ThreatQuotient

ThreatQ Data Exchange (TQX) Guide

Version 1.4.0

July 27, 2021

ThreatQuotient
11400 Commerce Park Dr., Suite 200
Reston, VA 20191

Support
Email: support@threatq.com
Web: support.threatq.com
Phone: 703.574.9893

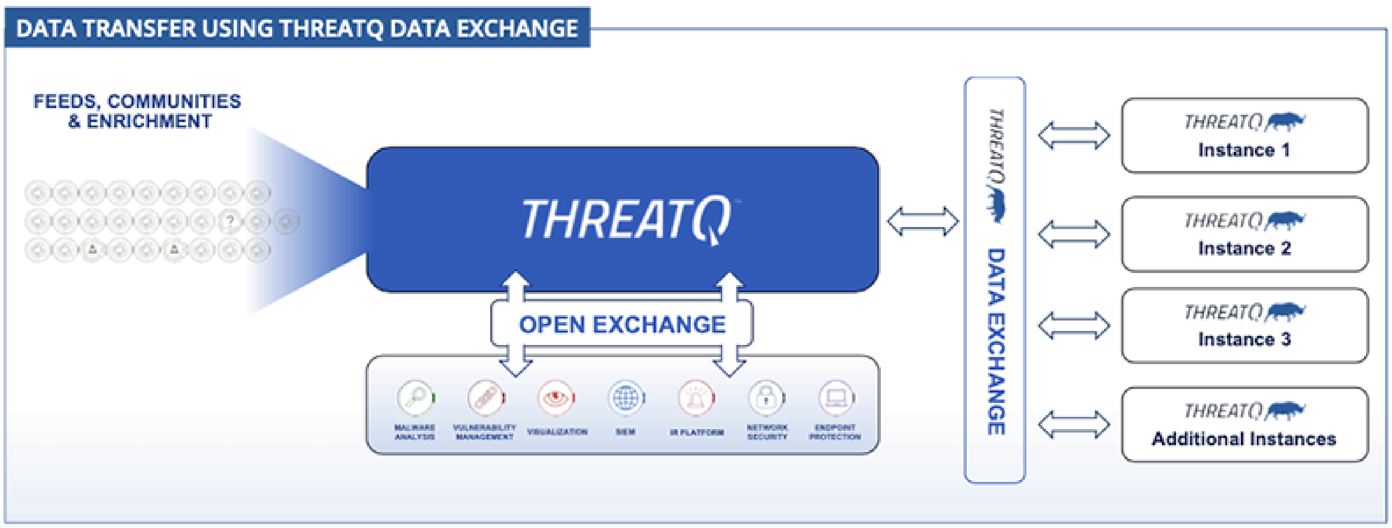
Warning and Disclaimer

ThreatQuotient, Inc. provides this document “as is”, without representation or warranty of any kind, express or implied, including without limitation any warranty concerning the accuracy, adequacy, or completeness of such information contained herein. ThreatQuotient, Inc. does not assume responsibility for the use or inability to use the software product as a result of providing this information.

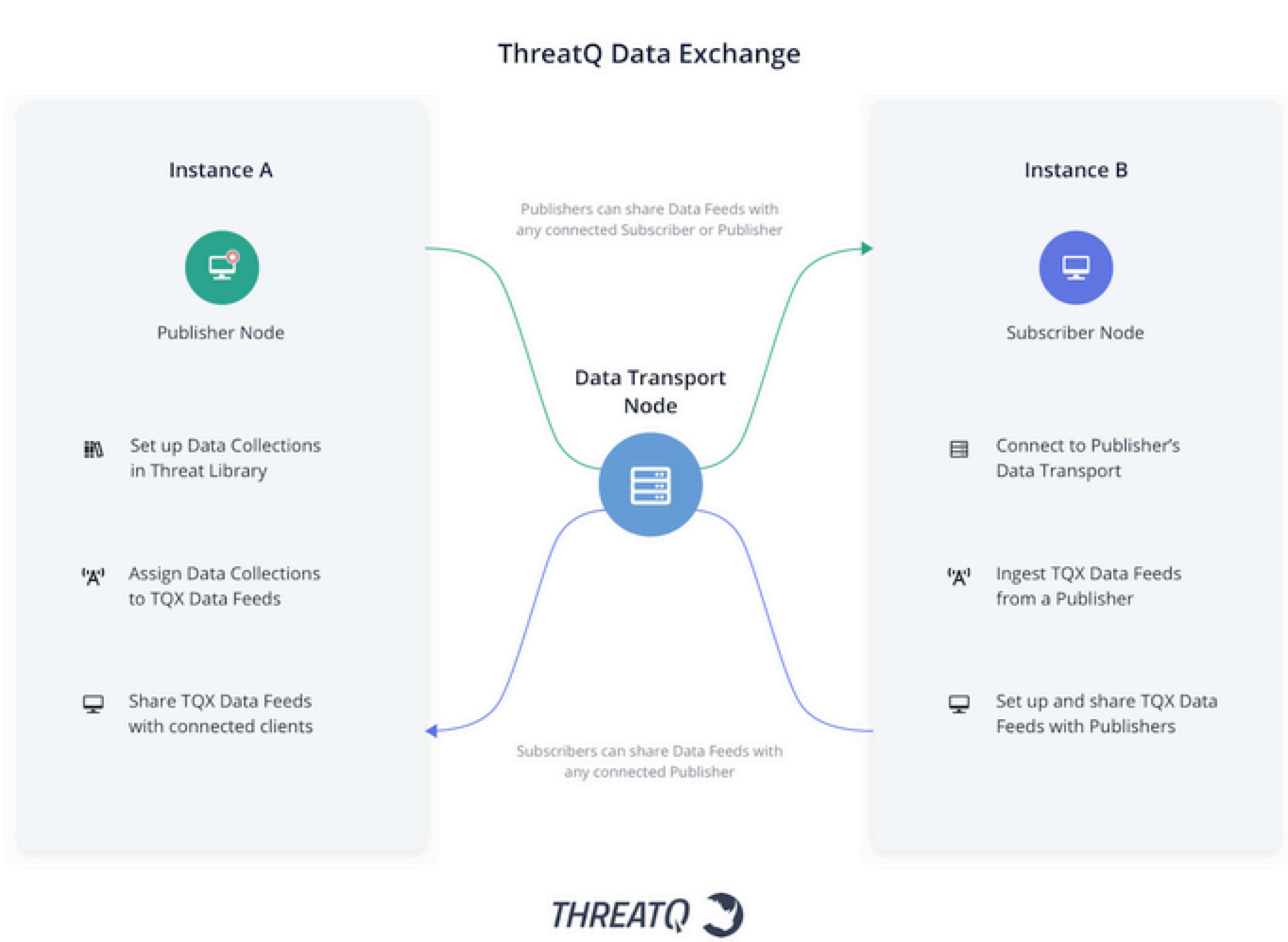
Contents

Overview

The ThreatQ Data Exchange (TQX) allows the bi-directional sharing of threat intelligence across multiple ThreatQ instances. This allows your organization to build a centralized threat repository, referred to as a Publisher, that can transmit specific intel to various departments within your organization, known as Subscribers. These Subscribers can analyze the data they ingest and provide feedback to the Publisher via a new Data Feed.



How it Works



Instance Types

There are two different types of TQX instances available: Subscriber and Publisher.

Upgrading an instance to a Publisher license allows you to create data connection bundles, which are used to create connections with Subscribers. Once connected to a Subscriber, you can send and receive system objects in the form of Data Feeds. See the Publisher topic for further information.

> You will need at least one Publisher instance in order to utilize TQX.

Upon upgrading to ThreatQ version 4.49+, your ThreatQ instance will have Subscriber permissions by default. As a Subscriber, you can connect to the data transport using the connection bundle sent to you by the Publisher and select the Data Feeds you want to receive as well as create Data Feeds and share them with the Publisher. See the Subscriber topic for further information.

Connection Bundles

Publishers can create connection bundles that allow Subscribers to connect via a data transport. This connection is a bi-directional connection between the Publisher and Subscriber and allows the sharing of data collections in the form of Data Feeds.

Publishers and Subscribers use a multi-step wizard to create their first connections. Additional connections are managed through your Topology View.

See the Getting Started - First Connections, Publisher, and Subscriber topics for further information.

Data Feeds

Users can create and edit Data Feeds that they wish to obtain specific data from in order to send information to others through the ThreatQ Data Exchange.

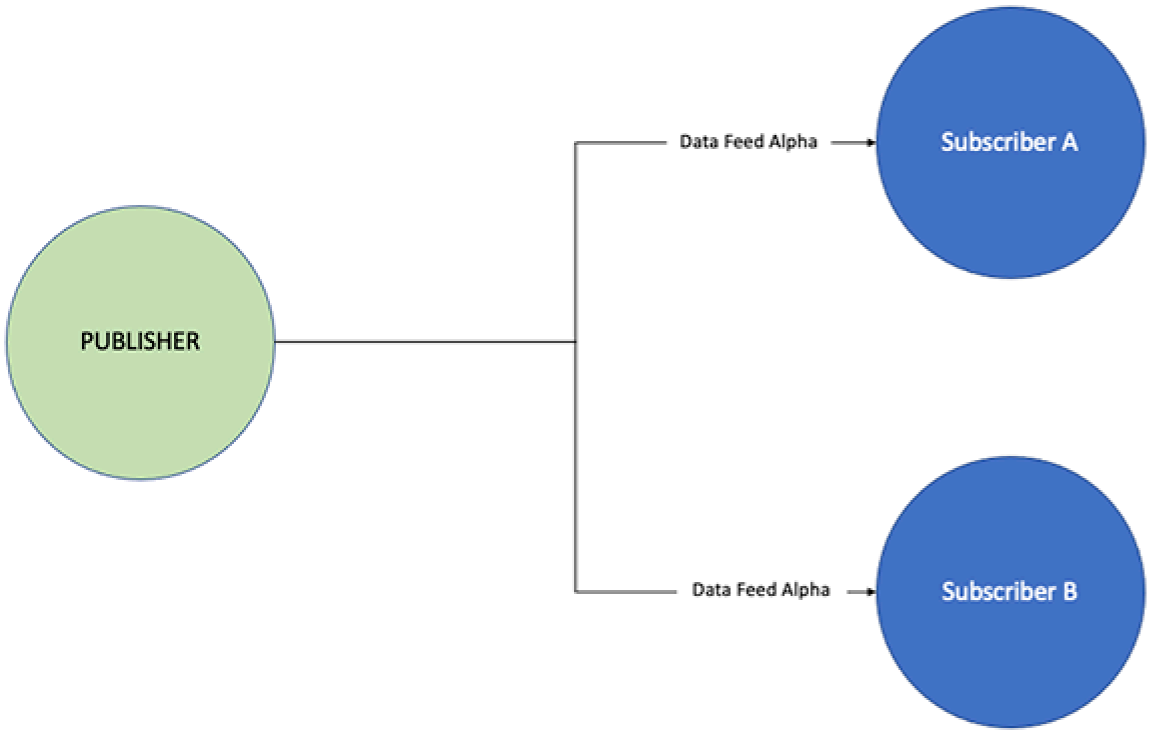
A Publisher can use a saved Data Collection from the ThreatQ Threat Library to create a Data Feed. That Data Feed can be offered to one or more recipients, which can be Subscribers or Publishers, for subscription. Once a recipient subscribes to the Data Feed, he receives data from it at a user-defined frequency.

> A Publisher can send and receive Data Feeds to/from a Subscriber. A Subscriber can send and receive Data Feeds to/from a Publisher. A Subscriber cannot send Data Feeds to another Subscriber. Subscribers are **not** be able to see another Subscriber in their Topology View.

See the Data Feeds topic for further details.

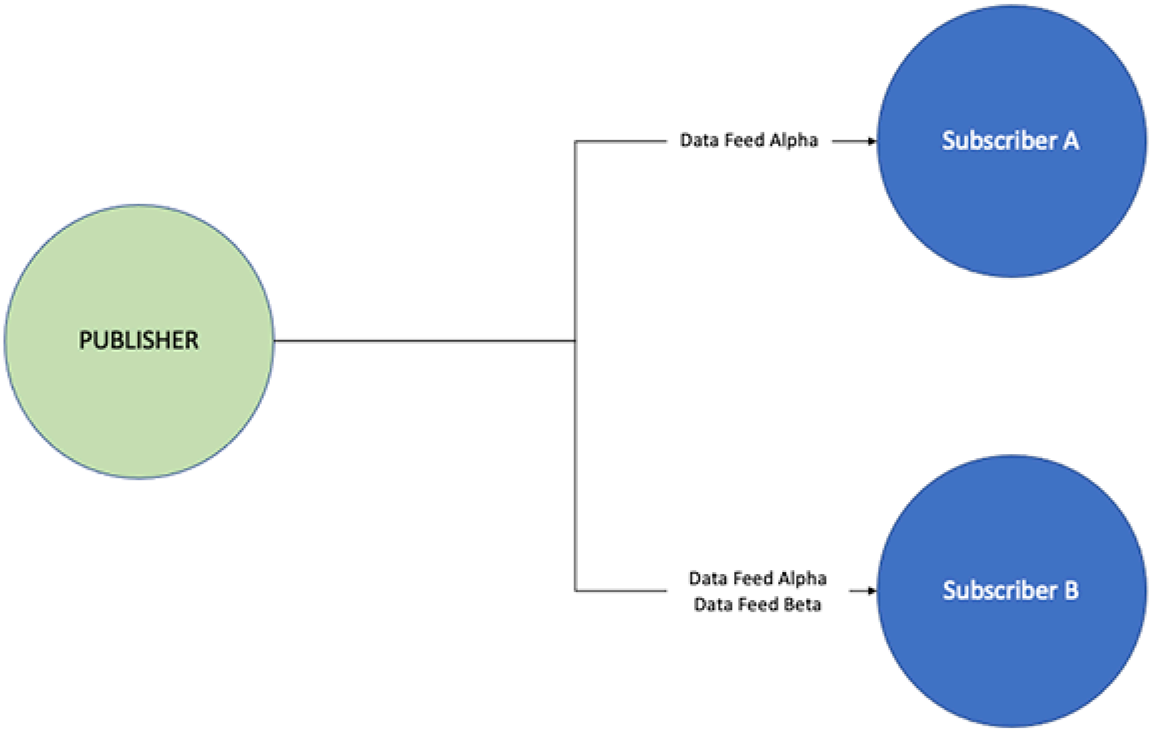
Example - One Publisher, Two Subscribers

A Publisher creates a Data Feed, named Alpha, and assigns it to two connected Subscribers with a publish frequency set to hourly. When they subscribe to the Data Feed, both Subscribers will receive Data Feed Alpha's information every hour.



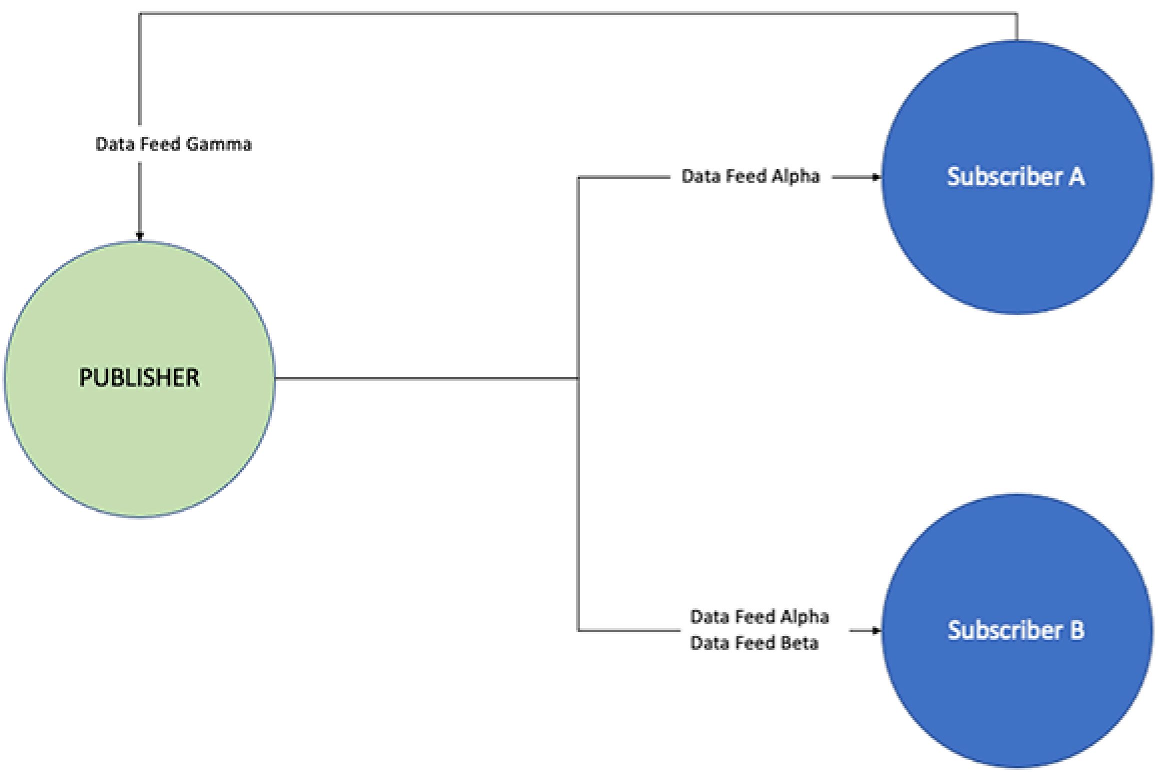
Example - One Publisher, Two Subscribers with Different Data Feeds

In this example, the Publisher is offering Data Feeds to two Subscribers. The Publisher selects one feed to be offered to Subscriber A and two feeds to be offered to Subscriber B. In this scenario, Subscriber A and B can subscribe to Data Feed Alpha. Additionally, Subscriber B also has the option to subscribe to a second Data Feed, Beta, from the Publisher.



Example - One Publisher, Two Subscribers with a Subscriber sending a Feed to the Publisher

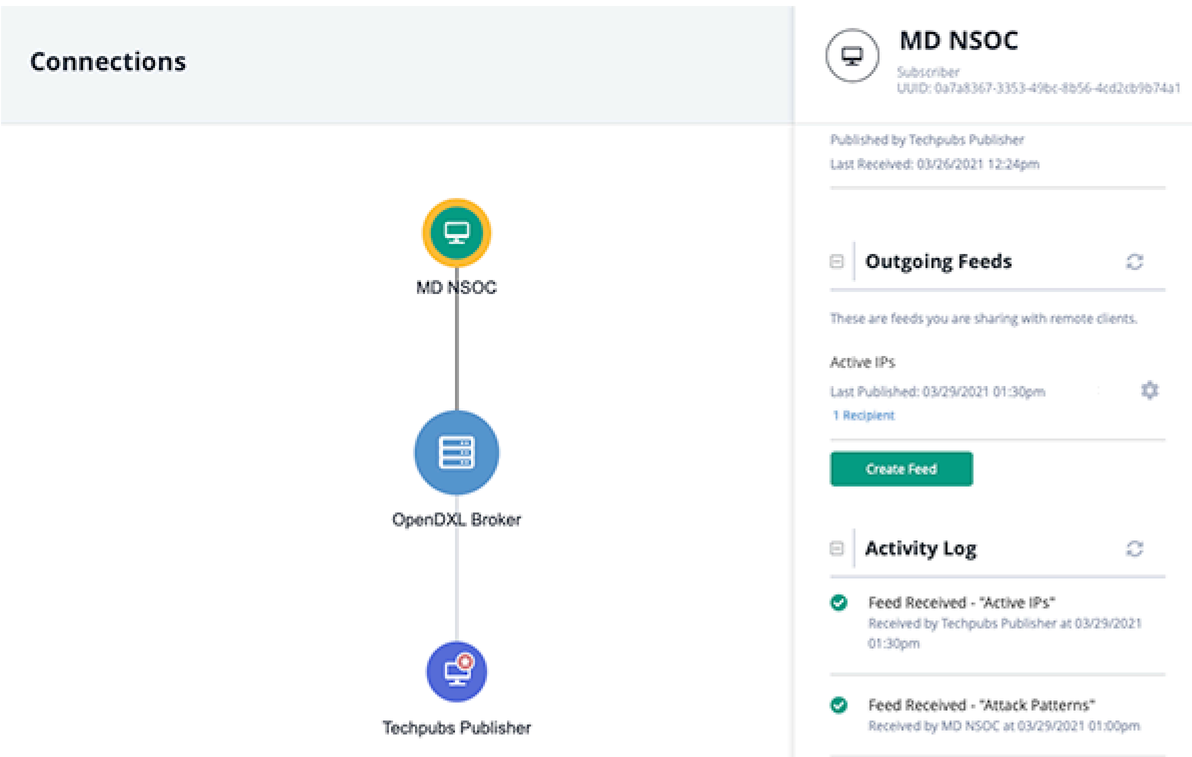
In this example, in addition to subscribing a Data Feed from a Publisher, Subscriber A is also offering its own Data Feed back to the Publisher for subscription.



Managing Connections

Publishers and Subscribers can view connections, instance details, and activity logs via a node-based interface referred to as the Topology View.

> Publishers can see all Subscribers that they are connected to in the Topology View. Subscribers only see their instance node and the Publisher(s) they are connected to in the view. Subscribers cannot see or submit/receive data from other Subscribers.



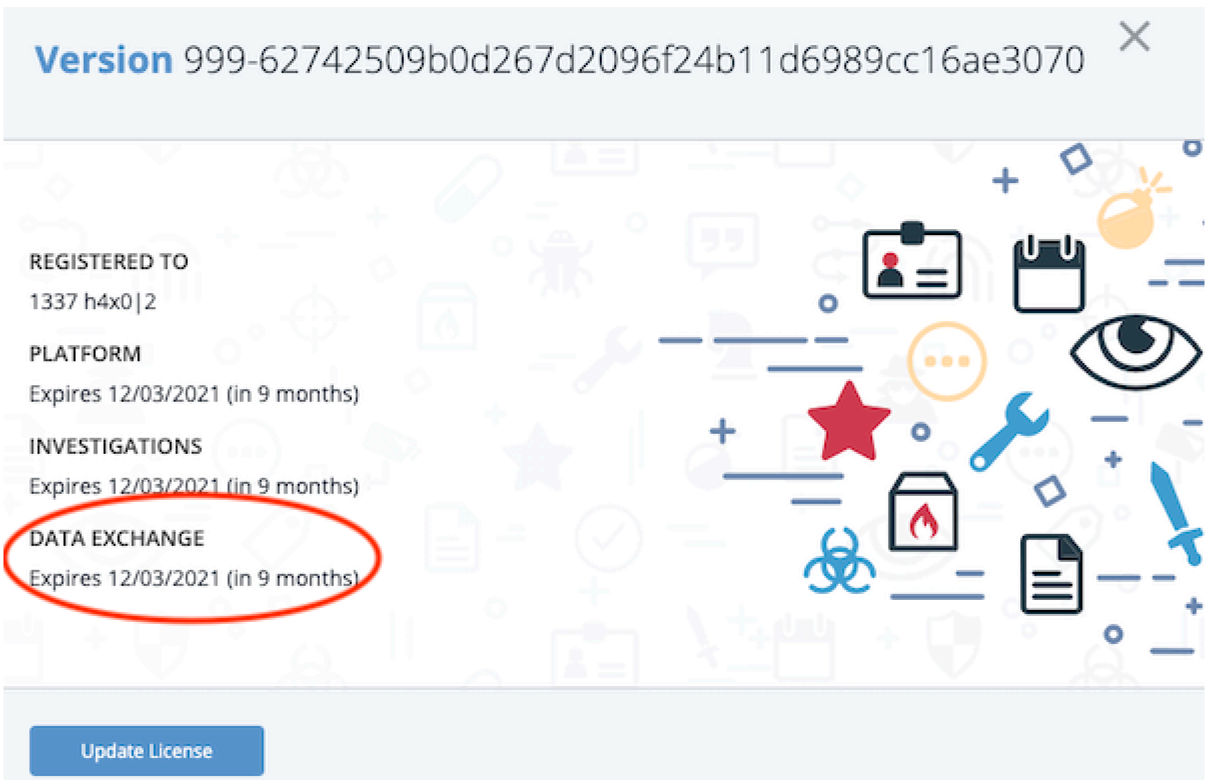
The view and available actions differ based on your instance type (Publisher, Subscriber). See the Publisher and Subscriber topics for more details.

Requirements

The following is a list of the minimum requirements for the ThreatQ Data Exchange:

- Two ThreatQ instances running ThreatQ version 4.49+
  - One instance must have a Publisher license

    Publisher instances see the Data Exchange license information in their about window. This can be accessed by clicking on the settings gear icon and selecting **About** from the dropdown.

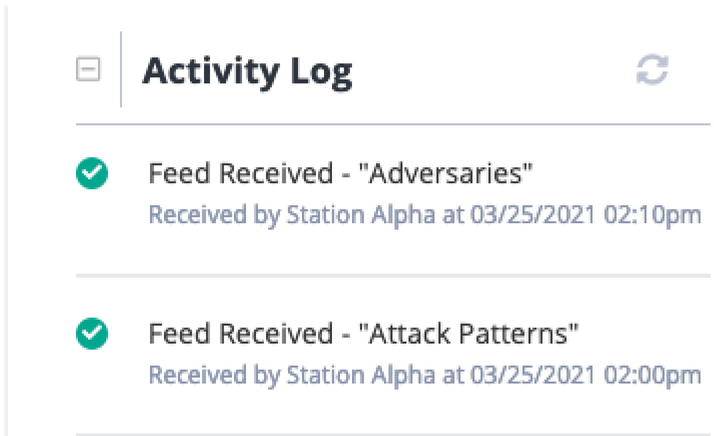
  - One instance with the standard ThreatQ platform license

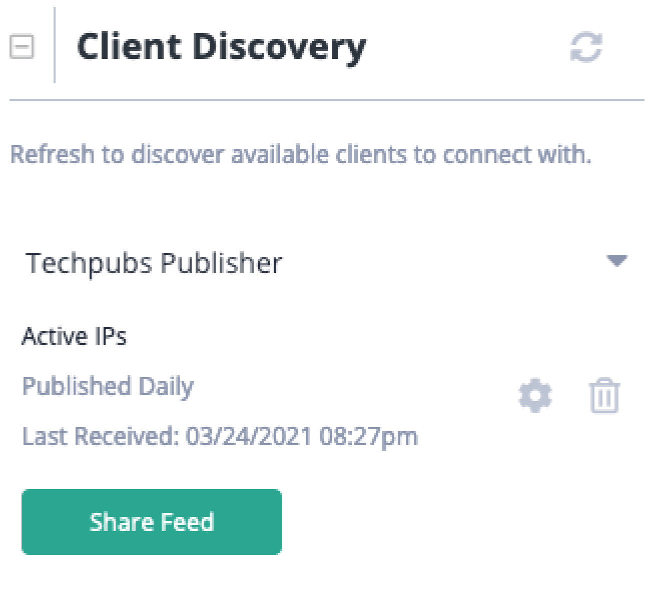
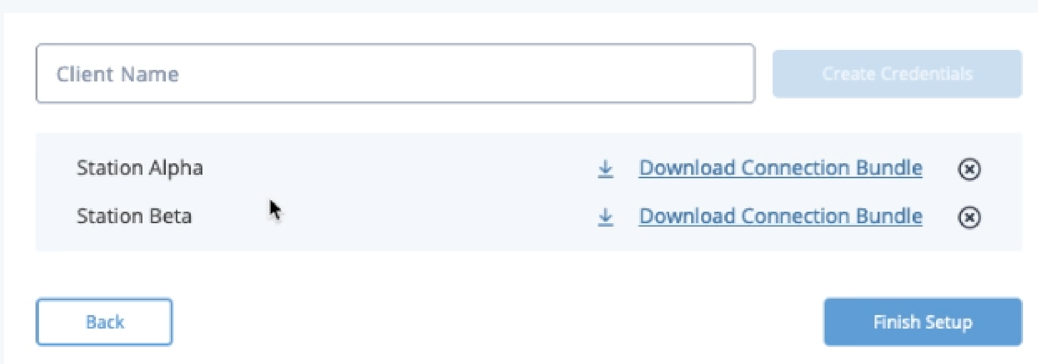
    > All ThreatQ instances on version 4.49+ will have Subscriber permissions. Subscribers will not see the Data Exchange license on their About window.

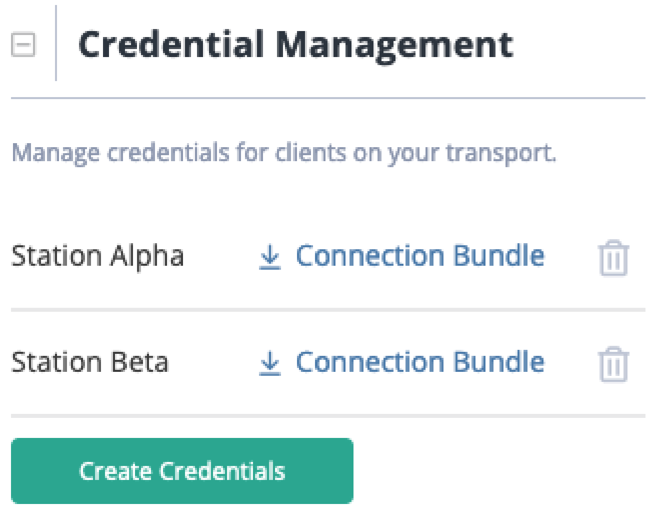
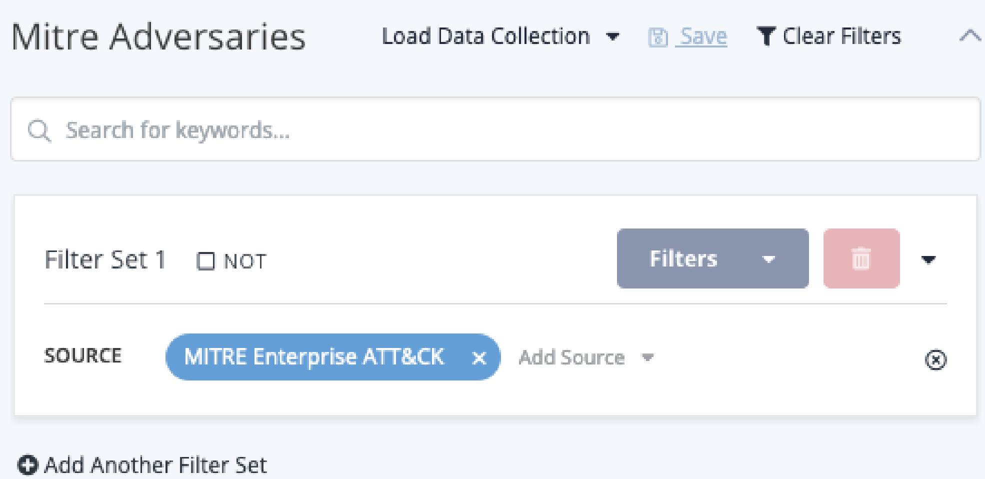
- One Data Collection saved.
- Network access for both instances.

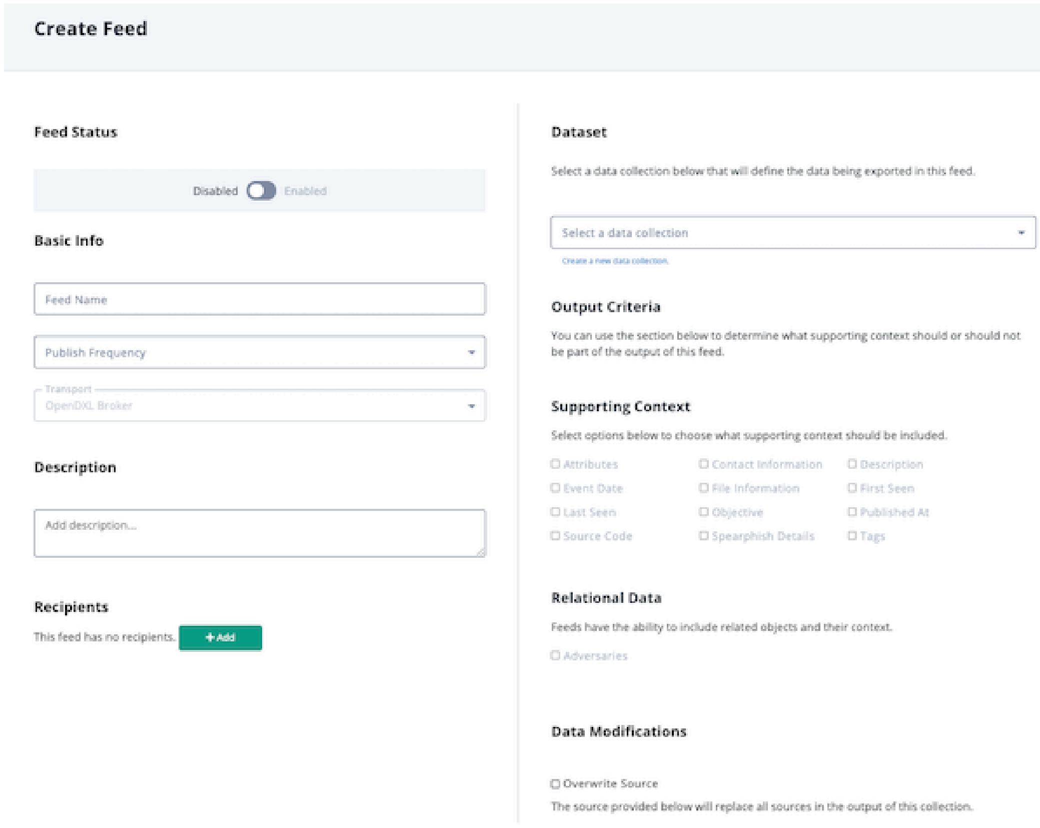
Components

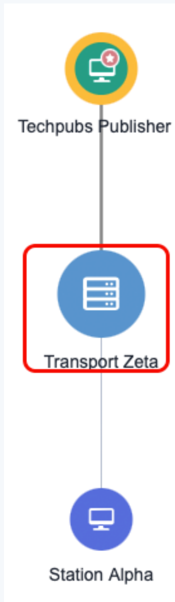
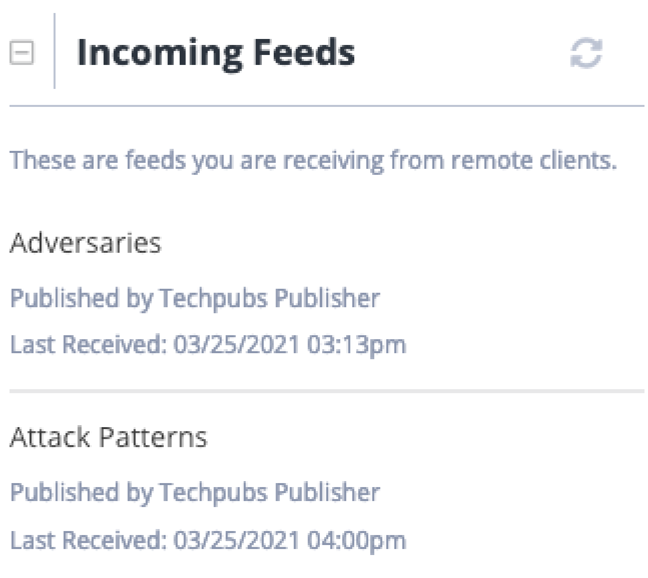
The following table contains key components, terms, and definitions regarding the ThreatQ Data Exchange service.

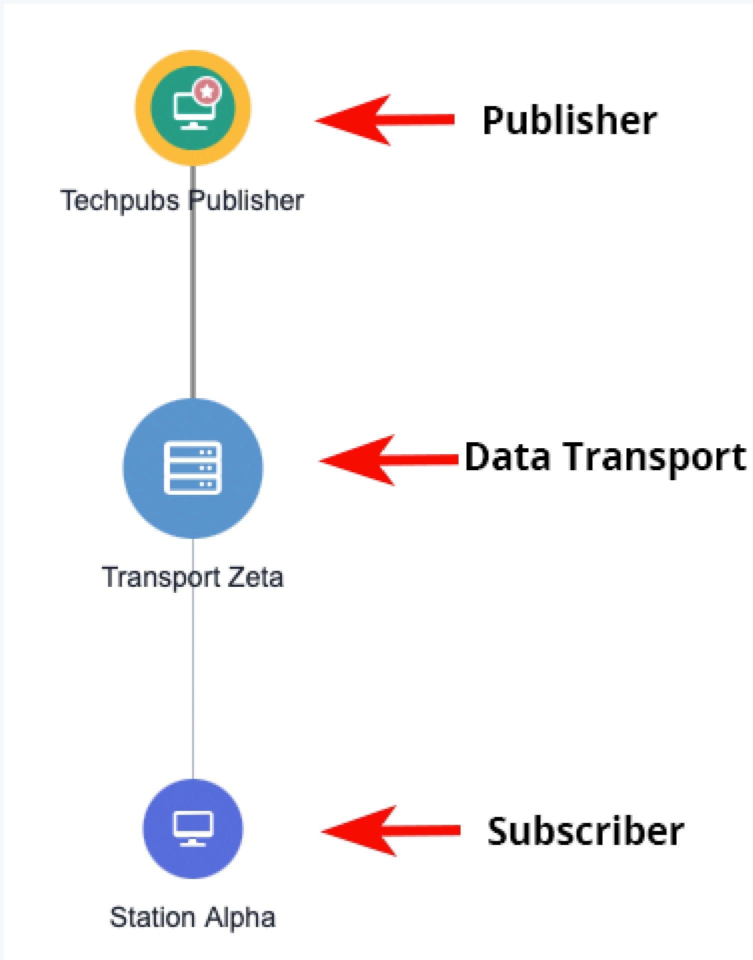
COMPONENT/ TERM	DEFINITION
Activity Log	The Activity Log, located on the bottom-right of the Topology View, provides an audit trail for TQX activity such as when a new node has been added to your connection and when you submitted or received information from a Data Feed. 
Client	The term Client is used to refer to other platform instances when creating a Connection Bundle.
Client Discovery Pane	The Client Discovery pane is accessible by clicking on the transport node in your Topology View. Users can view the instances they are connected with and which data feeds they are submitting to those instances.

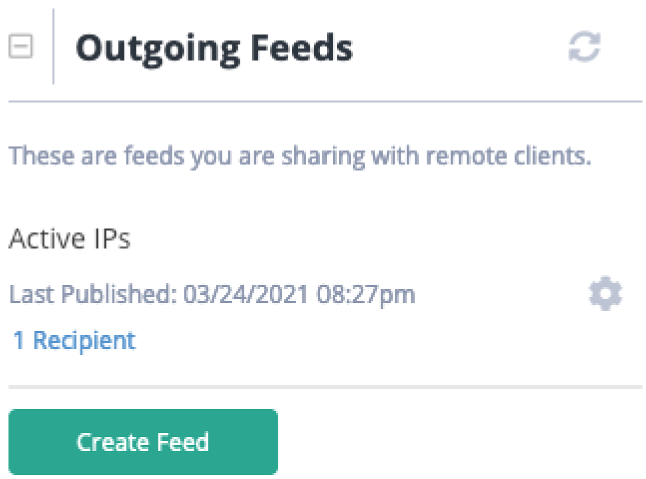
COMPONENT/ TERM	DEFINITION
	
Connection Bundle	The connection bundle is a zip file containing connection information for the Data Transport. A connection bundle is created by a Publisher when creating a new connection, such as adding a new Subscriber. The connection bundle zip must be uploaded by the Subscriber when connecting to a Publisher. 
Credential Management	The Credential Management pane is accessible after clicking on the transport node in the Topology View and is only accessible by Publishers. Publishers can use this pane to create new connection bundles, download existing connection bundles, and delete connection bundles.

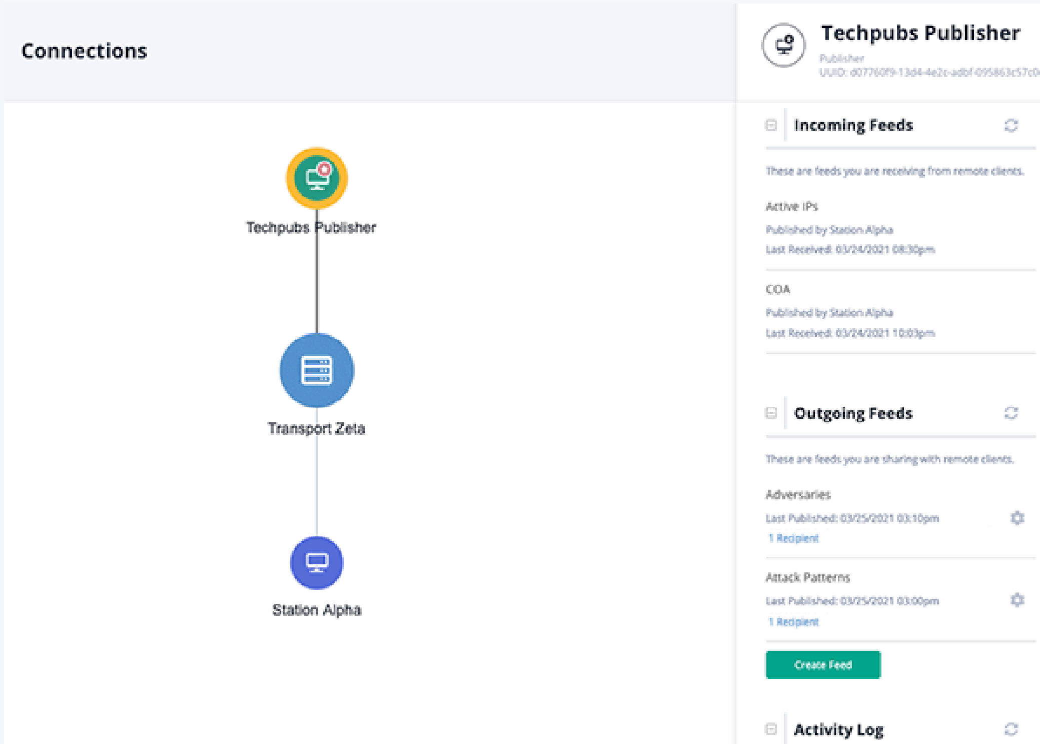
COMPONENT/ TERM	DEFINITION
	
Data Collection	A data collection is a saved ThreatQ Threat Library query that can be used to create a Data Feed. 
Data Feeds	Data Feeds transmit selected Data Collections to user-selected instances (Publishers, Subscribers). You can select which data collection to use, whether or not to include associated attributes, and also rename the source for the feed so that the receiver can easily identify system objects ingested from the data feed.

COMPONENT/ TERM	DEFINITION
	
Data Transport	The Data Transport is how data is shared between TQX nodes, using OpenDXL by default. Currently, you can only use the TQX default transport included with a Publisher license. Additional transport options, including the ability to use your own, will be introduced in future releases.

COMPONENT/ TERM	DEFINITION
	
Incoming Feeds Pane	The Incoming Feeds pane is accessible from the right menu pane after clicking a Subscriber or Publisher node in your Topology View. You can see the name of the feed you are subscribed to, the instance that sent it, the publish rate, and the last received time stamp. 

COMPONENT/ TERM	DEFINITION
Nodes	A node is a basic unit of a data structure within TQX, such as an instance (Publisher/Subscriber) or data transport, that can be viewed on the Topology view. You can click on a node to view specific information. 
Outgoing Feeds Pane	The Outgoing Feeds pane is accessible from the right menu pane after clicking a Subscriber or Publisher node in your Topology View. You can see the name of the feed you are subscribed to, the instance that will receive it, the publish rate, and the last published time stamp. You also have an option to create a new feed from this pane.

COMPONENT/ TERM	DEFINITION
	
Publisher	A ThreatQ instance with a TQX broker license, which allows a user to create a connection bundle. At least one Publisher instance is required in order to create a connection. In TQX, Publisher nodes will have a star badge icon in the Topology View.
Subscriber	A ThreatQ instance on version 4.49+ that does not have a TQX broker license. A Subscriber can subscribe to Data Feeds from a Publisher and offer Data Feeds to the Publisher for subscription. However, a Subscriber can neither see nor offer Data Feeds to other Subscribers connected to the Publisher.
Topology View	The Topology View provides you with a visual representation of your TQX connections. You can access the view by clicking on the Data Exchange menu and selecting **Connections**. From this view, you can click on various nodes to view specific information. Publishers can create/offer Data Feeds and create new connection bundles from this view as well.

<table>
<tr><th>COMPONENT/ TERM</th><th>DEFINITION</th></tr>
<tr><td></td><td>


</td></tr>
</table>

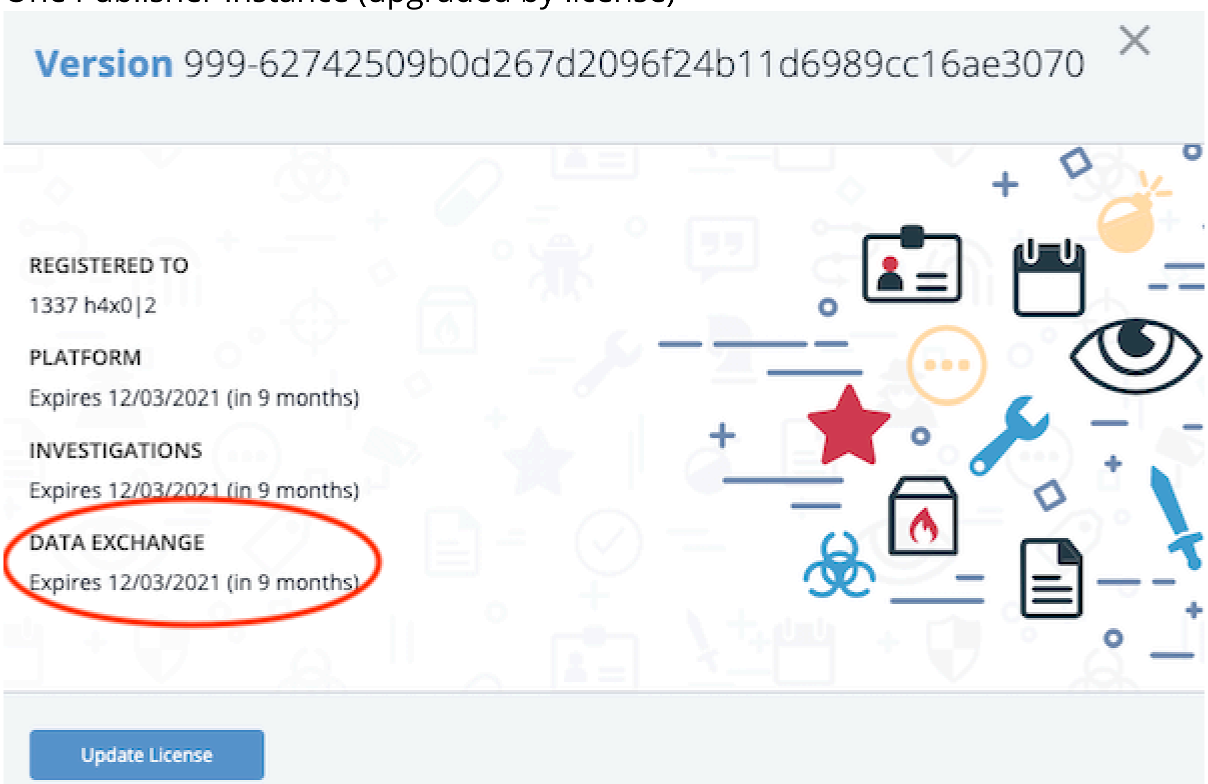
Getting Started

The information found in this topic will provide the initial steps to create a connection bundle, set up a subscriber, and to create your first Data Feed.

Confirm Requirements

Confirm that you have the following:

- Two separate ThreatQ instances
    - One Publisher Instance (upgraded by license)

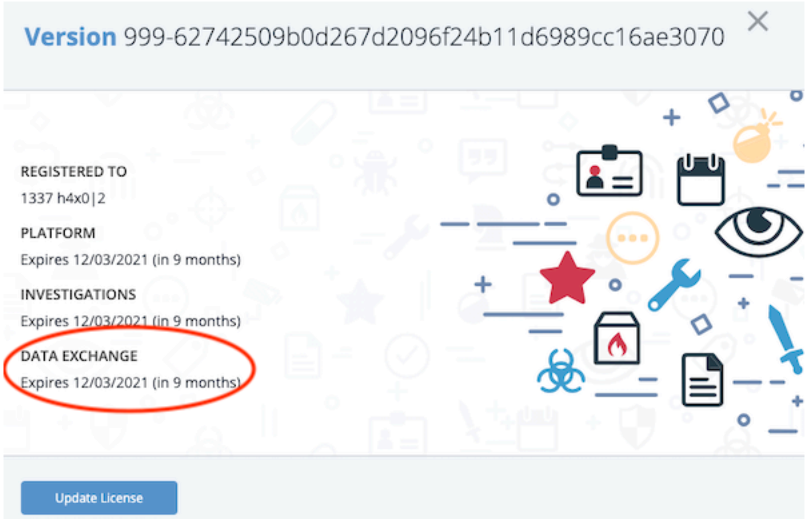


    - One Subscriber Instance (included with standard ThreatQ License version 4.49+)
- Network connection between the two instances
- At least one saved Data Collection (Publisher instance)

Publisher - Creating a Connection Bundle

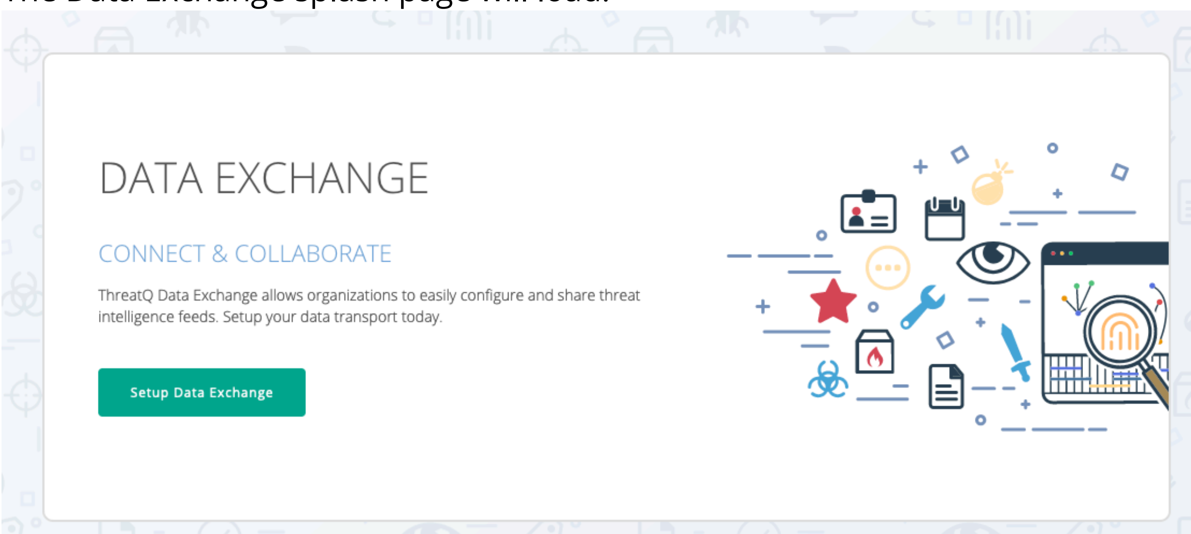
1. Click on the settings icon and select **About**.

2. Confirm that the **Data Exchange** license information is displayed. This confirms that your instance has the Publisher permissions via your license.



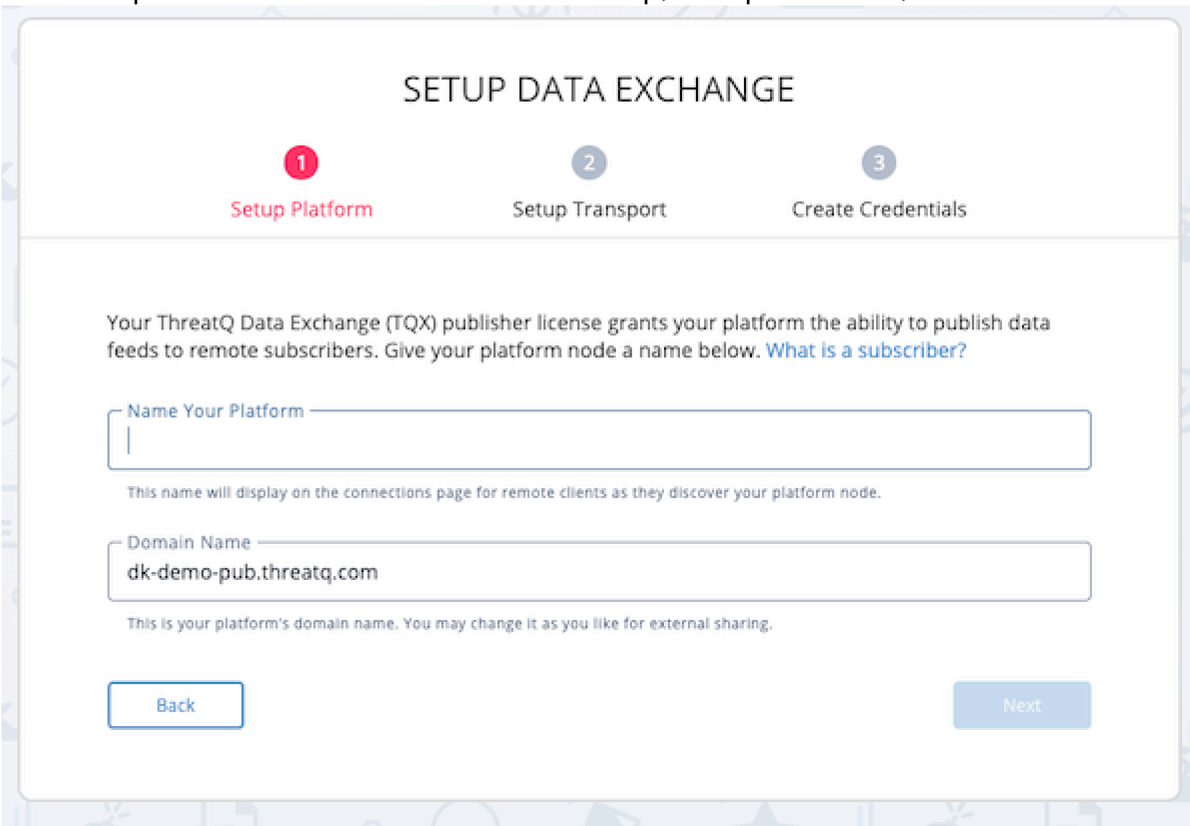
3. Click on the **Data Exchange** icon and select **Connections** in the top navigation bar.

   The Data Exchange splash page will load.



4. Click on **Setup Data Exchange**.

The Setup Wizard will load with the first step, Setup Platform, selected.

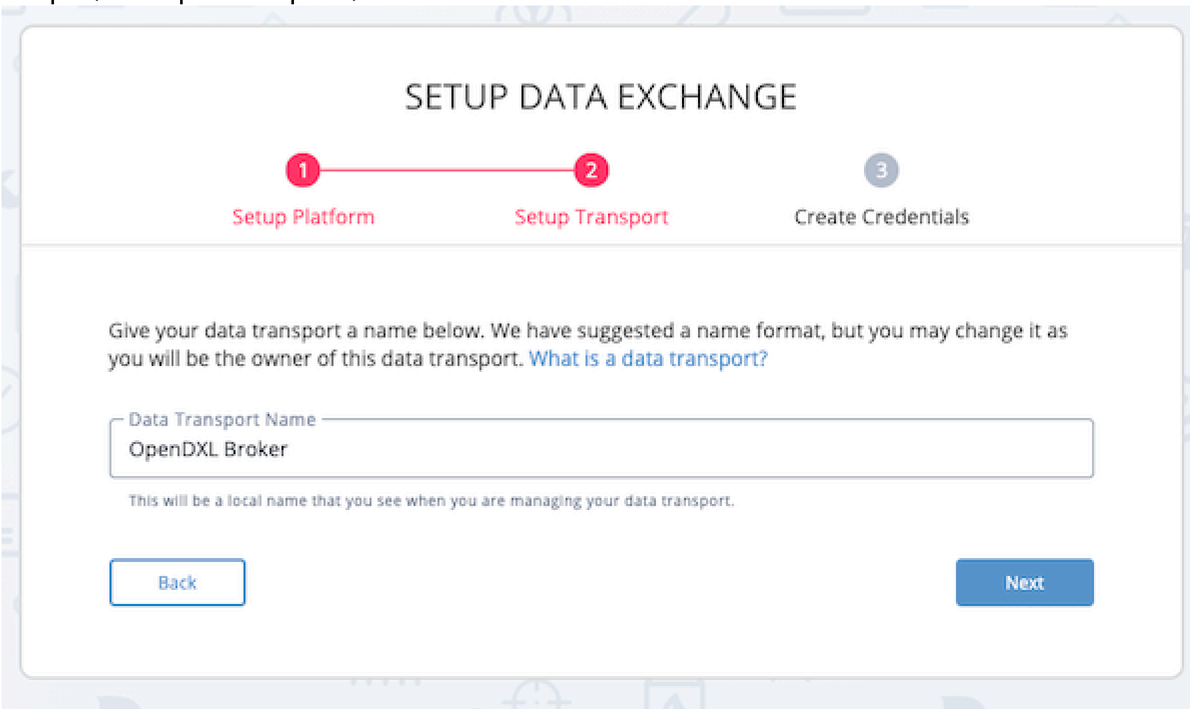


5. Enter a **Platform Name** for your instance. This is the name that you will use to identify yourself on the connections page. Subscribers will also see this name when viewing their Topology view.

> You can change this name later but it will only affect your view. Subscribers will still see the name you entered for this step.

6. The **Domain Name** field is automatically populated based on your ThreatQ instance. Leave this field as is.
7. Click on **Next**.

Step 2, Setup Transport, will load.

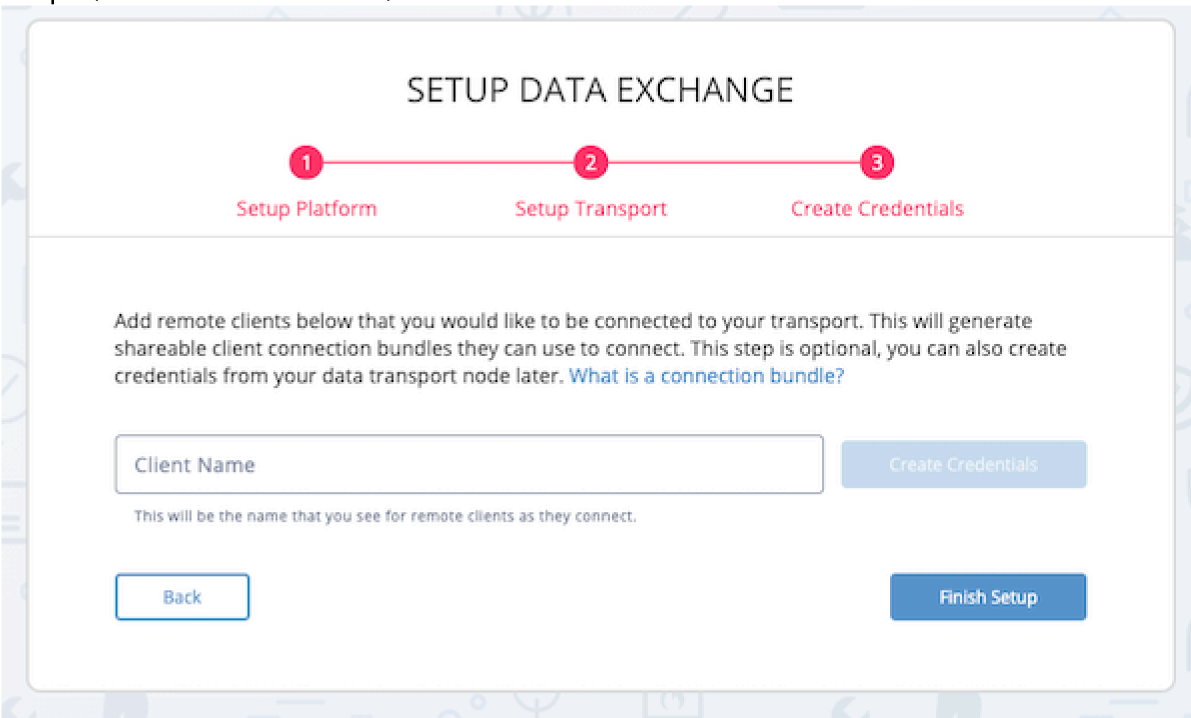


8. Update the **Data Transport Name** if desired, otherwise use the default entry. This name will be used to identify the Broker node in your Topology view.

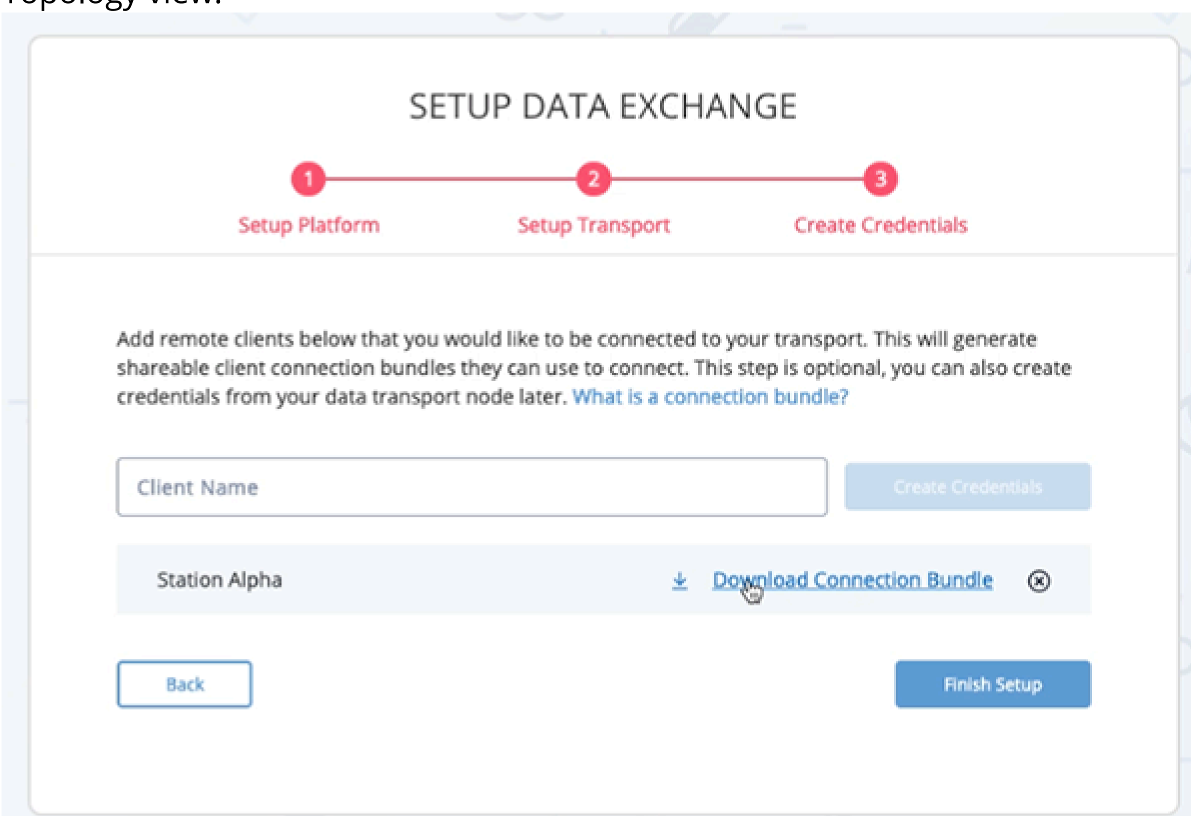
> Subscribers are given the option to name the Data Transport during their connection setup. The name you enter in this field will not affect what Subscribers see.

9. Click the **Next** button.

Step 3, Create Credentials, will load.



10. Enter a **Client Name** and click on **Create Credentials** for each Subscriber you will connect to using ThreatQ Data Exchange. The names you enter here will only affect your Topology view.



> Publisher names a Subscriber: Station Alpha.
> Subscriber names their platform: East Wing NSOC
>
> The Publisher will see the Subscriber node as: Station Alpha
> The Subscriber will see his/her platform as: East Wing NSOC

11. Repeat step 10 to create credentials for additional subscribers.
12. Click the **download** icon to download the Connection Bundle for each client.

> Subscribers will need the Connection Bundle file during their setup.

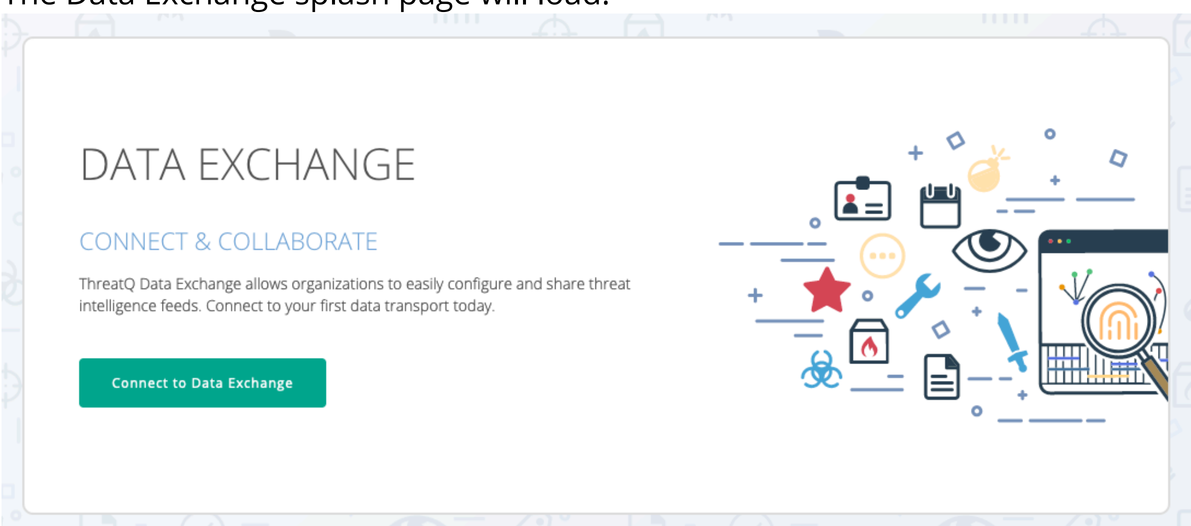
13. Click the **Finish Setup** button.
14. Send the Connect Bundle(s) you downloaded in step 12 to the Subscriber(s).

    The Subscriber will now need to perform their setup to continue the setup process. If you have not done so already, send the connection bundles to the Subscriber.

Subscriber - Connecting to a Publisher

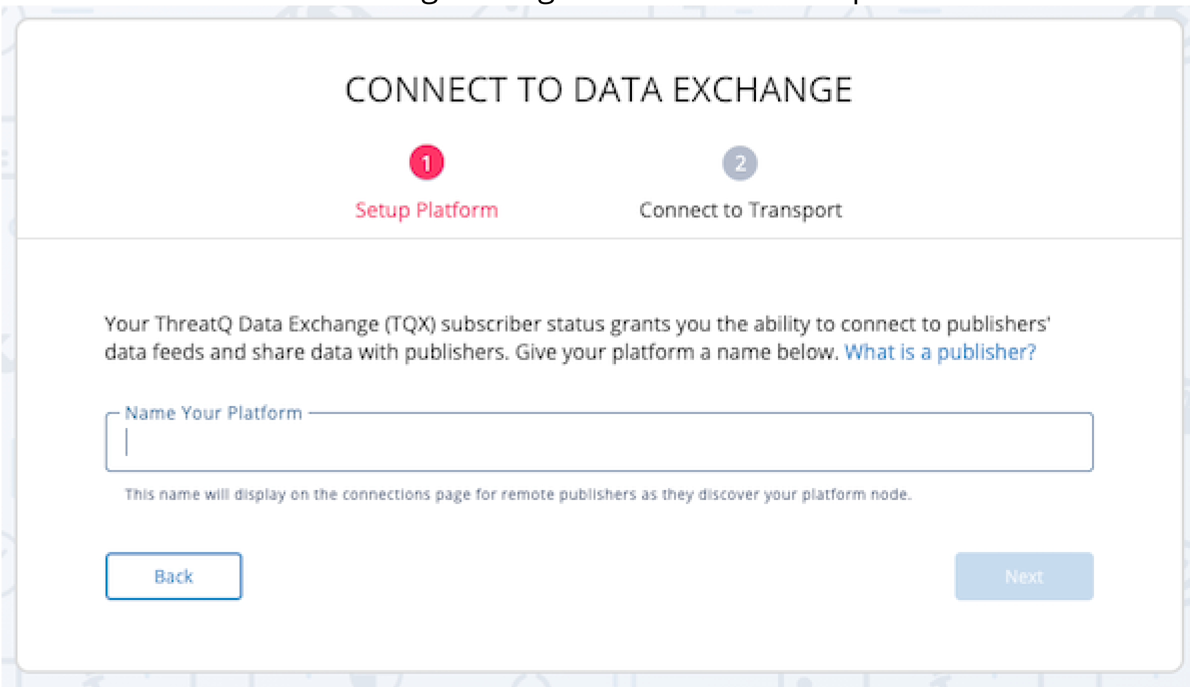
1. Click on the **Data Exchange** icon in the top navigation bar of ThreatQ and select **Connections**.

   The Data Exchange splash page will load.



2. Click on **Connect to Data Exchange**.

The Connect to Data Exchange dialog box will load on Step 1.

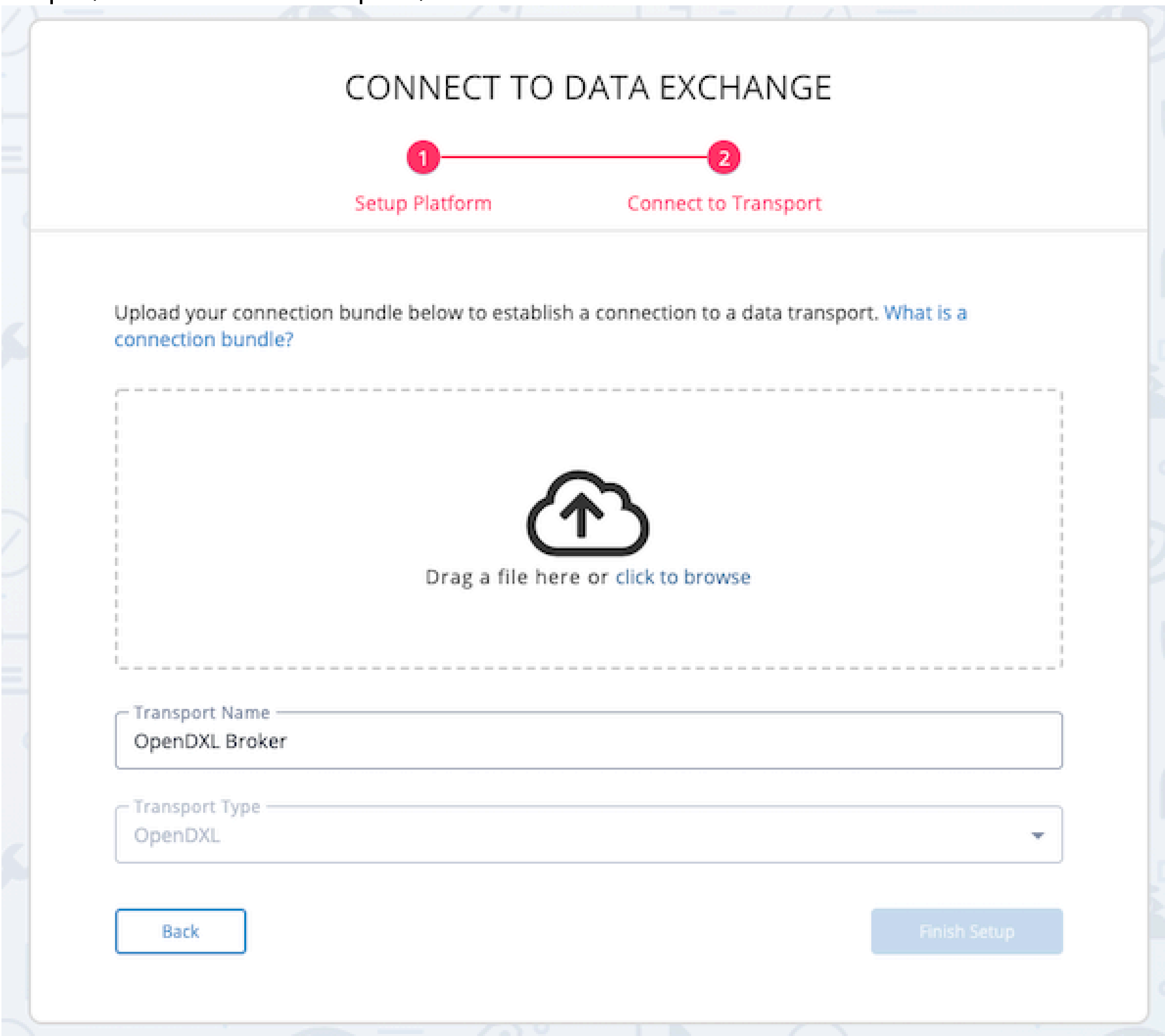


3. Enter a name for your platform instance. You will use this name to identify your instance in your Topology view.

> You can change this name later but it will only affect your view. Publishers may have a different a different name for your instance but will only see it in their Topology view.

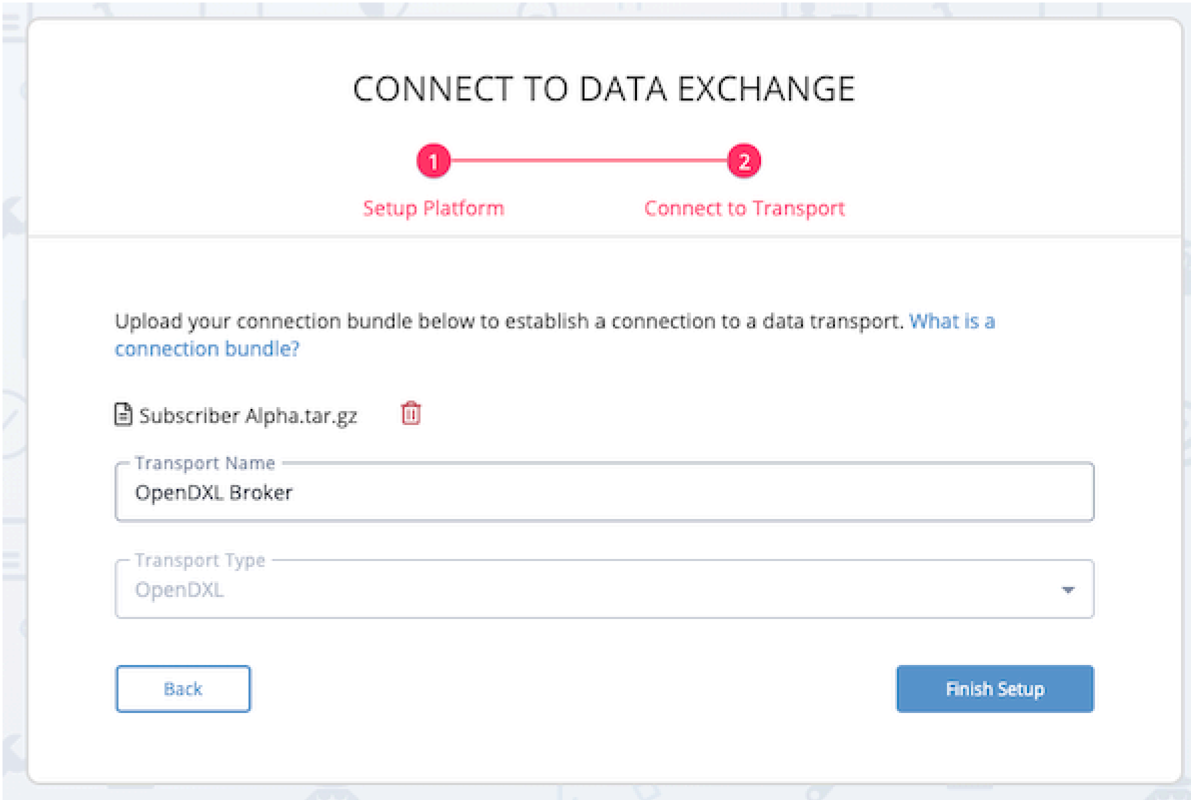
4. Click on **Next**.

Step 2, Connect to Transport, will load



5. Upload the **Connection Bundle** file by either:
    - Dragging and dropping the file into window
    - Clicking on the **Click to Browse** link to locate the file saved on your local drive.

> The Connection Bundle file is obtained from the user that set up the Publisher ThreatQ instance.

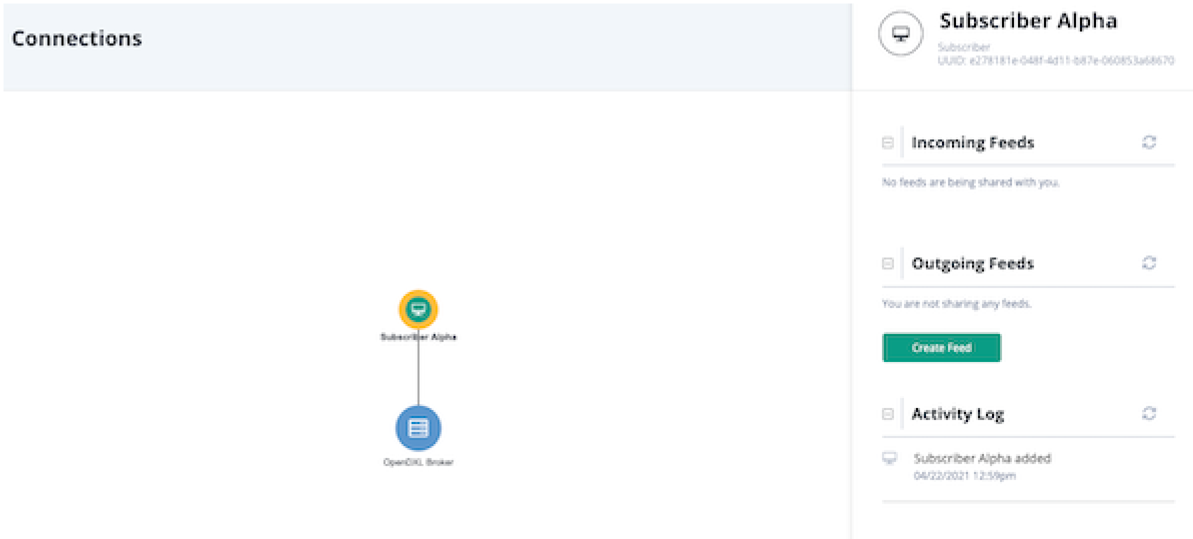


6. Update the **Data Transport Name** if desired, otherwise use the default entry. This name will be used to identify the transport node in your Topology view.
7. Leave the **Transport Type** dropdown field as is.

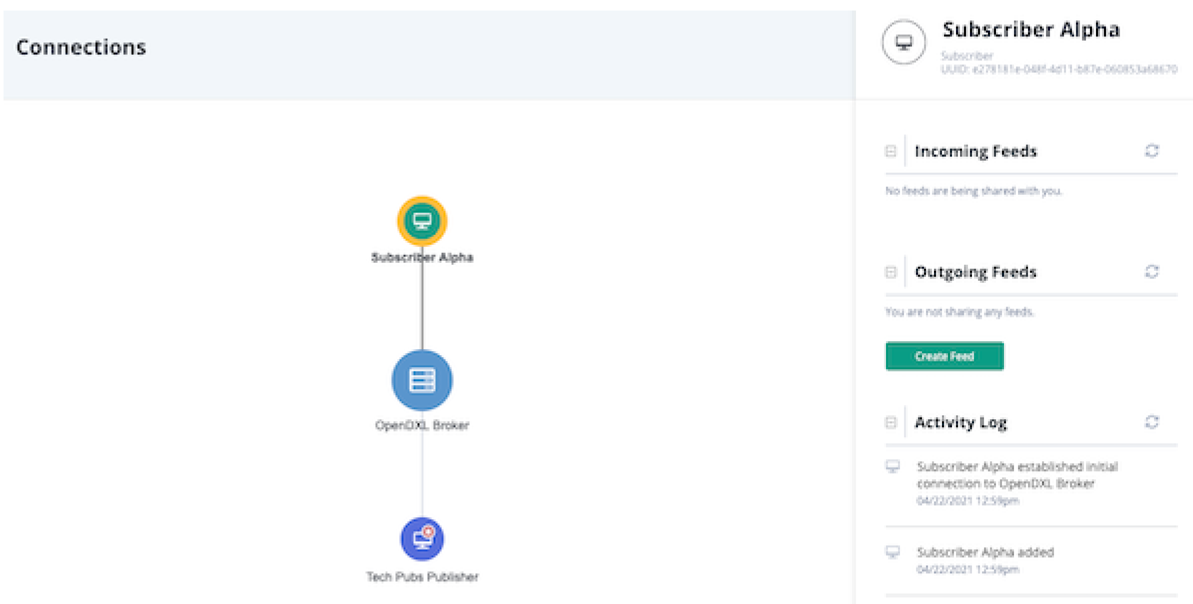
> The system default transport is the only transport available. The option for additional transports will be added in future releases of the ThreatQ platform.

8. Click on the **Finish Setup** button.

   The Connections page will load. You will see your platform, identified as a green node, and the transport, identified as a blue node. Pause until the Subscriber and Publisher instances discover each other.



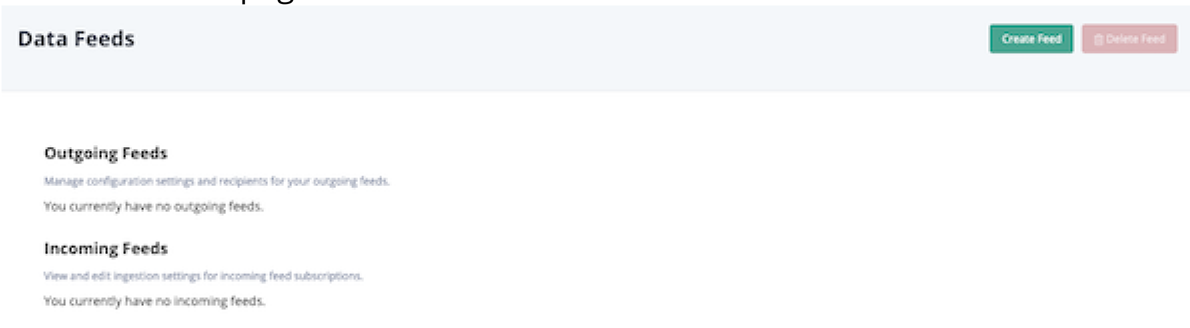
It can take up to 30 seconds for the discovery process to complete. Refresh the page in order to see the new connection. After the instances have discovered each other, the Connections pages will show the connections. The publisher will now see the subscriber node and the subscriber will now see the publisher node.



Publisher - Creating a Data Feed

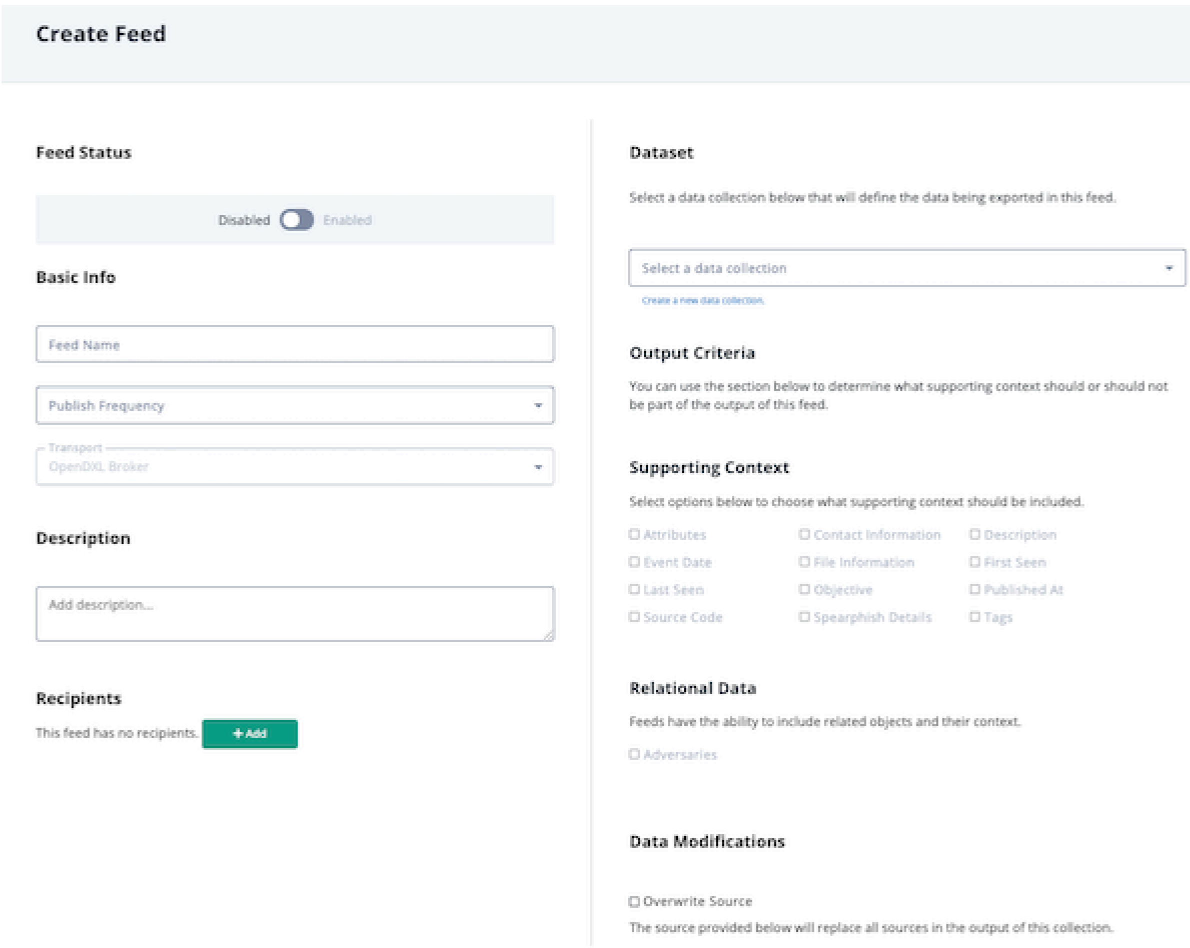
1. Click on the **Data Exchange** icon in the top navigation bar of ThreatQ and select **Data Feeds**.

The Data Feeds page will load.



2. Click on **Create Feed**.

The Create Feed form will load.



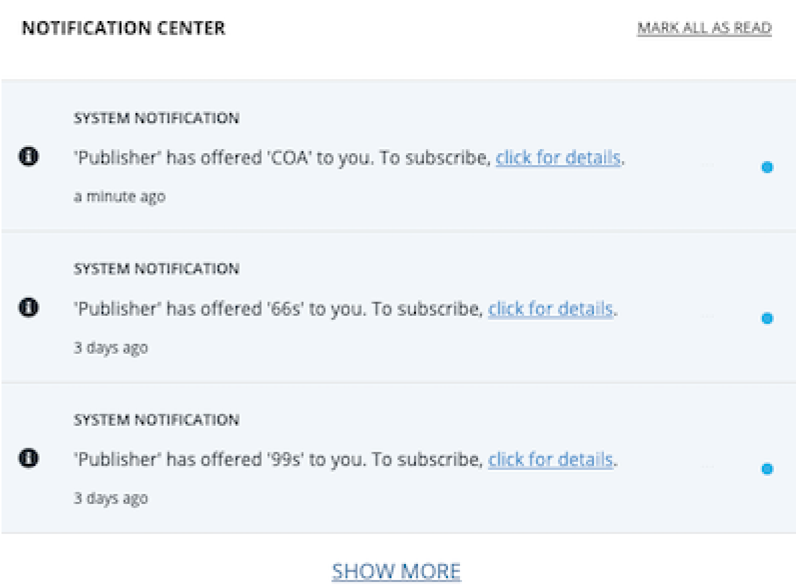
3. Populate the following form sections to specify the content and recipients of your feed:

SECTION	DESCRIPTION
Feed Status	Defaults to Disabled. Click the toggle to enable the feed.

Basic Info	• **Feed Name** - Enter the name you want to use for your feed. • **Publish Frequency** - Select Daily or Hourly depending on how often you want the feed to be published to Subscribers • **Transport** - At this time, you can only use the default transport provided by TQX. Additional transport options will be made available in future ThreatQ platform releases.
Recipients	**Offer Feed to Public** - Check this box to give all clients connected to the Transport the option to subscribe to the feed. After you save your feed settings, the Recipients section displays the clients eligible to subscribe to the feed. **OR** Click the **+Add** button to access the Add Recipients window which lists all the connection bundles you created. Select a recipient and click **Add Recipient**. Subscribers do not have to be connected yet to be assigned to a Data Feed. The Subscriber will not receive the Data Feed connection profile or system objects until they connect to the transport and subscribe to the feed.
Dataset	Select the Threat Library Data Collection to be exported with feed. **OR** Click the **Create a New Data Collection**

	option to open the Threat Library in a new tab and create a Data Collection.
Output Criteria	Select the supporting context that should be included in the feed using the checkboxes supplied. Only fields used in the data exported are selectable. Fields not associated with the data collection selected are greyed out. Check the Adversaries box to include related adversaries in the transfer. However, related attributes of the related adversary are not included.
Data Modifications	To override the default source name for the feed, check the **Overwrite Source** checkbox and enter the new source name. A Subscriber can view the data feed source name under object sources in their object details page.

4. Click the **Save** button. The recipients of the feed receive a system notification that a new feed is available for subscription. This notification includes a link to the Data Feeds page which allows the recipient to review feed details before subscribing.



Data Feeds

Data Feeds are used to transmit threat intel data from one instance to another. You select a Data Collection to configure the information to share with other instances, determine the support context included with the intel, and select the instances to share this data with. You also have the ability to override the source of the Data Feed. After you create the feed, the recipients receive a system notification. They can then subscribe to the feed to begin receiving data from it.

> It is recommended that you allow your subscribers to connect to your instance before assigning a Data Feed. This allows your instance to push out the Data Feed immediately. If you assign a Data Feed to an instance that has yet to connect, the Data Feed will be pushed at the next frequency if there are new objects in the Data Feed.

You can manage feeds from the Data Feeds page and the Topology View. The Data Feeds page allows you to create/edit feeds and provides you with a comprehensive list of the Data Feeds you send (Outgoing Feeds) and the ones you receive (Incoming Feeds). Based on the Feed type, Outgoing or Incoming, you can perform different actions.

For incoming feeds, you can:

- Subscribe to/Unsubscribe from a Feed
- Specify Feed Ingestion Settings

For outgoing feeds, you can:

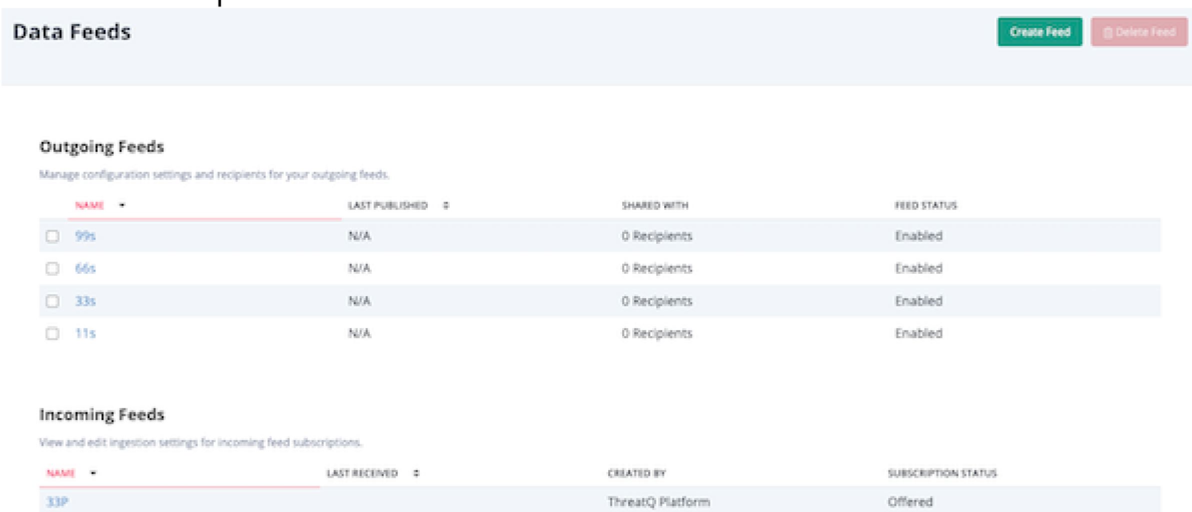
- Edit Feed Options
- Add Recipients
- Remove Recipients
- Delete a Feed

Creating a Data Feed

1. Click the **Data Exchange** icon in the top navigation bar of ThreatQ and select **Data Feeds**.

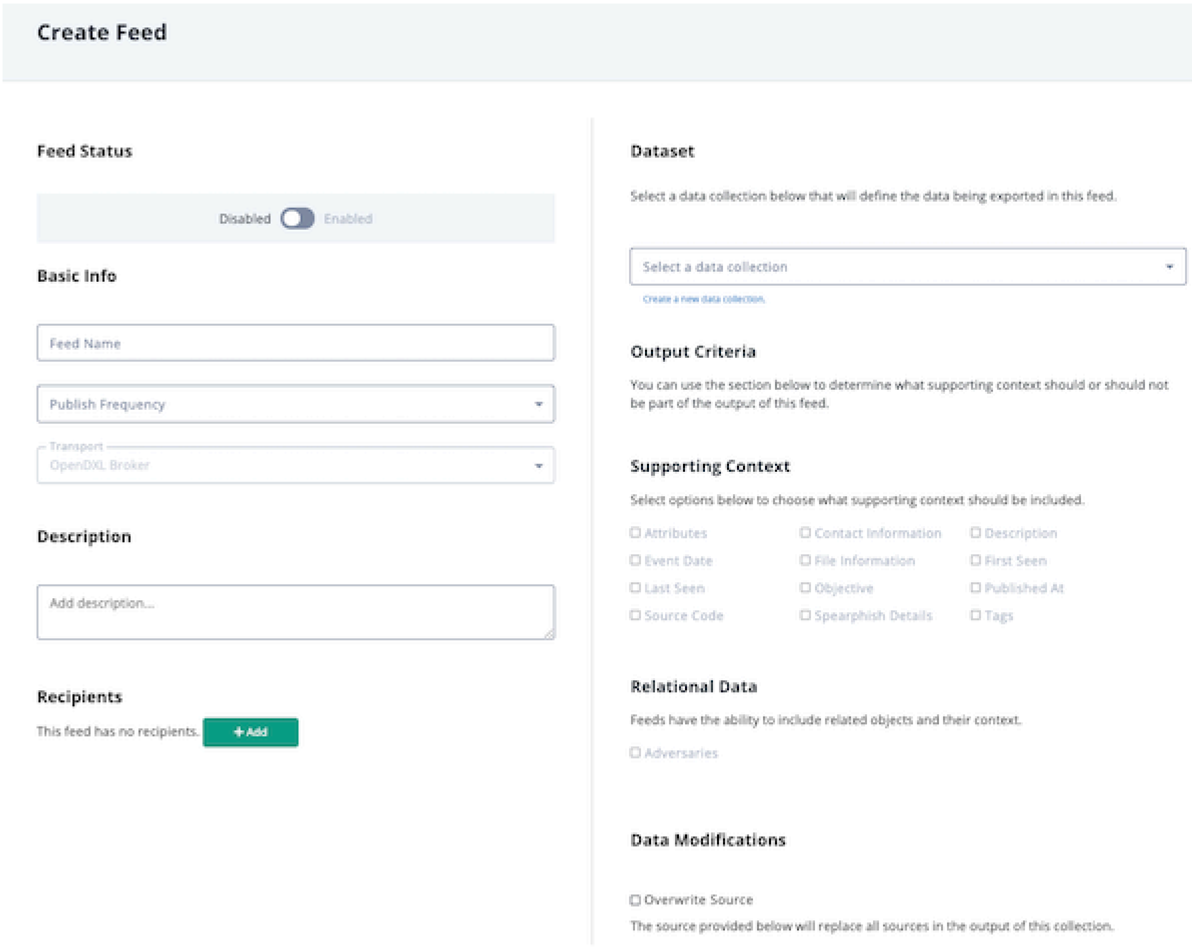
> You can also click the **Create Feed** button under the Outgoing Feeds pane in your Topology View after selecting your instance node. This will automatically load the Create Feed form in step 2.

The Data Feeds page loads. To make it easier to work with your active feeds, both the Incoming and Outgoing Feeds sections are sorted by feed status. With Enabled feeds listed at the top.



2. Click the **Create Feed** button.

   The Create Feed form loads. Both Publishers and Subscribers can create feeds. Publishers can make a feed available to all clients connected to the data transport. Subscribers can only share feeds with Publishers and do not have this option.



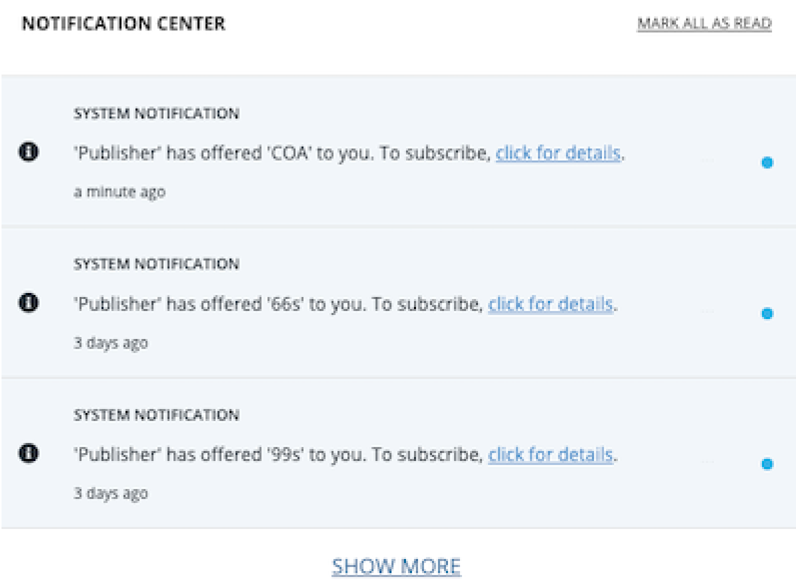
3. Populate the following form sections to specify the content and recipients of your feed:

SECTION	DESCRIPTION
Feed Status	Defaults to Disabled. Click the toggle to enable the feed.
Basic Info	• **Feed Name** - Enter the name you want to use for your feed. • **Publish Frequency** - Select Daily or Hourly depending on how often you want the feed to be published to Subscribers • **Transport** - At this time, you can only use the default transport provided by TQX. Additional transport options will

	be made available in future ThreatQ platform releases.
Description	Enter a brief description of the feed.
Recipients	If you are a Publisher, you can check the **Offer Feed to Public** box to give all clients connected to the Transport the option to opt into the feed. After you save your feed settings, the Recipients section displays the clients eligible to opt into the feed. **OR** If you are a Publisher or Subscriber, you can click the **+Add** button to access the Add Recipients window which lists all the connection bundles you created. Select a recipient and click **Add Recipient**. Subscribers do not have to be connected to be assigned to a Data Feed. The Subscriber will not receive the Data Feed connection profile or system objects until they have connected to the transport and subscribed to the feed.
Dataset	Select the Threat Library Data Collection to be exported with feed. **OR** Click the **Create a new data collection** option to open the Threat Library in a new tab and create a Data Collection.
Output Criteria	Select the supporting context that should be included in the feed using the checkboxes supplied. Only fields used in the data exported are selectable. Fields

	not associated with the data collection selected are greyed out. Check the **Adversaries** box to include related adversaries in the transfer. However, related attributes of the related adversary are not included.
Data Modifications	To override the default source name for the feed, check the **Overwrite Source** checkbox and enter the new source name. A Subscriber can view the Data Feed source name under object sources in their object details page.

4. Click the **Save** button.
   The recipients of the feed receive a system notification that a new feed is available for subscription. This notification includes a link to the Data Feeds page which allows the recipient to review feed details before subscribing.



Editing a Data Feed

The Edit Feeds page allows feed owners to edit a Data Feed. The Recipients section within this page also allows them to review information on feed recipients such as:

- **Client Name** - The recipients to whom you offered the feed.
- **Subscription Status** - Subscribed recipients are subscribed and actively receiving data from the feed. Offered recipients have been offered a feed but have not yet subscribed to it. Inactive recipients subscribed at one point and have since unsubscribed.

- **Last Received** - Date/time the recipient last received data from the feed.

There are two ways to edit a feed:

Method 1 - Data Feeds Link

1. Click the **Data Exchange** link in the top navigation and select **Data Feeds**.
2. Click a Data Feed in the Outgoing Feeds section to load the Edit Feed page.

Method 2 - Topology View

1. Click the **Data Exchange** link in the top navigation and select **Connections**.
2. Click your instance node in the Topology View.
3. Click the gear icon next to the feed under the **Outgoing Feeds** pane to open the Edit Feed page.

Subscribing to/Unsubscribing from a Feed

When you subscribe to a feed, your request enters a brief pending state until you receive an automatic confirmation from the feed publisher. When a subscription is pending, you can click the toggle icon to delete it. When you do this, the **Are you sure window?** prompts you to confirm the deletion.

Unsubscribing from a feed does not remove the objects you have already ingested nor does it reverse any source overrides applied to the feed.

Method 1 - Feed Ingestion Setting Page

1. From the Data Feeds page, click an Incoming Feed.
2. From the Feed Ingestion Settings page, click the **Unsubscribed/Subscribed** toggle to change your feed setting.
3. Click the **Save** button.

Method 2 - Topology View, Incoming Feeds

1. From the Connections page, click your local node in the Topology View.
2. In the Incoming Feeds section, click the gear icon next to the feed to which you want to subscribe.
   The Feed Ingestion Settings page is displayed.
3. Click the Feed Status toggle to subscribe to/unsubscribe from the feed.

4. Click the **Save** button.

Specifying Feed Ingestion Settings

The Feed Ingestion Settings page allows you subscribe to/unsubscribe from a feed and to change the status assigned to Indicators and Signatures ingested from a Data Feed from the default status of Review to a status of Active, Expired, Indirect, Review, or Whitelisted.

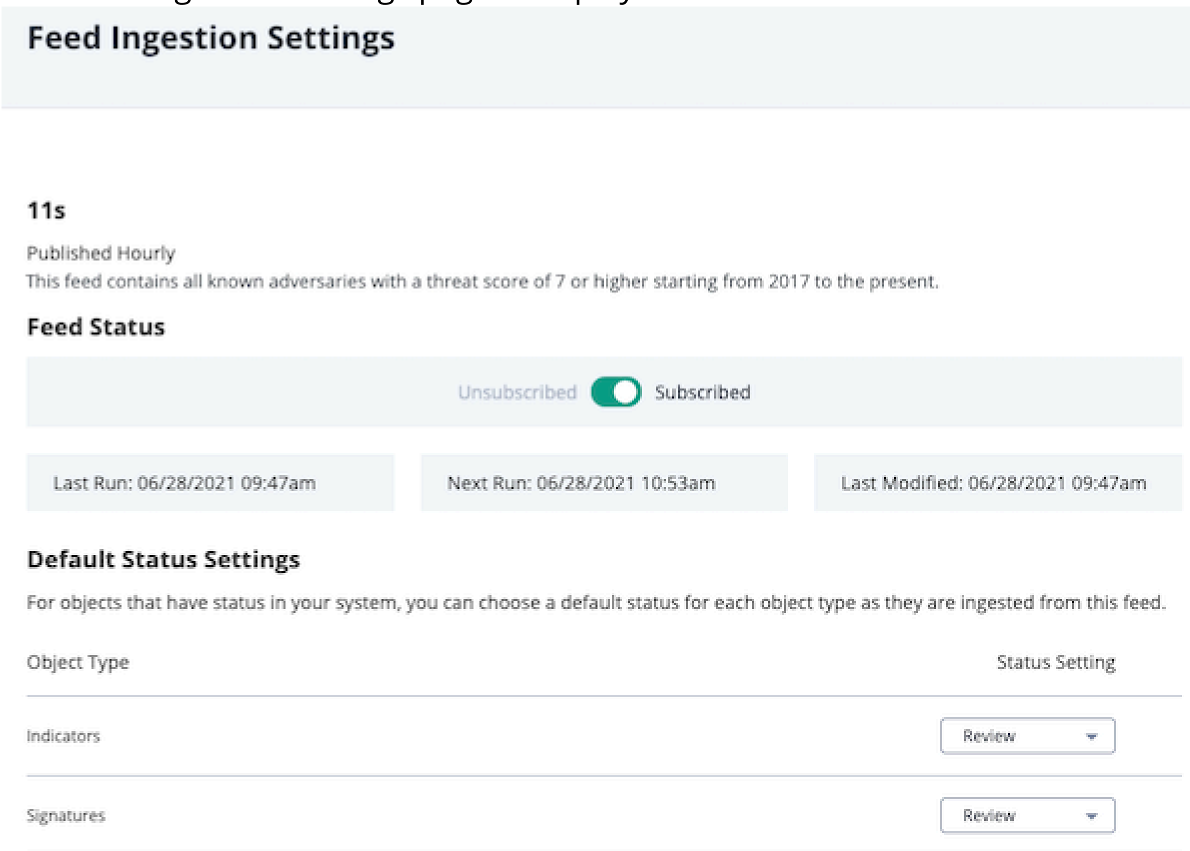
> if the Review status does not exist on the receiving instance, then the status type defaults to the first status in the list for that object type.

> If the status you assign to an Indicator or Signature is deleted, objects from the feed will not be ingested until the default status is updated from the Feed Ingestion Settings page for the feed.

Method 1 - Data Feeds Form

1. Click the **Data Exchange** link in the top navigation and select **Data Feeds**.
2. Click the Data Feed to edit to access the Edit Feed page.

3. In the Incoming Feeds section, click one of your incoming feeds.
   The Feed Ingestion Settings page is displayed.



4. Click the **Unsubscribed/Subscribed** toggle to subscribe to/unsubscribe from the feed.
5. In the Status Setting column, select a default status for ingested Indicators and/or Signatures.
6. Click the **Save** button.

Method 2 - Topology View

1. Click on the **Data Exchange** link in the top navigation and select **Connections**.
2. Click on your local node in the Topology View.
3. In the Incoming Feeds section, click the gear icon next to the feed you want to update.
   The Feed Ingestion Settings page is displayed.
4. Click the Feed Status toggle to subscribe to/unsubscribe from the feed.
5. In the Status Setting column, select a default status for ingested Indicators and/or Signatures.
6. Click the **Save** button.

Adding a Recipient

You can share a Data Feed with another instance if you are the owner of that feed.

Publishers can share feeds with other Subscribers. Subscribers can only share feeds with the Publisher.

Method 1 - Data Feeds Form

You can add recipients to your Data Feed from the Data Feeds form.

1. Click the **Data Exchange** link in the top navigation and select **Data Feeds**.
2. In the Outgoing Feeds section, click the Data Feed you want to edit to access the Edit Feed page.
3. Click the **Add** button and check the box next to the instance you want to add.
4. Click the **Add Recipient** button.

Method 2 - Topology View

1. Click the **Data Exchange** link in the top navigation and select **Connections**.
2. Click your transport node in the Topology View.
3. In the Client Discovery section, click an instance name to reveal its details.
4. Click the **Share Feed** button.
   The Share Feed Dialog box will open.
5. Select the feed to share with the instance and click on **Share Feed**.

> You also have the option to create a new feed by clicking the **Create New Feed** button to access the Create Feed page.

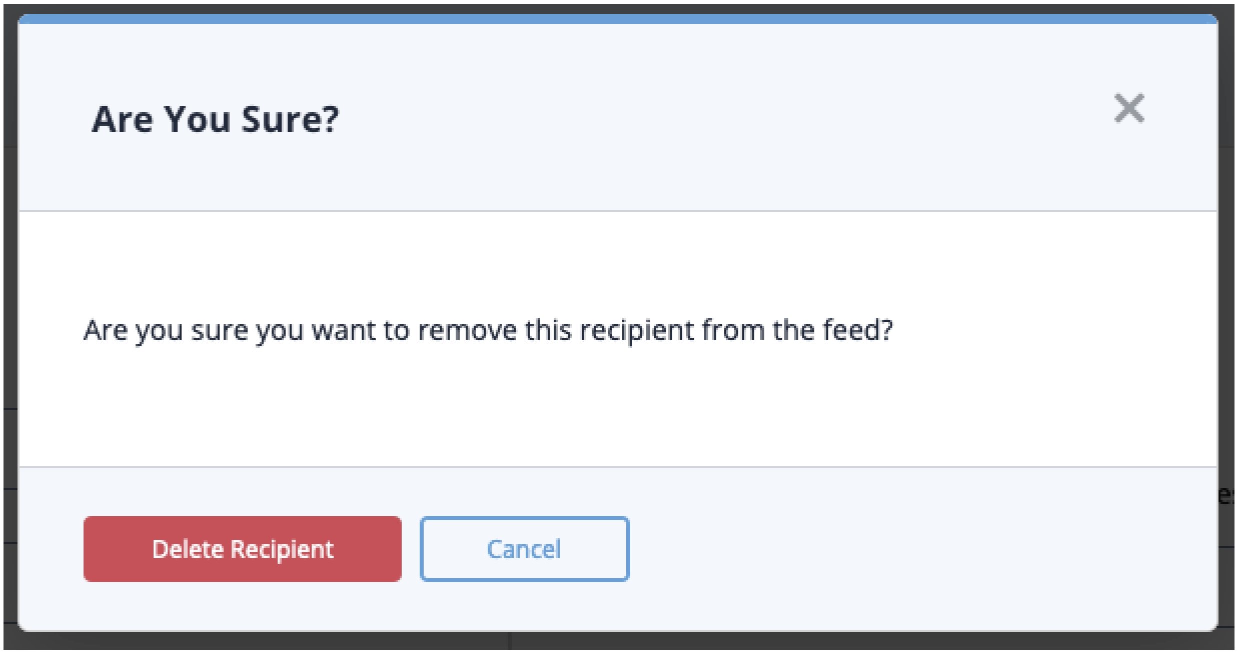
Removing a Recipient

Use the following steps to remove recipients with whom you are sharing your Data Feed.

Method 1 - Data Feeds Form

1. Click the **Data Exchange** link in the top navigation and select **Data Feeds**.
2. Click the Data Feed to access the Edit Feed page.
3. In the Recipients section, click the delete icon to the right of the recipient's name.

4. Click **Delete Recipient** when prompted to confirm removal.



Method 2 - Topology View - Subscriber Node

1. Click the **Data Exchange** link in the top navigation and select **Connections**.
2. Click the recipient's node.
3. Locate the feed to remove in the node's Outgoing Feeds section and click the delete icon.

4. When prompted, click the **Delete Feed** button, to remove the recipient from the feed.

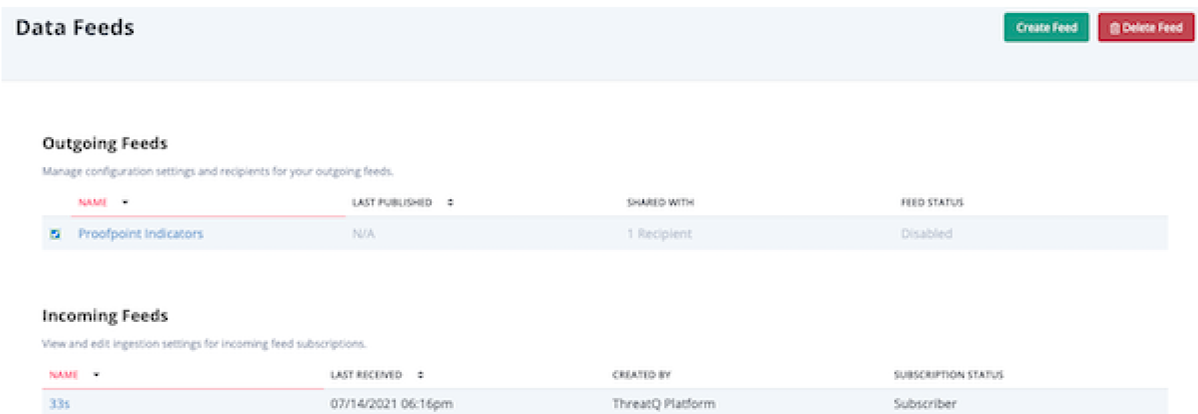
This will not delete the actual Data Feed. It will remove the instance from the feed's recipient list.

Deleting a Data Feed

The **Delete Feed** button in the Data Feeds page allows you to delete one or more feeds. However, you can only delete the feeds you have created.

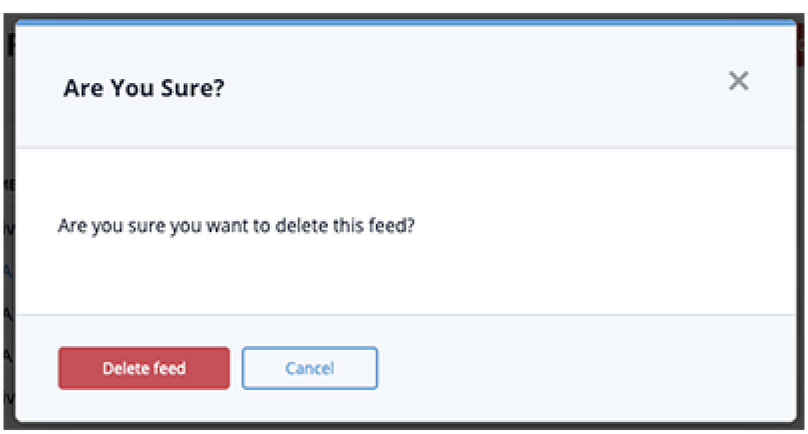
Method 1 - Data Feeds page (delete one or more feeds)

1. From the Outgoing Feeds section in the Data Feeds screen, check the box next to each feed you want to delete.



2. Click the **Delete Feed** button.

   The **Are You Sure?** window lists the number of feeds to be deleted and prompts you to confirm the deletion.



3. Click the **Delete feed** button.

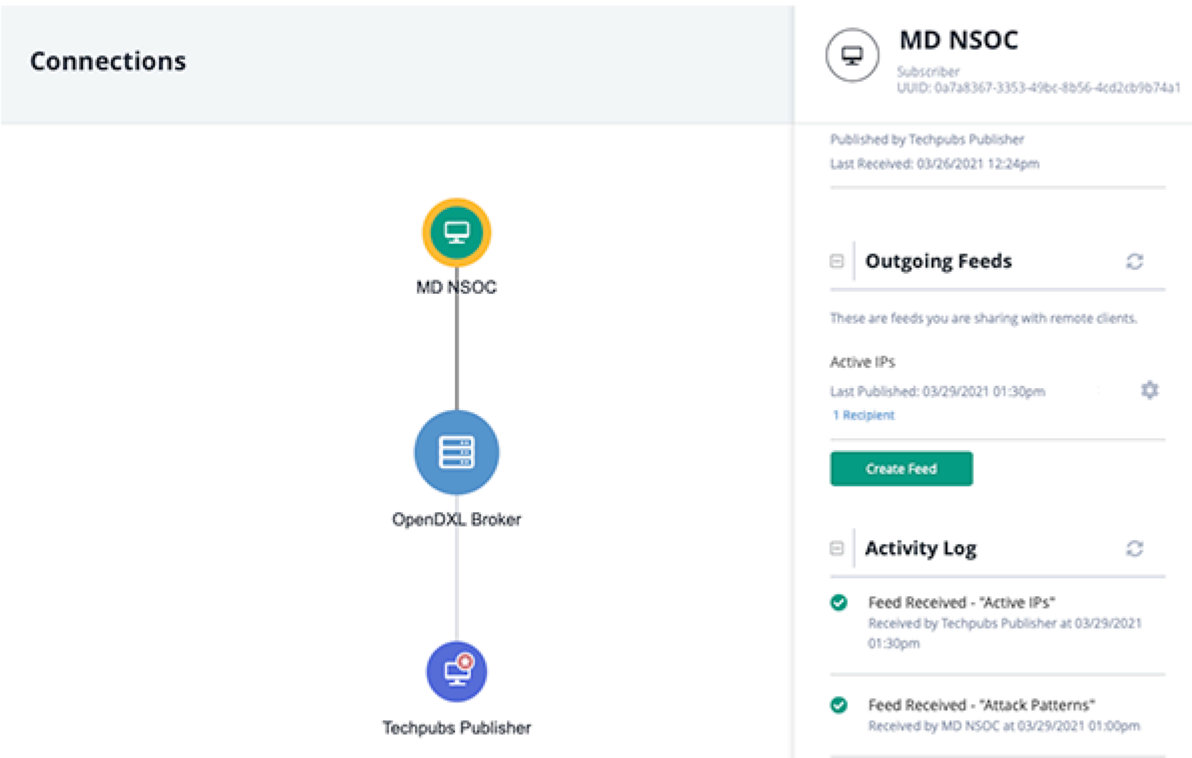
Method 2 - Edit Feed Page (Delete a Single Data Feed)

You can also delete a Data Feed from the Edit Feed page by clicking the **Delete Feed** button.

Topology View

You can access your instance's Topology View by clicking on the **Data Exchange** icon in the top navigation bar and selecting **Connections**.

The Topology View provides you with a node-based graph of your connections.



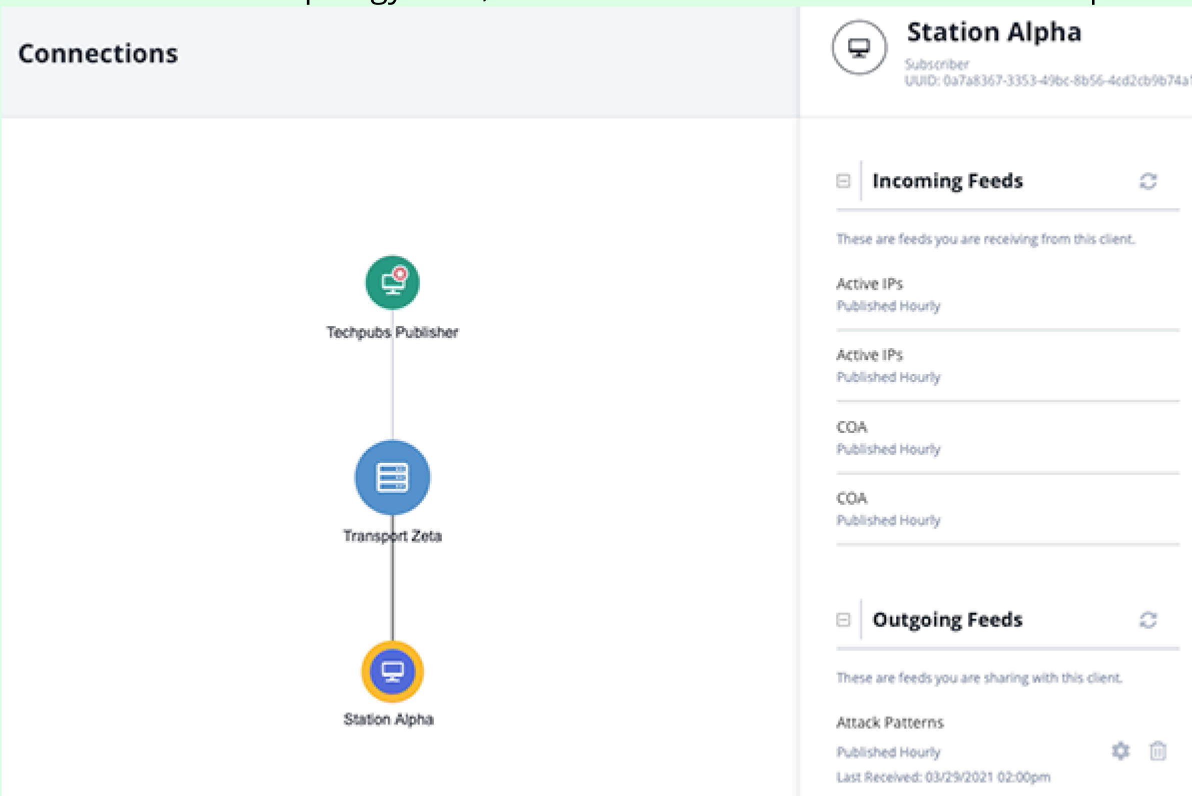
Clicking on a specific node allows you to view related information such as Data feeds you are sharing or receiving, an Activity Log, as well as the ability to create/download new and existing connection bundles (Publishers only).

Instance Naming

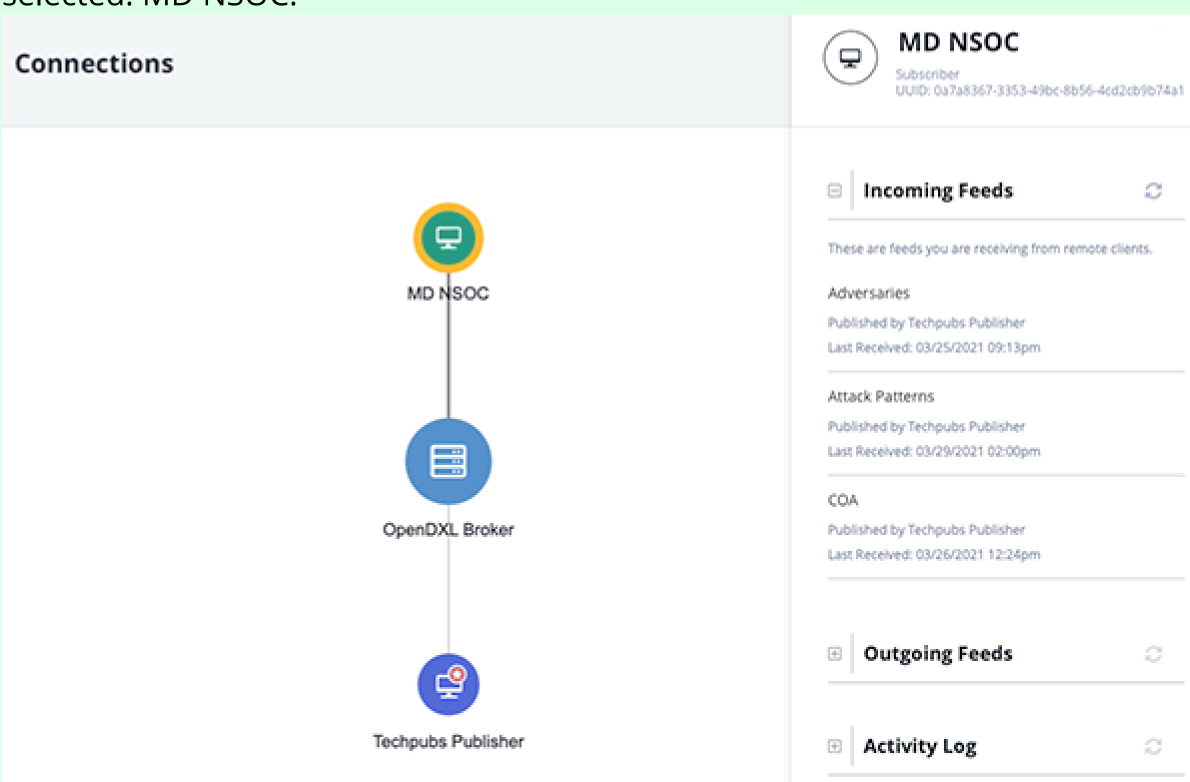
You can rename each node to your preference in order to easily identify other instances and transports in your view. This only affects your instance's Topology View. This allows each instance to use customized naming conventions without affecting other instances.

> The Publisher names an instance: Station Alpha when creating an integration bundle.
>
> The intended Subscriber will name his instance: MD NSOC.

In the Publisher's Topology View, the Subscriber will be named: Station Alpha



In the Subscriber's Topology View, the Subscriber will see the instance name he selected: MD NSOC.



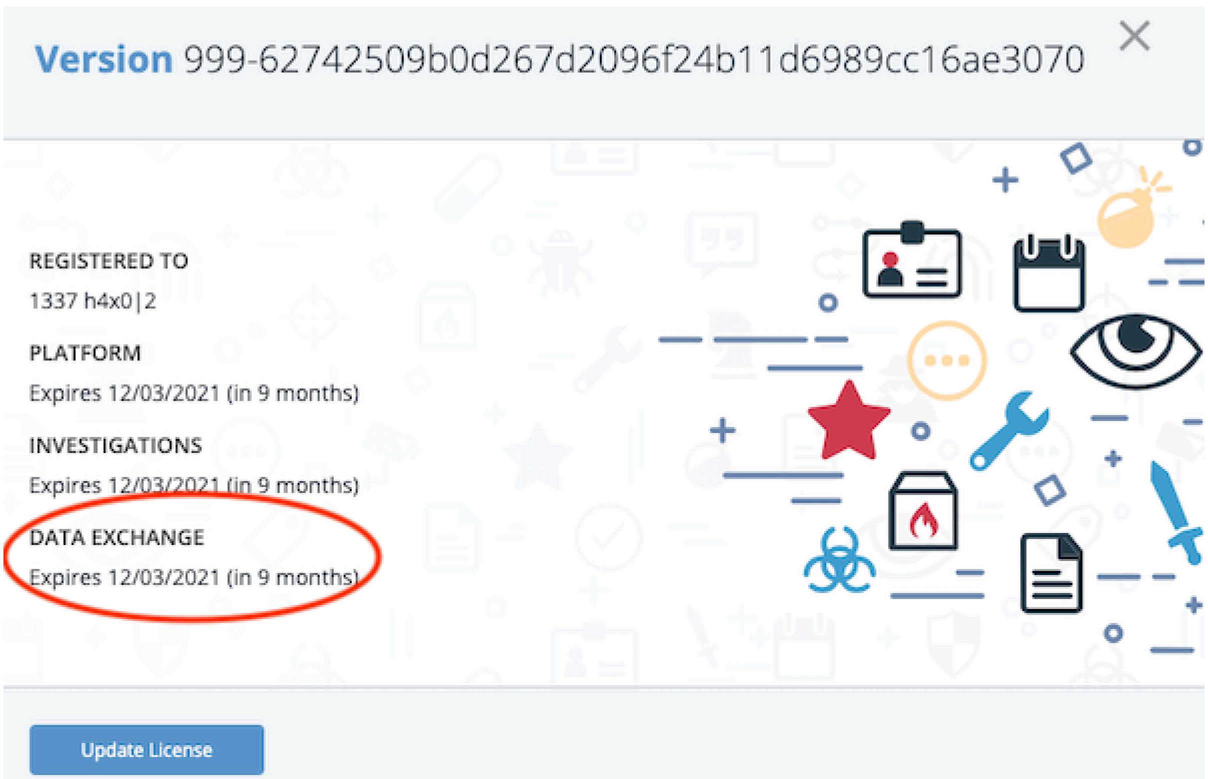
Actions

Depending on your instance types, there are various actions you can perform from the Topology View. See the Publisher Actions and Subscriber Actions topics for more details.

Instance Types

Your work in TQX is shaped by your user instance, Publisher or Subscriber. Your user instance defines the actions you can take and the information you can view. A Publisher has a TQ Broker license and can assign Data Collections to Subscribers. A Subscriber does not have a TQ Broker license and instead uses a standard ThreatQ license. A Subscriber can receive Data Collections from a Publisher and send Data Collections to the Publisher to be re-created and shared with other Subscribers. However, a Subscriber cannot assign Data Collections to other Subscribers.

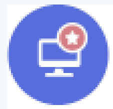
> To check your license status, click the gear icon in the upper right corner and select About. If your license window displays a Data Exchange license, you are a Publisher. If not, you are a Subscriber.



In addition to the user instances associated with individuals, the Data Transport is a OpenDXL transport method configured for sharing data between Publishers and Subscribers. It is the gateway through which the information in Data Feeds flows from Publisher to Subscribers and vice versa.

Icons

Even though the names assigned to Publisher, Client, and Data Transport nodes vary, you can quickly identify these nodes by their distinct icons.

	PUBLISHER VIEW	SUBSCRIBER VIEW
Publisher		
Subscriber		
Data Transport		

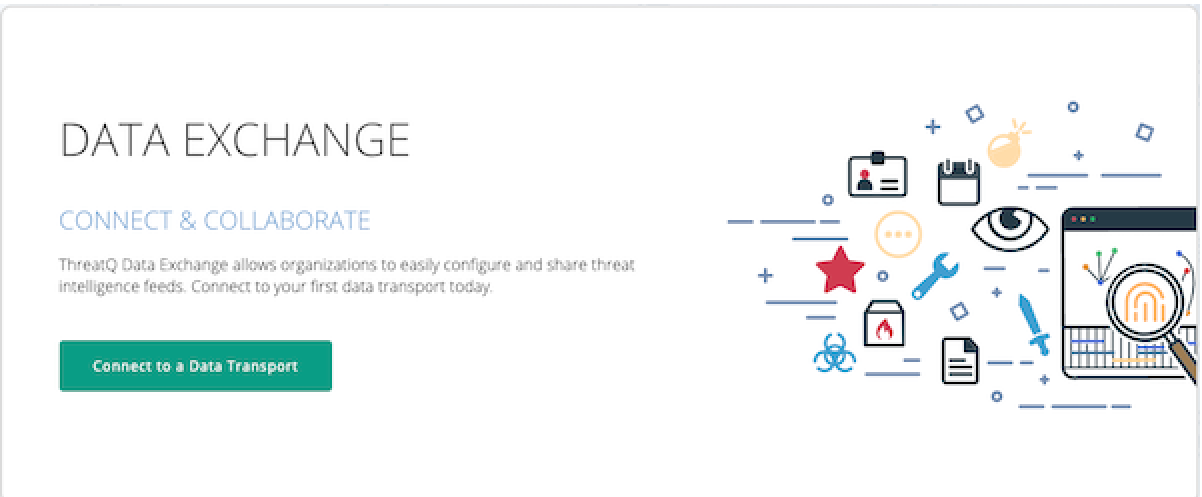
As shown above, icon color varies based on whether you are logged in as a Publisher or a Subscriber. However, the Publisher node is always stamped with a star in the upper right corner.

Tips and Tricks

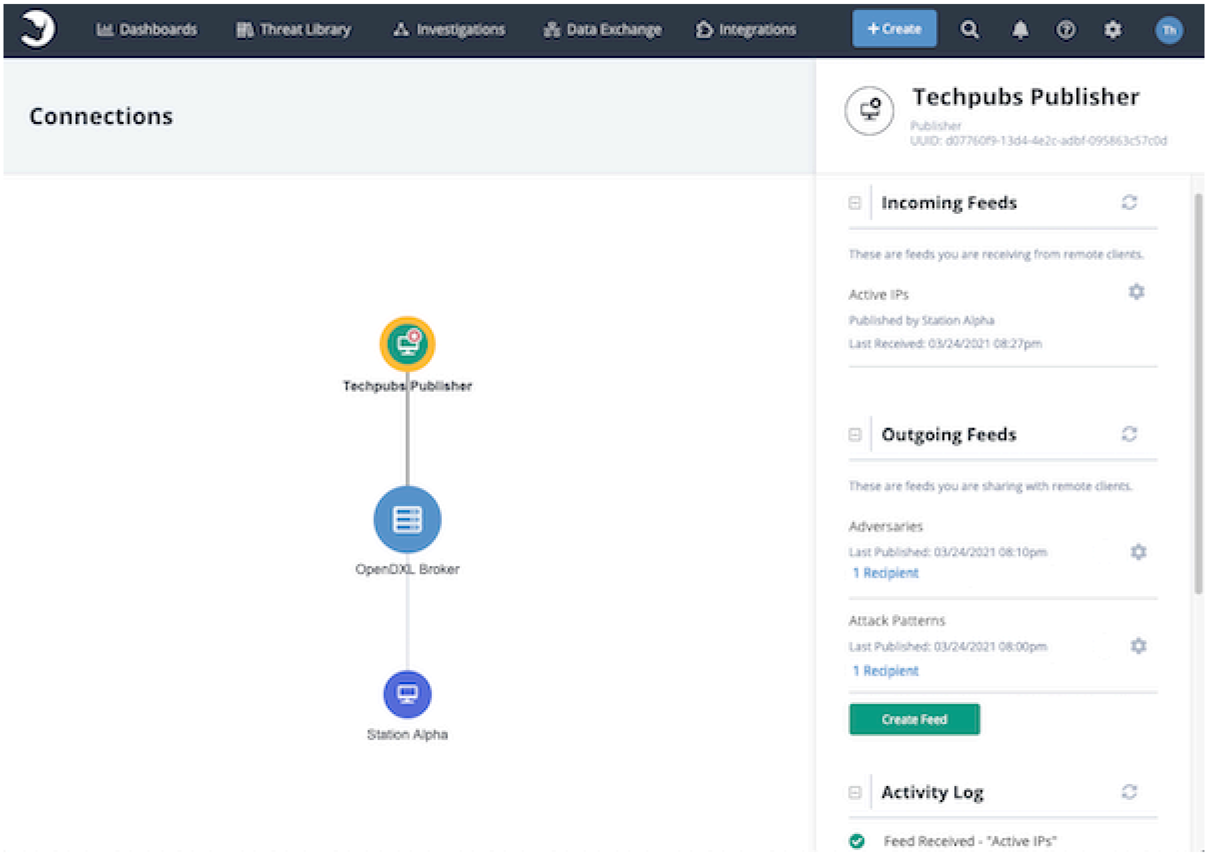
- Within the Connections screen, click the refresh button to refresh the data displayed.
- The Universally Unique Identifier (UUID) for each Publisher and Subscriber is displayed directly below the node name in the details panel. Publisher and Subscriber names can be changed, but this ID cannot.
- Changes to node names can take up to thirty seconds to display.
- You can use the scroll button on your mouse to zoom in and out on the Topology View in the Connections page.
- You can click and drag your Topology View to a different location in the Connections screen.
- You can click any node in the Topology View to view its details on the right side of the screen.

Publisher

Publishers are the driving force of TQX and this is reflected in the Topology View displayed in the Connections page. The first time a Publisher clicks an option on the Data Exchange menu, the Data Exchange wizard leads them through the process of setting up their first Subscriber(s). See the Getting Started - First Connections section for more information on setting up your first connection.



After the Publisher generates a Subscriber connection bundle and the Subscriber uploads it, the Topology View shows that the Publisher and Subscriber communicate via the Data Transport. In the following example, Techpubs Publisher can send Data Collections to Station Alpha via the OpenDXL Broker Data Transport.



Publisher Tasks

As a Publisher, TQX allows you to manage your shared feeds via the following tasks:

- View Your Outgoing and Incoming Data
- View Data Transport Details
- View Subscriber Details
- Update the Name of a Node
- Create a Client Connection Bundle
- Share a Data Collection with a Subscriber

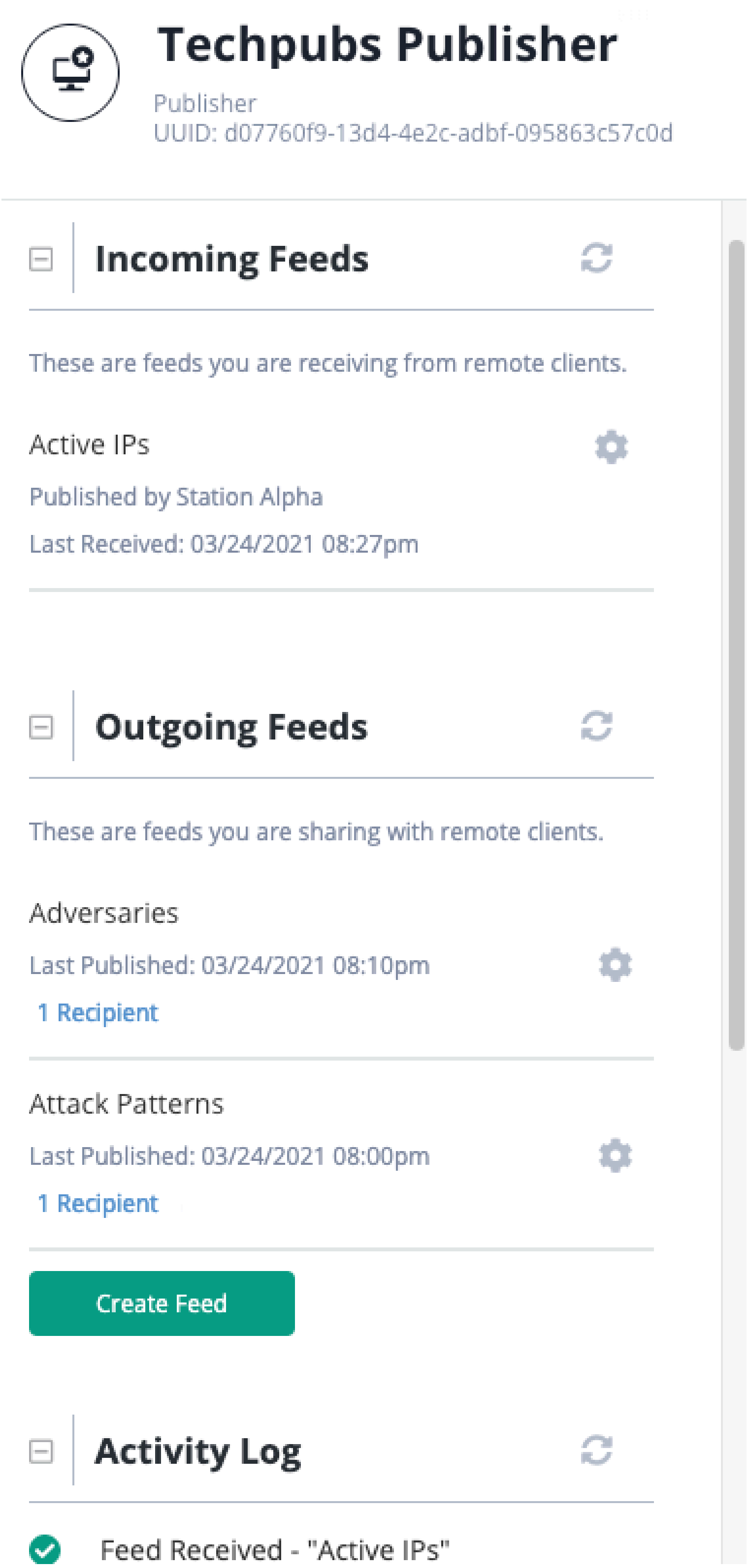
View Your Outgoing and Incoming Data - Publisher View

1. From the Connections screen, click the Publisher node.
   The right side of the screen displays a details panel including the following sections:

SECTION	DESCRIPTION	TASKS

Incoming Feeds	Lists the following information on feeds shared with you by a Subscriber: • Feed name • Publisher name • Date/time the you last received data from the feed	**Subscribe to a feed.** **Specify Indicator and Signature statuses for a feed.** See the Data Feeds topic for more information on these tasks.
Outgoing Feeds	Lists the Data Collections you have shared with Subscribers.	**View feed details.** - This section lists the date/time the feed was last published as well as the number of feed Subscribers. You can click the Recipients link to view the recipient names in the Edit Feeds page. **Edit a feed.** - Click the gear icon next to the feed name to access the Edit Feed screen. From this screen, you can: ◦ **Edit feed options.** - Enter your changes and click the Save button. ◦ **Delete a feed.** - Click the **Delete Feed** button. The **Are You Sure?** window prompts you to confirm the deletion by clicking the Delete Feed button. ◦ **Share a feed.** - Click the **Create Feed** button to access the Create Feed window and Share a Data Collection with a Subscriber.
Activity Log	Lists a time/date stamp and brief description for TQX activities such as your initial setup as a Publisher.	Click the **Show More** link to expand the activity log display.

2. Click the +/- button next to a section to expand/minimize details.



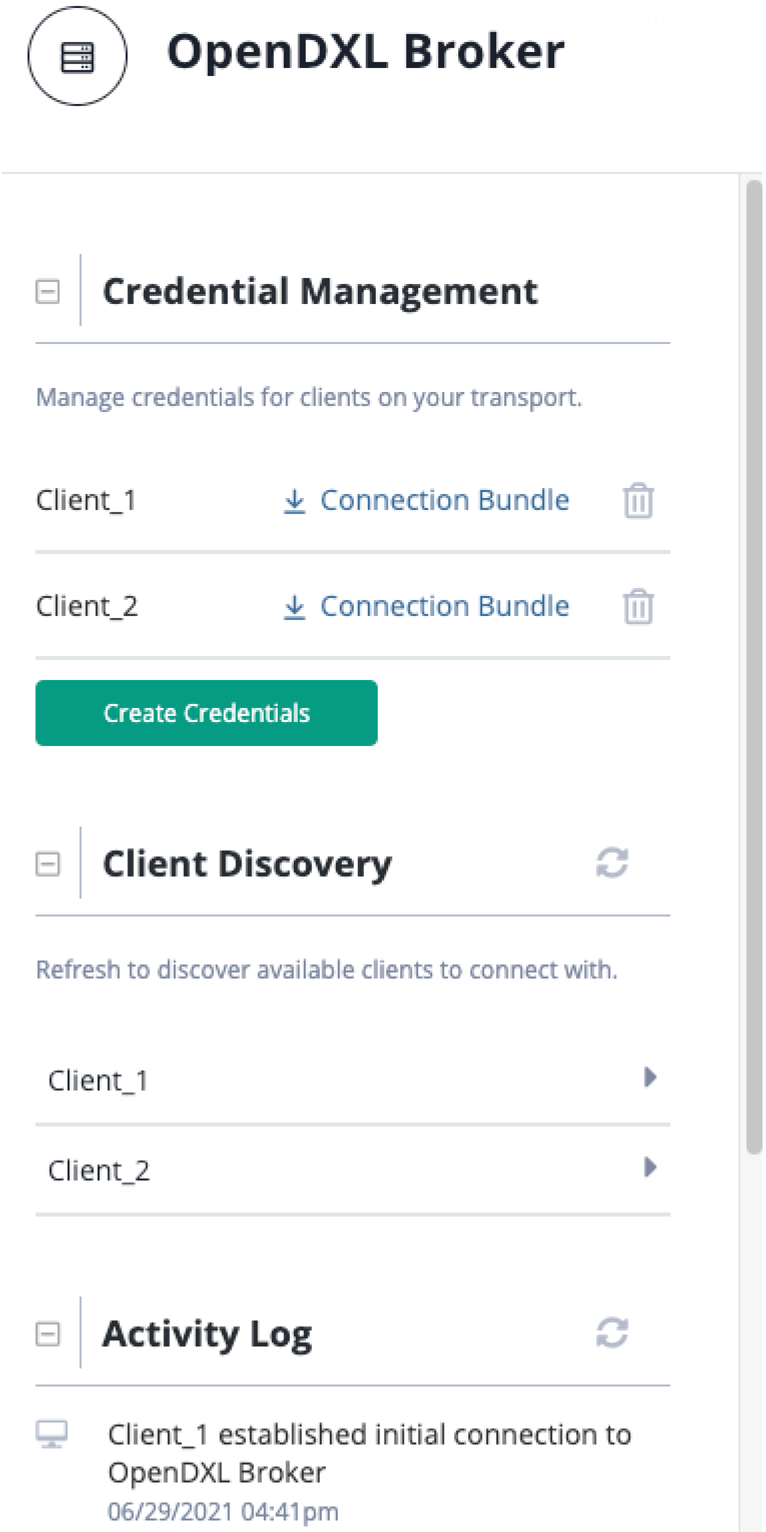
View Data Transport Details

1. From the Connections screen, click the Data Transport node.
   The right side of the screen displays a details panel including the following sections:

SECTION	DESCRIPTION	TASKS
Credential Management	Allows you to work with connection bundles for new or existing Subscribers connected to the Data Transport.	**Download a connection bundle.** - Click the Connection Bundle link next to the Subscriber name. **Delete a Subscriber's connection.** - Click the trashcan icon next to the Subscriber name to delete his connection to the data transport. **Create a connection bundle.** - See the Create a Client Connection Bundle section for more information on this process.
Client Discovery	Lists the Subscribers connected to the Data Transport and the Data Feeds they receive.	**View Subscriber feed details.** - Click the arrow next to the Subscriber name to view: • Feeds received by the Subscriber • Feed frequency (hourly or daily) • Date/time the Subscriber last received data from the feed **Remove a Subscriber from a feed.** - See the Data Feeds topic for more details. **Share/Create a feed.** - Click the Share Feed button to access the Share Feed window. From this window, you can: • **Share an existing feed.** - Click the checkbox next to an existing feed you want to share with the Subscriber. Then, click the Share feed button. • **Create a new feed.** - Click the Create New Feed button to access the Create Feed window and Share a Data Collection with a Subscriber.

Activity Log	Lists a time/date stamp and brief description for feed activities such as, the initial setup of the Publisher and Subscriber(s).	Click the **Show More** link to expand the activity log display.

2. Click the +/- button next to a section to expand/minimize details.

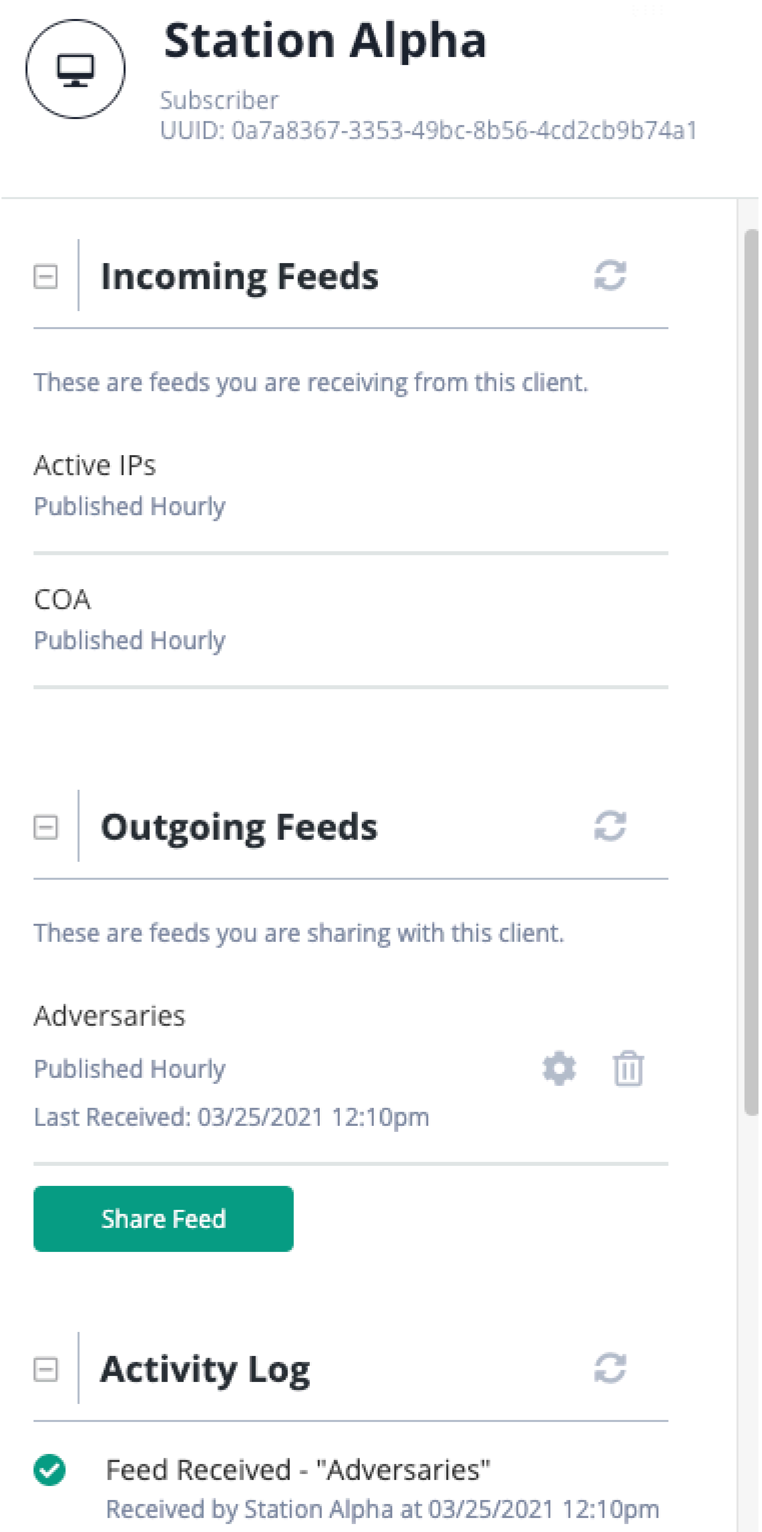


View Subscriber Details

1. From the Connections screen, click a Subscriber node.
   The right side of the screen displays a details panel including the following sections:

SECTION	DESCRIPTION	TASKS
Incoming Feeds	Lists feeds the Subscriber has shared with you.	
Outgoing Feeds	Lists the feeds you have shared with the Subscriber.	**Remove a Subscriber from a feed.** - See the Data Feeds topic for more details. **Edit a Data Feed.** - Click the gear icon next to the feed name to access the Edit Feed screen. From this screen, you can: • **Edit feed details.** - Enter your changes and click the Save button. • **Delete a feed.** - Click the Delete Feed button. The **Are You Sure?** window prompts you to confirm the deletion by clicking the Delete Feed button. **Share/create a feed.** - Click the Share Feed button to access the Create Feed window. From this window you can: • Click the Share Feed button to share an existing feed with the Subscriber. • Click the Create New Feed button to access the Create Feed window and Share a Data Collection with a Subscriber.
Activity Log	Lists a time/date stamp and brief description for feed activities such as, initial setup of the Subscriber.	Click the **Show More** link to expand the activity log display.

2. Click the +/- button next to a section to expand/minimize details.



Update the Name of a Node

TQX allows you to change the names of Publisher, Subscriber, and Data Transport nodes. Each Publisher and Subscriber node has a name and a Universally Unique Identifier (UUID).

Although you cannot change UUIDs, you can customize the names of the nodes in your Topology View.

1. From the Connections page, click the node's icon in the Topology View.
   The node details are displayed on the right side of the screen.
2. Click the node's name and enter your changes.
3. Click the checkmark on the right side of the field to save your change. TQX confirms your change with the following message: Node name updated.

> Name changes can take up to thirty seconds to update for all viewers.

Create a Client Connection Bundle

1. From the Connections page, click the Data Transport node. This triggers the display of the details panel on the right side of the Connections screen.
2. From the details panel, click the **Create Credentials** button in the Credential Management section to access the New Client window. Enter the new Subscriber's name in the Client Name field.
3. **Optional Step.** The Hostname field displays the name of your current TQX instance, however you have the option to update this name.
4. Click the Create Credentials button. The new Subscriber is displayed in the Credential Management section. From this point you can:
   - **Generate a connection bundle.** - Click the Connection Bundle link next to the client name to download the connection bundle. Send this file to the Subscriber to upload via their TQX instance.
   - **Delete the client.** - Click the trashcan icon next to the client name. Click the **Delete Client** button to confirm the deletion.

Share a Data Collection with a Subscriber

Both Publishers and Subscribers can create Data Feeds to share Data Collections. The only difference is that Publishers can share Data Feeds with Subscribers. Subscribers can only share a Data Feed with a Publisher.

1. Use one of the following methods to access the Create Feed page:
   - Click the **Create Feed** button in your Publisher details panel.
   - Click the **Share Feed** button in the Subscriber details panel to access the Share Feed window. Then, click the Create New Feed button.

- Select the Data Feeds option on the Data Exchange menu and click the **Create Feed** button.
- From the Client Discovery section in the Data Transport details panel, click the Subscriber name. Then, click the **Share Feed** button to access the Share Feed window and click the **Create New Feed** button.

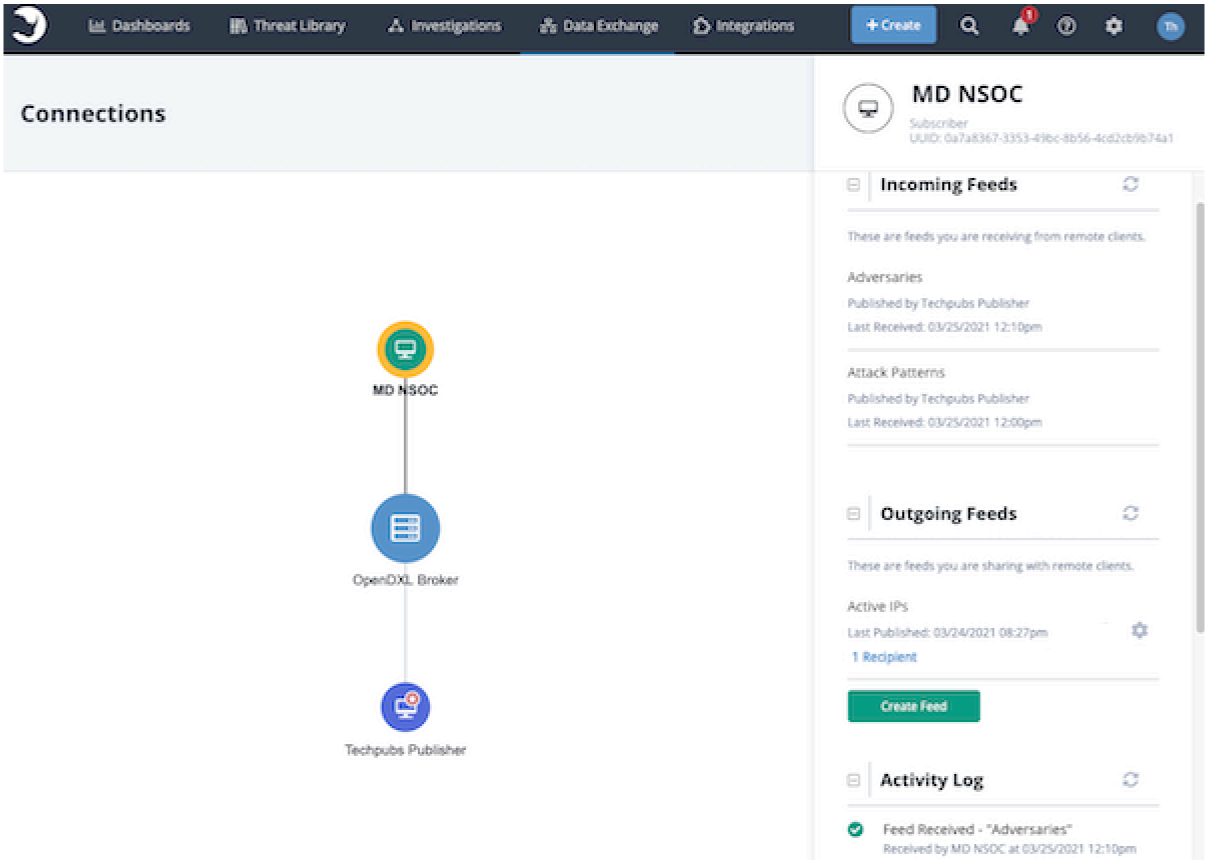
2. See the Data Feeds topic for more details on creating the Data Feed.

Subscriber

Subscribers benefit from the Data Collections created and sent to them by Publishers as Data Feeds. Although they can receive Data Feeds, they cannot send them to other Subscribers. However, they can send a Data Feed to the Publisher so the Publisher can recreate it and distribute it to other Subscribers.

The first time a Subscriber clicks an option on the Data Exchange menu, the Data Exchange wizard leads them through the process of setting up their first connection. See the Getting Started - First Connections section for more information on setting up your first connection.

After you set up a connection to a Publisher's Data Feed, the Connections screen displays the Topology View which provides a visual diagram of your relationship to the Data Transport and Publisher.



Subscriber Tasks

As a Subscriber, TQX allows you to manage your Data Feeds via the following tasks:

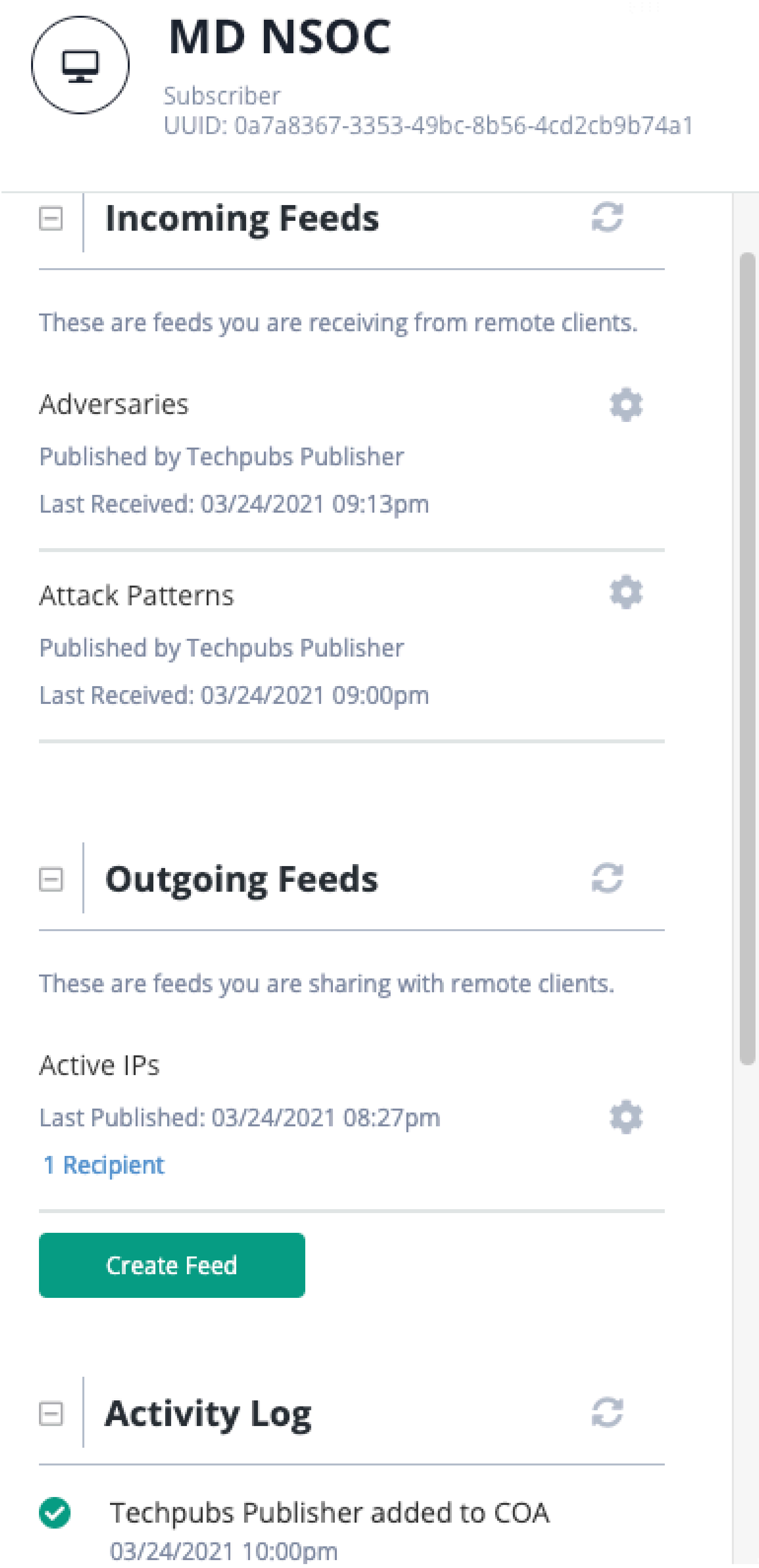
- View Your Incoming and Outgoing Data
- View Data Transport Details
- Delete a Data Transport
- Add a Data Transport
- View Publisher Details
- Update the Name of a Node
- Share a Data Collection with a Publisher

View Your Incoming and Outgoing Data - Subscriber View

1. From the Connections screen, click your Subscriber node.
   The right side of the screen displays a details panel including the following sections:

SECTION	DESCRIPTION	TASKS
Incoming Feeds	Lists the following information on feeds shared with you by a Publisher: • Feed name • Publisher name • Date/time the you last received data from the feed	**Subscribe to a feed.** **Specify Indicator and Signature statuses for a feed.** See the Data Feeds topic for more information on these tasks.
Outgoing Feeds	Lists the following information on feeds you have shared with a Publisher: • Feed name • Date/time the Publisher last received data from the feed • Publisher name	**View feed details** - This section lists the date/time the feed was last published as well as the number of feed Subscribers. You can click the Recipients link to view the recipient names in the Edit Feeds page. **Edit a feed.** - Click the gear icon next to the feed name to access the Edit Feed screen. From this screen, you can: • **Edit feed details.** - Enter your changes and click the **Save** button. • **Delete a feed.** - Click the **Delete Feed** button. The **Are You Sure?** window prompts you to confirm the deletion by clicking the **Delete Feed** button. **Share/create a feed.** - Click the **Share Feed** button to access the Create Feed window and Share a Data Collection with a Publisher.
Activity Log	Lists a time/date stamp and brief description for TQX activities such as your initial setup as a Subscriber.	Click the **Show More** link to expand the activity log display.

2. Click the +/- button next to a section to expand/minimize details.

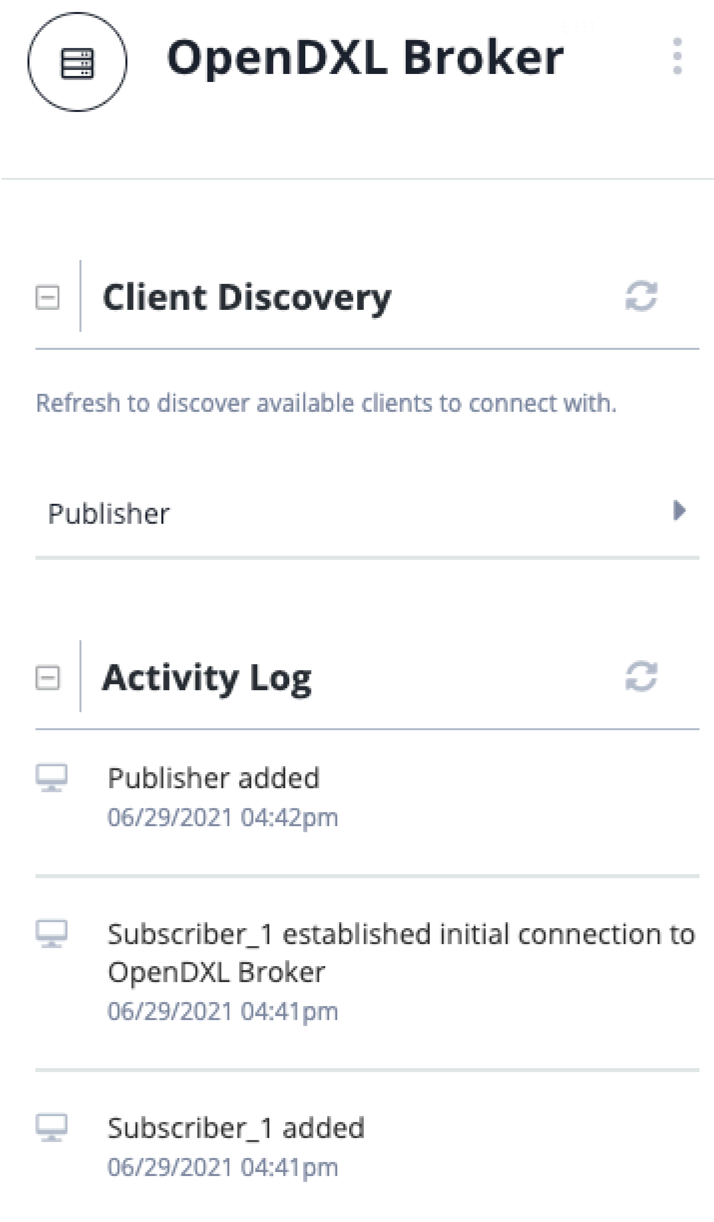


View Data Transport Details

1. From the Connections screen, click the Data Transport node.
   The right side of the screen displays a details panel including the following sections:

SECTION	DESCRIPTION	TASKS
Client Discovery	Lists the Publisher with whom you shared a Data Feed.	**View Publisher feeds.** - Click the arrow next to the Publisher name to view: • Feeds received by the Publisher • Feed frequency (hourly or daily) • Date/time the Publisher last received data from the feed(s). **Remove the Publisher from a Data Feed.** - See the Data Feeds topic for more details. **Update Data Feed options.** - Click the gear icon to access the Edit Feed window. After you enter your changes, click the **Save** button. **Share/Create a feed.** - Click the **Share Feed** button to access the Share Feed window. From this window, you can: • **Share an existing feed.** - Click the checkbox next to an existing feed you want to share with the Publisher. Then, click the **Share feed** button. • **Create a new feed.** - Click the **Create New Feed** button to access the Create Feed window and Share a Data Collection with a Publisher.
Activity Log	Lists a time/date stamp and brief description for TQX activities such as the receipt of a Data Feed by the Subscriber.	Click the **Show More** link to expand the activity log display.

2. Click the +/- button next to a section to expand/minimize details.



Delete a Data Transport

After you test a connection to a data transport, you may need to remove it. This halts your connection to the Data Feeds shared with you by the Publisher.

1. From the Connections screen, click the Data Transport node.
2. Click the vertical ellipses to the right of the Transport icon.
3. Select the **Delete Data Transport** option.
   The **Are You Sure?** window prompts you to confirm the deletion.
4. Click the **Delete Transport** button.
   The cleared Connections screen displays an **Add Data Transport** button

Add a Data Transport

If you have already completed the initial setup wizard used to add a data transport connection and then later deleted the data transport, the **Add Data Transport** button allows you to add a new data transport.

1. From a blank Connections screen, click the **Add Data Transport** button.
   The Add Data Transport window displays.
2. Use one of the following methods to add your connection file:
   - Drag and drop the file into the upload section.
   - Use the click to browse link to locate and upload the file.
3. Enter the name of the Data Transport in the Transport Name field.
4. Click the **Add Data Transport** button.
   The Topology View lists your Subscriber node and the new Data Transport node.

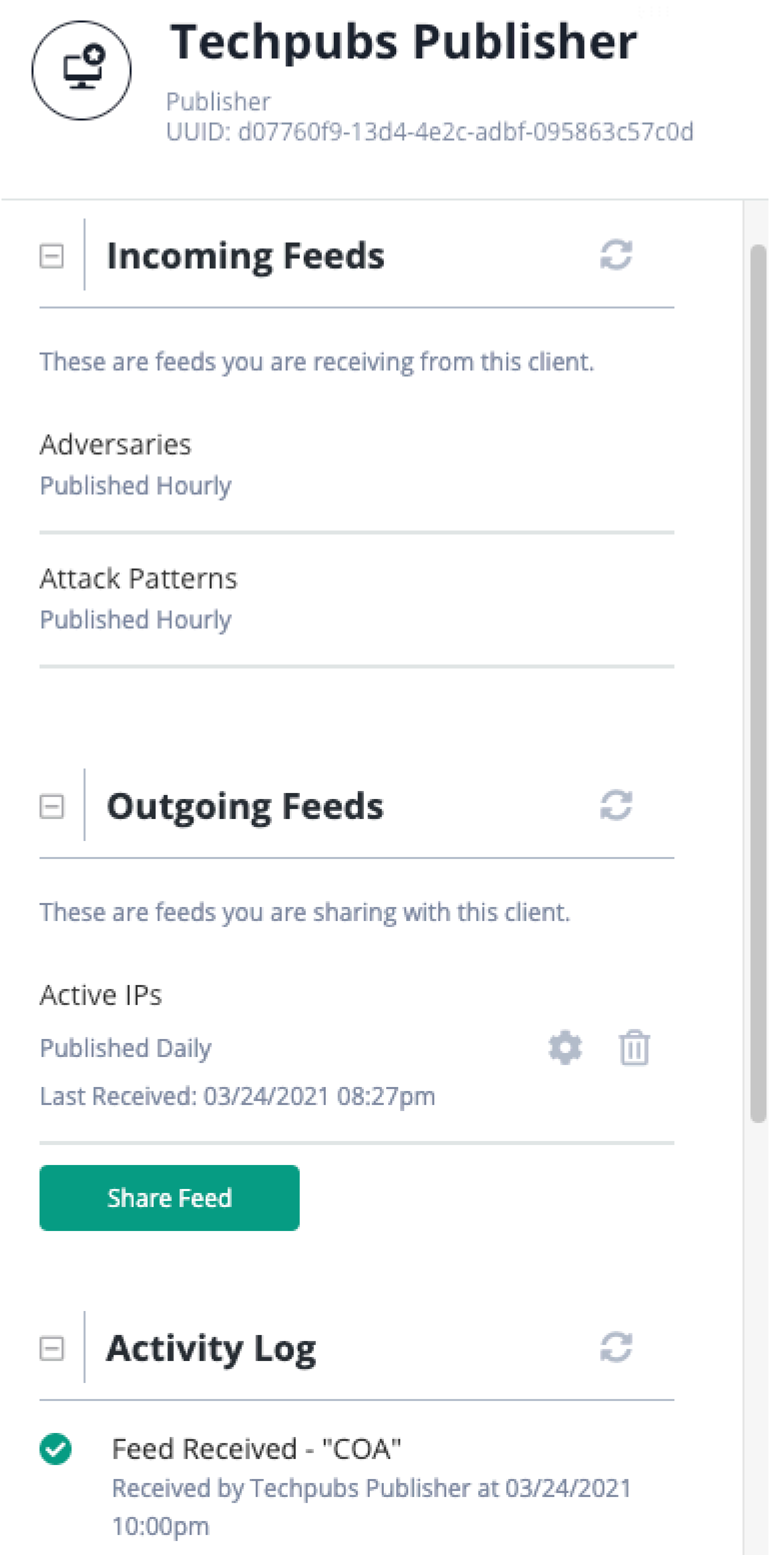
View Publisher Details

1. From the Connections screen, click the Publisher node.
   The right side of the screen displays a details panel including the following sections:

SECTION	DESCRIPTION	TASKS
Incoming Feeds	Lists the feeds this Publisher has shared with you as well as how often they are published.	
Outgoing Feeds	Lists the following information on feeds you have shared with a Publisher: • Feed name • Publication frequency (daily or hourly) • Date/time the Publisher last received data from the feed	**Remove the Publisher from a Data Feed.** - See the Data Feeds topic for more details. **Edit a Data Feed.** - Click the gear icon next to the feed name to access the Edit Feed screen. From this screen, you can: • **Edit feed details.** - Enter your changes and click the **Save** button. • **Delete a feed.** - Click the **Delete Feed** button. The **Are You Sure?** window

		warns prompts you to confirm the deletion by clicking the **Delete Feed** button. **Share/create a feed.** - Click the **Share Feed** button to access the Share Feed window. From this window, you can: • **Share an existing feed.** - Click the checkbox next to an existing feed you want to share with the Publisher. Then, click the **Share Feed** button. • **Create a new feed.** - Click the **Create New Feed** button to access the Create Feed window and Share a Data Collection with a Publisher.
Activity Log	Lists a time/date stamp and brief description for TQX activities such as the initial setup of the Data Feed you sent to the Publisher.	Click the **Show More** link to expand the activity log display.

2. Click the +/- button next to a section to expand/minimize details.


Techpubs Publisher
Publisher
UUID: d07760f9-13d4-4e2c-adbf-095863c57c0d
Incoming Feeds
These are feeds you are receiving from this client.
Adversaries
Published Hourly
Attack Patterns
Published Hourly
Outgoing Feeds
These are feeds you are sharing with this client.
Active IPs
Published Daily
Last Received: 03/24/2021 08:27pm
Share Feed
Activity Log
Feed Received - "COA"
Received by Techpubs Publisher at 03/24/2021 10:00pm

Update the Name of a Node

Each Publisher and Subscriber node has a name and a Universally Unique Identifier (UUID). Although you cannot change UUIDs, you can customize the names of the nodes in your Topology View.

1. From the Connections page, click the node's icon in the Topology View.
   The node details are displayed on the right side of the screen.
2. Click the node's name and enter your changes.
3. Click the checkmark on the right side of the field to save your change. TQX confirms your change with the following message: Node name updated.

> Name changes can take up to thirty seconds to update for all viewers.

Share a Data Collection with a Publisher

Both Publishers and Subscribers can create Data Feeds to share Data Collections. The only difference is that Publishers can share Data Feeds with Subscribers. Subscribers can only share a Data Feed with a Publisher.

1. Use one of the following methods to access the Create Feed page:
   - Click the **Share Feed** button in the Publisher details panel to access the Share Feed window. Then, click the **Create New Feed** button.
   - Click the **Create Feed** button in your Subscriber details panel.
   - Select the Data Feeds option on the Data Exchange menu and click the **Create Feed** button.
   - From the Client Discovery section in the Data Transport details panel, click the Subscriber name. Then, click the **Share Feed** button to access the Share Feed window and click the **Create New Feed** button.
2. See the Data Feeds topic for more details on creating the Data Feed.

FAQs

Can I install/use my own data transport?

Currently, TQX only supports the default OpenDXL transport installed with the product. However, future releases will give you the option to implement additional Data Transports.

As a Subscriber, can I offer a Data Feed to another Subscriber?

Subscriber instances can offer Data Feeds to Publishers. However, they cannot offer Data Feeds to other Subscribers. For added security, Subscribers will be unable to see other Subscribers connected to the Publisher.

What happens if my Data Feed contains indicators with a custom status that a Subscriber does not have in place on their instance?

At this time, custom statuses are not supported by TQX. In this event, the custom status would not be created on the Subscriber instance nor would the system objects with that status be ingested by the Subscriber instance.

What happens if my Data feed contains indicators with a set score?

Indicator Scores are not included when sending Data Feeds to another instance.

As a Subscriber, can I unsubscribe to a data feed?

Yes. You can unsubscribe from a data feed to stop the ingestion of data. You also have the option to re-subscribe to the data feed at a later date.

As a Subscriber, can I connect to multiple Publishers?

Currently, TQX only supports one data transport per instance. This allows Publishers to connect to multiple Subscribers through one data transport. Subscribers cannot connect to multiple Publishers as it would require additional data transports.

As a Publisher, can I connect to other Publishers?

No, at this time, data connection bundles are designed to provide Publisher > Subscriber and Subscriber > Publisher communication.

As a Publisher that is publishing multiple Data Feeds to a Subscriber, can I remove an individual data feed?

Publishers can remove recipient instances from Data Feeds. See the Data Feeds topic for more information.

How do I upgrade to a Publisher instance?

Contact ThreatQ Sales to purchase a Publisher license. Then, see the Licensing topic in the Help Center for information on adding this new license.

Change Log

- **Version 1.4.0**
  - Updates for version 4.54
- **Version 1.3.0**
  - Updates for version 4.53
- **Version 1.2.0**
  - Updates for version 4.52
- **Version 1.1.0**
  - Updates for version 4.50
- **Version 1.0.0**
  - Initial Release