

Integrations

StixTaxii For Director Console UI

V6.2.0

CONTENTS

1	StixTaxii	1
2	Installing StixTaxii	2
3	Uninstalling StixTaxii	5
4	Configuring StixTaxii	7
5	General Settings	13

STIXTAXII

StixTaxii is a [threat intelligence](#) source that fetches cyber threat intelligence (CTI) data written in *STIX* format from a *TAXII* server. You can enrich incoming logs of Logpoint with this fetched data by using the Threat Intelligence [process command](#).

StixTaxii support *STIX/TAXII* versions 1.0, 2.0 and 2.1.

INSTALLING STIXTAXII

Prerequisites

- Director Fabric v1.4.0 or later
- Director Console v1.6.0 or later
- Logpoint v6.12.2 or later
- Threat Intelligence v5.0.0 or later

To install StixTaxii:

1. Log in to Director Console.
2. Click **Assets** in the navigation bar.
3. Select **Plugins** from the **Assets Type** drop-down.
4. Click the *upload area* to browse, or drag and drop the StixTaxii .pak file.
5. Click **UPLOAD**.

Once uploaded, the **Assets** page adds the .pak file to the list of the available packages in the Fabric Server.

6. Select StixTaxii .pak from the list of available packages.
7. Click **INSTALL**.

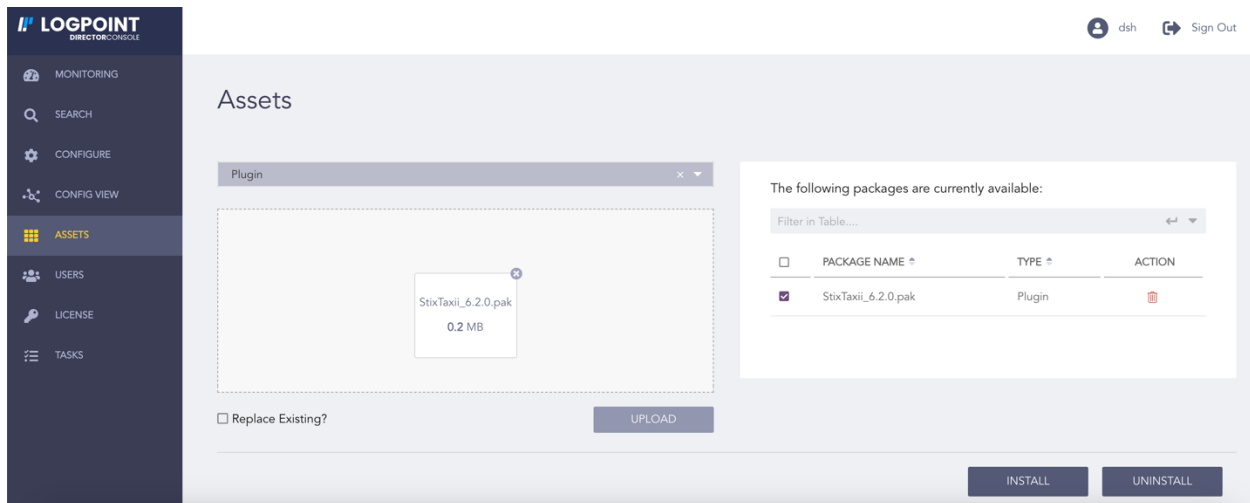


Fig. 1: Selecting the Package

8. Select Logpoint to install StixTaxii. You can select multiple Logpoints of different pools.

9. Click **NEXT**.

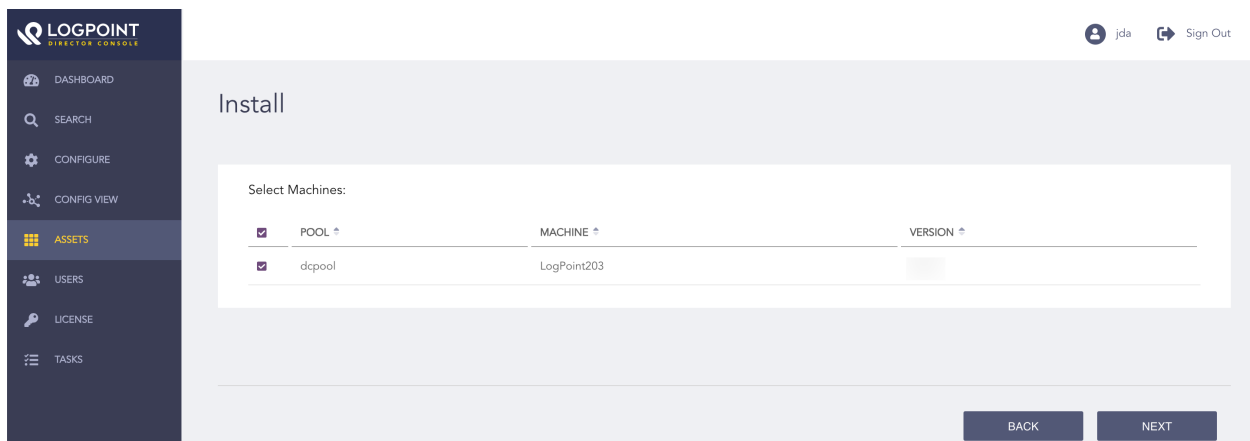


Fig. 2: Selecting Logpoint

10. Review your changes. You can go **BACK** to make any changes if necessary.

11. Click **INSTALL** and click **OK** to confirm.

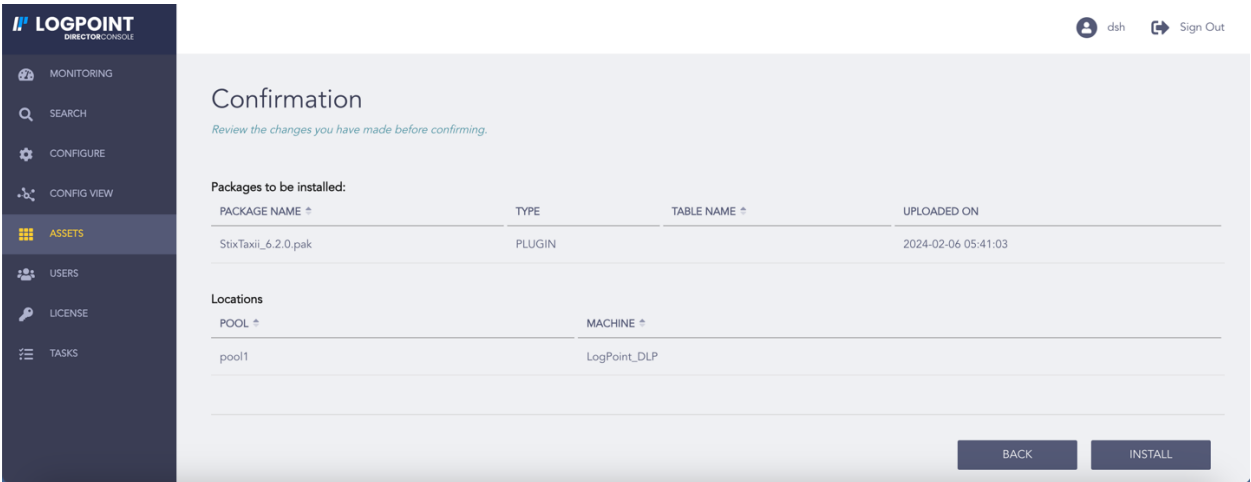


Fig. 3: Confirming the Changes

UNINSTALLING STIXTAXII

You must remove the StixTaxii configuration to delete it.

1. Click **Assets** in the navigation bar.
2. Click **UNINSTALL**.
3. Select the Logpoint where StixTaxii is installed. You can select multiple Logpoints of different pools.
4. Select **StixTaxii** from the list of available packages.
5. Click **NEXT**.

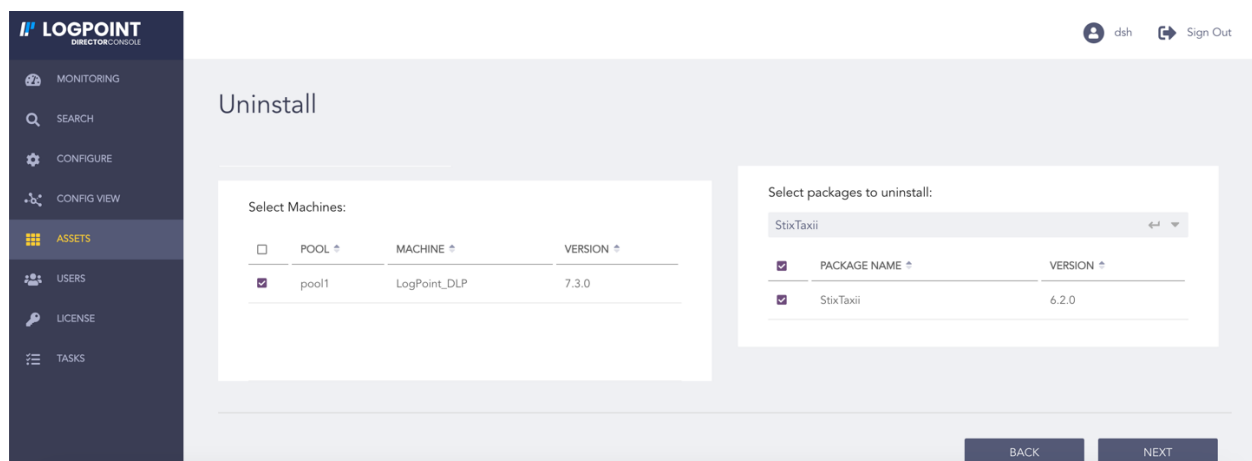


Fig. 1: Selecting StixTaxii

6. Review your changes. You can go **BACK** to make any changes if necessary.
7. Click **UNINSTALL** and click **OK** to confirm.

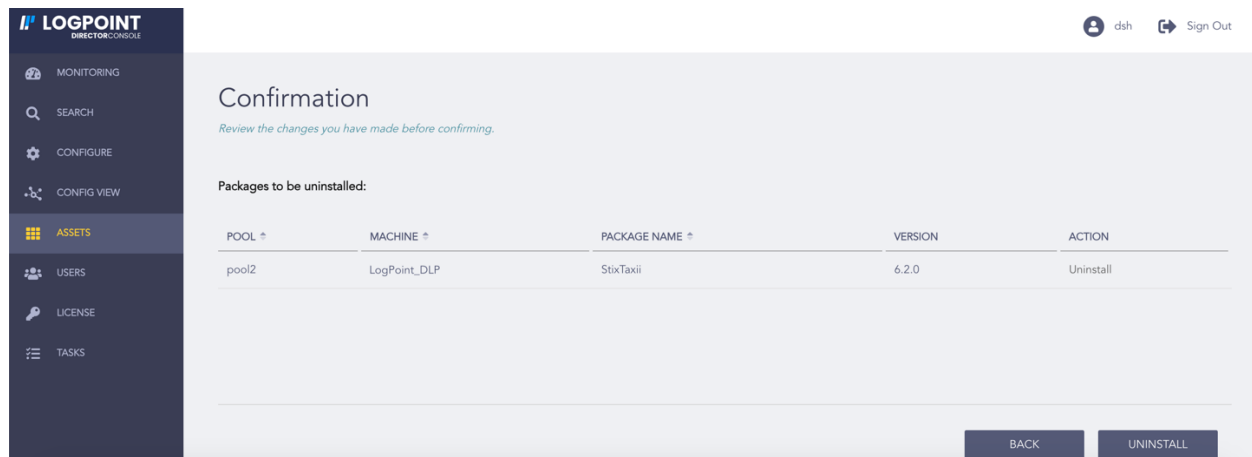


Fig. 2: Confirming the Changes

CONFIGURING STIXTAXII

For StixTaxii to fetch data, an initial setup where details like server endpoints, authentication credentials and data filtering options must be configured. You can perform this setup from Configure.

1. Click **CONFIGURE** in the navigation bar.
2. Under *Settings*, click **PLUGINS**.
3. Select the **STIX/TAXII Enrichment Source** from the **Select Plugin Type** drop-down.
4. Select Logpoint to configure the STIX/TAXII enrichment source. You can select multiple Logpoints of different pools.

Note:

- You cannot select a subscriber Logpoint to configure the STIX/TAXII enrichment source. The subscriber Logpoint receives these configurations from its provider Logpoint.
 - You can use **Refresh List** to sync the data between Logpoint and Director Fabric.
-

5. Click **NEXT**.

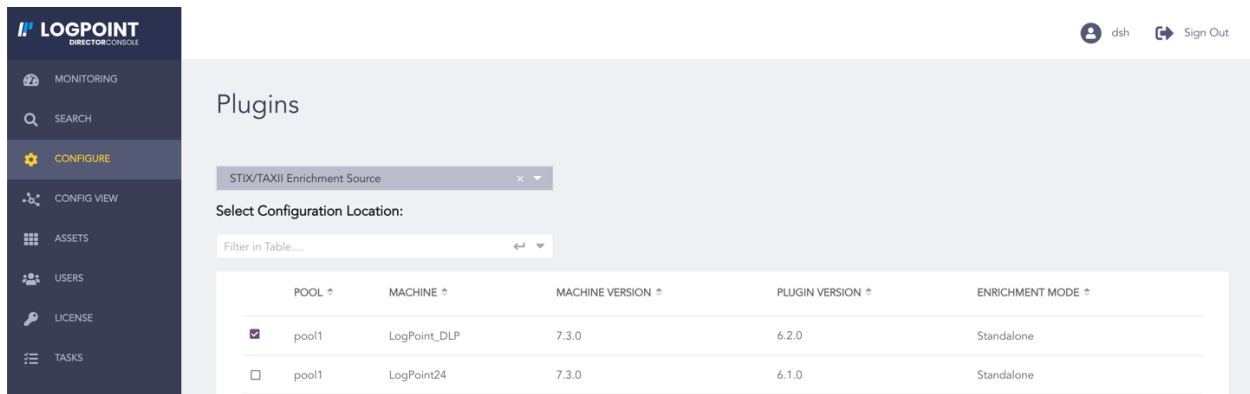


Fig. 1: Selecting Logpoint

6. Select **Enable Source** to fetch STIX data from a *TAXII* server.
7. Enter the **Discovery URL**, which is the location of the discovery service in the *TAXII* server.
8. Select a **STIX Version**.
 - 8.1. If you select version **1.X**, select **Fetch From** date and **Fetch From Unit**. StixTaxii fetches data from the specified date.
 - 8.2. If you select **2.0** and **2.1**, you can **Enable Pagination** to separate data fetching into pages.
 - 8.2.1. Select the number of data to be retrieved in a page in **Fetch Per Page**.
9. Enter the **Fetch Interval**.
10. Select **Fetch Interval Unit** in either hours or days.

The screenshot shows a configuration form for an STIX/TAXII Enrichment Source. It includes several sections with checkboxes and input fields. The 'Enable Source' checkbox is checked. The 'Discovery URL' field contains 'https://[redacted].eset.com/taxii2/'. The 'Version' section has three radio buttons: '1.X', '2.0', and '2.1', with '2.1' selected. The 'Enable Pagination' checkbox is checked. The 'Fetch Per Page' field contains '10000'. The 'Fetch Interval' field contains '1'. The 'Fetch Interval Unit' dropdown menu is set to 'Hours'.

☒ Enable Source

Discovery URL *

https://[redacted].eset.com/taxii2/

Version *

☐ 1.X ☐ 2.0 ☒ 2.1

☒ Enable Pagination

Fetch Per Page *

10000

Fetch Interval *

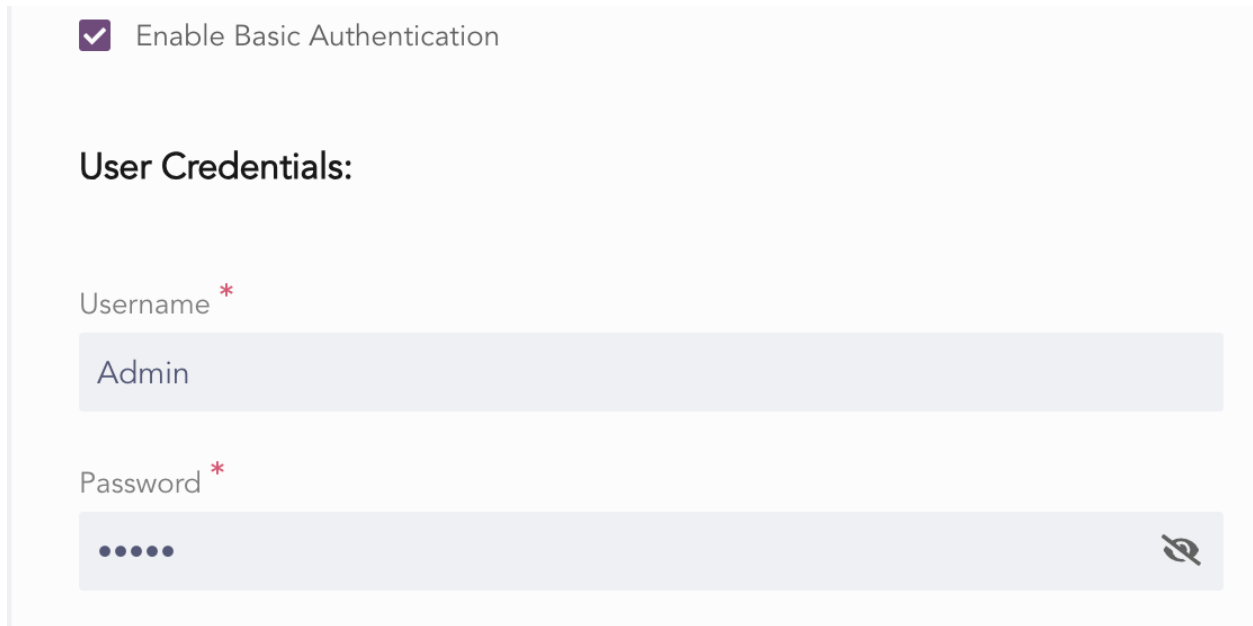
1

Fetch Interval Unit *

Hours

Fig. 2: Configuring STIX/TAXII Enrichment Source

11. Select **Enable Basic Authentication** if the *TAXII* server uses basic authentication.
12. In **User Credentials**, enter the *TAXII* server **Username** and **Password**.



☒ Enable Basic Authentication

User Credentials:

Username *

Admin

Password *

..... 

Fig. 3: Enabling Basic Authentication

13. Select **Enable SSL Authentication** if the *TAXII* server uses SSL authentication.

13. In **SSL Configuration**:

13.1. Enter the **Key Password**, which is the password used to decrypt the SSL key.

13.2. Upload the SSL certificate in the **Certification File**.

13.3. Upload the SSL key in the **Certificate Key**.

☒ Enable SSL Authentication

SSL Configuration:

Key Password

Certificate File *



Click to upload or drag and drop the files here.

UPLOAD

Certificate Key *



Click to upload or drag and drop the files here.

UPLOAD

Fig. 4: Enabling SSL Authentication

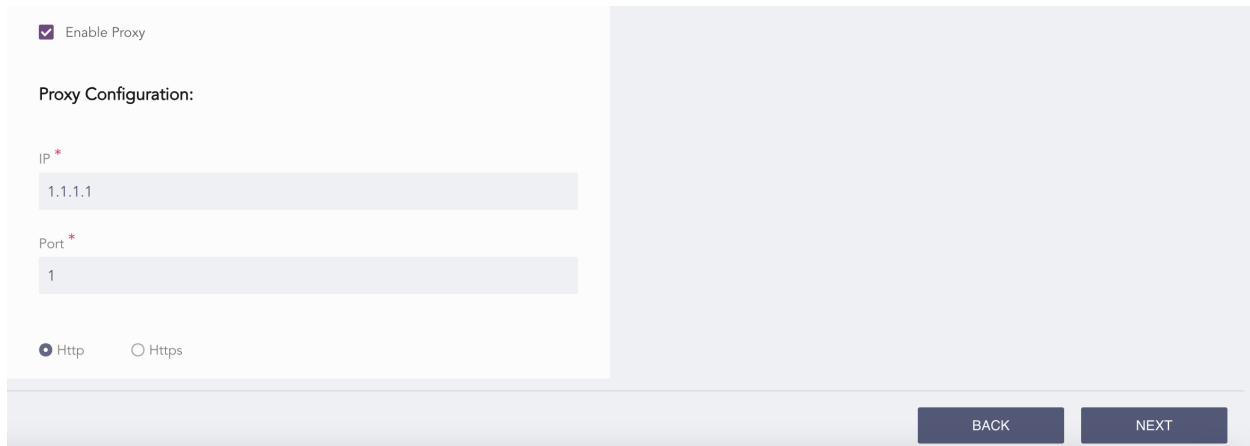
14. Select **Enable Proxy** to use a proxy server.

15. In **Proxy Configuration**:

15.1. Enter the proxy server **IP** address and the **Port** number.

15.2. Select the required **Http** or **Https** protocol.

16. Click **NEXT**.



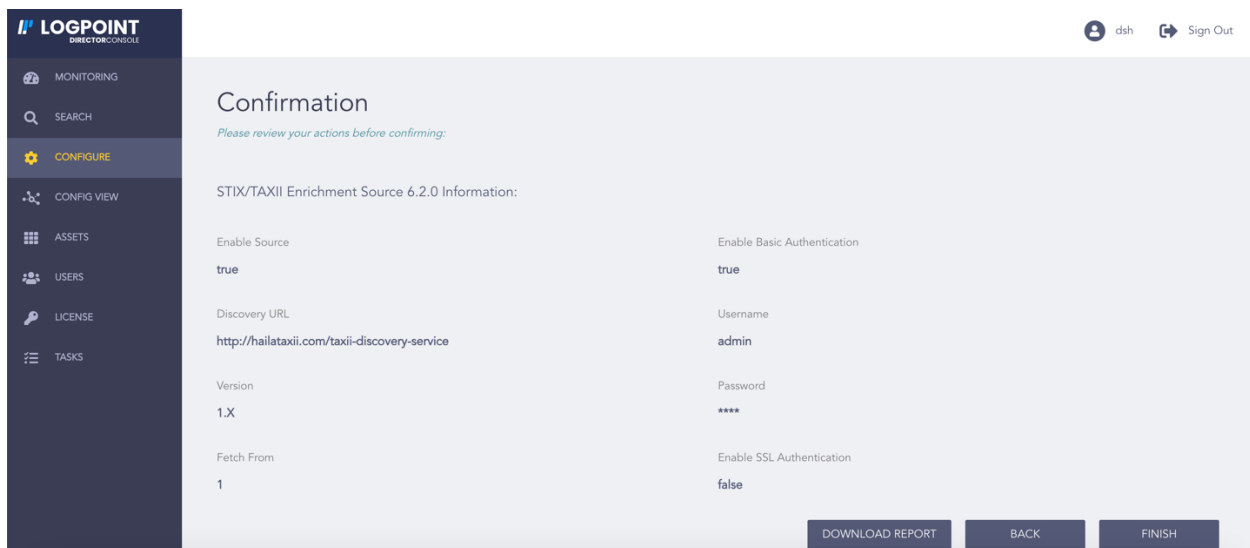
The screenshot shows a 'Proxy Configuration' form. At the top, there is a checkbox labeled 'Enable Proxy' which is checked. Below this, the form has two input fields: 'IP' with the value '1.1.1.1' and 'Port' with the value '1'. At the bottom, there are two radio buttons: 'Http' (selected) and 'Https'. At the bottom right of the form, there are two buttons: 'BACK' and 'NEXT'.

Fig. 5: Enabling Proxy Server

17. Review your changes. You can go **Back** to make any changes if necessary.

18. Click **Finish**.

19. Click **OK**.



The screenshot shows the 'Confirmation' page in the Logpoint Director Console. The page has a dark sidebar on the left with the Logpoint logo and navigation links: MONITORING, SEARCH, CONFIGURE (highlighted), CONFIG VIEW, ASSETS, USERS, LICENSE, and TASKS. The main content area is titled 'Confirmation' and includes a warning: 'Please review your actions before confirming:'. Below this, it displays 'STIX/TAXII Enrichment Source 6.2.0 Information:'. The information is organized into two columns. The left column lists: 'Enable Source' (true), 'Discovery URL' (http://hailataxii.com/taxii-discovery-service), 'Version' (1.X), and 'Fetch From' (1). The right column lists: 'Enable Basic Authentication' (true), 'Username' (admin), 'Password' (****), and 'Enable SSL Authentication' (false). At the bottom right, there are three buttons: 'DOWNLOAD REPORT', 'BACK', and 'FINISH'.

Fig. 6: Confirming the Changes

GENERAL SETTINGS

General Settings consists of all the details about the fetched data. You can find the total number of logs fetched in **Number of Entries** and the status of fetched data in **Status**. You can also find the most recent attempt made to fetch data in **Last Fetch Attempt** and the last date and time when data was successfully fetched in **Last Successful Fetch**.

1. Click **Configure** from the left navigation bar.
2. Under *Settings*, click **Plugins**.
3. Select **ThreatIntelligence** from the **Select Plugin Type** drop-down.
4. Select Logpoint to view the details. You can select multiple Logpoint of different pools.
5. Select **General Settings** from the **Select Plugin Sub-type** drop-down.
6. Click **Next**.

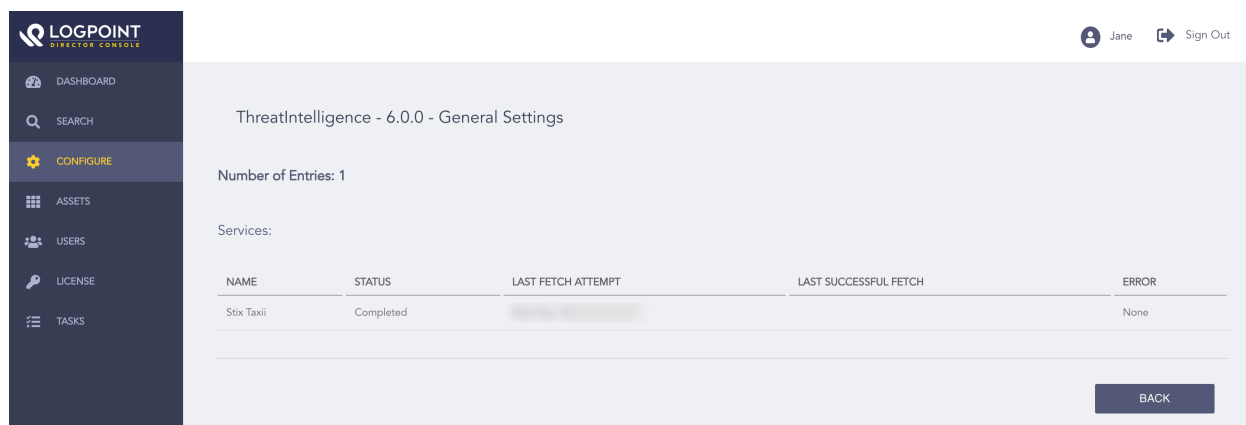


Fig. 1: General Settings