LOGPOINT

Integrations

Threat Intelligence For Director Console UI

V6.3.0

CONTENTS

CHAPTER

ONE

THREAT INTELLIGENCE

Threat Intelligence (TI) fetches information and insights about existing or potential cyber threats and risks from various sources. It then assembles, processes and analyzes the fetched information and uses it to predict data breaches, vulnerable attacks and any evidence of pre-planned attacks or threats.

Supported Sources

- Emerging Threats
- Critical Stack
- CSIS
- Custom CSV
- MISP
- Blueliv
- Recorded Future
- StixTaxii

Threat Intelligence Components

1. **Enrichment Source**
    - ThreatIntelligence
2. **Process Command**
    - ti

CHAPTER

TWO

INSTALLING THREAT INTELLIGENCE

Prerequisite

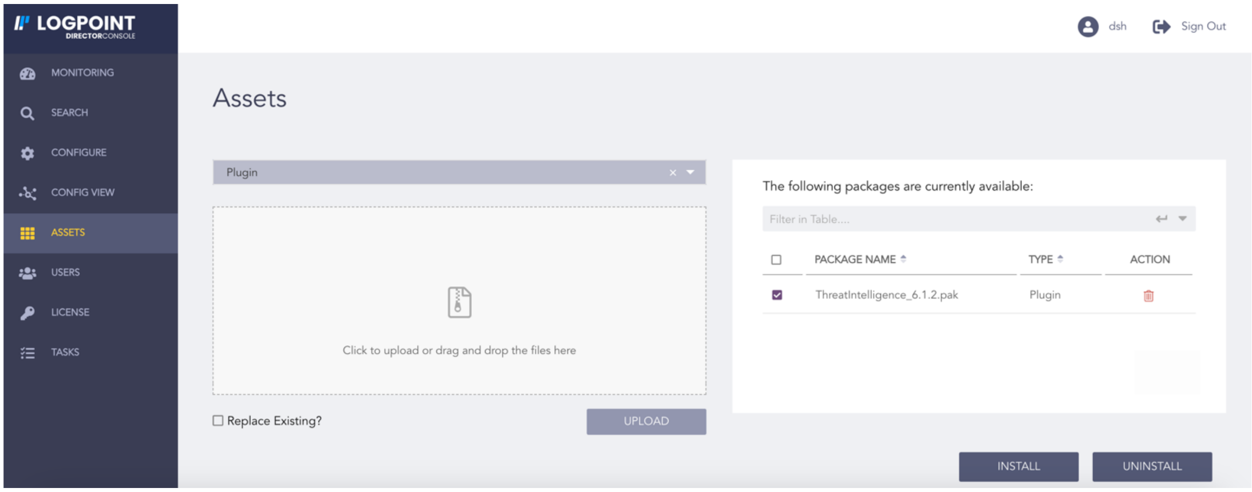
- Logpoint v7.5.0 or later
- Director Fabric v1.10.0 or later
- Director Console v1.10.0 or later

To install Threat Intelligence in Director Console:

1. Log in to Director Console.
2. Click **Assets** in the navigation bar.
3. Select **Plugins** from the **Assets Type** dropdown.
4. Click the *upload area* to browse, or drag and drop the Threat Intelligence .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 Threat Intelligence .pak from the list of available packages.
7. Click **INSTALL**.



□ Replace Existing?

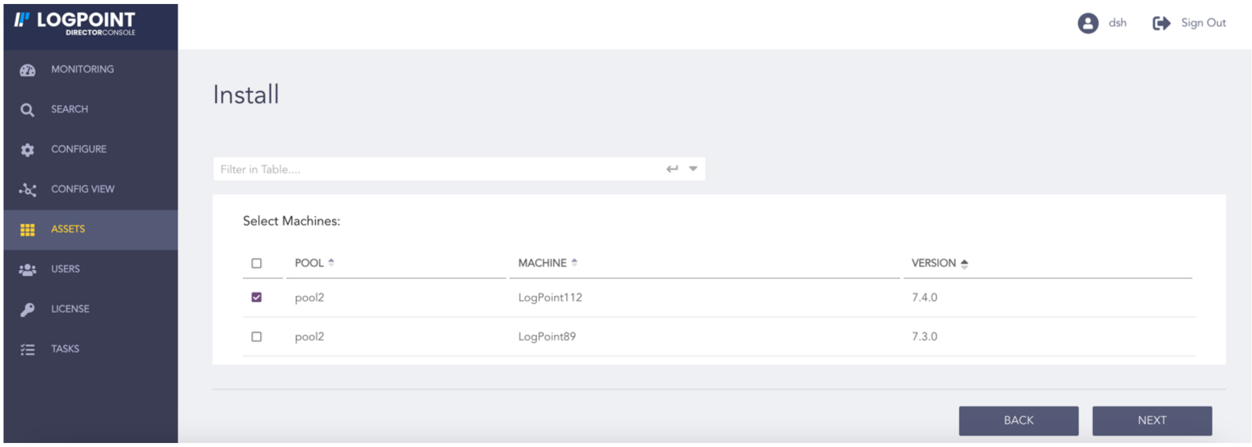
The following packages are currently available:

Filter in Table....

□	PACKAGE NAME	TYPE	ACTION
☑	ThreatIntelligence_6.1.2.pak	Plugin	🗑

Fig. 1: Selecting a Package

8. Select a Logpoint to install Threat Intelligence. You can select multiple Logpoints of different pools.
9. Click **NEXT**.



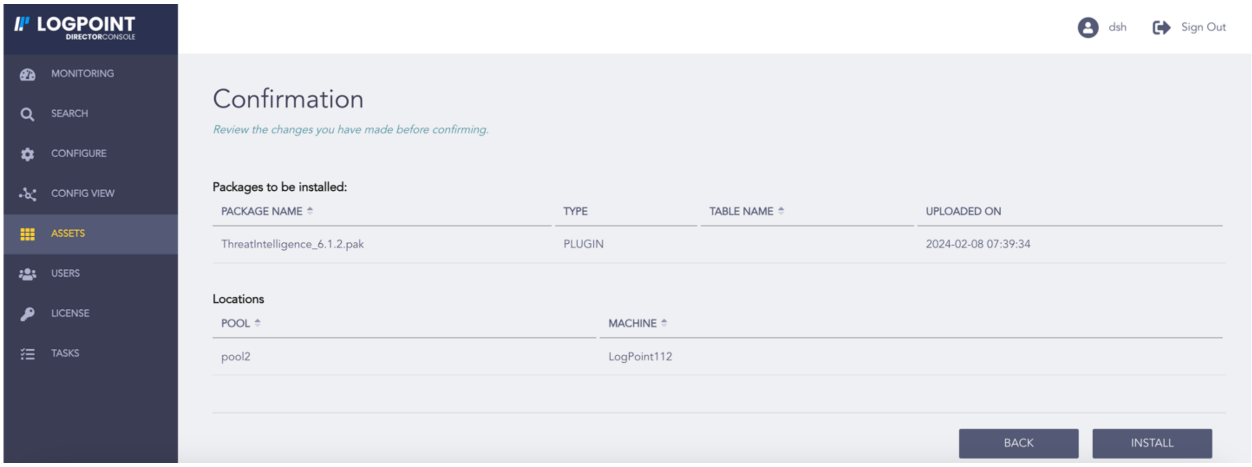
Filter in Table....

Select Machines:

□	POOL	MACHINE	VERSION
☑	pool2	LogPoint112	7.4.0
□	pool2	LogPoint89	7.3.0

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.



Confirmation

Review the changes you have made before confirming.

Packages to be installed:

PACKAGE NAME	TYPE	TABLE NAME	UPLOADED ON
ThreatIntelligence_6.1.2.pak	PLUGIN		2024-02-08 07:39:34

Locations

POOL	MACHINE
pool2	LogPoint112

Fig. 3: Confirming the Changes

CHAPTER

THREE

UNINSTALLING THREAT INTELLIGENCE

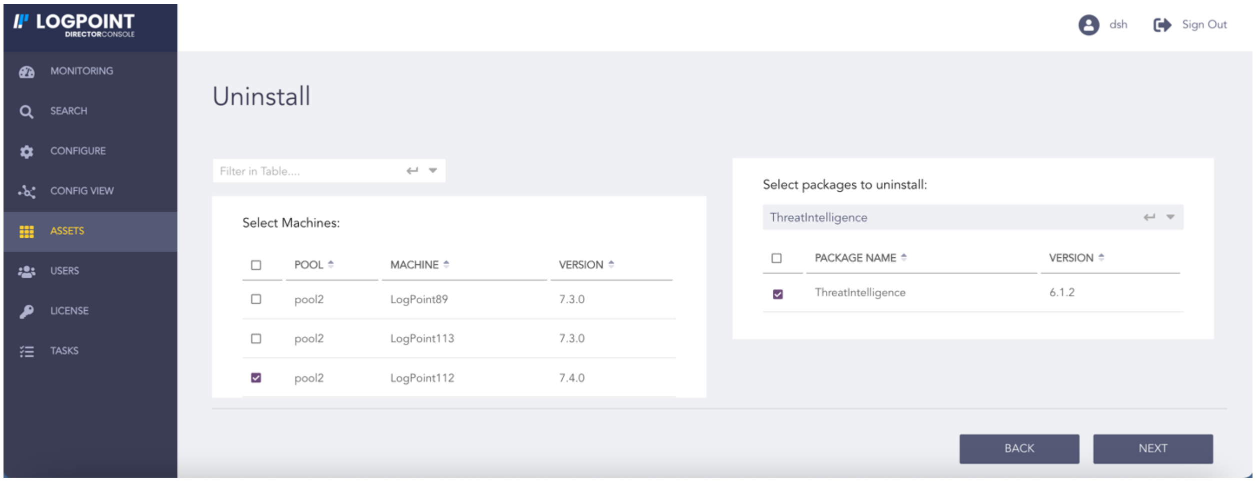
You must first remove Threat Intelligence source configuration to uninstall it.

To remove the configurations:

1. Click **Configure** in the navigation bar.
2. Under *Settings*, click **Plugins**.
3. Select **ThreatIntelligence** from the **Select Plugin Type** drop-down.
4. Select a Logpoint where the threat sources are configured. You can select multiple Logpoints of different pools.
5. Select the configured source from the **Select Plugin Sub-type** drop-down.
6. Deselect **Enable Source** of the activated Threat Intelligence source.
7. Click **NEXT**
8. Review your changes. You can go **BACK** to make any changes if necessary.
9. Click **FINISH**.
10. Click **OK**.

To uninstall Threat Intelligence:

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



Uninstall

Select Machines:

☐	POOL	MACHINE	VERSION
☐	pool2	LogPoint89	7.3.0
☐	pool2	LogPoint113	7.3.0
☑	pool2	LogPoint112	7.4.0

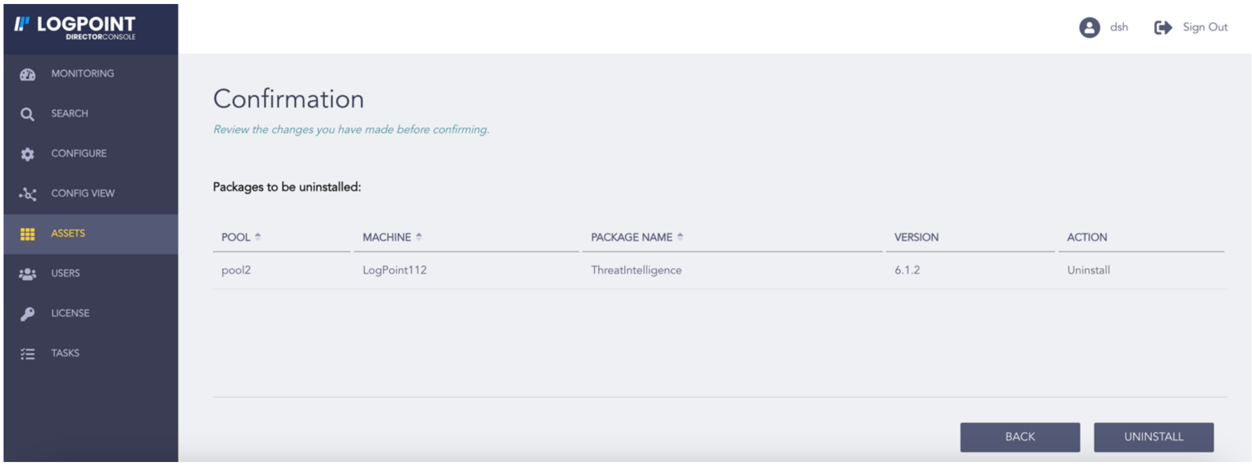
Select packages to uninstall:

ThreatIntelligence

☐	PACKAGE NAME	VERSION
☑	ThreatIntelligence	6.1.2

Fig. 1: Selecting Threat Intelligence

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



Confirmation

Review the changes you have made before confirming.

Packages to be uninstalled:

POOL	MACHINE	PACKAGE NAME	VERSION	ACTION
pool2	LogPoint112	ThreatIntelligence	6.1.2	Uninstall

Fig. 2: Confirming the Changes

CHAPTER

FOUR

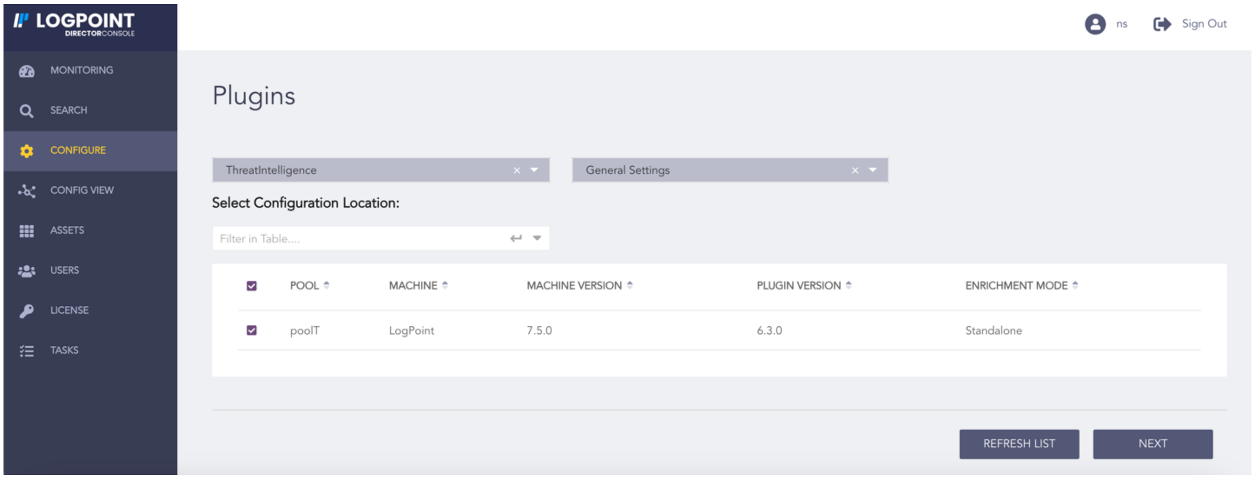
CONFIGURING THREAT INTELLIGENCE

For Threat Intelligence to fetch information and insights from sources, an initial setup where information such as the sources API name, API key and Base URL must be configured. The sources are Emerging Threats, Critical Stack, CSIS, Custom CSV, MISP, Blueliv, Recorded Future, and StixTaxii. You must also specify how to standardize the fetched information in Mapping and whether to assign a pseudoname to fields of the fetched information in Alias.

4.1 General Settings

General Settings consists of all the details about the fetched data. You can 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 Fetch Date**. The information of a disabled Threat Intelligence source is not displayed.

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



Plugins

ThreatIntelligence × ▾ General Settings × ▾

Select Configuration Location:

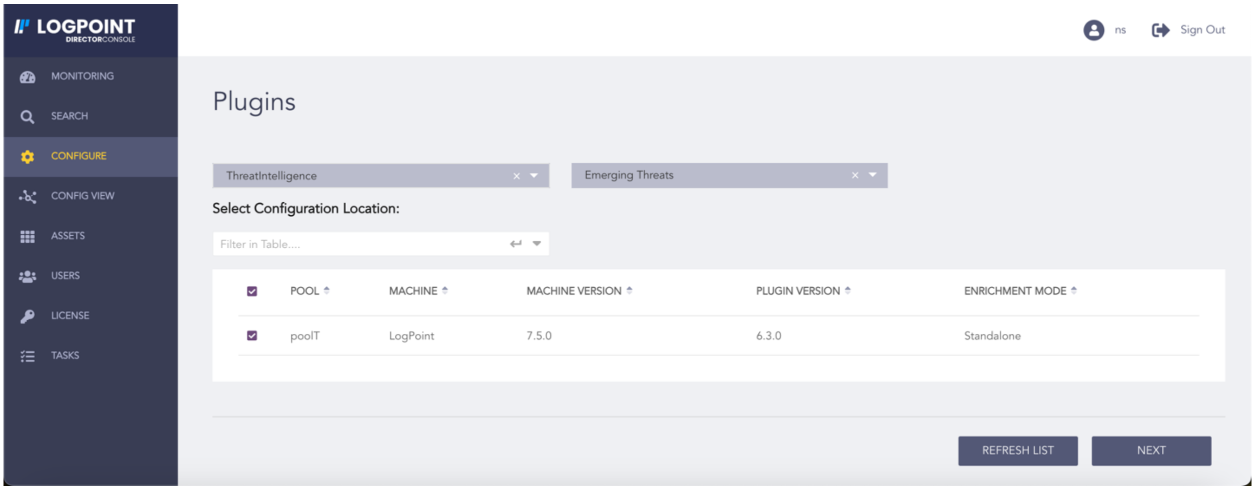
Filter in Table....

☑	POOL	MACHINE	MACHINE VERSION	PLUGIN VERSION	ENRICHMENT MODE
☑	poolT	LogPoint	7.5.0	6.3.0	Standalone

Fig. 1: Selecting General Settings

4.2 Emerging Threats

1. Click **Configure** in the navigation bar.
2. Under *Settings*, click **Plugins**.
3. Select **ThreatIntelligence** from the **Select Plugin Type** drop-down.
4. Select a Logpoint to configure Emerging Threats. You can select multiple Logpoints of different pools.
5. Select **Emerging Threats** from the **Select Plugin Sub-type** drop-down.
6. Click **NEXT**.



Plugins

ThreatIntelligence × ▾ Emerging Threats × ▾

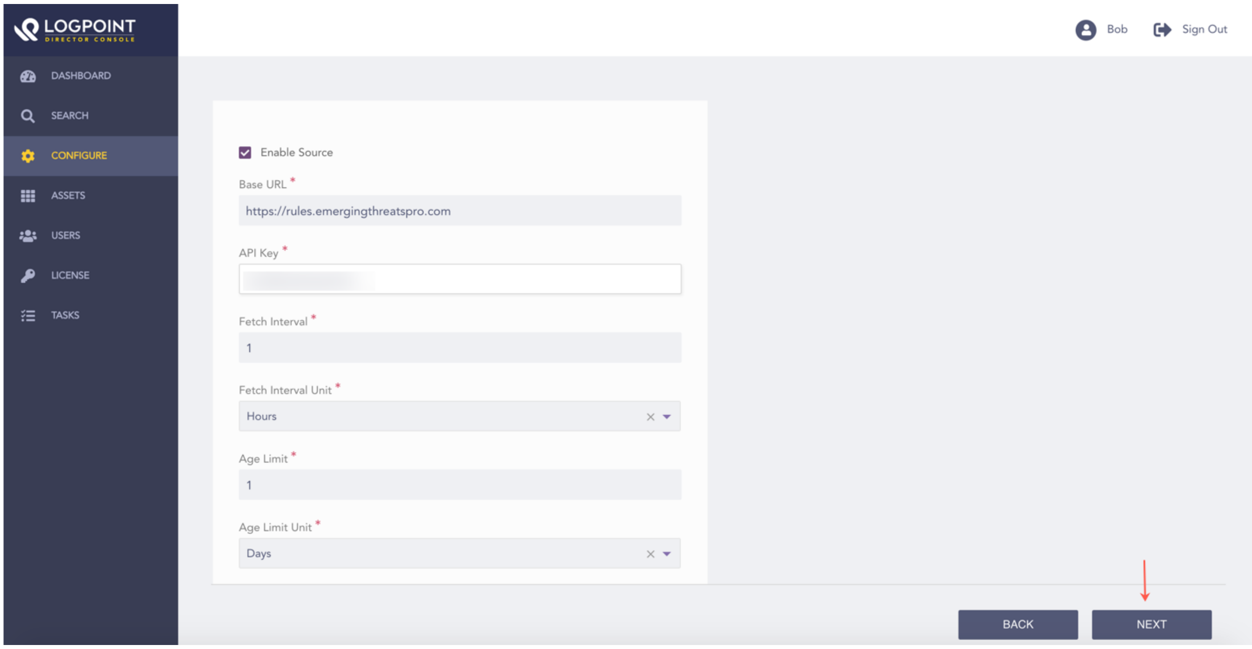
Select Configuration Location:

Filter in Table....

☑	POOL	MACHINE	MACHINE VERSION	PLUGIN VERSION	ENRICHMENT MODE
☑	poolT	LogPoint	7.5.0	6.3.0	Standalone

Fig. 2: Selecting Emerging Threats

7. Select **Enable Source** to activate Emerging Threats.
8. Enter the *Emerging Threats* **Base URL** and **API Key**. In **API Key**, you must enter the API generated after you configure the required feeds of Threat Intelligence data on Emerging Threat.
9. Enter the frequency at which data is retrieved in **Fetch Interval**.
10. Select the **Fetch Interval Unit** in hours or days.
11. Enter the **Age Limit**, which is the retention period of the fetched data in days or hours. Enter it as *0* to retain the last fetched data until the next successful fetch.
12. Select the **Age Limit Unit** in hours or days.



☑ Enable Source

Base URL *

https://rules.emergingthreatspro.com

API Key *

[redacted]

Fetch Interval *

1

Fetch Interval Unit *

Hours

Age Limit *

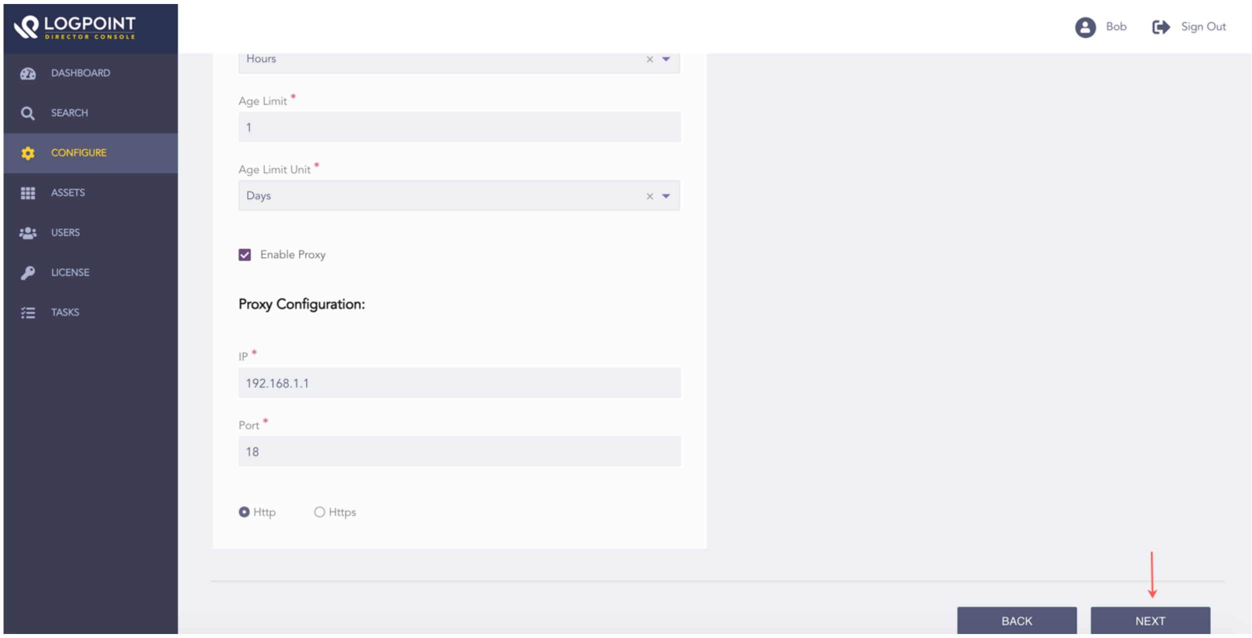
1

Age Limit Unit *

Days

Fig. 3: Enabling Emerging Threats

13. Select **Enable Proxy** to use a proxy server.
14. In **Proxy Configuration**:
    - 14.1. Enter the proxy server **IP** Address and **Port number**.
    - 14.2. Select the **Http** or **Https** protocol as required.
15. Click **NEXT**.



Hours

Age Limit *

1

Age Limit Unit *

Days

☑ Enable Proxy

Proxy Configuration:

IP *

192.168.1.1

Port *

18

● Http ○ Https

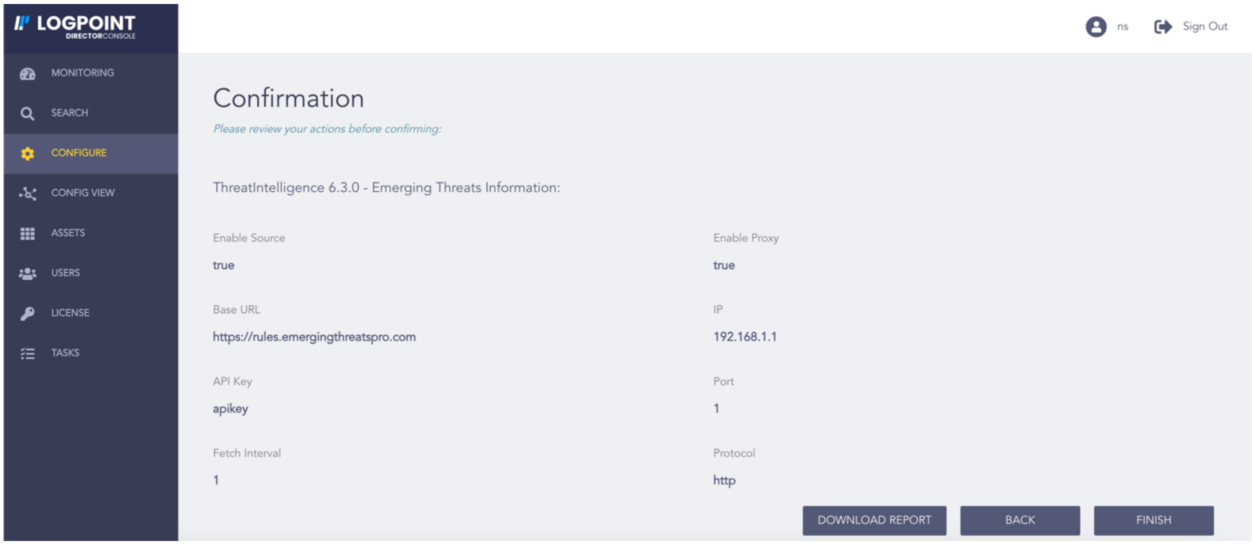
Fig. 4: Enabling Proxy Server

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

Note: Click **Download Report** to get a summary as a PDF.

17. Click **FINISH**.

18. Click **OK**.



Confirmation

Please review your actions before confirming:

ThreatIntelligence 6.3.0 - Emerging Threats Information:

Enable Source true	Enable Proxy true
Base URL https://rules.emergingthreatspro.com	IP 192.168.1.1
API Key apikey	Port 1
Fetch Interval 1	Protocol http

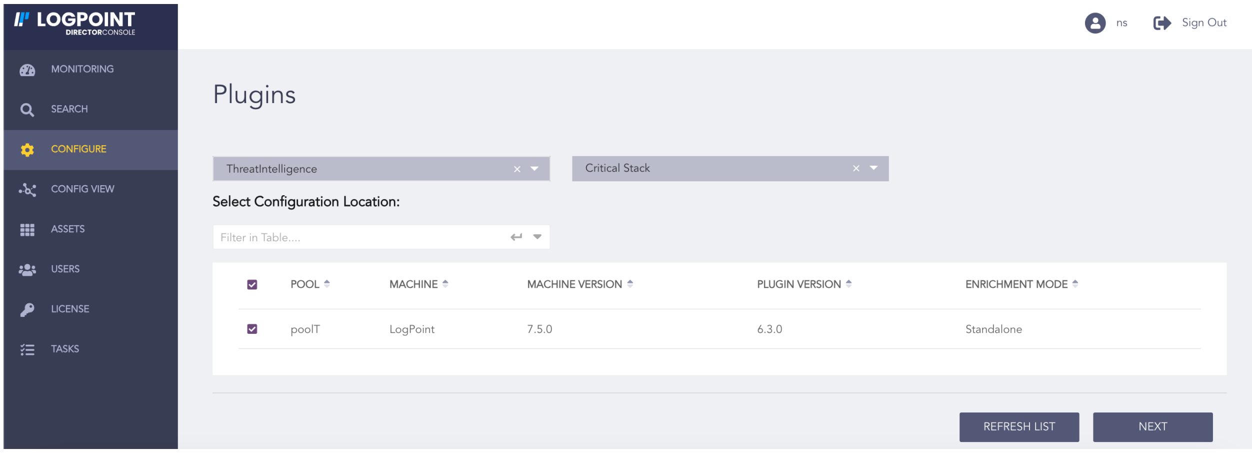
Fig. 5: Confirming the Changes

4.3 Critical Stack

> **Important:** We will be removing the critical stack threat source from the upcoming version, so it is recommended to use the MISP threat source.

4.3.1 Adding a Critical Stack API

1. Click **Configure** in the navigation bar.
2. Under *Settings*, click **Plugins**.
3. Select **ThreatIntelligence** from the **Select Plugin Type** drop-down.
4. Select the Logpoint to configure Critical Stack API. You can select multiple Logpoints of different pools.
5. Select **Critical Stack** from the **Select Plugin Sub-type** drop-down.
6. Click **NEXT**.



Plugins

ThreatIntelligence

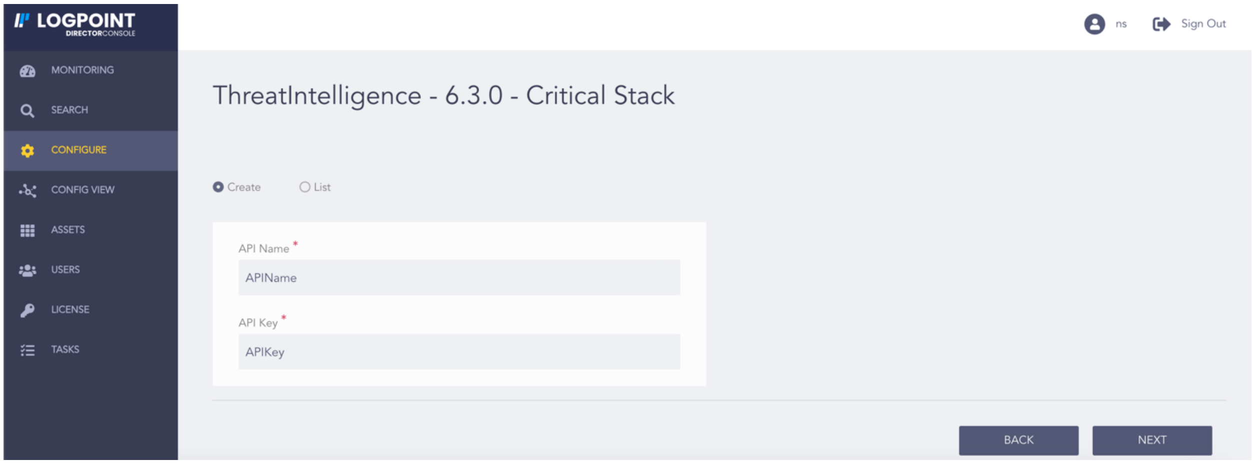
Critical Stack

Select Configuration Location:

☑	POOL	MACHINE	MACHINE VERSION	PLUGIN VERSION	ENRICHMENT MODE
☑	poolT	LogPoint	7.5.0	6.3.0	Standalone

Fig. 6: Selecting Critical Stack

7. In **Create**, enter the Critical Stack **API Name** and **API Key**. You can see the lists of all the Critical Stack source configurations in *List*.
8. Click **NEXT**.



ThreatIntelligence - 6.3.0 - Critical Stack

● Create ○ List

API Name *

APIName

API Key *

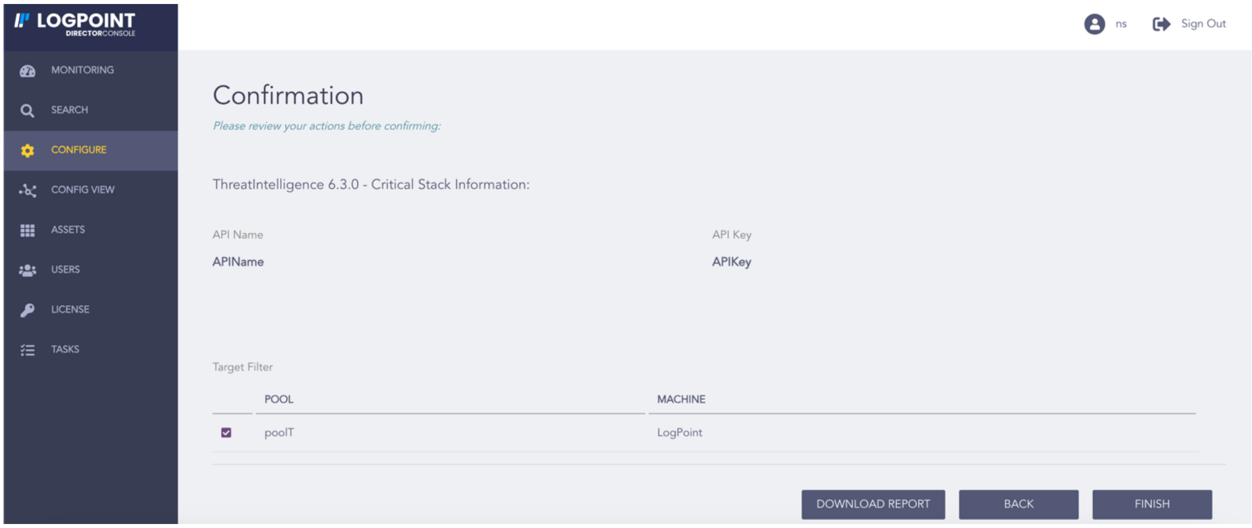
APIKey

Fig. 7: Critical Stack

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

Note: Click **Download Report** to get a summary as a PDF.

10. Click **FINISH**. Click **OK** to confirm.



Confirmation

Please review your actions before confirming:

ThreatIntelligence 6.3.0 - Critical Stack Information:

API Name	API Key
APIName	APIKey

Target Filter

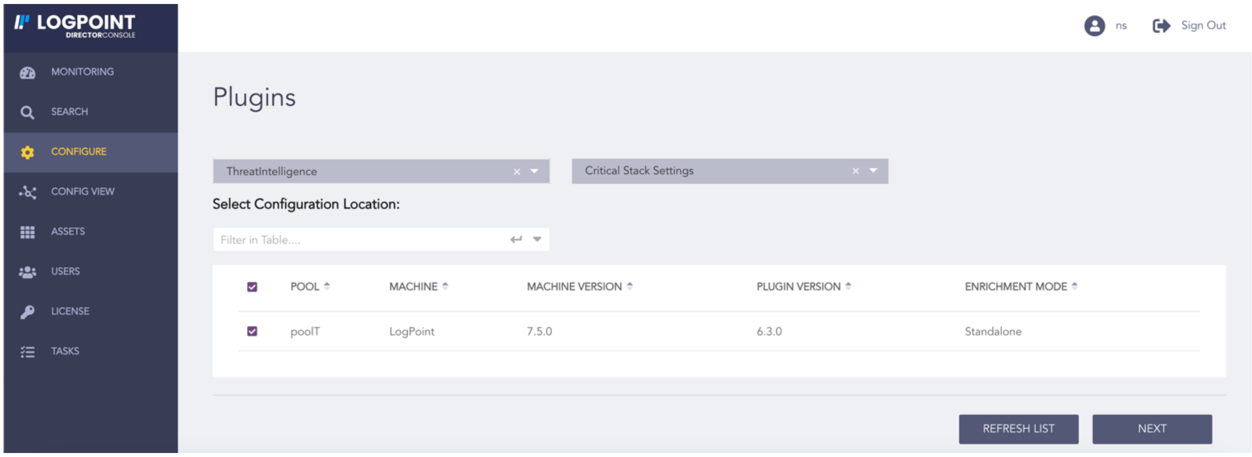
	POOL	MACHINE
☑	poolT	LogPoint

Fig. 8: Confirming the Changes

4.3.2 Configuring the Critical Stack Source

1. Click **Configure** in the navigation bar.

2. Under *Settings*, click **Plugins**.
3. Select **ThreatIntelligence** from the **Select Plugin Type** drop-down.
4. Select the Logpoint to configure Critical Stack Source. You can select multiple Logpoints of different pools.
5. Select **Critical Stack Settings** from the **Select Plugin Sub-type** drop-down.
6. Click **NEXT**.



Plugins

ThreatIntelligence

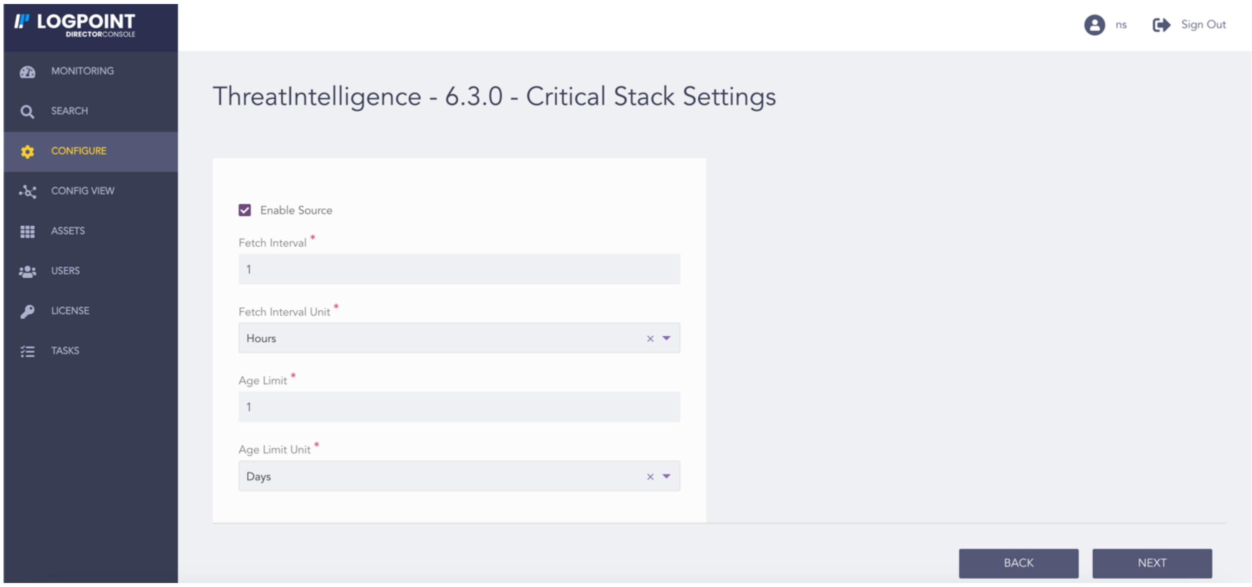
Critical Stack Settings

Select Configuration Location:

☑	POOL	MACHINE	MACHINE VERSION	PLUGIN VERSION	ENRICHMENT MODE
☑	poolT	LogPoint	7.5.0	6.3.0	Standalone

Fig. 9: Selecting Critical Stack Settings

7. Select **Enable Source** to activate Critical Stack.
8. Enter the frequency at which data is retrieved in **Fetch Interval**.
9. Select the **Fetch Interval Unit** in hours or days.
10. Enter the **Age Limit**, which is the retention period of the fetched data in days or hours. Enter it as *0* to retain the last fetched data until the next successful fetch.
11. Select the **Age Limit Unit** in hours or days.



ThreatIntelligence - 6.3.0 - Critical Stack Settings

☑ Enable Source

Fetch Interval *: 1

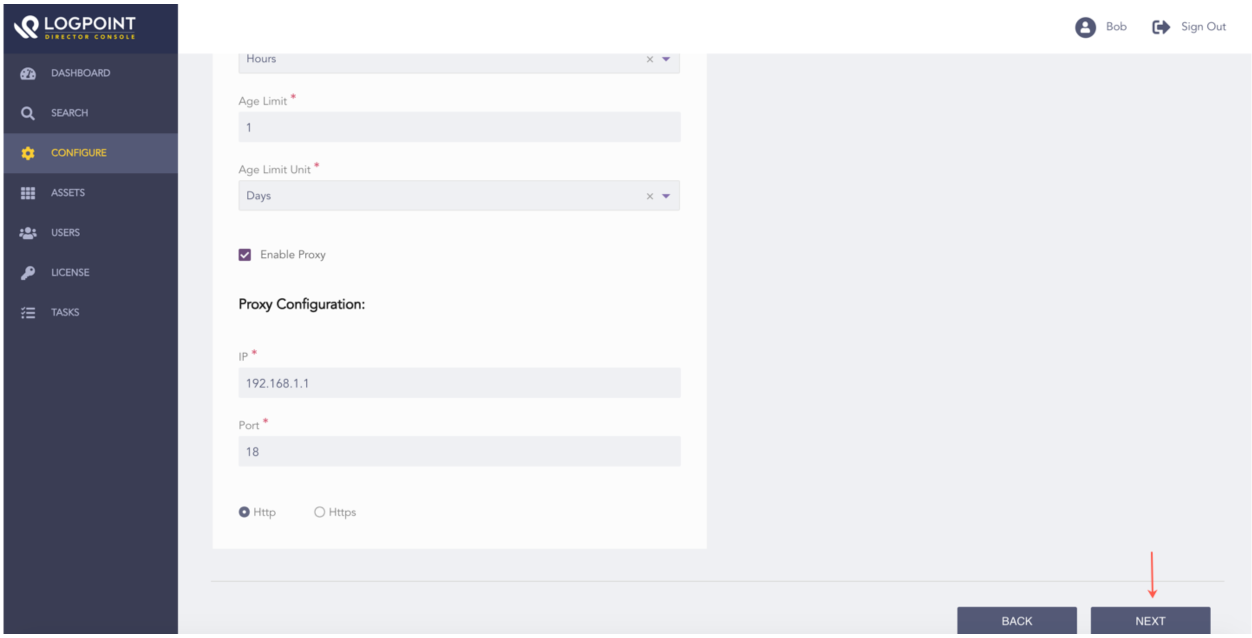
Fetch Interval Unit *: Hours

Age Limit *: 1

Age Limit Unit *: Days

Fig. 10: Enabling Critical Stack

12. Select **Enable Proxy** to use a proxy server.
13. In **Proxy Configuration**:
    13.1. Enter the proxy server **IP** Address and **Port number**.
    13.2. Select either **Http** or **Https** protocol.
14. Click **NEXT**.



Hours

Age Limit *: 1

Age Limit Unit *: Days

☑ Enable Proxy

Proxy Configuration:

IP *: 192.168.1.1

Port *: 18

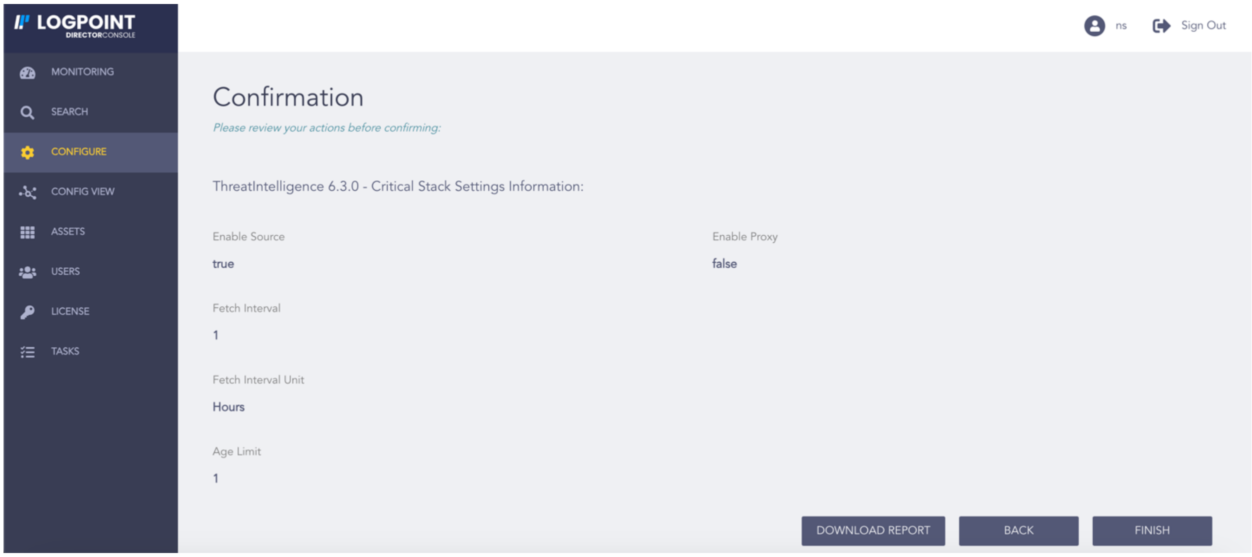
● Http ○ Https

Fig. 11: Enabling Proxy Server

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

Note: Click **Download Report** to get a summary as a PDF.

16. Click **FINISH**. Click **OK** to confirm.



Confirmation

Please review your actions before confirming:

ThreatIntelligence 6.3.0 - Critical Stack Settings Information:

Enable Source
true

Enable Proxy
false

Fetch Interval
1

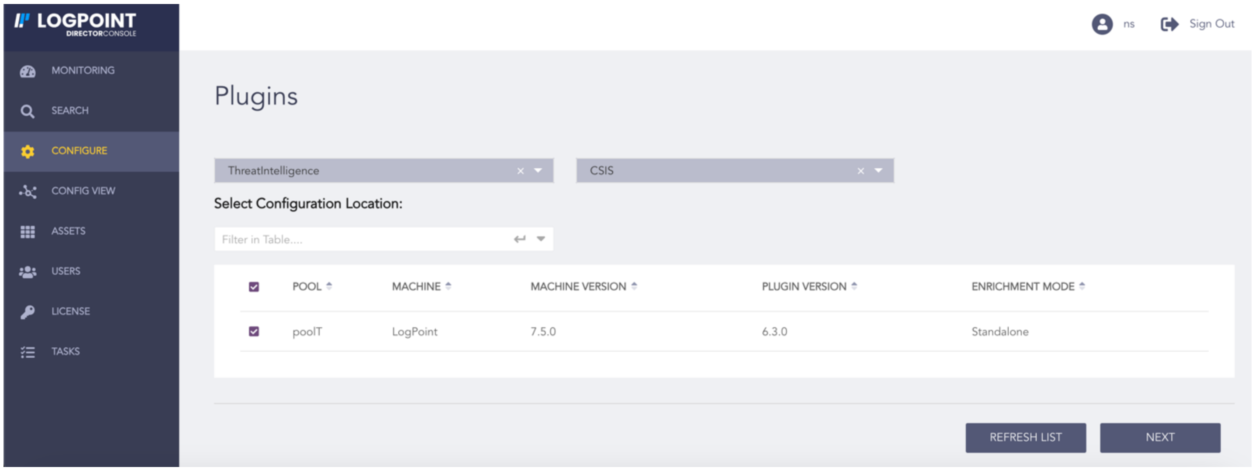
Fetch Interval Unit
Hours

Age Limit
1

Fig. 12: Confirming the Changes

4.4 CSIS

1. Click **Configure** in the navigation bar.
2. Under *Settings*, click **Plugins**.
3. Select **ThreatIntelligence** from the **Select Plugin Type** drop-down.
4. Select the Logpoint to configure CSIS. You can select multiple Logpoints of different pools.
5. Select **CSIS** from the **Select Plugin Sub-type** drop-down.
6. Click **NEXT**.



Plugins

ThreatIntelligence

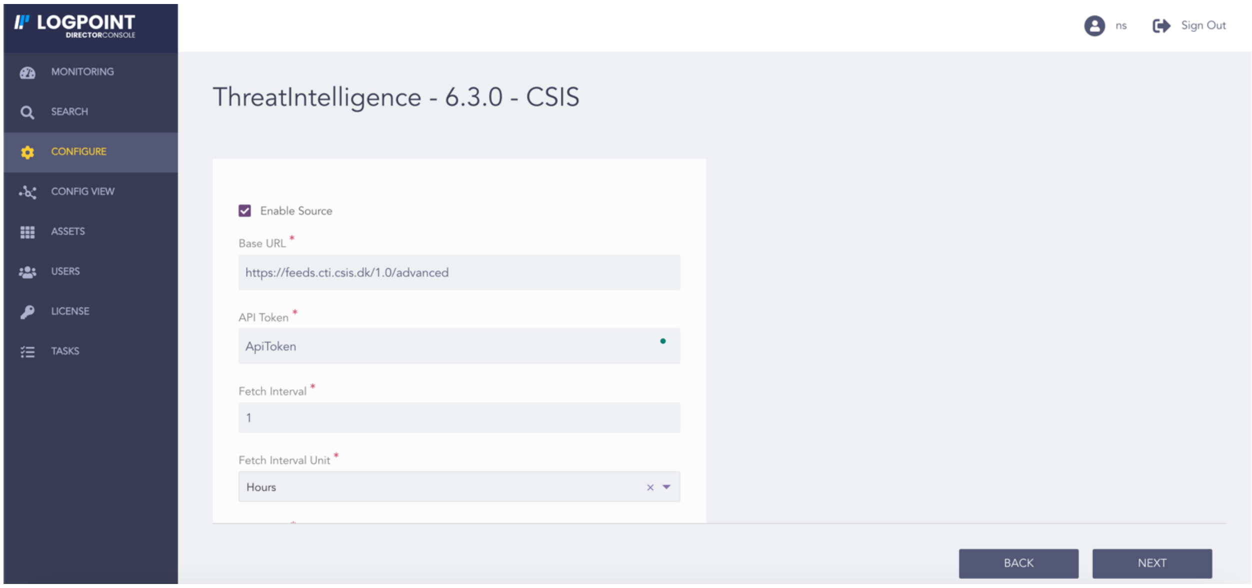
CSIS

Select Configuration Location:

☑	POOL	MACHINE	MACHINE VERSION	PLUGIN VERSION	ENRICHMENT MODE
☑	poolT	LogPoint	7.5.0	6.3.0	Standalone

Fig. 13: Selecting CSIS

7. Select **Enable Source** to activate CSIS.
8. Enter the CSIS **Base URL** and **API Token**.
9. Enter the frequency at which data is retrieved in **Fetch Interval**.
10. Select the **Fetch Interval Unit** in hours or days.
11. Enter the **Age Limit**, which is the retention period of the fetched data in days or hours. Enter it as *0* to retain the last fetched data until the next successful fetch.
12. Select the **Age Limit Unit** in hours or days.



ThreatIntelligence - 6.3.0 - CSIS

☑ Enable Source

Base URL *
https://feeds.cti.csis.dk/1.0/advanced

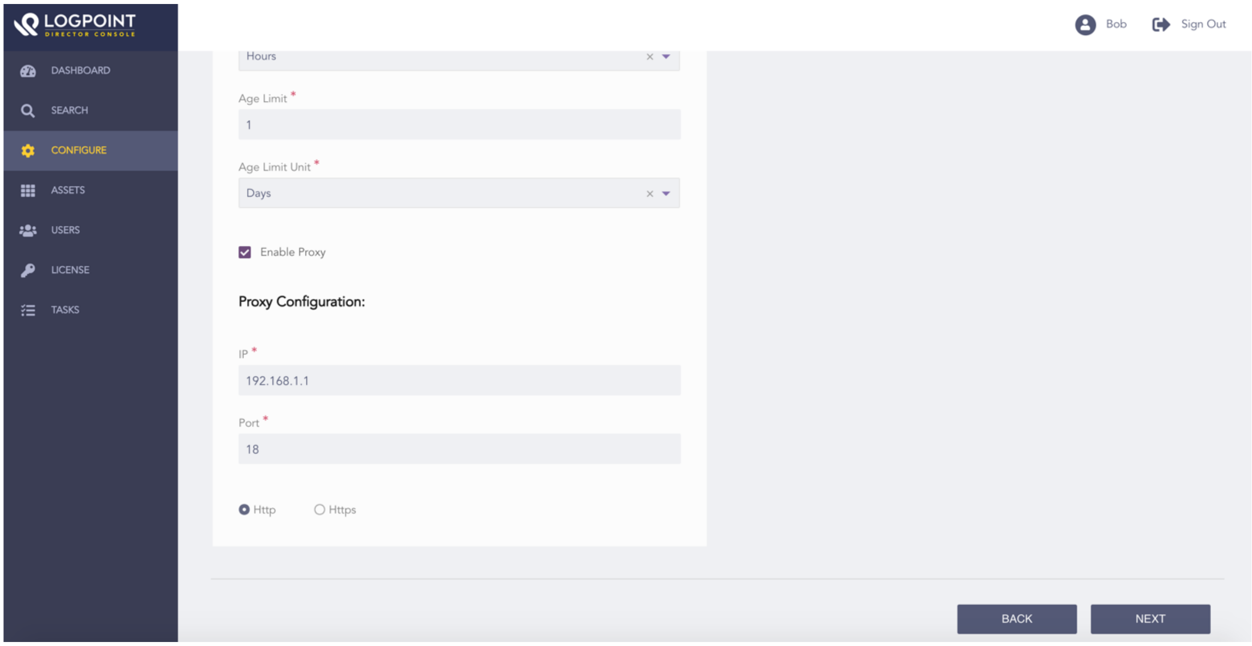
API Token *
ApiToken

Fetch Interval *
1

Fetch Interval Unit *
Hours

Fig. 14: Enabling CSIS

13. Select **Enable Proxy** to use a proxy server.
14. In **Proxy Configuration**:
    14.1. Enter the proxy server **IP** Address and **Port number**.
    14.2. Select either **Http** or **Https** protocol.
15. Click **NEXT**.



Hours

Age Limit *
1

Age Limit Unit *
Days

☑ Enable Proxy

Proxy Configuration:

IP *
192.168.1.1

Port *
18

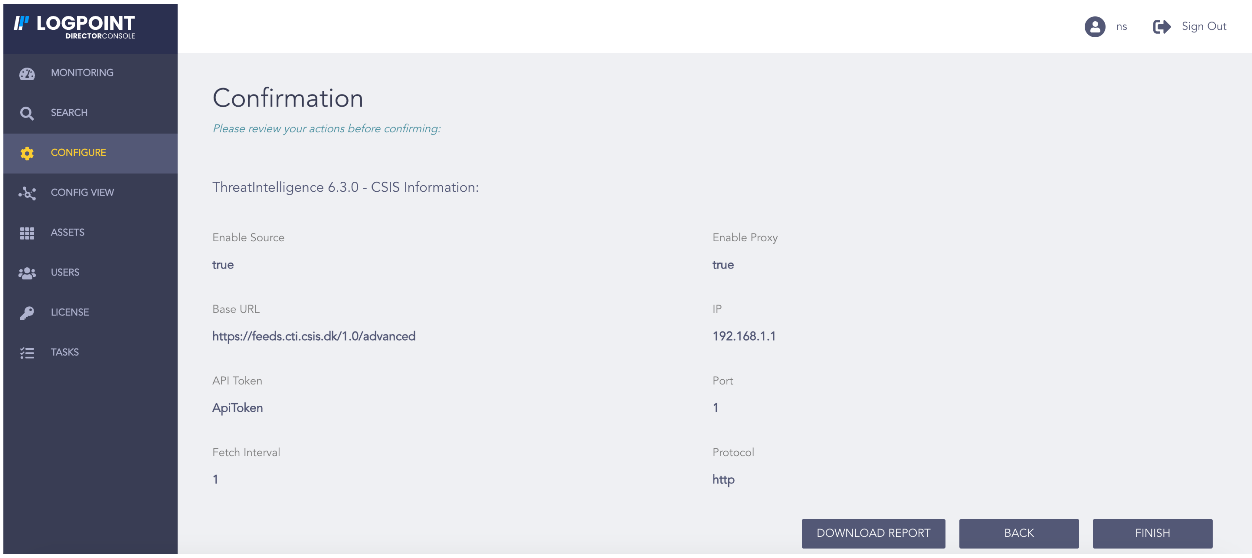
● Http ○ Https

Fig. 15: Enabling Proxy Server

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

Note: Click **Download Report** to get a summary as a PDF.

17. Click **FINISH**. Click **OK** to confirm.



Confirmation

Please review your actions before confirming:

ThreatIntelligence 6.3.0 - CSIS Information:

Enable Source: true

Enable Proxy: true

Base URL: https://feeds.cti.csis.dk/1.0/advanced

IP: 192.168.1.1

API Token: ApiToken

Port: 1

Fetch Interval: 1

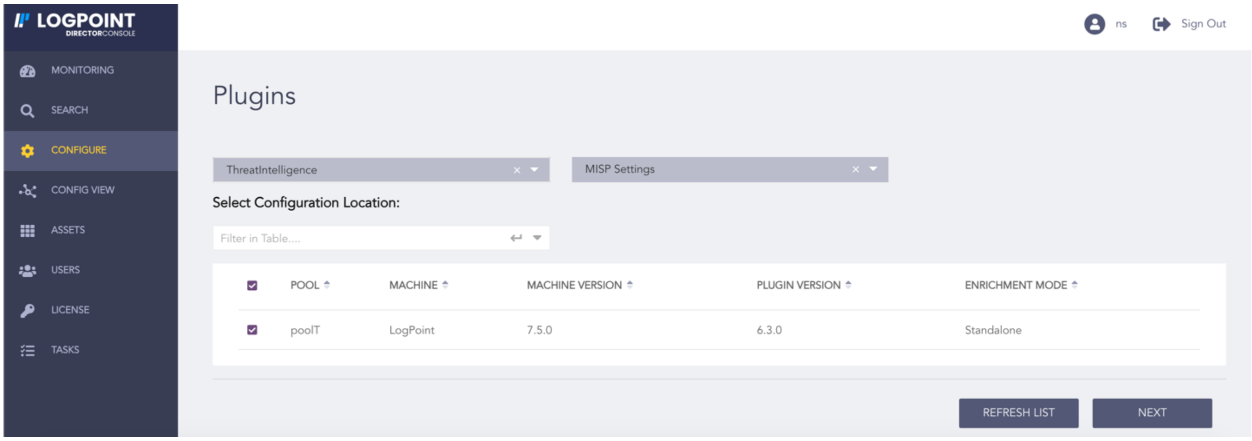
Protocol: http

Fig. 16: Confirming the Changes

4.5 MISP

4.5.1 Configuring MISP Settings

1. Click **Configure** in the navigation bar.
2. Under *Settings*, click **Plugins**.
3. Select **ThreatIntelligence** from the **Select Plugin Type** drop-down.
4. Select the Logpoint to configure MISP Settings. You can select multiple Logpoints of different pools.
5. Select **MISP Settings** from the **Select Plugin Sub-type** drop-down.
6. Click **NEXT**.



Plugins

ThreatIntelligence

MISP Settings

Select Configuration Location:

Filter in Table....

☑	POOL	MACHINE	MACHINE VERSION	PLUGIN VERSION	ENRICHMENT MODE
☑	poolT	LogPoint	7.5.0	6.3.0	Standalone

Fig. 17: Selecting MISP Settings

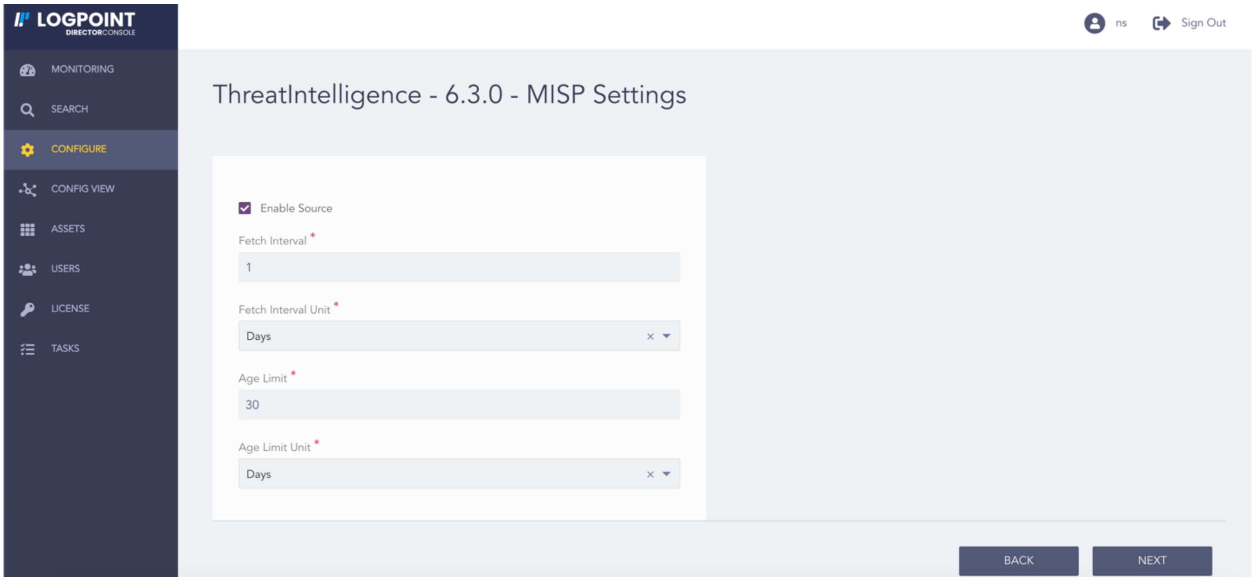
7. Select **Enable Source** to activate MISP.

8. Enter the frequency at which data is retrieved in **Fetch Interval**.

9. Select a **Fetch Interval Unit**.

10. Enter the **Age Limit**, which is the retention period of the fetched data in days or hours. Enter it as *0* to retain the last fetched data until the next successful fetch.

11. Select an **Age Limit Unit**.



ThreatIntelligence - 6.3.0 - MISP Settings

☑ Enable Source

Fetch Interval *
1

Fetch Interval Unit *
Days

Age Limit *
30

Age Limit Unit *
Days

Fig. 18: Enabling MISP

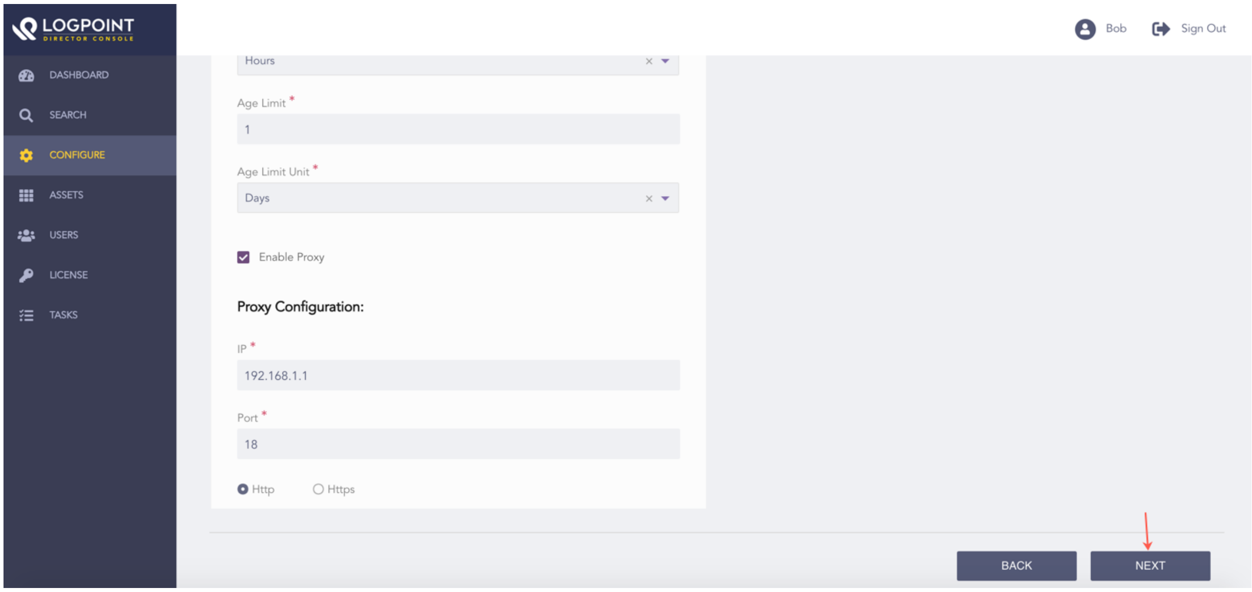
12. Select **Enable Proxy** to use a proxy server.

13. In **Proxy Configuration**:

    13.1. Enter the proxy server **IP** Address and **Port number**.

    13.2. Select either **Http** or **Https** protocol.

14. Click **NEXT**.



Hours

Age Limit *

1

Age Limit Unit *

Days

☑ Enable Proxy

Proxy Configuration:

IP *

192.168.1.1

Port *

18

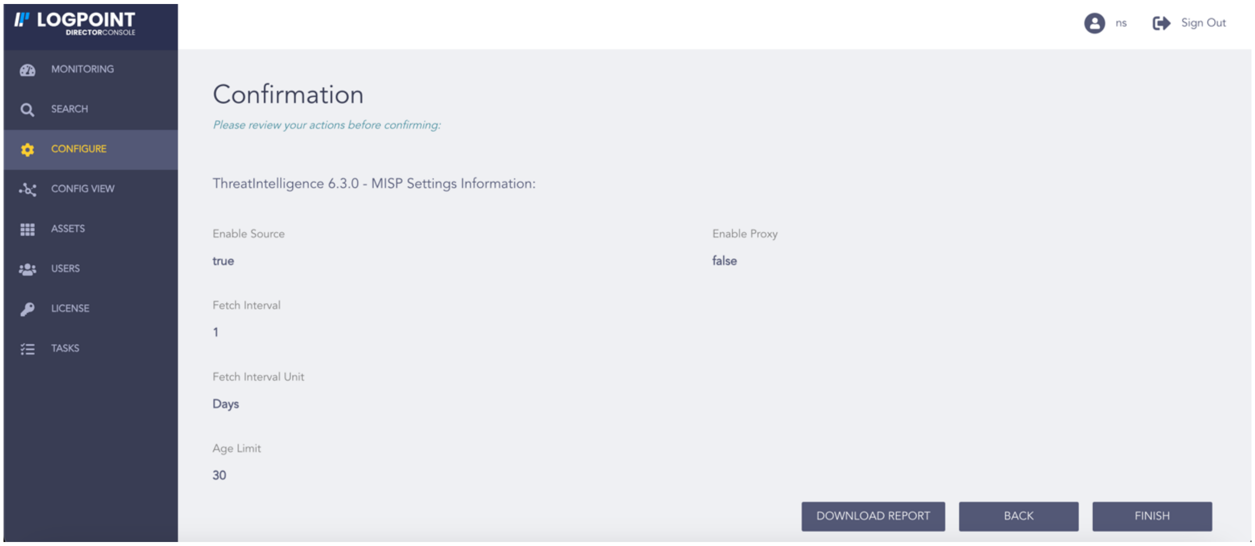
● Http ○ Https

Fig. 19: Enabling Proxy Server

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

Note: Click **Download Report** to get a summary as a PDF.

16. Click **FINISH**. Click **OK** to confirm.



Confirmation

Please review your actions before confirming:

ThreatIntelligence 6.3.0 - MISP Settings Information:

Enable Source	Enable Proxy
true	false

Fetch Interval

1

Fetch Interval Unit

Days

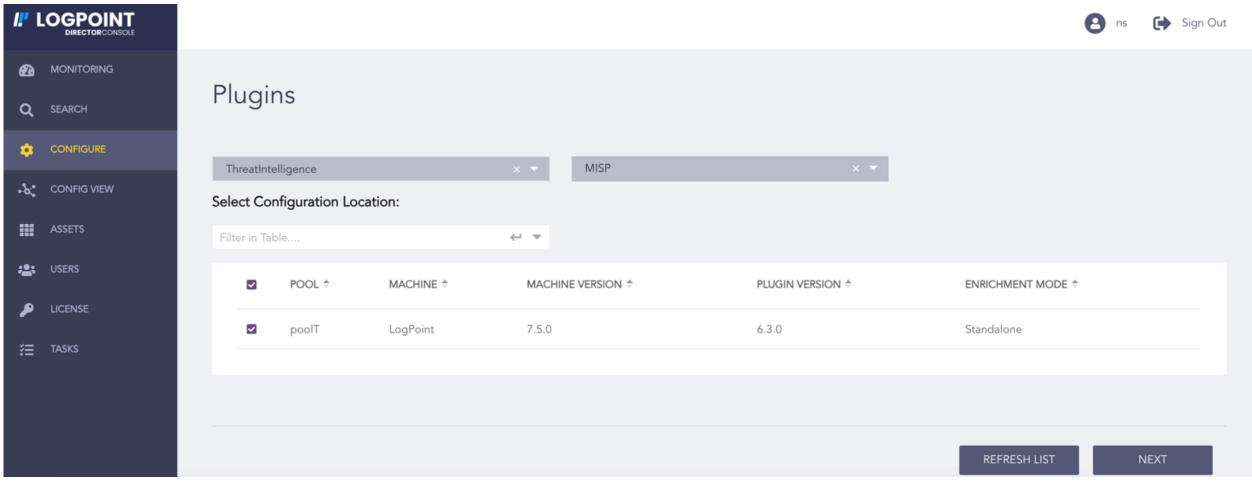
Age Limit

30

Fig. 20: Confirming the Changes

4.5.2 Configuring MISP

1. Click **Configure** in the navigation bar.
2. Under *Settings*, click **Plugins**.
3. Select **ThreatIntelligence** from the **Select Plugin Type** drop-down.
4. Select the Logpoint to configure MISP. You can select multiple Logpoints of different pools.
5. Select **MISP** from the **Select Plugin Sub-type** drop-down.
6. Click **NEXT**.



Plugins

ThreatIntelligence

MISP

Select Configuration Location:

☑	POOL	MACHINE	MACHINE VERSION	PLUGIN VERSION	ENRICHMENT MODE
☑	poolT	LogPoint	7.5.0	6.3.0	Standalone

Fig. 21: Selecting MISP

7. Select **API** to use an API key to fetch *MISP* feeds or select **Free Feed** to fetch free *MISP* feeds.

   Threat Intelligence configures the Botvrij.eu free MISP feed by default. However, it is only configured if Threat Intelligence is freshly installed or if MISP is not configured while upgrading Threat Intelligence.

8. If **API** is selected:

   8.1. Enter the *MISP* **Base URL** and the **API Key**.

   8.2. Enter the *MISP* source parameters in a JSON format in **Filter Parameter** to filter incoming logs. Go to the MISP documentation for the list of parameters.

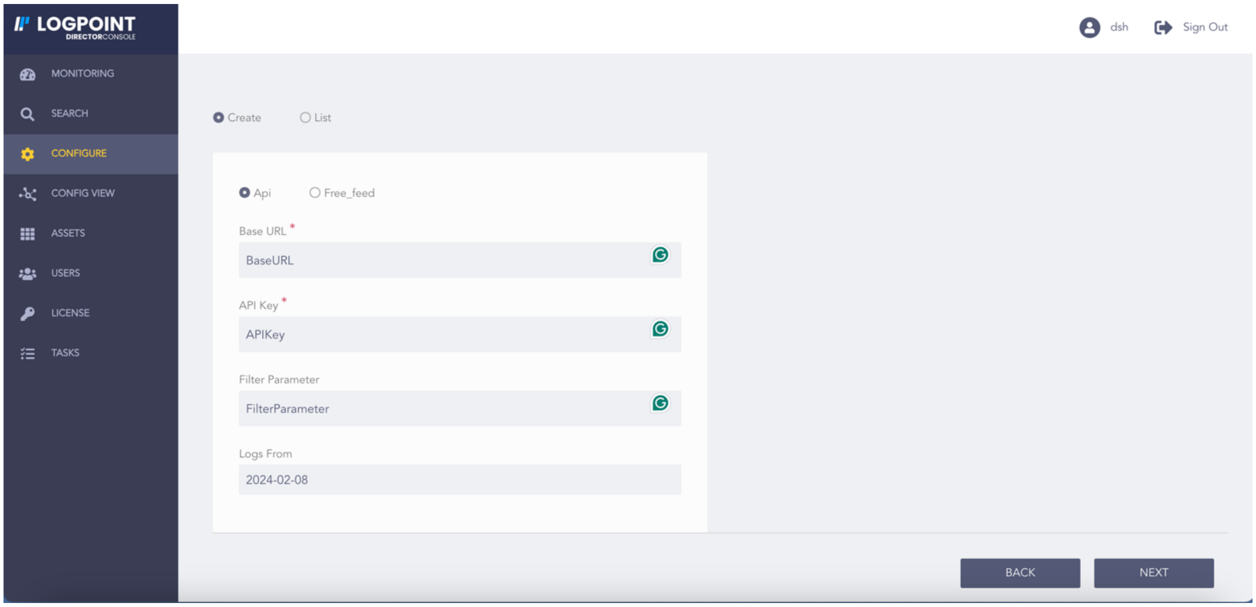
   8.3. Select a date from when Threat Intelligence is to fetch logs in **Logs From**.

   8.4. Select **Verify** to ensure a secure connection.

   8.5. Select **Upload Certificate File** to use a self-signed SSL certificate.

   8.6. Browse for the location of the self-signed SSL certificate and click **Open**.

   8.7. Click **Upload**.



● Create ○ List

● Api ○ Free_feed

Base URL *
BaseURL

API Key *
APIKey

Filter Parameter
FilterParameter

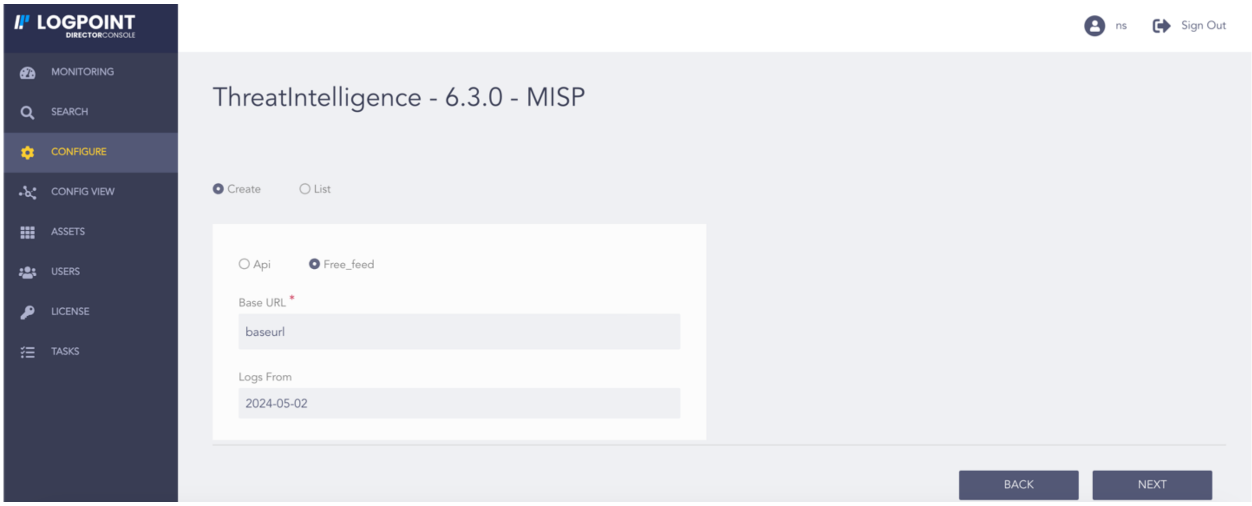
Logs From
2024-02-08

Fig. 22: Selecting API

9. If **Free Feed** is selected:

   9.1. Enter the *MISP* **Base URL**.

   9.2. Select a date from when Threat Intelligence is to fetch logs in **Logs From**.



ThreatIntelligence - 6.3.0 - MISP

● Create ○ List

○ Api ● Free_feed

Base URL *

baseurl

Logs From

2024-05-02

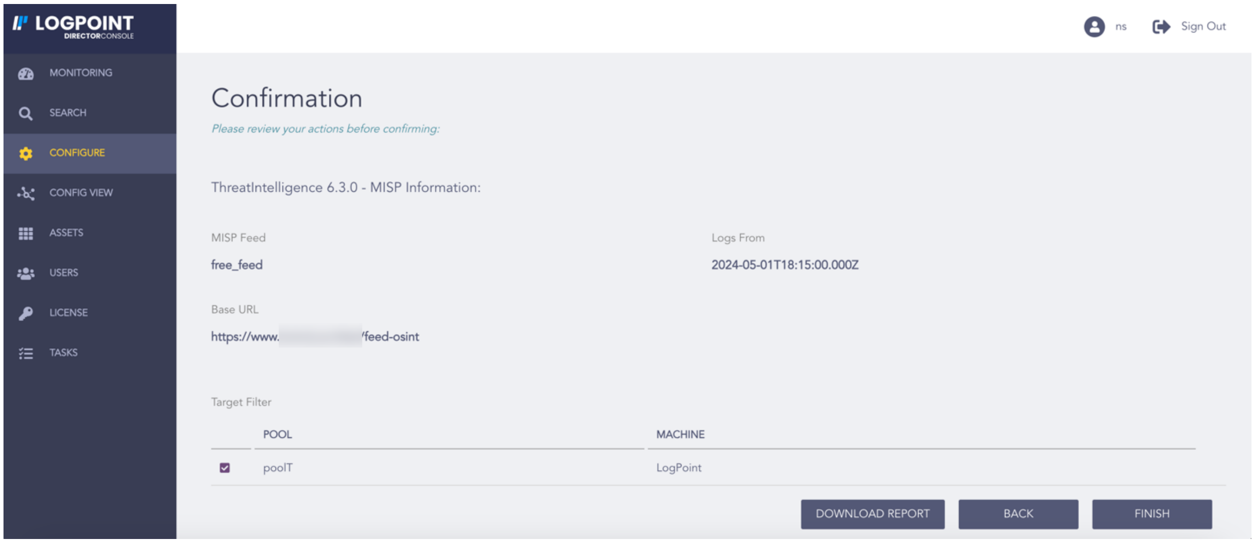
Fig. 23: Selecting Free Feed

You can find the lists all the MISP configurations in **List**.

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

Note: Click **Download Report** to get a summary as a PDF.

12. Click **FINISH**. Click **OK** to confirm.



Confirmation

Please review your actions before confirming:

ThreatIntelligence 6.3.0 - MISP Information:

MISP Feed

free_feed

Logs From

2024-05-01T18:15:00.000Z

Base URL

https://www.[redacted]/feed-osint

Target Filter

	POOL	MACHINE
☑	poolT	LogPoint

Fig. 24: Confirming the Changes

4.6 Custom CSV

Custom CSV enables you to upload a custom CSV file as a TI source. The CSV file must have the following headers:

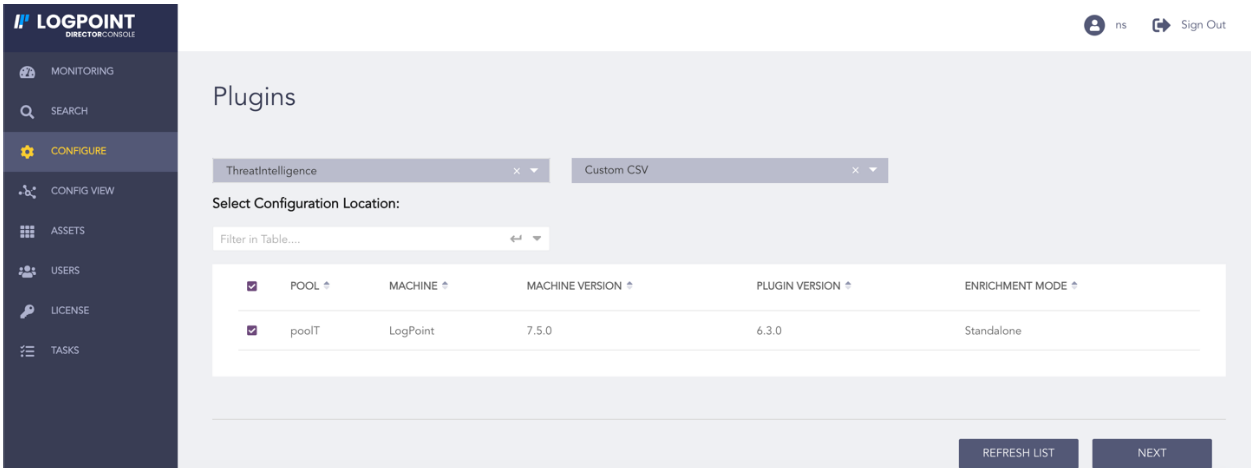
```
domain, category, score, first_seen, last_seen, ports, ip, url, type, file_hash
```

Note:

- The field **ports** is optional. You can specify multiple ports by separating it with space.
- The **first_seen** and **last_seen** data fields must have the *yyyy-mm-dd* format.
- Threat Intelligence ignores fields and their values if the CSV is not in the above format.

To configure the Custom CSV:

1. Click **Configure** in the navigation bar.
2. Under *Settings*, click **Plugins**.
3. Select **ThreatIntelligence** from the **Select Plugin Type** drop-down.
4. Select the Logpoint to configure Custom CSV. You can select multiple Logpoints of different pools.
5. Select **Custom CSV** from the **Select Plugin Sub-type** drop-down.
6. Click **NEXT**.



Plugins

ThreatIntelligence

Custom CSV

Select Configuration Location:

Filter in Table....

☑	POOL	MACHINE	MACHINE VERSION	PLUGIN VERSION	ENRICHMENT MODE
☑	poolT	LogPoint	7.5.0	6.3.0	Standalone

Fig. 25: Selecting Custom CSV

7. Select **Enable Source** to activate custom CSV.

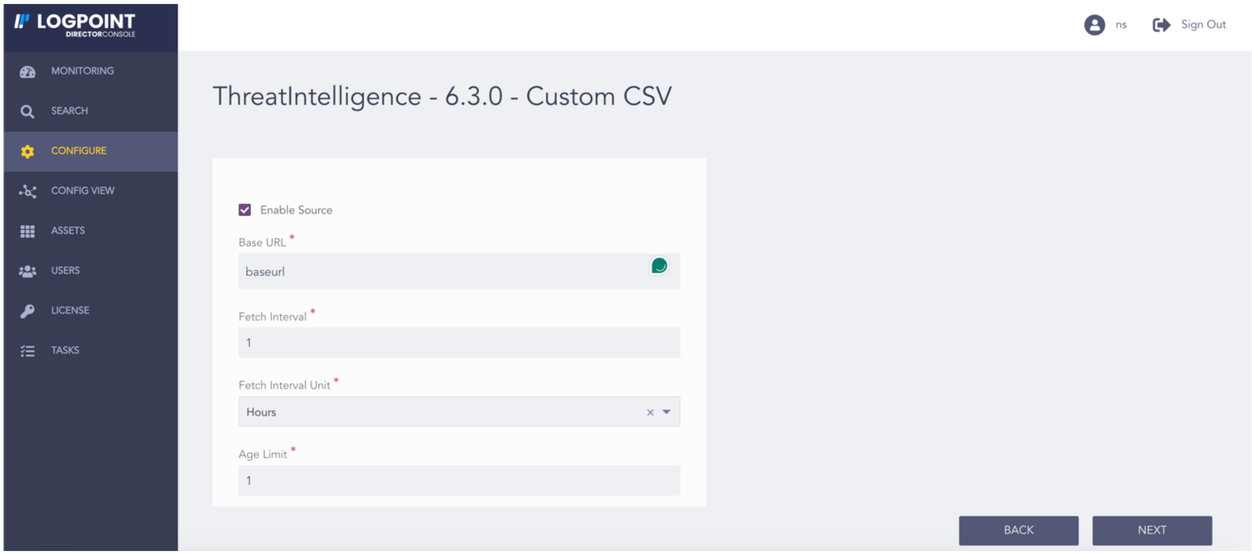
8. Enter the **Base URL**. It must link to the **custom CSV** file.

9. Enter the frequency at which data is retrieved in **Fetch Interval**.

10. Select the **Fetch Interval Unit** in hours or days.

11. Enter the **Age Limit**, which is the retention period of the fetched data in days or hours. Enter it as *0* to retain the last fetched data until the next successful fetch.

12. Select the **Age Limit Unit** in hours or days.



ThreatIntelligence - 6.3.0 - Custom CSV

☑ Enable Source

Base URL *

baseurl

Fetch Interval *

1

Fetch Interval Unit *

Hours

Age Limit *

1

Fig. 26: Enabling Custom CSV

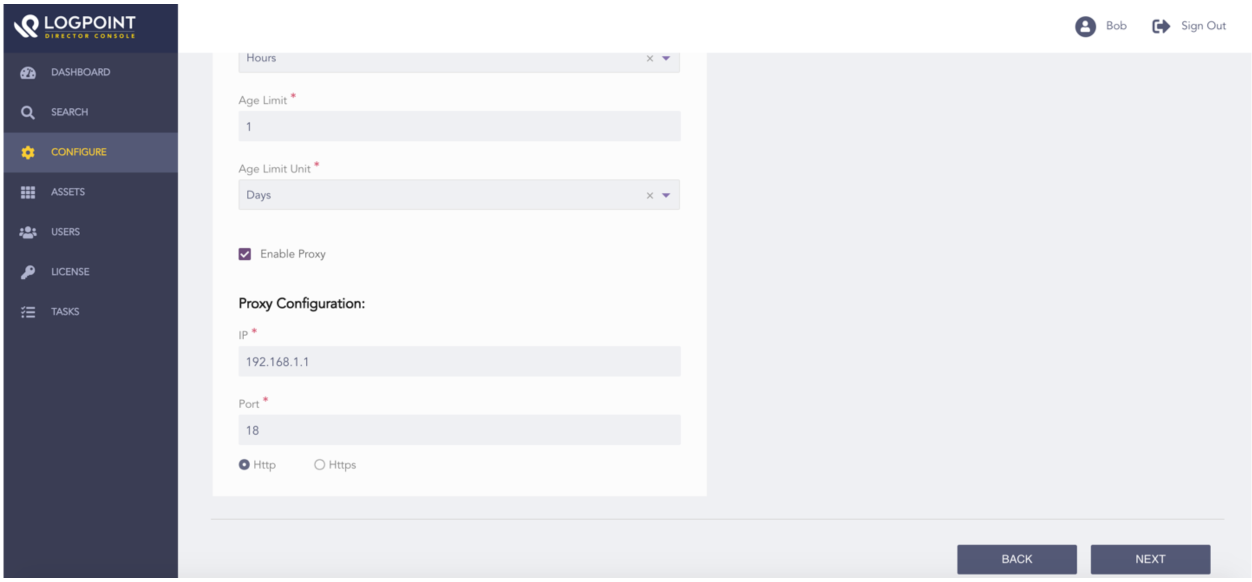
13. Select **Enable Proxy** to use a proxy server.

14. In **Proxy Configuration**:

    14.1. Enter the proxy server **IP** Address and **Port number**.

    14.2. Select either **Http** or **Https** protocol.

15. Click **NEXT**.



Hours

Age Limit *
1

Age Limit Unit *
Days

☑ Enable Proxy

Proxy Configuration:

IP *
192.168.1.1

Port *
18

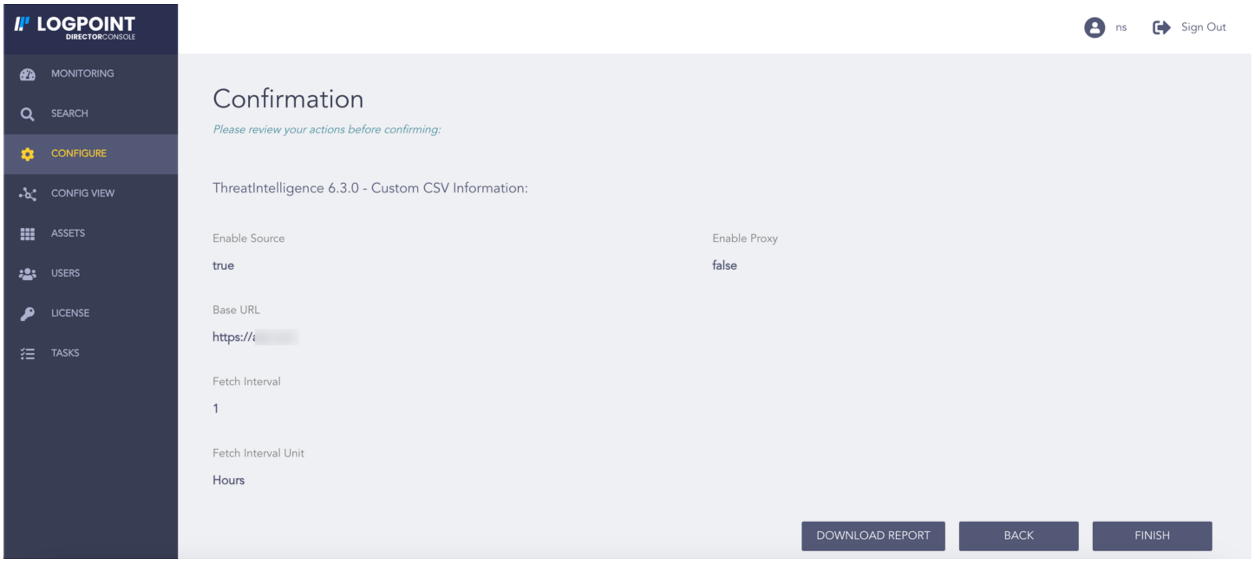
● Http ○ Https

Fig. 27: Enabling Proxy Server

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

Note: Click **Download Report** to get a summary as a PDF.

17. Click **FINISH**. Click **OK** to confirm.



Confirmation

Please review your actions before confirming:

ThreatIntelligence 6.3.0 - Custom CSV Information:

Enable Source
true

Enable Proxy
false

Base URL
https://[redacted]

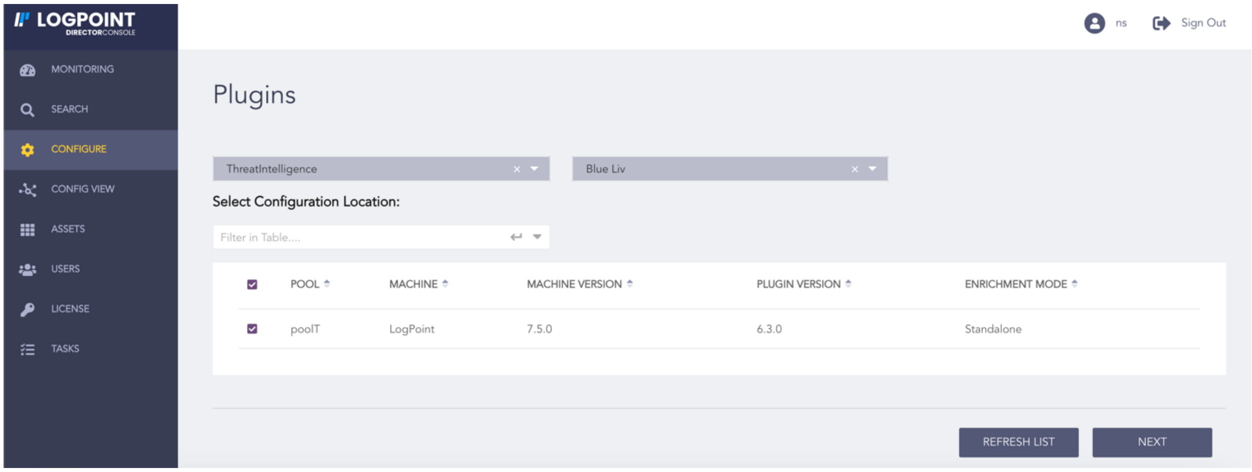
Fetch Interval
1

Fetch Interval Unit
Hours

Fig. 28: Confirming the Changes

4.7 Blueliv

1. Click **Configure** in the navigation bar.
2. Under *Settings*, click **Plugins**.
3. Select **ThreatIntelligence** from the **Select Plugin Type** drop-down.
4. Select the Logpoint to configure Blueliv. You can select multiple Logpoints of different pools.
5. Select **Blue Liv** from the **Select Plugin Sub-type** drop-down.
6. Click **NEXT**.



Plugins

ThreatIntelligence

Blue Liv

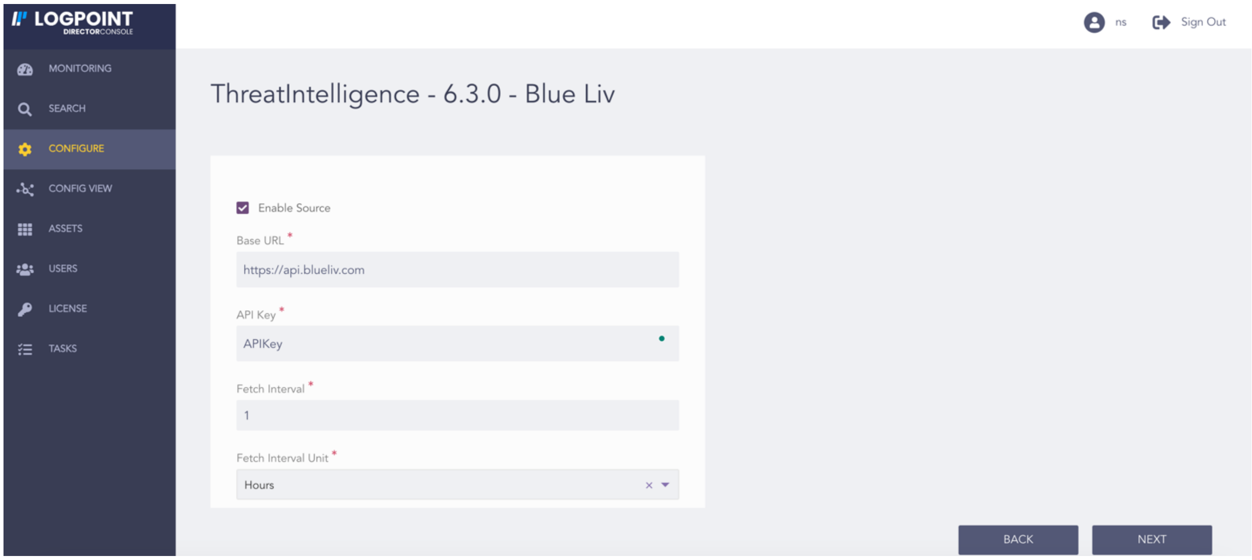
Select Configuration Location:

Filter in Table....

☑	POOL	MACHINE	MACHINE VERSION	PLUGIN VERSION	ENRICHMENT MODE
☑	poolT	LogPoint	7.5.0	6.3.0	Standalone

Fig. 29: Selecting Blue Liv

7. Select **Enable Source** to activate Blue Liv.
8. Enter the *Blueliv* **Base URL** and **API Key**.
9. Enter the frequency at which data is retrieved in **Fetch Interval**.
10. Select the **Fetch Interval Unit** in hours or days.
11. Enter the **Age Limit**, which is the retention period of the fetched data in days or hours. Enter it as *0* to retain the last fetched data until the next successful fetch.
12. Select the **Age Limit Unit** in hours or days.



ThreatIntelligence - 6.3.0 - Blue Liv

☑ Enable Source

Base URL *
https://api.blueliv.com

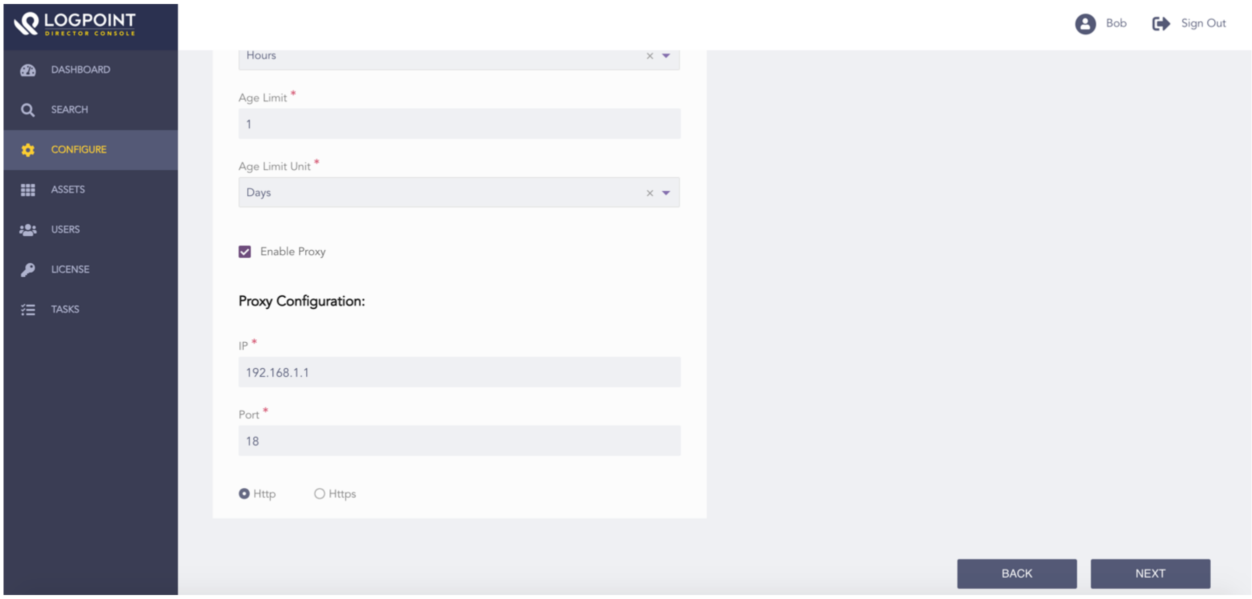
API Key *
APIKey

Fetch Interval *
1

Fetch Interval Unit *
Hours

Fig. 30: Enabling Blue Liv

13. Select **Enable Proxy** to use a proxy server.
14. In **Proxy Configuration**:
    - 14.1. Enter the proxy server **IP** Address and **Port number**.
    - 14.2. Select either **Http** or **Https** protocol.
15. Click **NEXT**.



Hours

Age Limit *
1

Age Limit Unit *
Days

☑ Enable Proxy

Proxy Configuration:

IP *
192.168.1.1

Port *
18

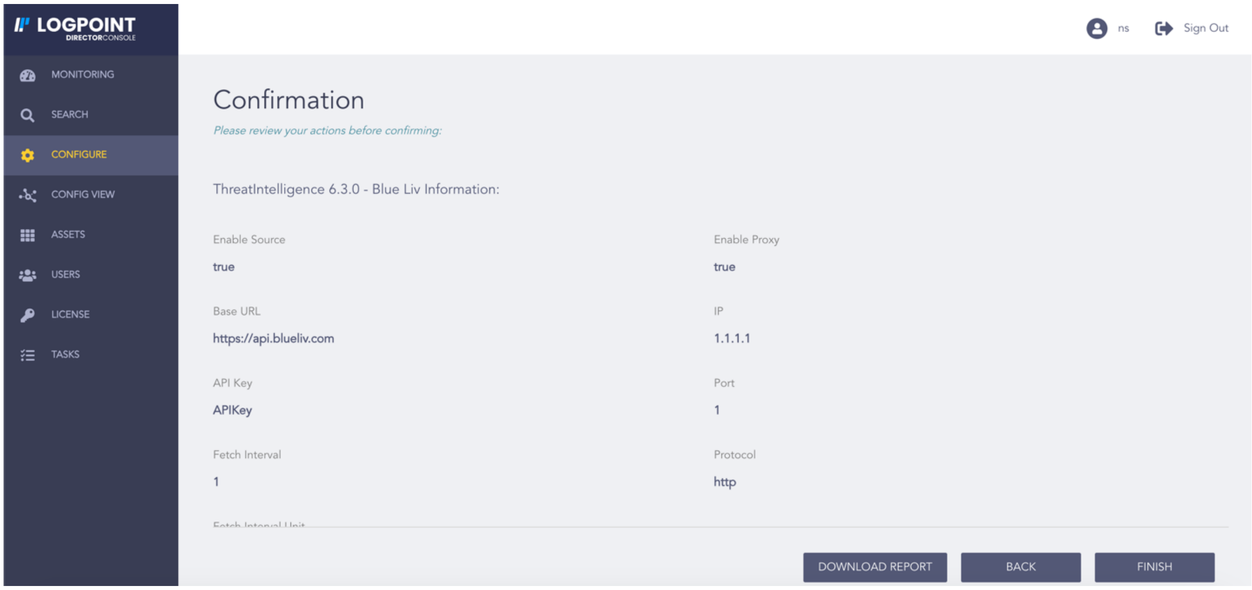
● Http ○ Https

Fig. 31: Enabling Proxy Server

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

Note: Click **Download Report** to get a summary as a PDF.

17. Click **FINISH**. Click **OK** to confirm.



Confirmation

Please review your actions before confirming:

ThreatIntelligence 6.3.0 - Blue Liv Information:

Enable Source
true

Enable Proxy
true

Base URL
https://api.blueliv.com

IP
1.1.1.1

API Key
APIKey

Port
1

Fetch Interval
1

Protocol
http

Fetch Interval Unit

Fig. 32: Confirming the Changes

4.8 Mapping

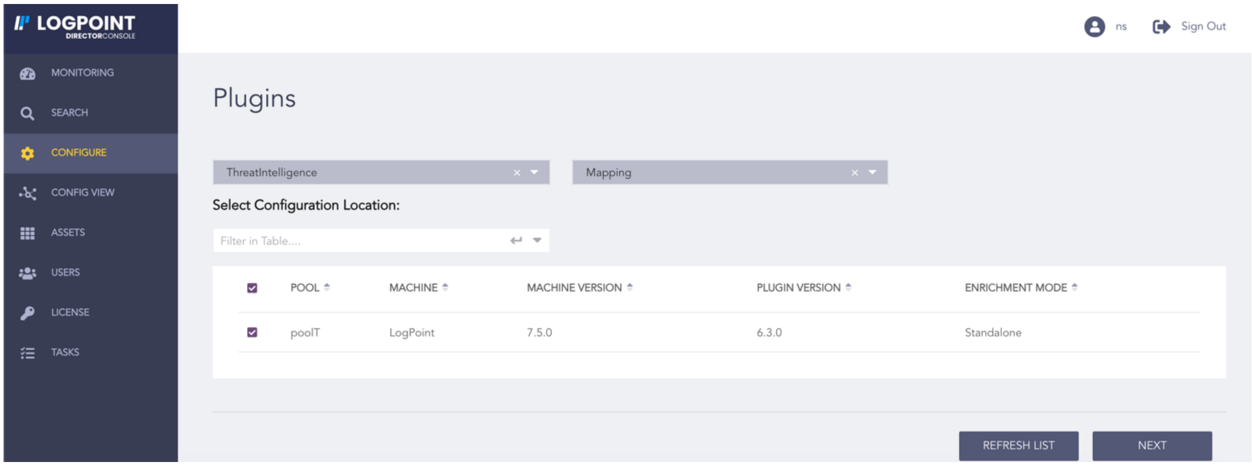
Mapping enables you to standardize logs by assigning the fields of fetched logs to the fields of the *Logpoint Threat Intelligence Taxonomy*. Threat Intelligence initially validates if you have mapped the field of a search query. If you have not mapped the field, Threat Intelligence searches the column with the same field name and enriches the logs.

The following fields are mapped by default:

- source_address to ip_address
- destination_address to ip_address

To map:

1. Click **Configure** in the navigation bar.
2. Under *Settings*, click **Plugins**.
3. Select **ThreatIntelligence** from the **Select Plugin Type** drop-down.
4. Select the Logpoint to configure Mapping. You can select multiple Logpoints of different pools.
5. Select **Mapping** from the **Select Plugin Sub-type** drop-down.
6. Click **NEXT**.



Plugins

ThreatIntelligence

Mapping

Select Configuration Location:

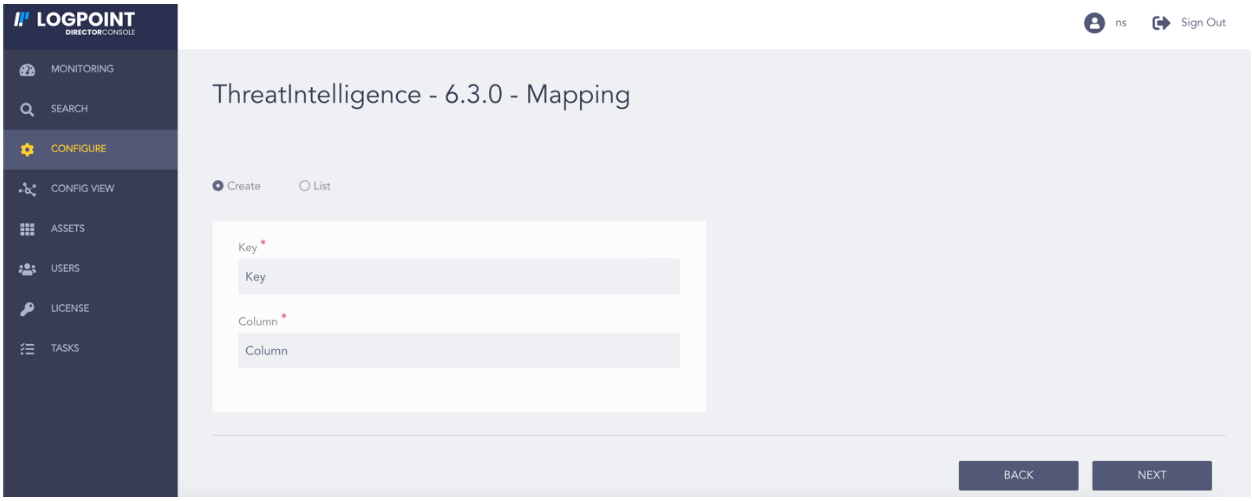
☑	POOL	MACHINE	MACHINE VERSION	PLUGIN VERSION	ENRICHMENT MODE
☑	poolT	LogPoint	7.5.0	6.3.0	Standalone

Fig. 33: Selecting Mapping

7. In **Create**:
   7.1. Enter the **Key** from the incoming log to map.
   7.2. Enter the **Column** name from the Logpoint taxonomy to map the key.

You can find all the mapping configurations in **List**.

8. Click **NEXT**.



ThreatIntelligence - 6.3.0 - Mapping

● Create ○ List

Key *

Key

Column *

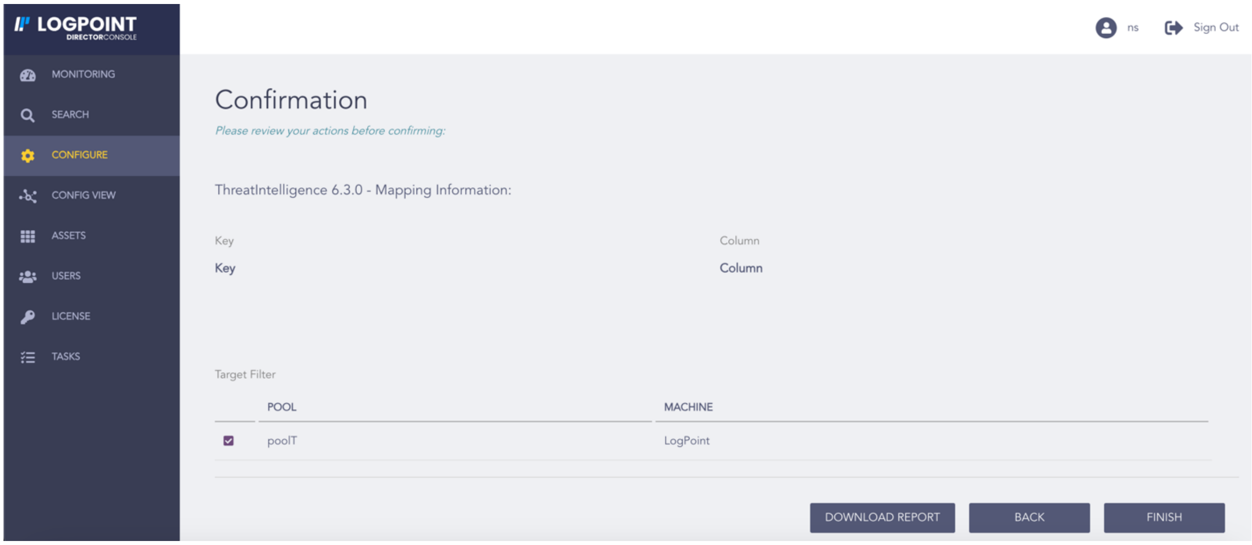
Column

Fig. 34: Mapping

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

Note: Click **Download Report** to get a summary as a PDF.

10. Click **FINISH**. Click **OK** to confirm.



Confirmation

Please review your actions before confirming:

ThreatIntelligence 6.3.0 - Mapping Information:

Key: Key

Column: Column

Target Filter

	POOL	MACHINE
☑	poolT	LogPoint

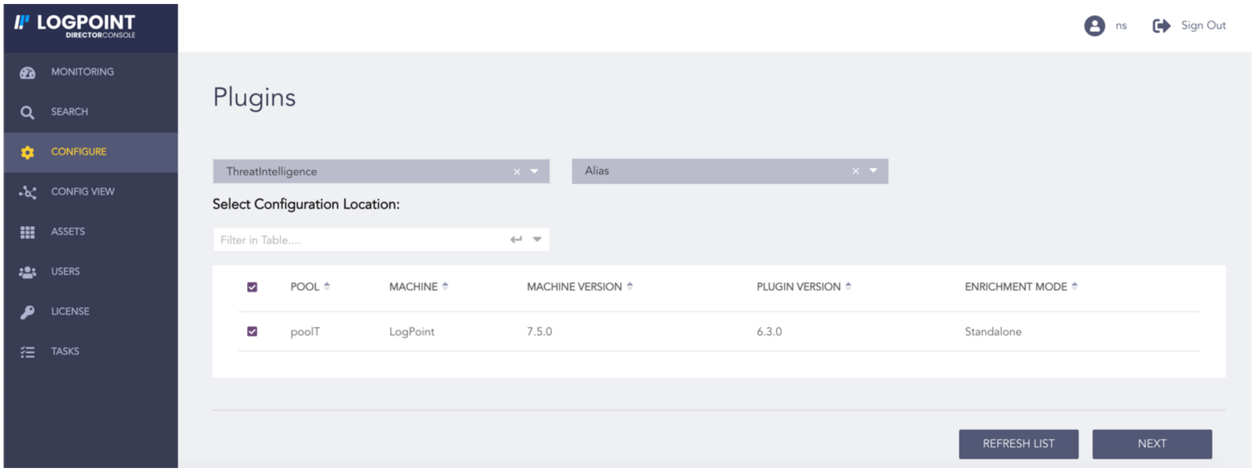
Fig. 35: Confirming the Changes

4.9 Alias

Alias enables you to assign a pseudoname to one or multiple field names of the incoming log.

To assign an alias:

1. Click **Configure** in the navigation bar.
2. Under *Settings*, click **Plugins**.
3. Select **ThreatIntelligence** from the **Select Plugin Type** drop-down.
4. Select the Logpoint to configure Alias. You can select multiple Logpoints of different pools.
5. Select **Alias** from the **Select Plugin Sub-type** drop-down.
6. Click **NEXT**.



Plugins

ThreatIntelligence

Alias

Select Configuration Location:

☑	POOL	MACHINE	MACHINE VERSION	PLUGIN VERSION	ENRICHMENT MODE
☑	poolT	LogPoint	7.5.0	6.3.0	Standalone

Fig. 36: Selecting Alias

7. In **Create**:

   7.1 Enter the **Alias** name.

   7.2 Enter the name of one or more **Fields** to which the alias needs to refer.

8. Select a mode of display:

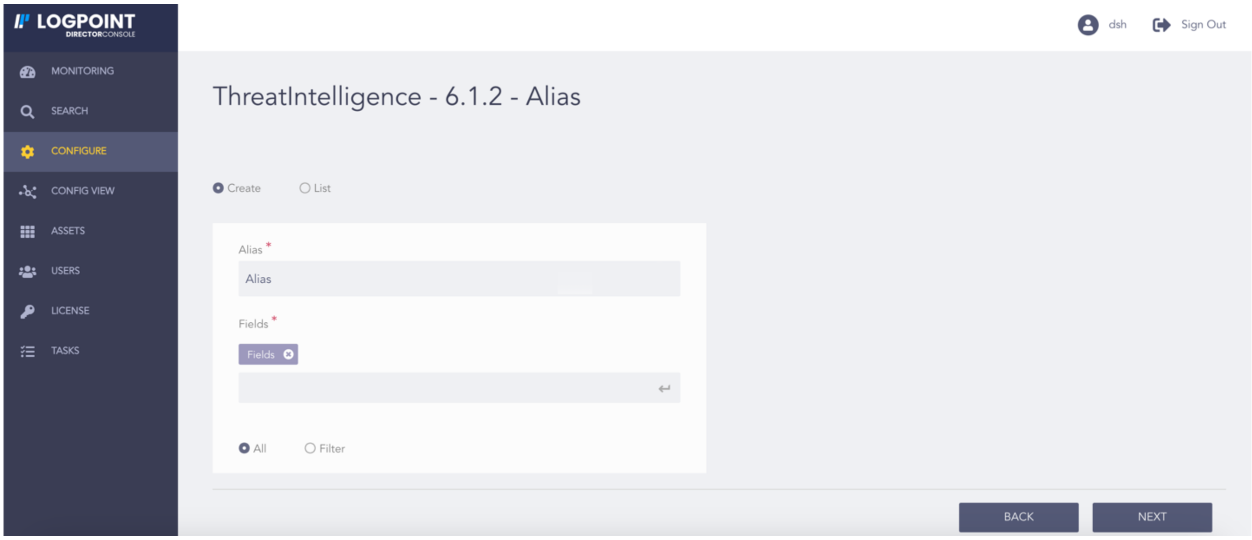
   8.1. Select **All** to display both the matched and the unmatched logs. However, only the matched logs are enriched.

   8.2. Select **Filter** to display only the matched logs.

You can find all the alias configurations in **List**.

9. Click **NEXT**.

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



ThreatIntelligence - 6.1.2 - Alias

● Create ○ List

Alias *: Alias

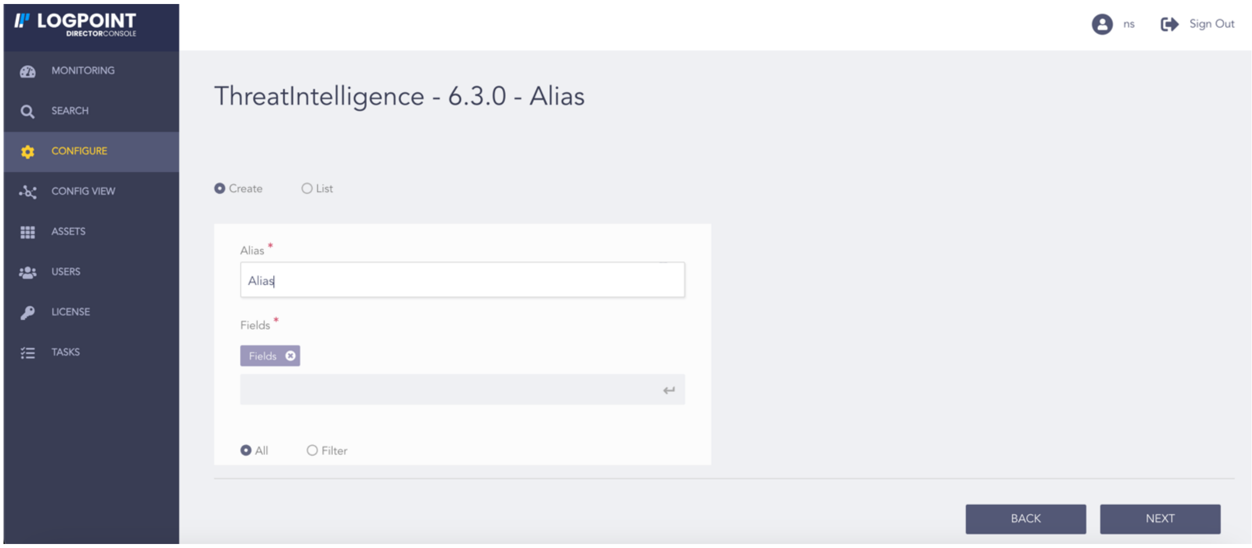
Fields *: Fields

● All ○ Filter

Fig. 37: Configuring Alias

Note: Click **Download Report** to get a summary as a PDF.

11. Click **FINISH**. Click **OK** to confirm.



ThreatIntelligence - 6.3.0 - Alias

● Create ○ List

Alias *: Alias

Fields *: Fields

● All ○ Filter

Fig. 38: Confirming the Changes

CHAPTER

FIVE

APPENDIX

5.1 Logpoint Threat Intelligence Taxonomy

The Logpoint Threat Intelligence taxonomy specifies the following fields:

*accessed_ts, application, authentication, caller_user, computer, created_ts,
destination_address, destination_port, directory, disabled, domain, email,
end_ts, file, fqdn, gateway, group_name, hardware_address, hash, hash_type,
host, ip_address, locked_out, login_ts, loggoff_ts, logon_type, modified_ts, port,
priority, process, protocol, proxy_server, referer, request_method,
rights, security_id, server_address, service, source_address, source_port,
start_ts, status, status_code, url, user, user_agent*

Among these field names, only *domain, url, category, type, threat_source, file_hash, ip_address, score, port, _eviction_timestamp, start_ts, and end_ts* are functional in Threat Intelligence.