Integrations

StixTaxii For Director Console UI

V6.0.0

CONTENTS

CHAPTER

ONE

STIXTAXII APPLICATION

The StixTaxii application adds a threat intelligence source in LogPoint's Threat Intelligence application to enrich logs with cyber threat intelligence (CTI). The CTI is written in *STIX* format and is shared via a *TAXII* server. The application supports *STIX version 1.0 and 2.0.*

CHAPTER

TWO

INSTALLATION

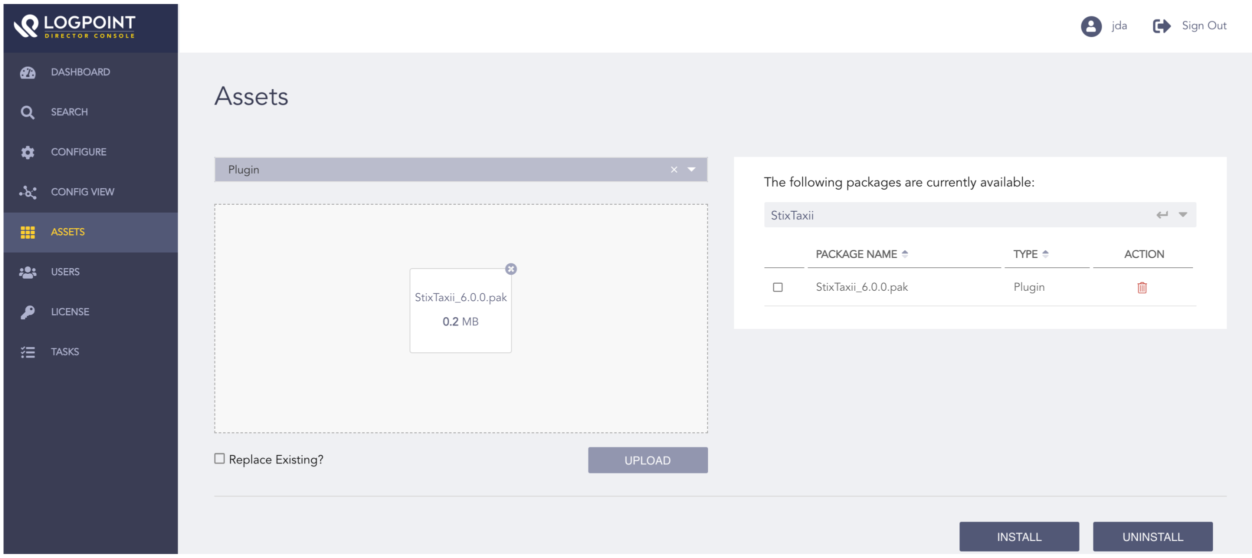
2.1 Prerequisites

- 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

2.2 Uploading the StixTaxii Application in Director Console

1. Click **Assets** from the left navigation bar.
2. Select the **Assets Type** you want to upload.
3. Click the *upload area* to browse, or drag and drop the **StixTaxii_6.0.0.pak** file.
4. Click **Upload.**

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



The following packages are currently available:

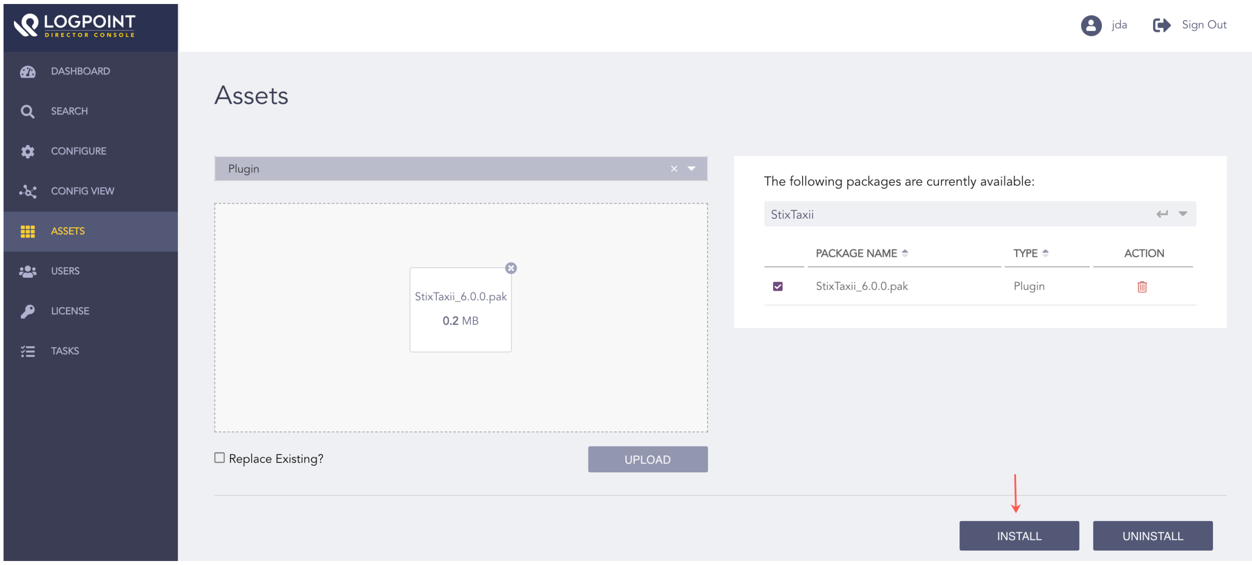
StixTaxii

	PACKAGE NAME	TYPE	ACTION
☐	StixTaxii_6.0.0.pak	Plugin	🗑

Fig. 1: Uploading StixTaxii Pak File

2.3 Installing the StixTaxii Application in Director Console

1. Click **Assets** from the left navigation bar.
2. Select **StixTaxii_6.0.0.pak** from the list of available packages.
3. Click **Install.**



The following packages are currently available:

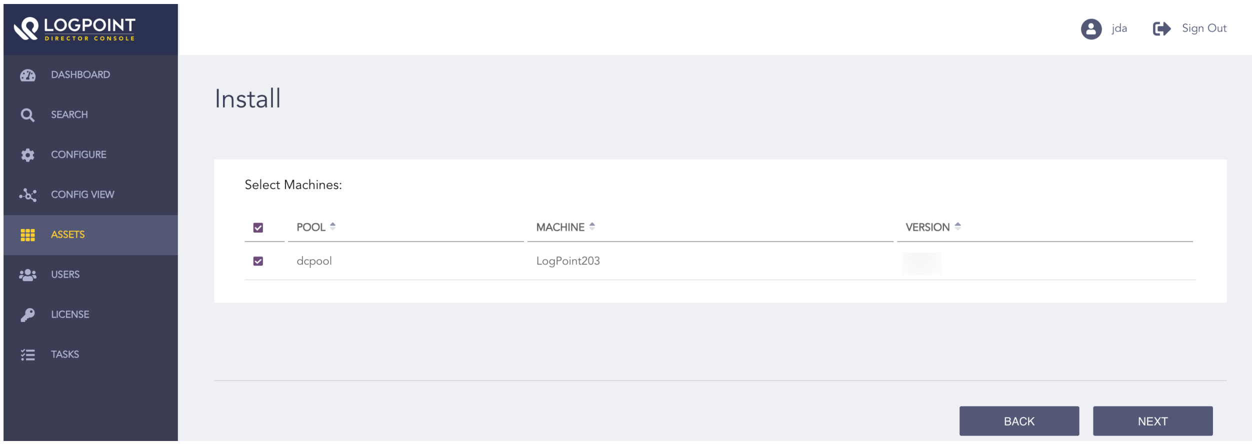
StixTaxii

	PACKAGE NAME	TYPE	ACTION
☑	StixTaxii_6.0.0.pak	Plugin	🗑

Fig. 2: Selecting the StixTaxii Package

4. Select LogPoint machines to install the StixTaxii application. You can select multiple machines of different pools.

5. Click **Next.**



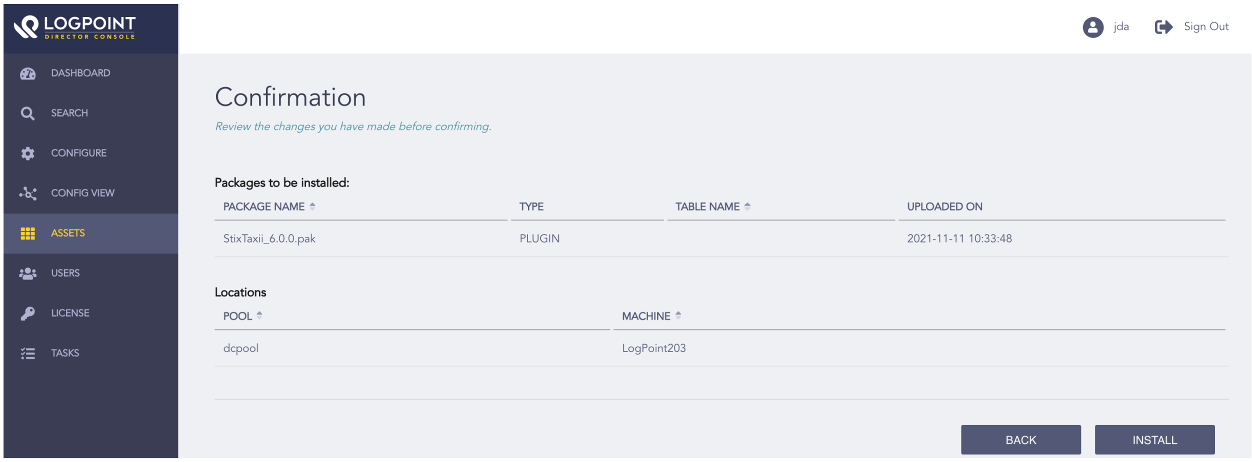
Install

Select Machines:

☑	POOL	MACHINE	VERSION
☑	dcpool	LogPoint203	

Fig. 3: Selecting LogPoint Machines

6. Review your changes. You can go **Back** to make any changes if necessary.
7. Click **Install**.
8. Click **OK**.



Confirmation

Review the changes you have made before confirming.

Packages to be installed:

PACKAGE NAME	TYPE	TABLE NAME	UPLOADED ON
StixTaxii_6.0.0.pak	PLUGIN		2021-11-11 10:33:48

Locations

POOL	MACHINE
dcpool	LogPoint203

Fig. 4: Confirming the Changes

CHAPTER

THREE

CONFIGURATION

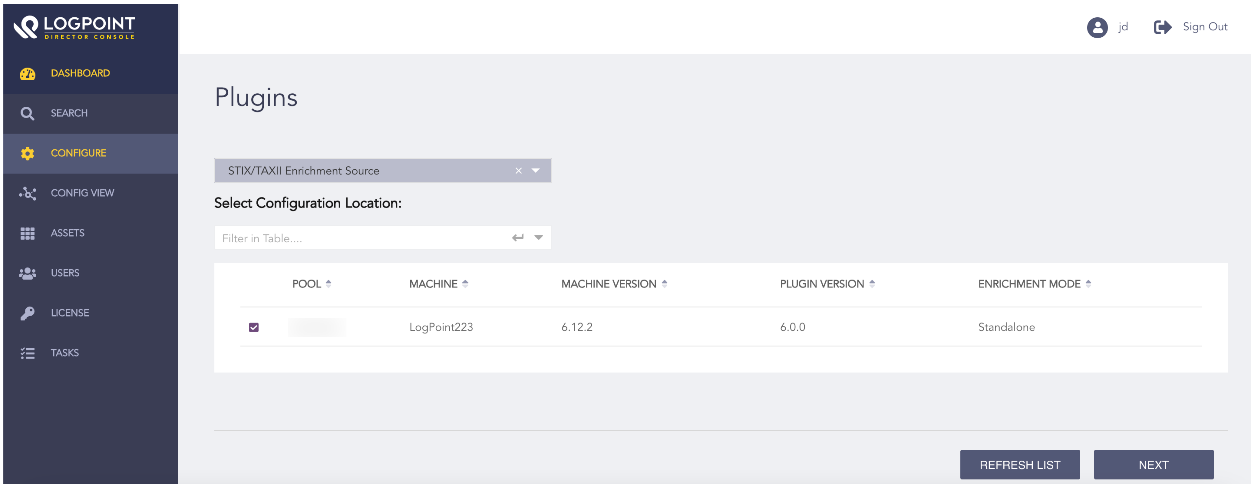
3.1 Configuring the STIX/TAXII Enrichment Source in Director Console

1. Click **Configure** from the left navigation bar.
2. Click **Plugins**.
3. Select the **STIX/TAXII Enrichment Source** from the **Select Plugin Type** drop-down.
4. Select LogPoint machines to configure the STIX/TAXII enrichment source. You can select multiple machines 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.**



Plugins

STIX/TAXII Enrichment Source

Select Configuration Location:

Filter in Table....

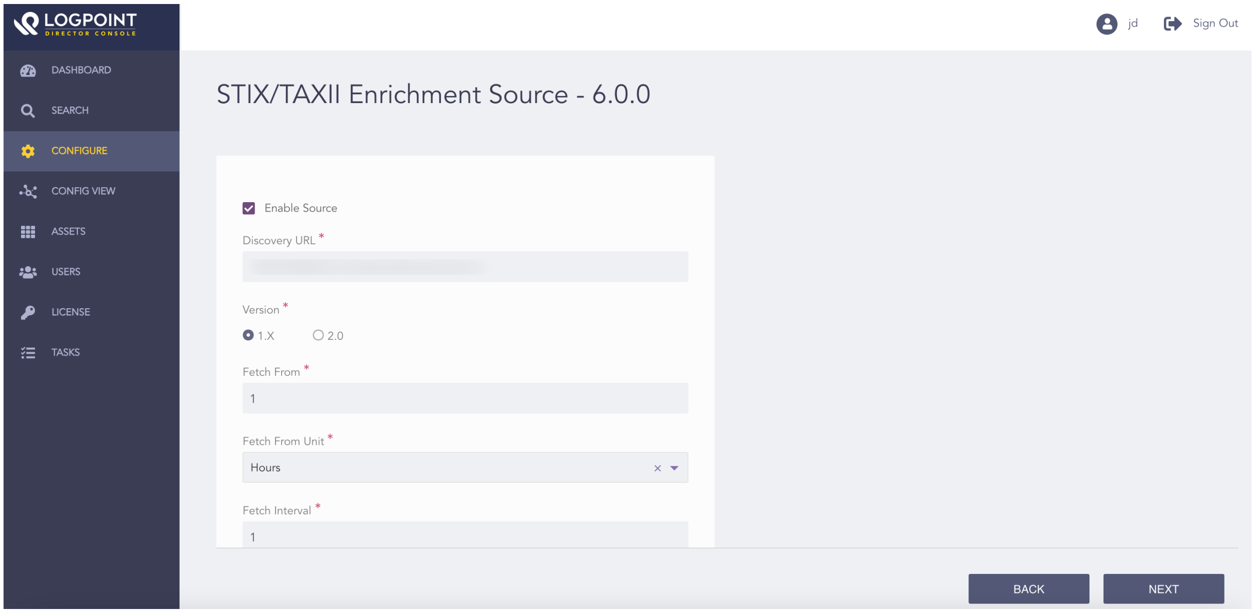
	POOL	MACHINE	MACHINE VERSION	PLUGIN VERSION	ENRICHMENT MODE
☑	[redacted]	LogPoint223	6.12.2	6.0.0	Standalone

Fig. 1: Selecting LogPoint Machines

6. Select the **Enable Source** option 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 the **1.X** version:

    8.1.1. Enter the **Fetch From**. The application fetches data from the selected hour or day.
    8.1.2. Select the **Fetch From Unit** option in hours, months, or days.
    8.1.3. Enter the **Fetch Interval**.
    8.1.4. Select the **Fetch Interval Unit** option in either hours or days.



STIX/TAXII Enrichment Source - 6.0.0

☑ Enable Source

Discovery URL *

[redacted]

Version *

● 1.X ○ 2.0

Fetch From *

1

Fetch From Unit *

Hours

Fetch Interval *

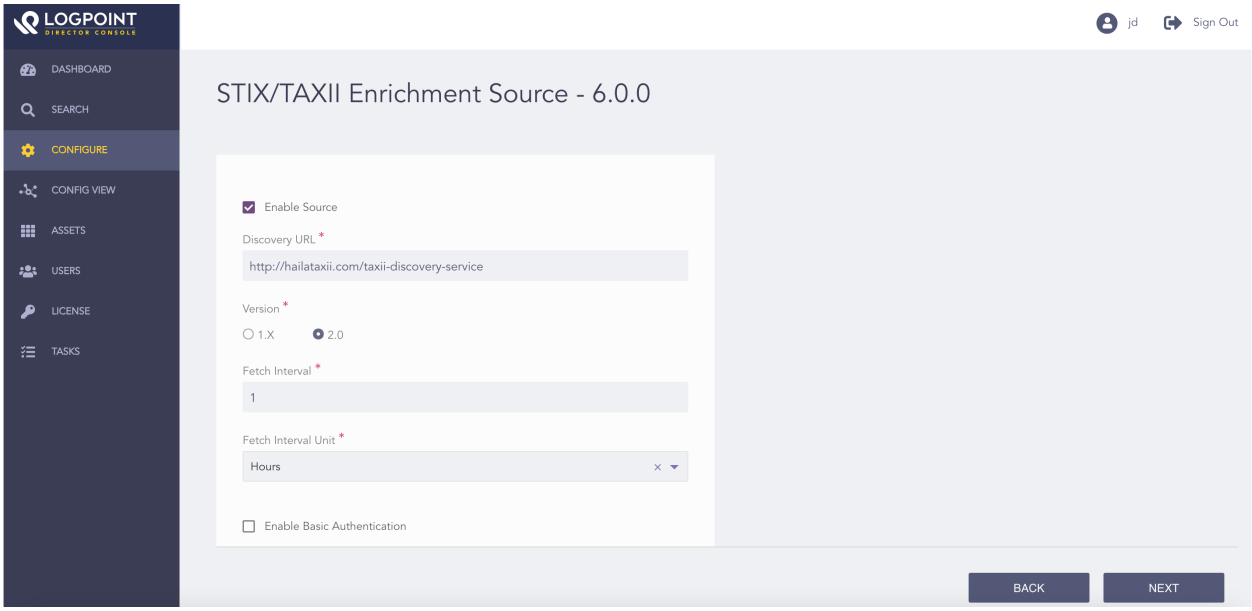
1

Fig. 2: Selecting STIX 1.X Version

8.2. If you select the **2.0** version,

8.2.1. Enter the **Fetch Interval**.

8.2.2. Select the **Fetch Interval Unit** option in either hours or days.



STIX/TAXII Enrichment Source - 6.0.0

☑ Enable Source

Discovery URL *

http://hailataxii.com/taxii-discovery-service

Version *

○ 1.X ● 2.0

Fetch Interval *

1

Fetch Interval Unit *

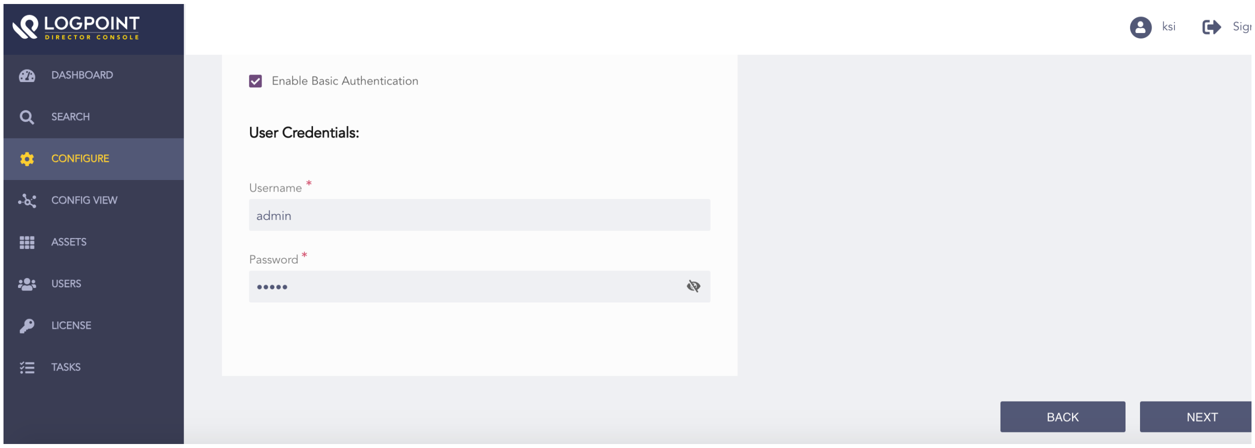
Hours

□ Enable Basic Authentication

Fig. 3: Selecting STIX 2.0 Version

9. Select the **Enable Basic Authentication** option if your *TAXII* server uses basic authentication.

10. In the **User Credentials** section, enter your **Username** and **Password** of the *TAXII* server.



☑ Enable Basic Authentication

User Credentials:

Username *
admin

Password *
•••••

Fig. 4: Continued Configuring STIX/TAXII Enrichment Source

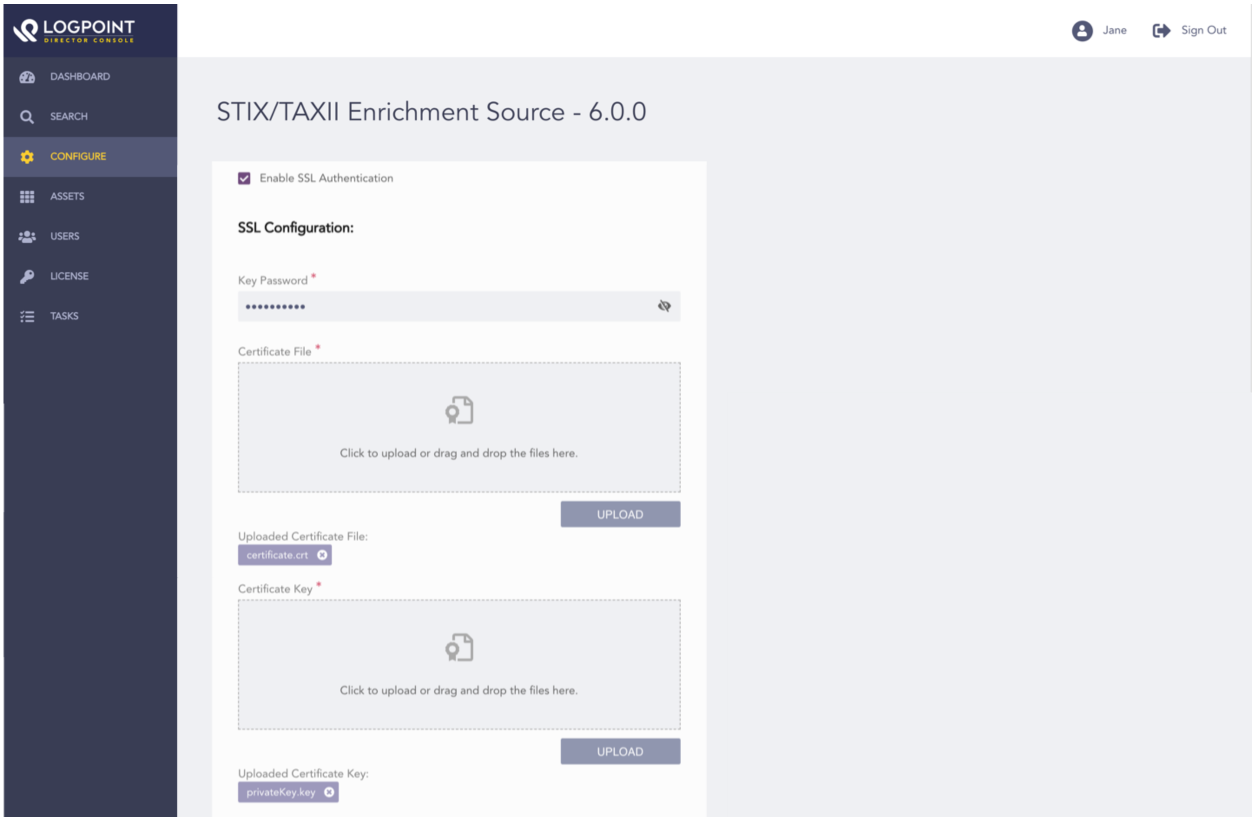
11. Select the **Enable SSL Authentication** option if your *TAXII* server uses SSL authentication.

12. In the **SSL Configuration** section:

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

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

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



STIX/TAXII Enrichment Source - 6.0.0

☑ Enable SSL Authentication

SSL Configuration:

Key Password *

••••••••••

Certificate File *

Click to upload or drag and drop the files here.

Uploaded Certificate File:

certificate.crt

Certificate Key *

Click to upload or drag and drop the files here.

Uploaded Certificate Key:

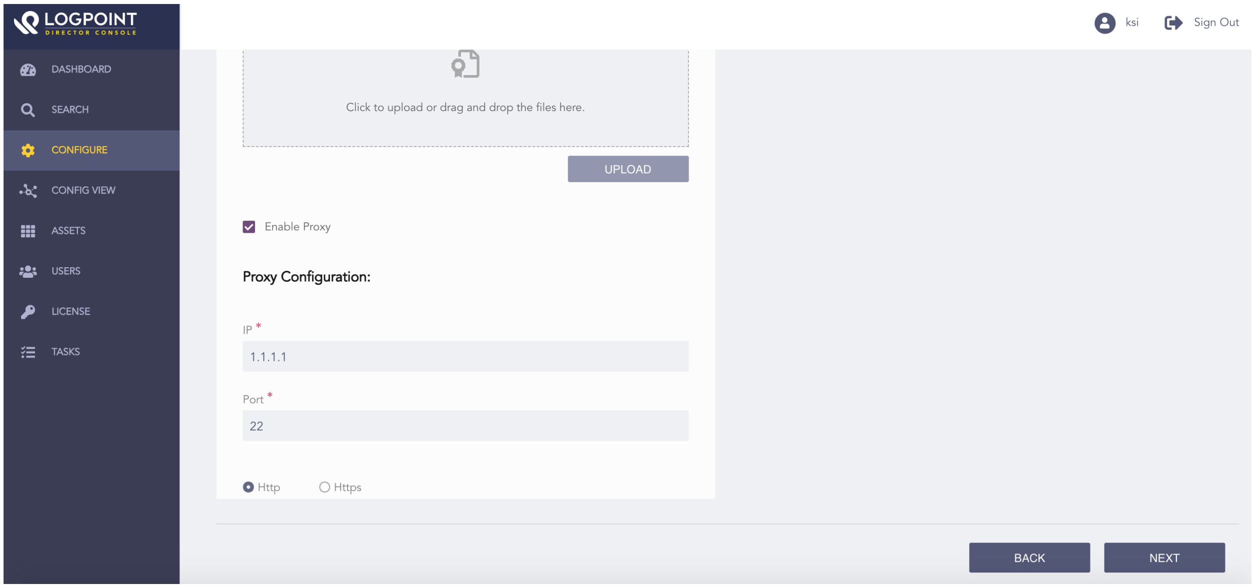
privateKey.key

Fig. 5: Continued Configuring STIX/TAXII Enrichment Source

13. Select the **Enable Proxy** option to connect the *TAXII* server via a proxy server.
14. In the **Proxy Configuration** section:

    14.1. Enter the **IP** address and the **Port** number of the proxy server.

    14.2. Select **Http** or **Https** protocol as required.
15. Click **Next.**



☑ Enable Proxy

Proxy Configuration:

IP *

1.1.1.1

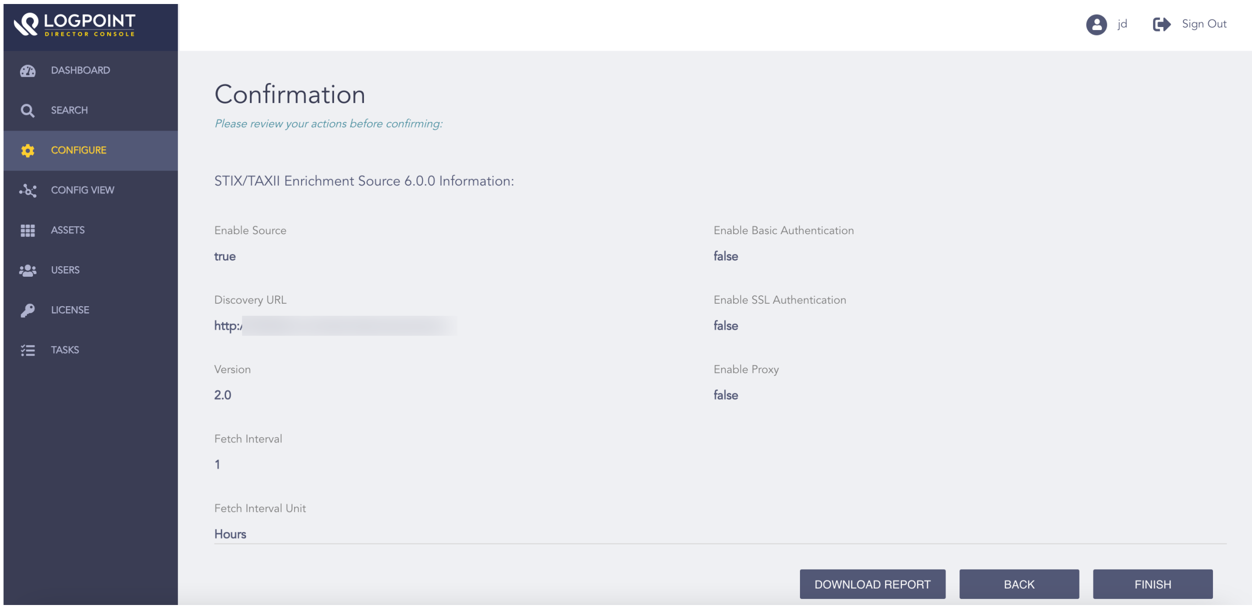
Port *

22

● Http ○ Https

Fig. 6: Continued Configuring STIX/TAXII Enrichment Source

16. Review your changes. You can go **Back** to make any changes if necessary.
17. Click **Finish.**
18. Click **OK.**



Confirmation

Please review your actions before confirming:

STIX/TAXII Enrichment Source 6.0.0 Information:

Enable Source true	Enable Basic Authentication false
Discovery URL http:/[redacted]	Enable SSL Authentication false
Version 2.0	Enable Proxy false
Fetch Interval 1	
Fetch Interval Unit Hours	

Fig. 7: Confirming the Changes

CHAPTER

FOUR

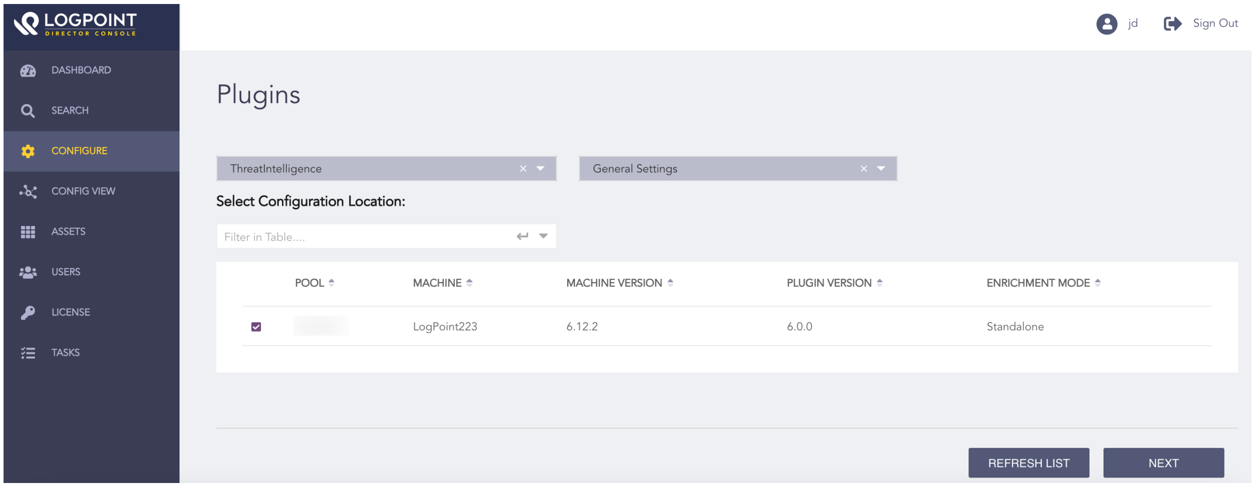
GENERAL INFORMATION

4.1 Viewing the General Information in Director Console

You can view the general information of *STIX/TAXII* data in the **ThreatIntelligence - General Settings** page. The page displays the status of fetched data with the time for **Last Fetch Attempt** and the **Last Successful Fetch**.

Follow these steps to view the General Information:

1. Click **Configure** from the left navigation bar.
2. Click **Plugins**.
3. Select **ThreatIntelligence** from the **Select Plugin Type** drop-down.
4. Select LogPoint machines to view the general information of *STIX/TAXII* data . You can select multiple LogPoint machines of different pools.



Plugins

ThreatIntelligence

General Settings

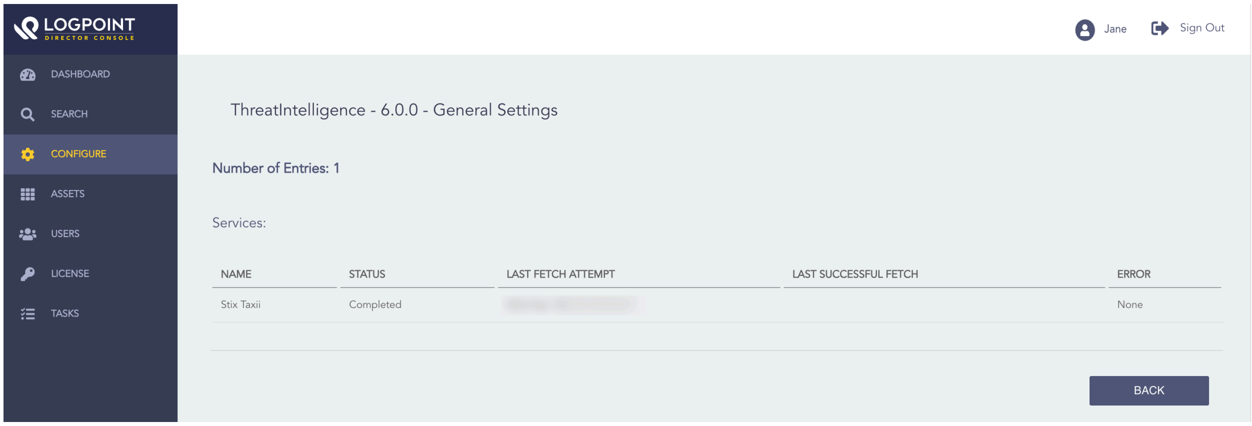
Select Configuration Location:

	POOL	MACHINE	MACHINE VERSION	PLUGIN VERSION	ENRICHMENT MODE
☑	[redacted]	LogPoint223	6.12.2	6.0.0	Standalone

Fig. 1: Selecting LogPoint Machines

Note: You can **Refresh List** to sync the data between LogPoint and Director Fabric.

5. Select **General Settings** from the **Select Plugin Sub-type** drop-down.
6. Click **Next.**



ThreatIntelligence - 6.0.0 - General Settings

Number of Entries: 1

Services:

NAME	STATUS	LAST FETCH ATTEMPT	LAST SUCCESSFUL FETCH	ERROR
Stix Taxii	Completed	[redacted]		None

Fig. 2: Viewing the General Information of StixTaxii

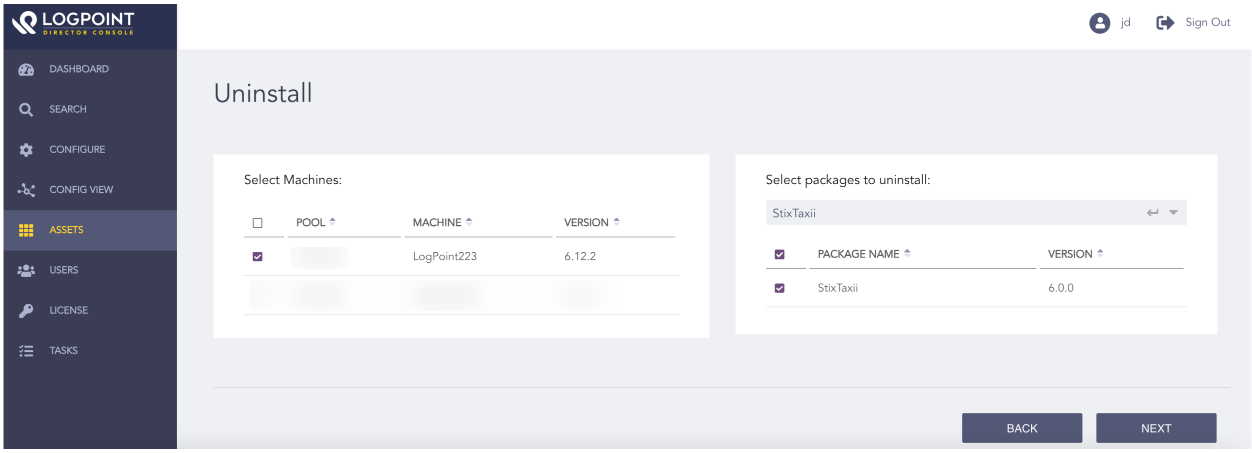
CHAPTER

FIVE

UNINSTALLATION

5.1 Uninstalling the StixTaxii Application in Director Console

1. Click **Assets** from the left navigation bar.
2. Click **Uninstall.**
3. Select LogPoint machines to uninstall the StixTaxii application. You can select multiple machines of different pools.
4. Select **StixTaxii** from the list of available packages.
5. Click **Next.**



Uninstall

Select Machines:

□	POOL	MACHINE	VERSION
☑	[redacted]	LogPoint223	6.12.2
[redacted]	[redacted]	[redacted]	[redacted]

Select packages to uninstall:

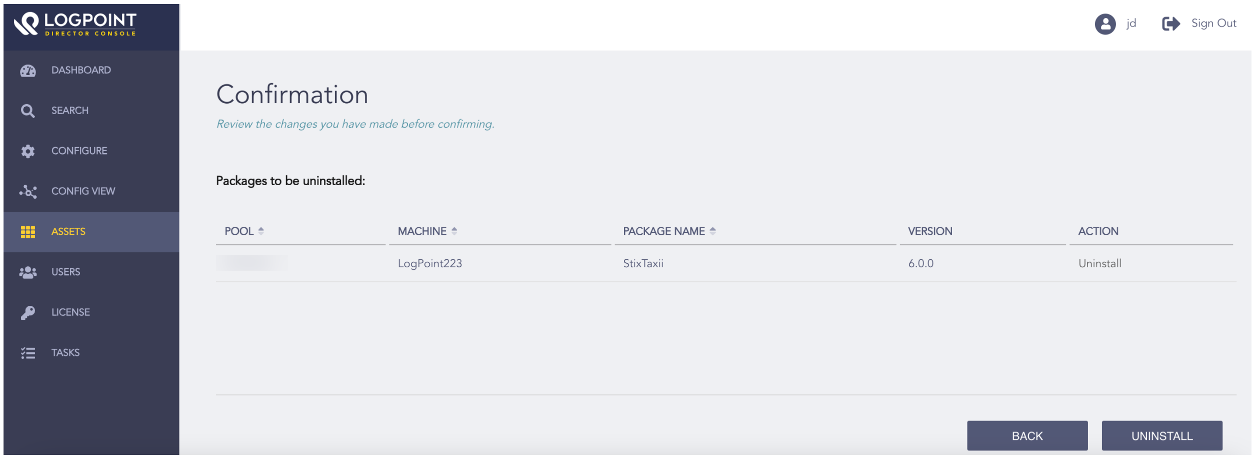
StixTaxii

☑	PACKAGE NAME	VERSION
☑	StixTaxii	6.0.0

Fig. 1: Selecting LogPoint Machines

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

8. Click **OK.**



Confirmation

Review the changes you have made before confirming.

Packages to be uninstalled:

POOL	MACHINE	PACKAGE NAME	VERSION	ACTION
[redacted]	LogPoint223	StixTaxii	6.0.0	Uninstall

Fig. 2: Confirming the Changes