNECT using any of the available sign-in options. To learn how to sign in, see [Log into CONNECT](#).

#### Step 1B: Subscribe to CONNECT data services

Before you can use CONNECT data services, you need to subscribe to it within CONNECT. To learn how to complete this process, see [Subscribe to CONNECT data services](#).

#### Step 1C: Create a folder and enable CONNECT data services

Start by creating a folder for CONNECT data services. A *folder* is an organizational unit used to partition data. They are similar to folders in a traditional tree explorer. Within CONNECT data services, folders map one-to-one with *namespaces*, which is the CONNECT data services term for a folder. Folders and namespaces are synonymous.

To learn how to create a folder and enable CONNECT data services, see [Create a folder and enable CONNECT data services](#).

For information and best practices on folders, see [Folders and namespaces](#) and [Folder best practices](#).

## Log into CONNECT

You can log into CONNECT using one of the following sign-in methods:

- Corporate sign-in: federation for single sign-on
- Single user sign-in
- Third-party user access

If you attempt a sign-in ten times consecutively with a wrong password from the same location (IP address), then your login is blocked. If this happens, contact [AVEVA Customer Support](#) to unlock your account.

### Corporate sign-in: federation for single sign-on

Some CONNECT accounts use Active Directory Federation Services (AD FS), which enables authentication and authorization to CONNECT applications using the corporate user identity. This enables you to use single sign-on with the user account from the corporate domain.

To sign-in with single sign-on:

1. Browse to [CONNECT](#).
2. Select **Sign in**.
3. Sign in with your credentials.

The CONNECT home page displays.

### Single user sign-in

To sign in as a single user:

1. Browse to [CONNECT](#).
2. Select **Sign in**.
3. Sign in with your credentials.

The CONNECT home page displays.

## Third-party user access

A connection code enables third-party users to access specific accounts associated with an Identity Provider. Any accounts that are not intended for the third-party user are hidden.

To sign in as a third-party user using a connection code:

1. Browse to [CONNECT](#).
2. Select **Have a connection code?**

The screenshot shows the AVEVA logo at the top. Below it, a text box contains the instruction: "If you have a connection code to access your account, enter it here." A note below states: "Note that this is only relevant to customers authenticating via a specific federated connection." A text input field is labeled "Connection code". At the bottom are two buttons: "BACK" on the left and "NEXT" on the right.

3. Enter your connection code. This code is provided by AVEVA.

A direct sign-in link can be provided to enable quick access to restricted accounts. The third-party user will receive an email invitation that contains the direct link.

4. Select **Next**.
5. Select the desired account.

The CONNECT home page displays for the selected account.

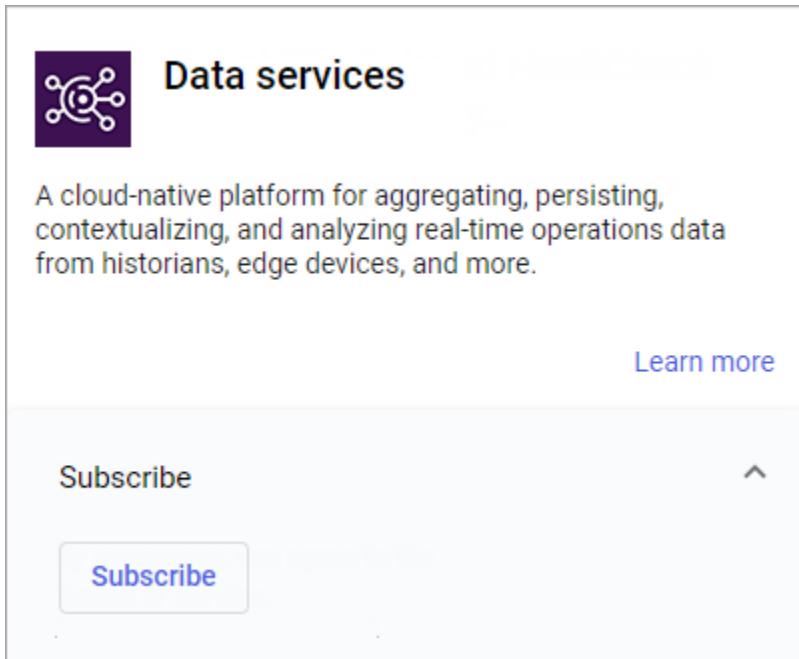
## Subscribe to CONNECT data services

Before your organization can use CONNECT data services, you must first subscribe to the CONNECT data services service within CONNECT. You must be a CONNECT administrator to complete the subscription process.

**Note:** If you have any questions or issues related to this procedure, contact [AVEVA customer support](#).

1. From the CONNECT home page, select **Services Catalog**.
2. Scroll to **Data services**. Select **Subscribe**.  
The Services Catalog page displays a list of AVEVA Cloud service offerings.
3. Scroll to the Data services tile.
4. On the Data services tile, select the carat to the right of **Subscribe**.

The Subscribe section expands as shown in the image below.



5. Select **Subscribe**.

The CONNECT data services service subscription is enabled for your organization.

**No option to subscribe?** Contact your AVEVA Account Manager.

## Create a folder and enable CONNECT data services

Before CONNECT data services can be accessed, you must create a folder in CONNECT (or select an existing folder) and turn on the CONNECT data services service for that folder. This action creates a namespace within CONNECT data services that will be linked to the CONNECT folder and have its name. A namespace in CONNECT data services is where data and resources are stored. For example, you can create CONNECT folders (and, in turn, CONNECT data services namespaces) such that your data is stored in a region that meets your data location requirements. For more information, see [Folders and namespaces](#).

### Create a folder

Perform the following steps to create a folder in CONNECT:

1. From the CONNECT home page, select **Folder management**.

**Note:** This action is only available to CONNECT Account Administrators. See [View Role Assignments](#) in the CONNECT documentation.

2. Select **Add folder**.
3. In the **Folder name** field, enter the name of the new folder. This will also be the name of your CONNECT data services namespace.
4. To change the default region, select **Change**, choose a region from the dropdown selector, and select **Save**.

Support for CONNECT data services is limited to specific geographical regions, listed in the following table. The table also lists the mapping between region labels in CONNECT and CONNECT data services. If your CONNECT folder region is not supported by CONNECT data services, you will be prompted to select a different region for the CONNECT data services instance when you enable CONNECT data services for the folder.

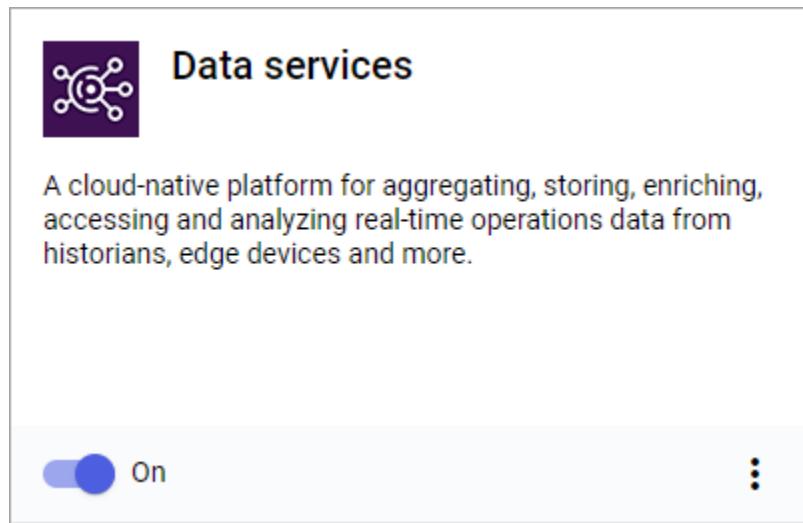
CONNECT region label	CONNECT data services region label
US-West	(westus)
EU-West	(northeurope)
Australia	(australiaeast)

5. Select an **Image** to represent the folder. Either upload your own image or select a stock image.
6. Select **Save**.

## Enable CONNECT data services

To enable CONNECT data services for a folder:

1. Select **Folder Management**. Open the folder.
2. Set **CONNECT data services** to **On**. Then select **Enable** to confirm the selection.



**Note:** The default maximum number of namespaces for a tenant (CONNECT account) is five. To increase this maximum, customers must communicate this request to AVEVA.

## Folders and namespaces

A CONNECT account can only be associated with one CONNECT data services tenant. Each tenant may have more than one namespace, and each namespace maps to a unique folder in a CONNECT account.

A namespace represents a logical unit of organization for data within a tenant. When you create a folder in CONNECT and enable the CONNECT data services tile, a namespace is automatically created in CONNECT data services. Multiple folders in CONNECT can have CONNECT data services turned on. Each folder represents a namespace, and all of the namespaces are part of one tenant and one CONNECT account.

Data processing resources are allocated to a namespace after you create a folder and turn on CONNECT data services. For example, SDS and asset services, and the associated storage resources are allocated to support a namespace. Each namespace and its resources are distinct and separate from all other namespaces. For example, you can create an SdsType or an SdsStream object with the same name in two different namespaces.

Identity resources in CONNECT data services, such as users and clients, are scoped globally across namespaces. For example, it is not possible to have User1 in the Production namespace but not in the Staging namespace. In CONNECT, users are globally-scoped with the ability to exist and have permissions across all folders in a CONNECT account.

Data stored within a namespace is tied to the namespace's region. You cannot directly transfer this data to any other namespace (or region). To move data between namespaces, you must export the data from the source namespace in CONNECT data services, then import it into the destination namespace (for more information, see [Transfer PI System data to CONNECT data services](#)).

As the administrator or developer setting up folders and namespaces, consider the following important points:

- Before CONNECT data services can receive data for a given tenant, a namespace must exist within the scope of the CONNECT data services tenant.
- A namespace is linked to an associated CONNECT folder.
- The CONNECT folder specifies the data storage region; for example, West US or Northern Europe. Alternatively, a CONNECT data services namespace can have its own defined region separate from its CONNECT folder's region if CONNECT data services does not support the CONNECT folder's region.
- The folder name is saved as the namespace name.
- A namespace's name can only be changed by editing the associated CONNECT folder name.

## Best practices

We recommend that you create CONNECT data services namespaces for each region that data needs to be stored in to help meet data sovereignty requirements or latency requirements. Another option would be to use CONNECT data services namespaces to segment data for development, staging, and production scenarios. Note that objects (such as streams) and collections (such as Data Views) do not automatically inherit security from the namespace with which they are associated.

## PI Server counterpart

A namespace is similar to a full PI Server. Much like a PI Server, a namespace has its own resources and it is not typical or easy to use data from multiple namespaces at the same time. It is reasonable for a tenant to have only one namespace.

## Namespace IDs

A namespace ID is defined by the solution ID in the CONNECT folder. You can view a namespace's ID by selecting the **Change Namespace** dropdown list in the CONNECT data services portal. The namespace name is synchronized with the CONNECT folder name.

## Querying data across namespaces

When querying API endpoints, the namespace ID is part of the URL. The API URL takes the form `https://{{server}}/api/{{version}}/Tenants/{{tenant_id}}/Namespaces/{{namespace_id}}`, followed by the API path, such as `/Streams`. Because the URL contains the namespace, it is not possible to make a single API request for data across multiple namespaces.

## Namespace deletion

A namespace gets suspended when the administrator turns off the CONNECT data services tile in a CONNECT folder. The customer then has 30 days to get the namespace reactivated. During the 30-day suspension period, neither reading or writing to the namespace is permitted. After 30 days, the namespace is deleted.

# Set up CONNECT users and groups

CONNECT data services users and groups are managed through CONNECT. You must first add users and groups in CONNECT before those users can access CONNECT data services. This section guides you through creation of users and groups in CONNECT. Later, in [Set up CONNECT data services groups, roles, and permissions](#), you will add these users and groups to CONNECT data services.

### Step 2A: Add users

Add the users that will use CONNECT data services to CONNECT. For instructions on completing this process, see [Add users in CONNECT](#).

### Step 2B: Add groups

AVEVA recommends managing users as groups, so you should create one or more groups to organize your users. For instructions, see [Add groups in CONNECT](#).

### Step 2C: Add users to a group

Place your users in the appropriate groups. For instructions, see [Add users to a group in CONNECT](#).

### Step 2D: Assign groups the CONNECT data services viewer role

Before you or any other user can log into CONNECT data services from CONNECT, you must first assign your user group the Data services Viewer role in CONNECT. This role allows users to see the service tile within CONNECT that allows you to log into CONNECT data services. For instructions, see [Assign the Data services Viewer role to a group in CONNECT](#).

## Add users in CONNECT

As an administrator, you set up new users in CONNECT. When a new user is added and assigned to a role, an email is sent to the user with an invitation to access CONNECT.

To set up new users:

1. From the CONNECT home page, select **User Management**.
2. Select **Users**.
3. Select **Add user**.
4. In the **Username** field, enter the user's email address.
5. Skip the **Groups** and **Add individual role** controls for now. You will add users to groups and apply roles to them in future steps.
6. Select **Save**.

The user is created and an email invitation to CONNECT is sent to the user's email address.

## Add groups in CONNECT

To be assigned access to CONNECT data services, Users must belong to one or more groups (unless you have assigned individual roles to your users). By default, all users created in your account belong to the User group in CONNECT. AVEVA recommends creating groups for each of your business units.

To create groups:

1. From the CONNECT home page, select **User Management**.
2. Select **Groups**.
3. Select **Add group**.
4. In the **Group name** field, enter a group name.
5. In the **Group description** field, enter a description for the group.
6. Skip the **Users** field for now. You will add users to the groups in future steps.
7. Select **Save**.

The group is created and users are assigned to the group. The new group does not have permissions to perform tasks in CONNECT data services until you assign a role to the group. You can modify existing groups from the **Groups** tab. After you select an existing group from the list, you can add or remove existing users from that group and assign or revoke roles to the existing users in that group.

## Add users to a group in CONNECT

As a best practice, AVEVA recommends assigning users to groups so that they can be managed as a single object in CONNECT data services. Add the users that you created in [Add users in CONNECT](#) to the appropriate groups that you created in [Add groups in CONNECT](#).

To add users to a group:

1. From the CONNECT home page, select **User Management**.
2. Select the **Groups** tab.
3. Select the group that you want to add users to.  
You can search for the required group by typing in the **Filter by group name** field.
4. Select **Add users** to add users to the group.

5. Enter the usernames of the users you want to add to this group. You can add multiple users at a time.
6. After you have added users, select **Save**.

## Assign the Data services Viewer role to a group in CONNECT

Assigning groups the Data services Viewer role allows users to see the Data services tile on the CONNECT home page.

To assign roles to a group:

1. From the CONNECT home page, select **User management**.
2. Select **Roles**.
3. Select **Assign role**.
4. Verify that the **Service** role option is selected.
5. From **Service**, select **Data services**.
6. From **Folder**, select the folder that you created in [Create a folder and enable CONNECT data services](#).
7. From **Role**, select **Data services Viewer**.
8. From **Groups**, select the groups that you created in [Add groups in CONNECT](#).
9. Select **Save** to save these changes.

The Data services Viewer role is now assigned to the selected groups.

## Set up CONNECT data services groups, roles, and permissions

Add the groups that you created in CONNECT to CONNECT data services, and then assign roles and permissions to your users.

### Step 3A: Log In to CONNECT data services

From CONNECT, log into CONNECT data services. For instructions, see [Log into CONNECT data services](#).

### Step 3B: Add groups and assign roles

Add the groups that you created in CONNECT to CONNECT data services. Then assign one or more roles to the groups. For instructions, see [Add groups and assign roles in CONNECT data services](#).

### Step 3C: Manage namespace permissions

Assign namespace permissions to each user role using the Namespace Settings window. For instructions, see [Manage permissions for namespaces](#).

### Step 3D: Manage resource permissions

Assign permissions for system resources to each user role using the Manage Permissions window. For instructions, see [Permissions management](#).

## Log into CONNECT data services

[Log into CONNECT data services](#).

**Note:** CONNECT data services supports the latest versions of Microsoft Edge, Google Chrome, and Mozilla

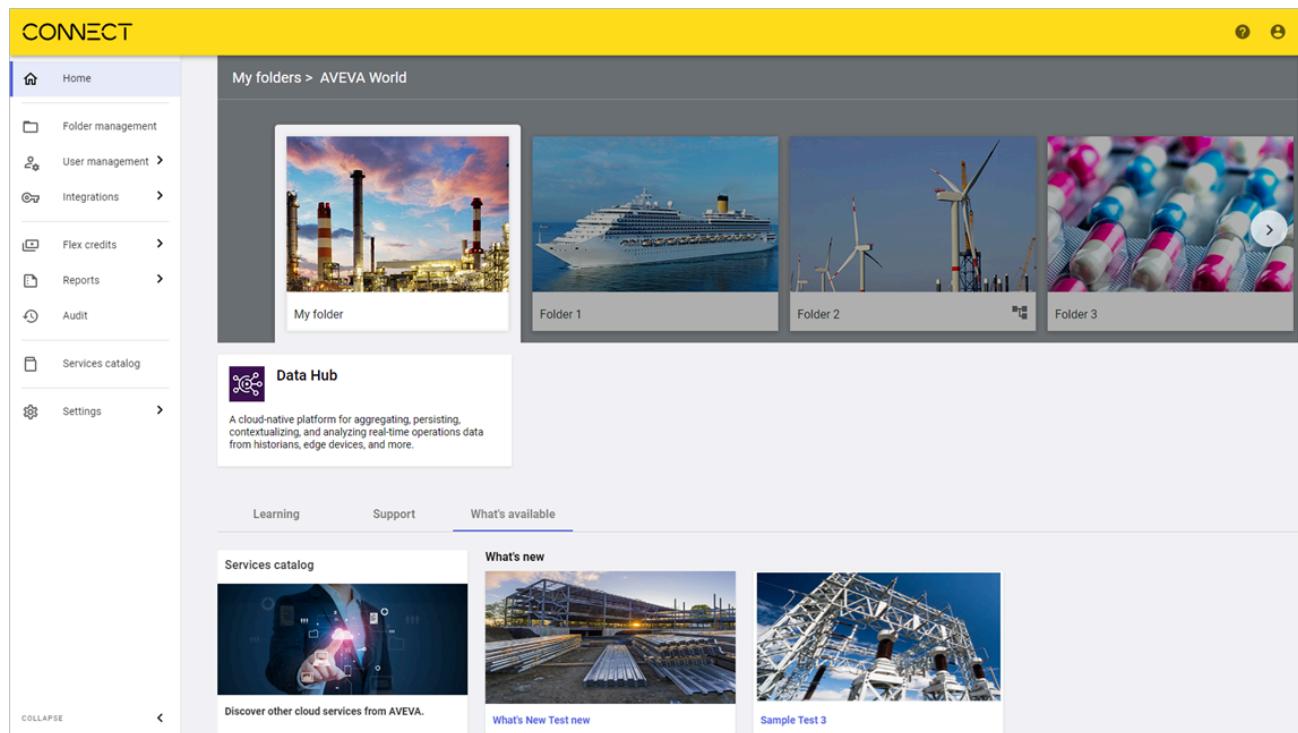
---

Firefox.

1. Open CONNECT.

If single sign-on is enabled, you only need to provide your email address when signing in to CONNECT. You may be prompted to sign into your corporate Sign-In page.

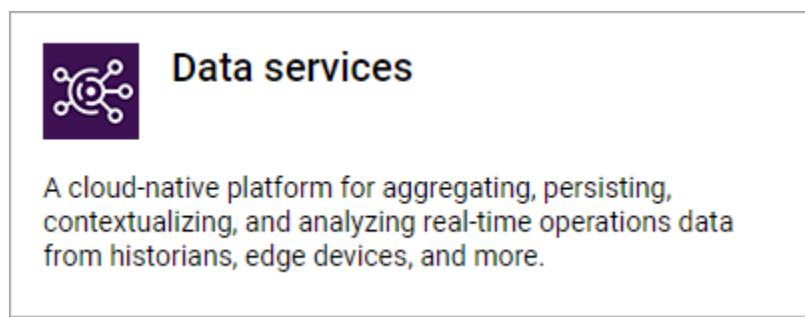
2. From the CONNECT home page, select the folder that represents your organization's services.



The screenshot shows the AVEVA CONNECT Data Hub interface. On the left is a navigation sidebar with options like Home, Folder management, User management, Integrations, Flex credits, Reports, Audit, Services catalog, and Settings. The main area shows a folder structure under 'My folders > AVEVA World'. It includes four folder tiles: 'My folder' (industrial facility), 'Folder 1' (cruise ship), 'Folder 2' (wind turbines), and 'Folder 3' (pharmaceuticals). Below this is a 'Data Hub' section with a description: 'A cloud-native platform for aggregating, persisting, contextualizing, and analyzing real-time operations data from historians, edge devices, and more.' There are tabs for Learning, Support, and What's available. Under 'What's available', there are sections for 'Services catalog' (with a thumbnail of a person interacting with a digital interface) and 'What's new' (with thumbnails of industrial structures and a complex metal framework).

The applications available from this namespace account are displayed below the folder.

3. Select the Data services tile.



The screenshot shows the AVEVA Data services portal. It features a purple icon with a network of nodes and the text 'Data services'. Below it is a descriptive paragraph: 'A cloud-native platform for aggregating, persisting, contextualizing, and analyzing real-time operations data from historians, edge devices, and more.'

The CONNECT data services portal opens.

## Add groups and assign roles in CONNECT data services

Add existing CONNECT groups to CONNECT data services and then assign roles to the group. Roles control the individual permissions assigned to users in the group, controlling the actions they can make in CONNECT data services.

To assign an existing CONNECT group to a role in CONNECT data services:

1. Open the CONNECT data services portal.
2. From the left pane, select **Security > Groups**.
3. Select **Add Group**.
4. In the **Name** field, enter the name or first few characters of a CONNECT group name, then press Enter.
5. Assign a role, or multiple roles, to the group to control the actions members can take in the CONNECT data services portal, then select **Save**.

AVEVA recommends mapping the CONNECT groups that you created in [Add groups in CONNECT](#) to the built-in tenant roles.

- For more information on the six built-in tenant roles, see [CONNECT data services roles](#).
- For more information on creating a custom role, see [Add a role in CONNECT data services](#).

## Manage permissions for namespaces

If you are assigned the **Manage Permissions** access right, then you can configure namespace permissions for other user roles in your tenant. You can granularly assign individual namespace permissions to each user role.

### Prerequisites

To manage namespace permissions, you must be assigned the **Manage Permissions** access right.

### To manage permissions for namespaces

Use the **Namespaces** dropdown list that is available on all pages to edit permissions for a namespace.

1. From the **Namespaces** dropdown list, select the namespace that you want to edit permissions for.
2. Select the **Manage Settings**  icon.  
The **Manage Permissions** tab of the Namespace Settings window opens.
3. Use this window to:
  - (Optional) Add user roles that have permissions on the namespace.
  - Edit namespace permissions for each user role.  
[For more information, see Permissions management.](#)
4. When you are finished editing permissions, select **Save**.

## Permissions management

Within CONNECT data services, permissions are applied to [CONNECT data services roles](#) per resource. The user roles assigned to each user determine whether they can access the resource. You can granularly edit permissions for the following system resources. Open the following pages for instructions on how to edit permissions for each system resource.

- [Manage permissions for agents](#)
- [Manage permissions for asset rules](#)

- Manage permissions for asset types
- Manage permissions for assets
- Manage permissions for data views
- Manage permissions for namespaces
- Manage permissions for streams
- Manage permissions for types

## Manage Permissions window

All system resources are managed using the Manage Permissions window. Use this window to apply permissions to each user role for a system resource. This window displays a matrix of roles, permissions, and permission settings for the resource you are managing. Use the matrix to:

- Add new roles that have permissions on the resource.
- Update individual permission settings.

### Namespace Settings

[Manage Permissions](#) [Data Sharing](#)

Access control is managed by assigning permissions to Roles in your tenant. Users will be able to perform an access operation (read, write, delete, or manage permissions) if they have a role which is assigned an access type of **Allow** and they do not have a role which is assigned an access type of **Deny** for that operation. The user or application who created a resource, identified as the **Owner**, is always guaranteed complete access on that resource.

Entries in the table are pre-populated with Roles that contain assigned permissions. To add additional Roles and assign permissions, click the **Add Role** button and select the Roles you want to assign permissions to. Roles not included in the table will have their permissions reset.

**+ Add Role**

Role	Read ⓘ	Write ⓘ	Delete ⓘ	Manage Permissions ⓘ
Tenant Administrator	Allow	Allow	Allow	Allow
Tenant Contributor	Allow	Allow	-	-
Tenant Member	Allow	-	-	-

[Cancel](#) [Save](#)

Use this window to complete the following actions:

- Add roles
- Remove roles

- Edit permissions
- Clear permissions

## Add roles

Add roles that have permissions for the resource by selecting **Add Role** > **Add** .

## Remove roles

Remove newly added roles by selecting  **Remove**. Roles that were added previously cannot be removed because they already have permissions assigned that must be cleared first.

## Edit permissions

Read, Write, Delete, and Manage Permissions permissions can be edited for each user role that has permissions on the resource. Data stream resources include an additional Share permission to support [Communities](#). Mouse over each Information  icon for more information about each permission.

- To allow a permission, select  **Allow**.

**Note:** If you set a **Write** permission to **Allow** while the **Read** permission is cleared, **Read** is automatically set to **Allow** because write permissions require read permissions.

- To explicitly deny a permission, select  **Deny**.

**Note:** When a user is assigned multiple user roles with conflicting permissions, a setting of  **Deny** supersedes a setting of  **Allow** or undefined (-).

## Clear permissions

Clear the permissions applied to a role by selecting  **Remove**.

### Notes:

- Allow Manage Permissions access is required on at least one role.
- If you clear all permissions from a role for a resource, the role is not listed the next time that you manage permissions for the resource.

## Modified roles

Roles that are highlighted indicate that one of more of its permissions settings have been modified. Newly added roles are highlighted as well. You can restore the original settings by selecting **Cancel**.

## Namespace Settings

Manage Permissions Data Sharing

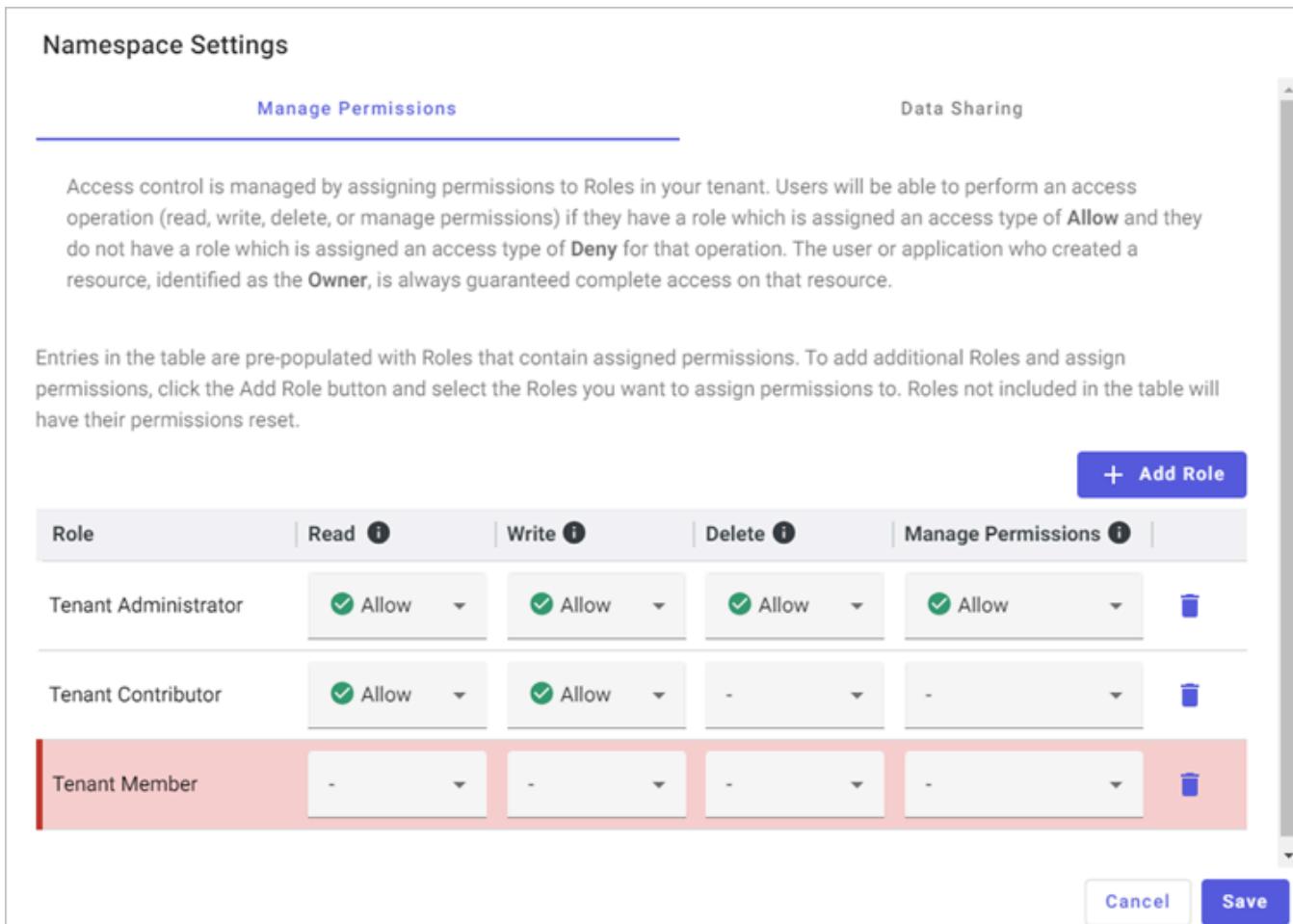
Access control is managed by assigning permissions to Roles in your tenant. Users will be able to perform an access operation (read, write, delete, or manage permissions) if they have a role which is assigned an access type of **Allow** and they do not have a role which is assigned an access type of **Deny** for that operation. The user or application who created a resource, identified as the **Owner**, is always guaranteed complete access on that resource.

Entries in the table are pre-populated with Roles that contain assigned permissions. To add additional Roles and assign permissions, click the Add Role button and select the Roles you want to assign permissions to. Roles not included in the table will have their permissions reset.

+ Add Role

Role	Read ⓘ	Write ⓘ	Delete ⓘ	Manage Permissions ⓘ
Tenant Administrator	<input checked="" type="checkbox"/> Allow			
Tenant Contributor	<input checked="" type="checkbox"/> Allow	<input checked="" type="checkbox"/> Allow	-	-
Tenant Member	-	-	-	-

Cancel Save



## Cross-region data sharing

By default, CONNECT data services processes operational data from your tenant's namespaces and communities in geographical regions other than the originally chosen geographical region. CONNECT data services shares this data for the following purposes:

- Performance optimization
- Enabling users to search and access data that may be stored across regions

For example, if you have a namespace in CONNECT data services that stores operational data in the US-West region, CONNECT data services may process that data in the EU-West region.

## Cross region data sharing scenarios

Cross-region data sharing is enabled by default. When cross-region data sharing is enabled, CONNECT data services may share operational data for a namespace across regions under the following circumstances.

## Additional processing

Each namespace in CONNECT data services is bound to a geographical region. Operational data stored in each namespace is usually processed within that region, which is chosen while adding the namespace.

However, CONNECT data services may process a namespace's operational data in a different region (in other words, *cross-region*). For example, if you create a namespace in the US-West region, CONNECT data services may process its operational data cross-region in EU-West.

Processing operational data usually involves reshaping it. In these instances where operational data is processed cross-region, data from your region may reside in the cross-region processing service memory up to several hours.

## Data augmentation

In use cases where your operational data is stored within both the chosen region and cross-region, CONNECT data services may process data from the chosen region in a different region. CONNECT data services then adds and processes additional operational data from the cross-region before it displays in your browser session. In these instances, your data from both regions resides in the cross-region processing service memory up to several hours.

## Temporary storage

In some instances where CONNECT data services sends operational data stored in your namespace's region for processing or data augmentation cross-region, CONNECT data services may temporarily persist data from your region across regions before it is processed. This temporary storage is used for performance optimization. In these instances, data from your region persists in the cross-region processing service storage and memory up to several hours.

## Opt out of cross-region data sharing

Optionally, you can opt out of sharing operational data from namespaces and communities across regions. If you opt out of cross-region data sharing, your operational data is not processed or stored outside of the namespace's assigned region.

### To opt out of cross-region data sharing for namespace

When you disable cross-region data sharing, any queries for namespace data are routed to the appropriate region for complete results to be returned. Repeat these steps for each namespace that you want to disable cross-region data sharing.

1. From the **Namespace** dropdown, select a namespace for which you want to opt out of cross-region data sharing.
2. Select the **Manage Settings**  icon next to the **Namespace** dropdown.
3. Select the **Data Sharing** tab.
4. Enable **Opt-out for Namespace** and select **Save**.

**Important!** If you opt out of cross-region data sharing for a namespace that includes streams shared with a

---

community, you should also update the community preferred region setting. Using this setting, you can override the default region to explicitly choose where operational data is processed. For more information, see [Manage preferred region](#).

---

## Ingress data

Ingress data into your CONNECT data services tenant using any of the following options. For a full list of data ingress sources for CONNECT data services, see [Data ingress sources](#).

### Option A: Collect data from PI Server

Transfer on-premises PI Data Archive and Asset Framework (AF) data into CONNECT data services via a PI to CONNECT Agent.

1. [Install the PI to CONNECT Agent](#).
2. [Run the PI to Data Hub Agent Configuration Utility](#).
3. [Create a data transfer](#).

### Option B: Collect data from OMF applications

Collect data from edge devices and other sources using the following OMF applications:

- AVEVA Adapters
- Edge Data Store
- AVEVA Historian (2023 and later releases)
- PI Interfaces (health and diagnostics data only)
- Custom OMF applications provided by others

**Prerequisite:** You must have the OMF application installed and configured.

1. Review [OMF connections best practices](#).
2. Add a client-credentials client. The OMF application uses this client to authenticate with CONNECT data services.
3. [Configure an OMF connection](#). Connect your OMF application to CONNECT data services.

### Option C: Collect data from custom applications

APIs provide programmatic access to bring sequential data into CONNECT data services. You can do this through the development of custom applications provided by others.

## Manage your data

After initial setup, you can begin to manage your data and the different components available in CONNECT data services, including:

- [Get started with streams](#)
- [Get started with assets](#)
- [Get started with communities](#)

## Get started with streams

Streams are a collection of ordered events, or a series of events, where each event is an instance of the type you have defined. You create and write data to streams using a simple REST API. The streams you create can be used to store simple or complex data types to suit your application needs. You can define simple or complex indexes to arrange and relate your data.

For additional information about stream best practices, see [Manage streams](#).

### 1. Sequential Data Store

The *Sequential Data Store* (SDS) is a streaming database optimized for storing sequential data, typically time-series data. It can store any data that is indexed by an ordered sequence. For each namespace that is created, an SDS instance or SDS resources is created. Use SDS to store, retrieve, and analyze data.

### 2. Search queries

From the Sequential Data Store, use the **Search for Streams** field to find streams that you want to work with. For more information on using the field and specifying search criteria, see [Search queries](#).

### 3. Create a trend session

Using a *Trend session*, you can look for patterns in your streams over time. Trend sessions display property values from your streams with a given time range. You can view multiple streams in a Trend session, and you can view all property data for each stream.

### 4. Add a type

A *type* defines the shape and structure of events and how to associate events within a stream of data. A type is comprised of at least two properties. One property serves as the primary index, most commonly a timestamp or DateTime. In addition, it has one or more additional properties called value properties that describe the data in each stream event. Each value property can have a different property type. A wide variety of property types are supported.

#### Additional documentation:

- [Types best practices](#)
- [Learn more about types in the Developer Guide](#)

### 5. Create a metadata rule

When possible, you should explicitly include metadata when you create streams. However, when that is not possible, you can use metadata rules to leverage a consistent naming pattern for streams to embed metadata.

Metadata, or data about data, is a collection of attributes that stream instances of a stream type are expected to provide. The type and units of measure for the value can be defined. Metadata enriches sequential data in CONNECT data services and it logically silos and contextualizes data. It supports data analysis, visualization, organization, and search capabilities.

A metadata rule is a user-defined stream name pattern in which each part is assigned a metadata type. Metadata rules capture any streams currently stored in a namespace, as well as matching streams that are subsequently added to the namespace.

**Additional documentation:**

- [Stream metadata rules](#)
- Learn more about metadata rules in the API Reference

## 6. Stream views

A stream view is a logical overlay that enables you to customize your view of streaming data so it is most useful to you. While you cannot change the properties of types, stream views enable you to create a view of a stream, so it appears as if you had changed the type. You create a stream view by choosing a source and target type, and then defining mappings between the properties of the two types. The source type is the type associated with the stream. The target type includes the properties you want to include in the stream view. In effect, you can remove, rename, or add properties without altering the original stream type.

# Get started with assets

An *asset* is a digital entity that can be used to model real-world entities. For example, a wind turbine or a mixing tank. An asset consists of three parts: metadata, property and status.

For additional information about asset best practices, see [Assets](#).

## 1. Add an asset

Assets are digital twins of real-world equipment. Using assets, you can apply:

- *Metadata* – Add static metadata to your assets - information about the asset that does not change. This metadata provides contextual knowledge for assets. For example, if you are adding metadata for a wind turbine, you can add information such as its region or manufacturer number.
- *Properties* – Properties are references that associate real-time data streams with an asset. They also add extra context, such as when a user adds a stream reference to an asset. Properties provide a user-friendly name for reference, such as "temperature" or "pressure", to add context to underlying streams that often have naming conventions that may be difficult to understand.
- *Status* – Map statuses to a variety of values that indicate the asset status. Then use that status to filter through assets in the Asset Explorer using real-time measurements, viewing their current status based on a property value. You can choose an enumeration or integer property on the asset and map its values to "Good", "Warning", or "Bad" as the asset status. These statuses help you filter through assets and locate those that need immediate attention.

## 2. Create an asset type

An *asset type* is a template for creating assets that share a common structure or type. When you create an asset type, you define the expected metadata, stream references, and status for assets created from that asset type. With a defined asset type, you can easily replicate assets sharing common metadata and properties.

Before working with asset types, review the following documentation: [Asset types](#).

There are two ways to create an asset type:

- From nothing ([Create an asset type](#))
- From an existing asset ([Convert an asset to an asset type](#))

## 3. Create an asset rule

Use asset rules to efficiently scale creation of assets. An asset rule identifies patterns in the naming convention for streams and uses this information to automatically create or update assets.

**Additional documentation:**

- [Asset rules](#)

## Get started with communities

Communities allow a tenant to create a private group where operational data can be shared and viewed across other tenants. Using communities, industrial companies can share their data streams externally with trusted business partners, service providers, and analytics providers.

- **Seamless Data Sharing:** Facilitate easy and secure data exchange among engineering and operational partners.
- **Enhance Operational Efficiency:** Collaboratively streamline operations and minimize waste through shared operations data.
- **Uncover Hidden Issues:** Detect and troubleshoot equipment and process problems with insights from your partners' operational data and expertise.
- **Proactive Failure Prediction:** Predict and prevent future failures by leveraging collective data intelligence.

To create or join a community, follow the applicable scenario listed in the headings below. Regardless of which scenario you follow, reviewing the following documentation on communities is recommended:

- [Communities](#)
- [Community setup](#)

### Scenario A: Create community and invite other tenants

To create a community, invite other tenants, and share streams into the community, complete the instructions in the following topic: [Workflow: Create a community](#).

### Scenario B: Join an existing community

To join a community that another tenant has invited you to, complete the instructions in the following topic: [Workflow: Join a community](#).

## Egress data

Within CONNECT data services, *egress* is the concept of data stored within CONNECT data services leaving or exiting the system. You can egress data from CONNECT data services for use in other applications.

## Data Views

Data views allow you to access subsets of data items from CONNECT data services in data-driven applications, where the items can be used for data science enablement. With data views, you can prepare your raw CONNECT data services data for third-party applications like Microsoft Power BI, where it can be used for analytics, machine learning, reporting, and visualization. Users can programmatically retrieve data view content using the CONNECT data services API. Data views deliver shaped data that is ready for consumption because it is

normalized, aligned, and contextualized.

First, you must create and configure a data view. The CONNECT data services resources included in the data view are based on the result of one or more queries, which you must configure. Streams, assets, and other CONNECT data services resources that can be included in a data view are known as *data items*. Streams shared to communities can also be included. Properties from data objects and information about the data items (such as Id and Metadata) can be included in the data view as *fields*.

Refer to the following topic for a workflow of how to get started creating and configuring a data view: [Create and configure a data view](#).

## API Console and REST API

CONNECT data services includes an API console that you can use to create and refine requests to the CONNECT data services REST API. After building and refining your requests using the console GUI—including edits to the URI, query parameters, request headers, and request body—you can implement the request in your own application. For more information about the console, see [API console](#).

For a list of service endpoints available within the API console, refer to the CONNECT data services API Reference. This reference lists each service available within CONNECT data services, their available endpoints, and their available parameters. Enter these endpoints and parameters into the API console to create and refine API requests.

## Microsoft Power BI

The CONNECT data services Power BI Connector retrieves data views from CONNECT data services and makes them available in Microsoft Power BI where it can be used for analytics, machine learning, reporting, and visualization. You can also use Microsoft Power BI to edit the query generated from the connector to modify the dates, edit the interpolation interval, and enable an incremental refresh of data.

Refer to the following topics for more information on how to setup Microsoft Power BI for CONNECT data services and retrieve existing data views:

1. [Power BI Connector setup](#)
2. [Retrieve data views with Power BI Connector](#)

# Data management

The Data Management menu provides a number of tools for managing your data within CONNECT data services:

- Use the Sequential Data Store (SDS) to store, retrieve, and organize any type of streaming data.
- Use the Communities feature to create a private group to share data streams with external business partners, service providers, and analytics providers.
- Use Stream Metadata Rules to identify metadata such as location, asset class, and asset ID in stream names, then assign that defined metadata to all streams in a given namespace matching the stream name pattern.
- Use Asset Rules to identify patterns in a stream name and use this information to automatically create assets.
- Use Change Broker to create and view API Signups that monitor SDS streams and provide change data updates.

## Sequential Data Store

Use the Sequential Data Store (SDS) to store, retrieve, and organize any type of streaming data.

SDS types define the structure of data to be collected. A type is analogous to a template that defines each instance in a stream of data.

SDS stream data contains values or events of the same SDS type and is ordered (indexed) by one or more properties defined by the stream's SDS type, usually a timestamp.

## Streams

Sequential Data Store (SDS) stream data are values or events of the same SDS type. SDS stores stream data and indexes it by one or more properties defined in the stream's SDS type.

The SDS stream is the container that holds the data. When you create a stream, you add it to a specific namespace. Then you define an SDS type for that stream that determines the values and events in the stream, their data type, and the properties used to index the data. Once you create a stream, you cannot change its SDS type.

The SDS stream container uses metadata and tags to define information about the stream container itself. Metadata are key-value pairs that add context to the data, for example, the metadata key, Manufacturer, and a metadata value, Caterpillar. Tags are string values that represent stream attributes, for example, region. Organizing data using metadata tags and tags makes it much easier to retrieve data streams.

## PI Server counterpart

An SDS stream is comparable to a PI point in the Data Archive. For example, a float32 PI point might be sent to CONNECT data services as an SDS stream with a type that contains a timestamp index and float32 value. If you use PI to CONNECT to import data into SDS, each PI point in the Data Archive is created in SDS as an individual stream and the data itself is added as values in the stream.

## Manage streams

The Sequential Data Store gives you capabilities to manage stored streams. The capabilities function the same if you are working in the context of a namespace or a community.

### Streams best practices

The following best practices are recommended when creating streams:

- Ensure that the default stream permissions are configured before you begin creating streams. While you can later do a bulk update of stream permissions, it is easier to configure the default permissions before the streams are created. Permissions that vary from the default are configured on the individual streams.
- Use a meaningful pattern when naming streams. For example, a naming pattern might be "*Company\_name.{Region}.{Site}.{Equipment}*". This makes it possible for tools, such as metadata rules, to use this naming schema to find relevant data. Metadata like this can also be stored as key-value pairs on the stream, but a well-defined naming pattern allows metadata to be generated automatically.
- Use the stream description field, metadata, and tags to capture any other relevant information about the stream. This information is useful to search for specific streams in the system, especially as systems become large. If possible, use consistent patterns in description, metadata, and tags.
  - Use metadata for information that follows a specific or consistent pattern, such as the location, manufacturer, and site.
  - Use tags for simple information about the stream that does not adhere to any particular pattern.
  - Use the description field for longer descriptions of the stream and what it represents.

### Add a stream

Sequential Data Store (SDS) stream data are values or events of the same SDS type. SDS stream data are stored in the Sequential Data Store and indexed by one or more properties defined by the stream's SDS type.

To add a stream, follow these steps:

1. In the left pane, select **Data Management > Sequential Data Store**.
2. From the **Streams** dropdown list, select **Streams**.
3. Select **Add Stream**.
4. In the Add Stream pane, complete the following fields:
  - **Id** – (Optional) Enter an identifier for referencing the stream. If you do not enter an Id, a GUID is generated.
  - **Name** – (Optional) Enter a user-friendly name for the stream. If you do not enter a name, the **Id** is used as the name.
  - **Description** – (Optional) Enter a user-friendly description of the stream.
  - **Type** – SDS type identifier of the type used in this stream.

---

**Important:** Only types that have a key configured are available for selection. If you want to use a type that is not listed, you must first configure a key. For more information see [Add a type](#).
5. To add tags to the stream, select the **Tags** tab.

6. For each tag you want to add, enter the name of the tag in the **New Tag** field, and then select **+**.
7. Select the **Metadata** tab.
8. For each metadata you want to add, select **Add Metadata**, and then in the **Metadata Key** and **Metadata Value** fields, enter the key and corresponding value for the metadata.
9. To save the stream, select **Save**.

## Remove streams

When you remove a stream, you are deleting it.

1. From the left pane, select **Data Management > Sequential Data Store**.
2. Select one or more streams.
3. Select **More options**  > **Remove Stream**.
4. In the confirmation window, select **Remove** to confirm the deletion.

## Add tags or metadata

Tags and metadata allow you to associate additional information with a stream. For example, tags can denote special attributes for a stream. Metadata consists of keys and their associated values.

1. From the left pane, select **Data Management > Sequential Data Store**.
2. Select a stream.
3. Select **Edit Stream** .
4. Add tags.
  - Select the **Tags** tab, if it is not already selected. In the New Tag box, enter the name of the tag, and then select **Add Tag**  icon.
  - To remove a tag, select the **Remove Tag**  icon beside the tag name.
5. Add metadata.
  - Select the **Metadata** tab, and then select **Add Metadata**  . In the Metadata Key box, enter the name of the key and in the Metadata Value box, enter a value for that key.
  - To remove a metadata, select the **Remove Metadata**  icon beside the row to be deleted.

## Share streams

Users with permissions to share a data stream within a [community](#) can do so from the Sequential Data Store.

- For more information on sharing a stream with a community, see [Share streams](#).
- For more information on unsharing a data stream with a community, see [Unshare streams](#).

## View in trend

From the Sequential Data Store, you can select one or more streams for viewing within a trend session.

1. From the left pane, select **Data Management > Sequential Data Store**.
2. Select one or more stream.  
You can view up to 20 streams in a trend session.
3. Select **View in Trend**.

The Trend page opens in a new tab with each selected stream added to the trend session. For more information on working with trend sessions, see [Trend visualization](#).

## View stream data

You can view each data value for a stream by choosing it from the Sequential Data Store.

1. In the left pane, select **Data Management > Sequential Data Store**.
2. Select the stream that you want to view data for.  
**Tip:** Use [Search queries](#) to find your stream.
3. Select **View Data**.

By default, the last data value available for the stream displays. However, you can change which data values are displayed by editing the **Query Type** dropdown. See the heading below for more information.

**Tip:** You can manually add data values to a stream by adding an event. For more information, see [Add event](#).

## Edit query type

Edit the query type for the stream to view its first value, last value, or a range of data.

To edit the query type, ensure that the **First Value/Last Value/Range Query** button is enabled. Then select a value from the **Query Type** dropdown.

Query Type	Description
Get First Value	Gets the first recorded value for the stream.
Get Last Value	Gets the last recorded value for the stream.
Get Range Values	Gets a range of recorded values for the stream. For more information on setting a range, see the heading below.

## Range values

Ranged value queries get a range of recorded values for a stream. You can either query by count of data points or by range between a start and end index.

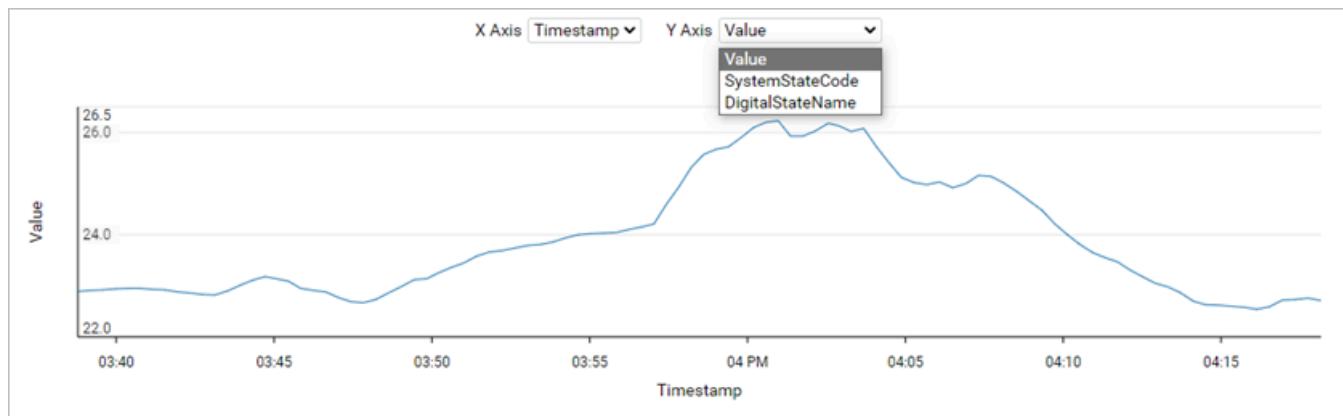
To query by count, select **By count** and configure the following parameters:

Parameter	Description
Start Index	The start index for the range. Choose a date and time. By default, this value is the current date and time.
Count	The maximum number of data values returned by the query. By default, this value is 100.
Reversed	The order that data is queried from the start index—forward or reversed. When set to <b>True</b> , the query returns data searching reversed through time (reverse chronologically). When set to <b>False</b> , the query returns data forward through from the provided start index (chronologically). By default, this setting is set to <b>True</b> .

To query by range, select **By range** and configure the following parameters:

Parameter	Description
Start Index	The start index for the range. Choose a date and time. By default, this value is the current date and time.
End Index	The end index for the range. Choose a date and time. By default, this value is the current date and time.

Select **Apply** to apply your parameters and execute the query. The data values included in the query are listed on screen, and they are plotted in a graph as well. For streams with multiple properties, you can view different data values included in the stream by editing the **X Axis** and **Y Axis** dropdowns, as depicted in the image below.



## Add event

While viewing the data for a stream, you can add *events*, which are data values that the user manually adds to a stream. Any events that you add to a stream can then be visualized while viewing the stream's data or viewing the stream in a Trend session.

To add an event to a stream, complete the following steps.

1. In the left pane, select **Data Management > Sequential Data Store**.
2. Select the stream to add an event for and choose **View Data**.

**Tip:** Use [Search queries](#) to find your stream.

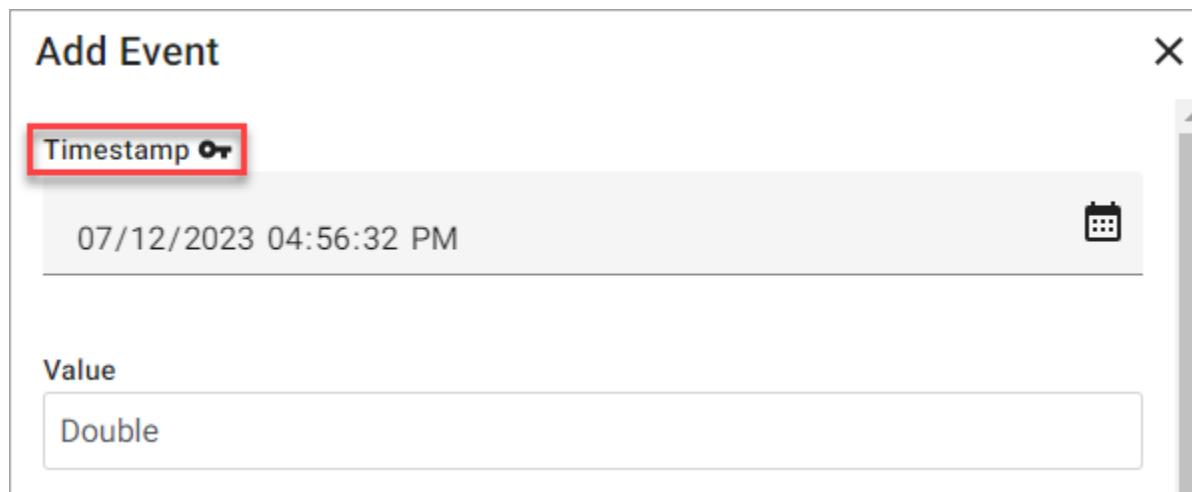
3. Select **Add Event**.

The Add Event panel opens.

4. (Required) Configure the key property for the event.

The key property is the index value for the event. This property is usually a DateTime value, but there is no restriction as to what data type the index can be within SDS.

#### Key property



The screenshot shows the 'Add Event' dialog box. At the top, it says 'Add Event'. Below that, there's a section labeled 'Timestamp' with a red border around it. To the right of the input field is a small calendar icon. Underneath the timestamp field, the date and time '07/12/2023 04:56:32 PM' are displayed. Further down, there's a section labeled 'Value' with a dropdown menu showing 'Double'.

5. Configure the remaining property values for the event.

For enumerated data types, values map to the friendly name rather than an integer.

6. Select **Save**.

The event is added to the stream. You can view the new event in your list of data values creating a ranged query that includes your new event.

#### Edit event

You can edit the values for any existing event.

1. In the left pane, select **Data Management > Sequential Data Store**.
2. Select the stream to edit an event for and choose **View Data**.

**Tip:** Use [Search queries](#) to find your stream.

3. Edit **Query Type** and its options to display the event that you want to edit.

For more information on editing the query type, see [Edit query type](#).

4. Choose the event that you want to edit and select the **Edit** icon.

5. Enter or select a value for each data type value.

For enumerated data types, values map to the friendly name rather than an integer.

6. Select **Save**.

The stream event is edited.

## Remove event

You can remove any existing event from a stream.

1. In the left pane, select **Data Management > Sequential Data Store**.
2. Select the stream to remove an event for and choose **View Data**.  
**Tip:** Use [Search queries](#) to find your stream.
3. Edit **Query Type** and its options to display the event that you want to remove.  
For more information on editing the query type, see [Edit query type](#).
4. Select the event that you want to remove. Then select **More options**  > **Remove Event**.
5. To confirm the removal, choose **Remove**.

The stream event is removed.

## Manage permissions for streams

If you are assigned the Manage Permissions access right, then you can configure stream permissions for other user roles in your tenant. You can granularly assign individual stream permissions to each user role.

### Prerequisites

To manage data stream permissions, you must be assigned the Manage Permissions access right.

### To manage permissions for streams

When managing permissions for streams, you can either edit them one at a time or in bulk.

When editing permissions for a single stream, each user role that has permissions assigned are pre-populated in the window that opens.

1. From the left pane, select **Data Management > Sequential Data Store**.
2. Select a single stream that you want to manage permissions for.
3. Select **More options**  > **Manage Permissions**.

The Manage Permissions for Stream window opens. Because you are editing permissions for a single stream, all user roles that have permissions on the stream are displayed along with their settings.

**Manage Permissions for stream 1**

Entries in the table are pre-populated with Roles that contain assigned permissions. To add additional Roles and assign permissions, click the Add Role button and select the Roles you want to assign permissions to. Roles not included in the table will have their permissions reset.

Role	Read <i>i</i>	Write <i>i</i>	Delete <i>i</i>	Manage Permissions <i>i</i>	Share <i>i</i>	
Tenant Administrator	<input checked="" type="checkbox"/> All... <i>v</i>	<input checked="" type="checkbox"/> All... <i>v</i>	<input checked="" type="checkbox"/> All... <i>v</i>	<input checked="" type="checkbox"/> Allow	- <i>v</i>	<i>trash</i>
Tenant Contributor	<input checked="" type="checkbox"/> All... <i>v</i>	<input checked="" type="checkbox"/> All... <i>v</i>	- <i>v</i>	- <i>v</i>	- <i>v</i>	<i>trash</i>
Tenant Data Steward	<input checked="" type="checkbox"/> All... <i>v</i>	- <i>v</i>	- <i>v</i>	- <i>v</i>	<input checked="" type="checkbox"/> All... <i>v</i>	<i>trash</i>
Tenant Member	<input checked="" type="checkbox"/> All... <i>v</i>	- <i>v</i>	- <i>v</i>	- <i>v</i>	- <i>v</i>	<i>trash</i>

**+ Add Role**

**Cancel** **Save**

4. Use the Manage Permissions for Stream window to:
  - (Optional) Add user roles that have permissions on the stream.
  - Edit stream permissions for each user role.
 For more information, see [Permissions management](#).
5. When you are finished editing permissions, select **Save**.

When editing permissions for multiple streams, no user roles or permission settings are pre-populated in the window because the permissions for each stream are unique. Therefore you must add each user role that you want to have permissions on the stream before editing each permission setting.

Updating streams in bulk uses a patch operation, meaning only the permissions for role entries that you edit are updated, and any previously existing permissions assigned to each role remain in place.

1. From the left pane, select **Data Management > Sequential Data Store**.
2. Select the streams that you want to manage permissions for.
3. Select **Manage Permissions**.

The Manage Permissions for Selected Streams window opens. Because you are editing permissions for multiple streams, no user roles or settings are listed, as the permission settings for each stream are different.

---

**Note:** If your user account does not have permissions to manage permissions for a selected stream, **Manage Permissions** is unavailable. Contact an administrative user to request permissions to share the stream.

#### Streams without pre-populated user roles and permissions

Manage Permissions for Selected Streams ⓘ

Operation Update

Modifying stream permissions in bulk utilizes an update operation. This means that only the permissions for role entries in the table below will be updated for each stream and the permissions for any other role will remain untouched.

+ Add Role

Role	Read ⓘ	Write ⓘ	Delete ⓘ	Manage Permissions ⓘ	Share ⓘ
------	--------	---------	----------	----------------------	---------

Click Add Role to start managing stream permissions

Cancel Save

4. Use the Manage Permissions window to:
  - Add user roles that have permissions on the stream.
  - Edit stream permissions for each user role.

For more information, see [Permissions management](#).

5. When you are finished editing permissions, select **Save**.

The edited permissions and roles are updated. This action overwrites any previous permission settings applied to the affected user roles. For more information, see Bulk stream permission management notifications.

## To manage default permissions for new streams

You can edit the default user roles and permissions added to a stream when it is created.

1. From the left pane, select **Data Management > Sequential Data Store**.
2. Select **More options :** > **Manage Default Permissions**.
3. Use the Manage Default Permissions window to edit default user roles and stream permissions. For more information, see [Permissions management](#).
4. (Optional) To update all existing data streams within the namespace with your selected default settings, select **Apply to all existing streams in the Namespace**. Only the roles and permissions that you edit are updated for all existing streams.

**Warning!** Use of this option applies updated permission settings to *all* streams in the namespace. Use this option with care, as it overwrites existing permission settings.

**Manage Default Permissions for New Streams *i***

Entries in the table are pre-populated with Roles that contain assigned permissions. To add additional Roles and assign permissions, click the Add Role button and select the Roles you want to assign permissions to. Roles not included in the table will have their permissions reset.

**+ Add Role**

Role	Read <i>i</i>	Write <i>i</i>	Delete <i>i</i>	Manage Permissions <i>i</i>	Share <i>i</i>	
Tenant Administrator	<input checked="" type="checkbox"/> All... <i>v</i>	<input checked="" type="checkbox"/> All... <i>v</i>	<input checked="" type="checkbox"/> All... <i>v</i>	<input checked="" type="checkbox"/> Allow	- <i>v</i>	<span style="color: blue;">Delete</span>
Tenant Contributor	<input checked="" type="checkbox"/> All... <i>v</i>	<input checked="" type="checkbox"/> All... <i>v</i>	- <i>v</i>	- <i>v</i>	- <i>v</i>	<span style="color: blue;">Delete</span>
Tenant Member	<input checked="" type="checkbox"/> All... <i>v</i>	- <i>v</i>	- <i>v</i>	- <i>v</i>	- <i>v</i>	<span style="color: blue;">Delete</span>

Apply to all existing streams in the namespace

**You are performing a patch operation on every stream in the Systems Engineering Namespace. The permissions in the highlighted rows in the above table will be applied to every stream in the Namespace. Entries highlighted with unset permissions will be included in the update and will clear any existing permissions for that role.**

**Cancel** **Save**

- When you are finished editing permissions, select **Save**.

## Bulk stream permission management notifications

When you update stream permissions in bulk or use the Manage Default Permissions window to update all namespace stream permissions by selecting the **Apply to all existing streams in the namespace** option, CONNECT data services runs a job to update applicable permissions. When this job completes, the completed operation is listed in your notifications . If this job fails to update any streams, the job notification links to a page that lists resource identifiers and errors for the applicable streams. Select the link to review job errors.

The screenshot shows the AVEVA CONNECT Data Services interface. On the left, a sidebar displays 'Production' status with a dropdown menu, a bell icon with a red notification count of 3, and three buttons: 'Mark All as Read' and 'Clear All'. Below this, there are three notifications:

- Aug 2, 2022, 3:53:09 PM**: Partial Failure - Failed to Update Some Stream's Permissions. The message states: 'The permissions for 1 stream were not updated. Refer to the job [page](#)'.
- Aug 2, 2022, 3:53:02 PM**: Default Stream Permissions Updated. The message states: 'Default streams permissions have been updated.'
- Aug 2, 2022, 3:52:57 PM**: Stream Update Permissions In Progress. The message states: 'The selected streams are in the process of being Permissions updated. You'll receive a notification when this is completed.'

A red arrow points from the 'page' link in the first notification to a detailed error message window on the right. The error message is titled 'Failed to update these resource permissions from namespace Production (Job ID 1f475f9f-d42b-4785-92e0-d077eeb35398)'. It contains two columns: 'Resource Id' and 'Error'. The 'Resource Id' column lists 'resource-identifier'. The 'Error' column provides details: 'Error: Insufficient permission. OperationId: 6df581552bc0e486712c8eb7aa93ee07 Parameters: Reason: 'ManageAccessControl' or 'Share' permissions are required to perform Resolution: Contact your administrator about access.'

- Select **Download Failed Jobs** to download the listed error messages in JSON format.
- Select **Copy** to copy the error message text to your clipboard.

**Note:** Stream permissions jobs are only accessible from your notifications. If you clear the notification for a job, you must re-run the job to view its result again.

## Download stream data

While viewing streams in the Sequential Data Store, you can download the streams listed on screen as a .csv file.

1. In the left pane, select **Data Management > Sequential Data Store**.
2. From the upper-left dropdown menu, ensure **Streams** is selected.
3. (Optional) Search or filter the page for the streams that you want to download in .csv format.  
Use the **Search for Streams** field to query for specific streams. For more information on querying for specific streams, see [Search queries](#).  
Use the Filter Communities pane to filter for streams from a specific community.
4. (Optional) Choose the streams that you want to include in the download.
  - To download all streams for your current search and filter settings, select no streams and continue to the next step.
  - To download specific streams listed on the page, select their checkboxes and continue to the next step.
5. Select **More options** > **Download as CSV**.

The .csv file of stream data is downloaded to your computer. The .csv will only include streams that you have searched for, filtered for, or selected.

## Types

A Sequential Data Store (SDS) type defines the shape and structure of events and how to associate events within a stream of data. A type is comprised of at least two properties. One property serves as the primary index, most commonly a timestamp or DateTime. In addition, it has one or more additional properties called value properties that describe the data in each stream event. Each value property can have a different property type. A

wide variety of property types are supported.

**Note:** You can also create complex secondary indexes.

Types are immutable; once created, they cannot be updated. Therefore, it is important to determine the correct type definition before you begin building streams and data in the Sequential Data Store.

## PI Server counterpart

An SDS type is comparable to PI point type in Data Archive. For example, a PI point of type float32 is comparable to an SDS type with a DateTime index property and a float32 value property. Because they are similar, if you use PI to CONNECT to import data into SDS, some "PI-\*" types are created automatically in SDS that map to existing PI point types. Data Archive has a predefined list of supported PI point types. The data structure of the Sequential Data Store is more flexible because SDS types can include multiple data measurements of different data types, and data can be indexed using a non-time-series index or multiple indexes.

## Types best practices

The following best practices are recommended for types and streams:

- When you create SDS types, it is important to remember that types are immutable. Once created, additional properties or information cannot be added and existing properties cannot be deleted.
- An SDS type can include multiple data measurements of different data types. Each data measurement is a property of the type.

For example, assume the SDS type, MyData.PumpState, has two measurements represented by the Temperature and Pressure properties. You would define the following fields for each property: Id, Name, Description, Type, and Key. In SDS, the key of type is also an index. At least one property in the SDS type must be an index, most commonly a timestamp. For the Temperature and Pressure measurements, the Timestamp property is the index. Each property is a value in each event of this type. Therefore, in an event of the MyData.PumpState type, there is a value for Timestamp, Temperature, and Pressure.

**Note:** You may use the REST API or client libraries to define additional optional fields, including Value, Order, and InterpolationMode for each property. Therefore, it may be preferable to create types programmatically.

- Ensure that each property is defined completely. A common error is to add a unit of measure (UOM) to the type definition after its creation, but a UOM can only be defined for the type during creation. InterpolationMode and UOM on the type are inherited by the stream; however, these fields can be overridden. If they are not defined on the type, they can be added on the stream.
- If properties are added to a type later, you must create a new type that includes all the properties of the original type, plus the new properties. Use a stream view to convert the existing streams to the new stream type and migrate the data. There are no values for the new properties for the existing streams, and null values are assigned. Before you migrate your data, consider the effect of the null values on your application and ensure that the application will not break if it encounters null values.
- For custom applications using the SDS client libraries or Open Message Format (OMF), use the client libraries to define the type rather than defining them in the portal. This ensures that the type the application expects matches the type in the Sequential Data Store. You can also take advantage of the custom property fields such as UOM when defining a property using the .NET client libraries methods.

## Property patterns

When defining value properties to add to a type in the Sequential Data Store (SDS), types fall into these common patterns:

- Inextricably linked data:
  - The data contains multiple properties that must all be present to interpret the data.
  - Examples include latitude and longitude, value and quality, and X Y and Z coordinates.
  - In this case, use a single type with all required properties.
- Independent data:
  - The data is not always captured together, rarely used together, or must be independently secured.
  - Examples include existing PI points and separate equipment or assets.
  - In this case, use separate types for each property or use a single type with one index and a generic value property.
- Data that is always captured together, but not inextricably linked:
  - All of the data is collected by the same equipment at the same time and could be used together.
  - An example is multiple measurements taken by different instruments on the same equipment.
  - In this case, use a single type if data is likely to be used together, can be secured together, does not exceed 15 properties, and the list of properties is not likely to change. Otherwise, split the data into multiple types.

## Add a type

Sequential Data Store (SDS) types define the shape and structure of events and how to associate events with streams of data. Once created, you cannot modify a type. You can add one of two types: **Standard Types** or **Enum Types**.

To add a base type:

1. In the left pane, select **Data Management > Sequential Data Store**.
2. From the **Streams** dropdown list, select **Types**.
3. Select **Add Type**.  
The Add Type pane opens.
4. Ensure **Standard Type** is selected.
5. Complete the following fields:
  - **Id** – Enter the Id for the type.
  - **Name** – (Optional) Enter a user-friendly name. If you do not enter a name, the **Id** is used as the name.
  - **Description** – (Optional) Enter a user-friendly description of the type.
  - **Type** – (Optional) To base the new type on an existing standard type, select the existing type from the dropdown. The new type inherits the properties of the base type. Inherited properties are read only and cannot be modified.
6. For each property to add to the type, select **Add Property** and complete the following fields:
  - **Key** – Select the checkbox to indicate the property is an index. Only system SDS types can be designated

as keys. You can select up to three properties as indexes. Drag and drop the properties in the list to reorder the index keys.

---

**Important:** You can only create streams from types that have an indexed defined. In other words, the type must have a key defined, or the type will not be available for selection when [Manage streams](#).

- **Id** – Enter the identifier for referencing the property.
- **Name** – Enter the name of the property. If you do not enter a name, the **Id** is used as the name.
- **Base Type** – Select the SDS type of the property from the dropdown.

---

**Note:** To find the type in the list, filter the property types by entering text in the **Filter Types** field and use the **System** or **Tenant** controls to include or exclude these types. **Tenant** includes any types that were previously created in the selected namespace for a particular tenant. **System** includes SDS types that are provided and defined such as `string`, `integer`, `double`, `datetime`, and `Boolean`.

- **UOM** – (Optional) Select a unit of measure for the property from the list.

7. To save the type, select **Save**.

You can also create enumeration types that you can include as a property in standard types.

To add an enum type:

1. In the left pane, select **Data Management > Sequential Data Store**.
2. From the **Streams** dropdown list, select **Types**.
3. Select **Add Type**.

The Add Type pane opens.

4. Select **Enum Type**.
5. In the Add Enum Type pane, complete the following fields:

- **Id** – Enter the Id for the type.
- **Name** – (Optional) Enter a user-friendly name. If you do not enter a name, the **Id** is used as the name.
- **Description** – (Optional) Enter a user-friendly description of the type.
- **Enum Type** – Select the enum type from the dropdown.

6. For each property to add to the enum type, select **Add Property** and complete the following fields:
  - **Id** – Enter the identifier for referencing the property.
  - **Value** – Enter the numeric value of the property.

---

**Note:** Accepted numeric values change based on the selected **Enum Type**. Refer to the following table for accepted values for each type.

Enum Type	Int <sup>1</sup>	-Int <sup>2</sup>	Nullable <sup>3</sup>
ByteEnum	✓	✗	✗
Int_X_Enum	✓	✓	✗
NullableByteEnum	✓	✗	✓
NullableInt_X_Enum	✓	✓	✓

Enum Type	Int <sup>1</sup>	-Int <sup>2</sup>	Nullable <sup>3</sup>
NullableSByteEnum	✓	✓	✓
NullableUInt_X_Enum	✓	✗	✓
SByteEnum	✓	✓	✗
UInt_X_Enum	✓	✗	✗

<sup>1</sup>: Integer<sup>2</sup>: Negative Integer<sup>3</sup>: Nullable fields can be left empty

- To save the type, select **Save**.

## Manage permissions for types

If you are assigned the Manage Permissions access right, then you can configure type permissions for other user roles in your tenant. You can granularly assign individual type permissions to each user role.

### Prerequisites

To manage type permissions, you must be assigned the Manage Permissions access right.

### To manage permissions for types

- From the left pane, select **Data Management > Sequential Data Store**.
- From the **Streams/Types/Stream Views** dropdown list, select **Types**.
- Select the types that you want to edit permissions for.
- Select **More options :** > **Manage Permissions**.  
The Manage Permissions for Type window opens.
- Use the Manage Permissions for Type window to:
  - (Optional) Add user roles that have permissions on the type.
  - Edit type permissions for each user role.  
For more information, see [Permissions management](#).
- When you are finished editing permissions, select **Save**.

### To manage default permissions for new types

You can edit the default user roles and permissions added to a type when it is created.

- From the left pane, select **Data Management > Sequential Data Store**.
- From the **Streams/Types/Stream Views** dropdown list, select **Types**.

3. Select **More options**  > **Manage Default Permissions**.  
The Manage Permissions for New Types window opens.
4. Use the Manage Default Permissions for New Types window to edit default user roles and type permissions.  
For more information, see [Permissions management](#).
5. When you are finished editing permissions, select **Save**.

## Stream views

A stream view is a logical overlay that enables you to customize your view of streaming data so it is most useful to you. While you cannot change the properties of types, stream views enable you to create a view of a stream so it appears as if you had changed the type. You create a stream view by choosing a source and target type, and then defining mappings between the properties of the two types. The source type is the type associated with the stream. The target type includes the properties you want to include in the stream view. In effect, you can remove, rename, or add properties without altering the original stream type.

Using a stream view on data retrieval affects only the data retrieved, and does not alter the original source data. For example, a process engineer and a maintenance technician might want to see different data that exists in the same stream. By creating a stream view, you can change the appearance of the data to meet the needs of both users, without changing the original data. In addition, you can use stream views to convert units of measure and change property names so they are more appropriate for a particular audience.

Use the CONNECT data services portal to set up stream views, or use REST APIs to define stream views programmatically. If you are using the .NET framework, client libraries are available to help create and use stream views.

## PI Server counterpart

While there is no direct counterpart for stream views in PI Server, the closest analog is the PI point data reference in PI AF. Like stream views, PI point data references allow you to give a friendly name and unit of measure on top of an existing PI point, effectively viewing it in a different way. PI point data references do not alter the underlying PI point, just as stream views do not change the source stream or type in the Sequential Data Store.

## Stream views best practices

The following best practices are recommended when working with stream views:

- Stream views can be useful when you are using PI to CONNECT. PI to CONNECT creates streams with many additional flags, for example `IsQuestionable`, `IsSubstituted`, and `IsAnnotated`. You can use stream views to limit these properties or to give them a more meaningful name.
- When you use a stream view, use caution when not all properties in the target type exist in the source type. Properties that are not mapped return their default value in the target type. For example, if the target type contains a property of data type double that is not mapped, data transformation gives that property a value of 0. Assume you have a source type with the properties, `Timestamp` and `Pressure`. You create a stream view that maps to a type with the properties `Timestamp`, `Pressure`, and `Temperature`. If `Temperature` is of data type double, a value of 0 (zero) is always returned for it, because it cannot be mapped from the source type.
- You can use a stream view to change a stream's underlying type. Use caution if you do so, because any

source properties that cannot be mapped to a target property are removed from the stream data. Unmapped target properties are set to their default value for all existing events. For example, if you have a source type that has the properties Timestamp, Pressure, and Temperature, and you use a stream view to map to a type with the properties Timestamp, Pressure, and Depth, you can map only Timestamp and Pressure. In this case, the source data for the Temperature field will be lost, and the existing events will be given a value of 0 for the new Depth property.

## Communities

Communities allow a tenant to create a private group where operational data can be shared and viewed across other tenants. Using communities, industrial companies can share their data streams externally with trusted business partners, service providers, and analytics providers.

- **Seamless Data Sharing:** Facilitate easy and secure data exchange among engineering and operational partners.
- **Enhance Operational Efficiency:** Collaboratively streamline operations and minimize waste through shared operations data.
- **Uncover Hidden Issues:** Detect and troubleshoot equipment and process problems with insights from your partners' operational data and expertise.
- **Proactive Failure Prediction:** Predict and prevent future failures by leveraging collective data intelligence.

Want to set up a community now? See [Workflow: Create a community](#).

## Community data flow

The following diagram shows the data flow of an established community.



Within this diagram, an administrative user (1) from **Tenant A** has invited **Tenant B** to form a community.

Both **Tenant A** and **Tenant B** have multiple streams stored in each of their tenants, as depicted by 2. The data from these streams are being collected from various sources: PI Servers, edge devices, and other industrial data sources (3).

Both tenants are sharing only one of their data streams within the community (**A** and **B**). A data steward with sharing privileges on the stream must explicitly share it into a community that they have read access to.

All data streams shared within the community can be viewed by any community member (**4**). Within a community, community administrators can invite and manage which users within their tenant can participate in the community and view shared data. Sharing a stream provides access to that stream across tenants. It does not copy data from one tenant to another tenant.

## Community data consumption methods

You can consume data streams shared into a community the same ways that you consume your own native tenant data. Access community data using the following CONNECT data services features:

- **Trending:** View data streams shared into a community in a trend data session, visualizing community data. For more information, see [Visualization](#).
- **Data Views:** Include data streams shared into a community within a data view, allowing you to view data within a third-party tool for data science purposes. For more information, see [Create and configure a data view](#).

## Community features and benefits

Communities allow you to easily and securely share operational data with trusted business partners.

### Connect with trusted business partners

Establish a community by creating it and then inviting your trusted business partners to join from their tenant. Each invitation is a three-way handshake. The tenant that establishes the community, known as the Administrative Tenant, sends an email invitation to an administrator from the business partner's tenant. The trusted business partner then accepts the invitation. The Administrative Tenant then confirms the invitation, allowing the trusted partner to join the community. After confirmation, users from the business partner's tenant can view data from other community tenants or share data streams from their own tenant with the community.

### Scalable

Communities allow you to share your data streams with multiple trusted business partners in a standardized way. Each community supports membership for an unlimited number of tenants, and each tenant can join an unlimited number of communities.

### Multi-tenant users and permissions

Communities support multi-tenant management of users and permissions.

Within each tenant, community administrators can independently invite or remove users, separating users and permissions from other tenants in the community. Each tenant within the community has individual control over which of its users can access the community or share data within it. Community administrators cannot control users or permissions in other tenants.

Additionally, community roles allow each tenant to manage users and roles specifically for communities. Users can be assigned granular permissions to view community data or share data streams within the community.

### Secure data sharing

Communities allow tenants to securely share operational data with their trusted business partners.

Any tenant invited to a community must accept the community invitation and be confirmed by the inviting tenant before they can share data with other tenants or view shared data from other tenants. After joining a community, each tenant must explicitly share any data stream that they want the community to view. Each

tenant shares individual data streams with the community—not their entire operational data set.

Each *tenant* in the community can stop sharing their data streams at any time. When you stop sharing a data stream, the other tenants within the community can no longer view it, nor its history. When you share data streams, you provide the community with access to your streams rather than copying data across tenants.

Because tenants can share their data natively within CONNECT data services, IT departments no longer have to:

- Manage access for external users within a corporate firewall.
- Create workarounds like VPNs or custom apps.
- Allow business partners onsite to access local operational systems.

#### Easy setup

Because communities are in the cloud, using them does not require installation of additional hardware or software.

Communities can accommodate trusted business partners who are not sharing data or do not have a PI system or another historian system of their own. With communities, business partners can sign up for their own CONNECT data services tenant to read and gain access to data shared, without having to implement an on-premises PI System or other software.

## Communities page

The Communities page, accessible at **Data Management > Communities**, is the entry point for creating and participating in communities. Depending on your user roles and permissions, this page displays a different inventory of communities and options.

### Community list

Each community that your tenant participates in is listed on the Communities page. From this page, you can review high level details for the community and view if you have access to view data streams from the community.

The following table describes each field listed for a community:

Field	Description
<b>Community Details</b>	Opens the Community details page for the community, displaying more information about the community.
<b>Tenants</b>	The number of tenants participating in the community.
<b>Sharing Status</b>	Indicates whether one or more tenant in the community is sharing data streams. Statuses include: <ul style="list-style-type: none"><li>•  <b>Sharing Active</b>: No tenants in the community have paused sharing.</li></ul>

Field	Description
	<ul style="list-style-type: none"> <li>● <b>Sharing Paused:</b> One or more tenant in the community has paused sharing their data streams. The total number of tenants that have sharing paused are also listed.</li> </ul>
<b>Member Status</b>	<p>Indicates whether you are a <a href="#">Community Member</a> and can view data shared to the community within Sequential Data Store. If the field displays a status of <b>Cannot view shared data</b>, then you are not a Community Member. If you are a Community Member, this field is omitted.</p> <p>For more information on adding a Community Member, see <a href="#">Manage users in a community</a>.</p>

Select **Community Detail** to administrate the community or view more information about it. For more information on administrative actions, see the following topics:

- [Community administration](#)
- [Community tenant administration](#)

You can also toggle between a card view and a list view.

View	Icon	Description
List view		Lists each community your tenant participates in as list items.
Card view		Lists each community your tenant participates in as cards.

## Community list sorting

While in **Card view**, you can sort the community list by using the following sorting options:

Option	Description
<b>Community Membership</b>	Sorts communities by whether you are a member or the community.
<b>Name</b>	Sorts communities alphabetically by name.
<b>Description</b>	Sorts communities alphabetically by description.
<b>Tenant Count</b>	Sorts communities numerically by the number of tenants in the community.

Option	Description
<b>Sharing Status</b>	Sorts communities alphabetically by its current sharing status: <b>Paused</b> or <b>Sharing Active</b> .

Select the **Sort**  icon to sort the communities by ascending or descending order for the applied option.

While in **List view**, you can sort the community list by clicking each column header. The list is sorted by the last column header that you click.

## Community toolbar

Use the controls available in the toolbar to find, create, or manage a community.

Control	Description
<b>Filter Communities</b>	Type criteria to find a specific community.
<b>Add community</b> <sup>1</sup>	Creates a new community. For more information on this process, see <a href="#">Workflow: Create a community</a> .
<b>View invitations</b> <sup>1</sup>	View any invitations that your tenant has pending to join a community. For more information on pending invitations, see <a href="#">View pending community invitations</a> .
<b>More options</b>  > <b>Manage Default Community Administrators</b> <sup>1</sup>	Configures which roles are automatically added as the default Community Administrators while you are creating or joining a community. For more information, see <a href="#">Manage default community administrators</a> .

<sup>1</sup>Requires [Community Administrator](#) permissions.

## Community details

When you select a community, additional details about the community open in a side pane. The following table lists each field that displays in the side pane:

Field	Description
<b>Id</b>	The identifier for the community.
<b>Name</b>	The name of the community.
<b>Date created</b>	The date that the community was created.
<b>Description</b>	The description of the community.
<b>Sharing Status</b>	Indicates whether one or more tenant in the community is sharing data streams. Statuses include:

Field	Description
	<ul style="list-style-type: none"> <li>● <b>Sharing Active:</b> No tenants in the community have paused sharing.</li> <li>● <b>Sharing Paused:</b> One or more tenant in the community has paused sharing their data streams. The total number of tenants that have sharing paused are also listed.</li> </ul>
<b>Total Streams Shared</b>	<p>The number of streams shared into the community. If the field displays an <b>Information</b>  icon, then you are not a Community Member. For more information on adding a Community Member, see <a href="#">Manage users in a community</a>.</p> <hr/> <p><b>Tip:</b> Select the <b>Launch</b>  icon to view shared streams for the community in SDS Explorer.</p>

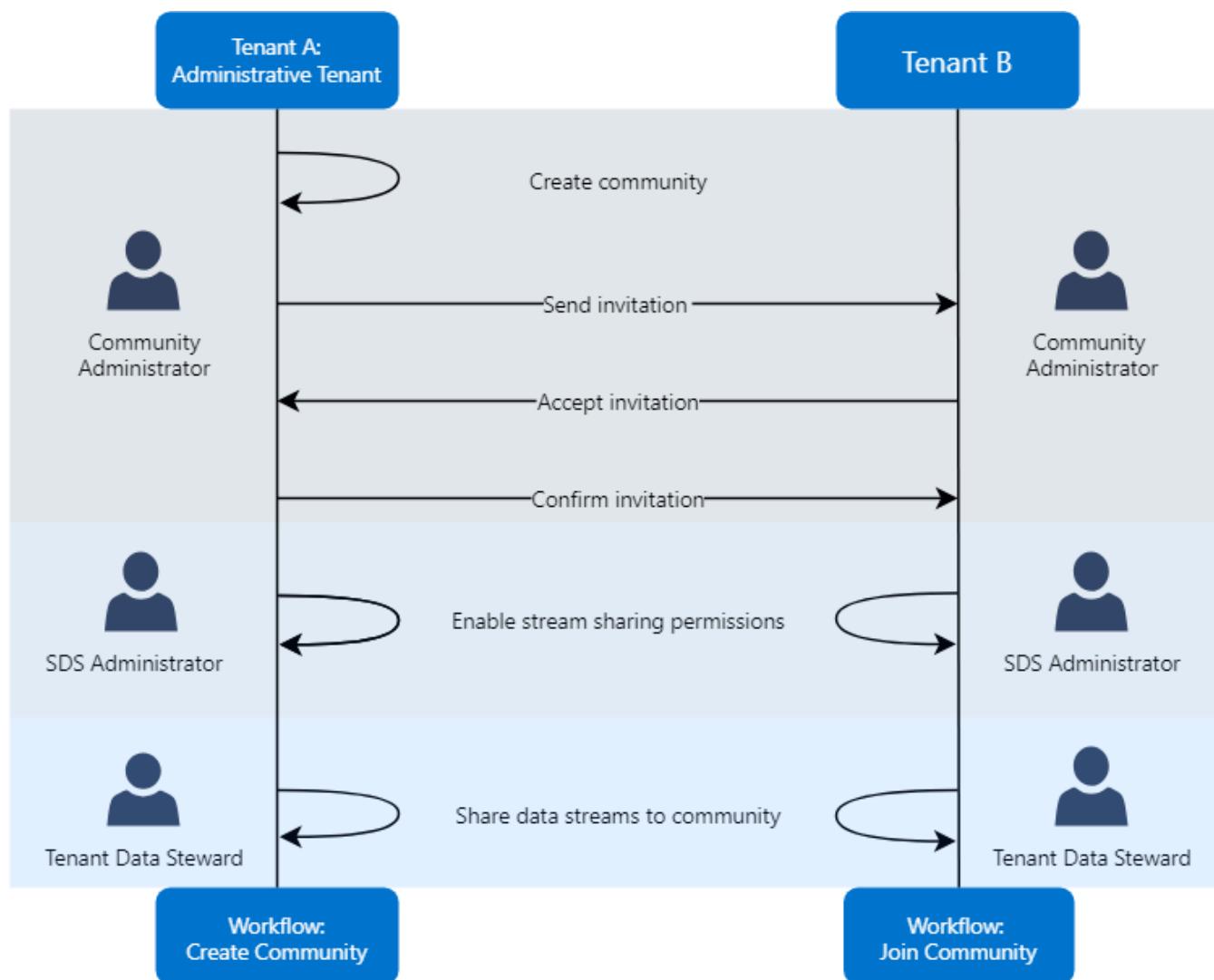
This pane also lists each tenant that holds membership in the community, along with its sharing status and contact email. Select a contact email to email the recipient. The tenant denoted with the **Crown**  icon is the **Administrative Tenant** for the community.

## Community setup

Establish a community by creating it and then inviting your trusted business partners to join from their tenant. Each invitation is a three-way handshake where one tenant sends an invitation, the invited tenant accepts, and then the original tenant confirms that the expected tenant accepted.

### Workflow: Community setup

Setup of a community involves coordination between two tenants and users with different user roles and permissions. Before you start setup of a community, review the figure below to better understand the entire community setup process.



This diagram lists each task that must be completed to form an operational community, broken down by each user role that performs them. Each of these tasks are documented in the upcoming sections:

- [Workflow: Create a community](#)
- [Workflow: Join a community](#)
- [Share streams](#)

## Community user roles

To allow different tenants and users participating in a community to safely and securely share data streams with one another, CONNECT data services includes several default user roles specifically for communities. These roles include granular permissions to allow different tenants and users to share specific data streams while keeping the remaining, unshared data streams private. When using Communities, you must assign the appropriate community roles to users that administrate or participate in the community. During community setup, you will need to assign different users with these roles.

- **Community Administrators**

Community administrator permissions are required to perform administrative actions for the community within the scope of the tenant, such as community membership management. When a tenant creates or joins a new community, they are prompted to assign new community administration permissions to one or more existing roles. All users from your tenant that are assigned these roles inherit administrative permissions within the community. By default, the Community Administrators and Tenant Administrator roles have these permissions.

- **SDS Administrator**

Communities require a user with privileges to allow other users to share streams within Sequential Data Store (SDS) explorer, such as the Tenant Administrator. Although the SDS Administrative user is not technically a community role, they are important during community setup because they grant different data stewards permissions to share streams into a community. Communities require a role with **manage permissions** access within SDS explorer to share streams. By default, the Tenant Administrator is an SDS administrative user and can manage stream permissions for other roles.

- **Tenant Data Stewards**

Users that have permissions to share a data stream into a community are known as *Tenant Data Stewards*. Share permissions are required to share a stream into a community. Additionally, the user must be a Community Member. AVEVA recommends that you assign share permissions to the Tenant Data Steward role, but you can use any role that you want.

- **Community Member**

The Community Member role is a role that can be shared among multiple tenants participating in a community. This role is authorized to read any data shared in the community. Users assigned the Community Member role have read permissions within the community by default.

By default, the Tenant Data Steward role has the Share permissions on all new streams. If you want to have different data steward roles for different sets of streams, it is recommended that you do not place any users in the Tenant Data Steward role and create additional data steward roles that are given Share privileges for different groupings of streams—for example, Site A Data Steward and Site B Data Steward. You can configure default permissions by [managing default permissions for new streams](#).

- **Administrative Tenant**

Each community has an administrative tenant, which is the tenant that administers the community itself. When you create a new community, your tenant is automatically configured as the administrative tenant. Users assigned community administrator permissions on the administrative tenant have additional permissions for managing the community itself that affect all tenants within it.

## Next steps

Depending on whether you are creating or joining a community, proceed to one of the following topics:

- To create a community, see [Workflow: Create a community](#).
- To join a community, see [Workflow: Join a community](#).

## Understand community roles

To allow different tenants and users participating in a community to safely and securely share data streams with one another, CONNECT data services includes several user roles specifically for communities. These roles include granular permissions to allow different tenants and users to share specific data streams while keeping the

remaining, unshared data streams private. When using Communities, you must assign the appropriate community roles to users that administrate or participate in the community.

Communities include the following roles, ordered from least privileged to most privileged.

## Community Member

The Community Member is a role that is shared among multiple tenants participating in a community. This role is authorized to read any data shared in the community.

When a new community is created, a new Community Member role is automatically added to the system, which is named using the following convention: <Community Name> Community Member. For example, if you create a new community named Test, a new community role is added to the tenant named Test Community Member.

This new role is also shared with other tenants that join the community. For example, a tenant that joins Test will have the Test Community Member role added to their tenant as well.

Users assigned the Community Member role have read permissions within the community by default. However, to allow community members to share data streams within a community, you must assign the Share permission for streams to their assigned tenant roles.

- For more information on assigning the Community Member role to users (or unassigning it), see [Manage users in a community](#).
- For more information on the actions Community Members can perform, see [Community data sharing and viewing](#).

## Community Administrators

Community administrator permissions are required to perform administrative actions for the community within the scope of the tenant, such as community membership management.

When a tenant creates or joins a new community, they are prompted to assign new community administration permissions to one or more existing roles. All users from your tenant that are assigned these roles inherit administrative permissions within the community.

- For more information on assigning community administrator permissions to an existing user role, see [Manage community administrators](#).
- For more information on the actions that Community Administrators can perform, see [Community tenant administration](#).

## Administrative Tenant

Each community has an administrative tenant, which is the tenant that administers the community itself. When you create a new community, your tenant is automatically configured as the administrative tenant. Users assigned community administrator permissions on the administrative tenant have additional permissions for managing the community itself that affect all tenants within it.

In addition to the tasks listed in [Community tenant administration](#), Community Administrators for the Administrative Tenant can also perform the tasks listed in [Community administration](#).

## Workflow: Create a community

To begin the process of sharing data, create a new community and invite other tenants to join.

---

**Tip:** Looking for instructions on how to join a community? See [Workflow: Join a community](#).

---

### Prerequisites

To create a new community, you must:

- Be assigned [community administration permissions](#).
- Have the email address for a user that is assigned community administration permissions from the tenant that you are inviting to the community.

### Create community outline

Complete the following procedures to start a new community and invite other tenants.

- [Create a community](#)

The first part of establishing a community is to create it. When you create a community, you are prompted to define a community name and description, the user roles that have administrative permissions within the community for your tenant, and the users and groups considered Community Members within your tenant.

- [Invite a tenant to a community](#)

This procedure provides instruction on how to invite other tenants to join your community. After sending an invitation, wait for the invited tenant to accept it. Once the invited tenant accepts, you can confirm the tenant's participation.

- [Enable stream sharing permissions](#)

Manage permissions for data streams to allow Community Members from your tenant to share streams with the community.

### Create a community

The first part of establishing a community is to create it. When you create a community, you are prompted to define a community name and description, the user roles that have administrative permissions within the community for your tenant, and the users and groups considered Community Members within your tenant.

### Prerequisites

You must be assigned a user role with [community administration permissions](#) on the administrative tenant.

### To create a community

To create a community:

1. In the left pane, select **Data Management > Communities**.

2. Select **+ Add Community** in the upper right hand corner.

The Create Community wizard opens to the Details page.

3. On the Details page, enter the following information and select **Next**:

Detail	Description
<b>Name</b>	The name of the community.
<b>Description (optional)</b>	A description of the community.
<b>Contact Email</b>	An email address that your business partners can use to contact you for any questions or issues related to this community. This field defaults to the email address for your user account, but you can override it by selecting  and entering a new address.

**Tip:** You can update your **Contact Email** later. For more information, see [Configure contact email](#).

4. On the Community Administrators page, choose the **CONNECT data services roles** that are assigned **community administration permissions**. Users assigned these roles can perform administration tasks for both their own tenant and the entire community. You can either accept the default roles or add new ones.

- To add community administrator permissions to a user role, select the **Add Roles** dropdown menu and then select **Add Role**  for any role that you want to function as community administrator.
- To remove community administrator permissions from a user role, select **Remove Role**  for the role that you want to remove.

**Tip:** You can edit the default roles that are listed. For more information, see [Manage default community administrators](#).

5. After you finish, select **Next**.

6. On the Community Members page, add **Community Members**, which are users within your tenant that have read access to the community and its data.

To add new Community Members, select **Add Members**  and search for each user or group that you want to add.

**Note:** Community Administrators are not automatically added as Community Members. If you want your Community Administrators to also be Community Members with access to shared resources, you must manually add them.

7. After you finish, select **Create**.

The community is created and added to the Communities page.

## Next steps

Invite tenants to your community. Continue to [Invite a tenant to a community](#).

### Invite a tenant to a community

Before another tenant can join your community, you must send them an invitation, they must accept it, and then

you must confirm it. In other words, you must complete a three-step handshake that requires collaboration with another tenant.

Complete the following procedures in order.

## Prerequisites

- You must be assigned a user role with [community administration permissions](#).
- You must have the email address for a user assigned community administration permissions from the tenant that you are inviting to the community.

## Step 1: Invite a tenant to the community

To invite another tenant to the community:

1. In the left pane, select **Data Management > Communities**.
2. Select the community you want to invite another tenant to and choose **Community Details**.
3. On the **Tenants** tab, select **Invite Tenant**.
4. Enter the email address for a community administrator from the invited tenant. Then select **Invite**.

An email is sent to the community administrator.

## Step 2: Wait for invited tenant to accept invitation

After you invite another tenant, wait for its community administrator to accept the email invitation. To monitor whether the invitation is accepted, select the **Invitations** tab and view the invitation recipient for a status of **Invitation Accepted**. You may need to refresh the page to see an updated status.

Invitations are valid for 14 days before they expire. If the invitation is not accepted within that time, you must [resend the invitation](#). You must also resend the invitation if the invited tenant does not receive the initial email.

## Step 3: Confirm the invitation

To confirm an invitation:

1. In the left pane, select **Data Management > Communities**.
2. On the Communities overview page, select the community that you have invited another tenant to and choose **Community Details**.
3. On the Community Details page, select the **Invitations** tab.
4. Select an invitation with a status of **Pending Confirmation**.
5. On the Invitation Details pane, select **Confirm Tenant**.

---

**Important!** When prompted for confirmation, review that the expected tenant is joining before you select **Confirm Tenant**.

---

The invitee's tenant is now part of the community.

## Next steps

Edit permissions for data streams to allow tenant data stewards to share them with the community. Continue to [Enable stream sharing permissions](#).

### Enable stream sharing permissions

Before data can be shared into a community and accessed by external tenants, a user with the **Share** permission on one or more streams in the Sequential Data Store must share the streams into a community that they have read access to. By default, the [CONNECT data services roles](#) role is intended for users in the tenant to share resources with other external tenants using communities. However, the Tenant Data Steward role is not assigned the **Share** permission on streams by default. Therefore, an administrative user assigned **Manage Permissions** on the streams must first grant the Tenant Data Steward role the **Share** permission on streams before they can be shared by users within that role. Granting **Share** permissions to the Tenant Data Steward role is recommended, but you can give those permissions to other roles instead.

### Prerequisites

Your user role must be assigned the **Share** permissions for applicable data streams. If you do not have these permissions, request them from a user that can manage Sequential Data Store permissions (such as a [CONNECT data services roles](#)).

### To enable stream sharing permissions

When enabling stream sharing permissions, you can either enable them for an entire namespace or on specific streams, stream-by-stream basis. Enabling streams for an entire namespace is more convenient; enabling specific streams is more secure.

You can change permissions for all streams in a namespace with a single action.

1. From the left pane, select **Data Management > Sequential Data Store**.
2. From the **Namespace** dropdown list, select the namespace that includes the streams that you want to share.
3. Select **More options**  **> Manage Default Permissions**.  
The Manage Default Permissions for New Streams window opens.
4. Allow **Share** permissions for the user roles that you want to be able to share data.
  - a. Update each applicable **Share** permission dropdown list to **Allow**. If necessary, select **Add Role** to add a new role.
  - b. Select **Apply to all existing streams in the namespace**.

**Manage Default Permissions for New Streams**

Entries in the table are pre-populated with Roles that contain assigned permissions. To add additional Roles and assign permissions, click the Add Role button and select the Roles you want to assign permissions to. Roles not included in the table will have their permissions reset.

Role	Read <i>i</i>	Write <i>i</i>	Delete <i>i</i>	Manage Permissions <i>i</i>	Share <i>i</i>	
Tenant Administrator	✓ All... ▾	✓ All... ▾	✓ All... ▾	✓ Allow ▾	✓ All... ▾	
Tenant Contributor	✓ All... ▾	✓ All... ▾	- ▾	- ▾	- ▾	
Tenant Member	✓ All... ▾	- ▾	- ▾	- ▾	- ▾	
Tenant Data Steward	✓ All... ▾	- ▾	- ▾	- ▾	✓ All... ▾	

**2**  Apply to all existing streams in the AVEVA World namespace

You are performing a patch operation on every stream in the AVEVA World Namespace. The permissions in the highlighted rows in the above table will be applied to every stream in the Namespace. Entries highlighted with unset permissions will be included in the update and will clear any existing permissions for that role.

**1**

**Note:** For more information on this window, see [Permissions management](#).

5. Select **Save**.

To apply sharing permission to specific streams in a namespace:

1. From the left pane, select **Data Management > Sequential Data Store**.
2. Select one or more streams that you want to allow sharing on.
3. From the right pane, select **Manage Permissions**.

**Note:** If you only have one stream selected, select **More options :** > **Manage Permissions** instead.

The Manage Permissions for Streams window opens.

4. For user roles that you want to have the ability to share data, update each **Share** permission dropdown list to **Allow**.

**Manage Permissions for Selected Streams i**

**Operation Update**  
Modifying stream permissions in bulk utilizes an update operation. This means that only the permissions for role entries in the table below will be updated for each stream and the permissions for any other role will remain untouched.

**Add Role**

Role	Read <span style="color: #0070C0;">i</span>	Write <span style="color: #0070C0;">i</span>	Delete <span style="color: #0070C0;">i</span>	Manage Permissions <span style="color: #0070C0;">i</span>	Share <span style="color: #0070C0;">i</span>
Tenant Administrator	<input checked="" type="checkbox"/> All... <span style="font-size: small;">▼</span>	<input checked="" type="checkbox"/> All... <span style="font-size: small;">▼</span>	<input checked="" type="checkbox"/> All... <span style="font-size: small;">▼</span>	<input checked="" type="checkbox"/> Allow <span style="font-size: small;">▼</span>	<input type="checkbox"/> - <span style="font-size: small;">▼</span> <span style="float: right;"><span style="color: #0070C0;">i</span></span>
Tenant Community Adm...	<input checked="" type="checkbox"/> All... <span style="font-size: small;">▼</span>	- <span style="font-size: small;">▼</span>	- <span style="font-size: small;">▼</span>	- <span style="font-size: small;">▼</span>	- <span style="font-size: small;">▼</span> <span style="float: right;"><span style="color: #0070C0;">i</span></span>
Tenant Data Steward	<input checked="" type="checkbox"/> All... <span style="font-size: small;">▼</span>	- <span style="font-size: small;">▼</span>	- <span style="font-size: small;">▼</span>	- <span style="font-size: small;">▼</span>	<input checked="" type="checkbox"/> All... <span style="font-size: small;">▼</span> <span style="float: right;"><span style="color: #0070C0;">i</span></span>

**Cancel** **Save**

**Tips:** For more information on this window, see [Permissions management](#).

5. Select **Save**.

## Managing multiple streams with multiple roles

To configure different roles to allow different data stewards to share different sets of data, do not use the default Tenant Data Steward role and instead create the number of roles needed to manage this within your organization. Then repeat the steps above to grant the share permission for those roles on the specific sets of streams/data that each role will manage.

## Next steps

Communicate to your tenant data stewards that your tenant's data streams are available to share into a community. For more information about sharing streams, see [Share streams](#).

## Workflow: Join a community

To join a community, accept the invitation sent by the owning tenant and set stream sharing permissions.

## Prerequisites

You must be assigned a user role with [community administration permissions](#).

## Join community outline

Complete the following procedures to join a community after receiving an invitation.

- [Accept community invitation](#)

This procedure provides instruction on how to accept an invitation to join a community. After you accept the invitation, choose which roles can administer it, and choose which users and groups from your tenant become Community Members.

- [Enable stream sharing permissions](#)

Manage permissions for data streams to allow Community Members from your tenant to share streams with the community.

## Accept community invitation

When another tenant invites you to a community, you receive an email invitation that you can use to join.

---

**Note:** Invitations are valid for 14 days before they expire. If you do not accept the invitation within that time, or you do not receive an invitation email, you must request a new invitation from the administrative tenant.

---

## Prerequisites

You must be assigned a user role with [community administrator permissions](#).

### To accept an invitation:

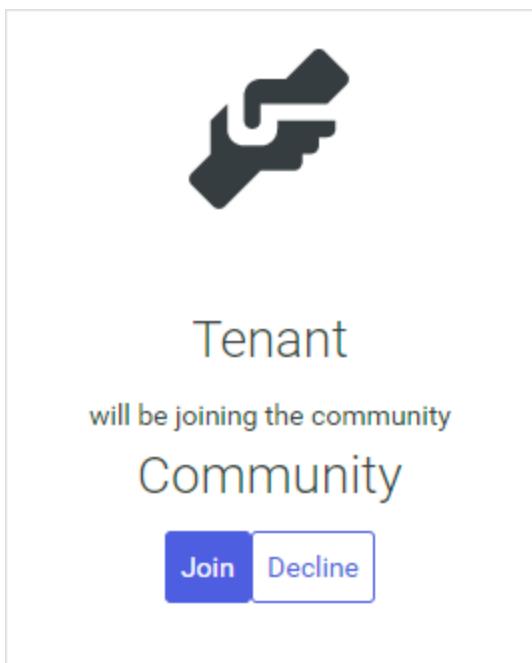
1. Open and review the email invitation from CONNECT data services.
2. Select the **VIEW COMMUNITY INVITE** link.
3. If prompted, enter the tenant ID or tenant alias for your tenant and select **Continue**.

---

**Important!** If you have multiple tenants, verify that you are logging into the correct tenant.

---

4. If prompted, log in to CONNECT data services.  
A page opens and displays that your tenant will join the community that issued the invitation.
5. Select **Join**.



The tenant that invited you to the community is updated that you accepted their invitation.

6. Wait for a Community Administrator from the inviting tenant to confirm your tenant. Your tenant does not officially join the community until the inviting tenant confirms the invitation.

When the administrative tenant confirms your tenant, you receive a notification email.

**Tip:** You can view or cancel your invitations that are pending confirmation from the Communities page. For more information, see [View pending community invitations](#).

7. After your tenant is confirmed for the community, select **Data Management > Communities**, choose your community, and then choose **Community Details** to set up Community Administrators and Community Members for your tenant.

A setup wizard opens.

8. From the **Welcome** page, verify the **Contact Email** address and then select **Next**.

The **Contact Email** is an email address that your business partners can use to contact you for any questions or issues related to this community. This field defaults to the email address for your user account, but you can override it by selecting **X** and entering a new address.

**Tip:** You can update your **Contact Email** later. For more information, see [Configure contact email](#).

9. On the Community Administrators page, choose the **CONNECT data services roles** that are assigned **community administration permissions**. Users assigned these roles can perform administration tasks within their own tenant, but not the entire community. You can either accept the default roles or add new ones.

- To add community administrator permissions to a user role, select **Add Roles > Add Role**  for any role that you want to function as community administrator.
- To remove community administrator permissions from a user role, select **Remove Role**  for the role that you want to remove.

**Tip:** You can edit the default roles that are listed. For more information, see [Manage default community administrators](#).

10. After you finish, select **Next**.
11. On the Community Members page, add **Community Members**, which are members within your tenant that have read access to the community and its data.

To add new Community Members, select **Add Members > Add User**  for each user or group that you want to add.

**Note:** Community Administrators are not automatically added as Community Members. If you want your Community Administrators to also be Community Members with access to shared resources, you must manually add them.

12. After you finish, select **Save & Close**.

## Next steps

Edit permissions for data streams to allow tenant data stewards to share them with the community. Continue to [Enable stream sharing permissions](#).

### Enable stream sharing permissions

Before data can be shared into a community and accessed by external tenants, a user with the **Share** permission on one or more streams in the Sequential Data Store must share the streams into a community that they have read access to. By default, the [CONNECT data services roles](#) role is intended for users in the tenant to share resources with other external tenants using communities. However, the Tenant Data Steward role is not assigned the **Share** permission on streams by default. Therefore, an administrative user assigned **Manage Permissions** on the streams must first grant the Tenant Data Steward role the **Share** permission on streams before they can be shared by users within that role. Granting **Share** permissions to the Tenant Data Steward role is recommended, but you can give those permissions to other roles instead.

### Prerequisites

Your user role must be assigned the **Share** permissions for applicable data streams. If you do not have these permissions, request them from a user that can manage Sequential Data Store permissions (such as a [CONNECT data services roles](#)).

### To enable stream sharing permissions

When enabling stream sharing permissions, you can either enable them for an entire namespace or on specific streams, stream-by-stream basis. Enabling streams for an entire namespace is more convenient; enabling specific streams is more secure.

You can change permissions for all streams in a namespace with a single action.

1. From the left pane, select **Data Management > Sequential Data Store**.
2. From the **Namespace** dropdown list, select the namespace that includes the streams that you want to share.
3. Select **More options :** > **Manage Default Permissions**.  
The Manage Default Permissions for New Streams window opens.
4. Allow **Share** permissions for the user roles that you want to be able to share data.
  - a. Update each applicable **Share** permission dropdown list to **Allow**. If necessary, select **Add Role** to add a new role.
  - b. Select **Apply to all existing streams in the namespace**.

**Manage Default Permissions for New Streams**

Entries in the table are pre-populated with Roles that contain assigned permissions. To add additional Roles and assign permissions, click the Add Role button and select the Roles you want to assign permissions to. Roles not included in the table will have their permissions reset.

Role	Read	Write	Delete	Manage Permissions	Share
Tenant Administrator	All... <input checked="" type="button"/>	All... <input checked="" type="button"/>	All... <input checked="" type="button"/>	Allow <input checked="" type="button"/>	All... <input checked="" type="button"/> <span style="color: blue;">(1)</span>
Tenant Contributor	All... <input checked="" type="button"/>	All... <input checked="" type="button"/>	- <input type="button"/>	- <input type="button"/>	- <input type="button"/>
Tenant Member	All... <input checked="" type="button"/>	- <input type="button"/>	- <input type="button"/>	- <input type="button"/>	- <input type="button"/>
Tenant Data Steward	All... <input checked="" type="button"/>	- <input type="button"/>	- <input type="button"/>	- <input type="button"/>	All... <input checked="" type="button"/> <span style="color: blue;">(1)</span>

**2**  Apply to all existing streams in the AVEVA World namespace

You are performing a patch operation on every stream in the AVEVA World Namespace. The permissions in the highlighted rows in the above table will be applied to every stream in the Namespace. Entries highlighted with unset permissions will be included in the update and will clear any existing permissions for that role.

**Cancel** **Save**

**Note:** For more information on this window, see [Permissions management](#).

5. Select **Save**.

To apply sharing permission to specific streams in a namespace:

1. From the left pane, select **Data Management > Sequential Data Store**.
2. Select one or more streams that you want to allow sharing on.
3. From the right pane, select **Manage Permissions**.

**Note:** If you only have one stream selected, select **More options :** > **Manage Permissions** instead.

The Manage Permissions for Streams window opens.

4. For user roles that you want to have the ability to share data, update each **Share** permission dropdown list to **Allow**.

**Manage Permissions for Selected Streams i**

**Operation Update**  
Modifying stream permissions in bulk utilizes an update operation. This means that only the permissions for role entries in the table below will be updated for each stream and the permissions for any other role will remain untouched.

**Add Role**

Role	Read <span style="color: #0070C0;">i</span>	Write <span style="color: #0070C0;">i</span>	Delete <span style="color: #0070C0;">i</span>	Manage Permissions <span style="color: #0070C0;">i</span>	Share <span style="color: #0070C0;">i</span>
Tenant Administrator	<input checked="" type="checkbox"/> All... <span style="color: #0070C0;">i</span>	<input checked="" type="checkbox"/> All... <span style="color: #0070C0;">i</span>	<input checked="" type="checkbox"/> All... <span style="color: #0070C0;">i</span>	<input checked="" type="checkbox"/> Allow	<input type="checkbox"/> - <span style="color: #0070C0;">i</span>
Tenant Community Adm...	<input checked="" type="checkbox"/> All... <span style="color: #0070C0;">i</span>	<input type="checkbox"/> - <span style="color: #0070C0;">i</span>	<input type="checkbox"/> - <span style="color: #0070C0;">i</span>	<input type="checkbox"/> - <span style="color: #0070C0;">i</span>	<input type="checkbox"/> - <span style="color: #0070C0;">i</span>
Tenant Data Steward	<input checked="" type="checkbox"/> All... <span style="color: #0070C0;">i</span>	<input type="checkbox"/> - <span style="color: #0070C0;">i</span>	<input type="checkbox"/> - <span style="color: #0070C0;">i</span>	<input type="checkbox"/> - <span style="color: #0070C0;">i</span>	<input checked="" type="checkbox"/> All... <span style="color: #0070C0;">i</span>

**Cancel** **Save**

**Tips:** For more information on this window, see [Permissions management](#).

5. Select **Save**.

## Managing multiple streams with multiple roles

To configure different roles to allow different data stewards to share different sets of data, do not use the default Tenant Data Steward role and instead create the number of roles needed to manage this within your organization. Then repeat the steps above to grant the share permission for those roles on the specific sets of streams/data that each role will manage.

## Next steps

Communicate to your tenant data stewards that your tenant's data streams are available to share into a community. For more information about sharing streams, see [Manage shared streams](#).

## Community administration

Although each tenant manages its own users and streams within a community, there are some administration tasks that can only be performed by community administrators on the administrative tenant, which is the tenant that established the community. These community administrative tasks affect the entire community rather than a single tenant.

## Prerequisites

You must be assigned a user role with [community administration permissions](#) on the [administrative tenant](#).

## Community tenant administration tasks

The following tasks can only be performed by community administrators on the administrative tenant.

**Note:** Community administrators on the administrative tenant can perform all tasks listed in [Community tenant administration](#) in addition to the tasks listed below.

- [Invite a tenant](#)

Invite other tenants to join the community.

- [Resend email invitation](#)

If you invite a tenant to the community but they do not receive an invitation email, you can resend it.

- [Remove a tenant from a community](#)

Remove tenants from a community.

- [Edit a community](#)

Edit the community name, description, contact email, and alias.

- [Delete a community](#)

Delete the community.

- [Manage preferred region](#)

Each community includes settings to manage the preferred region, which controls the geographical regions where operational data shared within a community is processed.

## Invite a tenant

After creating a new community, you can invite other CONNECT data services tenants to participate in the community.

### Prerequisites

- You must be assigned a user role with [community administration permissions](#).
- You must have the email address for a user assigned community administration permissions from the tenant that you are inviting to the community.

### Step 1: Invite a tenant to the community

To invite another tenant to the community:

1. In the left pane, select **Data Management > Communities**.
2. Select the community you want to invite another tenant to and choose **Community Details**.
3. On the **Tenants** tab, select **Invite Tenant**.
4. Enter the email address for a community administrator from the invited tenant. Then select **Invite**.  
An email is sent to the community administrator.

## Step 2: Wait for invited tenant to accept invitation

After you invite another tenant, wait for its community administrator to accept the email invitation. To monitor whether the invitation is accepted, select the **Invitations** tab and view the invitation recipient for a status of **Invitation Accepted**. You may need to refresh the page to see an updated status.

Invitations are valid for 14 days before they expire. If the invitation is not accepted within that time, you must [resend the invitation](#). You must also resend the invitation if the invited tenant does not receive the initial email.

## Step 3: Confirm the invitation

To confirm an invitation:

1. In the left pane, select **Data Management > Communities**.
2. On the Communities overview page, select the community that you have invited another tenant to and choose **Community Details**.
3. On the Community Details page, select the **Invitations** tab.
4. Select an invitation with a status of **Pending Confirmation**.
5. On the Invitation Details pane, select **Confirm Tenant**.

---

**Important!** When prompted for confirmation, review that the expected tenant is joining before you select **Confirm Tenant**.

---

The invitee's tenant is now part of the community.

## Resend an email invitation

If you invite another tenant to the community but it does not receive the invitation email, you can resend it.

---

**Note:** Invitations are valid for 14 days before they expire. If the invitation is not accepted within that time, you must resend the invitation.

---

## Prerequisites

You must be assigned a user role with [community administration permissions](#) on the [administrative tenant](#).

## To resend an invitation

To resend an invitation:

1. In the left pane, select **Data Management > Communities**.
2. On the Communities overview page, select the applicable community and choose **Community Details**.
3. On the Community Details page, select the **Invitations** tab.
4. Find the **Invitation Recipient** who has not received the email invitation with a **Status** of **Invitation Pending**. Select the recipient, and then select **Resend Invitation**.

## Remove a tenant from a community

Use this procedure to remove a tenant from a community. This action might be necessary if a business relationship changes or if the tenant's organization experiences a security breach.

### Prerequisites

You must be assigned a user role with [community administration permissions](#) on the [administrative tenant](#).

### To remove a tenant from a community

To remove a tenant from a community:

1. In the left pane, select **Data Management > Communities**.
2. Select the community you want to modify and choose **Community Details**.
3. On the Community Details page, select the **Tenants** tab.
4. Select the tenant you want to remove from the community.
5. On the Tenant Details pane, select **Remove Tenant**. When prompted for confirmation, select **Remove Tenant** again.

### What happens to shared data when you leave a community?

When your tenant is removed from a community, it stops sharing all data streams that were previously shared within that community. All tenants that remain in the community can no longer access your data, and you can no longer access theirs.

## Edit a community

After you create a community, you can edit its name and description at any time. You can also edit your contact email or add a community alias.

### Prerequisites

You must be assigned a user role with [community administration permissions](#) on the [administrative tenant](#).

### To edit a community

1. In the left pane, select **Data Management > Communities**.
2. Select the community you want to edit and choose **Community Details**.
3. Select **More Options**  > **Edit Community**.
4. In **Edit Community**, edit the community **Name** and **Description**.
5. (Optional) Edit the community **Alias**.

Use this field to provide an alias for the community. This alias replaces the community name in all places the

name is referenced within CONNECT data services. The alias applies to your tenant only; other tenants in the community do not see it.

---

**Note:** If you use an alias, the only location that you can see both the community name and the alias is the Community Detail page.

6. (Optional) Edit the community **Contact Email**.

Use this field to provide a contact email address that your business partners can use to communicate with your organization for any questions or issues related to the community.

7. Select **Update**.

## Delete a community

Deleting a community removes all access to all data in the community from all tenants. Deleting a community also removes all users from the community. After you delete a community, no users can access it again.

### Prerequisites

You must be assigned a user role with [community administration permissions](#) on the [administrative tenant](#).

### To delete a community

To delete a community:

1. In the left pane, select **Data Management > Communities**.
2. On the Communities page, select the community you want to delete and choose **Community Details**.
3. On the Community Details page at the top-right, select **More Options**  > **Delete Community**.
4. Confirm the deletion by entering the name of the community to delete and select **Delete**.

## Manage preferred region

Each community includes settings to manage the preferred region, which controls the geographical regions where operational data shared within a community is processed. By default, operational data is primarily processed in the West-US region for most requests, but data can be processed in other regions as well. Using the preferred region settings, you can override the default region to explicitly choose where operational data is processed.

### Why would I want to manage my preferred region?

For more information, see [Cross-region data sharing](#).

### Prerequisites

- To manage the **Community Preferred Region** setting, you must be assigned a user role with [community administration permissions](#) on the [administrative tenant](#).

- To manage the **My Preferred Region** setting, you must be assigned a user role with [community administration permissions](#). Being a user of the administrative tenant is not required.

## Manage preferred region settings

Edit the **Community preferred region** or **My preferred region** from a community's details.

1. In the left pane, select **Data Management > Communities**.
2. Select the community you want to edit and choose **Community Details**.
3. Select **More Options :** > **Manage Preferred Region**.
4. Edit the preferred region settings and select **Update**.

- **Community Preferred Region**

This setting is used to optimize access to community shared data. It ensures that queries are sent to the appropriate region if a tenant in the community opts-out of cross-region data sharing, which prohibits processing of data outside of the primary region where it resides. If no value is set, then **Community Preferred Region** setting defaults to the West-US region. Select the region where you expect most of the data in this community to reside.

- **My Preferred Region**

This setting overrides the **Community Preferred Region** for your tenant and allows you to control which region your tenant's queries to this community are sent to.

## Community tenant administration

After a community is established, users assigned a community administrator role can manage their community. Each community administrator can only perform administrative actions within their own tenant. They cannot manage other tenants within the community.

### Prerequisites

You must be assigned a user role with [community administration permissions](#).

### Community tenant administration tasks

Users assigned a community administrator role can perform the following tasks:

- [View pending community invitations](#)

You can view the status of all pending community invitations that your tenant has accepted, but have not yet been confirmed by the issuing tenant.

- [Remove your own tenant from a community](#)

Remove your own tenant from the community.

- [Pause sharing a community](#)

Pause or resume sharing all data streams that your tenant shares with a community.

- [Manage users in a community](#)

Add or remove users within your tenant as Community Members.

- [Manage groups in a community](#)

Add or remove groups within your tenant as Community Members.

- [Manage clients in a community](#)

Add or remove programmatic access for an application to shared community data and resources using REST API.

- [Configure contact email](#)

After your tenant provides an initial contact email during the invitation process, you can later update the contact email for the tenant if it changes.

- [Manage community administrators](#)

Add or remove roles that have community administration permissions within your tenant.

- [Manage default community administrators](#)

Update the default system roles added as community administrators when you create or join a community.

## View pending community invitations

You can view the status of all pending community invitations that your tenant has accepted, but have not yet been confirmed by the issuing tenant. You can also cancel any pending invitations in which you no longer want to join the community.

### Prerequisites

You must be assigned a user role with [community administration permissions](#).

### To view pending community invitations

1. In the left pane, select **Data Management > Communities**.
2. From the toolbar, select **View invitations**.
3. (Optional) If you want to cancel a pending request, select the communities that you no longer want to join and select **Cancel Invitations**.

## Remove your own tenant from a community

Use this procedure to remove your own tenant from a community. After removing your tenant, you can be re-invited to the community, but all data that your tenant previously shared must be shared again.

### Prerequisites

You must be assigned a user role with [community administration permissions](#).

### To remove your own tenant from a community

To remove your tenant from a community:

1. In the left pane, select **Data Management > Communities**.
2. Select the community you want to leave and choose **Community Details**.
3. On the Community Details page, select the **Tenants** tab.
4. Select **More Options :** > **Remove Tenant**.
5. In the confirmation window, enter the name of your own tenant and select **Remove**.

## What happens to shared data when you leave a community?

When your tenant is removed from a community, it stops sharing all data streams that were previously shared within that community. All tenants that remain in the community can no longer access your data, and you can no longer access theirs.

## Pause sharing a community

Community Administrators can temporarily pause the data streams that their tenant is sharing into a community so that other tenants cannot access them.

### Prerequisites

You must be assigned a user role with [community administration permissions](#).

### Pause sharing

To pause sharing data streams from your tenant into a community, follow these steps:

1. In the left pane, select **Data Management > Communities**.
2. Select the community that you want to pause sharing for and choose **Community Details**.
3. Select **More Options :** > **Pause Sharing**.
4. In the confirmation window, select **Pause**.

Your tenant pauses sharing for all shared data streams and the tenant status updates to **Sharing Paused**.

**Note:** The status immediately updates to **Sharing Paused**, but it may take up to five minutes to take effect.

### Resume sharing

To resume sharing all shared data streams from your tenant with the community, follow these steps:

1. In the left pane, select **Data Management > Communities**.
2. Select the community that you want to resume sharing for and choose **Community Details**.
3. Select **More Options :** > **Resume Sharing**.
4. In the confirmation window, select **Resume**.

Your tenant resumes sharing for all shared data streams and the tenant status updates to **Sharing Active**.

**Note:** The status immediately updates to **Sharing Paused**, but it may take up to five minutes to take effect.

## Where can I view tenants that have sharing paused?

You can view that tenants have paused sharing into a community from either the Communities page or the Community Details page.

From the Communities page, each tile displays if there is one or more tenant in the community that has paused sharing.

### Communities page tile: Paused tenants



The Community Details page **Tenants** tab displays:

1. The total number of tenants that have paused data sharing within the community.
2. The sharing status for each tenant, listed within the **Status** column.

### Community Detail page: Paused tenants

The screenshot shows the "Tenants" tab of the Community Details page. At the top, it shows a summary: "Community" (with a ID), "1 Tenant Paused" (highlighted with a red box labeled 1), and "Created May 6, 2022". Below this is a table of tenants:

Name	Status	Users (180)	Clients (2)	Streams (15)
Data Hub Integration	Paused	177	2	15
HyperionTestingConnect	Active	0	0	0
OSI - ProjectTile	Active	3	0	0

A red box labeled 2 points to the "Paused" status of the first tenant.

## Manage users in a community

Add users to make them Community Members, which are users that can view the community and the data streams shared by other tenants. You can only add users from your own tenant. Each tenant manages its own community membership.

### Prerequisites

You must be assigned a user role with [community administration permissions](#).

## Add users to a community

To add users from your own tenant to a community:

1. In the left pane, select **Data Management > Communities**.
  2. Select the community where you want to add users and choose **Community Details**.
  3. On the **My Members** tab, select **Add Member**.
  4. Select tenant users for membership.
- 
- Tip:** If necessary, you can filter the list of users by typing in the **Filter users** field.
5. Select **Save**.

Each user is added to the community and assigned the Community Member role.

## Remove users from a community

To remove tenant users from a community:

1. In the left pane, select **Data Management > Communities**.
  2. Select the community where you want to remove users and choose **Community Details**.
  3. On the **My Members** tab, select one or more users.
- 
- Tip:** If necessary, filter the list of users by typing in the **Filter members** field.
4. On the detail pane, select **Remove Member(s)**. When prompted for confirmation, select **Remove**.

The users that you remove from the community can no longer view it nor which data streams are shared within it.

## Users from groups

The Members tab lists implicit users that hold community membership through a group. These users are denoted by the From a Group icon . These implicit users cannot be edited individually. Instead, you must manage them through the group. For more information, see [Manage groups in a community](#).

## Manage groups in a community

Add groups to make its users Community Members, which are users that can view the community and the data streams shared by other tenants. You can only add groups from your own tenant. Each tenant manages its own groups.

## Prerequisites

- You must be assigned a user role with [community administration permissions](#).
- Your tenant must be configured for one or more identity provider enabled.

## Add groups to a community

To add groups from your own tenant to a community:

1. In the left pane, select **Data Management > Communities**.
2. Select the community where you want to add groups and choose **Community Details**.
3. On the **My Groups** tab, select **Add Group**.
4. Select tenant groups for membership. If necessary, you can filter the list of groups by typing in the **Filter groups** field.
5. Select **Save**.

Each group is added to the community and its users are assigned the Community Member role. Additionally, each group user is implicitly added to the **Members** tab. For more information, see [Manage users in a community](#).

## Remove groups from a community

To remove tenant groups from a community:

1. In the left pane, select **Data Management > Communities**.
2. Select the community where you want to remove groups and choose **Community Details**.
3. On the **My Groups** tab, select one or more groups. A details pane appears. If necessary, filter the list of groups by typing in the **Filter groups** field.
4. On the detail pane, select **Remove Groups**. When prompted for confirmation, select **Remove**.

The groups that you remove from the community can no longer view it nor which data streams are shared within it.

## Manage clients in a community

Clients are applications that act on behalf of users and allow programmatic access from APIs to shared data and resources. The Community Details page lets you add existing clients to a community. You can only add [client-credentials clients](#) from your own tenant.

## Prerequisites

To manage clients in a community:

- You must be assigned a user role with [community administration permissions](#).
- There must be at least one existing client-credentials client added to the tenant (which is typically done by a Tenant Administrator). For more information, see [Add a client-credentials client](#).

## Add clients to a community

To add a client to a community:

1. In the left pane, select **Data Management > Communities**.
2. Select the community where you want to add clients and choose **Community Details**.
3. On the Community Details page, select the **My Clients** tab.
4. Select **Add Client**.
5. Select the clients to add. If necessary, filter the list of clients by typing in the **Filter clients** field.
6. Select **Add**.

## Remove clients from a community

Remove a client from a community to remove an application's access to the REST API. To remove a client from a community:

1. In the left pane, select **Data Management > Communities**.
2. Select the community where you want to remove clients and choose **Community Details**.
3. On the Community Details page, select the **My Clients** tab.
4. Select a client to remove. If necessary, filter the list of clients by typing in the **Filter clients** field.
5. Select **Remove Client**. When prompted for confirmation, select **Remove** again.

## Configure contact email

After your tenant provides an initial contact email during the invitation process, you can later update the contact email for the tenant if it changes.

### Prerequisites

You must be assigned a user role with [community administration permissions](#).

### To configure a contact email

1. In the left pane, select **Data Management > Communities**.
2. Select the community you want to edit and choose **Community Details**.
3. Select **More Options**  > **Edit Community**.
4. Edit the community **Contact Email**.
5. Select **Update**.

The contact email for the tenant is updated. Other tenants can view your contact information by browsing to the community and selecting the **Tenants** tab. Your contact email is displayed in the right pane when your tenant is selected, as shown below.

The screenshot shows the AVEVA Data Management interface. On the left, there's a sidebar with a 'Community' icon and a 'Community' section showing 'All Tenants Active' and 'Created May 6, 2022'. Below this is a table of tenants:

Name	Status	Users (180)	Clients (2)
Data Hub Integration	Active	177	2
HyperionTestingConnect	Active	0	0
OSI - ProjectTile	Active	3	0

On the right, a modal window titled 'Data Hub Integration' is open, showing 'Tenant Details' for the 'Administrative Tenant'. It includes fields for 'Name' (Data Hub Integration), 'Contact Email' (admin@admin.com), and 'Status' (Active). A red box highlights the 'Contact Email' field. Below this is a 'Data Overview' section with 'User Count' (177) and 'Client Count' (2).

## Manage community administrators

Although you initially configure which tenant roles can administer a community during community creation, you can edit which roles can administer the community at any time.

### Prerequisites

You must be assigned a user role with [community administration permissions](#).

### Add community administrators

To add community administrator permissions to a user role:

1. In the left pane, select **Data Management > Communities**.
2. Select the community you want to leave and choose **Community Details**.
3. Select **More Options** > **Manage Community Administrators**.
4. Select **Add Roles** and then select **Add Role** for any role that you want to function as community administrator.
5. Select **Save**.

### Remove community administrators

You can remove roles as that can administer the community at any time. To remove community administrator

permissions from a user role:

1. In the left pane, select **Data Management > Communities**.
2. Select the community you want to leave and choose **Community Details**.
3. Select **More Options**  > **Manage Community Administrators**.
4. Select **Remove Role**  for each role that you want to remove as community administrator.
5. Select **Save**.

## Manage default community administrators

When you create or join a community, you are prompted to assign community administration permissions to one or more role within your tenant. By default, these permissions are assigned to two default system roles: Community Administrator and Tenant Administrator. However, you can update these default roles to any system role. For example, you can configure a custom system role named Community Manager as the default community administrator.

### Prerequisites

You must be assigned a user role with [community administration permissions](#).

### To manage default community administrators

To manage default community administrators:

1. In the left pane, select **Data Management > Communities**.
2. Select **More Options**  > **Manage Default Community Administrators**.
3. Add or remove roles as default community administrators.

To add a role, select **Add Roles** and then select **Add Role**  for any role that you want to function as community administrator.

To remove a role, select **Remove Role** .

4. Select **Save**.

The default community administrator roles are updated. The next time that you create or join a community, the community administrator defaults to your settings.

---

**Note:** Updating default community administrators does not affect permissions for existing communities. To update permissions for existing communities, edit their permissions that are already in place. For more information, see [Manage community administrators](#).

---

## Community data sharing and viewing

After a community is established, Community Members can view data streams their tenant or another tenant has shared. Community Members with additional sharing permissions can share data streams with a community.

## Data sharing and viewing tasks

Community data sharing actions include:

- [Enable stream sharing permissions](#)  
Edit permissions on data streams to allow sharing them with a community.
- [Manage shared streams](#)  
Share or unshare a data stream with the community.
- [View shared streams](#)  
View which streams you or another tenant has shared within a community.
- [View shared data in a trend session](#)  
View the data from a stream that another tenant has shared in a community.

## Enable stream sharing permissions

Before data can be shared into a community and accessed by external tenants, a user with the **Share** permission on one or more streams in the Sequential Data Store must share the streams into a community that they have read access to. By default, the [CONNECT data services roles](#) role is intended for users in the tenant to share resources with other external tenants using communities. However, the Tenant Data Steward role is not assigned the **Share** permission on streams by default. Therefore, an administrative user assigned **Manage Permissions** on the streams must first grant the Tenant Data Steward role the **Share** permission on streams before they can be shared by users within that role. Granting **Share** permissions to the Tenant Data Steward role is recommended, but you can give those permissions to other roles instead.

### Prerequisites

Your user role must be assigned the **Share** permissions for applicable data streams. If you do not have these permissions, request them from a user that can manage Sequential Data Store permissions (such as a [CONNECT data services roles](#)).

### To enable stream sharing permissions

When enabling stream sharing permissions, you can either enable them for an entire namespace or on specific streams, stream-by-stream basis. Enabling streams for an entire namespace is more convenient; enabling specific streams is more secure.

You can change permissions for all streams in a namespace with a single action.

1. From the left pane, select **Data Management > Sequential Data Store**.
2. From the **Namespace** dropdown list, select the namespace that includes the streams that you want to share.
3. Select **More options :** > **Manage Default Permissions**.  
The Manage Default Permissions for New Streams window opens.
4. Allow **Share** permissions for the user roles that you want to be able to share data.
  - a. Update each applicable **Share** permission dropdown list to **Allow**. If necessary, select **Add Role** to add a

new role.

- Select **Apply to all existing streams in the namespace.**

**Manage Default Permissions for New Streams**

Entries in the table are pre-populated with Roles that contain assigned permissions. To add additional Roles and assign permissions, click the Add Role button and select the Roles you want to assign permissions to. Roles not included in the table will have their permissions reset.

**Add Role**

Role	Read	Write	Delete	Manage Permissions	Share
Tenant Administrator	All... ▾	All... ▾	All... ▾	Allow	All... ▾
Tenant Contributor	All... ▾	All... ▾	- ▾	- ▾	- ▾
Tenant Member	All... ▾	- ▾	- ▾	- ▾	- ▾
Tenant Data Steward	All... ▾	- ▾	- ▾	- ▾	All... ▾

**1**

**2**  Apply to all existing streams in the AVEVA World namespace

You are performing a patch operation on every stream in the AVEVA World Namespace. The permissions in the highlighted rows in the above table will be applied to every stream in the Namespace. Entries highlighted with unset permissions will be included in the update and will clear any existing permissions for that role.

**Cancel** **Save**

**Note:** For more information on this window, see [Permissions management](#).

- Select **Save**.

To apply sharing permission to specific streams in a namespace:

- From the left pane, select **Data Management > Sequential Data Store**.
- Select one or more streams that you want to allow sharing on.
- From the right pane, select **Manage Permissions**.

**Note:** If you only have one stream selected, select **More options** > **Manage Permissions** instead.

The Manage Permissions for Streams window opens.

- For user roles that you want to have the ability to share data, update each **Share** permission dropdown list to **Allow**.

**Manage Permissions for Selected Streams i**

**Operation Update**  
Modifying stream permissions in bulk utilizes an update operation. This means that only the permissions for role entries in the table below will be updated for each stream and the permissions for any other role will remain untouched.

**Add Role**

Role	Read <span style="color: #0070C0;">i</span>	Write <span style="color: #0070C0;">i</span>	Delete <span style="color: #0070C0;">i</span>	Manage Permissions <span style="color: #0070C0;">i</span>	Share <span style="color: #0070C0;">i</span>
Tenant Administrator	<input checked="" type="checkbox"/> All... <span style="color: #0070C0;">i</span>	<input checked="" type="checkbox"/> All... <span style="color: #0070C0;">i</span>	<input checked="" type="checkbox"/> All... <span style="color: #0070C0;">i</span>	<input checked="" type="checkbox"/> Allow	<input type="checkbox"/> - <span style="color: #0070C0;">i</span>
Tenant Community Adm...	<input checked="" type="checkbox"/> All... <span style="color: #0070C0;">i</span>	- <span style="color: #0070C0;">i</span>	- <span style="color: #0070C0;">i</span>	- <span style="color: #0070C0;">i</span>	- <span style="color: #0070C0;">i</span>
Tenant Data Steward	<input checked="" type="checkbox"/> All... <span style="color: #0070C0;">i</span>	- <span style="color: #0070C0;">i</span>	- <span style="color: #0070C0;">i</span>	- <span style="color: #0070C0;">i</span>	<input checked="" type="checkbox"/> All... <span style="color: #0070C0;">i</span>

**Cancel** **Save**

**Tips:** For more information on this window, see [Permissions management](#).

5. Select **Save**.

## Manage shared streams

Users assigned share permissions for data streams in Sequential Data Store—also known as *data stewards*—can share those streams into communities where they are a member. These same users can unshare data streams from communities as well.

### Prerequisites

Your user role must be assigned the **Share** permissions for applicable data streams. If you do not have these permissions, request them from a user that can manage Sequential Data Store permissions (such as a [CONNECT data services roles](#)).

### Share streams

User with permissions to share a data stream within a community can do so from the Sequential Data Store page. To share streams with other communities:

1. In the left pane, select **Data Management > Sequential Data Store**.
  2. If it is not already selected, select **Streams** from the upper-left dropdown list.
  3. Select one or more streams to share with a community.
- Tip:** Use the **Search for streams** field to search for specific streams. For more information on using this field, see [Search queries](#).
4. From the right pane, select **Share Streams**.

**Tips:**

- If you only have one stream selected, select **More options**  > **Share Stream** instead.
  - If **Manage Permissions** is unavailable, you do not have permissions to share a selected stream. You must request permissions from a user that can manage stream permissions. For more information, see [Enable stream sharing permissions](#).
  - When sharing a large numbers of streams, edit the **Items per page** dropdown to a value that accommodates the number of streams that you want to share.
5. From the Share Streams window, confirm the streams you are about to share, and then select the communities that you want to them with, and then select **Share**.

**Getting Namespace does not allow data to be processed outside of the region where it resides?** See Namespace warning.

The chosen streams are shared with the chosen communities. All members of the selected communities are able to read data from the shared streams.

## Unshare streams

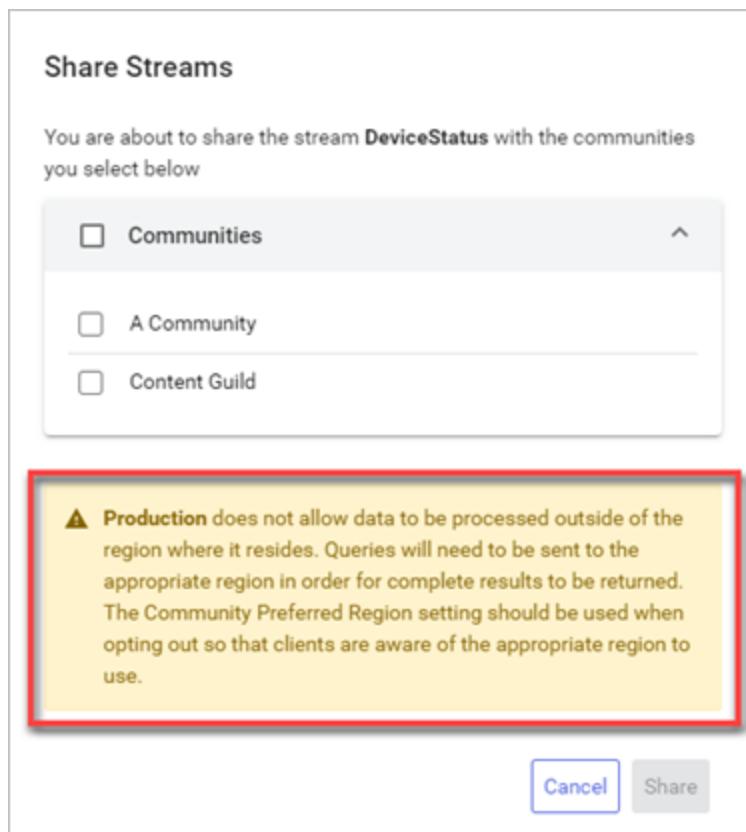
When you want to stop sharing streams with a community, you can unshare them from the Communities page.

1. In the left pane, select **Data Management > Communities**.
2. Select the community where you are sharing streams and choose **Community Details**.
3. On the Community Details page, select the **Tenants** tab.
4. Select your own tenant. A pane opens on the right.
5. On the **Streams** tab, select the streams you want to stop sharing, then select **Unshare Streams**. Confirm the streams you are unsharing, and then select **Unshare**.

The streams are unshared from the community. Other tenants in the community can no longer view them.

## Namespace warning

If you receive the following warning while sharing streams from a namespace into a community a namespace, you can resolve it by updating the Community Preferred Region setting to the appropriate region. For more information on how to change this setting, see [Manage preferred region](#).



## View shared streams

After a community is established, you can view which data streams are shared into it. You can view both the streams that your tenant is sharing, as well as the streams that other tenants are sharing. You can view shared data streams in one of two ways: from the Communities page or Sequential Data Store. Your access to view shared data stream information depends upon your assigned user roles and permissions.

### To view shared streams

You can view shared streams from both the Communities page and Sequential Data Store. Select one of the tabs for more information on how to view which data streams are shared.

From the Communities page **Tenants** tab, you can view which data streams each tenant has shared with the community.

1. From the left panel, select **Data Management > Communities**.
2. Select the applicable community and choose **Community Details**.  
The community details open. For more information about each field, see [Community details](#).
3. From the **Tenants** tab, select a tenant to view which streams that it shares with the community.  
Details for the community open in the right pane.
4. From the right pane, select the **Streams** tab.  
The **Streams** tab lists each data stream that the tenant shares with the community.

---

**Tip:** Want to view more details about the shared streams? Select  **View Streams** to open it within Sequential Data Store in a new tab.

---

When working from Sequential Data Store, you can view which data streams are shared within communities, sorting by either stream or community.

## View shared streams by community

1. From the left panel, select **Data Management > Sequential Data Store**.
2. If necessary, enable the **Filter Communities** panel by selecting the **Filter** icon .
3. Select a community to filter for.

The page is filtered to list only data streams shared in the selected communities.

## View communities for a shared stream

While viewing individual data streams in Sequential Data Store, you can view each community that the stream is shared with that you have read access to.

1. From the left panel, select **Data Management > Sequential Data Store**.
2. (Optional) Select one or more community to filter for.
3. Select a single data stream. Details for the community open in the right pane.
4. From the right pane, select the **Sharing** tab.

The tab lists each community that the stream is shared to for which you have read access. This tab does not list all communities that the stream is shared with—only those that you have read access to.

---

**Tip:** Want to view a community that the selected stream is shared to? Select the **Launch** icon  for the community.

---

## View shared data in a trend session

After streams are shared within a community, any **Community Member** can visualize those streams within the Trend page as if it were a data stream from their own tenant.

## To view shared data in a trend session

1. From the left panel, select **Data Management > Communities**.
2. Select the applicable community and choose **Community Details**.  
The community details open. For more information about each field, see [Community details](#).
3. From the **Tenants** tab, select a tenant.  
Details for the community open in the right pane.
4. From the right pane, select the **Streams** tab.  
The **Streams** tab lists each data stream that the tenant shares with the community.
5. Select the streams that you want to view in a trend session and select **More options**  **> Trend Streams**.

The selected streams are launched in a trend session. For more information on use of a trend session, see [Trend visualization](#).

## View community usage

The **Usage** tab displays consumption information for the streams created and viewed within the selected community. You can view these streams by your usage of them within the community or by Community Usage.

### To view community usage

When viewing streams usage, you can view stream consumption in one of two ways: how your tenant consumes data shared by other tenants, or how other tenants in the community consume shared data.

To view how your tenant consume data shared by other tenants, select the **My Usage** chart.

1. In the left pane, select **Data Management > Communities**.
2. Select the community that you want to view usage for, then choose **Community Details**.
3. Select the **Usage** tab.
4. From the left dropdown list, select **My Usage**.
5. From the right dropdown list, choose **Monthly View** or a **Daily View** for a given day. For more information, see [View](#).
6. (Optional) Select **Download Usage** to download the displayed data as a CSV file.

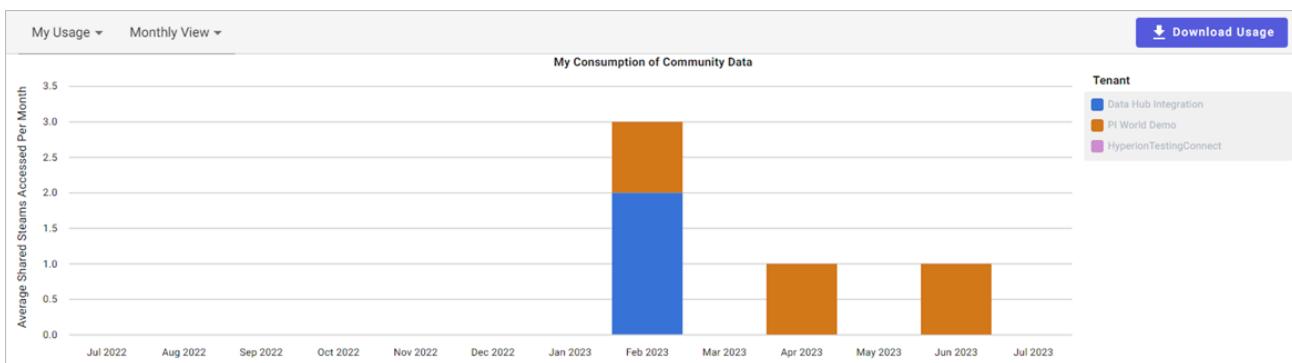
To view how other tenants in the community consume data, select the **Community Usage** chart.

1. In the left pane, select **Data Management > Communities**.
2. Select the community that you want to view usage for, then choose **Community Details**.
3. Select the **Usage** tab.
4. From the left dropdown list, select **Community Usage**.
5. From the right dropdown list, choose **Monthly View** or a **Daily View** for a given day. For more information, see [View](#).
6. (Optional) Select **Download Usage** to download the displayed data as a CSV file.

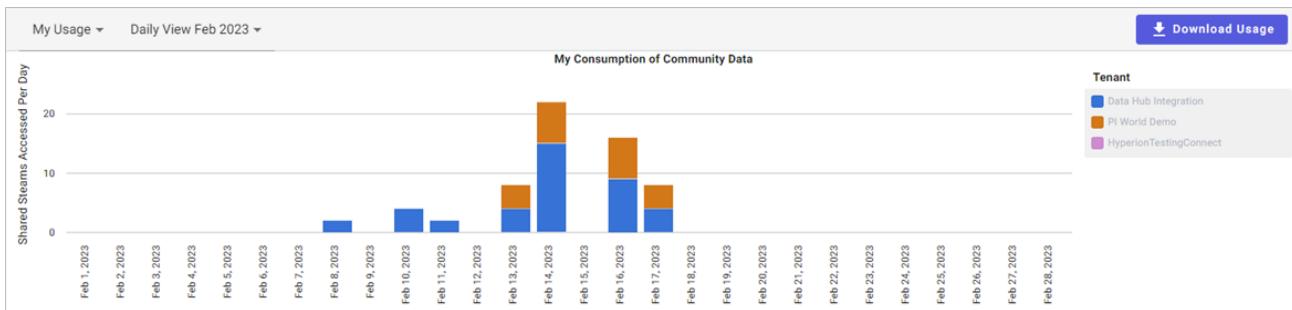
## View

Use the view dropdown to display streams accessed by month or day. Choose between the following options:

- **Monthly:** Displays usage data for the chosen data source for the past seven months, broken down by month.



- **Daily:** Displays usage data for the chosen data source for each day in a chosen month. There is a daily view for each day of the month that shared stream access occurred.



## Legend

Legend
OSisoft Testing
CommunityTest2
Community Test 1

## Tabular data

Regardless of which parameters or chart you choose, the data displayed in the bar graph is also displayed below it as tabular data. View the Legend to see how the stream data maps to a data source. You can export this data in CSV format by selecting **Download Usage**.

## Stream metadata rules

The value of metadata lies in its capacity to enrich sequential data, and to facilitate logical segregation and contextualization of data. Other services and applications, such as data views, leverage stream metadata to simplify finding data and to provide context about stream data. When possible, you should explicitly include metadata when you create streams. When that is not possible, you can use metadata rules to leverage a

consistent naming pattern for streams to embed metadata.

You create metadata rules by selecting parsable metadata from a stream name structure, such as location, facility, asset class, or asset Id, and applying the rule to identify streams whose names match the defined pattern. The metadata rule identifies all streams that match the pattern, then CONNECT data services parses each stream and builds out the metadata following the defined rules.

## PI Server counterpart

Metadata rules do not have a similar counterpart in PI Server because PI points cannot store generic metadata.

## Metadata best practices

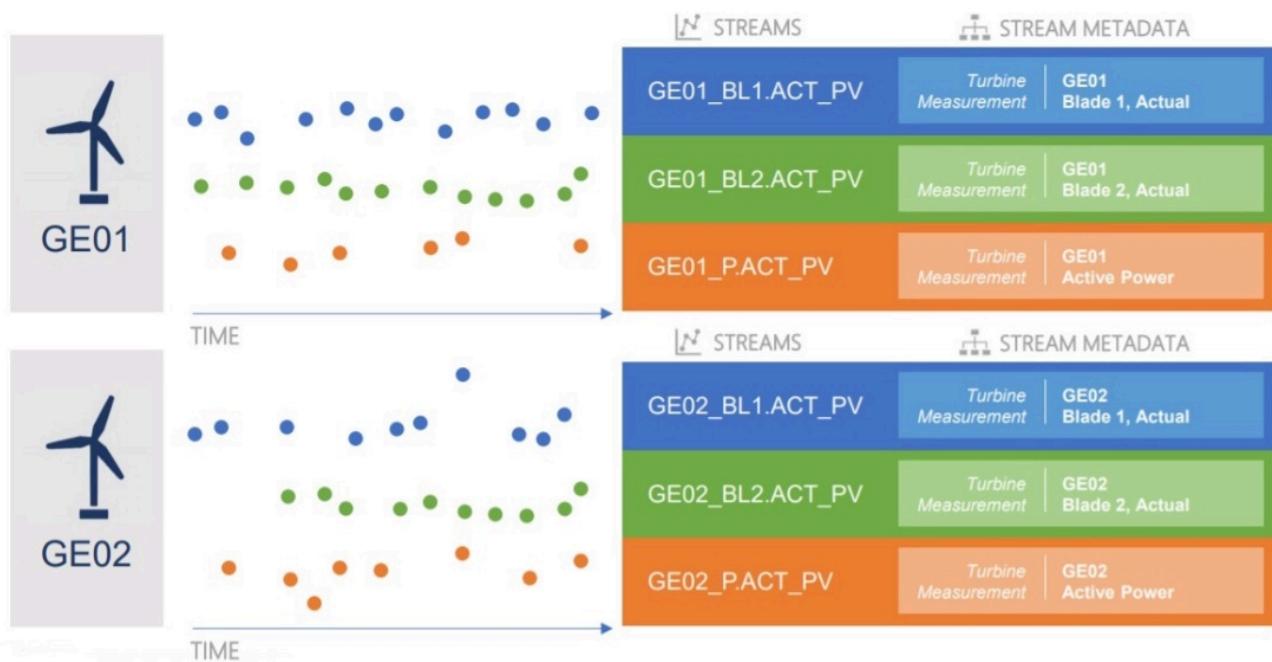
Follow these best practices to make it easier to add metadata to streams:

- The easiest way to explicitly add metadata is when streams are created. Whenever possible, add metadata during stream creation.
- There may be situations where streams are created from an external source and you cannot explicitly include metadata fields. If possible, establish and apply a naming pattern for stream names that can be used with metadata rules. The following is an example of a naming pattern:  
`{Region}.{Site}.{Equipment}.{Measurement}`. Use delimiters to separate the parts in the naming pattern.
- If possible, manually create a few streams with your proposed stream naming pattern. Then experiment with creating metadata rules to ensure that you can collect all of the metadata that you want from the stream name. Once you have confirmed that all of the metadata is captured in the stream name, then proceed with creating the remainder of your streams.

## Using metadata rules to add metadata to streams

The following diagram shows metadata for two turbines named GE01 and GE02, each with three data streams:

- The color-coded data streams show the specific data each stream is tracking, which is detailed in the **Stream Metadata** column.
- The basic description of the stream data is encoded in the stream name. For example, for the third stream in the table, the metadata rule translated `GE01_P.ACT_PV` into meaningful information. You see that `GE01` is the name of the turbine and that `Active Power` is the measurement in this stream.
- A metadata rule based on this stream naming pattern can capture active power values for all turbines in each wind farm.



Create metadata rules by selecting a stream as a template and then define the criteria to match with other streams. In the example below, CONNECT data services shows a stream selected for metadata rule and identifies characters you could use to divide the stream name into parts using a + sign.

1 Select Stream   2 Create Pattern   3 Define Mappings   4 Preview

### Create Pattern

Use the (+/-) buttons to divide the stream name into sections, and then designate each section as Metadata, String Literal, or Wildcard.

NO PATTERN DEFINED

23TANK09TS.PV

"23TANK09TS.PV"

Assign a metadata type to each part of the stream name, using the following metadata types:

- wildcard – variable information
- metadata – a key that identifies values in the stream; part of a key-value pair
- string literal – static characters that convey information

In the following example, all data comes from wind turbines on a wind farm and the template stream name has three parts: GE01, P.ACT, and PV. The first part of the stream name identifies the wind turbine and is different for each wind turbine. This part of the stream name is a wildcard. The second part of the stream name, P.ACT, identifies the measurement Active Power. This part of the stream name is metadata. The third part of the stream name, PV, stands for Pine Valley Wind Farm and is a string literal.

When the parts are combined, this metadata rule creates metadata for streams coming from turbines for Active Power in the Pine Valley Wind Farm.

The screenshot shows the 'Create Pattern' step of a four-step process. The stream name 'GE01\_P.ACT.PV' is being broken down into segments. The first segment, 'GE01', is set to 'Wildcard'. The second segment, 'P.ACT', is set to 'Metadata' with a key named 'Measurement'. The third segment, 'PV', is set to 'String Literal'. The interface includes a toolbar at the top with steps 1 through 4, and a note below the stream name about using (+/x) buttons to divide the stream name into sections.

When you create a metadata rule, CONNECT data services applies it to all existing streams and subsequently to any new streams added to the namespace. You can edit a metadata rule, but the modified rule may capture a different set of streams.

## Create a metadata rule

Use metadata rules to identify groups of similar streams for analytical purposes. You select a stream name to use as a name pattern and assign metadata to selected stream name segments, such as a plant location or device category. The resulting stream name pattern with assigned metadata parts defines a metadata rule. Metadata rules assign defined metadata to all streams in a given namespace matching the stream name pattern defined in the rule.

(Optional) To copy a stream name for the basis of the metadata rule:

1. In the left pane, select **Data Management > Sequential Data Store**.
2. On the Sequential Data Store page, select **Streams**.
3. Select the stream to use as the basis for the metadata rule and from the **Details** tab, copy its name.

To create a new metadata rule:

1. In the left pane, select **Data Management > Stream Metadata Rules**.
2. Select **Add Metadata Rule**.
3. On the Select Stream page in the **Search for streams** field, enter the stream name to use as a model for the stream name pattern.

For more information on using the field, see [Search queries](#).

All streams that match the name pattern display.

4. Select the stream name to use for the metadata rule and select **Next**.
5. On the Create Pattern page, select the + sign above each selected delimiter to separate sections of the stream name. Conversely, you can select the X to ignore a delimiter.

6. For each delimited segment of the stream name you select, use the dropdown list to assign a segment type. The following table describes the available segment types.

Segment type	Description
<b>Metadata</b>	<p>Assigned to the data values provided by each stream matching the name pattern of the metadata rule. At least one section must have this type.</p> <p>If you select metadata type <b>Metadata</b>, you must also enter a metadata key. A metadata key is the key portion of a key-value pair, typically the type of data provided, such as Measurement. This is helpful when streams that match the rule provide different types of data. Entries in the <b>Map To</b> portion of mapping represent the value part of the key-value pair. For example, <i>Power</i> would be the defined key, while different types of data could be <i>Demand</i>, <i>TOTAL/Electricity</i>, or <i>Metering</i>. The mapping entries specify the labels you want to display for each of those values.</p>
<b>String Literal</b>	<p>Only stream names with the specified string in the part designated will match the name pattern of this metadata rule.</p>
<b>Wildcard</b>	<p>Designates a part of the stream name pattern in which any value is accepted by this metadata rule.</p>

7. After assigning all metadata type entries, select **Next**.
8. On the Define Mappings page, for each metadata key do one of the following:
- To display the raw stream data for the specified metadata key, select **Copy Values** under **Mapping Type**.
  - To assign a label to data values:
    - Select **Map Values** and select **Generate Mappings**.
    - In the **Map To** field, enter the label to display for each defined metadata key.
    - (Optional) Select **Add Mapping** to define a mapping for any other stream name part.
- When you have defined mappings for a metadata key, a green check mark appears next to the key.
9. Select **Next**. All matching streams for the rule are displayed.
10. On the Preview and Run page, complete the following fields:
- **Name** – Enter a name to identify the metadata rule.
  - **Description** – Enter a description for the metadata rule.
11. Select **Save & Execute**.

## Maintain a metadata rule

### Edit a metadata rule

To edit an existing metadata rule:

1. In the left pane, select **Data Management > Stream Metadata Rules**.
2. Select an existing metadata rule.
3. Select **Edit metadata rule**.
4. To reset the pattern and all mappings, select **Reset Pattern**, then proceed as when creating a new rule. See [Create a metadata rule](#).
5. To update the mappings, on the Update Mappings page do one of the following for each metadata key:
  - To display the raw stream data for the specified metadata key, select **Copy Values** under **Mapping Type**.
  - To assign a label to data values:
    - Select **Map Values** and select **Generate Mappings**.
    - In the **Map To** field, enter the label to display for each defined metadata key.
    - (Optional) Select **Add Mapping** to define a mapping for any other stream name part.
- When you have defined mappings for a metadata key, a green check mark appears next to the key.
6. Select **Next**. All matching streams for the rule are displayed.
7. On the Preview and Run page, edit the **Name** and **Description**, if needed.
8. Select **Save & Execute**.

### Remove a metadata rule

To remove an existing metadata rule:

1. In the left pane, select **Data Management > Stream Metadata Rules**.
2. Select an existing metadata rule.
3. Select **Remove metadata rule**.
4. If you do not wish to remove all stream metadata written by this rule, uncheck **Remove Associated Metadata**.
5. Select **Remove** to confirm.

### Set permissions for a metadata rule

Once a metadata rule has been created, you can set permissions to manage access to it.

To set permissions for a metadata rule:

1. In the left pane, select **Data Management > Stream Metadata Rules**.
2. Select a metadata rule and select **Manage Permissions**.
3. On the Manage Permissions page, select a role from the **Selected role** dropdown list.
4. Select **Allow** or **Deny** for each of the following permissions: **Read**, **Write**, **Delete**, and **Manage Permissions**.

5. Select **Save**.

## Asset rules

An asset rule identifies patterns in a stream name and uses this information to automatically create assets. In order to generate assets, the stream names must have the following characteristics:

- A pattern that can be mapped for configuration.
- A set of characters that uniquely identify the asset.
- A unique set of characters that identifies one stream from another for the same asset. For example, the stream name could include an abbreviation for the stream measurement.

The asset rule identifies the pattern and the parts of the stream name and stream metadata that provide information about the asset. A token is created for each part of the pattern and piece of information. The tokens are used to construct the asset and add references to the relevant streams. For more information, see [How tokens are used to generate assets](#).

Depending on the definition and consistency of the stream names, you may have to create multiple rules to capture all the relevant streams for your asset. For more information, see [Use multiple asset rules to create assets](#).

### Asset rules and generated assets

An asset rule and the assets generated from that rule remain linked in the following ways:

- If you delete an asset rule, then any assets created with the rule are also deleted. There may be a short delay between the time the rule is deleted and when the related assets are deleted.
- If you edit the properties of assets created with asset rules, those edits take precedence over the asset rule configuration. For example, if you edit the asset name, the rule does not overwrite this edit.
- If you manually delete an asset, the deletion is treated as an edit of the asset and overrides the rule. Therefore, if you delete an asset created by an asset rule, you cannot recreate that asset with the same Id. If you inadvertently delete an asset, you can recover the asset by deleting the rule. This action deletes any assets created with this rule. Then you can recreate the rule and configure the Id so that it resolves to a different Id. For example, assume that the asset Id in the first rule resolves to Boiler Tank 1 and this asset is deleted in error. You then create a second rule which the Id resolves to Region 1 - Boiler Tank 1. CONNECT data services sees this as different asset and creates it.

## Create an asset rule

Use the following procedure to create an asset rule.

### Tank Rule A example

The [Use the Asset Rule Builder to create the asset rule](#) procedure uses the following simple example to illustrate how to create an asset rule. For example, the following stream names could be used to identify three tank assets: SL-Tank01, SL-Tank02, and PHI-Tank03. There are two streams for each tank, one stream with

temperature data, indicated by *Temp* in its name, and the other with pressure data, indicated by *Press* in its name. The following table shows the six streams, the asset associated with the stream, and the measurement in each stream.

Stream Name	Asset Name	Stream Measurement
SL-Tank01Press	Tank 01	Pressure
SL-Tank01Temp	Tank 01	Temperature
SL-Tank02Press	Tank 02	Pressure
SL-Tank02Temp	Tank 02	Temperature
PHI-Tank03Press	Tank 03	Pressure
PHI-Tank03Temp	Tank 03	Temperature

We will construct an asset rule, named *Tank Rule A*, that creates three assets, one for each tank. Each asset will include references to the two streams that belong to that tank.

## Add an asset rule and select the stream

1. In the left pane, select **Data Management > Asset Rules**.
2. Select the **Change Namespace** button in the upper-right toolbar, then select the desired namespace.
3. Select **Add a Rule**.
4. In the Create New Asset Rule window, enter the following:
  - **Name** – Name of the asset rule. The name must be unique within a namespace.  
In this example, the asset rule is named *Tank Rule A*.
  - **Description** – (Optional) Description of the rule.
  - **Asset Type** – (Optional) Asset type on which the asset is based. The assets created with the asset rule inherit the properties of the asset type, including stream type, metadata, and status configurations.  
For example, the asset type is named *Boiler Tank*.  
For more information on asset types, see [Asset types](#) and [Add an asset based on an asset type](#).
5. Select **Continue**.
6. In the Select Stream window, select the stream to use as the basis of the naming pattern for the asset rule.

**Tip:** Select a stream with a name that models the pattern of the stream names the rule is intended to identify.

The *Tank Rule A* examples uses the *PHI-Tank03Press* stream to create the stream pattern.
7. Select **Add**.  
The Asset Rule Builder page displays.

## Use the Asset Rule Builder to create the asset rule

The Asset Rule Builder walks you through the following steps to create and execute the asset rule:

1. Extract tokens from the stream name
2. Map the tokens to values
3. Configure the asset
4. Preview the asset

### Step 1: Extract tokens from the stream name

In this step, you specify the naming pattern used to find and match the appropriate streams. You isolate each part of the stream name and create a token for it. The rule contains intelligence to recognize special characters in the stream name as delimiters, such as periods, dashes, and underscores. By default, the rule uses any special characters in the name to isolate the stream parts and facilitates the rule-building process. In this step, you also create tokens for the stream metadata.

1. In the Stream Name pane, move the slider to highlight the first identifiable section of the stream name.
2. In the **Match** list, select the option that describes how to identify the value in the stream name.
3. In the **and name it** text field, enter a name for the token.
4. Select **Capture**.

In the Tank Rule A example above, the first part of all stream names identifies the site location. This is represented by the characters *SL* or *PHI*. In the *PHI-Tank03Press* stream, the site location is represented by the characters *PHI*. This part of the stream name is selected in the screen capture below.

The **1. Match** list of choices displays different ways to identify this string of characters. Some of the choices would work with the example stream, but they would fail to identify the site information in all stream names. For example, *the string literal "PHI"* or *the next 3 characters* would not identify *SL* as the site.

When you create tokens, keep in mind that the **Match** option selected must identify the correct information for all the streams the rule needs to identify. The rule must also exclude any streams that you do not want identified with this rule, for example, streams that belong to a pump asset. In this example, *letters preceding the delimiter "-" will extract the site information for all streams*.

The token is assigned the name *site*.

The token and the placeholder value, *{site} - PHI*, are added to the Tokens pane.

5. Repeat steps 1-4 for each part of the stream name.

In this example, the second part of the stream name is the type of equipment. Notice that the match options change depending on what portion of the stream name is highlighted. The first option is disabled because it cannot be applied. *Tank* is matched using the *next group of letters*. The token is assigned the name *equipment\_type*.

---

**Note:** There are other matching options which could be used with the example streams, *the string literal "Tank"* or *the next 4 letters*. This rule needs to identify equipment other than tanks and equipment with names that are not 4 letters long, so these are not good choices.

---

The next part of the stream name is a number that identifies the equipment Id. *03* is matched using the *next group of numbers*, and this token is assigned the name *equipment\_id*. Because we anticipate using this rule to create assets with Ids running into the thousands, we do not use the *next 2 numbers* to match

the Id.

The last part of the stream name identifies what is being measured in the stream. This token uses the rest of the stream name and is named measurement.

6. In the Token Sources pane on the left, select **Stream Metadata**.

The stream metadata are displayed in the center pane.

7. Select the checkbox for each stream metadata to use to construct assets.

The metadata tokens are added to the Tokens pane.

8. In the Token Sources pane on the left, select **Stream Name** and review the screen.

The description of the stream pattern is displayed in the Stream Name pane. The Tokens pane shows the tokens that make up the stream name pattern.

9. When you have completed identifying all the tokens in the stream name, select **Next**.

## Step 2: Map the tokens to values

In this step, you specify the token that identifies the stream measurement in the stream. Then you map values for each token.

1. In the Configure Stream Reference Name Token pane, select the  icon to open the Select Stream Reference Name Token window.

2. Select the token that identifies the stream measurement and select **Select**.

In the Tank Rule A example, the token for the last part of the stream name identifies the measurement, either Press or Temp, and we gave this token the name measurement. The Token Mappings Status pane displays a list of all the tokens identified on the previous page. The token for the measurement is indicated with the  icon.

3. Select a token in the **Token Mappings Status** list.

4. In the Token Value Mappings pane on the right, select one of the following:

- **Use Existing Token Values** – Use the value in the stream name that corresponds to the token.
- **Rename Token Values** – Replace the values in the stream name and stream metadata with mapped values.

In the Tank Rule A example, the equipment\_type and equipment\_id tokens use the existing token values.

5. If you selected **Rename Token Values**, select **Generate Mappings** to display the list of token values for streams that match the stream pattern.

In the Tank Rule A example, the site token is selected. **Rename Token Values** is selected, and **Generate Mappings** generates two values, PHI and SL.

6. For each value on the left, enter or select the value to use in its place in the text field on the right.

If the asset rule is based on an asset type, select the text field to display a list of measurements or properties that are defined in the asset type and select the value to map to the token value. If the asset rule is not based on a type, then you must manually enter the values for each of the mappings.

In this example, PHI is mapped to Philadelphia, and SL is mapped to San Leandro.

Name: Press Assets Asset Type: Press

1 Extract Tokens      2 Map Tokens to Values      3 Asset Configuration      4 Asset Preview

**Configure Stream Reference Name Token**  
Select the token which contains the measurement [?](#)

{measurement} - Press [Edit](#) [Copy](#)

**Token Mappings Status**  
Specify the token values for each of the tokens listed below.

(site) - PHI	✓ <input checked="" type="radio"/>
(equipment_type) - Tank	✓ <input type="radio"/>
(equipment_id) - 03	✓ <input type="radio"/>
(measurement) - Press	✓ <input checked="" type="radio"/>

**Token Value Mappings**  
Token Value of PHI from Stream Name PHI-Tank03Press

Use Existing Token Values  
 Rename Token Values

[Generate Mappings](#) [Add Mapping](#) [Remove All Mappings](#)

Mappings

PHI	→ Philadelphia	X
SL	→ San Leandro	X

Cancel Back Next

7. To manually add additional mappings, select **Add Mapping**.
8. When you have configured the token values for all tokens, indicated by the green check mark, select **Next**.

### Step 3: Configure the asset

In this step, you specify how the rule builds assets by assigning the tokens to asset fields. When the assets are generated, the tokens are replaced with the value mappings.

1. In the Configure Asset pane, for each of the following asset fields enter the sequence of tokens and characters that resolve to create a value for each asset. To pick from a list of tokens, enter { and select a token.
  - **Id** – The Id must be unique for each asset. If the ID is not unique, the generated assets may incorrectly reference streams that belong to another asset.

For the Tank Rule A example above, a combination of the site, equipment type, and equipment ID creates a unique ID for the tank.

- **Name** – Enter the sequence of tokens and characters that resolve to create the name for each asset. To pick from a list of tokens, enter { and select a token.
  - **Description** – Optional.
  - **Stream Reference Name** – The token that was configured in Step 2 as the measurement. You will receive an error if you attempt to use this token in other fields.
2. To map metadata values, do one of the following:
    - If the asset rule is based on an asset type, the list of metadata is automatically populated based on the asset type and you cannot add or delete metadata. In the **Value Expression** field for each metadata you want defined for your assets, enter the sequence of tokens and characters that resolve to create the value for the metadata. To pick from a list of tokens, enter { and select a token. Leave the **Value Expression** field blank for metadata you do not want mapped.

- If the asset rule is not based on an asset type, complete the following steps for each metadata you want to add:
  - a. Select **Add Metadata**.
  - b. In the **Name** field, enter the name for the metadata.
  - c. In the **Value Expression** field, enter the sequence of tokens and characters that resolve to create the value for the metadata. To pick from a list of tokens, enter { and select a token.
  - d. In the **Type** field, select the data type for the metadata from the dropdown list.
  - e. When you are finished mapping tokens to asset fields and metadata, select **Next**.

## Step 4: Preview the assets

The asset preview displays a list of the assets that will be created using the asset rule. Use the preview to verify that the rule creates all the assets you expect and they are created correctly.

1. Review the assets. Verify that they are created as you expect and verify that the correct streams are referenced.

---

**Note:** The  icon identifies the metadata and the  icon identifies the stream references.

The stream Id is identified for each stream. In the example above, the Id of the stream in the first row is PHI-TNK01.

---

2. To show or hide information in the preview, select the **Settings** tab in the Preview Information pane, and select the following options:

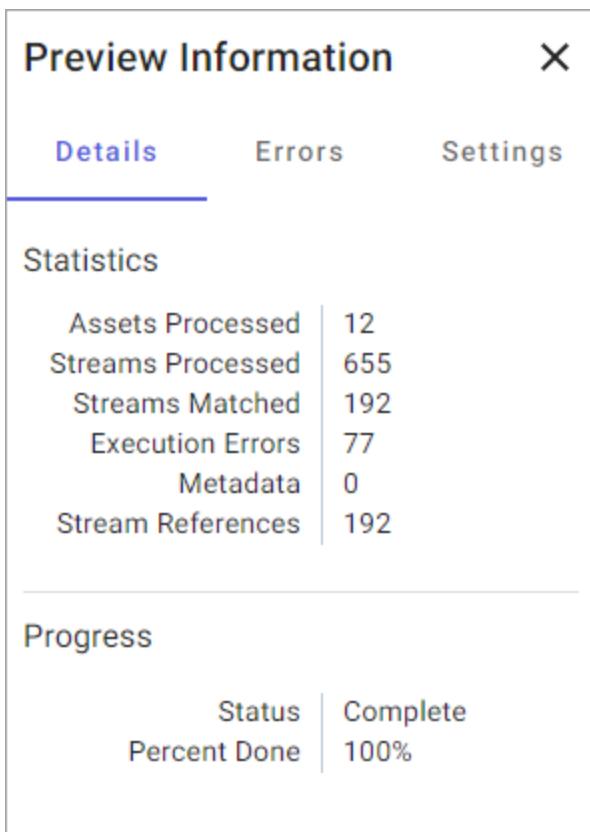
- **Show Asset Type**
- **Show Metadata**
- **Show Stream References**

3. To filter the data in a column, select  in the column header, enter the text to find, and press Enter.

4. On the **Details** tab of the Preview Information pane, review the asset rule statistics to validate that the rule produced the expected number of assets and the expected number of streams were processed.

In the Tank Rule A example above, we expect to see three assets as indicated in the **Assets Processed** field.

**Streams Processed** is the total number of streams in the namespace. The asset rule checks every stream name in the namespace to see if it matches the specified pattern. In this example, six of the nine streams matched the pattern.



5. To return to earlier steps and make any changes to the tokens, token mapping, or asset configuration, select **Back**.
6. To save the rule configuration without running it, select **Save as Draft**. Use this option to continue modifying the rule later.
7. To save the rule configuration and run the rule, select **Save & Execute**.

The rule appears in the Asset Rule Builder list and a message confirms that the rule was successfully created. The rule is executed and applied to the streams, and the assets are created.

---

**Note:** Select the rule in the Asset Rule Builder list to open a pane that displays any errors that occurred during the execution of the rule.

---

## Review the assets

Once the asset rule is successfully executed, review the created assets and confirm the results.

1. In the left pane, select **Visualization > Asset Explorer**.
2. Use search and the metadata filters to find the assets you expect to be created. For information, see [Filter and search assets](#).
3. Select an asset to see its details.

---

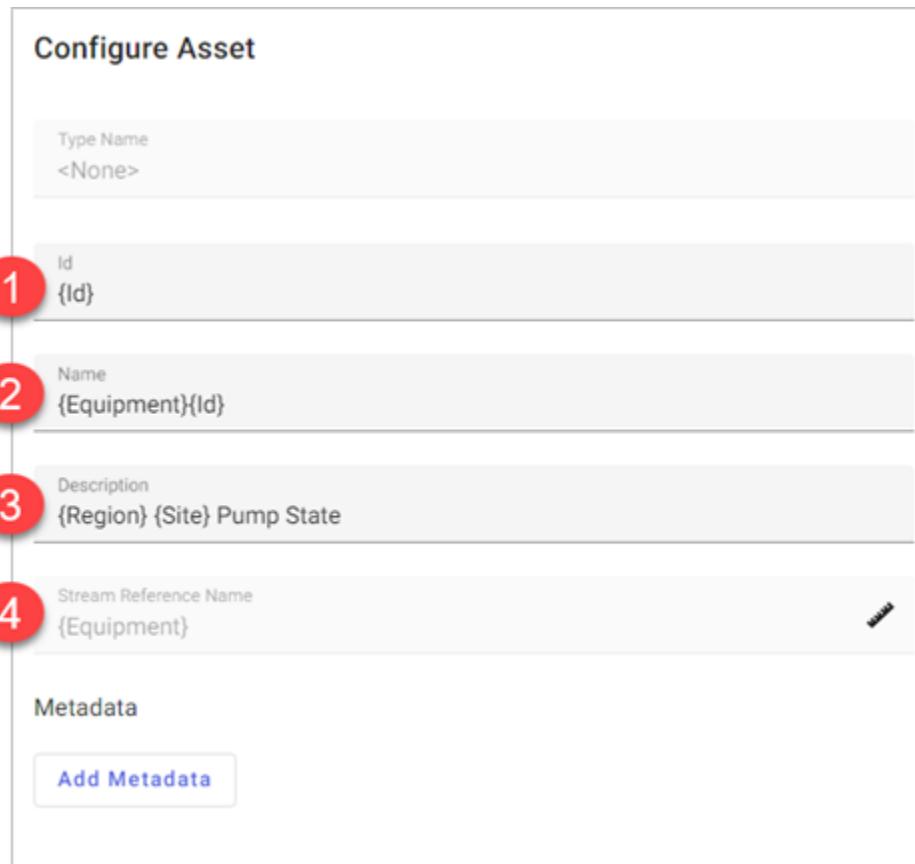
**Tip:** Select the pencil icon in the toolbar to see the individual streams referenced in the asset.

---

## How tokens are used to generate assets

When creating asset rules, use tokens to represent the parts of an asset name. A *token* is a placeholder for a part of the naming pattern and used to construct an asset and add references to the relevant streams.

The following screen capture shows the Configure Asset window for the Tank Rule A example in [Create an asset rule](#). The numbers identify the different fields and the tokens assigned to those fields. These tokens are used to configure the assets created with the rule.

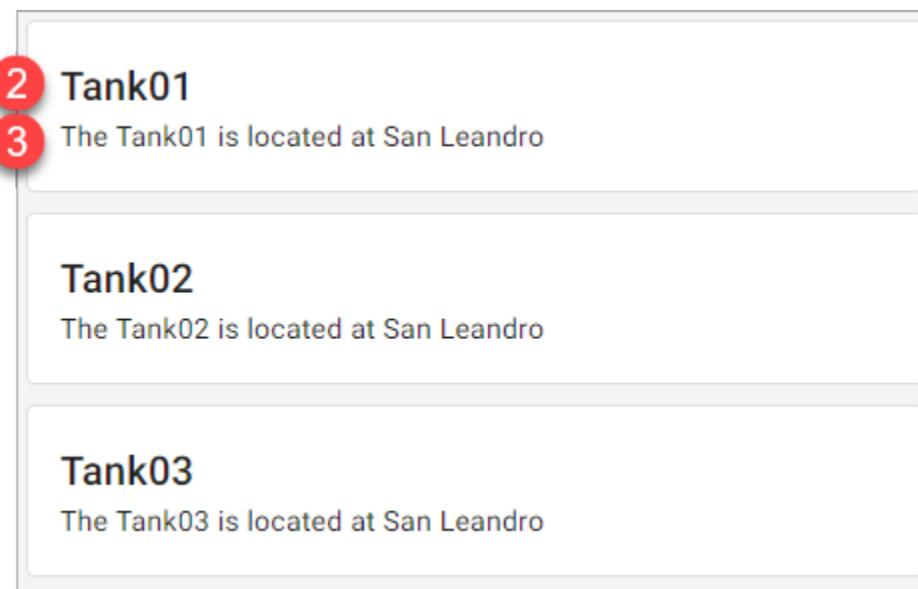


The following table shows the token definitions for the Tank rule and the resulting values for one of the assets (Tank 01) when the rule is applied.

#	Configuration field	Token definition	Values for the Tank 01 asset
<b>1</b>	Id	{site} {equipment_type}.{equipment_id}	San Leandro Tank.01
<b>2</b>	Name	{equipment_type} {equipment_id}	Tank 01
<b>3</b>	Description	{site}	San Leandro

#	Configuration field	Token definition	Values for the Tank 01 asset
4	Stream Reference Name	{equipment}	Pump

The screen capture below displays the three assets that were created with the example Tank rule. The numbers identify the properties of Tank 01 that are derived by applying the asset rule. Refer to the table above to match the value with the configuration field and token definition.



The following screen capture is an example of what you might see when you edit the Tank 01 asset in Asset Explorer. The numbered fields—asset name, Id, description, and stream references—are generated by the asset rule. For example, the `_site {equipment_type}.{equipment_id}` expression is used to generate the San Leandro Tank.01 Id.

Tank 01 Cancel

2 Asset Name  
Tank 01

1 Id  
c866ec0f-55a5-4697-8615-d09f26a62829

3 Asset Type  
MyData.PumpType

Description  
Tank 01 is located at San Leandro

Metadata Properties Status

Add Stream References Configure Preview

Stream References

4 T Pump ▼

## Use multiple asset rules to create assets

There are situations where a single asset rule cannot identify all the streams required to create your assets. In these situations, you must create additional asset rules to accommodate different asset naming patterns.

In the [Tank Rule A example](#), the stream names follow a single pattern that can be defined with one asset rule. Returning to the Tank Rule A example, assume that there is one stream name that deviates from this pattern and cannot be identified by this rule. In the table below, PHI-Tank03-Temp differs from the other stream names and contains a hyphen delimiter between the third and fourth parts of its name, that is, between *03* and *Temp*.

Stream Name	Asset Name	Stream Measurement
SL-Tank01Press	Tank 01	Pressure
SL-Tank01Temp	Tank 01	Temperature
SL-Tank02Press	Tank 02	Pressure
SL-Tank02Temp	Tank 02	Temperature
PHI-Tank03Press	Tank 03	Pressure
<b>PHI-Tank03-Temp</b>	Tank 03	Temperature

Therefore, you must create a second asset rule, called Tank Rule B, to identify this stream. The stream name pattern is identical to Tank Rule A, except for the third part of the stream name. In Tank Rule A, this part of the stream name was matched with the next group of numbers option. In Tank Rule B, to correctly identify the PHI-Tank03-Temp stream, 03 must be matched using everything preceding the delimiter "-" option. This token for the third part of the stream name is assigned the name equipment\_Id, the same name as in Tank Rule A.

**Note:** Use the same names for all of the tokens in both rules. This naming pattern makes it easier to manage the rules and troubleshoot any problems that may occur.

**Stream Name**

4. Match:  everything preceding the delimiter "-"  
 the next 1 numbers  
 the next group of numbers  
 the string literal "03"

and name it:

[Undo Capture](#) [Capture](#)

Set up the mappings and configure the asset as described in [Create an asset rule](#).

**Note:** The **Id** and **Name** for both rules must resolve to the same values to achieve the intended result, that is one asset that references both streams. If the IDs are different, then two assets with the name Philadelphia 03 are created, one that references the Pressure stream and the other that references the Temperature stream.

Be sure to configure the other asset fields, **Description** and **Metadata** the same in both rules.

The following is the asset preview of Tank Rule B which matches the PHI-Tank03-Temp stream for the Philadelphia Tank 03 asset.

<b>Id</b>	<b>Type</b>	<b>Name</b>	<b>Description</b>	<b>Temperature</b>
Philadelphia Tank 03	Boiler Tank	Tank 03	The Tank 03 is locate...	PHI-TNK03-Temp

Tank Rule A, applied to the streams in this example, creates three tanks with the Philadelphia Tank 03 missing the Temp measurement as shown below.

<b>Id</b>	<b>Type</b>	<b>Name</b>	<b>Description</b>	<b>Pressure</b>	<b>Temperature</b>
Philadelphia Tank 03	Boiler Tank	Tank 03	This Tank 03 is locat...	PHI-TNK01Press	
San Leandro Tank 01	Boiler Tank	Tank 01	This Tank 01 is locat...	SL-TNK01Press	SL-TNK01Temp
San Leandro Tank 02	Boiler Tank	Tank 02	This Tank 02 is locat...	SL-TNK02Press	SL-TNK02Temp

The two rules complement each other and both are required to create the three assets with stream references for pressure and temperature.

## Manage permissions for asset rules

If you are assigned the **Manage Permissions** access right, then you can configure asset rule permissions for other user roles in your tenant. You can granularly assign individual asset rule permissions to each user role.

### Prerequisites

To manage asset rules permissions, you must be assigned the **Manage Permissions** access right.

### To manage permissions for asset rules

1. From the left pane, select **Data Management > Asset Rules**.
2. Select an asset rule and choose **Manage Permissions**.  
The Manage Permissions for Asset Rule window opens.
3. Use the Manage Permissions for Asset Rule window to:
  - (Optional) Add user roles that have permissions on the asset rules.
  - Edit asset rules permissions for each user role.  
For more information, see [Permissions management](#).
4. When you are finished editing permissions, select **Save**.

### To manage default permissions for new asset rules

You can edit the default user roles and permissions added to a asset rule when it is created.

1. From the left pane, select **Data Management > Asset Rules**.
2. Select **More options :** > **Manage Default Permissions for New Rules**.
3. Use the Manage Default Permissions for New Asset Rules window to edit default user roles and stream permissions. For more information, see [Permissions management](#).

- When you are finished editing permissions, select **Save**.

## Change broker

Change broker is an Enterprise-scale egress capability for CONNECT data services. Update streaming is crucial to enterprise-scale analytics, data science, visualization, and integration. Operations data is always changing. The change broker helps you navigate live data, delayed uploads, late manual measurements, recalculations, and even rare occurrences of incorrect readings that require change data.

### Change Data

This feature solves both new and changing data issues, and can provide near real-time data. More specifically, change broker monitors changes to the streams' data values. The change data supported by the Signup includes the following capabilities: Update, Insert, Replace, Remove, and RemoveWindow. These are all write modes supported by Sequential Data Store (SDS). This capability serves both customers and partners for analytics, visualization/dashboarding, rules processing, evolving search indexes, anomaly detection, application providers, transaction processing, and digital service providers.

Change broker is designed to support the egress of millions of data events per second, retain the events for a period of time (1 hour), and serve that data to multiple, parallel consumers. A Signup is retained for 24 hours relative to the last query made. If a Signup is idle (without interaction) for 24 hours, it becomes Inactive from disuse and given an ExpiredDate. There is no known limitation on the size of data that can be held in a Signup during the one-hour expiration window.

### REST API

A REST consumer creates a "Signup" for change data from a defined list of Stream IDs in a namespace (for example, data from Stream1 through Stream10). Signups have a lifecycle which includes states such as Active (ready for use) and Inactive (abandoned). Consumers poll an active Signup to pull the change data via GET Updates, and with each response, receive a Bookmark for the next request.

Reading is not destructive, as with a queue. Reading data from your Signup advances your bookmark, but does not immediately delete the data in the Signup. The data will expire based on the expiration assigned to it. For example, an hour expiration from the activation of a Signup or most recent query.

Bookmarks are unique to a Signup. You cannot use bookmarks for more than one Signup.

To receive change data from streams in different namespaces (for example, MyTenant/MyNamespace and CommunityFriend/TheirNamespace), a Signup is made for each namespace.

### Application for the change broker

Some practical uses for change broker include:

- Data Science
  - Improves accuracy of algorithms by providing recent data
  - Simplifies integration that sends recent data to an algorithm
  - Supports reference architectures
- Remote Operations Monitoring

- Allows apps to retrieve near real-time data
- Reduces components customers must manage
- Standardizes how change data transfers to trusted business partners
- Maintenance & Risk Reduction
  - Near real-time data feeding alarm systems

## Disaster Recovery

In the event of an CONNECT data services service failure, we will initiate a recovery process in accordance with the Recovery Point Objective (RPO) and Recovery Time Objective (RTO) as defined in the [service description](#). This does not include change broker's Signups and associated change data as part of the recovery effort.

The reasons for the exclusion of change broker from disaster recovery are as follows:

- Change data is only available within a Signup for one hour, which is shorter than CONNECT data services's RPO. Therefore, even if a Signup were to be recovered, the change data would be expired and unavailable.
- During a service failure that also impacts data ingress and data storage, CONNECT data services will not capture change data.
- If data ingress was captured during change broker service failure, it will be available in Sequential Data Store.

## Change broker best practices

We recommend the following best practices when using change broker.

- Maximize the number of streams and data in a write operation:

When you leverage Open Message Format (OMF) for data collection, you are in control of how much data is written to a stream and how many streams are included in a single write operation. For the PI to CONNECT Agent, this is already automatically optimized and you cannot adjust this.

With minimal processing, change broker serves this write operation to the user or client querying a Signup. This means that if a stream has 10 timestamp-value pairs included in each write operation, then change broker will preserve this and serve the stream's data packet (referred in the JSON format as an "event") as a group of 10 timestamp-value pairs when a Signup is queried. Change broker is designed with minimal processing of the write operation to optimize for speed and throughput.

For more information on streams, read [Streams](#).

- Create, modify, and remove Signups iteratively if response times are too long:

For most scenarios, creating, modifying, and removing Signups concurrently should complete in less than a second. Within a namespace, as the number of data streams in a Signup and the number of Signups grow very large, durations for these actions to complete could become long and not meet the needs of some use cases. In these scenarios, we recommend you perform a set of, or all these actions, iteratively to help achieve the desired performance in lieu of performing the actions simultaneously.

- Maximize the number of streams per Signup to optimize performance:

Change broker was designed to handle a large number of streams in few Signups for each namespace. Tests showed that each namespace could support a few Signups of up to 100,000 streams per Signup. Although change broker is not yet explicitly designed to do so, many Signups (up to 100) with a few streams (up to 25) were also shown to be performant within a single namespace.

With performance, there are many factors at play such as data frequency within streams, write operation design, and query frequency of the Signup. If you are approaching or near the aforementioned test scenarios, contact [AVEVA customer support](#) for further guidance and details.

- Query on a schedule that optimizes the number of events returned and retrieval time:

Write operations for a stream are preserved by change broker. The grouping of data that is written to a stream in a single write operation is the same grouping when queried via a Signup. This is labeled in the Signup's /Update response as an "event" for a stream.

Change broker can return up to 100,000 events in a single query. To optimize performance, you should aim to have as many events as possible per query. You can increase your query cadence or adjust the Signup definition to include streams with higher data frequency so that your higher frequency queries have more events in each query.

- Ensure a Signup is queried within one hour of its previous query to ensure no change data is missed:

A bookmark is only valid for an hour. A bookmark is either created when the Signup's SignupState first becomes Active or when the Signup is queried via the /Update route. These two scenarios determine the start of the lifetime of a bookmark.

Although the Signup is available beyond one hour of inactivity (no queries to a bookmark defines inactivity), the bookmark will expire and will not have any change data queued for querying. You can create a new bookmark to start queuing change data once again as long as the Signup has not expired.

Your Signup is available for up to 24 hours of inactivity. After the 24-hour period, the Signup will not be retrievable and you will no longer be able to query for updates or modifying the Signup. The Signup's definition will remain viewable in the portal for several days once expired, unless deleted.

## Manage change broker stream data updates

You can use the API console to configure a Signup that collects data updates from a defined list of stream Id(s) of interest. This works with the Sequential Data Store (SDS). For more on SDS and streams, read [Sequential Data Store](#).

Follow the steps below to create a Signup, activate a Signup, and receive change data updates. Note that all three steps must be done in order.

For developer API documentation, read the [change broker API reference guide](#).

### Create a Signup

To sign up for data event updates from streams of interest, perform the following steps:

1. In the left pane, select **Developer Tools > API Console**.
2. Select **v1** in the Full Path dropdown selector.
3. Select **POST** in the Verb dropdown selector.

The **POST** button appears.

4. In the URI field, type `/` at the end of the existing text, then select your desired Namespace. Then, type `/Signups` to go to the Signups endpoint.
5. Insert body text. There are two options:
  - Select the **Insert Signup Template** button. This will generate a Signup template for you. Define the name of the Signup and add the stream Id(s) in the Resourcelds field.

- Paste the body text in the Body field. You should include the name of your Signup in the Name field, the resource type in the ResourceType field (currently, Stream is the only ResourceType supported by change broker), and the stream Id(s) in the ResourceIds field. See below for an example:

```
{  
  "Name": "<resource name>",  
  "ResourceType": "Stream",  
  "ResourceIds": [  
    "<resource Id>"  
  ]  
}
```

For more information on the Signups API, read the Signups topic in API reference.

#### 6. Select the **POST** button.

You should receive output containing a Signup Id and a SignupState of Activating.

```
{  
  "Id": "<GUID>",  
  "Name": "<resource name>",  
  "Owner": {  
    "Type": "User",  
    "ObjectId": "<GUID>",  
    "TenantId": "<GUID>"  
  },  
  "CommunityId": "",  
  "Type": "Stream",  
  "CreatedDate": "2019-08-24T14:15:22Z",  
  "ModifiedDate": "2019-08-24T14:15:22Z",  
  "SignupState": "Activating"  
}
```

## Activate a Signup

To activate stream updates, perform the following steps:

- Copy the Id provided in the previous output.
- Select **GET** in the Verb dropdown selector.  
The **GET** button appears.
- In the URI field, type / at the end of the existing text, then paste in your Id.
- Select the **GET** button.

A SignupState of Active appears in the output. This indicates that change data is being collected for the Streams in the Signup. A bookmark also appears in the output.

```
{  
  "bookmark": "<GUID>",  
  "Id": "<GUID>",  
  "Name": "<resource name>",  
  "Owner": {  
    "Type": 1,  
    "ObjectId": "<GUID>",  
    "TenantId": "<GUID>"  
  },  
  "CommunityId": "<GUID>",  
  "Type": "Stream",  
  "CreatedDate": "2019-08-24T14:15:22Z",  
  "ModifiedDate": "2019-08-24T14:15:22Z",  
  "SignupState": "Active",  
  "Status": "Success",  
  "Message": ""  
}
```

```
"CreatedDate": "2019-08-24T14:15:22Z",
"ModifiedDate": "2019-08-24T14:15:22Z",
"SignupState": "Active"
}
```

5. Copy the bookmark to receive change data updates.

Bookmarks are a unique identifier to a Signup and cannot be used for multiple Signups.

## Receive change data updates

To receive stream updates, perform the following steps:

1. Copy the bookmark from the GET Signup endpoint body.
2. In the URI field, delete /Resources and type /Updates.
3. Paste your bookmark in the Parameters field of the API console.
4. Select the **GET** button.

The stream updates appear in the output.

```
{
  "data": [
    {
      "resourceId": "<resource Id>",
      "operation": "Update",
      "events": [
        {
          "Timestamp": "<timestamp>",
          "Value": <GUID>
        }
      ]
    }
  ],
  "bookmark": "<GUID>"
}
```

You will now receive data event updates via the Change Data Broker. You must use the provided bookmark in this output in the next /Updates call to receive the next set of change data.

## (Optional) View accessible resources

Tenant admins can view all Signups created by users in the tenant. However, only the Signup owner is able to query a Signup.

To view the streams that are accessible for data event updates, perform the following steps:

1. In the URI field, type /Resources after your Id.
2. Select **GET**.

The AccessibleResources and InaccessibleResources appear in the output.

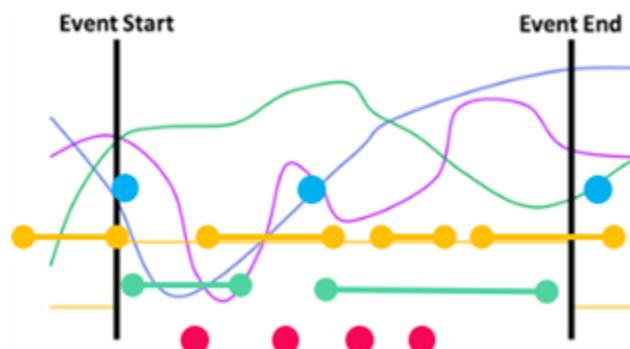
```
{
  "resources": [
    {
      "resourceId": "Value",
      "type": "Accessible"
    }
  ]
}
```

```
"isAccessible": false
}
]
}
```

## Events

Events capture meaningful observations at a specific point-in-time, or over a span of time, and can be used to model transactional data from a Manufacturing Execution System or Batch Execution System, equipment utilization data, equipment startups and shutdowns, shifts, or process excursions like high temperature events.

Events can help put process data into a business context. You can think of events as bookmarks for your process data, helping to shorten the time to insight.



Some of the questions you can answer by having event context are:

- What was my process doing during the event?
- What was the maximum temperature of my equipment during the event?
- What happened leading up to the event or after the event?

You can look across events and ask:

- Which types of events are occurring most frequently?
- When did my wind turbines have a fault in the past month?
- What was the temperature for my last 30 batches?

Events can be queried, created, modified, and deleted through the REST API and GraphQL API.

## Reference data

Reference data captures master data and additional metadata to add context to events. You can use reference data to model data such as material definitions, products, alarm severity categories, or downtime reasons that can be referenced in the context of an event to provide useful additional context when data is consumed, analyzed, visualized, and reported on.

Reference data can be queried, created, modified, and deleted through the REST API and GraphQL API.

## Benefits of event data

Value provided by events:

- Events make it easier to analyze an occurrence, and easier to find related data to the event.
- Production performance and quality can be analyzed across sites, making reporting easier.
- Events provide a clearer picture of processes.
- Events allow you to view your time-series data in a meaningful way.

There is also great value in having multisite data centralized across the enterprise and more accessible to a greater number of users and applications in the cloud. Having event data on a cloud platform offers advantages such as:

- Analytics are easier to facilitate with cloud-based data science and machine learning tools.
- The cloud provides a single place for you to aggregate data so partner applications can leverage it.
- The data is easier to share with your trusted business partners from the cloud.
- The cloud is designed to naturally scale to handle events across your enterprise.

## Model events and reference data

Events and reference data can be used to model simple events like process excursions or complex events like production data from a Manufacturing Execution System.

### Types

Event Types and Reference Data Types are templates for creating events or reference data that share a common structure. When you create a type, you define the metadata and relationships for events or reference data created from that type. All events and reference data must be created from a type.

All event and reference data types include the following common set of properties:

- id
- name
- description
- createdDate
- modifiedDate
- createdByUser
- authorizationTags

Event types also include additional common properties that are specific to event data:

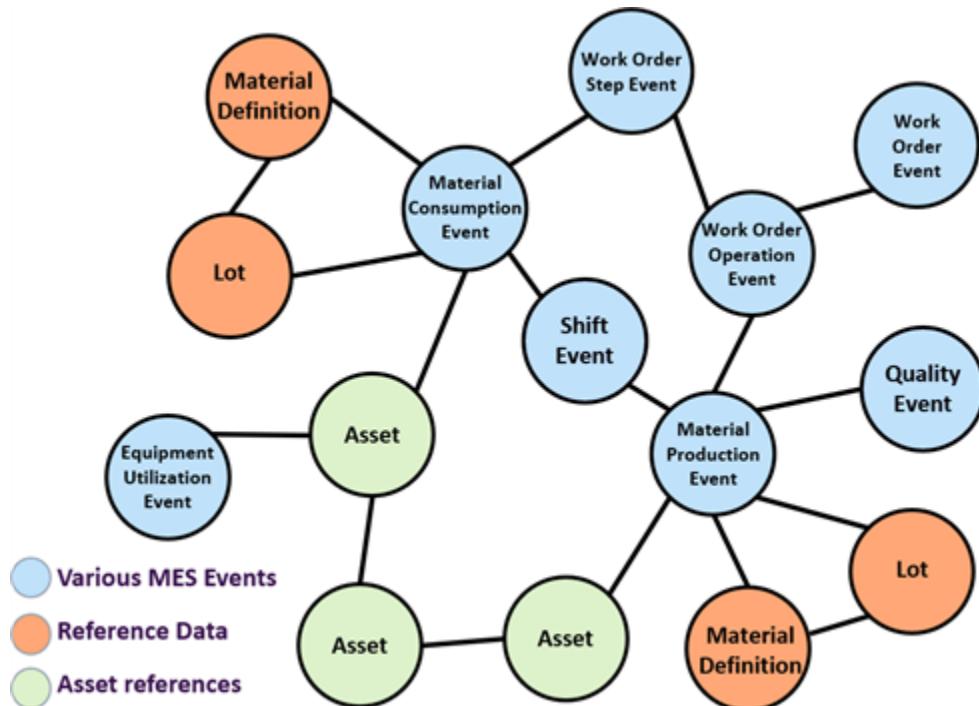
- startTime
- endTime
- duration

- state
- asset

When you create an Event Type or Reference Data Type, you can define additional properties to capture data specific to events and reference data.

Properties can also be configured to model flexible relationships that point to other events or reference data or assets. Any event property can be configured to reference another event, reference data, or asset. In this way you can model the unique relationships in your data.

The diagram below gives an example of how you can model complex data using relationships between different types of events, reference data, and assets.



## Manage permissions for events and reference data

You can manage permissions to view and edit events and reference data using authorization tags. Each event and reference data item contains a list of authorization tags. By controlling access to the authorization tags, you can manage permissions to events in bulk without modifying the permissions to each individual event.

You grant permissions to authorization tags based on user roles. A user can access events or reference data items for all the authorization tags to which their user role has access. If a user has multiple roles, access for each role is independent.

You can configure each Event Type and Reference Data Type with a default authorization tag that applies to every event or reference data item of that type.

The `BaseAuthorizationTag` is a special authorization tag that applies to all events and reference data and can override other authorization tags. Assigning permissions to the `BaseAuthorizationTag` can be used to give a role read access to all events and reference data or to provide admin-level access.

## Prepare CONNECT data services to use events

The basic steps to begin using event data in CONNECT data services are:

- Create a set of Event Types, which are definitions for domain-specific events and surrounding metadata, using the Event Type Store REST APIs. See [Event Types](#).

- Create a set of Reference Data Types to add contextual data and information. See [Reference Data Types](#).

Code examples for Event Types and Reference Data Types can be found in [Event Type Store and GraphQL API usage examples](#). For AVEVA MES and AVEVA Advanced Analytics users these types will be created automatically.

- Write events and reference data to CONNECT data services using the GraphQL or REST APIs, the [AVEVA Events to CONNECT agent](#), or AVEVA Advanced Analytics.

The AVEVA Events to CONNECT agent runs on premises and polls sources like AVEVA MES for data. It supports writing Assets, Events, Reference Data and Enumerations to CONNECT data services in realtime as well as historical data.

- Use the [GraphQL console](#) to create complex queries or mutations for your data.

Our GraphQL API allows customers, developers, and partners to build complex queries that leverage information between related events and reference data. The GraphQL API Console allows you to explore the schemas for your specific event and reference data types.

You can use the UI to visually build your query by selecting what properties you want to return, specifying where conditions, aggregating data, and other features. You can then copy the queries into your code and other tools.

## Integrate events with AVEVA Advanced Analytics

Events in CONNECT data services are integrated with AVEVA Advanced Analytics.

AVEVA Advanced Analytics is a no-code analytics product where you can perform calculations and build analytics models including machine learning to glean new insights from your data.

AVEVA Advanced Analytics can read data from streams, assets, and events to feed analytics models for use cases like predictive quality, predictive throughput, and predictive energy efficiency.

With AVEVA Advanced Analytics, you can also generate events based on your analytics models and process data.

# Data collection

The Data Collection menu provides a number of methods for collecting data from external sources to bring into CONNECT data services:

- Use Edge Data Store & Adapters to monitor the health and manage the software configuration on systems.
- Use PI Agents to set up a transfer of data from an on-premises PI Server to CONNECT data services or from CONNECT data services to a PI Server. PI to CONNECT maps Data Archive points to SDS types and streams. CONNECT to PI transfers data from SDS streams to a Data Archive.
- Use OMF Connections to pass JSON messages to CONNECT data services using an HTTP client. OMF is a platform-independent format that can provide a high-throughput data feed into CONNECT data services.

For a full list of data ingress sources for CONNECT data services, see [Data ingress sources](#).

## Data ingress sources

The following is a list of the current ways of ingressing industrial data into CONNECT data services:

### Edge Data Store & Adapters

- [Edge Data Store](#)
- [AVEVA Adapter for Azure Event Hubs](#)
- [AVEVA Adapter for BACnet](#)
- [AVEVA Adapter for DNP3](#)
- [AVEVA Adapter for Modbus TCP](#)
- [AVEVA Adapter for MQTT](#)
- [AVEVA Adapter for OPC UA](#)
- [AVEVA Adapter for RDBMS](#)
- [AVEVA Adapter for Structured Data Files](#)
- [Client Failover Service](#) (for adapter-level health data)

### PI System

- [PI to CONNECT Agents](#)
- [CONNECT to PI Agents](#) (egress data from CONNECT to the PI System)

### System Platform & AVEVA Historian

- [AVEVA Historian](#)

## AVEVA MES

- AVEVA MES cloud integration
- AVEVA Events to CONNECT agent

## AVEVA Production Management

- AVEVA Events to CONNECT agent

## Custom Open Message Format (OMF) applications

- Open Message Format (OMF)
- OMF connections

# Edge Data Store & Adapters

CONNECT data services provides a centralized location to monitor the health and manage the software configuration of edge modules and systems, including Edge Data Store and AVEVA Adapters. This shows you the data collection software that deploys to remote devices. To be available in CONNECT data services, a system must have an CONNECT data services health endpoint configured. For information on configuring health endpoints, see the specific system product documentation.

Systems have product executables that you install on devices in the field. Use Edge Data Store & Adapters to create configuration files that you then deploy directly on those devices.

Edge modules have the same functionality as their corresponding systems, but are deployed and managed through AVEVA Edge Management. Edge modules operate in Alpine Linux containers on devices. Each edge module deployment includes the container OS, the system, and its configuration files. For details, see the [AVEVA Edge Management](#) documentation.

## Health monitoring

The Edge Data Store & Adapters Systems page displays a list of system digital twins. Each system twin is a virtual representation of an actual system that is currently writing health data to the selected namespace. You can review health information for systems, including the current status of each system and when it last communicated with CONNECT data services. Use sort and filter functionality to navigate system twins to pinpoint problems and identify gaps in data collection. View detailed health information for your systems to understand their overall health.

## Configuration management

Use the Edge Data Store & Adapters Systems page to review detailed information about each system, its components, and its configurations. You can also manage, create, and edit system software configurations.

Use the Edge Data Store & Adapters Configuration Templates page to create and maintain a collection of configuration templates that you can apply to systems. Create each configuration template from either a default configuration or an imported configuration. Then modify configurations using the portal's built-in editor, which identifies formatting errors as you work, helping you avoid problems later. Export a configuration template to

manually apply it to a physical system in the field or to deploy it using AVEVA Edge Management. For more information, see the [AVEVA Edge Management](#) documentation.

In the field, you may need to customize a configuration template for a specific system. Once a system configuration is complete and it is writing data to health data to CONNECT data services, the Edge Data Store & Adapters page shows its corresponding system twin. To store, review, and access configurations from a central location, import the actual configurations from the field to the corresponding system twins.

## View and monitor a system

You can view and monitor the health status and configuration information for systems, including Edge Data Store and PI Adapters, for a selected namespace. You can filter and sort the list of edge devices, and open a trend displaying diagnostic data for a specific device or component.

---

**Note:** A system appears on the Edge Data Store & Adapters Systems page once it is writing health data to CONNECT data services. For information on configuring health endpoints, see the specific system product documentation.

---

### View a system

1. From the left pane, select **Data Collection > Edge Data Store & Adapters**.
2. Verify that the **Systems/Configuration Templates** selector is set to **Systems**.
3. (Optional) To sort by a column in descending order, select the column header. To sort in ascending order, select the header again.
4. (Optional) To filter the edge systems shown based on **Status**, **Type**, or **Tags**, use the checkboxes on the left. For more information on edge system statuses, see [System status definitions](#).
5. (Optional) To search for specific systems, select the **Search for Systems** search bar. The search function provides examples for filtering by criteria such as device name, status, version, and tags. For more information, read [Search queries](#).
6. To open the right pane that displays information for a device, select the device.
7. To see the system installed on the device and the configured components, select the **Details** tab.
8. To review the configuration details, select the **Configuration** tab.
9. To open a trend showing diagnostic data in a new window, select **More Options**  in the **System Details** pane and select the  **Open in Trend** icon.

The level where you select the icon determines what data is included:

- To see all available diagnostic data for the device, select the icon at the top level.
- To see the diagnostic data available for a specific system, select the icon at the system level.
- To see the diagnostic data available for a specific component, select the icon at the component level.

### Hide a system

If you no longer want to monitor a system, you can hide systems from the list in CONNECT data services.

1. In the left pane, select **Data Collection > Edge Data Store & Adapters**.
2. Verify that the **Systems/Configuration Templates** selector is set to **Systems**.
3. Find and select the edge device to hide.

4. Select **More Options**  in the **System Details** pane, and select **Hide**.
5. To confirm removing the selected system from the list, select **Hide**.

### Unhide a system

1. In the left pane, select **Data Collection > Edge Data Store & Adapters**.
2. Verify that the **Systems/Configuration Templates** selector is set to **Systems**.
3. In the filters pane, find **Visibility** and select **Show hidden systems**.
4. Find and select the edge device to unhide.
5. Select **More Options**  in the **System Details** pane, and select **Unhide**.
6. To confirm restoring the selected system from the list, select **Unhide**.

To remove a system completely, remove the corresponding health asset. See [Remove assets](#) for more information on how to remove an asset.

### Video Tutorial: View, monitor, and hide a system in CONNECT data services

[https://player.vimeo.com/video/901610515?badge=0&autoplay=0&player\\_id=0&app\\_id=58479](https://player.vimeo.com/video/901610515?badge=0&autoplay=0&player_id=0&app_id=58479)

#### [Video Transcript \(Select to expand\)](#)

This video shows you how to view, monitor, and hide a system in AVEVA Data Hub.

Open AVEVA Date Hub, select Data Collection from the lefthand navigation and then select Edge Data Store and Adapters.

Verify that the Systems/Configuration Templates selector is set to Systems.

From the Systems view, you can sort, filter, and search for specific systems.

Select a system to view more information in a new pane on the right side of the screen. Select the details tab to see more information.

To review the configuration details, select the configuration tab.

From the configuration tab, you can select the trend icon to view diagnostic data for devices, systems, and components.

To hide a system, select the more options button and then select "Hide." Confirm your choice by selecting the "Hide" button.

To unhide a system, select "Show Hidden Systems," select the system you want to unhide, select the more options button, and then select "Unhide." Confirm your choice by selecting the "Unhide" button.

## System status definitions

The following table lists the system status definitions for systems in CONNECT data services.

Status	Meaning
Good	The system is connected to the data source and it is collecting data.
Starting	The system is currently in the process of starting up and is not yet connected to the data source.
Attempting Failover	The system is switching to the standby server due to failure or scheduled downtime.
Connected / No Data	The system is connected to the data source but it is not receiving data from it.
Not Configured	The system is created but not yet configured.
Server Error	The system encountered an error either while connecting to the data source or attempting to collect data.
Unknown	The system is experiencing an unknown connection error.
Device in error	The system encountered an error either while connecting to the data source or attempting to collect data.
Removed	The system has been removed and will no longer collect data.
Shutdown	The system is either in the process of shutting down or has finished.

## Add and edit configuration templates

You can create and edit configuration templates for systems in CONNECT data services. Once the configuration is

complete, export the configuration in a text file to manually apply it to the system in the field or to deploy it to the edge module using AVEVA Edge Management. You can also use an exported configuration text file as a template for configuring other systems by importing it. Default configurations are available for supported system types. The maximum size for a configuration file is 16 MB.

You can create configuration templates for the following system types:

- AVEVA Adapter for Azure Event Hubs
- AVEVA Adapter for BACnet
- AVEVA Adapter for DNP3
- AVEVA Adapter for Azure Event Hubs
- AVEVA Adapter for BACnet
- AVEVA Adapter for DNP3
- Edge Data Store
- AVEVA Adapter for Modbus TCP
- AVEVA Adapter for MQTT
- AVEVA Adapter for OPC UA
- AVEVA Adapter for RDBMS
- AVEVA Adapter for Structured Data Files

---

**Note:** You can only deploy edge modules using AVEVA Edge Management.

---

The *namespaceId* in the data and health endpoint URLs defaults to the namespace where the configuration template is created. For example, if the namespace of the configuration template is *MyData*, the endpoint URL would be <https://website.com/api/v1/Tenants/{tenantId}/Namespaces/MyData/0mf>.

## Edge module configuration

For edge modules, use variables to denote secrets in configuration files. Variables must be used within the configuration file in place of actual secret and password values. Use the following variables as required for your specific configuration:

- {{EgressEndpointSecret}} – Use this variable for the secret or password value to connect to the egress endpoint. When sending data to CONNECT data services, use this variable in place of the client secret. When sending data to PI Web API, use this variable in place of the password.
- {{AdditionalEgressEndpointSecret}} – Use this variable when egressing data to more than one endpoint, when the other endpoint requires a different secret or password.
- {{DataSourceSecret}} – Use this variable in place of a data source password when the data source you are connecting to requires a password in order to connect.
- {{AdditionalDataSourceSecret}} – Use this variable when connecting to more than one data source, when the other data source requires a different password in order to connect.

When you deploy the configuration in AVEVA Edge Management, you define values for the variables and securely transfer those values to the device. For more information, see [Deploy a system module](#).

## Add a new configuration template

To create a system configuration template and export it for use:

1. In the left pane, select **Data Collection > Edge Data Store & Adapters**.
2. Verify that the **Systems/Configuration Templates** selector is set to **Configuration Templates**.
3. Select **New Configuration Template**.
4. In the **Configuration Template Name** field, enter a name to identify the configuration.
5. In the **Type** and **Version** fields, select the system type and version for which to create the configuration.  
The default configuration for the selected system type displays.
6. To import a configuration, select **Import Configuration**, then browse to the JSON file that contains the configuration, and select **Import**.
7. (Optional) In the **Section Select** dropdown list, select the section of the configuration to modify. The default option of **JSON Configuration** shows the entire configuration.
8. Modify the JSON as needed. For configuration guidelines, refer to the specific system documentation.

---

**Warning:** For security reasons, do not include secrets in the configuration. Secrets cannot be stored or exported in a configuration. For edge modules, variables must be used within the configuration file in place of actual secret and password values. For more details, see the [Configure a Module](#) topic in the AVEVA Edge Management documentation.

---

Errors in the JSON syntax are underlined. To see an explanation of the issue, hold the mouse over the underlined text. The overall status of the JSON syntax is displayed over the right pane.

9. To export the completed configuration, do one of the following:
  - To export just the selected section, select **Export Section** in the right pane.
  - To export the entire configuration in one file, select **Export Configuration**.  
The JSON file is downloaded to your browser.
10. When you have finished, select **Save & Close**.
11. Select **Save & Close** to confirm the changes.

## Video Tutorial: Add configuration templates in CONNECT data services

[https://player.vimeo.com/video/1008581723?badge=0&autoplay=0&player\\_id=0&app\\_id=58479](https://player.vimeo.com/video/1008581723?badge=0&autoplay=0&player_id=0&app_id=58479)

Video transcript (Select to expand)

This video shows you how to add a configuration template in CONNECT data services.

Open CONNECT data services, select Data Collection from the lefthand navigation, and then select Edge Data Store and Adapters.

Set the Systems/Configuration Templates selector to Configuration Templates.

To add a new configuration template, select the Add Configuration Template button.

Enter a name in the Name field. You also have the option to add a description. You should choose a name that you can easily remember and filter for later. Then, select the relevant product type and version from the drop-down menus to get the corresponding configuration template.

Select Next.

A default JSON configuration is provided. You can either edit this file or import a custom configuration JSON file.

To import a custom JSON, select the more options button and then select Import Configuration.

Resolve any errors detected in your JSON file by selecting the View Errors button. After resolving the errors, select Save and Close to create your configuration template. Confirm your choice and select Create and Close. Your template has been added to CONNECT data services.

## Edit an existing configuration template

To modify a configuration template and export it for use:

1. In the left pane, select **Data Collection > Edge Data Store & Adapters**.
2. Verify that the **Systems/Configuration Templates** selector is set to **Configuration Templates**.
3. Find and select the configuration template to modify.

4. (Optional) To search for specific configuration templates, select the **Search for Configuration Templates** search bar. The search function provides examples for filtering by criteria such as device name and version. For more information, read [Search queries](#).
5. In the right pane, select the edit icon .
6. Modify the configuration template name, **Type**, and **Version** as needed.
7. (Optional) In the **Section Select** dropdown list, select the section of the configuration to modify. The default option of **JSON Configuration** shows the entire configuration.
8. Modify the JSON as needed. For configuration guidelines, refer to the specific system documentation.

**Warning:** For security reasons, do not include secrets or passwords in the configuration. Secrets and passwords cannot be stored or exported in a configuration. Client secrets and passwords must be applied directly on the device. For edge modules, variables must be used within the configuration file in place of actual secret and password values. For more details, see the [Configure a Module](#) topic in the AVEVA Edge Management documentation

Errors in the JSON syntax are underlined. To see an explanation of the issue, hold the mouse over the underlined text. The overall status of the JSON syntax is displayed over the right pane.

9. To export the completed configuration, do one of the following:
  - To export just the selected section, select **Export Section** in the right pane.
  - To export the entire configuration in one file, select **Export Configuration**.

The JSON file is downloaded to your browser.

10. When you have finished, select **Save & Close**.
11. To confirm the changes, select **Save & Close**.

## Deploy a system configuration

After you export a system configuration, you have to manually deploy the configuration to the edge device in the field.

For details on how to deploy a configuration, see the specific system product documentation:

- [AVEVA Adapter for Azure Event Hubs](#)
- [AVEVA Adapter for BACnet](#)
- [AVEVA Adapter for DNP3](#)
- [Edge Data Store](#)
- [AVEVA Adapter for Modbus TCP](#)
- [AVEVA Adapter for MQTT](#)
- [AVEVA Adapter for OPC UA](#)
- [AVEVA Adapter for RDBMS](#)
- [AVEVA Adapter for Structured Data Files](#)

After deploying the configuration, manually update the configuration file on the device to replace any mustache tokens used as place holders for secrets with the actual secrets. Then, to have an accurate record of the configuration, import the configuration file, including any modifications made in the field except secrets, to the corresponding system twin in CONNECT data services.

## Data source scenarios

If you need to access multiple data sources on the same device, you need to differentiate the data sources. You can use the following options to identify the data sources:

- Static IP address
- Fully qualified device name

We recommend you review your specific scenario with your network administrator to determine the appropriate configuration for your use case.

## Deploy a system module

After you export a system module configuration, use AVEVA Edge Management to add the configuration to the module and deploy it to edge devices in the field. For details on how to configure and deploy an edge module, see the [AVEVA Edge Management](#) documentation.

For modules that require secrets, use secret variables and the secret store to complete the secure transfer of secret values. Enter secret variables in configuration files as placeholders for the actual secrets and passwords. Complete the secret store configuration in AVEVA Edge Management to define values for the secret variables. AVEVA Edge Management encrypts the values and provides the `Setup module secret` command. After you deploy the module configuration, run the `Setup module secret` command in a Linux terminal on the device to replace the secret variables with the encrypted values.

After deploying the configuration, import the configuration file, including any modifications made in the field, to the corresponding system twin in CONNECT data services. This provides an accurate record of the configuration.

## Manage system configurations

You can import a system configuration from the field to its corresponding system digital twin as a record. You can also create a new configuration, using a default configuration or a configuration template. Once the configuration is complete, you can export the configuration file for each component or for the system. You can use an exported configuration file to configure other systems by importing it. The maximum size for a configuration file is 16 MB.

Configuration is available for the following system types:

- AVEVA Adapter for Azure Event Hubs
- AVEVA Adapter for BACnet
- AVEVA Adapter for DNP3
- Edge Data Store
- AVEVA Adapter for Modbus TCP
- AVEVA Adapter for MQTT
- AVEVA Adapter for OPC UA
- AVEVA Adapter for RDBMS
- AVEVA Adapter for Structured Data Files

The namespaceId in the data and health endpoint URLs defaults to the namespace where the configuration template is created. For example, if the namespace of the configuration template is MyData, the endpoint URL would be <https://website.com/api/v1/Tenants/{tenantId}/Namespaces/MyData/Omf>.

A system appears on the Edge Data Store & Adapters Systems page once it is writing health data to CONNECT data services. For information on configuring health endpoints, see the specific system product documentation at [docs.aveva.com](https://docs.aveva.com).

For systems, use mustache tokens, in the format {{SecretA}}, to denote secrets in configuration files. Secrets are managed using clients. The token name must match an Edge Management System property defined for the system. Tokens must be used in fields where isEncrypted=true. After deploying the configuration to the device, you must manually update the configuration on the device with the secret.

For edge modules, use variables, in the format {{VariableA}}, to denote secrets in configuration files. The variable is associated with a secret in AVEVA Edge Management.

## Import a system configuration

To import a system configuration from the field to the corresponding system digital twin:

1. In the left pane, select **Data Collection > Edge Data Store & Adapters**.
2. Verify that the **Systems/Configuration Templates** selector is set to **Systems**.
3. Find and select the system to configure.
4. In the right pane, select **Edit System** .
5. Select **Import Configuration**.
6. In the Import Configuration window, choose **Select file**, browse to the configuration file to import, and then select **Open**.
7. Select **Import**.
8. Review the imported file to ensure the contents are correct.
9. When you have finished, select **Save & Close**.
10. To confirm the changes, select **Save & Close**.

## Copy a configuration from a configuration template

To copy a system configuration from a template to the corresponding system digital twin:

1. In the left pane, select **Data Collection > Edge Data Store & Adapters**.
2. Verify that the **Systems/Configuration Templates** selector is set to **Systems**.
3. Find and select the system to configure.
4. In the right pane, select **Edit System** .
5. Select **Copy From Configuration Template**.
6. Use the **Filter Templates** search bar to find the configuration template you want to apply to your system.
  - You can filter by configuration template name, description, or version number.
  - Select **Edit Configuration Template** to edit a configuration template before you apply it to a system.
7. Select the configuration template you want to apply to a system.

8. To confirm the changes, select **Save and Close**.

## Edit a system

To edit a system configuration and export it for use:

1. In the left pane, select **Data Collection > Edge Data Store & Adapters**.
2. Verify that the **Systems/Configuration Templates** selector is set to **Systems**.
3. Find and select the system to configure.
4. In the right pane, select **Edit System** .
5. To manage the tags for a system, select **Add Tag**  and then do the following:
  - To add a tag, enter the tag text in the **New Tag** field and press Enter.
  - To delete a tag, select  in the tag bubble.
6. To set the configuration, do one of the following:
  - To use a configuration template, select **Copy From Configuration Template**.
  - To select a JSON file that contains the configuration, select **Import Configuration**.
7. (Optional) In the **Section Select** dropdown list, select the section of the configuration to modify. The default option of **JSON Configuration** shows the entire configuration.
8. Modify the JSON as needed. For configuration guidelines, refer to the specific system documentation.

---

**Warning:** Do not include secrets in the configuration. Secrets cannot be stored or exported in a configuration.

---

Errors in the JSON syntax are underlined. To see an explanation of the issue, hover over the underlined text. The overall status of the JSON syntax is displayed over the right pane.

9. To export the completed configuration, do one of the following:
  - To export just the selected section, select **Export Section** in the right pane.
  - To export the entire configuration in one file, select **Export Configuration**.

The JSON file downloads to your browser.

10. When you have finished, select **Save & Close**.
11. To confirm the changes, select **Save & Close**.

## PI agents

PI Agents allow you to transfer time-series data between CONNECT data services and PI Servers.

- PI to CONNECT enables you to transfer on-premises data from Data Archive and Asset Framework (AF) to CONNECT data services.
- CONNECT to PI enables you to send data from CONNECT data services streams to PI Server tags in an on-premises Data Archive.

## PI to CONNECT Agents

**Note:** PI to Data Hub is now known as PI to CONNECT, which is how it is shown within CONNECT data services. However, until the next release of the installation kit, the installable agent service and configuration utility will reflect the previous name. This documentation uses PI to CONNECT except for procedures and troubleshooting information that refer to the installation kit and configuration utility.

PI to CONNECT enables you to transfer on-premises data from Data Archive and Asset Framework (AF) to CONNECT data services. PI to CONNECT also enables AVEVA PI Data Infrastructure – aggregate tag licensing model. With this licensing option, customers no longer need to worry about accurately estimating the count of PI tags needed at every PI Server installation. Instead, they can purchase PI tags in aggregate and be able to use more than the committed number of aggregate tags across any number of deployed PI Servers. A PI to CONNECT Agent is required with every PI Server that is part of the aggregate tag model. The aggregate tag model is offered at three tiers of small (100,000 tags), medium (250,000 tags), and large (500,000 tags). These sizes denote the minimum number of aggregate tags to which a customer commits. At any time, the aggregate PI Server tag count may surpass this minimum number, and the customer will be able to pay for the additional tags on a daily rate.

### PI to CONNECT architecture

PI to CONNECT enables you to use one PI to CONNECT Agent to connect and transfer your on-premises data to CONNECT data services from one Data Archive and one optional Asset Framework (AF) server. The PI to CONNECT Agent creates and sends a transfer that contains the requested PI point data (metadata and PI events) and assets (AF elements and attributes) to CONNECT data services. The transfer and all communication are encrypted with HTTPS. For customers on AVEVA PI Data Infrastructure - aggregate tag, the PI to CONNECT Agent sends license usage information from the connected Data Archive to CONNECT data services.

### Restrictions of PI to CONNECT architecture

These are some restrictions to the PI to CONNECT architecture:

- The connecting AF server must reference the connected Data Archive. The list of available Data Archive servers is based on what servers are referenced by the AF elements selected in your transfer.
- Only one PI to CONNECT Agent can be installed on a given host computer.
- For a given namespace, only a single PI to CONNECT Agent is allowed to transfer data from a given Data Archive. Attempting to register a second agent from a different host computer against the same Data Archive will fail. This restriction is intended to prevent excess load on a given Data Archive. One workaround for this restriction is to configure a transfer to a different namespace. Consider, however, that agents on different machines do not coordinate data collection, potentially causing more archives to be pulled into memory than if the same number of PI points were transferred with a single agent.
- Open Id Connect (OIDC) is currently not supported for PI to CONNECT Agent connections to Data Archive or AF server.

See also [Limitations of PI to CONNECT](#).

### PI to CONNECT best practices

- Windows integrated security is recommended for connections to Data Archive. Alternatives, such as local

Windows Accounts or PI trusts, can be used but they are not as secure as using Active Directory on a Windows Domain. For remote connections to Data Archive, using a dedicated domain account as the Run As user for the PI to CONNECT Agent service provides the finest granularity. The PI to Data Hub Agent Configuration Utility can configure PI mappings to Data Archive. If you want to use a different security mechanism, such as PI trusts, you can use a different tool to configure the PI trusts, such as PI System Management Tools. When OIDC connections are supported by the PI to CONNECT Agent, OIDC will provide a secure alternative to Windows integrated security.

- For heavy workloads, install the PI to CONNECT Agent on a host computer that is separate from the Data Archive deployment.
- We advise against installing the PI to CONNECT Agent on test or ancillary PI Servers that are licensed with the aggregate tag model, or their usage will be reported and count against your aggregate tag tier.
- Keep the PI to CONNECT Agent software version up-to-date. The portal indicates when an agent is out of date and needs to be updated.
- Turn off compression only for PI points that do not update often. Turning compression off on a PI point instructs PI to CONNECT to collect the snapshot value rather than the most recently archived value for that PI point. If compression is left on for tags that update infrequently, there may be long delays before seeing data in CONNECT data services.

## Set up PI to CONNECT Agent

The PI to CONNECT Agent setup occurs prior to data transfer and involves temporarily disabling Internet Explorer enhanced security, downloading and installing the PI to CONNECT Agent, and connecting to data sources.

### Downloading the Agent Setup Kit

There are two options for downloading and installing the PI to CONNECT Agent setup kit.

#### Direct download option

You can download the setup kit from the PI Agents page on the portal and then transfer it to the computer that will host the agent.

#### PI Server installation kit option

The agent is available as an individual feature in the PI Server installation kit in PI Server 2023 and greater. When you select the PI to CONNECT feature for installation, the PI Server setup kit downloads and installs the latest version of the agent setup kit from the portal.

Be aware that, for a new installation, when you select the Data Archive server role, the individual agent feature is also selected by default. If you are planning on transferring a large amount of data, you can choose to deselect this feature and install the agent on a separate host computer from Data Archive, as per the "heavy workloads recommendation" mentioned in [PI to CONNECT Agents](#) best practices.

### PI to CONNECT minimum system requirements

The following table lists the system requirements of PI to CONNECT.

System component	Requirement
PI Server	<ul style="list-style-type: none"><li>• Minimum version: Data Archive 2016 R2. For full support of PI to CONNECT features, use Data Archive 2017 R2 or later.</li><li>• PI AF 2017 R2 or later</li></ul> <p><b>Note:</b> PI AF is only required if you wish to connect to an AF server.</p>
Operating system	<ul style="list-style-type: none"><li>• Windows 10, Windows 11, Windows Server 2016, Windows Server 2019, or Windows Server 2022 CORE editions of the Windows Server operating systems are supported with silent installations.</li><li>• Processor: 1 gigahertz (GHz) or faster compatible processor or System on a Chip (SoC)</li><li>• RAM: 4GB</li><li>• Hard drive size: 32GB or larger hard disk</li></ul>
Network	<ul style="list-style-type: none"><li>• An Internet connection that allows outbound connections over port 443 for communication with CONNECT data services.</li><li>• If the agent is installed on a computer other than the Data Archive, an Internet connection that allows outbound connections over port 5450 for communication with the Data Archive.</li><li>• If the agent is installed on a computer other than the AF Server, an Internet connection that allows outbound connections over port 5457 for communication with the AF Server.</li><li>• Internet connectivity of at least 10 Mbps.</li></ul>
Specific PI to CONNECT features	<ul style="list-style-type: none"><li>• Transfer out of order (OOO) events: Data Archive 2017 R2 or later and PI AF 2017 R2 or later</li></ul>

## Administrator privileges

Privileges	Requirement
Installation privileges	To install a PI to CONNECT Agent, you must be an administrator on the agent host computer.
Configuration privileges	To configure a PI to CONNECT Agent after the installation is complete, you must have the Tenant Administrator role in CONNECT data services. For silent installations, you have the option to create the requisite client ID and secret prior to the installation.

## Ensure write access to stream and asset collections

The PI to CONNECT Agent has write permission to the streams collection in CONNECT data services. The configuration utility generates a client ID that has the Tenant Contributor role, which provides write permission by default.

If write access is removed, certain operations on the stream collection will fail, such as updates to Units of Measure (UOM).

For AF server transfers, write permission on the assets collection is also required to create assets in CONNECT data services.

To remove items from a transfer and also the corresponding streams and/or assets from the portal via Edit transfer mode, the user account used to edit the transfer must be the owner with write permission on the items.

## Open firewall port for communication to PI to CONNECT

Port 443 must be opened for https communication to the PI to CONNECT gateway. The URL used for https communication depends on the namespace to which the agent is communicating, as indicated in the following table.

Region	URL
West US	uswe.datahub.connect.aveva.com
Northern Europe	euno.datahub.connect.aveva.com
East Australia	auea.datahub.connect.aveva.com

Although each of the above URLs currently corresponds to a public static IP Address, we recommended you use the URL rather than the IP address in firewall rules. If required, you can determine the IP Address by pinging the URL.

## Disable IE enhanced security

If Internet Explorer Enhanced Security Configuration (IE ESC) is turned on, you will receive an error message to disable this setting before you can log on and register the PI to CONNECT Agent. To turn off Internet Explorer Enhanced Security Configuration:

1. On the computer where the agent is installed (Windows Server operating system), enter **Server Manager** in Windows search to start Server manager application.
2. Select **Local Server**.
3. In the **Properties** section, locate the **Internet Explorer Enhanced Security Configuration** setting, then select the current setting to open the property page.  
The Internet Explorer Enhanced Security Configuration dialog box opens.
4. Under **Administrators**, select the **Off** option.
5. Select **OK**.

You should now be able to connect via the PI to Data Hub Agent Configuration Utility.

---

**Note:** You can turn on IE Enhanced Security Configuration after you complete the PI to CONNECT Agent installation. See [FAQ about IE ESC](#) for more information.

---

## Install the PI to CONNECT Agent

The PI to CONNECT Agent can be installed as part of the PI Server installation kit, or as a standalone install.

## Configure access to Data Archive Security tables, PI point data, and optional AF server

For the following Data Archive security configuration items, you will need to enable read access to the PI identity, PI group, or PI user that the PI to CONNECT Agent is connecting as.

- Archive data (PIARCDATA Security table)
- The PI points configuration table (PIPOINT Security table)
- The PI points and data to be transferred

For AF Server security configuration, ensure the AF Identity that the PI to CONNECT Agent is connecting as has read access to the elements and attributes to be transferred.

---

**Note:** Due to a known issue, the Run As user of the PI to CONNECT Agent must have read access to all AF databases, even databases for which no data is being transferred. Otherwise, the agent will encounter issues with AF indexing, causing the agent to stop collecting data on restart.

---

## Install the PI to CONNECT Agent

This section describes how to install the PI to CONNECT Agent using the standalone PI to Data Hub Agent installation kit. For guidance on installing the PI to CONNECT Agent with the PI Server installation kit, refer to the PI Server 2023 (or greater) documentation.

To install the standalone PI to CONNECT Agent:

1. In the left pane, select **Data Collection > PI Agents**.
2. From the agents dropdown list, select **PI to CONNECT Agents**.
3. Select **Download Agent**.
4. On the Agent Installer Download window, select **Download**. When the download completes, select **Cancel** to close the window.
5. Open the downloaded PI to CONNECT Agent installation file, then select **Yes** to confirm running the installation file.

The Welcome page of the PI to CONNECT Agent window opens.

6. On the Welcome page, select **Next**.

The Service Account page opens.

---

**Note:** The Service Account page is shown only for new installations.

7. On the Service Account page, select the service account type for the connection:

- **NT Service** – Select NT account for the service to run as NT SERVICE\PIToDataHubAgent.
- **This account** – Specify a username and password (domain\account) for the Run as user for the PI to Data Hub Agent service.

---

**Note:** For Windows integrated security, the service account selected on this page determines the account to use for PI identity mapping and AF mapping. The Run as user can be changed after the installation from the Windows Service control panel. Changing this account may require configuration changes to PI mapping and AF mapping, but changing the account will not otherwise affect the access to local resources needed by the agent.

8. Select **Install**.

9. After the agent is installed, select **Close**.

The PI to Data Hub Agent Configuration Utility opens. See [Run the PI to Data Hub Agent Configuration Utility](#) for instructions.

---

**Note:** Agent registration is not complete until you add and configure a Data Archive server in the PI to Data Hub Agent Configuration Utility.

## Silent installation

There are several use cases for doing a silent installation of the PI to CONNECT Agent.

- Silent installations are useful for automating deployments.
- Silent installations avoid browser logins to PI to CONNECT. A new, interactive installation requires that Internet Explorer Enhanced Security be disabled, and some customers cannot disable this security.
- Installations of the PI to CONNECT Agent on Windows Server Core Operating System are supported only with silent installation.

## Silent installs for new installations

These instructions can be used to set up a new installation of the PI to CONNECT Agent, configured with connections to CONNECT data services, without needing to run the PI to Data Hub Agent Configuration Utility. The command lines in this section can be used for upgrades as well, but tenant, namespace, Data Archive, and AF server cannot be changed during an upgrade. Command line parameters related to this will be ignored. For

the minimal command line needed for upgrades, see Silent installs for upgrades or minimal new installations.

1. Create a client-credentials client with an assigned role of Tenant Contributor and add a secret. See [Add a client-credentials client](#).

**Note:** Be sure to securely store the Client Id and Client Secret where you can access it again, because this is the only time you will have access to this information. You will need this information to proceed with the silent install.

2. Find the TENANTID and record it where you can access it.

When you log into CONNECT data services, the TENANTID is visible in the URL. It is the long GUID.

`https://datahub.connect.aveva.com/tenant/[YOUR TENANT ID]/dashboard`

Alternatively, select **Developer Tools > API Console** and the TENANTID displays in the Full Path.

`uswe.datahub.connect.aveva.com/api/v1/Tenants/[YOUR TENANT ID]/Namespaces`.

3. Find the NAMESPACE Id and record it where you can access it.

Select **Developer Tools > API Console** and select **GET**. The NAMESPACE Id appears as the **Id** field in the response.

```

Body
Details
1 [
2 {
3   "Id": "{NAMESPACE_ID}",
4   "Region": "westus",
5   "Self": "https://uswe.datahub.connect.aveva.com/api/v1/tenan"
6   "Description": "Bar Team (No Data Views)",
7   "State": 1,
8   "RegionId": "westus",
9   "InstanceId": "{INSTANCE_ID}",
10  "Name": "Bar Team (No Data Views)",
11  "AllowCrossRegionProcessing": true
12 },
13 {
14   "Id": "{NAMESPACE_ID}",
15   "Region": "westus",
16   "Self": "https://uswe.datahub.connect.aveva.com/api/v1/tenan"
17   "Description": "RSHB",
18   "State": 1,
19   "RegionId": "westus",
}

```

**Note:** If you have multiple namespaces, you will have multiple entries in this list. Be sure to select the NAMESPACE Id of the namespace where you want PI to CONNECT Agent to send data.

4. Record the GATEWAYBASEURL for your region where you can access it. See [Regional endpoints](#).
5. Open a Windows command prompt as an administrator.
6. Change to the folder where you have downloaded the PI to Data Hub Agent installation kit.
7. If you do not need to configure an Alternate Display Name for your Data Archive or AF servers, enter the following command. This command will immediately register the agent with the actual Data Archive name specified by the DATAARCHIVE command line argument.

**Note:** The TENANTID, CLIENTID, CLIENTSECRET, and NAMESPACE keywords are required for the agent to connect to CONNECT data services at installation time. All keywords are case sensitive. SERVICEACCOUNT and SERVICEPASSWORD provide the Run As user and password, respectively, for the PI to Data Hub Agent service.

```

PItoDataHubAgent_SetupKit.exe TENANTID=[tenantid] CLIENTID=[clientid]
CLIENTSECRET=[clientsecret] NAMESPACE=[namespaceID] GATEWAYBASEURL=[regionalendpoint]
DATAARCHIVE=[DataArchiveName] AFSERVER=[AFServerName] SERVICEACCOUNT=[user]
SERVICEPASSWORD=[password] AGENTDESCRIPTION="Your Description" /quiet

```

8. If you need to configure an Alternate Display Name for your Data Archive or AF servers, enter the following command. The Data Archive, AF server, and Alternate Display Names will be configured in a subsequent step.

**Note:** The TENANTID, CLIENTID, CLIENTSECRET, and NAMESPACE keywords are required for the agent to connect to CONNECT data services at installation time. All keywords are case sensitive.

```
PItoDataHubAgent_SetupKit.exe TENANTID=[tenantid] CLIENTID=[clientid]  
CLIENTSECRET=[clientsecret] NAMESPACE=[namespaceID] GATEWAYBASEURL=[regionalendpoint]  
AGENTDESCRIPTION="Your Description" /quiet
```

9. Check that the PItoDataHubAgent service is running.

From an administrative command prompt, run the command `net start | find "PI"` and verify that "PI to CONNECT Agent" is in the list.

10. Check the event logs for any errors.

- a. Right-click on Start and select **Event Viewer**.
- b. Select **Applications and Services Logs** and double-click **PI to Data Hub**.

For Windows Server Core operating systems, you can connect to the Event Viewer remotely.

11. Check the setup logs.

- a. Open a command prompt and navigate to `%ProgramData%\OSIsoft\Setup\log`.
- b. Logs can be listed from oldest to newest with the command `dir /od`.

12. (Optional) Configure an Alternate Display Name for Data Archive and/or AF server.

**Note:** For a silent install an Alternate Display Name is required to use the PI to Data Hub Agent Configuration Utility.

- a. Open an administrative command prompt and navigate to `%ProgramData%\OSIsoft\PItoOCS`.
- b. Run the command `notepad.exe appsettings.json`.
- c. To specify an alternate display name for the Data Archive, add the following `AlternateDisplayName` entry. If you did not specify `AFSERVER` and `DATAARCHIVE` on the command line above, you will need to add the server names in this step as well as specifying the alternate display name.

```
"PIDataArchiveServerNames": [  
    {  
        "Name": "MyActualDataArchiveServerName",  
        "AlternateDisplayName": "AlternateDisplayName",  
        "ConnectionTimeout": 10,  
        "OperationTimeout": 60  
    }  
],
```

- d. To specify an alternate display name for AF, add the following `AlternateDisplayName` Entry:

```
"PIAssetFrameworkServerNames": [  
    {  
        "Name": "MyActualAFServerName",  
        "AlternateDisplayName": "AlternateDisplayName",  
        "ConnectionTimeout": 10,  
        "OperationTimeout": 60  
    }  
],
```

- e. Save the changes and restart the PI to Data Hub Agent service from an administrative command prompt with the commands:

```
net stop pitodatahubagent  
net start pitodatahubagent
```

13. Verify your agent is visible on the PI Agents page in the portal and ready to configure.

## Silent installs for upgrades or minimal new installations

These instructions can be used to upgrade the PI to CONNECT Agent. They can also be used for a new installation of the PI to CONNECT Agent, but the installation requires configuration with the PI to Data Hub Agent Configuration Utility for the new installation.

1. Open a Windows command prompt as an administrator.
2. Change to the folder where you have downloaded the PI to Data Hub Agent installation kit.
3. Run the following command:

```
PIToDataHubAgent_SetupKit.exe /quiet
```

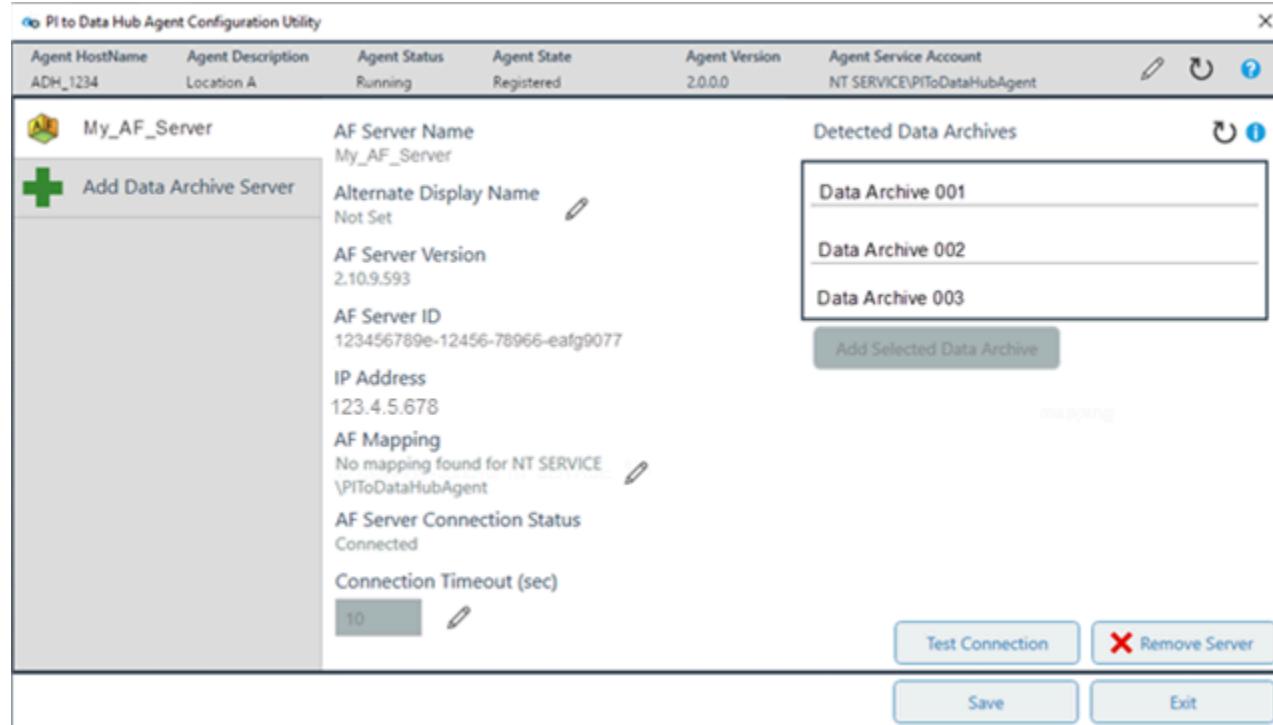
The above command is sufficient for an upgrade. For a new installation, run the PI to Data Hub Agent Configuration Utility to register the PI to CONNECT Agent after the silent installation completes.

## Run the PI to CONNECT Agent Configuration Utility

Use the PI to Data Hub Agent Configuration Utility to set up and configure AF server and Data Archive data sources before creating a data transfer. After installing or upgrading a PI to CONNECT Agent, use the utility to select a source AF server or Data Archive, view connection details, create AF and PI mappings, set data privacy settings, and register the agent.

**Note:** A connection to CONNECT data services with the post-installation utility cannot be established if the system time is not correct. Additionally, you will not be able to connect to CONNECT data services if Internet Explorer Enhanced Security Configuration is enabled. For more information, see [Disable IE enhanced security](#).

The following table provides descriptions of the fields shown in the configuration utility. The image shows the AF server selected, but the fields are similar when a Data Archive server is selected.



Field	Description
Agent HostName	Name of the host computer where the agent is installed.
Agent Description	An optional name for the agent.
Agent Status	Displays the agent's status.
Agent State	Displays the agent's registration state.
Agent Version	The installed PI to CONNECT Agent version.
Agent Service Account	Type of agent service account.
Agent Settings 	Set data privacy options and assign an agent description.
Refresh Display 	Refresh the displayed agent and server information.
AF Server Name/Data Archive Server Name	Source AF or Data Archive server name.
Alternate Display Name	An optional, alternate name for an AF or Data Archive server.
AF Mapping/PI Mapping	The type of AF/PI mapping configured on the service account.
Connection Timeout	The time before the agent connection times out.

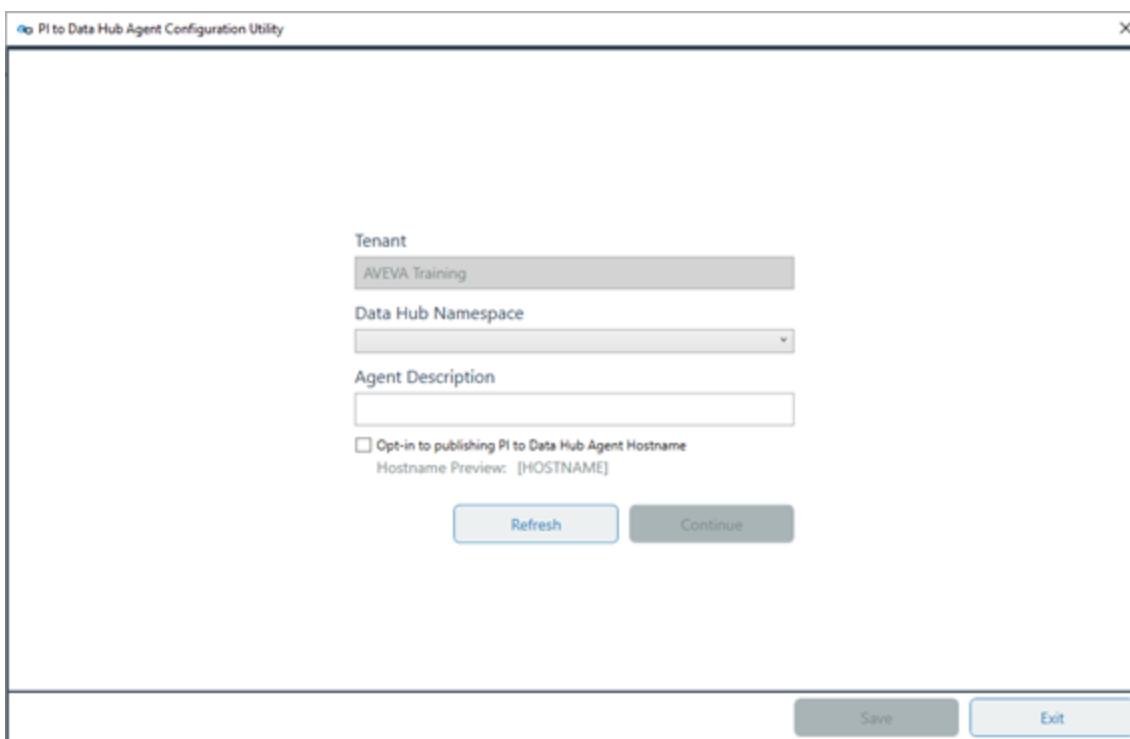
## Open the PI to Data Hub Agent Configuration Utility

The PI to Data Hub Agent Configuration Utility opens after you install or upgrade a PI to CONNECT Agent. You can open the PI to Data Hub Agent Configuration Utility at any time to change server connections and other settings after initial setup.

To open the PI to Data Hub Agent Configuration Utility:

1. Select **Start > AVEVA > PI to Data Hub Agent Configuration Utility**, and then select **Yes** to confirm.
2. Select **Connect to Data Hub**.

This opens <https://signin.connect.aveva.com/login> in a web browser for login. After successful authentication, return to the configuration utility. The namespace configuration view opens.



3. Select a namespace from the **Data Hub Namespace** dropdown list.
4. (Optional) In the **Agent Description** field, enter a descriptive name for the agent.
5. (Optional) To display the hostname in the portal, select the **Opt-in to publishing PI to Data Hub Agent Hostname** option.
6. Select **Continue**.

## Add an AF server

Optionally, add an AF server to the utility to be able to use it in data transfers. The utility validates an AF server connection to ensure the version of PI Asset Framework (AF) installed on the AF server supports the features required for transfers.

To add an AF server:

1. Open the PI to Data Hub Agent Configuration Utility.
2. In the PI to Data Hub Agent Configuration Utility window, select the **AF** button.

---

**Note:** If a Data Archive server was added first, select **Add Asset Framework Server** on the left side of the window instead.

---

3. In the **AF Server Name** field, enter the name of the AF server, and then select **Add Server**.

The utility displays the server details.

---

**Note:** Once an AF server has been added, the utility scans the configured AF server for referenced Data Archives. As the utility finds Data Archives, they are shown in the **Detected Data Archives** list. You can select and add the desired Data Archive. You do not have to wait for the scan to complete. You can also select **Add Data Archive Server** on the left and manually enter the name of the Data Archive if you do not want to wait for the scan.

---

4. Select one of the Data Archives listed under **Detected Data Archives**, and then select **Add Selected Data**

**Archive.**

**Note:** You can select **Add Data Archive Server** on the left at any time to add a Data Archive before the scan completes.

5. Review the AF source server details to ensure they are correct:
  - AF server name, version, and ID
  - IP address
  - Connection status and timeout
6. (Optional) To add an alternate display name, select the pencil icon, type an alternate name, select **Set Display Name** and then select **Close**. CONNECT data services stores the alternate display name instead of the actual AF server name. See [Usage of server names and alternate display names within CONNECT data services](#).
7. (Optional) To change the length of time the agent checks for a server connection before timing out, select the pencil icon next to **Connection Timeout**.
8. (Optional) To check that the connection to the AF server is working, select **Test Connection**.
9. (Optional) To delete a server connection, select **Remove Server**, then select **Remove AF Server** to confirm.
10. To keep the current AF server configuration settings and restart the agent, select **Save**.

**Note:** After you save the AF server configuration settings, you need to select a default Data Archive in PI System Explorer to resolve substitution references for AF element attributes.

## Usage of server names and alternate display names within CONNECT data services

The AF server name, or its alternate display name, displays on the PI Agents page within CONNECT data services and is referenced in the path of an asset's metadata, which is visible in Asset Explorer (`__Path`).

The Data Archive name, or its alternate display name, appears in the PI Agents page within CONNECT data services, and is used in the StreamIds created by a transfer. StreamIds have the format `PI_[DataArchiveServerName]_[PIPointIDNumber]`.

**Note:** Setting an alternate display name for a Data Archive must be done *before* the initial start of a transfer. StreamIds are immutable. Once a stream is built, to change it you must delete all the original streams, configure the alternate display name, and restart the transfer.

The maximum character length for an AF server alternate display name is 63 and the maximum character length for the Data Archive alternate display name is 86. The difference is due to added information. Both fields start with a maximum of 100 characters because Asset Id and Stream Id have a 100-character limit. To form an Asset Id, the agent adds an underscore and a 36-character GUID to an AF server alternate display name, allowing 63 characters (100-37) for the alternate display name. To form a Stream Id, the agent prepends the Data Archive alternate display name with `PI_` and appends `_[PIPointIDNumber]` (maximum of 10 characters), allowing 86 characters (100-14) for the alternate display name.

## Select the default Data Archive in PI System Explorer

You need to specify the default Data Archive, also referred to as the default data server, for the PI System and PI AF database after setting an AF server. By default, PI AF databases inherit the PI AF Server's local default data server. See [Find the default Data Archive server](#) for more information.

To select the default Data Archive:

1. Open PI System Explorer on the client machine.
2. Select **File > Server Properties**.
3. In the PI AF Server Properties window, select the data server from the **Default Data Server** dropdown list.
4. Select **Apply**, then select **OK** to save the selection.
5. Close PI System Explorer.

## Create an AF mapping

You can assign an AF mapping to an AF identity. AF mappings enable a specific service account assigned to an AF identity in PI System Explorer to read and transfer AF element and AF attribute data. You can also edit mappings with the utility.

---

**Note:** The user account used to launch the utility must have permission to create mappings.

To create an AF mapping:

1. Open the PI to Data Hub Agent Configuration Utility.
2. Select the pencil icon next to **AF Mapping**.
3. In the Configure AF Mapping window, select an identity and select **Create**.

The AF mapping is created for the selected identity.

---

**Note:** If an AF mapping has been created with another tool, a warning is displayed.

4. Select **Close** to return to the utility.

## Add a Data Archive

If you plan on transferring AF server data, we recommend you add an AF server first, because the PI to Data Hub Agent Configuration Utility will detect automatically the Data Archive servers that are referenced by AF server. This allows you to select the source Data Archive that contains the PI points you want to transfer. However, you can also add a Data Archive without adding an AF server.

---

**Note:** There is a one-to-one (1:1) Data Archive to PI to CONNECT Agent constraint for PI to CONNECT transfers. If your AF server references multiple Data Archives, only one Data Archive can be selected and configured for the transfer.

The list of available Data Archive servers is based on the servers referenced by AF elements on the AF server you selected. If you are upgrading an agent, the PI to Data Hub Agent Configuration Utility maintains the previously selected Data Archive configuration.

---

**Note:** If you are not adding an AF server, select the Data Archive icon on the first page of the PI to Data Hub Agent Configuration Utility.

To add a Data Archive:

1. Open the PI to Data Hub Agent Configuration Utility.
2. In the PI to Data Hub Agent Configuration Utility window, select the **Data Archive Server** button.

---

**Note:** If an AF server was added first, select **Add Data Archive Server** on the left side of the window instead.

3. In the **Data Archive Server Name** field, enter the name of the Data Archive server, and then select **Add Server**.

The Data Archive connection is added and details about the newly added Data Archive are displayed.

4. Review the following details for the Data Archive:
  - Server name, version, and server ID
  - IP address
  - Connection status and timeout
5. (Optional) To add an alternate name, select the **Alternate Display Name** pencil icon, type an alternate name, select **Set Display Name** and then select **Close**.  
**Note:** Setting an alternate display name for a Data Archive must be done *before* the initial start of a transfer. See Usage of server names and alternate display names within CONNECT data services.
6. (Optional) To change the length of time the agent checks for a server connection before timing out, select the pencil icon next to **Connection Timeout (sec)**.
7. (Optional) To confirm that the connection to the Data Archive is working, select **Test Connection**.
8. (Optional) To remove the configured Data Archive, select **Remove Server**.
9. To retain the current Data Archive configuration, select **Save**.

## Create a PI mapping

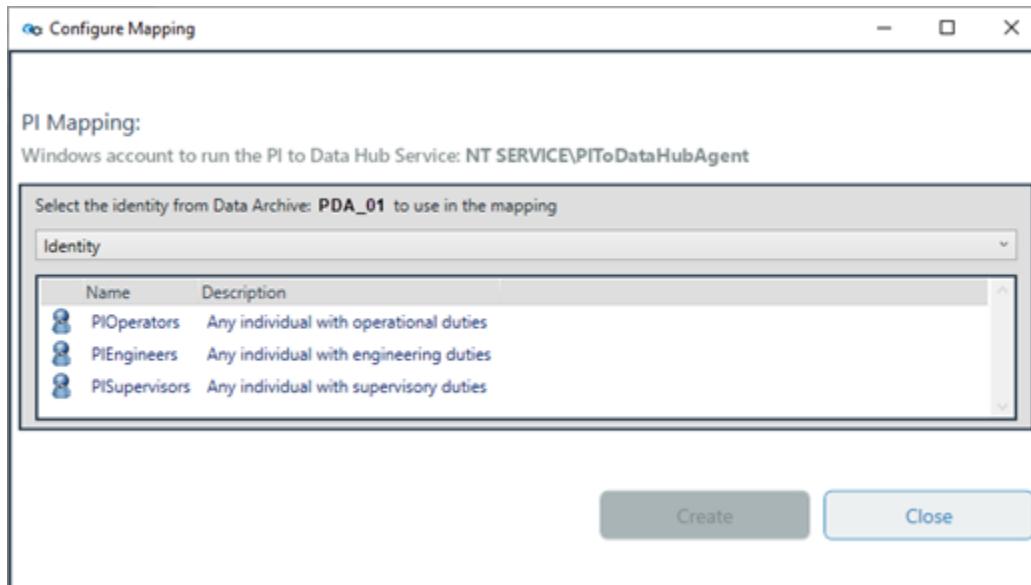
PI mappings enable access to data stored on a Data Archive by service accounts assigned to a PI identity. PI mappings can be created for a PI identity, user, or group. Accounts assigned to a PI identity can read and transfer PI point data to CONNECT data services. For more information, see [What are PI identities and mappings?](#). You can also edit mappings with the utility.

**Note:** The user account used to launch the utility must have permissions to create mappings.

To create a PI mapping:

1. Open the PI to Data Hub Agent Configuration Utility.
2. Select the Data Archive server on the left side of the window.
3. Select the pencil icon next to **PI Mapping**.

The Configure Mapping window opens.



- Select an identity for the PI mapping, then select **Create**.

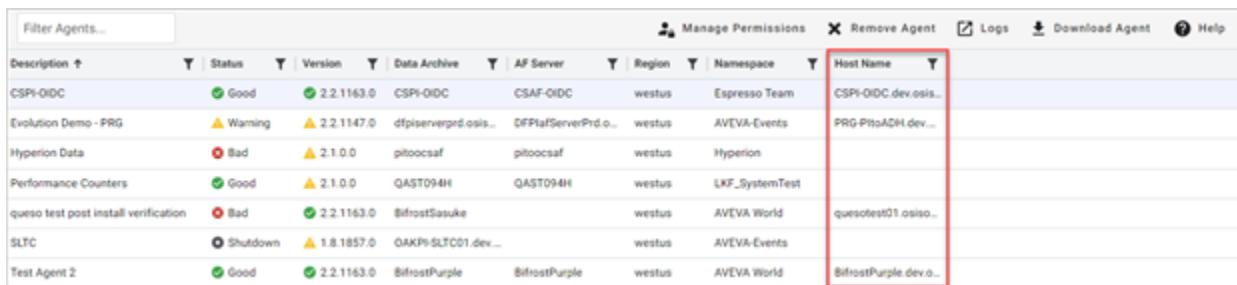
The PI mapping is created for the selected PI identity, PI group, or PI user.

**Note:** If a PI mapping has already been created with another tool, a warning is displayed.

- Select **Close** to return to the utility, and then select **Save** in the utility.

## Set data privacy and edit an agent description

Use the PI to CONNECT Agent Settings to edit the descriptive name for the agent and to change the data privacy setting. This description appears where the agent is referenced and allows you to search by agent description. The data privacy setting controls whether the host name of a Data Archive is published and displayed in CONNECT data services. By default, host names are not published. If you opt to have a host name published, it appears in the portal on the PI Agents page as shown below:



Description	Status	Version	Data Archive	AF Server	Region	Namespace	Host Name
CSPI-OIDC	Good	2.2.1163.0	CSPI-OIDC	CSAF-OIDC	westus	Espresso Team	CSPI-OIDC.dev.osiso...
Evolution Demo - PRG	Warning	2.2.1147.0	dftserverprd.osiso...	DFPilotServerProd.o...	westus	AVEVA-Events	PRG-PilotADH.dev...
Hyperion Data	Bad	2.1.0.0	pitoccsaf	pitoccsaf	westus	Hyperion	
Performance Counters	Good	2.1.0.0	QAST094H	QAST094H	westus	LKF_SystemTest	
queso test post install verification	Bad	2.2.1163.0	BifrostSasuke		westus	AVEVA World	quesotest01.osiso...
SLTC	Shutdown	1.8.1857.0	OAKPi-SLTC01.dev...		westus	AVEVA-Events	
Test Agent 2	Good	2.2.1163.0	BifrostPurple	BifrostPurple	westus	AVEVA World	BifrostPurple.dev.o...

- Open the PI to Data Hub Configuration Utility.
- To open the PI to CONNECT Agent Settings window, select the pencil icon to the right of **Agent Service Account**.
- To publish the hostname, select the **Opt-in to publishing...** option under **Data Privacy**.
- (Optional) In the **PI to CONNECT Agent Description** field, enter a descriptive name for the agent.
- To save your selections, select **Ok**, and then select **Save** in the utility.

## List of agent states

After saving in the PI to Data Hub Agent Configuration Utility, it may take a few minutes for the PI to CONNECT Agent to register with CONNECT data services. The table below lists the various states that may appear under **Agent State** in the PI to Data Hub Agent Configuration Utility.

State	Description
Data Source Connection Issue	Indicates the PI to CONNECT Agent cannot connect to the Data Archive. Some reasons for this status include the Data Archive is turned off, a firewall issue is preventing connections, or an incorrect name is configured for the Data Archive. For example, the agent is trying to connect to a machine that does not exist or was renamed. There may be additional reasons for this status.
Data Source Security Issue	Indicates the Data Archive connection security settings

State	Description
	need to be addressed.
Missing Configuration	The Data Archive server has not been configured in the PI to CONNECT Agent.
Registration Failed	Contact <a href="#">AVEVA Customer Support</a> for assistance.
Registering	The PI to CONNECT cloud portion is creating the necessary resources for the PI to CONNECT Agent.
Shutdown	The last communication that the PI to CONNECT cloud had with the agent was a shutdown message.

## Support for slow moving data

If you have PI points that do not update often, you might want the data in CONNECT data services before it is archived on the source Data Archive. To accomplish this task, turn off compression for these PI points to ensure snapshot data is collected.

Turn off compression only for PI points that do not update often. In general, this practice is not required for most tags and can cause unnecessary overhead and data collection.

## Transfer PI System data to CONNECT data services

To transfer AF elements and PI System data to CONNECT data services, you must set filter criteria and select the data for the transfer. Then, you can stream the selected AF elements and PI points from your on-premises PI System to CONNECT data services.

The following tasks must be performed before you can complete a data transfer:

1. Download and install the PI to CONNECT Agent.
2. Configure your PI System data source connections by adding the desired Data Archive and optional AF server.
3. Create a data transfer by adding the desired AF elements and/or PI points.

## Historical transfer

During the creation of a transfer, you have the option of including historical data. You specify the start time for a historical data transfer. When the start time is in the past, before \* in PI terminology, the PI to CONNECT Agent asks Data Archive for past data. The PI to CONNECT Agent retrieves the data between the start time and the time when the transfer started. The data it collects is referred to as the historical transfer.

## Backfilling

When a PI to CONNECT Agent shuts down in the middle of a transfer, it needs to fill this gap after it starts back up. During normal operation, the agent signs up for updates from Data Archive. This signup is lost when the agent shuts down. When the agent starts back up, it signs up for updates again, but it must fill the gap for the

shutdown period by retrieving historical data from Data Archive. The gap-filling process is called backfilling and this part of the transfer is referred to as a "backfill transfer job."

For example, if the service shuts down for two hours, the PI to CONNECT Agent will have to sign up for updates when it starts back up again. However, the agent cannot use updates to retrieve the data for the two hours the service was down. Instead, the agent queries Data Archive for historical data. In this example, the "backfill transfer job" fills the gap for these two hours.

## Historical transfer versus backfilling

Historical transfer fills the gap between a configured, past start time and the time the transfer started. Backfilling fills the data from the time the transfer stopped to the time the transfer resumed.

### Create a PI to CONNECT data transfer

You create a data transfer from the PI Agents page. A transfer can consist of PI points and AF elements or AF elements that reference at least one PI point. AF elements reference PI points via AF attributes that have a PI point data reference.

PI points can be added to a transfer explicitly using a tag search or implicitly using AF element references. For information about the difference between implicit and explicit references, see [Explicit versus implicit PI points](#).

**Before you begin:** Download and install the PI to CONNECT Agent. Register your Data Archive and AF data sources using the PI to CONNECT Agent Configuration Utility.

Transfer creation consists of the following tasks:

1. Name the transfer and set data privacy settings. Assign a name, description, and optional historical start time for data retrieval.
2. Select Stream Metadata Replication Policy (High, Medium, Low, or None) to control which PI point attributes the transfer stores as metadata in SDS streams. This policy provides a level of data privacy in cases where sensitive information is stored in PI point attributes that you do not want replicated to the cloud.
3. Build an AF elements transfer list. For agents with AF server configured, search for AF elements to add to the transfer. Add AF elements to the transfer. PI points referenced by AF elements will be implicitly added to the transfer. Points added to the transfer in this manner are referred to as **Implicit PI points**.
4. Build a PI points transfer list. Instead of or in addition to adding AF elements, you can search for PI points explicitly and add these to the transfer. Points added to the transfer in this manner are referred to as **Explicit PI points**.
5. View transfer details.
6. Save the transfer. Before you can save a transfer, at least one **Implicit** or **Explicit** PI point must be added to the transfer and the **Implicit** or **Explicit** PI points must correspond to the same Data Archive.

---

**Note:** If you have configured an AF server, you will not be able to create a transfer until AF indexing is complete. AF indexing status is listed on the **Manage Agent** tab in the PI Agents page. The following image shows AF indexing in progress.

---

Manage Agent Transfer Metrics

Agent Overview

Agent Description	Agent1
Agent Namespace	Namespace1
Agent Status	Registered
Agent Version	2.0.1.359
AF Server Index Status	Succeeded
PI Points Index Status	Succeeded
Communication Time	Jul 28, 2022, 3:02:46 PM

## Name the transfer and set data privacy settings

To name the data transfer:

1. In the left pane, select **Data Collection > PI Agents**.
2. From the agents dropdown list, select **PI to CONNECT Agents**.
3. In the PI Agents page, select the agent for the data transfer.
4. In the **Manage Agent** tab, select **Create Transfer**.

The Transfer Settings window opens.

**Transfer Settings** ?

Name

Description

Historical Start Time  
07/12/2023 02:53:31 PM

Namespace  
AVEVA World

Data Archive  
BifrostPurple

AF Server  
BifrostPurple

Stream Metadata Replication Policy ?

High  Medium  Low  None

Automatically delete Streams and Assets from the cloud ?  
 Enable Verbose Logging

5. In the **Name** and **Description** fields, enter a name and description for the transfer.
6. (Optional) In the **Historical Start Time** field, enter a historical time context for the data retrieval. Be sure to enter the historical start date and time correctly to ensure all data is included in the transfer. No data before the historical start time will be captured and stored in SDS. See [Transfer PI System data to CONNECT data services](#) to learn more about transferring historical data.

**Note:** The PI to CONNECT Agent supports transferring out-of-order events written to Data Archive.

7. To set the data privacy level for the transfer, select the **Stream Metadata Replication Policy**. In this context, metadata refers to PI point attributes transferred as SDS stream metadata.
  - **High:** Sends all supported PI point attributes as metadata.
  - **Medium:** Default. Sends metadata without logical addresses from the data source.
  - **Low:** Sends no metadata from the data source namespace. Locally configured metadata such as point source and local aliases is allowed (point name, point ID and point source only).
  - **None:** Sends only the point ID and point name; no metadata is included in the transfer.

**PI point attributes transferred with each Stream Metadata Replication Policy (data privacy) setting**

	<b>High</b>	<b>Medium</b>	<b>Low</b>	<b>None</b>
Name	X	X	X	X
Descriptor	X	X		
EngUnits	X	X		
ExDesc	X			
InstrumentTag	X			
PointId	X	X	X	X
Pointsource	X	X	X	
PointType	X	X		
SourceTag	X	X		
Step	X	X		

1. (Optional) To have streams and assets automatically removed from the transfer when their corresponding PI points and AF elements are removed, select the **Automatically delete Streams and Assets from the cloud** option.
2. Select **Ok**.

The transfer is created and the Transfer page opens.

---

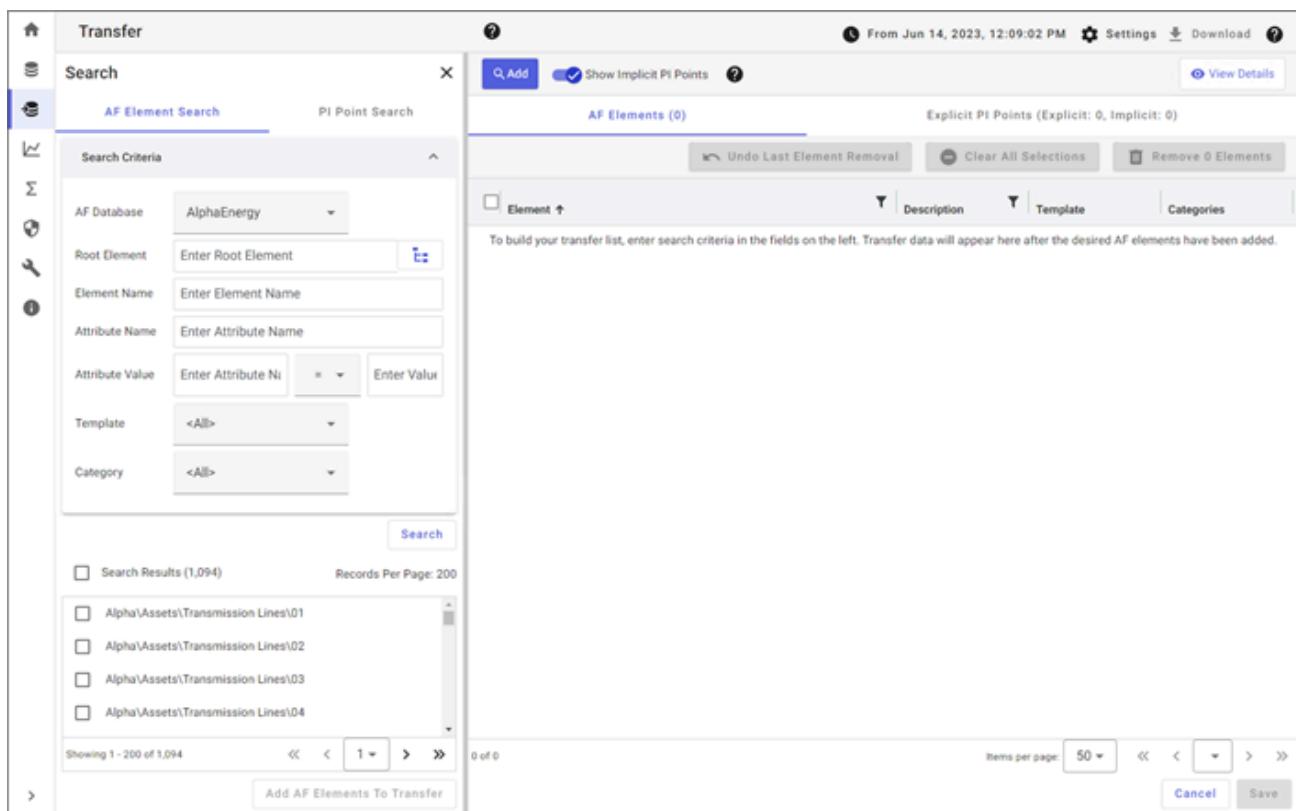
**Note:** To modify the transfer settings, select **Settings** to access the Transfer Settings window and modify the name, description, historical start time, and data privacy settings as needed.

---

**Build an AF elements transfer list**

After naming the transfer, build an AF elements transfer list by setting query criteria and then selecting AF elements. You can narrow your search by filtering by element name, root element, attribute name/value, template, and category. A corresponding asset is created for every AF element in your transfer. Static AF element attributes become asset metadata.

1. On the Transfer page, select the source AF database from the **AF Database** dropdown list.



2. (Optional) Select **Root Element**.
3. (Optional) In the Select Root Element window, select the plus buttons to drill down to the root element in the AF database hierarchy, select a root element, then choose **Select**.
4. (Optional) In the **Element Name** field, enter search criteria to filter by part or an entire AF element name.  
**Note:** If you do not enter filter criteria, the search defaults to \* or all.
5. (Optional) In the **Attribute Name** field, enter the attribute name.
6. (Optional) In the **Attribute Value** fields, filter attribute values by specifying the following information:  
**Note:** Custom units of measure (UOMs) are not supported. During the transfer of AF element data, AF elements with custom UOMs will not have their corresponding asset's UOM property set.
  - In the first field, enter an attribute name.
  - In the second field, use the dropdown list to select an operator (=, <, >, <=, >=, In).
  - In the last field, enter an attribute value.**Note:** Custom units of measure (UOMs) are not supported. During the transfer of AF element data, AF elements with custom UOMs will not have their UOM property set.
7. (Optional) To narrow your search by template name, in the **Template** field, select a template from the dropdown list.
8. (Optional) To narrow the search by a specific AF category, in the **Category** field, select a category from the dropdown list.
9. To execute the query and retrieve results, select **Search**.  
When dealing with large data sets, a search query can take a significant amount of time. Select **Cancel** to stop the query if necessary.
10. In the Search Results list, select each AF element you want added to the transfer.

A check mark appears next to each selected AF element.

**Tip:** To select a range of elements, select an element, hold the Shift key, and select a non-adjacent element. To advance through multiple-paged query results, select the back and forward arrows or enter a page number in the **Page** field.

11. When you are done selecting elements, select **Add AF Elements To Transfer**.  
The elements are added to the transfer and listed on the **AF Elements** tab.
12. To add additional elements from other AF databases, repeat these steps.

**Note:** AF indexing must complete before you can view implicit PI points and start the transfer process.

## View AF element details

You can view details about an individual AF element such as related attribute names, values, and data references.

1. Select an AF element on the **AF Elements** tab.
2. Select **View Details**.  
The AF Element Information pane opens and displays details about AF element attributes.
3. To view the paths of referenced AF elements, select the **Reference AF Elements** tab.
4. (Optional) To view health messages for the selected AF element, select the **Health Events** tab.
5. To view details for another AF element, deselect the currently selected element, and then select a different element in the transfer list.
6. To close the AF Element Information pane, select **X** in the upper-right corner of the pane.

## Build a PI points transfer list

You build a PI points transfer list by setting query criteria and then adding the desired PI points. A PI points transfer list may contain both implicit and explicit PI points. See Explicit versus implicit PI points for more information.

To build a PI points transfer list:

1. Select the **PI Point Search** tab.
2. To filter the results, do the following:

Criteria To Filter By	Action To Take
Common PI point attributes	<p>Enter criteria in any of the following fields:</p> <ul style="list-style-type: none"><li>• <b>Name</b> (alias for tag attribute)</li><li>• <b>Point Source</b></li></ul> <p><b>Note:</b> Enter * to retrieve all PI points.</p>
Point descriptions	<p>Enter criteria in the following fields:</p> <ul style="list-style-type: none"><li>• <b>Descriptor</b></li><li>• <b>Extended Descriptor</b></li></ul>

Criteria To Filter By	Action To Take
Engineering units	Enter criteria in the <b>Engineering Units</b> field.
PI point type	Select one of the following point types from the <b>Point Type</b> dropdown list: <ul style="list-style-type: none"> <li>• <b>Float32</b></li> <li>• <b>Float64</b></li> <li>• <b>Int16</b></li> <li>• <b>Int32</b></li> <li>• <b>Digital</b></li> <li>• <b>Timestamp</b></li> <li>• <b>String</b></li> </ul>
Specific location code(s)	Enter up to five location code values in the <b>Location Codes</b> field.

1. (Optional) To collapse or expand the criteria section, select the **Search Criteria** bar.
2. To execute the query and retrieve matching results, select **Search**.

When dealing with large data sets, a search query can take a significant amount of time. Select **Cancel** to stop the query if necessary.

3. In the **Search Results** area, select each PI point to add to the data transfer.  
A check mark appears next to each selected PI point.

**Tip:** To select a range of PI points, select a PI point and then hold Shift and select a non-adjacent PI point. To advance through multiple-paged query results, select the back and forward arrows or enter a page number in the **Page** field.

4. When you are done selecting PI points, select **Add PI Points to Transfer**.  
The points are added to the transfer and listed on the **PI Points** tab.

## Explicit versus implicit PI points

PI points added to a transfer are assigned one of the following reference types:

- Explicit – PI points directly retrieved from a Data Archive.
- Implicit – PI points referenced by AF element attributes that have been retrieved by searching an AF server.

The reference type for each PI point is listed in the Reference Type column on the **PI Points** tab.

## SDS streams created for PI point types

Transferred SDS streams have an ID in the format **PI\_[DataArchiveServerName]\_[PIPointIDNumber]** and **Name=[TagName]**. For additional details on naming, including data privacy concerns, see [Usage of server names and alternate display names within CONNECT data services](#).

UOMs and InterpolationMode are set directly on the SDS stream in certain circumstances, as described below.

Property	Description
UOMs	For implicit PI points, the UOMs of dynamic AF attributes appear as an <a href="#">SdsStreamPropertyOverride</a> on the transferred SDS stream. For explicit PI points, UOMs are not transferred. Even for implicit PI points, there are limitations on which UOMs can be transferred, as described in <a href="#">AF data that can be transferred</a> . For example, custom UOMs are not transferred.
InterpolationMode	The default InterpolationMode for streams of type PI-Int16, PI-Int32, PI-Float32, and PI-Float64 is ContinuousNullableLeading. However, if the associated PI point has its STEP attribute set to 1, then the InterpolationMode of the stream will be set to StepwiseContinuousLeading. Note that when the STEP attribute is changed on the PI point, the InterpolationMode is not updated on the SDS stream until the agent is restarted.

## SDS types created for PI point types

The following table shows the SDS types created for the corresponding PI point types.

PI Point Type	SDS Type	SDS Type Properties	SDS Type Code	Description
Digital	PI Digital	Timestamp	16 (DateTime)	Contains the timestamp of the PI event.
		Value	109 (NullableInt32)	Contains the offset of the digital state of the PI event for good or questionable PI events, or null for bad PI events.
		IsQuestionable	3 (Boolean)	Contains true if the PI event is questionable. Otherwise, false.
		IsSubstituted	3 (Boolean)	Contains true if the PI event is substituted.

PI Point Type	SDS Type	SDS Type Properties	SDS Type Code	Description
				Otherwise, false.
		IsAnnotated	3 (Boolean)	Contains true if the PI event is annotated. Otherwise, false. Note that the associated annotation is not included in the transfer.
		SystemStateCode	109 (NullableInt32)	Contains null for good or questionable PI events, or set to the digital state offset of the System Digital Set for bad PI events.
Float32	PI Float32	DigitalStateName	18 (String)	Contains the digital state name corresponding to the offset of the digital state of the PI point's digital set for good or questionable PI events.  For bad PI events, contains the digital state name corresponding to the offset into the System Digital Set.
		Timestamp	16 (DateTime)	Contains the timestamp of the PI event.
		Value	113 (NullableSingle)	Contains the value of good or questionable PI events, or null for

PI Point Type	SDS Type	SDS Type Properties	SDS Type Code	Description
				bad PI events.
		IsQuestionable	3 (Boolean)	Contains true if the PI event is questionable. Otherwise, false.
		IsSubstituted	3 (Boolean)	Contains true if the PI event is substituted. Otherwise, false.
		IsAnnotated	3 (Boolean)	Contains true if the PI event is annotated. Otherwise, false. Note that the associated annotation is not included in the transfer.
		SystemStateCode	109 (NullableInt32)	Contains null for good or questionable PI events, or set to the digital state offset of the System Digital Set for bad PI events.
		DigitalStateName	18 (String)	Contains null for good or questionable PI events. Otherwise, contains the digital state name corresponding to the offset into the System Digital Set.
Float64	PI Float64	Timestamp	16 (DateTime)	Contains the timestamp of the PI event.

PI Point Type	SDS Type	SDS Type Properties	SDS Type Code	Description
		Value	114 (NullableDouble)	Contains the value of good or questionable PI events, or null for bad PI events.
		IsQuestionable	3 (Boolean)	Contains true if the PI event is questionable. Otherwise, false.
		IsSubstituted	3 (Boolean)	Contains true if the PI event is substituted. Otherwise, false.
		IsAnnotated	3 (Boolean)	Contains true if the PI event is annotated. Otherwise, false. Note that the associated annotation is not included in the transfer.
		SystemStateCode	109 (NullableInt32)	Contains null for good or questionable PI events, or set to the digital state offset of the System Digital Set for bad PI events.
		DigitalStateName	18 (String)	Contains null for good or questionable PI events. Otherwise, contains the digital state name corresponding to the offset into the System Digital Set.
Int16	PI Int16	Timestamp	16 (DateTime)	Contains the timestamp of the PI

PI Point Type	SDS Type	SDS Type Properties	SDS Type Code	Description
				event.
		Value	107 (NullableInt16)	Contains the value of good or questionable PI events, or null for bad PI events.
		IsQuestionable	3 (Boolean)	Contains true if the PI event is questionable. Otherwise, false.
		IsSubstituted	3 (Boolean)	Contains true if the PI event is substituted. Otherwise, false.
		IsAnnotated	3 (Boolean)	Contains true if the PI event is annotated. Otherwise, false. Note that the associated annotation is not included in the transfer.
		SystemStateCode	109 (NullableInt32)	Contains null for good or questionable PI events, or set to the digital state offset of the System Digital Set for bad PI events.
		DigitalStateName	18 (String)	Contains null for good or questionable PI events. Otherwise, contains the digital state name corresponding to the offset into the System Digital Set.

PI Point Type	SDS Type	SDS Type Properties	SDS Type Code	Description
Int32	PI Int32	Timestamp	16 (DateTime)	Contains the timestamp of the PI event.
		Value	109 (NullableInt32)	Contains the value of good or questionable PI events, or null for bad PI events.
		IsQuestionable	3 (Boolean)	Contains true if the PI event is questionable. Otherwise, false.
		IsSubstituted	3 (Boolean)	Contains true if the PI event is substituted. Otherwise, false.
		IsAnnotated	3 (Boolean)	Contains true if the PI event is annotated. Otherwise, false. Note that the associated annotation is not included in the transfer.
		SystemStateCode	109 (NullableInt32)	Contains null for good or questionable PI events, or set to the digital state offset of the System Digital Set for bad PI events.
		DigitalStateName	18 (String)	Contains null for good or questionable PI events. Otherwise, contains the digital state name corresponding to the offset into the

PI Point Type	SDS Type	SDS Type Properties	SDS Type Code	Description
				System Digital Set.
String	PI String	Timestamp	16 (DateTime)	Contains the timestamp of the PI event.
		Value	18 (String)	Contains the value of good or questionable PI events, or null for bad PI events.
		IsQuestionable	3 (Boolean)	Contains true if the PI event is questionable. Otherwise, false.
		IsSubstituted	3 (Boolean)	Contains true if the PI event is substituted. Otherwise, false.
		IsAnnotated	3 (Boolean)	Contains true if the PI event is annotated. Otherwise, false. Note that the associated annotation is not included in the transfer.
		SystemStateCode	109 (NullableInt32)	Contains null for good or questionable PI events, or set to the digital state offset of the System Digital Set for bad PI events.
		DigitalStateName	18 (String)	Contains null for good or questionable PI events. Otherwise, contains the digital

PI Point Type	SDS Type	SDS Type Properties	SDS Type Code	Description
				state name corresponding to the offset into the System Digital Set.
Timestamp	PI Timestamp	Timestamp	16 (DateTime)	Contains the timestamp of the PI event.
		Value	116 (NullableDateTime)	Contains the value of good or questionable PI events, or null for bad PI events.
		IsQuestionable	3 (Boolean)	Contains true if the PI event is questionable. Otherwise, false.
		IsSubstituted	3 (Boolean)	Contains true if the PI event is substituted. Otherwise, false.
		IsAnnotated	3 (Boolean)	Contains true if the PI event is annotated. Otherwise, false. Note that the associated annotation is not included in the transfer.
		SystemStateCode	109 (NullableInt32)	Contains null for good or questionable PI events, or set to the digital state offset of the System Digital Set for bad PI events.
		DigitalStateName	18 (String)	Contains null for good or questionable PI

PI Point Type	SDS Type	SDS Type Properties	SDS Type Code	Description
				events. Otherwise, contains the digital state name corresponding to the offset into the System Digital Set.

## View PI point details and hide implicit PI points

You can view attribute details for selected PI points in a transfer. Implicit PI points are PI points referenced only by AF elements in a transfer. You can hide implicit PI points to temporarily remove them from view on the **PI Points** tab. Hidden implicit PI points are still included in a transfer unless the referencing AF elements are removed from the transfer list.

1. In the Transfer pane, select the **PI Points** tab.
2. Select a PI point and select **View Details**.  
The PI Point Information pane opens.
3. To view the path of any AF elements that reference the PI point, select the **Source AF Elements** tab.
4. (Optional) To view health messages for the selected PI point, select the **Health Events** tab.
5. (Optional) To hide implicit PI points on the PI points list, turn off the **Show Implicit PI Points** toggle.

---

**Note:** Implicit PI points are referenced by AF element attributes and retrieved from an AF server. Hiding implicit PI points does not remove them from a transfer.

---

6. (Optional) To show hidden implicit PI points, turn on the **Show Implicit PI Points** toggle.
7. To view another PI point's details, select a different PI point in the transfer list.
8. To close the PI Point Information pane, select **View Details** or x.

## Save a transfer

Before you can transfer data to CONNECT data services, you must save the transfer.

1. To ensure your data transfer definition is correct and contains all the data you want transferred, review it for accuracy.
2. (Optional) Add or remove PI points and/or AF elements as needed.
3. To save the transfer and return to the PI Agents page, select **Save** in the lower right-hand corner.

---

**Note:** In order to save the transfer, it must include at least one valid PI point.

---

## Start a PI to CONNECT data transfer

Once you create a data transfer, you can start the transfer. During the transfer, events are sent asynchronously. Historical events are sent first, followed by current events. Data is transferred from on-premises to the cloud every 30 seconds or for every 50,000 events, whichever occurs first.

To start a data transfer:

1. In the PI Agents page, select **PI to CONNECT Agents** from the agents dropdown selector.
2. Select the PI to CONNECT Agent associated with the data transfer.
3. (Optional) In the **Manage Agent** tab, expand the Transfer Overview section.
4. Select **Start Transfer**, then select **Start**.

The data transfer begins, and transfer status is updated in the Transfer Overview section on the **Manage Agent** tab.

---

**Note:** The **Manage Agent** tab provides information about the agent associated with the transfer and the transfer progress.

---

5. In the Transfer Overview section, view the transfer status as data is sent to the agent and stream data is created.

**Note:** The rate at which data transfers varies and depends on the density of data in the source Data Archive and/or AF server. See [PI to CONNECT data transfer status](#) for a list of transfer statuses and descriptions. To find out more information about an asset error, agent status, or asset create/update error, select **Logs** above the list of agents to access more information. Possible statuses that appear in the **Current Activity** field may indicate an issue and include Uncategorized Error, PI Point Type Change Detected, and No Valid PI Points In Transfer.

---

6. (Optional) To view more information about an agent's status, select **Agent Health Events**.
7. (Optional) To see more information about log messages for the transfer, select **Logs**. See [Logs](#) for more information.
8. (Optional) To view transfer progress and metrics for stream and/or asset creation, select the **Transfer Metrics** tab.
9. (Optional) To stop a transfer, select **Stop Transfer**, then select **Stop**.
10. (Optional) To remove a transfer, select **Remove Transfer**, select the **Delete Streams and Assets from the cloud** option if applicable, then select **Remove**.

## Health Events window

The Health Events window provides information about an agent's activity and status. Health events are based on log messages. You can sort messages by severity, source, time, and message content.

The screenshot shows a 'Health Events' window with the following details:

- Header:** Health Events, Clear All Events, Refresh icon.
- Columns:** Severity (dropdown), Source (dropdown), Health Event (dropdown), Timestamp (dropdown), Message.
- Data:**
  - Severity: Warning, Source: Stream, Health Event: UnableToFindSup..., Timestamp: Jun 30, 2023, 11:46:48 ..., Message: Unable to create stream for PI Point '32315', check point security and configuration.
  - Severity: Information, Source: Agent, Health Event: StartingTransferJob, Timestamp: Jun 30, 2023, 11:46:52 ..., Message: Transfer Job 'b284908e-7702-4740-8db637d603b': Starting transfer j
- Bottom:** Items per page: 25, Page: 1 - 1 of 1, Navigation icons, Close, Download.

The following table provides descriptions for the elements of the Health Events window.

Element	Description
Severity	The severity level of the log message. To filter by a particular severity level (Critical, Error, Warning, Information, Debug or Trace), select the filter icon and select one or more severity levels.
Source	The source of an error message. To filter by source (agent, PI point indexing or AF indexing), select the filter icon and select one or more sources.
Health Event	The health event that occurred.
Timestamp	The date of the event. To filter log messages by a particular date and/or time, select the filter icon, then enter the date and/or time in Month 00, 000 00:00:00 PM format.
Message	The actual log message. To filter by a word or phrase, select the filter icon, then enter the word or phrase.
Clear All Events	Select <b>Clear All Events</b> to remove all events from the view.
Export	Select <b>Export</b> to save a copy of the health event messages to a .csv file.

## Transfer metrics

The **Transfer Metrics** tab displays details about a transfer's progress by server connection. Metrics for streaming

and historical events and the progress of stream and asset creation are shown.

The following table provides a description of the fields in the **Transfer Metrics** tab.

Field name	Description
Data Archive Server Version	The version of Data Archive that is installed on the source server configured to send PI point data via the agent.
Last Streaming Read	The date of the latest stream value read.
Streaming Events Per Second	The average number of streaming events transferred to the PI to CONNECT Agent per second over the last minute. This value is updated every 10 seconds during data transfer.
Historical Events Per Second	The average number of historical events transferred to the PI to CONNECT Agent per second over the last minute. This value is updated every 10 seconds during data transfer.
Historical Transfer	Transfer progress for historical data.
Historical Start	The historical start date of the transfer.
Historical End	The historical end date of the transfer.
Total PI Points In Transfer	Total number of PI points selected for transfer.
Total Points Updated	The number of PI points added to or removed from the transfer configuration.
Stream Creation Status	The progress of streams creation during transfer progression.
Total Streams Created	Total number of streams created.
Total Streams Updated	Total number of streams updated with new configuration and metadata.
Total Streams Deleted	Total number of deleted streams.
Stream Creation Errors	Total number of errors generated while creation streams.
Stream Update Errors	Number of errors generated while updating streams. See the Transfer Overview section on the <b>Manage Agent</b> tab for error details.
Stream Deletion Errors	Number of errors generated during stream deletion. See the Transfer Overview section on the <b>Manage Agent</b> tab for error details.

Field name	Description
AF Server Version	The version of Asset Framework (AF) that is installed on the source server configured to send AF element data via the agent.
Total Elements in Transfer	The number of AF elements configured in the transfer.
Assets Created Per Second	The number of assets created per second during the transfer.
Total Assets Created	The total number of assets created.
Assets Updated	The number of assets created or updated during data transfer.
Total Assets Deleted	The total number of deleted assets.
Asset Create/Update Errors	The number of errors generated during asset creation or updating.
Asset Deletion Errors	The number of errors generated during asset deletion. See the Transfer Overview section on the <b>Manage Agent</b> tab for error details.

## PI to CONNECT data transfer status

The status and progress of a PI to CONNECT data transfer is shown in the Transfer Overview section of the **Manage Agent** tab. The following table lists these data statuses and their meanings.

Data status	Meaning
Sending Historical Data	Historical data is being sent.
Sending Streaming Data	PI point data is currently being streamed.
Backfilling Streaming Gap	Data streaming is resuming. Data will be backfilled from the interrupted time to now and will then continue with normal streaming.
Uncategorized Error	Data transfer has been interrupted due to an unknown cause.
Streaming Error Consumer Removed	Due to an error during streaming, the consumer has been removed.
Streaming Error Update Queue Overflow	Agent not receiving streaming data from Data Archive.
Streaming Error Signup Dropped	Agent not receiving streaming data from Data Archive.
Streaming Error Producer Removed	Agent not receiving streaming data from Data Archive.

Data status	Meaning
Streaming Error Unknown	An unknown error occurred during data streaming.
PI Point Type Change Detected	PI point type change was detected during data transfer. See <a href="#">PI to CONNECT change synchronization</a> for more information.
Creating Streams	Streams are in the process of being created.
Done	Data transfer is complete. Streams have been created.

## Confirm data retrieval from a PI Server

Confirm that SDS streams have been created and your data has transferred by viewing the streams and types created in the portal.

To review the data:

1. In the left pane, select **Data Management > Sequential Data Store**.
2. To review the streams created, in the **Streams** dropdown list, select **Streams**.

---

**Note:** By default, the grid displays the SDS streams created by the PI to CONNECT data transfer. The grid lists the first 50 SDS streams in alphabetical order. You can change how many streams are displayed per page.

3. (Optional) In the **Search** field, enter search criteria to locate specific streams, and then press Enter.
4. (Optional) To view details about the stream metadata and type, select a stream.
5. To review the types created, in the **Streams** dropdown list, select **Types**.
6. (Optional) In the **Search** field, enter search criteria to locate specific types, and then press Enter.

## Edit a PI to CONNECT transfer

You can edit saved transfer settings and add or remove AF elements and/or PI points with Edit Mode. You must be the owner of a stream or asset to remove it from a transfer and cloud storage.

---

**Note:** Your transfer settings affect whether streams and data get replicated or deleted from cloud storage after you have removed elements or explicit PI points from a transfer. See [Name the transfer and set data privacy settings](#) for details.

To edit an existing transfer:

1. In the PI Agents page, select **PI to CONNECT Agents** from the agents dropdown selector.
2. Select the agent that contains the transfer you want to edit.
3. Select **View/Edit Transfer**.
4. In the transfer pane, select the **Edit Mode** toggle.  
Edit mode is enabled and the **Search** pane opens.
5. (Optional) To add PI points to a transfer, enter search criteria on the **PI Point Search** tab, select **Search**, select desired PI points, then select **Add PI Points to Transfer**.
6. (Optional) To add AF elements to a transfer, enter search criteria on the **AF Elements Search** tab, select

Search, select desired PI points, and then select **Add AF Elements to Transfer**.

7. (Optional) To remove PI points from a transfer, select the **PI Points** tab, select the PI points you want removed, select **Remove Points**, then select **Remove** to confirm.

**Note:** You can only remove explicit PI points from a transfer. To remove implicit PI points from a transfer, you will need to remove the associated AF element.

8. (Optional) To add the removed PI points back to the transfer, select **Undo Last Point Removal**.
9. (Optional) To remove AF elements from a transfer, select the **AF Elements** tab, select the AF elements you want removed, select **Remove Elements**, then select **Remove**.

The removed AF elements are marked as **Removed** in the **AF Elements** list.

**Note:** Any implicitly referenced PI points that are not referenced by another AF element will also be removed from the transfer.

10. (Optional) To add the removed PI points back to the transfer, select **Undo Last Element Removal**.
11. (Optional) To open the Transfer Settings dialog box and edit transfer settings, select **Settings** and then perform the desired action(s):
  - To change the transfer name and description, enter a new name and description in the **Name** and **Description** fields.
  - To change the transfer's historical start time, enter or select a new time in the **Historical Start Time** field.
  - To change the transfer's data privacy settings, select one of the **Stream Metadata Replication Policy** options.
  - To change whether streams or assets are removed automatically, select or deselect the **Automatically delete Streams and Assets from the cloud** option.
12. After transfer edits are done, select **Save** to retain these changes and return to the PI Agents page.

**Note:** If a transfer was started and in progress when edits were made, these changes will be processed after the transfer is saved.

## Download transfer details

You can download a list of all the PI points added to a transfer for your records. Downloaded details are saved to a .csv file and contain the transfer name as well as the PI point path and name.

To download transfer details:

1. In the left pane, select **Data Collection > PI Agents**.
2. From the agents dropdown list, select **PI to CONNECT Agents**.
3. In the PI Agents page, select the agent that contains the transfer.
4. On the **Details** pane, select **View Transfer**.
5. Select **Download** in the upper-right corner.
6. In the Download Transfer window, select the transfer details to include in the .csv file. Data sources to include are:
  - AF elements
  - PI points (Implicit)
  - PI points (Explicit)

For each selected data source, you can choose to include **All**, **Filtered**, or **Selected** data.

7. Select **Download**.
8. In the Save As window, navigate to the location where you want to save the file, enter a name for the .csv file, and then select **Save**.

## Download a list of missing PI points

Sometimes, PI points cannot be transferred because they have been removed on the source Data Archive. When this occurs, the points are flagged as missing and a message is displayed. You can download a file that contains a list of these missing PI points for your records. The .csv file contains the following information:

- Transfer name
- The missing PI point IDs
- The name of the source PI Server

To download a list of PI points missing from a transfer:

1. In the left pane, select **Data Collection > PI Agents**.
2. From the agents dropdown list, select **PI to CONNECT Agents**.
3. In the PI Agents page, select the transfer that contains the unresolved PI points.
4. In the Details pane, select **View Transfer**.

The screenshot shows the AVEVA Data Collection interface. In the top navigation bar, there are tabs for Transfer, Edit Mode, Health Events, a timestamp (From Apr 4, 2023, 6:05:21 PM), Settings, Download, and Help. Below the tabs, there is a notification banner: "1 implicit PI Point Id could not be found on the PI Data Archive. [Download](#)". The main content area is titled "AF Elements (52)" and "Explicit PI Points (Explicit: 517, Implicit: 230)". It includes a table with columns: Element, Description, Template, and Categories. Two entries are listed: "\Database1\Element1" and "\Database1\Element10".

A transfer that is missing PI points will have a notification banner on the Transfer page.

5. Select **Download** to the right of the notification.
- The Save As window opens.
6. In the Save As window, navigate to the location where you want to save the file, enter a name for the .csv file, and then select **Save**.

## AF data that can be transferred

You can transfer the following AF element data into CONNECT data services:

- Dynamic AF attributes with PI point data references
- Static AF attributes (attributes with no data reference)

Supported dynamic AF attributes can reference a PI point via a Data Archive server name and tag name. This transferred data does not include any data retrieval qualifiers. The associated event data contains simple PI point

attributes with the same historical and streaming transfer mechanism as explicit PI points.

The table below lists the AF objects that can be included in a PI to CONNECT data transfer and what those objects appear as in CONNECT data services.

AF Object	CONNECT data services Object
Elements	Assets
Dynamic AF attributes with PI point data references  <b>Note:</b> Dynamic AF attributes are transferred only if they are on AF elements. They are not transferred if they are on AF element templates.  <b>Note:</b> Only AF Attribute Templates with a basic type (Boolean, Byte, DateTime, Double, GUID, Int16, Int32, Int64, Single, or String) and Enumeration Set are supported and will be transferred.	Asset stream reference properties
Static AF attributes  <b>Note:</b> Static AF attributes configured as type 'Boolean' are not supported and will not be transferred.	Metadata properties on assets and asset types
Element templates	Asset types

These AF objects are not included in a PI to CONNECT data transfer and no CONNECT data services objects will be created from them:

- Analysis data reference attributes
- Attributes that reference a non-registered data source/Data Archive
- AF categories
- AF enumeration sets
- AF models/layers/connections/ports
- AF tables
- Custom units of measure (UOMs)
- Event frames
- Excluded attributes
- Extended properties and annotations on assets not supporting AF versioning
- Formula data reference attributes
- Implicit PI points with attributes that reference other attributes
- Implicit PI points with multiple attributes on an AF element (only one attribute will be transferred)
- PI point arrays
- String builder attributes
- Table lookup attributes

When an AF element is transferred and a corresponding CONNECT data services asset is created, if any attributes are undefined in the element but have default attribute values defined in the applicable AF element template,

the default values will be shown in the Asset Explorer.

## Limitations of element search

When building an AF element transfer list in the portal, the AF element search does not detect element references, those elements shown in PI System Explorer with a shortcut icon next to them. The search returns only child elements that have reference types of either composition or parent-child. This means that while you can add any element to a transfer, there are limitations with how the search results are displayed, and, because of these limitations, each element appears only once in the search results.

## Limitations of `_ParentId` and `_ParentName`

The asset resulting from a transfer will have only one `_ParentId` metadata item and one `_ParentName` metadata item. In AF an element can have multiple parents, though the additional parents are via element references.

As an example, say element "A" has a child element "A-Child" and element "B" has an *element reference* of "A-Child." The child element is distinctly different from the element reference. In PI System Explorer, element "A-Child" appears as a child of both A and B, albeit with the shortcut icon for B. If you include "A-Child" in a PI to CONNECT transfer, its `_ParentId` and `_ParentName` will refer only to A. Also, the type of the reference does not transfer. That is, there is no distinction between parent-child and composition reference types in the resultant asset.

## Units of Measure (UOM) transfer

An AF attribute can have two different UOMs set, both the [Default UOM](#) and the [Source UOM](#) (also called DataReference UOM). CONNECT data services only allows for one UOM. PI to CONNECT considers an attribute's UOM to be its Source UOM if set; otherwise, it uses the default UOM. If both are set and they are different UOM classes, PI to CONNECT logs a warning that they are mismatched, but still uses the Source UOM.

Multiple PI point data reference attributes can reference the same PI point. If multiple attributes reference the same PI point but have different UOMs, a stream UOM is not transferred. If you update your AF attributes to resolve the conflict, the UOM will be transferred.

Custom units of measure (UOMs) do not transfer.

## Performance metrics: AF data transfer

The average data transfer rate is approximately 120-150 assets per second, and 1,000 assets per minute. Streams are created first, followed by AF element and asset data. If you use the same stream for various elements, the transfer time may be shorter.

---

**Note:** There may be some variance to these numbers.

## PI to CONNECT change synchronization

The PI to CONNECT Agent supports synchronizing changes in the Data Archive and PI Asset Framework. Updates are automatically sent to CONNECT data services without any user interaction.

## Data Archive synchronization

The PI to CONNECT Agent signs up for the following updates to stay in sync with the Data Archive:

- PI point updates
  - **Adding a PI point:** If PointId was listed in the transfer specification, a stream is created and the data streams to SDS.
  - **Updating a PI point name:** The SDS stream name is updated.
  - **Updating metadata:** The corresponding SDS stream metadata is updated.
  - **Deleting a PI point:** The SDS stream is deleted if the AutoDeleteCloudObject flag is enabled in the transfer settings.
- Digital state updates
  - **Update set name/values:** The SDS stream values are changed to the updated digital state set/name. See the Data Archive synchronization limitations table below.
- Data updates
  - **Point compression updates.**

Sign-up for PI point updates and digital state updates occurs when the agent starts, while data updates do not begin until the start of a transfer.

## Data Archive synchronization limitations

Issue	Restrictions
Toggling compression	<p>Toggling On to Off: It is possible that the PI point's corresponding SDS stream may be missing an event near the time when the PI point's compression setting was changed from On to Off.</p> <p>Toggling Off to On: There is a small chance for an extra event (an event which was compressed out from the server) to be in SDS near the time when the PI point's compression setting was changed from Off to On.</p>
Analysis backfilling and rapid succession of data addition and deletion	<p>There is a possibility for a data gap after an analysis backfill operation due to the nature of rapid data deletion and insertions being performed by the analysis service on the PI point.</p>
Updating digital state	<p>The SDS stream will store the updated state name and values at time of change. Previously stored state values are preserved.</p> <p>Updated digital state values will not be backfilled</p>

Issue	Restrictions
	or recalculated for existing data saved to the corresponding SDS stream.

## Asset Framework synchronization

The agent performs an indexing of the AF server after agent registration is successful. The indexing caches all known elements and templates along with their attributes. The agent updates this index periodically.

When a transfer starts, the agent builds out the implicit PI points referenced by the element IDs specified in the transfer specification to enable change synchronization.

The supported AF change synchronization events and the result of each change are listed below:

- Database
  - **Database addition:** No effect on the existing transfer, but elements from the new database will be available to add if the transfer is edited.
  - **Database rename:** The path metadata of assets referencing the database is updated.
  - **Database deletion:** All elements and templates that were also deleted because of the database being removed will propagate and synchronize.<sup>1</sup>

- Element

- **Updates to Name, Description, Template:** The corresponding asset property is updated.
- **Addition or updates to attributes:** An SDS stream is created if newly referenced in transfer. The stream reference of the asset is added or updated.

---

**Note:** If an AF element has a PI point reference that is not yet created when the transfer is started, creating that PI point reference will not trigger change synchronization. The PI point reference must be created before a transfer is started.

---

- **Deletion of attributes:** The stream reference is removed from the asset. The SDS stream is removed if a point is no longer referenced in the transfer.<sup>1</sup>

- **Deletion of the element:** The asset is deleted.<sup>1</sup>

- Point attributes

- **Metadata updates (Name, Description, etc.):** The asset property is updated to reflect the change.
- **PI point reference updates:** The stream reference of the asset on the cloud changes to the updated stream. If the previously referenced point is no longer referenced implicitly or explicitly in the transfer, the SDS stream is removed.<sup>1</sup>
- As of release 2.2.2174, new point attributes added directly to the cloud asset will not be overwritten by the PI to CONNECT Agent.

- Static attributes

- **Metadata updates (Name, Description, etc.):** The asset metadata associated with the attribute is updated.
- **Value updates:** The value of the attribute is updated.
- As of release 2.2.2174, new static attributes added directly to the cloud asset will not be overwritten by the PI to CONNECT Agent.

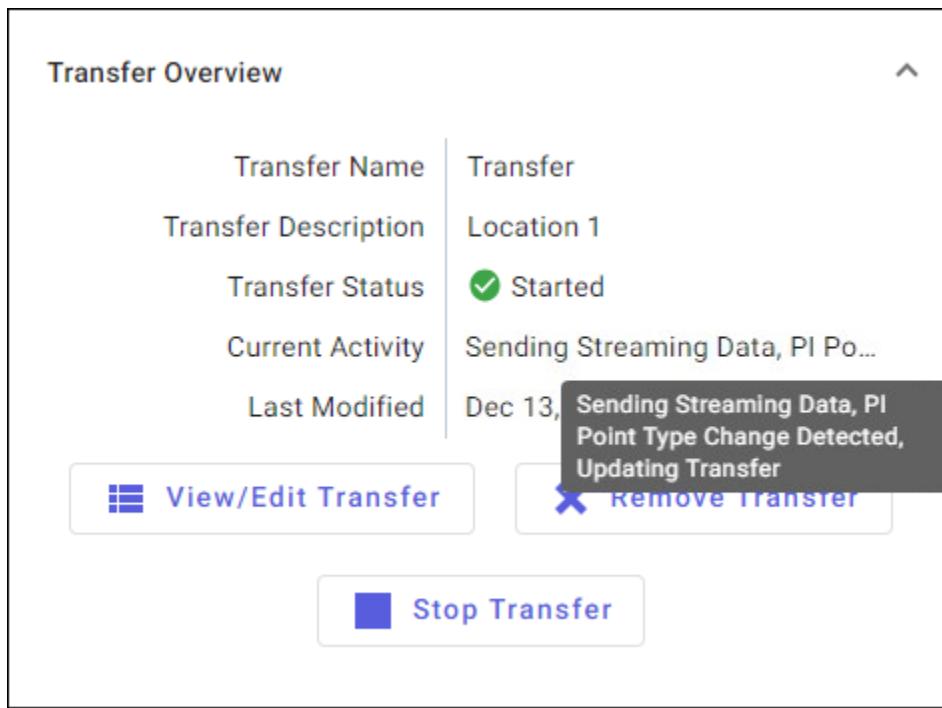
- Template
  - **Updates to Name, Description, Template:** The corresponding property is updated on the asset type.
  - **Addition or updates to attribute templates:** The stream reference and metadata associated with the asset type is updated.
  - **Deletion of attribute templates:** The stream reference and metadata is removed from the asset type.
  - **Deletion of the template:** The asset type is removed.<sup>1</sup>
- Point attribute templates
  - **Metadata updates (Name, Description, etc.):** The asset type property is updated to reflect the change.
  - **PI point reference updates:** The stream reference is updated on the asset type.
- Static attribute templates
  - **Metadata updates (Name, Description, etc.):** The asset type metadata associated with the attribute is updated.
  - **Asset type value updates:** The asset type metadata is updated.

<sup>1</sup> This action occurs only if the AutoDeleteCloudObject flag is enabled in the transfer settings.

## PI point type change

When the PI to CONNECT Agent detects that a PI point's type is changed on the source Data Archive after the corresponding stream has been created in the SDS database, it takes the following actions:

- The PI Point Type Change Detected message displays next to **Current Activity** in the Details pane, as shown below:



- The agent prevents data being sent from the source PI point to the SDS stream until the type is changed to match the corresponding SDS stream type.

- The agent logs details about the corresponding SDS stream in both the Windows Event Viewer and CONNECT data services logs.

## Causes for PI point type changes

A point change can occur for multiple reasons, including:

- The source PI point data and type is configured incorrectly. The data and point must be deleted and recreated.
- The source PI point was misconfigured initially. For example, the point needs to be updated from *Float32* to *Float64*. The data is still relevant and should be kept.

## Resume streaming data to an existing SDS stream after a type change

After you create an SDS stream, its underlying SdsType cannot change. As a result, new data from the PI point in question cannot be stored in the same stream. You can resume streaming data from the PI point to the existing SDS stream by taking the following corrective actions:

1. View the [View PI to CONNECT Agent logs in the Windows Event Viewer](#) or [Logs](#) to determine which PI point incurred a PI point type change.

**Note:** The Windows Event Viewer logs are the preferred source of information for PI point type changes.

2. Change the PI point type to match the SDS stream type and then restart the transfer.

To see what types of point coercions are supported in Data Archive, refer to the [Allowable point type coercions](#) topic.

## PI to CONNECT Agent maintenance

PI to CONNECT Agents require maintenance from time to time. This section explains how to uninstall, update, repair, search for, and view performance metrics for agents.

### View PI to CONNECT Agent metrics

You can quickly view key performance indicator (KPI) metrics for installed PI to CONNECT Agents on the home page.

To view PI to CONNECT Agent metrics:

1. To open the portal home page, select **Home** in the left pane.

The screenshot shows the AVEVA CONNECT Data services dashboard. On the left is a vertical navigation bar with icons for Home, Stream, System, Security, and Help. The main area has several tiles:

- Latest Service Updates:** CONNECT to PI Agent 1.0.1470 is released on Aug 14, 2024, at 10:41:46 AM. A detailed description follows.
- Quick Links:** Includes links to API documentation, code samples, service blog, user management, client secrets, and REST API console.
- Yesterday's Resource Usage:** Shows Stream statistics: Stored (22,204), Accessed (7,112), and Shared Streams Accessed (3).
- System Health:** Shows a green heart icon with "Ok" status.
- PI to CONNECT Agents:** Shows 18 Total Agents. Breakdown: 5 Good, 0 Warning, 13 Bad, 0 Stopped.
- Systems:** Shows 21 Total Systems. Breakdown: 5 Good, 15 Warning, 1 Bad, 0 Stopped.
- CONNECT to PI Agents:** Shows 18 Total Agents. Breakdown: 4 Good, 14 Warning, 0 Bad.

- View the information in the PI to CONNECT Agents tile to see the current state of your agents. States are:
  - Good
  - Warning
  - Bad
  - Stopped
- To see the agents on the PI Agents page filtered by state, select the state on the PI to CONNECT Agents tile.

## Repair a PI to CONNECT Agent

An agent installed on a host machine may need to be repaired to fix and update files.

To repair an agent:

- Select Windows **Start**, then select **Settings > Apps > Apps & features**.
- In the Settings window, select **PI to Data Hub Agent** in the list of installed apps, select **Modify**, and then select **Yes**.
- In the **PI to Data Hub Agent** window, select the **Repair** option, and then select **Next** twice. The Installation window opens and the repair process begins.
- After the repair process has completed, select **Close** to exit.

## Search for a PI to CONNECT Agent

You can search for PI to CONNECT Agents that have been installed on host machines at your organization to quickly locate agents of interest. For example, you may want to remove older agents. The global filter feature allows you to search by agent name, status, version number, hostname, Data Archive or AF server name, region, and namespace.

To search for an agent in the portal:

1. In the left pane, select **Data Collection > PI Agents**.
2. Select **PI to CONNECT Agents** from the agents dropdown selector.
3. In the **Filter Agents** field, enter the first few characters of the agent's name or version number.  
Agents that meet the filter criteria are displayed in the list of agents.
4. (Optional) To clear the search, remove all characters from the **Filter Agents** field.

## Remove a PI to CONNECT Agent

You remove a PI to CONNECT Agent by first uninstalling it from the host machine and then the portal. There are two parts to removing an agent:

- Uninstall the agent from the host machine
- Remove the agent listing in CONNECT data services

## Uninstall the PI to CONNECT Agent on the host machine

To remove the PI to CONNECT Agent application from a host machine, uninstall it from the Apps & features window and then follow the prompts in the PI to CONNECT Agent window.

1. Select Windows **Start**, then select **Settings > Apps > Apps & features**.
2. In the Apps & features window, select **PI to Data Hub Agent** in the list of installed apps.
3. Select **Uninstall** twice, then select **Yes** in the User Account Control window.
4. In the **PI to Data Hub** Agent (Administrator) window, select the **Uninstall** option, then select **Next**.
5. Select the **Unregister agent from Data Hub** option, then select **Next**.

The agent's associated client and connection information is also removed from CONNECT data services during the uninstall process.

6. Select the user account to use to log on, then close the browser window.
7. In the **PI to Data Hub** Agent window, select **Uninstall**, then select **Close**.

The PI to Data Hub Agent application is uninstalled on the host machine.

## Remove the PI to CONNECT Agent on the portal

If the agent was uninstalled without the **Unregister agent from Data Hub** option, you also need to remove the agent from the portal.

1. In the left pane, select **Data Collection > PI Agents**.

2. Select **PI to CONNECT Agents** from the agents dropdown selector.
  3. Select an agent in the list.
  4. In the agent details pane, select **More Options**  > **Remove Agent**.
  5. In the Remove Agent window, select **Remove**.
- The agent is removed in the portal.

## Manage permissions for agents

If you are assigned the **Manage Permissions** access right, then you can configure agent permissions for other user roles in your tenant. You can granularly assign individual agent permissions to each user role.

### Prerequisites

To manage agent permissions, you must be assigned the **Manage Permissions** access right.

## To manage permissions for agents

1. In the left pane, select **Data Collection > PI Agents**.
2. Select **PI to CONNECT Agents** from the agents dropdown selector.
3. Select an agent and choose **Manage Permissions**.
4. Use the Manage Permissions window to:
  - (Optional) Add user roles that have permissions on the agent.
  - Edit agent permissions for each user role.  
For more information, see [Permissions management](#).
5. When you are finished editing permissions, select **Save**.

## PI to CONNECT logs

PI to CONNECT logs help you troubleshoot errors, and view information about account-related activity for both on-premises and cloud components.

### View PI to CONNECT Agent logs in the Windows Event Viewer

To view information about account related activity for on-premises components, you can also view PI to CONNECT Agent logs in the Windows Event Viewer.

To view the PI to CONNECT Agent logs:

1. Select the Windows **Start** button, then select **Windows Administrative Tools > Event Viewer**.
2. In the Event Viewer window, select the **Applications and Services Logs** option in the left pane.  
A list of logs by service type is revealed.
3. In the left pane under **Applications and Services Logs**, select **PI to Data Hub**.
4. In the PI to Data Hub pane, scroll through and select an event to display event details.

## View PI to Data Hub Agent Configuration Utility logs

To view information about account related activity for PI to Data Hub Agent Configuration Utility, you can view log information in the Windows Event Viewer.

To view the PI to Data Hub Agent Configuration Utility logs:

1. Select the Windows **Start** button, then select **Windows Administrative Tools > Event Viewer**.
2. In the Event Viewer window, select **Applications and Services Logs > PI to Data Hub Configuration Utility**.
3. In the PI to Data Hub Configuration Utility pane, select an event to display event details.
4. When you are finished viewing the logs, close the Event Viewer window.

## Common Event Viewer log messages

The following table summarizes the most common messages logged by the Event Viewer.

Message	ID	Description
Started Agent	0	The PI to CONNECT Agent has been started.
Stopped Agent	2	The PI to CONNECT Agent has been stopped.
Connected To Data Archive	18	The PI to CONNECT Agent has connected to source Data Archive. Data Archive information will be printed in the message.
Error Performing Point Query	19	The PI to CONNECT Agent has encountered an error querying for PI points in the source Data Archive. The exception reason and the query ID will be displayed.
Failed To Get Data Archive Info	21	The PI to CONNECT Agent has encountered an error while trying to get archive file information from the source Data Archive. The exception reason will be displayed. Depending on the exception, this call may or may not be automatically retried.
Data Archive Version Not Supported	24	The source Data Archive version is not supported. Currently, the PI to CONNECT Agent only supports Data Archive 2016 R2 (3.4.415.1188) and above. Please upgrade your Data

Message	ID	Description
		Archive if you wish to use PI to CONNECT.
Failed To Perform Point Query - Element Invalid	27	One or more the query objects (Point Mask and/or Point Source Mask) is invalid. If this query is made from the portal, users should not get this error.
Agent Registration Completed	30	The PI to CONNECT Agent registration was successful.
Agent Registration Failed	33	The PI to CONNECT Agent registration was not successful. The most frequent reasons why this would occur are as follows: 1) The source Data Archive was already tied to an existing Connection; and, 2) The Connection is already tied to another PI to CONNECT Agent.
Agent Received Unregister Request	60	The PI to CONNECT Agent received an unregister request from the portal. As a result, the PI to CONNECT Agent will unregister and shutdown.
Agent Unregistered	62	Confirmation message that the PI to CONNECT Agent is unregistered after receiving event ID 60.
Processing Transfer Job Request	65	The PI to CONNECT Agent has received the new transfer request. The message will contain information about the contents of the transfer such as the transfer historical start time and the number of involved points.
Done Transferring Data To CONNECT data services For Transfer Job	70	The PI to CONNECT Agent has completed the given transfer job. At this moment, the only transfer jobs which will complete are the historical and backfilling transfer jobs. By the very nature of streaming data, streaming transfer job will never complete.

Message	ID	Description
Error Reading From Data Archive	90	The PI to CONNECT Agent was unable to read data from Data Archive. The event will contain the exception message.
Failed To Get Streaming Updates From Data Archive	96	The PI to CONNECT Agent was not unable to get streaming data from Data Archive. The message will contain the exception message.

## Enable verbose logging for PI to CONNECT

If there are problems with a transfer, you can enable verbose logging from the Transfer Settings window to capture more detailed logs for specific PI points and AF elements.

Verbose logging records events for each step in the transfer process related to the tagged PI points and AF elements. These messages are classified as warnings. This information is found in the PI to CONNECT Agent logs, which are viewable in the Windows Event Viewer. See [View PI to CONNECT Agent logs in the Windows Event Viewer](#).

The number of events recorded can be very large, so there is a limit of 10 PI points and 10 AF elements that can be tagged. The duration of the verbose logging should also be for a limited time. The default duration is a day and the maximum is 30 days.

To enable verbose logging:

1. In the PI Agents page, select the agent that contains the transfer you want to edit.
2. Select **View/Edit Transfer**.
3. In the transfer pane, select the **Edit Mode** toggle.  
Edit mode is enabled and the **Search** pane opens.
4. To open the Transfer Settings window, select **Settings**, then select the **Enable Verbose Logging** option, and select **Ok**.
5. Select **Verbose Logging** to display the Verbose Logging pane.
6. To include PI points in the verbose logging, select the **PI Points** tab, select the PI points, then select **Add Points** in the Verbose Logging pane.

**Note:** Up to 10 PI points can be added.

7. To include AF elements in the verbose logging, select the **AF Elements** tab, select the elements, then select **Add Elements** in the Verbose Logging pane.

**Note:** Up to 10 AF elements can be added.

8. In the **Log until** field, enter an ending time for the verbose logging, up to a maximum of 30 days.

**Note:** When the verbose logging time expires, it deselects the **Enable Verbose Logging** option in Transfer Settings.

9. Select **Save** to retain these changes and return to the PI Agents page.

## Removing PI points and AF elements

If you edit a transfer and remove PI points or AF elements from the Verbose Logging pane, any corresponding information is removed from the log.

## Troubleshoot PI to CONNECT

You can use the information in this section to troubleshoot common PI point errors, failed AF indexing, missing Data Archive configuration, and failed PI mapping.

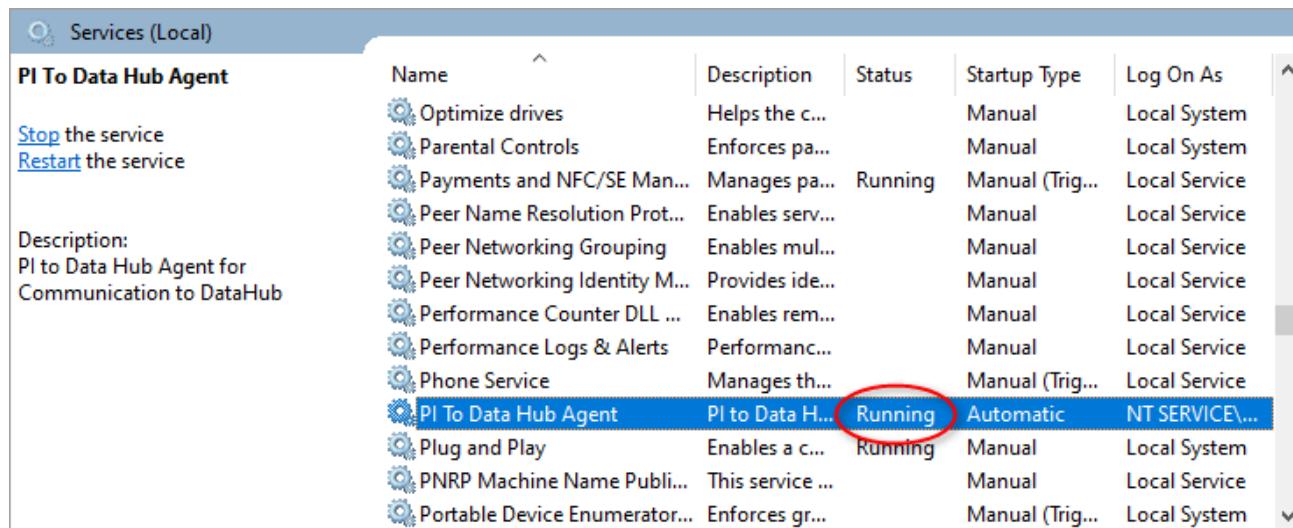
### Verify the PI to CONNECT Agent is running and registered

As a first step in troubleshooting, check that the PI to Data Hub Agent Windows service is running on the machine where the agent is installed. You also should confirm the agent is registered in CONNECT data services. For a new installation, the PI to Data Hub Agent service will not be running and registered until the PI to Data Hub Agent Configuration Utility is completed.

1. On the computer where the agent is installed, open the Microsoft Management Console (MMC) snap-in for Services.

**Tip:** Enter *services.msc* in Windows search to locate the application.

2. In the Services window, find the PI to Data Hub Agent service and verify that the status is *Running*, then close the window.



The screenshot shows the Windows Services (Local) console. The 'PI To Data Hub Agent' service is listed in the table. The 'Status' column for this service shows 'Running'. A red circle highlights the word 'Running' in the table cell. Other services listed include Optimise drives, Parental Controls, Payments and NFC/SE Manager, Peer Name Resolution Protocol, Peer Networking Grouping, Peer Networking Identity Manager, Performance Counter DLL, Performance Logs & Alerts, Phone Service, and Portable Device Enumerator.

Name	Description	Status	Startup Type	Log On As
Optimize drives	Helps the c...	Manual	Local System	
Parental Controls	Enforces pa...	Manual	Local System	
Payments and NFC/SE Manager	Manages pa...	Running	Manual (Trig...	Local Service
Peer Name Resolution Protocol	Enables serv...	Manual	Local Service	
Peer Networking Grouping	Enables mul...	Manual	Local Service	
Peer Networking Identity Manager	Provides ide...	Manual	Local Service	
Performance Counter DLL	Enables rem...	Manual	Local Service	
Performance Logs & Alerts	Performanc...	Manual	Local Service	
Phone Service	Manages th...	Manual (Trig...	Local Service	
<b>PI To Data Hub Agent</b>	<b>PI to Data H...</b>	<b>Running</b>	<b>Automatic</b>	<b>NT SERVICE\...</b>
Plug and Play	Enables a c...	Running	Manual	Local System
PNRP Machine Name Publisher	This service ...	Manual	Local Service	
Portable Device Enumerator	Enforces gr...	Manual (Trig...	Local System	

3. In the CONNECT data services portal, in the left pane, select **Data Collection > PI Agents**.
4. On the PI Agents page, select the connection you created.
5. On the Details pane, verify that Registered appears next to **Agent Status**.

The screenshot shows the AVEVA CONNECT Data Services interface. At the top, there's a header bar with tabs for "Manage Agent" and "Transfer Metrics". Below this is a "Agent Overview" section containing details like Agent Description (SystemTest), Agent Namespace (SystemTest), Agent Status (Registered), Agent Version (2.1.0.0), AF Server Index Status (Succeeded), PI Points Index Status (Succeeded), and Communication Time (Jul 12, 2023, 2:17:34 PM). Below the Agent Overview is a "Transfer Overview" section for Transfer1, showing Transfer Name (Transfer1), Transfer Description (empty), Transfer Status (Started), Current Activity (Sending Streaming Data), and Last Modified (Apr 21, 2023, 1:45:46 PM). At the bottom of the Transfer Overview section are three buttons: "View/Edit Transfer", "Remove Transfer", and "Stop Transfer".

**Note:** The PI to Data Hub Agent Configuration Utility also displays agent status. For a list of states and descriptions that explain why an agent may not be running, see [Run the PI to Data Hub Agent Configuration Utility](#).

### Troubleshoot client Id and secret

If there is a problem with a PI to CONNECT Agent's client Id and secret, a client Id and secret can be reapplied or a new client Id and secret can be applied through the service start parameters.

1. On the computer where the agent is installed, open the Microsoft Management Console (MMC) snap-in for Services.
- Tip:** Enter `services.msc` in Windows search to locate the application.
2. In the Services window, right-click on the **PI to Data Hub Agent** service and select **Stop**
  3. Right-click on the **PI to Data Hub Agent** service and select **Properties**.

4. In the *Start parameters* field, add the following, substituting your client ID and secret:  
-CLIENTID:guid -CLIENTSECRET:secret
5. Select **Start** from the properties dialog.
6. Select **OK**.

### Troubleshoot failed AF indexing

Immediately after PI to CONNECT Agent registration, AF indexing is initiated and must finish successfully before a new transfer can be defined. The progress of AF indexing is displayed next to **AF Server Index Progress** on the Agent Overview pane, as shown in the image below.

The screenshot shows the 'Agent' interface with the 'Manage Agent' tab selected. Under 'Agent Overview', there is a table of agent configuration and status:

Agent Description	Agent
Agent Namespace	AVEVA World
Agent Host Name	host.dev.org.int
Agent Status	✓ Registered
Agent Version	✓ 2.2.1163.0
AF Server Index Status	AF Indexing Failed! <span style="color: blue;">C</span>
PI Points Index Status	✓ Succeeded <span style="color: blue;">C</span>
Communication Time	Jul 18, 2023, 5:20:12 PM

At the bottom of the pane is a blue button labeled 'Create Transfer'.

If the "AF Indexing Failed!" message appears, follow these steps to reinitiate AF indexing:

1. Navigate to the cache files on the local PC where the agent runs: **C:\ProgramData\OSisoft\PIToAVEVA Data Hub\Cache**.
2. Delete the **Cache** folder.
3. Reboot the host machine that the PI to Data Hub Agent runs on (recommended) or stop/restart the PI to

Data Hub service.

**Note:** It is possible for an agent to complete and indicate that indexing has completed, but still need to re-index. Additionally, there may be times when an agent appears to be working, but you are unable to create a transfer. In both cases, CONNECT data services advises to restart the PI to CONNECT Agent to initiate AF indexing.

## Troubleshoot a failed PI mapping

If you encounter an error message and the PI to Data Hub Agent Configuration Utility crashes after an attempt to create or edit a PI mapping, follow these steps to troubleshoot and correct the issue:

1. Take one of the following steps:
  - a. Reinstall the PI to CONNECT Agent with a service account that has access to the configured Data Archive.
  - b. Add a different Data Archive that the service account has permission to access.
2. Relaunch the PI to Data Hub Agent Configuration Utility: Select **Start > AVEVA > PI to Data Hub Agent Configuration Utility**.
3. Successfully connect and authenticate to CONNECT data services.
4. In the PI to Data Hub Agent Configuration Utility, select the pencil icon to the right of **PI Mapping**.
5. Follow the steps in [Create a PI mapping section](#) to add a PI mapping.
6. After adding the PI mapping, save your changes.

## Troubleshoot missing Data Archive configuration

If a PI to CONNECT Agent's status appears as *No Data Archive Configured* in the PI to CONNECT Agent window, you may be missing a PI mapping from your Data Archive server to your agent service account. You can correct this issue in the PI to Data Hub Agent Configuration Utility.

**Note:** There may be different reasons why the *No Data Archive Configured* status appears under **Data Archive Connection Status** in the PI to Data Hub Agent Configuration Utility. This topic addresses troubleshooting due to a missing PI mapping.

To add a missing Data Archive mapping:

1. Open the [PI to Data Hub Agent Configuration Utility](#) and connect to the portal.
2. After successful authentication, select the Data Archive tab, then select the pencil icon under **PI Mapping**.  
The Configure Mapping dialog box opens.
3. Under the **Identity** list, select the identity, group or user for the PI mapping.
4. Select **Create**.  
The PI mapping is created for the selected identity, group, or user.
5. Select **Close** to exit out of the Configure Mapping dialog box.
6. To remove the server and return to the first screen of the PI to Data Hub Agent Configuration Utility, select **Remove Server**, then select **Yes**.
7. Add the Data Archive server back to the configuration. See [Run the PI to Data Hub Agent Configuration Utility](#) for more information.
8. After the Data Archive has been successfully added, select **Save** to save the newly added server

configuration.

## Troubleshoot common PI point errors

Certain PI point errors can occur when the AF server is indexing. The following table lists a few common PI point errors and troubleshooting solutions.

PI point error	Troubleshooting solution
PI Point Not Found	Ensure the PI point exists on the configured Data Archive. Verify that the identity is mapped to the service account running the PI to CONNECT Agent and has read permission on the PI point and the PI point data.
PI Point Type Change Detected	Check the <a href="#">PI to CONNECT event logs</a> in the Windows Event Viewer for the cause of the error. Filter the logs by "Type Change" or event ID "204" to locate the error message that contains the ID of the PI point that had its type changed. Change the type of this point to match its respective SDS Stream type. Then, restart the transfer to ensure all data is sent from the PI point in question. For more information, see <a href="#">PI to CONNECT change synchronization</a> .
Cannot connect to the Data Archive. Windows authentication trial failed because insufficient privilege to access the Data Archive. Trust authentication trial failed because insufficient privilege to access the Data Archive.	Configure a PI mapping for the service account running the PI to CONNECT Agent that can connect to Data Archive. We recommend this approach as it is the most secure connection method. For information on creating PI mappings, see the section on how to create a PI mapping in the <a href="#">Run the PI to Data Hub Agent Configuration Utility</a> topic.
[ -10722] PINET: Timeout on PI RPC or System Call	Ensure the Data Archive is turned on, responsive, and able to receive connections over port 5450.

## Troubleshoot insufficient RPC threads for concurrent queries

If there are insufficient RPC threads for a large PI to CONNECT transfer, the transfer will fail and the event log will contain the error OSISoft.PI.Net.PIException: [-10767] Client exceeded maximum concurrent queries in RPC thread pool.

To resolve this issue, increase the *OperationTimeout* parameter in **C:\ProgramData\OSISoft\PIToOCS\appsettings.json** to 300 ("OperationTimeout": 300).

---

**Note:** For new installations, the default is 300 seconds. If the value is 30 seconds, it is likely that you have upgraded from an older version.

---

## Limitations of PI to CONNECT

The following table lists the known limitations for PI to CONNECT.

Issue	Restrictions
Restrictions for PI point transfers	<ul style="list-style-type: none"><li>Point must belong to the classic or base point class.</li><li>Point type must be Float16, Float32, Float64, Int16, Int32, Digital, Timestamp, or String.</li><li>Must not be a future PI point.</li></ul>
High availability (HA) & collectives	<ul style="list-style-type: none"><li>PI to CONNECT does not support the high availability (HA) feature of failover between collective nodes. Connecting to a Data Archive collective is supported, but the agent must explicitly point to either the primary or secondary server. The agent will not fail over between members of the collective if a connection to the configured endpoint is lost.</li><li>AF elements or attributes that reference a collective name instead of one of the nodes are not supported.</li><li>AF Collectives are supported natively by PI to CONNECT.</li></ul>
PI to CONNECT Agent registration	<ul style="list-style-type: none"><li>Multiple PI to CONNECT Agents can connect to and transfer data from the same Data Archive if the agents are installed on different machines and assigned to different namespaces. Only one agent can be installed on each computer.</li></ul>
Data Archive	<ul style="list-style-type: none"><li>PI to CONNECT does not write events back to Data Archive from CONNECT data services.</li></ul>
SDS streams indexes	<ul style="list-style-type: none"><li>Does not support multiple values at a given index.</li><li>If a Data Archive tag has multiple values at a given timestamp, CONNECT data services will store the first value returned.</li></ul>

Issue	Restrictions
Custom UOM data	<ul style="list-style-type: none"> <li>Custom units of measure (UOMs) that are not one of the predefined UOM classes in CONNECT data services are not supported. During the transfer of AF element data, AF elements with custom UOMs will not have their corresponding asset's UOM property set.</li> </ul>
PI Analysis Service	<ul style="list-style-type: none"> <li>If you use PI to CONNECT with the PI Analysis Service, be sure to save analysis outputs to PI points.</li> </ul>
Multiple UOMs	<ul style="list-style-type: none"> <li>If multiple attributes reference the same PI point but have different UOMs, a stream UOM is not transferred.</li> </ul>
AF data limitations	<ul style="list-style-type: none"> <li>For limitations on the transfer of AF data, see <a href="#">AF data that can be transferred</a>.</li> </ul>

## PI to CONNECT known issues

The following are known issues in PI to CONNECT:

- If there is no default PI Server associated and listed for your AF server, you will not be able to transfer data to CONNECT data services.
- Data Archive servers that have a non-GUID server ID are not supported in PI to CONNECT. See [Generate a new server ID for Data Archive](#) for how to address this issue.
- PI to Data Hub Agent Configuration Utility: Detected Data Archives fail to load if the user does not have permissions to one or more of the referenced Data Archives. The workaround is to add the Data Archive by selecting the green plus icon in the utility and then manually typing the name of the Data Archive.
- Query search results that contain a very large number of PI points (> 1 million) will generate an exception error and not be processed.
- PI points with the type Float16 are supported, but the data is sent as Float32 to the cloud. The initial streaming value is rounded in the historical archive, so historical retrieval of the value may not match the initial value exactly.
- There is a known issue where streaming updates can be lost if the user is deleting events, which is common only when the user is deleting and recalculating events via the PI Analysis service. In this case, we suggest setting the *StreamingSendTaskCount* parameter in `C:\ProgramData\OSIsoft\PIToOCS\appsettings.json` to 1 ("StreamingSendTaskCount": 1) so that events are guaranteed to be sent to CONNECT data services in the order they are received.

- The PI to CONNECT Agent requires read access to all AF databases, even databases for which no data is being transferred. Otherwise, the agent will encounter issues with AF indexing, causing the agent to stop collecting data on restart. The error reported in the PI to Data Hub Agent Windows Event Log will be:

EventId: 191, Failure during AF indexing operation: ProcessChangesAsync  
Exception: System.NullReferenceException: Object reference not set to an instance of an object.

## PI to Data Hub 2.2.2174 Release Notes

### Overview

Version 2.2.2174, released November 7, 2024, is a maintenance release.

This release enhances how the PI to Data Hub Agent transfers AF elements and AF element templates to the cloud. Specifically, this release contains the following two enhancements:

- When an AF element template is transferred to the cloud, the asset type that is created or updated in CONNECT data services now includes both type references and metadata. Prior to this release, the resultant asset type would contain only metadata.
- Users can now edit assets and asset types that have been transferred to the cloud, while the agent continues to transfer subsequent changes to these same AF elements and AF element templates. Prior to this release, any user edits made to assets and asset types would be removed the next time the corresponding AF element or AF element template was edited in the on-premises AF database.

These enhancements enable full support of expected features in CONNECT visualization. Type references are used for asset relative displays for assets of the same asset type, and the preservation of user edits is expected to help fine-tune these displays.

For a full list of changes in this release, please reference Fixes and Enhancements below.

For more information on product features and functions, including system requirements and installation/uninstallation instructions, refer to [PI to CONNECT Agents](#) documentation.

### Enhancements

Work Item	Description
111668	When transferring AF element templates to CONNECT data services both dynamic and static AF attributes are now included in the transfer, allowing both type references and metadata, respectively, to be included in the resultant asset type. Previously only static AF attributes were included in the transfer, which resulted in asset types that included only static metadata values.
111398	Support was added to the PI to Data Hub Agent service to enable asset/asset type PATCH

Work Item	Description
	operations. This enhancement allows a user to edit asset and asset types in CONNECT data services without losing their edits when the corresponding AF elements or AF element templates are re-transferred because of on-premises changes to the AF database. This means that on-premises changes will continue to be synchronized while also preserving additional independent changes that are applied in CONNECT data services.
105315	The streaming step can stop due to an unexpected exception. These unexpected exceptions cause the transfer to stop and will not restart automatically. In this release, additional log messages were added to track down the source of these errors.

## Fixes

Work Item	Description
110973	If a user enabled verbose logging for PI points or AF elements in the CONNECT data services portal, the agent would continue logging verbose messages for these points/elements even after disabling verbose logging in the portal, until the original expiration date that was set for verbose logging expires. This problem has been fixed. Disabling verbose logging in the portal now causes verbose logging to stop immediately.

## Known issue when upgrading to 2.2.2174

After upgrading the PI to Data Hub Agent to version 2.2.2174, it may fail to connect to PI Data Archive 2023 and greater when TLS is enabled on the Data Archive server and the PI to Data Hub agent computer does not trust the Data Archive certificate. If you are affected by this problem, the agent will report the error "The certificate chain was issued by an authority that is not trusted" in the PI to Data Hub Agent Windows Event Viewer log. Testing the connection with the PI to Data Hub Configuration Utility also fails with this same error.

This error will occur when the following conditions are met:

- The PI to Data Hub Agent is on a remote computer from Data Archive

- The PI Data Archive is version 2023 or later
- TLS is configured for PI Data Archive 2023
- The TLS certificate configured for the Data Archive is not trusted on the agent computer. This can occur if a self-signed certificate was used to configure TLS for Data Archive, which is not recommended in production environments. It may also occur if an AVEVA Platform Common Service SMS-generated certificate is utilized by the Data Archive but the root authority established by SMS is not present on the agent computer.

To address this issue, the certificate used by the Data Archive must be trusted on the agent computer. More information about troubleshooting the certificate can be found in the knowledge base article "[The certificate chain was issued by an authority that is not trusted.](#)" | [Data Archive and Asset Framework 2023](#).

## Security information and guidance

We are [committed to releasing secure products](#).

We [proactively disclose](#) aggregate information about the number and severity of security vulnerabilities addressed in each release.

## Distribution Kits

Product	Software Version
PI to Data Hub Agent Installation	2.2.2174

©2024 AVEVA Group plc and its subsidiaries. All rights reserved.

## PI to CONNECT release history

### 2.2.1567 release: 01/17/2024

#### Overview

This release covers the PI to Data Hub Agent, a component that is installed on-premises to replicate data, assets, and licensed PI Point counts from PI System to CONNECT data services. Version 2.2.1567, released January 17, 2024, fixes a problem related to overcharging Flex credits for AVEVA PI Data Infrastructure – aggregate tag.

Although PI to Data Hub Agent Version 2.2.1567 is an optional upgrade, you should upgrade to this version if your agent connects to Data Archive 2023 or greater.

For more information on product features and functions, including system requirements and installation/uninstallation instructions, refer to [PI to CONNECT Agents](#) documentation.

#### Enhancements

There are no enhancements in this release.

## Fixes

Work Item	Description
100961	In some cases, the license file for a PI Data Infrastructure – aggregate tag unlimited server included 16 additional PI tags. The agent update accounts for that difference and will now consider a license with MaxPointCount greater than or equal to 999,999,999 tags as unlimited and report the actual tags created, not the MaxPointCount as tags used.

## Security information and guidance

We are [committed to releasing secure products](#).

We [proactively disclose](#) aggregate information about the number and severity of security vulnerabilities addressed in each release.

## Distribution Kits

Product	Software Version
PI to Data Hub Agent Installation	2.2.1567

©2024 AVEVA Group plc and its subsidiaries. All rights reserved.

## 2.2.1539 release: 12/11/2023

### Overview

This release covers the PI to Data Hub Agent, a component that is installed on-premises to replicate data, assets, and licensed PI Point counts from PI System to CONNECT data services. Version 2.2.1539, released December 11th, 2023, fixes several bugs and has performance improvements.

Customers who are upgrading to this version should be aware of a **behavior change** (item 96143 under Fixes). After upgrading, your agent may connect via Windows Authentication rather than a PI trust. Although this behavior change is desirable—Windows Authentication is the more secure option—it is possible that your agent will now connect to Data Archive with a PI identity that does not have permission to read the data in your transfer. The expectation is that few, if any, customers will be adversely affected.

Customers upgrading to this version should also consider changing OperationTimeout to 300 in **C:\ProgramData\OSIsoft\PIToOCS\appsettings.json** (item 97181 under Enhancements).

Although PI to Data Hub Agent Version 2.2.1539 is an optional upgrade, it is **highly recommended for all customers**. A summary of the most important fixes and enhancements are highlighted in the list below. For a full list of changes, see the sections Enhancements and Fixes below.

- If your agent connects to Data Archive 2023 or greater, upgrade to this version. This release contains a fix (item 97857 under Fixes), where certain license files are now correctly identified as unlimited. Correct identification of the license is essential for the new licensing model, AVEVA PI Data Infrastructure – aggregate tag. More information on this feature can be found in the [PI to CONNECT release history](#).
- If you are seeing performance issues (slow transfers), upgrade to this version. This release contains performance improvements (item 97168 under Enhancements). For example, in a transfer where the agent was in eastern United States and the CONNECT data services namespace in western United States, there would be enough latency between agent and cloud (~100 milliseconds) to cause significant slowdowns, especially when a large number of string or digital PI Points were included in the transfer or when there were a large number of PI Points in the transfer with a small number of events per archive.
- If you are seeing data gaps or issues with their transfer appearing “stuck”, upgrade to this version. Specifically, this release contains the following Fixes: 74686 (fix transfer progress), 99974 (agent should retry forever when errors are retriable).
- If you are seeing data inconsistencies between Data Archive and CONNECT data services, upgrade to this version. Specifically, this release contains the following Fixes: 95557 (fix for range delete with backfill).

For more information on product features and functions, including system requirements and installation/uninstallation instructions, refer to [PI to CONNECT Agents](#) documentation.

## Enhancements

Work Item	Description
97181	The default operation timeout for the agent has been increased from 30 seconds to 300 seconds (5 minutes). The default was changed because Data Archive RPCs typically have timeouts of 270 seconds (4 minutes and 30 seconds). The mismatch in timeouts lead to cascading problems and data loss. The new default takes effect only for new installations and must be manually applied for upgrades. Customers upgrading to this version should consider changing <b>OperationTimeout</b> to 300 in <b>C:\ProgramData\OSIsoft\PIToOCS\appsettings.json</b> to avoid putting unnecessary load on Data Archive when timeouts occur.
97168	When sending historical data to the cloud, messages are now batched together. This significantly improves performance under some conditions. The biggest improvements are seen when there is high latency between agent and cloud (such as a transfer from an agent in eastern US to a namespace in western US) and when a

Work Item	Description
	large number of string or digital PI Points are being transferred.
97704	Added a log message that reports the breakdown of the PI points included in the transfer by point type.
97705	Added a new appsetting.json setting, HistoricalReadTaskCount, to allow the preferred number of Data Archive read threads to be configured. Typically, this value should not be changed except when advised by technical support.
97706	Changed the behavior of an existing appsetting.json setting, HistoricalSendTaskCount, so that it can be increased to at least 12, regardless of processor count. This setting can be used to increase the parallelization of sends to the cloud, possibly improving performance in high-latency scenarios, such as transferring data from an agent in eastern US to a namespace in western US. The benefits of increasing HistoricalSendTaskCount should be weighed against the increased likelihood of sending data out of order to the cloud. Typically, this value should not be changed, except when advised by technical support.
97195	Added extra logging around the "transport message too large" errors so that root cause can be determined from the log message. Example error: Transport message too large to persist in Event Hub and will not be sent! Actual: 253075 Max: '235929'.

## Fixes

Work Item	Description
97857	Treat license count of 999,999,999 as an unlimited license for purposes of charging Flex credits for AVEVA PI Data Infrastructure –

Work Item	Description
	aggregate tag PI Servers.
97183	<p>The agent now caps the maximum events per query to 150,000 events when timeouts occur or errors occur that might indicate that Data Archive is busy. Previously, capping the events to 150,000 was done only when ArcMaxCollect was exceeded (error-11091). The new behavior is to cap requests at 150,000 events when the following occur:</p> <ul style="list-style-type: none"><li>• PI timeout exception</li><li>• Error -11140 is (Archive_MaxQueryExecutionSec exceeded)</li><li>• Error -10746 (MaxMessageLength exceeded)</li></ul> <p>A customer ran into a situation, where switching to 150,000 event chunks would have reduced pressure on Data Archive. They were doing a backup of Data Archive and they were querying streams with over 1 million events for a particular archive. They were running into timeouts on the agent side (PI timeout exception) and also exceeding Archive_MaxQueryExecutionSec on the server side.</p>
74686	The transfer could appear to get "stuck" during the Historical transfer step. For example, if there were 10 archives in the transfer, the progress reported in the CONNECT data services portal could indicate, indefinitely, that archive 9 of 10 was being transferred. Although this was only an issue with the progress report, this problem, combined with item 99974 below, would make it appear that the agent was still attempting to fill data gaps when, in actuality, the historical portion of the transfer was already complete.
99974	During the historical transfer step, data gaps could occur if there were communication problems with Data Archive that lasted longer than 5 minutes. This problem has been fixed. The

Work Item	Description
	agent now retries indefinitely when retriable errors occur.
78720	If Data Archive was shut down during agent registration, the agent would stop unexpectedly. This problem has been fixed.
98497	When messages with event IDs of 43 and 122 appeared in the event log, the agent could get into a bad state and consume all memory on the computer. The memory growth problem has been mitigated. The agent will now log an error message and move on to the next message in the queue.
95557	Extra values or incorrect values can be sent by the PI to Data Hub Agent after a range delete operation followed by a backfill. This operation is common in AF Analytics when recalculating analyses. The incorrect value problem has been fixed in the agent. Note, however, that there will still be some cases in which extra values appear in the cloud, though these extra values within the compression deviation tolerance. This work item only addresses agent side fixes for range delete. There was a separate bug fix on the cloud side, as described by work item 2824330. Specifically, the cloud service was not processing range delete or individual delete events in the order sent by the agent. Both of these problems are now fixed.
98282	When starting a transfer, a transfer job can fail to start if the transfer job status is requested from the cloud service before all steps are added to the transfer. This bug could affect the startup phase of any transfer. This problem has been fixed.
97194	Fixed thread safety issue when reporting agent progress. The error was reported in the log was: "System.InvalidOperationException: Collection was modified; enumeration operation may not execute."
97167	Transfer edits could cause a very large number of

Work Item	Description
	time ranges to be resent to CONNECT data services. This problem has been fixed.
96143	Windows Authentication is now favored over PI trusts for connections to Data Archive. The authentication order was reversed in all previous versions (2.2.1163 and earlier), where the agent would first try to connect using a PI trust (less secure) before trying to connect using Windows security (more secure).

## 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](#).

## Distribution Kits

Product	Software Version
PI to Data Hub Agent Installation	2.2.1539

©2023 AVEVA Group plc and its subsidiaries. All rights reserved.

## 2.2.1163 release: 06/29/2023

### Overview

This release covers the PI to Data Hub Agent, a component that is installed on-premises to replicate data, assets, and licensed PI point counts from PI System to CONNECT data services.

Version 2.2.1163, released 06/29/2023, is a feature release adding the capability to send the count of created or licensed PI tags to CONNECT through CONNECT data services, which enables customers to take advantage of a new licensing model of AVEVA PI Data Infrastructure – aggregate tag. With this new licensing option, customers no longer need to worry about accurately estimating the count of PI tags needed at every PI Server installation. Instead, they can purchase PI tags in aggregate and be able to use more than the committed number of aggregate tags across any number of deployed PI Servers. PI to Data Hub Agent is required with every PI Server that is part of the aggregate tag model. The aggregate tag model is offered at three tiers of small (100,000 tags), medium (250,000 tags), and large (500,000 tags). These sizes denote the minimum number of aggregate tags to which a customer commits. At any time, the aggregate PI Server tag count may surpass this minimum number, and the customer will be able to pay for the additional tags on a daily rate.

This is also the first release where the PI to Data Hub Agent is available as a feature in the PI Server installation kit. On a new installation, when a user selects the Data Archive server role, the agent feature will also be selected by default. Adding the agent to the PI Server installation kit is part of a larger effort to support hybrid deployments of PI System, with the goal of enabling seamless integration between PI System and CONNECT data services. With this release, customers can configure transfers of on-premises data immediately after installing PI Server.

The PI to Data Hub Agent will also remain available as a separate download from the CONNECT data services portal.

**Note:** PI to Data Hub Agent Version 2.2.1163 is an optional upgrade for existing PI to Data Hub users.

For more information on product features and functions, including system requirements and installation/uninstallation instructions, refer to [PI to CONNECT Agents](#) documentation.

## Enhancements

The following features were added:

- For customers who are on AVEVA PI Data Infrastructure - aggregate tag, the PI to Data Hub Agent now sends license usage information to CONNECT data services. If the Data Archive has a license file corresponding to the aggregate PI point model, then the actual PI point count of the Data Archive will be sent to CONNECT data services. If Data Archive has a traditional PI point count limit, then the maximum PI point count associated with the license will be sent as the usage information. For customers on SRP or AVEVA PI Data Infrastructure (without aggregate tag), license usage information is discarded and not stored in the cloud.
- For a new installation of the PI to Data Hub Agent, the initial connection and registration to CONNECT data services has been moved from the PI to Data Hub Agent installation kit into the PI to Data Hub Agent Configuration Utility. This change facilitates a consistent post-installation user experience whether the agent is installed with the PI Server installation kit or the standalone installer.

## Fixes

There were no fixes in this release.

## 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](#).

## Distribution Kits

Product	Software Version
PI to Data Hub Agent Installation	2.2.1163

©2023 AVEVA Group plc and its subsidiaries. All rights reserved.

## 2.1.0 release: 11/14/2022

### Overview

This release covers the PI to Data Hub Agent, a component that is installed on-premises to replicate data and assets from the PI System to CONNECT data services. Version 2.1, released 11/14/2022, is a feature release addressing change synchronization.

---

**Note:** PI to Data Hub Agent Version 2.1 is a required upgrade for existing PI to Data Hub users. Failure to upgrade will result in loss of ability to configure an AF Server for the PI to Data Hub Agent.

---

For more information on product features and functions, including system requirements and installation/uninstallation instructions, refer to [PI to CONNECT Agents](#) documentation.

### Enhancements

The following features were added:

### Change synchronization

PI to Data Hub now supports change synchronization. If you make a configuration change on your PI System to an item that is part of a transfer, PI to Data Hub will automatically detect and replicate this change to CONNECT data services.

Examples include:

- Changing a PI Point Name
- Changing a PI Point Attribute
- Changing an AF Element Name
- Changing an AF Element Attribute Name
- Changing a PI Point Reference in an AF Attribute
- Adding a PI Point Reference in an AF Element that is part of the transfer.

PI to Data Hub will also replicate changes in data in your PI Server. If you edit archived events in the Data Archive, and that event is part of a PI to Data Hub Transfer, the agent will replicate that change to CONNECT data services.

---

**Note:** The PI to Data Hub Agent and transfer must be running to detect and replicate changes.

---

### Fixes

The following items were resolved:

- PI to Data Hub Agent 2.0 sometimes stopped allowing transfer edits. This has been fixed.
- PI to Data Hub Agent 2.0 sometimes did not allow the user to configure an AF Server. This has been fixed.
- If a transfer is creating a large number of streams, and the user decided to remove the transfer, PI to Data Hub would continue creating the streams. This has been fixed.

## Known issues

- Query search results that contain a very large number of PI points (> 1 million) will generate an exception error and may not be processed.
- The AF Server must have a default Data Archive server specified for PI to Data Hub to operate properly.
- Streams with AF elements and referenced PI points are not deleted even when the **Automatically remove Streams and Assets** option has been selected; this exception includes instances of assets not created for AF elements due to errors (for example, attribute errors).
- Configuring two transfers in the same namespace where the transfers references the same AF element(s) results in the asset properties of one transfer overridden/replaced by the second transfer.

## Security information and guidance

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

AVEVA [proactively discloses](#) 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](#).

## Distribution Kits

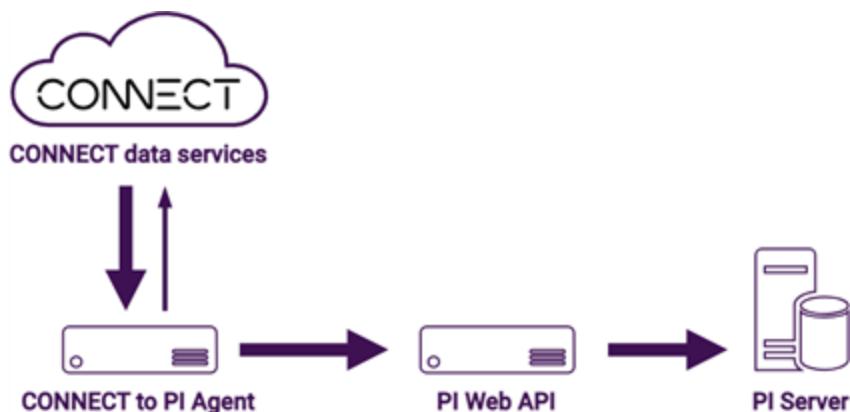
Product	Software Version
PI to Data Hub Agent Installation	2.1

## CONNECT to PI Agents

CONNECT to PI enables you to transfer data from CONNECT data services SDS streams to an on-premises Data Archive. This can be used for many applications, such as performing analysis in the cloud and sending the results to a PI Server.

## CONNECT to PI architecture

The diagram below shows the flow of data when using CONNECT to PI.



The CONNECT to PI Agent communicates with CONNECT data services via REST calls and with the PI Server via the OMF endpoint on the PI Web API.

The agent reads SDS stream data from CONNECT data services to PI and writes OMF stream data to PI Points.

The agent sends health and diagnostics data to CONNECT data services which is presented in the CONNECT to PI Agent portal and is available as SDS stream data.

The agent does not have to be in the same network as the PI Server, but it does need to have access to PI Web API and internet access to CONNECT data services.

## Restrictions of the CONNECT to PI architecture

These are a few restrictions with the existing CONNECT to PI architecture:

- Only one CONNECT to PI Agent can be installed on a given host computer.
- The CONNECT to PI Agent transfers stream data from a namespace to PI Points in a Data Archive. No data is transferred to a PI AF Server.
- Each CONNECT to PI Agent is tied to one Data Archive through the specified PI Web API endpoint.
- The CONNECT data services namespace you select during the agent configuration process is used to store the agent and transfer configuration. However, you can configure a transfer to use any namespace within the given tenant.
- A transfer sends data from a single namespace to a single Data Archive. Multiple transfers can be configured from multiple namespaces within the given tenant, using a single agent, but each transfer sends data to a single Data Archive. A second agent on a second host computer can be configured to transfer data from one or more namespaces to a different Data Archive, if required.

## CONNECT to PI best practices

- We recommend configuring buffering between PI Web API and the Data Archive. For Data Archive collectives, buffering is required. Ensure the PI Buffer Subsystem is configured on the PI Web API node following the procedure detailed in [Buffering services](#).
- If PI Point compression is typically used in the Data Archive, it should be configured after the PI Points are created by the agent. Compression can be set in bulk using tools such as PI Builder. See [Edit PI Points](#). However, no compression will occur, regardless of the PI Point configuration, if the PI Buffer Subsystem is configured. Thus, a decision on the importance of buffering versus compression is required.
- If you are transferring large amounts of historical data from CONNECT data services, we recommend you

increase the buffer size of the agent to avoid buffer overrun. The buffer size is adjustable using the maxBufferSizeMB property in the agent configuration. Increase the buffer size to maximize the buffering capacity while not exceeding the amount of available disk space on the computer. See [Configure agent buffering](#).

- For heavy workloads, install the CONNECT to PI Agent on a host computer that is separate from the PI Web API and Data Archive host computers.
- Keep the CONNECT to PI software version up-to-date. The portal indicates when an agent is out of date and needs to be updated.

## Set up CONNECT to PI Agent

Before you can start transferring data between systems, you will need to set up the CONNECT to PI Agent, which includes connecting to the PI Web API and registering with CONNECT.

You can download the setup kit from the PI Agents page on the CONNECT data services portal and then move it to the computer that will host the agent.

## Required privileges

Certain permissions that are required before you start using the CONNECT to PI Agent.

Privileges	Requirement
Download	To download the CONNECT to PI Agent, you need at least the Tenant Member role (the default role for anyone invited to a tenant) on CONNECT data services.
Installation	To install a CONNECT to PI Agent, you must be an administrator on the agent host computer.
Configuration	To configure a CONNECT to PI Agent after installation, you will need to have the following prepared: <ul style="list-style-type: none"><li>• CONNECT data services: Ensure the user configuring the CONNECT to PI Agent has the Tenant Administrator role in the namespace you plan to use for agent registration.</li><li>• Agent service: If you plan to use Negotiate authentication (Kerberos) to PI Web API, make sure that the desired service account is created and that trust is configured on the PI side.</li><li>• PI Web API: Make sure PI Web API is configured and the OMF endpoint information is available.</li></ul>
Transfer management	To create and manage transfers, you need to have at least the Tenant Contributor role in the namespace where the data resides.

## CONNECT to PI minimum system requirements

The following table lists the system requirements of CONNECT to PI.

System component	Requirement
PI Server	<ul style="list-style-type: none"><li>• AVEVA PI Server 2018 SP3 Patch 3 or later is recommended AVEVA PI Server 2023 or later is required if using OIDC authentication</li></ul>
PI Web API	<ul style="list-style-type: none"><li>• PI Web API 2023 SP1 or later</li></ul>
Operating system	<ul style="list-style-type: none"><li>• Windows 10, Windows 11, Windows Server 2019, or Windows Server 2022 CORE editions of the Windows Server operating systems are supported only with silent installations.</li><li>• Processor: 1 gigahertz (GHz) or faster compatible processor or System on a Chip (SoC)</li><li>• RAM: 4GB</li><li>• Hard drive space: 32GB or larger</li></ul>
Network	<ul style="list-style-type: none"><li>• An Internet connection that allows locally-initiated connections to CONNECT data services port 443.</li><li>• If the agent is installed on a computer other than the PI Web API, a network connection that allows locally-initiated connections into the PI Web API on its configured listener port (443 by default).</li><li>• Internet connectivity of at least 10 Mbps.</li></ul>

## Install the CONNECT to PI Agent

To download the CONNECT to PI Agent, you need at least a Tenant Member role in CONNECT data services. To install the CONNECT to PI Agent, you need the administrator rights on the host computer.

To download and install the CONNECT to PI Agent:

1. In the left pane of the CONNECT data services portal, select **Data Collection > PI Agents**.
2. Select **CONNECT to PI Agents** from the agents dropdown selector.
3. Select **Download Agent**.
4. On the Agent Installer Download window, select **Download**. When the download completes, select **Cancel** to

close the window.

5. Open the downloaded CONNECT to PI Agent installation file.

The Welcome page of the CONNECT to PI Agent window opens.

6. On the Welcome page, select **Next**.

The Configuration page opens.

7. Make changes to the default installation folder and port, if needed, and select **Next**.

---

**Note:** The port is used for agent configuration and administration tasks.

---

8. Select **Install**.

9. After the agent is installed, select **Finish**.

The CONNECT to PI Configuration Utility opens. See [Run the CONNECT to PI Configuration Utility](#) for instructions.

---

**Note:** If the data storage region of the namespace in which your agent will be registered is North Europe ("euno") or East Australia ("auea"), you will need to create a PowerShell script with the following commands and execute it on the machine where the agent is installed. If you are unsure which region your namespace is associated with, navigate to **Developer Tools > API Console** in CONNECT data services and find the prefix of the Full Path.

---

#### North Europe

```
$DataSourceUri = "http://localhost:5590/api/v1/configuration/CloudLink/DataSource";
$response = Invoke-WebRequest -Uri $DataSourceUri
$updatedContent = $response.Content.Replace("//uswe.", "//euno.")
Invoke-RestMethod -Uri $DataSourceUri -Method PUT -Body $updatedContent -ContentType "application/json"
```

#### Australia East

```
$DataSourceUri = "http://localhost:5590/api/v1/configuration/CloudLink/DataSource";
$response = Invoke-WebRequest -Uri $DataSourceUri
$updatedContent = $response.Content.Replace("//uswe.", "//auea.")
Invoke-RestMethod -Uri $DataSourceUri -Method PUT -Body $updatedContent -ContentType "application/json"
```

## Run the CONNECT to PI Configuration Utility

The CONNECT to PI Configuration Utility launches automatically when installation is complete, or it can be launched from **Start > PI System > CONNECT to PI Configuration Utility**.

To use the configuration utility, the CONNECT user must have the Tenant Administrator role in CONNECT data services.

1. If a banner displays the message "Run the utility as administrator to change settings," select **Relaunch as Administrator**.  
The **Configuration / Cloud** page displays.
2. Select **Sign in to CONNECT data services**.
3. Enter your user credentials.

This opens <https://signin.connect.aveva.com/login> in a web browser for login. The browser will indicate that the user has been successfully authenticated. After successful authentication, return to the configuration utility.

---

**Note:** You must have the role of Tenant Administrator.

4. Return to the CONNECT to PI Configuration Utility and enter an **Agent Name**.
  5. Select the **Namespace** field to bring up a list of available namespaces and select the namespace in which your agent will be registered.
  6. Select **Confirm** to verify the connection. An error message will appear if there is an issue.
  7. Select **Next** to continue to the Service Account page.
  8. Select **Edit** to configure the **Service Account**.
  9. Choose the account which CONNECT to PI will run as. See [Authentication](#) for information on Data Archive authentication methods. If using Windows authentication, this account requires write permissions to the PI Server using PI and AF Mappings. See [Create mappings](#) in the PI Server documentation. Select **Edit** to make changes and select the Account Type:
    - **Default Virtual Account** – The default account for the service runs as NT SERVICE\PIAdapterCONNECT.
    - **Custom Account** – Specify a username and password (domain\account) for the Run as user for the CONNECT to PI Agent service.
  10. Select **Confirm** to test the service account credentials.
  11. Select **Next** to continue to the PI Web API page.
  12. Enter your **PI Web API Server URL**.
  13. Select the **Authentication Type** for PI Web API:
    - **Windows** – Uses the Service Account you configured the agent to run as.
    - **Basic** – Specify a username and password.
    - **OpenID Connect** – Specify the Client ID and Client Secret.
  14. Select the checkbox to acknowledge that you understand that the entity selected in the Authentication Type must have a PI and AF mappings to write data. Refer to [Manage mappings](#) in the PI System Management Tools documentation and [PI AF identities and mappings](#) in the PI System Explorer documentation.
  15. Select **Confirm** to test the PI Web API Server authentication.
  16. Select **Next** to continue to the Review page.

The Review page lists all the configuration settings and shows a green checkmark on those items that have been validated. You can select **Edit** next to any setting to return to that page and make changes.
  17. Select **Submit**.
- You should see messages that validation and registration are successful. You can view the successfully registered agent in the CONNECT data services portal by navigating to **Data Collection > PI Agents** page and selecting **CONNECT to PI Agents** from the agents dropdown selector.
- 
- Note:** During registration, a non-expiring client id and client secret required for communication with CONNECT data services are stored on the agent machine. If these client credentials ever need to be replaced, the user can do this by running the utility again, signing into CONNECT data services and then navigating to the Review page where the user can select **Submit** to update their registration.

## Install and configure a CONNECT to PI Agent silently

There are several use cases for doing a silent installation of the CONNECT to PI Agent.

- Silent installations are useful for automating deployments.

- Installations of the CONNECT to PI Agent on Windows Server Core Operating System are supported only with silent installation.

To set up a new installation of a CONNECT to PI Agent without needing to run the CONNECT to PI Configuration Utility:

1. Create a client-credentials client with an assigned role of Tenant Contributor and add a secret. See [Add a client-credentials client](#).

**Note:** Be sure to securely store the Client Id and Client Secret where you can access it again, because this is the only time you will have access to this information. You will need this information to proceed with the silent install.

2. Find the tenantId and record it where you can access it.

When you log into CONNECT data services, the tenantId is visible in the URL. It is the long GUID.

```
https://datahub.connect.aveva.com/tenant/[YOUR TENANT ID]/dashboard
```

Alternatively, select **Developer Tools > API Console** and the tenantId displays in the Full Path. For example:

```
uswe.datahub.connect.aveva.com/api/v1/Tenants/[YOUR TENANT ID]/Namespaces
```

3. Find the namespaceId and record it where you can access it.

Select **Developer Tools > API Console** and select **GET**. The results are listed on the right-hand side of the page under the Body tab. The namespaceId appears as the Id field in the response. The namespaceId is a GUID similar to the tenantId.

**Note:** If you have multiple namespaces, you will have multiple entries in this list. Be sure to select the namespaceId of the namespace where you want the CONNECT to PI Agent to retrieve data.

4. Open a Windows command prompt as an administrator.
5. Change to the folder where you have downloaded the CONNECT to PI Agent installation kit.
6. Enter the following command to install the agent:

```
msiexec /i CONNECTtoPIAgent_SetupKit.exe /qb- /l*v myLog.txt
```

7. Enter one of the following commands, depending on your PI Web API authentication type:

- Windows

```
Aveva.DataHubToPI.ConfigurationUtility.Application.exe register --  
AGENTNAME="<agentName>" --CLIENTID="<clientId>" --CLIENTSECRET="<clientSecret>" --  
TENANTID="<tenantId>" --NAMESPACEID="<namespaceId>" --PIWEBAPIURL="<piWebApiUrl>" --  
PIWEBAPIAUTENTICATIONTYPE="Windows" --AGENTSERVICEUSERNAME="<agentServiceUsername>"  
--AGENTSERVICEPASSWORD="<agentServicePassword>"
```

- Basic

```
Aveva.DataHubToPI.ConfigurationUtility.Application.exe register --  
AGENTNAME="<agentName>" --CLIENTID="<clientId>" --CLIENTSECRET="<clientSecret>" --  
TENANTID="<tenantId>" --NAMESPACEID="<namespaceId>" --PIWEBAPIURL="<piWebApiUrl>" --  
PIWEBAPIAUTENTICATIONTYPE="BASIC" --PIWEBAPIBASICUSERNAME="<piWebApiBasicUsername>"  
--PIWEBAPIBASICPASSWORD="<piWebApiBasicPassword>" --  
AGENTSERVICEUSERNAME="<agentServiceUsername>" --  
AGENTSERVICEPASSWORD="<agentServicePassword>"
```

- OpenID Connect

```
Aveva.DataHubToPI.ConfigurationUtility.Application.exe register --  
AGENTNAME="<agentName>" --CLIENTID="<clientId>" --CLIENTSECRET="<clientSecret>" --  
TENANTID="<tenantId>" --NAMESPACEID="<namespaceId>" --PIWEBAPIURL="<piWebApiUrl>" --  
PIWEBAPIAUTENTICATIONTYPE="OpenIDConnect" --PIWebApiClientId="<piWebApiClientId>" --
```

```
PIWebApiClientSecret="<piWebApiClientSecret>" --
AGENTSERVICEUSERNAME="<agentServiceUsername>" --
AGENTSERVICEPASSWORD="<agentServicePassword>"
```

**Note:** AGENTSERVICEUSERNAME and AGENTSERVICEPASSWORD specify a custom account username and password (domain\account) for the CONNECT to PI Agent service Run as user. Remove these optional parameters to set up CONNECT to PI to run as the default account (NT SERVICE\PIAdapterCONNECT). In the case that Windows PI Web API authentication type is used, this service account requires a PI or AF mapping to read/write to the PI Server.

- Verify your agent is successfully registered and visible in the portal by navigating to **Data Collection > PI Agents** page and selecting **CONNECT to PI Agents** from the agents dropdown selector.

### View CONNECT to PI Agent status

You can view the status of registered agents in the CONNECT data services portal by navigating to **Data Collection > PI Agents** page and selecting **CONNECT to PI Agents** from the agents dropdown selector.

The Status column in the list of agents displays the agent status. Below is a table of the possible values:

Status	Description
Good	The agent is operating normally.
Lost Communication	The agent has lost communication with CONNECT data services.
No data endpoints configured	The agent is running, but endpoint configuration information is missing. To fix the issue, run the CONNECT to PI Configuration Utility and go through the configuration steps.

### Transfer data to a PI Server

After installing and configuring the CONNECT to PI Agent, you are ready to transfer data from CONNECT data services to a PI Server.

You create a data transfer to the configured destination Data Archive by selecting a transfer mode and other transfer settings, then identifying the streams to transfer. After creating the transfer you can start the transfer and monitor its progress.

### Create a CONNECT to PI data transfer

You can create a data transfer for a CONNECT to PI Agent from the PI Agents page.

- In the left pane of the CONNECT data services portal, select **Data Collection > PI Agents**.
- Select **CONNECT to PI Agents** from the agents dropdown selector.
- In the PI Agents page, select the agent for the data transfer.  
The agent details pane displays.
- Select **+ Add Transfer** in the agent details pane.

The Add Transfer window opens.

5. Edit the generated **ID** field, if needed.

---

**Note:** The transfer ID will be used as the Point Source for the PI points created in the Data Archive.

---

6. Enter a name for the transfer in the **Name** field.

7. Select the namespace from the **Namespace** dropdown list.

8. Select a **Transfer Mode**.

- **Streaming with History Recovery:** Streams are transferred normally with automatic backfill for periods of lost connection. This mode does not have a specified end time.
- **History Recovery Only:** Recovers data from a specified start time to a specified end time.

9. Enter your **Start Time**.

10. If you selected **History Recovery Only** as the transfer mode, enter an **End Time**.

11. (Optional) By default the PI Point names that are created in your Data Archive are set to their resolved source stream names. To add a prefix to the PI Point names, enter a value in the **PI Point Name Prefix** field.

12. Select **Continue**.

The Transfer Editor opens.

13. Use the **Search for...** field to search for specific streams.

14. Select the streams to include in the transfer and select **Add**.

The streams are added to the rows on the right. Select a stream to see its details and properties.

15. You may choose to override the **Create Future PI Point** setting that has been automatically configured.

A PI Data Archive must know at the time of PI Point creation whether the PI Point will hold future data. When CONNECT data services detects that a stream has future data this value is set to **Yes**.

16. The PI Point name is set to the resolved stream name with the optional **PI Point Name Prefix**. You can also specify a custom name manually. This is required if the stream name contains characters that are invalid for a PI Point name or duplicates another PI Point name.

- a. Hover over a stream and select the  icon.
- b. Select **Custom Name**.
- c. Enter a name in the **Custom Name** field.
- d. Select **Update**.

17. (Optional) To change any of your transfer settings, select  **Settings**.

---

**Note:** You may not change the name (source) of your namespace here. Editing the namespace resets all selected streams. To change your namespace, you will need to start a new transfer. You may change the Name, Mode, Start Time, and other Advanced Settings. When you are finished making changes to your settings, select **OK**.

---

18. Select **Save and Close** to save and return to the PI Agents page.

The status of the transfer is shown in the agent details pane.

## Edit a CONNECT to PI draft transfer

---

**Note:** You can edit saved transfer settings and add or remove streams **only** if the transfer has not been started. A transfer that has been created but not started is marked *Draft*.

---

To edit a draft version of a transfer:

1. In the PI Agents page, select **CONNECT to PI Agents** from the agents dropdown selector.
2. Select the agent that contains the transfer you want to edit.
3. Identify the transfer marked *Draft* that you want to edit.
4. Select **Edit** under the appropriate transfer in the agent details pane.
5. To add streams to a transfer, enter search criteria on the **Search for...** field, select the streams, then select **Add**.
6. To remove a stream from a transfer, select the  icon next to the stream. The State changes to **Removed**.
7. To enter a custom PI Point name for a stream:
  - a. Hover over a stream and select the  icon.
  - b. Select **Custom Name**.
  - c. Enter a name in the **Custom Name** field.
  - d. Select **Update**.
8. To edit transfer settings, select  **Settings** and then perform the desired action(s):
  - To change the transfer name, enter a new name in the **Name** field.
  - To change the Start Time or End Time, edit the date or time fields or use the calendar control.
  - To change the PI Point Name Prefix, enter a new prefix in the **PI Point Name Prefix** field.
  - Select **Apply** to save these changes.

---

**Note:** You may not change the namespace here. Editing the namespace resets all selected streams. To change your namespace, you will need to start a new transfer.
9. After transfer edits are done, select **Save and Close** to retain these changes and return to the PI Agents page.

## Start a CONNECT to PI data transfer

Once you create a data transfer, you can start the transfer.

---

**Note:** Once a transfer has been started, it cannot be edited.

---

1. In the PI Agents page, select **CONNECT to PI Agents** from the agents dropdown selector.
2. Select the CONNECT to PI Agent associated with the data transfer.
3. In the agent details pane, select **Start** under the appropriate transfer.  
The data transfer begins.
4. You can view the transfer status as data is sent to the agent and stream data is created in the Transfers section of the agent details pane.

The screenshot shows a detailed view of a transfer configuration. At the top, a green play button icon and the text "Wind anomaly scores" are displayed. Below this, a table provides key details:

Status	Good
Namespace	namespace
Stream Count	4
Current Activity	Sending Streaming Data

At the bottom of the configuration pane are five action buttons:

- Edit (pencil icon)
- View (magnifying glass icon)
- Monitor (bar chart icon)
- Stop (blue square icon)
- Remove (trash bin icon)

5. (Optional) To view the transfer configuration, select **View**.
6. (Optional) To view more detailed information about the transfer status, select **Monitor**. See [Monitor CONNECT to PI data transfer metrics](#).
7. (Optional) To stop a transfer, select **Stop**.
8. (Optional) To remove a transfer, select **Remove**.

## Transfer status

Once a transfer is configured, saved, and started, you can check the status of the transfer in the Transfers section of the agent details pane. Below is a table of the possible transfer status values:

Status	Description
Good	The transfer is operating as expected.
Warning	There may be a problem, though one that could be ignored.
Bad	There is a serious problem that will cause issues until remedied.

## Monitor CONNECT to PI data transfer metrics

To view CONNECT to PI transfer progress, select **Monitor** under the appropriate transfer in the agent details pane. This opens the Metrics window. The following table lists these data statuses and their meanings.

Category	Metric	Meaning
General	Stream Count	The number of streams in the transfer.  Stream count is also sent by the agent to CONNECT data services and stored in a stream that is available for viewing and analysis.  Stream name: StreamCount  Stream Id: <agent host machine name>.CONNECT.<transfer name>.StreamCount
General	Average Data Rate	The 1-minute rolling average rate at which data is received by the agent.  Average data rate is also sent by the agent to CONNECT data services and stored in a stream that is suitable for viewing and analysis.  Stream name: IORate  Stream Id: <agent host machine name>.CONNECT.<transfer name>.IORate
General	Average Error Rate	The 1-minute rolling average rate at which errors occur while data is being received by the agent.  Average error rate is also sent by the agent to CONNECT data services and stored in a stream that is suitable for viewing and analysis.  Stream name: ErrorRate  Stream Id: <agent host machine name>.CONNECT.<transfer name>.ErrorRate
General	Current Activity	The current transfer activity. Possible values are Sending Streaming Data, Sending Backfill Data, Sending Historical Data, or Inactive.
Streaming	Total Streamed Events	The total number of streaming events transferred to the agent during the transfer lifetime.
Streaming	Last Update Time	The last time at which a streaming

Category	Metric	Meaning
		event was received by the agent.
Streaming Backfill	Total Backfilled Events	The total number of streaming events recovered during the transfer lifetime. Recovery is necessary only when the agent has been offline for more than one hour, which causes the agent's bookmark into the Change Broker service to be invalidated. No data loss will occur as long as events are written in time order.
History Recovery	Historical Transfer	The completion percentage of the historical transfer. History recovery occurs only once during the transfer lifetime.
History Recovery	Recovered Events	The total number of historical events recovered during the transfer lifetime.

## CONNECT to PI Agent maintenance

CONNECT to PI Agents require maintenance from time to time. This section explains how to uninstall, update, repair, search for, and view performance metrics for agents.

### View CONNECT to PI Agent metrics

You can quickly view key performance indicator (KPI) metrics for installed CONNECT to PI Agents on the home page.

To view CONNECT to PI Agent metrics:

1. To open the portal home page, select **Home** in the left pane.

The screenshot shows the AVEVA CONNECT Data services dashboard. On the left is a vertical navigation bar with icons for Home, Services, Data, PI, Security, and Help. The main area has several tiles:

- Latest Service Updates:** CONNECT to PI Agent 1.0.1470 is released on Aug 14, 2024, at 10:41:46 AM. A detailed description follows.
- Quick Links:** Includes links to API documentation, code samples, service blog, user management, client secrets, and REST API console.
- Yesterday's Resource Usage:** Stream statistics: Stored 22,204, Accessed 7,112, Shared Streams Accessed 3.
- System Health:** Shows a green heart icon and the status "Ok".
- PI to CONNECT Agents:** 18 Total Agents. Breakdown: 5 Good, 0 Warning, 13 Bad, 0 Stopped.
- Systems:** 21 Total Systems. Breakdown: 5 Good, 15 Warning, 1 Bad, 0 Stopped.
- CONNECT to PI Agents:** 18 Total Agents. Breakdown: 4 Good, 14 Warning, 0 Bad.

- View the information in the CONNECT to PI Agents tile to see the current state of your agents. States are:
  - Good
  - Warning
  - Bad
- To see the agents on the PI Agents page filtered by state, select the state on the CONNECT to PI Agents tile.

## Repair a CONNECT to PI Agent

An agent installed on a host machine may need to be repaired to fix and update files.

To repair an agent:

- Select Windows **Start**, then select **Settings > Apps > Apps & features**.
- In the Settings window, select **CONNECT to PI Agent** in the list of installed apps, select **Modify**, and then select **Yes**.
- In the CONNECT to PI Agent window, select the **Repair** option, and then select **Next** twice. The Installation window opens and the repair process begins.
- After the repair process has completed, select **Close** to exit.

## Search for a CONNECT to PI Agent

You can search for CONNECT to PI Agents that have been installed on host machines at your organization to quickly locate agents of interest. For example, you may want to remove older agents. The global filter feature allows you to search by agent name, status, version number, namespace, or Data Archive.

To search for an agent in the portal:

1. In the left pane, select **Data Collection > PI Agents**.
2. Select **CONNECT to PI Agents** from the agents dropdown selector.
3. In the **Filter Agents** field, enter the first few characters of the agent's name or version number.  
Agents that meet the filter criteria are displayed in the list of agents.
4. (Optional) To clear the search, remove all characters from the **Filter Agents** field.

## Remove a CONNECT to PI Agent

You remove a CONNECT to PI Agent by first uninstalling it from the host machine and then the portal. There are two parts to removing an agent:

- Uninstall the agent from the host machine.
- Remove the agent listing in CONNECT data services.

## Uninstall the CONNECT to PI Agent on the host machine

To remove the CONNECT to PI Agent application from a host machine, uninstall it from the Apps & features window and then follow the prompts in the CONNECT to PI Agent window.

1. Select Windows **Start**, then select **Settings > Apps > Apps & features**.
2. In the Apps & features window, select **AVEVA CONNECT to PI Agent** in the list of installed apps.
3. Select **Uninstall** twice, then select **Yes** in the User Account Control window.

The CONNECT to PI Agent application is uninstalled on the host machine.

## Remove the CONNECT to PI Agent on the portal

To remove the agent from the portal:

1. In the left pane, select **Data Collection > PI Agents**.
2. Select **CONNECT to PI Agents** from the agents dropdown selector.
3. Select an agent in the list.
4. In the agent details pane, select **More Options :** > **Remove Agent**.
5. In the Remove Agent window, select **Remove**.

The agent is removed in the portal.

## Health and diagnostics

The CONNECT to PI Agent produces various types of health and diagnostics data. For details around the different health and diagnostics data available to you, see the following:

- [Health](#)
- [Diagnostics](#)

### Health

#### Available health data

The following health data is available for each transfer configured on an agent and for the agent's data egress component (which is named OmfEgress):

- Device status
- Next health message expected

This health data is sent every minute from the agent to CONNECT data services.

The health information for each transfer and for the agent's OmfEgress component are available in the following streams.

- Stream name: DeviceStatus  
Stream Id: <agent host computer name>.CONNECT.<transfer name>.DeviceStatus
- Stream name: NextHealthMessageExpected  
Stream Id: <agent host computer name>.CONNECT.<transfer name>.NextHealthMessageExpected
- Stream name: DeviceStatus  
Stream Id: <agent host computer name>.CONNECT.OmfEgress.DeviceStatus
- Stream name: NextHealthMessageExpected  
Stream Id: <agent host computer name>.CONNECT.OmfEgress.NextHealthMessageExpected

### Device Status

The device status indicates the health of each transfer and if it is currently communicating properly with CONNECT data services. A device status is also available for the agent's OmfEgress component. This time-series data is stored within a CONNECT data services stream. During healthy steady-state operation, a value of Good is expected.

Property	Type	Description
Time	string	Timestamp of the event
DeviceStatus	string	The value of the DeviceStatus

The possible statuses are:

Status	Meaning
Starting	The component is currently starting up and is not yet connected to the data source.
Shutdown	The component is either in the process of shutting down or has finished.
Not Configured	The agent component has been created but is not yet configured.

### Next health message expected

This property is similar to a heartbeat. A new value for NextHealthMessageExpected is sent by each transfer on a periodic basis while it is functioning properly. This value is a timestamp that indicates when the next value should be received.

When monitoring, if the next value is not received by the indicated time, this likely means that there is an issue. It could be, for example, an issue with the agent, with a transfer, or with the network connection between the agent and CONNECT data services.

The following table describes the associated properties:

Property	Type	Description
Time	string	Timestamp of the event
NextHealthMessageExpected	string	Timestamp when next value is expected

### Diagnostics

The each transfer produce various kinds of diagnostics data that is sent to CONNECT data services. The agent also sends diagnostics data about its OmfEgress component and its host computer.

### Available diagnostics data

The following diagnostics data are available:

- IO rate
- Error rate
- Stream count
- System

This diagnostics data is sent every minute from the agent to CONNECT data services.

The diagnostics information for each transfer and for the agent's host computer are available in the following streams.

- Stream name: IORate  
Stream Id: <agent host computer name>.CONNECT.<transfer name>.IORate
- Stream name: ErrorRate  
Stream Id: <agent host computer name>.CONNECT.<transfer name>.ErrorRate
- Stream name: StreamCount  
Stream Id: <agent host computer name>.CONNECT.<transfer name>.StreamCount
- Stream name: IORate  
Stream Id: <agent host computer name>.CONNECT.OmfEgress.<endpointId>.IORate
- Stream name: System  
Stream Id: <agent host computer name>.CONNECT.System.Diagnostics

## IO rate

The IORate stream information.

Property	Type	Description
timestamp	string	Timestamp of event
IORate	double	One-minute rolling average of data rate (streams/second)

## Error rate

The ErrorRate stream information.

Property	Type	Description
timestamp	string	Timestamp of event
ErrorRate	double	One-minute rolling average of error rate (streams/second)

## Stream count

The StreamCount stream details.

Property	Type	Description
timestamp	string	Timestamp of event
StreamCount	int	Number of streams created by the transfer
TypeCount	int	Number of types created by the transfer

**OMF egress IO rate**

The OmfEgress IORate stream information.

Property	Type	Description
timestamp	string	Timestamp of event
IORate	double	One-minute rolling average of data rate (streams/second)

**System**

The System stream information. This diagnostic stream contains system level information related to the host computer that the agent is running on.

Property	Type	Description
timestamp	string	Timestamp of event
ProcessIdentifier	int	Process Id of the host process
StartTime	string	Time at which the host process started
WorkingSet	long	Amount of physical memory in bytes, allocated for the host process
TotalProcessorTime	double	Total processor time for the host process expressed in seconds
TotalUserProcessorTime	double	User processor time for the host process expressed in seconds
TotalPrivilegedProcessorTime	double	Privileged processor time for the host process expressed in seconds
ThreadCount	int	Number of threads in the host process
HandleCount	int	Number of handles opened by the host process
ManagedMemorySize	double	Number of bytes currently thought to be allocated in managed memory Unit of Measure = megabytes
PrivateMemorySize	double	Amount of paged memory in bytes

Property	Type	Description
		allocated for the host process Unit of Measure = megabytes
PeakPagedMemorySize	double	Maximum amount of memory in the virtual memory paging file in bytes used by the host process. Unit of Measure = megabytes
StorageTotalSize	double	Total size of the storage medium in use by the system Unit of Measure = megabytes
StorageFreeSpace	double	Free space available Unit of Measure = megabytes

## Troubleshoot CONNECT to PI

The CONNECT to PI Agent provides features for troubleshooting issues related to connectivity, data flow, and configuration. For more information, check the pages specific to the issues you are seeing.

### Troubleshoot CONNECT to PI connection issues

#### Check connectivity and data flow

Perform the following steps to verify active connections to the data endpoints.

1. Verify CONNECT data services is operational.
  - a. Log into CONNECT data services.
  - b. View the **System Health** tile. A healthy system will display a green heart icon with a status of Ok.
  - c. Select the **System Health** tile to view detailed information on the health of all CONNECT data services. Healthy services will display a green check mark.
2. Verify the status of the agent.
  - a. From the CONNECT data services portal, select **Data Collection > PI Agents**, then select **CONNECT to PI Agents** from the agents dropdown selector.
  - b. Verify the agent status from the table. A healthy agent will have a *Good* status. An agent that is not connected to CONNECT data services will have a *Lost Communication* status. An agent that is missing data endpoint configuration will have a *No data endpoints configured* status; this can be fixed by running the CONNECT to PI Configuration Utility to recreate configuration files.
3. Verify the transfer is operational and transferring data. From the **CONNECT to PI Agents** page:
  - a. Select an agent.
  - b. Select a transfer.
  - c. Select **Monitor** on the transfer dialog.

- d. Verify data flow using the metrics Average Data Rate, Average Error Rate, Total Streaming Events, and Last Update Time.
4. Verify the data streams configured for transfer in the agent have data available for transfer.
  - a. From the CONNECT data services portal, select **Data Collection > PI Agents**, then select **CONNECT to PI Agents** from the agents dropdown selector.
  - b. Select an agent.
  - c. Select a transfer.
  - d. Select **View** on the transfer dialog.
  - e. Select a stream.
  - f. Select **View in Trend**.
  - g. From the trend, verify there is data available.
5. Verify the PI Point values are updating in the PI Server.
  - a. Open PI System Management Tools (PI SMT).
  - b. Use the Archive Editor to search for the PI Points and verify there is data available.
  - c. Refer to [PI System Management Tools 2023](#) for more details.
6. For additional details on agent connectivity and data flow, check the agent's [health and diagnostics](#) information.

## Agent health and diagnostics

The agent sends health and diagnostics information about itself, its host computer, and its network connectivity to CONNECT data services. The agent health and diagnostics information is available in the CONNECT data services portal, and reflected in the transfer Metrics window, but it is also available as data streams that can be viewed and analyzed. In addition, each transfer configured on the agent will send health and diagnostics information.

## CONNECT to PI Agent logs

The CONNECT to PI Agent writes daily log messages for the agent, the system, individual transfers, and OMF egress to flat text files in the following location:

%ProgramData%\OSIsoft\Adapters\CONNECT\Logs

Each message in the log displays the message severity level, timestamp, and the message itself.

Optionally, you can change the Log Level for each of these components via programmatic means using REST API calls. The most commonly used tools are Postman and Edge Command Utility.

To configure logging:

1. Using a text editor, create an empty text file.
2. Copy and paste the following example configuration for logging into the file:

```
{  
  "logLevel": "Information",  
  "logFileSizeLimitBytes": 34636833,  
  "logFileCountLimit": 31  
}
```

3. Update the example JSON parameters for your environment. See Logging parameters below for a table of all available parameters.
4. Save the file. For example, **ConfigureLogging.json**.
5. To initialize the logging configuration, send the **ConfigureLogging.json** content as request body by Postman (which uses the PUT method) to "http://localhost:5590/api/v1/configuration/<ComponentId>/Logging". You can change the Log Level for the following components:
  - System
  - OmfEgress
  - Individual Transfers

## Log levels

The following table describes the severity levels for messages.

Level	Description
Trace	<p>Logs that contain the most detailed messages. These messages may contain sensitive application data like actual received values, which is why these messages should not be enabled in a production environment.</p> <p><b>Note:</b> Trace is translated to Verbose in the log file.</p>
Debug	Logs that can be used to troubleshoot data flow issues by recording metrics and detailed flow-related information.
Information	<p>Logs that track the general flow of the application. Any non-repetitive general information like the following can be useful for diagnosing potential application errors:</p> <ul style="list-style-type: none"><li>• Version information related to the software at startup</li><li>• External services used</li><li>• Data source connection string</li><li>• Number of measurements</li><li>• Egress URL</li><li>• Change of state "Starting" or "Stopping"</li><li>• Configuration</li></ul>
Warning	Logs that highlight an abnormal or unexpected event in the application flow that does not otherwise cause the application execution to stop. Warning messages can indicate an unconfigured data source state, an insecure communication channel in use, or any other

Level	Description
	event that could require attention but that does not impact data flow.
Error	Logs that highlight when the current flow of execution is stopped due to a failure. These should indicate a failure in the current activity and not an application-wide failure. It can indicate an invalid configuration, unavailable external endpoint, internal flow error, and so on.
Critical	Logs that describe an unrecoverable application or system crash or a catastrophic failure that requires immediate attention. This can indicate application-wide failures like beta timeout expired, unable to start self-hosted endpoint, unable to access vital resource (for example, Data Protection key file), and so on.  <b>Note:</b> Critical is translated to Fatal in the log file.
None	Logging is disabled for the given component.

## Logging parameters

Parameter	Required	Type	Description
logLevel	optional	reference	<p>The LogLevel sets the minimum severity for messages to be included in the logs.</p> <p>Messages with a severity below the level set are not included.</p> <p>The log levels in their increasing order of severity are as follows: Trace, Debug, Information, Warning, Error, Critical, and None.</p> <p>Default: Information</p> <p>For detailed information about the log levels, see Log</p>

Parameter	Required	Type	Description
			levels.
logFileSizeLimitBytes	optional	integer	<p>The maximum size (in bytes) of log files that the service creates for the component. The value must be a positive integer.</p> <p>Minimum value: 1000</p> <p>Maximum value: 9223372036854775807</p> <p>Default: 34636833</p>
logFileCountLimit	optional	integer	<p>The maximum number of log files that the service creates for the component. The value must be a positive integer.</p> <p>Minimum value: 1</p> <p>Maximum value: 2147483647</p> <p>Default: 31</p>

## REST URLs

Relative URL	HTTP verb	Action
api/v1/configuration/System/Logging	GET	Retrieves the system logging configuration.
api/v1/configuration/System/Logging	PUT	Updates the system logging configuration.
api/v1/configuration/ <i>ComponentId</i> /Logging	GET	Retrieves the logging configuration of the specified agent component.
api/v1/configuration/ <i>ComponentId</i> /Logging	PUT	Updates the logging configuration of the specified agent component.

Relative URL	HTTP verb	Action
ging		agent component.

**Note:** Replace *ComponentId* with the Id of your agent component.

## CONNECT to PI Agent buffering

You can configure the CONNECT to PI Agent to buffer data egressed from the agent. The default maximum buffer size is 1024 MB. If you are transferring a large amount of data, you should increase the size of this buffer to ensure that all data is transferred correctly. Buffering is configured through the buffering configuration parameters in the system configuration.

**Note:** We recommend that you do not modify the default buffering location unless it is necessary. Changes to the buffering configuration parameters only take effect during agent service startup.

## Configure buffering

Complete the following steps to configure buffering. Use the PUT method in conjunction with the <http://localhost:5590/api/v1/configuration/system/buffering> REST endpoint to initialize the configuration.

1. Using a text editor, create an empty text file.
2. Copy and paste an example configuration for buffering into the file.  
For sample JSON, see the Retrieve the buffering configuration example below.
3. Update the example JSON parameters for your environment.  
For a table of all available parameters, see the Buffering parameters section.
4. Save the file. For example, `ConfigureBuffering.json`.
5. Open a command line session. Change directory to the location of `ConfigureBuffering.json`.
6. To initialize the buffering configuration, send the `ConfigureBuffering.json` content as request body by Postman (which uses the PUT method) to "`http://localhost:5590/api/v1/configuration/System/Buffering/`"

**Note:** If you installed the agent to listen on a non-default port, update 5590 to the port number in use.

For a list of other REST operations you can perform, like updating or replacing a buffering configuration, see the REST URLs section below.

## Buffering parameters

The following parameters are available for configuring buffering:

Parameter	Required	Type	Description
<b>enablePersistentBuffering</b>	Optional	boolean	<p>Enables or disables on-disk buffering.</p> <p>Allowed value: true or false</p> <p>Default value: true</p> <p><b>Note:</b> If you disable persistent buffering, in-memory buffering is used. On-disk and in-memory buffering are limited by value in the <b>MaxBufferSizeMB</b> property.</p>
<b>maxBufferSizeMB</b>	Optional	integer	<p>Defines the maximum size of the buffer that is persisted on disk<sup>1</sup> or used in memory<sup>2</sup>. The unit is specified in MB (1 Megabyte = 1048576 bytes). Consider the capacity and the type of storage medium to determine a suitable value for this parameter.</p> <p>Minimum value: 1 Maximum value: 2147483647 Default value: 1024</p> <p><b>Note:</b> The <b>MaxBufferSizeMB</b> property is applied to each configured endpoint. For example, if you set the <b>MaxBufferSizeMB</b> to 1024 and you configured the agent to send data to two endpoints (for example, AVEVA PI Server and CONNECT data services), the total maximum resources used for buffering will be 2048. The health endpoint is an</p>

Parameter	Required	Type	Description
			exception fixed at 20 MB.
<b>bufferLocation</b>	Required	string	<p>Defines the location of the buffer files. Absolute paths are required. Consider the access-control list (ACL) when you set this parameter. <b>BufferLocation</b> is used to buffer files when <b>EnablePersistentBuffering</b> is true.</p> <p>Allowed value: Valid path to a folder location in the file system  Default value:  Windows :%ProgramData%\OSIsoft\Adapters\CONNECT\Buffers</p>

<sup>1</sup> **Buffering to disk** - disk is only used if required:

- Data is only written to the disk buffer if queued in the memory buffer for more than 5 seconds.
- The **MaxBufferSizeMB** is applied per configured endpoint except the health endpoint.
- An agent creates 20 MB buffer files that are stored in **BufferLocation**.
- When **MaxBufferSizeMB** is reached, the oldest buffer file is deleted and a new buffer file is created.
- The health endpoint is fixed at 20 MB. When the health endpoint buffer file becomes full, a new buffer file is created and the previous buffer file is deleted.

The following rules apply in case of an error when creating a new buffer file:

- Attempt to delete oldest buffer file and retry.
- If unable to buffer, errors are logged to indicate data loss.
- If a buffer file is corrupted, an attempt is made to recover individual records and any failure to recover records is logged.

<sup>2</sup> **Buffering only to memory**:

- The **MaxBufferSizeMB** is applied per configured endpoint except the health endpoint.

- When **MaxBufferSizeMB** is reached, the oldest messages in the memory buffer are removed. Depending on the size of a new message, several old messages may be removed.
- The health endpoint is fixed at 20 MB. When the health endpoint buffer file becomes full, the oldest messages in the memory buffer are removed and new messages are added.

## Examples

The following examples are buffering configurations made through Postman.

### Retrieve the buffering configuration

```
GET "http://localhost:5590/api/v1/configuration/system/buffering"
```

Sample output:

```
{  
  "bufferLocation": "C:/ProgramData/OSIsoft/Adapters/CONNECT/Buffers",  
  "maxBufferSizeMB": 1024,  
  "enablePersistentBuffering": true  
}
```

200 OK response indicates success.

### Update MaxBufferSizeMb parameter

```
"PATCH http://localhost:5590/api/v1/configuration/system/buffering"  
{  
  "MaxBufferSizeMB": 100  
}
```

204 No Content response indicates success.

## REST URLs

Relative URL	HTTP verb	Action
api/v1/configuration/system/buffering	GET	Gets the buffering configuration
api/v1/configuration/system/buffering	PUT	Replaces the existing buffering configuration
api/v1/configuration/system/buffering	PATCH	Update parameter, partial configuration

## CONNECT to PI 1.0.1523 Release Notes

Adapter Framework: **1.8.3.49**

## Overview

CONNECT to PI Agent is a hybrid data connectivity software that delivers an intuitive user experience for natively managing the transfer of data from CONNECT data services to AVEVA PI Server. Together with PI to CONNECT Agent, you can now manage bi-directional data flow between PI Server and the CONNECT industrial intelligence platform.

CONNECT to PI Agent empowers customers by:

- Marrying the power of the cloud with the industry-leading AVEVA PI Server capabilities
- Enhancing collaboration between operations domain experts and other stakeholders
- Sending model and analytic results in the cloud back on-premises to turn insights into action using their familiar tools and existing workflows

## Features

CONNECT to PI Agent enables users to:

- Transfer CONNECT data services streams from a tenant to PI Tags in AVEVA PI Server
  - Natively supports real-time, historical, and future data transfer
  - Works with simple and complex stream types
  - Allows backfilling PI Tags from the cloud
- Centrally create, configure, and manage transfers within the CONNECT portal
- Authenticate to the PI Web API OMF endpoint with OIDC, Kerberos, or Basic

## CONNECT to PI Agent components

This hybrid release includes the following elements:

- **CONNECT to PI Agent Portal:** A web page in CONNECT where users can download the CONNECT to PI install kit and centrally create, configure, and manage data transfers.
- **CONNECT to PI Agent:** An installable agent that moves data from CONNECT data services to PI and creates tags as required via OMF and the PI Web API OMF endpoint. For architecture, basic data flow, and technical requirements and prerequisites, please see the documentation.

For more information, see [CONNECT to PI Agents](#).

## Security information and guidance

We are [committed to releasing secure products](#).

We [proactively disclose](#) aggregate information about the number and severity of security vulnerabilities addressed in each release.

## Overview of new vulnerabilities fixed or mitigated

This section is intended to provide relevant security-related information to guide your installation or upgrade decision. AVEVA is proactively disclosing aggregate information about the number and severity of CONNECT to PI Agent security vulnerabilities that are fixed in this release.

For this initial release of CONNECT to PI Agent, the following vulnerabilities have been identified.

#### Vulnerability Mitigations in CONNECT to PI Agent 1.0.1523 Release

Component	Version	CVE or Reference	CVSS	Mitigation
Microsoft.AspNetCore.Components.WebView.Maui	8.0.70	<a href="#">CVE-2024-35264</a>	8.1	Vulnerable code is not in execution path.
Mudblazor	6.21.0	<a href="#">CVE-2024-35264</a>	8.1	Vulnerable code is not in execution path.
System.Text.Json	8.0.3	<a href="#">CVE-2024-30105</a>	7.5	Vulnerable code is not in execution path.

#### Distribution Kits

Product	Software Version
CONNECT to PI Agent Installation	1.0.1523

©2024 AVEVA Group plc and its subsidiaries. All rights reserved.

## OMF connections

You can use Open Message Format (OMF) for programmatic access to data. OMF defines a set of message headers and bodies you can use to transfer data to CONNECT data services. Because it does not depend on a particular protocol, such as HTTP, you can use OMF to develop data-acquisition applications on platforms and in languages for which there are no supported AVEVA libraries. Using OMF, you can integrate data collection directly into a device or asset.

## OMF connections best practices

Successful OMF connections depend on using the correct client credentials and configuring security correctly. We recommend the following best practices for OMF connections:

- Each type of application or system that sends OMF data to CONNECT data services should have its own defined OMF connection, with the name and description referencing the data source.
- Each application instance or each device that sends OMF data to CONNECT data services should have its own client credentials client and its own secret. Connections allow a list of clients to be defined. When each application instance or device has its own client, security is improved because secrets can be managed at a granular level.
- The client credentials client should have the minimum roles and access. For example, a client may be granted access to write data, but it does not have permissions to delete data. Note, however, the permissions

associated with the OMF connection are separate from the client's permissions, and restrictions on the client do not impact permissions on OMF messages.

- For use cases that involve a large number of source applications or source devices, the API can be used to automatically assign a new client credentials client and secret whenever a new device is brought online.

## Configure an OMF connection

To send Open Message Format (OMF) data to CONNECT data services, you must first configure an OMF connection.

### Prerequisite

An OMF connection requires a client-credentials client.

### To configure an OMF connection

To configure an OMF connection:

1. In the left pane, select **Data Collection > OMF Connections**.
2. In the toolbar, select **Add OMF Connection**.  
The Add Connection pane appears.
3. In the Add Connection pane, complete the following fields:
  - **Name** – Enter a name for the OMF connection.
  - **Description** – (Optional) Enter a description for the connection.
4. Select **Add Client**.
5. Select a client in the list and select **Assign** to add it to the assigned clients.
6. Select **Save**.

An application can now use the selected client-credentials client to write OMF data to the namespace.

## Maintain an OMF connection

### Edit a connection

To edit an existing connection:

1. In the left pane, select **Data Collection > OMF Connections**.
2. Select an existing connection.
3. In the Connection pane, select **Edit Connection** .
4. In the Edit Connection pane, edit the name, description, and assigned clients of the connection.
5. Select **Save**.

## Remove a connection

To remove an existing connection:

1. In the left pane, select **Data Collection > OMF Connections**.
2. Select an existing connection.
3. In the Connection pane, select **More Options :** > **Remove OMF Connection**.
4. Select **Remove** to confirm.

## Set permissions for a connection

To set permissions for a connection:

1. In the left pane, select **Data Collection > OMF Connections**.
2. Select a connection.
3. In the Connection pane, select **More Options :** > **Manage Permissions**.  
The Manage Permissions window appears.
4. To add a role, select **Add Role** and choose a role from the dropdown list.
5. For any role listed, select **Allow** or **Deny** for each of the following permissions: **Read**, **Write**, **Delete**, and **Manage Permissions**.
6. Select **Save**.

# Visualization

The Visualization menu provides tools to allow you to view data trends and use assets to set up digital twins of real-world physical entities:

- Use the Trend page to monitor assets and streams, anticipate problems, and proactively perform preventative maintenance. On the Trend page, you can convert stream data to a graphic view, which can reveal patterns in data, data anomalies, or trouble spots. You can also visualize data from streams shared into a community from another tenant.
- Use the Asset Explorer page to create assets, then visualize data streams and properties to troubleshoot and analyze the associated devices.

## Create a trend session

Use trace data in a trend session to monitor assets, anticipate problems, and proactively perform preventative maintenance.

To create a trending session:

1. In the left pane, select **Visualization > Trend**.
2. In the Add Traces pane, select the **Assets or Streams** tab.

---

**Note:** Communities are only available for selection from the **Streams** tab.

3. Add one or more traces to the trend session.

To search for a trace, enter the asset name, stream name, or description in the **Enter search query** field. For more information on other ways to query, see [Search queries](#). When adding asset traces (but not stream traces), the search field includes autocomplete functionality.

After you find the traces that you want, select the **Add +** icon to add them to the Trend.

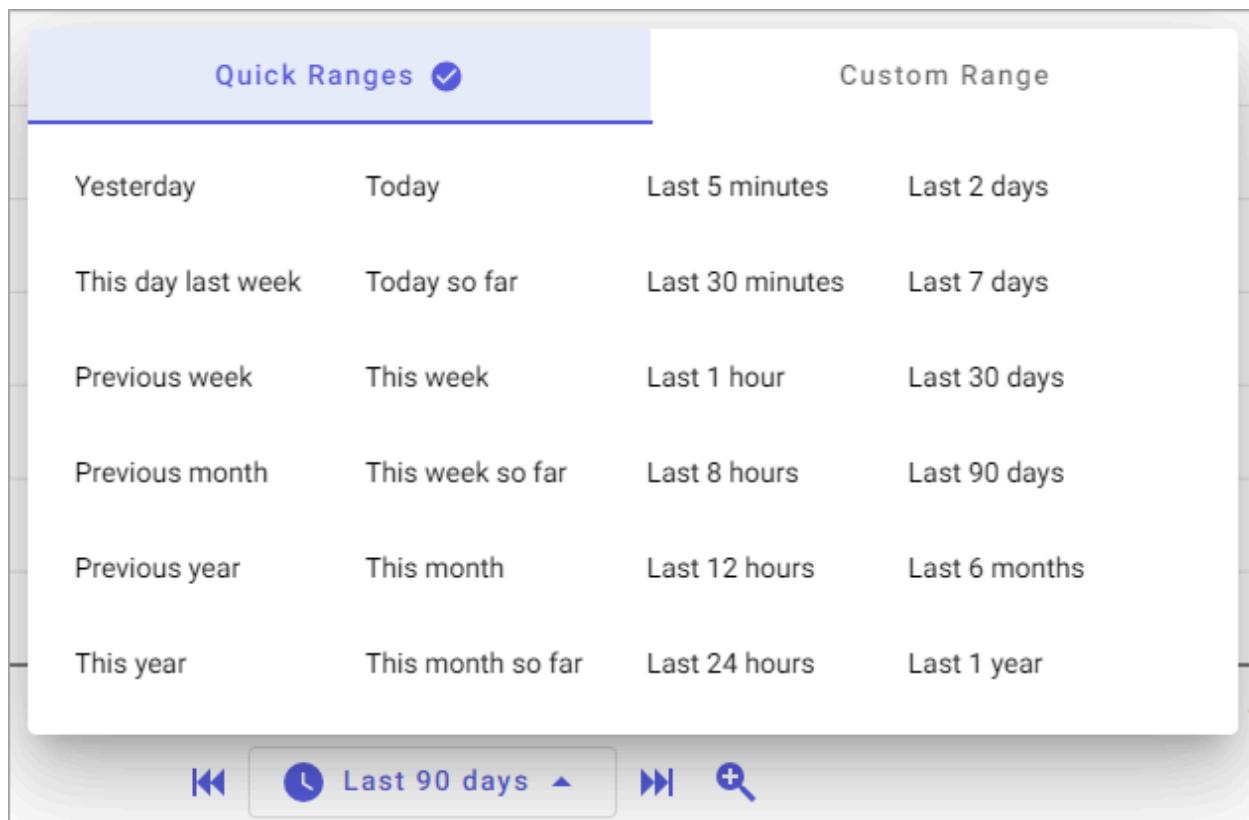
When you finish adding traces, select the **Close X** icon in the Add Traces pane to hide the pane and maximize the available area to display the trend session.

4. From the **Change Y-axis Mode**  menu, select a view:

Trend View	Icon	Description
Single mode		All traces display with the same scale on the same trend.
Multiple mode		Each trace displays with its own scale and all traces are on the same trend.
Stacked mode		Each measurement plots on its own trend.

5. From the **Time picker**, select the time range to view.

- Select the **Quick Ranges** tab to choose a predefined time range.
- Select the **Custom Range** tab to choose your own time range.



6. Select **Step backward** or **Step forward** to move the time range of the data displayed in the trend session.

The trace will move in time increments displayed in the time range picker. For example, if the trend session displays the last 8 hours, **Step backward** shows the previous 8-hour period. If it displays the last 30 days, **Step forward** shows the next 30-day period. Select the triangle to select another time range or specify a custom range.

The **Trend legend** displays the **Trend view** . It shows the legend for each trace, the last value, minimum, maximum, and average values in the displayed time range.

7. From the legend table, select a trace to view it for further analysis.

The selected trace is highlighted and two cursors automatically mark the minimum and maximum values for the displayed time range. These cursors, called *easy cursors*, remain as long as the trace is highlighted.



8. Select the **Add**  icon above the trace to lock the cursors in place.

The **Add**  icon turns into a **Close**  icon. To unlock the cursor, select the **Close**  icon.

**Note:** When two cursors are locked, the **Trend legend** displays summary calculations for the values between the two cursors, known as the **Cursor view** .

9. Select the **Share**  icon in the menu bar to copy the URL of the trend session.

You can share this URL with colleagues to give them the same view of the trend session that they can use to troubleshoot problems.

## Download trend data

After you create a trend session that includes traces from assets, streams, or both, you can download the data depicted in the trend session as a .csv file.

1. In the left pane, select **Visualization > Trend**.
2. Create a trend session using the instructions available in [Create a trend session](#).
3. From the toolbar, select **Download CSV**.
4. Select the data from the trend session that you want to download. Each option is downloaded as a separate .csv file.

- **Trend Data:** Downloads the data depicted in the **Trend** pane.
  - **UOM/Summary Data:** Downloads the data listed in the **Legend** table.
- For more information on the **Trend** and **Legend** panes, see [Trend visualization](#).

## 5. Select Download.

The selected trend session data is downloaded as .csv files.

**Note:** When downloading trend session data, the data is not retrieved from the trend session—rather, the data is retrieved from the assets and streams. This approach allows the downloaded data to include the actual stream data points, as the the data does not include interpolated or calculated data included in the trend session.

## Trend visualization

Use the Trend page to show data from assets and streams in a graphical format that traces the data over a specified period of time. Use trace data in a trend to monitor assets, anticipate problems, and proactively perform preventative maintenance. Display traces in a trend to better understand the data and gather useful information from it.

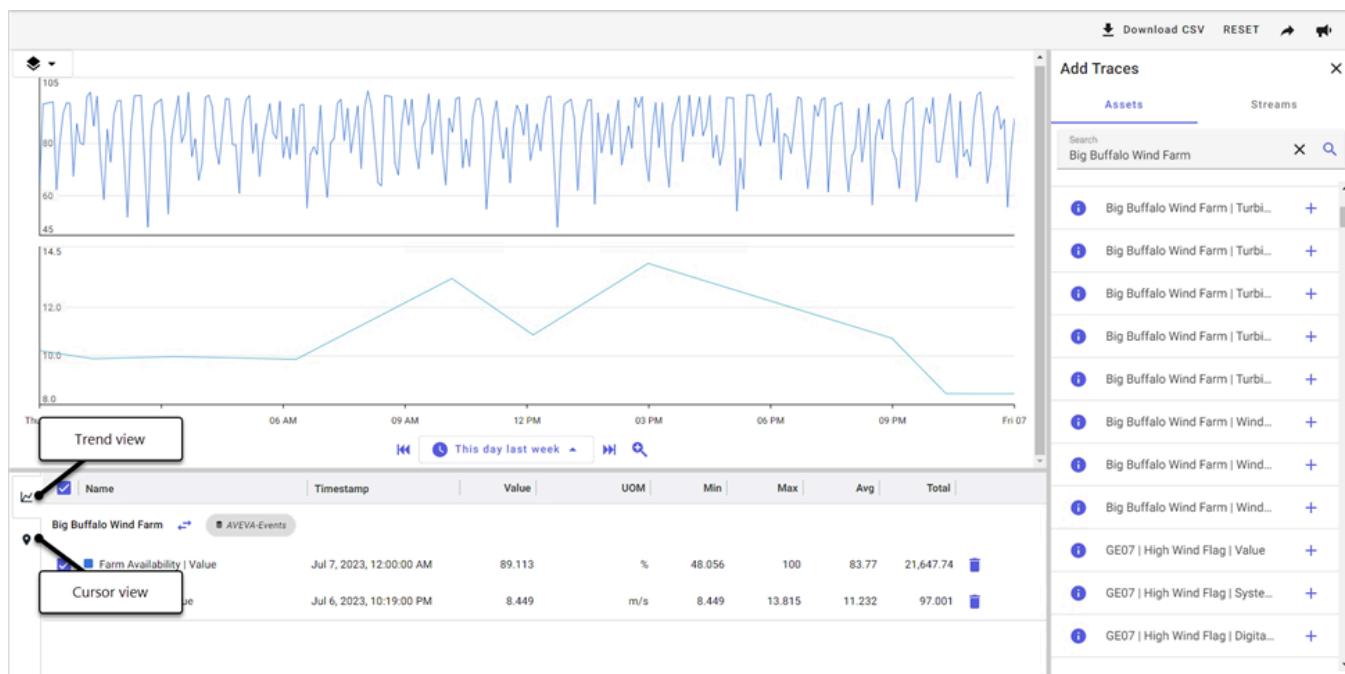
The following image shows the important elements of the Trend page, and the table below describes how to use these elements. For more information on how to use the Trend page to analyze traces, see [Create a trend session](#).



Callout	Description
1	Trend pane – Displays the selected traces. Line traces are displayed for numeric data and heat maps are displayed for string or enumerated data.
1A	Trend mode – Select to toggle between the stacked, single-scale, and multi-scale view modes.
1B	Cursor – Place cursors to get minimum, maximum, average, and delta values between two points in time.
1C	Time range picker – Specify the time range by selecting a time range, specifying a custom range, or using the step forward and step backward arrows.
2A	Namespace – Select the triangle and select the namespace from the list.
2B	Reset – Clears the workspace.
2C	Share  – Copies the workspace URL. Use this to share your workspace with others.
3	Add Traces pane – Select a Plus  to add a trace to the Trend pane.
4	Legend table – Displays information about the traces in the Trend pane. Toggle between the Trend and Cursor views.
4A	Trend view – Select the Trend  icon to display statistics about each trace in the Legend table. The screen capture shows the trend view.
4B	Cursor view – Select the Cursor  icon to display cursor statistics in the Legend table. The cursor must be locked to display the statistics (select Plus  above the cursor). With two or more locked cursors, summary statistics are displayed for contiguous cursors.

## Trend legend

On the Trend page, a legend table below the Trend pane lists information about the traces plotted within the trend session. You can toggle this legend table between two views: a **Trend**  view and a **Cursor**  view.



## Trend view

The Trend  view lists each trace depicted within the trend session. A trace is a stream or asset property data plotted in the session.

Each trace is listed within the Trend  view. Each trace listed includes icons that display more information about the trace origin. The following table describes each icon.

Icon	Description
	Indicates the origin namespace of the trace.
	Indicates that the trace originates from a <a href="#">community</a> . Mouse over the icon to view the community identifier.
	Indicates the tenant that is sharing the trace within the community. This icon displays only when the trace is shared within a community.

Under each trace, the **Legend** table lists each property added, along with additional data for the property. The following table describes the columns in the legend table.

Column	Description
Name	The name of the trace property depicted within the Trend pane. The color swatch for each property corresponds to its plotting within the trend session.
Timestamp	The date and time of the trace.

Column	Description
Value	The value of the property.
UOM	The unit of measure.
Min	The lowest value recorded for the property for easy cursors set in the <b>Trend</b> view.
Max	The highest value recorded for the property for easy cursors set in the <b>Trend</b> view.

Each property also includes controls to edit the trend session visualization:

- Select or clear the property checkboxes to display or hide the trace property in the trend session.
- Select the **Delete**  icon to remove the trace property from the trend session.

Name	Timestamp	Value	UOM	Min	Max
Scottsdale Weather   RobertTest					
temperature	11/30/2021 1:40:58 PM	80.000		80.000	80.000 
wind speed	11/30/2021 1:40:58 PM	10.000		10.000	10.000 

## Cursor view

The **Cursor**  view lists property values for each cursor added to the Trend pane. Cursors are listed chronologically according to their timestamps.

Timestamp	Scottsdale Weather   temperature	Scottsdale Weather   wind speed	Test Stream   Value
12/05/2021 11:55:11 AM	80.000	10.000	1.000
1d 6:00:43	Min: 80.000 Max: 80.000 Average: 80.000 Delta: 0	Min: 10.000 Max: 10.000 Average: 10.000 Delta: 0	Min: 1.000 Max: 1.000 Average: 1.000 Delta: 0
12/06/2021 05:55:54 PM	80.000	10.000	1.000
1d 6:08:57	Min: 80.000 Max: 80.000 Average: 80.000 Delta: 0	Min: 10.000 Max: 10.000 Average: 10.000 Delta: 0	Min: 1.000 Max: 1.000 Average: 1.000 Delta: 0
12/08/2021 12:04:51 AM	80.000	10.000	1.000

**Tip:** For more information on placing cursors, see [Create a trend session](#).

## Trend URL parameters

When you use the Share function to copy the URL for a trend, the function constructs a URL using parameters to specify the data in the trend. This URL allows you to access the same trend again and to share it with colleagues. You can construct a parameterized URL manually by adding parameters to the base URL for your CONNECT data services environment. This allows you to open a trend programmatically from other applications or to create a trend populated with specified data items.

You must have access to the data to access a trend using a parameterized URL. When you access a trend using a parameterized URL, the URL in the active browser is reset to the base URL.

To manually create a trend URL, add query string parameters to the base URL paths by following these basic syntax rules:

- Separate query string parameters from preceding base URL with a question mark (?).
- Separate each query string parameter with an ampersand (&).

---

**Note:** A URL must include URL-encoded characters where needed. For example, the plus sign (+) indicates Space in HTML. To enter an actual plus sign as part of a URL, it must be encoded as %2B. For the URL syntax: &EndTime=+8h you need to use: &EndTime=%2B8h. For more information about URL encoding, see the w3schools.com article [HTML URL Encoding Reference](#).

---

## Trend URL example

The following example trend URL includes multiple streams and cursors:

```
https://{{server}}/tenant/{{tenant_id}}/trend?origin={{Sample}}&trace=Tank%3B123;Temp%3B456&trace=Tank%3B234;Temp%3B789&starttime=2019-10-30T07:06:46.939Z&endtime=2019-10-30T07:06:46.939Z&mode=multiple&cursor=2019-10-30T08:06:46.939Z&cursor=2019-10-30T08:06:46.939Z
```

## Parameter reference

The following table describes the available URL parameters.

Parameter	Description	Syntax
<i>origin</i>	Source of data that contains the stream properties. Required.	origin={{namespace_Id}}
<i>trace</i>	The stream properties to be plotted. Consists of <i>streamId</i> and <i>propertyId</i> . The properties are separated by a semi-colon (;) and are URL encoded, which encodes the delimiter character, also a semi-colon, as %3B. You can add multiple stream properties.	trace=Tank%3B123;Temp%3B456 In this example, the decoded <i>streamId</i> is Tank;123 and the decoded <i>propertyId</i> is Temp;456.
<i>starttime</i>	Start time expressed as an ISO 8601 formatted timestamp.	starttime=2021-09-22T07:06:46.939Z
<i>endtime</i>	End time expressed as an ISO 8601 formatted timestamp. If either the <i>starttime</i> or <i>endtime</i> parameter is not specified, the default time range is displayed.	endtime=2021-09-22T15:06:46.942Z
<i>mode</i>	Trend display mode. Valid values are stacked, single, or multiple.	mode=stacked

Parameter	Description	Syntax
	If no mode is specified, the trend is displayed in stacked mode.	
<i>cursor</i>	Trend cursor expressed as an ISO 8601 formatted timestamp. You can add multiple cursors.	cursor=2021-09-22T15:06:46.940Z

## Swap assets in a Trend graph

On the Trend page, you can switch between assets that are created with the same asset type. Instead of searching for and adding the traces for each asset, use the Swap Asset feature to streamline this process. You add the traces for a single asset, and then you use the Swap Asset feature to replace the asset in the trend with another asset.

To switch assets in a trend:

1. In the left pane, select **Visualization > Trend**.
2. On the Trend page, select the **Assets** tab in the Add Traces pane.
3. Select the + sign to add one or more traces for the same asset to the trend.

**Note:** The asset must be created from an asset type.

The following image shows several traces for the Philadelphia Weather Station asset. The data displayed show the wind speed, wind direction, and the relative barometric pressure.



4. Select the **Swap Asset** icon next to the asset name in the legend table to open the Swap Asset window, which displays a list of assets of the same asset type.
5. Select the asset to view and select **Continue**.

**Note:** The Trend page replaces the traces of the original asset with the new asset.

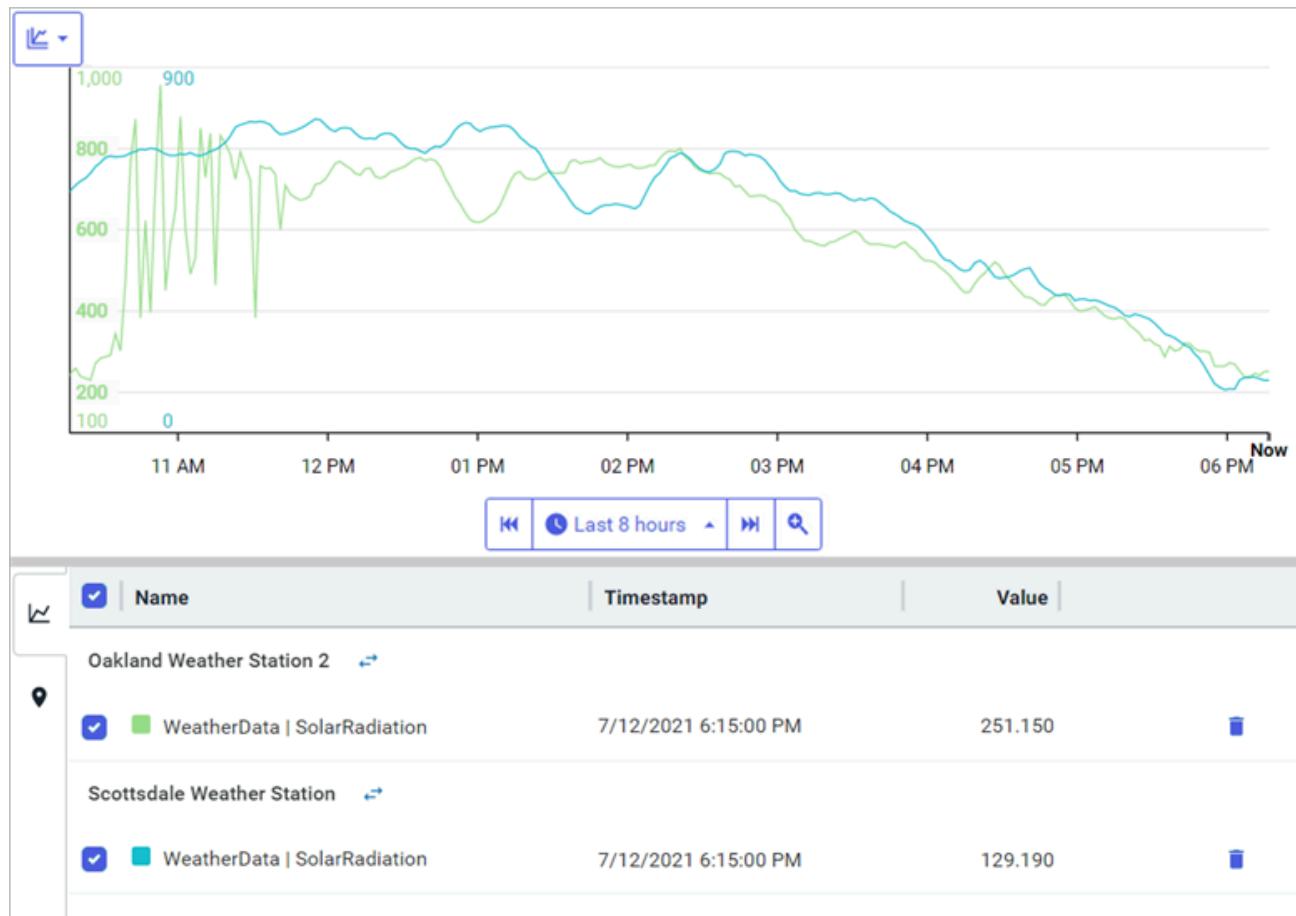
## Asset switch in performance testing

Switching between assets is useful in performance testing and benchmarking. For example, assume Asset A provides the standard against which other assets are compared. You add Asset A and Asset B to the trend and compare B against A. Then use the Asset Swap feature to replace Asset B with Asset C, and compare C to A.

To switch assets while performance testing:

1. In the left pane, select **Visualization > Trend**.
2. On the Trend page, select the **Assets** tab in the Add Traces pane.
3. Add a trace for the asset that provides the standard for all assets.
4. Add a second trace for an asset to compare against this standard.

In the following image, there are two traces with solar radiation data. In this example, the Oakland Weather Station is the standard and the Scottsdale Weather Station trace is compared against it.



5. Select the **Swap Asset** icon  for the asset you are comparing with the standard.

In this example, select the  icon for the Scottsdale Weather Station.

6. In the Swap Asset window, select another asset and select **Continue**.

In this example, the solar radiation trace for the Scottsdale Weather Station is replaced with the solar

radiation trace for the Philadelphia Weather Station. Now you can compare the trace for the Philadelphia Weather Station against the Oakland Weather Station.



## Asset explorer

Use the asset explorer to create assets, then visualize data streams and properties to troubleshoot and analyze the associated devices. You can create assets as needed, create them from an asset type, which acts as a template for creating similar assets, and generate them based on stream naming patterns using asset rules.

## Assets

An asset is a container for data streams and metadata associated with a particular device or object. Assets allow you to group related streams and provide context to the stream data.

When you create an asset, you select a namespace and a set of streams within that namespace. Assets typically represent devices with multiple data streams, but you can create an asset with only one stream if needed.

Use the asset explorer in the portal to create assets, then visualize data streams and properties to troubleshoot and analyze the associated devices. You can create assets as needed, create them from an asset type, which acts as a template for creating similar assets, and generate them based on stream naming patterns using asset rules.

## PI Server counterpart

Assets are comparable to elements in PI AF server. Like elements, assets include both dynamic and static information associated with the asset. The static information provides context for the dynamic data. Assets appear as a flat list that you can search using metadata values. This contrasts with the elements in PI AF server which are organized in a hierarchy.

## Assets best practices

We recommend the following best practices when you create assets:

- Use assets to bring together data from multiple streams and the static data associated with a logical asset. Assets make it easier to visualize and contextualize the data for a given logical asset.
- Define the UOM on the type whenever possible. The UOM can also be defined on the stream, but if it is defined in multiple places, ensure that the UOMs match. If a different UOM is configured, there is no conversion between the UOMs.

## Add an asset

Follow this procedure to create an asset, add and configure its metadata and properties, and select and configure a property whose status will be visible in the card or table view.

To create an asset:

1. In the left pane, select **Visualization > Asset Explorer**.
2. From the **Assets/Asset Types** selector, select **Assets**.
3. In the toolbar, select **Add Asset**.
4. In the Select Type for New Asset window, select **None** and select **Continue**.
5. In the right pane, complete the following fields:
  - **Asset** – Enter a name to identify the asset.
  - **Description** – (Optional) Add a description for the asset.
6. Select the **Metadata** tab.
7. For each metadata to add to the asset, select **Add Metadata** and complete the following fields:
  - **Metadata** – Enter an identifier for the metadata.
  - **Value** – Enter the value for the metadata.

---

**Note:** The value must match the selected type. The following date/time format is supported: MM/DD/(YY)YY hh:mm(:ss)

---

8. Select the **Properties** tab.
9. Select **Add Stream References**, select the stream in the Select Streams window, and then select **Add**. Selected streams and their properties are listed in the **Properties** tab.

---

**Tip:** To search for streams based on the stream name, description, or the type, enter the text to search for in

---

the **Enter search query** field. For more information on using this field, see [Search queries](#).

---

10. If needed, modify the stream names to make them easier to identify.
  11. To update the property units of measure for a stream, select **Configure UOMs** for the stream.
- 

**Note:** Units of measure can be set only on numeric types.

---

12. On the Configure UOMs page, update the property units of measure as needed and select **Save**.
- 

**Note:** When you select **Save**, any changes are immediately saved to the UOMs on the stream, regardless of any other actions you take on this asset. For example, the UOM changes to the stream are still saved even if you do not save the new asset.

---

13. To configure statuses for the asset, select the **Status** tab and select **Add Status Configuration**.
  14. In the Select Property window, select the property that determines the asset status and select **Continue**.  
You can only specify one property to determine the asset status, and that property must have enumerated states, string values, or integer values.
- 

For integer values:

- Up to 20 total integers can be used to define the value for the available statuses.
  - Integers can be separated by commas.
  - Integers cannot be repeated.
- 

**Tip:** You can switch to a different property by selecting the  icon. Each property must be configured separately.

---

15. For each value listed, select the status icon to map the value to a status. To add other values, select **Add Value Mapping**, enter the value(s), and select the corresponding status(es).
  16. To save the asset type, select **Save**.
- 

## Add an asset based on an asset type

An asset type is a template for creating assets that share a common structure or type. When you create an asset based on an asset type, the metadata and stream references are created from the asset type.

To create an asset based on an asset type:

1. In the left pane, select **Visualization > Asset Explorer**.
  2. From the **Assets/Asset Types** selector, select **Assets**.
  3. In the toolbar, select **Add Asset**.
  4. In the Select Type for New Asset window, select the type and select **Continue**.
  5. In the right pane, complete the following fields:
    - **Asset** – Enter a name to identify the asset.
    - **Asset Type** – Displays the asset type on which this asset is based.
    - **Description** – (Optional) Add a description for the asset.
  6. Select the **Metadata** tab.
  7. If needed, edit the values the metadata.
- 

**Note:** You can only edit the values. The metadata are derived from the asset type, as indicated by the **T** and, therefore, you cannot add or delete metadata or change the type.

---

8. Select the **Properties** tab.
9. To see the stream reference configuration details, select the caret ^ icon.
10. To save the asset, select **Save**.

## Manage permissions for assets

If you are assigned the **Manage Permissions** access right, then you can configure asset permissions for other user roles in your tenant. You can granularly assign individual asset permissions to each user role.

### Prerequisites

To manage asset permissions, you must be assigned the **Manage Permissions** access right.

### To manage permissions for assets

1. From the left pane, select **Visualization > Asset Explorer**.
2. From the **Assets/Asset Types** selector, select **Assets**.
3. Select an asset. From the side panel, select **More options :** > **Manage Permissions**.  
The Manage Permissions for Asset window opens.
4. Use the Manage Permissions for Asset window to:
  - (Optional) Add user roles that have permissions on the asset.
  - Edit assets permissions for each user role.  
For more information, see [Permissions management](#).
5. When you are finished editing permissions, select **Save**.

### To manage default permissions for new assets

You can edit the default user roles and permissions added to an asset when it is created.

1. From the left pane, select **Visualization > Asset Explorer**.
2. From the **Assets/Asset Types** selector, select **Assets**.
3. From the toolbar, select **More options :** > **Manage Default Permissions for New Assets**.
4. Use the Manage Default Permissions for New Assets window to edit default user roles and asset permissions. For more information, see [Permissions management](#).
5. When you are finished editing permissions, select **Save**.

### Remove assets

Follow this procedure to remove assets from CONNECT data services.

To remove a single asset:

1. From the left pane, select **Visualization > Asset Explorer**.
2. From the **Assets/Asset Types** selector, select **Assets**.
3. Select the checkbox for the asset you want to remove.
4. Select **More options**  in the Asset Details pane, then select **Remove**.
5. At the prompt, select **Remove**.

To remove multiple assets:

1. From the left pane, select **Visualization > Asset Explorer**.
2. From the **Assets/Asset Types** selector, select **Assets**.
3. Select the checkboxes for the assets you want to remove.
4. Select **Remove**.
5. At the prompt, select **Remove**.

---

**Note:** You may receive an error message when attempting to delete assets. Only the creator of the asset or a user with access can delete an asset.

---

## Asset types

An asset type is a template for creating assets that share a common structure or type. When you create an asset type, you define the expected metadata and stream references for assets created from that asset type. Using asset types to create assets makes it easier to compare assets of the same type and to ensure consistency across similar assets. Note these guidelines when creating an asset from an asset type:

- Configure the asset name, and, optionally, the description.
- Do not add or remove metadata from the asset; however, you can edit metadata values. The asset type determines the metadata and stream type associated with the asset.
- Configure stream references to point at streams of the type defined by the asset type.
- Do not change the mappings or select another measurement. Status mapping is determined by asset type.
- Asset configuration is read-only and inherited from an asset type.

There are two ways to create an asset type:

- Take an existing asset and convert it to an asset type. For more information, see [Convert an asset to an asset type](#).
- Create a new asset type. For more information, see [Create an asset type](#).

## PI Server counterpart

Asset types are comparable to element templates in the PI AF server. Like element templates, asset types are templates for creating assets. Using asset types ensures consistency and makes it easier to compare assets of the same type.

## Asset types best practices

When deciding whether or not to use asset types, consider whether all assets of a given type are similar enough that they can be modeled by a type. Additional metadata and stream references cannot be added to assets that are created from an asset type.

## Create an asset type

For more information on asset types, see [Asset types](#).

To create an asset type:

1. In the left pane, select **Visualization > Asset Explorer**.
2. From the **Assets/Asset Types** selector, select **Asset Types**.
3. In the toolbar, select **Add Asset Type**.
4. In the right pane, complete the following fields:
  - **Asset Type** – Enter a name to identify the asset type.
  - **Description** – (Optional) Add a description for the asset type.
5. Select the **Metadata** tab.
6. For each metadata to add to the asset type, select **Add Metadata** and complete the following fields:
  - **Metadata** – Enter an identifier for the metadata.
  - **Value** – Enter the value for the metadata.  

---

**Note:** The value must match the selected type. The following date/time format is supported: MM/DD/(YY)YY hh:mm(:ss)

---
  - **Type** – Select the value type from the dropdown list.
  - **UOM** – If the type is Integer or Double, select the unit of measure for the value.
7. Select the **Properties** tab.
8. Select **Add Stream Type Reference**, select the stream in the Select Stream Type window, and then select **Add**.  
The stream type reference is listed in the **Properties** tab.
9. To configure statuses for the asset type, select the **Status** tab and select **Add Status Configuration**.
10. In the Select Property window, select the property that determines the asset status and select **Continue**.  
You can only specify one property to determine the asset status, and that property must have enumerated states or string values.  

---

**Tip:** You can switch to a different property by selecting the  icon.

---
11. For each value listed, select the status icon to map the value to a status. To add other values, select **Add Value Mapping**, enter the value, and select the corresponding status.
12. To save the asset, select **Save**.
13. Select **Add Status Configuration**.
14. In the Select Property window, select the property that you want to display status for. Select **Continue**.
15. Select **Add Value Mapping**, enter a value, then select the status icons to map the status (Good, Warning, Bad) for each value.

---

**Tip:** You can switch to a different property by selecting the  icon.

16. Select **Save**.

## Convert an asset to an asset type

Convert an asset to an asset type to use the asset definition as a template to create additional assets. The original asset is still available after the asset type is created.

To convert an asset to an asset type:

1. In the left pane, select **Visualization > Asset Explorer**.
2. From the **Assets/Asset Types** selector, select **Assets**.
3. Select the asset to convert to an asset type. To search for an asset, use the **Search for Assets** field.
4. In the right pane, select the **Edit Asset**  icon.
5. Select **Save as Asset Type**.
6. In the Create an Asset Type window, modify the following fields as needed:
  - **Name** – Enter a name to identify the asset type.
  - **Description** – (Optional) Enter a description for the asset type.
7. Select **Create**.

## Manage permissions for asset types

If you are assigned the **Manage Permissions** access right, then you can configure asset types permissions for other user roles in your tenant. You can granularly assign individual asset type permissions to each user role.

### Prerequisites

To manage asset type permissions, you must be assigned the **Manage Permissions** access right.

### To manage permissions for asset types

1. From the left pane, select **Visualization > Asset Explorer**.
2. From the **Assets/Asset Types** selector, select **Asset Types**.
3. Select an Asset Type.
4. From the side panel, select **More options**  > **Manage Permissions**.  
The Manage Permissions for Asset Type window opens.
5. Use the Manage Permissions for Asset Type window to:
  - (Optional) Add user roles that have permissions on the asset types.
  - Edit asset types permissions for each user role.  
For more information, see [Permissions management](#).
6. When you are finished editing permissions, select **Save**.

## To manage default permissions for new asset types

You can edit the default user roles and permissions added to an asset type when it is created.

1. From the left pane, select **Visualization > Asset Explorer**.
2. From the **Assets/Asset Types** selector, select **Asset Types**.
3. From the toolbar, select **More options :** > **Manage Default Permissions for New Asset Types**.
4. Use the Manage Default Permissions for New Asset Types window to edit default user roles and asset type permissions. For more information, see [Permissions management](#).
5. When you are finished editing permissions, select **Save**.

## Remove asset types

Follow this procedure to remove asset types from CONNECT data services.

To remove a single asset type:

1. From the left pane, select **Visualization > Asset Explorer**.
2. From the **Assets/Asset Types** selector, select **Asset Types**.
3. Select the checkbox for the Asset Type you want to remove.
4. Select **More options :** in the Asset Types Details pane, then select **Remove**.
5. At the prompt, select **Remove**.

To remove multiple asset types:

1. From the left pane, select **Visualization > Asset Explorer**.
2. From the **Assets/Asset Types** selector, select **Asset Types**.
3. Select the checkboxes for the Asset Types you want to remove.
4. Select **Remove**.
5. At the prompt, select **Remove**.

---

**Note:** You may receive an error message when attempting to delete asset types. Only the creator of the asset type or a user with access can delete an asset type.

---

## Remote operations monitoring

Use remote operations monitoring (ROM) to monitor data from remote assets in real-time. This data allows you to anticipate problems and proactively perform preventative maintenance.

## Get started with remote operations monitoring

CONNECT data services makes it possible to monitor remote assets in real time. The immediate access to data about the status of assets gives you the ability to anticipate problems and proactively perform preventative

maintenance.

For example, a fleet manager of a mining truck dealer sells trucks to companies worldwide. The company provides monitoring and maintenance services to its customers. With remote monitoring, they review the status of the trucks each day, identify trucks with problems, use the data collected on different measurements to identify possible causes, review the history of these measurements over time, and share the information with colleagues in the field who can follow up on the problem.

The following procedure describes how to use the portal to monitor assets and quickly identify problems. The screen captures are taken from the scenario described in the example above.

To use the portal to monitor assets and identify problems:

1. From the left pane, select **Visualization > Asset Explorer**.

The asset explorer displays the available assets. In this example, it provides an overview of the health of the fleet of trucks.

---

**Tip:** Select the or icons in the toolbar to toggle between the card and table views of the assets.

---

2. Verify that the **Assets/Asset Type** selector is set to **Assets**.

3. To identify any assets with a problematic status, select the Metadata filters icon , and then select the checkbox for the status to review.

Each asset is identified with one of the following statuses:

Icon	Status
	Good
	Warning
	Bad
	Unknown

4. Select an asset to open the Asset Details pane.

The Asset Details pane provides metadata and property data on the asset that you can use to determine the cause of any problems. The **Metadata** tab displays metadata associated with the asset.

5. Select the **Properties** tab.

The Asset Details pane displays the following:

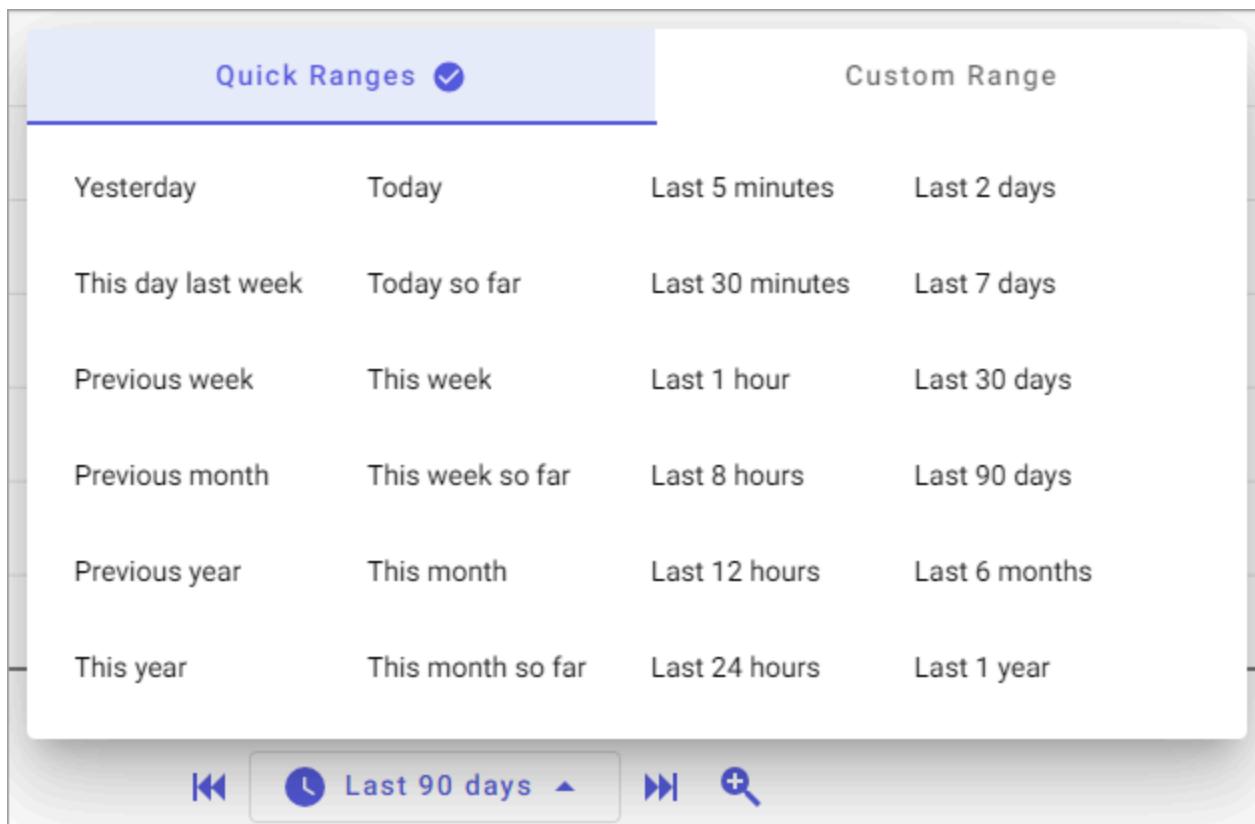
- Data associated with the asset. These values are updated in real time.
- A trend of the selected measurements.

6. Select one or more of the properties that might be the cause for the warning.

7. Review the history of the selected properties in the trend to see if the data suggests you have identified a potential cause.

By default, the trend shows the property data for the last 8-hour period. Use the navigational arrows on the **Time picker** to pick another time-range option or specify a custom time range.

**Time picker**



8. To see the details of these properties, select the **View full trend** icon  to see the Trend page.  
The Trend page shows the properties for the same time range shown in the Details pane of the Asset Editor.

9. (Optional) Select the  icon to change the view.

**Note:** The legend table shows the legend for each trace, the last value, minimum, maximum, and average values in the displayed time range.

Name	Timestamp	Value	UOM	Min	Max	Avg
Truck_121_109   Aftercooler Temperat...	6/15/2020 4:56:13 PM	65.605		61.416	68.372	65.033
Truck_121_109   Engine Coolant Temp...	6/15/2020 4:56:43 PM	90.739		84.479	95.138	89.836

10. (Optional) If the error did not occur in the time range currently in view, select **Step backward**  or **Step forward**  to move the time range backward or forward.

**Note:** The trace will move in increments of time that are displayed in the trend. If the trend displays the last 12 hours, use the step backward arrow in the Time picker to show the previous 12-hour period. If it displays the last 30 days, the step forward arrow shows the next 30-day period.

11. Select a trace to select it for further analysis.

The trace is highlighted, and two cursors automatically mark the minimum and maximum values for the displayed time range.



Select + above the trace to lock the cursor in place. The + turns into an x. Select the x to unlock the cursor.

12. To add other cursors at data points of interest, select + above the trace to lock the cursor in place.

---

**Note:** When two cursors are locked, the legend table displays summary calculations for the values between the two cursors.

13. Select the **Share Trending Session** icon ↗ in the menu bar to copy the URL of the workspace.

Share this link to give others the same view of the trend that they can then use to troubleshoot problems.

## Filter and search assets

Monitor and manage assets by applying filters or searching in the Asset Explorer. Filters allow you to find specific assets quickly regardless of how many assets your organization has. Customize and refine your search filter by selecting multiple filter values. Your view of assets is saved within a session or between sessions. Use metadata filters to refine your search using these filter facets:

- Status – Filter for assets that have the same status. For example, filter for assets with a status of Warning or Bad to identify assets that may need attention.
- Asset Type – Filter for assets based on asset type.
- Metadata – Filter for assets based on metadata, such as Location, Manufacturer, Province or State, Region, or Model.

## To filter assets in the Asset Explorer

1. In the left pane, select **Visualization > Asset Explorer**.
2. Verify that the **Assets/Asset Type** selector is set to **Assets**.
3. Select the **Metadata Filters** icon  to open the Metadata Filters pane.
  - Status and Asset Type always appear at the top of the filter facets list.
  - The remaining metadata facets appear in order, with the most frequently occurring facet first, followed by the remaining facets in descending order.
  - The first ten values of each facet are displayed. If there are more than ten values, select **Show More** to see the complete list of values.
4. Enter the name of the metadata facet in the **Search** field to find a particular facet.  
For more information, see [Search queries](#).
5. Select one or more values from one or more facets to apply the filters to the listed assets.  
If you select multiple choices within a facet, an **Or** operator is used. For example, if you filter on status values of Warning and Bad, assets that have a status of Warning or a status of Bad appear. Across facets, an **And** operator is used. For example, if you filter on status value of Bad and an asset type of GE Wind Turbine, only assets that have both values appear. As you select facet values, the assets that match the values are updated and displayed in real time. The asset search chips appear in the menu bar so you can see how the asset view is filtered.  
Apply multiple filters in combination to create a unique view for your fleet of assets. For example, you could set filters to see assets that have a status of Good, are based on the GE Wind Turbine asset type, and are either in the NA or NAMER region.
6. (Optional) To remove a facet filter, select the **X**, or to remove all facet filters, select **Clear All**.

## Share a view of your fleet

You may have many hundreds or even thousands of assets in your fleet. Working with colleagues on different computers and in different locations, you need to look at the same set of assets. The asset explorer allows you to filter and view a subset of the assets and share this view with others.

To filter and view a subset of assets:

1. In the left pane, select **Visualization > Asset Explorer**.
2. Verify that the **Assets/Asset Type** selector is set to **Assets**.
3. Enter a string in the **Search for Assets** field to search the assets that are displayed.
4. Select the **Shared Filtered Assets** icon  in the toolbar to copy the URL to the clipboard.

**Note:** Send this link to your colleagues and partners. When they paste this URL into a browser, they will see the fleet view you created.

---

**Tip:** Bookmark this link to return to this fleet view.

---

# Analytics

The Analytics menu provides tools for shaping and querying large datasets:

- Use the Data Views page to create subsets of data from asset and streams, including streams shared with communities that you are a member of.
- The Power BI Connector retrieves Data Views from CONNECT data services and makes them available in Microsoft Power BI for advanced data visualization and analysis.

## Data views

Data views allow you to access subsets of data items from CONNECT data services in data-driven applications, where the items can be used for data science enablement. With data views, you can bridge your raw CONNECT data services data to third-party applications like Microsoft Power BI, where it can be used for analytics, machine learning, and so on. Users can programmatically retrieve data view content using the CONNECT data services API. Data views deliver shaped data that is ready for consumption because it is normalized, aligned, and contextualized.

Working with a data view involves two phases:

1. Data view creation and configuration
2. Data set retrieval

### Data view creation and configuration

First, you must create and configure a data view. The CONNECT data services resources included in the data view are based on the result of one or more queries, which you must configure. Streams, assets, and other resources that can be included in a data view are known as *data items*. Streams shared to communities can also be included. Properties from data objects and information about the data items (such as Id and Metadata) can be included in the data view as *fields*.

For more information, see [Create and configure a data view](#).

### Data set retrieval

After you create and configure a data view, you can programmatically retrieve the data set that it resolves to using the CONNECT data services REST API. With a data-driven application (like Microsoft Power BI), you can leverage the data view for data science enablement.

For more information, see [Retrieve data for a data view](#).

## Create and configure a data view

This is an introduction to the recommended workflow for creating and defining data views.

## Before you start

Review the following information before creating a data view.

## Prerequisites

- To create a fully functioning data view, your instance of CONNECT data services must include [Streams](#) or [Assets](#) to include in the data view.
- If you want to include streams from a community within your data view, you must be a member of that community.

## Data view objects

A data view is a declarative query and shape for your data. It includes the following objects, which you will configure as you complete the data view creation workflow:

- **Query:** Determines what data items are included in a data view. Queries can include streams or assets. A data view can have multiple queries.
- **Data field set:** Collections of fields originating from the same query.
- **Data view shape:** Determines if the data should be returned in the standard grouped row format or a narrow view, which is a pivot of the standard table.
- **Index field:** Determines the primary index type and label of the index. The index must be a timestamp and displays in the first column of the data view.

**Note:** You can create data views with non-DateTime indexes using the REST API.

Data views also include other configurations such as grouping instructions and default date range and interval.

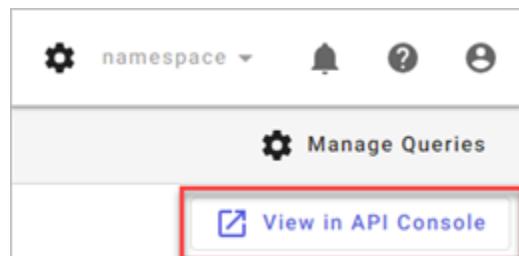
## Design in iterations

Designing and editing a data view is an iterative process. Your first iteration of the data view will likely not work as expected and will require additional iterations. Adjust the included queries and data fields until it meets your requirements.

## API console

While creating or editing a data view, use the  View in API Console to open the view in the [API console](#). The API console includes the URI and query values for accessing your data view in its current configuration.

### View in API Console button



## Data view creation workflow

To create and define a data view, complete these tasks in order.

- [Add a data view](#)

Begin creation of a data view by creating a data view object, which includes a name and description for the data view. The data view will not yet include any queries or data fields yet—you will add those later.

- [Add a query](#)

Each data view includes one or more query. These queries determine what data items (streams or assets) are included in the data view.

- [Select data field sets](#)

A data view includes one or more data field sets, which are collections of data fields originating from the same query. A data field is a property or metadata from the streams or assets included in a query. One field serves as the index while others contain information related to the data items (streams or assets).

When configuring a data view, you can configure the data field set for each query by choosing which data fields you want to include in the data view.

- [Configure data shape](#)

Data views can be configured to return data in either a standard shape or a narrow shape. Standard shape returns data in a grouped row format. Narrow shape is a pivot of the standard table.

- [Preview and save the data view](#)

As you work with your data view, you can generate a preview of how the data will be shaped and organized. After you are satisfied with how the data is organized in the preview, you can view its URI in the API console to begin working with the data in a third-party application.

## Add a data view

Begin creation of a data view by creating a data view object, which includes a name and description for the data view. The data view will not yet include any queries or data fields yet—you will add those later.

### To add a data view

1. In the left pane, select **Analytics > Data Views**.
2. In the Data Views pane, select **Add Data View**.
3. Enter a **Name** for the data view.
4. (Optional) Enter a **Description** for the data view.

### Next steps

Continue to [Add a query](#).

## Add a query

Each data view includes one or more query. These queries determine what data items (streams or assets) are

included in the data view.

## To add a query

1. (Optional) From **Query Id**, overwrite the default value of *Query1* with a unique identifier.
2. From **Query Source**, select a namespace  or community  to query operational data from. The source can either be a namespace from your own tenant or a community.

You can filter the namespaces and communities that are listed using the slide toggles and the filter field.

**Getting This namespace does not allow data to be processed outside of the region where it resides while adding a query?** See [Data view troubleshooting](#).

3. From **Query Type**, select the type of object that you want to search for in the query source: **Streams** or **Assets**.
4. From **Query Value**, enter a query to find the objects that you want to include in the data view. Then select **Search**.

For more information on how to enter a query, see [Search queries](#).

When the query populates with objects, you can view more about each object by selecting it from the table. The object details display in the pane on the right.

Each query is executed independently to generate the list of data items. It is possible to have duplicate data items resulting from different queries. This can be desirable or undesirable depending on the use case.

There is a maximum of 100,000 data items that can be included in a data view. Note that each stream included will generate a data item, and as such a single asset may contribute multiple data items if it contains multiple stream references. Data items are ordered alphabetically by data item id within the data items collection.

5. (Optional) To add additional queries to the data view, select **Add Query** and repeat the steps listed above.
6. Once you are satisfied with your queries and query results, select **Save**.

## Ineligible data items

The collection of ineligible data items represents resources that match the queries but cannot be included in the data view. A data item is ineligible if it does not contain at least one eligible non-key data item field.

A data item field is ineligible if its index is not appropriate for the data view, or if the field has a data type that may not be included in data views.

The following are examples of ineligible index:

- The index is compound (multiple properties)
- The index property data type differs from the data view data type

The following are examples of ineligible field types:

- Objects (nested type)
- Array (collection type)
- TimeSpan (time spans and nullable time spans are currently unsupported)

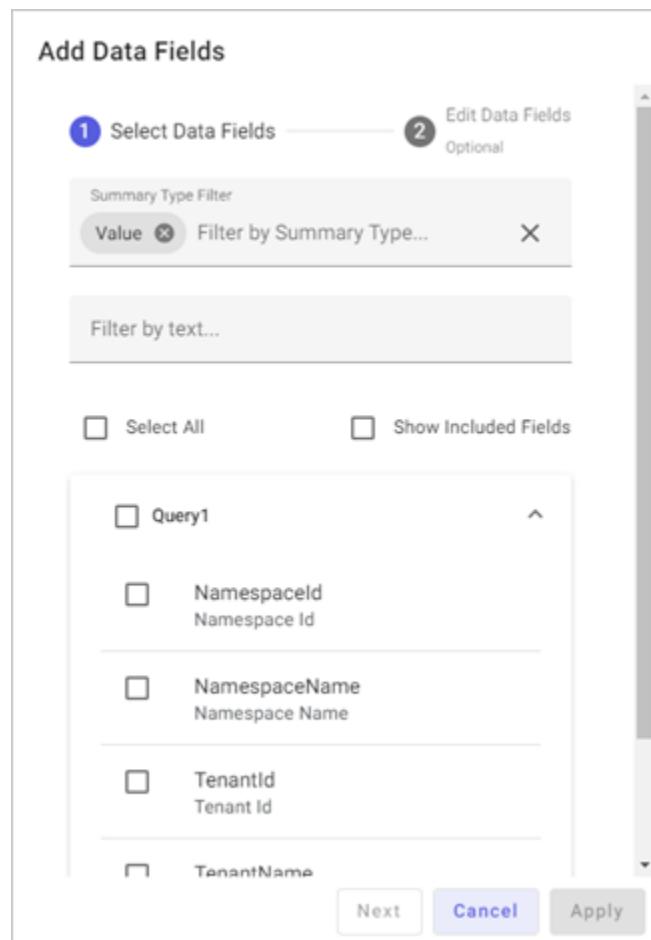
## Next steps

Continue to [Select data field sets](#).

## Select data field sets

After you save the queries that you create in the previous step, CONNECT data services prompts you to add data fields to the field set for each query in the Add Data Fields window. Data fields are metadata or properties from streams or assets that are included in your data view.

### Add Data Fields window



## To select data fields

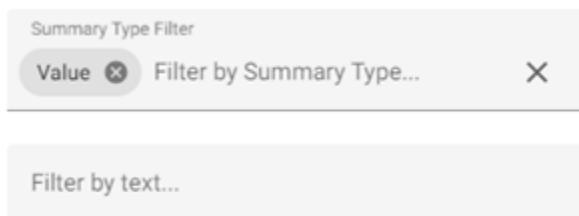
From the Add Data Fields window, select the fields that you want to include in your data view. If you have more than one query, select fields for each query.

### Tips:

- Use the data field filters to find a specific field. For more information, see [Data field filters](#).
- To display which fields are already included in the data view, select **Show Included Fields**.

## Data field filters

You can filter the data fields listed for each query by summary type or by text.



### Filter by summary type

You can filter the data fields listed for each query by summary type, which returns different calculations for a given data field. The **Value** summary type is selected by default.

- To add a summary type chip, select the **Filter by Summary Type** field and select a value.
- To remove a summary type tag, select **X** for the chip.
- To remove all summary type tags, select **X** for the **Filter by Summary Type** field.

### Filter by text

You can further filter the data fields listed for each query by field name or field type—in other words, by metadata or property id.

## Next steps

After you choose data fields, perform one of the following actions:

- Apply options to your data field sets. Select **Next** to edit the selected data fields and apply other field set options. Proceed to [Field set options](#).
- If you are satisfied with your field sets, select **Apply** and proceed to [Configure data shape](#).

### Field set options

A data view includes one or more data field sets, which are collections of data fields originating from the same query. A data field is a property or metadata from the streams or assets included in a query. One field serves as the index while others contain information related to the data items (streams or assets).

After adding your initial field sets in [Select data field sets](#), when configuring a data view, you can configure the data field set for each query by choosing which data fields you want to include in the data view.

### Optional steps

After adding data fields to your field sets, you have the option to organize and group each field set with procedures outside of the configuration workflow. If you want to use these options, complete the applicable tasks below and then return to this configuration workflow to complete intial setup of a data view.

- [Edit data field labels](#)
- [Edit grouping fields](#)
- [Edit identifying fields](#)
- [Link data fields](#)
- [Edit field set order](#)

## Configure data shape

Data views can be configured to return data in either a standard shape or a narrow shape. Standard shape returns data in a grouped row format. Narrow shape is a pivot of the standard table.

With a standard shape, each row in the resolved data view includes all the data fields for a single event or observation. With a narrow shape, each row in the resolved data view includes only one data field. This results in a narrow output schema where one column contains all the data field values, so the schema remains fixed regardless of changes to the included data fields. Narrow shape may be used when an invariant output schema is required.

### Standard

The standard table column structure is built horizontally from left to right. The index field is first, followed by the grouping fields, if any exist. Data field sets come next, in the order they are presented in the data view. Fields are presented in order of appearance within each data field set for each data item from the associated query.

Vertically, the standard structure depends on the inclusion of grouping fields. If grouping fields are not defined, each resultant index appears only once, and all interpolated data is in that row. If grouping fields are defined, then the resultant indexes will repeat vertically for each group. The groups are presented in alphabetical order.

#### Standard data shape

Timestamp	Name	Active Power kW ⓘ	Wind Speed m/s2 ⓘ
Jun 1, 2022, 12:00:00 AM	GE01	1097.3243	10.29832
Jun 1, 2022, 1:00:00 AM	GE01	1492.8794	12.881066
Jun 1, 2022, 2:00:00 AM	GE01	832.4266	8.642148
Jun 1, 2022, 3:00:00 AM	GE01	966.0364	10.404172
Jun 1, 2022, 4:00:00 AM	GE01	1093.3597	10.058291
Jun 1, 2022, 5:00:00 AM	GE01	257.8425	6.9067173
Jun 1, 2022, 6:00:00 AM	GE01	739.96954	9.173307
Jun 1, 2022, 7:00:00 AM	GE01	165.65184	5.4625187
Jun 1, 2022, 8:00:00 AM	GE01	141.52252	3.994674
Jun 1, 2022, 9:00:00 AM	GE01	192.54079	5.4230576
Jun 1, 2022, 10:00:00 AM	GE01	250.27881	5.633816
Jun 1, 2022, 11:00:00 AM	GE01	206.1291	5.961183
Jun 1, 2022, 12:00:00 PM	GE01	88.52169	4.6573987
Jun 1, 2022, 1:00:00 PM	GE01	123.69634	4.012771
Jun 1, 2022, 2:00:00 PM	GE01	161.18558	4.9811983
Jun 1, 2022, 3:00:00 PM	GE01	184.49428	4.721823

Showing 1 - 50 of 15,370 Items per page: 50 ▾ 1 ▾ >

## Narrow

The narrow table pivots the standard table. Each data field becomes a row comprised of the following columns:

- Index column
- Grouping value column(s)
- Field column, which holds the resolved column label of the field
- Value column, which holds the field value such as the property or metadata value

The column label of the index and grouping value columns may vary depending on the resolved label. The Field and Value column labels are not modifiable.

The data view is built vertically by grouping field, if present, then by field.

Data views resolving into multiple data items with the same property ids or names, should use a grouping field or an identifier in order to differentiate the data rows.

### Narrow data shape

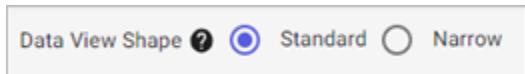
Timestamp	Name	Field	Value ⓘ
Jun 1, 2022, 12:00:00 AM	GE01	Active Power kW	1097.3243
Jun 1, 2022, 1:00:00 AM	GE01	Active Power kW	1492.8794
Jun 1, 2022, 2:00:00 AM	GE01	Active Power kW	832.4266
Jun 1, 2022, 3:00:00 AM	GE01	Active Power kW	966.0364
Jun 1, 2022, 4:00:00 AM	GE01	Active Power kW	1093.3597
Jun 1, 2022, 5:00:00 AM	GE01	Active Power kW	257.8425
Jun 1, 2022, 6:00:00 AM	GE01	Active Power kW	739.96954
Jun 1, 2022, 7:00:00 AM	GE01	Active Power kW	165.65184
Jun 1, 2022, 8:00:00 AM	GE01	Active Power kW	141.52252
Jun 1, 2022, 9:00:00 AM	GE01	Active Power kW	192.54079
Jun 1, 2022, 10:00:00 AM	GE01	Active Power kW	250.27881
Jun 1, 2022, 11:00:00 AM	GE01	Active Power kW	206.1291
Jun 1, 2022, 12:00:00 PM	GE01	Active Power kW	88.52169
Jun 1, 2022, 1:00:00 PM	GE01	Active Power kW	123.69634
Jun 1, 2022, 2:00:00 PM	GE01	Active Power kW	161.18558
Jun 1, 2022, 3:00:00 PM	GE01	Active Power kW	184.49428

Showing 1 - 50 of 980 Items per page: 50 ▾ ◀ 1 ▶

## To configure data shape

To choose a data shape, choose between the **Standard** and **Narrow** options at the top of the page.

### Data view shape options



## Next steps

[Continue to Preview and save the data view.](#)

## Preview and save the data view

As you work with your data view, you can generate a preview of how the data will be shaped and organized. After you are satisfied with how the data is organized in the preview, you can view its URI in the API console to begin working with the data in a third-party application. You can also use the preview to select a default date and time for your index for when you launch the data view in the API console.

## Index configuration

Before retrieving your data view with third-party software for the purposes of data science, you can preview what it will look like by configuring a start and end index that limits the data included in the data view.

All data in a data view is associated with a index value derived from a timestamp. If there are multiple groups in the data view, the index and grouping field values together form a unique identifier for each data record.

**Note:** The index configuration settings available on the Data View page are primarily for preview purposes. When working with the data view in third-party software, you can modify the index configuration programmatically—the data view preview index configurations can be edited freely.

## To configure the index and preview the data view

To configure the index, select an index start and end value. Then generate the preview.

- From the **Configure Data View Retrieval Type** dropdown, select a retrieval type:

Type	Description
<b>Interpolated</b>	Returns data between specified intervals. Streams in SDS may be configured to have non-default interpolation and extrapolation behavior. These behaviors are observed when stream data is included in data views. Data view data is always treated as dense, even if SDS returns sparse data.
<b>Stored</b>	Returns stored or window data. The resulting data view data will include only index values that exist in the underlying data from the data items.

- Select the **Configure Data View Index Configuration** dropdown and define the following settings:

Setting	Description
<b>Start Index</b>	The timestamp for the starting data point of the index.
<b>End Index</b>	The timestamp for the ending data point of the index. <b>Tip:</b> Select <b>Now</b> to set the current date and time.
<b>Time Interval</b> <sup>1</sup>	The interval between data points.
<b>Save Defaults with Data View</b>	If checked, the index configuration parameters are saved as defaults and used when these parameters are not explicitly included in an API request.

<sup>1</sup>This setting is only available for the **Interpolated** retrieval type.

- Select **Apply**.

The data view preview is updated according to your index configuration. When you are done editing your

data view, select **Save and Close** to finish initial configuration of your data view.

## Next steps

Launch your data view in the API console and retrieve it with a data-driven application. For more information, see [Retrieve data for a data view](#).

# Manage data views

After initial creation of a data view, you can later edit its name and description. You can also remove data views that are no longer useful.

## To create a data view

For information on creating and configuring a data view, see [Create and configure a data view](#).

## To edit a data view name and description

Edit an existing data view to edit its name and description.

1. In the left pane, select **Analytics > Data Views**.
2. Select the data view that you want to edit.
3. Select  **Edit Data View**.

**Getting Unknown Community?** For more information, see [Data view troubleshooting](#).

4. Edit the **Name** and **Description**.
5. Select **Save**.

---

**Tip:** Looking for documentation on how to edit queries, shape, or field sets? Refer to the following topics:  
[Manage queries](#) or [Manage data field sets](#).

## To duplicate a data view

You can create a new data view using an existing data view as a template.

1. In the left pane, select **Analytics > Data Views**.
2. Select the data view that you want to duplicate.
3. In the right pane, select **More options :** > **Duplicate**.
4. Enter a **Name** and **Description**.
5. Select **Save**.

## To remove a data view

Remove a data view if you no longer use it.

1. In the left pane, select **Analytics > Data Views**.
2. Select the data view that you want to remove.
3. Select **More options**  > **Remove Data View**.
4. Confirm by selecting **Remove**.

## Manage queries

Following initial configuration of a data view, you can go back to add new queries to it or remove existing ones.

### Manage queries for a data view

Following initial addition of a data view, you can add queries or remove them from a data view by managing its queries.

1. In the left pane, select **Analytics > Data Views**.
2. Select the data view that includes the queries that you want to manage.
3. Select **Edit Data View**.  
The data view opens.  

---

**Getting Unknown Community?** For more information, see [Data view troubleshooting](#).
4. Select **Manage Queries**.

### Add queries to a data view

You can add new queries to a data view the same way that you added one during initial data view creation and configuration. For more information on adding a new query to a data view, see [Add a query](#).

### Remove queries from a data view

Remove a query to remove its selected data streams from the data view.

---

**Note:** You can remove a query from a data view only when it contains more than one query. You cannot remove queries with a message of Unknown Community. For more information, see [Data view troubleshooting](#).

---

1. In the left pane, select **Analytics > Data Views**.
2. Select the data view that includes the query that you want to remove.
3. Select **Edit Data View**.  
The data view opens.
4. Select **Manage Queries**.
5. Select one or more query that you want to remove.
6. Select **Remove Query**.
7. Select **Apply**.

## Manage data field sets

Following initial creation and configuration of a data view and its data field sets for each query, you can go back and edit each field set, adding new fields, editing existing fields, or removing fields from the field set.

Data field set tasks include:

- [Manage data fields](#)
- [Edit data field labels](#)
- [Edit grouping fields](#)
- [Edit identifying fields](#)
- [Link data fields](#)
- [Edit field set order](#)

## Manage data fields

Each data field set is composed of data fields from streams or assets. You can organize your data view to use one or more of these fields to group your data view. The fields you choose to use for grouping display in the data view to the immediate right of the index field.

### To add data fields to field set

1. In the left pane, select **Analytics > Data Views**.
2. Select the data view that you want to edit.
3. Select **Edit Data View**.
4. From the left panel, select **Add**.

The Add Data Fields window opens, listing the field set for each query.

5. Add the data fields that you want to include in your field sets.

---

**Note:** Each data field set must include at least one field. If you edit a data view that includes a query with no data fields in its field set, you are prompted to add data fields to the set.

6. Select **Apply**.

The data fields are added to the field set.

### To remove data fields from a field set

1. In the left pane, select **Analytics > Data Views**.
2. Select the data view that you want to edit.
3. Select **Edit Data View**.
4. Select the fields that you want to remove.
5. Select **Remove**.

## Edit data field labels

Edit data field labels to create a friendly name for a field that displays in your data view.

### Data field labels

A data field label is a friendly name that you can specify directly or using rules. Null, empty, or whitespace is not allowed for a data field label.

When the data view is resolved and data fields produce field mappings, labels are trimmed of whitespace and used as the field mappings' identifier. For example:

```
| Timestamp | Power In Value | Power Out Value |
```

In cases where the identifiers are not unique, the identifier is suffixed with an ordinal number, its position. For example:

```
| Timestamp.0 | Value.1 | Value.2 |
```

To edit data field labels, enter { to display tokens to use as a data field label. There are a variety of special tokens available for use in field labels. These tokens resolve to a specific value for a field. The following list describes each available token.

Token	Description
{CommunityId}	The identifier of the community associated with the data field set's query, or empty if a namespace was queried instead.
{CommunityName}	The name of the community associated with the data field set's query, or empty if a namespace was queried instead. If a community alias is in effect, the alias is used instead of the community name
{IdentifyingValue}	The value of the identifying field.
{Key}	The value of the first of the <i>Key</i> objects specified on the field.
{NamespaceId}	The identifier of the namespace where the corresponding stream/asset originates from. For community queries, this is the owner's namespace from which this stream/asset was shared.
{NamespaceDescription}	The description of the namespace where the corresponding stream/asset originates from. For community queries, this is the owner's namespace from which this stream/asset was shared.
{QueryId}	The identifier of the query that produced the field.
{StreamReferenceName}	The value of the first of the <i>StreamReferenceName</i> objects specified on the field.

Token	Description
{SummaryType}	The value of the summary type of the field (if defined).
{SummaryDirection}	The value of the summary direction of the field (if summary type is defined).
{TenantId}	The identifier of the tenant where the corresponding stream/asset originates from. For community queries, this is the owner's tenant from which this stream/asset was shared.
{TenantName}	The name of the tenant where the corresponding stream/asset originates from. For community queries, this is owner's tenant from which this stream/asset was shared.
{Uom}	The value of the unit of measure of the field (if UOM is present in the source).

If a special parameter fails to resolve, it becomes an empty string, "".

## To edit data field labels

1. From the **Data Field Label** field, enter one or more tokens to use as a label. At the time of data view resolution, the labels resolve to values pulled from the data item (stream or asset). For more information on each available token, see the table above.
2. (Optional) Select the **Include UOM as a Column** checkbox. This option includes the unit of measure as a column in your data view.
3. (Optional) Select a **Summary direction**. This option controls whether the start or end index of the summary is used by the data view to calculate the summary values.
4. Review the **Data Field Preview**. This preview lists each data field and property included within the affected data view queries.
5. Select **Apply**.

## Edit grouping fields

You can organize the data items within a data view by grouping them, which is one method of producing a meaningful, consumable shape of data. Configure grouping fields using the **Grouping Fields** accordion panel. Grouping is optional when defining the data view.

Without grouping, all of the data items returned by a query appear side-by-side. If the view includes many data items, its data records will be vast. The fields are also likely to be ambiguous.

Configuring identifying fields to identify the items within each field set is one way to disambiguate the fields (more on this in the next topic), but only one field may be an identifying field. What if multiple metadata fields are required to fully describe each data item? Grouping can organize the data items into shapes that are consumable, represent a physical asset, or both.

Only certain fields are eligible to be used as grouping fields. Fields are only eligible if they include one of the following source types listed in the table below. All source types require a field label. Some source types also require having a key defined. The following table lists eligible data sources along with additional requirements for field labels and keys.

Eligible source type	Field label required?	Key required?
Id	✓	✗
Name	✓	✗
Metadata	✓	✓
Tags	✓	✓

- If you define **Grouping Fields**, the data view shows multiple groups, each with the list of data items for the group and its field values displaying. If a data item does not match any group, it is added to all groups.
- Within the data view preview, groups are ordered alphabetically by the first grouping value for each group. Within each group, data items are ordered alphabetically by data item id.
- If you are using multiple grouping fields, you can arrange their order by drag and drop. For more information, see [Edit field set order](#).
- If **Grouping Fields** is not defined on the data view, the resolved data view shows a single group with all eligible data items.

## Grouping field example

Use grouping fields to group metadata and data fields in a data view by asset name so that each row contains only the data and metadata for a single asset.

### Without grouping

Timestamp.0	Name.1 ⓘ	Active Power Value kW.2 ⓘ	Wind Speed Value m/s2.3 ⓘ	Name.4 ⓘ	Active Power Value kW.5 ⓘ	Wind Speed Value m/s2.6 ⓘ
Sep 1, 2022, 12:00:00 AM	AE01	599.8845	7.9111986	AE02	759.43225	8.684403
Sep 1, 2022, 1:00:00 AM	AE01	754.92694	9.412169	AE02	794.3154	8.749558
Sep 1, 2022, 2:00:00 AM	AE01	561.2532	8.3074465	AE02	577.2053	8.357386
Sep 1, 2022, 3:00:00 AM	AE01	376.43158	7.138565	AE02	525.34875	8.081926
Sep 1, 2022, 4:00:00 AM	AE01	1003.4248	10.144971	AE02	974.9372	9.711035
Sep 1, 2022, 5:00:00 AM	AE01	962.859	9.419114	AE02	758.49786	8.97884
Sep 1, 2022, 6:00:00 AM	AE01	859.6577	9.526905	AE02	731.7433	8.608316
Sep 1, 2022, 7:00:00 AM	AE01	236.278	6.2405276	AE02	484.2801	8.197634
Sep 1, 2022, 8:00:00 AM	AE01	138.13988	5.7228956	AE02	31.163708	3.6633625
Sep 1, 2022, 9:00:00 AM	AE01	313.1794	6.4766717	AE02	196.8194	6.105624
Sep 1, 2022, 10:00:00 AM	AE01	223.28218	6.365391	AE02	331.0095	7.4503617

Showing 1 - 50 of 673 Items per page: 50 ▾ 1 ▾ >

## Grouping by asset name

Timestamp	Name	Active Power Value ⓘ	Wind Speed Value ⓘ
Sep 1, 2022, 9:00:00 PM	AE01	302.6579	6.3601394
Sep 1, 2022, 10:00:00 PM	AE01	636.4158	8.343973
Sep 1, 2022, 11:00:00 PM	AE01	624.8182	8.902645
Sep 2, 2022, 12:00:00 AM	AE01	350.29532	7.152937
Sep 1, 2022, 12:00:00 AM	AE02	759.43225	8.684403
Sep 1, 2022, 1:00:00 AM	AE02	794.3154	8.749558
Sep 1, 2022, 2:00:00 AM	AE02	577.2053	8.357386
Sep 1, 2022, 3:00:00 AM	AE02	525.34875	8.081926
Sep 1, 2022, 4:00:00 AM	AE02	974.9372	9.711035
Sep 1, 2022, 5:00:00 AM	AE02	758.49786	8.97884
Sep 1, 2022, 6:00:00 AM	AE02	731.7433	8.608316
Sep 1, 2022, 7:00:00 AM	AE02	484.2801	8.197634

Showing 1 - 50 of 325 Items per page: 50 ▾ ◀ 1 ▶

## To add a grouping field

To add a grouping field, select **Add a Grouping Field** and choose an eligible field. You can add as many eligible fields as you prefer.

- From the **Grouping Fields** accordion, select **Add a Grouping Field**.

The screenshot shows the 'Grouping Fields' section of a user interface. A dropdown menu is open under the 'Add a Grouping Field' button. The visible options are:

- IdentifyingValue Id
- IdentifyingValue Latitude Uom
- Metadata - Latitude
- IdentifyingValue Location Uom
- Metadata - Location

- Choose a grouping field.

**Note:** The list of available fields only includes fields that you have added to the field set. If you want to choose a different field that is not listed, you must first add it to the field set. For more information on adding fields to an existing data view field set, see [Manage data fields](#).

- (Optional) Repeat the steps above to add additional grouping fields.

## To ungroup a field

To ungroup a field, select **More options**  > **Ungroup Field** > **All Eligible Queries**.

## To remove a grouping field

Removing a field from grouping fields completely removes the field from the data view rather than merely ungrouping it.

To remove a field, select **More options**  > **Remove**.

## Other grouping tasks

Similar to field sets, the following tasks can be performed on grouping fields:

- [Edit data field labels](#)
- [Link data fields](#)
- [Edit field set order](#)

## Edit identifying fields

An identifying field can be used to uniquely identify data items within a group. For example, if a query contains an ambiguously named stream property such as Value, you might choose a metadata property that uniquely describes the stream as the identifying field.

If the field set resolves to multiple data items in any group (or if grouping is not used), then you should designate an **Identifying field** for the field set. The identifying field of a data field set specifies the primary field to identify multiple items in a group. This identification method allows the identifying field value to be used automatically in field labels of the group. If a lone criterion is not a sufficient or useful way of disambiguating the fields, then grouping by additional criteria may be necessary.

Fields are only eligible if they include one of the following source types listed in the table below. All source types require a field label. Some source types also require having a key defined. The following table lists eligible data sources along with additional requirements for field labels and keys.

Eligible source type	Field label required?	Key required?
Id	✓	✗
Name	✓	✗
Metadata	✓	✓
Tags	✓	✓

## Identifying field example

Identifying fields are most useful for stream queries in a data view where the stream property does not provide a useful name. For example, many streams created have a property called "value". You can use this property as an identifying field to provide canonical meaning to the field. In the example below, the data view includes streams for measurements on the inlet pumps for three production lines. Additional metadata is added to each stream using stream metadata rules to describe the measurement captured in each stream. The metadata is then used as an identifying field in the data view.

### Without identifying field

Timestamp.0	Line.1	Value.2 ⓘ	Value.3 ⓘ	Value.4 ⓘ	Value.5 ⓘ
Dec 1, 2022, 12:00:00 AM	Line 1	169.51581663732222	0	Unknown	0
Dec 1, 2022, 1:00:00 AM	Line 1	145.35074140672074	453.07065194499245	Unknown	147
Dec 1, 2022, 2:00:00 AM	Line 1	211.4044696474003	439.85731686808043	Unknown	147
Dec 1, 2022, 3:00:00 AM	Line 1	112.64416812387427	439.9439956654999	Unknown	153
Dec 1, 2022, 4:00:00 AM	Line 1	170.11310308036073	0	High Temperature	0
Dec 1, 2022, 5:00:00 AM	Line 1	146.33162395268687	442.93712429024146	Unknown	148
Dec 1, 2022, 6:00:00 AM	Line 1	113.22254202371418	444.18203055704106	Unknown	153
Dec 1, 2022, 7:00:00 AM	Line 1	210.28106274073062	446.125721865625	Unknown	153
Dec 1, 2022, 8:00:00 AM	Line 1	112.141788197992	453.17362471980675	Unknown	145
Dec 1, 2022, 9:00:00 AM	Line 1	171.99205435526125	461.19607970989125	Unknown	151

Showing 1 - 50 of 75

Items per page: 50 ▾

< 1 >

### With identifying field

Timestamp	Line	Bearing Temperature Value ⓘ	Flow Rate Value ⓘ	Reason Code Value ⓘ
Dec 1, 2022, 12:00:00 AM	Line 1	169.51581663732222	0	Unknown
Dec 1, 2022, 1:00:00 AM	Line 1	145.35074140672074	453.07065194499245	Unknown
Dec 1, 2022, 2:00:00 AM	Line 1	211.4044696474003	439.85731686808043	Unknown
Dec 1, 2022, 3:00:00 AM	Line 1	112.64416812387427	439.9439956654999	Unknown
Dec 1, 2022, 4:00:00 AM	Line 1	170.11310308036073	0	High Temperature
Dec 1, 2022, 5:00:00 AM	Line 1	146.33162395268687	442.93712429024146	Unknown
Dec 1, 2022, 6:00:00 AM	Line 1	113.22254202371418	444.18203055704106	Unknown
Dec 1, 2022, 7:00:00 AM	Line 1	210.28106274073062	446.125721865625	Unknown
Dec 1, 2022, 8:00:00 AM	Line 1	112.141788197992	453.17362471980675	Unknown
Dec 1, 2022, 9:00:00 AM	Line 1	171.99205435526125	461.19607970989125	Unknown

Showing 1 - 50 of 75

Items per page: 50 ▾

&lt; 1 &gt;

For asset queries, this canonical meaning is provided by the asset property name so an identifying field is usually not necessary.

## To add an identifying field

To add an identifying field to the field set for a query, select an eligible field from the **Identifying field** dropdown.

- From the **Identifying Fields** accordion, select **Add an Identifying Field**.

The screenshot shows a user interface for managing data queries. At the top, there's a header with a checkbox labeled 'Query1', a 'Production' button, and an 'Assets' dropdown. Below this, an 'Identifying Field' dropdown is open, showing a list of options: 'None', 'Id', 'Metadata · Latitude', and 'Metadata · Longitude'. The 'None' option is highlighted, indicating it is the current selection.

- Choose an identifying field.

## Edit field set order

By default, fields added to a field set are listed alphabetically within your data view. However, you can manually edit the order that fields display. Fields will display in your data view in the configured order, immediately following grouping fields.

### To edit field order

You can either edit the field order by using **page controls** or **drag and drop**.

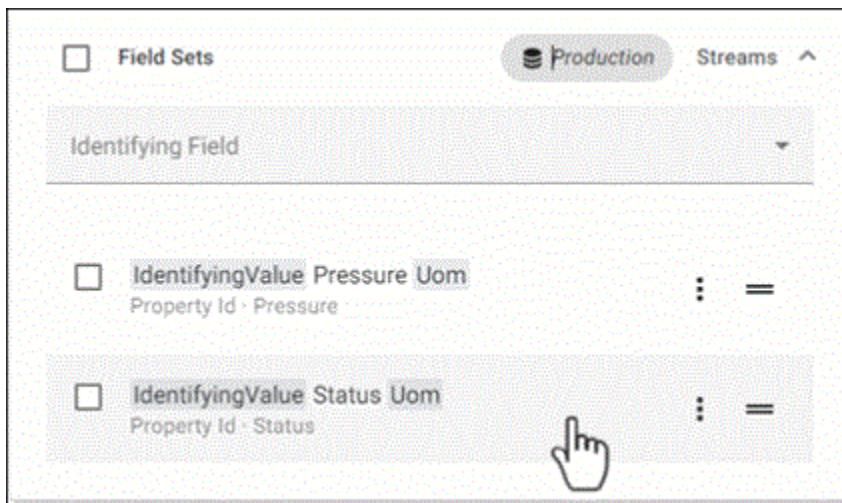
#### Page controls

1. Within a field set, select the field that you want to reorder.
2. Select **Arrow up** ↑ or **Arrow down** ↓ to move the field to the new position within the field set.

#### Drag and drop

To reorder data fields within a data field set, you can also drag and drop a field to its new position.

##### Drag and drop fields



#### Link data fields

Data items included in a data view may have slight differences in property naming, despite those properties representing the same logical thing. For example, data from one equipment manufacturer reports *Temperature*, while another reports *Temp* instead.

Data views can overcome property naming differences by linking these similar properties into a single data field. This applies to stream properties referenced by Id or by name, and to stream metadata keys. Asset properties can also be linked.

When data fields are linked, CONNECT data services converts the data types in the linked fields into compatible data types. For more information, see [Data view data type conversion](#).

## To link fields

To link data items, drag and drop one field onto another. Properties can only be linked to other properties of the same data type. Metadata can only be linked to other metadata of the same data type.



## To unlink fields

To unlink a linked field, select **More options** : > **Unlink All**.

## Manage permissions for data views

If you are assigned the **Manage Permissions** access right, then you can configure data view permissions for other user roles in your tenant. You can granularly assign individual data view permissions to each user role.

### Prerequisites

To manage data view permissions, you must be assigned the **Manage Permissions** access right.

## To manage permissions for data views

1. From the left pane, select **Analytics > Data Views**.
2. Select a data view.
3. From the side panel, select **More options** : > **Manage Permissions**.  
The Manage Permissions for Data View window opens.
4. Use the Manage Permissions for Data View window to:
  - (Optional) Add user roles that have permissions on the data views.
  - Edit data view permissions for each user role.  
For more information, see [Permissions management](#).
5. When you are finished editing permissions, select **Save**.

## To manage default permissions for new data views

You can edit the default user roles and permissions added to a data view when it is created.

1. From the left pane, select **Analytics > Data Views**.
2. From the toolbar, select **More options :** > **Manage Default Permissions for New Data Views**.
3. Use the Manage Default Permissions for New Data Views window to edit default user roles and data view permissions. For more information, see [Permissions management](#).
4. When you are finished editing permissions, select **Save**.

## Retrieve data for a data view

After you create and configure a data view, you can programmatically retrieve the data set that it resolves to using the CONNECT data services REST API. With a data-driven application (like Microsoft Power BI), you can leverage the data view for data science enablement.

### Data retrieval options

To retrieve a data view, you can either use the CONNECT data services Power BI Connector, or you can interact directly with the CONNECT data services REST API using an example GitHub project as a starting point.

#### Option A: Microsoft Power BI

You can retrieve a data view using Microsoft Power BI. Retrieving a data view in Microsoft Power BI requires installation of CONNECT data services Power BI Connector. The banner at the top of the [Create and configure a data view](#) page contains a link to the Connector.

1. Install the CONNECT data services Microsoft Power BI Connector.

Install the CONNECT data services Power BI Connector. The banner at the top of the page contains a link to the Connector. If you dismiss the banner, you can still download the connector by selecting **More options :** > **Power BI Connector**.

For more information on installing the CONNECT data services Power BI Connector, see [Power BI Connector setup](#).

2. Use Microsoft Power BI to retrieve your data view.

Use Microsoft Power BI to retrieve your data views. For more information, see [Retrieve data views with Power BI Connector](#).

#### Option B: Interact with the REST API

Alternative to using Microsoft Power BI, you can interact with the CONNECT data services REST API directly by using a sample project provided by AVEVA. Sample projects for the following technologies are available on GitHub:

- [Grafana](#)

- Jupyter
- Python
- R
- .NET
- Java

Complete the following steps to retrieve a data view using the REST API.

1. Create a client-credentials client.

To retrieve a data view from CONNECT data services, you must authenticate with a valid Client Id and Client secret. You can obtain an Id and secret by creating a set of client-credentials. When you create the client-credentials, accept the default expiry of 3600 seconds. When you receive the client secret, keep it secure, as there is no way to see the secret again. If you lose it, you need to create a new set of client-credentials.

For more information on creating client-credential clients, see [Add a client-credentials client](#).

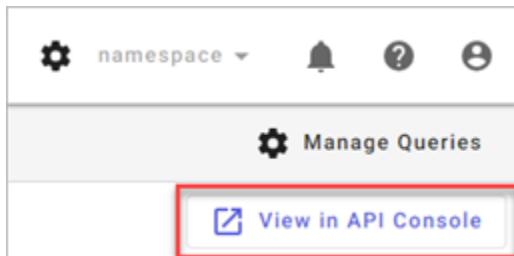
2. Configure your sample project and retrieve your data view.

Use one of the starter projects listed above. Pass your project client-credentials to authenticate and provide it with the URI for your data view. For more information on this process, see the link above.

### Tip: Use the API Console to retrieve your data view

While creating or editing a data view, use  **View in API Console** to open the view in the [API console](#). The API console includes the URI and query values for accessing your data view in its current configuration.

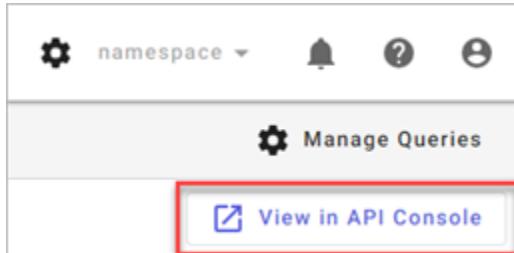
#### View in API Console button



### Data views and the API Console

While creating or editing a data view, you can launch it within the API Console by choosing the **View in API Console** button. Launching the data view in the API console allows you to refine the data view endpoint query before specifying its URI in your application code or Microsoft Power BI.

#### View in API Console button



## Data view API console parameters

When viewing a data view from the API Console, you can edit the default parameters that you configured during initial creation of the data view. Additionally, you can provide continuation tokens (in support of data pagination), caching data, or choose different support response formats.

Field	Description
startIndex	The inclusive start boundary of the data view data.
endIndex	The inclusive end boundary of the data view data.
count	The number of data points included in the request.
interval	The requested interval between index values.
continuationToken	The field for specifying a continuation token when a request returns. For more information on this field and the <b>Load from Response</b>  button, see <a href="#">API console</a> .
cache	The field for setting cache behavior. Values include: <ul style="list-style-type: none"> <li><i>Preserve</i> (default): Uses cached information, if available.</li> <li><i>Refresh</i>: Forces the resource to re-resolve.</li> </ul>
form	The file format that request response returns. For information on the response forms available, see the table below.

## Response forms

When requesting data views from the API Console, the REST API is capable of returning requests in a variety of file formats. Select a form from the dropdown. Supported response forms include:

Form	Description
default (JSON)	Object-style JSON.
table (Table)	Table-style JSON.
tableh (Table with headers)	Table-style JSON with header row.
csv (Comma separated values)	Comma-separated values.
csvh (Comma separated values with headers)	Comma-separated values with header row.
parquet (Apache Parquet)	Parquet format. For more information on the Parquet

Form	Description
	format, see <a href="#">Parquet data format</a> .

## Data view data type conversion

When you request a data view that includes multiple data types in a single column:

1. The data view converts two or more SDS data types into a compatible SDS data type wide enough to accommodate all types without losing information. This conversion occurs to accommodate the strongly-typed data in the [Parquet data format](#).
2. When you request a data view in the Parquet format, an additional conversion takes place. The compatible SDS data type referenced in step 1 is converted to a Parquet data type. This conversion occurs because the Parquet format does not support all data types natively.

## SDS data type conversion

The following table lists the resulting SDS data type when two are converted:

Type1	Type2	Becomes
SByte	Byte	Int16
SByte	Int16	Int16
SByte	UInt16	Int32
SByte	Int32	Int32
SByte	UInt32	Int64
SByte	Int64	Int64
SByte	UInt64	Decimal
SByte	Single	Single
SByte	Double	Double
SByte	Decimal	Decimal
Byte	Int16	Int16
Byte	UInt16	UInt16
Byte	Int32	Int32
Byte	UInt32	UInt32

Type1	Type2	Becomes
Byte	Int64	Int64
Byte	UInt64	UInt64
Byte	Single	Single
Byte	Double	Double
Byte	Decimal	Decimal
Int16	UInt16	Int32
Int16	Int32	Int32
Int16	UInt32	Int64
Int16	Int64	Int64
Int16	UInt64	Decimal
Int16	Single	Single
Int16	Double	Double
Int16	Decimal	Decimal
UInt16	Int32	Int32
UInt16	UInt32	UInt32
UInt16	Int64	Int64
UInt16	UInt64	UInt64
UInt16	Single	Single
UInt16	Double	Double
UInt16	Decimal	Decimal
Int32	UInt32	Int64
Int32	Int64	Int64
Int32	UInt64	Decimal
Int32	Single	Double
Int32	Double	Double
Int32	Decimal	Decimal

Type1	Type2	Becomes
UInt32	Int64	Int64
UInt32	UInt64	UInt64
UInt32	Single	Single
UInt32	Double	Double
UInt32	Decimal	Decimal
Int64	UInt64	Decimal
Int64	Decimal	Decimal
UInt64	Decimal	Decimal
Single	Double	Double

Nullable types and non-nullable types convert into a nullable type. If CONNECT data services cannot convert two data types into a compatible type, it will convert them into strings. When you request a data view in the Parquet format with the **Narrow** data view shape selected, CONNECT data services converts combined columns into strings.

## SDS to Parquet data type conversion

The following table lists the SDS data types and their corresponding Parquet data types.

SDS Type Code/CLR Type	Physical Type	Converted Type	Logical Type
Byte (Byte)	INT32	UNIT_8	INT (8, false)
SByte (Sbyte)	INT32	INT_8	INT (8, true)
Int16 (Short)	INT32	INT_16	INT (16, true)
UInt16 (Ushort)	INT32	UINT_16	INT (16, false)
Int32 (Int)	INT32	INT_32	INT (32, true)
UInt32 (Uint)	INT32	UINT_32	INT (32, false)
Boolean (Bool)	BOOLEAN	UTF8	
String (String)	BYTE_ARRAY	UTF8	STRING
Single (Float)	FLOAT	UTF8	
Int64 (Long)	INT64	INT_64	INT (64, true)
UInt64 (Ulong)	INT64	UINT_64	INT (64, false)

SDS Type Code/CLR Type	Physical Type	Converted Type	Logical Type
Double (Double)	DOUBLE	UTF8	
Decimal (Decimal)	FIXED_LEN_BYTE_ARRAY	DECIMAL	DECIMAL
DateTime (DateTime)	INT64	UTF8	TIMESTAMP (false, MICROS)
DateTimeOffset (DateTimeOffset)	INT64	UTF8	TIMESTAMP (false, MICROS)
Char (char)	BYTE_ARRAY	UTF8	STRING
Guid (Guid)	BYTE_ARRAY	UTF8	STRING
Version (Version)	BYTE_ARRAY	UTF8	STRING

## Parquet data format

CONNECT data services can output your data view in Apache Parquet, an open source, column-oriented data file format designed for efficient data storage and retrieval. This binary file format allows you to easily upload CONNECT data services data into data lakes and data warehouses. Parquet is a common format for working with data in technologies like Databricks, Snowflake, Azure, AWS, and others.

### Parquet data serialization

When you request a data view in Parquet format, CONNECT data services serializes the data from text-based data to the Parquet binary file format, which is not human-readable. To read the Parquet file, you will need to open it with a programming language routine or application capable of deserialization, such as Databricks, Snowflake, Azure, AWS, or another compatible application.

### Parquet file download

When you make requests against a dataview in the [API console](#) with the Parquet form selected, you can download the request as a Parquet file. Select **Download Parquet File** to download the file.

For more information on how to request a data view in the Parquet format, see [Data views and the API Console](#).

[API Console: Download Parquet File](#)

Parquet Details

Preview Unavailable

Previewing Parquet files is not supported. Use the "Download Parquet File" button below to download the Parquet File. For more information see the [Data Views Documentation](#)

[Download Parquet File](#)

## Handling multiple data types

When you request a data view that includes multiple data types in a single column:

1. The data view converts two or more SDS data types into a compatible SDS data type wide enough to accommodate all types without losing information. This conversion occurs to accommodate the strongly-typed data in the Parquet format.
2. The data view converts the compatible SDS data type to a Parquet data type. This conversion occurs because the Parquet format does not support all data types natively.

For more information on the conversion, see [Data view data type conversion](#).

## Data view troubleshooting

While working with data views, you may encounter warnings about your data view configuration settings. This topic details possible warnings and how to address them.

### Data Views page

While browsing the list of data views, you may encounter the following warnings.

### Alert tag

Query sources that include a yellow or red alert tag indicate that you have an issue affecting your view of the data view. There are several contexts for when an alert tag displays:

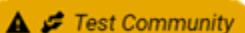
- Unknown community tag



Yellow alert tags that read Unknown Community indicate that you have insufficient permissions to access the community or that has been deleted. You must be a member of the community to access its data.

Additionally, you cannot edit the query for the community until you are member of the community. Request that a community administrator add you to the community.

- Read access tag with community name



Yellow alert tags that display the community name indicate that you are a Community Administrator or Community Member with read access, but not a member of the community itself. Community Administrators can use the visible community name to add users to the community. For more information on adding a user to the community, see [Manage users in a community](#).

- Cross region opt out tag



Red alert tags indicate that the data view queries a namespace that has opted out of [Cross-region data sharing](#), but the data view resides in a different region. For more information, see below.

## Data View page

You may encounter the following warnings while editing a data view.

### No included fields

If the field set for a query includes no fields, an alert of No Included Fields displays. You can correct this error by adding one or more fields to the query. For more information, see [Manage data fields](#).

### No Included Fields

The screenshot shows a data view configuration interface. At the top, there's a search bar labeled 'Query1' and a button for 'Production Assets'. Below the search bar is a dropdown menu labeled 'Identifying Field'. At the bottom of the screen, a yellow warning box contains a warning icon (a triangle with a exclamation mark) and the text 'No Included Fields'.

There are included fields that don't map to anything

If one of your queries includes fields that do not map to anything, an error of There are included fields that don't map to anything displays at the bottom of the field sets.

### Field set error

**⚠ There are included fields that don't map to anything**

You can correct this error by finding the individual fields that do not map to anything and removing them. Fields that do not map to anything are denoted by the alert **⚠** icon. For more information on removing a field from a field set, see [Manage data fields](#).

## Manage Queries

While managing data view queries, you may encounter the following warning.

### Cross region processing opt out

If you encounter a warning of This namespace does not allow data to be processed outside of the region where it resides, this message indicates that the namespace has opted out of sharing its data across regions, and the currently selected namespace has a different primary geographical region. Therefore, the data view cannot be processed in the currently selected namespace. For additional information, see [Cross-region data sharing](#).

You can encounter the message above in different contexts:

- **While adding a query**

While you are adding a query, CONNECT data services compares the region of the current namespace against the region of the namespace you are adding to the data view. If you attempt to add a namespace that has opted out of cross region data sharing, and the currently selected namespace has a different geographical region than that namespace, the source is unavailable and therefore cannot be added. A tooltip displays if you mouse over the source:

The screenshot shows the 'Query Source' section of the AVEVA interface. It includes a search bar, filter options for 'Namespaces' and 'Communities', and a list of namespaces. The 'Production' namespace is selected and highlighted with a red border. A tooltip message appears over the 'Production' entry: 'Namespace Production: This namespace does not allow data to be processed outside of the region where it resides.'

Name	Region	Description
WestUS	Automated e2e namespace	
NebulaTesting	WestUS	namespace for nebula testing
Production	WestUS	
QuesoTestEU	WestEurope	Testing for hyperion
UxieTesting	WestUS	UxieTesting

- **While managing an existing query**

If a data view is created that includes a namespace that later opts out of cross region data sharing, an alert displays in the Query panel that the data view includes a source that cannot be shared across region:

The screenshot shows the 'Query1' interface. A red button labeled 'Production' is selected. An alert message box is displayed: 'Production does not allow data to be processed outside of the region where it resides.' Below the alert, a yellow bar indicates 'No Included Fields'.

When the query that includes a disabled source is selected, the following message displays:

Cross Region Data Sharing Disabled: This namespace does not allow data to be processed outside of the region where it resides.

## Data view invalidation

If the data view is modified, any cached information is reset. The data view re-resolves the next time that information is requested.

No guarantee is made of the durability or lifespan of cached information. If cached information is invalidated, the data view is re-resolved the next time that information is requested.

Cached information may be reset under any of the following circumstances:

- The data view is modified
- A community referenced by the data view is modified (for example, sharing is paused)
- The cached information expiration time elapses
- System maintenance

## Virtual tables (Preview)

Virtual tables enable integration between CONNECT data services and third-party analytics platforms like Databricks, Snowflake, and Microsoft Fabric.

Virtual tables allow you to:

- Access operations data for analytics initiatives.
- Support the integration of operations data into existing business and financial data infrastructures for data exploration, reporting, and analytics.
- Make [Data views](#) available on-demand to third-party data and analytics platforms as an external data source.

Your third-party cloud analytics platforms will be able to interact with data from CONNECT data services using the native languages and tools you are familiar with.

---

**Note:** Databricks is the only integration currently available.

---

## Virtual tables workflow

1. If you have none available, create [Data views](#).
2. [Create a share](#) to connect CONNECT data services to your third-party analytics program.
3. [Create a virtual table](#) using your data views and share.
4. [Manage permissions for virtual tables](#) if you need to add new roles or adjust existing roles. For more information on roles, see [CONNECT data services roles](#).

## Shares

Shares create a connection between CONNECT data services and a third-party analytics platform. This allows CONNECT data services to send data compiled in a data view and organized in a virtual table to your third-party analytics platform.

## Create a share

A share must be established between CONNECT data services and Databricks before you can create a virtual table.

Before you begin, get the Databricks sharing identifier for the metastore with which you want to create a share.

To create a share, perform the following steps:

1. In the left pane, select **Analytics > Virtual Tables**.
2. Select the **Shares** tab.
3. Select **Create share**.
4. Give your share a name in the **Name** box.

Names may only contain upper and lower-case letters, numbers, and underscores. Incorrectly formatted share names will cause the virtual table assignment to fail.

5. Copy your Databricks sharing identifier from your Databricks instance and paste it into the **Sharing identifier** box.  
The Databricks sharing identifier is in a <provider>:<region>:<metastoreid> format such as `azure:westus:f12dcb34-5678-9d4c-1234-c5ac67f8b90a`.
6. Select **Create**.

## Edit a share

To edit a share, perform the following steps:

1. In the left pane, select **Analytics > Virtual Tables**.
2. Select the **Shares** tab.
3. Select the share you want to edit.
4. Select **More Options**  and then select **Edit share**.  
You can edit the name and Databricks sharing identifier.
5. Select **Save**.

## Delete a share

To delete a share, perform the following steps:

1. In the left pane, select **Analytics > Virtual Tables**.
2. Select the **Shares** tab.
3. Select the share you want to edit.
4. Select **More Options**  and then select **Delete share**.
5. At the prompt, select **Delete**.

## Create a virtual table

A share must be established between CONNECT data services and Databricks before you can create a virtual table.

To create a virtual table, perform the following steps:

1. In the left pane, select **Analytics > Virtual Tables**.

2. Select the **Virtual Tables** tab.
3. Select **Create virtual table**.
4. Select a data view for use in your virtual table.  
For more information on data views, read [Data views](#).
5. Select **Next**.
6. Type a name for your virtual table in the **Name** box.  
The name of your chosen data view is visible for reference.
7. Select an **Interpolated** or **Stored** retrieval mode.
  - **Interpolated**: Returns data between specified intervals.  
If you select Interpolated, provide an **Interpolation interval** (dd.hh:mm:ss).
  - **Stored**: Returns stored or window data.  
For more information on data retrieval types, see [Preview and save the data view](#).
8. Select a Retrieval interval and provide a time window.
  - **Time-Fixed Window**: contains a beginning and an end time.
  - **Time-Extending Window**: only contains a start time.
9. Provide a **Refresh interval**.
10. Select **Next**.
11. Select the **Share(s)** you want in your virtual table.  
If you do not have an available share, select **Create share**. For more information on how to create a share, see [Create a share](#).
12. Select **Next**.
13. Review the summary of your virtual table and select **Save**.  
Once the virtual table has been shared with the target Databricks metastore, your Databricks metastore administrator will need to create a catalog for your workspace from the share. The virtual table will then appear in the catalog.

## Edit a virtual table

To edit a virtual table, perform the following steps:

1. In the left pane, select **Analytics > Virtual Tables**.
2. Select the **Virtual Tables** tab.
3. Select the virtual table you want to edit.
4. Select **More Options**  and then select **Edit virtual table**.  
You can edit the name, data collection configuration, and the scheduler configuration.
5. Select **Save** once you finish editing your virtual table.

## Manage permissions for virtual tables

For more information on roles, see [CONNECT data services roles](#).

## Manage permissions for a single virtual table

1. In the left pane, select **Analytics > Virtual Tables**.
2. Select the **Virtual Tables** tab.
3. Select a virtual table.
4. Select **More Options**  and then select  **Manage virtual table permissions**.
  - Select  **Add Role** to add a new role for the virtual table.
  - You can update permissions for read, write, delete, and manager permissions.
  - Select  **Clear permissions** to remove the permissions from your virtual table.
5. Select **Save** when you finish updating the permissions for your virtual table.

## Manage default permissions for virtual tables

1. In the left pane, select **Analytics > Virtual Tables**.
2. Select the **Virtual Tables** tab.
3. Select **More Options**  and then select  **Manage default permissions for new virtual tables**.
  - Select  **Add Role** to add a new roles for virtual tables.
  - You can update permissions for read, write, delete, and manager permissions.
  - Select  **Clear permissions** to remove the permissions from new virtual tables.
4. Select **Save** when you finish updating the default permissions for new virtual tables.

## Delete a virtual table

To delete a virtual table, perform the following steps:

1. In the left pane, select **Analytics > Virtual Tables**.
2. Select the **Virtual Tables** tab.
3. Select the virtual table you want to delete.
4. Select **More Options**  and then select **Delete virtual table**.
5. At the prompt, select **Delete**.

## Power BI Connector

The CONNECT data services Power BI Connector retrieves data views from CONNECT data services and makes them available in Microsoft Power BI for advanced data visualization and analysis. You can also use Microsoft Power BI to edit the query generated from the connector to modify the dates, edit the interpolation interval, and enable an incremental refresh of data.

## Power BI Connector setup

You must install the CONNECT data services Power BI Connector to retrieve data views for use with Microsoft Power BI.

### System requirements

The following are required before you install and use the CONNECT data services Power BI Connector.

- Operation Systems: Windows 10, Windows 11, Windows Server 2012 R2, Windows 8.1, Windows Server 2016, Windows Server 2019, Windows Server 2022
- For desktop installation: Microsoft Power BI Desktop 2.91.884.0 or later
- For on-premises Data Gateway installation: Microsoft Power BI On-premises Data Gateway 3000.89.6 or later
- Microsoft Edge WebView 2 Runtime
- A user account with Administrator privileges to install CONNECT data services Power BI Connector on a local machine.

### Download Power BI Connector

1. In the left pane, select **Analytics > Data Views**.
2. Select **More options :** > **Download Power BI Connector**.
3. On the Power BI Connector Installer Download window, select **Download**. When the download completes, close the window.

### Install Power BI Connector

You can install Power BI Connector by wizard or command line.

#### Wizard installation

1. Open the Power BI Connector installation file then select **Yes** to confirm running the installation file.
2. Accept or change the temporary setup extraction folder and select **OK**.  
The Power BI Connector Setup Wizard opens.
3. Select **Next**.
4. (Optional) To install the connector to an on-premises data gateway, select **On-premises data gateway installation** and specify the custom data connector directory for your on-premises data gateway.  
For more information about on-premises data gateway installations, see the Microsoft documentation [Use custom data connectors with the on-premises data gateway](#).
5. Select **Next**.
6. Select **Install**.
7. Select **Finish** to exit the Setup Wizard.

#### Command line silent installation

To silently install Power BI Connector, open a command line session, change to the installation file download

directory, and enter the following command:

```
.\CONNECT_data_services_Power_BI_Connector_x_x_x_x.exe -Y INSTALLDIR=<install path>  
/quiet
```

- Replace x\_x\_x\_x with the version number of the installer.
- Power BI Connector supports silent installation for on-premises data gateway installations.

## Retrieve data views with Power BI Connector

Use CONNECT data services Power BI Connector to retrieve data views for use in Microsoft Power BI.

### Prerequisites

While retrieving a data view from CONNECT data services, Power BI Connector prompts you to authenticate with Microsoft Power BI. You have two options for authentication:

- **Organizational account**

Authenticate the connection between CONNECT data services and Microsoft Power BI using the same organizational account that you use to sign into CONNECT. If you use this authentication option, Power BI Connector prompts you to reauthenticate the connection every seven days.

If you choose this authentication option, you can begin the task below without completing any prerequisites.

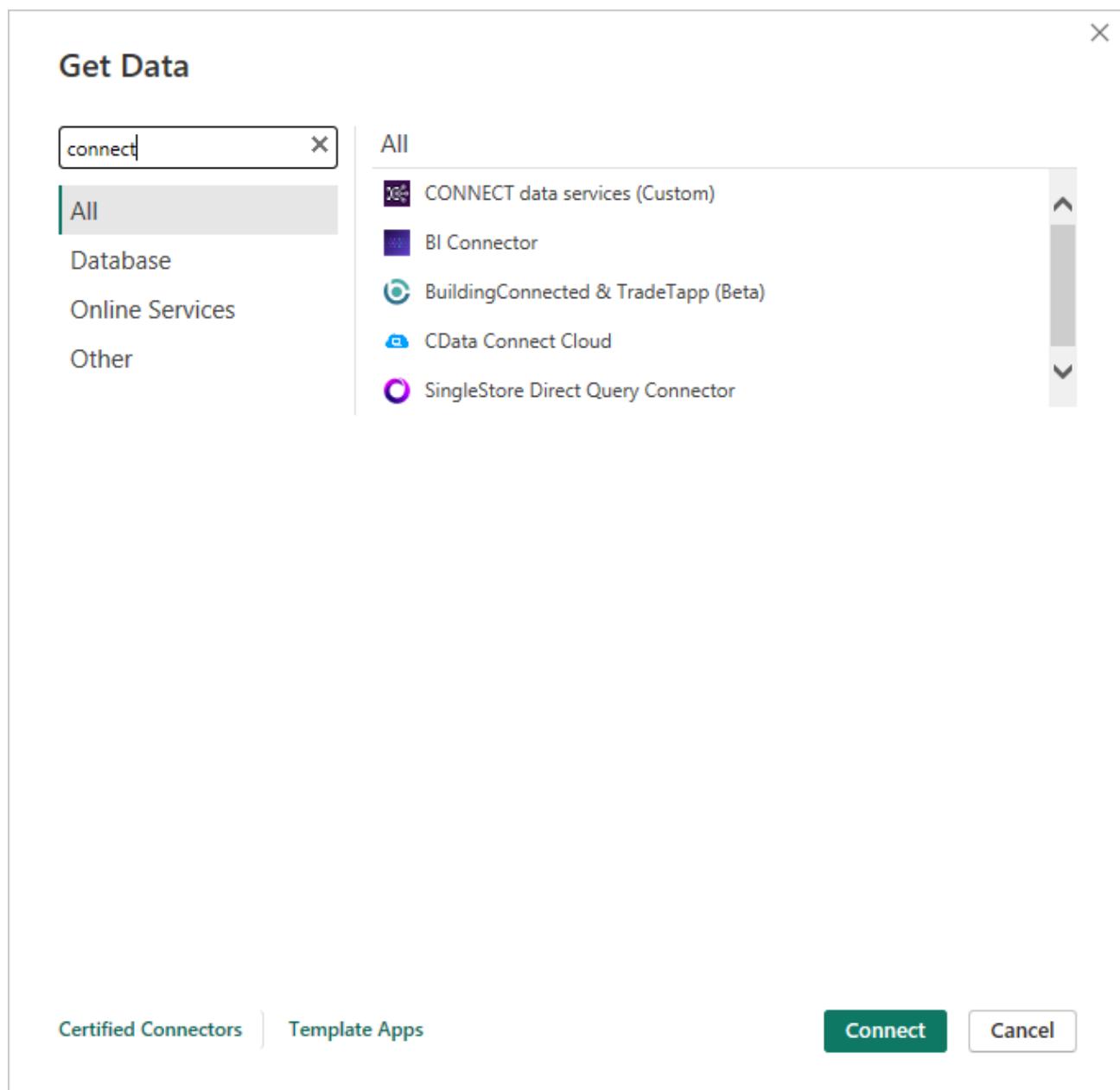
- **Client-credential client**

Use a CONNECT client-credential client Id and client secret to authenticate with Microsoft Power BI. This authentication option is preferred over organizational account because it allows Microsoft Power BI to remain securely connected with CONNECT data services without prompting you to reauthenticate every seven days.

If you choose this option, you must create and configure a client-credential client for use during authentication. These credentials are used while completing the task below. For instructions on creating these credentials, see [Add a client-credentials client](#). While creating the credentials, select one or more **Tenant Roles** that provide access to the data view, applying the concept of [Least Privilege](#). While creating the credentials, record the **Client Id** and **Client Secret** to enter while retrieving a data view.

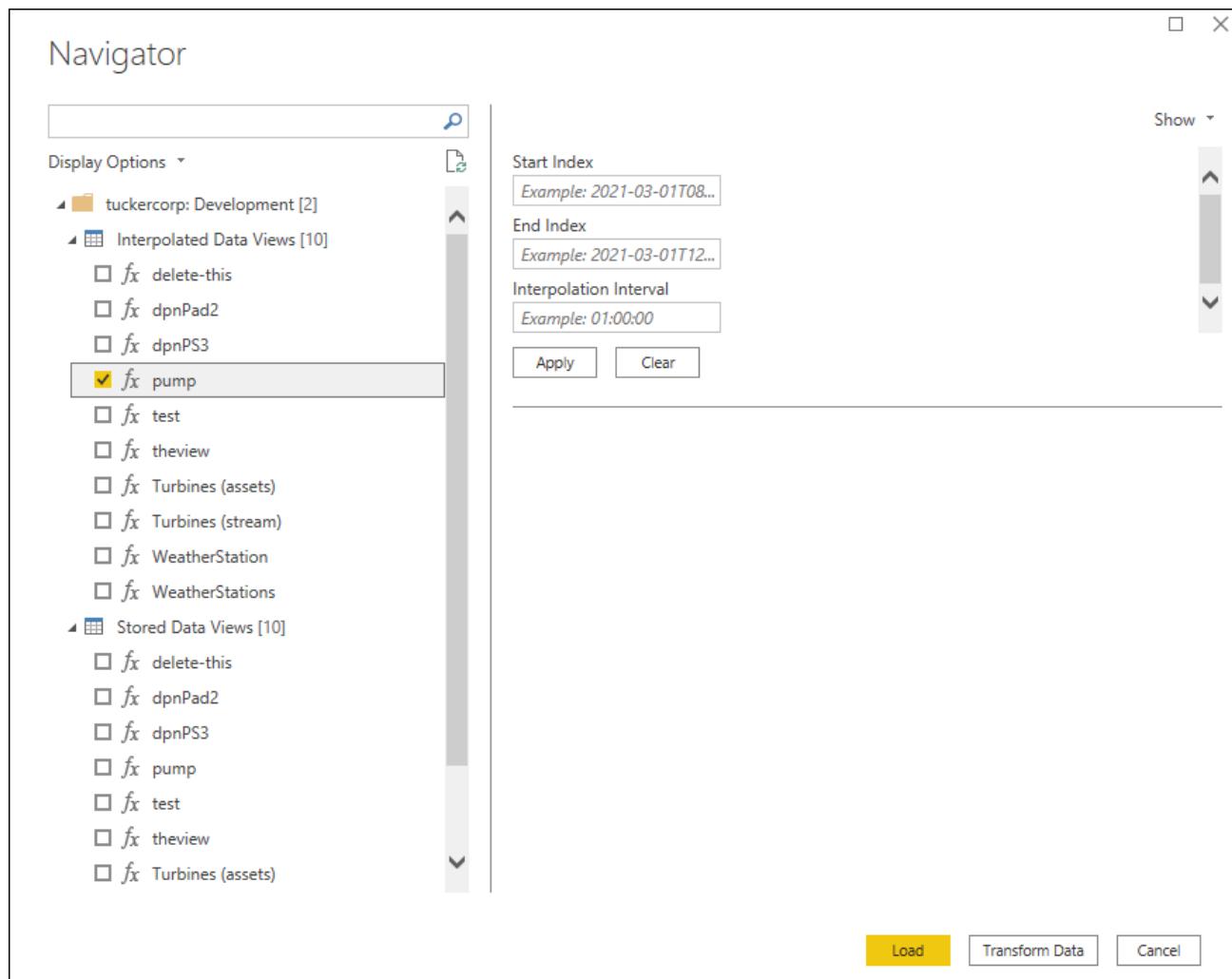
### To retrieve data views

1. In Microsoft Power BI Desktop, in the entry field of the Get Data window, type connect.  
The CONNECT data services (Custom) connector file displays in the All pane.



2. Select the **CONNECT data services (Custom)** connector file, and then select **Connect**.
3. Select **Continue** in the Connecting to a third-party service warning.
4. In the CONNECT data services window, enter the namespace for the data views you want to access, and then select **OK**.
5. Authenticate the connection between CONNECT data services and Microsoft Power BI.
  - **Organizational Account:**  
Select **Organizational account**. Then select **Log in**. Enter the credentials you use to sign in with CONNECT.
  - **Client Credentials:**  
Select **Client Credentials**. Then enter the **ClientId** and the **Client Secret** for the client credential clients that you created while fulfilling the prerequisites.
6. Select **Connect** to connect CONNECT data services to Microsoft Power BI.

- In the **Navigator** pane, choose a data view to work with from either **Interpolated Data Views** or **Stored Data Views**.



- Specify a **Start Index** and **End Index** for the data that you want to work with. Enter the date in YYYY-MM-DDTHH:mm:ss format.
- If you are working with an **Interpolated Data Views**, you must specify an **Interpolation Interval** as well. Enter it in dd.hh:mm:ss format.
- If a data view you are working with has default index values or default interpolation interval values defined, you can override them by entering new values and selecting **Apply**.

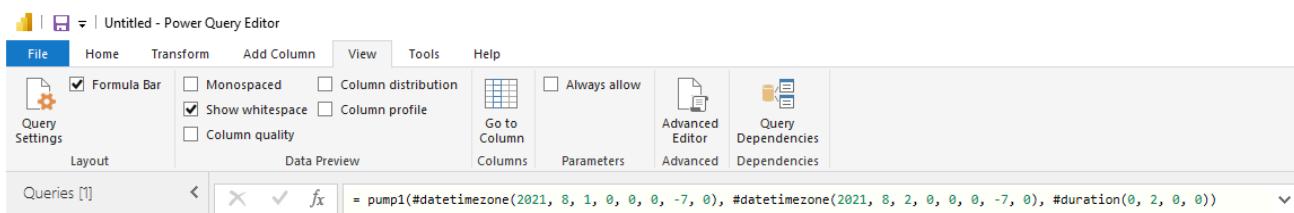
The screenshot shows the Microsoft Power BI Navigator pane. On the left, there's a tree view of data sources and views. Under 'tuckercorp: Development [2]', the 'Interpolated Data Views [10]' node is expanded, showing items like 'delete-this', 'dpnPad2', 'dpnPS3', and 'pump'. The 'pump' item has a checked checkbox next to it. On the right, there are filter settings for 'Start Index' (set to 2021-08-01), 'End Index' (set to 2021-08-02), and 'Interpolation Interval' (set to 02:00:00). Below these filters is a preview table titled 'pump' with columns: Timestamp, Sensor0, Sensor1, Sensor10, and Sensor11. The table contains 14 rows of data. At the bottom of the pane are three buttons: 'Load' (highlighted in yellow), 'Transform Data', and 'Cancel'.

11. Select **Load** at the bottom of the Navigator pane to load all selected data views to Microsoft Power BI.
12. (Optional) If you are using an on-premises data gateway in combination with the **Client Credentials** authentication method, we recommend creating a new data source connection within the Power BI Service that uses your client credentials for authentication.
13. For more information on creating a data source connection in the Power BI Service, see the Microsoft document [Add or remove a gateway data source](#). The client credentials authentication method is recommended when using the CONNECT data services Power BI Connector as a data source in the Power BI Service.

## Edit a data view query in Microsoft Power BI

Use Microsoft Power BI to edit a query generated from the connector to modify the Start Index and End Index to fixed dates or relative dates, as well as edit the Interpolation Interval (if applicable). You can also use Microsoft Power BI to enable an incremental refresh of data.

1. In Microsoft Power BI, select **Transform data** to view the query with Power Query Editor.
2. Select **View**, and then select **Formula Bar** to view the query function from the connector.



As shown in the example, the function begins with the first set of code for the Start Index, #datetimezone(2021, 8, 1, 0, 0, 0, -7, 0), followed by the second set for the End Index, #datetimezone(2021, 8, 2, 0, 0, 0, -7, 0), and lastly the Interpolation Interval, #duration(0, 2, 0, 0).

3. Modify the Start Index and End Index to fixed dates or to relative dates in the function with Power Query M Formula Language code.
  - Modify for fixed dates:
    - a. Navigate to **APPLIED STEPS** in the Query Settings pane, right-click on the parameter labeled **Invoked Function <nameofdataview>**, and then select **Edit Settings** in the dropdown menu.
    - b. Edit the parameter values for Start Index and End Index. If applicable, edit the Interpolation Interval.



- Modify for relative dates:
  - a. Edit the query function with Power Query M Formula Language code. For information about Power Query M Formula Language code, see [Microsoft Power Query M formula language](#) and [Power Query M function reference](#) for functions you can use in your query. Below are common relative time configurations you can use in your query function.

Query function description	Code
Rolling 2 month period Start Index: 2 months ago End Index: Now	Date.AddMonths(DateTimeZone.LocalNow(), -2), DateTimeZone.LocalNow()
Rolling 1 day period Start Index: 1 day ago End Index: Now	Date.AddDays(DateTimeZone.LocalNow(), -1), DateTimeZone.LocalNow()
Start of last month through now	Date.StartOfMonth(Date.AddMonths(DateTime

Query function description	Code
Start Index: First day of last month at midnight End Index: Now	Zone.LocalNow(), -1)), DateTimeZone.LocalNow()

4. Select **Close & Apply**, and then select **Close & Apply** in Power Query Editor to save your query.
5. (Optional) Use Microsoft Power BI Desktop to enable an incremental refresh of data.
  - a. In Microsoft Power BI, select **Transform data** to open Power Query Editor.
  - b. Select **Manage Parameters**, and then select **Manage Parameters** in the menu.
  - c. Add the following parameters in the Manage Parameters window, and then select **OK**.

Parameter	Code
<i>RangeStart</i>	Description: <optional> Required: selected Type: Date/Time Suggested Values: <Any value>, <List of values>, <Query> Current Value: <Start date of the date range>
<i>RangeEnd</i>	Description: <optional> Required: selected Type: Date/Time Suggested Values: <Any value>, <List of values>, <Query> Current Value: <End date of the date range>

**Note:** *RangeStart* and *RangeEnd* must be named and mixed-cased as is for incremental refresh to work. Type must always be Date/Time.

- d. Edit the query function to use the *RangeStart* and *RangeEnd* parameters defined in the previous step. For example:

`DateTimeZone.From(RangeStart), DateTimeZone.From(RangeEnd), #duration(0, 1, 0, 0)`

- e. Select **Close & Apply**, and then select **Close & Apply** in Power Query Editor.
- f. Select **Home**, and in the Fields pane, right-click the data view type, and then choose **Incremental Refresh** in the dropdown menu.
- g. Turn on **Incremental Refresh**, edit the values in the **Store rows in the last** fields, and select **Apply all** to save.

This builds a cache of data in Microsoft Power BI so you will not need to re-query the original data view. The following example image shows that incremental refresh is turned on, will cache 30 days of data, and the last 5 days will be a rolling refresh of data.

Incremental refresh

⚠️ Unable to confirm if the M query can be folded. It is not recommended to use incremental refresh with non-foldable queries. [Learn more](#)

You can improve the speed of refresh for large tables by using incremental refresh. This setting will apply once you've published a report to the Power BI service.

ⓘ Once you've deployed this table to the Power BI service, you won't be able to download it back to Power BI Desktop. [Learn more](#)

Table Incremental refresh

pump  On

Store rows in the last:

30 Days

Refresh rows in the last:

5 Days

Detect data changes [Learn more](#)

Only refresh complete days [Learn more](#)

Apply all Cancel

For more information about incremental refresh, see the Microsoft [Incremental refresh for datasets](#) page.

## CONNECT data services Power BI Connector release notes

The CONNECT data services Power BI Connector allows CONNECT data services data views to be imported into Power BI so the data can be visually analyzed or utilized in Power BI reports or dashboards.

The Power BI Connector can be installed on Windows operating system installations of Power BI Desktop. The connector can also be used with the Power BI Service through installation of an on-premises data gateway. Data sets using CONNECT data services data views can be configured for scheduled refresh in the Power BI service to create and share dynamically updating Power BI dashboards with data from CONNECT data services.

## New features

Release 2.1.0.0 adds a new option for authentication between Microsoft Power BI and CONNECT data services: Client-credential clients authentication. Authentication using client-credential clients allows Microsoft Power BI to remain securely connected with CONNECT data services without having to reauthenticate every seven days as you do with the original authentication option, OAuth. This new authentication method improves user experience without sacrificing security.

The new client-credential client authentication method does not replace the original authentication option of using your organizational account. Client credentials are recommended when using the CONNECT data services Power BI Connector for scheduled refresh in the Power BI service (but not when using the connector with Power BI Desktop).

For more information on authentication options and how to configure them, see [Retrieve data views with Power BI Connector](#).

## Resolved issues

The following issues have been resolved for the 2.1.0.0 release:

Work Item	Description
401709	Namespace name is not recognized when folder is renamed in CONNECT.
385539	Data views do not load after retrying from a "No Data Views found for Namespace" error.

## Known issues

The known issues and limitations from release 2.0.0.54 have not been resolved and remain in release 2.1.0.0.

## CONNECT data services Power BI Connector 2.0.0.54

The following known issues and limitations are included for release 2.0.0.54.

## Known issues

Work item	Description
248772	When the same installer runs twice, the dialog appears offering the user the chance to uninstall the connector. If the user clicks on Uninstall option and then clicks on the Back button, the user is brought to a screen from which she did not start. The uninstall will work, however, if the

Work item	Description
	user moves forward through the screens.

## Known limitations

When loading a data view which has multiple pages, the loading screen prints the JSON body of the call that is used to retrieve the pages of data.

When selecting a data view from the navigation table which does not have default start and end index values defined, the name of the previous data view persists on the page title even though the user navigated away from it.

## Requirements and setup

For more information on system requirements and installation, see [Power BI Connector setup](#).

### Distribution kit files

The installer is released as a self-extracting executable file that contains:

- ADHDataviews.pqz
- ADHDataviews\_LICENSE

## Upgrading Power BI Connector

To upgrade a previous installation of AVEVA Power BI Connector to the latest version, run the latest version of the installer on the host that has the previous version installed.

## Uninstalling Power BI Connector

Remove the product using **Uninstall a program** in the Windows Control Panel for both desktop and on-premise data gateway installations.

## Security information and guidance

### AVEVA's commitment

Because the PI System often serves as a barrier protecting control system networks and mission-critical infrastructure assets, AVEVA is committed to (1) delivering a high-quality product and (2) communicating clearly what security issues have been addressed. This release of CONNECT data services Power BI Connector is the highest quality and most secure version of the Power BI Connector released to date. AVEVA's commitment to improving the PI System is ongoing, and each future version should raise the quality and security bar even further.

## Vulnerability communication

The practice of publicly disclosing internally discovered vulnerabilities is consistent with the [Common Industrial Control System Vulnerability Disclosure Framework](#) developed by the [Industrial Control Systems Joint Working Group \(ICSJWG\)](#). Despite the increased risk posed by greater transparency, AVEVA is sharing this information to help you make an informed decision about when to upgrade to ensure your PI System has the best available protection.

For more information, refer to [Ethical Disclosure Policy](#) (<https://www.osisoft.com/terms-and-conditions/ethical-disclosure>).

To report a security vulnerability, refer to [Report a Security Vulnerability](#) (<https://www.osisoft.com/terms-and-conditions/report-security>).

## Vulnerability scoring

AVEVA has selected the [Common Vulnerability Scoring System \(CVSS\)](#) to quantify the severity of security vulnerabilities for disclosure. To calculate the CVSS scores, AVEVA uses the [National Vulnerability Database \(NVD\)](#) calculator maintained by the National Institute of Standards and Technology (NIST). AVEVA uses Critical, High, Medium, and Low categories to aggregate the CVSS Base scores. This removes some of the opinion related errors of CVSS scoring. As noted in the [CVSS specification](#), Base score range from 0 for the lowest severity to 10 for the highest severity.

# Security

The Security menu provides tools to manage access to CONNECT data services:

- Use Identity Providers to add third-party services that store and authenticate users.
- Use the Groups page to assign and manage roles for groups of users.
- Use the Users page to add, edit, or remove users.
- Use Roles to add roles, which manage access to assets, resources, and services, and assign these roles to identities, which include users, groups, and client-credentials clients.
- Use Clients to create and manage clients, which are used to authenticate against CONNECT data services from outside the portal.

## CONNECT data services groups

Groups allow you to assign and manage roles for groups of users.

You must create groups in the identity provider, CONNECT. Users are assigned to groups within CONNECT as well. After they are created in CONNECT, you can add groups within CONNECT data services and assign roles to them.

We recommend using groups to manage roles in CONNECT data services. Assigning roles on the individual user level is not recommended.

### Add a group in CONNECT data services

Groups allow you to assign and manage roles for groups of users.

#### Prerequisite

You must have the role of Tenant Administrator to add and manage groups.

#### Procedure

To add a group:

1. In the left pane, select **Security > Groups**.
2. In the toolbar, select **Add Group**.
3. Begin entering text in the **Name** field to search for an existing group and then select the group you want to add for access to assets, resources and services.

---

**Note:** The group must exist in CONNECT before adding it within CONNECT data services.

---

4. Specify the roles to assign to this new group.
5. Select **Add**.

## Video Tutorial: Provide groups in CONNECT with access to CONNECT data services

[https://player.vimeo.com/video/848733404?badge=0&autoplay=0&player\\_id=0&app\\_id=58479](https://player.vimeo.com/video/848733404?badge=0&autoplay=0&player_id=0&app_id=58479)

### [Video Transcript \(Select to expand\)](#)

This video shows you how to provide a group from AVEVA Connect with access to AVEVA Data Hub.

Open AVEVA Connect and select the Data Hub tile from the AVEVA Connect home page.

In AVEVA Data Hub, select Security, and then select Groups.

From the Groups page, select Add Group.

Begin to type the name of the group in the Name field and select it when it appears.

The Name field displays all available groups from AVEVA Connect.

Select the applicable roles to specify the permissions for the group.

By default, AVEVA Data Hub assigns the Tenant Member role to each group.

This role provides members of the group with read access to all resources in an ADH tenant.

Select Save to complete the process.

## Maintain a group in CONNECT data services

### Prerequisite

You must have the role of Tenant Administrator to add and manage groups.

## Manage group roles

To manage the roles for a group:

1. Select the group from the list.
2. Select **Manage Roles** in the **Roles** tab.
3. Select the roles you want to assign to the group.
4. Select **Save**.

## Remove a group

Removing a group does not remove it from the identity provider. Instead, the group no longer has any role mappings, cannot be given access to assets, resources and services, and will not be displayed in the list of groups on the Groups page.

To remove a group:

1. Select a group from the list.
2. Select **Remove Group**.
3. To confirm that you want to remove the group, select **Remove** in the message window or select **Cancel** to cancel the request.

## CONNECT data services users

A user in CONNECT data services is an identity that has access to a tenant. Roles assigned to a user determine what permissions the user has on resources. See [CONNECT data services roles](#) for more information. Users log in to the CONNECT data services portal and are authenticated through CONNECT.

We recommend using groups to manage roles in CONNECT data services. Assigning roles on the individual user level is not recommended.

---

**Note:** Identity resources such as users and clients, are global across CONNECT data services. These resources are not scoped to a particular namespace, but globally scoped across namespaces in CONNECT data services.

Users log in to the CONNECT data services portal through a user account in CONNECT, and users authenticate to custom web applications when using hybrid clients and authorization code clients. Therefore, at least one user should already be added to a tenant when the portal is first accessed.

Some points to note about adding and managing users:

1. Users are added and granted access to CONNECT data services in CONNECT.
2. Make sure the user has been assigned the Data services Viewer role in CONNECT before sending the invitation to access CONNECT data services. See [Add users in CONNECT](#). In CONNECT data services, you can map a user or group to a CONNECT data services role to control what actions they can take.

---

**Note:** The CONNECT data services Tenant Member role grants read access to everything in the tenant. If a user should not have read access to some resources, the Tenant Member role can be limited.

3. Any CONNECT user who is assigned to the Administrator role is automatically assigned the Tenant Administrator role in CONNECT data services.

4. Additional CONNECT users can be granted access to an associated CONNECT data services tenant using one of the following methods:
  - a. Search for the user in CONNECT data services and then add the user and assign roles.
  - b. Add a CONNECT group to the CONNECT data services tenant, then add that group to CONNECT data services and assign the necessary CONNECT data services roles. Any user that belongs to the CONNECT group is automatically granted access to the CONNECT data services tenant with the associated set of CONNECT data services roles.

---

**Note:** You must belong to the Tenant Administrator role to add and manage users in a tenant.

---

## PI Server counterpart

A user is comparable to a mapping in Data Archive. For example, in Data Archive a mapping may be added from a Microsoft Windows account to a specified PI identity. The user enters their Windows credentials to authenticate against Data Archive and gets the permissions specified by the PI identity. CONNECT handles authentication for CONNECT data services, and users get their permissions from the roles that are assigned to them.

## Add a user in CONNECT data services

A user is an identity that has access to a tenant. Roles assigned to a user determine what permissions the user has on resources.

### Prerequisite

You must have the role of Tenant Administrator to add and manage users.

### Procedure

To add a user to a tenant:

1. In the left pane, select **Security > Users**.
2. In the toolbar, select **Add User**.
3. In the **Contact First Name** and **Contact Last Name** fields, enter a first and last name for the user.
4. In the **User Email** field, enter the first few characters of the user's contact email and then select the correct email address from the dropdown list.

---

**Note:** The user must exist in CONNECT before being added within CONNECT data services.

---

5. (Optional) On the **Tenant Roles** tab, assign additional roles to the user. By default, the user is assigned the Tenant Member role which cannot be removed. Roles can be modified after the user is added.
6. Select **Add**.

A welcome email is sent to the email address specified in the **Contact Email** field.

## Maintain a user in CONNECT data services

### Prerequisite

You must have the role of Tenant Administrator to add and manage users.

### Edit a user

To edit an existing user:

1. In the left pane, select **Security > Users**.
2. Select an existing user.
3. Select **Edit User**.
4. Make changes to the user information fields or roles.
  - For advanced integration identity providers, you will only be able to edit the roles assigned to the user.
  - For other identity providers, you can edit the **Contact First Name**, **Contact Last Name**, **Contact Email**, and assigned roles.
5. Select **Save**.

### Resend a user invitation

To resend an expired user invitation:

1. In the left pane, select **Security > Users**.
2. Select an existing user.
3. Select **Resend Invitation**.

### Remove a user

To remove an existing user:

1. In the left pane, select **Security > Users**.
2. Select an existing user.
3. Select **Remove User**.
4. Select **Remove** to confirm.

## CONNECT data services roles

Administrators use roles to manage access to assets, resources, and services. They can then assign these roles to identities, which include users, groups, and client-credentials clients. When an identity tries to access a resource, CONNECT data services checks the assigned roles against the permissions on the resource to determine their access level.

Roles defined in CONNECT data services are unique and separate from roles defined in CONNECT and CONNECT visualization.

There are six built-in CONNECT data services roles that cannot be removed from a tenant:

- Tenant Administrator – Administrator with full permissions by default. This is the highest privilege role, with the ability to create new and remove existing users, clients and secrets.  
**Note:** It is strongly recommended you do not assign the Tenant Administrator role to client-credential clients. This role can be assigned via the Tenant Management API.
- Community Administrator – A role with full administrative rights. These rights include all the privileges of a Community Moderator plus the ability to delete a community, invite and confirm tenant invitations, and remove tenants from the community. See [Community roles](#) for more information.
- Tenant Contributor – This role has read and write permissions by default.
- Tenant Data Steward – This role has no specific permissions by default.
- Tenant Viewer – This role has no specific permissions by default.
- Tenant Member – This role cannot be removed and is assigned to all users or clients. Tenant members are granted read access by default.

You can add custom roles to further control access. By default, custom roles do not have any specific permissions. You must have the Tenant Administrator role to add and manage roles for a tenant.

Access to resources is a combination of 1) the roles assigned to a user and group, and 2) the permissions set on the resources. For any resource, you set access on the resource for specific roles, rather than on specific users or clients. Access is managed for resources in the Manage Permissions dialog box.

## PI Server counterpart

Roles are comparable to PI identities in Data Archive or identities in PI AF server. An administrator grants permissions to roles instead of directly to individual users or clients. This is similar to how PI Server uses identities to assign permissions for a set of users or clients.

## Roles best practices

Consider the following best practices when you create and assign roles:

- Consider whether the read access granted by the Tenant Member role is acceptable for all users and clients in your tenant. Specifically, if you plan to invite users from outside your organization, you may want to limit their read access. One way to do this is to create a custom role for external users so that their permissions can be explicitly managed.
- When using PI to CONNECT, ensure write access to stream and asset collections. The PI to CONNECT Agent has write permission to the streams collection in CONNECT data services. By default, the Tenant Contributor role provides write permission to the automatically generated PI to CONNECT Agent Client User. Write permission to this collection is required to enable stream creation.
- Use caution when granting the Tenant Administrator role. Make sure to assign a different role to users and clients who should not manage permissions. Avoid assigning the Tenant Administrator role to client-credentials clients.
- Ensure that the roles assigned to client-credentials clients only grant the minimum set of permissions

required by the application that uses these clients. This minimizes the potential damage in the event a client secret is compromised or a problem arises with the application.

- Use caution when denying permissions because this supersedes any allowed access to a role. For example, if a user is allowed write access through one role but is denied write access through another role, the user will not have write access. Because all users and clients are assigned the Tenant Member role, you cannot deny permissions to the Tenant Member role. Doing so would deny the given permission to every user in the tenant.

## Add a role in CONNECT data services

Roles are used to manage access to assets, resources, and services. By default, a new role does not have any access granted or denied.

### Prerequisite

You must have the role of Tenant Administrator to add and manage roles.

### Procedure

To create a role:

1. In the left pane, select **Security > Roles**.
2. In the toolbar, select **Add Role**.
3. Enter a **Name** for the role and, optionally, a **Description**.
4. Select **Add** to create the new role.

---

**Note:** The Role Type is Tenant Custom for all custom (or non-default) roles.

---

You can now specify permissions for this role when managing permissions on assets, resources, and services. For more information, see [Manage permissions for user roles in CONNECT data services](#).

## Maintain a role in CONNECT data services

### Prerequisite

You must have the role of Tenant Administrator to add and manage roles.

### Manage identities for a role

To manage the identities to which a role is assigned:

1. In the left pane, select **Security > Roles**.
2. Select an existing role.
3. Select **Manage Identities**.
4. A list of assigned identities is shown. Select **X** to the right of an identity to remove the role from it.

5. To add an identity, select **Add Identity**, enter a partial name or email to filter by if needed, and select **+** to the right of an identity in the list to add the role to it.
6. Select **Save**.

## Edit a role

To edit an existing custom role:

1. In the left pane, select **Security > Roles**.
2. Select an existing role.  
**Note:** Built-in roles cannot be edited.
3. Select **Edit Role**.
4. Make changes to the **Name** or **Description**.
5. Select **Save**.

## Remove a role

To remove an existing custom role:

1. In the left pane, select **Security > Roles**.
2. Select an existing role.  
**Note:** Built-in roles cannot be removed.
3. Select **Remove Role**.
4. Select **Remove** to confirm.

## Manage permissions for user roles in CONNECT data services

You can edit the permissions applied to a user role from any page in CONNECT data services. You can apply different permissions to different user roles for each namespace. To manage permissions for user roles:

1. From the **Namespace** dropdown list, select the namespace that you want to edit permissions for.
2. Select the **Manage Settings**  icon.



The **Manage Permissions** tab of the Namespace Settings window opens.

3. Use this window to:
  - Add user roles that have permissions in the namespace.
  - Edit permissions for each user role.  
For more information, see [Permissions management](#).
4. When you are finished editing permissions, select **Save**.

---

**Note:** This action overwrites any previous permission settings applied to the affected user roles.

---

## CONNECT data services clients

Clients allow applications to authenticate against CONNECT data services from outside the portal. The following types of clients are supported, and each supports different types of applications:

- Client-credential clients
- Authorization code clients
- Hybrid clients

You must have the Tenant Administrator role to add and manage clients in a tenant.

### Client-credentials clients

Use client-credentials clients for server-to-server communication that does not require user interaction. The client typically authenticates with the token endpoint using its client ID and secret. A secret is a unique key generated for each client to connect to assets, resources, and services for a time-limited period. Because secrets allow access to data, you need to keep them secure.

### Client-credentials client PI Server counterpart

Client-credentials clients are very similar to Microsoft Windows service accounts that applications can use to authenticate against Data Archive or PI AF server.

### Client-credentials client best practices

We recommend the following best practices with a client credentials client:

- Create a separate client-credentials client for each device or instance of an application that connects to CONNECT data services. This ensures that secrets can be discretely managed for individual applications and that you know which applications are connecting to CONNECT data services.
- Ensure that client secrets are stored securely where they are used.
- Use secrets that expire and rotate them on a schedule. When it is time to switch to a new secret, we recommend that you create the new secret, redirect the application to use the new secret, and only delete the old secret from the client when it is no longer being used.

### Authorization code clients

Authorization code clients are used with customer web applications that use CONNECT data services as their backend. They provide a secure means of authenticating users of the website to view assets. The authorization code client is paired with a client ID. The web application that is using the client to authenticate users must include the client ID in its code.

Authorization code clients are used to authenticate using any supported browser. Upon successful authentication, an authorization code is provided to the client. This authorization code is exchanged for an

access token using PKCE (Proof of Key Code Exchange) which is a more secure authentication flow. No refresh token is provided.

## Authorization code client PI Server counterpart

Authorization code clients have no direct PI Server equivalent, but they are similar to the combined behavior of a trust and mappings in Data Archive. These clients are similar to trusts because they only allow users to access the portal if the application that uses them meets certain criteria, for example, the application must be served at a specific URL. However, like a mapping, authorization code clients require the user to authenticate as a known user account within the tenant.

## Authorization code client best practices

We recommend the following best practices for an authorization code client:

- Use authorization code clients in web applications or with services where users must be authenticated and it is not possible to store a client secret securely.
- Because refresh tokens are not generated in this flow, web applications should use an iframe to request a new token before the existing token expires. Otherwise, the user will have to explicitly log in again to get a new token once their token expires.

## Hybrid clients

Use hybrid clients for native and server-side web applications. This client utilizes the user credentials to authenticate with the identity provider. Once the user is authenticated, then the server-side client steps in and server-to-server communication commences. Authentication can be performed using any browser. The server-side code retrieves an access token and a refresh token can also be provided.

## Hybrid client PI Server counterpart

Hybrid clients have no direct PI Server equivalent, but they are similar to the combined behavior of a trust and mappings in Data Archive. These clients are similar to trusts because they only allow users to access the portal if the application that uses them meets certain criteria, for example, the application must be served at a specific URL. However, like a mapping, hybrid clients require the user to authenticate as a known user account within the tenant.

## Hybrid client best practices

We recommend the following best practices for a hybrid client:

- Use hybrid clients in web applications or services where users authenticate against CONNECT data services through a supported browser, but a secure backend that stores the secrets performs the actual authentication.
- Use caution when deciding whether to allow refresh tokens for your hybrid client. Where possible, it is a more secure practice to use an iframe to request a new token before the old token expires rather than use a refresh token.

## Add a client-credentials client

Client-credentials clients are used for server-to-server communication where no user interaction is required.

### Prerequisite

You must have the role of Tenant Administrator to add and manage clients.

### Procedure

To add a client-credentials client:

1. In the left pane, select **Security > Clients**.
2. In the **Client Type** dropdown list, select **Client-Credentials Client**. This option is displayed by default.
3. In the toolbar, select **Add Client**.  
The Add Client pane opens.
4. In the **Name** field, enter a name to identify the device or application that will use this client.
5. (Optional) In the **Token Lifetime** field, enter the length of time in seconds that the access token functions before it expires.  
The default, 3600 seconds (one hour), is the maximum length of time. The minimum value is 60 seconds.
6. In the **Tenant Roles** and **Community Roles** tabs, select the roles that are appropriate for the client.  
By default, the client has the Tenant Member role which cannot be removed. Roles can be modified after the client is created.
7. Select **Next**.  
The Create Secret pane opens.
8. (Optional) In the **Description** field, enter a description for the client secret.
9. In the **Expiration Date** field, enter a date and time that the secret expires.  
Ensure that the expiration date is valid for the secret. By default, the secret is set to expire one year after creation. Select the **Never Expires** checkbox to specify that the secret does not expire. Secrets can be deleted later, including secrets that are set to never expire.
10. Select **Save**.  
The Client Successfully Created window opens and displays the **Client Id** and **Client Secret**.

---

**Important:** Select **Copy**  to the right of each field and store the client secret and client Id in a secure place. You need this information to connect your applications. Once the window is closed, the client secret cannot be accessed or retrieved.

---
11. Select **Close**.

---

**Note:** In the list of secrets, the **Client Id** is still visible. If you did not save the client secret, see [Maintain a client](#) for instructions on adding a new secret.

---

## Add a hybrid client

Hybrid clients are used by native and server-side web applications. Authentication can be performed using any browser. The server-side code retrieves an access token and a refresh token can also be provided.

### Prerequisite

You must have the role of Tenant Administrator to add and manage clients.

### Procedure

To add a hybrid client:

1. In the left pane, select **Security > Clients**.
  2. In the **Client Type** dropdown list, select **Hybrid Clients**.
  3. In the toolbar, select **Add Client**.  
The Add Client pane appears.
  4. In the **Name** field, enter a name to identify the application that will use this client.
  5. (Optional) Select the **Allow Refresh Token** checkbox if the application uses refresh tokens to keep users logged in to the portal.
  6. In the **Allowed Redirect URL(s)** field, enter a URL and select **+** to add it to the list.  
The application specifies one of the URLs in this list during authentication, and the CONNECT data services identity server returns the results of the authentication to this URL.
  7. (Optional) In the **Allowed Logout Redirect URL(s)** field, enter a URL and select **+** to add it to the list.  
The application specifies a URL from this list when it logs out, and the CONNECT data services identity server sends the user to this URL after a successful logout.
  8. (Optional) In the **Token Lifetime** field, enter the length of time in seconds that the access token functions before it expires.  
The default, 3600 seconds (one hour), is the maximum length of time. The minimum value is 60 seconds.
  9. Select **Next**.  
The Create Secret pane opens.
  10. (Optional) In the **Description** field, enter a description for the client secret.
  11. In the **Expiration Date** field, enter a date and time that the secret expires.  
Ensure that the expiration date is valid for the secret. By default, the secret is set to expire one year after creation. Select the **Never Expires** checkbox to specify that the secret does not expire. Secrets can be deleted later, including secrets that are set to never expire.
  12. Select **Save**.  
The Client Successfully Created window opens and displays the **Client Id** and **Client Secret**.
- 
- Important:** Select **Copy**  to the right of each field and store the client secret and client Id in a secure place. You need this information to connect your applications. Once the window is closed, the client secret cannot be accessed or retrieved.
- 
13. Select **Close**.

---

**Note:** In the list of secrets, the **Client Id** is still visible. If you did not save the client secret, see [Maintain a client](#) for instructions on adding a new secret.

---

## Add an authorization code client

Authorization code clients provide a secure means of authenticating users to customer web applications that use CONNECT data services as their backend.

### Prerequisite

You must have the role of Tenant Administrator to add and manage clients.

### Procedure

To add an authorization code client:

1. In the left pane, select **Security > Clients**.
2. In the **Client Type** dropdown list, select **Authorization Code Clients**.
3. In the toolbar, select **Add Client**.

The Add Client pane appears.

4. In the **Name** field, enter a name to identify the device or application that will use this client.
5. In the **Allowed Redirect URL(s)** field, enter a URL and select **+** to add it to the list.

The application specifies one of the URLs in this list when it authenticates against CONNECT data services, and the CONNECT data services identity server returns the results of the authentication to this URL.

6. (Optional) In the **Allowed Logout Redirect URL(s)** field, enter a URL and select **+** to add it to the list.
7. (Optional) In the **Allowed CORS Origin(s)** field, enter a URL and select **+** to add it to the list.

Designate other URLs from which the application is allowed to make requests against CONNECT data services. For example, this may be necessary if the user authenticates from an application running at one URL but the result of the authentication is sent to an application running at a different URL.

8. (Optional) In the **Token Lifetime** field, enter the length of time in seconds that the access token functions before it expires.

The default, 3600 seconds (one hour), is the maximum length of time. The minimum value is 60 seconds.

9. Select **Save**.

The Client Successfully Created window displays the client Id for the client. The application must specify this client Id when it makes an authentication request. To copy the client Id, select **Copy** . After you close this window, you can also retrieve the client Id from the list of clients.

## Maintain a client

### Prerequisite

You must have the role of Tenant Administrator to add and manage clients.

### Edit a client

To edit an existing client:

1. In the left pane, select **Security > Clients**.
2. In the **Client Type** dropdown list, select the appropriate client type.
3. Select an existing client.
4. In the Details pane, select **Edit Client** .
5. Make any desired changes to the client configuration.
6. Select **Save**.

### Disable/enable a client

To disable a client without removing it:

1. In the left pane, select **Security > Clients**.
2. In the Client Type dropdown list, select the appropriate client type.
3. Select an existing client.
4. In the Details pane, next to Status, select **Disable Client** .
5. Select **Disable** to confirm.
6. To reenable the client, in the Details pane, next to Status, select **Enable Client** .
7. Select **Enable** to confirm.

### Remove a client

To remove an existing client:

1. In the left pane, select **Security > Clients**.
2. In the **Client Type** dropdown list, select the appropriate client type.
3. Select an existing client.
4. In the Details pane, select **More Options**  > **Remove Client**.
5. Select **Remove** to confirm.

## Create a new secret

To create a new secret for an existing Client-Credentials or Hybrid client:

1. In the left pane, select **Security > Clients**.
2. In the **Client Type** dropdown list, select the appropriate client type.
3. Select the client in the list.
4. In the Details pane, select the **Secrets** tab.
5. Select **Add Secret**.
6. (Optional) In the **Description** field, enter a description for the client secret.
7. In the **Expiration Date** field, enter a date and time that the secret expires.  
Ensure that the expiration date is valid for the secret. By default, the secret is set to expire one year after creation. Select the **Never Expires** checkbox to specify that the secret does not expire. Secrets can be deleted later, including secrets that are set to never expire.
8. Select **Add**.

## Edit secret details

To edit secret details for a client:

1. In the left pane, select **Security > Clients**.
2. In the **Client Type** dropdown list, select the appropriate client type.
3. Select the client in the list.
4. In the Details pane, select the **Secrets** tab.
5. Select an existing secret and select **Edit Secret**.
6. Make any changes and select **Save**.

## Remove a secret

To remove a secret from a client:

1. In the left pane, select **Security > Clients**.
2. In the **Client Type** dropdown list, select the appropriate client type.
3. Select the client in the list.
4. In the Details pane, select the **Secrets** tab.
5. Select an existing secret and select **Remove Secret**.
6. Select **Remove** to confirm.

# Developer tools

The Developer Tools menu provides helpful tools and information for developers:

- Code Samples illustrates several ways for applications to interact with the CONNECT data services REST API.
- The API Console provides a graphical interface for using the REST API.
- The GraphQL Console provides a graphical interface for using the GraphQL API.
- Use the OMF Editor to build and validate Open Message Format (OMF) messages to send to the Sequential Data Store.

For developer documentation, read the [Developer guide](#).

## Code samples

The [CONNECT data services-Samples](#) illustrate several ways for applications to interact with the CONNECT data services REST API.

The examples cover the basics of interacting with CONNECT data services, such as:

- Connecting to CONNECT data services
- Creating SdsTypes and instances of SdsStreams
- Sending data to and retrieving data from SdsStreams
- Performing queries against SdsStreams
- Removing SdsStreams and SdsTypes

Currently, the samples are available in these languages:

- .NET
- Java
- Python
- Node.js
- Angular

Because the examples are intended for demonstration purposes, they represent some example practices. The patterns may change as CONNECT data services continues to develop. Be sure to follow the [OSI-Samples-ADH](#) repository on GitHub for updates.

## API console

The API Console provides a graphical interface for using the CONNECT data services REST API. Developers can use this console to configure and test API requests before implementing them in their own applications. To use the API Console, select **Developer Tools > API Console** from the left pane.

## Request area

Use the request area to configure an API request. Choose a version of the API, the request scope, the request verb, and the URI endpoint. This area is also used to configure the request header, body, and parameters.

The screenshot shows the AVEVA API Request area. At the top, there's a dropdown for 'v1' and a blue 'Home' icon. Below that, the 'Full Path (readonly)' field contains the URL: 'uswe.datahub.connect.aveva.com/api/v1/Tenants/{TENANT\_ID}/Namespaces'. Underneath, the 'Verb' dropdown is set to 'GET' and the 'URI' field shows '/Namespaces/123-456-789/DataViews/JN%20Test%20%23%20Data%20View/Data/'. To the right of the URI is a star icon. Below these fields are two tabs: 'Headers' and 'Parameters', with 'Parameters' being the active tab. Under 'Parameters', there are several input fields: 'startIndex' with value '2024-04-26T04:00:00:000Z', 'endIndex' with value '2024-05-26T04:00:00:000Z', 'count' (empty), 'interval' with value '00:01:00:00', and 'continuationToken' (empty). On the far right of the parameter list is a small edit icon. At the bottom right of the request area are two buttons: 'Copy Request URI' and a blue 'GET' button with a right-pointing arrow.

## API version

Select a version from the dropdown list. For more information on the available versions, see [CONNECT data services API versioning](#).

## Tenant path

Select the Root/Tenant path enabled icon to toggle between a tenant-scoped path or a root-scoped path. The Full Path field (which is readonly) updates according to your selection.

The **Full Path** field shows an encrypted version of the selections you have made. Based on your selections, other fields may also be automatically prepended to the path. Together, these fields produce a path to a REST endpoint.

## Verb

Use the **Verb** dropdown to select a request method. By default the API Console selects the GET method for new request. You can use a variety of other methods to send data to your APIs, including:

- GET: Retrieves data.
- POST: Adds new data.
- PUT: Replaces existing data.
- DELETE: Deletes existing data.

- PATCH: Updates existing data.

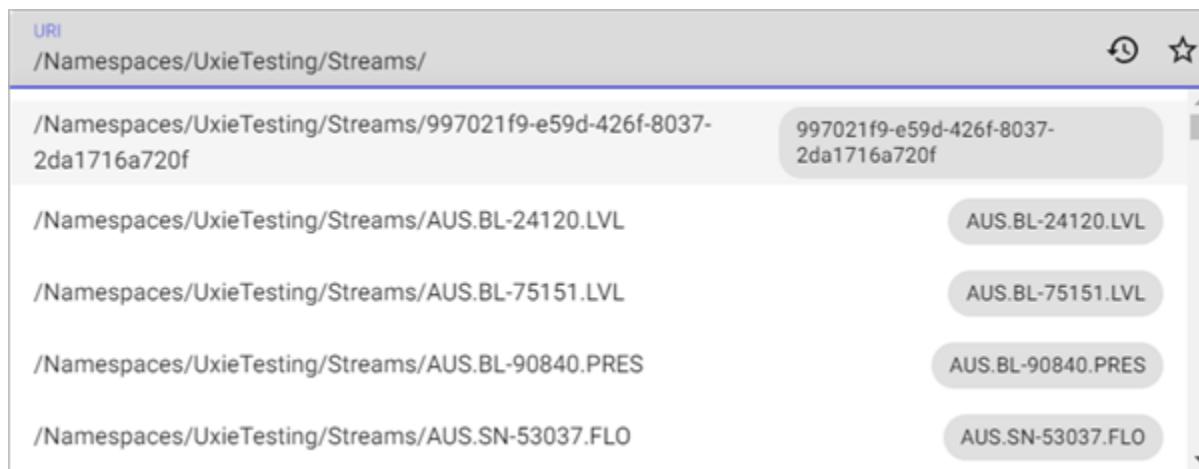
## URI

Use the **URI** field to enter an API route to make a request against. If your request is tenant-scoped, you can type a forward slash (/) in the field to display a dropdown list of path autocomplete options. If you select a root-scoped path, a different dropdown list gives you other categories of data.

For a complete reference of URI endpoints available in the CONNECT data services API, refer to the [CONNECT data services API reference](#).

## Path autocomplete

When entering a URI for an API request, the API console automatically suggests available identifiers for path completion. Additionally, a tag next to the identifier displays the resource name that it resolves to. Resources are listed in alphabetical order.



## Session request history

Select the Session request history icon to view a list of previous requests made from the API console.

## Favorites

Select the Favorites icon to add the configured API request to the Favorites list in the right pane. Use this feature when you find yourself making an API request repeatedly.

## Headers

Use the **Headers** tab to provide more metadata about the operation you are performing. Enter any key-value pairs you need to include in your request.

Calls to the API from other sources do not include Accept-Verbosity as a standard. The Accept-Verbosity heading needs to be specified. If you do not include the the Accept-Verbosity heading, all calls except for data view calls will be non-verbose and dataview calls will be verbose.

When set to non-verbose, properties with null values are omitted from the response to reduce bandwidth. This behavior is only applicable to the JSON format, as all other formats represent a table which cannot have omitted values. Verbose has no impact on writes; writes return only error messages.

The default response format for SDS is JSON. Default JSON responses do not include any values that are equal to the default value for their type. Note that the Accept-Verbosity header for SDS differs as its default is set to non-verbose. Verbose has no impact on writes; writes return only error messages.

## Request body

When making POST, PUT, or PATCH requests, you can enter your JSON payload in the **Body** area.

## Parameters

When making GET requests, you can specify parameters available for the route on the **Parameters** tab. The parameter fields available will change based on the route configured in the URL field. Query parameters are appended to the end of the request URI. For more information on the parameters available for each route, refer to the [CONNECT data services API reference](#).

## Continuation token

The continuation token field is used in support of server-side pagination. A continuation token is a mechanism used to handle large amounts of data efficiently. When you request data from a data view using the CONNECT data services REST API, there might be too many results to retrieve all at once. To address this, the API provides you with a subset of the data and a continuation token.

The continuation token parameter is available when working with streams or data views. When working with streams, select the checkbox to include the parameter in your request when no value is set.

The continuation token serves as a marker or reference point that helps you keep track of your progress and indicates where you left off. When you want to fetch the next portion of the data, you include the continuation token in your subsequent API request. Continuation tokens are only supported for GET requests.

When the **Load from Response**  button is enabled, the continuation token from the last API console data view request is loaded into the `continuationToken` field automatically. The continuation token will be loaded from the response when all of the following conditions are met:

- The request verb is GET.
- There is a response present.
- The current response verb, path, and query parameters (excluding the `continuationToken`) all match the current request.

## Copy request URI

This button copies the request URI to your clipboard.

## Execute request

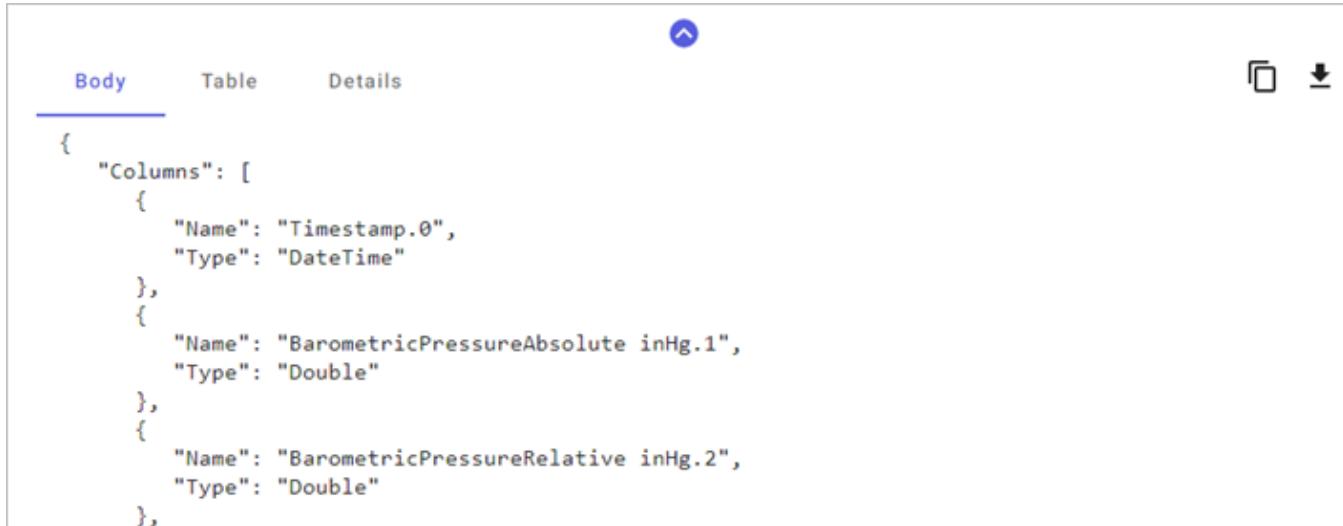
When you are done configuring your API request and are ready to make your call, select the **Execute request**

button. The label on the button changes according the method that you selected.

**Warning:** Making a POST, PUT, DELETE, or PATCH request will alter your data. Use these methods with care.

## Response area

Use the response area to view the API response to your previous request. This area includes metadata about the request, along with the response payload.



```
{  
  "Columns": [  
    {  
      "Name": "Timestamp.0",  
      "Type": "DateTime"  
    },  
    {  
      "Name": "BarometricPressureAbsolute inHg.1",  
      "Type": "Double"  
    },  
    {  
      "Name": "BarometricPressureRelative inHg.2",  
      "Type": "Double"  
    }  
  ]  
}
```

### Body

The **Body** tab displays the JSON payload returned by the API following a request.

### Table

The **Table** tab displays the JSON response body in tabular form.

### CSV

For routes that support responses in CSV format, such as Data Views, a CSV tab is available. This tab displays the response body as CSV.

### Parquet

When making requests to the Data view data API route, responses are available in the Parquet format. For more information, see [Parquet data format](#).

### Trend

Some routes include a **Trend** tab that you can use to visualize data.

## Details

The **Details** tab lists metadata related to the previous API request, including:

- **URI Path:** This field displays the method and URI used in the previous API request. Select **Copy**  to copy the URI to your clipboard.
- **HTTP status:** The server issues HTTP response status codes when a client makes a request over HTTP. In response to the requests made to CONNECT data services, the system returns a status code. For more information about the possible status codes, see [HTTP status codes](#).
- **Link:** For GET requests that include a [continuation token](#), one or more link header is included in support of pagination. Each header is a clickable link that updates the request metadata.

## Toolbar icons

While making requests using the API console, you can copy or download the response body by choosing the appropriate icon.

- Choose **Copy**  to copy the response body to your clipboard.
- Choose **Download**  to download the response body.

When working with Data Views resources, response bodies are downloaded in the file format specified in the **form** dropdown. Response bodies for other resources are downloaded as JSON.

## GraphQL console

The GraphQL console provides a graphical interface for creating queries for the GraphQL API. The GraphQL API returns event data and associated reference data stored in CONNECT data services.

You can run a query within the console, or use it to create a query that can be used by an external application.

To use the GraphQL console:

1. In the left pane, select **Developer Tools > GraphQL Console**.  
The GraphQL Explorer pane populates with your organization's schema.
2. Select the **Query** tab in the GraphQL Explorer pane to compose a data retrieval request, or the **Mutation** tab to upsert or delete data.
3. Select  next to an object in the GraphQL Explorer to drill down and show the available filtering options and fields.
4. Use the GraphQL Explorer tree to create a request.
  - Use the selections under the **where**: argument to filter by fields that equal, contain, start with, or end with a specified value, or are included in an array of values.
  - Use the selections under the **options**: argument to retrieve a specified count of objects or to sort the data returned. If you select multiple sort fields, the order in which you select them determines the sort order.
  - For fields that can be arrays, when an item is selected or entered, a new blank item appears below it to

allow for additional values.

- For upsert or delete operations, use the selections under **input**: to identify the object to update or delete.
- Select the fields to include in the response.
- Select **Reset** to clear all selections.
- Select  in the Request or Variables pane to copy the contents of that pane to the clipboard.
- Select  to hide or show the GraphQL Explorer pane.
- Select  to hide or show the Response pane.

---

**Note:** The GraphQL Explorer and Request panes work in both directions. The request updates as you make selections in the GraphQL Explorer tree, and editing the text directly in the request or pasting a complete request updates the GraphQL Explorer tree. When editing the request directly, select  to automatically format the request.

---

5. Select  to return to the top level and repeat the process with other objects, as needed.
6. When your query is complete, select **Send Request** to run the query.

The results of your query appear in the Response pane.

- When you request a certain amount of fields, such as `count: 1`, and there are more fields available to display, a continuation token appears in the response. Select **Resend with Continuation** to view the next item.
- Select  in the Response pane to copy the response to the clipboard.
- Select  to download the JSON file.
- Select  to show the session request history, then select any of the displayed requests to reload it into the Request pane.

## Variables

Rather than entering specific values for your query, you can use variables.

1. Select the  icon that appears next to an argument when you hover over it.
2. Enter a variable name in the box that appears.

A variable declaration is added to the Request pane and the new variable is added to the Variables pane in JSON format. The variable is assigned a value of `null` by default.

3. Edit the value in the Variables pane to assign a value to the variable.

You can also make an array a variable and include multiple values, such as `[98, 99, ...]`.

If you manually edit the variable name within the Request pane, select to automatically update the variable name in the header and Variables pane.

## Fragments

GraphQL supports reusable units called fragments. With fragments you construct sets of fields once, and then reuse them in multiple locations in a query.

1. In the Request pane, add the fragment text above or below the query. The location does not matter.

For example:

```
fragment AlarmFields on Alarm {  
    id  
    eventStartTime  
    eventState  
    severity  
}
```

2. Within the query, place instances of the fragment in the format ...[fragment name].

Fragments appear only in the Request pane and are not reflected in the GraphQL Explorer. They persist when you make changes in the GraphQL Explorer.

## OMF editor

The Open Message Format (OMF) defines a set of message headers and message bodies. You write messages in JSON format that generate compliant messages for data ingress. The OMF specification is generic in that it does not specify a particular back-end system. You can use OMF to create types, create streams, and populate streams with data. There are three message formats you can use to accomplish these tasks: type messages, container messages, and data messages.

Use the OMF Editor to build and validate OMF messages to send to the Sequential Data Store.

To build a message using the OMF Editor:

1. Select **Developer Tools > OMF Editor** from the left pane.
2. Choose the message type from the **OMF Type** selector: **Type, Container or Data**.
3. Select the OMF version from the **OMF Version** selector.
4. Edit your message and use the following options:
  - Select **Copy OMF** to copy the message content to the clipboard.
  - Select **More Options** : > **Format OMF** to reset template content alignment after making changes.
  - Select **More Options** : > **Download OMF** to download the message content to your local drive.
  - Select **More Options** : > **Reset Template** to delete any changes you have made to the message content.

As you edit a message, the editor indicates whether it is valid in the upper right and displays any errors in the Errors pane.

# Support

The Support menu provides access to documentation, logs, support links, the service blog, and other useful information:

- Documentation provides a link to this documentation.
- Logs provides troubleshooting information, including messages about tenant-related activity, errors, and system messages.
- Contact Support provides a link to contact software support.
- Service Blog displays bulletins, announcements and reported system-wide issues.
- Supported Browsers provides a current list of supported web browsers.
- Cookie Settings allows you to change whether you allow the portal to use cookies.

## Downloads

The Downloads page provides a location to download locally-installed agents and connectors that work with CONNECT data services.

- Select **Download** on a tile to download the agent or connector installation file.
- Select **More Info** on a tile to open the documentation for that product.

## Logs

The CONNECT data services logs contain troubleshooting information, including messages about tenant-related activity, errors, and system messages. By default, logs report on activities that occurred within the past month. Logs are purged after 90 days.

To download a tenant log in a .csv file:

1. In the left pane, select **Support > Logs**.
2. (Optional) To view logs by namespace, select the **Namespace** option.
3. (Optional) To filter logs, complete the following fields, and then select **Apply Filters**:
  - **Start** – Enter the start date and time of messages to include.
  - **End** – Enter the end date and time of messages to include.
  - **Severity** – Select the severity of messages to include.
  - **Source** – Select the sources of messages to include.
4. To download the logs, select **Download Logs**.

The .csv log file is downloaded to your computer.

## Service Blog

The Service Blog page displays bulletins, announcements and reported system-wide issues. The last ten entries are displayed by default. To view additional entries, select the arrows to navigate through pages, or enter a page number to jump directly to that page.

## How CONNECT data services charges flex credits

This document outlines the key concepts and processes behind what usage CONNECT data services reports and how that creates Flex Credit charges.

### Usage reporting

There are many forms of usage in CONNECT data services: visualizing values of data streams, viewing the definition of an asset, determining who has access to a data view, and so on. CONNECT data services only reports three types of usage to CONNECT:

- **Data storage in your CONNECT data services tenant's namespaces (*streams stored*)**

CONNECT data services reports the number of data streams stored in a day, labelled *streams stored*, to CONNECT. This number is the count of CONNECT data services streams that exist for each namespace at the end of the day, 12:00 AM UTC.

- **Access of data from your CONNECT data services tenant's namespaces (*streams accessed*)**

CONNECT data services reports daily usage to CONNECT for the number of unique data streams accessed within a day for each namespace, ending 12:00 AM UTC. The number of unique data streams accessed in a day, labelled *streams accessed*, increases by one when an authorized user or client accesses a data stream's data for the first time. Subsequent accesses to this same data stream within the same day by any authorized user or client do not further contribute to an increase in *streams accessed*. For example, if two separate users access the same data stream in the same day, only a single data stream counts toward *streams accessed* usage.

- **Access of data from a community your CONNECT data services tenant is a member of (*shared streams accessed*)**

CONNECT data services reports daily usage to CONNECT for the number of unique shared data streams accessed in each community of which a tenant is a member. The number of unique shared data streams accessed in a day, labelled *shared streams accessed*, increases by one when an authorized user or client accesses a shared data stream's data for the first time. Subsequent accesses to this same shared data stream within the same day by any authorized user or client do not further contribute to an increase in *shared streams accessed*. Shared streams can include a data stream that you shared into a community from a namespace in your CONNECT data services tenant, or a data stream shared by another CONNECT data services tenant into a community to which your CONNECT data services tenant has access.

Authorized users and clients from other CONNECT data services tenants who you have granted access to your data streams, via a community, can access your data streams without contributing towards your *shared streams accessed* count. In other words, each CONNECT data services tenant that consumes data from one or more communities will only contribute to their own *shared streams accessed* count.

CONNECT data services reports usage to CONNECT daily per namespace for *streams accessed* and *streams*

*stored*, and daily per community for *shared streams accessed*. The usage values for *streams accessed* and *shared streams accessed* are also reported daily under a fourth usage metric called *total streams accessed*. Therefore, each usage value reported to CONNECT, either for *streams accessed* or *shared streams accessed*, has an equivalent usage value reported for *total streams accessed*. CONNECT data services rate plans that are purely consumption based (based only on the data you access) utilize this *total streams accessed* usage metric to determine Flex Credit transaction charges.

## Flex credit transactions

Flex credits are units of virtual currency used to pay for consumption within CONNECT data services (or other CONNECT applications). You can commit to an amount of flex credits for cloud offerings and spend them how you like across a portfolio of cloud offerings, allowing you the flexibility to adjust mid-contract how you spend those flex credits based on how your usage evolves.

Depending on the CONNECT data services rate plan to which your tenant is subscribed, flex credits are debited from your account in one of two ways:

- The daily usage in your tenant for *streams stored*, *streams accessed*, and *shared streams accessed*.  
This type of rate plan creates a Flex Credit transaction for each *streams stored* and *streams accessed* metric reported per namespace as well for each *shared streams accessed* metric reported per community. Whether each daily transaction debits Flex Credits depends on how the summation of each metric compares to a threshold defined in your rate plan. Generally, this rate plan charges a monthly fixed fee, which allows you to have daily usage up to a certain threshold for each of the three aforementioned metrics. When daily usage goes beyond this threshold, additional variable charges apply.  
This threshold applies for each usage metric across all namespaces (for *streams stored* and *streams accessed*, separately) and communities (for *shared streams accessed*). For example, just considering the *streams stored*, all *streams stored* usage will be summed across namespaces for a day and checked against the *streams stored* threshold; if the summed usage for *streams stored* is greater than its threshold, the difference between the *streams stored* usage and its threshold will be multiplied by its per-stream daily rate. This additional variable charge is only applied to the day it occurs. Once the day concludes, usage starts again from zero for the new day and at the end of this new day usage is checked against thresholds to determine if variable charges apply for the day. The method explained for *streams stored* is also used, separately, for *streams accessed* (summing across namespaces) and *shared streams accessed* (summing across communities).
- The daily usage in your tenant for *total streams accessed*.  
This type of rate plan creates a Flex Credit transaction for each *total streams accessed* metric reported per namespace and per community. Similarly, to the first rate plan, a summation is tracked within a day for *total streams accessed*; unlike the first rate plan, this summation is done across namespaces and communities for the single *total streams accessed* metric. For each Flex Credit transaction, the usage contributes to a summation that is checked against the multiple tiers in your rate plan. Each tier has a range of *total streams accessed* to which a particular per-stream daily rate applies. Therefore, the number of *total streams accessed* that fall in the first tier's range will get charged the first tier's per-stream daily rate; then the number of total streams accessed that fall in the second tier's range will get charged at the second tier's per-stream daily rate; and so on. This usage check against the rate plan's various tiers is done once a day at the end of the day. Once the day is completed, usage starts again from zero for the new day and its usage is checked against the various tiers' thresholds once this new day is completed.

Flex credit transactions are executed daily. CONNECT data services records stream usage throughout the day,

presenting a final summary to CONNECT after the day's conclusion.

## **Evolution of rate plans**

While the structure of rate plans is generally a function of usage, the pricing and features they include may evolve over time. The rate plans aim to accommodate varying customer needs and usage patterns.

## **Flex credit customer support**

In cases of confusion or inquiries about flex credits, customers can seek clarification from the [AVEVA support team](#).

## **Additional flex credit documentation**

- For more information about flex credits, such as information about credit agreements or rate plans, see the [CONNECT documentation](#).
- For a description of each AVEVA cloud service available, see [AVEVA Service Descriptions for Cloud Services](#).



**AVEVA Group plc**  
High Cross  
Madingley 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.