Infoblox

Deployment Guide

# Infoblox Integration with ThreatConnect

# Table of Contents

# 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:

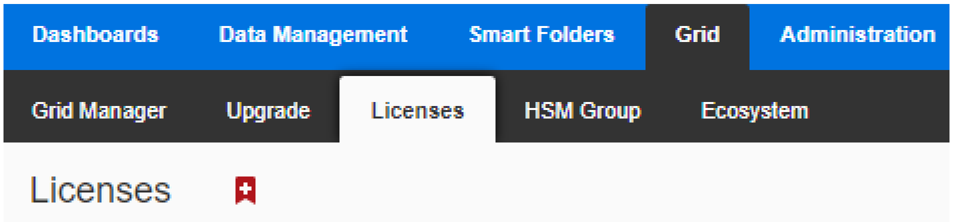
1. Create a new Outbound TAXII exchange
2. Test the configuration

## Infoblox Configuration

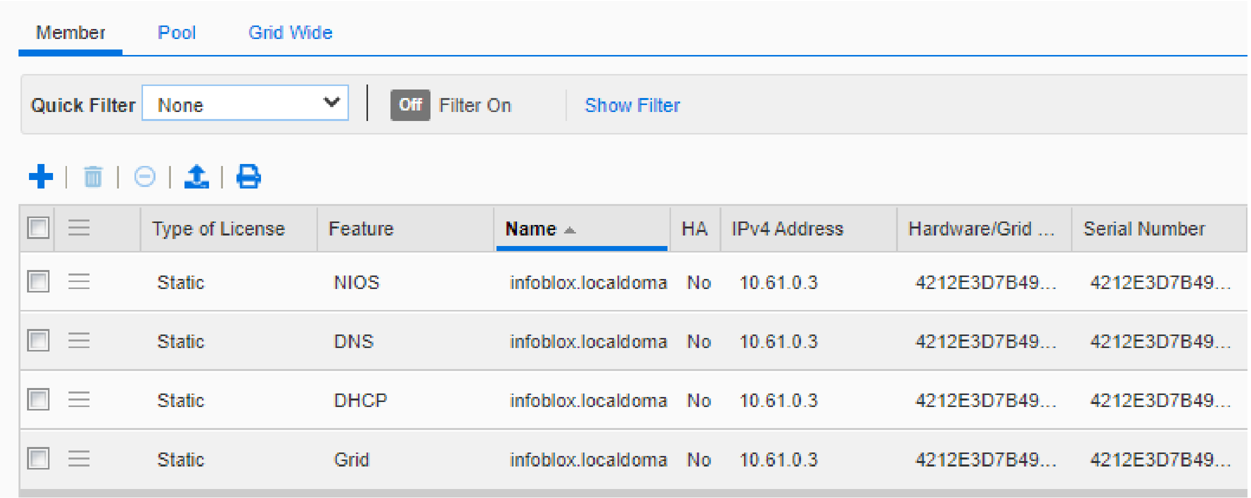
### Verify that the correct licenses are installed

The Infoblox and ThreatConnect integration require DNS, RPZ and Security Ecosystem Licenses:

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

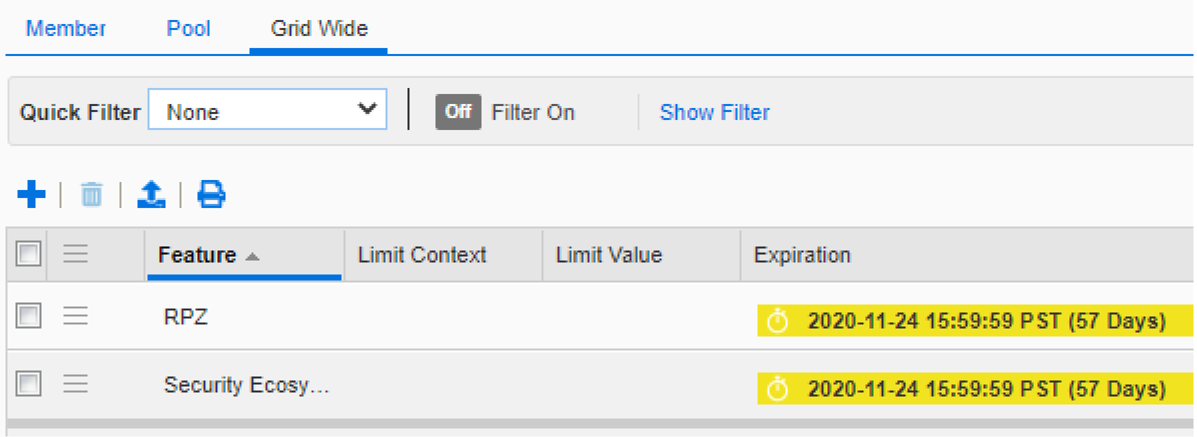


2. Click the **Member** tab of the Licenses page, and check for a valid **DNS** license.



| ☐ | | Type of License | Feature | Name ▲ | HA | IPv4 Address | Hardware/Grid ... | Serial Number |
|---|---|---|---|---|---|---|---|---|
| ☐ | ☰ | Static | NIOS | infoblox.localdoma | No | 10.61.0.3 | 4212E3D7B49... | 4212E3D7B49... |
| ☐ | ☰ | Static | DNS | infoblox.localdoma | No | 10.61.0.3 | 4212E3D7B49... | 4212E3D7B49... |
| ☐ | ☰ | Static | DHCP | infoblox.localdoma | No | 10.61.0.3 | 4212E3D7B49... | 4212E3D7B49... |
| ☐ | ☰ | Static | Grid | infoblox.localdoma | No | 10.61.0.3 | 4212E3D7B49... | 4212E3D7B49... |

3. Click the **Grid Wide** tab of the Licenses page, and check for valid **RPZ** and **Security Ecosystem** licenses.



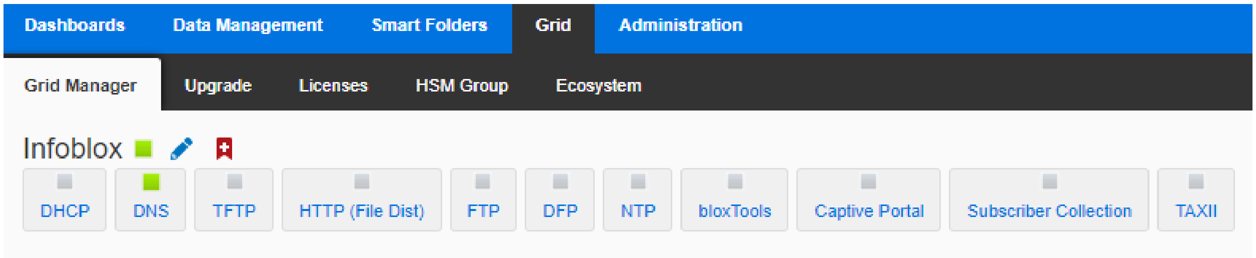
| ☐ | Feature ▲ | Limit Context | Limit Value | Expiration |
|---|---|---|---|---|
| ☐ | RPZ | | | 2020-11-24 15:59:59 PST (57 Days) |
| ☐ | Security Ecosy... | | | 2020-11-24 15:59:59 PST (57 Days) |

*Note: If any licenses are missing, the integration with ThreatConnect will fail. Please contact your Infoblox Sales representative to acquire the licenses you are missing.*

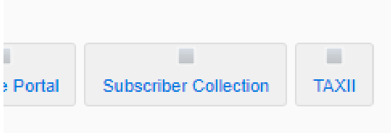
## Enable the TAXII service

To enable the TAXII service perform the following steps:

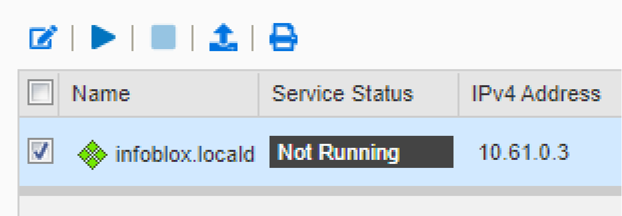
1. On the Web interface of the Infoblox Grid, navigate to **Grid** → **Grid Manager**.



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

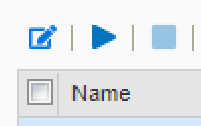


3. Click the **Checkbox** Associated with the Grid Master.

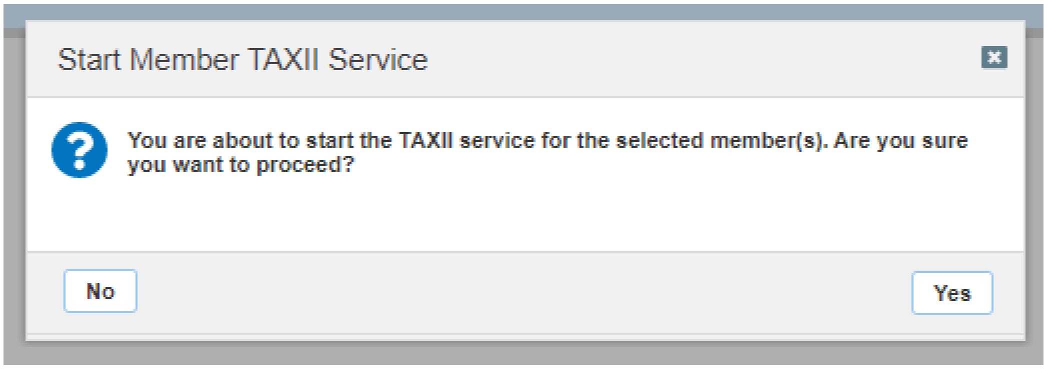


| ☐ | Name | Service Status | IPv4 Address |
|---|---|---|---|
| ☑ | infoblox.locald | Not Running | 10.61.0.3 |

4. Click the **Start** Icon.

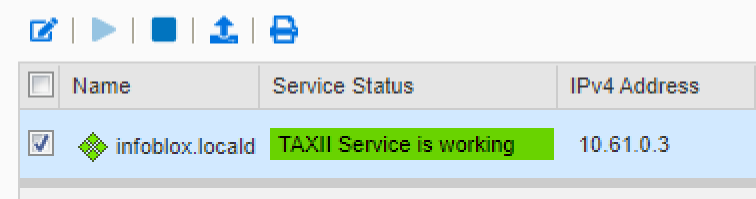


5. In the **Start Member TAXII Service** dialog box, click **Yes**.


Start Member TAXII Service

You are about to start the TAXII service for the selected member(s). Are you sure you want to proceed?

6. Wait 2-3 minutes then **Refresh** the page. Verify that the TAXII service is running.

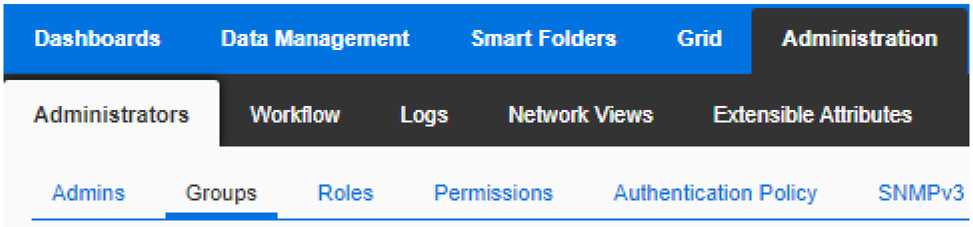


|  | Name | Service Status | IPv4 Address |
|---|---|---|---|
| ☑ | infoblox.locald | TAXII Service is working | 10.61.0.3 |

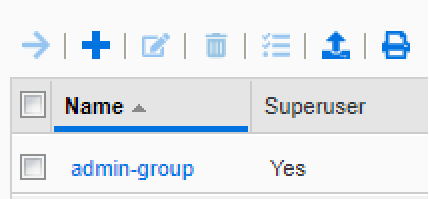
## Create an Admin with TAXII access

To an Admin with TAXII access perform the following steps:

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

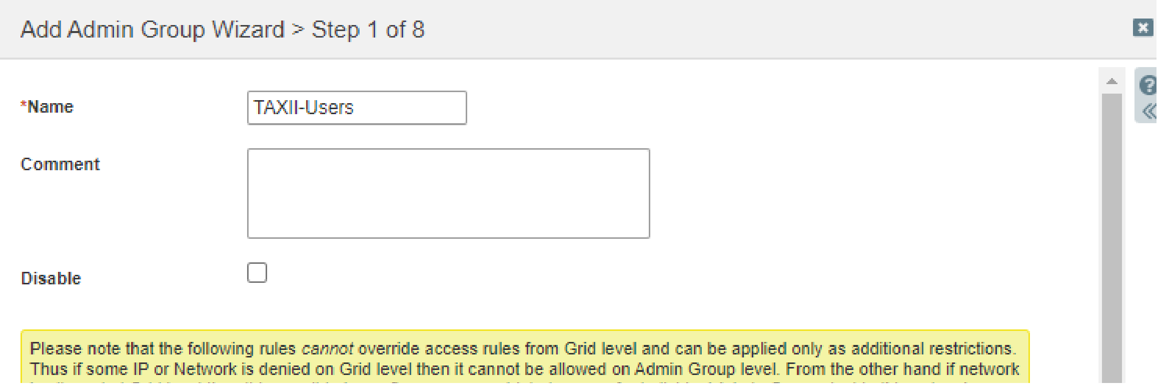


2. Click the **Add** icon located above the list of Admin Groups.



|  | Name | Superuser |
|---|---|---|
| □ | admin-group | Yes |

3. Give the **Admin Group** a relevant **Name**.



Add Admin Group Wizard > Step 1 of 8

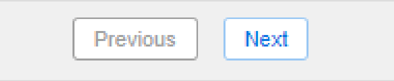
*Name: TAXII-Users

Comment:

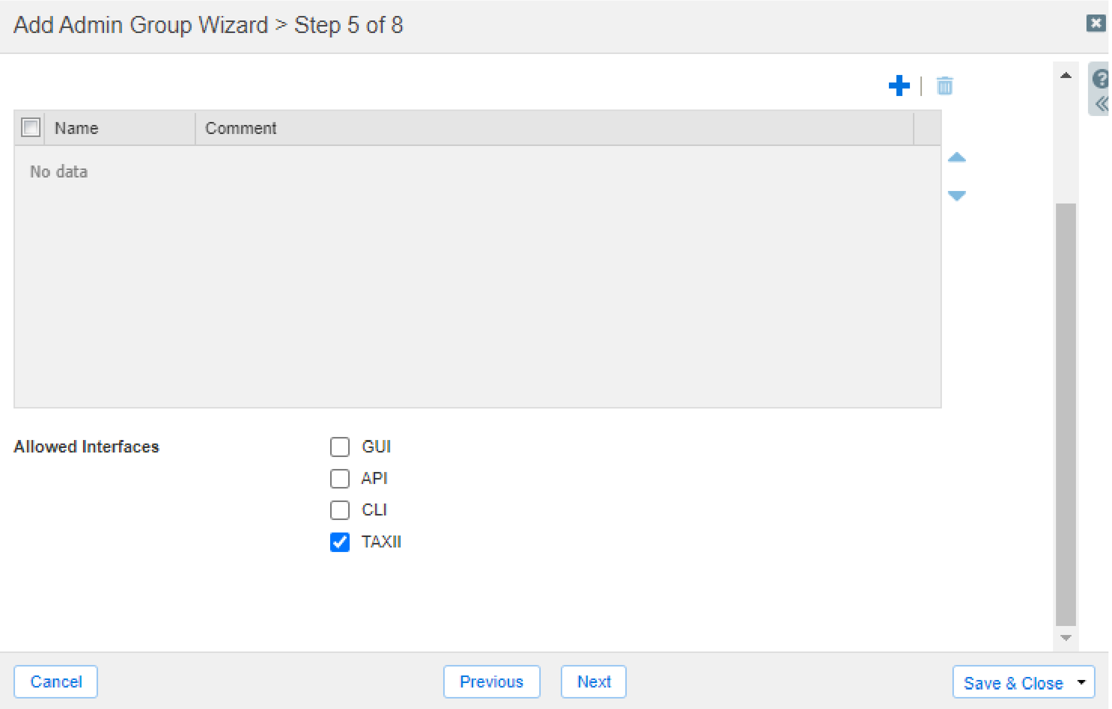
Disable: ☐

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

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.

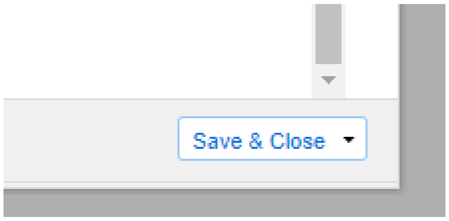


Add Admin Group Wizard > Step 5 of 8

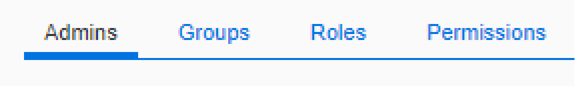
| ☐ | Name | Comment |
|---|---|---|
| | No data | |

Allowed Interfaces:
☐ GUI
☐ API
☐ CLI
☑ TAXII

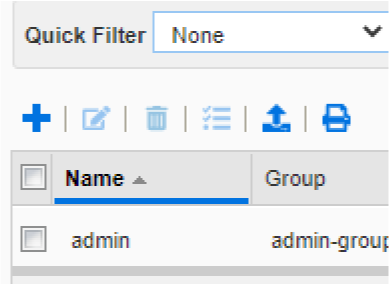
6. Click **Save & Close** to confirm the creation of the Admin Group.



7. Click the **Admins** tab.

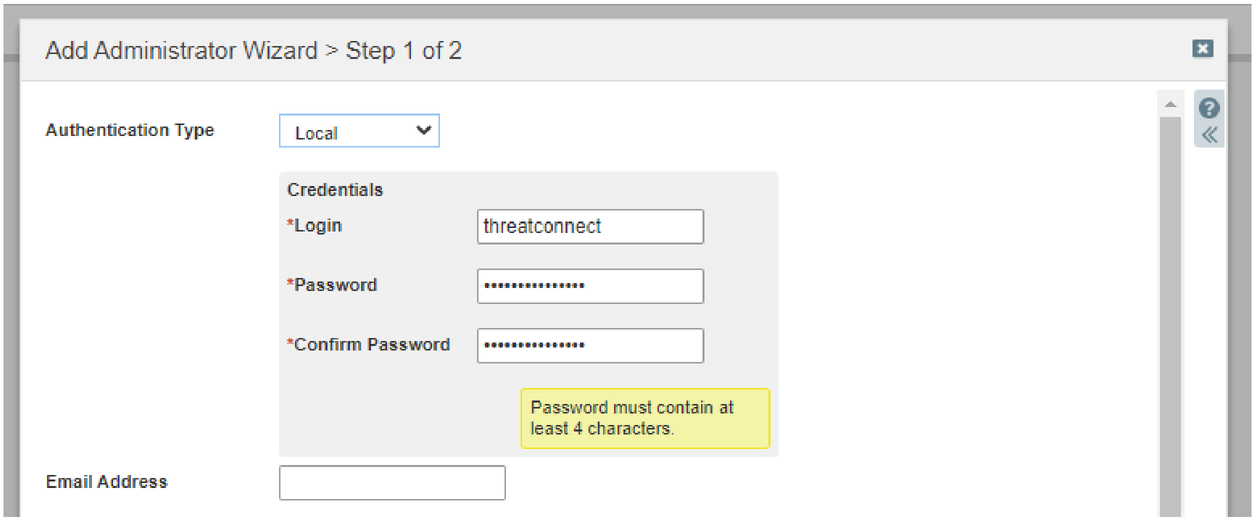


8. Click the **Add** icon located above the list of Admins.


Quick Filter: None

| □ | Name ▲ | Group |
|---|---|---|
| □ | admin | admin-group |

9. In the Add Administrator Wizard, give the new Administrator a **Login**, a **Password**, and **Confirm** the Password.


Add Administrator Wizard > Step 1 of 2

Authentication Type: Local

Credentials

*Login: threatconnect

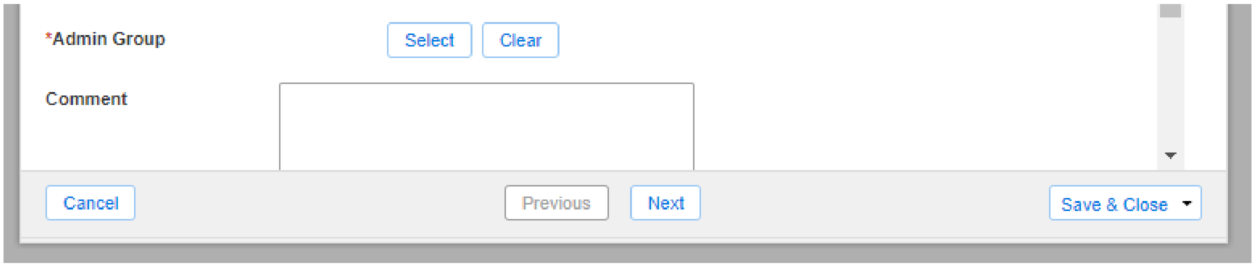
*Password: •••••••••••••••

*Confirm Password: •••••••••••••••

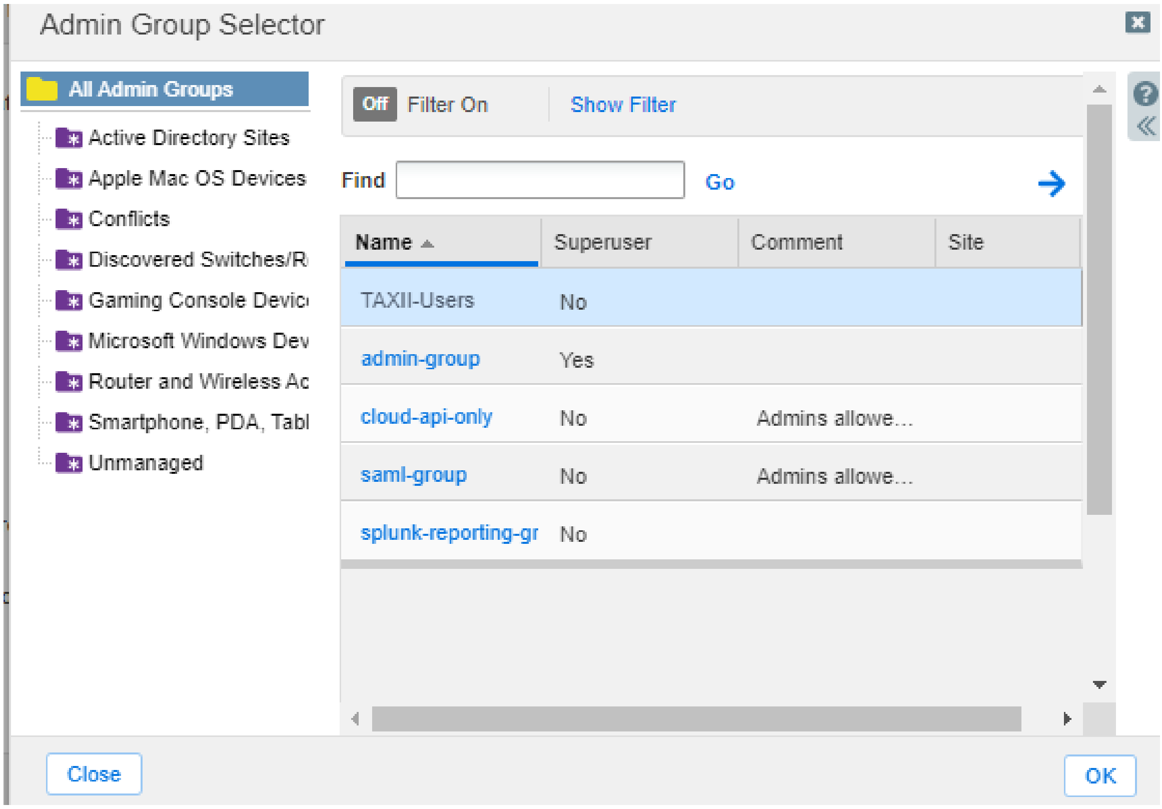
Password must contain at least 4 characters.

Email Address:

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



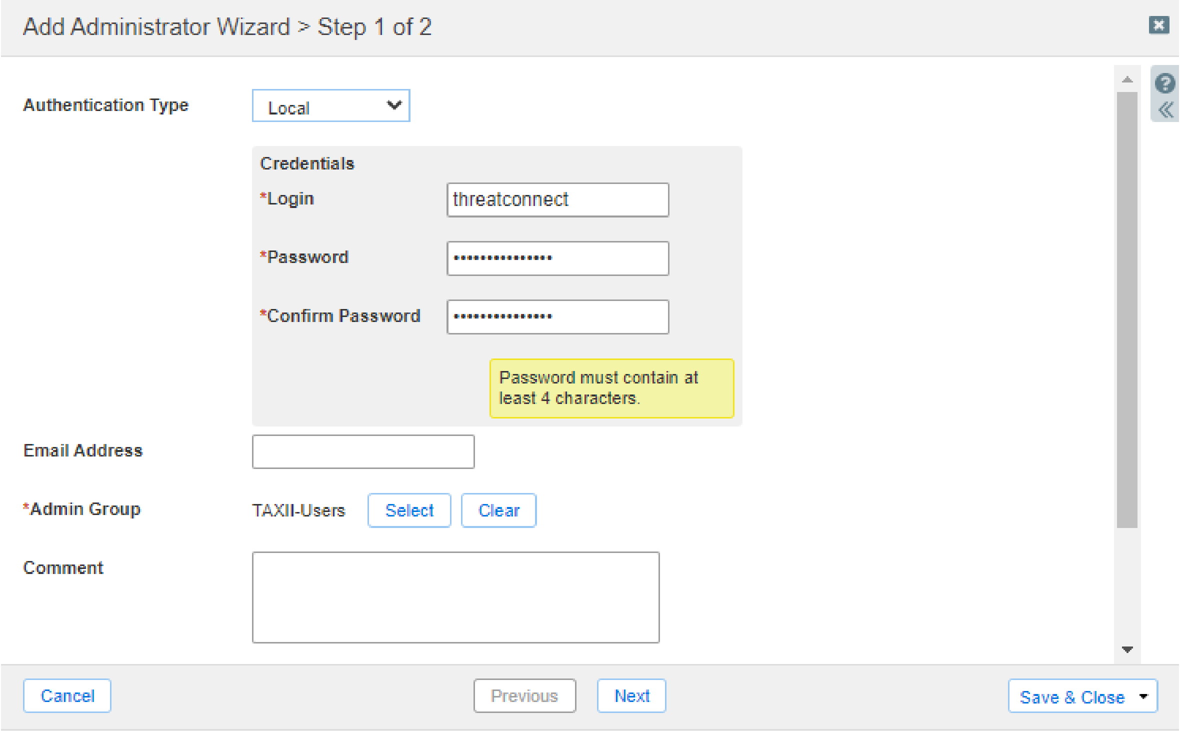
11. Locate and **Select** the **Admin Group** that was created on [pages 5 and 6](). Then, Click **OK** to confirm the selection.



Admin Group Selector

| 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.



Add Administrator Wizard > Step 1 of 2

Authentication Type: Local

Credentials

*Login: threatconnect

*Password: •••••••••••••••

*Confirm Password: •••••••••••••••

Password must contain at least 4 characters.

Email Address:

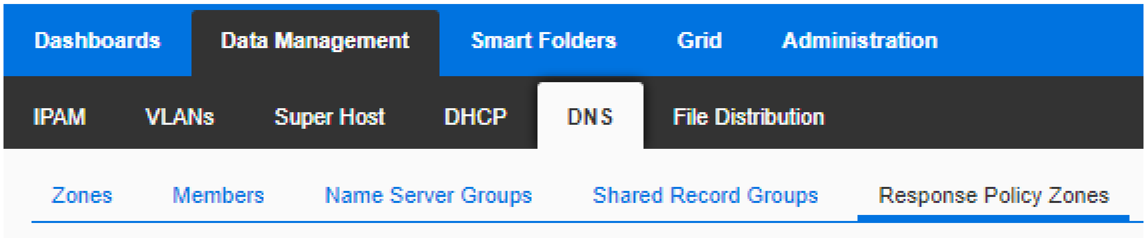
*Admin Group: TAXII-Users

Comment:

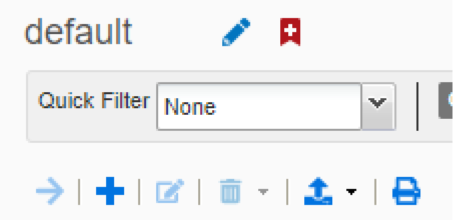
## Create a Response Policy Zone

To create a Response Policy Zone perform the following steps:

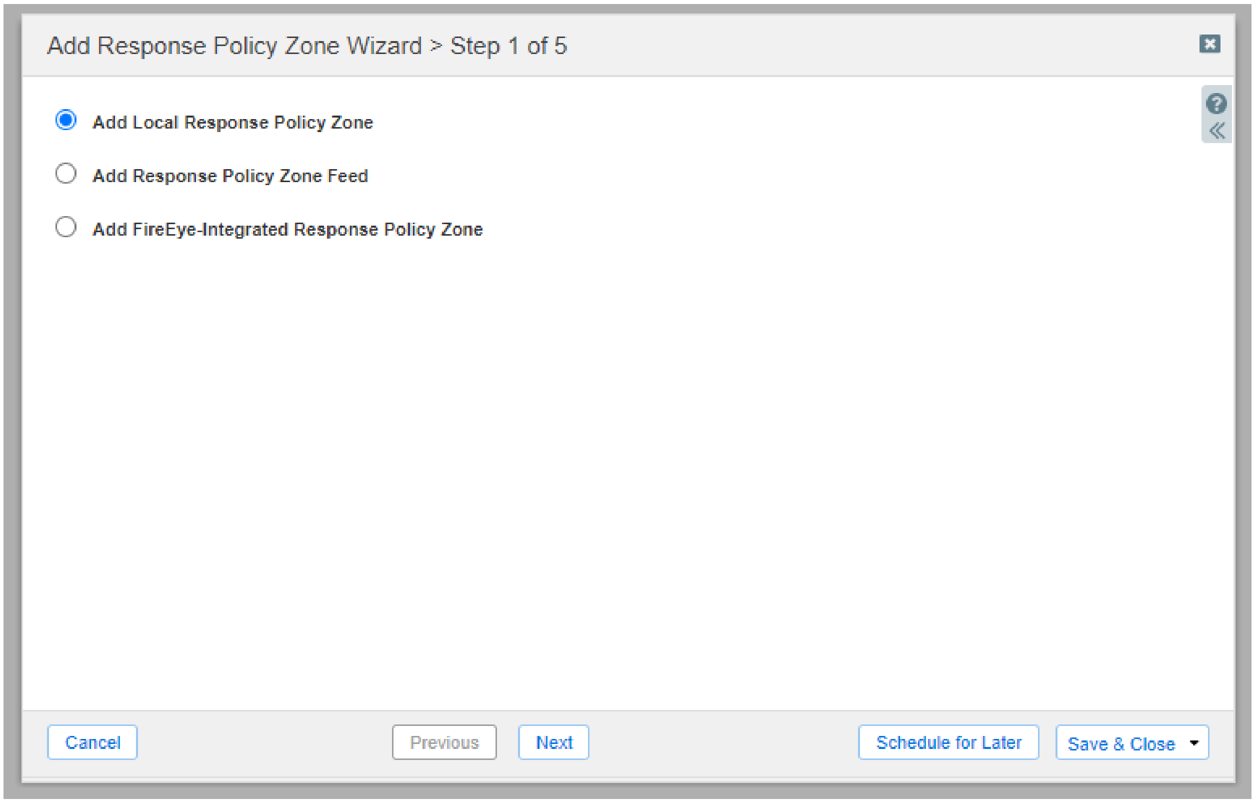
1. On the Web interface of the Infoblox Grid, navigate to **Data Management** → **DNS** → **Response Policy Zone**.



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**.



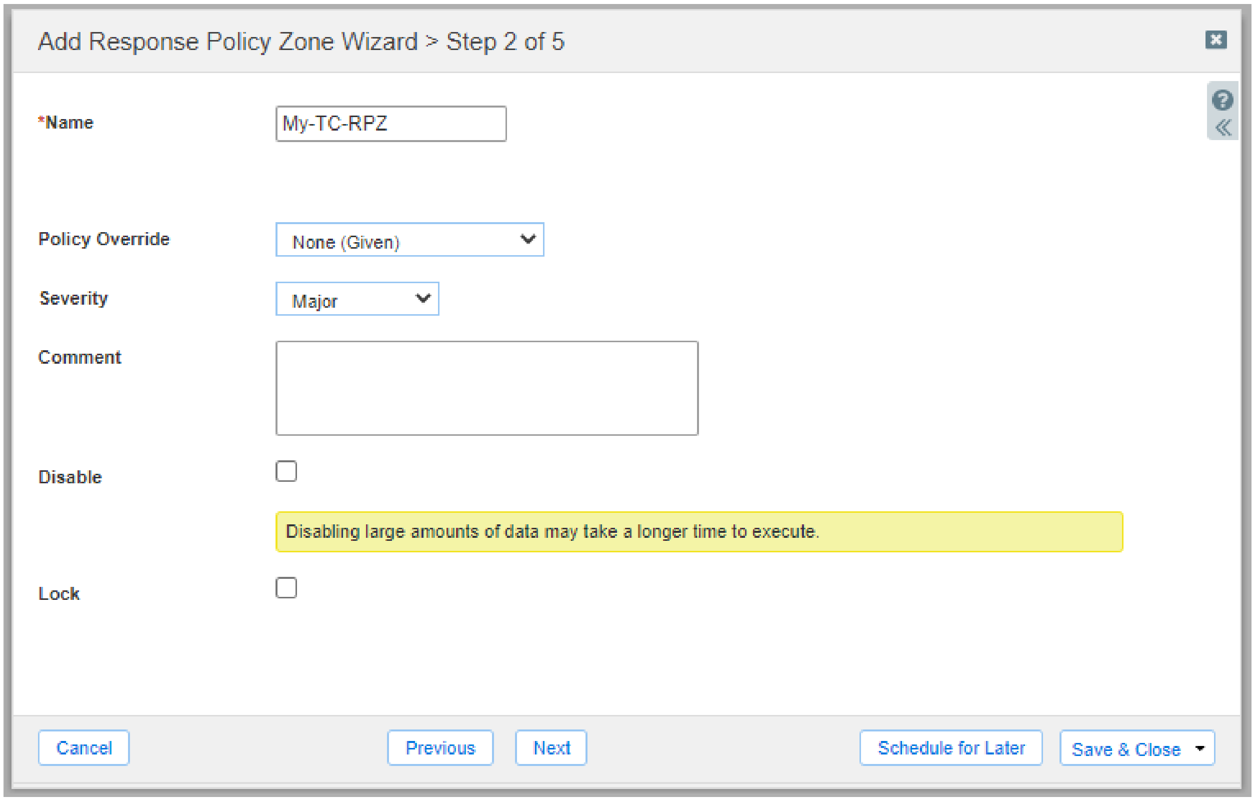
Add Response Policy Zone Wizard > Step 1 of 5

● Add Local Response Policy Zone

○ Add Response Policy Zone Feed

○ Add FireEye-Integrated Response Policy Zone

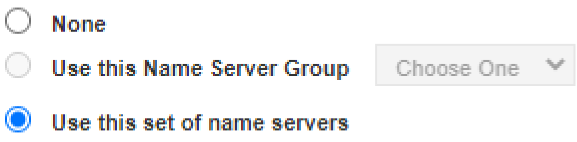
4. Give the Response Policy Zone a **Name** and set all relevant parameters. Then, click **Next**.



Add Response Policy Zone Wizard > Step 2 of 5

| | |
|---|---|
| *Name | My-TC-RPZ |
| Policy Override | None (Given) |
| Severity | Major |
| Comment | |
| Disable | □ |
| | Disabling large amounts of data may take a longer time to execute. |
| Lock | □ |

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

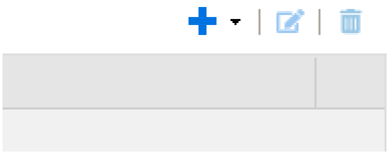


○ None

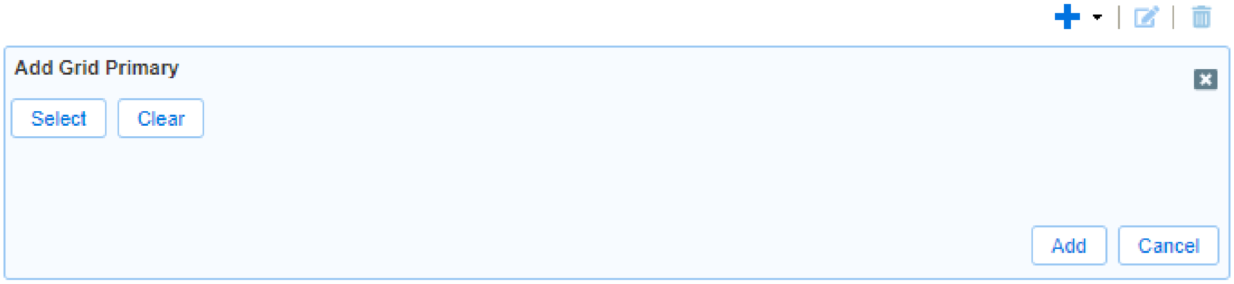
○ Use this Name Server Group   Choose One

● Use this set of name servers

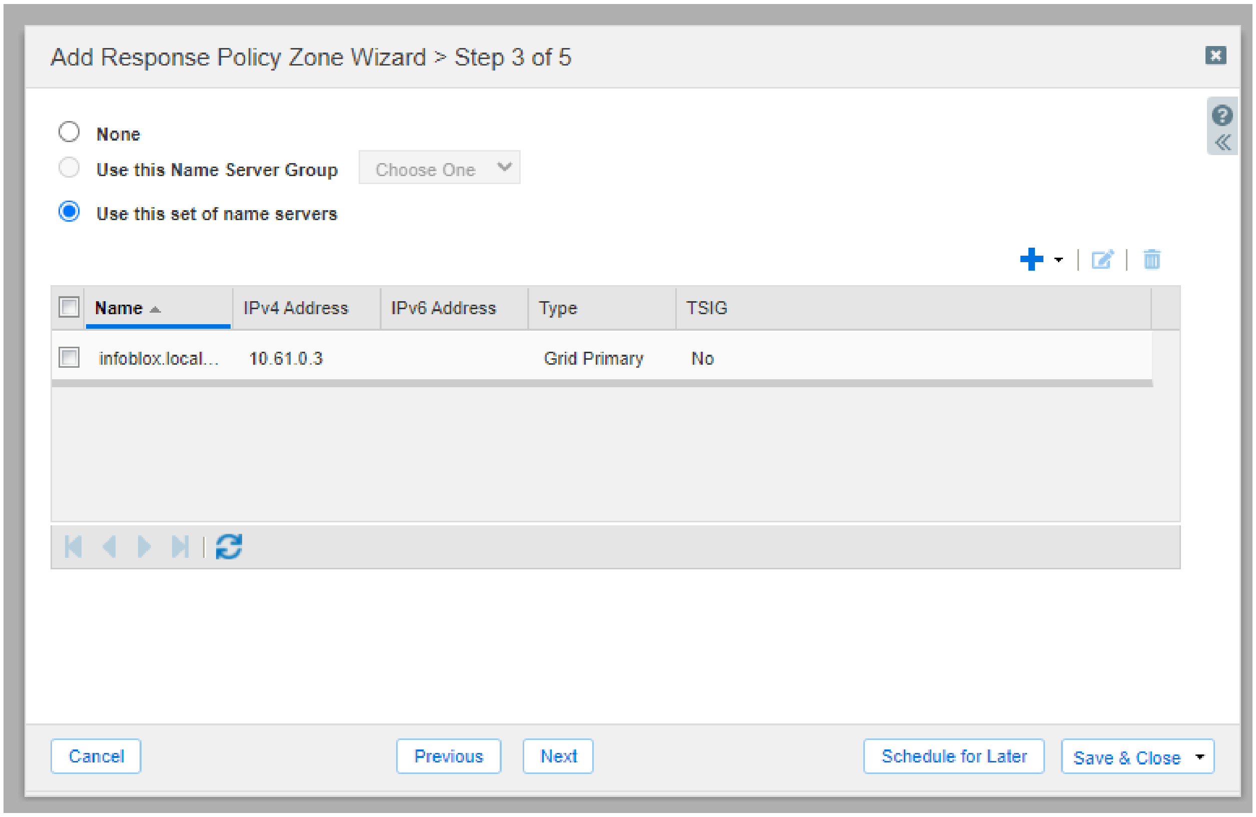
6. Click the **Add** icon.



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.



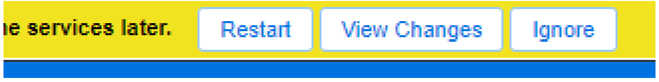
8. Click **Save & Close** to confirm the creation of the new Response Policy Zone.


Add Response Policy Zone Wizard > Step 3 of 5

○ None
○ Use this Name Server Group [Choose One]
● Use this set of name servers

| □ | Name ▲ | IPv4 Address | IPv6 Address | Type | TSIG |
|---|---|---|---|---|---|
| □ | infoblox.local... | 10.61.0.3 |  | Grid Primary | No |

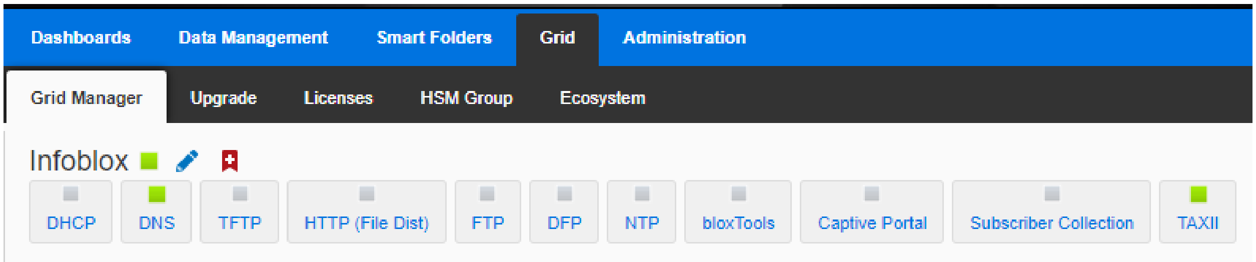
13. When prompted, restart all relevant services by clicking **Restart** located on the banner at the top.



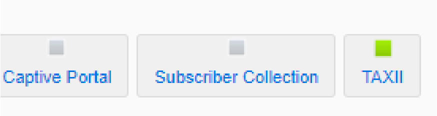
## Assign a Response Policy Zone to Sync with ThreatConnect

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

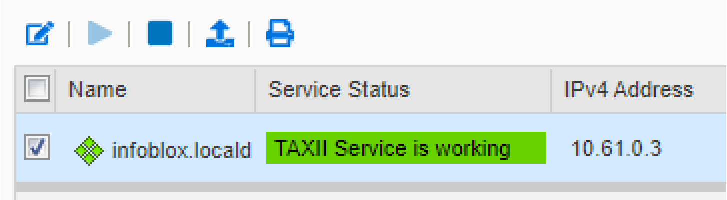
1. On the Web interface of the Infoblox Grid, navigate to **Grid** → **Grid Manager**.



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

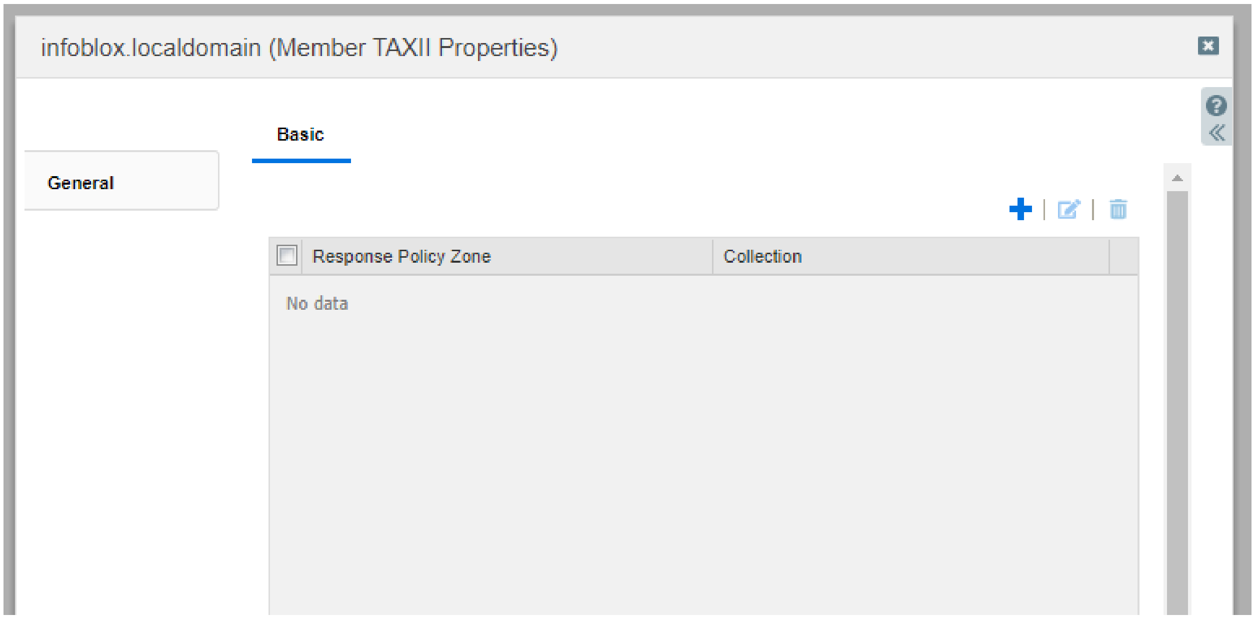


3. Click the **checkbox** associated with the **grid member** that is currently running the TAXII service. Then, Click the **Edit** icon located above the table of members.



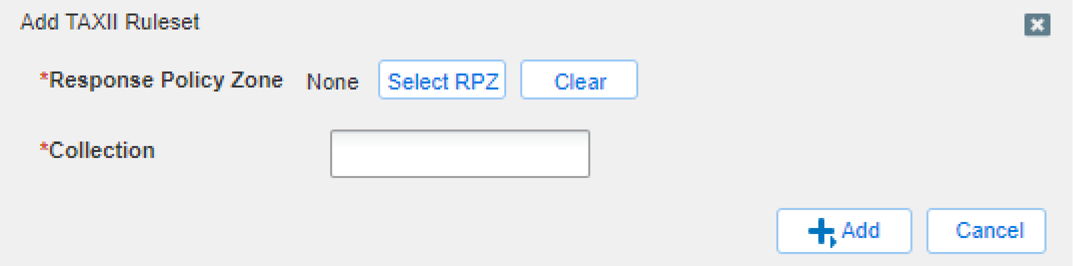
| □ | Name | Service Status | IPv4 Address |
|---|---|---|---|
| ☑ | infoblox.locald | TAXII Service is working | 10.61.0.3 |

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


infoblox.localdomain (Member TAXII Properties)

| □ | Response Policy Zone | Collection |
|---|---|---|
| No data | | |

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

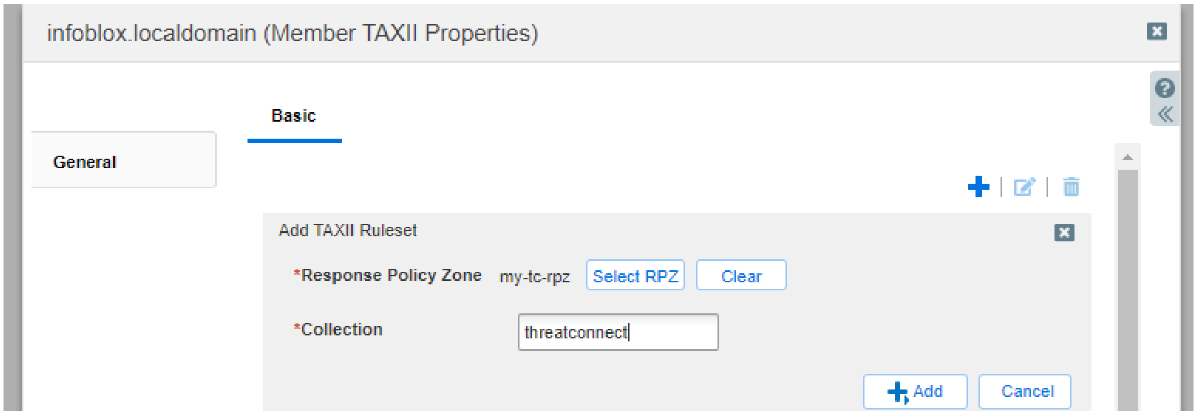


Add TAXII Ruleset

*Response Policy Zone None

*Collection

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.*



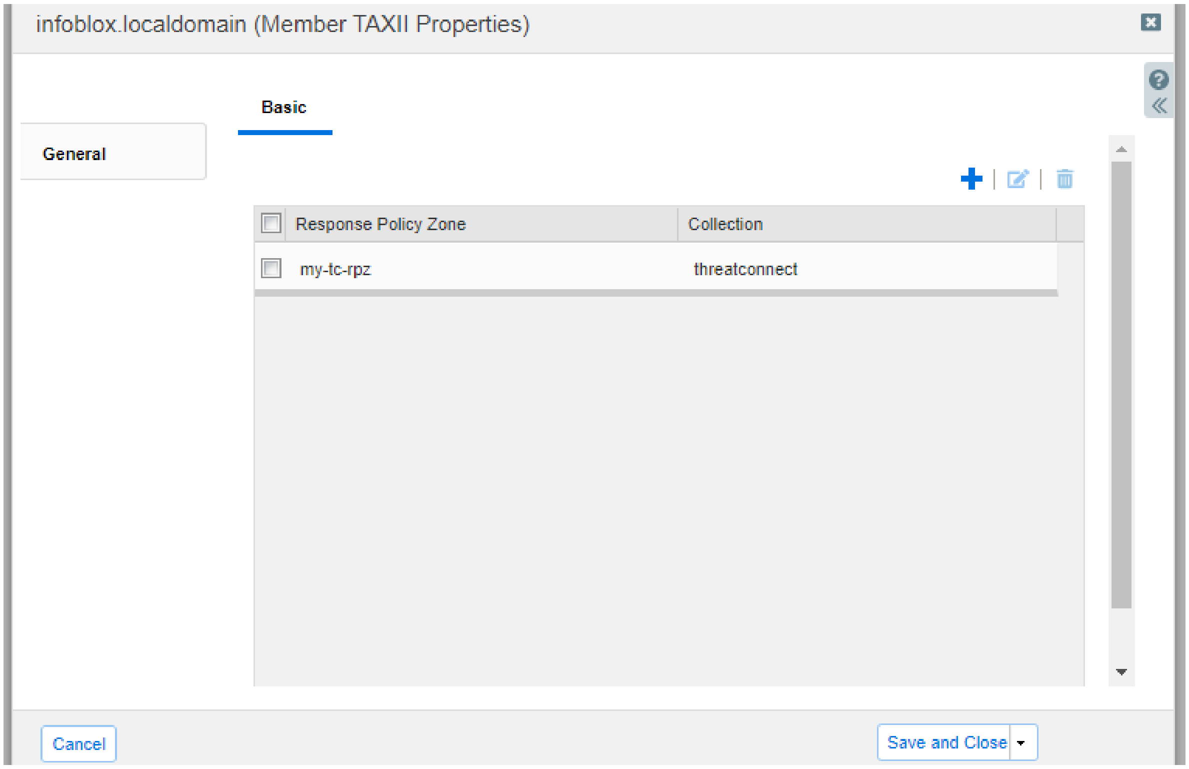
infoblox.localdomain (Member TAXII Properties)

Add TAXII Ruleset

*Response Policy Zone my-tc-rpz

*Collection threatconnect

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



infoblox.localdomain (Member TAXII Properties)

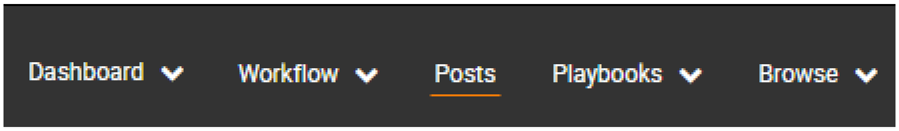
| □ Response Policy Zone | Collection |
|---|---|
| □ my-tc-rpz | threatconnect |

## ThreatConnect Configuration

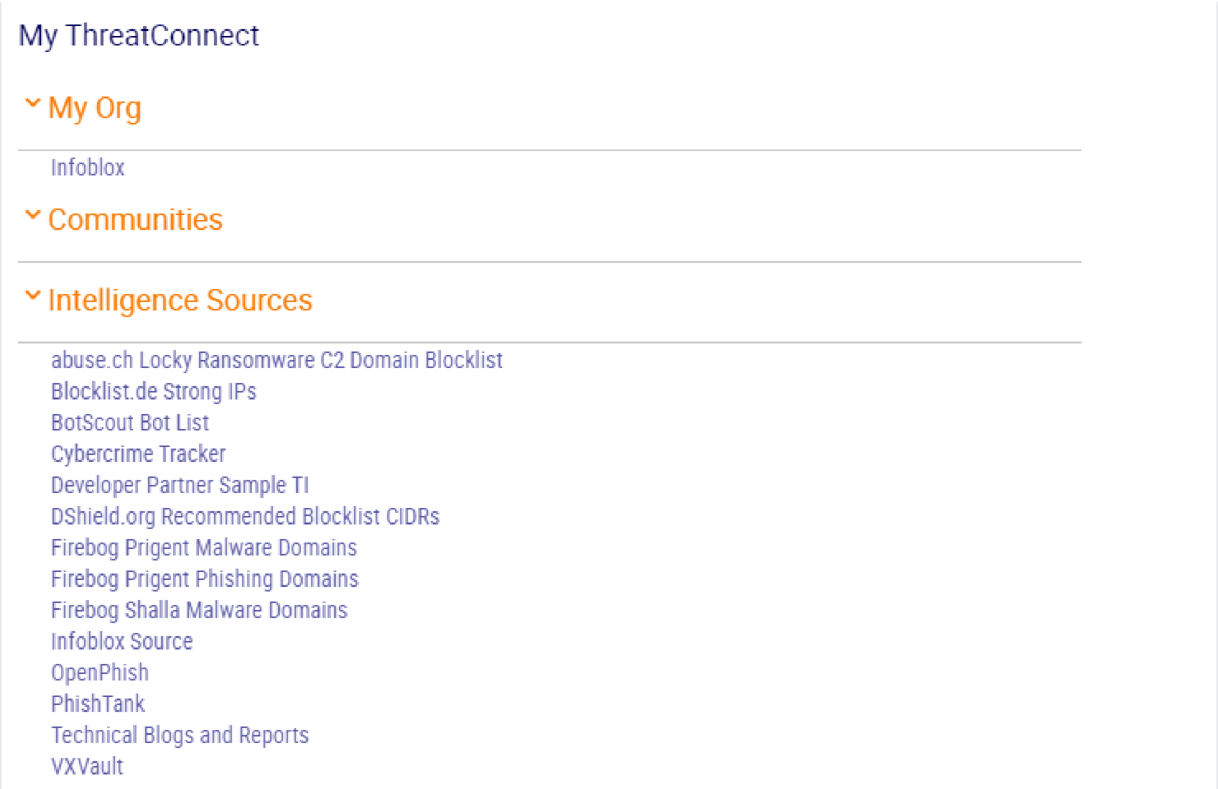
### Create an Outbound TAXII Exchange

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.



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

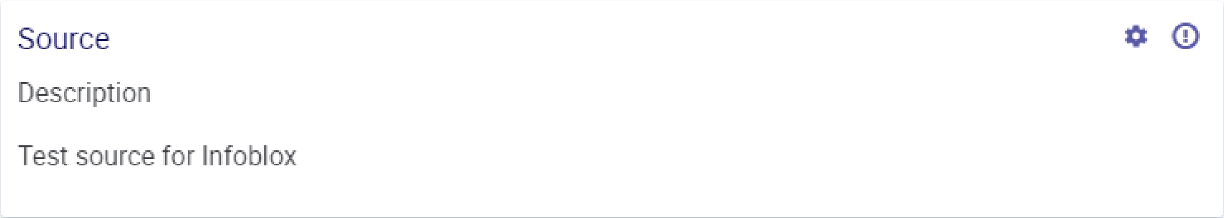
Infoblox

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.

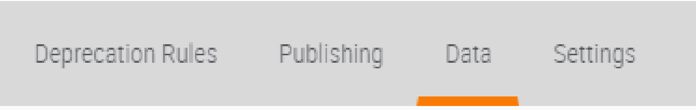


Source

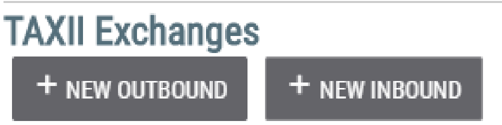
Description

Test source for Infoblox

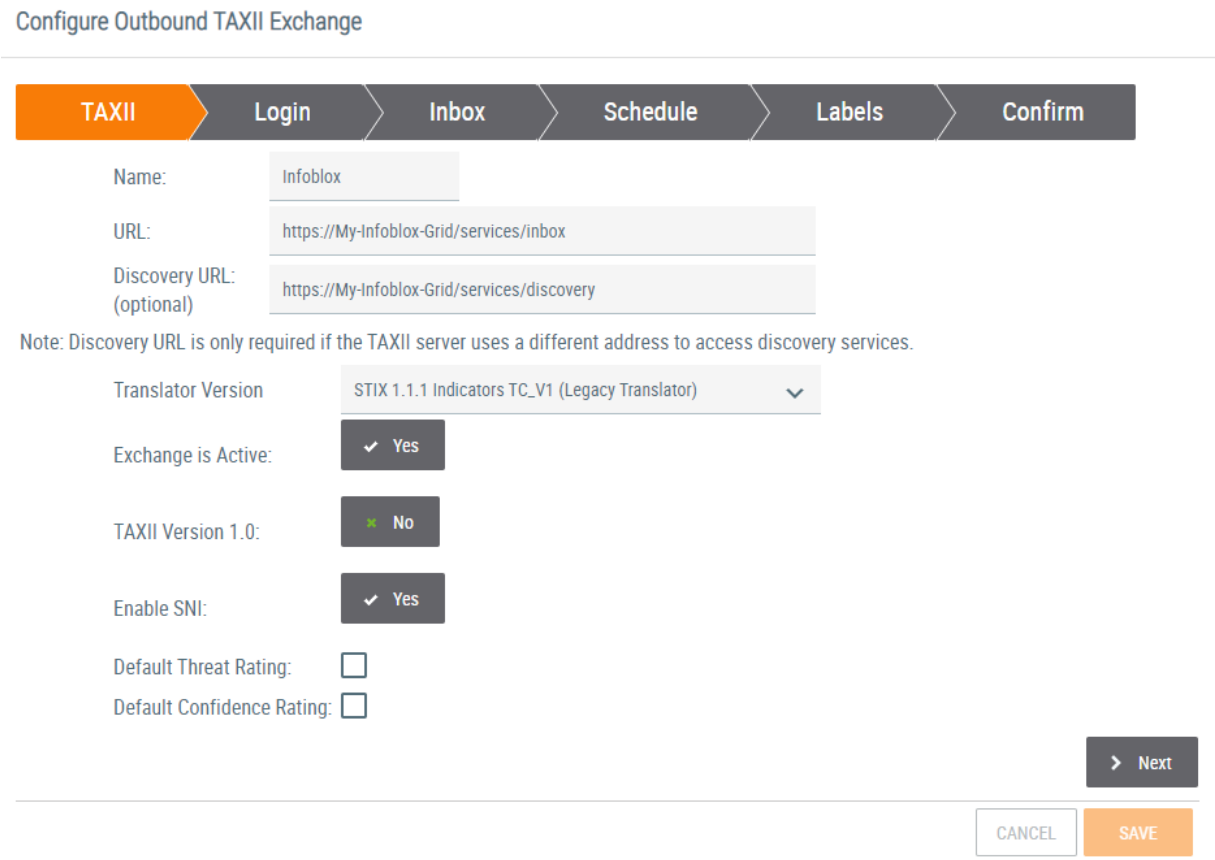
4. Click **Data** in the navigation bar at the top of the screen.



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



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



Configure Outbound TAXII Exchange

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

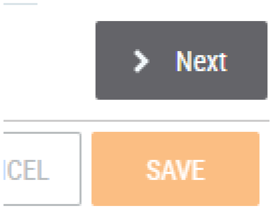
Enable SNI: ✓ Yes

Default Threat Rating: □

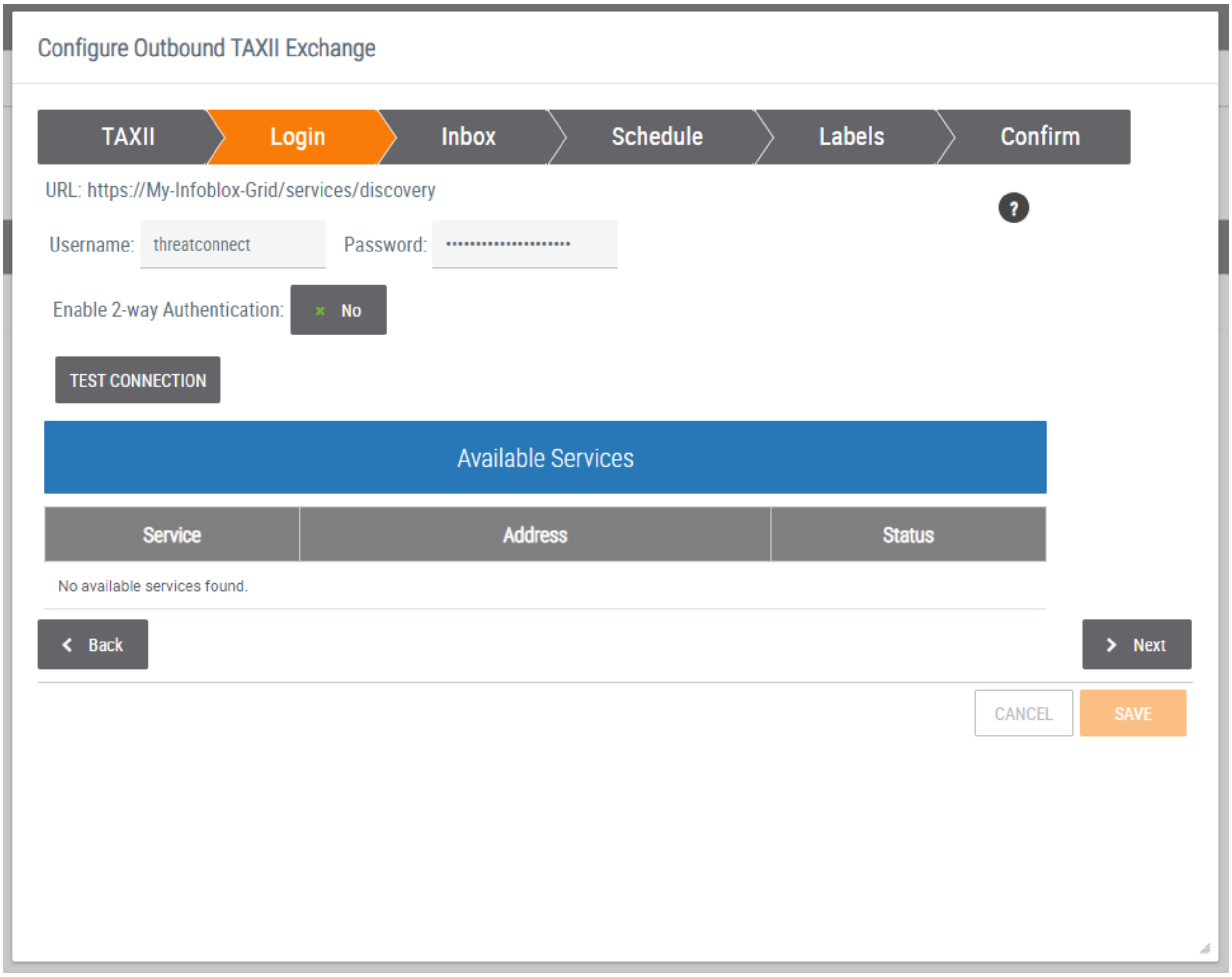
Default Confidence Rating: □

- **Name**: Input a relevant name for this Outbound TAXII Exchange.
- **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.*
- (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.*
- (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 5 of this document.


Configure Outbound TAXII Exchange

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

Username: threatconnect Password: ••••••••••••••••••••••

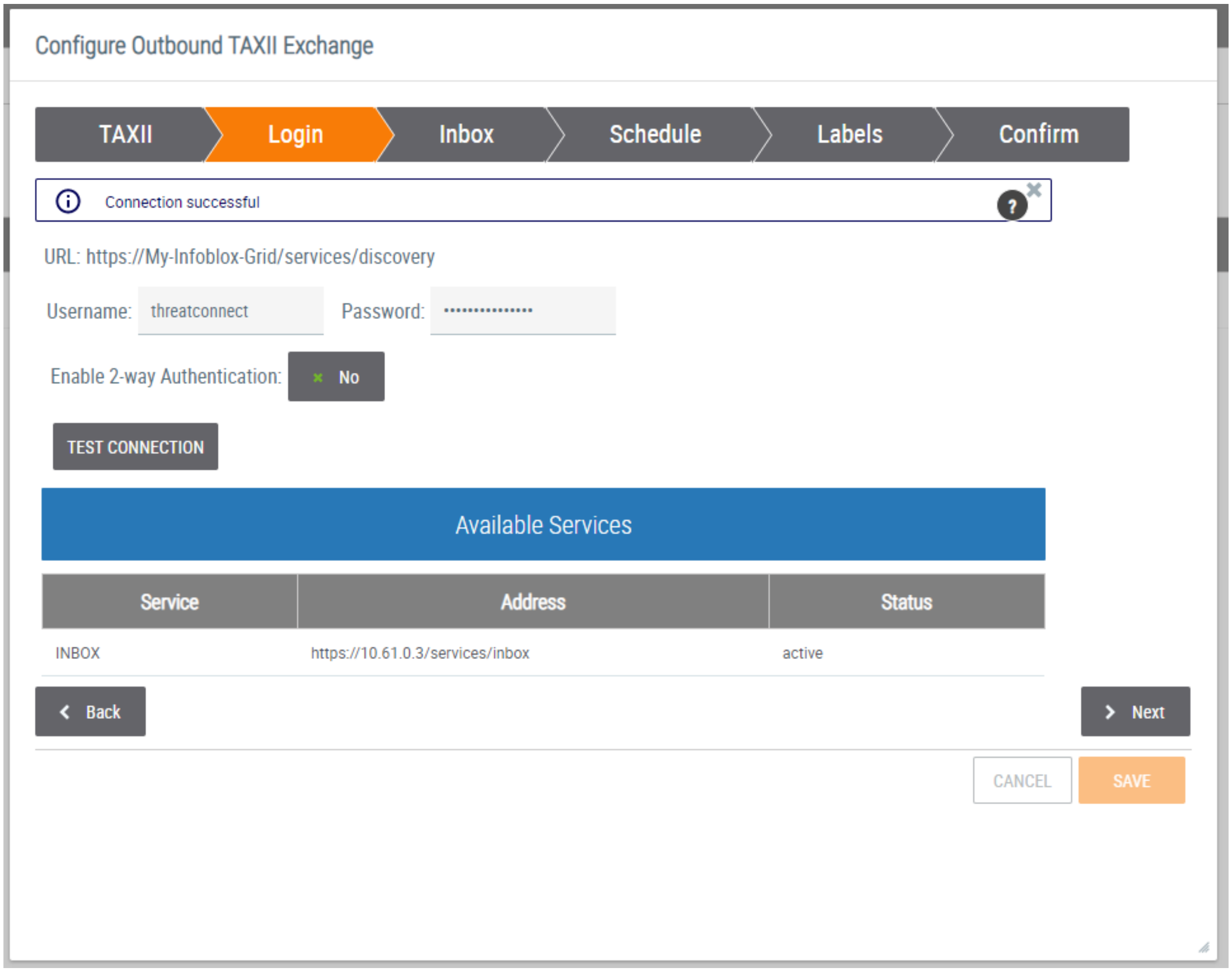
Enable 2-way Authentication: ✗ No

Available Services

| Service | Address | Status |
|---|---|---|

No available services found.

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



Configure Outbound TAXII Exchange

Connection successful

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

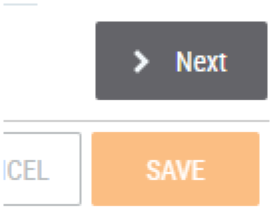
Username: threatconnect Password: •••••••••••••••

Enable 2-way Authentication: ✕ No

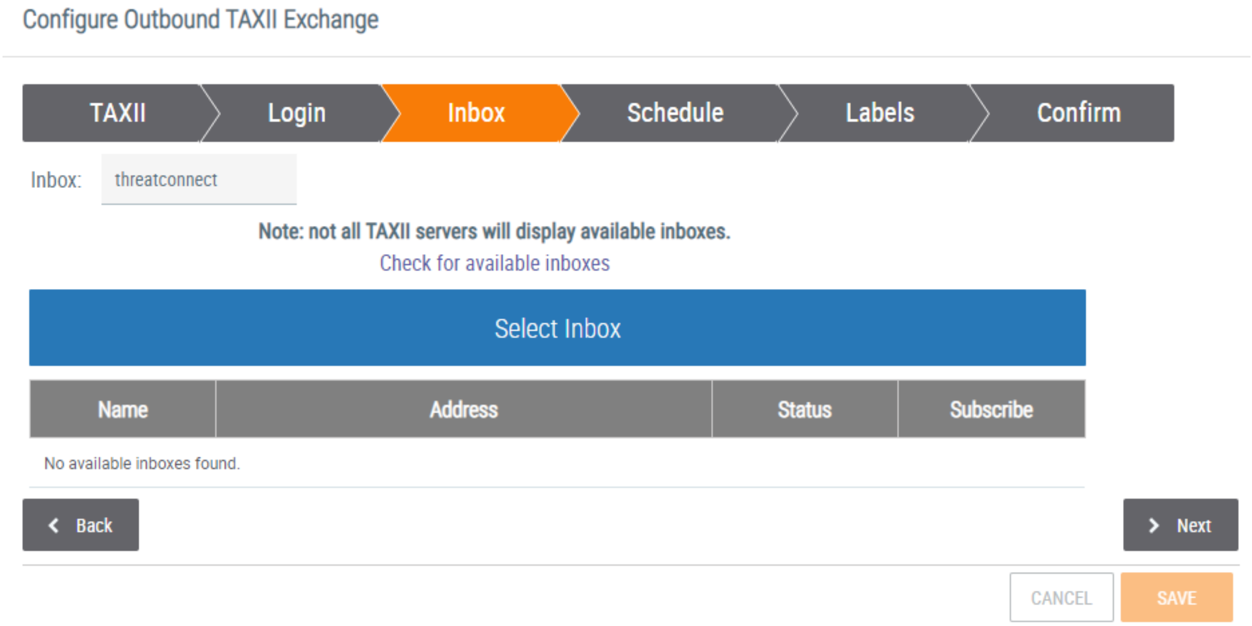
Available Services

| Service | Address | Status |
|---|---|---|
| INBOX | https://10.61.0.3/services/inbox | active |

10. Click **Next**.



11. Input an **Inbox.** *Note: this value should correspond to the Collection that was assigned in infoblox on [pages 12 and 13](#).*



Configure Outbound TAXII Exchange

Inbox: threatconnect

Note: not all TAXII servers will display available inboxes.

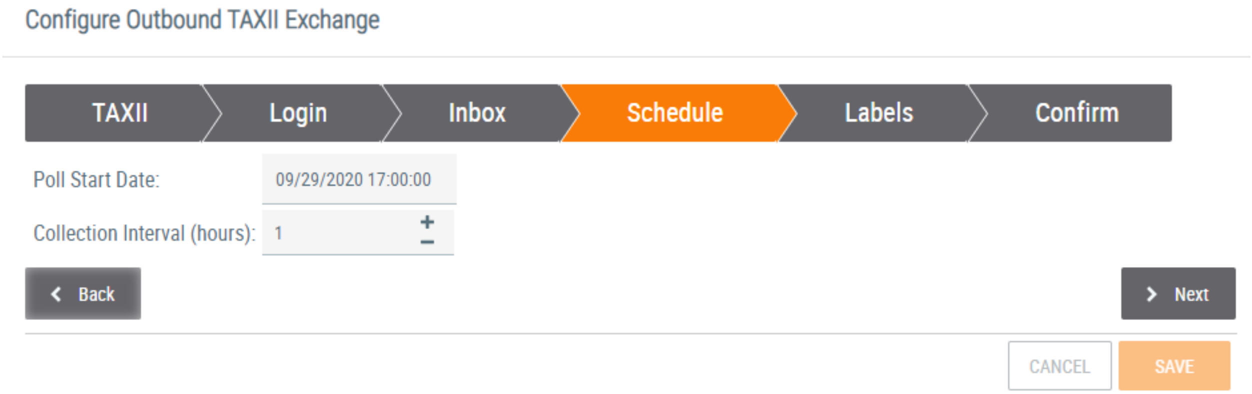
Check for available inboxes

Select Inbox

| Name | Address | Status | Subscribe |
|---|---|---|---|

No available inboxes found.

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

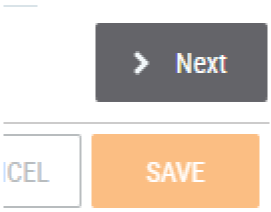


Configure Outbound TAXII Exchange

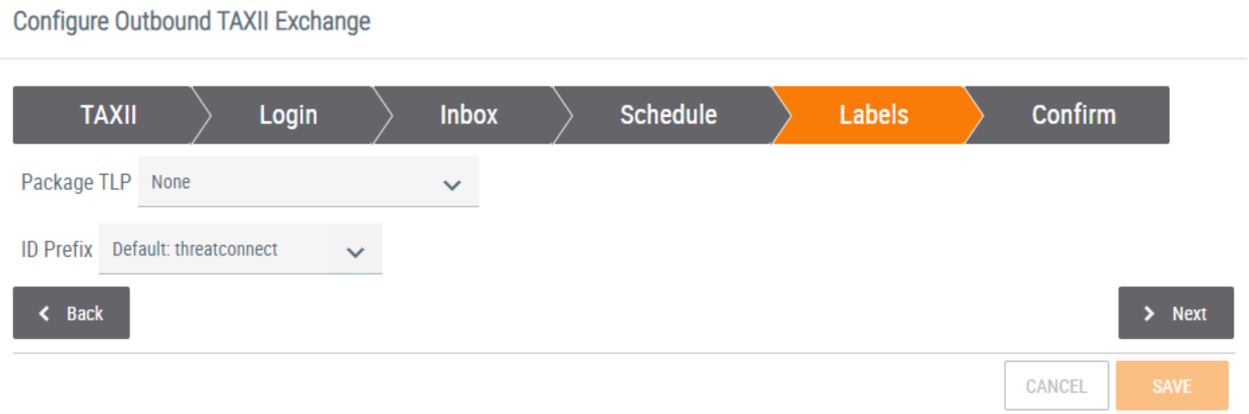
Poll Start Date: 09/29/2020 17:00:00

Collection Interval (hours): 1

13. Click **Next.**



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

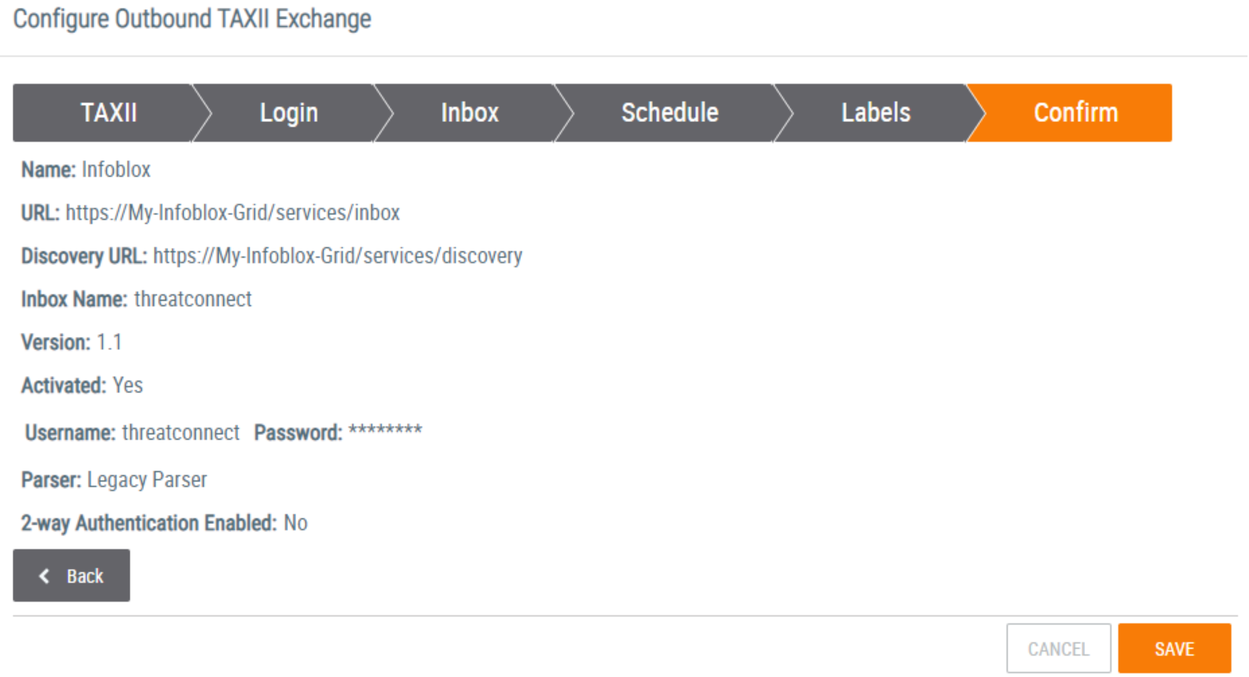


Configure Outbound TAXII Exchange

Package TLP: None

ID Prefix: Default: threatconnect

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



Configure Outbound TAXII Exchange

**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:** ********

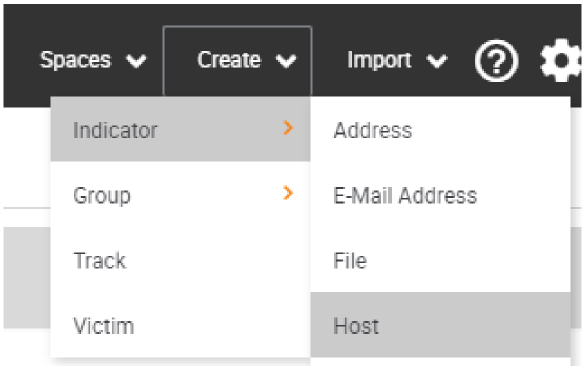
**Parser:** Legacy Parser

**2-way Authentication Enabled:** No

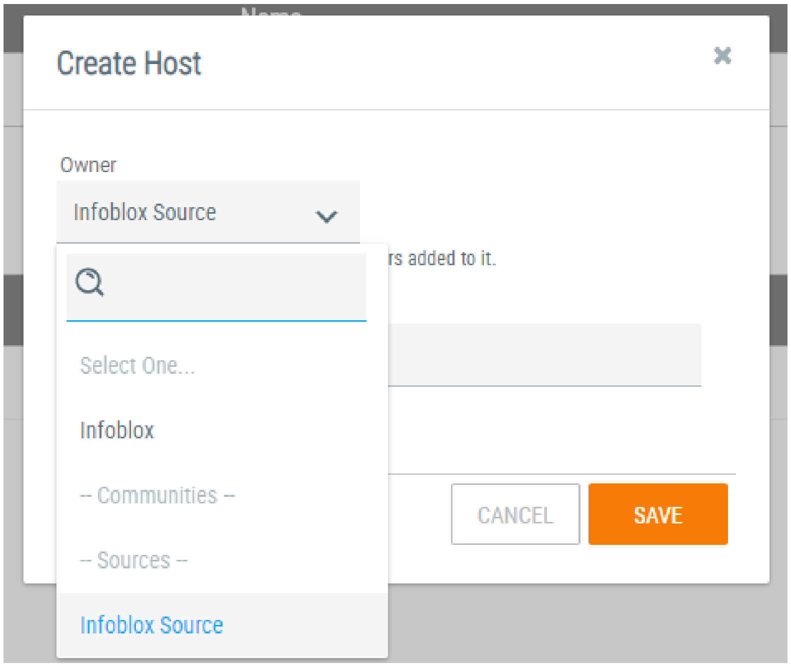
### Test the configuration

To 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**.

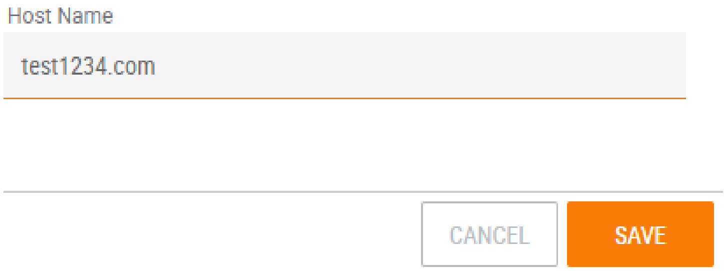


2. Click the drop-down associated with the **Owner**. Change the **Owner** to your **Org's Source**. *Note: In the example screenshot the Org is Infoblox, and the source is Infoblox Source.*

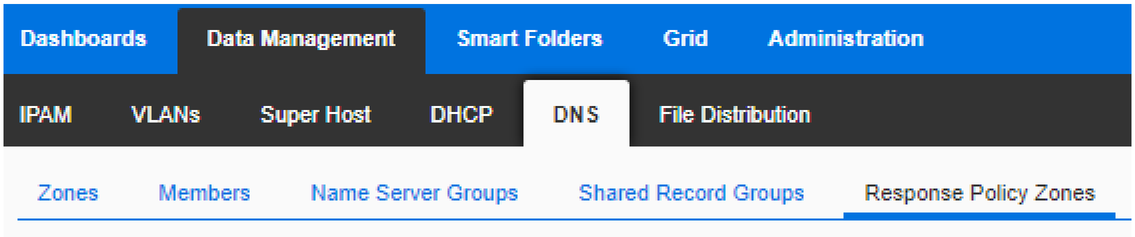

Create Host

Owner: Infoblox Source

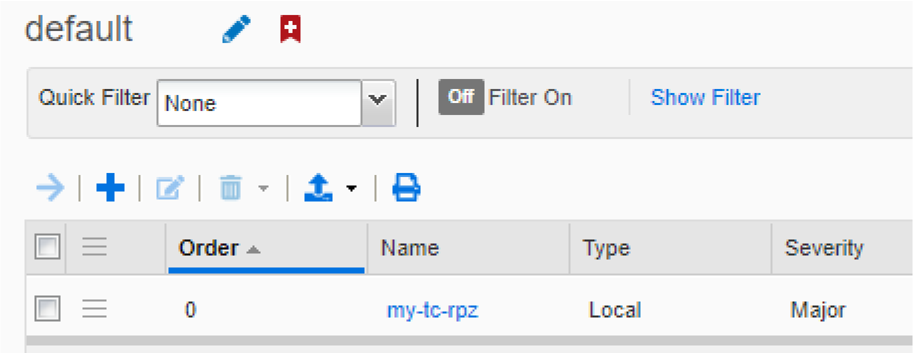
3. In the **Host Name** text field, input an example domain name. Then, click **Save**.


Host Name: test1234.com

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.

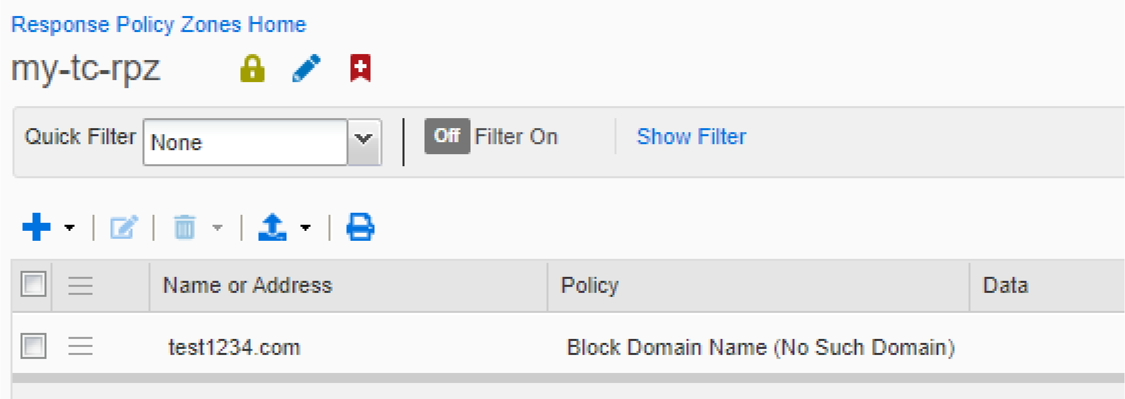

default

Quick Filter None

Off Filter On

| Order ▲ | Name | Type | Severity |
|---|---|---|---|
| 0 | my-tc-rpz | Local | Major |

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



my-tc-rpz

Quick Filter None

Off Filter On

| Name or Address | Policy | Data |
|---|---|---|
| test1234.com | Block Domain Name (No Such Domain) | |

## Additional Resources

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

1. Infoblox Documentation Website: https://docs.infoblox.com/
2. Infoblox Website: https://www.infoblox.com/
3. Infoblox Community Website: https://community.infoblox.com/
4. ThreatConnect Website: https://threatconnect.com/

Corporate Headquarters | 2390 Mission College Boulevard, Ste. 501 | Santa Clara, CA | 95054
+1.408.986.4000 | info@infoblox.com | www.infoblox.com