Infoblox
CONTROL YOUR NETWORK

DEPLOYMENT GUIDE

Integrating ActiveTrust TIDE IoC into Cisco Firepower Management Center

Contents

Introduction 3
Requirements 3
ActiveTrust Configuration Instructions 4
Cisco Threat Intelligence Director Configuration Instructions 6
Viewing Status and Data 9

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.

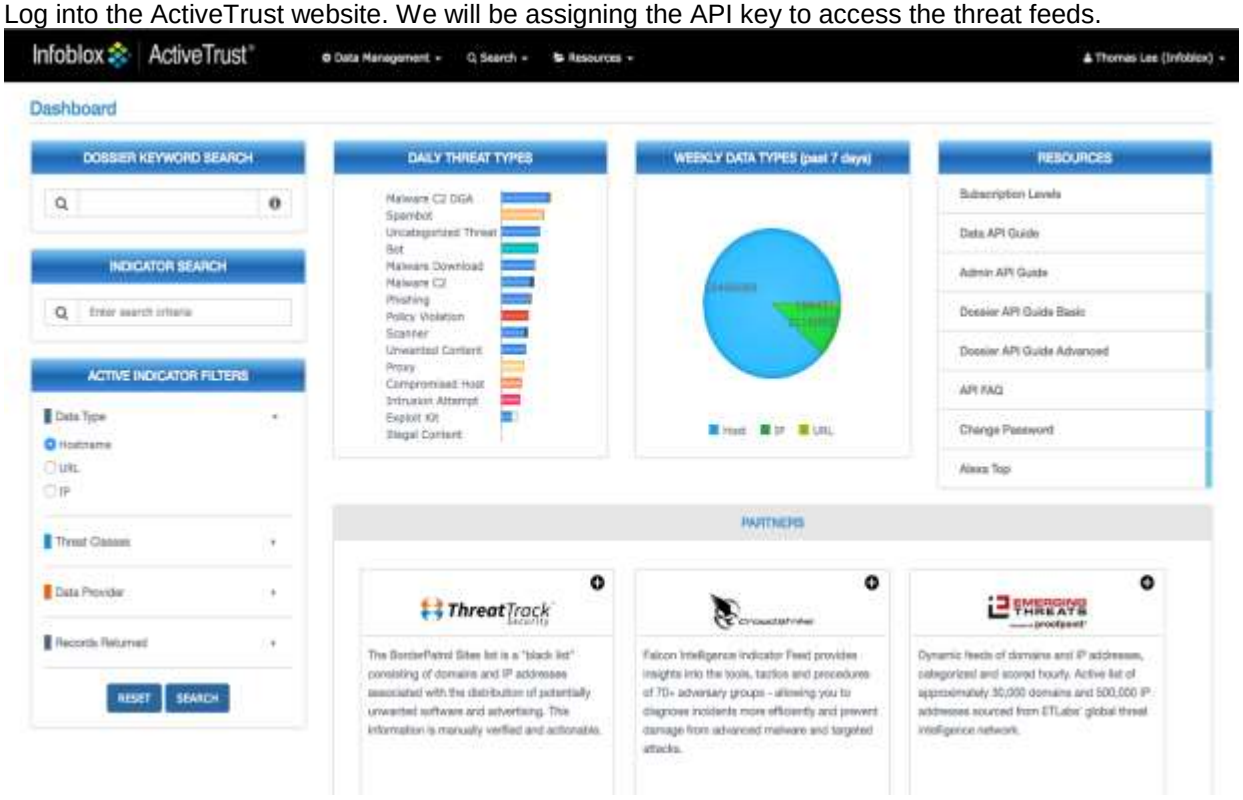
This deployment guide shows you how to upload the Infoblox ActiveTrust TIDE feeds into Threat Intelligence Director.

Requirements

- Access to ActiveTrust TIDE.
- Cisco Firepower Management Center version 6.2.2 or above.

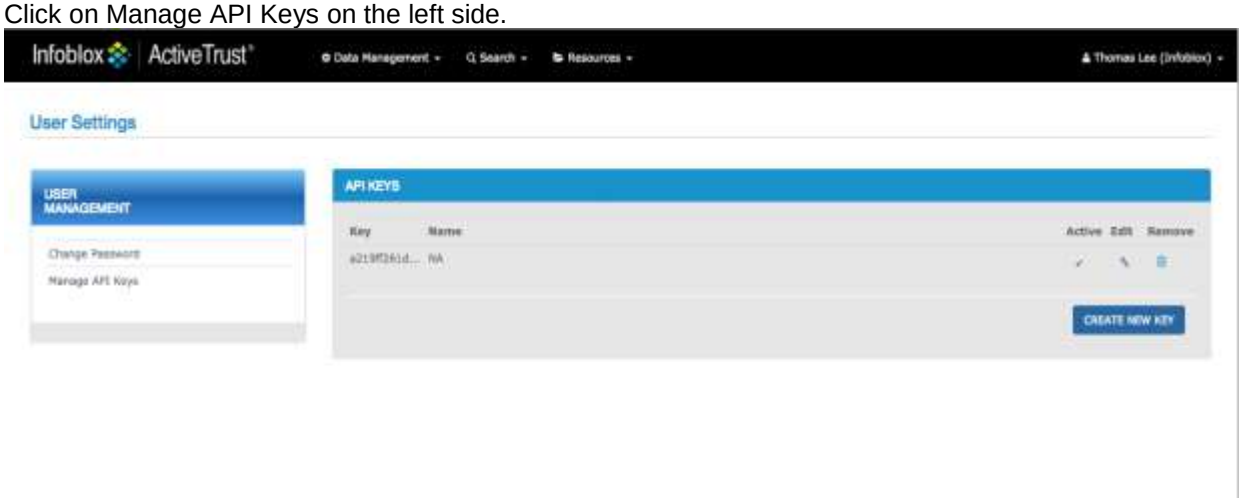
ActiveTrust Configuration Instructions

1. Log into the ActiveTrust website. We will be assigning the API key to access the threat feeds.

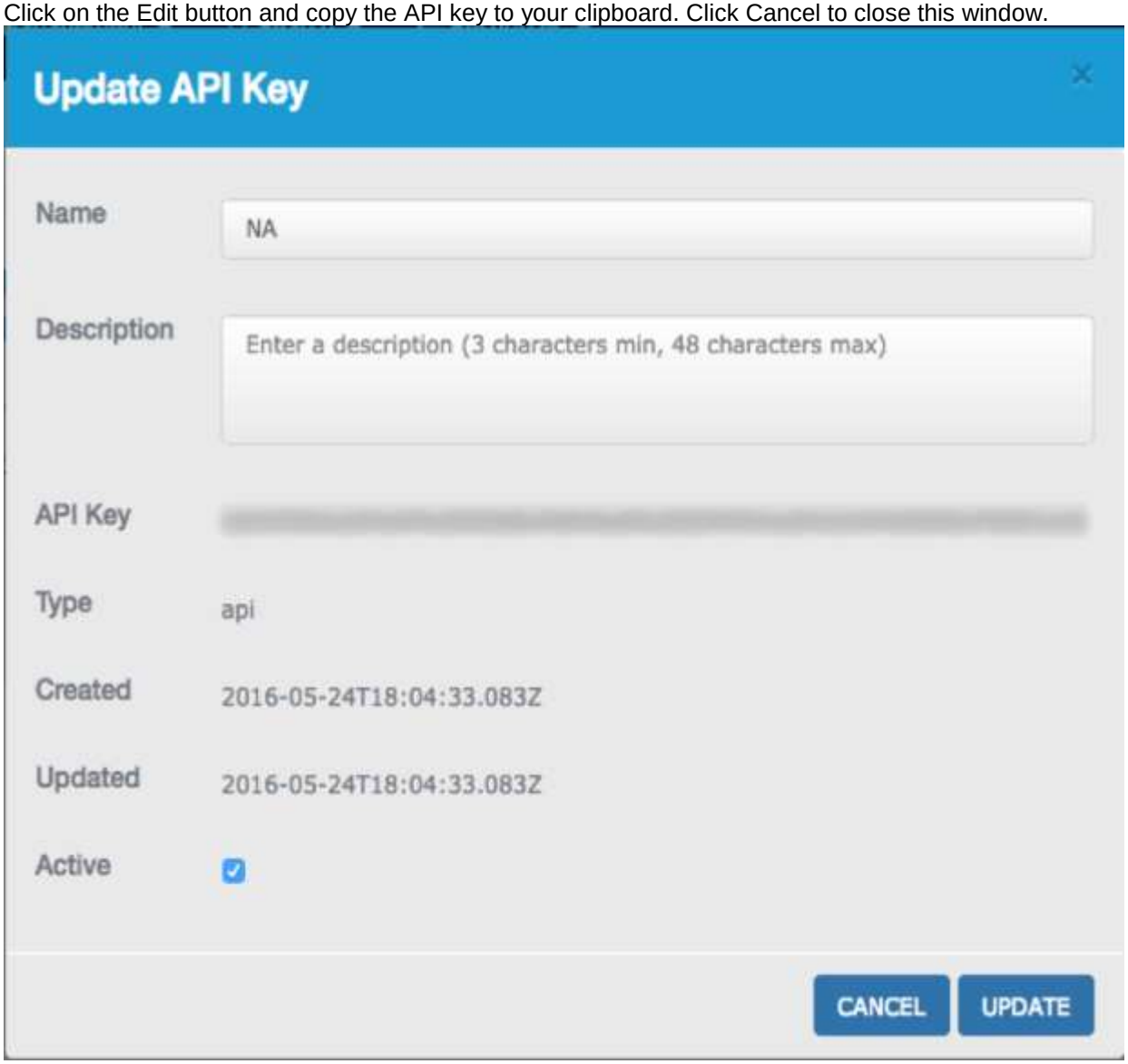


2. In the upper right corner of the screen, click on the username and select User Settings.

3. Click on Manage API Keys on the left side.



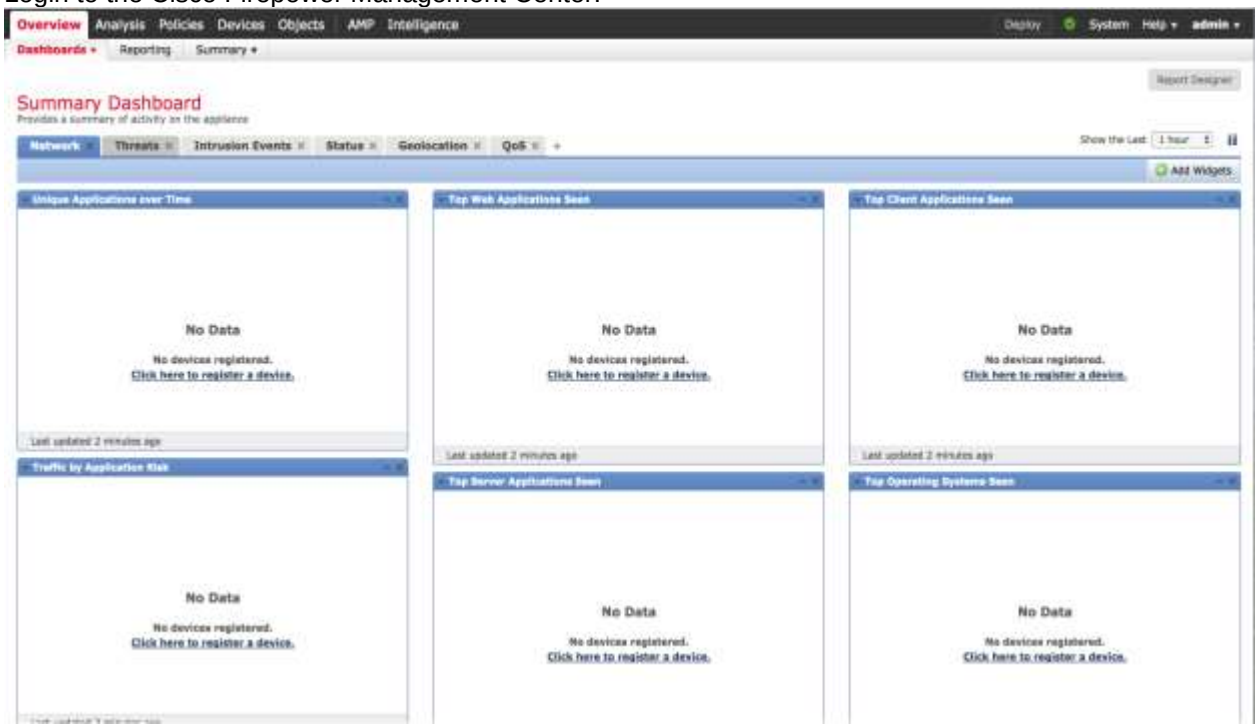
4. Click on the Edit button and copy the API key to your clipboard. Click Cancel to close this window.



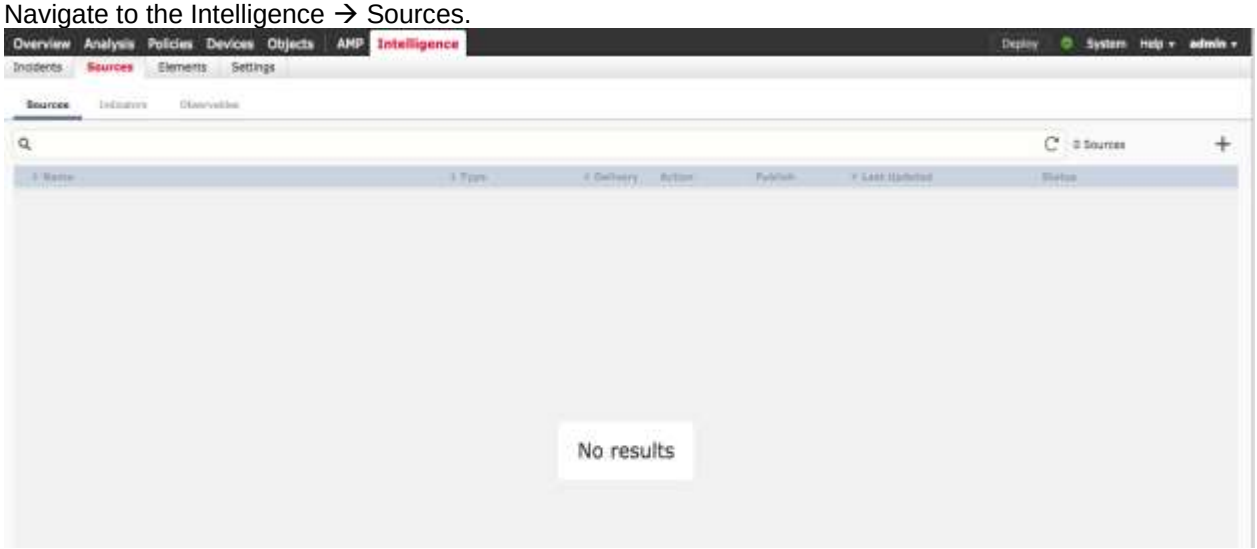
5. Refer to the Dossier and TIDE quick start guide to assign the API key and creation of URLs.

Cisco Threat Intelligence Director Configuration Instructions

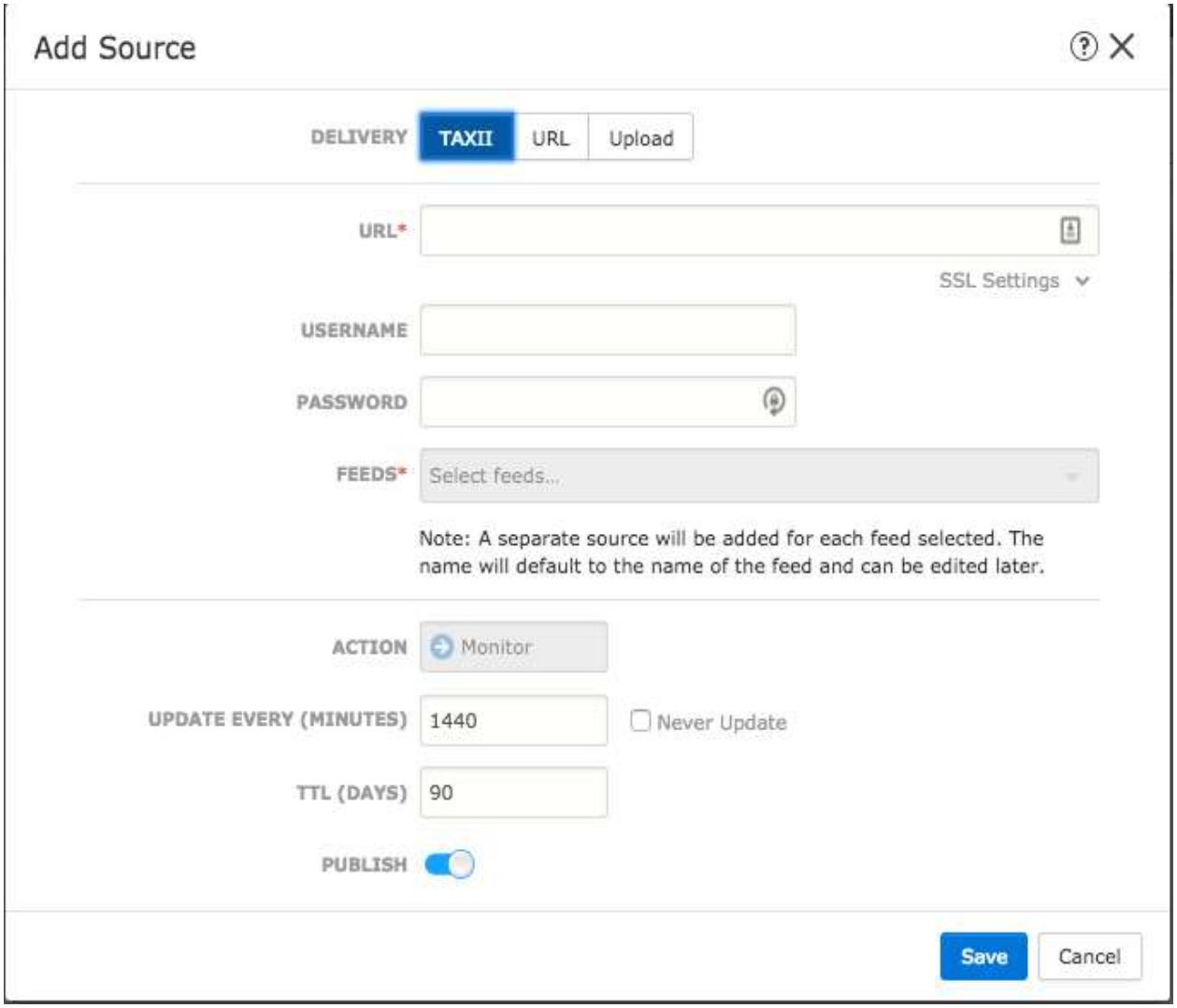
1. In this example, you will need to create three request URLs: one for bad hosts, bad IPs, and bad URLs. They will look similar to the following:
    a. **host:** https://<api key> @platform.activetrust.net:8000/api/data/threats/host?data_format=stix&rlimit=1000
    b. **IP:** https://<api key> @platform.activetrust.net:8000/api/data/threats/ip?data_format=stix&rlimit=1000
    c. **URL:** https://<api key> @platform.activetrust.net:8000/api/data/threats/url?data_format=stix&rlimit=1000
2. To complete the request URLs above, you will need to prepend your user-specific API key and add an @ before the word platform. You will need to add the type of data before the ?data_format word. In the cases above, the types of data are: host, ip, and url. Lastly, you can adjust the number of records downloaded from the feed by modifying the limit value at the end of the URL. Refer to the filtering fields within the threat API section for additional ways filtering the feeds.
3. Login to the Cisco Firepower Management Center.



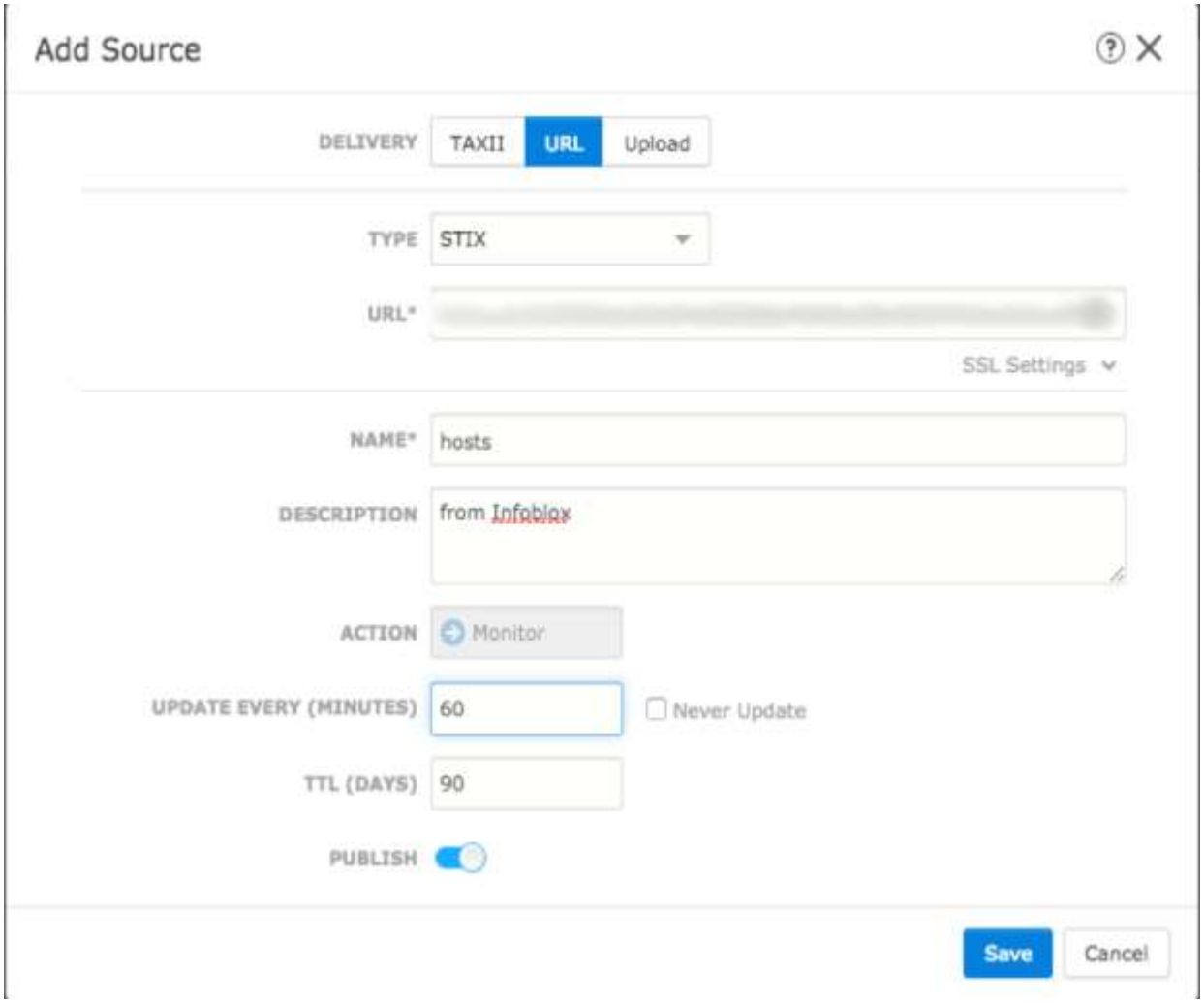
4. Navigate to the Intelligence → Sources.



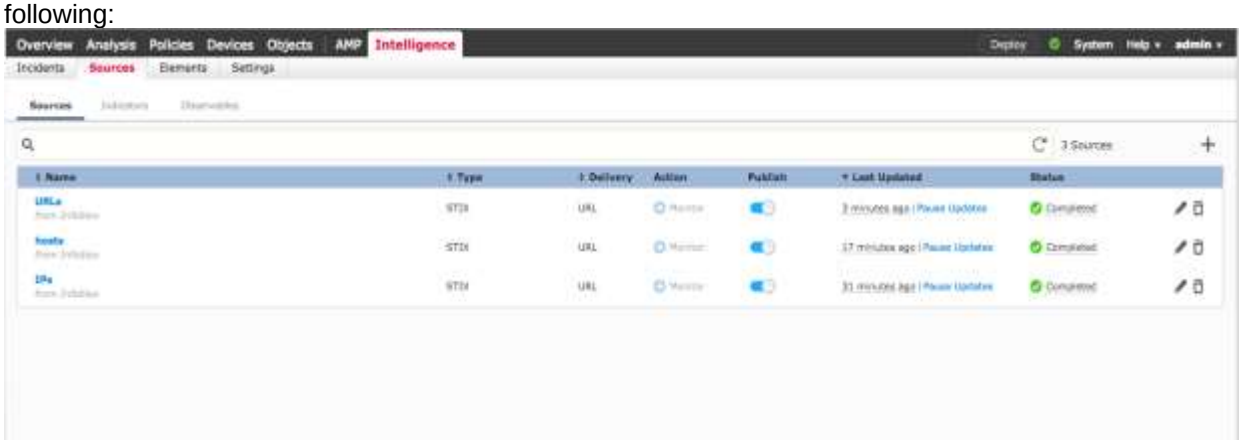
5. Click on the + button to add a source.



6. Click on the URL delivery button, enter one of the three URLs that are similar to the ones listed in step 1, enter the name of the source, enter a comment, and change the update time if you wish. 60 minutes is the minimum time. Click Save when done.

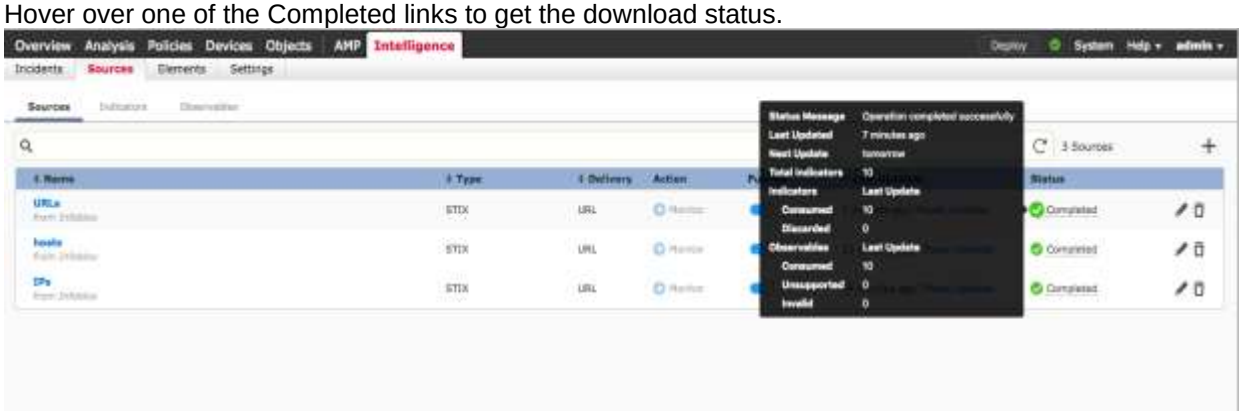


7. Repeat the above step to add IP and host feeds. When done the intelligence source should look like the following:

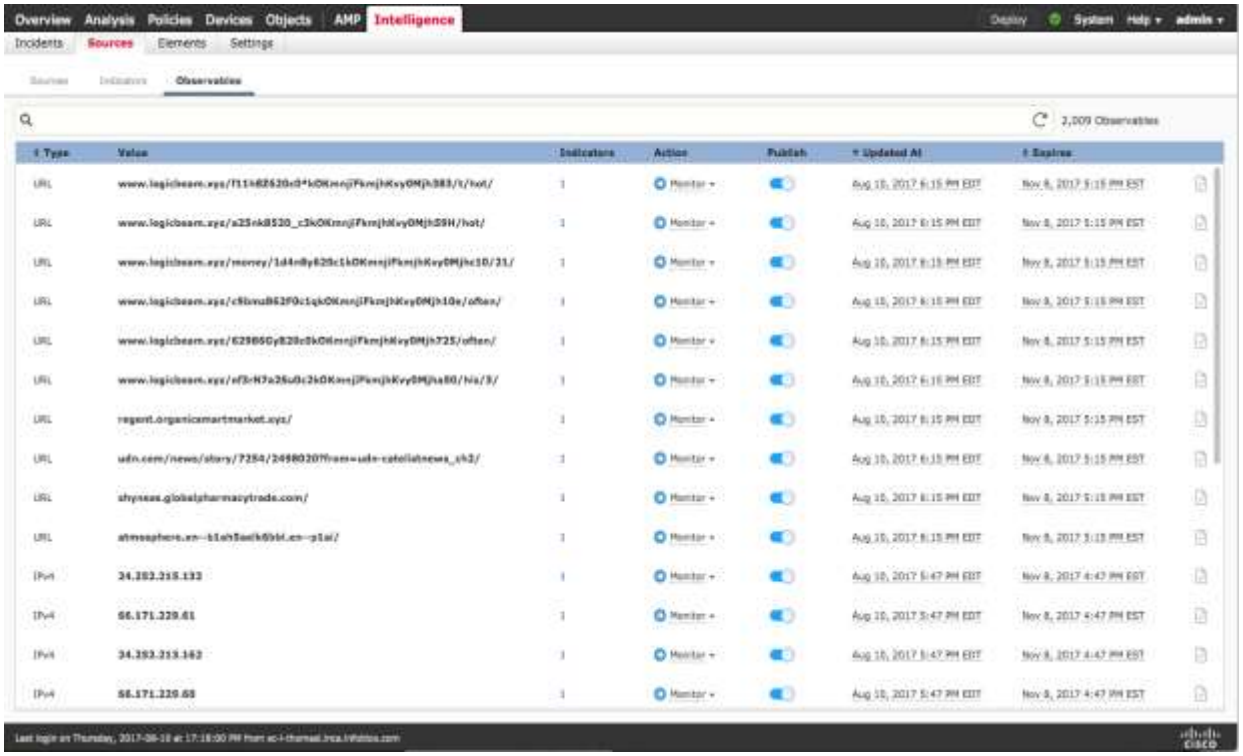


Viewing Status and Data

1. Hover over one of the Completed links to get the download status.



2. Click on the Observables tab to view the IoCs downloaded.



3. You can also search specific IoCs like an IP range. For example, set the type to IPv4 and set a value to 109.67. You may see the following:

4. Click on one of the Indicators link to see that the IoC is related to an Indicator for a spambot.

5. Click on the Source link and the screen shows you the source for the Indicator, which in this case is the ActiveTrust TIDE IP feed you configured above.