

Integrations

Threat Intelligence For Director Console UI

V6.4.0

CONTENTS

1	Threat Intelligence	1
2	Installing Threat Intelligence	2
3	Uninstalling Threat Intelligence	5
4	Configuring Threat Intelligence	7
4.1	General Settings	7
4.2	Emerging Threats	8
4.3	Critical Stack	11
4.4	CSIS	15
4.5	MISP	18
4.6	Custom CSV	24
4.7	Blueliv	27
4.8	Mapping	30
4.9	Alias	32
5	Editing Threat Intelligence	35
6	Appendix	37
6.1	Logpoint Threat Intelligence Taxonomy	37

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

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**.

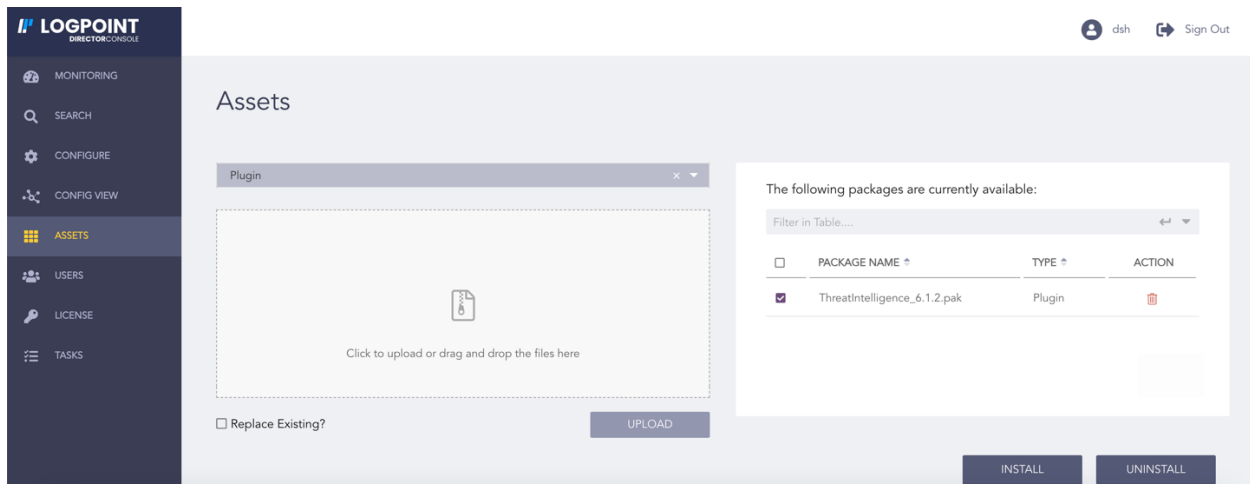


Fig. 1: Selecting a Package

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

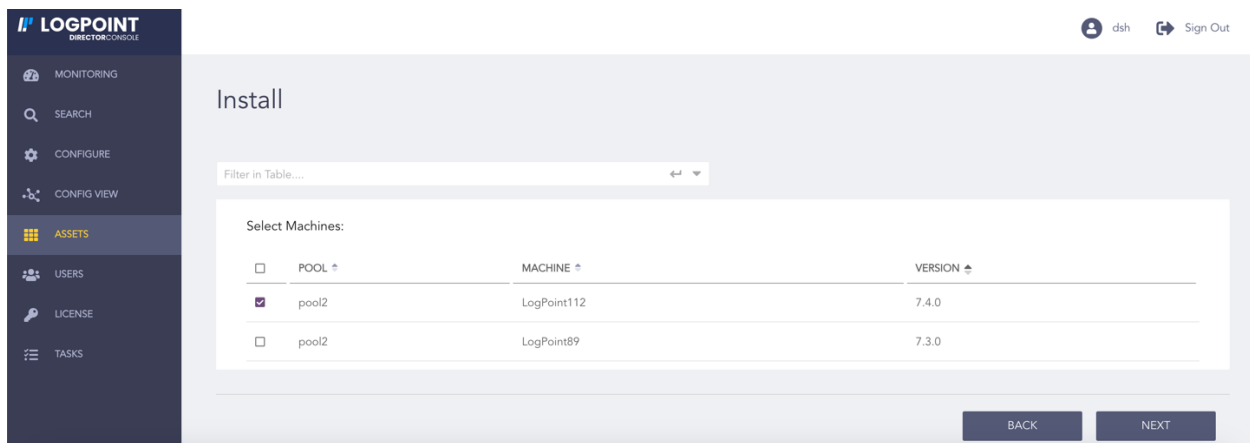


Fig. 2: Selecting Logpoint

10. Review your changes. You can go **BACK** to make any changes if necessary.
11. Click **INSTALL** and click **OK** to confirm.

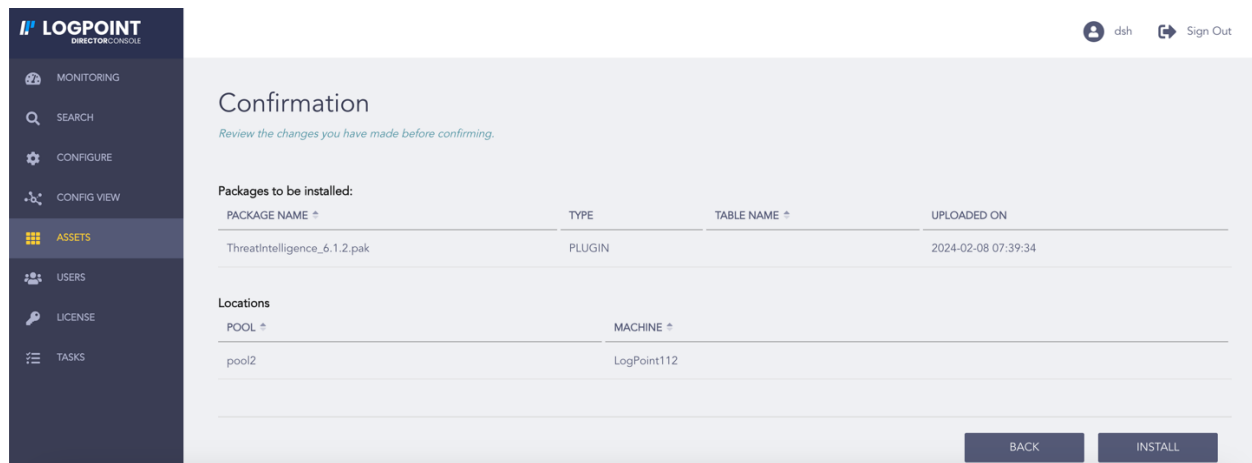


Fig. 3: Confirming the Changes

UNINSTALLING 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**.

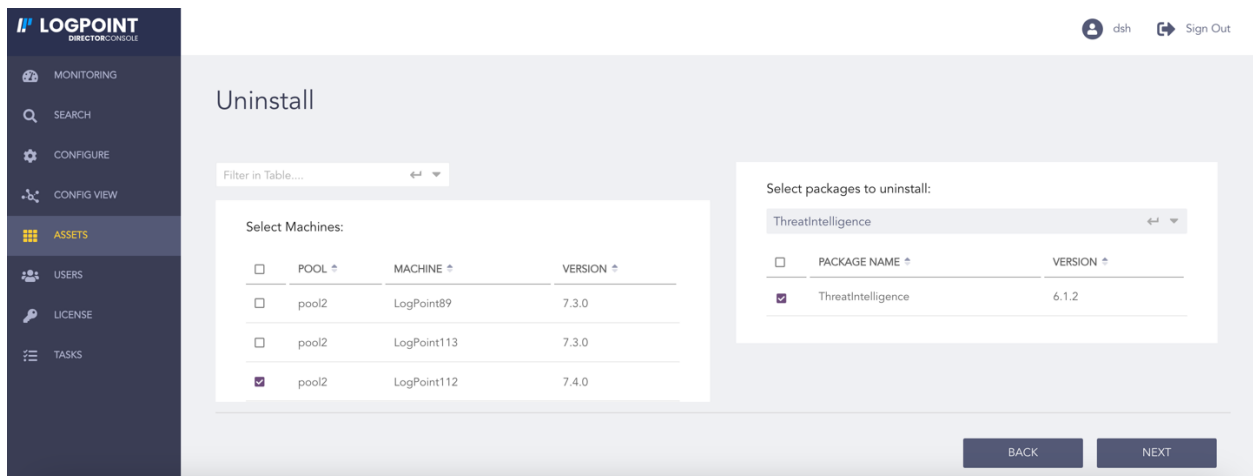


Fig. 1: Selecting Threat Intelligence

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

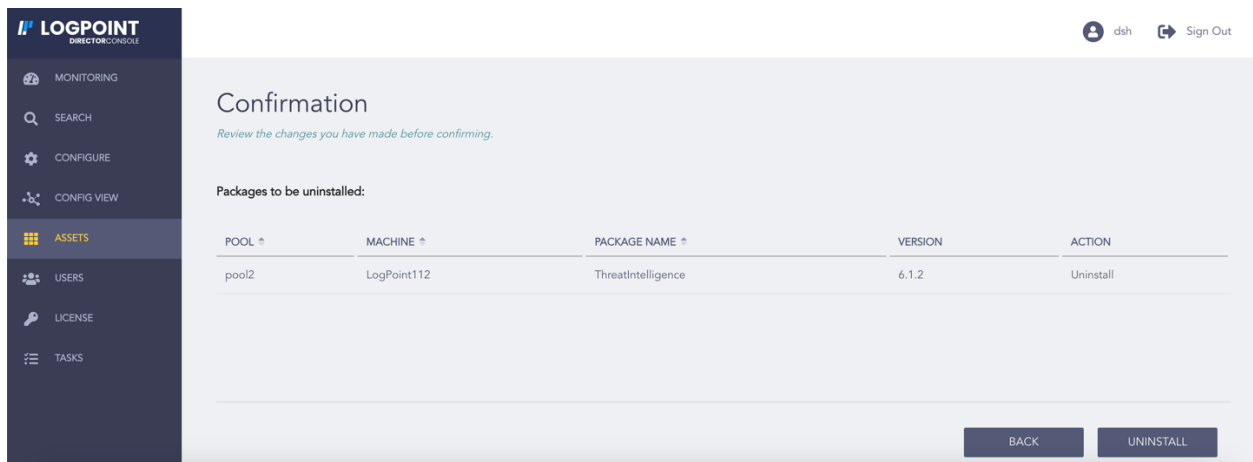


Fig. 2: Confirming the Changes

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**.

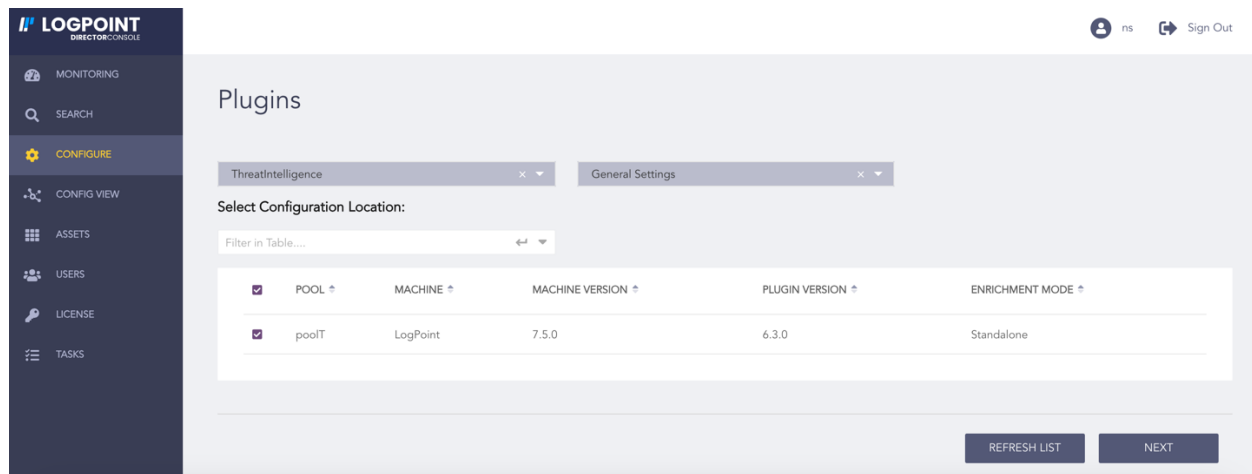


Fig. 1: Selecting General Settings

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**.

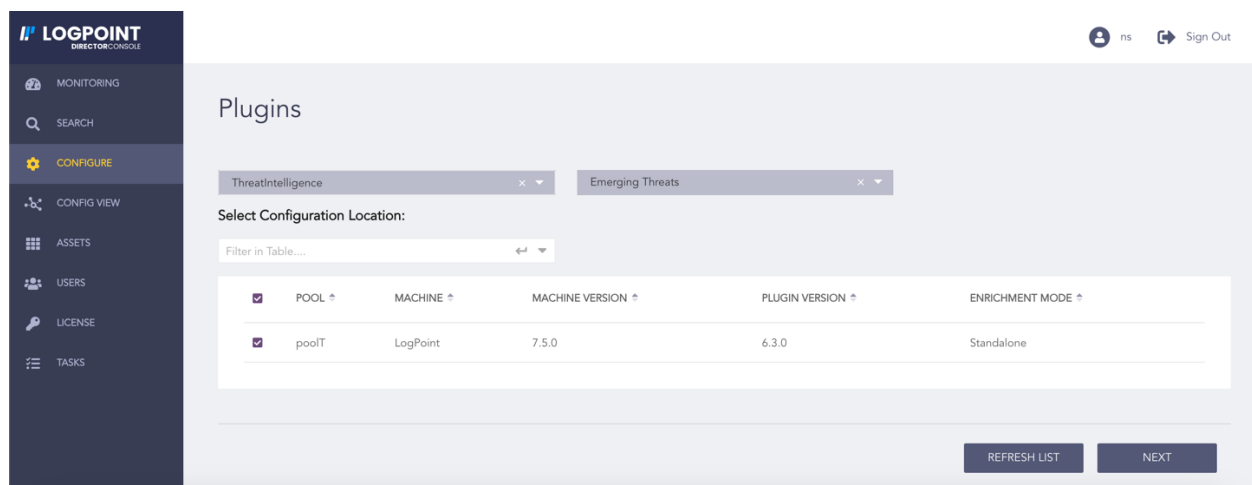


Fig. 2: Selecting Emerging Threats

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.

The screenshot shows the Logpoint Director Console UI. On the left is a dark sidebar with the Logpoint logo and navigation links: DASHBOARD, SEARCH, CONFIGURE (highlighted), ASSETS, USERS, LICENSE, and TASKS. The main area is light gray. At the top right, it says 'Bob' with a user icon and 'Sign Out' with a logout icon. The central form is titled 'Enable Source' with a checked checkbox. It contains the following fields: 'Base URL' with the value 'https://rules.emergingthreatspro.com', 'API Key' (empty), 'Fetch Interval' with the value '1', 'Fetch Interval Unit' with a dropdown menu showing 'Hours', 'Age Limit' with the value '1', and 'Age Limit Unit' with a dropdown menu showing 'Days'. At the bottom right of the form, there are two buttons: 'BACK' and 'NEXT'. A red arrow points down to the 'NEXT' button.

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**.

The screenshot shows the 'Configure' page in the Logpoint Director Console. The left sidebar contains navigation links: DASHBOARD, SEARCH, CONFIGURE (highlighted), ASSETS, USERS, LICENSE, and TASKS. The main content area is titled 'Hours' and contains the following fields:

- Age Limit: 1
- Age Limit Unit: Days
- Enable Proxy: ☒
- Proxy Configuration:
 - IP: 192.168.1.1
 - Port: 18
 - Protocol: ☒ Http, ☐ Https

At the bottom right, there are 'BACK' and 'NEXT' buttons. A red arrow points to the 'NEXT' button.

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**.

The screenshot shows the 'Confirmation' page in the Logpoint Director Console. The left sidebar contains navigation links: MONITORING, SEARCH, CONFIGURE (highlighted), CONFIG VIEW, ASSETS, USERS, LICENSE, and TASKS. The main content area is titled 'Confirmation' and contains the following information:

Please review your actions before confirming:

ThreatIntelligence 6.3.0 - Emerging Threats Information:

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

At the bottom right, there are 'DOWNLOAD REPORT', 'BACK', and 'FINISH' buttons.

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**.

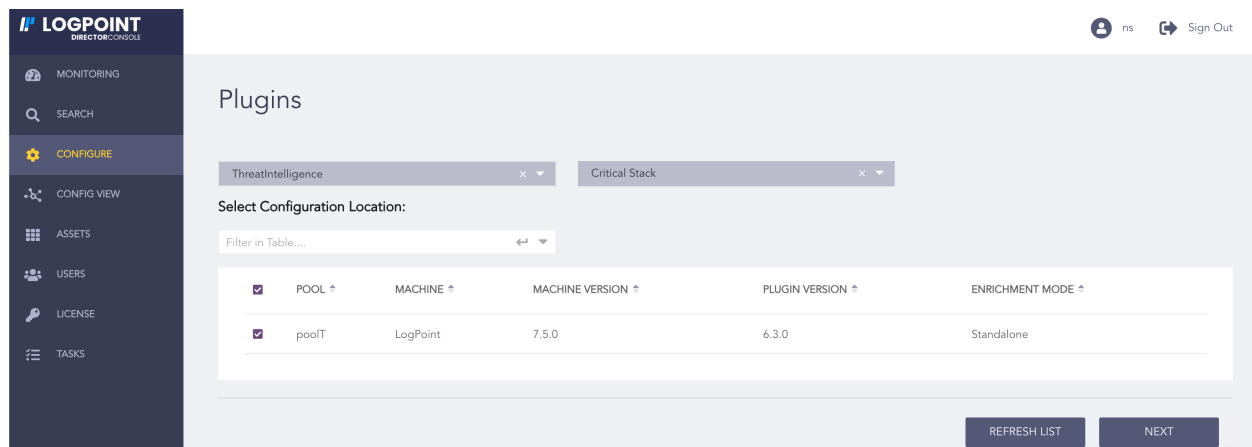


Fig. 6: Selecting Critical Stack

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**.

The screenshot shows the LogPoint Director Console interface. On the left is a dark navigation bar with the 'LOGPOINT DIRECTOR CONSOLE' logo and menu items: MONITORING, SEARCH, CONFIGURE (highlighted), CONFIG VIEW, ASSETS, USERS, LICENSE, and TASKS. The main content area is titled 'ThreatIntelligence - 6.3.0 - Critical Stack'. It features a 'Create' button and a 'List' button. Below these is a form with two input fields: 'API Name' (containing 'APIName') and 'API Key' (containing 'APIKey'). At the bottom right of the form area are 'BACK' and 'NEXT' buttons. The top right corner shows a user profile icon labeled 'ns' and a 'Sign Out' button.

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.

The screenshot shows the 'Confirmation' page in the LogPoint Director Console. The left navigation bar is identical to the previous figure. The main content area is titled 'Confirmation' with a sub-header 'Please review your actions before confirming:'. Below this is the text 'ThreatIntelligence 6.3.0 - Critical Stack Information:'. The page displays the configuration details: 'API Name' as 'APIName' and 'API Key' as 'APIKey'. There is a 'Target Filter' section with a table showing a selected 'poolT' under the 'POOL' column and 'LogPoint' under the 'MACHINE' column. At the bottom right are three buttons: 'DOWNLOAD REPORT', 'BACK', and 'FINISH'. The top right corner shows the user profile icon 'ns' and 'Sign Out' button.

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**.

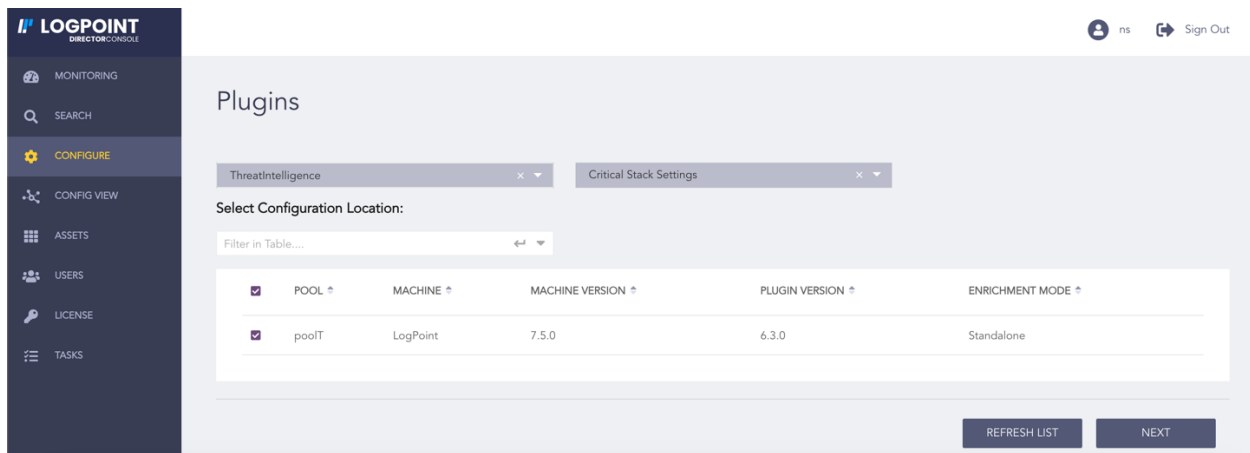


Fig. 9: Selecting Critical Stack Settings

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.

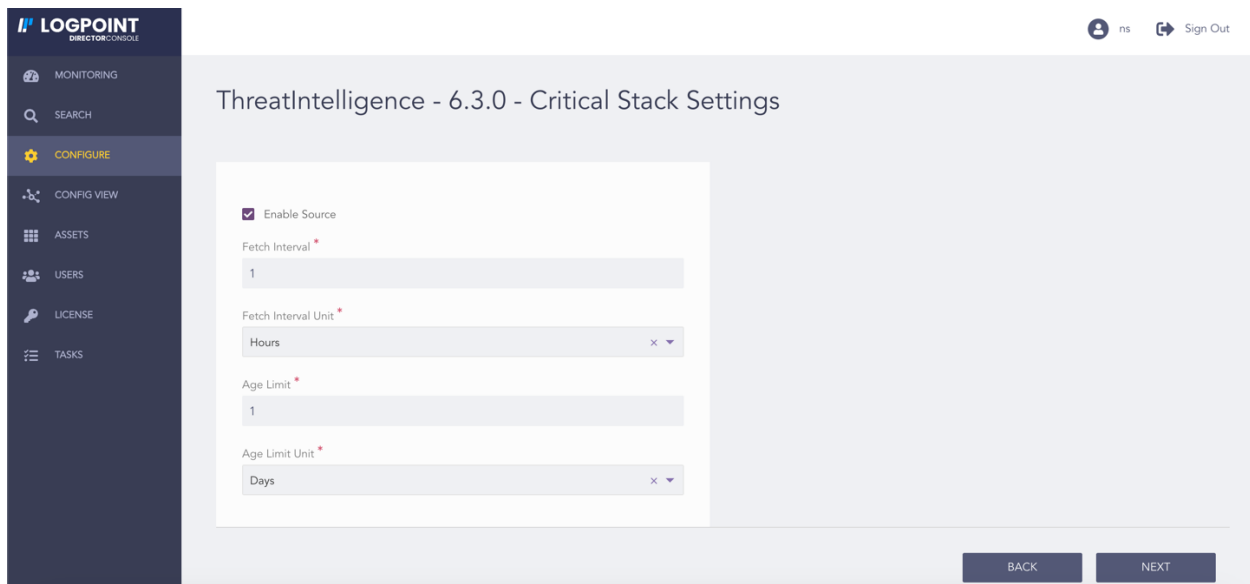


Fig. 10: Enabling Critical Stack

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**.

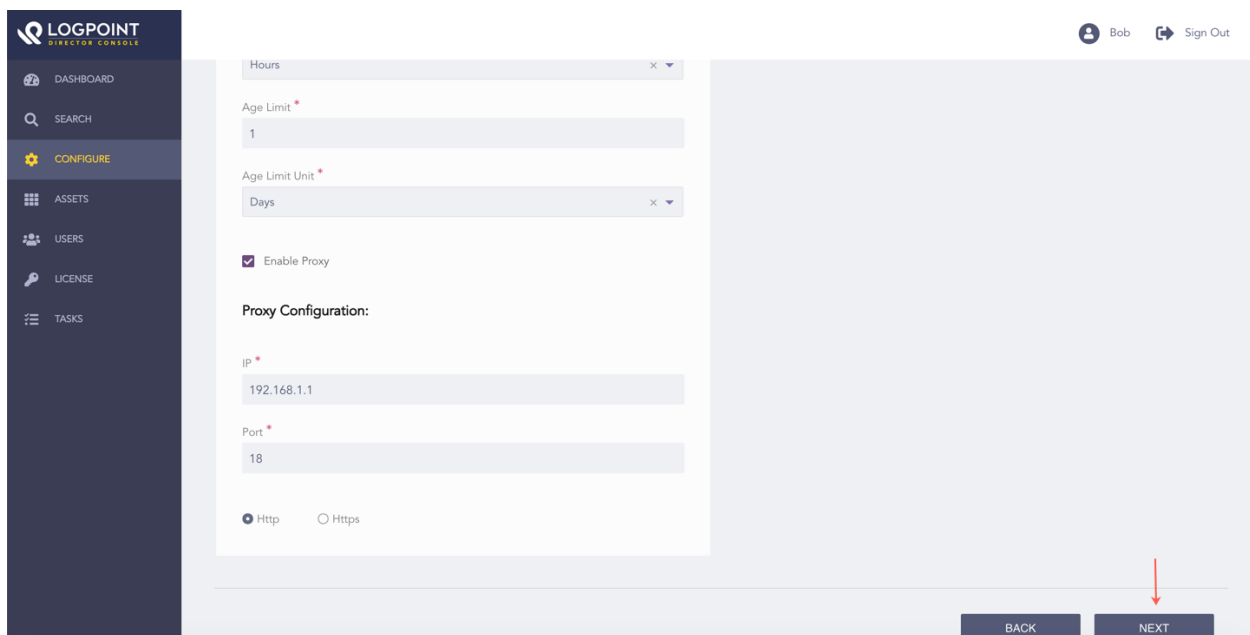


Fig. 11: Enabling Proxy Server

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.

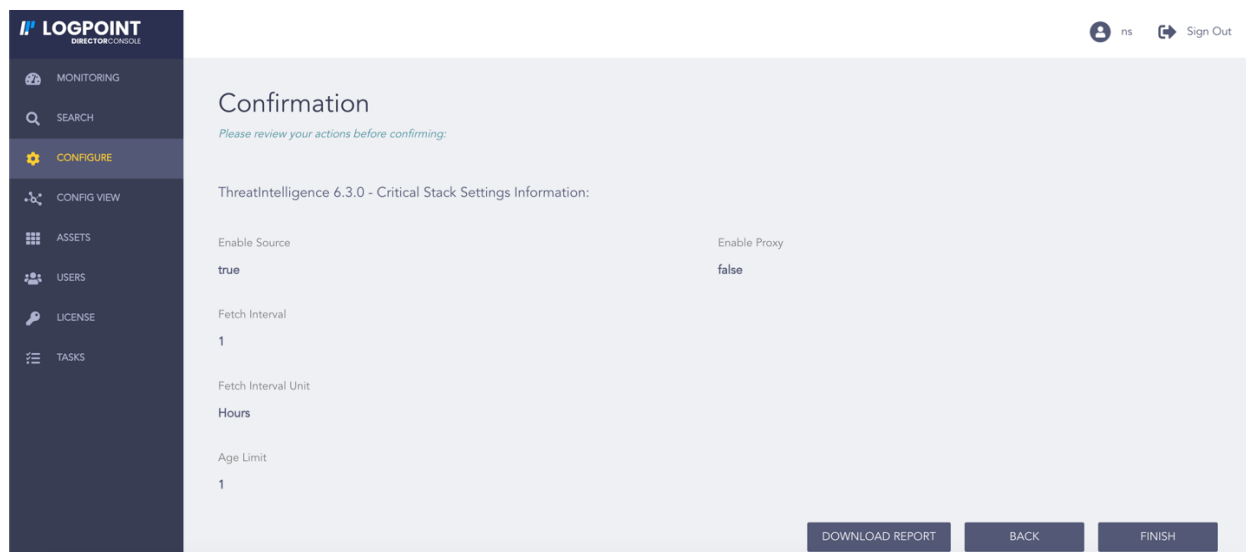


Fig. 12: Confirming the Changes

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**.

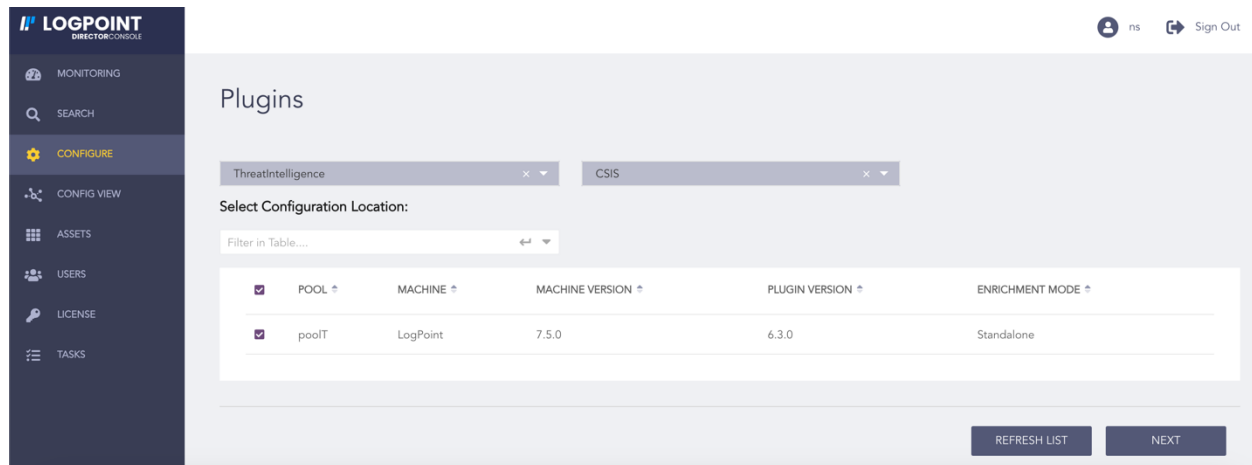


Fig. 13: Selecting CSIS

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.

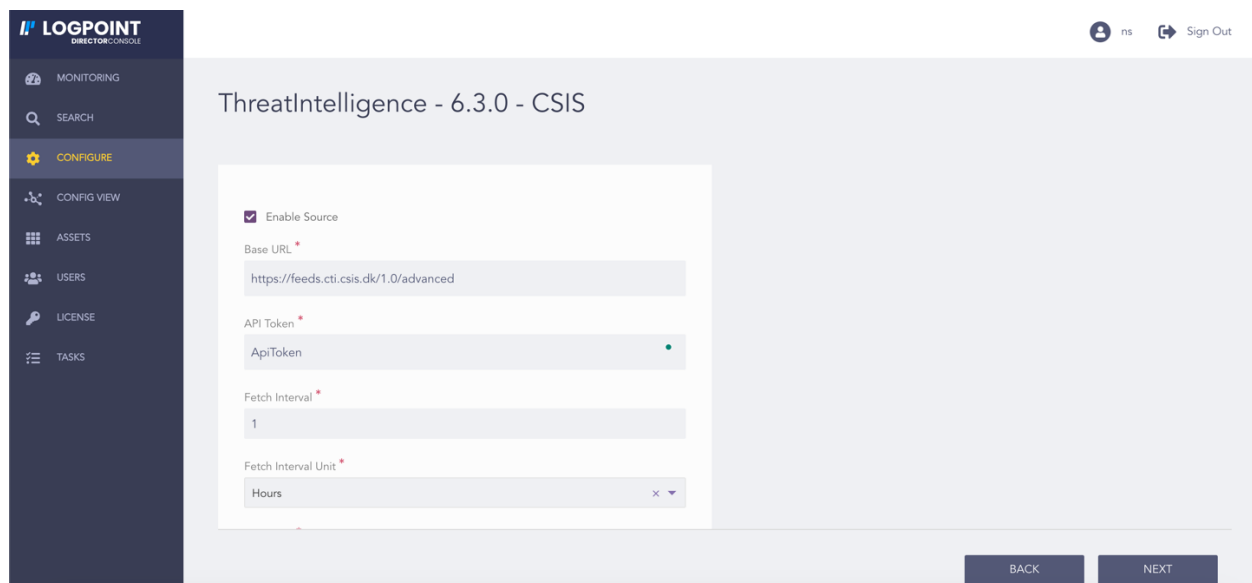
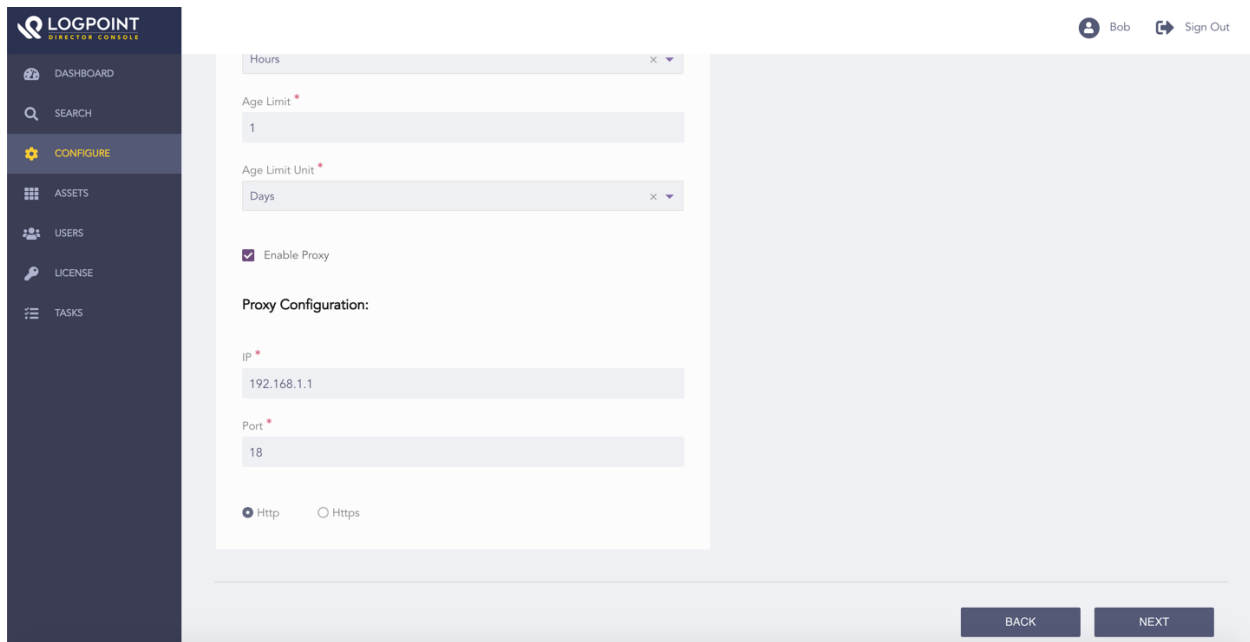


Fig. 14: Enabling CSIS

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**.



The screenshot shows the Logpoint Director Console interface. On the left is a dark sidebar with navigation links: DASHBOARD, SEARCH, CONFIGURE (highlighted), ASSETS, USERS, LICENSE, and TASKS. The main content area is titled 'Hours' and contains several configuration fields: 'Age Limit' with a value of '1', 'Age Limit Unit' set to 'Days', and a checked 'Enable Proxy' checkbox. Below this is the 'Proxy Configuration' section, which includes an 'IP' field with the value '192.168.1.1', a 'Port' field with the value '18', and radio buttons for 'Http' (selected) and 'Https'. At the bottom right of the main area are 'BACK' and 'NEXT' buttons. The top right corner shows a user profile 'Bob' and a 'Sign Out' link.

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.

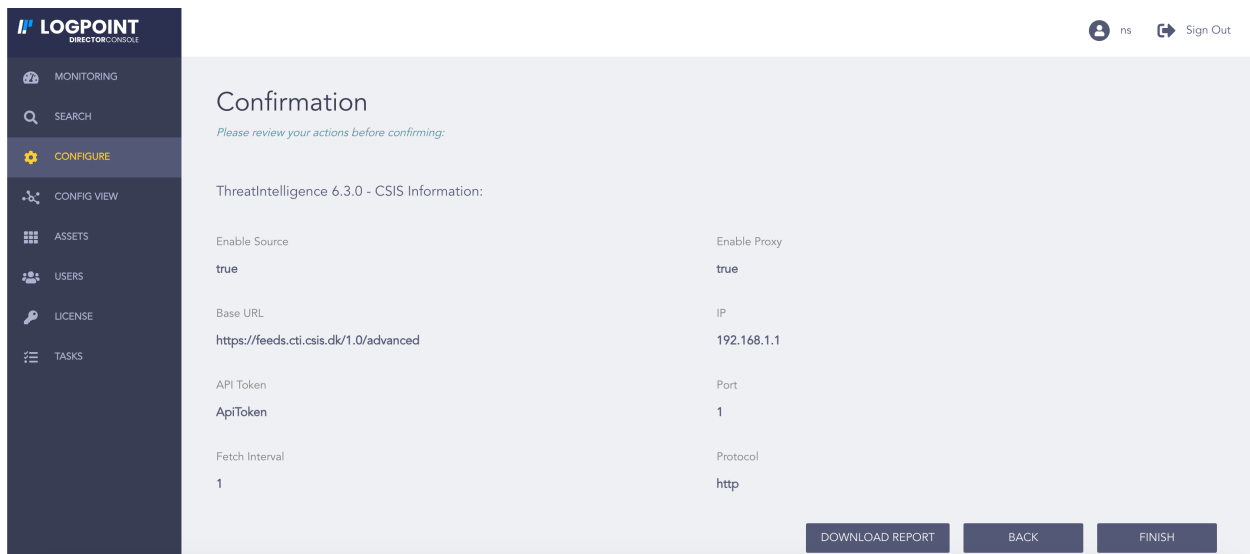


Fig. 16: Confirming the Changes

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**.

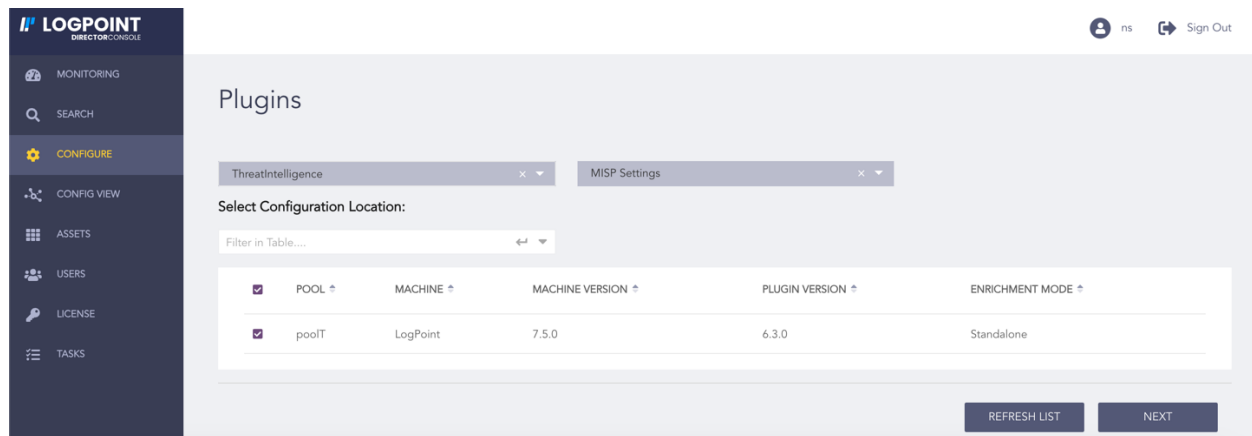


Fig. 17: Selecting MISP Settings

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**.

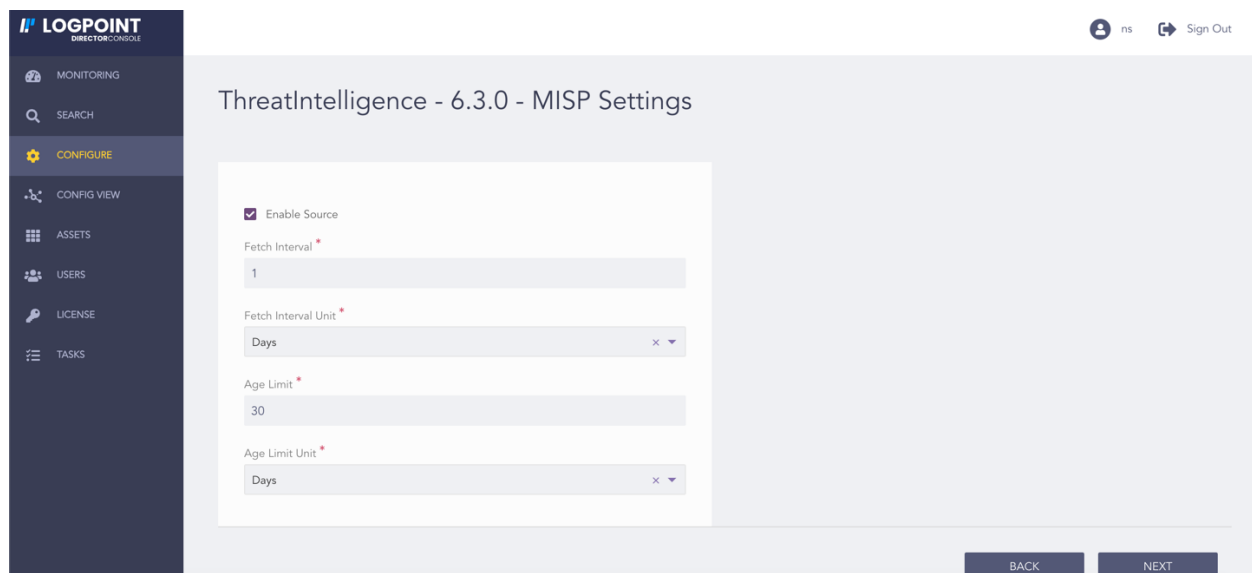


Fig. 18: Enabling MISP

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**.

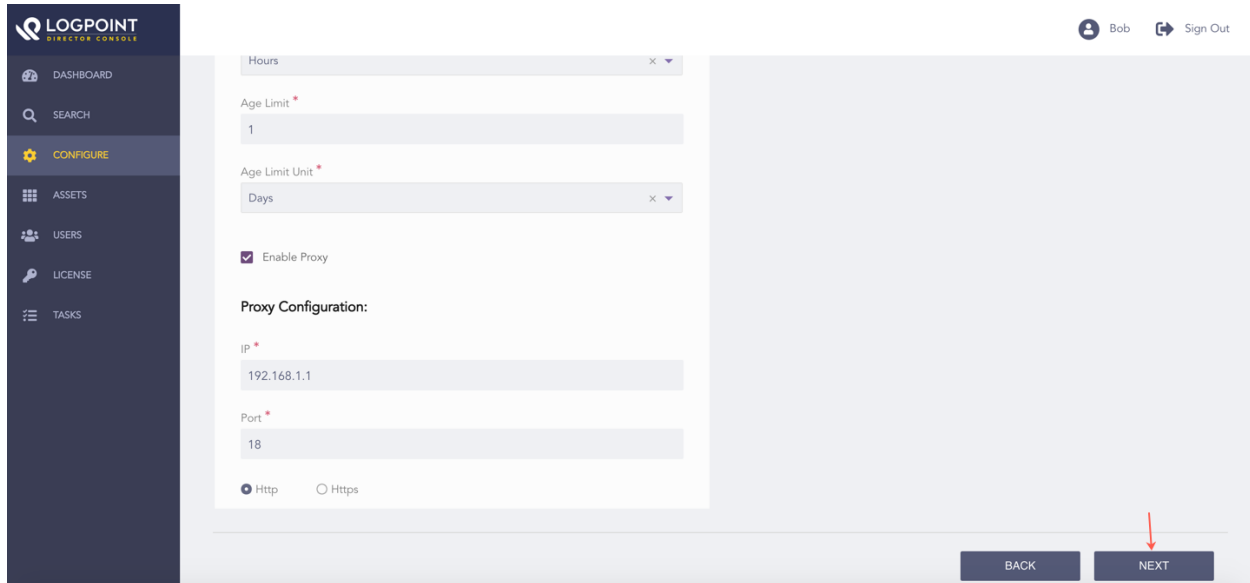
The screenshot shows the Logpoint Director Console interface. On the left is a dark sidebar with navigation links: DASHBOARD, SEARCH, CONFIGURE (highlighted), ASSETS, USERS, LICENSE, and TASKS. The main content area is titled 'Hours' and contains several configuration fields: 'Age Limit' with a value of '1', 'Age Limit Unit' set to 'Days', and a checked 'Enable Proxy' checkbox. Below this is the 'Proxy Configuration' section, which includes an 'IP' field with the value '192.168.1.1', a 'Port' field with the value '18', and radio buttons for 'Http' (selected) and 'Https'. At the bottom right of the main area are two buttons: 'BACK' and 'NEXT'. A red arrow points to the 'NEXT' button. The top right corner shows a user profile 'Bob' and a 'Sign Out' link.

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.

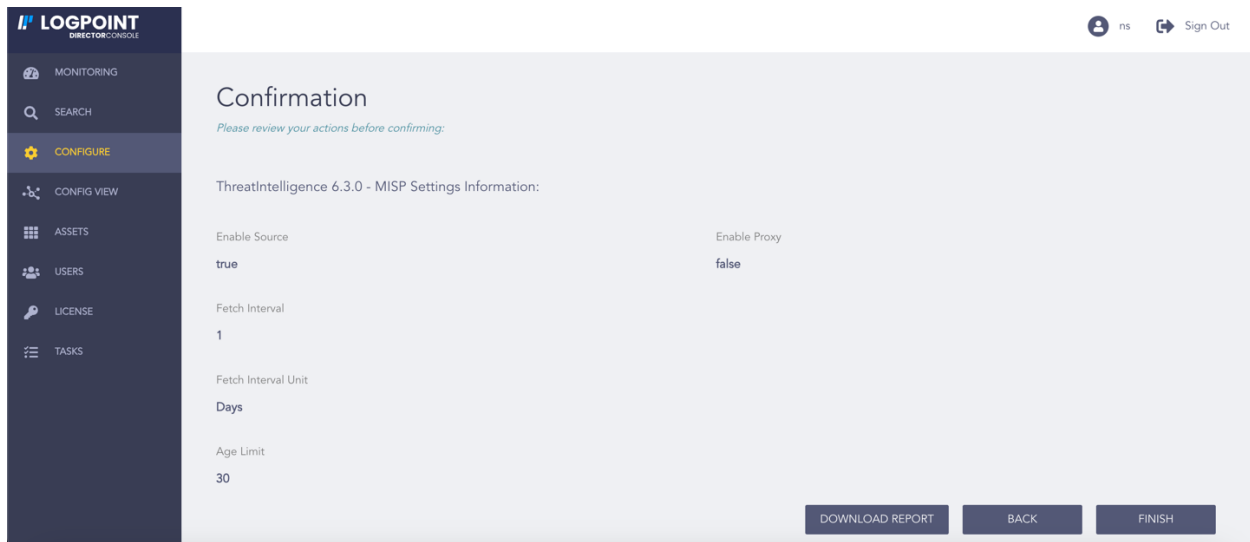


Fig. 20: Confirming the Changes

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**.

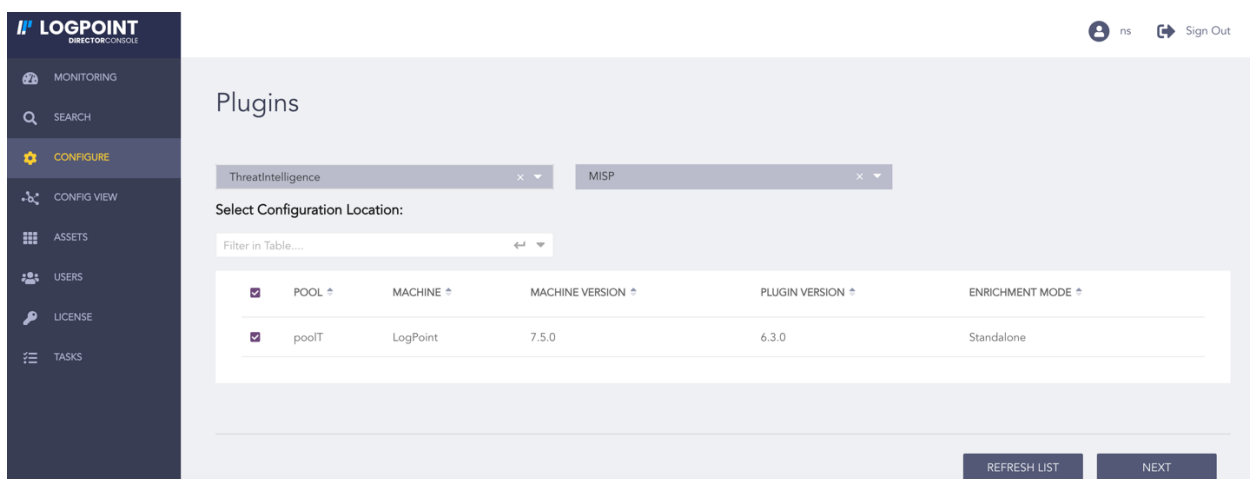


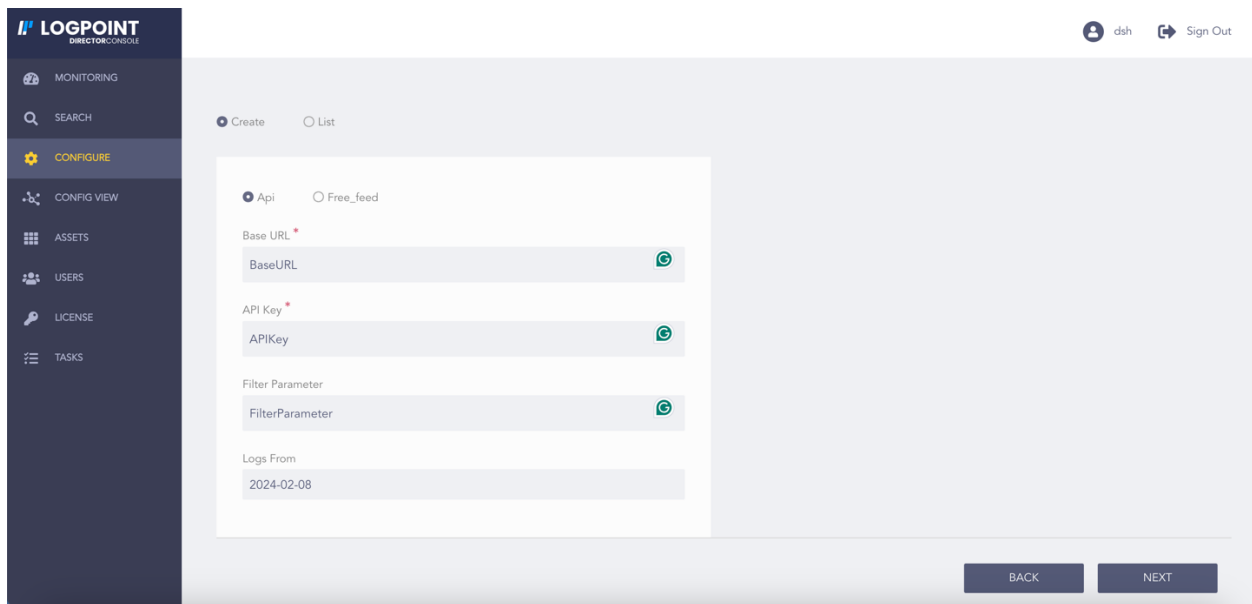
Fig. 21: Selecting MISP

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**.



The screenshot shows the Logpoint Director Console UI. On the left is a dark sidebar with navigation links: MONITORING, SEARCH, CONFIGURE (highlighted), CONFIG VIEW, ASSETS, USERS, LICENSE, and TASKS. The main content area has a light gray background. At the top right of the main area, there's a user profile icon labeled 'dsh' and a 'Sign Out' link. Below this, there are two radio buttons: 'Create' (selected) and 'List'. A white form is centered on the screen. It has two radio buttons at the top: 'Api' (selected) and 'Free_feed'. Below these are four input fields, each with a green checkmark icon on the right: 'Base URL' (with a red asterisk), 'API Key' (with a red asterisk), 'Filter Parameter', and 'Logs From' (containing the date '2024-02-08'). At the bottom right of the form area, there are two buttons: 'BACK' and 'NEXT'.

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**.

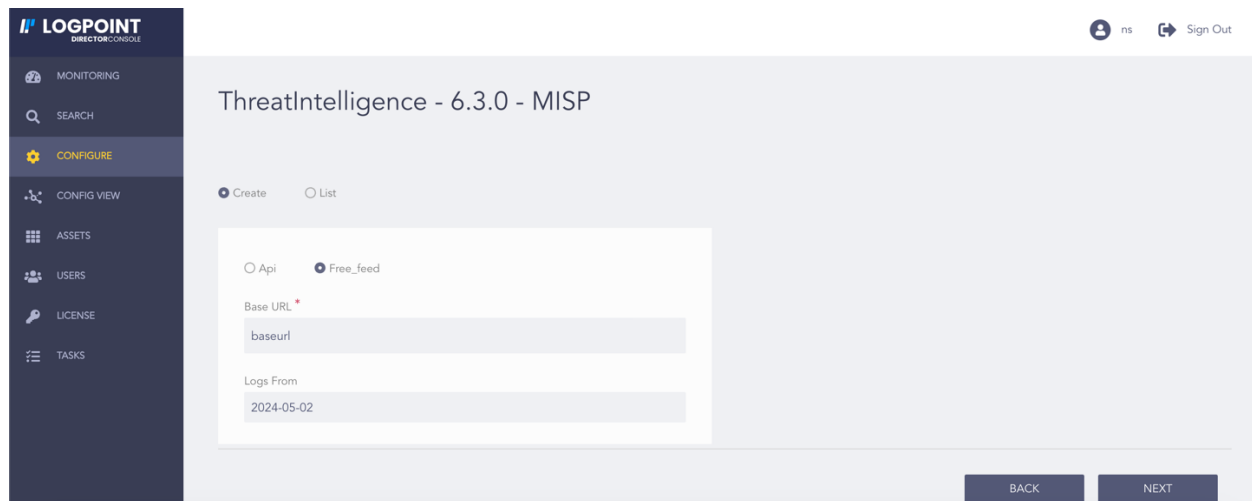


Fig. 23: Selecting Free Feed

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.

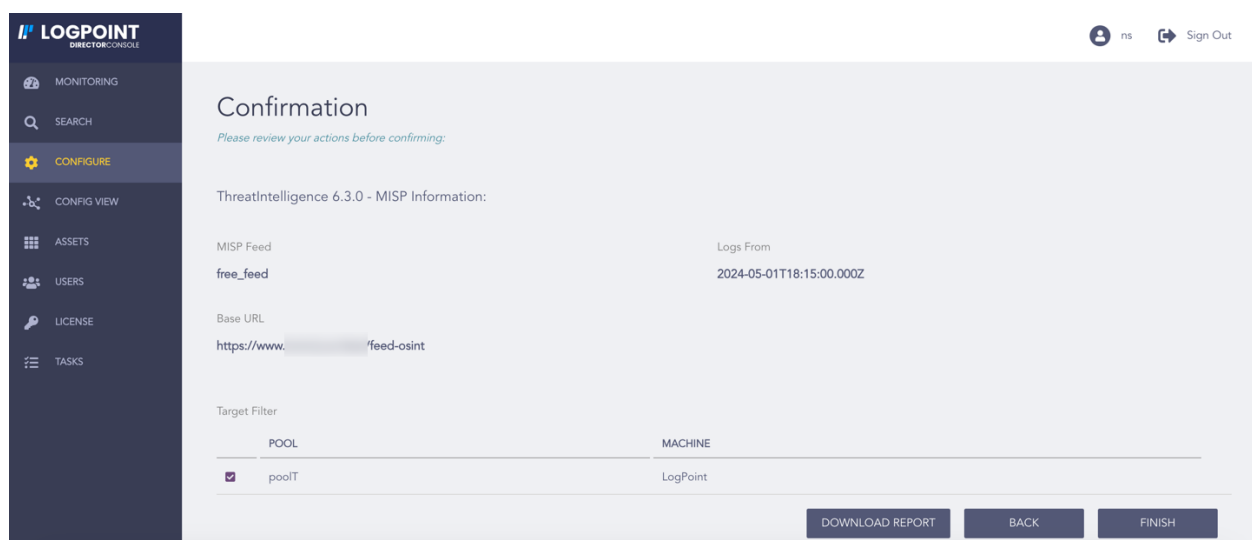


Fig. 24: Confirming the Changes

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**.

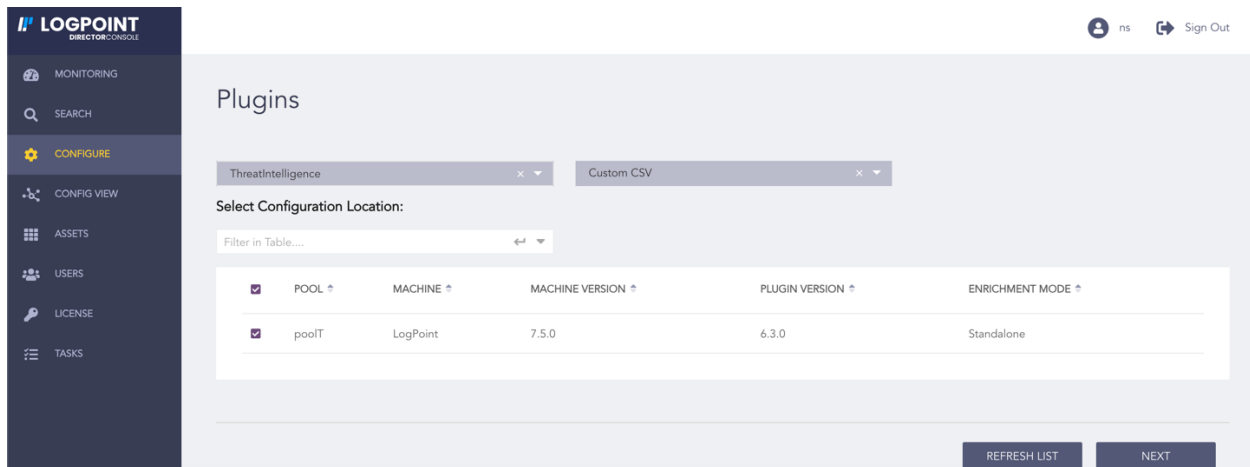


Fig. 25: Selecting Custom CSV

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.

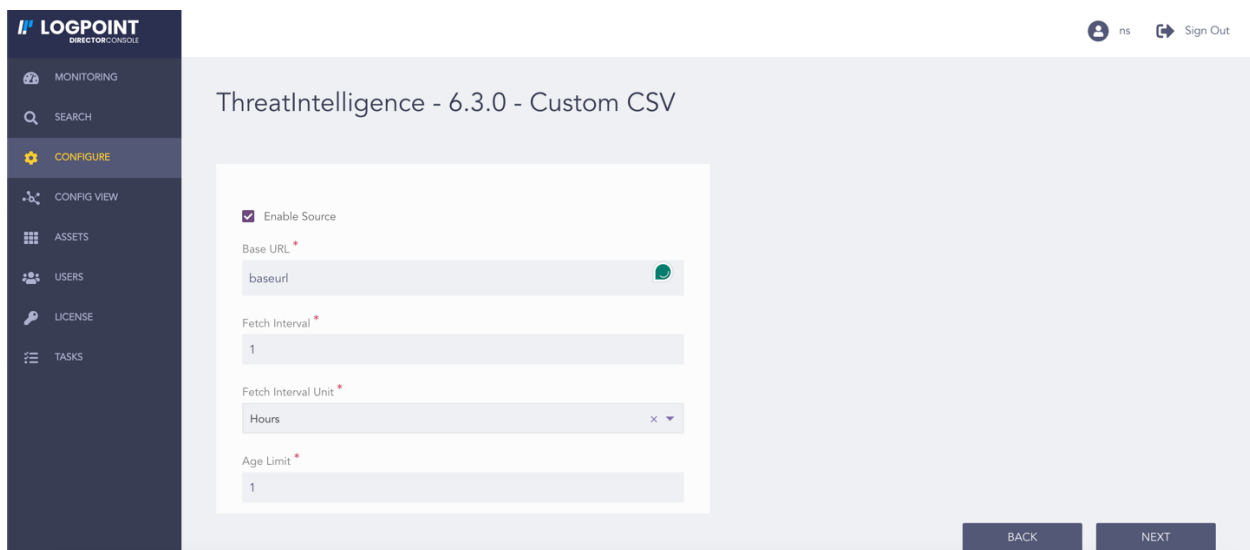


Fig. 26: Enabling Custom CSV

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**.

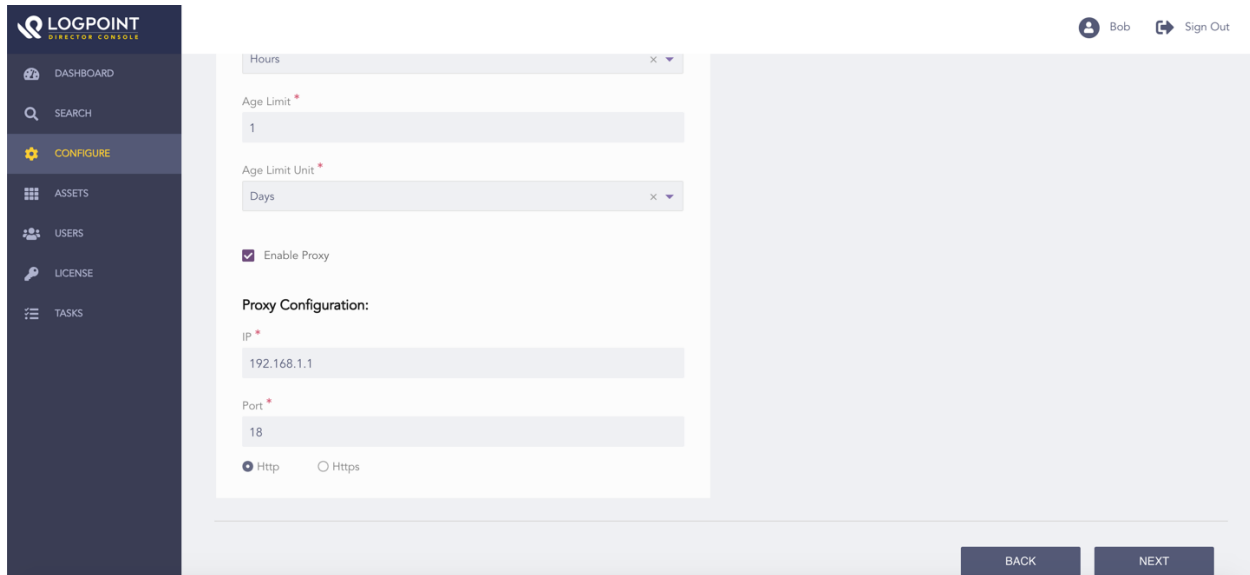
The screenshot shows the Logpoint Director Console interface. On the left is a dark sidebar with navigation links: DASHBOARD, SEARCH, CONFIGURE (highlighted), ASSETS, USERS, LICENSE, and TASKS. The main content area is light gray. At the top right, it shows a user profile 'Bob' and a 'Sign Out' button. The 'Hours' dropdown is set to 'x'. Below it, 'Age Limit' is '1' and 'Age Limit Unit' is 'Days'. The 'Enable Proxy' checkbox is checked. Under 'Proxy Configuration', the 'IP' field contains '192.168.1.1' and the 'Port' field contains '18'. The 'Http' radio button is selected over the 'Https' option. At the bottom right, there are 'BACK' and 'NEXT' buttons.

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.

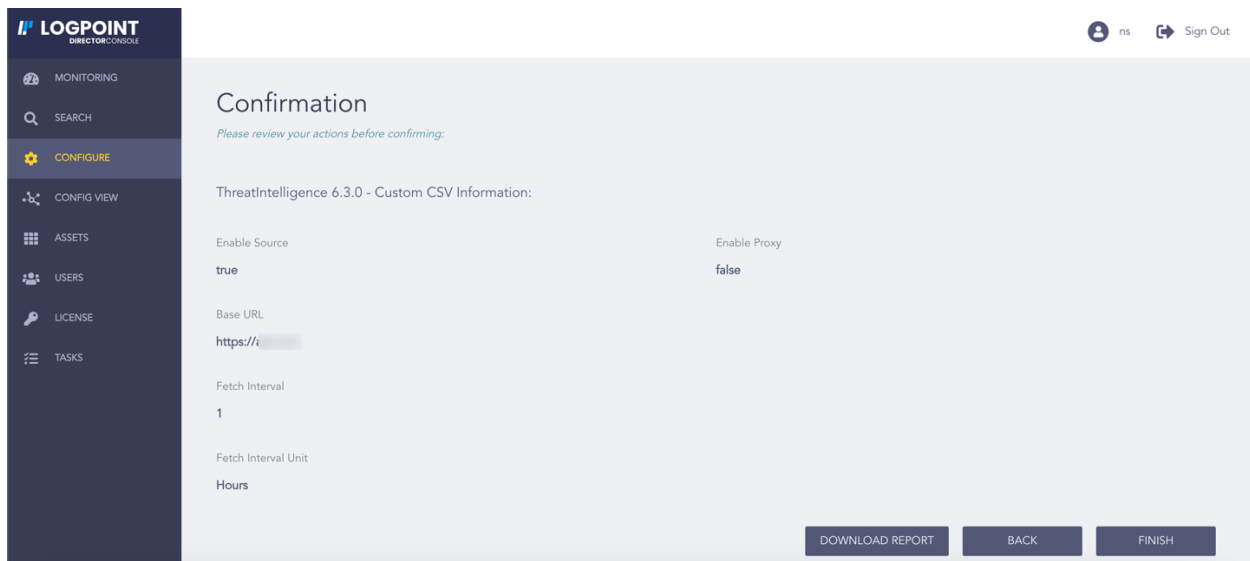


Fig. 28: Confirming the Changes

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**.

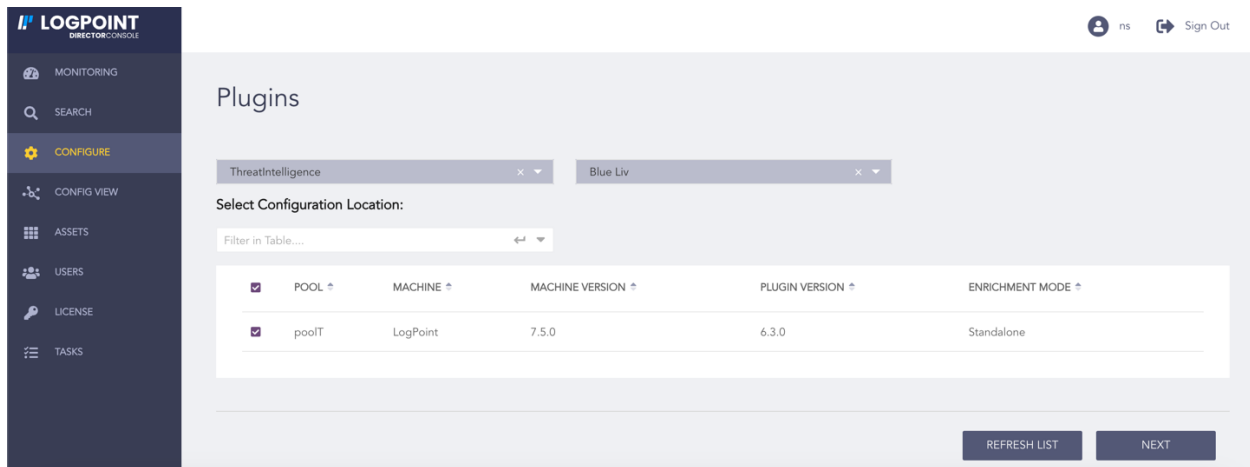


Fig. 29: Selecting Blue Liv

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.

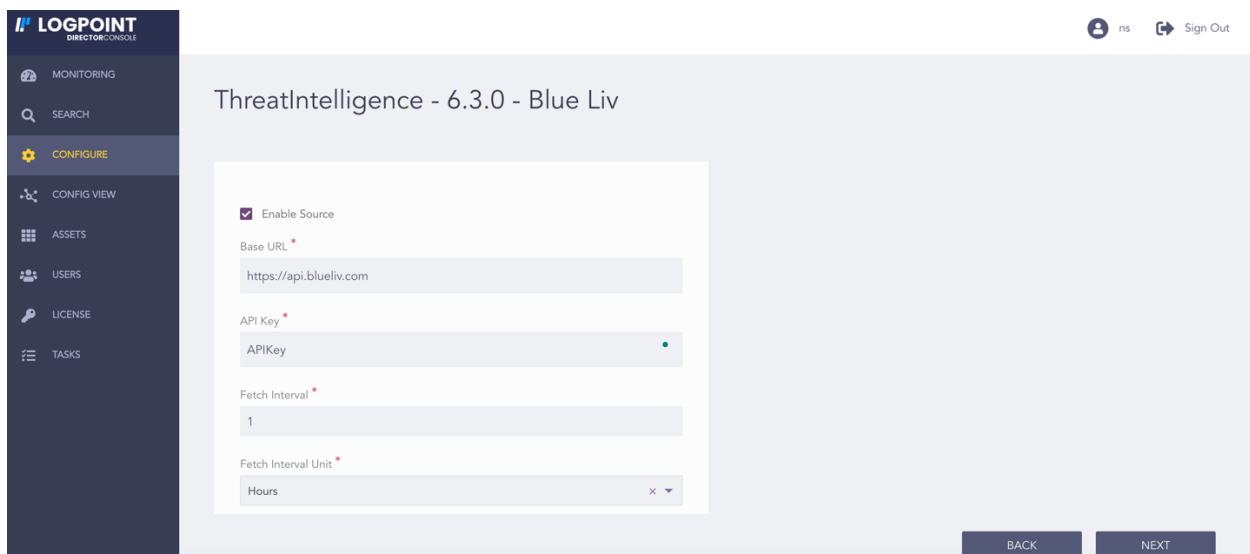


Fig. 30: Enabling Blue Liv

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**.

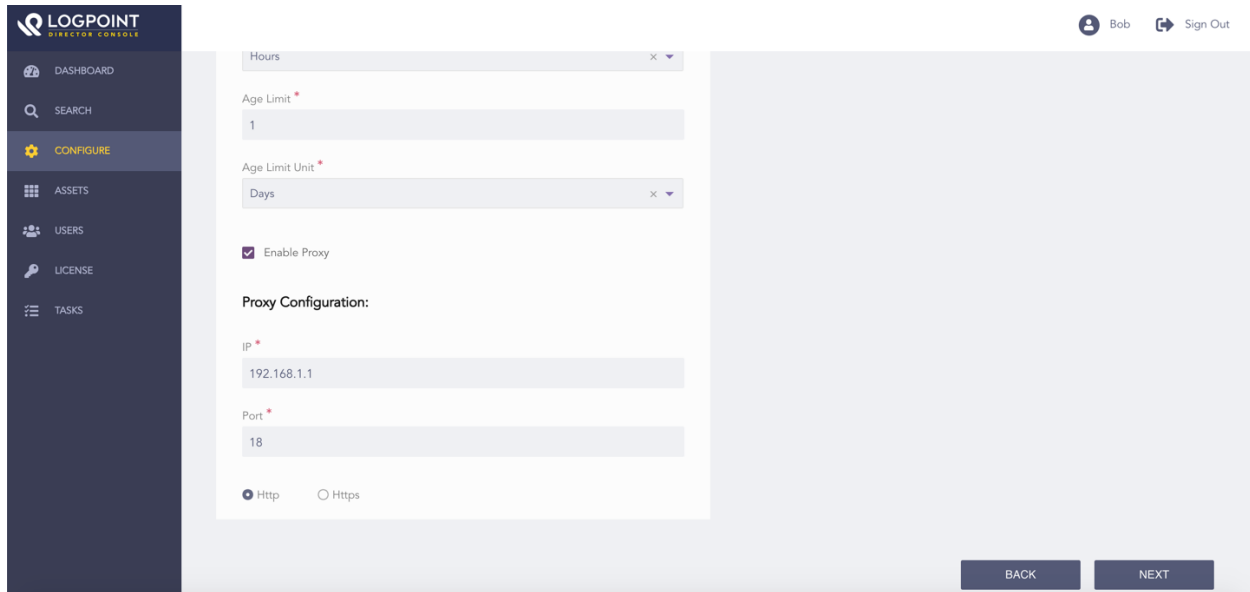
The screenshot shows the Logpoint Director Console interface. On the left is a dark sidebar with navigation links: DASHBOARD, SEARCH, CONFIGURE (highlighted), ASSETS, USERS, LICENSE, and TASKS. The main content area is light gray. At the top right, there's a user profile 'Bob' and a 'Sign Out' button. The 'Hours' dropdown is set to 'x'. Below it, 'Age Limit' is '1' and 'Age Limit Unit' is 'Days'. The 'Enable Proxy' checkbox is checked. Under 'Proxy Configuration', the 'IP' field contains '192.168.1.1' and the 'Port' field contains '18'. The 'Http' radio button is selected over 'Https'. At the bottom right, there are 'BACK' and 'NEXT' buttons.

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.

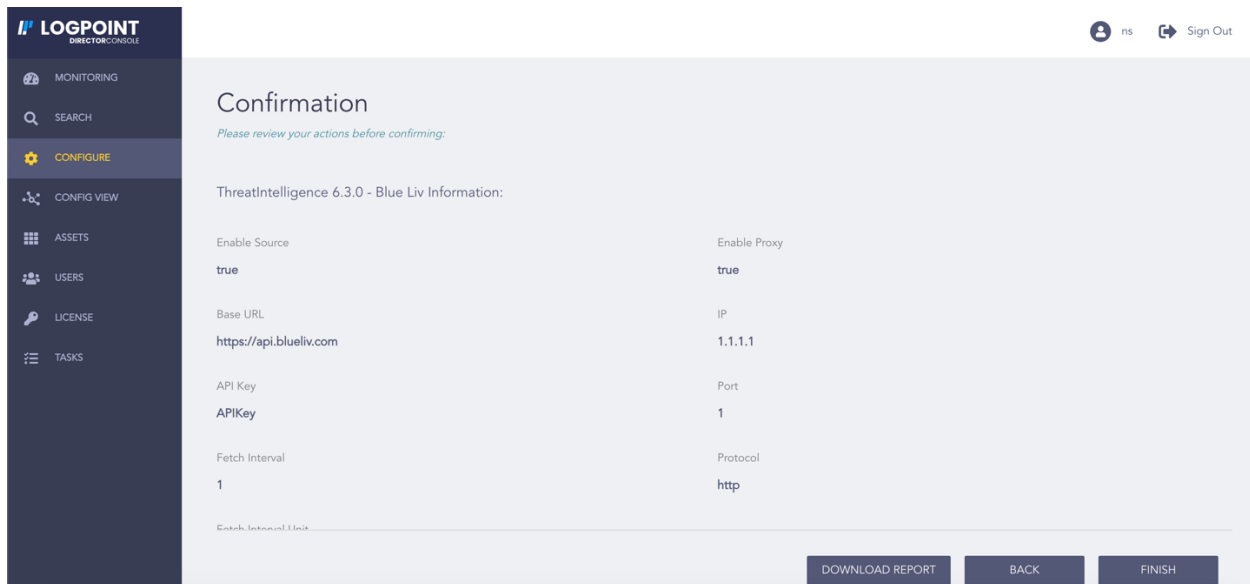


Fig. 32: Confirming the Changes

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**.

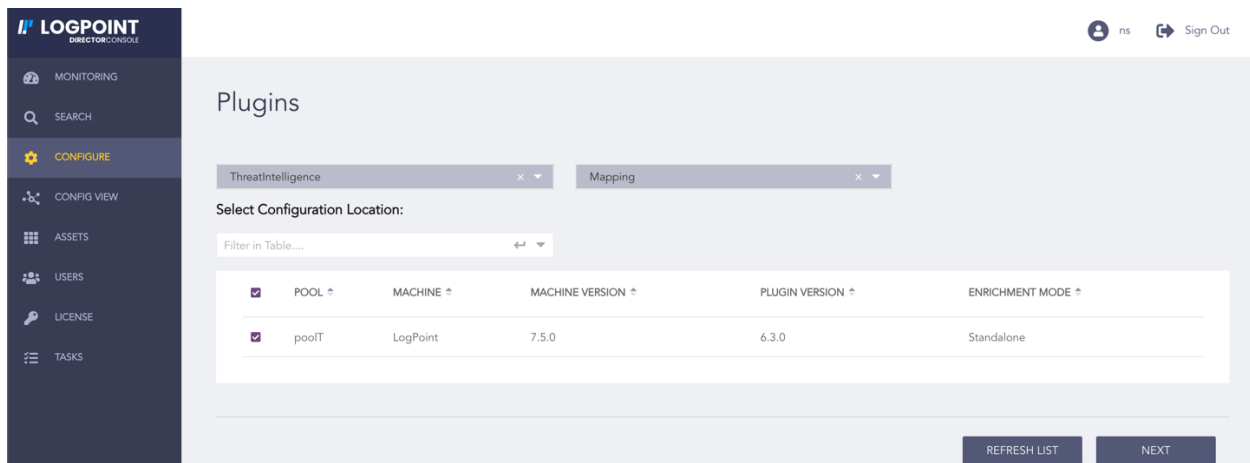


Fig. 33: Selecting Mapping

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**.

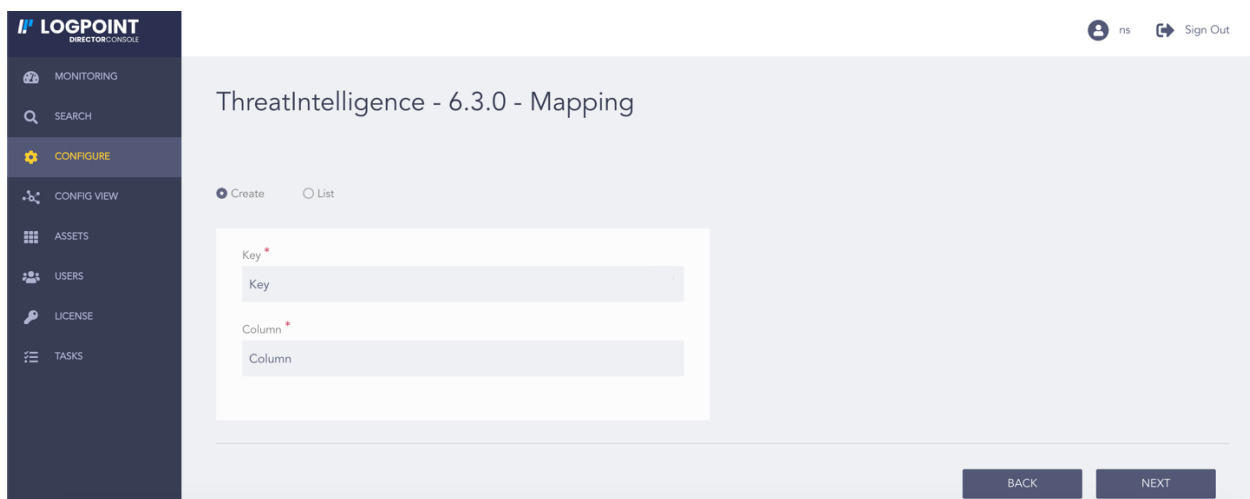


Fig. 34: Mapping

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.

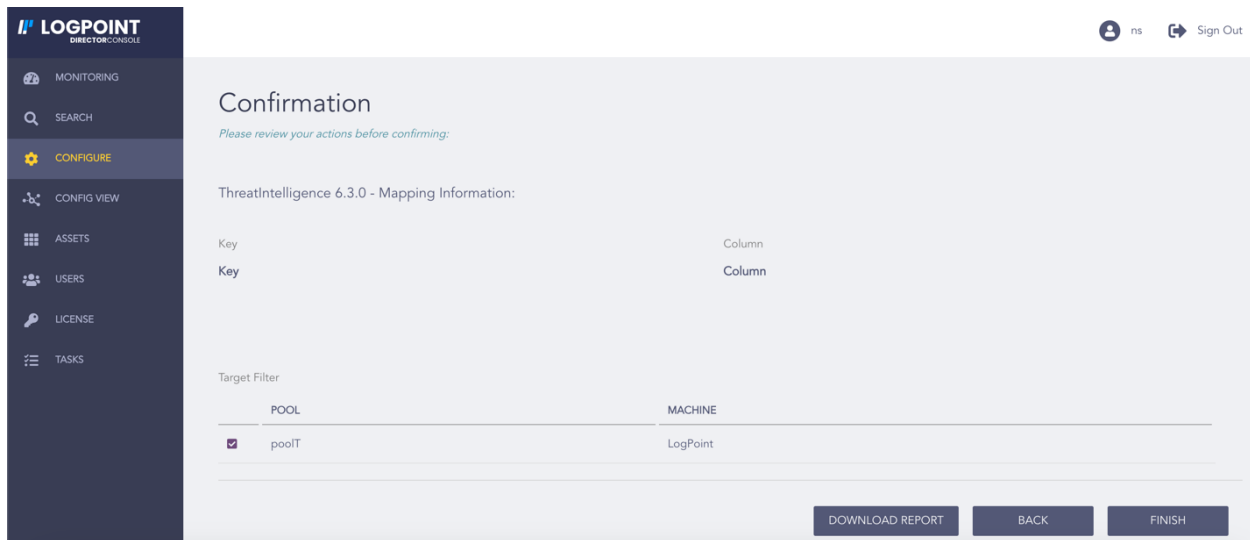


Fig. 35: Confirming the Changes

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**.

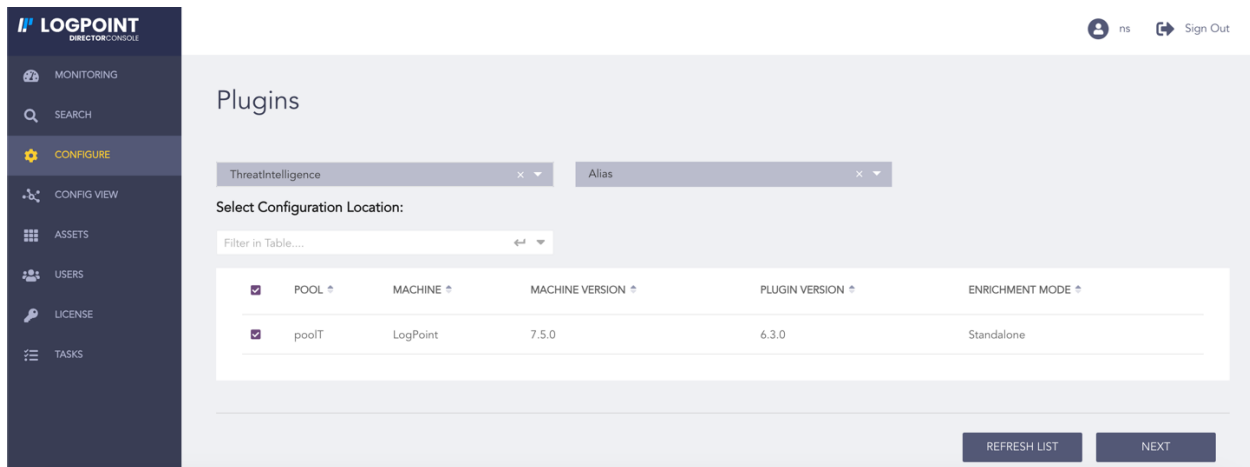


Fig. 36: Selecting Alias

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.

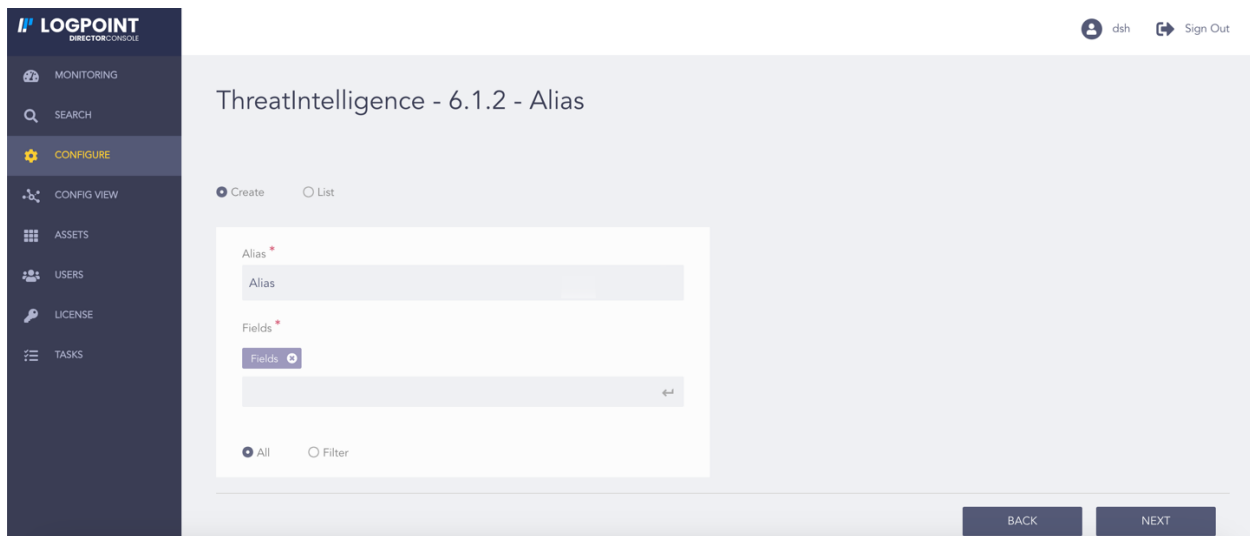


Fig. 37: Configuring Alias

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

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

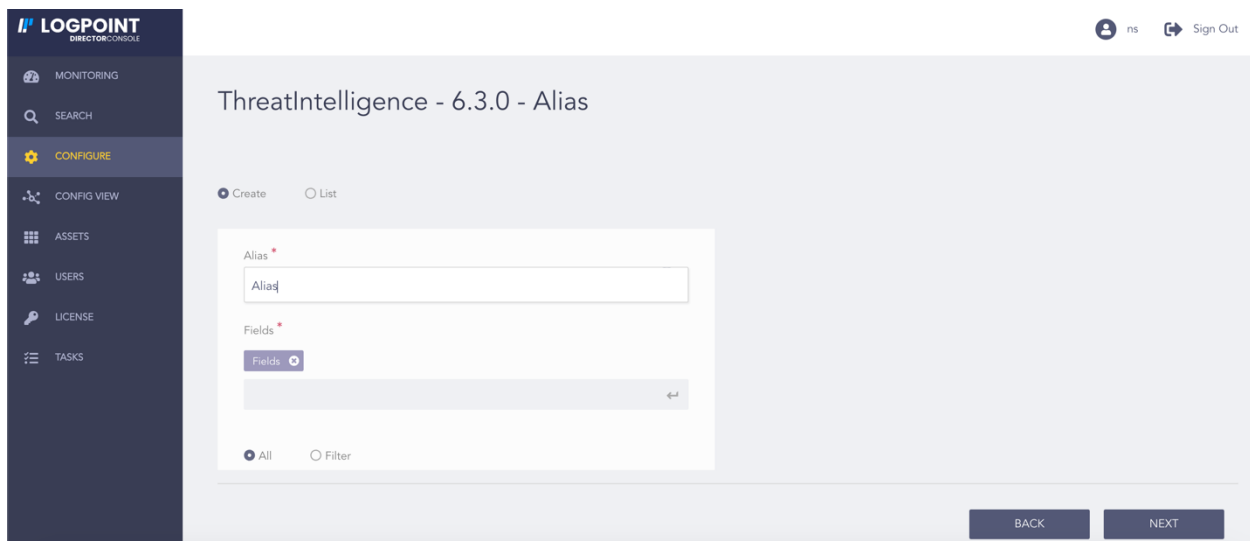


Fig. 38: Confirming the Changes

EDITING THREAT INTELLIGENCE

1. Click **CONFIGURATION** from the left navigation bar.
2. Under **Settings**, click **PLUGINS**.
3. Select **Threat Intelligence** from the **Select Plugin Type** drop-down.
4. Select Logpoint to edit the Threat Intelligence configuration. Multiple Logpoint can be selected from different pools.
5. Select **Plugin Sub-type**. Click **NEXT**.

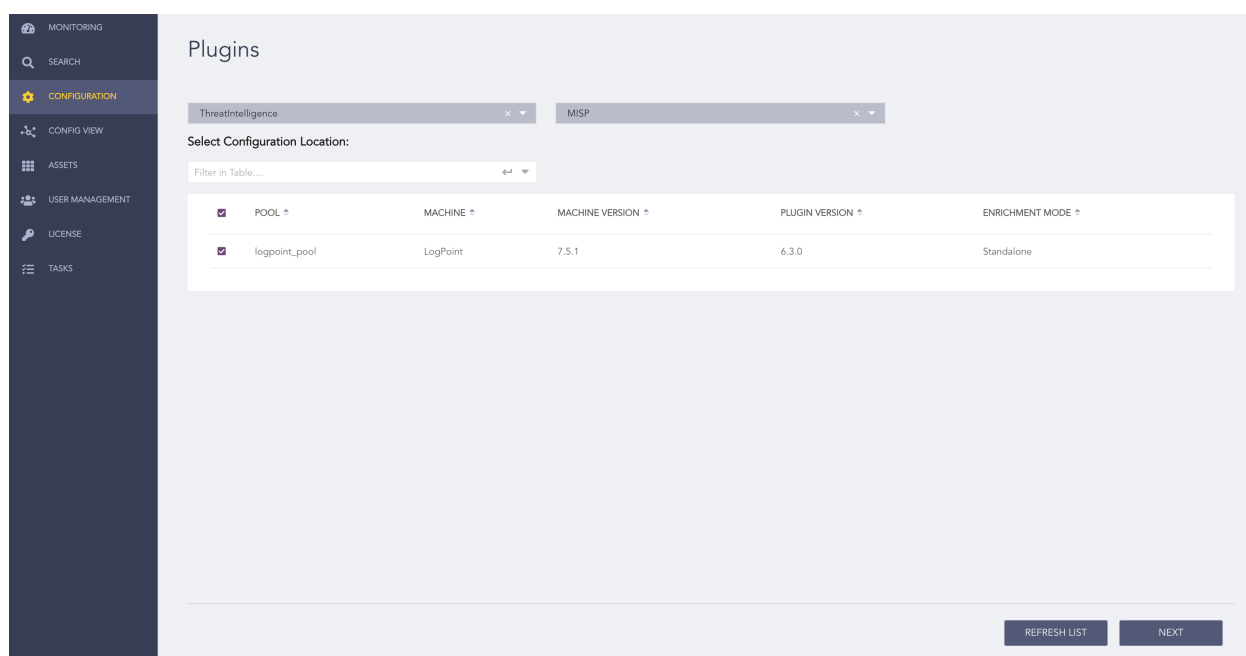


Fig. 1: Selecting Logpoint

6. Select **List**. The page lists the configurations that are common to all the selected Logpoint.

7. Click the **Edit** icon under **ACTION**.

8. Make the changes and click **EDIT**.

The **Action Status** of the configuration changes to **Changed**. To undo changes, click the **Undo** icon from **Action**.

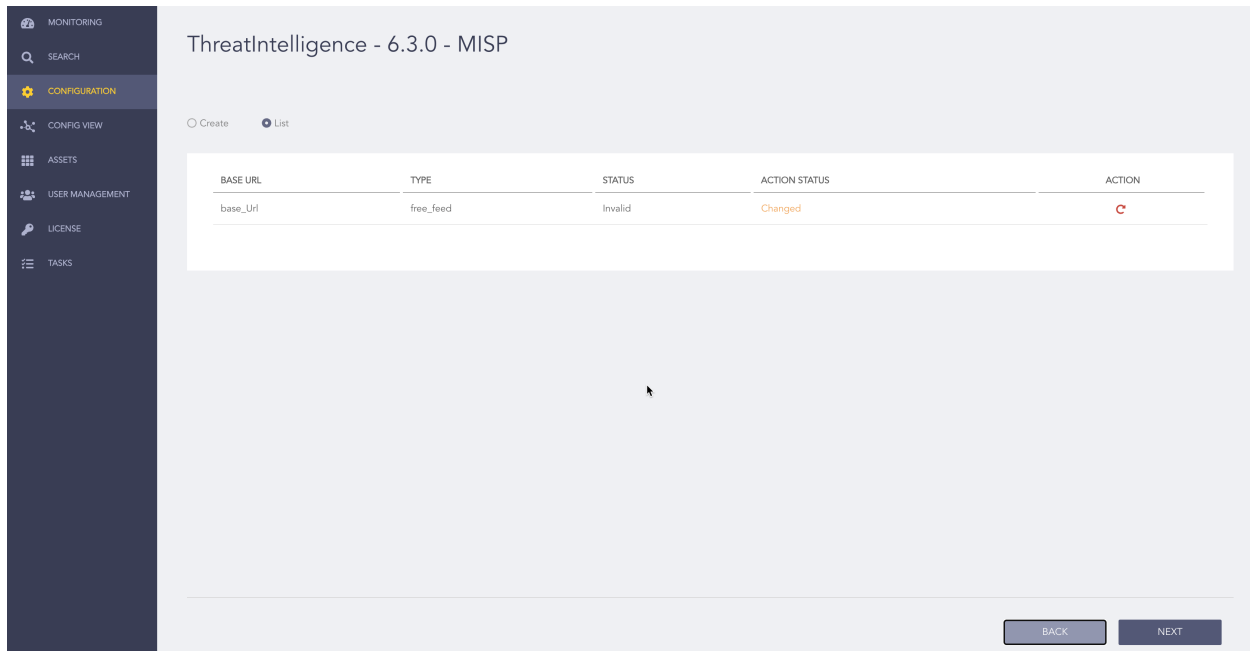


Fig. 2: Editing Threat Intelligence Configurations

9. Click **NEXT**.

10. Review your changes. Click **BACK** to make more changes. Click **DOWNLOAD REPORT** to get a summary as a PDF.

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

You are redirected to **TASKS**, which displays the Threat Intelligence edit progress.

6.1 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.