DEPLOYMENT GUIDE

# Infoblox Integration with Splunk Phantom

# Table of Contents

# Introduction

Infoblox with Splunk Phantom allows for security and incident response teams to leverage the power of a Security Orchestration, Automation and Response platform paired with DNS threat intel and granular network control. Infoblox's Dossier and DNS security offerings empower Splunk Phantom's ability to locate malicious URLs, eradicate threats, and prevent access to dangerous domains. Thus, improving your security posture while maximizing your ROI in both products.

# Prerequisites

The following is a list of prerequisites for full functionality of the Infoblox and Splunk Phantom integration:

Infoblox:

1. NIOS 8.3 or higher
2. NIOS license
3. API Only user
4. DNS, Response Policy Zone, and DHCP licenses for NIOS

1. BloxOne™ Threat Defense license (one of the following):
    - BloxOne™ Threat Defense Advanced
    - BloxOne™ Threat Defense Business - Cloud
    - BloxOne™ Threat Defense Business - On Premise
2. Pre-configured required services: DHCP, DNS, IPAM, RPZ, and Threat Analytics
3. NIOS API user with the following permissions (access via API only):
    - All IPv4 Host Addresses - RW
    - All IPv4 DHCP Fixed Addresses/Reservations - RW
    - All IPv6 DHCP Fixed Addresses - RW
    - All IPv6 Host Addresses - RW
    - All A records - RW
    - All AAAA Records - RW

- All PTR Records - RW
- All DNS Views - RW
- All Response Policy Zones - RW
- All Response Policy Rules - RW

Splunk Phantom:

1. Installed and configured Splunk Phantom device
2. Splunk Phantom license
3. Configured Office 365 App
4. Configured Service Now App
5. User access with the following permissions:
    - Basic Permissions:
        - Apps: View / EditAssets: View / Edit
            - Playbooks (optional) : Edit / View/ Execute / Edit Code
        - Label Permissions
            - Ingested Email List (used for testing) : Edit / View

## Known Limitations

For full functionality of the Infoblox requires the full list prerequisites, the Splunk Phantom apps may or may not fully work without them. For example, the Splunk App Infoblox DDI is reliant on an integrated Configuration Management Database (CMDB) such as Service Now to associate a device with an email. Without a configured CMDB or an integrated Email Server the Splunk Phantom App Infoblox DDI cannot be fully utilized.

## Best Practices

As with most infrastructure changes to a production environment, it is recommended that a lab environment is utilized to test the functionalities and impact of any changes being made. Please refer to the NIOS Administration guide about other best practices, limitations, and details on how to administrate your Infoblox grid.

## Workflow

Use the following workflow to deploy this integration:

1. Create Response Policy Zone in Infoblox
2. Create phantom_id Extensible Attribute
3. Acquire Dossier API key
4. Download and Configure Splunk Phantom Infoblox Apps
5. Test App functionality (Optional)

## Splunk Phantom Apps

This document describes how to install and configure Infoblox DDI and Infoblox Dossier Splunk Phantom apps. These apps were created and are supported by Splunk for use by our joint customers. If support is requested for a Splunk Phantom app, seek assistance at the Splunk community website: https://www.splunk.com/en_us/community.html

For all other Infoblox related Assistance please visit the Infoblox community website: https://community.infoblox.com/

## Extensible Attributes

Below is a table consisting of all extensible attributes utilized in this integration.

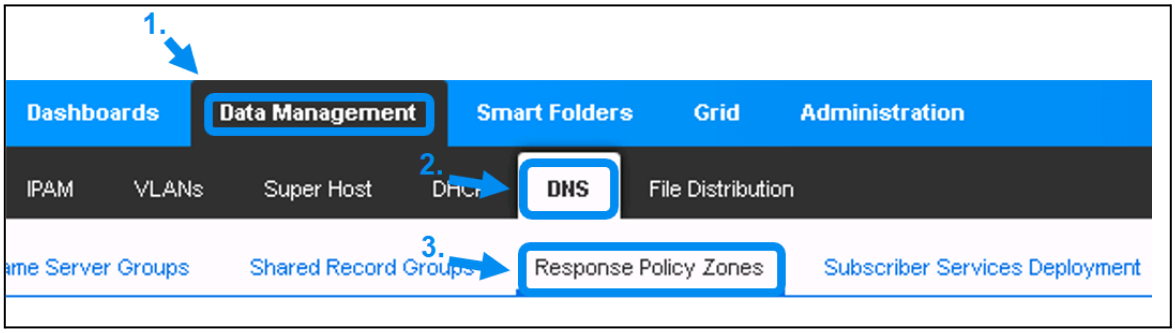
| Name | Description | Type |
|---|---|---|
| phantom_id | Extensible Attribute that is populated with a value representing a case id. | String |

## Infoblox Configuration

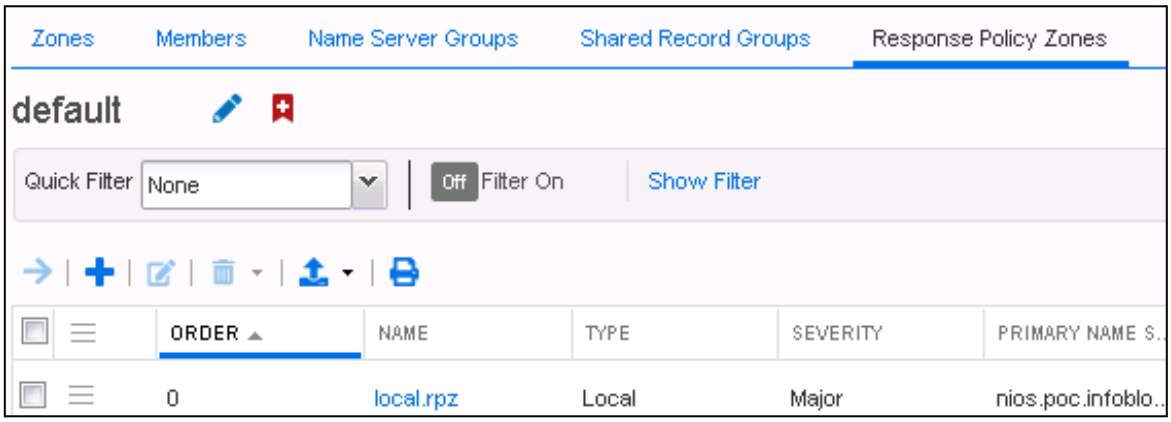
### Create phantom Response Policy Zone in Infoblox

To create a Response Policy Zone in Infoblox follow these steps:

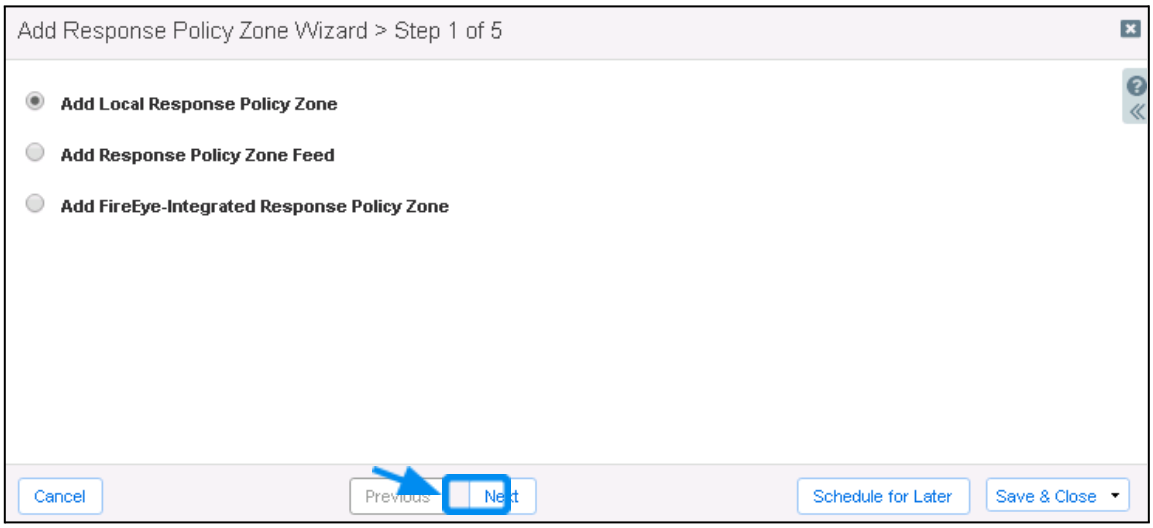
1. Navigate to **Data Management** > **DNS** > **Response Policy Zones**.



2. Click the **+ Icon**




3. In the following **Add Response Policy Zone** Wizard, click **Next**.




4. Give the Response Policy Zone a Name, then click **Save & Close**.

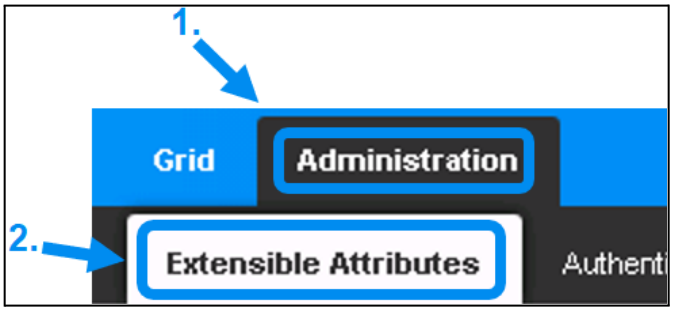
5. When prompted, restart any services if needed, click **Restart** located on the yellow banner at the top of the screen. Then, click Restart on the following window.


## Create phantom_id Extensible Attribute

Create an Extensible Attribute for the integration by performing the following steps:

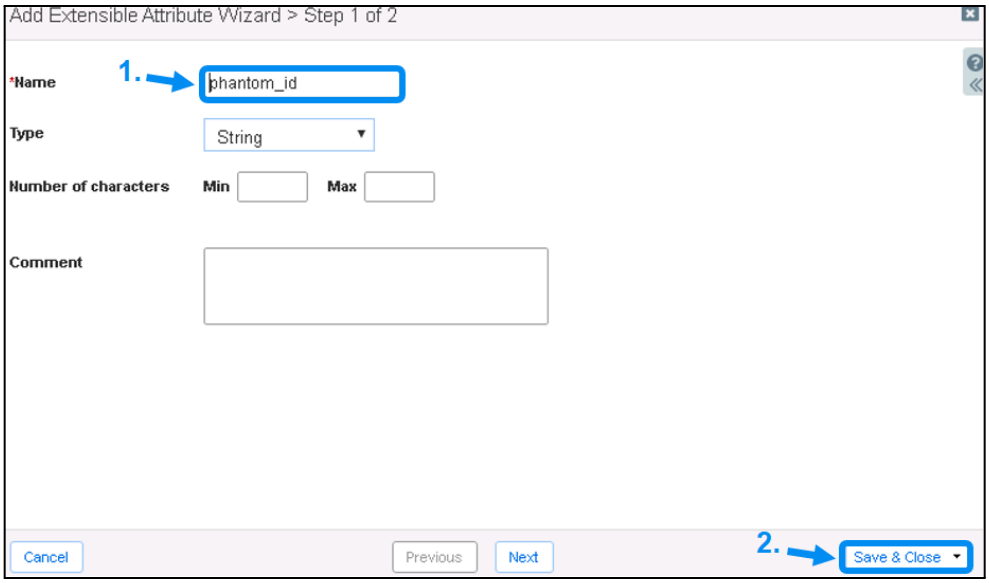
**Note: This Extensible Attribute is case-sensitive. This extensible attribute is required for inputting case ID into Infoblox from Phantom.**

1. Navigate to **Administration** > **Extensible Attributes**.




2. Click the **+ icon** located above the checkbox column.

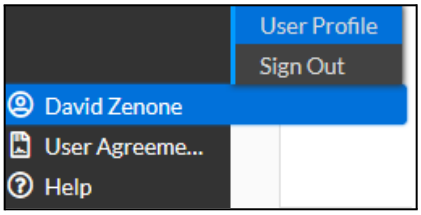

3. Input the name phantom_id. Then, click **Save & Close.** Please note the extensible attribute **phantom_id** is case-sensitive.




## Acquire Dossier API Key

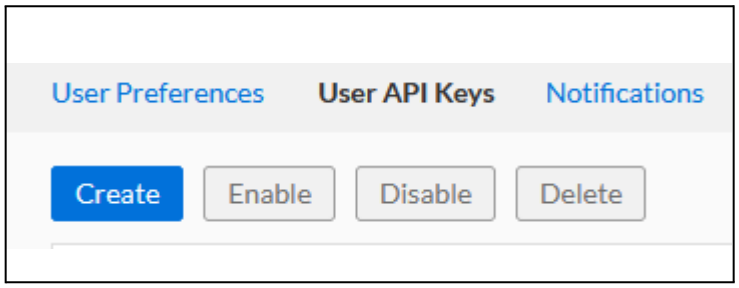
To acquire a Dossier API Key, perform the following steps:

1. Log into the Infoblox CSP. Once logged in, highlight your **username** located in the bottom left of the navigation panel, then click on **User Profile** in the list that is revealed.



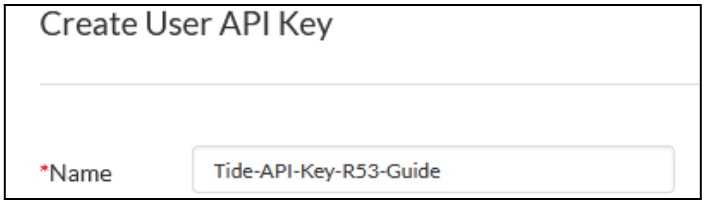

2. On the **User Profile** page, click the **User API Keys** tab located at the top of the page.

3. Click the **Create** button to begin creating an API key.



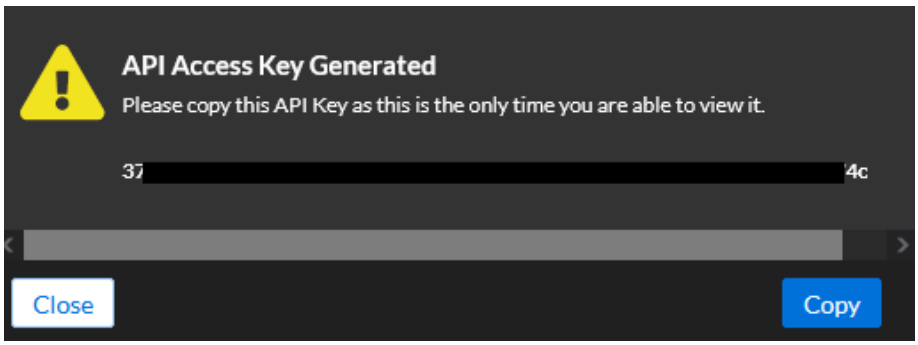

4. On the **Create Service API Key** panel that is revealed, give the API Key a Name.

5. (Optional) Change the API Keys expiration date by changing the **Expires** at field.




6. Click **Save & Close** to confirm the creation of the API key

7. After clicking Save & Close, a dialog box will appear. Copy the API key from this dialog box and save it to a text file for use later. Please note that once you close this dialog box, the API key will no longer be accessible.

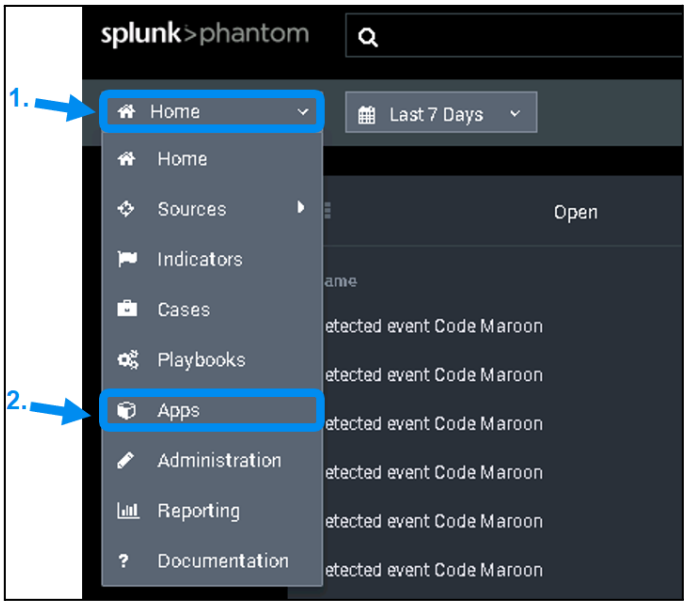


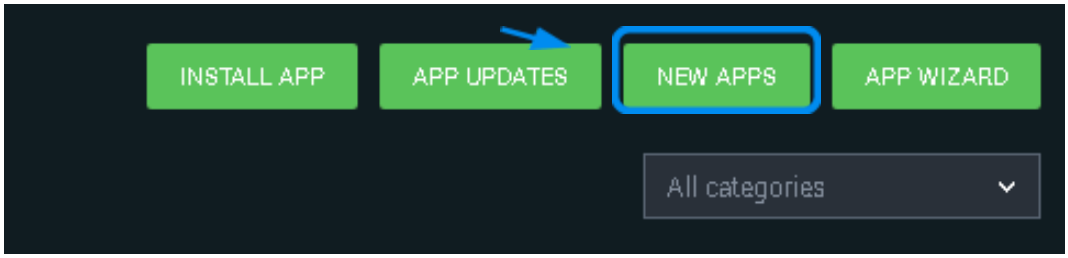

# Splunk Phantom Configuration

## Download and Configure Splunk Apps

To install the Splunk Phantom apps required for the integration, perform the following steps:

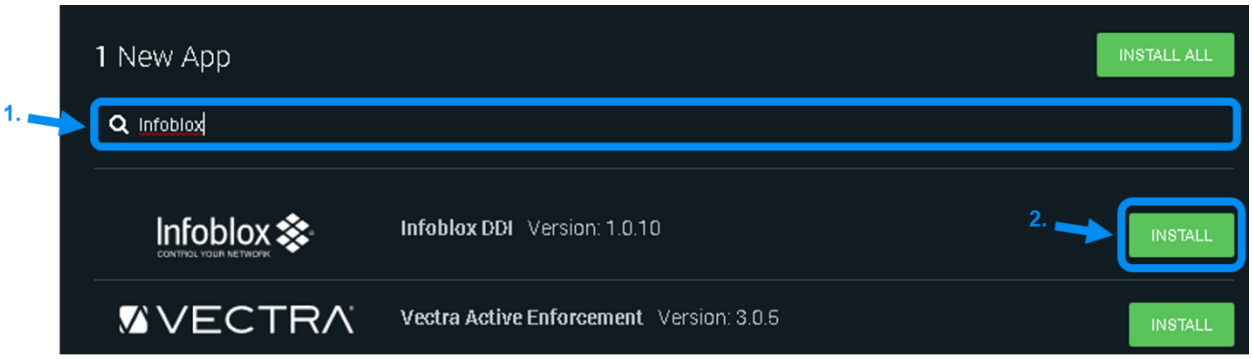
1. Access the Splunk Phantom web interface. Once logged in, click the navigation menu located on the top right of the window, then click **Apps**.Click **New Apps** located on the top right of the **Apps** page.



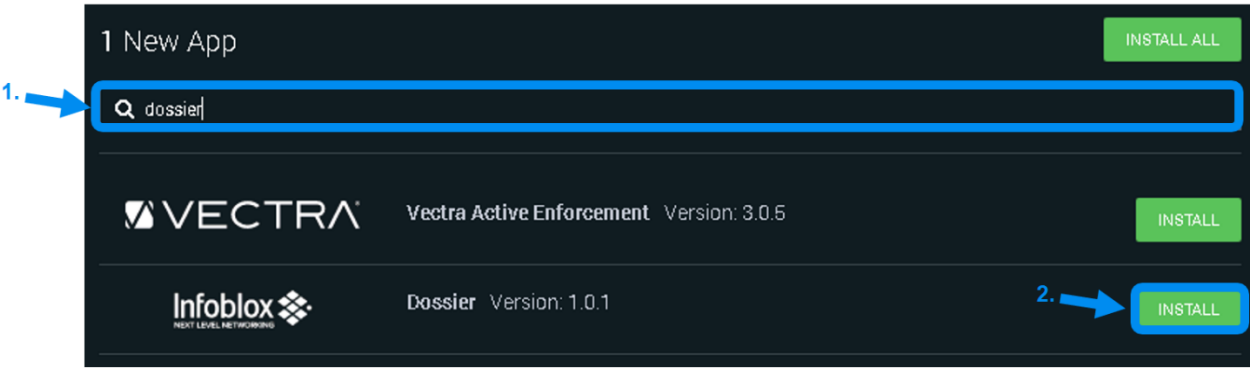



2. Click **New Apps** located on the top right of the Apps page.

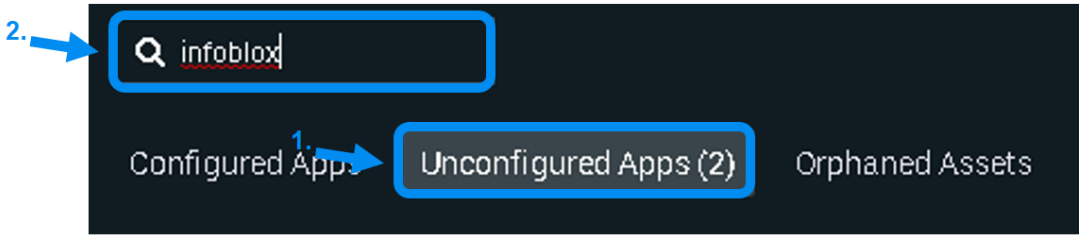
3. Type **Infoblox** in the Search window that is revealed. Then click the **Install** button that is associated with the Infoblox DDI App.



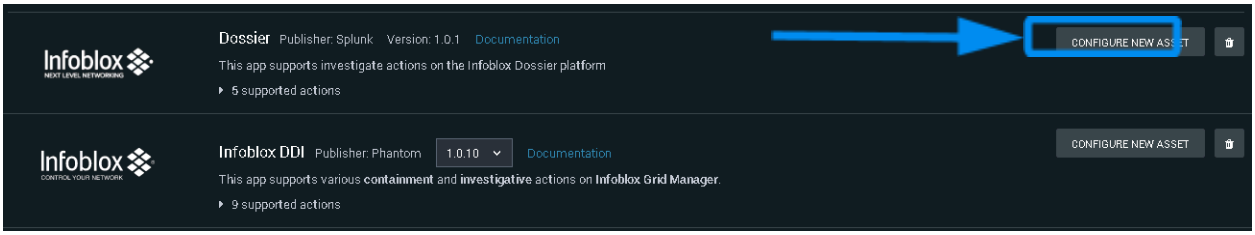

4. In the same window, type **Dossier** in the text box. Then click the **Install** button associated with the Infoblox Dossier app.



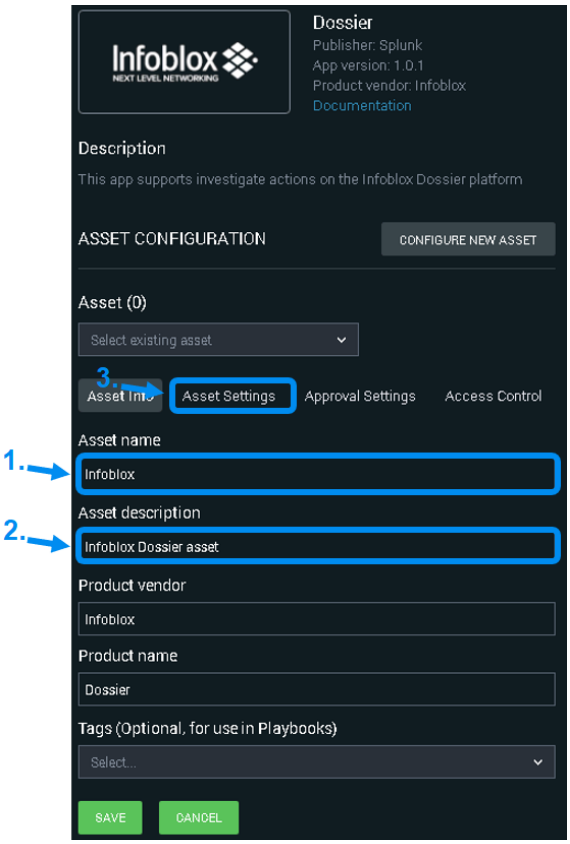

5. On the top left of the App window, Click **Unconfigured Apps**, then type in **Infoblox** in the search box.



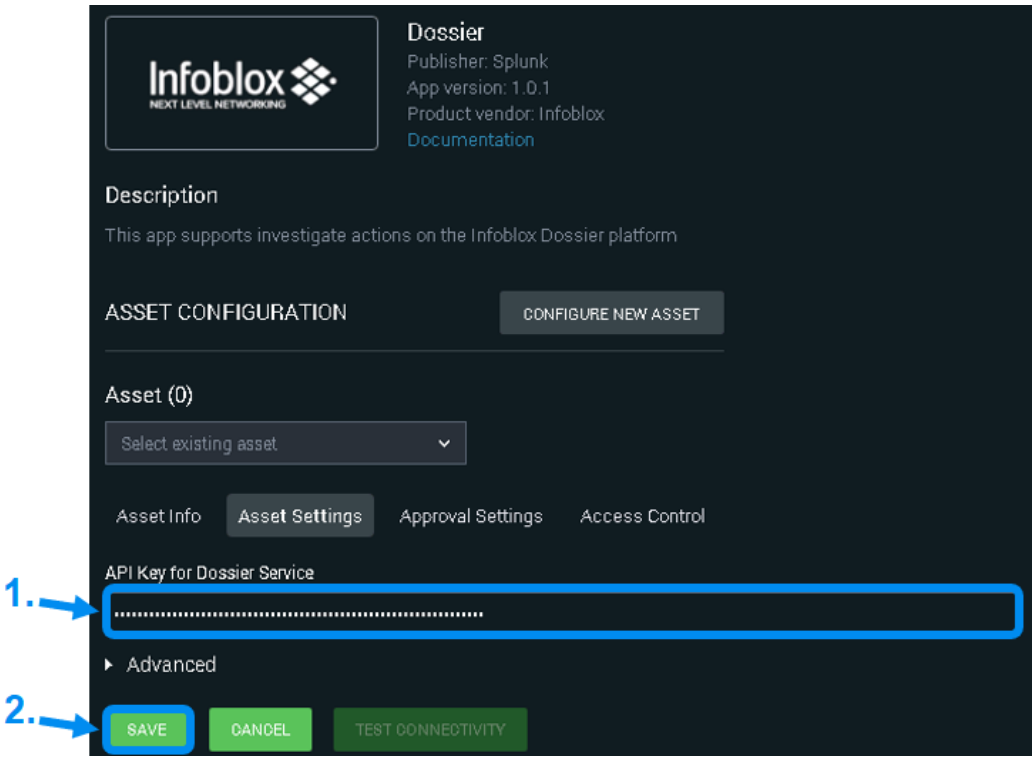

6. Locate the two newly installed apps Dossier and Infoblox DDI. Click the button titled **Configure New Asset** for the App Dossier.



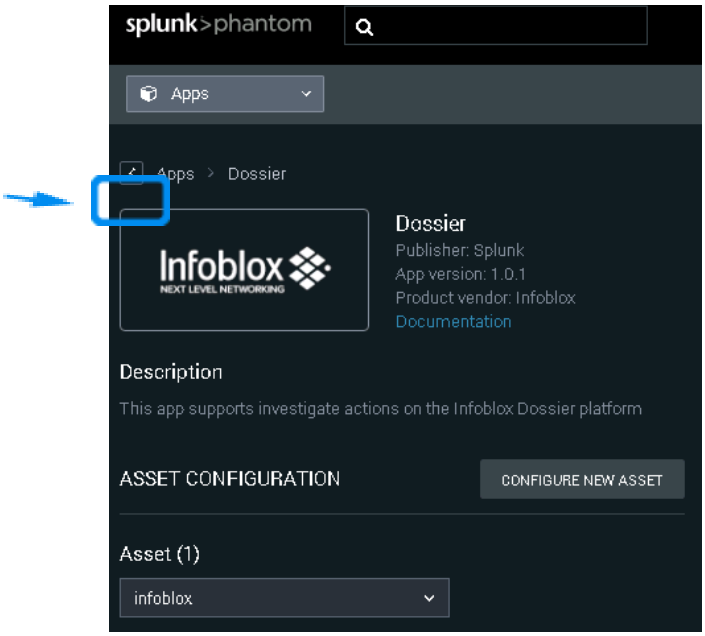

7. Input an **Asset Name**, and if desired an Asset Description. Then click on **Asset Settings**. *Note the Asset name is referenced when creating playbooks or running actions.*



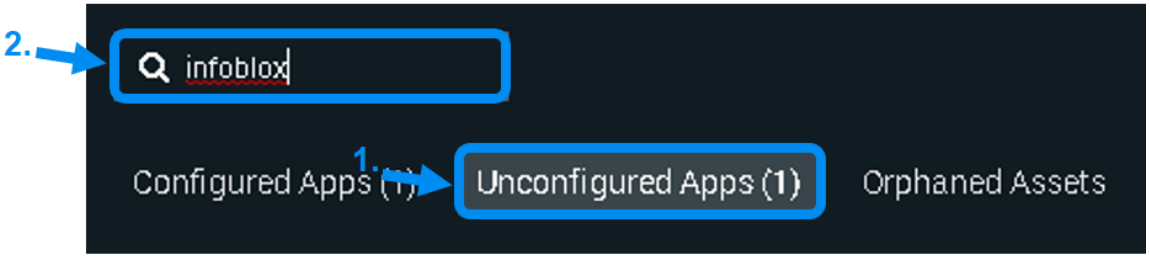
8. Input the **Dossier API Key** that was acquired earlier into the API Key for Dossier Service Textbox. Then, click **Save**.



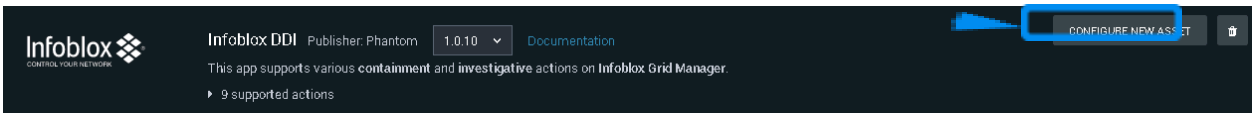

9. Click on **Apps** located at the top left of the App configuration page.



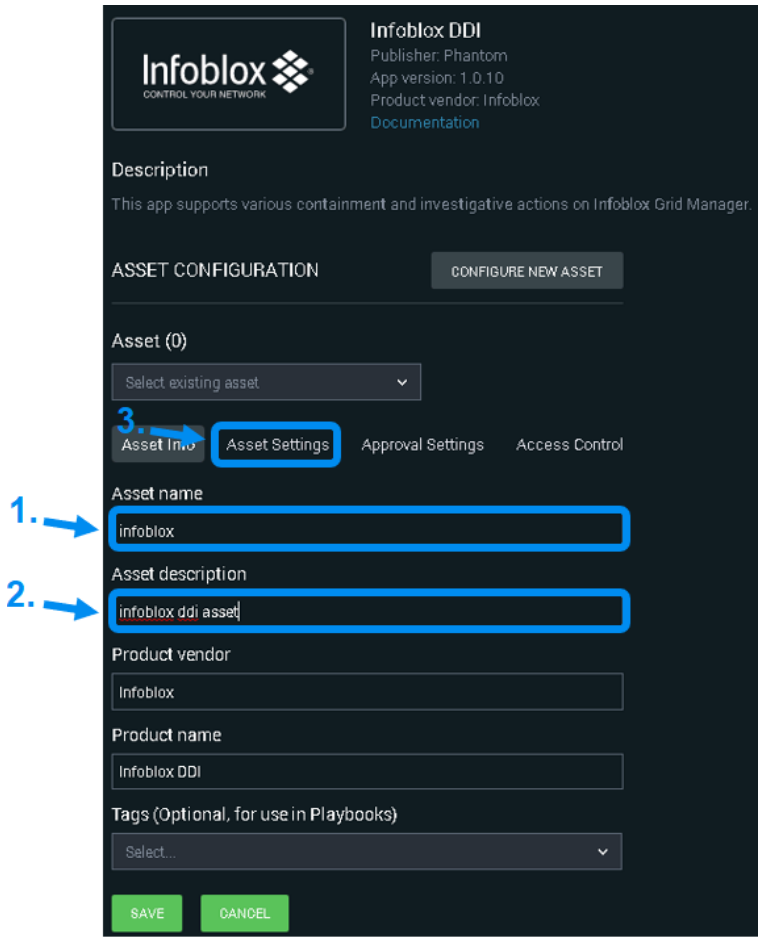
10. On the top left of the App window, Click **Unconfigured Apps**, then type in **infoblox** in the search box.



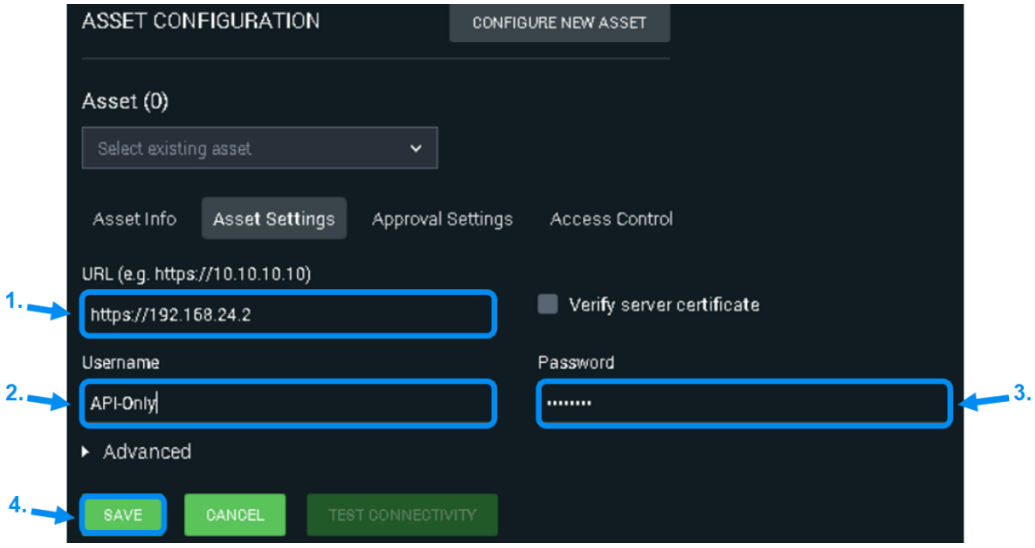

11. Click the button titled **Configure New Asset** for the App Infoblox DDI.




12. Input an **Asset Name**, and if desired an Asset Description. Then click on **Asset Settings**. Note the Asset name is referenced when creating playbooks or running actions.



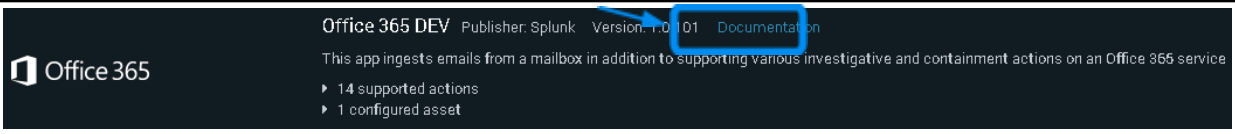
13. On the **Asset Configuration page**, input the **URL** of the Infoblox grid, the **Username** of a user who has API access that was specified in the prerequisites along with the associated **Password**. Then, click **Save** to finalize the creation of this asset.




## Test App functionality

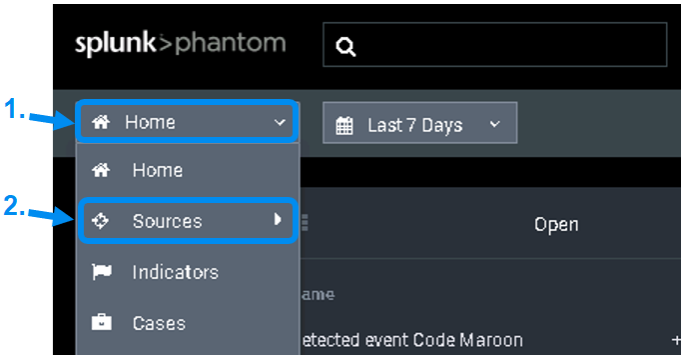
To test the functionality of the Apps, perform the following steps. Screenshots are taken from an environment with emails that have been ingested from an Office 365 server.

*Note: to test the functionality of the Dossier and DDI apps you must have integrated and preconfigured an Office 365 server with Splunk Phantom. For more information on how to integrate Office 365 into phantom, download and install the Office 365 App, then access the imbedded Documentation:*

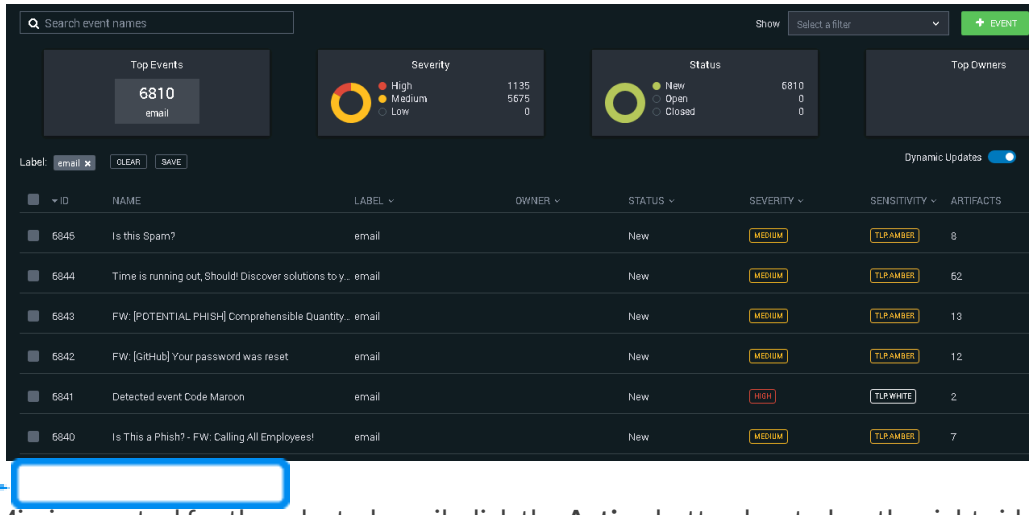



### Infoblox Dossier App

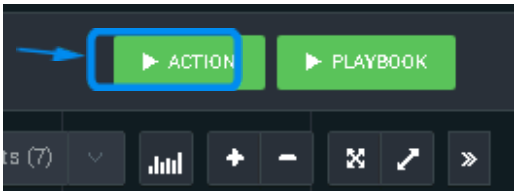
1. **Navigate** to the list of all ingested emails by clicking on the navigation menu labeled Home, then clicking on **Sources**.



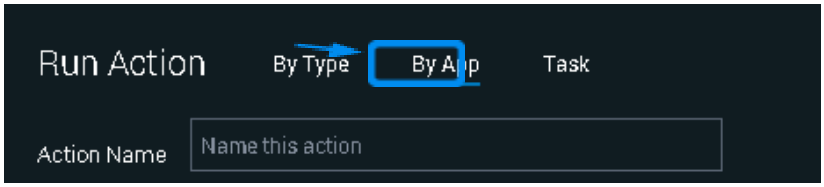
2. Navigate to an Email's Mission Control by clicking on an **Email**.



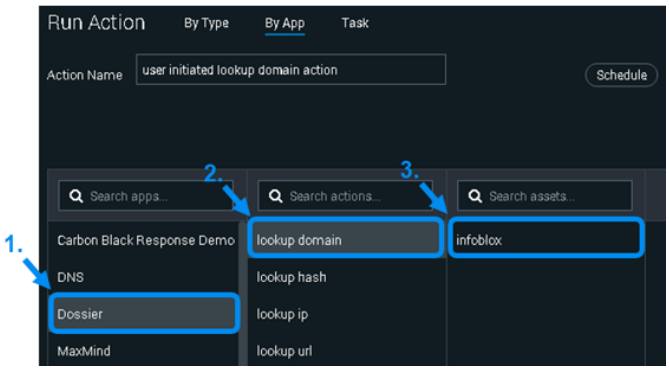

3. In Mission control for the selected email, click the **Action** button located on the right side of the window.



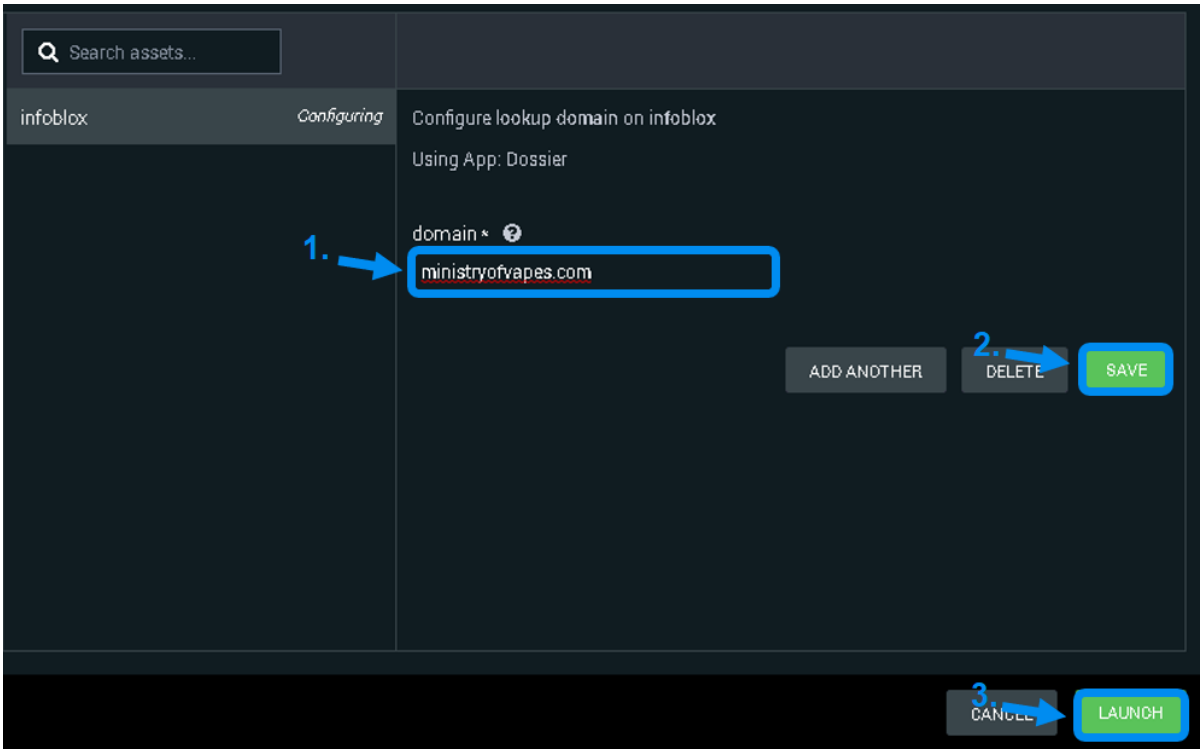

4. At the top of the Run Action window, click on **By App** to sort the list of actions by App.



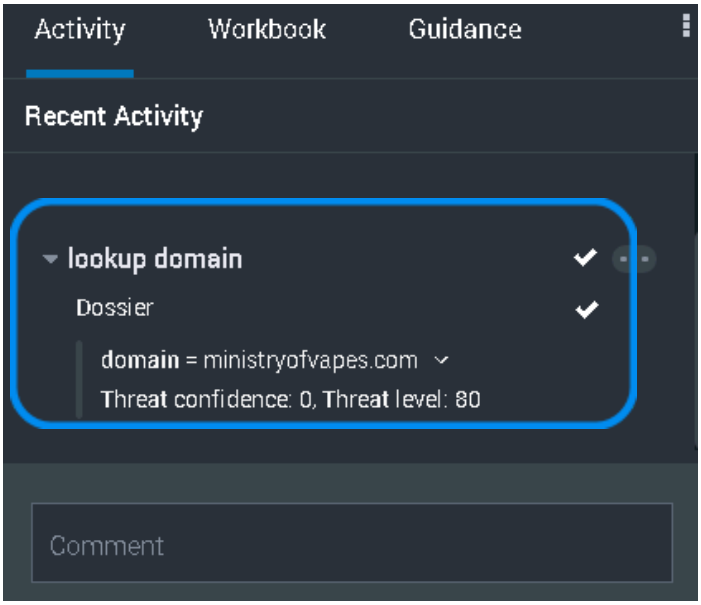

5. Click on the **Dossier** app, then click on the action lookup domain. Next, click on the recently created **Dossier Asset**.



6. Input a **domain** to check its Dossier data. Pictured is a known malicious domain Ministryofvapes. After inputting a domain, click **Save**, then click **Launch**. Note the domain that you lookup does not need to be listed in the email, however the domain must be a real domain.

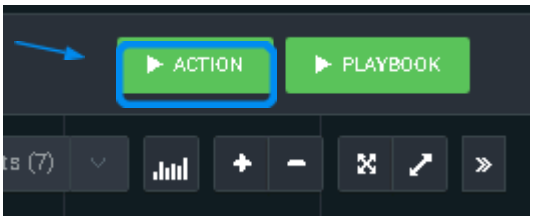



- Observe the results of the test in the **Activity** panel. If the test was successful, the Dossier asset has been properly configured and the Dossier app can now be used as a part of Splunk Phantom Playbooks.

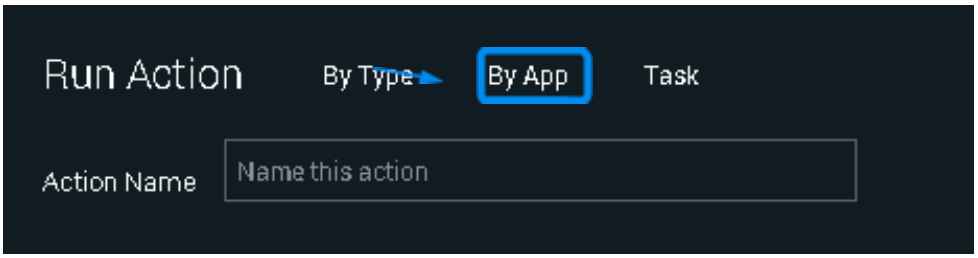


### Infoblox DDI App

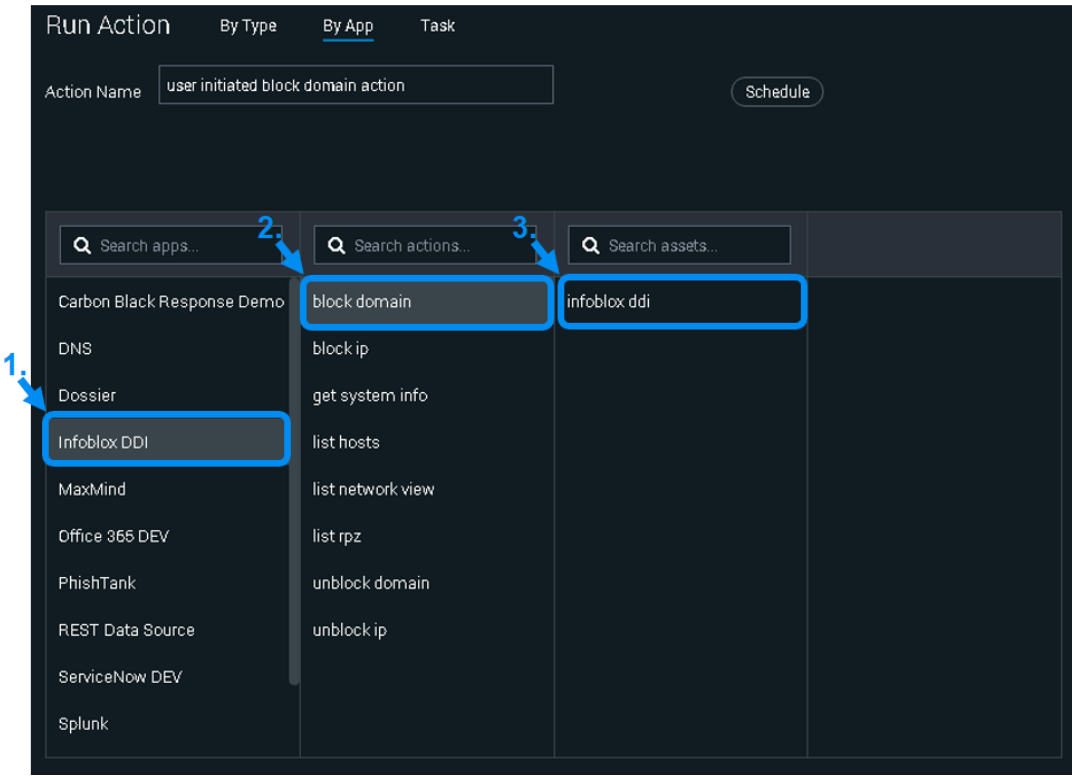
1. Using the same email that was used to test the Infoblox Dossier app, click the **Action** button located on the right side of the window.



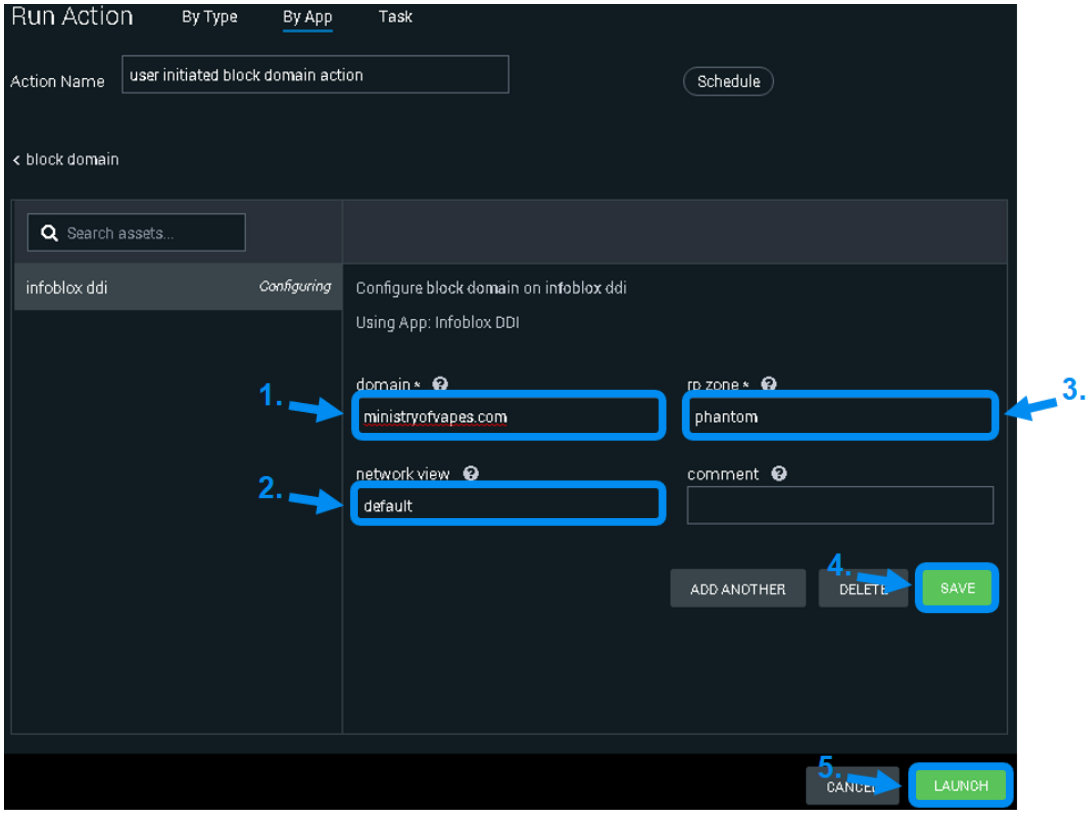

2. At the top of the Run Action window, click on **By App** to sort the list of actions by App.



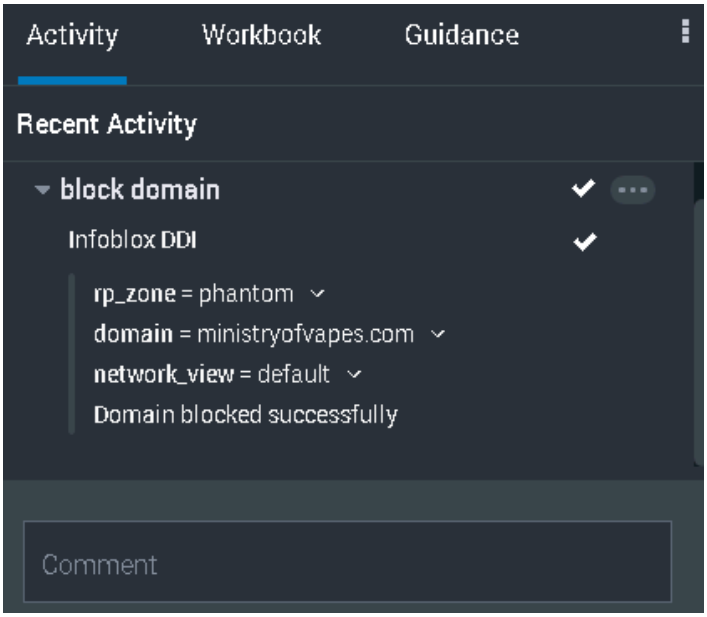

3. Locate and click on the I**nfoblox DDI** app. Then click on the **action block domain**. Next, click on the previously created infoblox DDI Asset.



4. Input a **domain** to be blocked. Then input a **Response Policy Zone** that exists on your Infoblox Grid.




- Observe the results of running the action in the **Activity** panel. If successful, the Infoblox DDI asset has been properly configured. You may now use the Infoblox DDI in Splunk Phantom Playbooks.



## Additional Resources

Infoblox community Website:

https://community.infoblox.com/

Infoblox NIOS Documentation:

https://docs.infoblox.com/display/nios84/Infoblox+NIOS+8.4

Splunk Community Website:

https://www.splunk.com/en_us/community.html

Splunk Phantom Website:

https://my.phantom.us

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