ThreatQuotient

ThreatQ Data Exchange User Guide

Version 3.1.0

December 06, 2023

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

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

Contents

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.

About ThreatQ Data Exchange

ThreatQ Data Exchange (TQX) allows you to share threat intelligence via an OpenDXL data transport and/or a TAXII server.

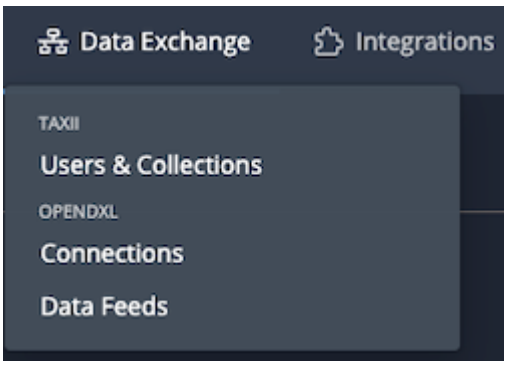
An OpenDXL data transport enables bi-directional sharing of threat intelligence across multiple ThreatQ instances. Using this transport type, Publisher and Subscriber instances share threat intelligence information specified within Threat Library Data Collections.

The TAXII server supports uni-directional sharing of threat intelligence where threat intelligence data specified within a Threat Library Data Collection is formatted as a STIX file and made available to individuals/organizations via a TAXII server. TQX allows you to generate and manage credentials that control access to the TAXI server.

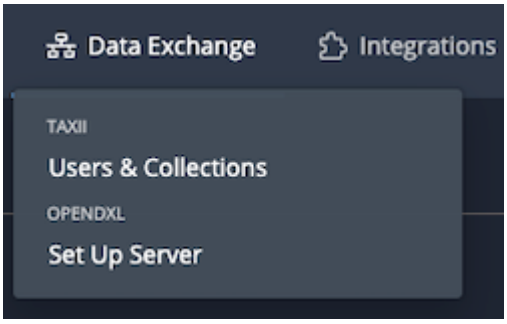
TQX Navigation

The TQX menu is divided into two sections, TAXII and OpenDXL, to provide easy access to OpenDXL data transport and TAXII server pages. The TQX menu options change based on which options you have already configured.

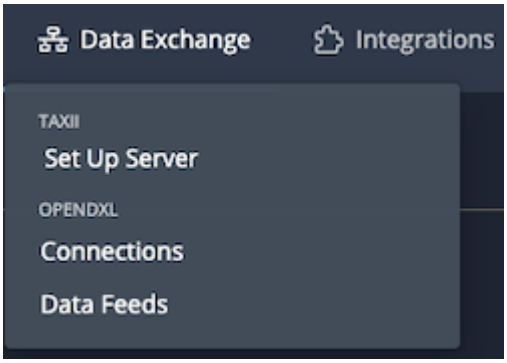
TAXII Server and OpenDXL Transport Configured



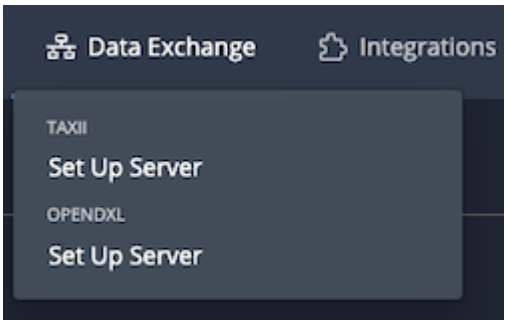
TAXII Server Configured



OpenDXL Transport Configured



Neither TAXII Server nor OpenDXL Transport Configured

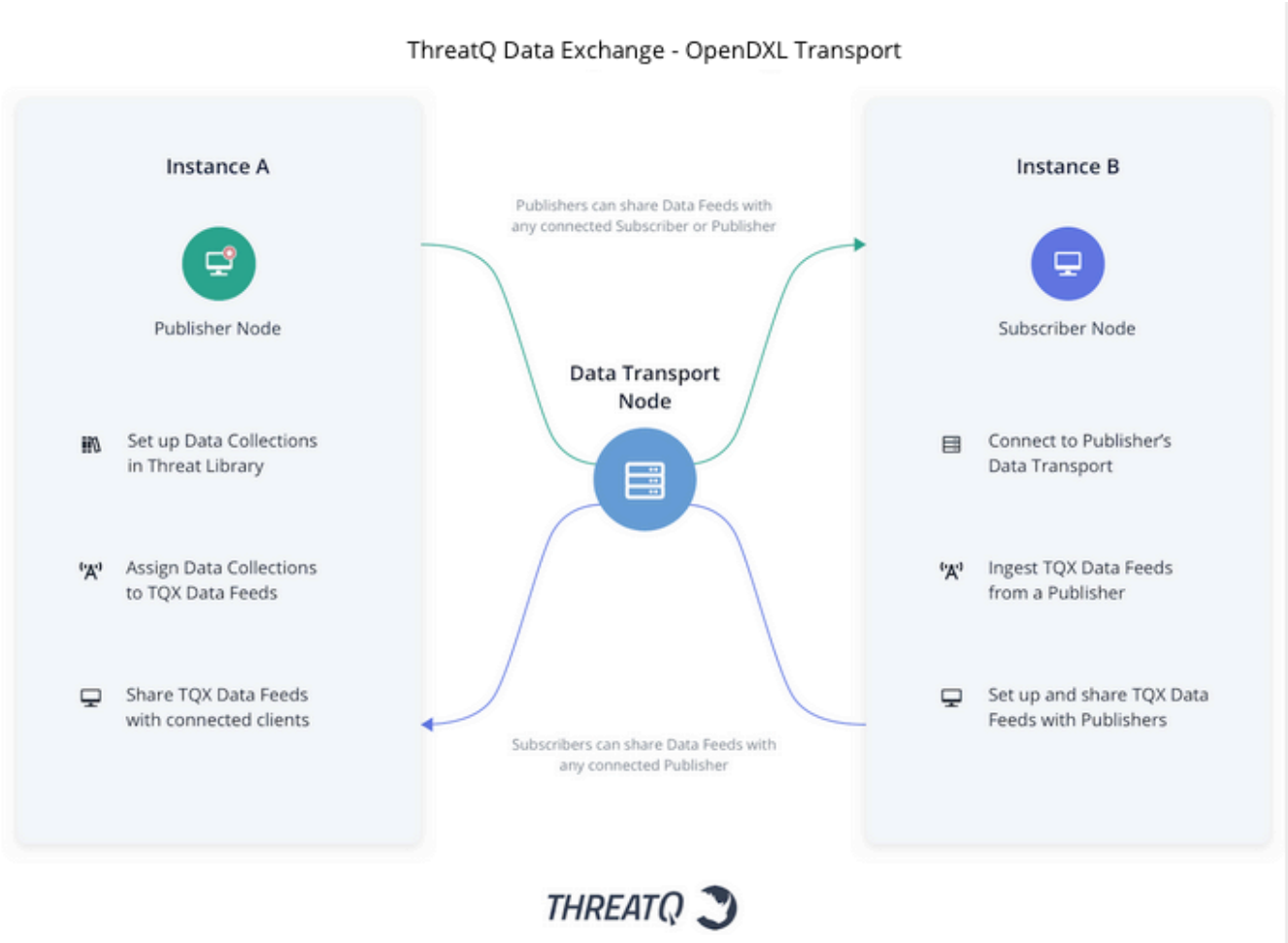


OpenDXL Transport

About OpenDXL Data Transport

OpenDXL data transport 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 Subscriber s. These Subscribers can analyze the data they ingest and provide feedback to the Publisher via a new Data Feed.

How It Works



Instance Types

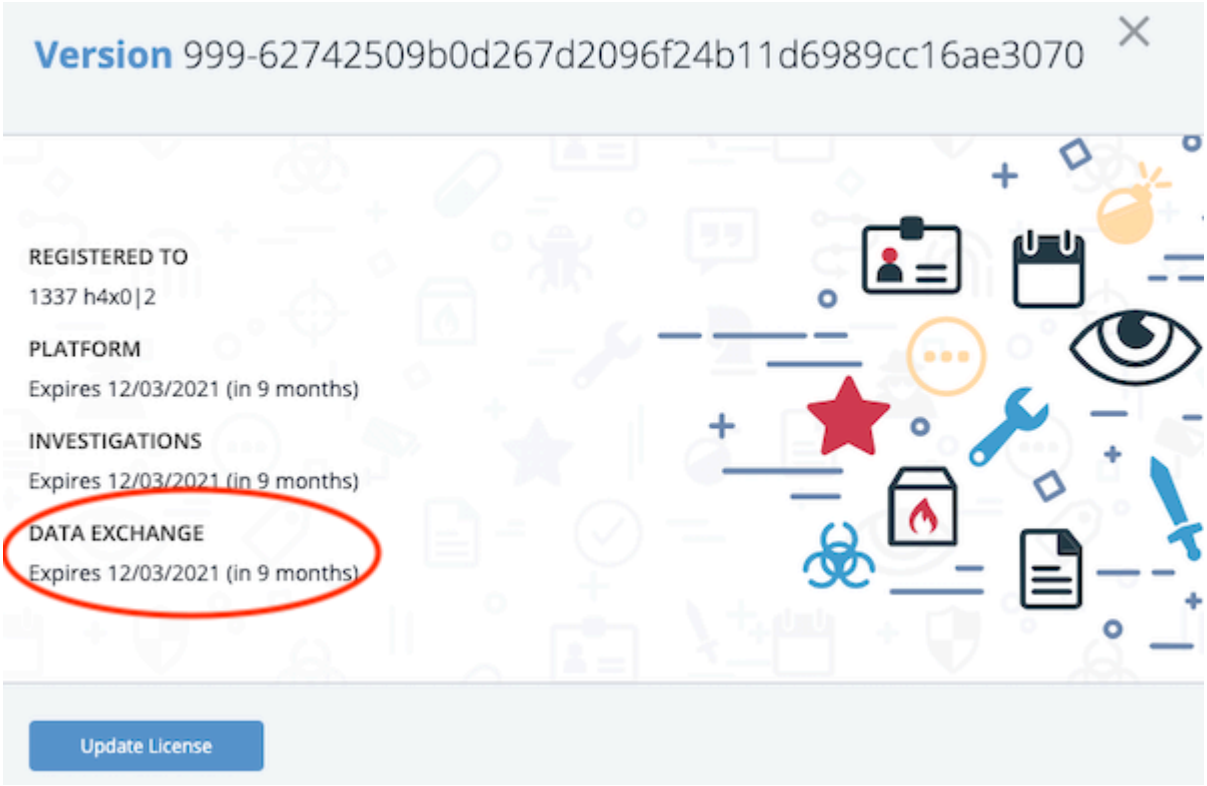
There are two different types of OpenDXL data transport instances available: Subscriber and Publisher.

Upgrading an instance to a Publisher license allows you to create Data Connection Bundle s, which are used to create Data Connections with Subscribers. Once connected to a Subscriber, you can send and receive system objects in the form of Data Feeds. See the Publisher section for further information.

> You will need at least one Publisher instance in order for an OpenDXL Transport.

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 section for further information.

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



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 OpenDXL Data Transport Connections topic, and the Publisher and Subscriber sections 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 OpenDXL data transport.

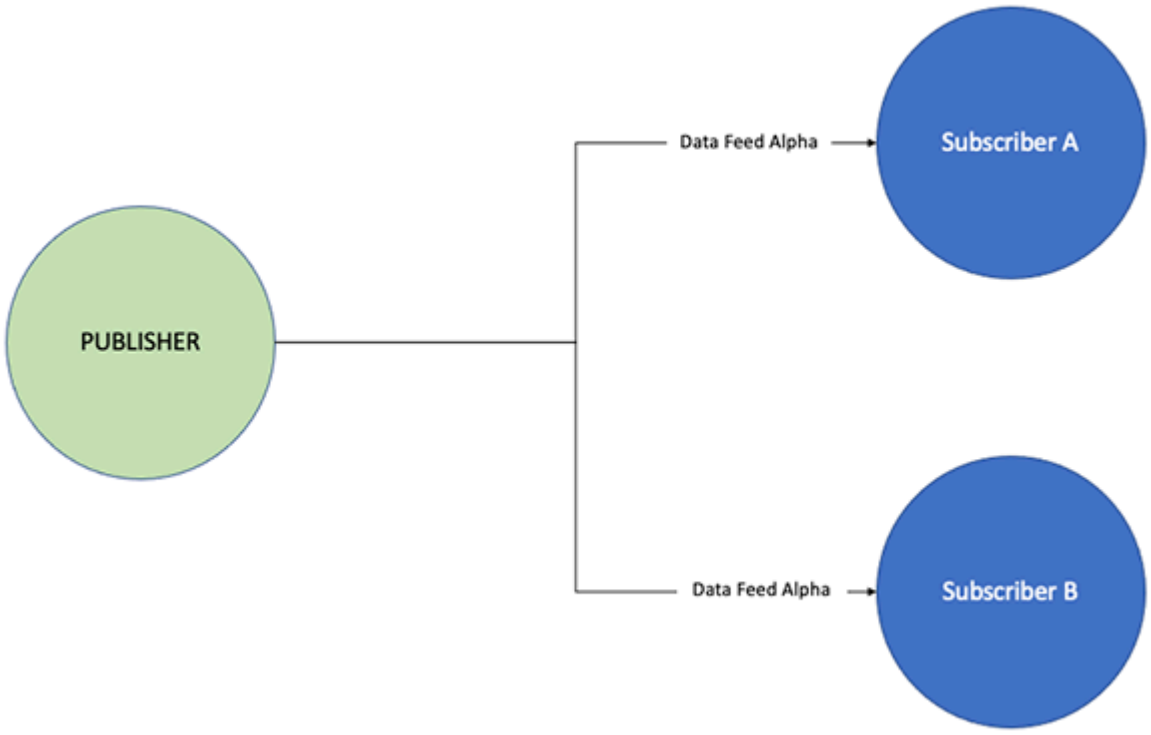
A Publisher can use a saved Data Collection from the ThreatQ Threat Library to create a Data Feed. That Data Feed can be offered to one or more recipients, which can be Subscribers or Publishers, for subscription. Once a recipient subscribes to the Data Feed, he receives data from it at a user-defined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

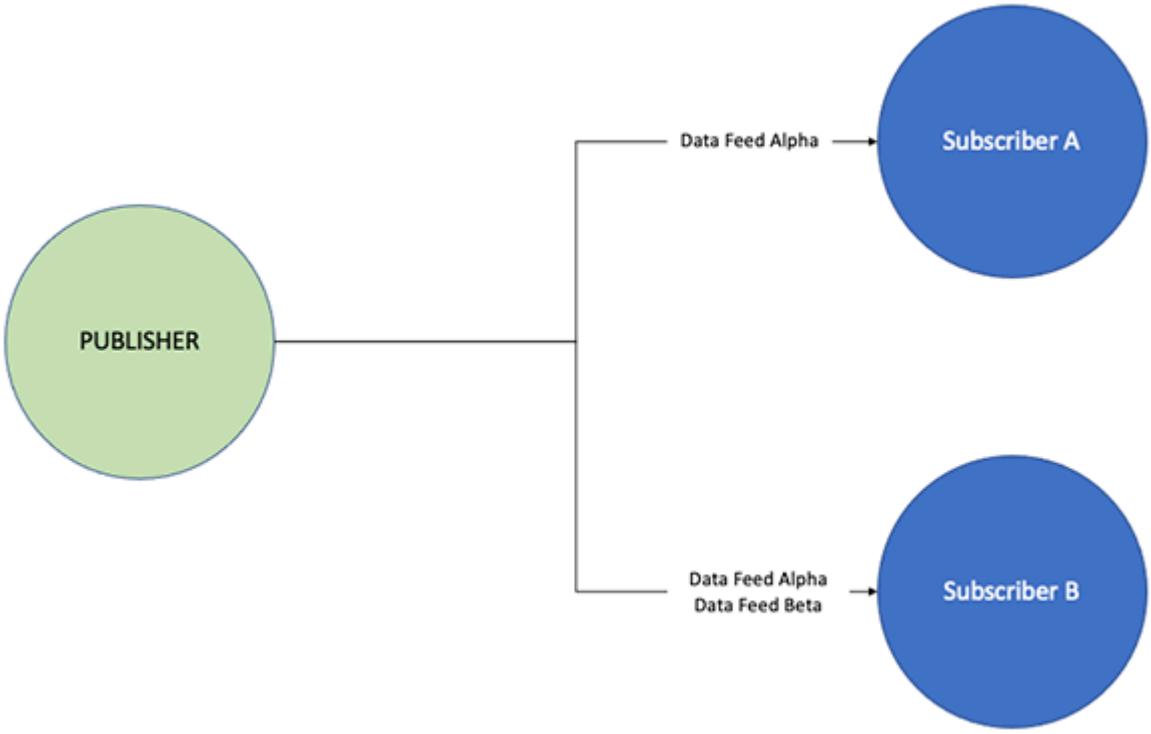
Example - One Publisher, Two Subscribers

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.



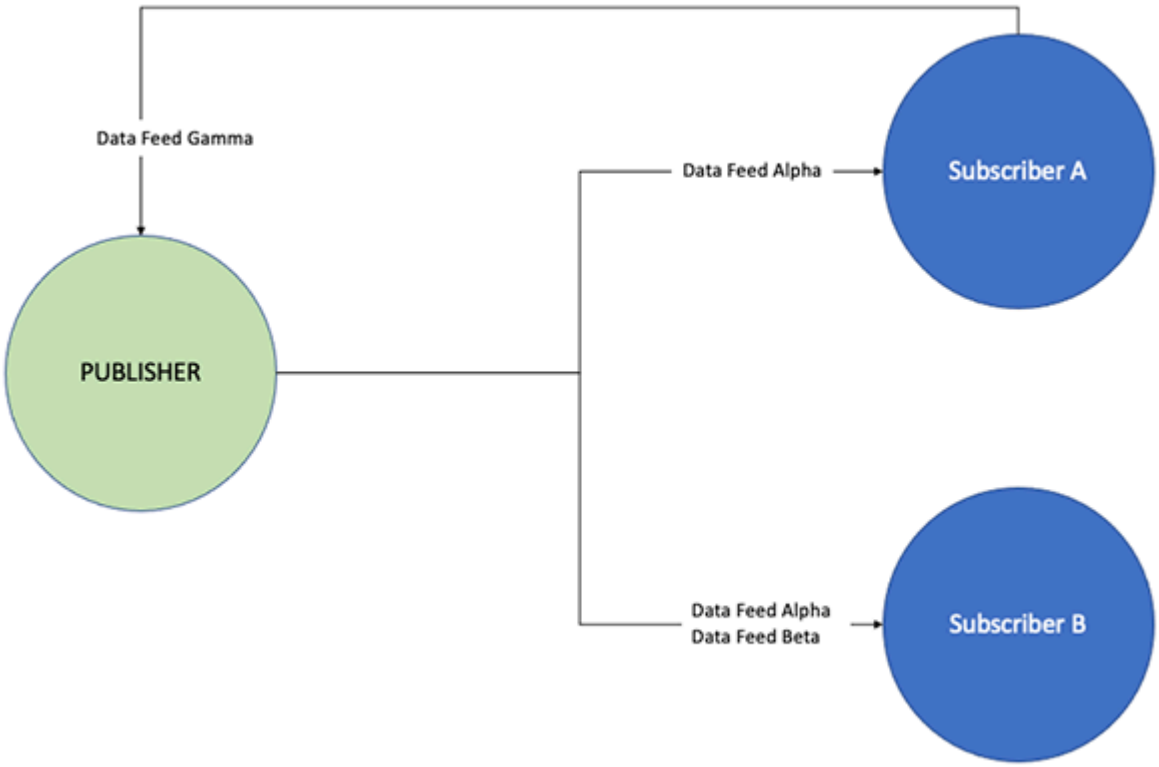
Example - One Publisher, Two Subscribers with Different Data Feeds

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

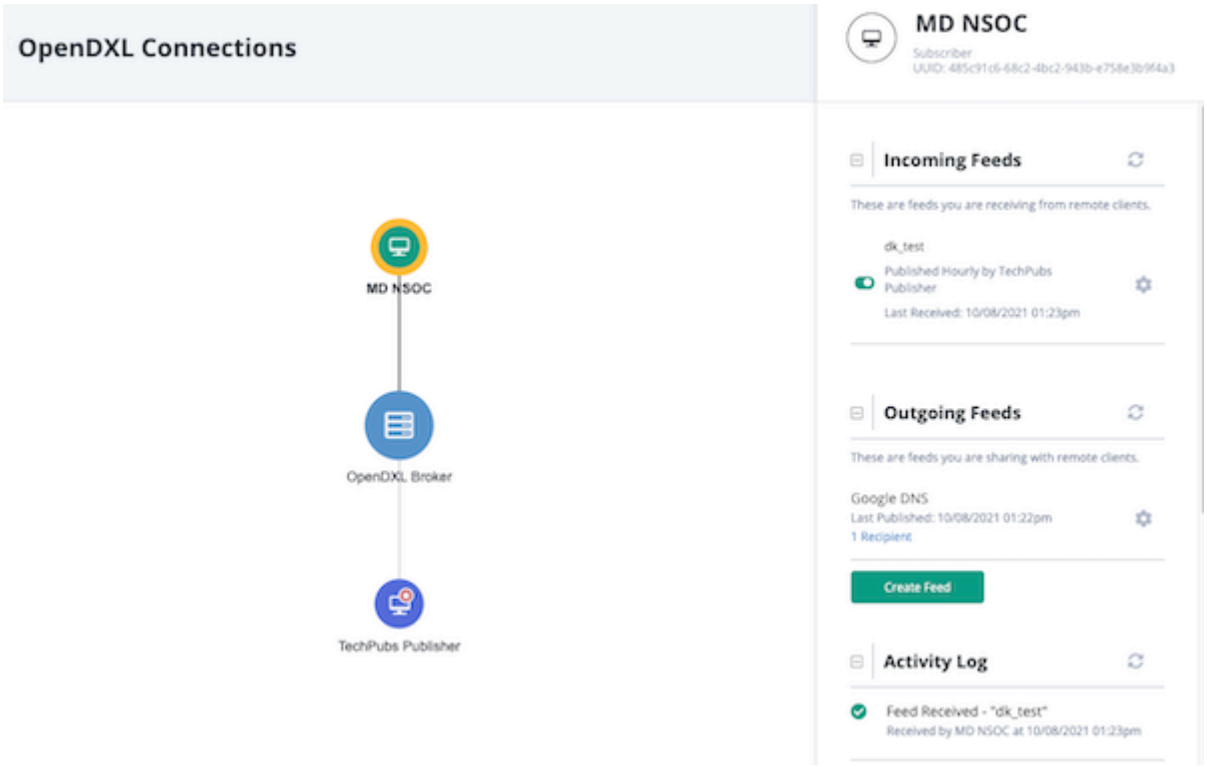
In this example, in addition to subscribing a Data Feed from a Publisher, Subscriber A is also offering its own Data Feed back to the Publisher for subscription.



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 sections for more details.

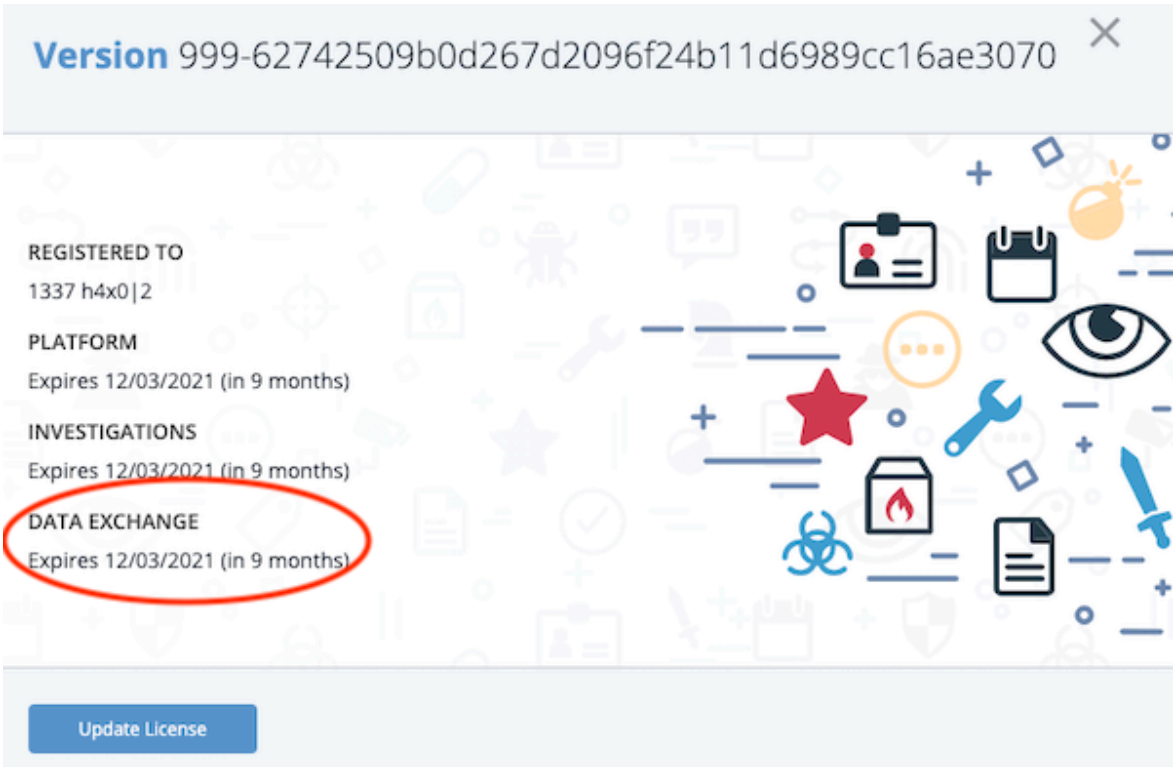
OpenDXL Data Transport Requirements

> After you implement TQX, you cannot change your system's timezone from UTC to another timezone. Doing so will cause TQX to stop functioning.

The following is a list of the minimum requirements to configure and use the ThreatQ Data Exchange OpenDXL Data Transport:

- 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

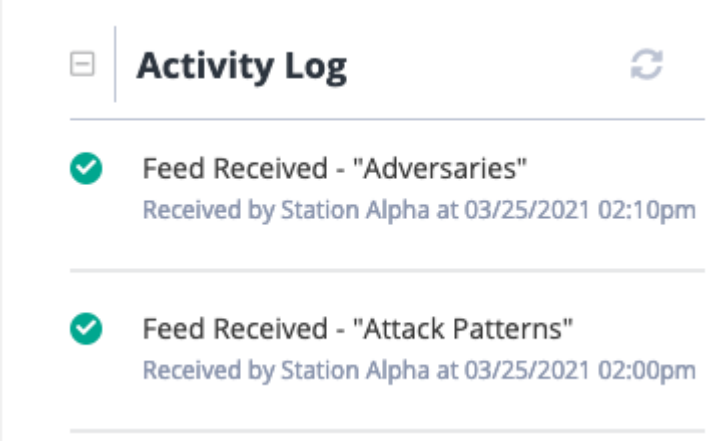
    > All ThreatQ instances on version 4.49+ will have Subscriber permissions. Subscribers will not see the Data Exchange license on their About window.

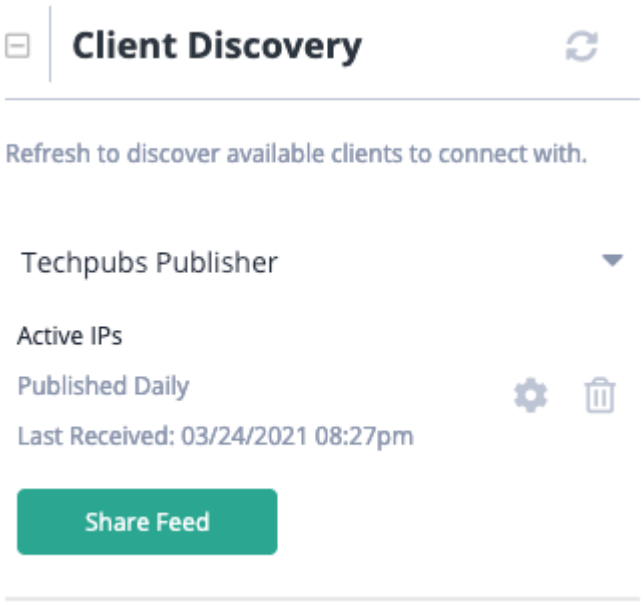
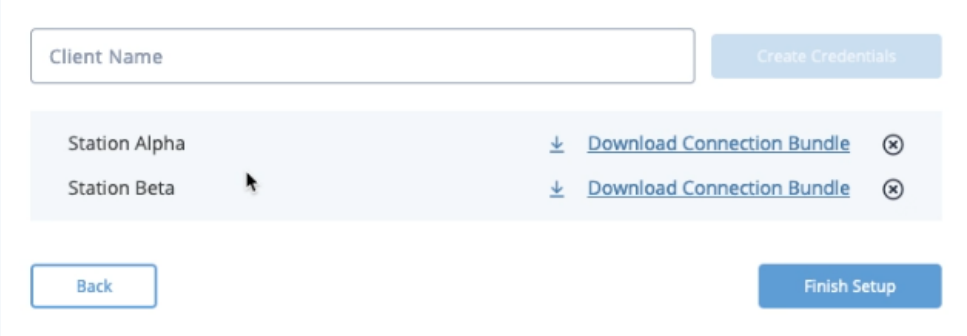
- ThreatQ login with Administrative or Maintenance access for both the Publisher and Subscriber instance.
- One Data Collection saved.
- Network access for both instances.

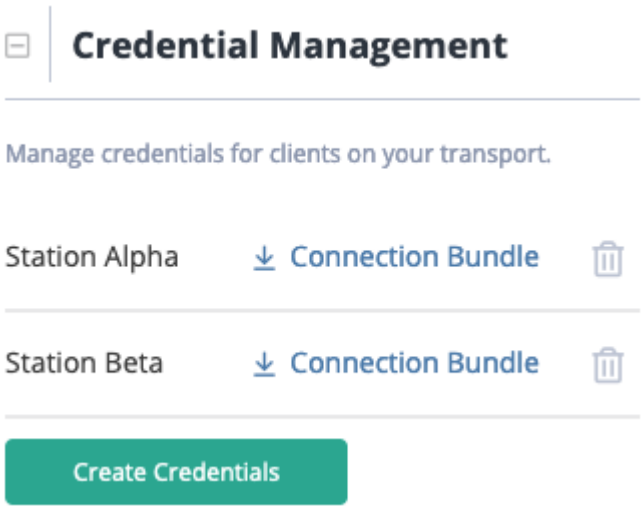
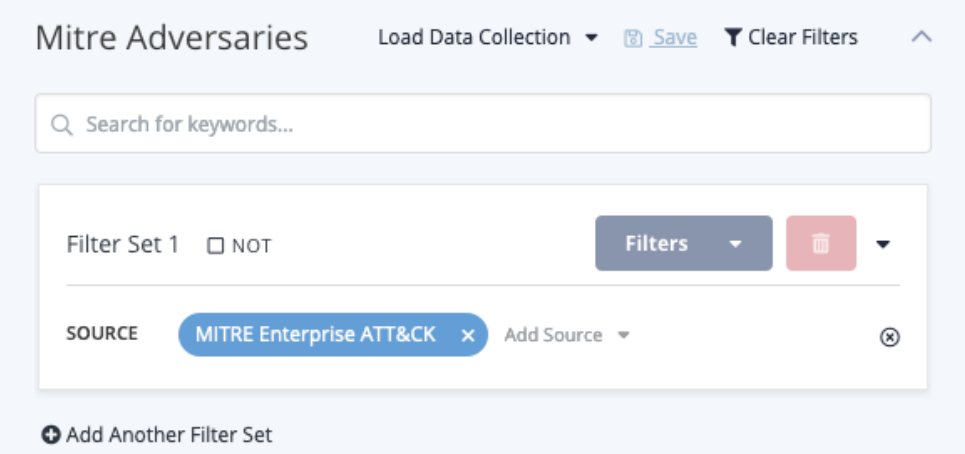
TQX requires a communications connection from Subscriber to Publisher. Users that are utilizing forwarding rules must ensure that the 8883/tcp port is open on the Publisher instance (the instance with the TQX license and running the broker service).

OpenDXL Data Transport Components

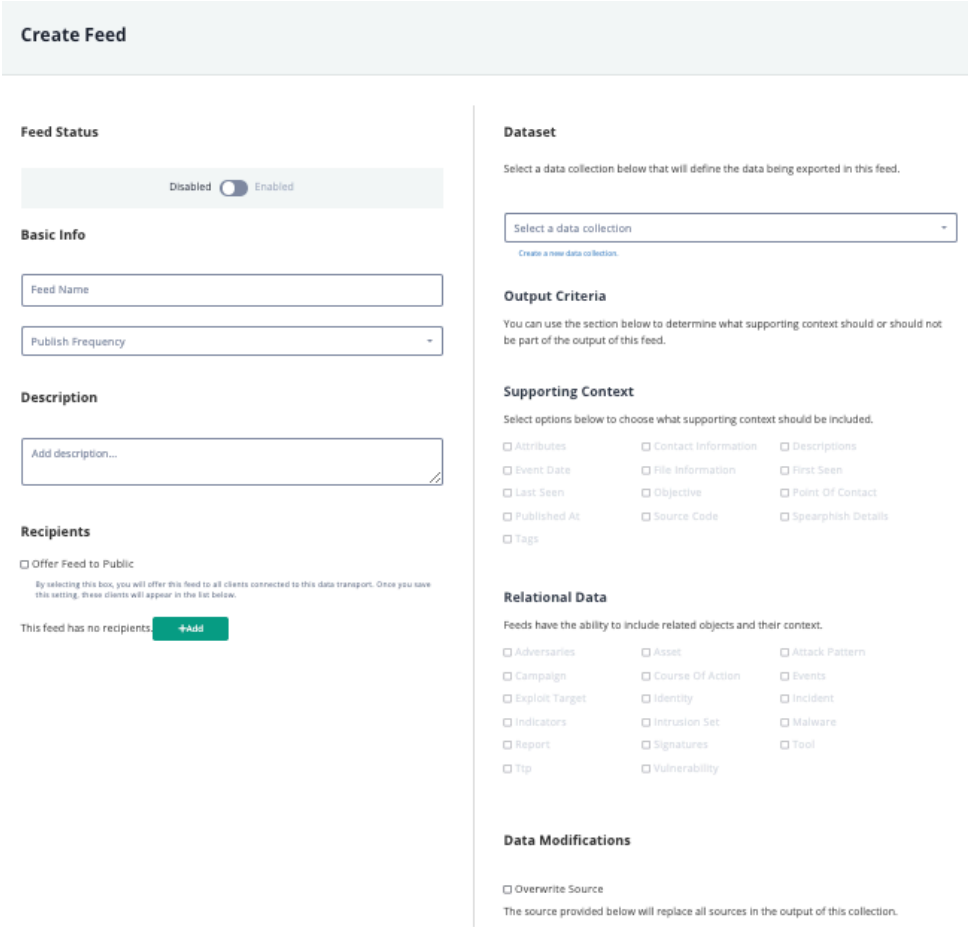
The following table contains key components, terms, and definitions regarding the ThreatQ Data Exchange OpenDXL Data Transport.

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.

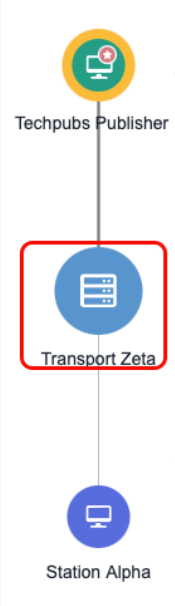
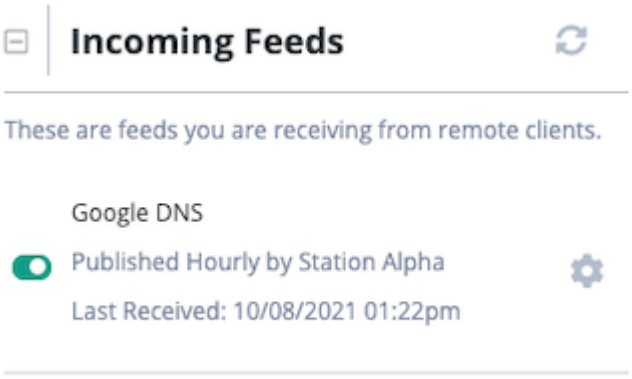
COMPONENT/ TERM	DEFINITION
	
Connection Bundle	The connection bundle is a zip file containing connection information for the Data Transport. A connection bundle is created by a Publisher when creating a new connection, such as adding a new Subscriber. The connection bundle zip must be uploaded by the 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.

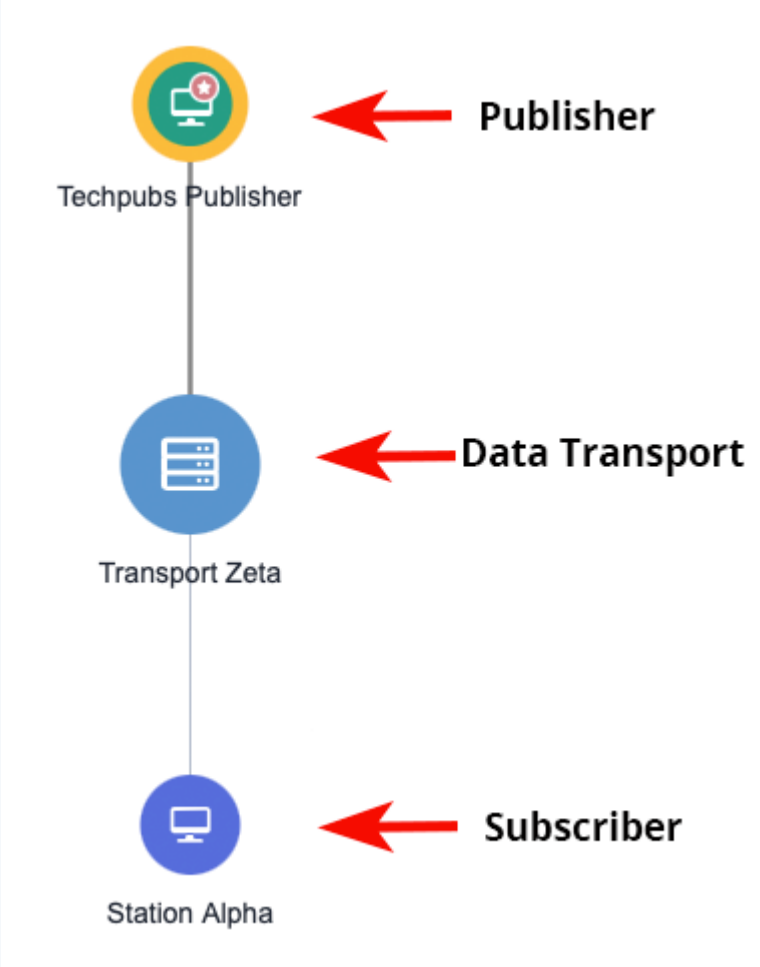
COMPONENT/ TERM	DEFINITION
	
Data Collection	A data collection is a saved ThreatQ Threat Library query that can be used to create a Data Feed. 
Data Feeds	Data Feeds transmit selected Data Collections to user-selected instances (Publishers, Subscribers). You can select which data collection to use, whether 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. See the Data Feeds section for more details. By default, a data feed includes the object types associated with its data

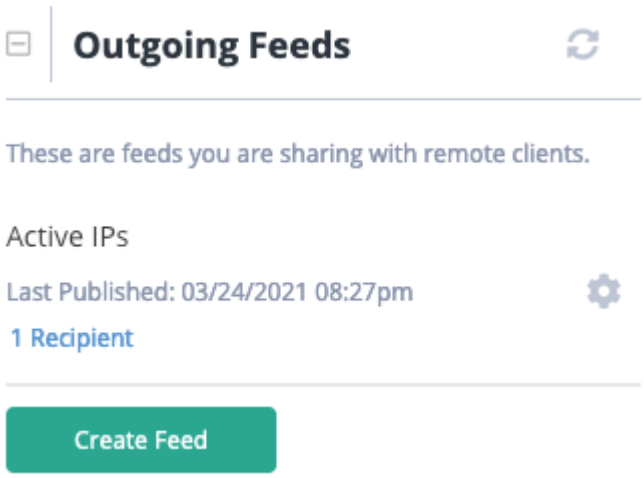
COMPONENT/ TERM	DEFINITION
	collection with the exception of tasks and files. In addition, you can use the the checkboxes in the Supported Context and Relational Data sections to include additional information.

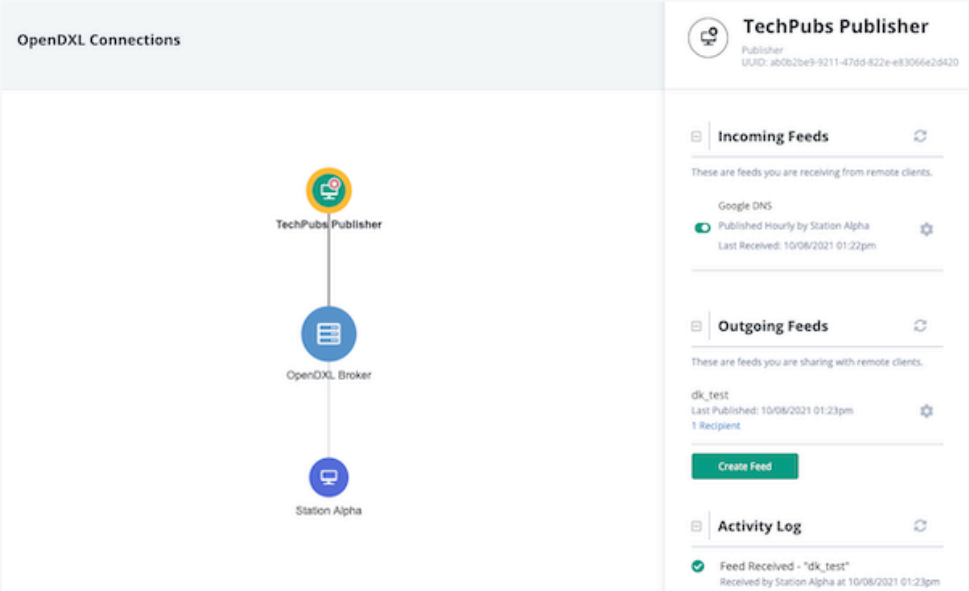


Data Transport	The Data Transport is how data is shared between TQX nodes, using OpenDXL by default. Currently, you can only use the TQX default transport included with a Publisher license. Additional transport options, including the ability to use your own, will be introduced in future releases.

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 names of the feeds offered to you, subscribe to/unsubscribe a feed, and view feed details such as the instance that sent it, the publish rate, and the last received time stamp. 
Nodes	A node is a basic unit of a data structure within the OpenDXL data transport, 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.

COMPONENT/ TERM	DEFINITION
	
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 names of the feeds you provide to other instances, the number of feed recipients, the publish rate, and the last published time stamp. You also have an option to create a new feed from this pane.

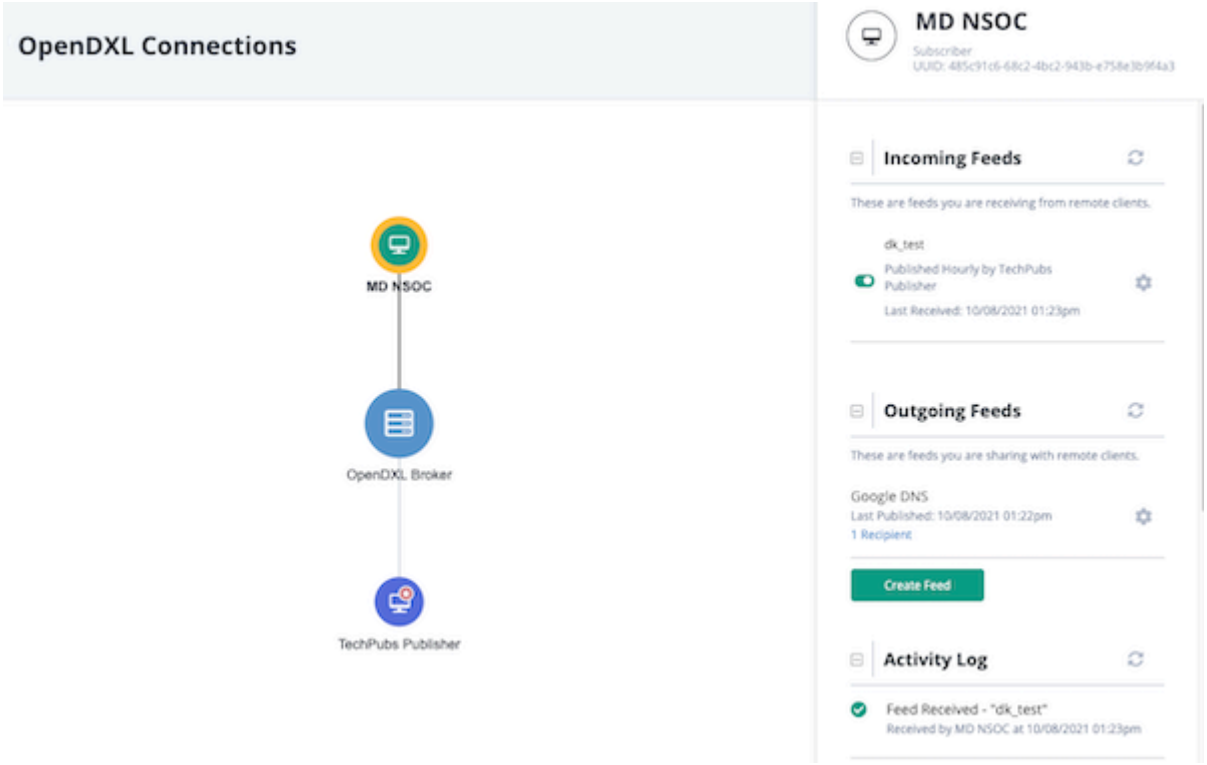
COMPONENT/ TERM	DEFINITION
	
Publisher	A ThreatQ instance with a TQX broker license, which allows a user to create a connection bundle. At least one Publisher instance is required in order to create a connection. In TQX, Publisher nodes have a star badge icon in the Topology View.
Subscriber	A ThreatQ 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.

COMPONENT/ TERM	DEFINITION
	

OpenDXL Data Transport 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.

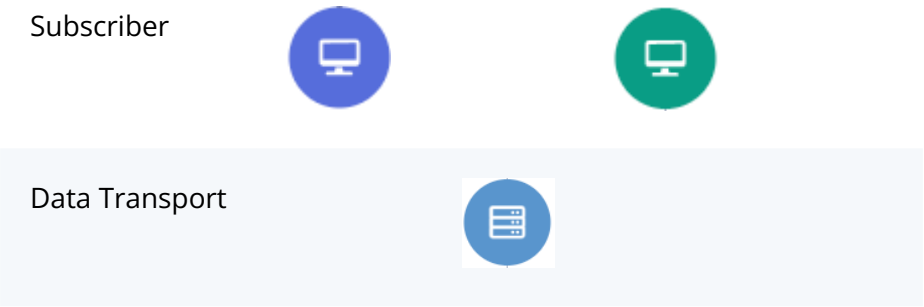


Clicking on a specific node allows you to view related information such as Data feeds you are sharing or receiving, an Activity Log, as well as the ability to create/download new and existing connection bundles (Publishers only).

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		



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.

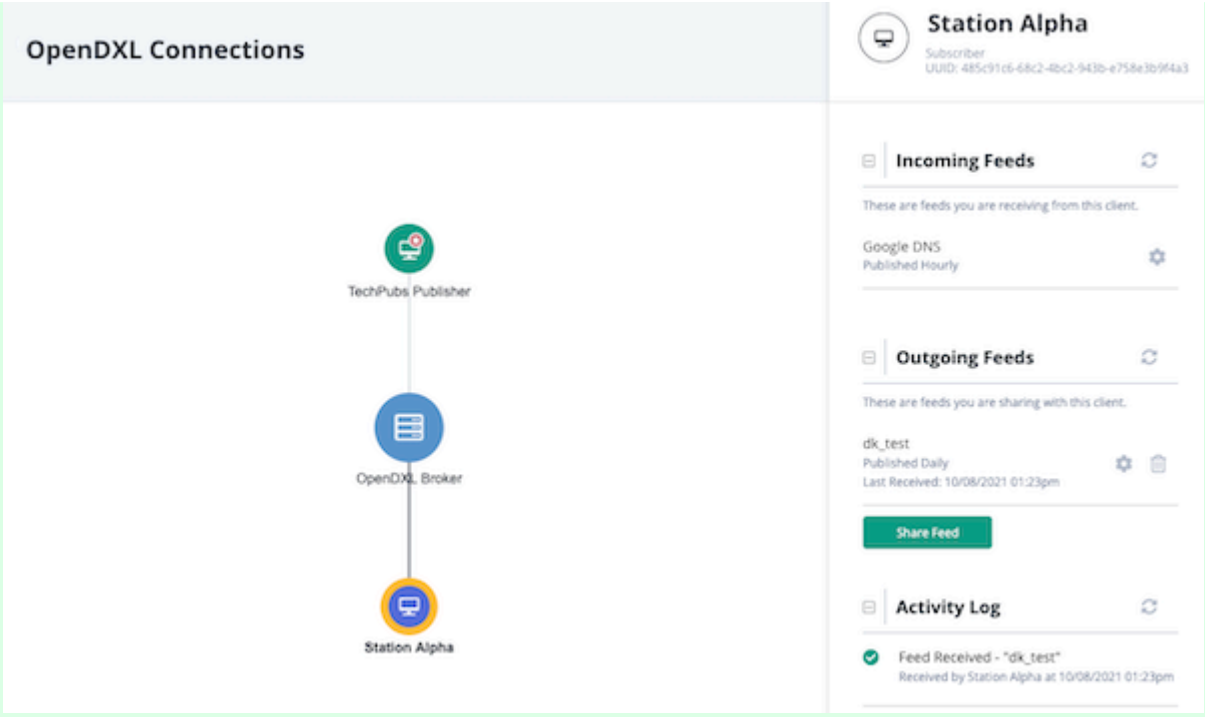
Tips and Tricks

- 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 OpenDXL Connections page.
- You can click and drag your Topology View to a different location in the OpenDXL Connections page.
- You can click any node in the Topology View to view its details on the right side of the page.

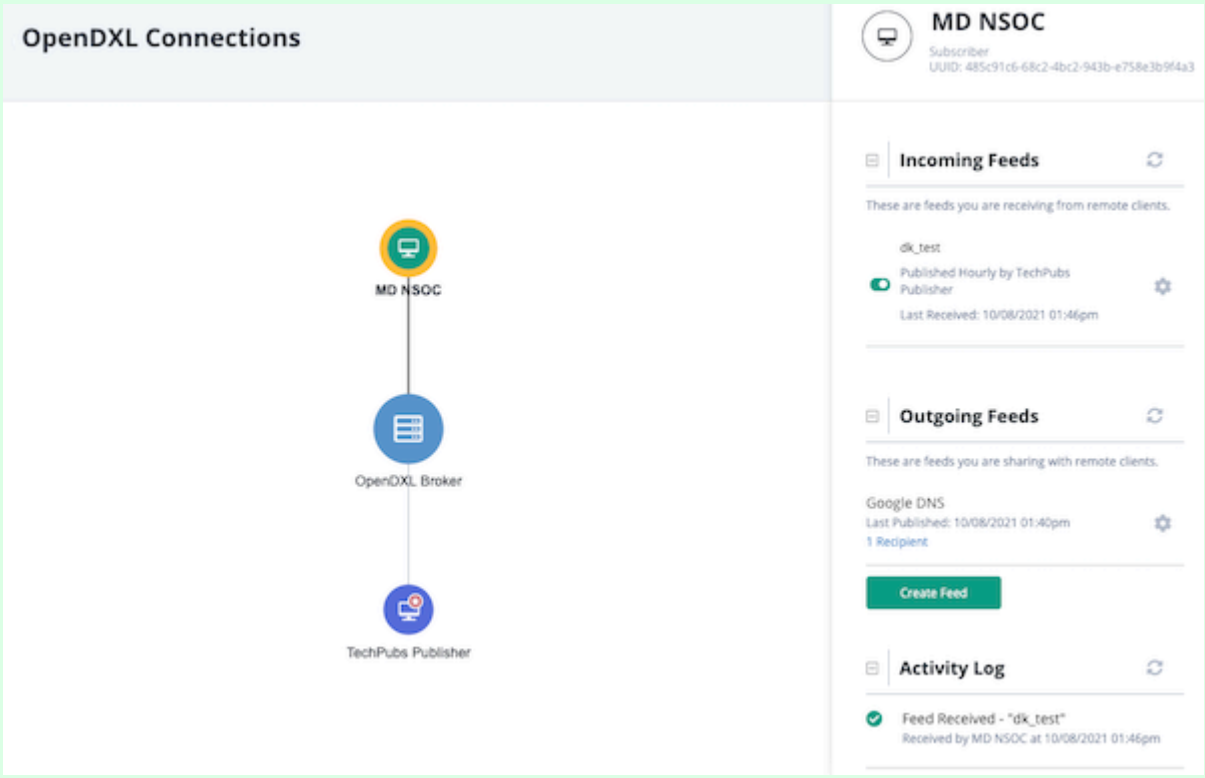
Instance Naming

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.



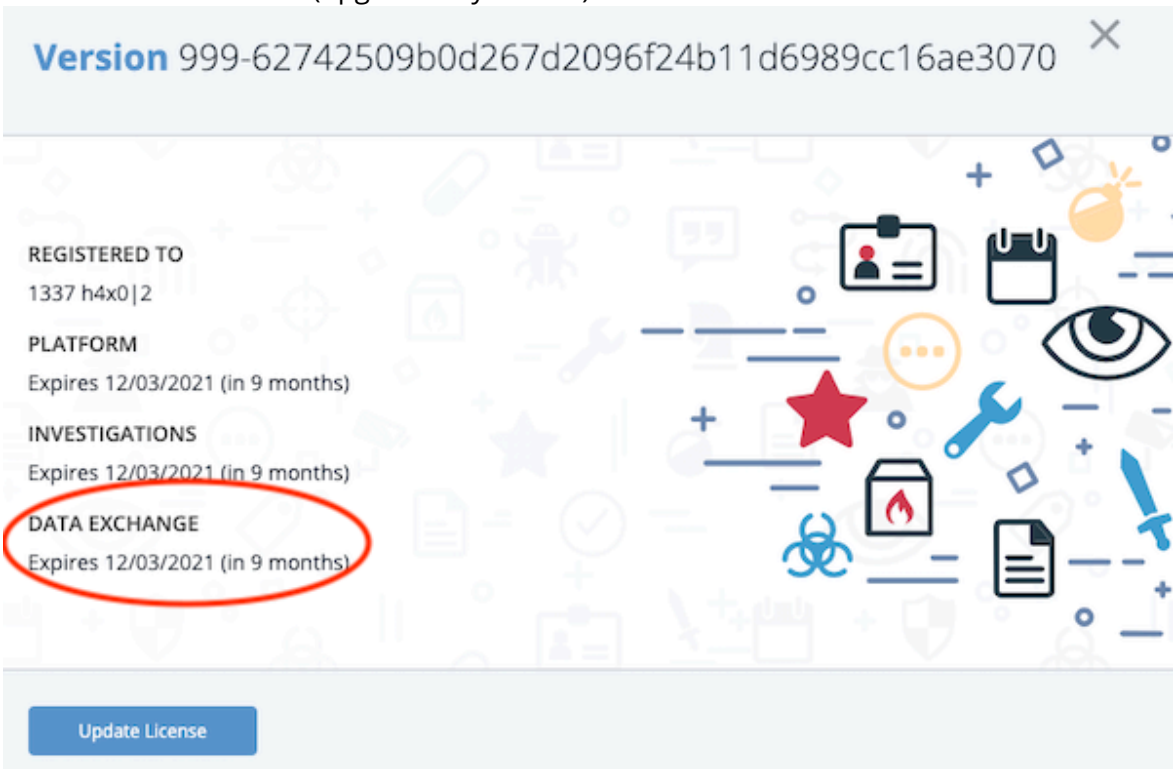
Getting Started - First OpenDXL Data Transport Connections

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 OpenDXL Data Feed.

Confirm Requirements

Confirm that you have the following:

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

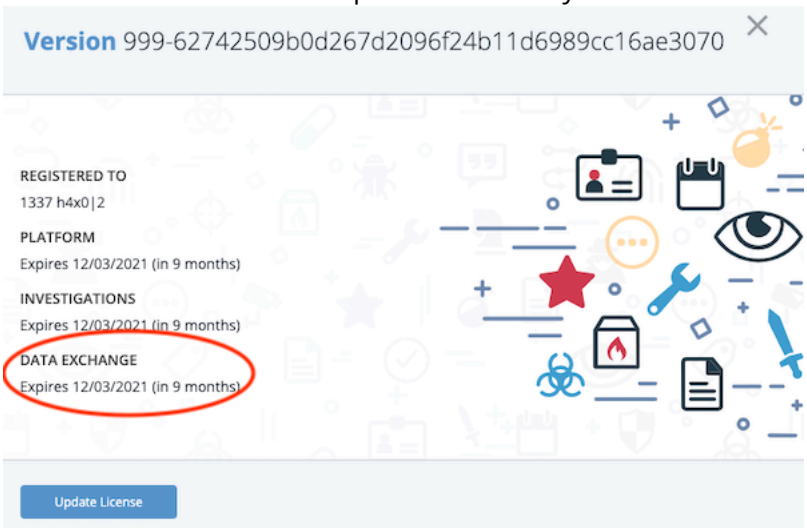


  - One Subscriber Instance (included with standard ThreatQ License version 4.49+)
- Network connection between the two instances
- At least one saved Data Collection (Publisher instance)

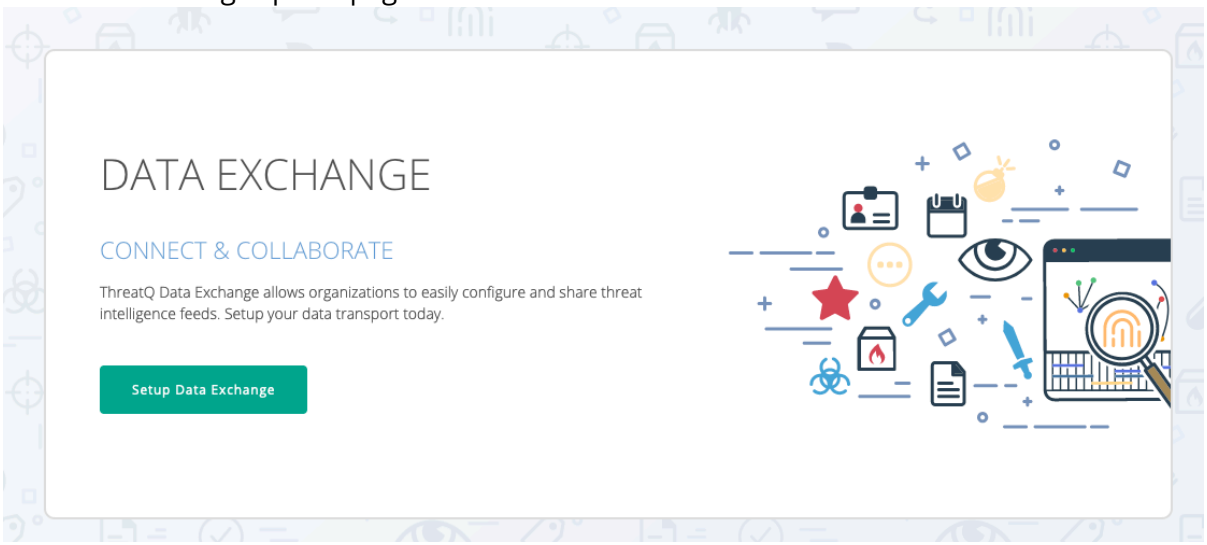
Publisher - Creating a Connection Bundle

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.

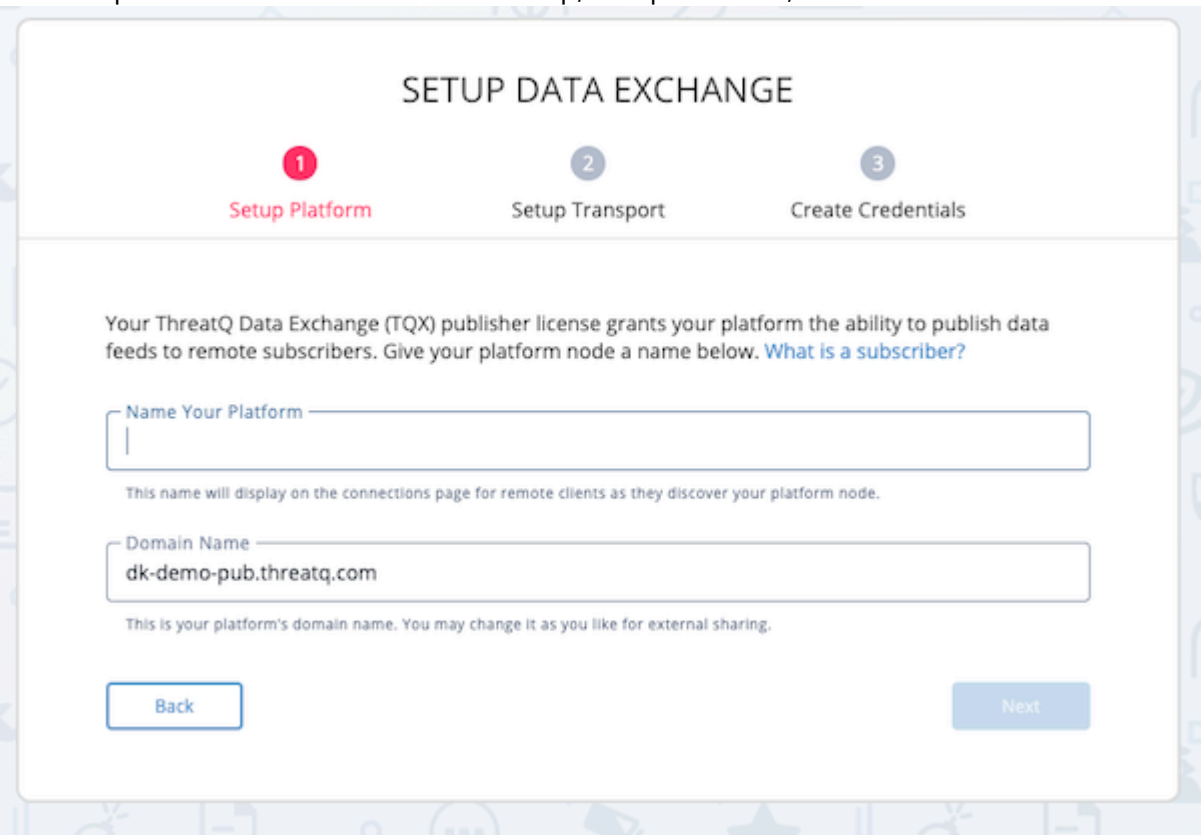


3. Click on the **Data Exchange** icon and select the **Set Up Server** option in the OpenDXL section. The Data Exchange splash page will load.



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

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

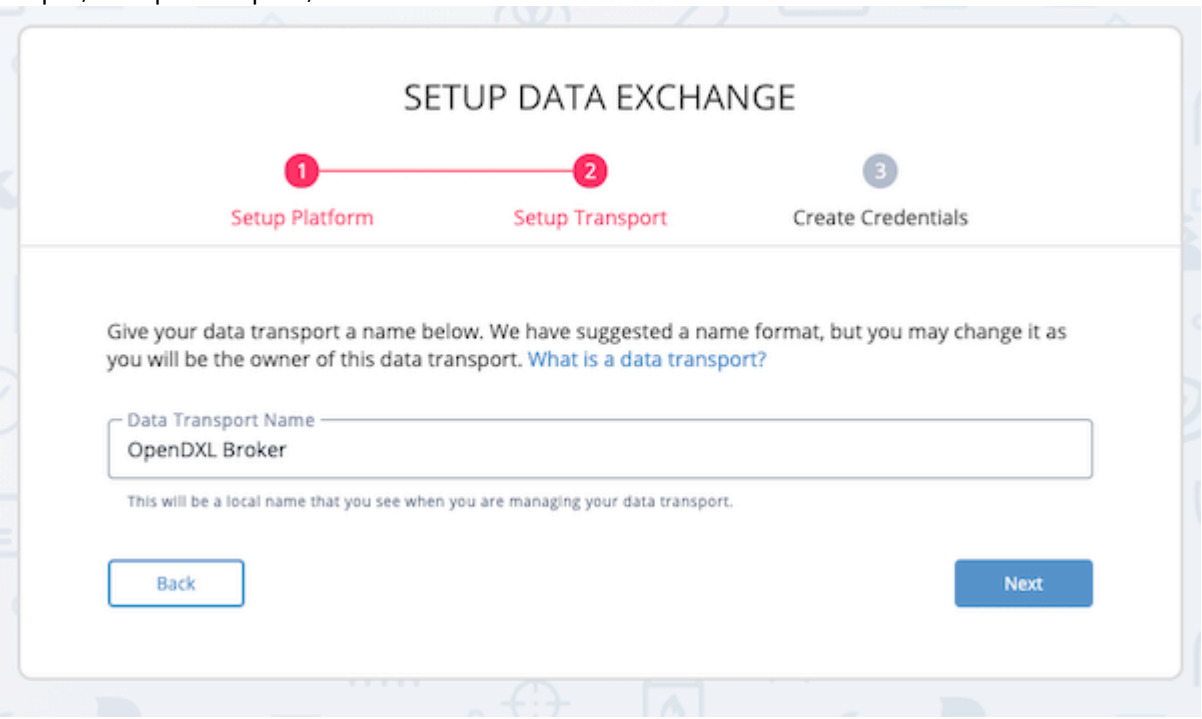


5. Enter a **Platform Name** for your instance. This is the name that you will use to identify yourself on the connections page. Subscribers will also see this name when viewing their Topology view.

   > 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.

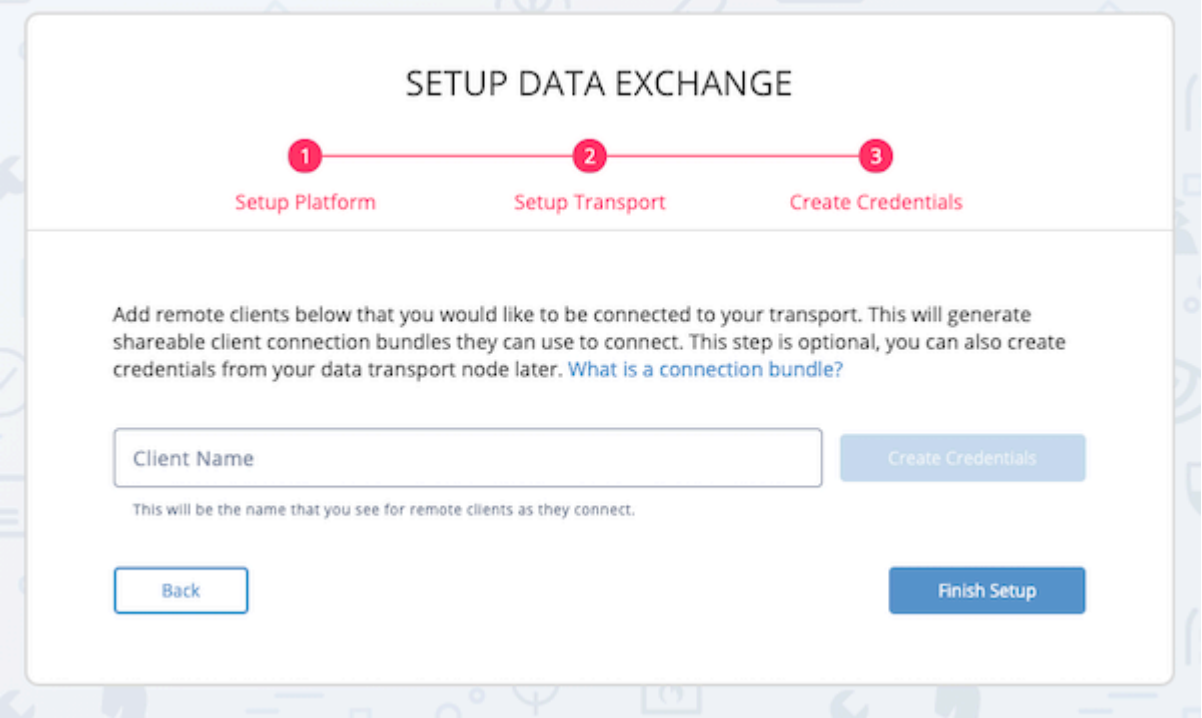


8. Update the **Data Transport Name** if desired, otherwise use the default entry. This name will be used to identify the Broker node in your Topology view.

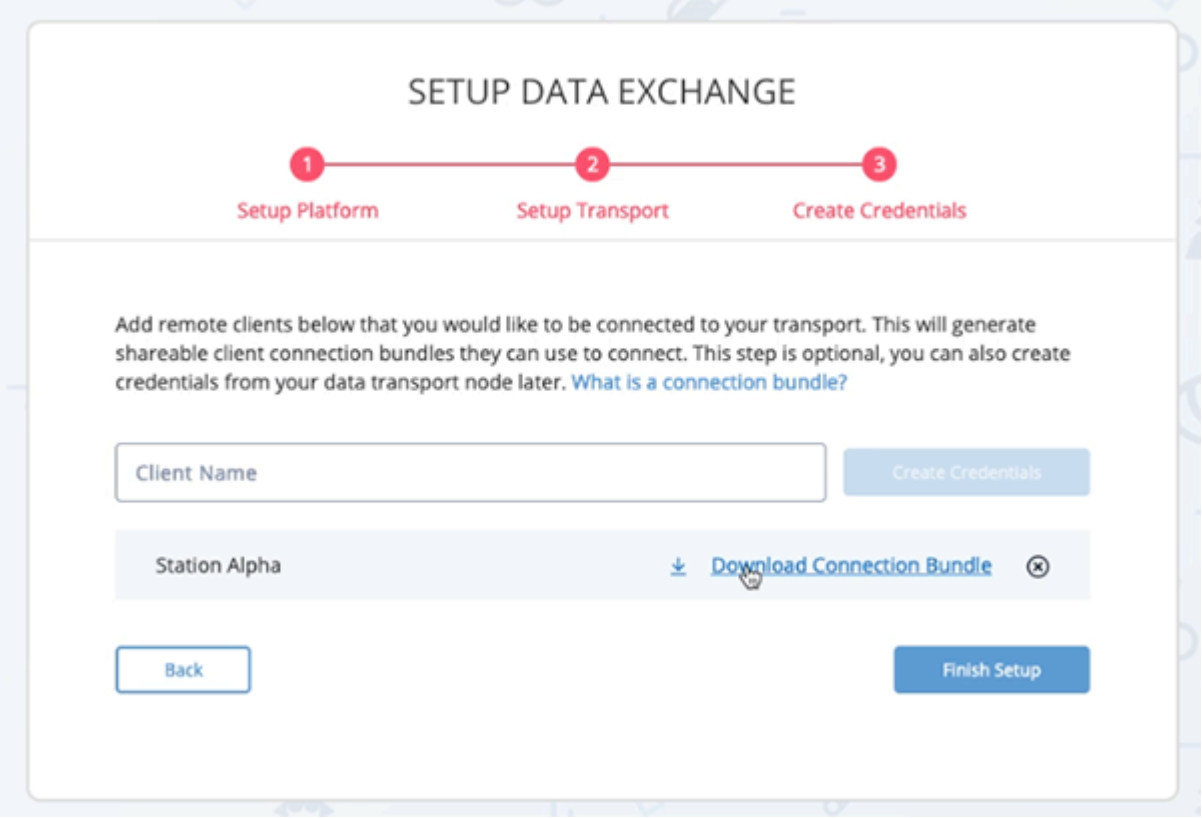
   Subscribers are given the option to name the Data Transport during their connection setup. The name you enter in this field will not affect what Subscribers see.

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 the OpenDXL data transport. 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.

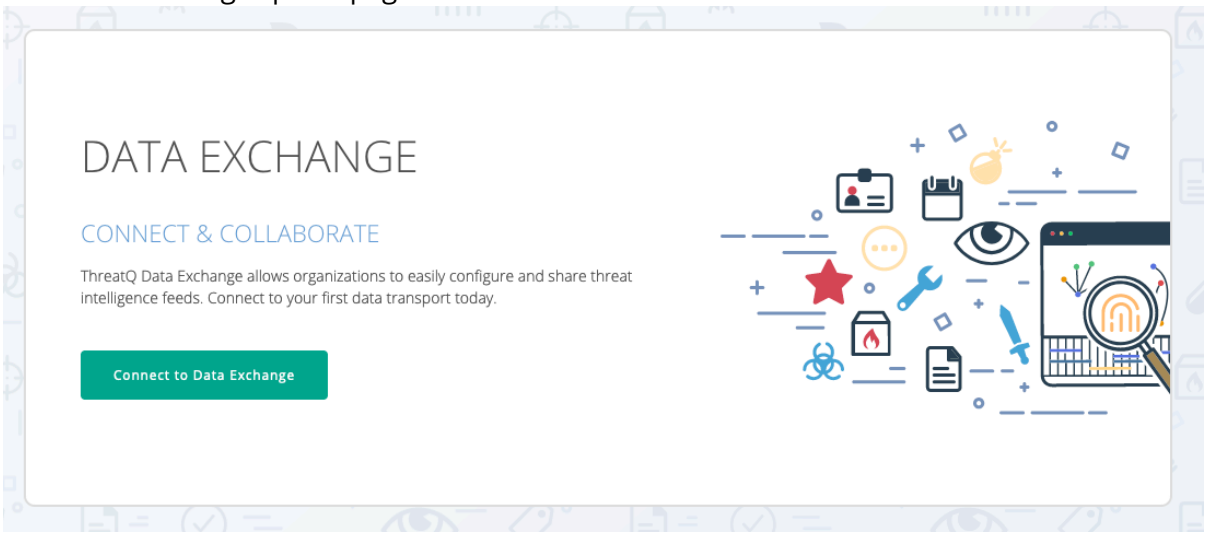
13. Click the **Finish Setup** button.
14. Send the Connect Bundle(s) you downloaded in step 12 to the Subscriber(s).

    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

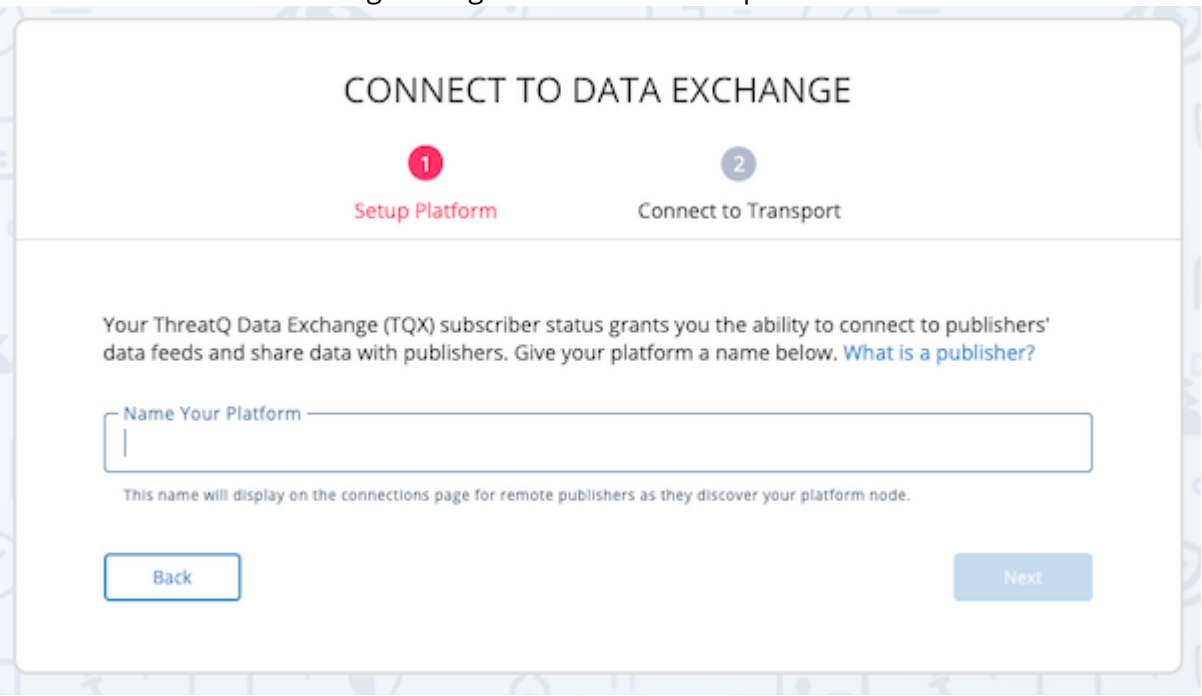
1. Click on the **Data Exchange** icon in the top navigation bar of ThreatQ and select **Connections**.

   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.

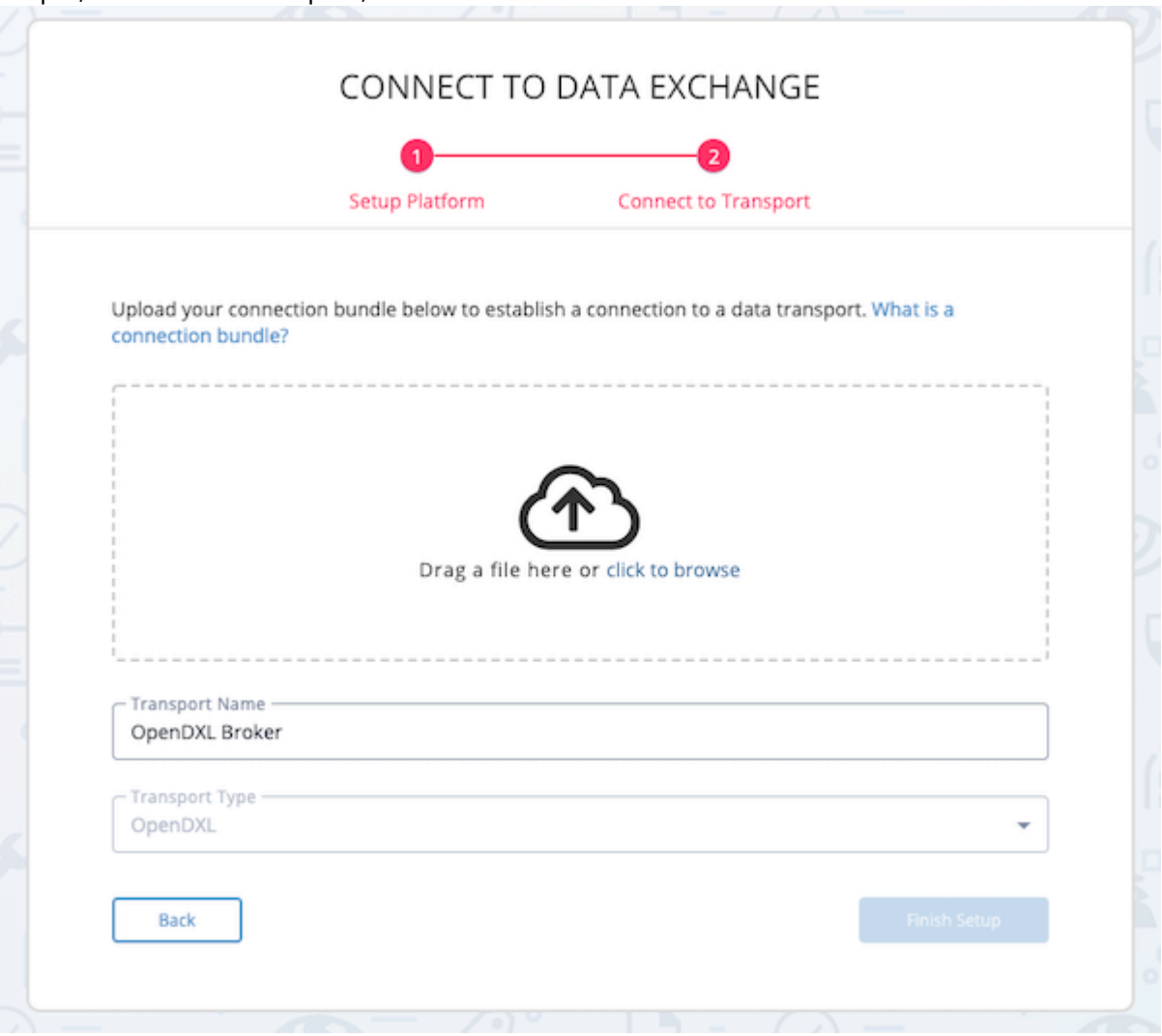


3. Enter a name for your platform instance. You will use this name to identify your instance in your Topology view.

   > 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.

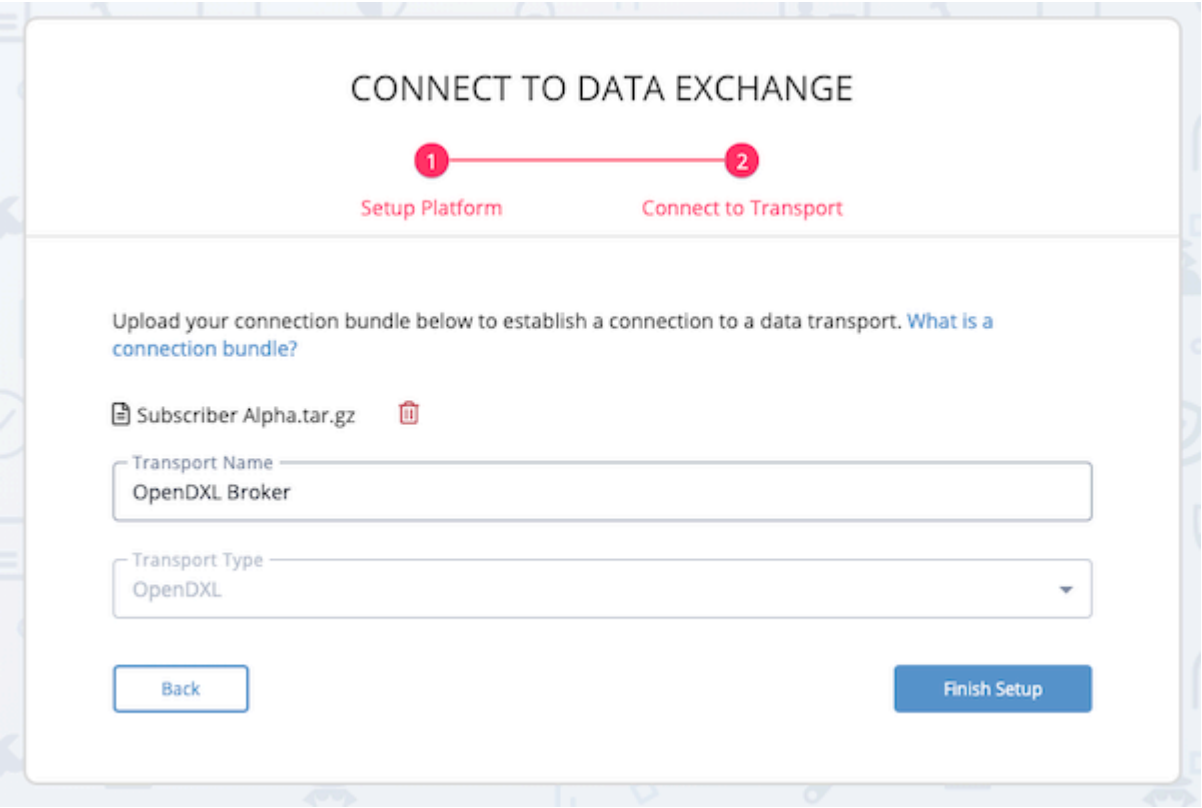
4. Click on **Next**.

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.

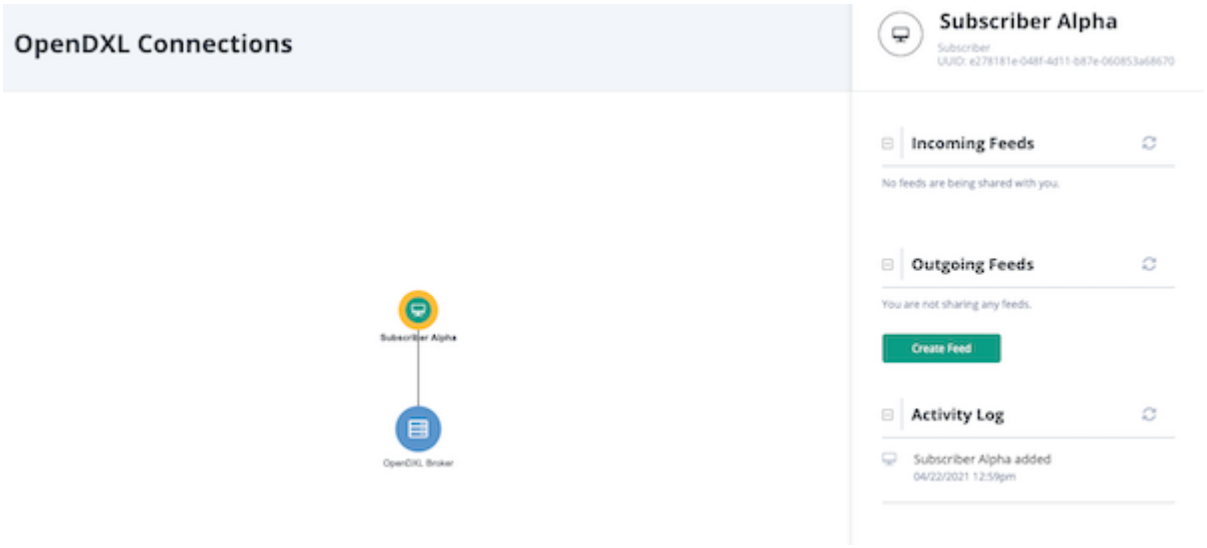


6. Update the **Data Transport Name** if desired, otherwise use the default entry. This name will be used to identify the transport node in your Topology view.
7. Leave the **Transport Type** dropdown field as is.

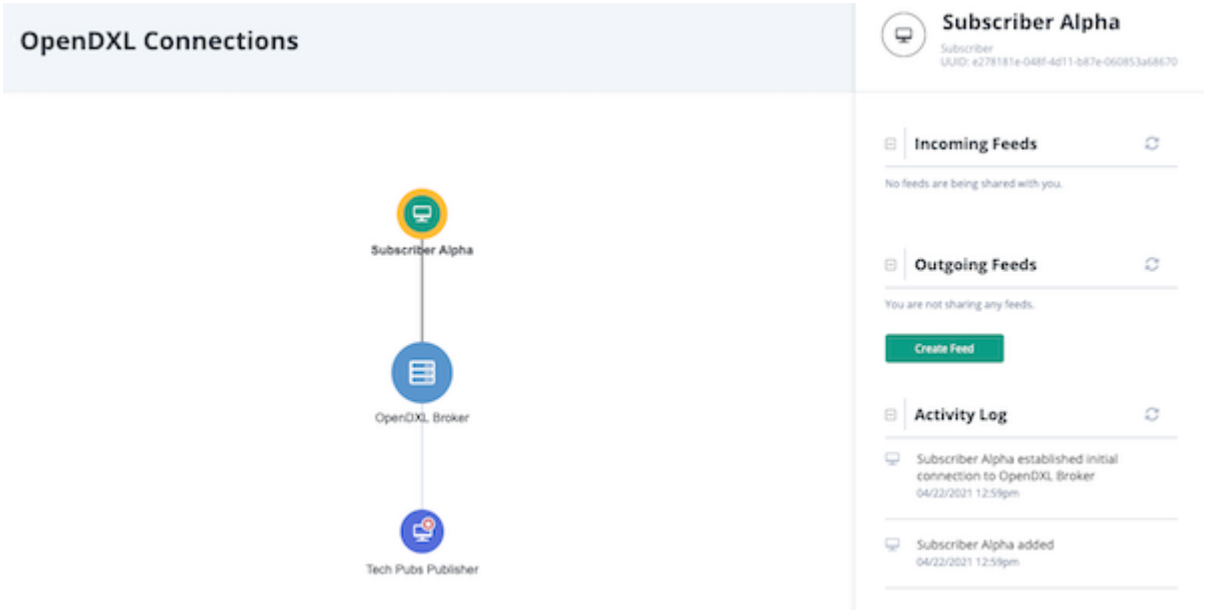
   The system default transport is the only transport available. The option for additional transports will be added in future releases of the ThreatQ platform.

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

   The OpenDXL 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.



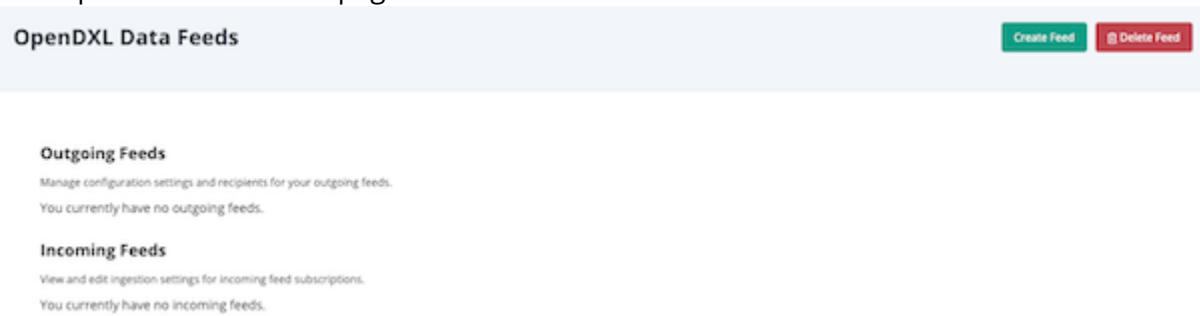
> It can take up to 30 seconds for the discovery process to complete. Refresh the page in order to see the new connection. After the instances have discovered each other, the OpenDXL Connections pages will show the connections. The publisher will now see the subscriber node and the subscriber will now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



Publisher - Creating a Data Feed

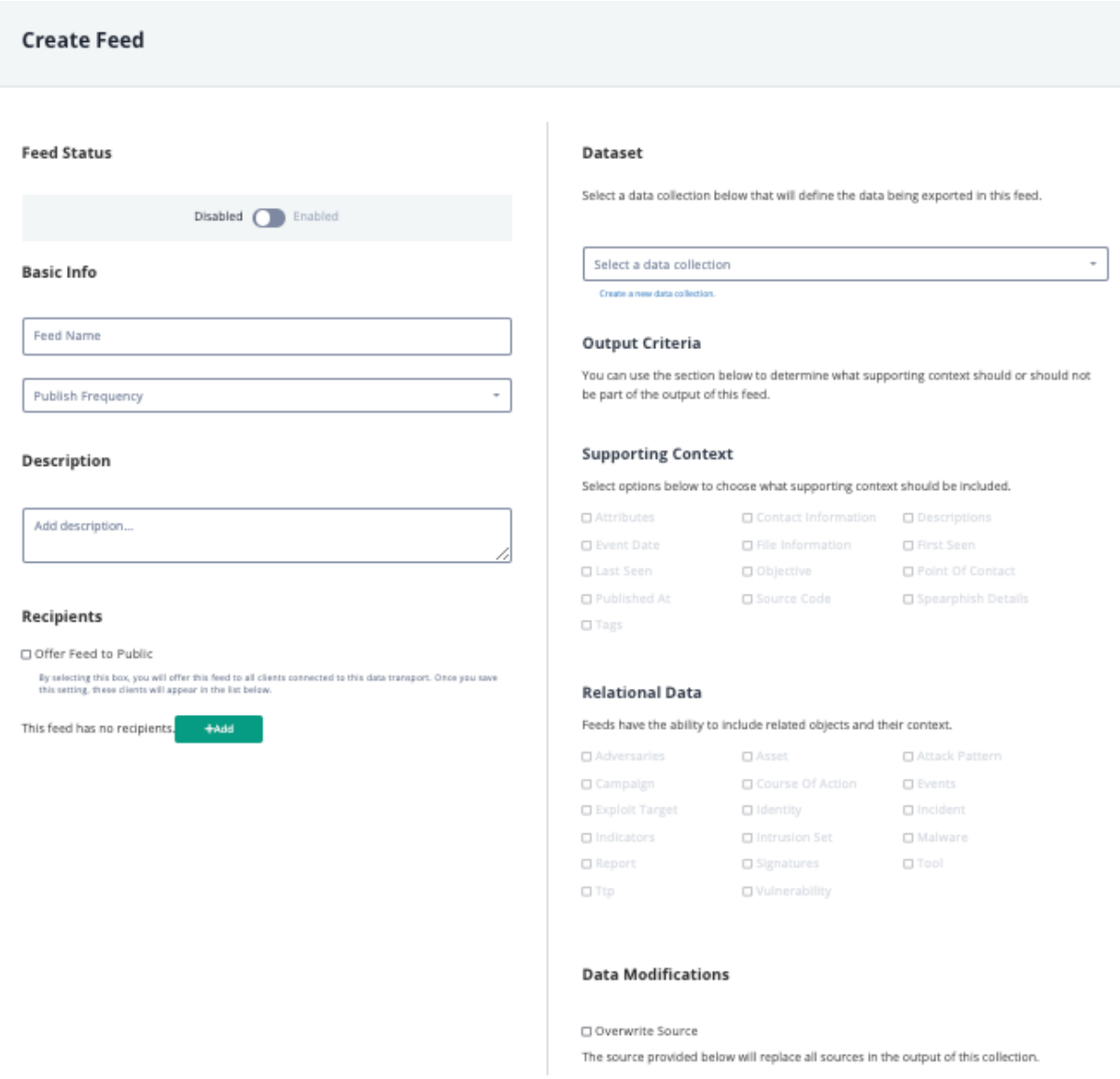
1. Click on the **Data Exchange** icon in the top navigation bar of ThreatQ and select **Data Feeds**.

The OpenDXL 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.

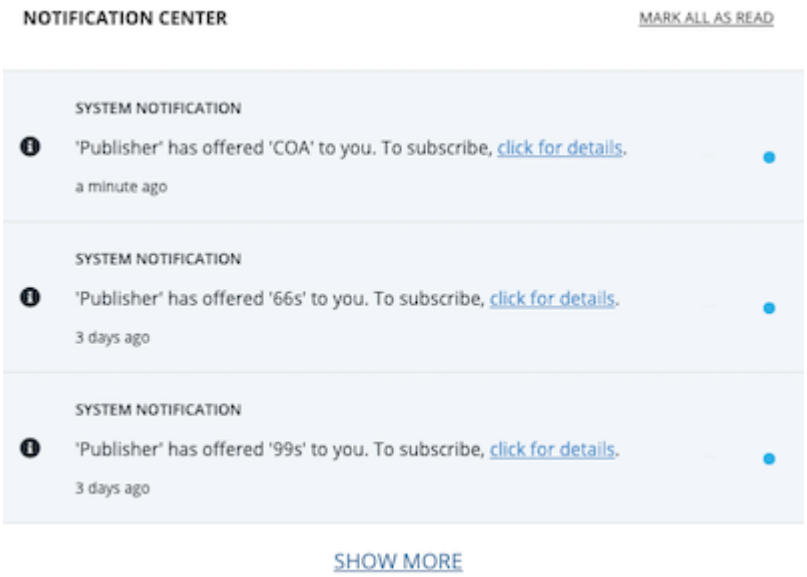
Output Criteria	Select the supporting context that should be included in the feed using the checkboxes supplied. Only fields used in the data exported are selectable. Fields not associated with the data collection selected are greyed out. Select the relational data to be included in the transfer. Based on the object you select the following data is included in the feed:

SYSTEM OBJECT	FIELDS
Indicator	type_id, status_id, class, value
Adversary	name
Event	type_id, title
Signature	type_id, status_id, name, value
Custom Objects	type_id, status_id, value

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 OpenDXL Data Feeds page

which allows the recipient to review feed details before subscribing.

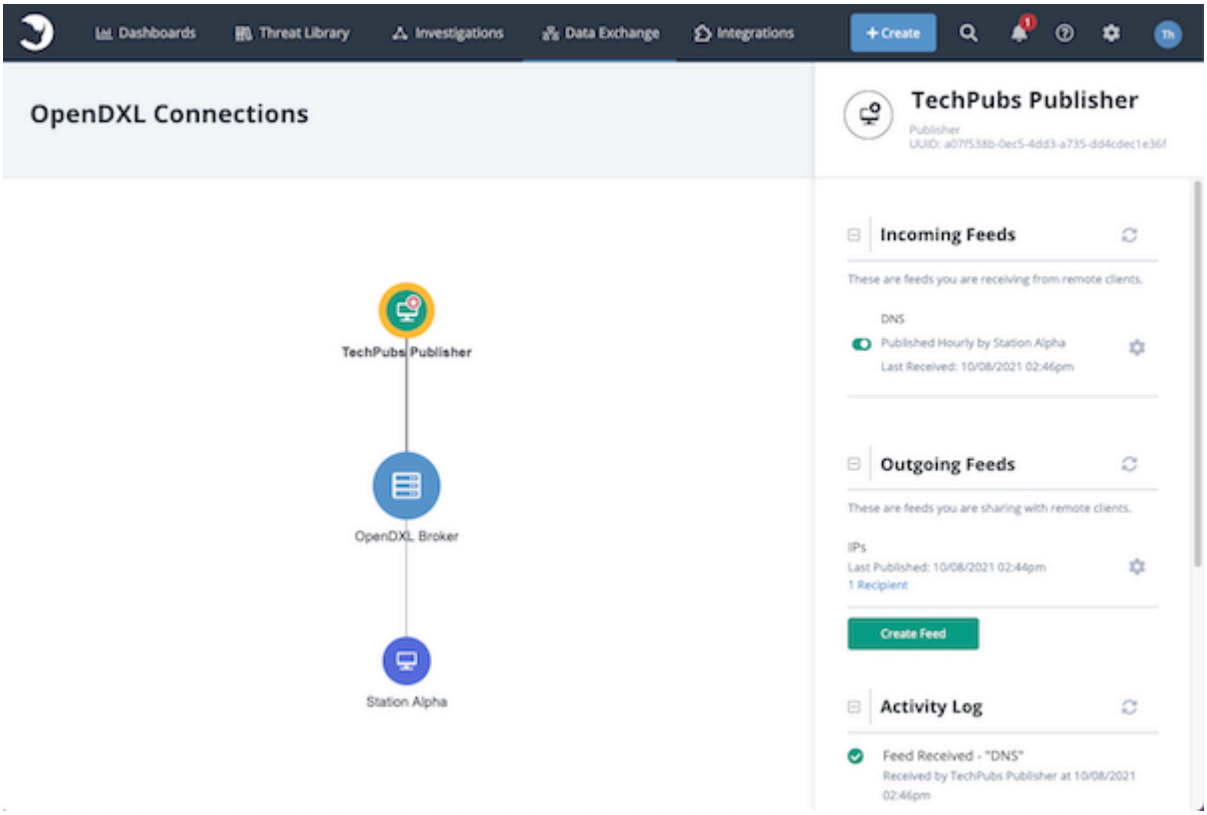


Publisher Instances

About Publisher Instances

Publishers are the driving force of the OpenDXL data transport and this is reflected in the Topology View displayed in the Connections page. When a Publisher clicks the OpenDXL Set Up Server 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 OpenDXL Data Transport 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.


Dashboards
Threat Library
Investigations
Data Exchange
Integrations
+ Create
OpenDXL Connections
TechPubs Publisher
OpenDXL Broker
Station Alpha
TechPubs Publisher
Incoming Feeds
These are feeds you are receiving from remote clients.
DNS
Published Hourly by Station Alpha
Last Received: 10/08/2021 02:46pm
Outgoing Feeds
These are feeds you are sharing with remote clients.
IPs
Last Published: 10/08/2021 02:44pm
1 Recipient
Create Feed
Activity Log
Feed Received - "DNS"
Received by TechPubs Publisher at 10/08/2021 02:46pm

Creating a Client Connection Bundle

As a publisher, you can create client bundles to add subscribers to your publisher instance. You can only create connection bundles for subscribers - a publisher cannot connect to another publisher instance.

Once a connection bundle has been created, you can send the bundle to the subscriber instance to connect - see the Connecting to a Publisher for more details on how a subscriber uploads the connection bundle.

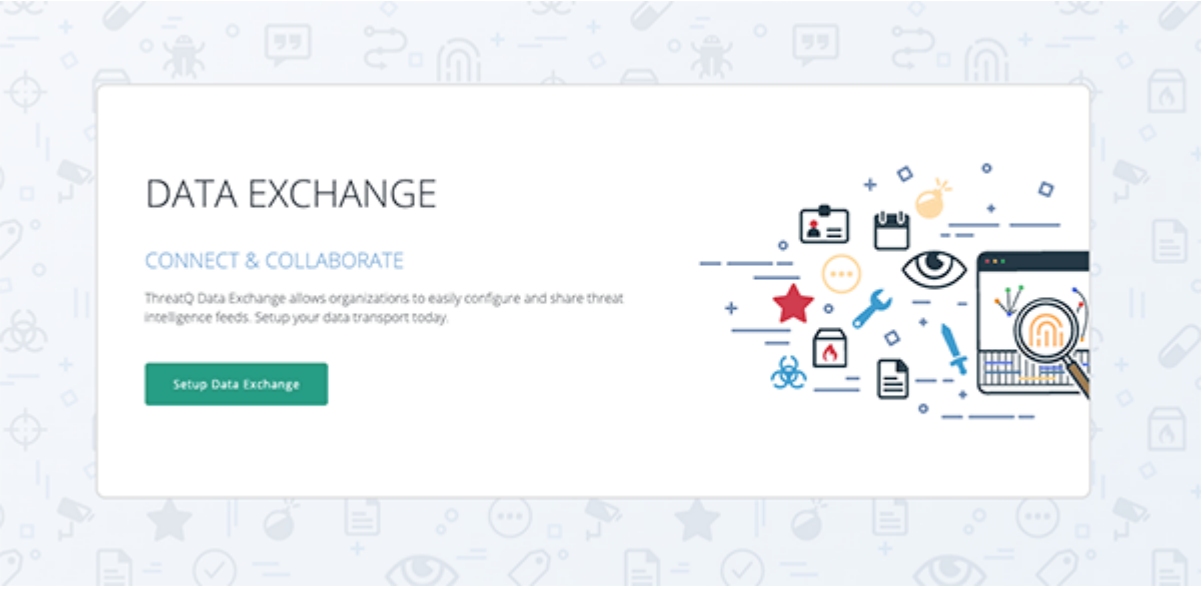
> The steps for creating your initial connection bundle when you setup your publisher instance and adding additional connections to functioning instance differ slightly.

Creating an Initial Client Bundle

Creating your first connection bundle can be performed from the Data Exchange initial landing page. This page will automatically load upon selecting the OpenDXL Set Up Server option.

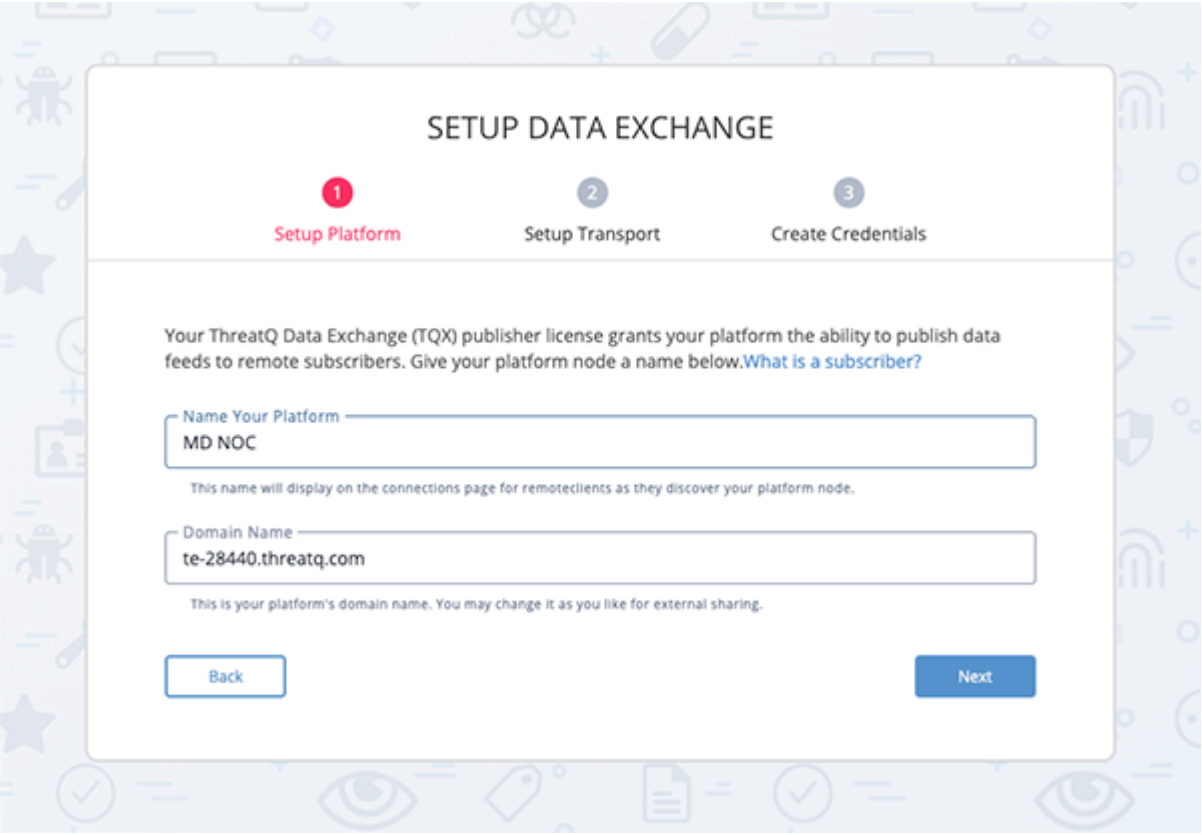
1. Click on the **Data Exchange** menu option and select the OpenDXL Set Up Server option.

   The Data Exchange setup landing page will load.



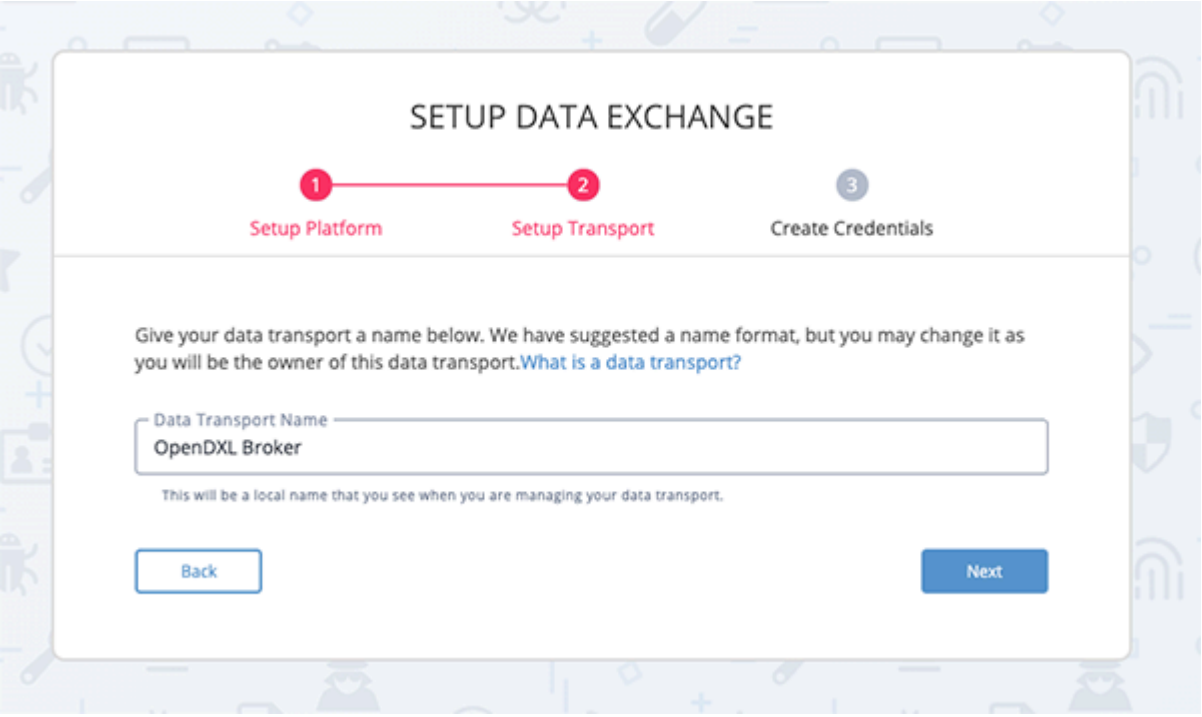
2. Click on the **Setup Data Exchange** button.
3. Enter the name that will be used to identify your instance in the TQX node view.

   > This name will appear as your instance for the subscriber.



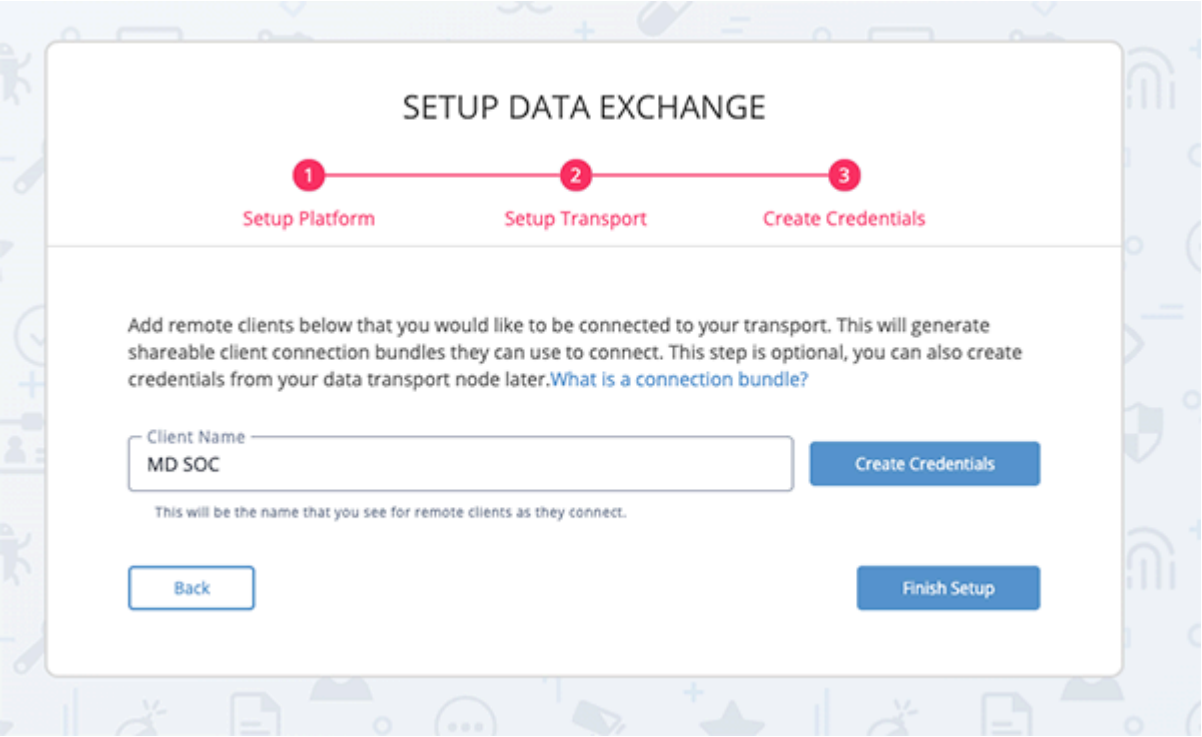
4. Click on **Next**.
5. Enter the name for the **Data Transport**.

> This will be the local name you will see when managing your data transport. You can also leave the default value: **OpenDXL Broker**.



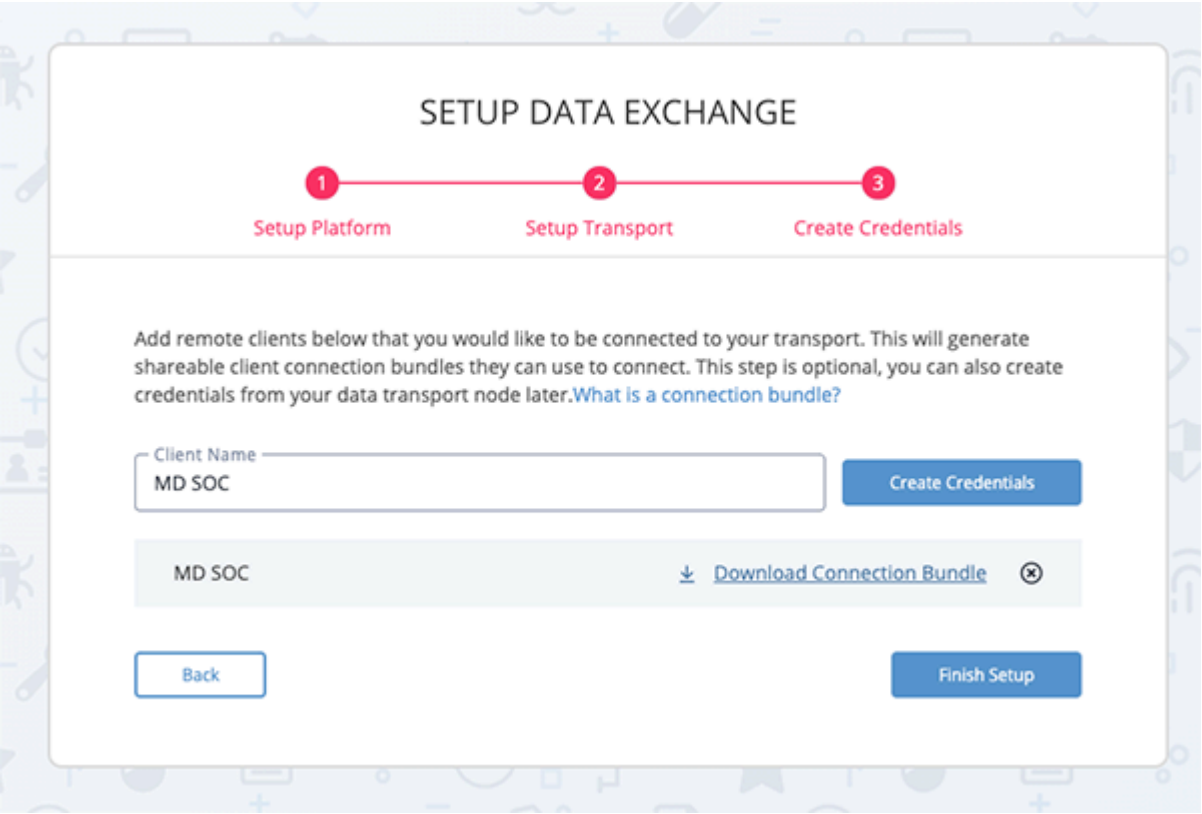
6. Click on **Next**.
7. Enter a **Client Name** for the subscriber.

   This name will be used to identify the subscriber in the TQX node view.



8. Click on the **Create Credentials** button.
9. Repeat steps 7 and 8 to create additional bundles.

10. Download the connection bundles that you have created using the links provided.



11. Click on **Finish Setup** when you have finished creating your bundles and transfer the downloaded connection bundles to the subscriber instances.

> In the event that you clicked on Finished Setup before downloading the bundle(s), you can download the connection bundles from the node view by clicking on the transport node. Connection bundles will be located under the Credential Management heading.

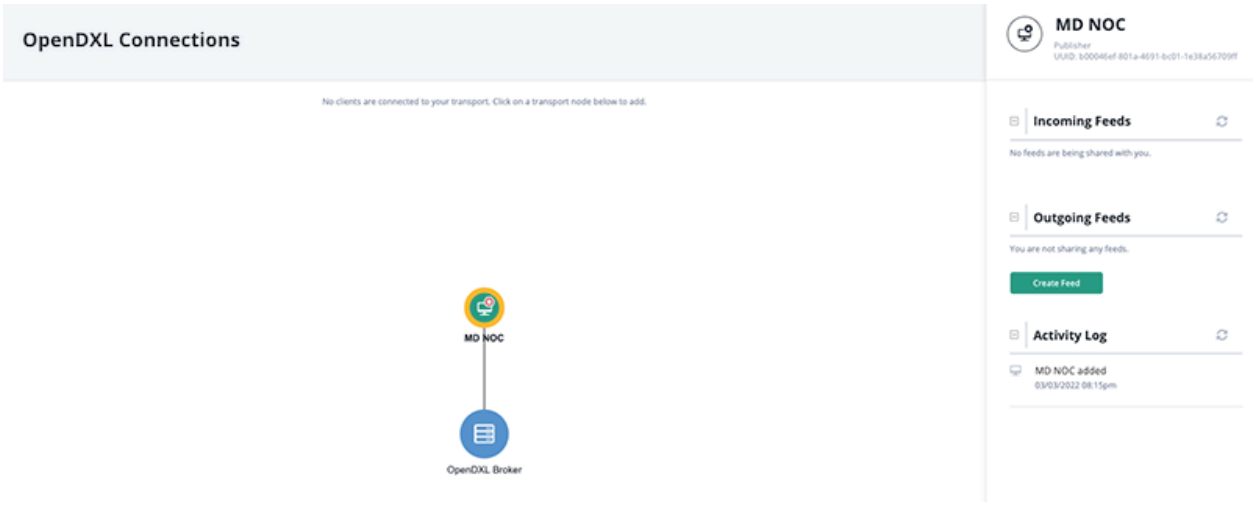
The node view will load with nodes for your instance and broker displayed. Once the subscriber has uploaded the connection bundle, created in steps 7-10, that node will also appear in the node view.

Creating Additional Client Bundles

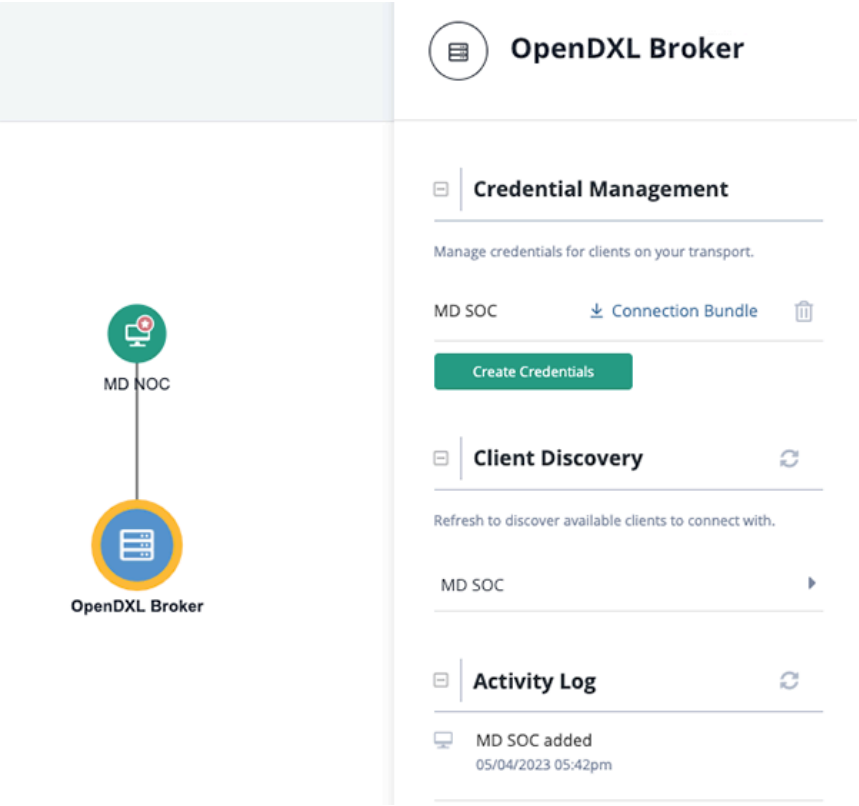
Once you have created a client bundle, the getting started wizard is no longer available. You can create additional bundles from the Connections node view.

1. Click on the **Data Exchange** navigation option and select **Connections**.

   The OpenDXL Connections node view will load.

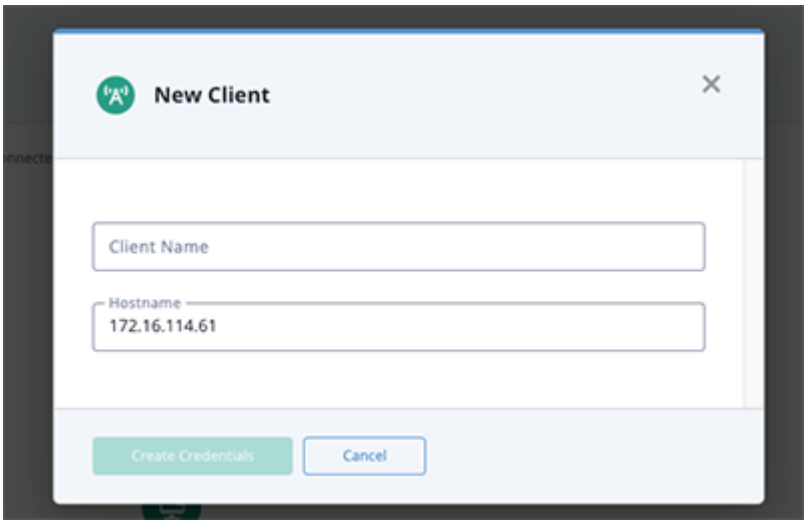


2. Click on the **blue transport node** to load its details in the right pane.



3. Click on the **Create Credentials** button located under the Credential Management heading.

   The New Client window will open.



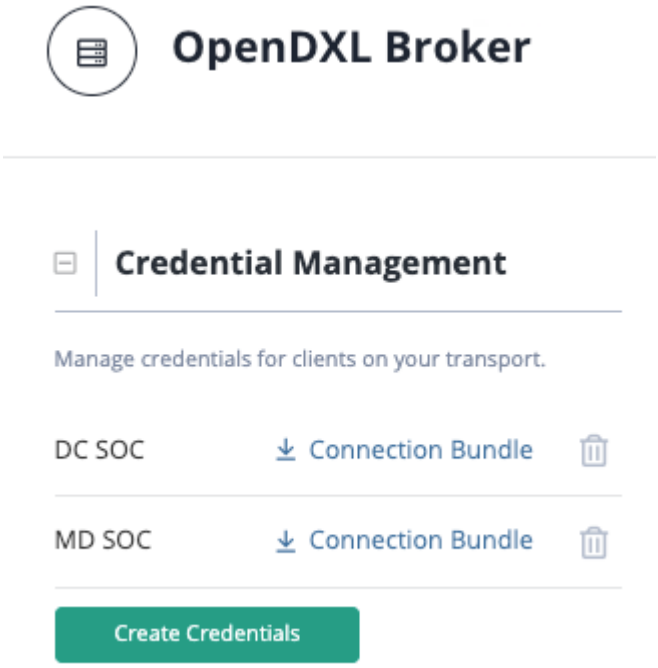
4. Enter the new Subscriber's name in the **Client Name** field.

   This name will be used to identify the subscriber in your node view.

5. **Optional -** The Hostname field displays the name of your current TQX instance, however you have the option to update this name.

6. Click the **Create Credentials** button.

   The new subscriber will be displayed in the Credential Management section.



7. Click on the **Connection Bundle** link next to the new connection to download the connection bundle. Send this file to the Subscriber to upload via their TQX instance.

Viewing Connection Details

You can view all data exchange details for your publisher instance, data transport, and subscriber instances from the OpenDXL Connections page.

Viewing Your Outgoing and Incoming Data

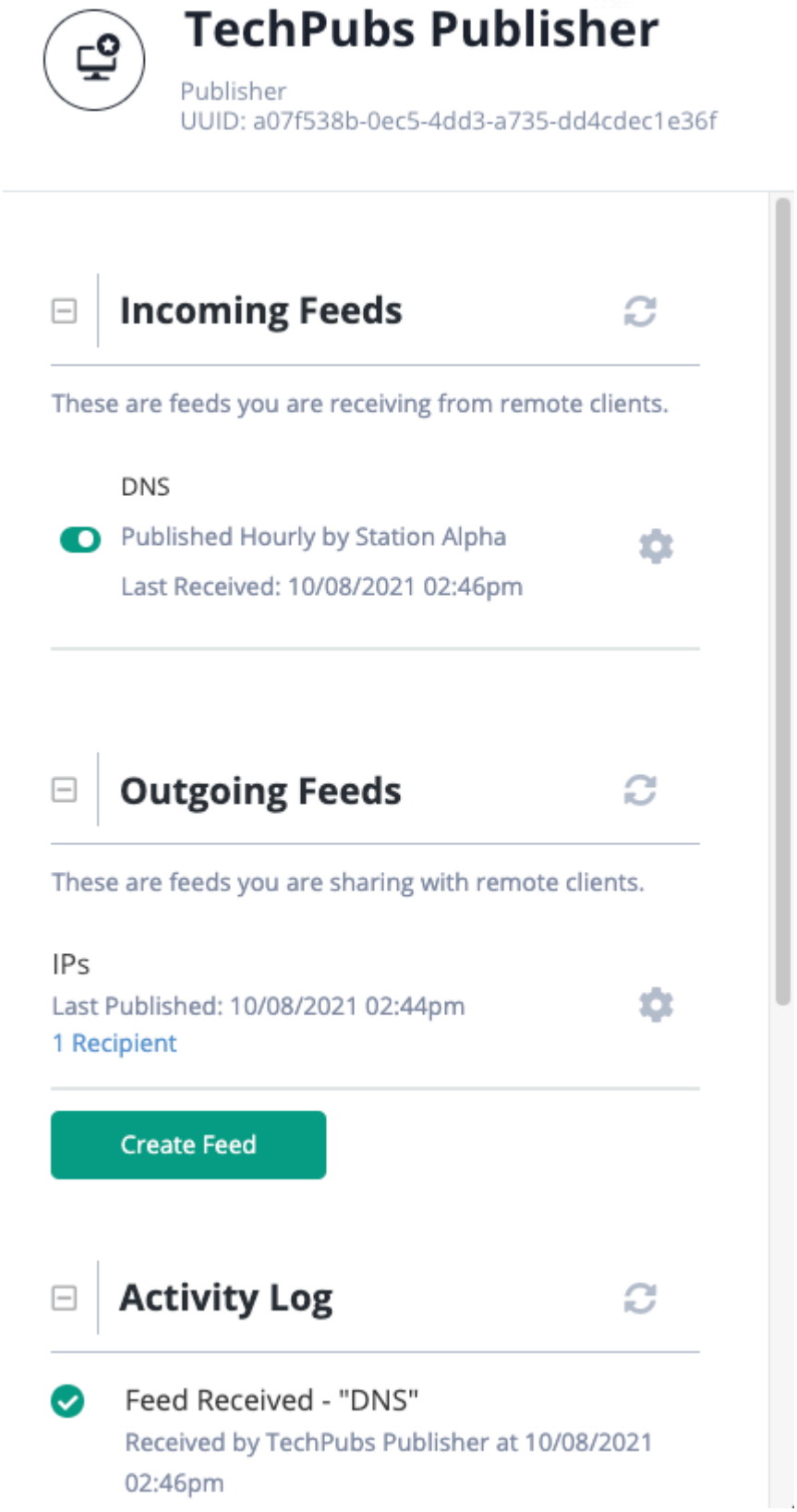
1. From the OpenDXL Connections page, click the Publisher node.

   The right pane will display the publisher details.
2. Click the +/- button next to a section to expand/minimize details.

   The following information is available:

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 section for more information on these tasks.
Outgoing Feeds	Lists the Data Collections you have shared with Subscribers.	**Editing Data Feeds** - Click the gear icon next to the feed name to access the Edit Feed screen where you can edit feed recipients, edit feed settings, and delete the feed. See the Editing a Data Feed and Data Feed Sharing Options topics for more details. **Create Data Feeds** - Clicking on the Create Feed button will open the Create Feed page - See the Creating a Data Feed for further details.
Activity Log	Lists a time/date stamp and brief description for TQX	Click the **Show More** link to expand the activity log display.

activities such as your initial setup as a Publisher.



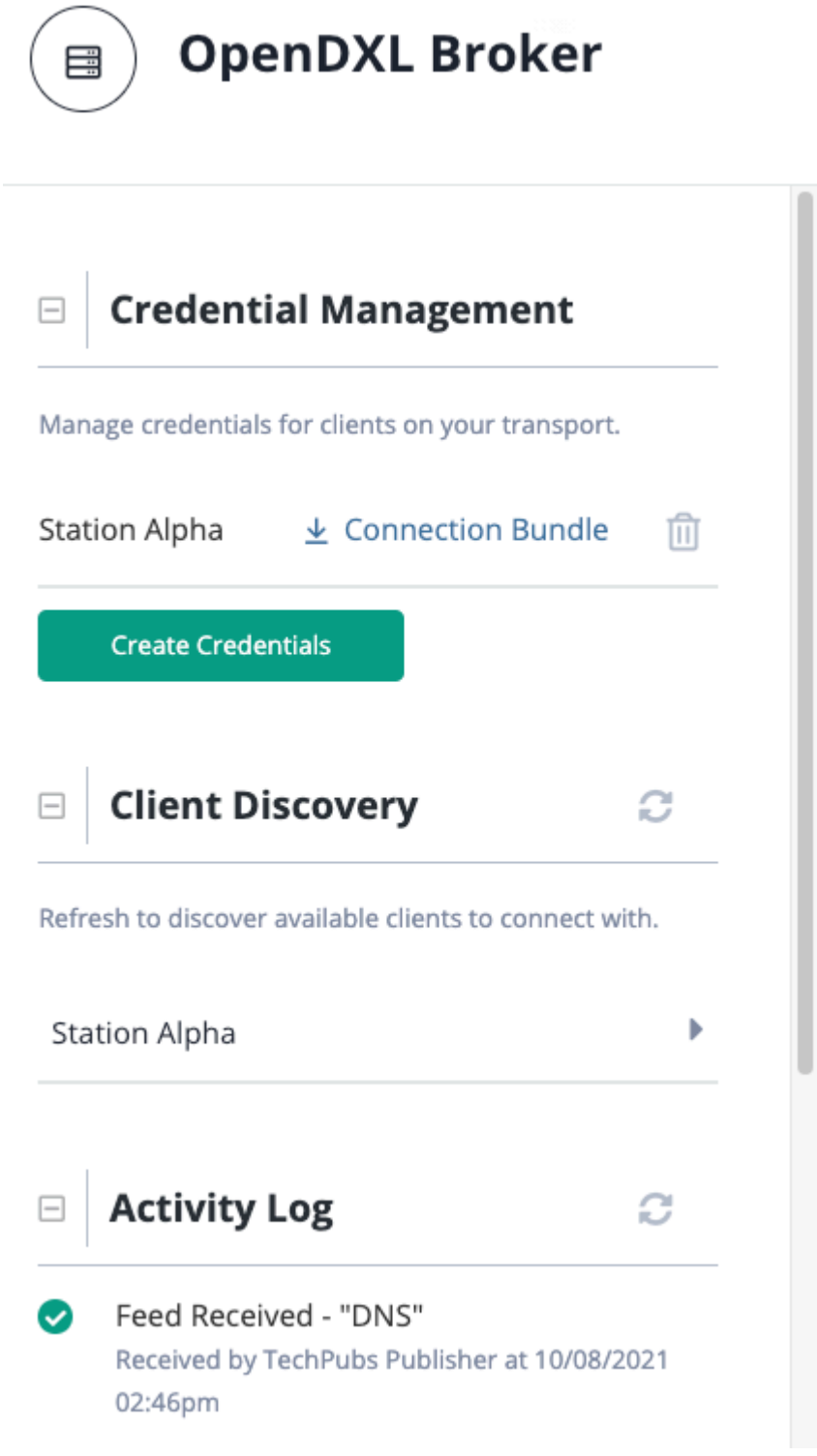
Viewing Data Transport Details

1. From the OpenDXL Connections screen, click the Data Transport node.
   The right panel will load the data transport details.
2. Click the +/- button next to a section to expand/minimize details.

   The following information is available:

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 topic 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 Feed Sharing Options 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..

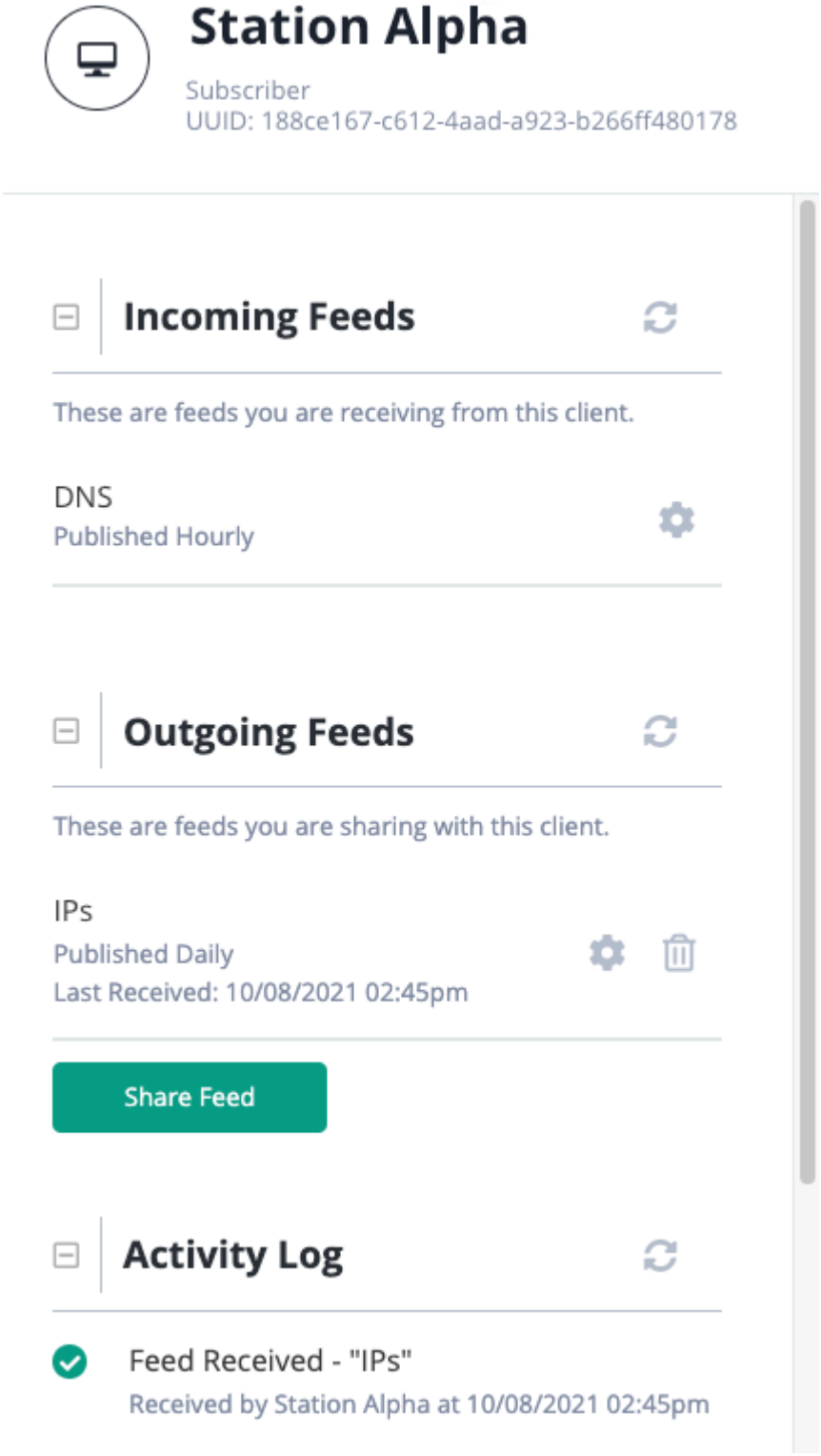


Viewing Subscriber Details

1. From the OpenDXL 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.	**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 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.



Updating 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.

Any name changes you perform on your instance will only apply to your instance.

Example: as a publisher, changing the name of a subscriber node in your connections view will not update the subscriber's name in their view on their subscriber instance.

1. From the OpenDXL 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 will confirm your change with the following message: **Node name updated**.

Name changes can take up to thirty seconds to update for all viewers on your instance.

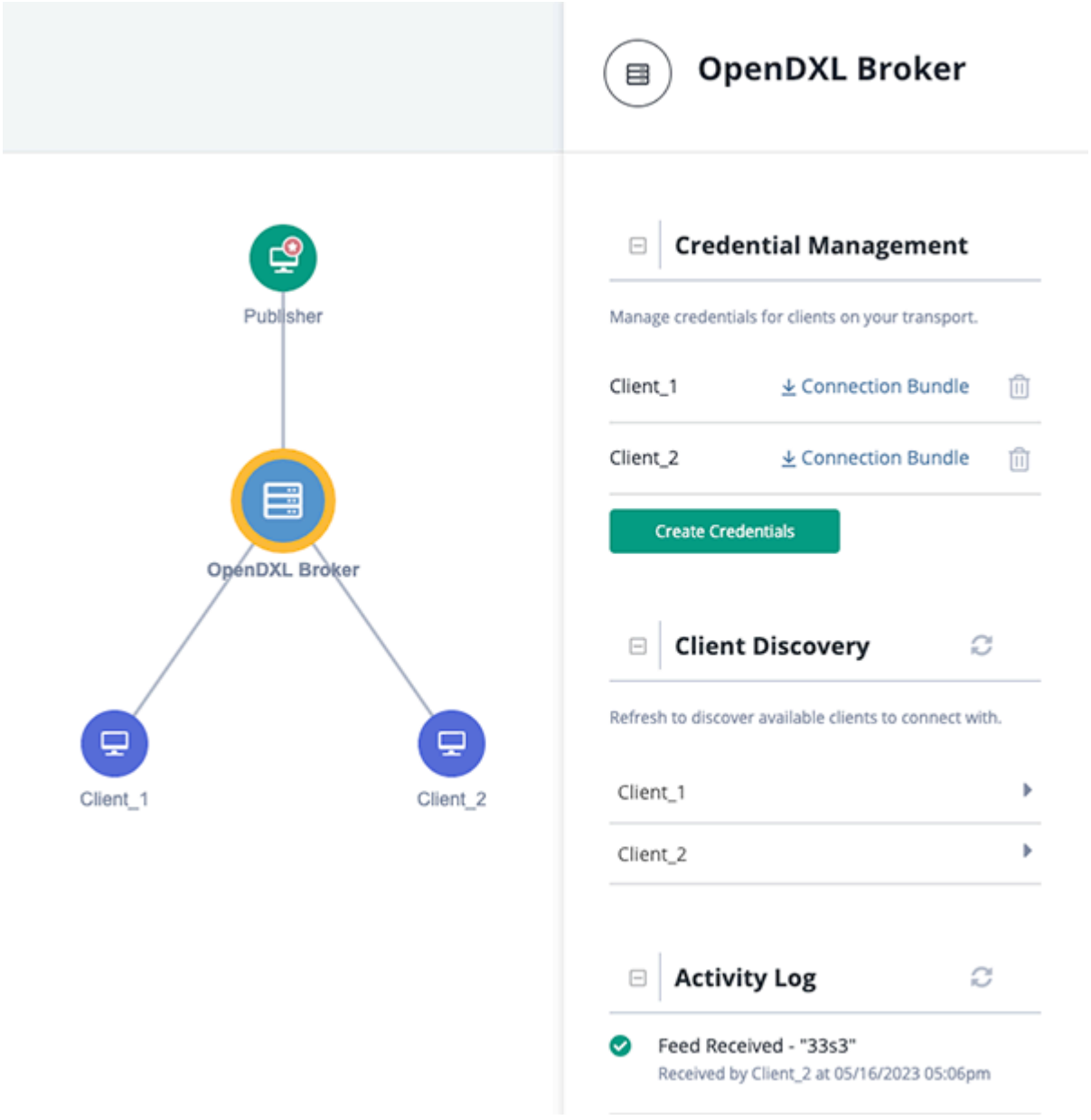
Deleting a Client Connection Bundle

Deleting a client connection bundle, which severs the connection between a publisher and subscriber, requires actions by both instances.

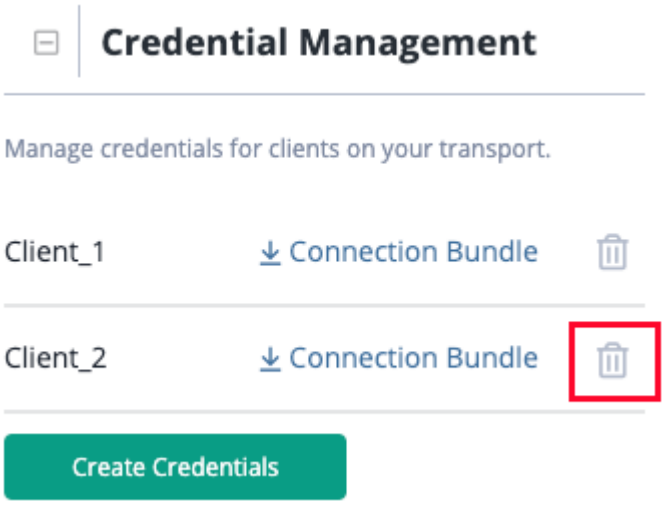
> You also elect to stop sharing all data feeds with a subscriber instead of deleting the client connection bundle.

> The steps must be performed in order. Otherwise, the discovery ping from the subscriber will result in the instances being reconnected.

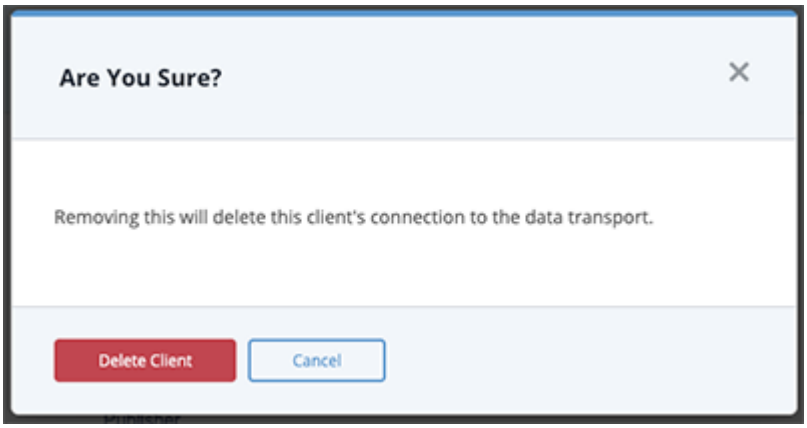
1. Instruct the subscriber to delete his data transport as described in the Deleting the Data Transport topic.
2. Navigate to the OpenDXL Connections page by clicking on the **Data Exchange** menu item and selecting **Connections**.
3. Click on the **transport node** to view its details in the right pane.


OpenDXL Broker
Publisher
OpenDXL Broker
Client_1
Client_2
Credential Management
Manage credentials for clients on your transport.
Client_1
Connection Bundle
Client_2
Connection Bundle
Create Credentials
Client Discovery
Refresh to discover available clients to connect with.
Client_1
Client_2
Activity Log
Feed Received - "33s3"
Received by Client_2 at 05/16/2023 05:06pm

4. Click on the **trashcan icon** located to the right of the connection bundle.



5. Click **Delete Transport** to confirm deletion.



The subscriber node and connection bundle listing will be removed from your view.

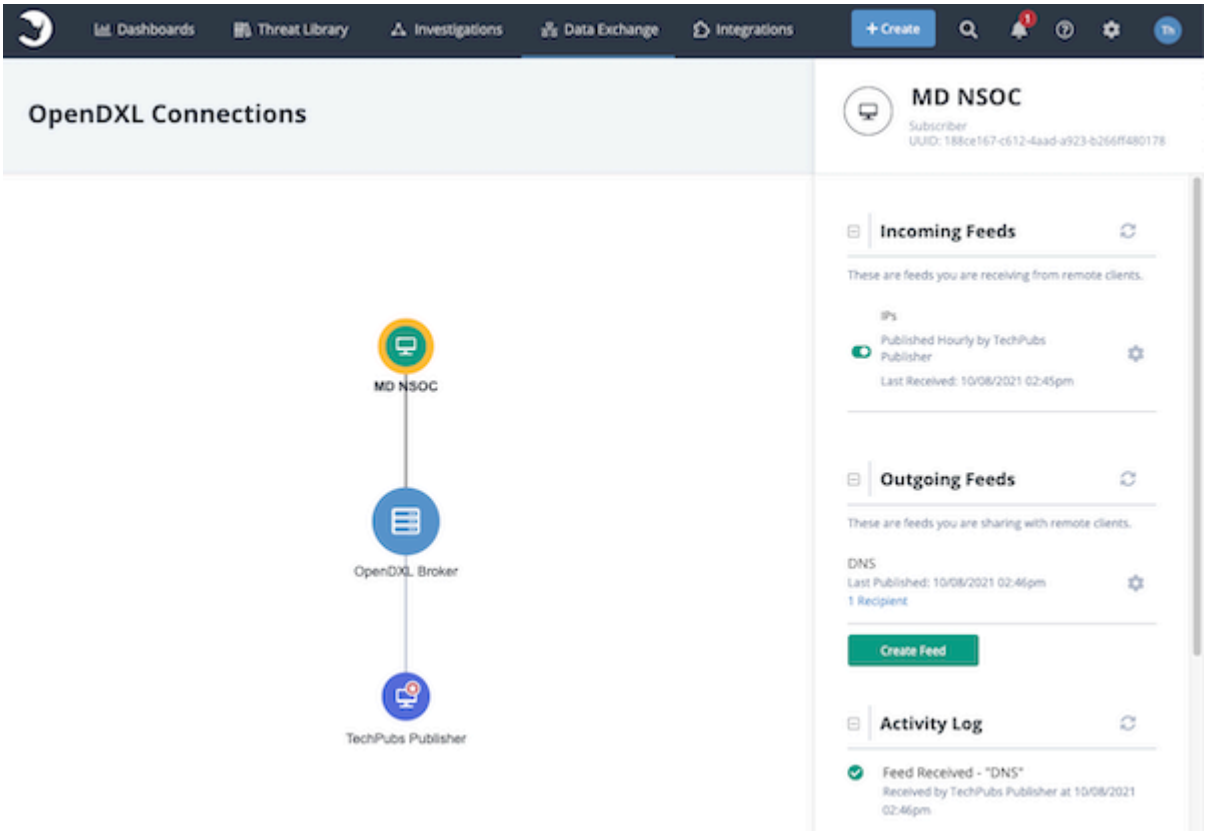
Subscriber Instances

About Subscriber Instances

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 OpenDXL Data Transport Connections section for more information on setting up your first connection.

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


Dashboards
Threat Library
Investigations
Data Exchange
Integrations
+ Create
OpenDXL Connections
MD NSOC
MD NSOC
OpenDXL Broker
TechPubs Publisher
Incoming Feeds
These are feeds you are receiving from remote clients.
IPs
Published Hourly by TechPubs Publisher
Last Received: 10/08/2021 02:45pm
Outgoing Feeds
These are feeds you are sharing with remote clients.
DNS
Last Published: 10/08/2021 02:46pm
1 Recipient
Create Feed
Activity Log
Feed Received - "DNS"
Received by TechPubs Publisher at 10/08/2021 02:46pm

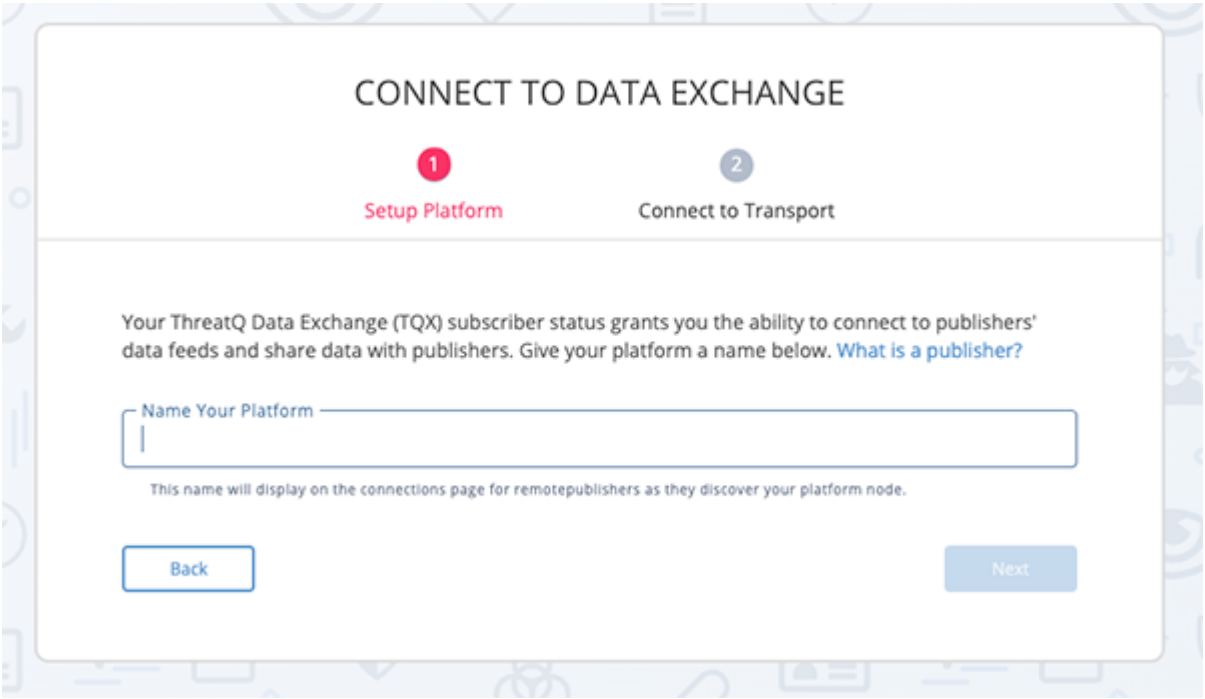
Connecting to a Publisher

As a subscriber, you can connect to a publisher to receive data feeds that have been shared your instance by the publisher. You can also create your own data feed to be shared with the publisher.

> Subscribers can only connect to a single publisher and cannot connect to another subscriber instance. Subscribers have the option of deleting the current connection they have with a publisher in order to connect with a different publisher.

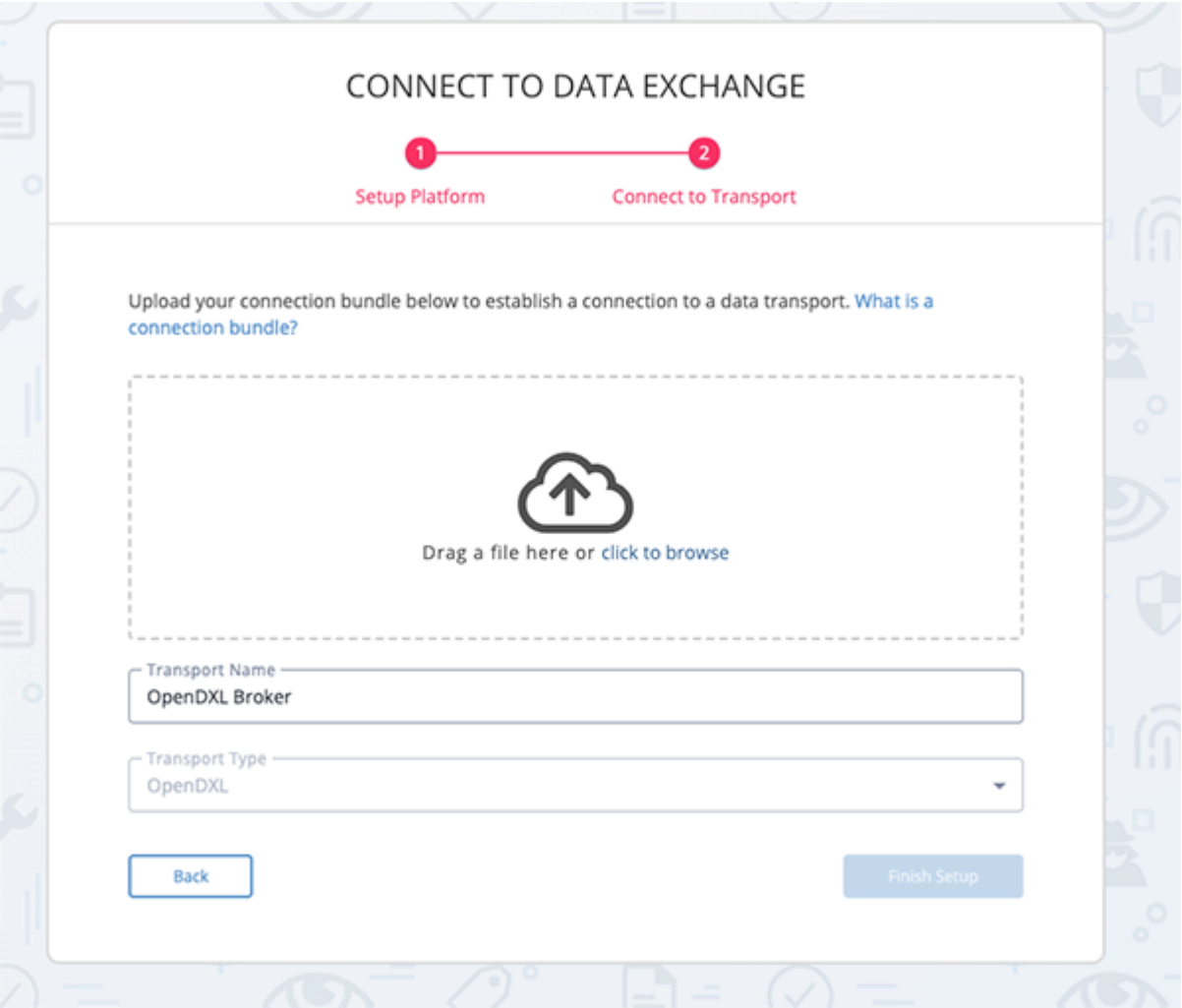
1. Click on the **Data Exchange** menu option located in the top navigation bar.

   The Connect to Data Exchange wizard will load.



2. Enter a name for your instance in the field provided. This name is what you will see your instance as in your node view. This name does not affect the publisher's view.
3. Click on **Next**.

   The Connect to Transport screen will load.



4. Optional - update the UI name for the Data Transport or leave the default - OpenDXL Broker. This name is what you will see the transport as in your node view and does not affect the publisher's view.
5. Upload the connection bundle from the publisher by either:
   - Clicking on the file and dragging it into the window
   - Using the **click to browse** option to select the file from your local machine.
6. Click on **Finish Setup**.

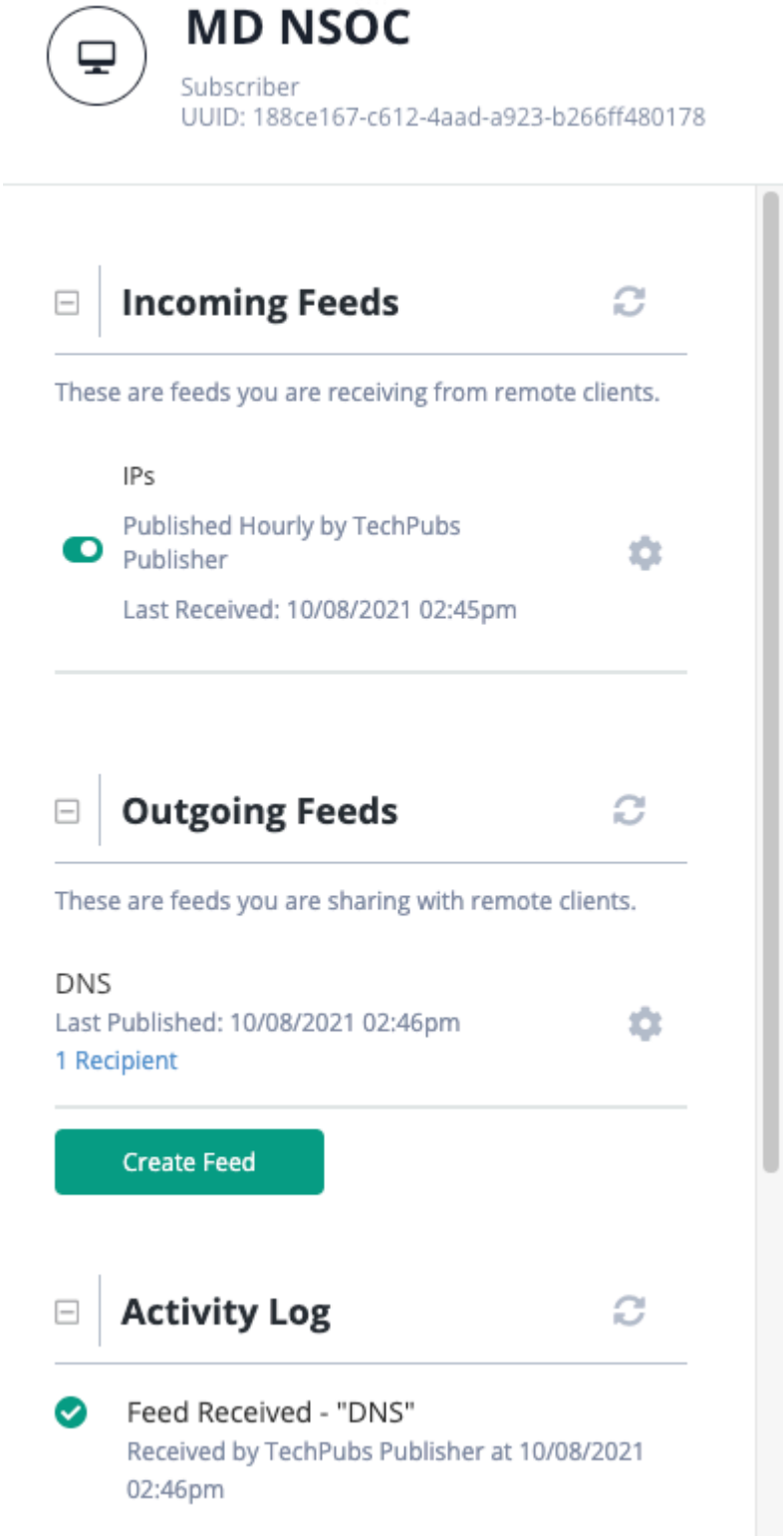
   You will now be connected to the publisher and can now subscribe to the data feeds offered by that publisher.

Viewing Connection Details

1. From the OpenDXL 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.

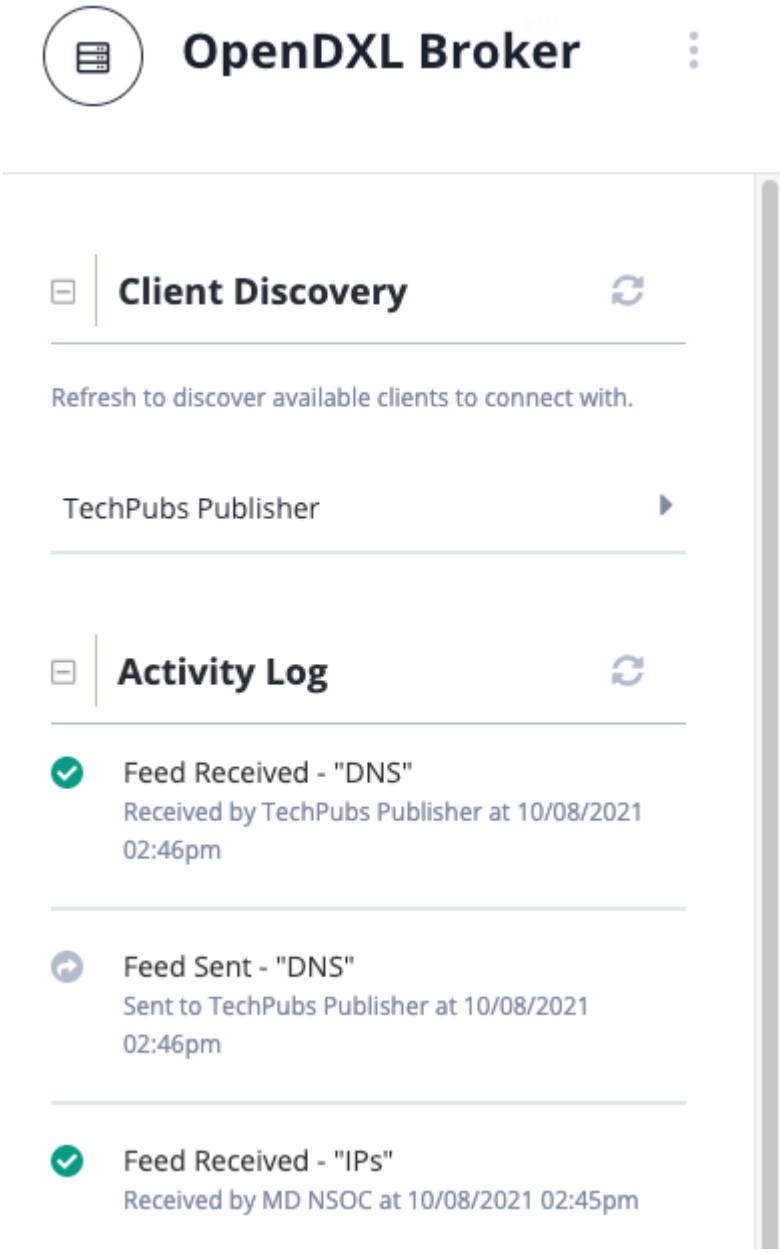


View Data Transport Details

1. From the OpenDXL 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.

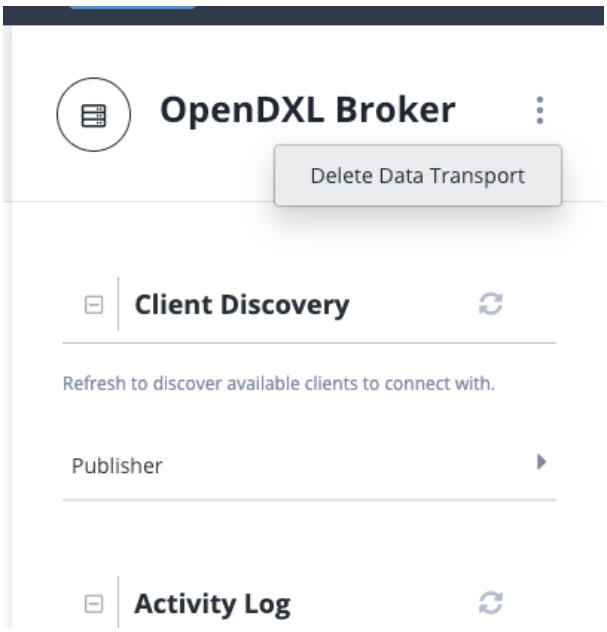

OpenDXL Broker
Client Discovery
Refresh to discover available clients to connect with.
TechPubs Publisher
Activity Log
Feed Received - "DNS"
Received by TechPubs Publisher at 10/08/2021 02:46pm
Feed Sent - "DNS"
Sent to TechPubs Publisher at 10/08/2021 02:46pm
Feed Received - "IPs"
Received by MD NSOC at 10/08/2021 02:45pm

Deleting the Data Transport

You can delete a data transport that will disconnect you from your current publisher. This will allow you to upload a new connection bundle from a different publisher instance.

> You also elect to unsubscribe from all data feeds from publisher instead of deleting the transport if you are not connecting to a new publisher instance.

1. Navigate to the OpenDXL Connections page by clicking on the **Data Exchange** menu item and selecting **Connections**.
2. Click on the **transport node** to view its details in the right pane.
3. Click on the **vertical ellipsis** to the right of the transport name and select **Delete Data Transport**.



4. Confirm deletion, when prompted, to the delete the transport.

Data Feeds

About 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.

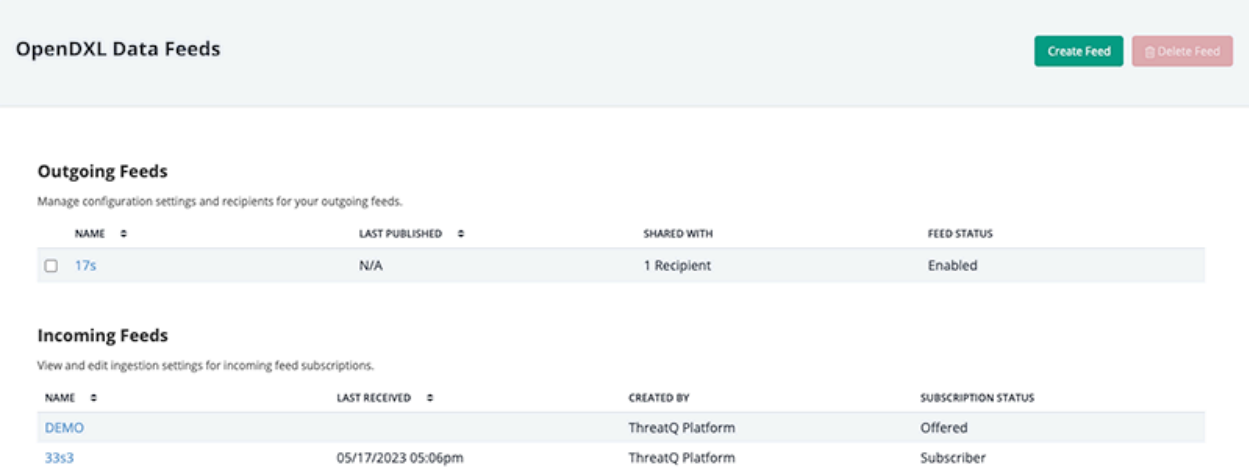
You can manage feeds from the OpenDXL Data Feeds page and the Topology View. The OpenDXL Data Feeds page allows you to create/edit feeds and provides you with a comprehensive list of the Data Feeds you send (Outgoing Feeds) and the ones you receive (Incoming Feeds). Based on the Feed type, Outgoing or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

Creating a Data Feed

Publisher and Subscriber instances can create data feeds to share. Publishers can share data feeds with all subscribers while subscribers can only share their data feeds with the publisher.

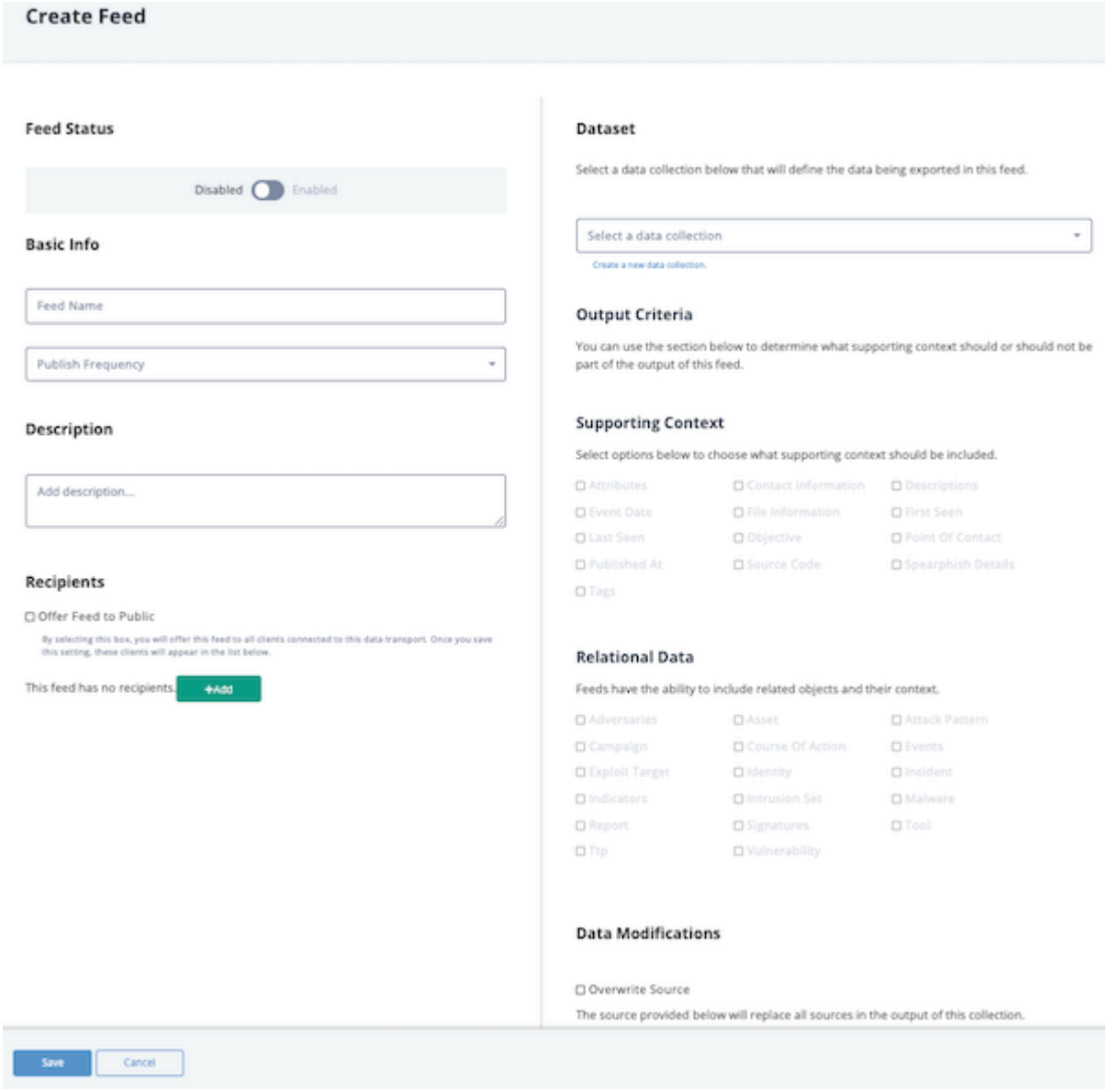
1. Click on the **Data Exchange** menu item and select **Data Feeds**.

   The OpenDXL Data Feeds page will load. Here you can view any existing incoming and outgoing feeds.



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

   The Create Feed form will load.



3. Enter a **Feed Name**. This is the name that will appear in the UI.
4. Select a **Publish Frequency** that which the feed will be sent out to other ThreatQ instances. Options include:
   - Daily
   - Hourly
5. Enter a **Description** for the data feed.
6. Select the **Recipients** to receive the data feed. You can select specific instances or enable the **Offer Feed to Public** option.

   Subscribers can only send data feeds to the publisher. Only the publisher will offered when selecting a recipient. The **Offer Feed to Public** option will not be offered. See the Data Feed Subscriptions topic for more details on subscribing and unsubscribing to a data feed.

7. Select a data collection for the **Dataset** field.

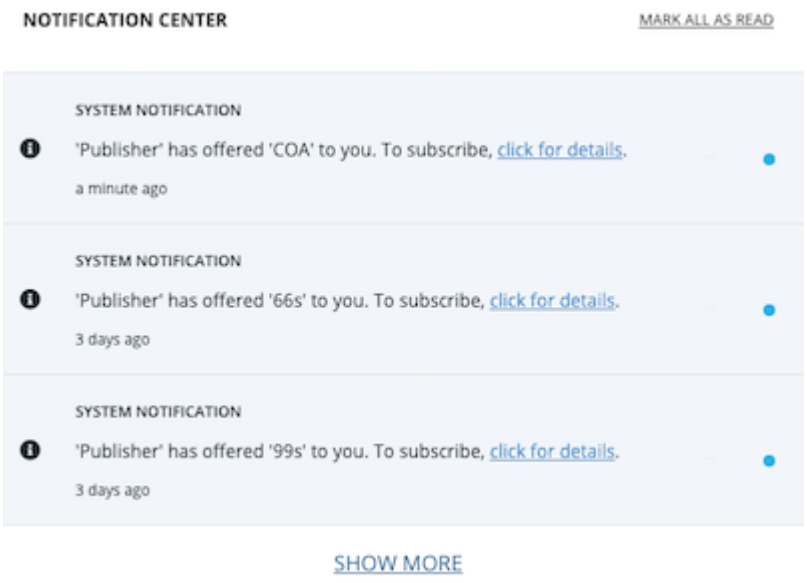
> You can also click on the **Create a New Data Collection** option to be taken to the Threat Library to create a data collection.

8. Select which **Supporting Context** will be included in the data feed using the checkboxes provided.
9. Select which **Relational Data** (related objects) to include in the data feed.
10. Use the **Override Source** checkbox under the **Data Modifications** heading and enter a name to override the default source name for the feed.

> A Subscriber can view the Data Feed source name under object sources in their object details page.

11. Click on the **Disabled/Enabled toggle** to enable the data feed.
12. Click on **Save** to create the data feed.

The OpenDXL Data Feeds page will load with the new feed listed. The recipients of the feed receive a system notification that a new feed is available for subscription. This notification includes a link to the OpenDXL Data Feeds page which allows the recipient to review feed details before subscribing.

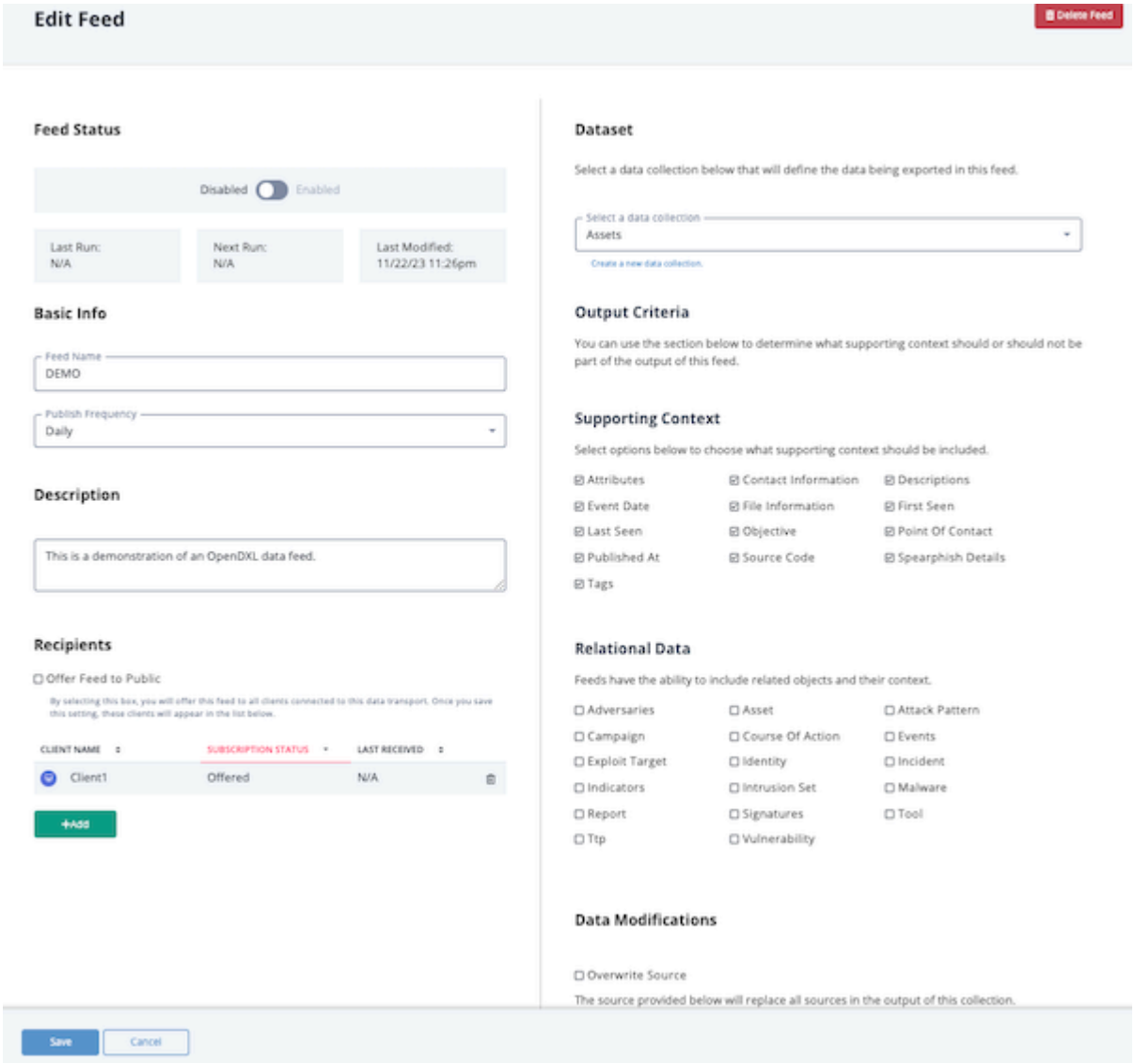


Editing a Data Feed

You can edit the name, publish frequency, data collection utilized, recipients, and what information is transmitted for an existing data feed.

1. Enter the Edit Feed page for a data feed by either:
   - clicking on the feed from the Data Feeds page.
   - clicking on the edit gear icon on the Connections Node view.

   The Edit Feed page will load.



2. Make your required edits and click on **Save**.

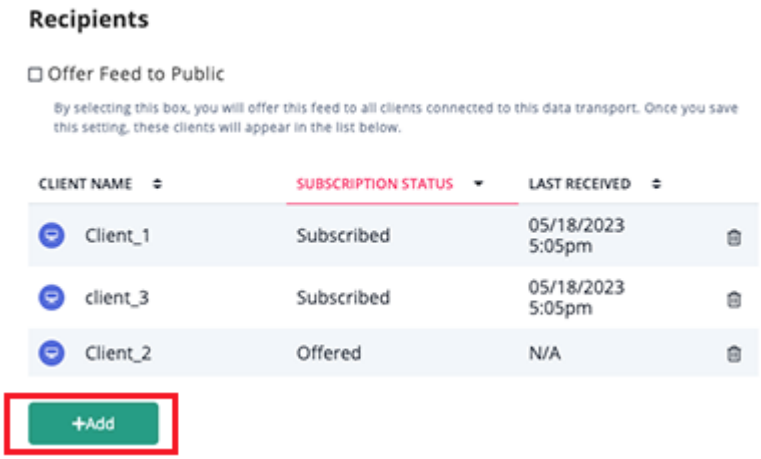
Data Feed Sharing Options

You can edit who you share your data feeds with from the data feed's details page. Publishers can share data feeds with all connected instances while subscribers can only share their data feeds with the publisher instance they are connected to in TQX. Once you have shared a feed another instance, it will appear as an offered incoming feed. The instance will then be able to subscribe to the shared feed.

Sharing a Data Feed

1. Navigate to the Data Feed's details page by either:
   - Connection Node View - clicking on the gear icon next to the data feed under the Outgoing Feeds heading.
   - Accessing the OpenDXL Data Feeds page and clicking on the data feed under Outgoing Feeds heading.
2. Click on the **Add** button under the Recipients heading to select an instance to share the data feed with.

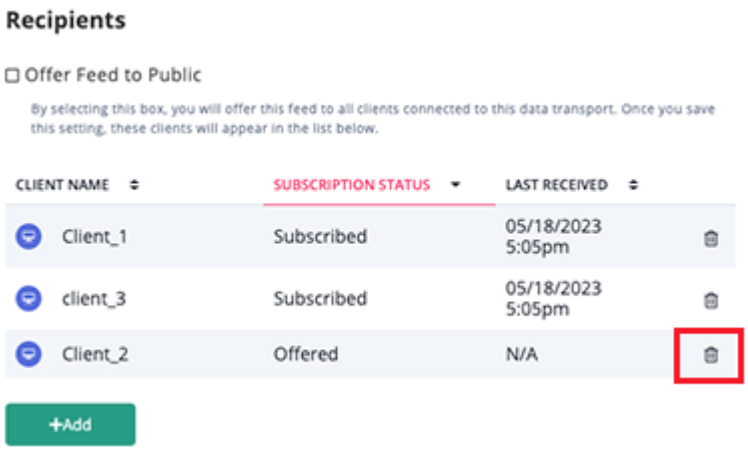
   > Publishers will have an additional option to **Offer Feed to Public**, which will share the feed with all instances connected. This option is not available to subscriber instances, who are only permitted to share data feeds with the publisher.



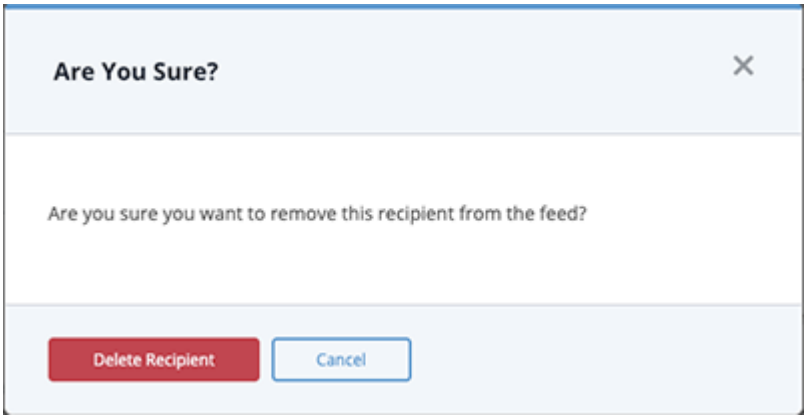
3. Click on **Save** to save your changes.

Unsharing a Data Feed from the OpenDXL Data Feed details Page

1. Navigate to the OpenDXL Data Feeds page.
2. Click on the data feed to edit under the Outgoing Feeds heading to open the Edit Feed page.
3. Locate the instance under the Recipients heading and click on the **trash icon** located to the right of row.

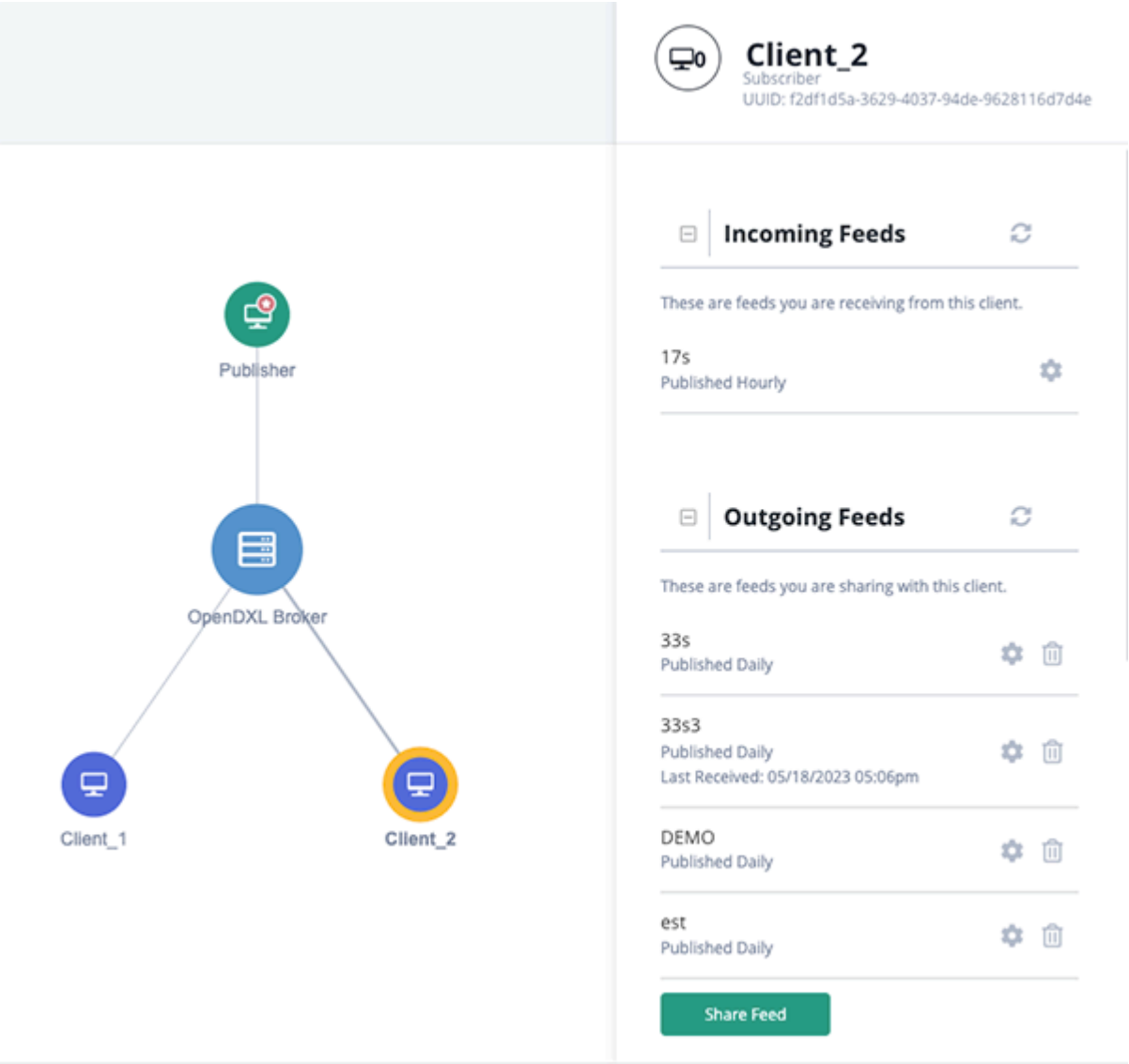


4. Click on **Delete Recipient**, when prompted, to confirm.

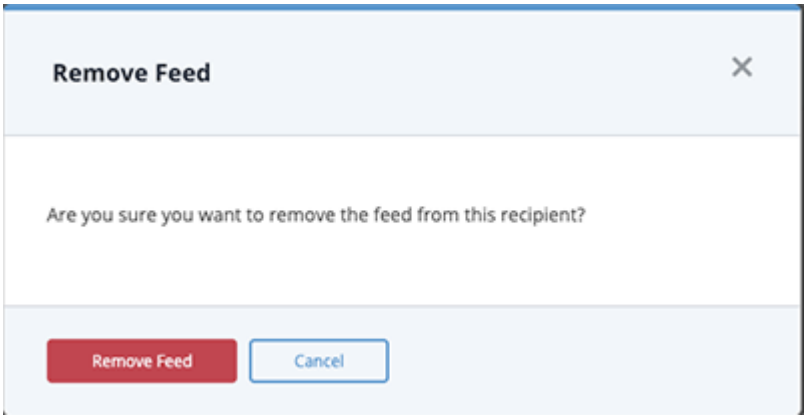


Unsharing a Data Feed from the OpenDXL Connections Node View

1. Click on the instance you no longer want to share the data feed with to load its details in the right pane.



2. Locate the data feed under the Outgoing Feeds heading and click on the **trash icon**.
3. Click on **Remove Feed**, when prompted, to confirm.



Data Feed Subscriptions

Once a data feed has been shared with you, it will appear in under your Incoming Feeds with a status of **Offered**. This indicates that the feed has been shared with your instance.

Subscribing/Unsubscribing to a Feed from the OpenDXL Connections Node View

The following provides you with steps on how to subscribe and unsubscribe to/from a data feed from the OpenDXL Connections Node view.

1. Navigate to your OpenDXL Connections Node view.
2. Click on your instance node to load its details in the right pane.
3. Locate the shared feed under the Incoming Feeds heading.

   Shared but not subscribed data feeds will be listed with a status of **Offered**.

4. Click on the enable/disable toggle switch to either subscribe or unsubscribe to the data feed.
5. If you are subscribing to a feed, you will be prompted to select the default statuses to apply to threat objects ingested from the feed. Set your default statuses and **Subscribe**.

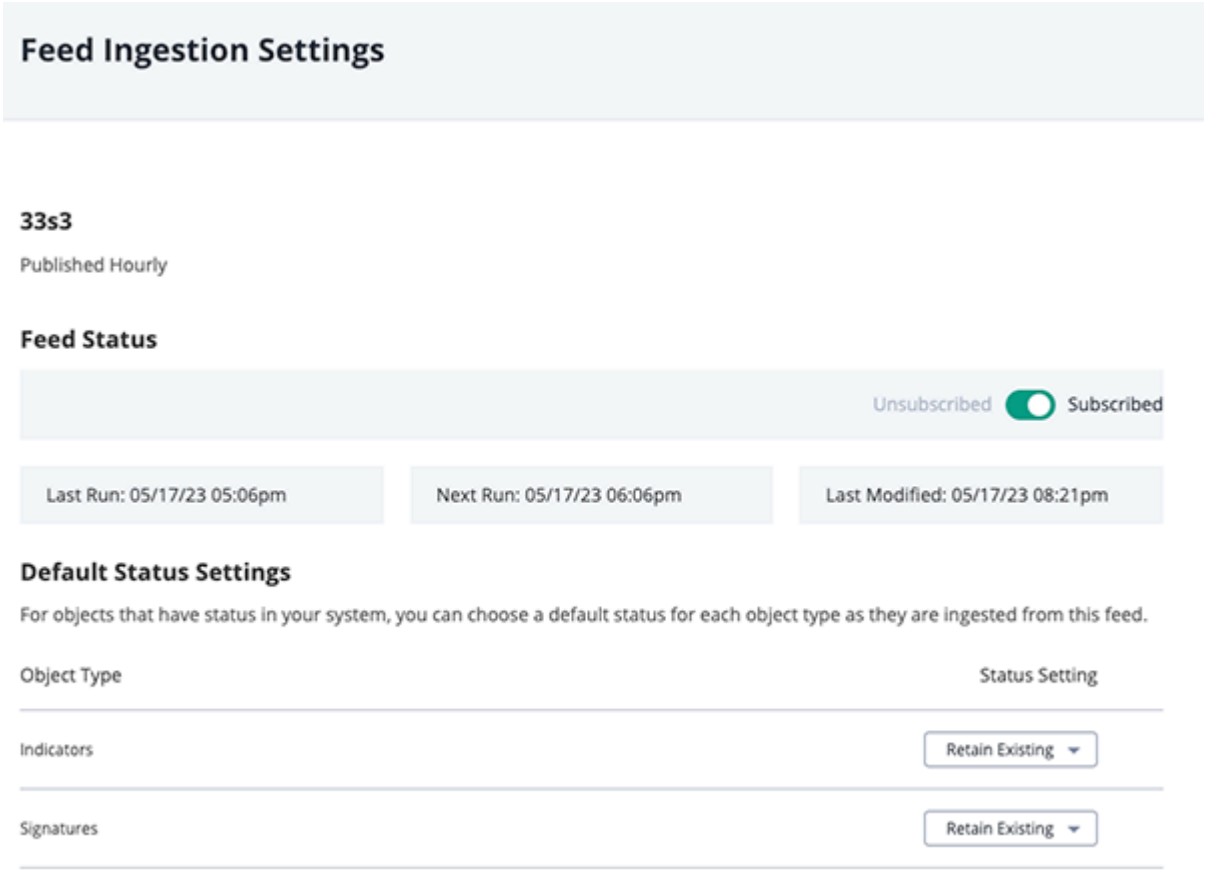
Subscribing/Unsubscribing to a Feed from the Feed Ingestion Settings Page

The following provides you with steps on how to subscribe and unsubscribe to/from a data feed from the Feed Ingestion Settings page.

1. Navigate to the OpenDXL Data Feeds page.
2. Click on the shared data feed under the Incoming Feeds header.

   Shared but not subscribed data feeds will be listed with a status of **Offered**.

3. Click on the subscription toggle option to subscribe or unsubscribe to the data feed.



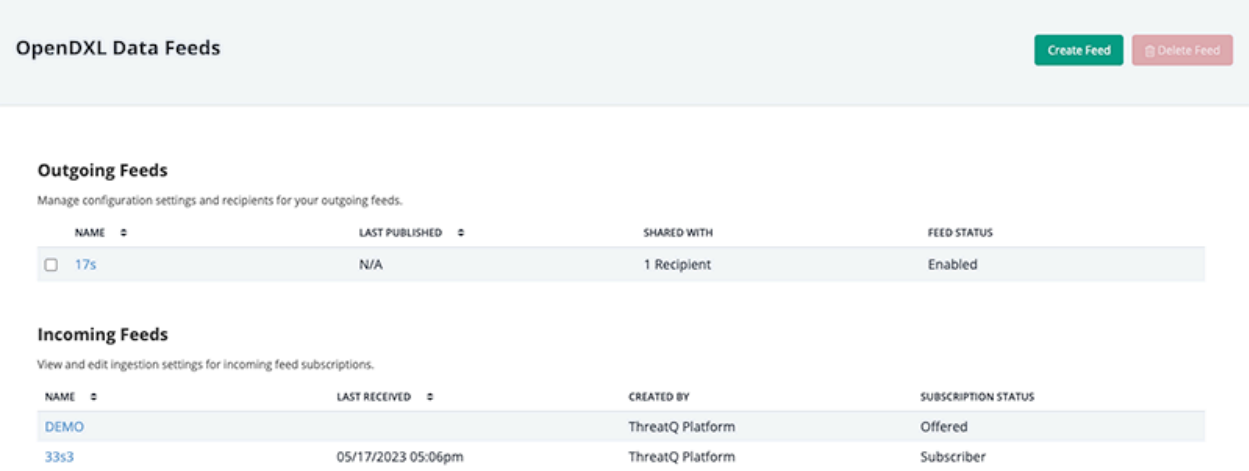
4. If you are subscribing to a feed, you will be prompted to select the default statuses to apply to threat objects ingested from the feed. Set your default statuses and **Subscribe**.

Editing Object Default Statuses

When you first subscribe to a data feed, you are prompted to select the default status of objects that are ingested. You can also update the default status that is assigned to threat data ingested by an incoming feed from the Feed Ingestion Settings page.

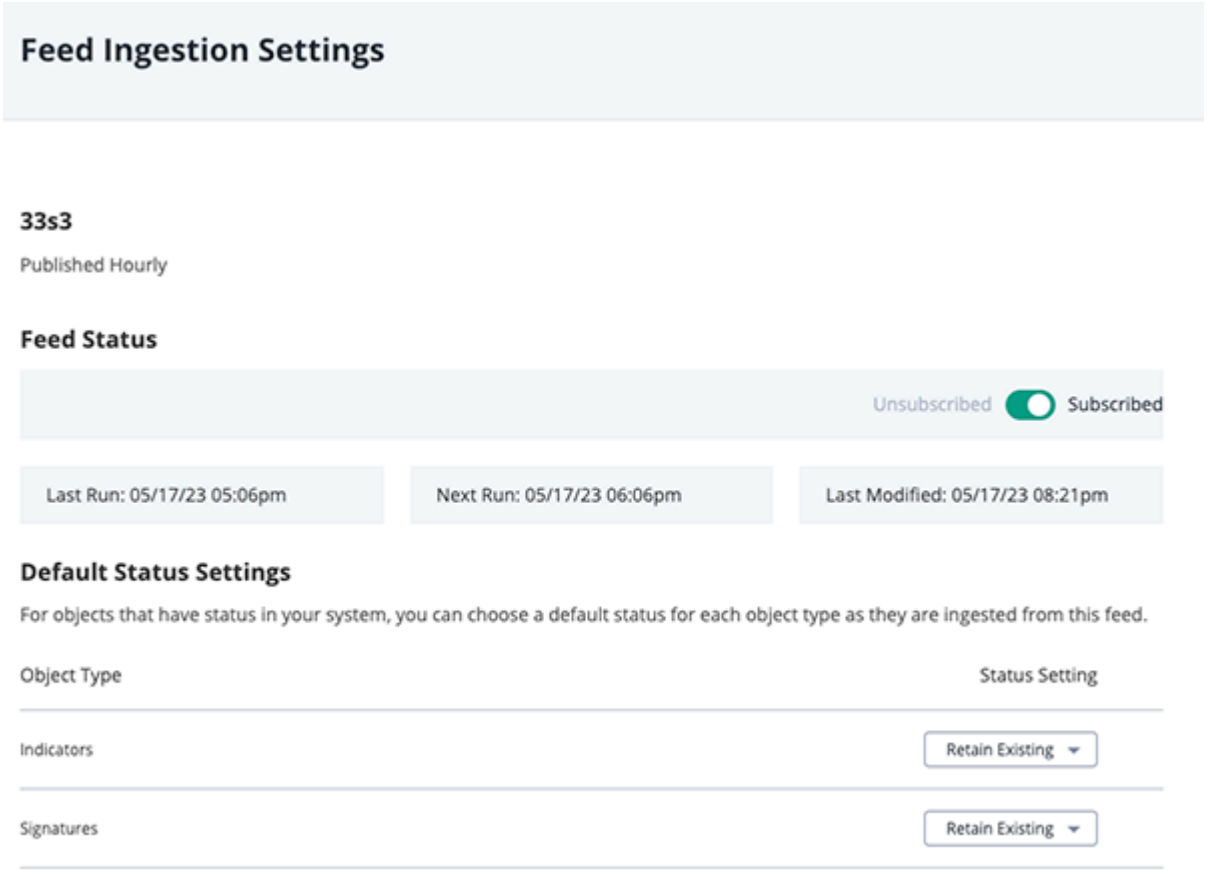
1. Click on the Data Exchange menu link and select **Data Feeds**.

   The OpenDXL Data Feeds page will load.



2. Click on a feed under the Incoming Feeds heading.

   The Feed Ingestion Settings page will load.



3. Use the dropdown menus provided to update the default status assigned to the objects as they are ingested from the data feed.

   You can also select **Retain Existing** to keep the status assigned to the object in the data feed.

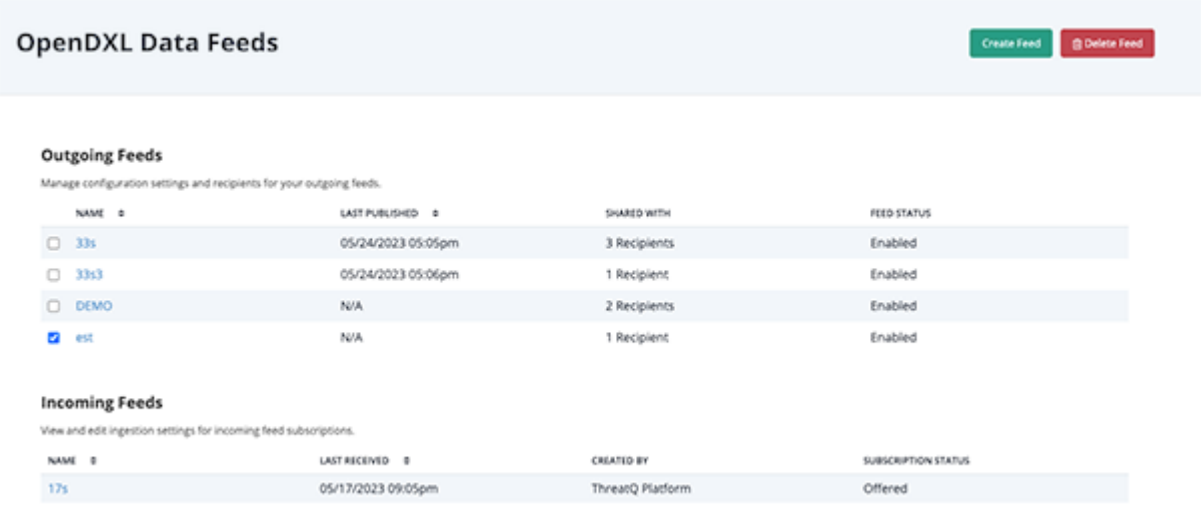
Deleting a Data Feed

You can delete your outgoing data feeds from the Data Feeds page as well as from the Edit Feed page.

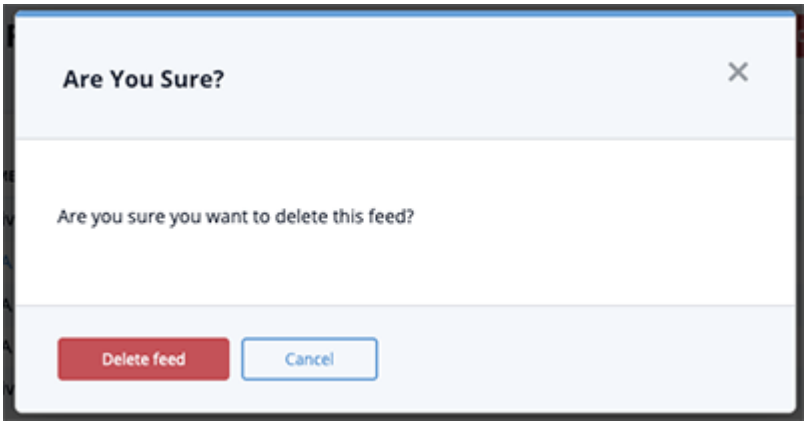
Deleting a Data Feed from the OpenDXL Data Feeds Page

You can delete one or multiple feeds at once from the Data Feeds page.

1. Navigate to the OpenDXL Data Feeds page.
2. Click on the checkboxes next to the data feed(s) to delete.



3. Click on the **Delete Feed** option located to the top right.
4. Click on **Delete Feed**, when prompted, to confirm deletion.

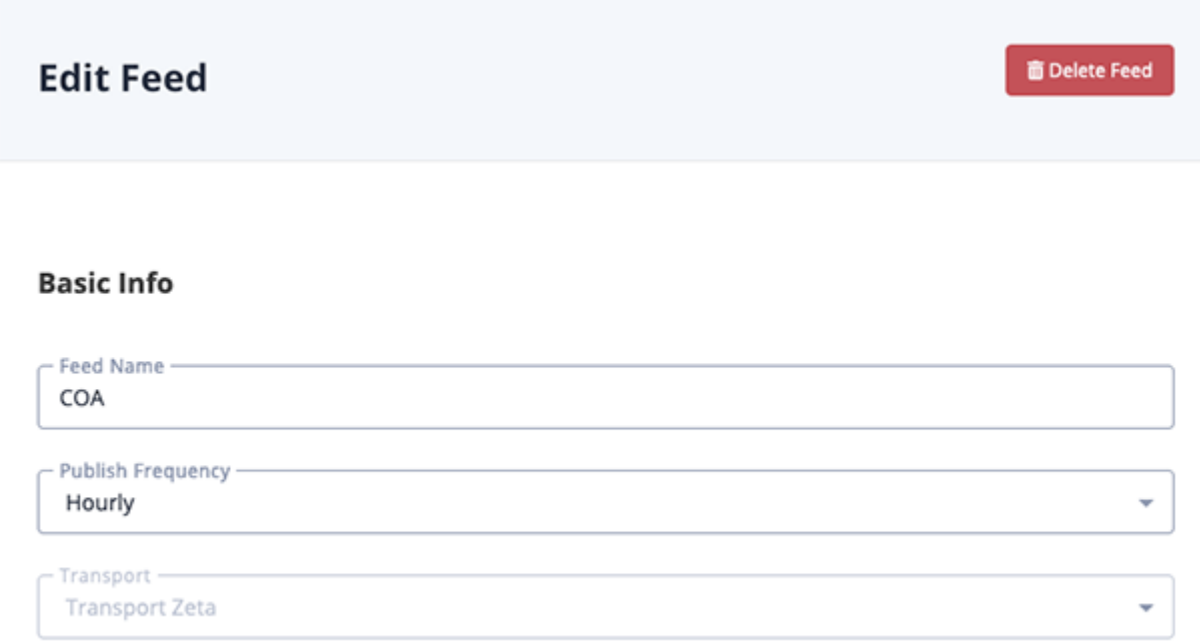


Deleting a Data Feed from the Edit Feed Page.

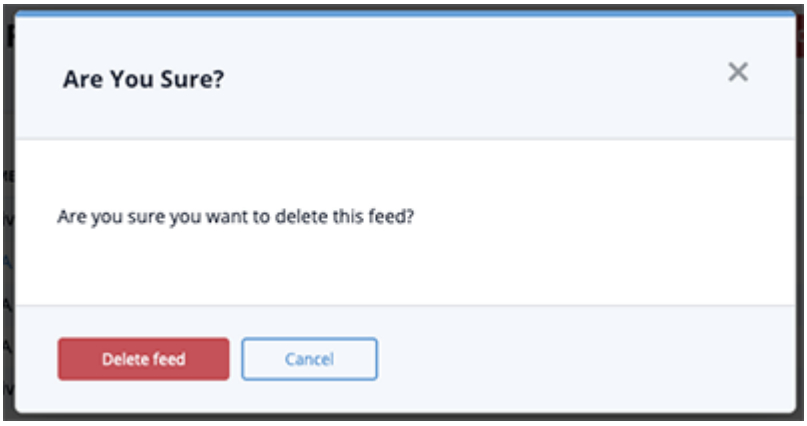
1. Navigate to the Edit Feed page for a data feed by either:
   - clicking on the feed from the OpenDXL Data Feeds page.

- clicking on the edit gear icon on the OpenDXL Connections Node view.

2. Click on the **Delete Feed** option located to the top right.



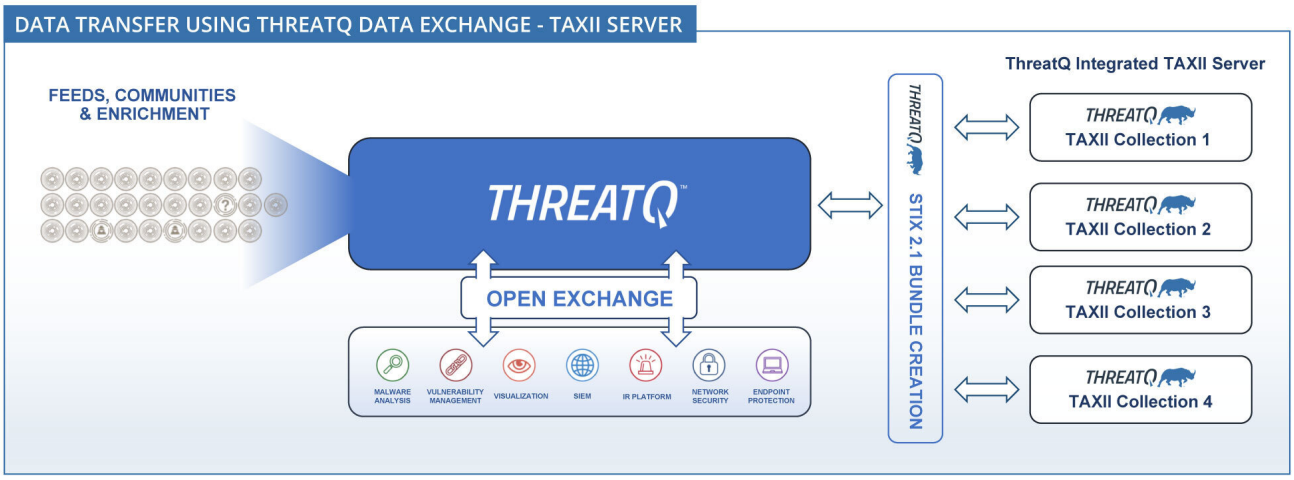
3. Click on **Delete Feed**, when prompted, to confirm deletion.



TAXII Server

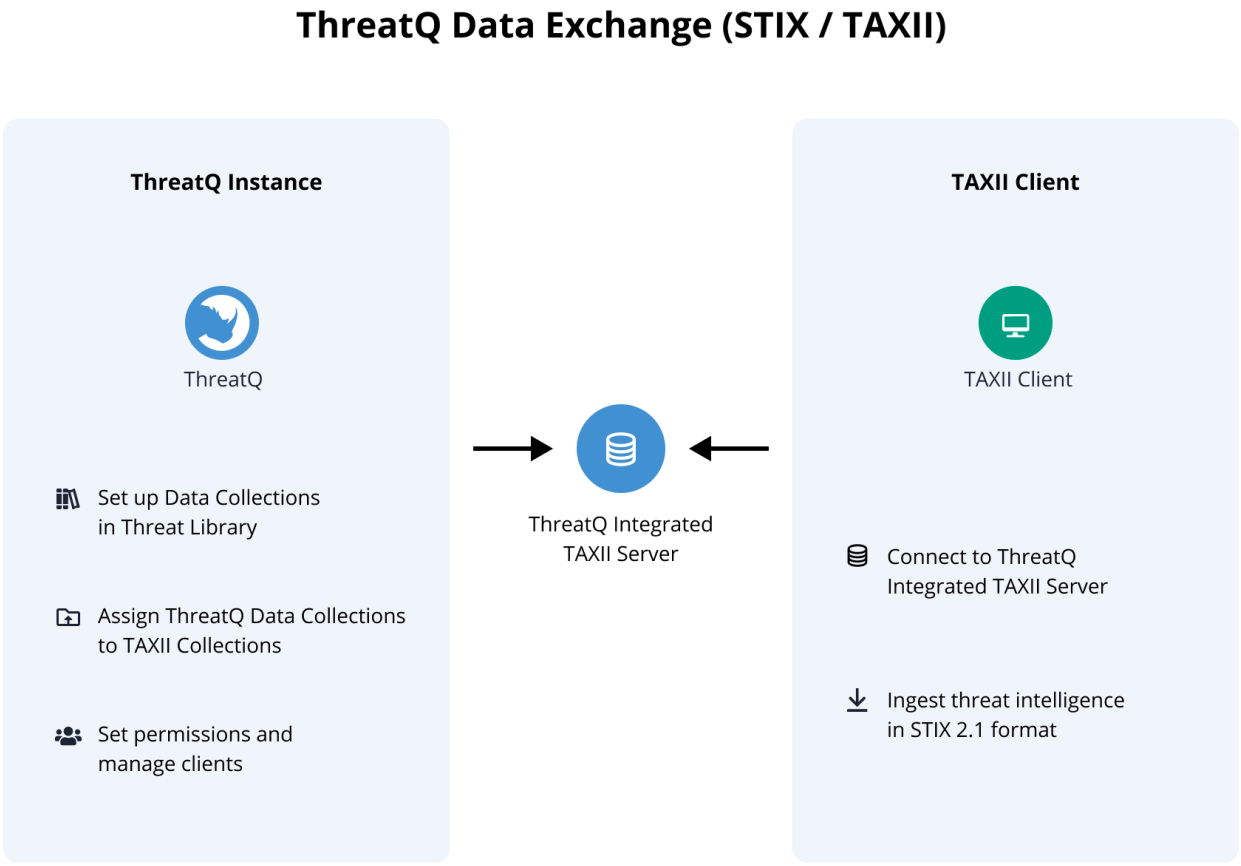
About the TAXII Server

Trusted Automated eXchange of Intelligence Information (TAXII) is a transport protocol for transmitting threat intelligence data over HTTPS. The data transported by TAXII is formatted and stored using the Structured Threat Information eXpression (STIX) language.



ThreatQ Data Exchange (TQX) allows you to configure a TAXII server, create a TAXII collection to specify the STIX object information you want to share, and add TAXII user credentials to control access to the TAXII collection files.

How It Works



Tips and Tricks

- The data collection associated with a TAXII collection can include other object types but must include at least one STIX object type and the TAXII collection will only pull STIX object data. If you update the data collection so that it no longer contains STIX objects, the TAXII collection will be empty after the next run.
- Currently, TAXII collections are published daily and include the full result set from the selected data collection, not a delta.
- When a TAXII collection is created, the first data pull will occur within 5 minutes. The next data pull will occur 24 hours after the first data pull started, unless:
  - The data collection changes.
  - The TAXII collection is disabled, and then re-enabled after 5 minutes have passed.
  - The threatq-taxii server is restarted.

  > Due to the time required to populate the data for a TAXII collection, it is not available immediately after a data pull.

- Each TAXII collection run pulls data on the newest 50K of each STIX object type. For example, if your data collection includes 150K objects, of which 75K are adversaries, 80K are campaigns,

and the remainder are not STIX objects, the TAXII collection run will pull information on the newest 50K adversaries and 50K campaigns.
- TAXII collections do not include additional context of relational data for STIX objects.
- Currently, TQX only supports the use of a Third Party application to access STIX data from your TAXII server. TQX does not support the use of the TAXII server to transfer STIX object data between ThreatQ instances.
- If you delete the data collection associated with a TAXII collection, the TAXII collection is automatically disabled.

STIX Objects

ThreatQ TAXII collections can include the following system objects:

- Adversaries
- Attack Pattern
- Campaign
- Course of Action
- Identity
- Indicators
- Intrusion Set
- Malware
- Tool
- Vulnerability

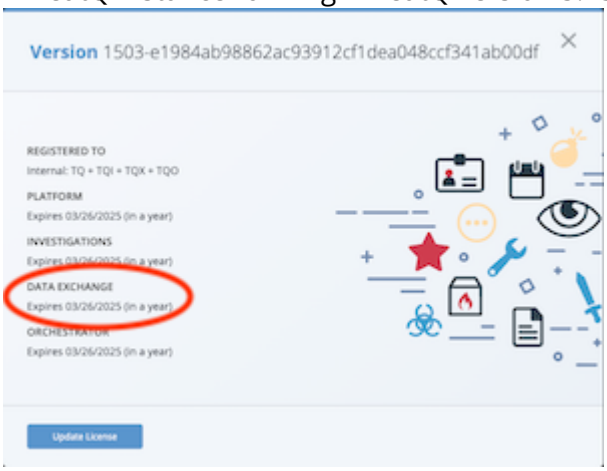
For indicators, TAXII collections can include the following indicator types:

- ASN
- Binary String
- CIDR Block
- CVE
- Email Address
- Email Attachment
- Email Subject
- File Path
- Filename
- FQDN
- IP Address
- IPv6 Address
- MAC Address
- MD5
- Mutex
- Password
- SHA-1
- SHA-256
- SHA-512
- x509 Serial
- x509 Subject
- URL
- User-agent
- Username
- X-Mailer

TAXII Server Requirements

The following is a list of the minimum requirements to configure and use the ThreatQ Data Exchange TAXII server:

- ThreatQ instance running ThreatQ version 5.23+ with a TQX license.



- Data Collection that includes STIX object types.
- ThreatQ login with Administrative or Maintenance access.
- SSL certificate in the NGINX host directory.

> If you are upgrading from ThreatQ v5.22.0 or later, the upgrade process moves your certificate automatically. If you are upgrading from an earlier 5x version, see Configuring Your SSL Certificate for NGINX for more information on moving your certificate.

Configuring Your SSL Certificate for NGINX

The TAXII server resides behind an NGINX proxy to handle incoming traffic. The NGINX proxy listens on an available port and proxies traffic to the TAXII server container. It also uses the same SSL certificates available for the Apache server for HTTPS traffic.

When you upgrade from 5.22 or later, the TQAdmin tool automatically moves your existing certificate to `/etc/docker/nginx/ssl` and concatenates the certificate authority (CA) to the certificate. The certificate is then used in the NGINX container at startup. If your environment does not have a CA certificate, NGINX uses `/etc/pki/tls/certs/localhost.crt` by default.

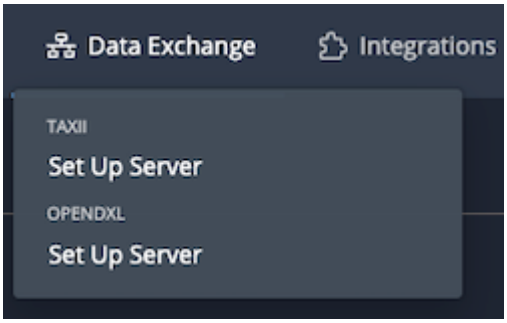
If you are upgrading to 5.23 or later from an earlier version than 5.22, use the following steps to configure your SSL certificate for use by NGINX:

1. Place your certificate files in the host directory `/etc/docker/nginx/ssl`. They will be automatically accessible to the container at the same path (/etc/docker/nginx/ssl).
2. Concatenate your domain certificate and the intermediate certificate into a single file. Ensure the domain certificate comes first, followed by the intermediate certificate.
   ```
   cat /etc/docker/nginx/ssl/yourdomain.crt /etc/docker/nginx/ssl/
   intermediate.crt > /etc/docker/nginx/ssl/yourdomain_combined.crtcat
   ```
3. Use the resulting concatenated file for the ssl_certificate directive in your NGINX configuration.
4. Configure SSL by adding certificate and private key details to `/etc/docker/nginx/conf.d/ssl-cert-paths.conf`.

   Example NGINX Configuration:
   ```
   [~]# cat /etc/docker/nginx/conf.d/ssl-cert-paths.conf ssl_certificate /
   etc/docker/nginx/ssl/yourdomain_combined.crt; ssl_certificate_key /etc/
   docker/nginx/ssl/yourdomain.key;
   ```

Getting Started - Configuring the TAXII Server

From the Data Exchange Menu select the Set Up Server option under the TAXII section.

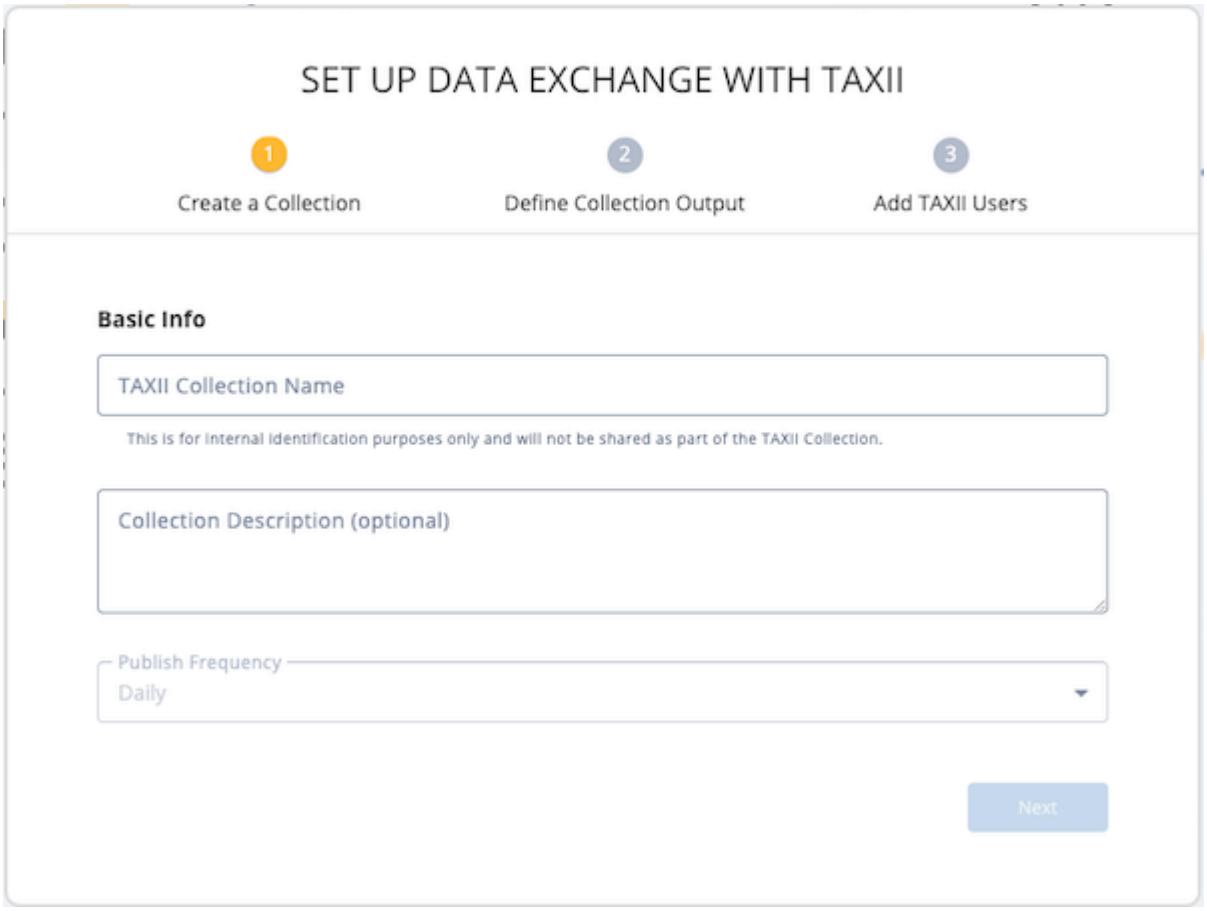


The Set Up Data Exchange with TAXII wizard opens. This wizard guides you through configuring your TAXII server, creating your first TAXII collection, selecting the data collection for the TAXII collection, and adding TAXII user credentials.

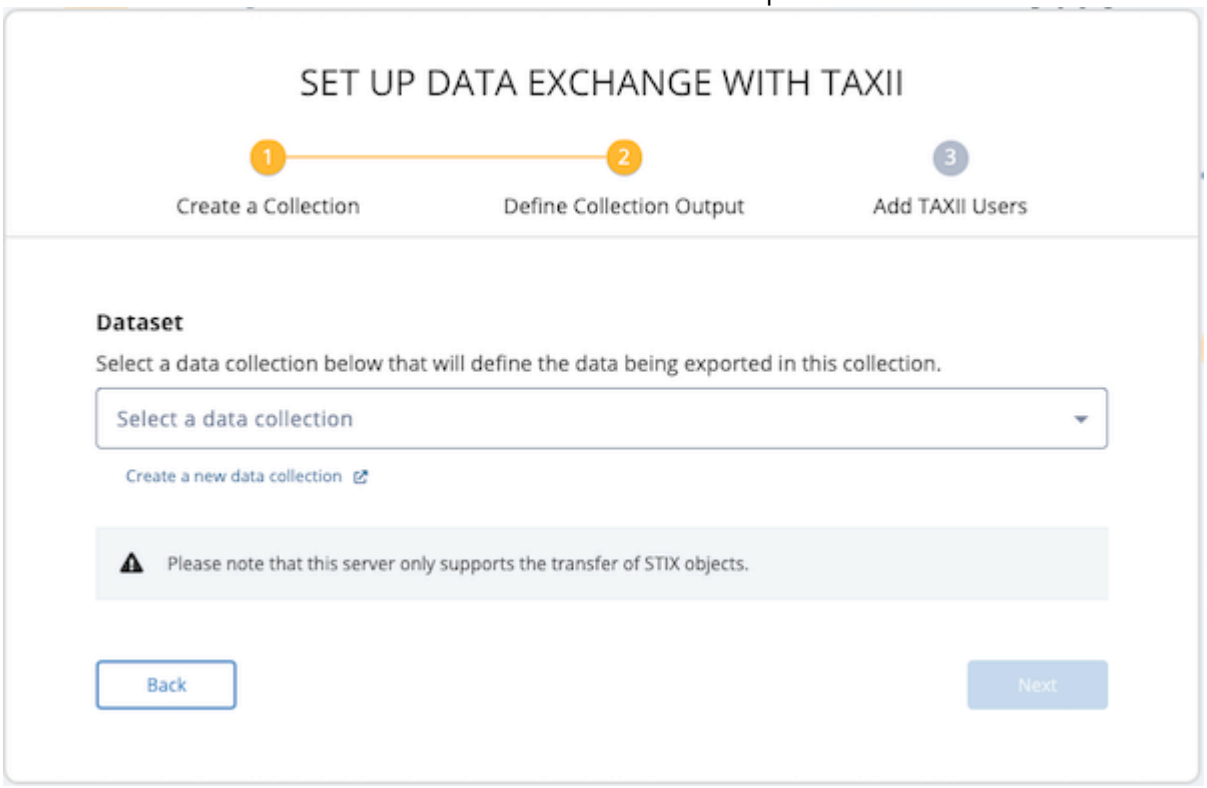
> This wizard is only available for the initial configuration of your TAXII server. To access it again, you must delete all existing TAXII collections and credentials. After doing this, you may need to clear your browser cache to access the Set Up Server option.

1. In the Create a Collection section, enter the name of the new TAXII collection and a brief description of the collection (optional). The Publish Frequency defaults to Daily.

   > You can click and drag the lower right corner of the Collection Description field to expand it.



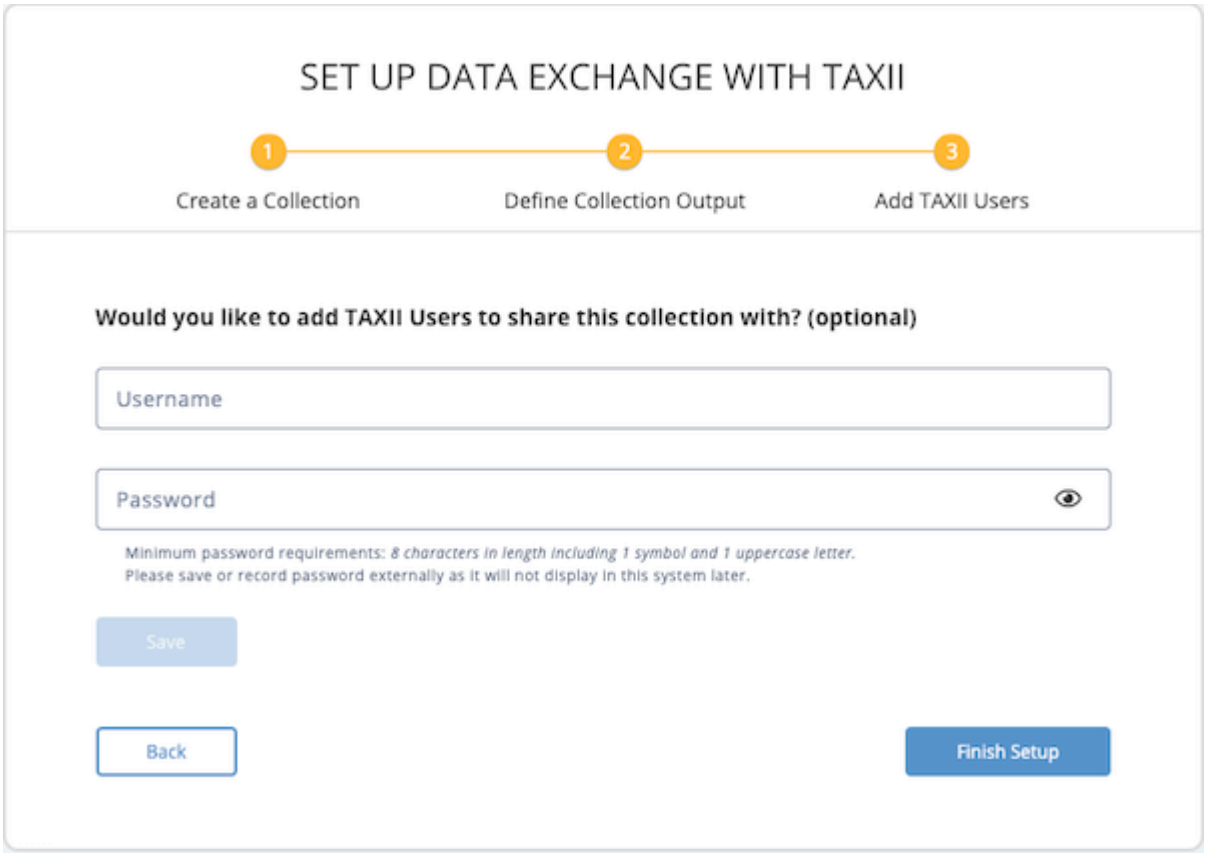
2. Click the **Next** button to move to the Define Collection Output section.



3. From this section, use one of the following methods to specify a data collection for the TAXII collection:
   - **Select an existing data collection** - Click the Select a data collection field and select an existing data collection.
   - **Create a new data collection** - Click the Create a new data collection option to access the Threat Library in another tab and create a new data collection.

   > The selection field only lists data collections that you have permission to access and that include STIX objects. The data collection can include other object types but must include STIX objects and the TAXII collection will only pull STIX object data.

4. Click the Next button to move to the Add TAXII Users section.



5. Optional. From this section, add the first TAXII user by entering the username and password. Go to step 6.
   Or, go to step 7 to finish creating the TAXII collection without adding users.

   > To view the password you entered, click the eye icon in the right side of the field.

   > Be sure to capture the TAXII password information you enter. This information is encrypted and not viewable after entry. If misplaced, you cannot retrieve the password. However, you can assign a new password.

6. Click the **Save** button to save the user entry. Then, click the **Add User** button to add another. Repeat this process as needed to add more users.

   From the Add TAXII Users section, you can use the edit or delete icons to update your entries.

7. After you enter the TAXII users, click the Finish Setup button. The TAXII Users & Collections screen is displayed.

   When you create a TAXII collection, every Admin user is assigned read-only permission for the associated data collection unless they already have permission to access it. In addition, each time you add a new Admin user, the new user is automatically granted viewer permissions for any data collections associated with a TAXII collection.

8. Before you can enable a TAXII collection, it must have at least one user. Then, you can click the toggle next to the TAXII Collection name to enable it.
   When you enable a TAXII collection, the first data pull begins in five minutes. The next data pull occurs twenty four hours later.

TAXII Collections

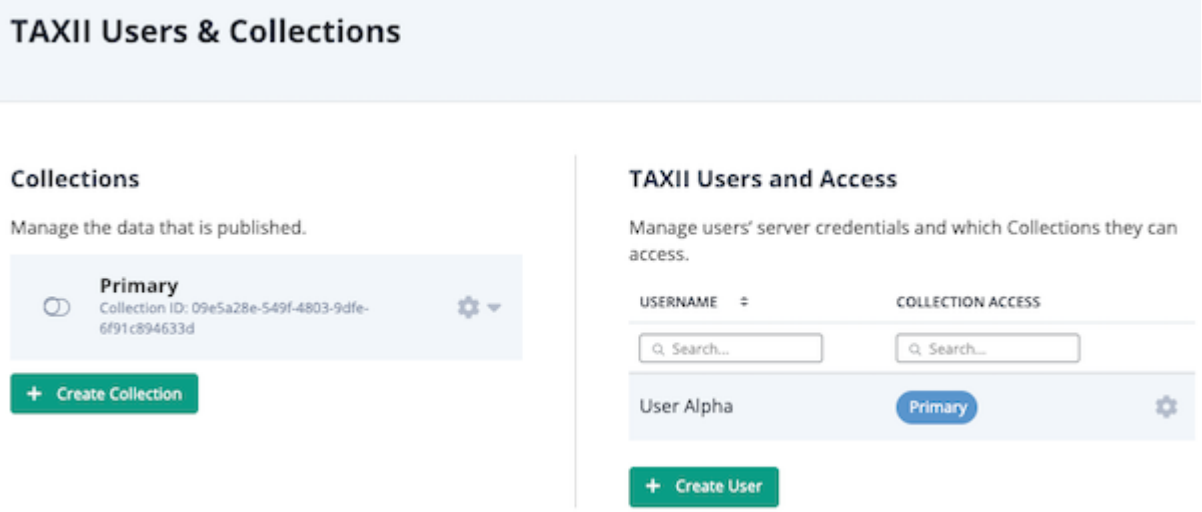
About TAXII Collections

A TAXII collection is a collection of STIX objects configured in the ThreatQ Platform and sent as a STIX Bundle to the TAXII Server where it can be retrieved from a TAXII API Endpoint. To create a STIX bundle, ThreatQ converts the information in a Data Collection to STIX format.

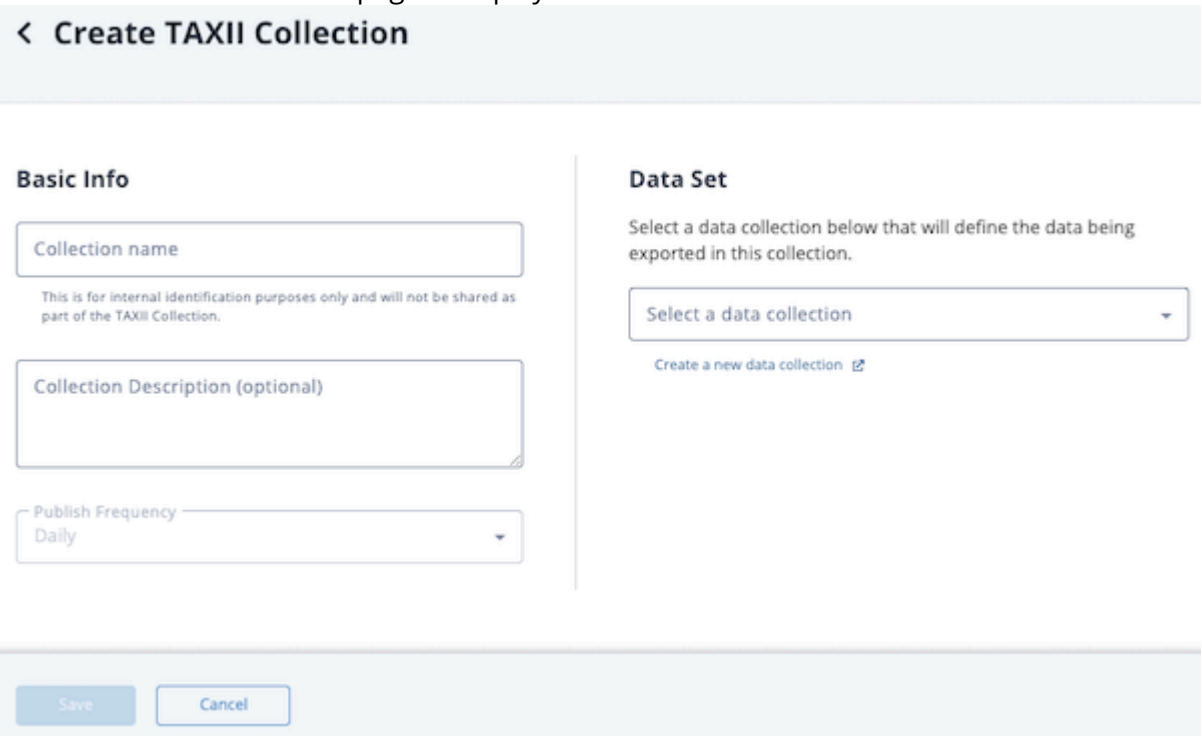
Creating a TAXII Collection

After you set up your TAXII server and first TAXII collection, you can use the TAXII Users & Collections page to create additional collections.

1. From the Data Exchange Menu select the Users & Collections option under the TAXII section. The TAXII Users & Collections page is displayed.



2. Click the **Create Collection** button.
The Create TAXII Collection page is displayed.



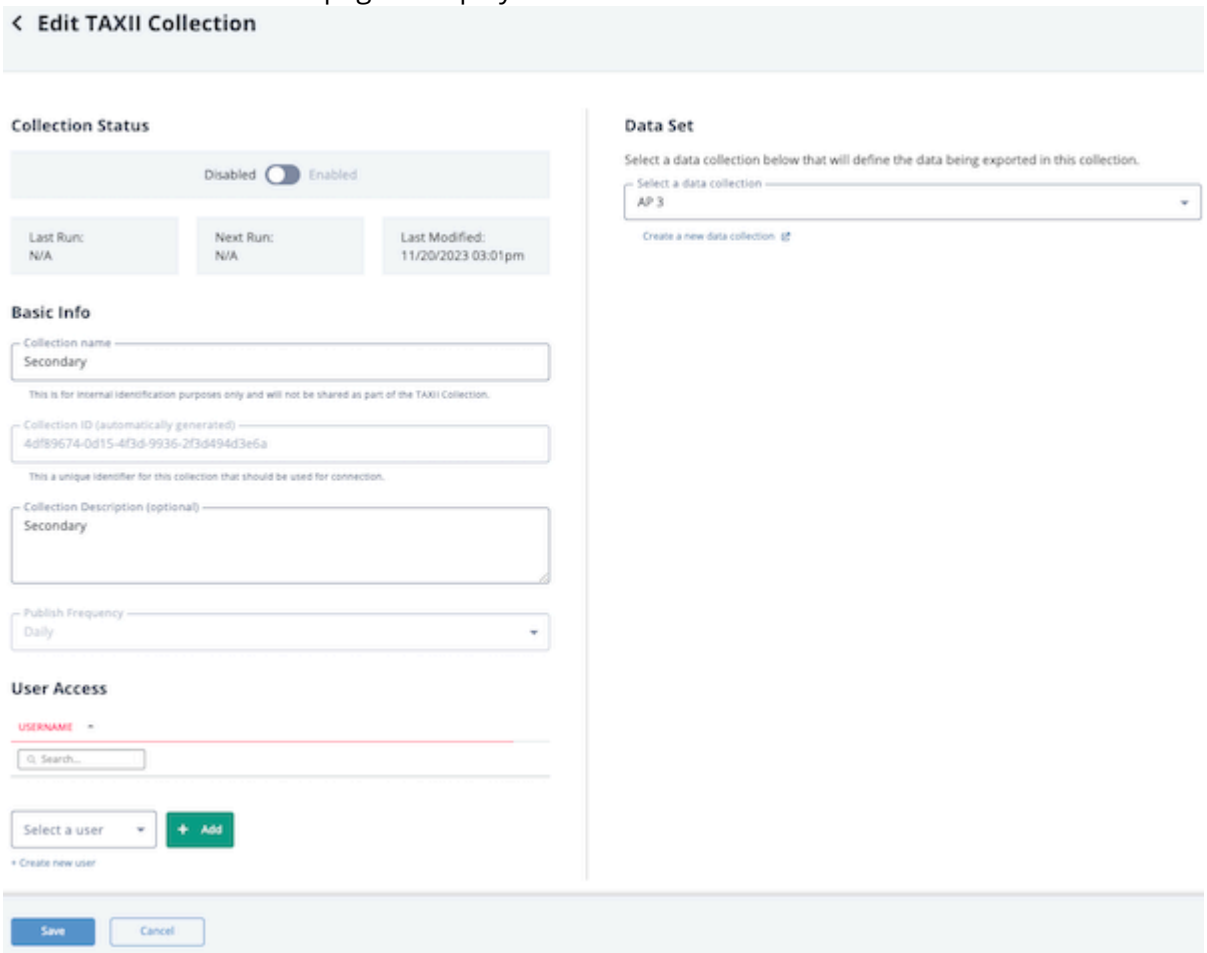
3. In the Basic Info section, enter the name of the new TAXII collection and a brief description of the collection. The Publish Frequency defaults to Daily.

> You can click and drag the lower right corner of the Collection Description field to expand it.

4. Use one of the following methods to specify a data collection for the TAXII collection:
   - **Select an existing data collection** - Click the Select a data collection field and select an existing data collection.
   - **Create a new data collection** - Click the Create a new data collection option to access the Threat Library in another tab and create a new data collection. After you create the new data collection, return to the setup wizard's tab and select the new data collection.

     > The selection field only lists data collections that you have permission to access and that include STIX objects. The data collection can include other object types but must include STIX objects and the TAXII collection will only pull STIX object data.

5. Click the **Save** button.
   The Edit TAXII Collection page is displayed.



6. In the User Access section, use one of the following methods to add a user to the TAXII collection:

- **Add an existing TAXII user** - Click the Select a user field and locate the user by browsing the drop down list or using the search field. After you select the user, click the Add button.
- **Add a new TAXII user** - Click the Create new user option to launch the Create New User window. Enter the username and password. By default, the user is assigned access to the TAXII collection you are creating. However, you can use the Add option to give the user access to additional TAXII collections. Then, click the Save button to return to the Edit TAXII Collection page.

  > Be sure to capture the TAXII password information you enter. This information is encrypted and not viewable after entry. If misplaced, you cannot retrieve the password. However, you can assign a new password.

  After you add a TAXII user, the username is displayed in the User Access section and you can use the Search box to locate a specific username and/or click the delete icon next to a user name to remove it from the collection.

7. You can repeat step 6 to continue adding users to the collection.
8. From the Edit TAXII Collection page, click the **Save** button to save your changes to the collection.

Updating a TAXII Collection's Publish Settings

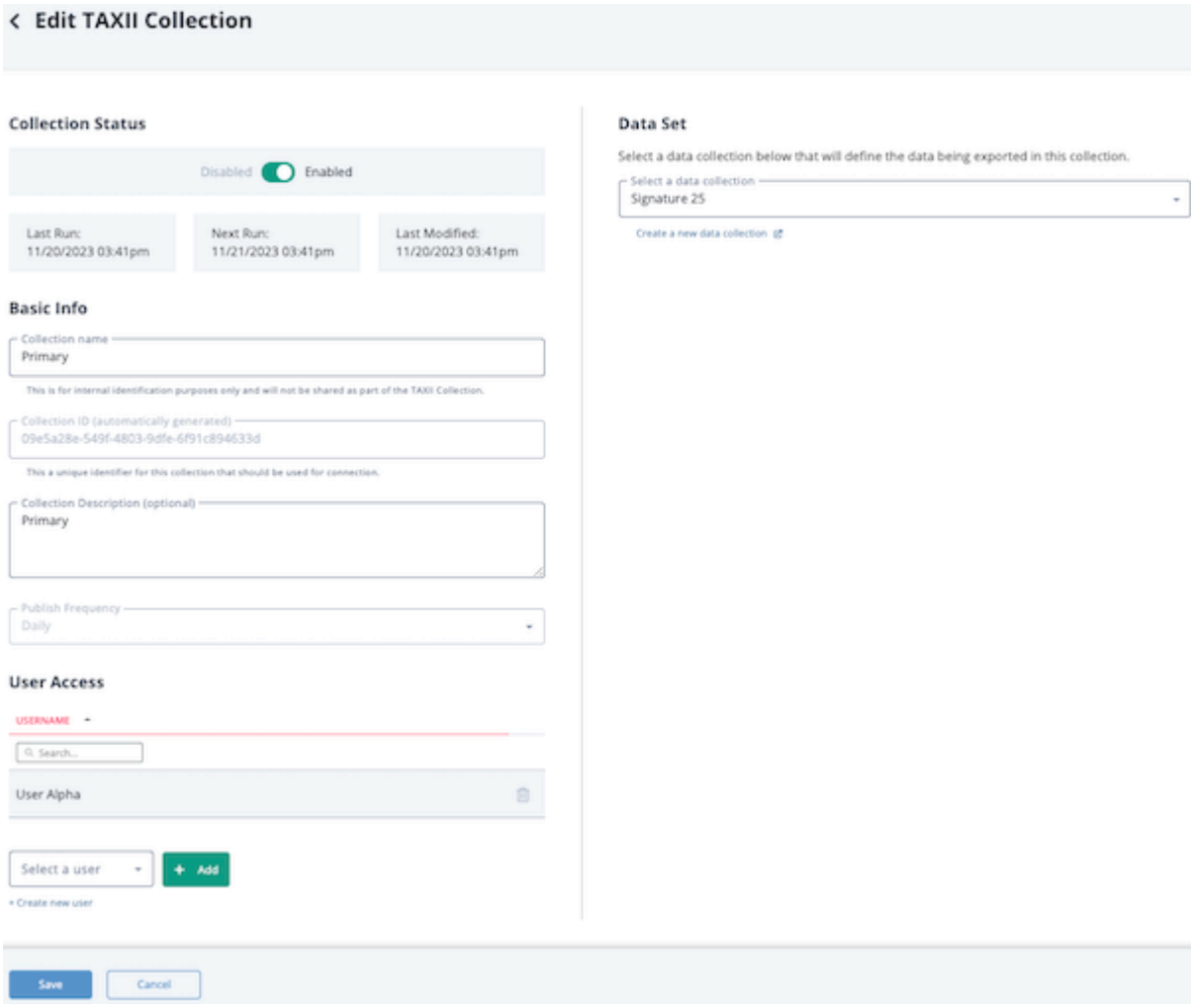
The Edit TAXII Collection page lists the collection's configuration details, time/date stamps for the collection's last and next run, and the date/time of the last change to the collection configuration.

FIELD NAME	DESCRIPTION
Last Run	The date/time of the last time the TAXII server pulled data for the TAXII collection.
Next Run	The date/time of the next time the TAXII service will pull data for the TAXII collection.
Last Modified	The date/time of the last updates to this collection including: • Enabling/disabling the collection. • Collection name or description updates. • Selection of a new data collection. • Addition/removal of TAXII users to the collection.

From this page, you can update the collection's name and description, add or remove users, and change the data collection.

> Updating a collection's name does not change its collection ID. The collection ID is created at the same time as the collection and cannot be changed.

1. From the TAXII Users & Collections page, click the gear icon next to the collection name.
2. Select the Publish Settings option to access the Edit TAXII Collection page. From this page you can:
   - Enable/disable the collection.
   - Change the collection name or description.
   - Add/remove collection users.
   - Select a new data collection



3. Enter your changes.

> If you remove all users from a TAXII collection or delete its data collection, the TAXII collection is automatically disabled.

4. Click the **Save** button.

Sharing TAXII Collections

To share a TAXII collection with another organization or individual you will need to provide:

- TAXII collection name and/or ID
- User credentials - The username and password you created in TQX
- The path for your TAXII server - `<your ThreatQ domain>:5910/taxii2/`

TAXII Users

About TAXII Users

A TAXII user is a set of credentials (username and password) used to determine access to one or more TAXII Collections on the TAXII Server. These credentials are managed in the ThreatQ Platform and provided to an organization or individual to allow them access.

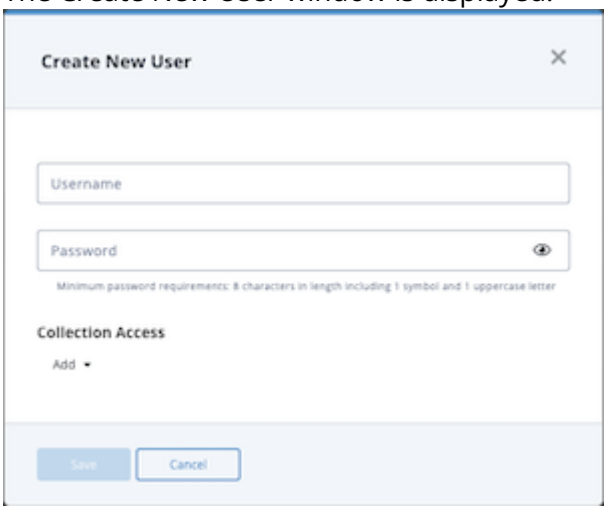
To locate a TAXII user, you can sort the user list by username or use the username or collection access search fields to locate a user.

Tips and Tricks

- TAXII user credentials cannot be used to access ThreatQ.
- TAXII users cannot be used as sources for system objects.
- To delete a user, you must first remove the user's access to all TAXII collections.

Creating a TAXII User

1. From the TAXII Users & Collections page, click the **Create User** button.
   The Create New User window is displayed.



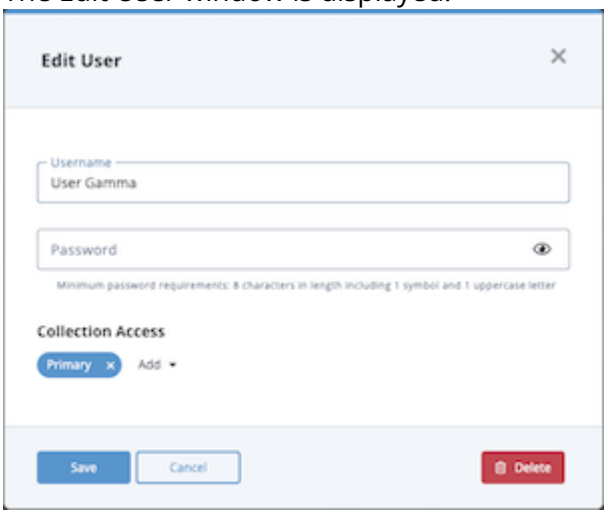
2. Enter the new username and password.

   > Be sure to capture the TAXII password information you enter. This information is encrypted and not viewable after entry. If misplaced, you cannot retrieve the password. However, you can assign a new password.

3. In the Collection Access section, click the Add option to give the user access to an existing TAXII collection. You can repeat this step to give the user access to multiple collections.
4. Click the Save button. The new username is displayed in the TAXII Users & Access section of the TAXII Users & Collections page.

Updating TAXII User Credentials

1. From the TAXII Users & Collections page, click the gear icon next to the username.
   The Edit User window is displayed.

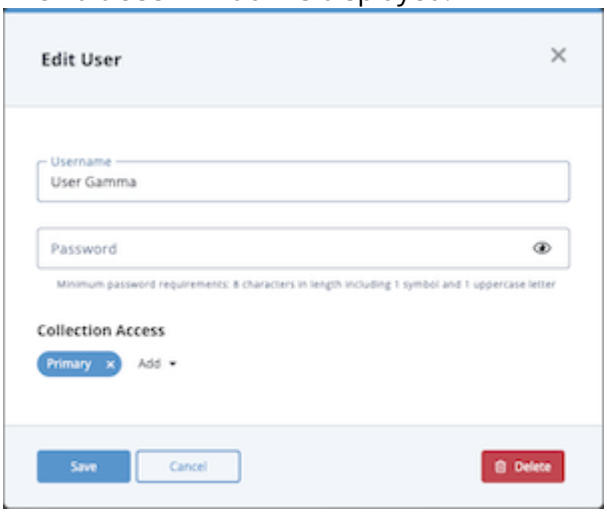


2. Enter your changes to the username and/or password.
3. From the Collection Access section, you can add or remove access to a TAXII collection:
   - **Add access to a collection** - Click the Add option to give the user access to a TAXII collection. You can repeat this step to give the user access to multiple collections.
   - **Remove access to a collection** - Click the **X** next to the collection name to remove a user's access to it.
4. Click the **Save** button to save your changes and return to the TAXII Users & Collections page.

Removing TAXII User Credentials

Before you can remove a TAXII username, you must remove its access to all TAXII collections.

1. From the TAXII Users & Collections page, click the gear icon next to the username.
   The Edit User window is displayed.



2. Remove the user's access to all TAXII collections by clicking the **X** next to each collection name.
3. Click the Delete button.
   The TAXII Users & Collections page is displayed and the username is no longer displayed in the TAXII Users and Access section.

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 Feed Sharing Options 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 3.1.0**
  - TAXII Server functionality in ThreatQ version 5.23.0
- **Version 3.0.0**
  - Bug fixes included with ThreatQ version 5.12.0
- **Version 2.0.0**
  - Updates included with ThreatQ version 5.6.0
- **Version 1.6.0**
  - Updates included with ThreatQ version 4.57
- **Version 1.4.0**
  - Updates included with ThreatQ version 4.56
- **Version 1.4.0**
  - Updates included with ThreatQ version 4.54
- **Version 1.3.0**
  - Updates included with ThreatQ version 4.53
- **Version 1.2.0**
  - Updates included with ThreatQ version 4.52
- **Version 1.1.0**
  - Updates included with ThreatQ version 4.50
- **Version 1.0.0**
  - Initial Release