



DEPLOYMENT GUIDE

Infoblox BloxOne[®] Threat Defense Cloud Add-on for Splunk Enterprise



Table of Contents

Introduction	2
Prerequisites	2
Known Limitations	2
Best Practices	2
Configuration	2
Workflow	2
Infoblox Configuration	3
Acquire CSP API Keys	3
Splunk Enterprise Configuration	4
Verify that the correct Splunk add-ons are installed	4
Install the BloxOne Threat Defense Add-on	5
Test the Configuration	17
Additional Resources	19

Introduction

The Infoblox BloxOne Threat Defense Splunk Add-on was created by an Infoblox SE to support the syncing of comprehensive threat intelligence from BloxOne Threat Defense, and network intelligence from Infoblox to the SIEM Splunk. Please note that this Splunk add-on is not officially supported by Infoblox.

Prerequisites

The following are prerequisites for the Infoblox Add-on in Splunk:

- Infoblox
 - BloxOne Threat Defense
 - BloxOne Threat Defense Advanced License
 - Infoblox CSP user account with access to Dossier and CSP API Tokens
- Splunk
 - Splunk Account
 - Splunk Enterprise (Version 7.x, 8)
 - Splunk Add-ons:
 - Infoblox Splunk Enterprise Plug-in version 2.1.3 (<https://splunkbase.splunk.com/app/4941/#/details>)
 - Punchcard (<https://splunkbase.splunk.com/app/3129/>)
 - Splunk Dashboard Examples (<https://splunkbase.splunk.com/app/1603/>)
 - Splunk Sankey Diagram (<https://splunkbase.splunk.com/app/3112/>)
 - Treemap (<https://splunkbase.splunk.com/app/3118/>)

Known Limitations

For the full functionality of the Infoblox BloxOne Threat Defense add-on you will need to have a CSP account with access to a Infoblox CSP tenant with a BloxOne Threat Defense Advanced license. The acquisition of Security Hits is supported by all levels of a BloxOne Threat Defense subscription; however, IOC enrichment that is accomplished via Infoblox Dossier requires a BloxOne Threat Defense Advanced subscription.

Please note that this Splunk add-on is not officially supported by Infoblox.

Best Practices

Before proceeding with the Installation guide, ensure that all prerequisites have been met. If you do not install the correct Splunk Add-ons before installing the Splunk Add-on for Infoblox Intelligence the installation will likely fail.

For information regarding the installation of Add-ons for Splunk refer to this documentation: <https://docs.splunk.com/Documentation/AddOns/released/Overview/Installingadd-ons>

Configuration

Workflow

Infoblox CSP:

1. Acquire the API keys associated with your Infoblox CSP account.
 - o Dossier API Key
 - o CSP Tenant API Key

Splunk:

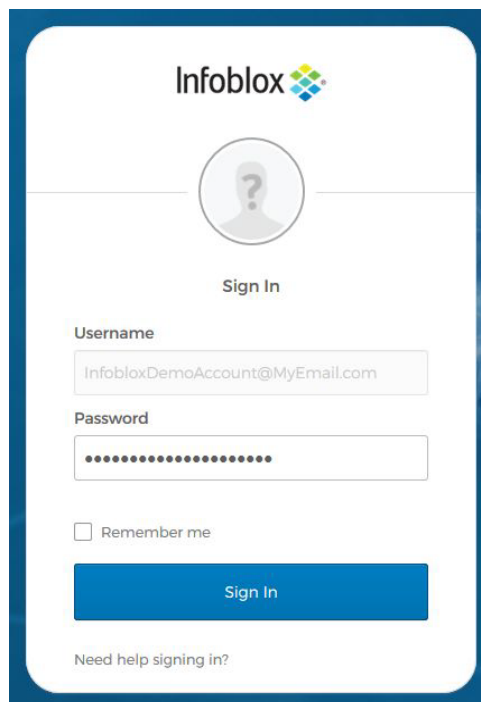
1. Verify that the correct Splunk add-ons are installed.
2. Install the BloxOne Threat Defense Splunk add-on.
3. Configure the BloxOne Threat Defense Splunk add-on to sync with the Infoblox CSP.
4. (Optional) Configure the BloxOne Threat Defense Splunk add-on to take inventory of all BloxOne Endpoints associated with your CSP account.
5. Test the configuration

Infoblox

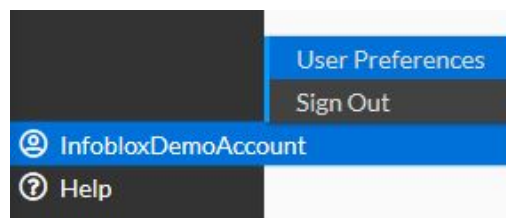
Configuration Acquire

To acquire the CSP API tokens that are required for the Infoblox Add-on, perform the following steps:

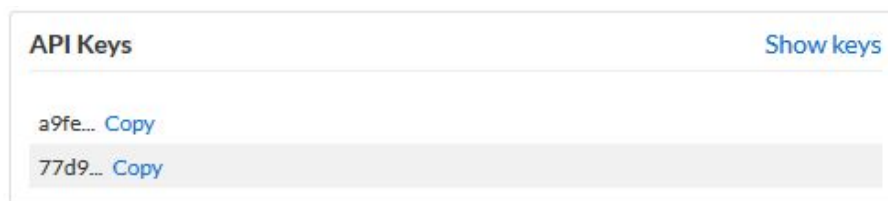
1. Log in to the Infoblox CSP with your CSP account.



2. Once logged in to the Infoblox CSP, Access your user Preferences. **Mouse-over** your **Username** on the bottom left of the CSP interface. Then, click **User Preferences**.



3. Locate and **Copy** both API Keys and paste these into a text file for use later. *Note: The shorter key is associated with the CSP account, and the longer key is associated with Dossier.*
 - o If you only see a single key in the list of API Keys, you will need to log in to <https://platform.activetrust.net> and access **User Settings** → **Manage API Keys** to acquire a Dossier key.



Splunk Enterprise Configuration

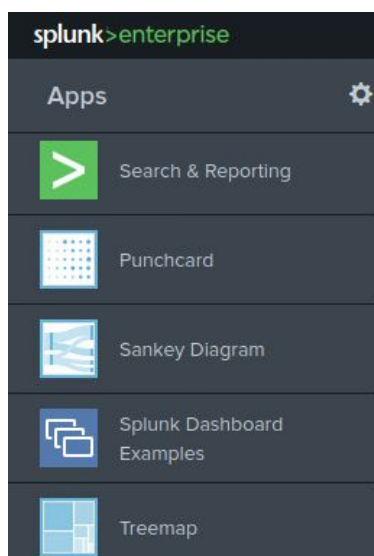
Verify that the correct Splunk add-ons are installed

To verify that all required Splunk add-ons are installed perform the following steps:

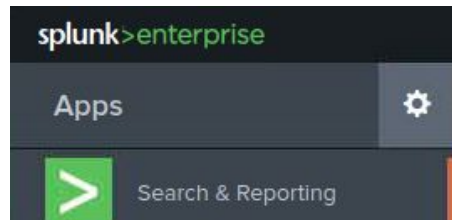
1. **Log in** to the web interface of the Splunk Enterprise device.



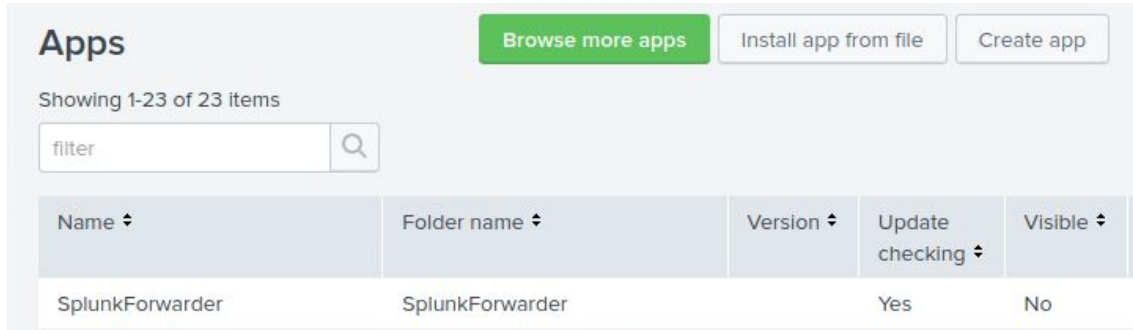
2. In the **Apps** list on the left side of the Splunk Enterprise window, ensure that the following addons are installed:
 - o Punchcard
 - o Sankey Diagram
 - o Splunk Dashboard Examples
 - o Treemap



- (Optional) Alternatively, you may click the **Cog** icon to access the Splunk Add-on interface.



- Here you can search for the add-ons that are required for the BloxOne Threat Defense add-on.

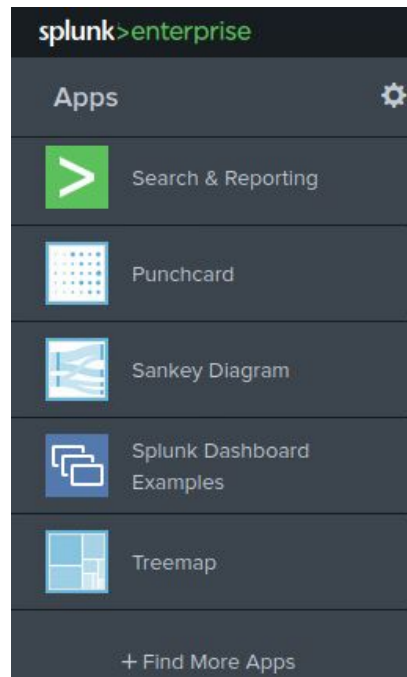


- If any add-ons are missing, install them according to the instructions located here: <https://docs.splunk.com/Documentation/AddOns/released/Overview/Installingadd-ons>

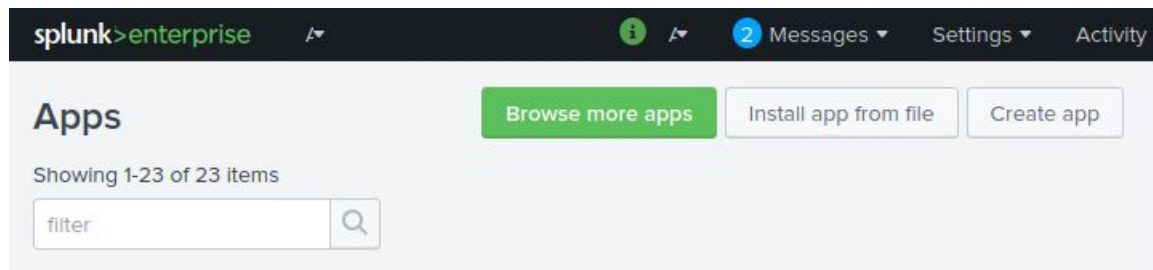
Install the BloxOne Threat Defense Add-on

To install the BloxOne Threat Defense Add-on perform the following steps:

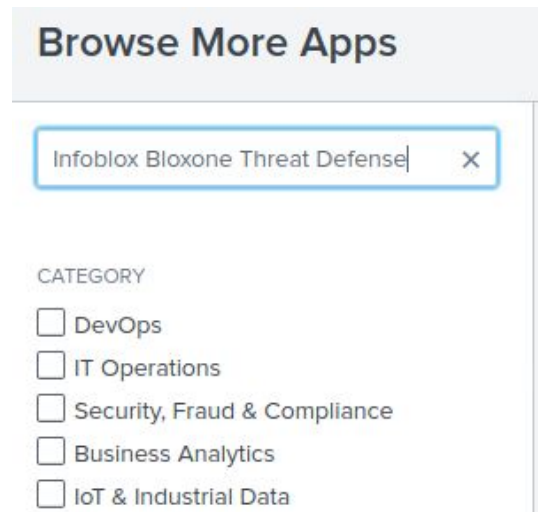
- On the Splunk Enterprise web interface click **+ Find More Apps** located near the bottom of the Apps list.



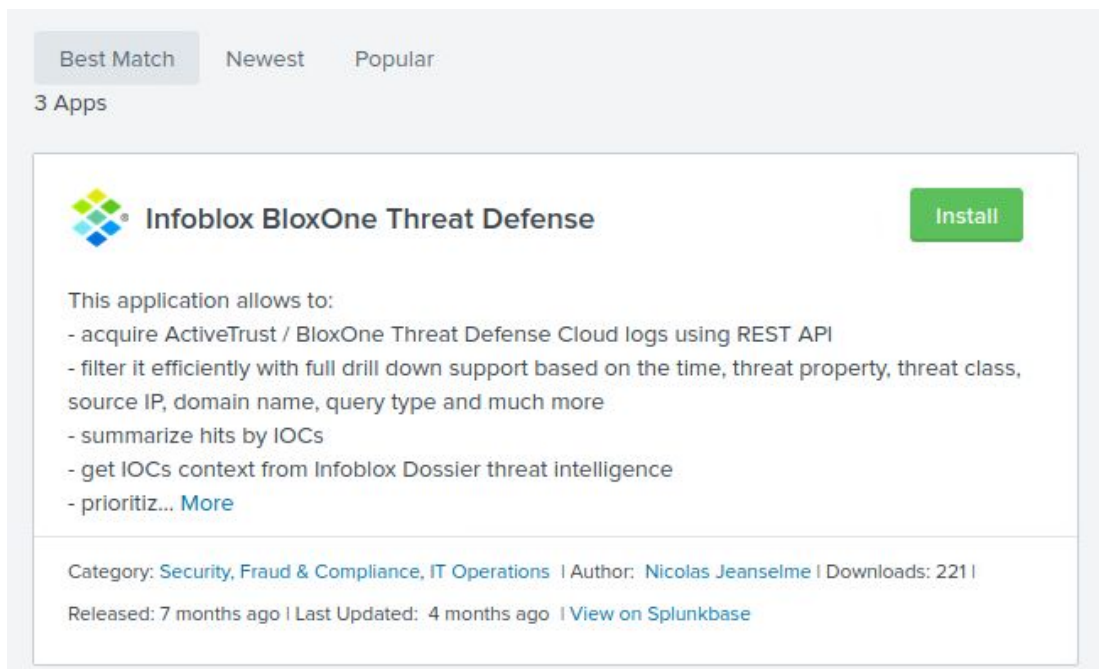
2. On the Apps page, click the **Browse more apps** button.



3. Search for **Infoblox Bloxone Threat Defense** by using the **Find apps by keyword...** text box on the Browse More Apps page.



4. Locate the [Infoblox BloxOne Threat Defense add-on](#) and click the **Install** button.



5. A Login dialog box will be displayed. Input your Splunk.com **username** and **password**.

Login ×

Enter your Splunk.com username and password to download the app.

admin

.....

[Forgot your password?](#)

The app, and any related dependency that will be installed, may be provided by Splunk and/or a third party and your right to use these app(s) is in accordance with the applicable license(s) provided by Splunk and/or the third-party licensor. Splunk is not responsible for any third-party app and does not provide any warranty or support. If you have any questions, complaints or claims with respect

Cancel Login and Install

6. Scroll down in the Dialog box and click the **checkbox** to accept the terms and conditions. Then, click **Login and Install** to begin the installation.

I have read the terms and conditions of the license and agree to be bound by them. I accept that Splunk will securely send my login credentials over the Internet to splunk.com

Cancel Login and Install

- Wait a few moments for the Installation to complete.
7. When prompted to restart Splunk, click **Restart Now**.

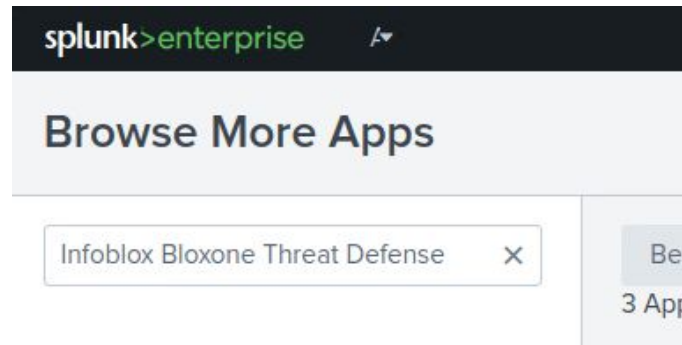
Restart Required ×

You must restart Splunk Splunk Enterprise to complete installation of Infoblox BloxOne Threat Defense.

Restart Later Restart Now

8. After the device has successfully restarted, **Log in** to the Splunk Enterprise device again.

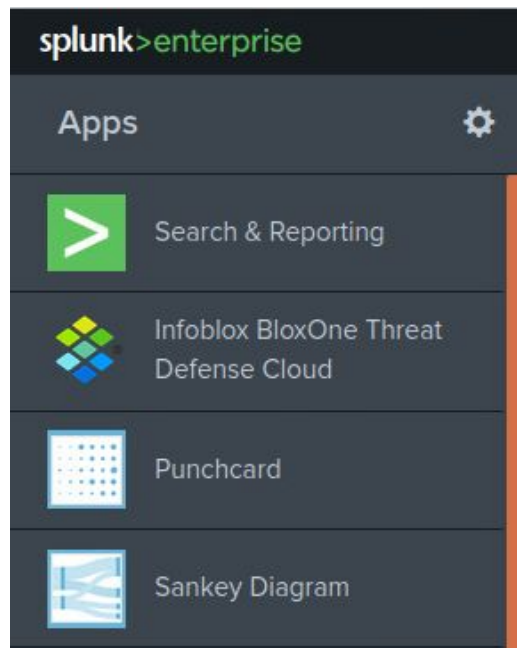
9. Navigate to the home page of the Splunk web interface by clicking the **splunk>enterprise** logo on the top left of the web page.



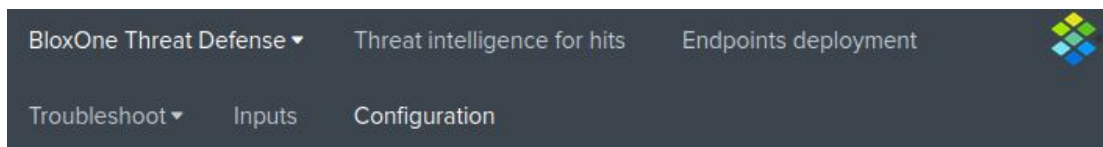
Configure the BloxOne Threat Defense Add-on

To configure the Infoblox BloxOne Threat Defense add-on perform the following steps:

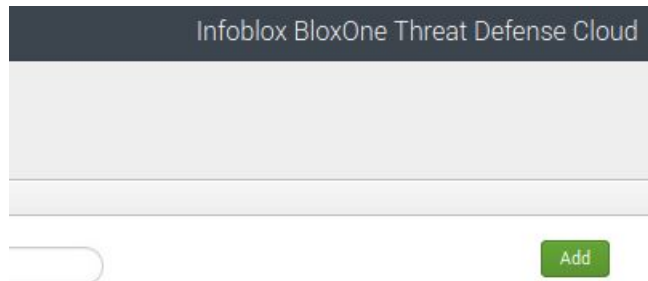
1. The add-on Infoblox BloxOne Threat Defense Cloud should now be visible in the splunk App list. Click the text **Infoblox BloxOne Threat Defense Cloud**.



2. In the Infoblox BloxOne Threat Defense Cloud app navigation bar, click **Configuration**.



3. On the Account tab of the Configuration page click **Add** located on the right side of the window.

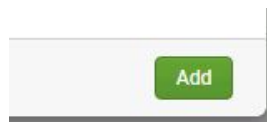


4. On the Add Account dialog box, input the following information:
 - o **Account name**, input the name **TA**.
 - o **Username**, input a **username** that has administrative permissions for this device.
 - o **Password**, input the **password** for the user that was used in the previous bullet.

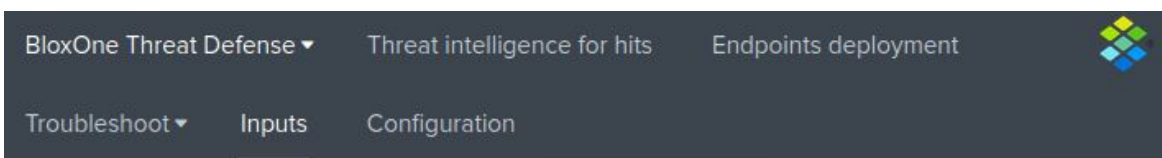
A screenshot of the "Add Account" dialog box. The title bar says "Add Account". There are three input fields:

- Account name ***: The text "TA" is entered. Below the field is the hint "Enter a unique name for this account."
- Username ***: The text "admin" is entered. Below the field is the hint "Enter the username for this account."
- Password ***: The text "*****" is entered. Below the field is the hint "Enter the password for this account."

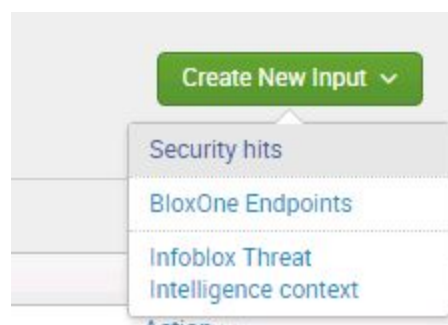
5. Click **Add** to confirm the addition of the Account.



6. In the Infoblox BloxOne Threat Defense Cloud app navigation bar, click **Inputs**.



7. On the Inputs page, click **Create New Input**. Then, click **Security hits** in the dropdown menu that is revealed.



8. In the **Add Security hits** dialog box input the following information:
 - o Name, input the name **DATA_INPUT**.
 - o **Interval**, input the value **15**.
 - o **Index**, input the text **main**.
 - o **Global Account**, select the Global Account **TA** that was created in steps 13-14.

Add Security hits

Name *
Enter a unique name for the data input

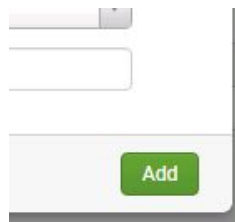
Interval *
Time interval of input in seconds.

Index *

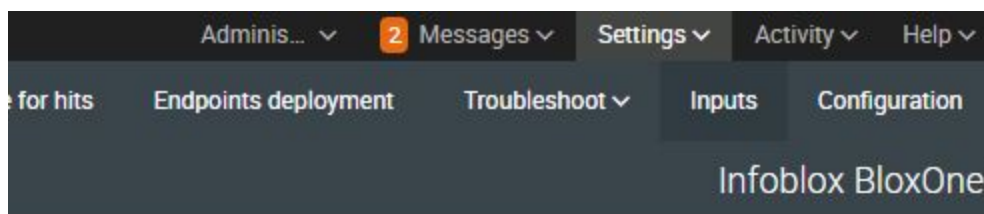
Global Account *

t0
start time for the first poll - unix timestamp if nothing specified, now

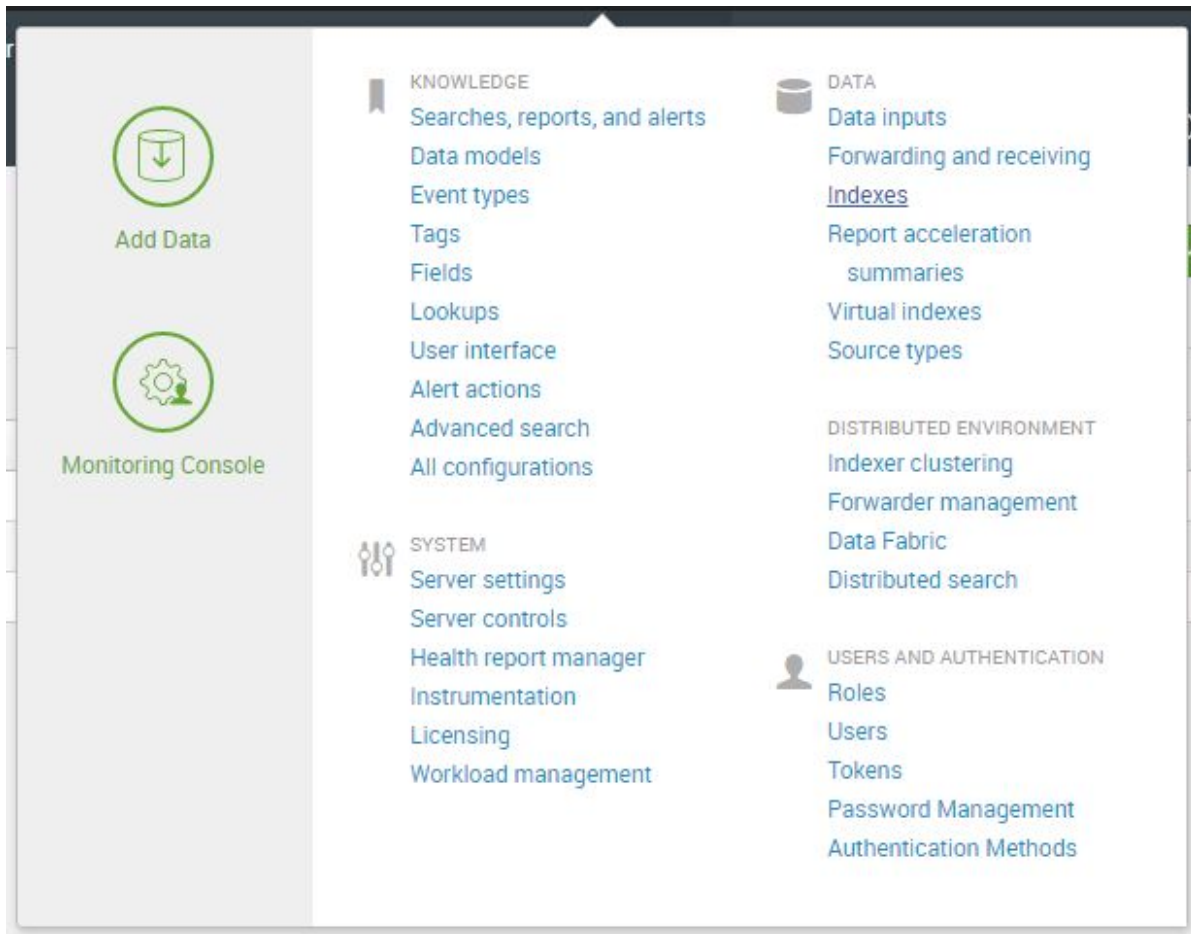
9. Click **Add** to confirm the addition of the Security hits input.



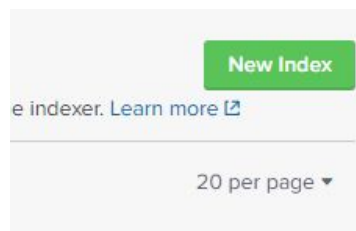
10. In the navigation bar of the Splunk interface, click **Settings**.



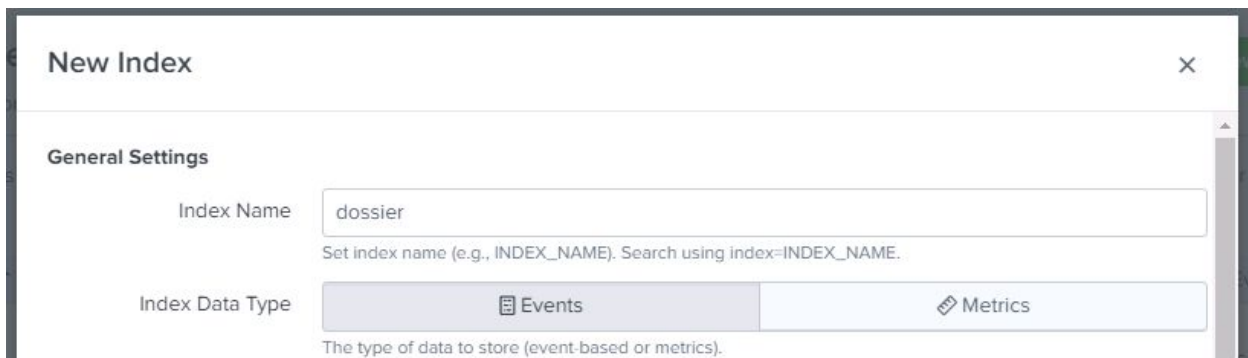
11. Click **Indexes** located under the Data header in the Settings menu.



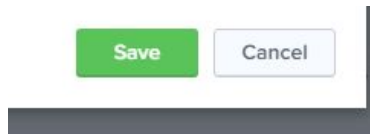
12. On the Indexes page, click the **New Index** button.



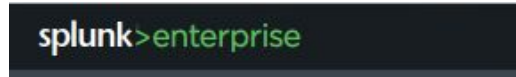
13. A **New Index** dialog box will be revealed. Input the Index Name **dossier**.



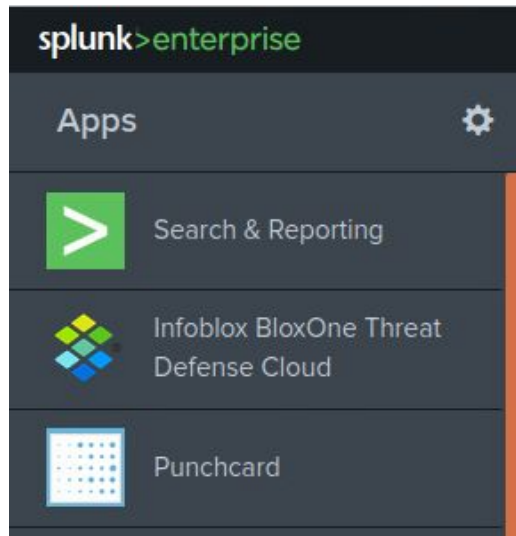
14. Click **Save** to confirm the creation of the new Index.



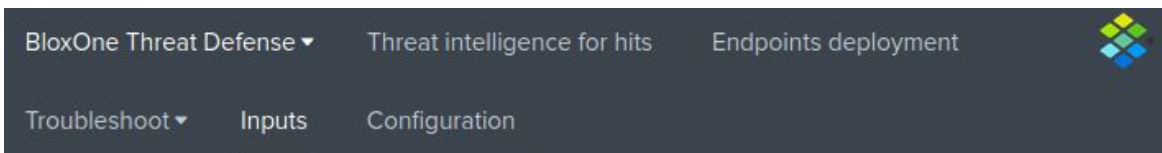
15. Navigate to the home page of the Splunk web interface by clicking the **splunk>enterprise** logo on the top left of the web page.



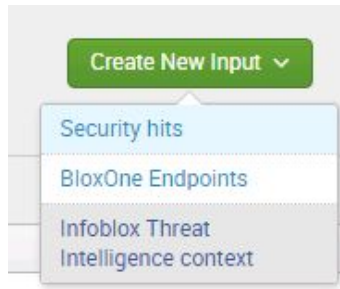
16. Click the text **Infoblox BloxOne Threat Defense Cloud** located in the list of Apps.



17. In the Infoblox BloxOne Threat Defense Cloud app navigation bar, click **Inputs**.



18. On the Inputs page, click **Create New Input**. Then, click **Infoblox Threat Intelligence context** in the dropdown menu that is revealed.



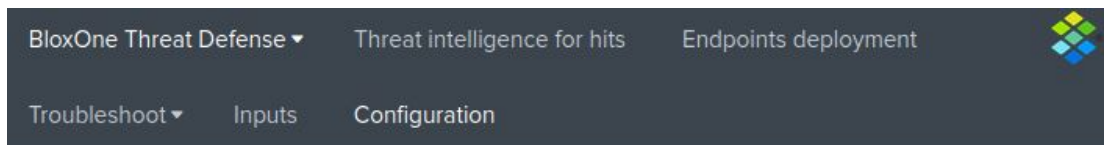
19. In the Add Infoblox Threat Intelligence context input the following information:
- **Name**, give the new Infoblox Threat Intelligence context the name **dossier**.
 - **Interval**, input the value **120**.
 - **Index**, select the index **dossier** that was created in steps 22-23.
 - **Global Account**, select the account **TA** that was created in steps 13-14.

A screenshot of a dialog box titled 'Add Infoblox Threat Intelligence context'. The dialog has a close button (X) in the top right corner. It contains four input fields, each with a red asterisk indicating it is required:

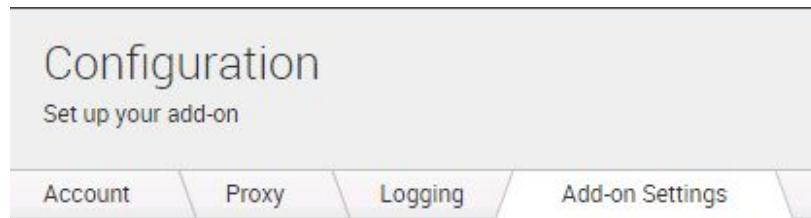
- Name ***: A text input field containing 'dossier'. Below the field is the placeholder text 'Enter a unique name for the data input'.
- Interval ***: A text input field containing '120'. Below the field is the placeholder text 'Time interval of input in seconds.'
- Index ***: A dropdown menu with 'dossier' selected.
- Global Account ***: A dropdown menu with 'TA' selected.

At the bottom of the dialog, there is a 'Cancel' button on the left and an 'Add' button on the right.

20. In the Infoblox BloxOne Threat Defense Cloud app navigation bar, click **Configuration**.



21. On the Account tab of the Configuration page click the **Add-on Settings** tab.



22. In the Add-on Settings tab:

- **Hostname**, input the domain **csp.infoblox.com**.
- **Cloud Service portal API key**, input the shorter API key that was acquired on page 4 of this document
- **Dossier Api key**, input the longer API key that was acquired on page 4 of this document

A screenshot of a configuration form. It has three input fields. The first is labeled "Hostname *" and contains the text "csp.infoblox.com". The second is labeled "Cloud Service portal API key *" and contains a series of asterisks. Below this field is a note: "Available in csp.infoblox.com in user preferences (short key)". The third is labeled "Dossier API key" and also contains a series of asterisks. Below this field is a note: "Available in csp.infoblox.com in user preferences (long key) and platform.activetrust.net".

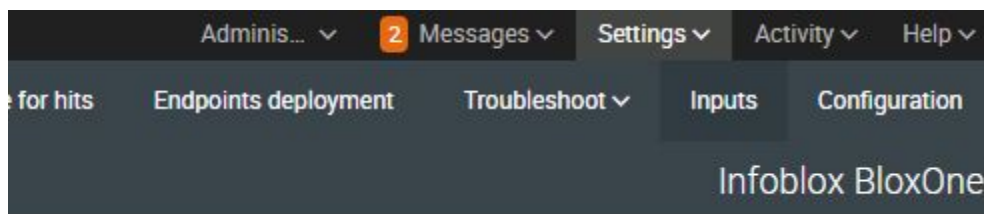
23. Click **Save** to confirm all changes.



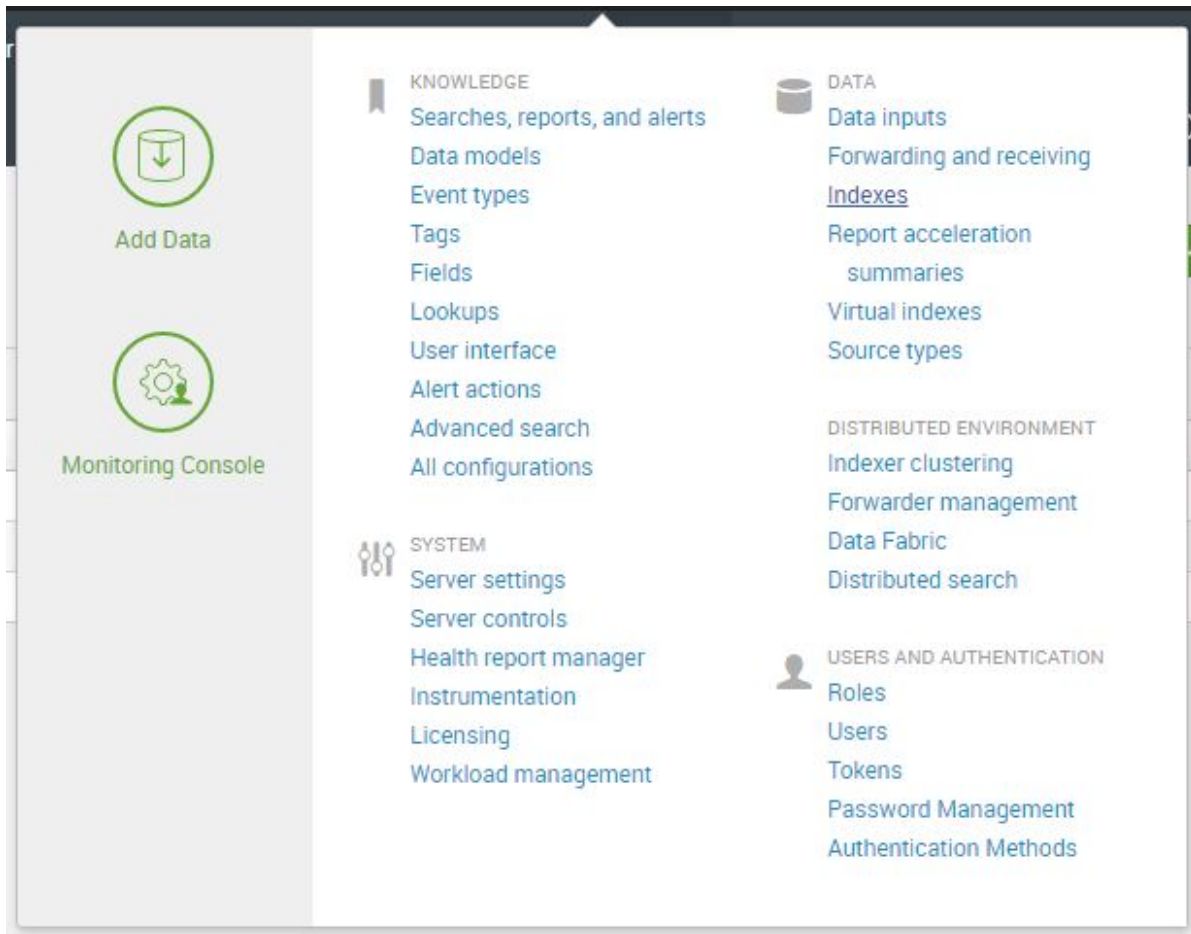
Configure the BloxOne Threat Defense Add-on to Take Inventory of all BloxOne Endpoints

This optional portion of the installation guide will show you how to configure the Infoblox BloxOne Threat Defense add-on to take inventory of all BloxOne Endpoints associated with your CSP account. To configure the BloxOne Threat Defense Add-on to perform this action, complete the following steps:

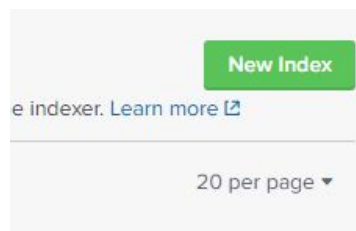
1. In the navigation bar of the Splunk interface, click **Settings**.



2. Click **Indexes** located under the Data header in the Settings menu.



3. On the Indexes page, click the **New Index** button.



4. A **New Index** dialog box will be revealed. Input the Index Name **endpoints**.

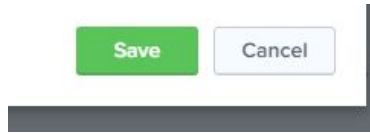
New Index ×

General Settings

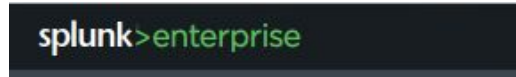
Index Name

Set index name (e.g., INDEX_NAME). Search using index=INDEX_NAME.

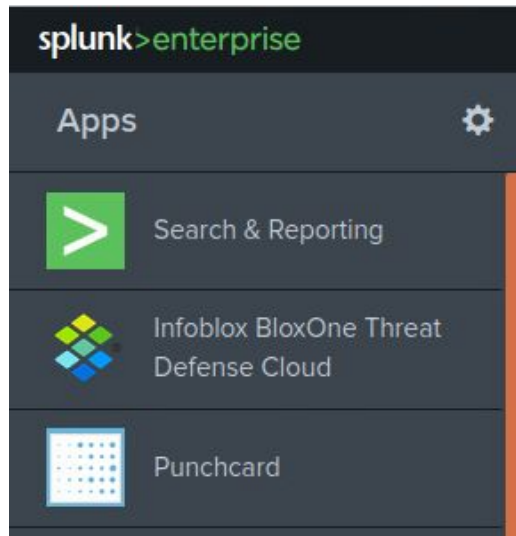
5. Click **Save** to confirm the creation of the new Index.



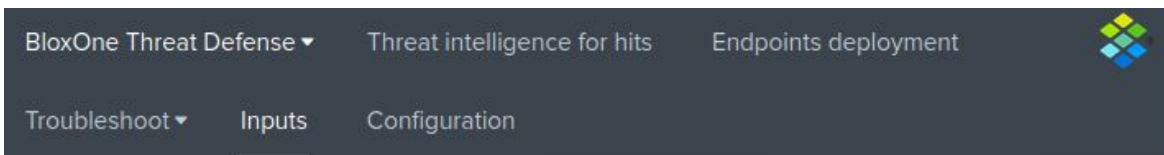
6. Navigate to the home page of the Splunk web interface by clicking the **splunk>enterprise** logo on the top left of the web page.



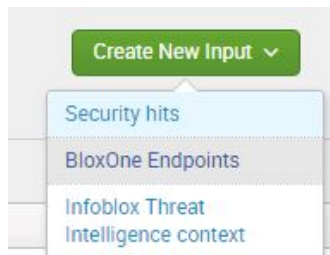
7. Click the text **Infoblox BloxOne Threat Defense Cloud** located in the list of Apps.



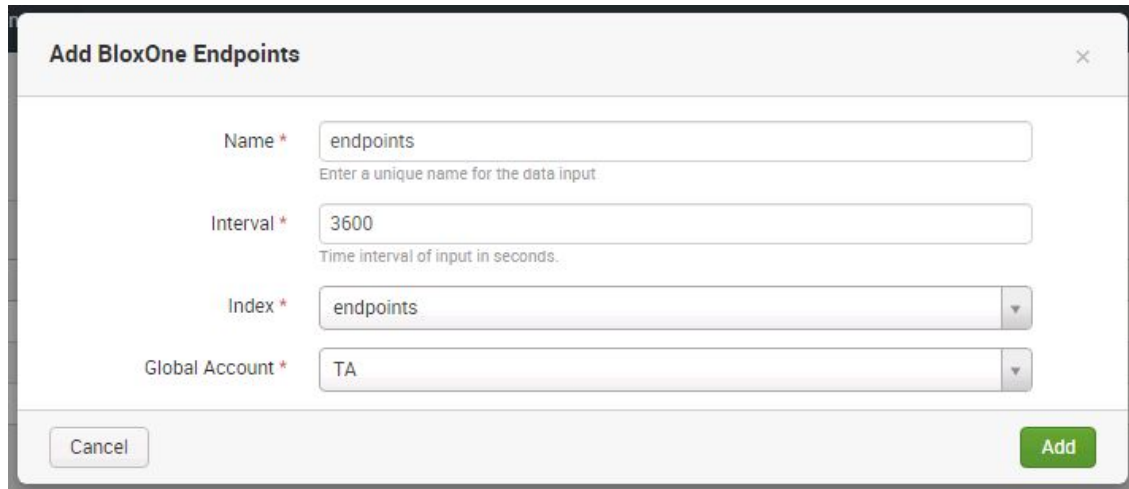
8. In the Infoblox BloxOne Threat Defense Cloud app navigation bar, click **Inputs**.



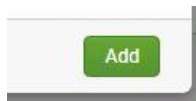
9. On the Inputs page, click **Create New Input**. Then, click **BloxOne Endpoints** in the dropdown menu that is revealed.



10. In the **Add BloxOne Endpoints** dialog box, input the following information:
- **Name**, input the Name **endpoints**.
 - **Interval**, input the value **3600**.
 - **Index**, select the index **endpoints** that was created in steps 4-5.
 - **Global Account**, select the global account **TA** that was created on page 9 of this document.



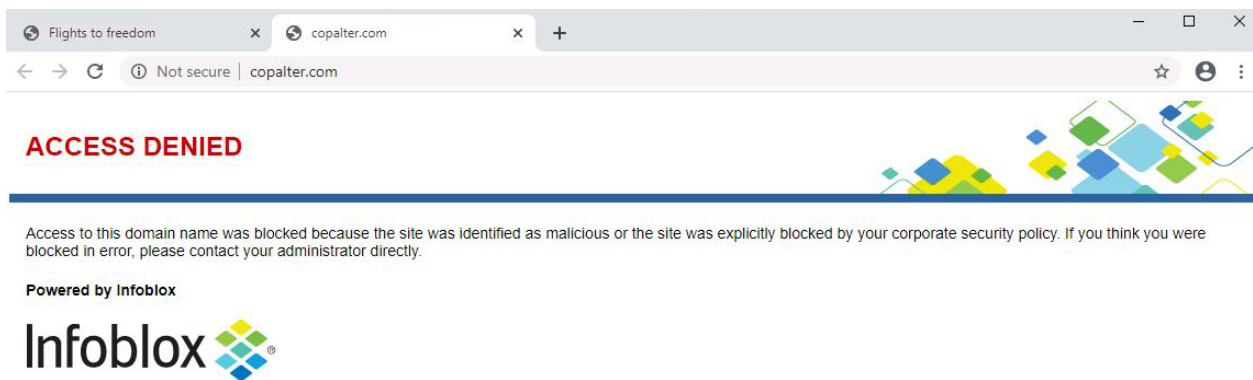
11. Click **Add** to confirm the creation of the input.



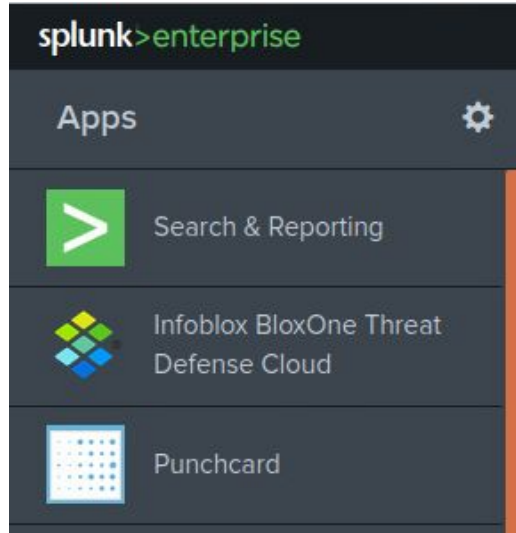
Test the Configuration

To verify that data is being transmitted from the CSP to the Splunk SIEM perform the following steps:

1. Access a device that has **BloxOne Endpoint** installed, or is using an **DNS Forwarding Proxy** as it's primary DNS.
2. Access a malicious website that is being blocked by a security policy in your CSP account. *Note: The screenshot uses the domain copalter[.]com which is an infoblox maintained domain that is blocked for demo purposes.*



3. Access the web interface of the Splunk device.
4. Click the text **Infoblox BloxOne Threat Defense Cloud** located in the list of Apps.



5. If the Infoblox BloxOne Threat Defense add-on was properly configured, the Security Hits page will populate with information on the malicious activity. *Note: the activity may take 2-3 minutes to populate in the database.*

Security Hits Edit Export ...

This dashboard allows to filter security hit by either selecting filter or drill down on any statistic table. To investigate an IOCs, click on it in filtered hits to open a dossier search in csp.

Time Last 1 day	Source All x	Category All x	Threat class All x
Threat property All x	Domain Name (e.g. www.c2.se) All	Query type All x	Device (e.g. 192.168.1.2) All
Network All x	User (e.g. cliu) All	Response Code All x	Severity All x
Confidence All x	Policy Name All x	Feed Name All x	Country All x

Reputation And / Or Behavioral
 Both
 Behavioral
 Reputation

Submit Hide Filters

Filtered Hits

2

Filtered hits over time

Additional Resources

For more information regarding Infoblox or Splunk Enterprise, access these websites:

1. Infoblox Documentation Website: <https://docs.infoblox.com/>
2. Infoblox Website: <https://www.infoblox.com/>
3. Infoblox Community Website: <https://community.infoblox.com/>
4. Splunk Enterprise Website (en_us): https://www.splunk.com/en_us/software/splunk-enterprise.html
5. Splunkbase (Splunk add-on website): <https://splunkbase.splunk.com/>



Infoblox is the leader in modern, cloud-first networking and security services. Through extensive integrations, its solutions empower organizations to realize the full advantages of cloud networking today, while maximizing their existing infrastructure investments. Infoblox has over 12,000 customers, including 70 percent of the Fortune 500.

Corporate Headquarters | 2390 Mission College Boulevard, Ste. 501 | Santa Clara, CA | 95054
+1.408.986.4000 | info@infoblox.com | www.infoblox.com



© 2020 Infoblox, Inc. All rights reserved. Infoblox logo, and other marks appearing herein are property of Infoblox, Inc. All other marks are the property of their respective owner(s).