

DEPLOYMENT GUIDE

Infoblox Integration with ThreatConnect

Table of Contents

| | |
|---|----|
| Introduction..... | 2 |
| Supported Platforms..... | 2 |
| Prerequisites..... | 2 |
| Known Limitations..... | 2 |
| Configuration..... | 3 |
| Workflow..... | 3 |
| Infoblox..... | 3 |
| ThreatConnect..... | 3 |
| Infoblox Configuration..... | 3 |
| Enable the TAXII service..... | 3 |
| Create an Admin with TAXII access..... | 4 |
| Create a Response Policy Zone..... | 7 |
| Assign a Response Policy Zone to Sync with ThreatConnect..... | 9 |
| ThreatConnect Configuration..... | 10 |
| Create an Outbound TAXII Exchange..... | 10 |
| Test the configuration..... | 15 |
| Additional Resources..... | 17 |

Introduction

TAXII stands for Trusted Automated eXchange of Indicator Information. Trusted Automated eXchange of Indicator Information (TAXII™) is a U.S. Department of Homeland Security (DHS)-led, community-driven effort to standardize the trusted, automated exchange of cyber threat information. TAXII defines a set of services and message exchanges that, when implemented, enable sharing of actionable cyber threat information across organization and product/service boundaries for the detection, prevention, and mitigation of cyber threats. TAXII is not a specific information sharing initiative, and it does not define trust agreements, governance, or non-technical aspects of cyber threat information sharing. Instead, TAXII empowers organizations to achieve improved situational awareness about emerging threats, and enables organizations to easily share the information they choose with the partners they choose, while leveraging existing relationships and systems.

The integration with ThreatConnect provides the ability to download malicious information from a TAXII client in the form of IP addresses and domain names. This deployment guide shows you how to configure your Infoblox Grid to receive TAXII transmissions from ThreatConnect.

Supported Platforms

The TAXII integration is supported on the following Infoblox appliances: IB-1410, IB-1415, IB-1420, IB-1425, IB-VM-1410, IB-VM-1415, IB-VM-1420, IB-VM-1425, TE-810, TE-815, TE-2210, TE-2215, TE-2220, TE-2215, IB-VM-4010, IB-4030, IB-4030-10GE, IB-VM-2220, IB-VM-2225, PT-1400, PT-2200, PT-4000, and PT-4000-10GE.

Prerequisites

The following prerequisites are required for the solution:

- Infoblox Grid or stand-alone Grid Master running NIOS 7.3 or higher with the following licenses:
 - Security Ecosystem License
 - DNS
 - RPZ
- ThreatConnect instance access:
 - User with Organization Administrator permissions

Known Limitations

As of NIOS 8.5.1, only Host and IP indicators can be synchronized from ThreatConnect to Infoblox. In order to receive TAXII transmissions from ThreatConnect, the Infoblox Grid Master's LAN or MGMT port must be reachable on a publicly routable IP, or a publicly resolvable URL.

Configuration

Workflow

Infoblox

1. Verify that the correct licenses are installed on NIOS, and install any that are missing:
 - Security Ecosystem
 - DNS
 - RPZ
2. Enable the TAXII service
3. Create a TAXII enabled user group
4. Create a new TAXII enabled Admin Group and a new Admin
5. Create a Response Policy Zone
6. Assign a Response Policy Zone to sync with ThreatConnect

ThreatConnect

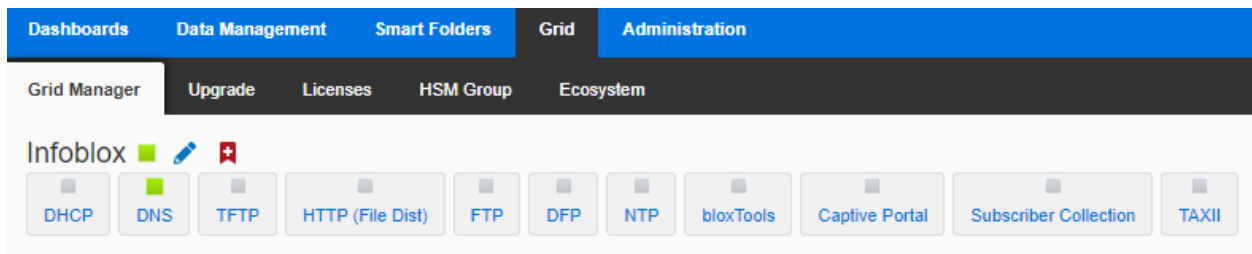
1. Create a new Outbound TAXII exchange
2. Test the configuration

Infoblox Configuration

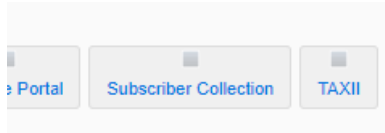
Enable the TAXII service

To enable the TAXII service perform the following steps:

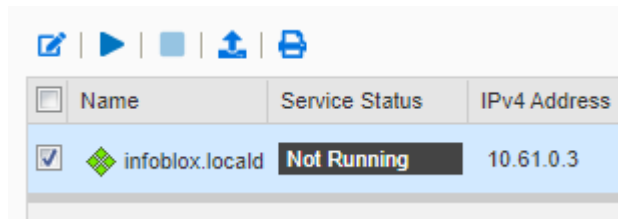
1. On the Web interface of the Infoblox Grid, navigate to **Grid** → **Grid Manager**.



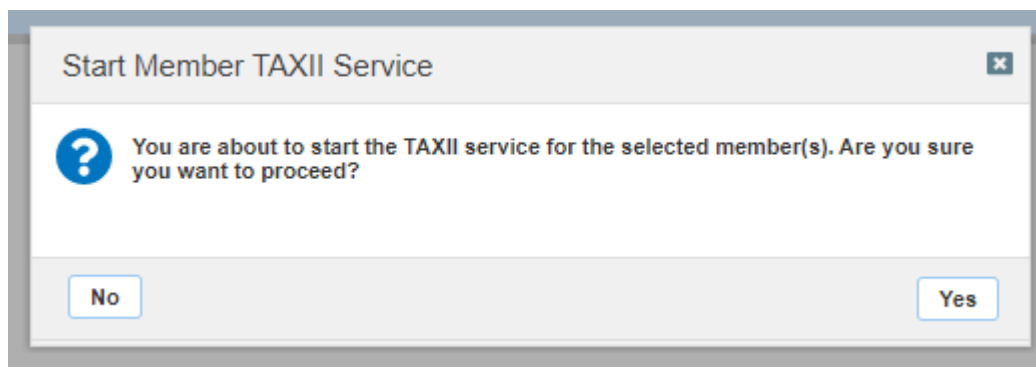
2. Click the **TAXII** box in the list of services.



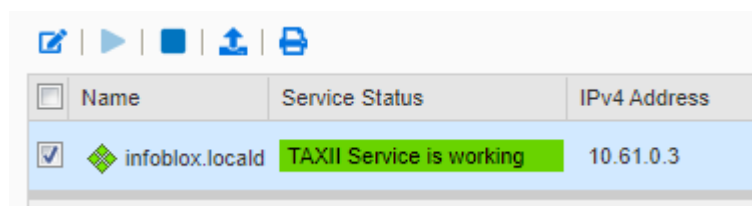
3. Click the **checkbox** associated with the Grid Master.



4. Click the **Start** Icon.
5. In the Start Member TAXII Service dialog box, click **Yes**.



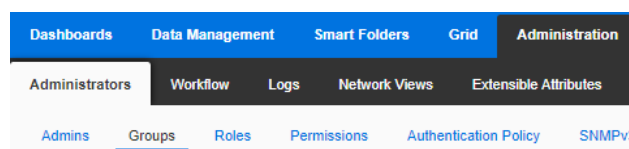
6. Wait 2-3 minutes then **Refresh** the page. After the page has refreshed, verify that the TAXII service is running.



Create an Admin with TAXII access

To an Admin with TAXII access perform the following steps:

1. On the Web interface of the Infoblox Grid, navigate to **Administration** → **Administrators** → **Groups**.



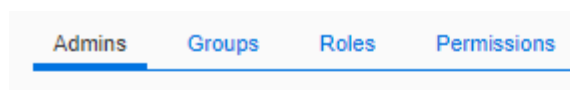
2. Click the **Add** icon located above the list of Admin Groups.
3. Give the Admin Group a relevant **Name**.

The screenshot shows the 'Add Admin Group Wizard > Step 1 of 8' form. It includes a text input for 'Name' with the value 'TAXII-Users', a larger text input for 'Comment', and a 'Disable' checkbox which is unchecked. A yellow warning box at the bottom states: 'Please note that the following rules cannot override access rules from Grid level and can be applied only as additional restrictions. Thus if some IP or Network is denied on Grid level then it cannot be allowed on Admin Group level. From the other hand if network'. On the right side, there is a vertical scrollbar and a help icon.

4. Click **Next** until you reach Step 5 of the Add Admin Group Wizard.
5. Near the bottom of the Add Admin Group Wizard, click the checkbox associated with TAXII and ensure that all other interfaces are unchecked.

The screenshot shows the 'Add Admin Group Wizard > Step 5 of 8' form. It features a table with columns 'Name' and 'Comment' that is currently empty, displaying 'No data'. Below the table, under the heading 'Allowed Interfaces', there are four checkboxes: 'GUI', 'API', 'CLI', and 'TAXII'. The 'TAXII' checkbox is checked, while the others are unchecked. At the bottom of the form, there are buttons for 'Cancel', 'Previous', 'Next', and 'Save & Close'.

6. Click **Save & Close** to confirm the creation of the Admin Group.
7. Click the **Admins** tab.



8. Click the **Add** icon located above the list of Admins.
9. In the Add Administrator Wizard, give the new Administrator a Login, a Password, and Confirm the Password.

10. On the same step of the Add Administrator Wizard, click the **Select** button that is associated with Admin Group.

11. Locate and Select the Admin Group that was created on [pages 4, 5 and 6](#). Then, Click **OK** to confirm the selection.

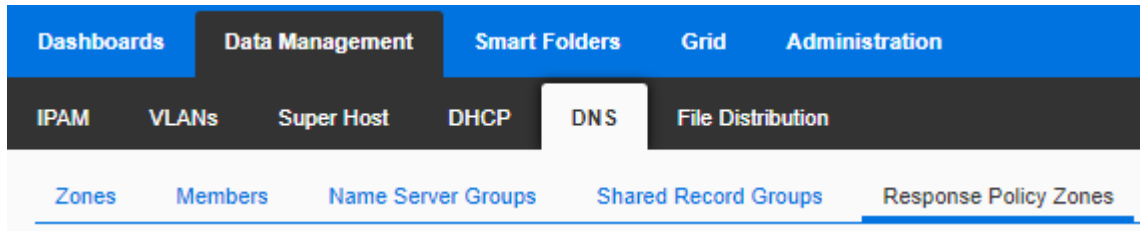
| Name | Superuser | Comment | Site |
|---------------------|-----------|------------------|------|
| TAXII-Users | No | | |
| admin-group | Yes | | |
| cloud-api-only | No | Admins allowe... | |
| saml-group | No | Admins allowe... | |
| splunk-reporting-gr | No | | |

12. Click **Save & Close** to confirm the creation of the new Admin.

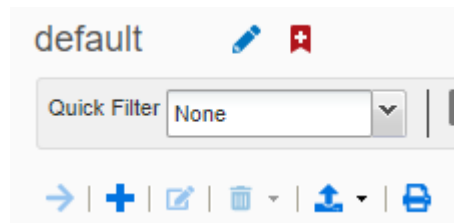
Create a Response Policy Zone

To create a Response Policy Zone perform the following steps:

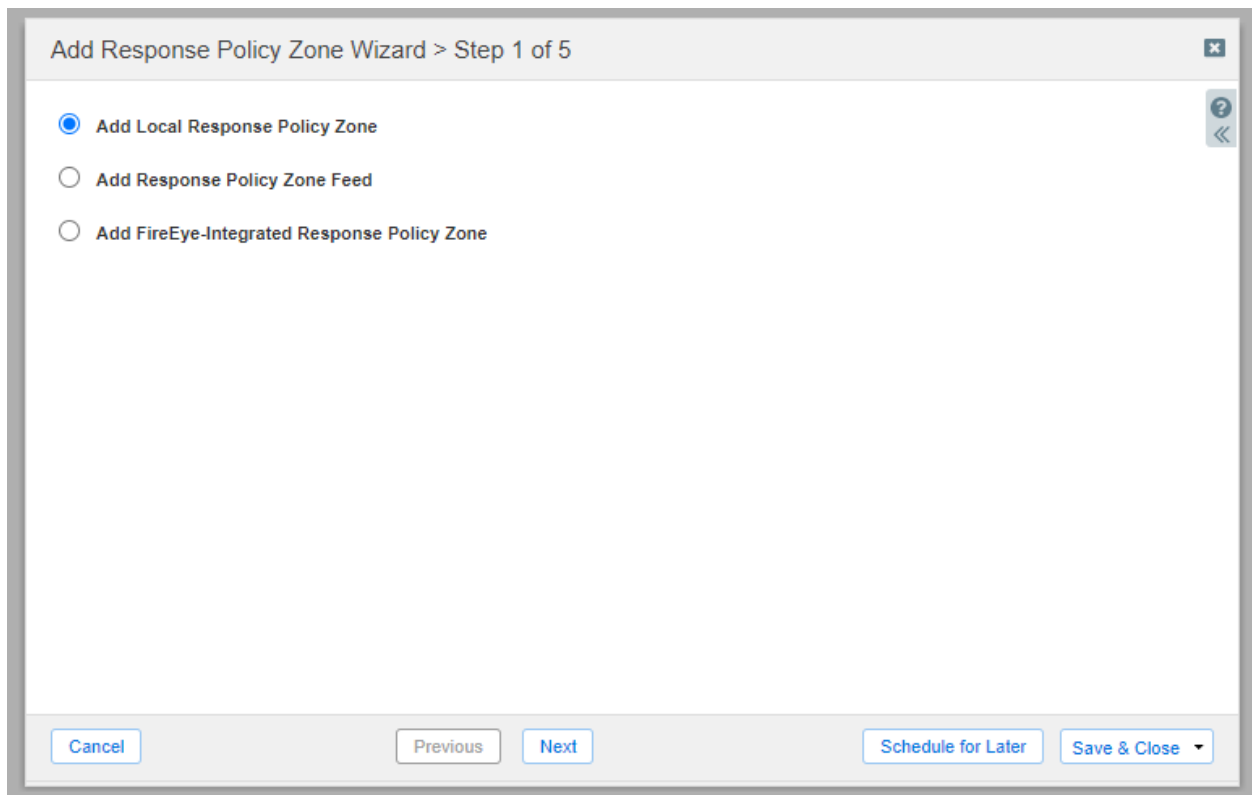
1. On the Web interface of the Infoblox Grid, navigate to **Data Management** → **DNS** → **Response Policy Zone**.



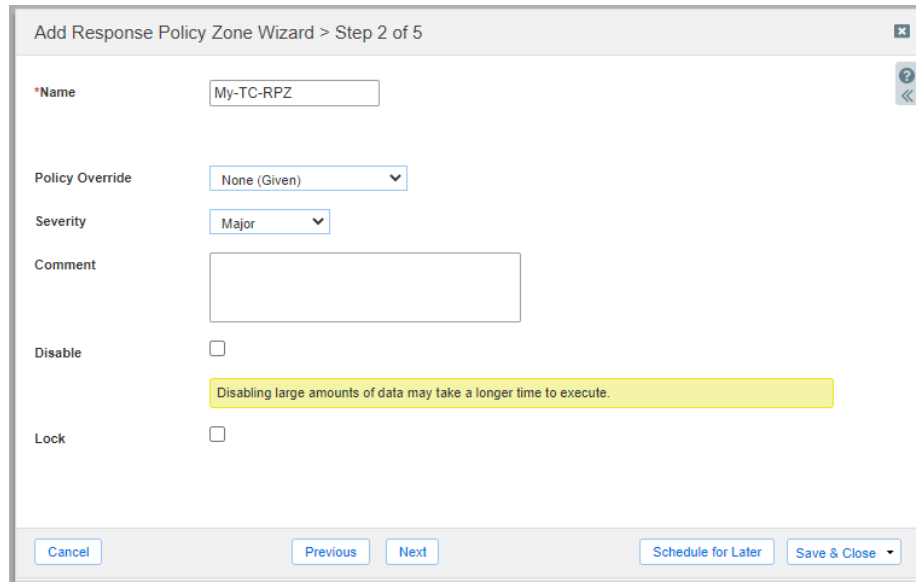
2. Click the **Add** icon located above the list of Response Policy Zones.



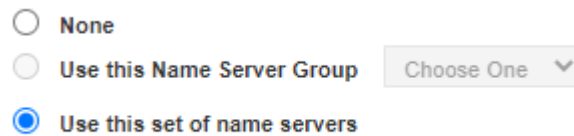
3. Click the **Add Local Response Policy Zone** bubble. Then, click **Next**.



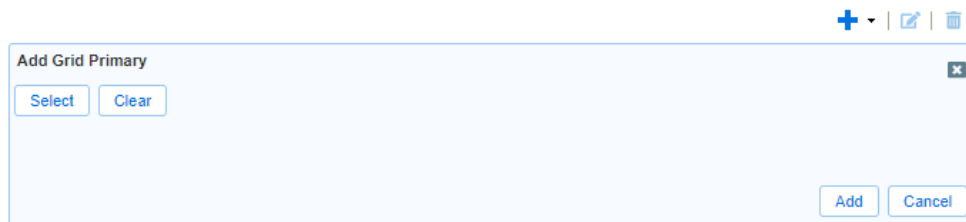
4. Give the Response Policy Zone a Name and set all relevant parameters. Then, click **Next**.



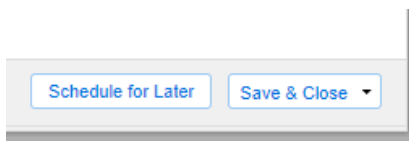
5. Click the **Use this set of name servers** bubble.



6. Click the **Add** icon.
7. Click **Select** to select the correct name server that this Response Policy Zone will apply to. Then, click the **Add** button to confirm the selection.



8. Click **Save & Close** to confirm the creation of the new Response Policy Zone.

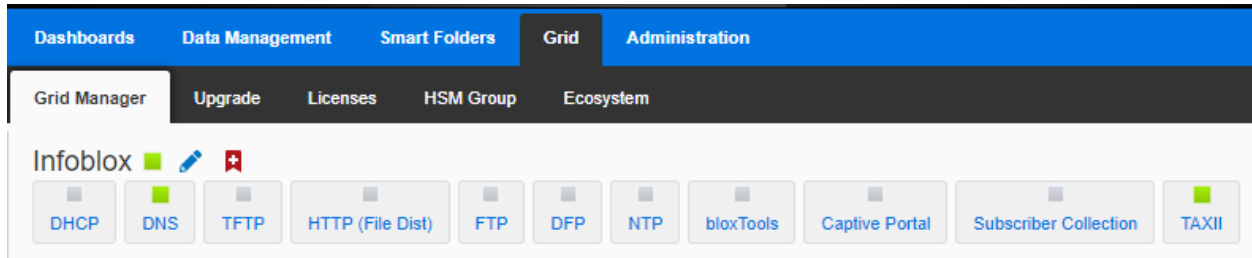


9. When prompted, restart all relevant services by clicking **Restart** located on the banner at the top.

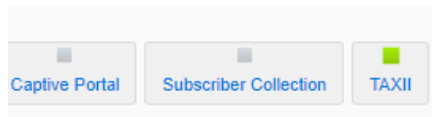
Assign a Response Policy Zone to Sync with ThreatConnect

To assign a Response Policy Zone to sync with ThreatConnect perform the following steps:

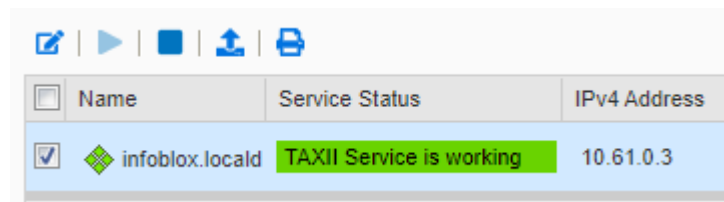
1. On the Web interface of the Infoblox Grid, navigate to **Grid** → **Grid Manager**.



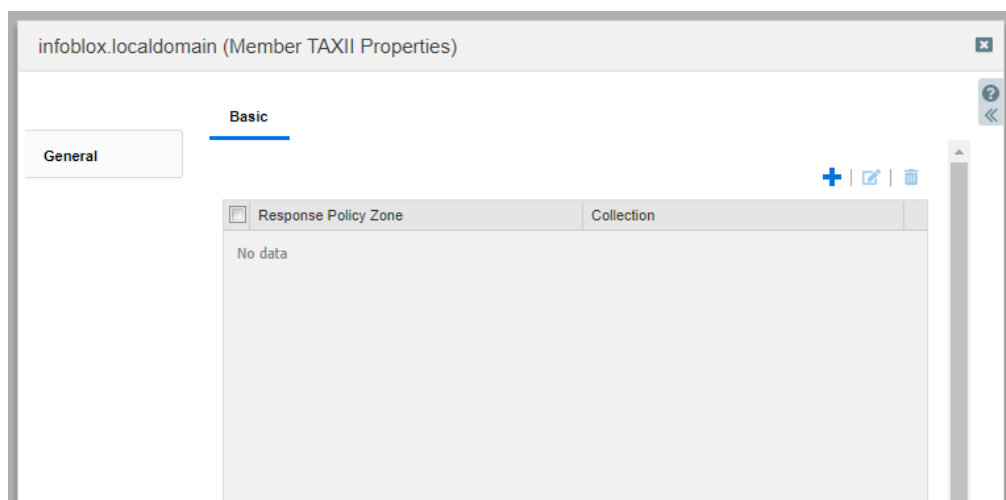
2. Click the **TAXII** box in the list of services.



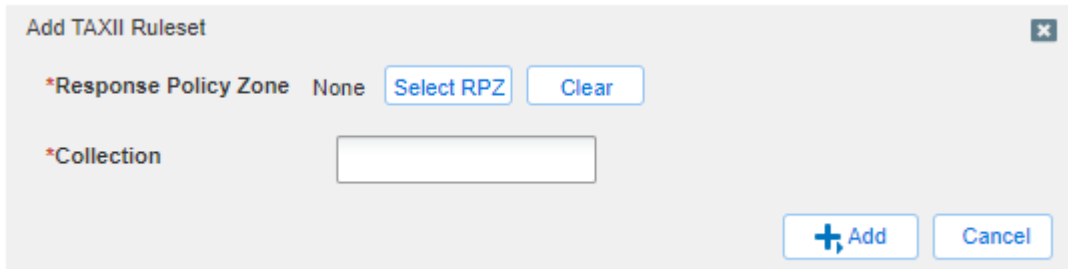
3. Click the checkbox associated with the grid member that is currently running the TAXII service. Then, Click the **Edit** icon located above the table of members.



4. In the Member TAXII Properties window that is revealed, click the **Add** icon located above the list of Response Policy Zones.

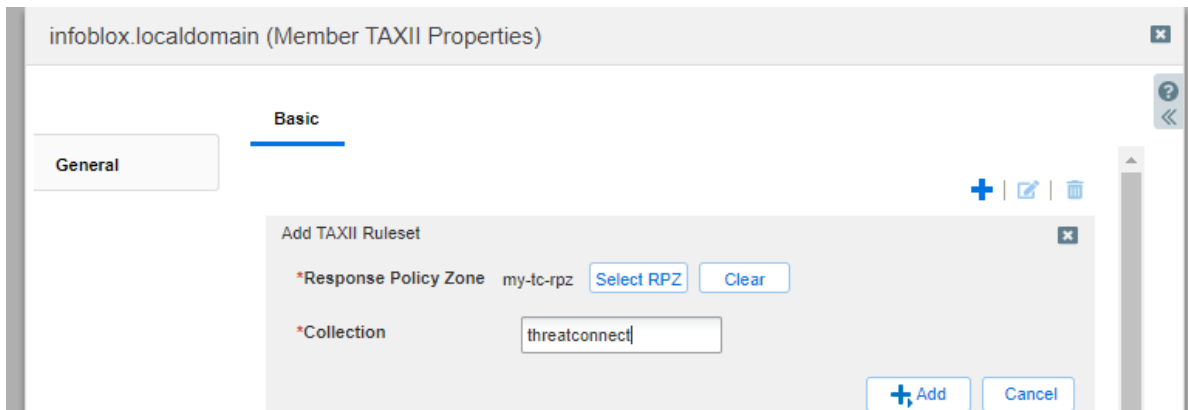


5. Click **Select RPZ** and select the relevant RPZ that was created earlier.



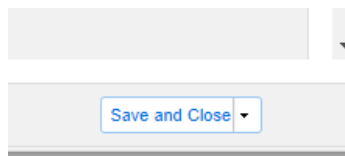
The dialog box titled "Add TAXII Ruleset" contains two fields: "*Response Policy Zone" with a dropdown menu showing "None" and buttons "Select RPZ" and "Clear"; and "*Collection" with an empty text input field. At the bottom right are buttons "+ Add" and "Cancel".

6. Input the name of a Collection that will be acquired from ThreatConnect. Then, click **Add**. Note: Only use valid URI characters for the collection name.



The window titled "infoblox.localdomain (Member TAXII Properties)" shows a "Basic" tab. Inside, there is an "Add TAXII Ruleset" dialog box where the "*Response Policy Zone" is set to "my-rc-rpz" and the "*Collection" is "threatconnect". The dialog has "+ Add" and "Cancel" buttons. The main window also has a "General" tab and a sidebar with icons for adding, editing, and deleting rulesets.

7. Click **Save and Close** to confirm all changes.



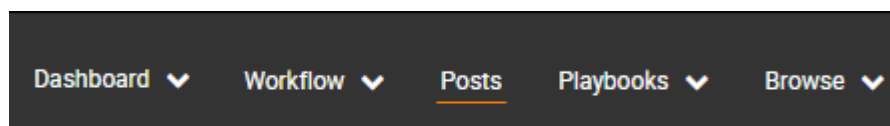
A button labeled "Save and Close" with a dropdown arrow.

ThreatConnect Configuration

Create an Outbound TAXII Exchange

To Create an Outbound TAXII Exchange on ThreatConnect, perform the following steps:

1. Log in to your instance of ThreatConnect. Then, click **Posts** located on the top right of the ThreatConnect window.



A dark navigation bar with the following items: "Dashboard" with a dropdown arrow, "Workflow" with a dropdown arrow, "Posts" (highlighted with an underline), "Playbooks" with a dropdown arrow, and "Browse" with a dropdown arrow.

2. Click the **Source** associated with your Org. *Note: In the example screenshot the Org is Infoblox, and the associated Org is Infoblox Source.*

My ThreatConnect

▼ My Org

Infoblox

▼ Communities

▼ Intelligence Sources

abuse.ch Locky Ransomware C2 Domain Blocklist

Blocklist.de Strong IPs

BotScout Bot List

Cybercrime Tracker

Developer Partner Sample TI

DShield.org Recommended Blocklist CIDRs

Firebog Prigent Malware Domains

Firebog Prigent Phishing Domains

Firebog Shalla Malware Domains

Infoblox Source

OpenPhish

PhishTank

Technical Blogs and Reports



VXVault

3. Click the **Cog** icon located on the top right of the Source panel.

Source

Description

Test source for Infoblox



4. Click **Data** in the navigation bar at the top of the screen.

Deprecation Rules

Publishing

Data

Settings

5. Click the **New Outbound** button located under the TAXII Exchanges header.

TAXII Exchanges

+ NEW OUTBOUND

+ NEW INBOUND

6. On the Configure Outbound TAXII Exchange window that is revealed, input the following information:

Configure Outbound TAXII Exchange

TAXII Login Inbox Schedule Labels Confirm

Name: Infoblox

URL: https://My-Infoblox-Grid/services/inbox

Discovery URL: (optional) https://My-Infoblox-Grid/services/discovery

Note: Discovery URL is only required if the TAXII server uses a different address to access discovery services.

Translator Version: STIX 1.1.1 Indicators TC_V1 (Legacy Translator)

Exchange is Active: Yes

TAXII Version 1.0: No

Enable SNI: Yes

Default Threat Rating: ☐

Default Confidence Rating: ☐

> Next

CANCEL SAVE

- o **Name:** Input a relevant name for this Outbound TAXII Exchange.
 - o **URL:** Input the URL for your Infoblox Grid. Note: This IP must be reachable by ThreatConnect. The IP must be associated with your Grid Masters MGMT or LAN interface with the URL format of http, or https://:<Your-Infoblox-Grid-IP-Here>/services/inbox.
 - o (Optional) **Discovery URL:** Input the URL for your Infoblox Grid to be used for Discovering TAXII related information on your Infoblox Grid. Note: This IP must be reachable by ThreatConnect. The IP must be associated with your Grid Masters MGMT or LAN interface with the URL format of http, or https://:<Your-Infoblox-Grid-IP-Here>/services/discovery.
 - o (Optional) **Translator version:** If desired, you may change the Translator Version.
7. Keep all other settings as their defaults. Then, click **Next**.
 8. Input the Username and Password of the TAXII admin that was created on [page 4](#) of this document.

Configure Outbound TAXII Exchange

TAXII
Login
Inbox
Schedule
Labels
Confirm

URL: https://My-Infoblox-Grid/services/discovery

Username: threatconnect Password:

Enable 2-way Authentication: No

TEST CONNECTION

Available Services

| Service | Address | Status |
|------------------------------|---------|--------|
| No available services found. | | |

< Back
Next >

CANCEL SAVE

- (Optional) If desired, click the **Test Connection** button to confirm that ThreatConnect can reach your Infoblox Grid.

Enable 2-way Authentication: No

TEST CONNECTION

Available Services

- Click **Next**.
- Input an Inbox. *Note: this value should correspond to the Collection that was assigned in Infoblox on [pages 9 and 10](#).*

Configure Outbound TAXII Exchange

TAXII > Login > **Inbox** > Schedule > Labels > Confirm

Inbox:

Note: not all TAXII servers will display available inboxes.
Check for available inboxes

Select Inbox

| Name | Address | Status | Subscribe |
|-----------------------------|---------|--------|-----------|
| No available inboxes found. | | | |

< Back > Next

CANCEL SAVE

12. (Optional) If desired, change the **Poll Start** date, and the interval at which data is transferred.

Configure Outbound TAXII Exchange

TAXII > Login > Inbox > **Schedule** > Labels > Confirm

Poll Start Date:

Collection Interval (hours): +
-

< Back > Next

CANCEL SAVE

13. Click **Next**.

> Next

CANCEL SAVE

14. Keep all settings as their defaults and click **Next**.

Configure Outbound TAXII Exchange

TAXII

Login

Inbox

Schedule

Labels

Confirm

Package TLP None

ID Prefix Default: threatconnect

< Back

> Next

CANCEL

SAVE

15. Verify that all settings are correct, then click **Save**.

Configure Outbound TAXII Exchange

TAXII

Login

Inbox

Schedule

Labels

Confirm

Name: Infoblox
URL: https://My-Infoblox-Grid/services/inbox
Discovery URL: https://My-Infoblox-Grid/services/discovery
Inbox Name: threatconnect
Version: 1.1
Activated: Yes
Username: threatconnect **Password:** *****
Parser: Legacy Parser
2-way Authentication Enabled: No

< Back

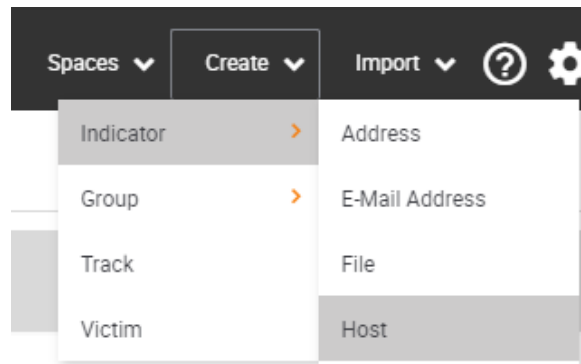
CANCEL

SAVE

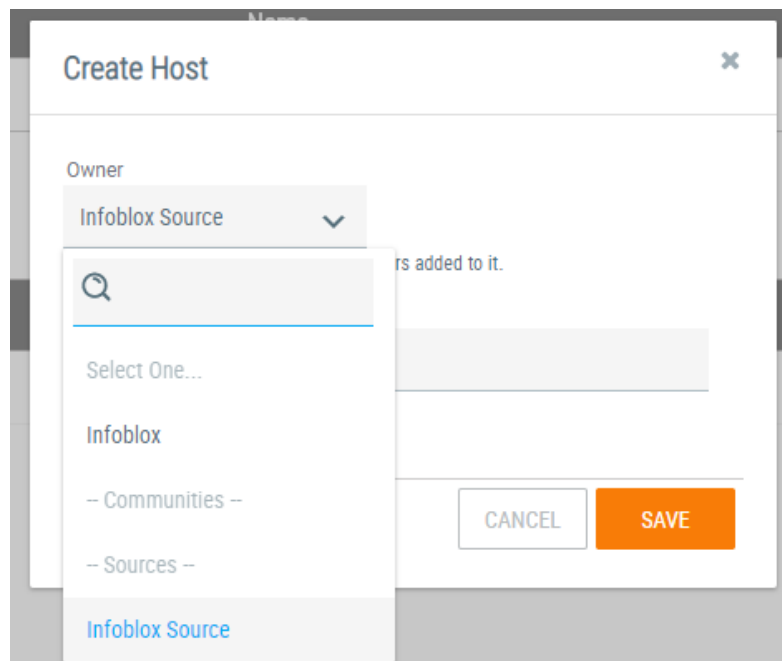
Test the configuration

To test the communication between ThreatConnect and Infoblox, perform the following steps:

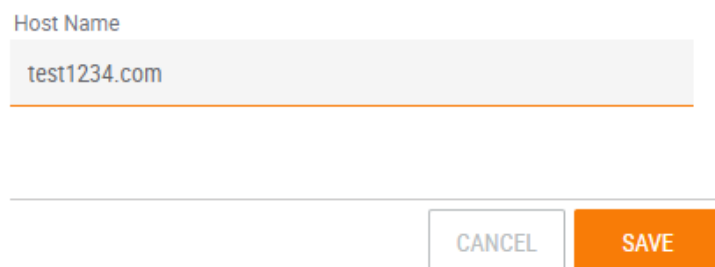
1. On the top right of the ThreatConnect webpage, click **Create**. Then highlight Indicator. Finally, click **Host**.



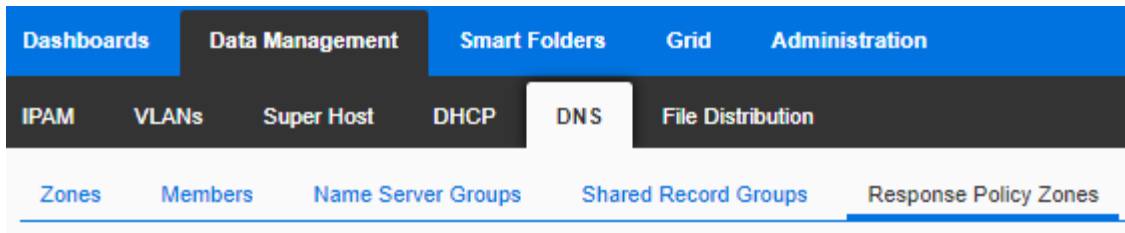
2. Click the **drop-down** associated with the Owner. Change the Owner to your Org's Source. *Note: In the example screenshot the Org is Infoblox, and the source is Infoblox Source.*



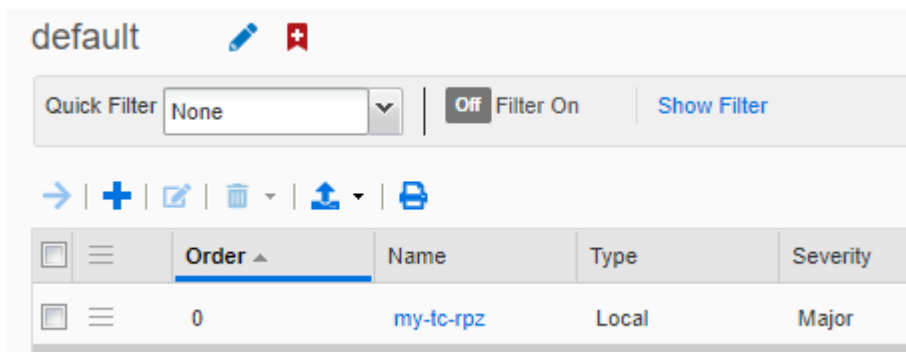
3. In the Host Name text field, input an example domain name. Then, click **Save**.



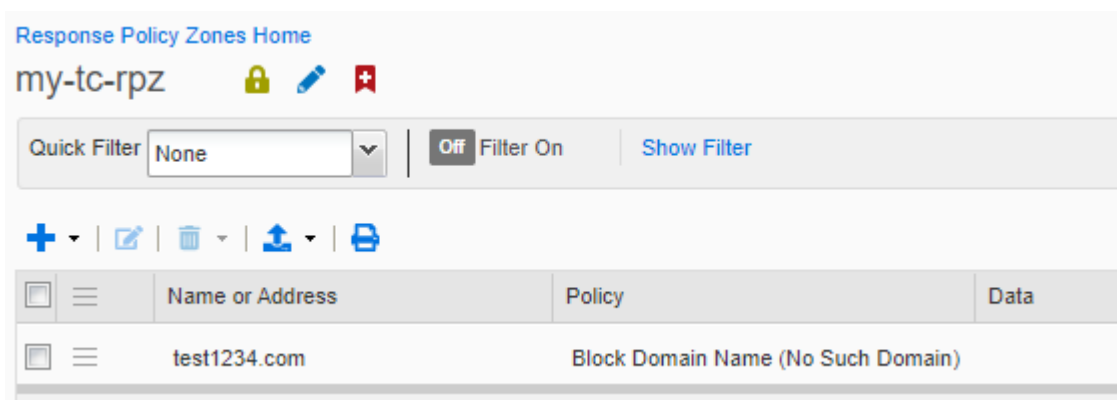
4. On the Infoblox Grid, Navigate to **Data Management** → **DNS** → **Response Policy Zones**.



5. Access the Response Policy Zone that was assigned to sync with ThreatConnect.



6. Inside the Response Policy Zone you will see the Host address that was added on ThreatConnect.



Additional Resources

For more information regarding Infoblox or ThreatConnect, access these websites:

1. [Infoblox Documentation Portal](#)
2. [Infoblox Website](#)
3. [Infoblox Community](#)
4. [ThreatConnect Website](#)



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