# Table of Contents

**Introduction** ......................................................................................................................................................... 3  
**Prerequisites** ........................................................................................................................................................... 3  
**Known Limitations** .................................................................................................................................................. 4  
**Best Practices** .......................................................................................................................................................... 4  
**Workflow** ................................................................................................................................................................. 4  
**Splunk Phantom Apps** ............................................................................................................................................. 4  
**Extensible Attributes** .............................................................................................................................................. 4  
**Infoblox Configuration** ........................................................................................................................................... 5  
  - Create phantom Response Policy Zone in Infoblox ............................................................................................... 5  
  - Create phantom_id Extensible Attribute .................................................................................................................. 6  
  - Acquire Dossier API Key ............................................................................................................................................ 7  
**Splunk Phantom Configuration** .................................................................................................................................. 8  
  - Download and Configure Splunk Apps ..................................................................................................................... 8  
  - Test App functionality ................................................................................................................................................ 13  
    - Infoblox Dossier App .............................................................................................................................................. 13  
    - Infoblox DDI App .................................................................................................................................................. 16  
**Additional Resources** ............................................................................................................................................... 18
Introduction
Infoblox with Splunk Phantom allow 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
5. BloxOne™ Threat Defense license (one of the following):
   o BloxOne™ Threat Defense Advanced
   o BloxOne™ Threat Defense Business - Cloud
   o BloxOne™ Threat Defense Business - On Premise
6. Pre-configured required services: DHCP, DNS, IPAM, RPZ, and Threat Analytics
7. NIOS API user with the following permissions (access via API only):
   o All IPv4 Host Addresses - RW
   o All IPv4 DHCP Fixed Addresses/Reservations - RW
   o All IPv6 DHCP Fixed Addresses - RW
   o All IPv6 Host Addresses - RW
   o All A records - RW
   o All AAAA Records - RW
   o All PTR Records - RW
   o All DNS Views - RW
   o All Response Policy Zones - RW
   o 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:
   o Basic Permissions:
     • Apps: View / Edit
     • Assets: 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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>phantom_id</td>
<td>Extensible Attribute that is populated with a value representing a case id.</td>
<td>String</td>
</tr>
</tbody>
</table>
Infoblox Configuration

Create phantom Response Policy Zone in Infoblox

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

Note: You may use a Local Response Policy Zone that has already been created. If you desire to do so, skip this step.

1. Navigate to Data Management → DNS → Response Policy Zones.

2. Click the + Icon.

<table>
<thead>
<tr>
<th>Zones</th>
<th>Members</th>
<th>Name Server Groups</th>
<th>Shared Record Groups</th>
<th>Response Policy Zones</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

   Quick Filter: None | Off Filter On | Show Filter

<table>
<thead>
<tr>
<th>ORDER</th>
<th>NAME</th>
<th>TYPE</th>
<th>SEVERITY</th>
<th>PRIMARY NAME S...</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>local.rpz</td>
<td>Local</td>
<td>Major</td>
<td>nios.poc.infoblo..</td>
</tr>
</tbody>
</table>

3. In the following Add Response Policy Zone Wizard, click Next.
4. Give the Response Policy Zone a **Name**, then click **Save & Close**.

Add Response Policy Zone Wizard > Step 2 of 5

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**. Note the extensible attribute **phantom_id** is case-sensitive.

![Add Extensible Attribute Wizard](image)

2. Click **Save & Close**.

**Acquire Dossier API Key**

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

1. With your credentials, log in to the Cloud Services Portal at [https://osp.infoblox.com](https://osp.infoblox.com).

![Cloud Services Portal](image)

2. Click on the text that contains your username. On the bottom left of the window to reveal a menu. Then, click on **User Preferences**.
3. In the User Preferences panel, locate the **API Keys** header. Then, click **Copy** to copy your **Dossier API key** for use later.

**User Preferences**

<table>
<thead>
<tr>
<th>Key</th>
<th>Copy</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Notification Subscriptions**

Choose which types of notifications you would like to receive.

**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**.
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 in **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 Infoblox 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.

   ![Run Action screenshot](image)

   - 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 enables next level network experiences with its Secure Cloud-Managed Network Services. As the pioneer in providing the world’s most reliable, secure and automated networks, we are relentless in our pursuit of network simplicity. A recognized industry leader, Infoblox has 50 percent market share comprised of 8,000 customers, including 350 of the Fortune 500.

Corporate Headquarters | 3111 Coronado Dr. | Santa Clara, CA | 95054
+1.408.986.4000 | 1.866.463.6256 (toll-free, U.S. and Canada) | info@infoblox.com | www.infoblox.com

© 2019 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).