DEPLOYMENT GUIDE

Integrating BloxOne Threat Defense TIDE IoC into Cisco Firepower Management Center

Table of Contents

Introduction

Cisco Firepower Management Center manages the following Cisco network security solutions:

- Firepower Next-Generation Firewall
- Firepower Next-Generation IPS
- ASA with Firepower Services
- Firepower Threat Defense for ISR
- Advanced Malware Protection (AMP) for Networks

A Cisco Firepower Management Center feature, Threat Intelligence Director, ingests third-party threat feeds and correlates enriched observations from Cisco security solutions to detect and alert on security incidents. By converting intelligence into actionable indicators of compromise, you can block or monitor more threats, reduce the number of alerts you must review, and improve your overall security posture.

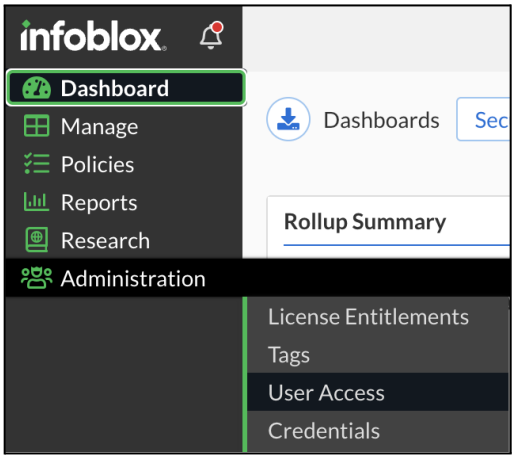
This deployment guide shows you how to upload the Infoblox BloxOne Threat Defense TIDE indicators into Cisco Firewall Management Center.

Requirements

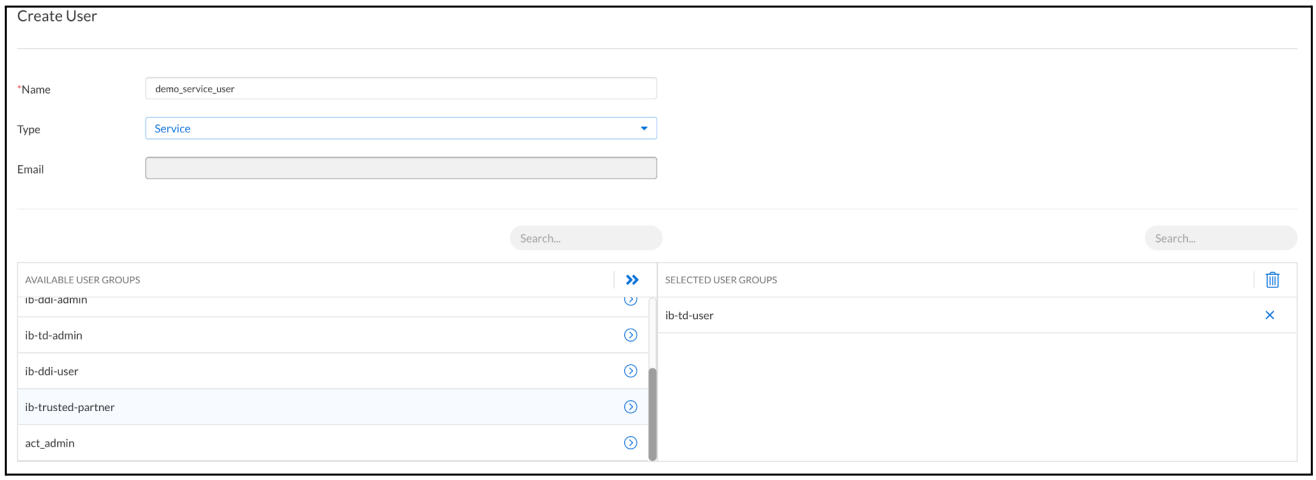
- Access to Infoblox Cloud Services Portal TIDE (Threat Intelligence Data Exchange).
- Cisco Firepower Management Center version 7.2.1 or above.

BloxOne TD Instructions

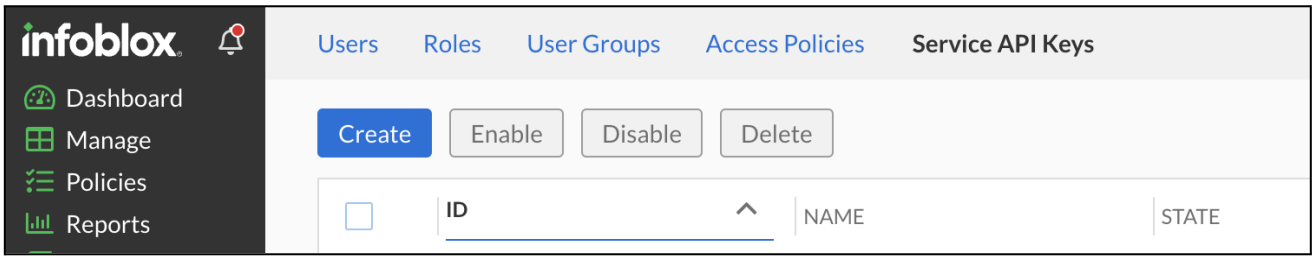
1. Log into the csp.infoblox.com website to acquire a Service API key to access the threat indicators.
2. Navigate to **Administration → User Access.**



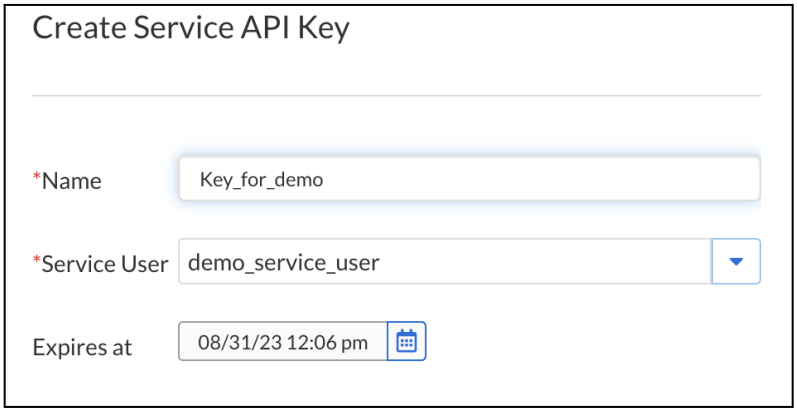
3. Under **Users** tab, click on **Create**, this opens the **Create User** window. Input the following:
    - **Name**: Input a name for this user.
    - **Type**: Select **Service** in the dropdown menu.
    - **Available User Groups**: In this section, select the appropriate user group/s which will inherit the permissions and roles to this service user. Click **Save and Close**.



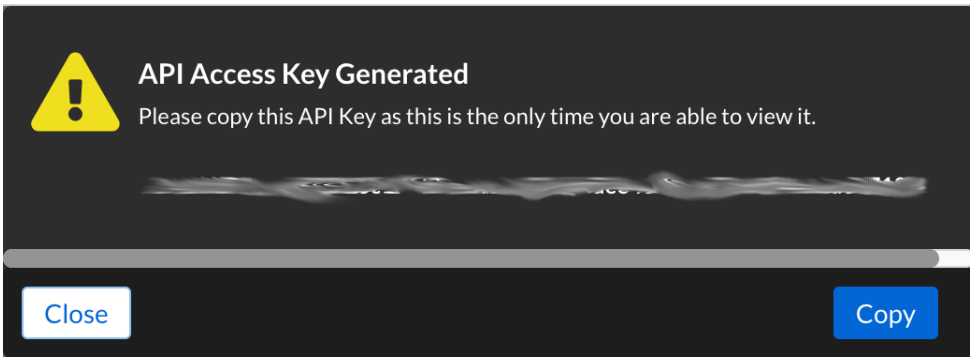
4. Click on the **Service API Keys** tab.



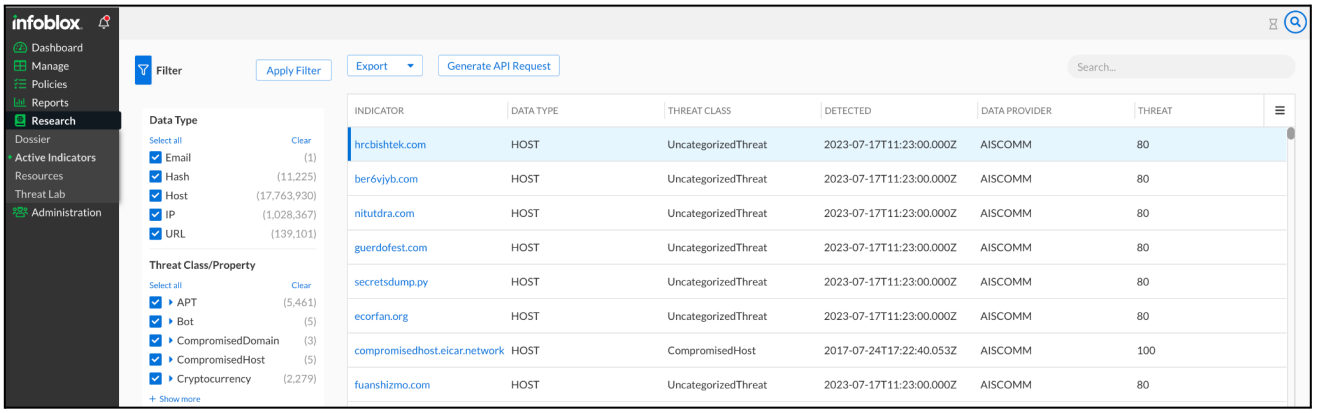
5. Click on **Create**. Type in a **name**, select the **Service User** you created earlier and select an **expiration date**. Click **Save and Close**.



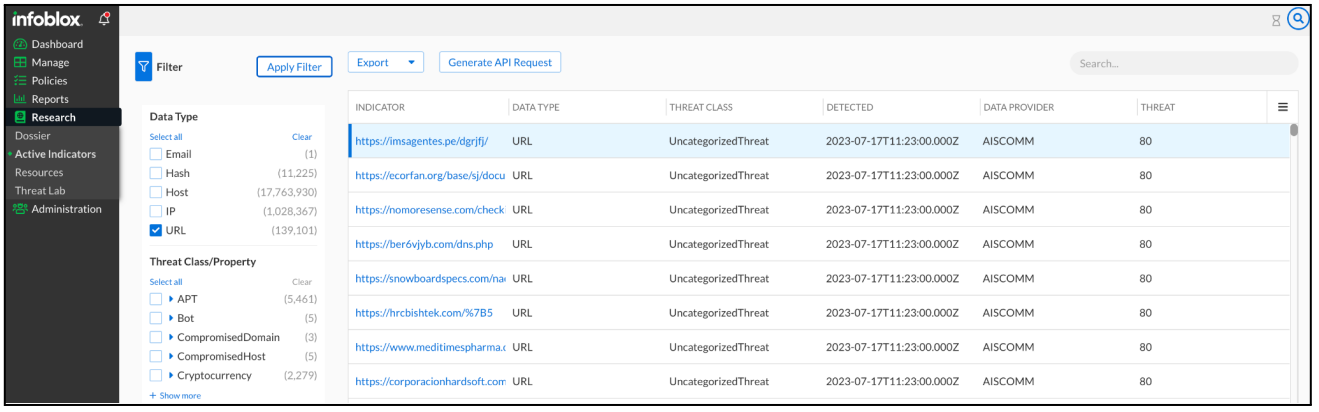
6. Copy the API key and save it to a file. This will be your only time that you can do so.



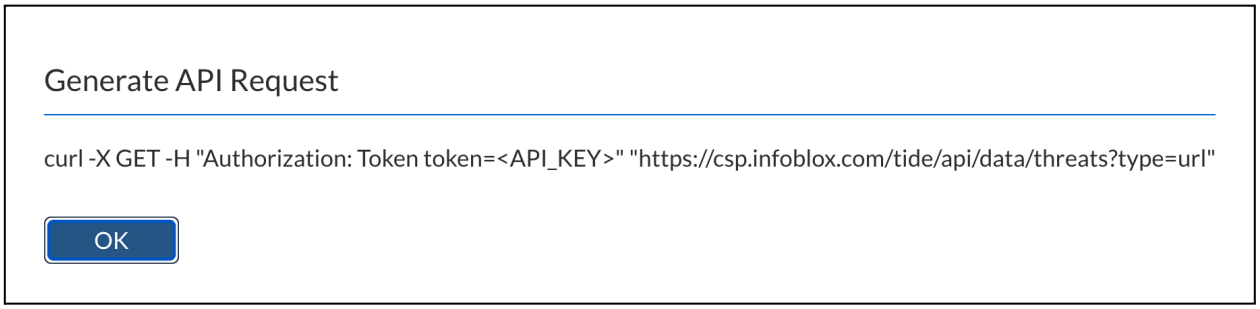
7. You are now ready to create the URL to download the IOCs that you request. Navigate to **Research → Active Indicators**.



8. Clear all of the check marks and then check the items that you want and then click on **Apply Filter**. For example, select **URL**.



9. Click on **Generate API Request**. This button will show you the basis of the API URL that you will add to the sources in Cisco Firewall Management Center. The screenshot below is an example.



10. Take the segment starting with HTTPS and do the following:

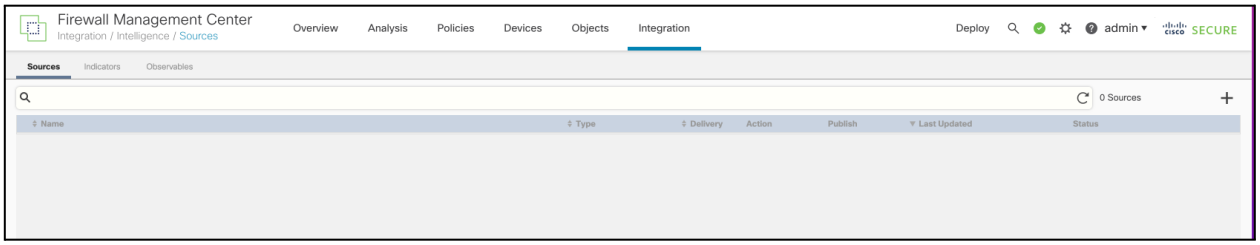
    - https://**<Service API Key>**@csp.infoblox.com/tide/api/data/**state**/threats?type=url**&rlimit=<# of IOCs>&data_format=STIX**

    - In the line above in bold, you add the service API key that was previously generated, the state parameter which provides the IOCs that are currently active, the number of IOCs, and the data format which is STIX.

Cisco Firepower Instructions

1. Log into the Cisco Firewall Management Center.

2. Click on **Integration → Intelligence → Sources.**

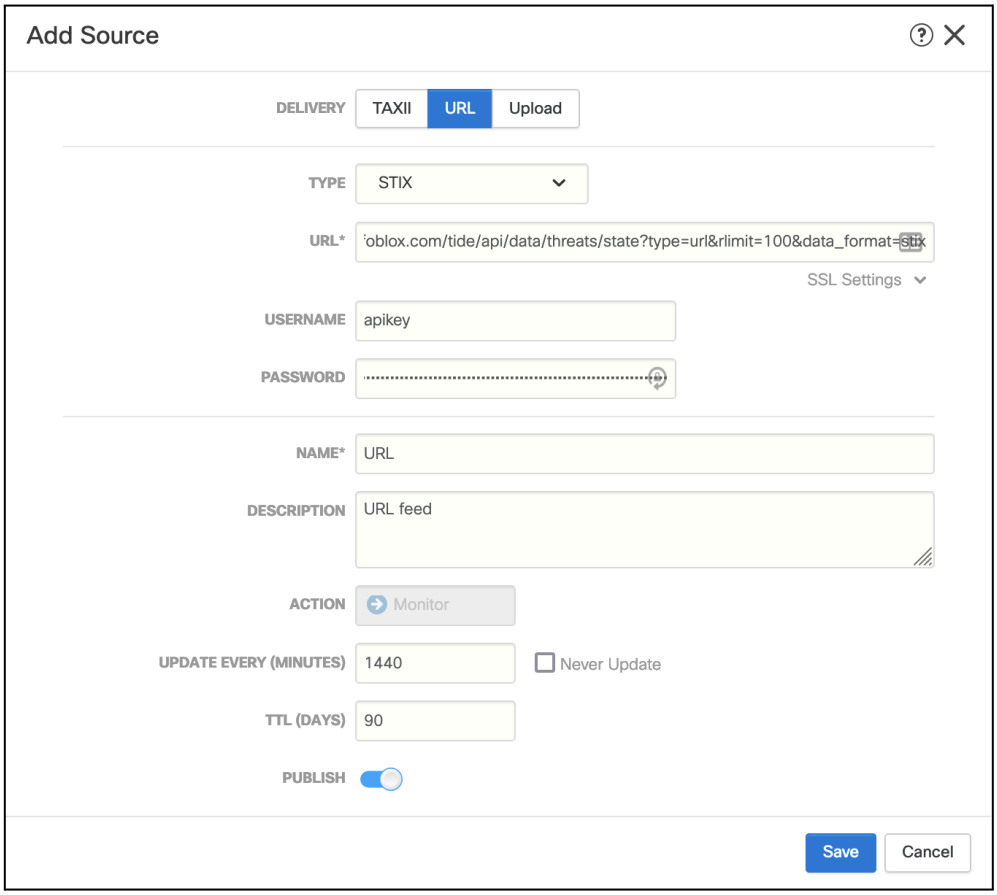


3. Click on the '**+**' button on the right side of the screen to add a source. Select delivery type of URL. Add the URL that was created in step 9. Here is an example:

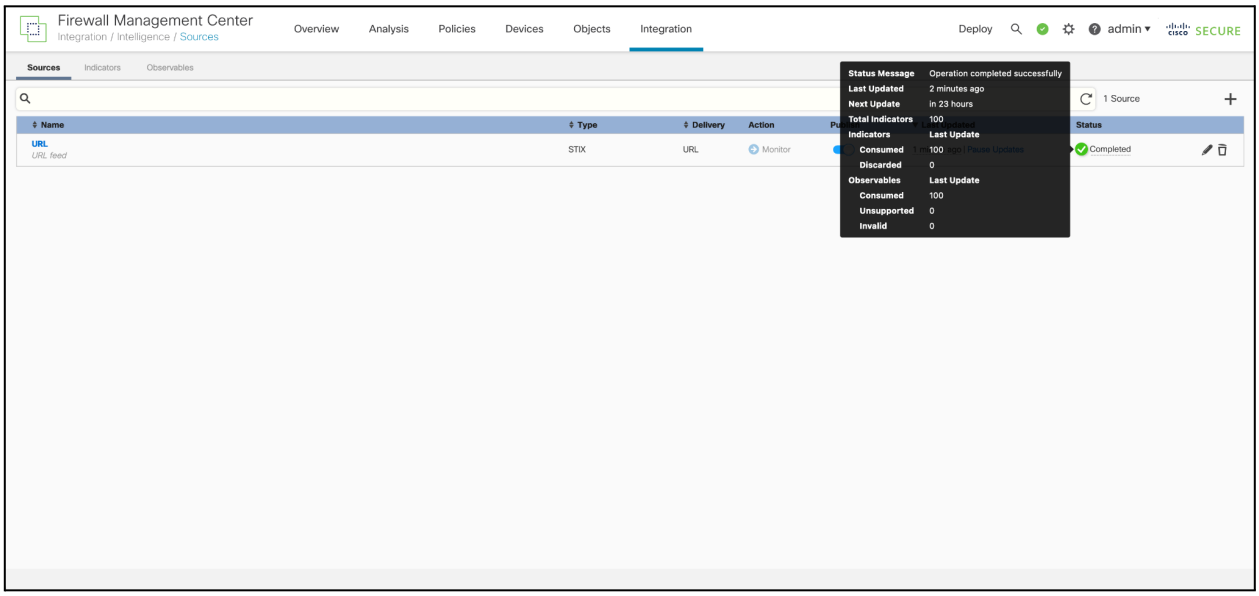
    - https://<service api key>
      @csp.infoblox.com/tide/api/data/threats/state?type=url&rlimit=100&data_format=stix

    - This URL will access 100 URL IOCs and output them in STIX format.

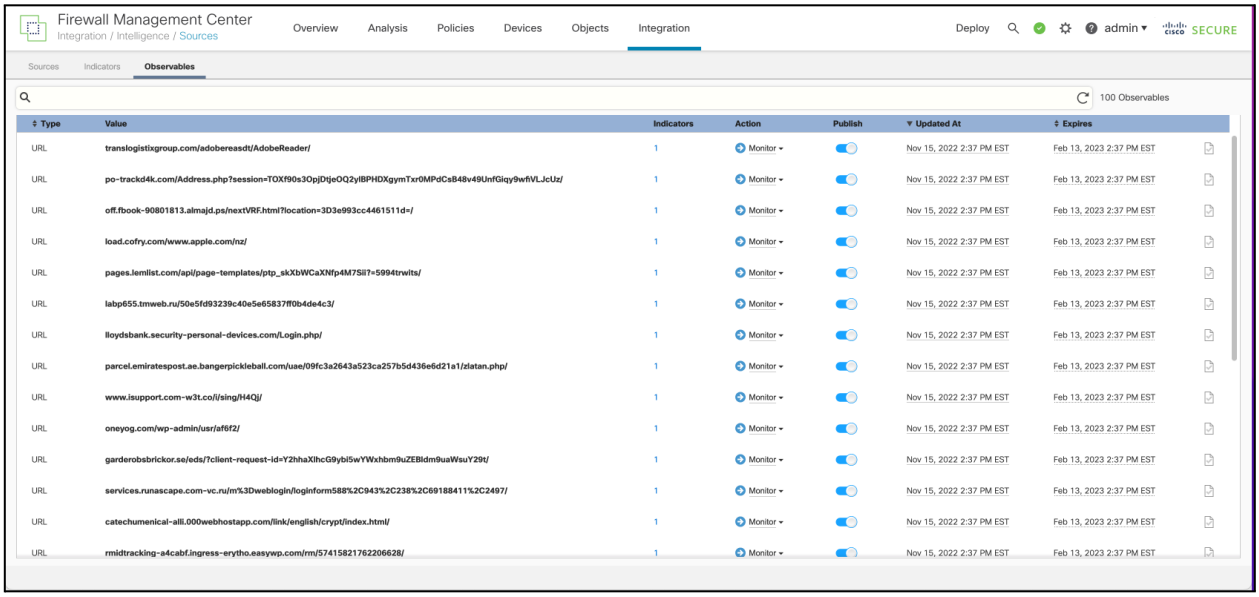
- Input the **username** of the api key.
- The **password** is the service api key.
- Input a **name** of the feed.
- Optionally, input a **description**.
- Input an **update interval**. This tells Firewall Management Center how often to query csp.infoblox.com for updates.
- Click '**Save**'.



4. Refresh the Sources screen and click on the status for results of the download.



5. Click on the Observables tab to get the results.



Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, we provide real-time visibility and control over who and what connects to your network, so your organization runs faster and stops threats earlier.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054
+1.408.986.4000
www.infoblox.com

© 2023 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).