

# Integrations

## StixTaxii For Director Console UI

V6.1.0

# CONTENTS

<b>1</b>	<b>StixTaxii</b>	<b>1</b>
<b>2</b>	<b>Installing StixTaxii</b>	<b>2</b>
<b>3</b>	<b>Uninstalling StixTaxii</b>	<b>5</b>
<b>4</b>	<b>Configuring StixTaxii</b>	<b>7</b>
<b>5</b>	<b>General Settings</b>	<b>13</b>

## STIXTAXII

StixTaxii enriches incoming logs with cyber threat intelligence (CTI) that is written in *STIX* format and is shared via a *TAXII* server. It support *STIX/TAXII* version 1.0, 2.0 and 2.1. StixTaxii is also a [threat intelligence](#) source.

## 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**.

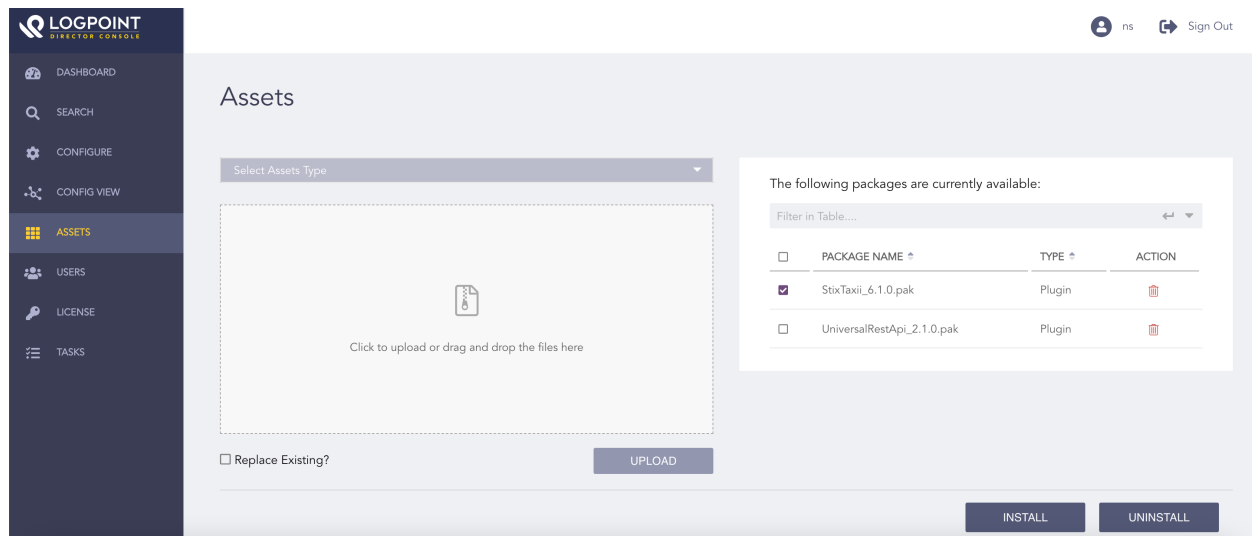


Fig. 1: Selecting the Package

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

9. Click **Next**.

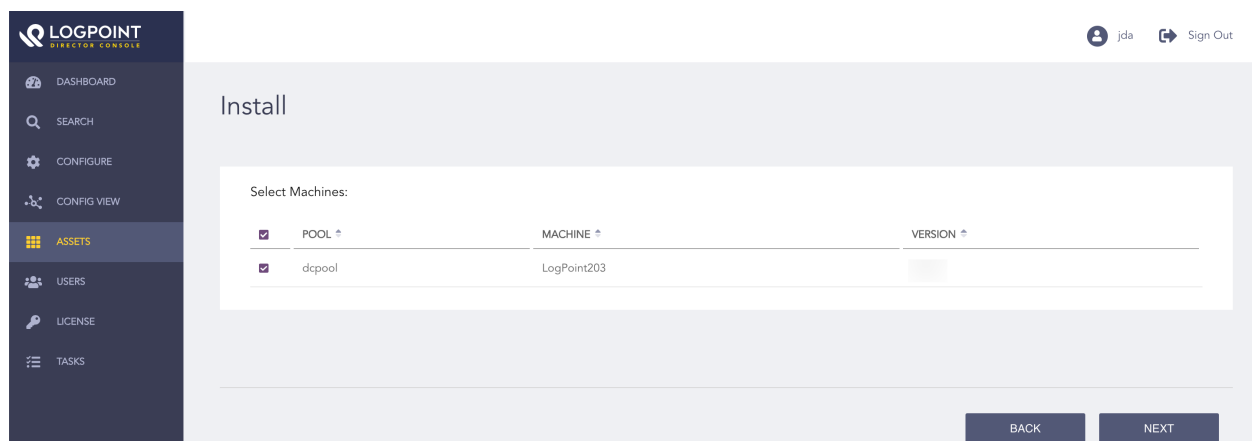


Fig. 2: Selecting Logpoint

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

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

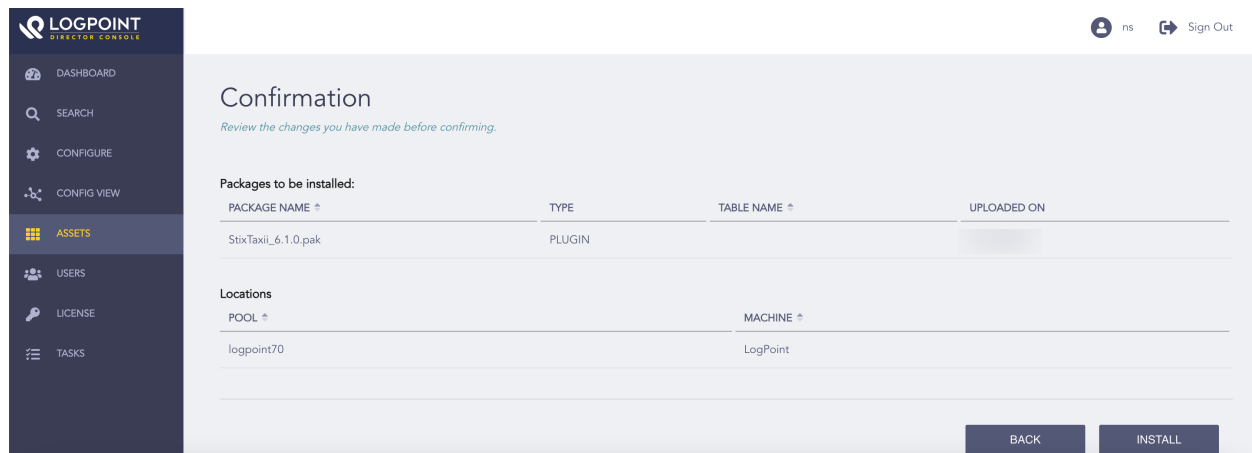


Fig. 3: Confirming the Changes

## 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**.

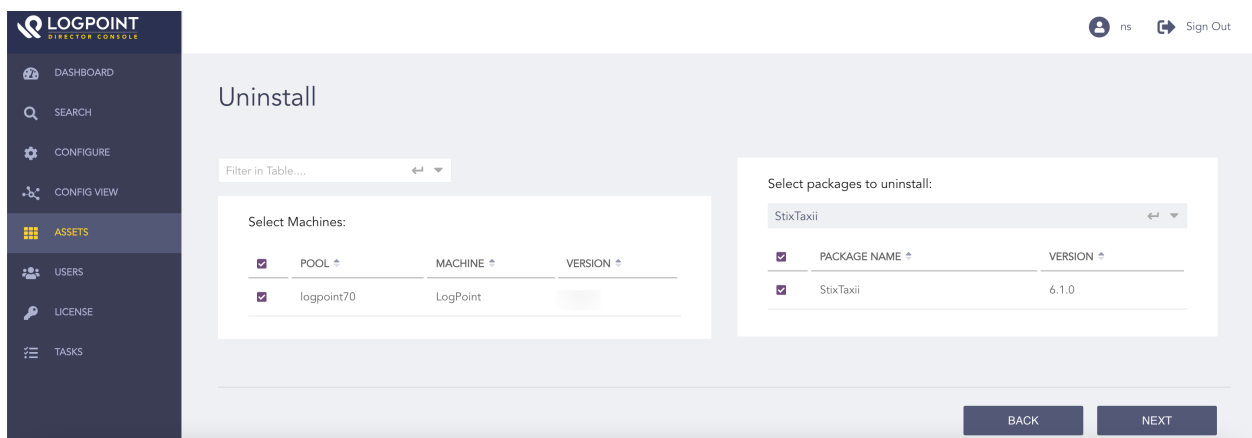


Fig. 1: Selecting StixTaxii

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

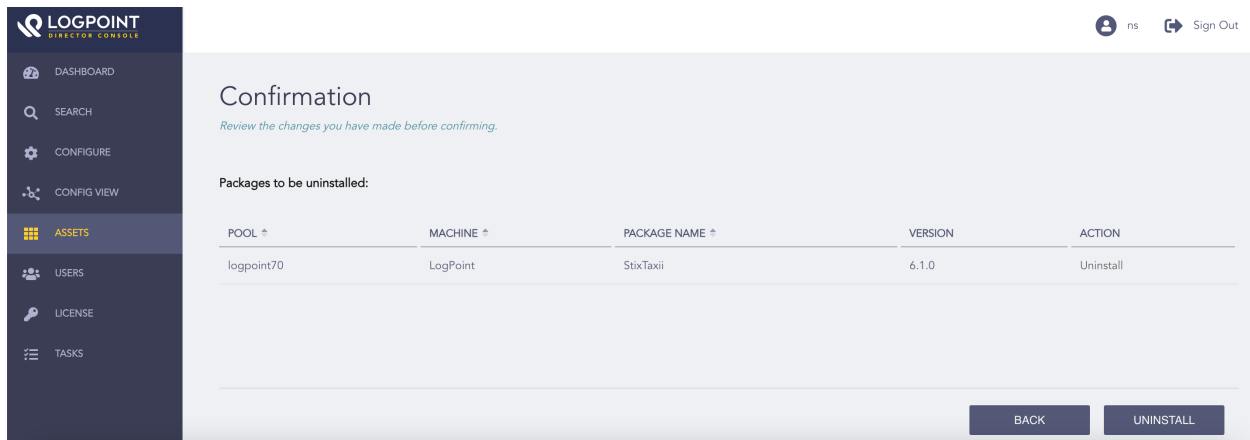


Fig. 2: Confirming the Changes



## CONFIGURING STIXTAXII

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**.

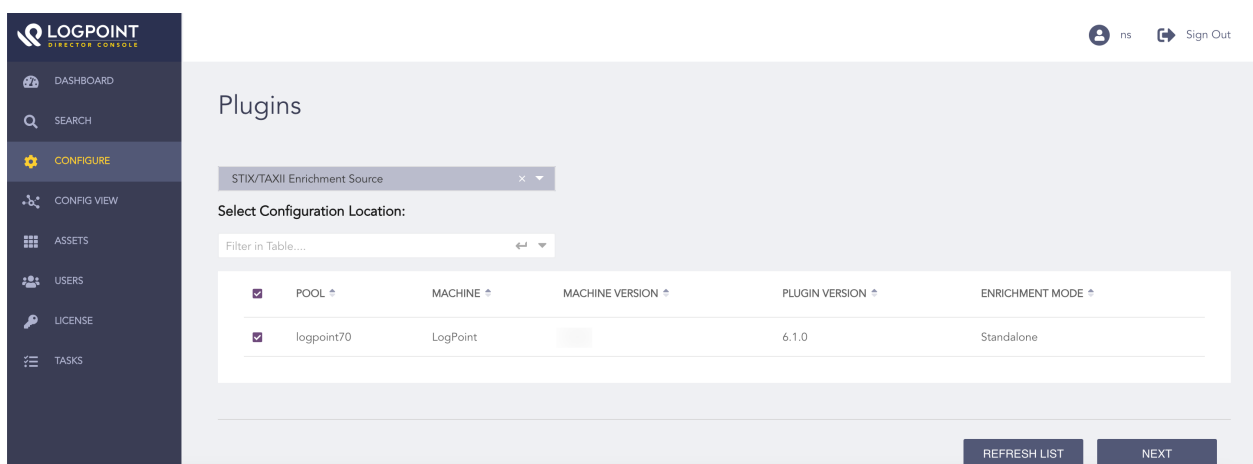
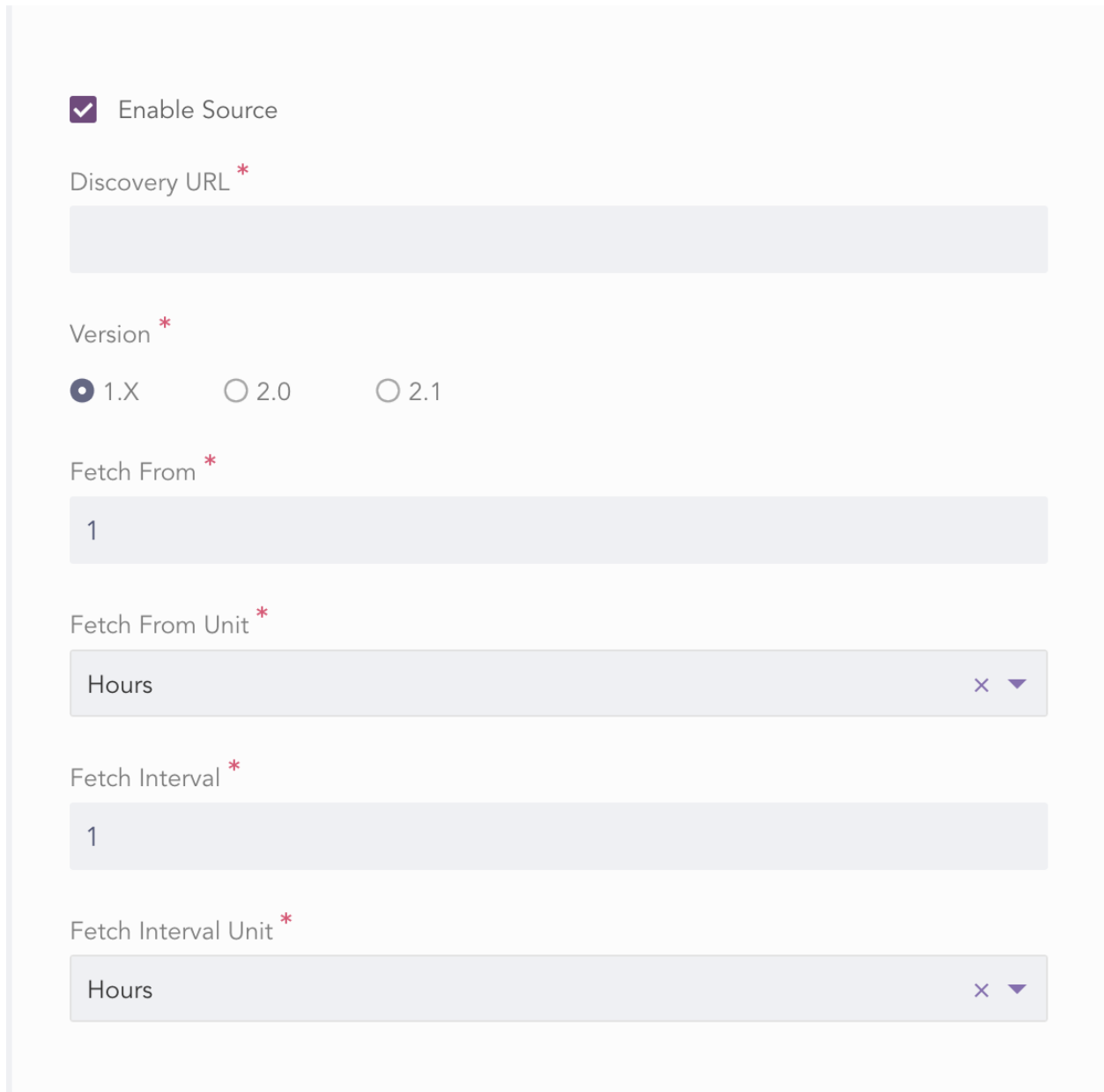


Fig. 1: Selecting Logpoint

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 logs from the specified date.
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 a checkbox for 'Enable Source', a text field for 'Discovery URL', a radio button group for 'Version' (1.X, 2.0, 2.1), a text field for 'Fetch From', a dropdown menu for 'Fetch From Unit' (set to 'Hours'), a text field for 'Fetch Interval', and a dropdown menu for 'Fetch Interval Unit' (set to 'Hours').

☒ Enable Source

Discovery URL \*

Version \*

☒ 1.X ☐ 2.0 ☐ 2.1

Fetch From \*

1

Fetch From Unit \*

Hours

Fetch Interval \*

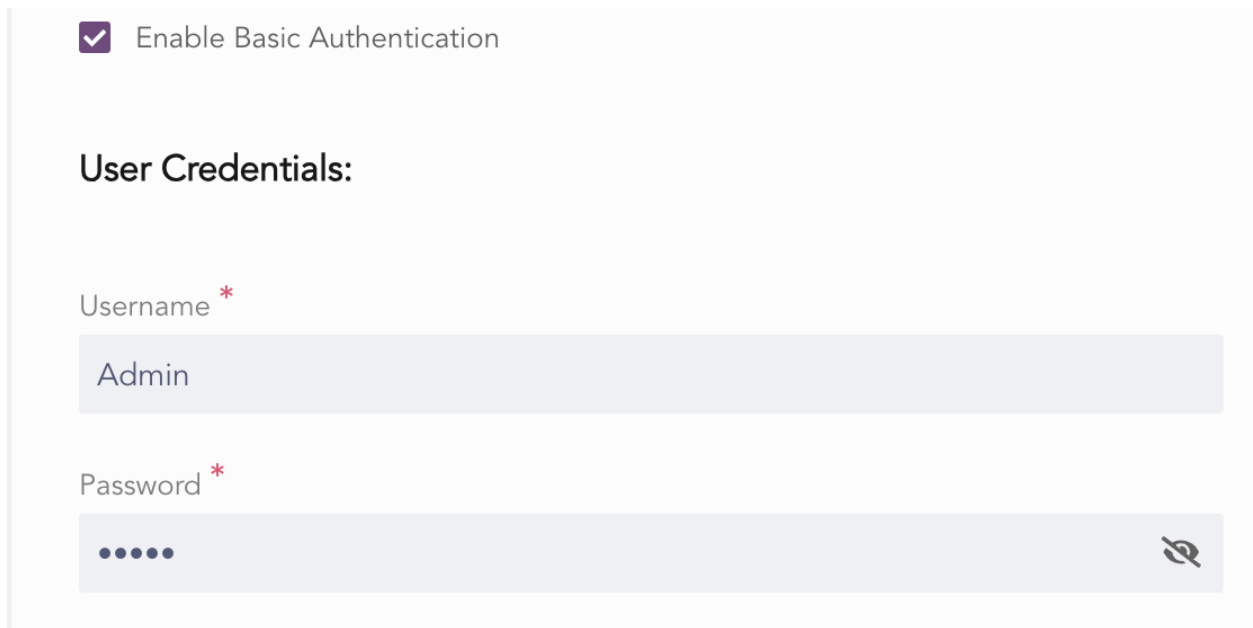
1

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**.



The screenshot shows a configuration interface for StixTaxii For Director. At the top, there is a checkbox labeled 'Enable Basic Authentication' which is checked. Below this, the section 'User Credentials:' is displayed. It contains two input fields: 'Username' with the value 'Admin' and 'Password' which is masked with dots. A red asterisk is next to the 'Password' label. A toggle icon is visible on the right side of the password field.

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

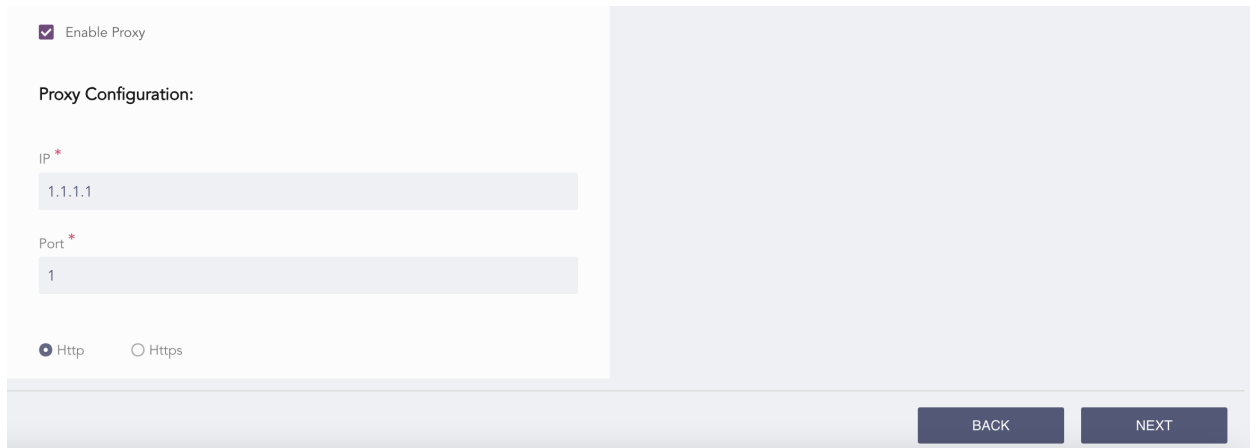
14. Select **Enable Proxy** to use a proxy server.

15. In **Proxy Configuration**:

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

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

16. Click **Next**.



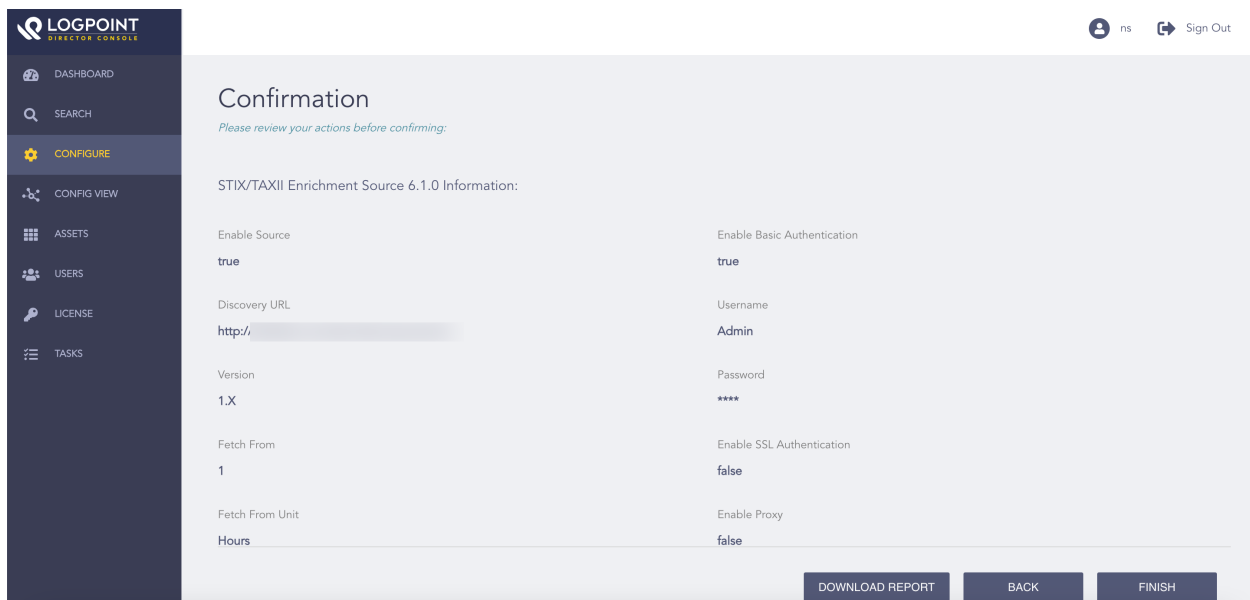
The screenshot shows the 'Proxy Configuration' section of the Logpoint Director Console. At the top, there is a checkbox labeled 'Enable Proxy' which is checked. Below it, the 'Proxy Configuration:' section contains three input fields: 'IP' with the value '1.1.1.1', 'Port' with the value '1', and a radio button selection for '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 left sidebar contains the navigation menu with 'CONFIGURE' highlighted. The main content area is titled 'Confirmation' and includes a sub-header 'STIX/TAXII Enrichment Source 6.1.0 Information:'. Below this, there are two columns of configuration details. The left column lists: 'Enable Source' (true), 'Discovery URL' (http://), 'Version' (1.X), 'Fetch From' (1), and 'Fetch From Unit' (Hours). The right column lists: 'Enable Basic Authentication' (true), 'Username' (Admin), 'Password' (\*\*\*\*), 'Enable SSL Authentication' (false), and 'Enable Proxy' (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**.

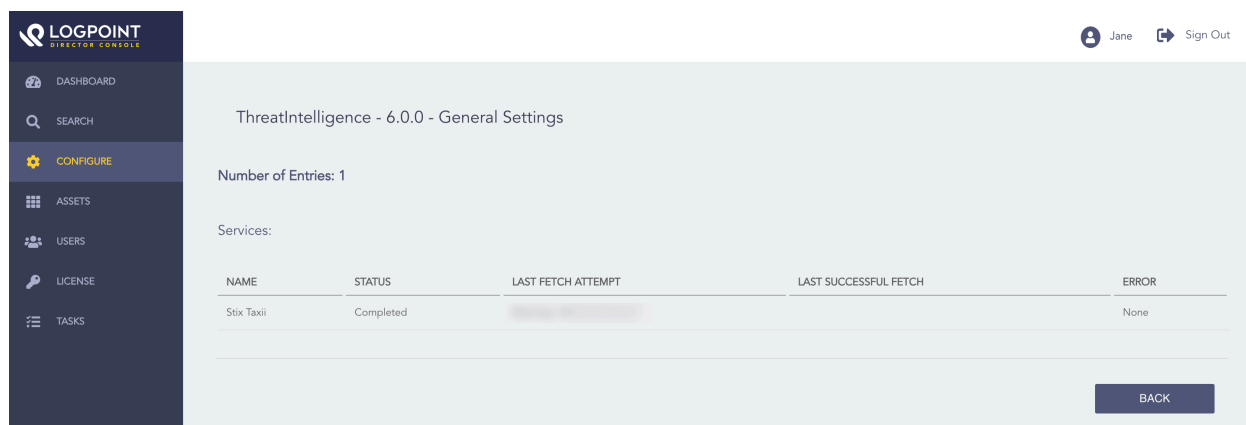


Fig. 1: General Settings