CONFIGURATION CHANGE GUIDE

NIOS RPZ Feeds Update for SURBL EOS

Table of Contents

Overview

This document is intended to assist with the transition associated with the end of sale of SURBL feeds in BloxOne Threat Defense, used in NIOS Response Policy Zones (RPZ). SURBL feeds will no longer be available to BloxOne Threat Defense customers because Infoblox has determined that indicators in these feeds are duplicated in other feeds or not relevant. For users currently including SURBL feeds in their policies, Infoblox recommends enabling other feeds provided in BloxOne Threat Defense. This document covers how to remove SURBL feeds from NIOS RPZ and replace them with feeds that offer more effective coverage.

This document covers the removal of the following feeds that are reaching EOS:

SURBL Multi: This feed is a data set of malicious domains or abused web sites.

SURBL Multi Lite: An alternate set of the SURBL Threat Feed.

SURBL Fresh: Fresh is a list of domains that have been recently added to TLD zone file delegations.

The following feeds should be used:

Infoblox NOED: The NOED feed consists of newly observed and emerging domains, some of which may not be inherently suspicious. However, monitoring traffic to these domains may be advisable because there is a low likelihood of their being visited under normal circumstances, which raises the possibility of their being used for potentially nefarious purposes.

Infoblox Suspicious NOED: This feed includes high-risk, newly active domains. These domains have only recently become active and share one or more characteristics with other known malicious domains to warrant concern.

Anti-Malware: This feed enables protection against hostnames that contain known malicious threats that can act on or take control of your system, such as malware command and control (C&C), malware download and active phishing sites.

Malware DGA: Domain generation algorithms (DGA) appear in various families of malware used to periodically generate many domain names that can act as rendezvous points with their C&C servers.

Base: The base feed enables protection against known hostnames that are dangerous as destinations and are sources of threats such as APTs, bots, compromised host/domains, exploit kits, malicious name servers and sinkholes.

Best Practices

Infoblox recommends the following as best practices for customers currently using the SURBL feeds described in this document.

- Remove all SURBL feeds from NIOS RPZ prior to the EOS date and replace with the recommendations below. When the SURBL feeds reach EOS, NIOS will no longer be able to sync them from the CSP, leading to an error state.
- When replacing feeds with the recommendations below, consider policy settings, e.g., logging vs blocking, of currently used feeds and replicate them for the replacements.
- Infoblox recommends all customers use the AntiMalware, Malware DGA, and Base feeds. Ideally, you are already syncing these feeds to NIOS RPZs. If you are not, enable them regardless of which SURBL feeds you are replacing.

Replacement Feed Mapping

This table shows the recommended replacements for each of the SURBL feeds. For **All Customers**, Feeds listed for Threat Defense Business should be used to replace the SURBL feeds.

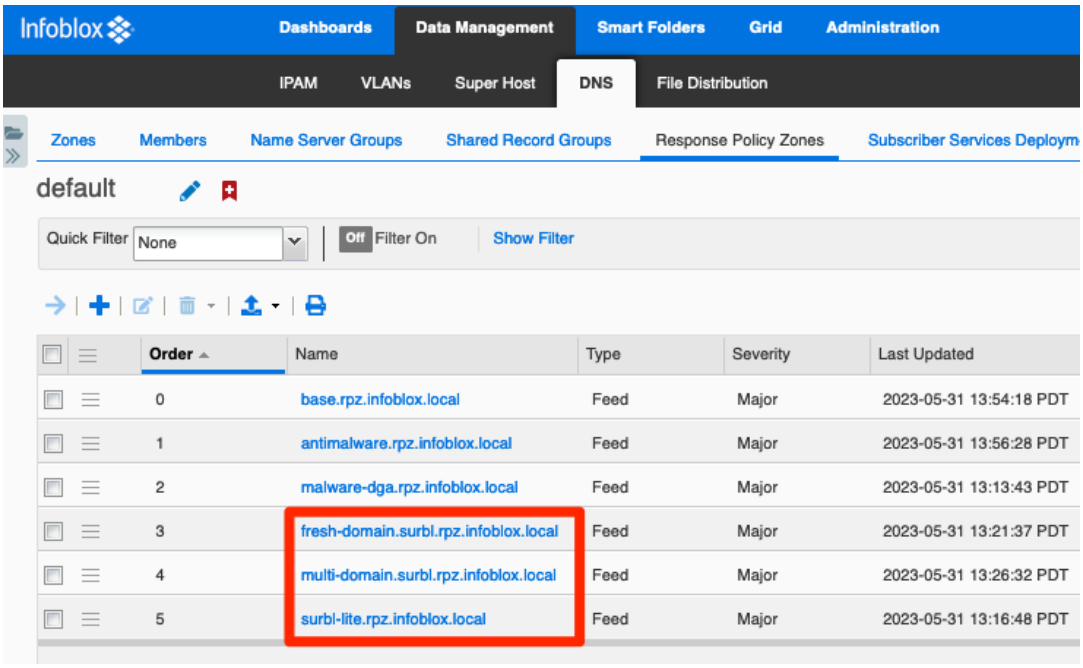
Customers with a BloxOne Threat Defense Advanced subscription should also consider enabling feeds shown for Threat Defense Advanced for even greater protection.

SURBL Feed	SURBL Fresh	SURBL Multi/SURBL Multi Lite
Threat Defense Business Feeds	Infoblox NOED	Antimalware Malware DGA Base
Threat Defense Advanced Feeds	Infoblox NOED Suspicious NOED	Antimalware Malware DGA Base Suspicious Domains Suspicious Lookalikes Suspicious NOED

Remove SURBL RPZ Feeds

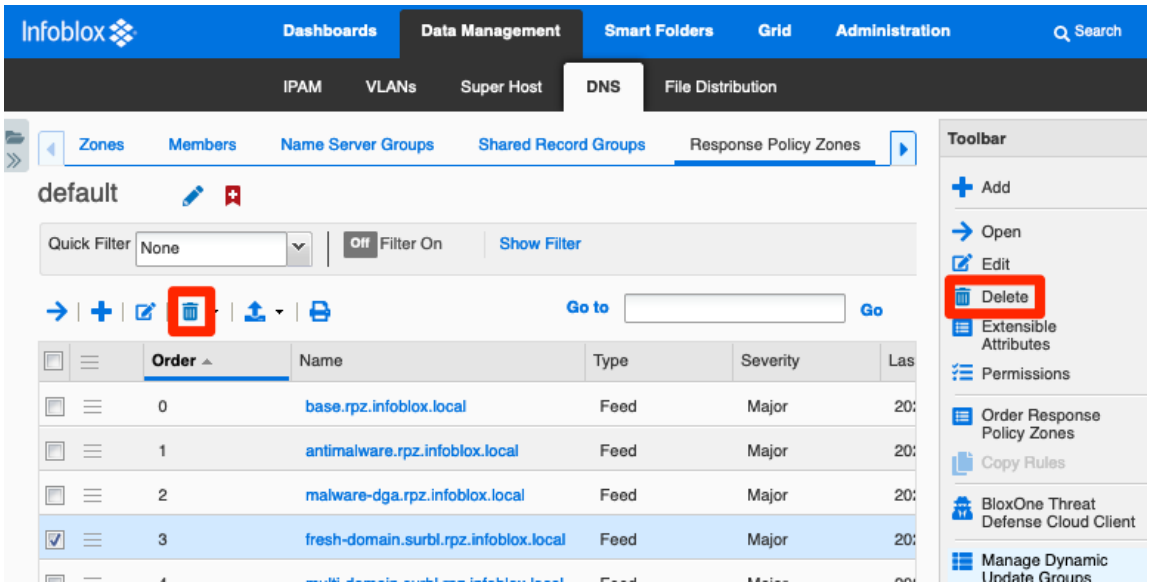
This section describes the process of identifying and removing SURBL feeds used for NIOS RPZs.

1. In NIOS Grid Manager, navigate to **Data Management → DNS → Response Policy Zones**.
2. Identify the SURBL feeds for removal. These can be identified by their Names: **fresh-domain.surbl.rpz.infoblox.local**, **multi-domain.surbl.rpz.infoblox.local**, and **surbl-lite.rpz.infoblox.local**.

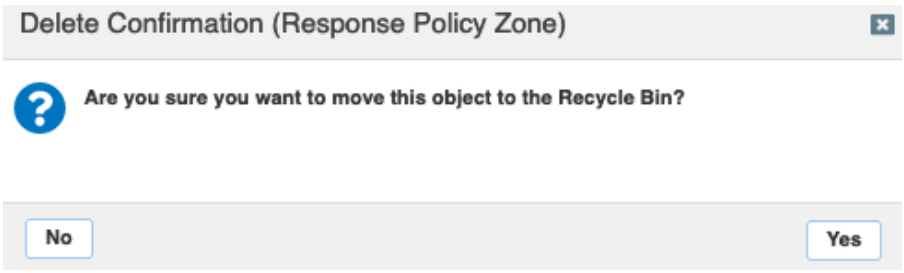


Note: If you have a large number of RPZs, use the search function to locate the SURBL feeds.

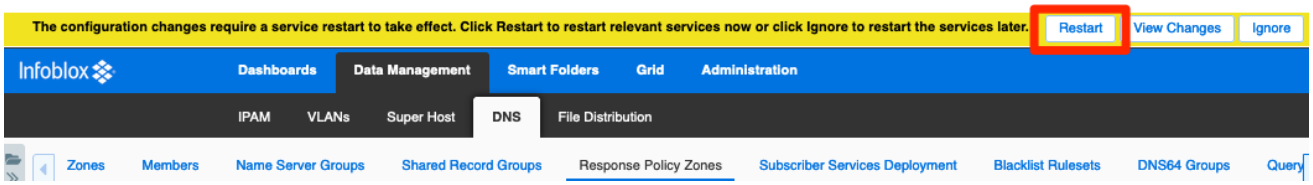
3. Select the **checkbox** associated with one of these feeds.
4. Click the (trashcan icon) or the **Delete** button in the Toolbar.



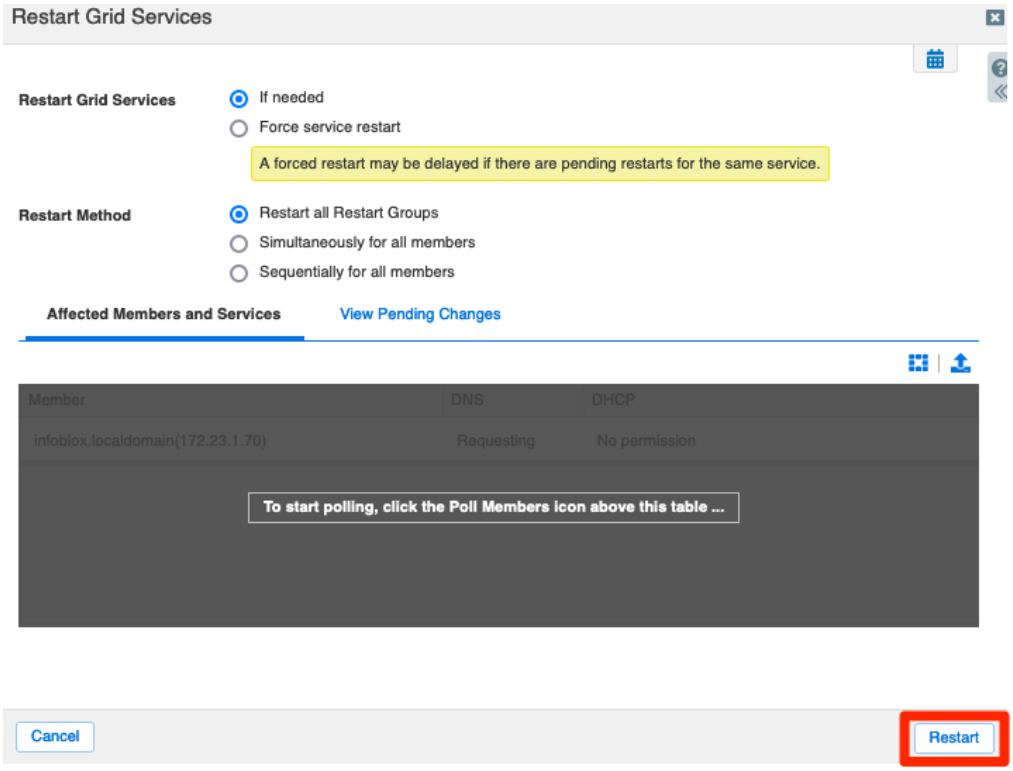
5. Click **Yes** in the Delete Confirmation dialog.



6. If you are removing multiple feeds, repeat steps 3-5 for each.
7. Deletion of RPZs requires a service restart to take effect. In the banner at the top of the Grid Manager window, click on **Restart**.



8. In the Restart Grid Services dialog, adjust Restart Method if desired and click **Restart**.

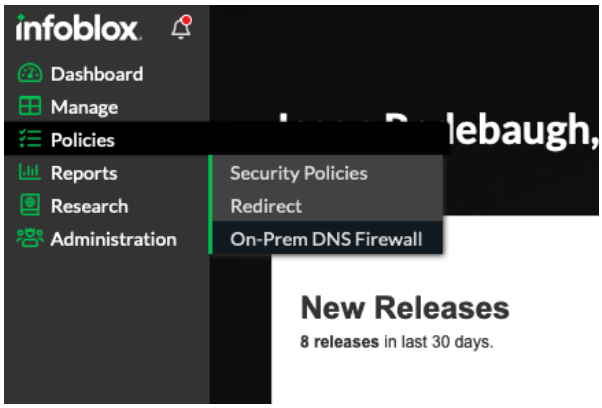

Restart Grid Services
Restart Grid Services
If needed
Force service restart
A forced restart may be delayed if there are pending restarts for the same service.
Restart Method
Restart all Restart Groups
Simultaneously for all members
Sequentially for all members
Affected Members and Services
View Pending Changes
Member
DNS
DHCP
infoblox.localdomain(172.23.1.70)
Requesting
No permission
To start polling, click the Poll Members icon above this table ...
Cancel
Restart

Add Replacement RPZ Feeds

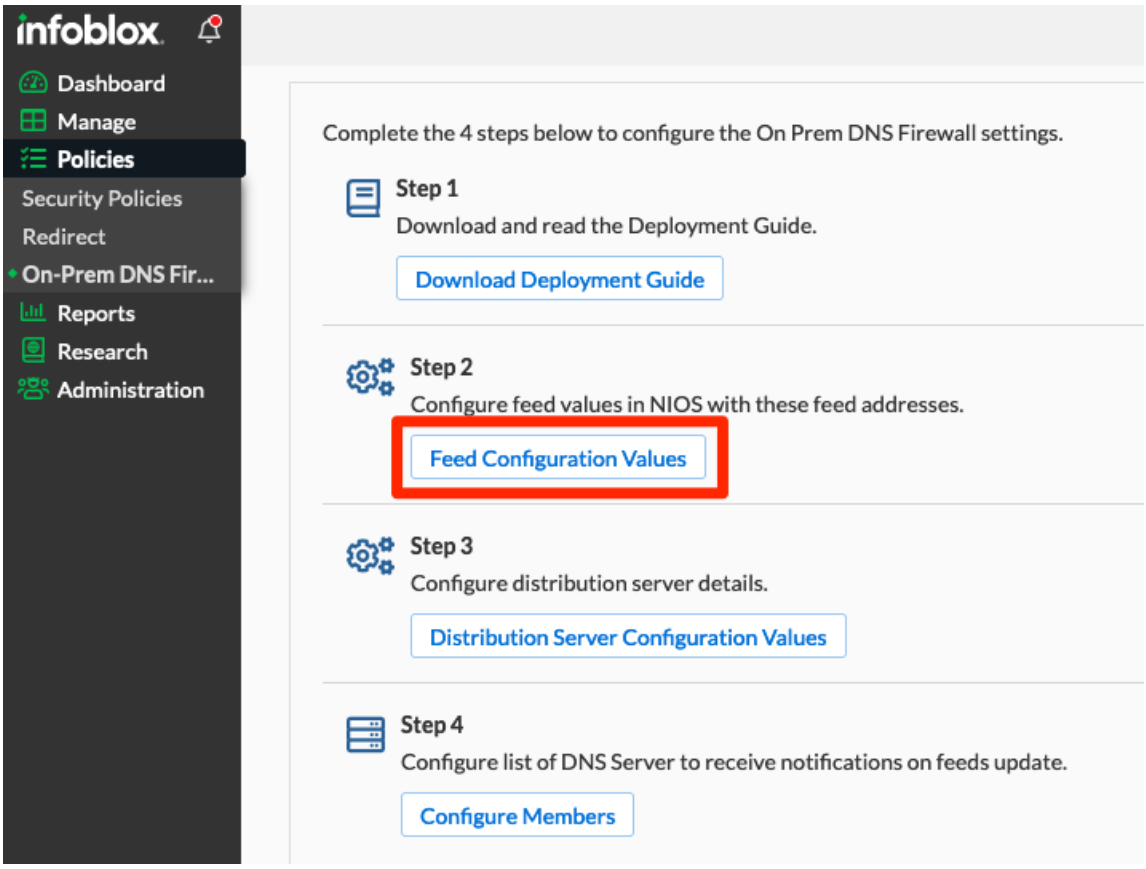
Feed and Distribution Server Configuration Values

This section describes the process to obtain configuration information from the Infoblox CSP which will be used to add the new RPZ feeds in NIOS. You will need to obtain feed name values and configuration information for the distribution server.

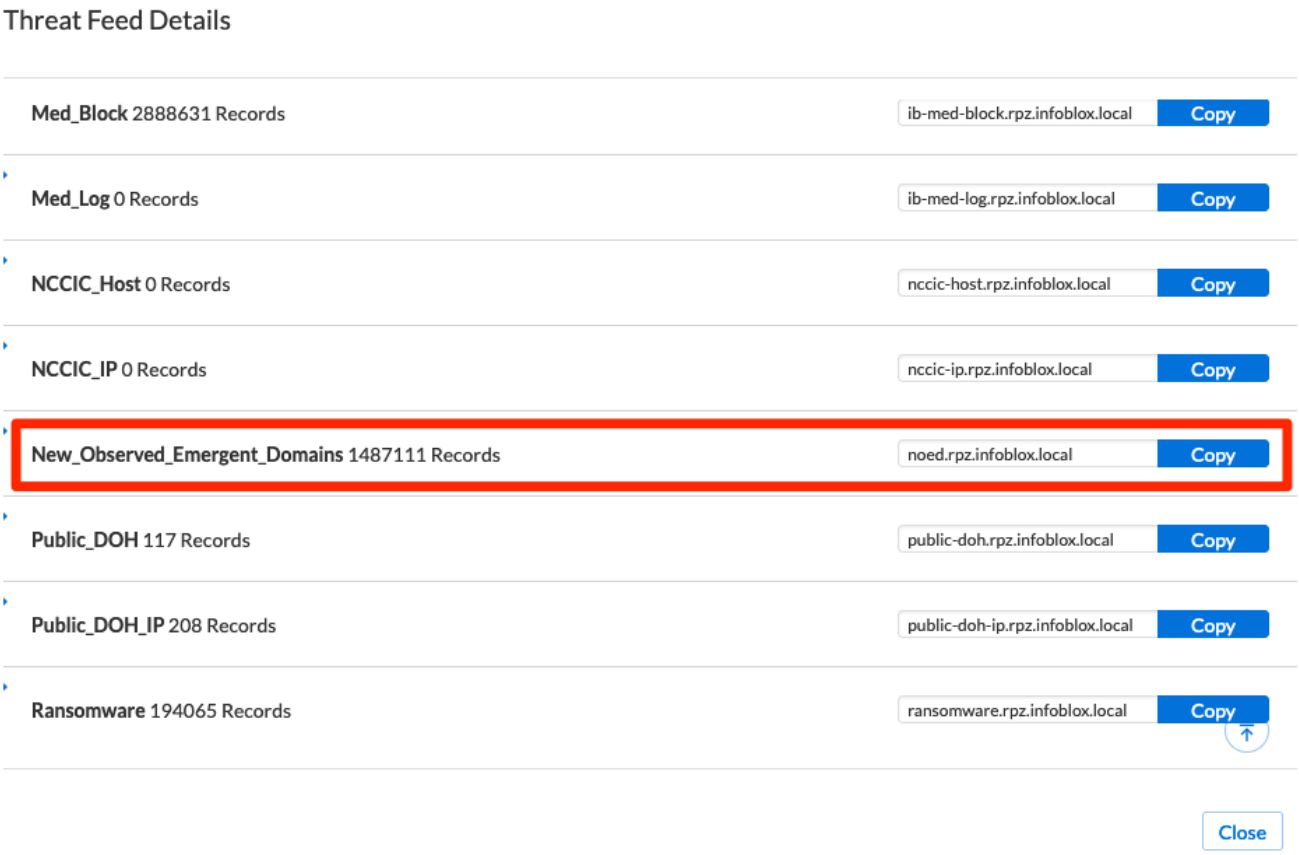
1. In the Infoblox CSP, use the navigation menu to select **Policies → On-Prem DNS Firewall**.



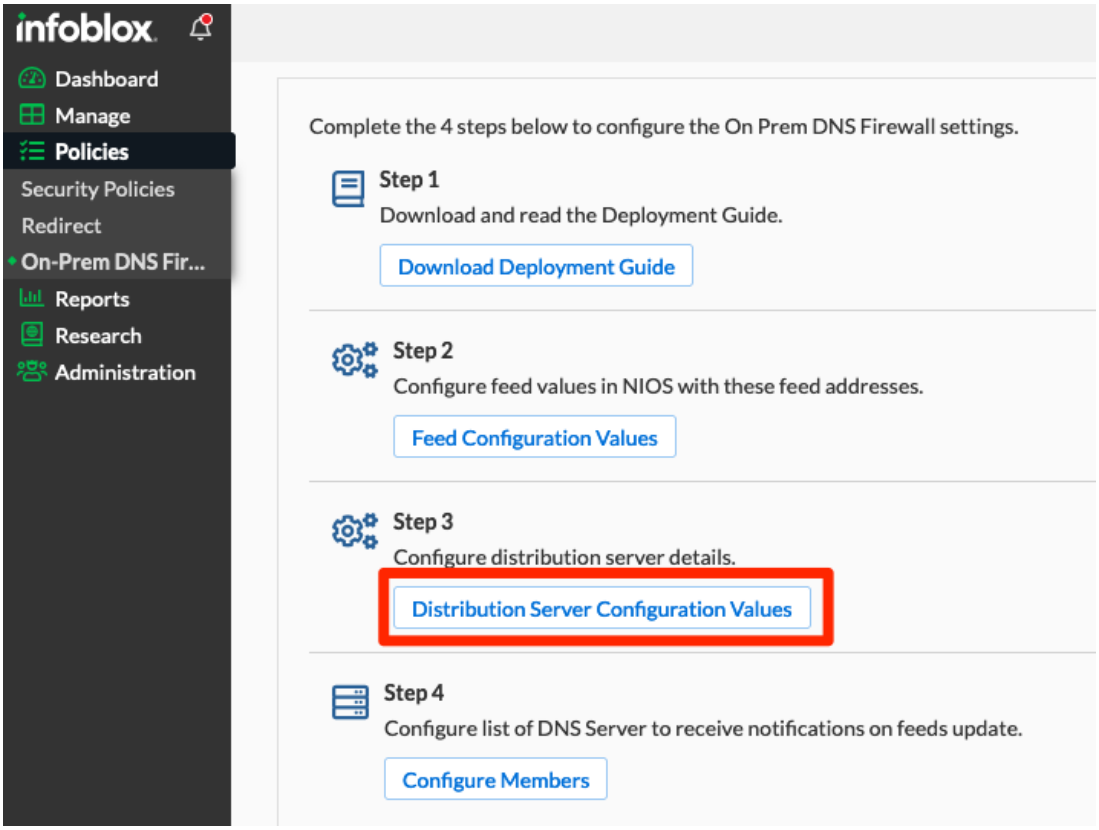
2. Click on **Feed Configuration Values**.



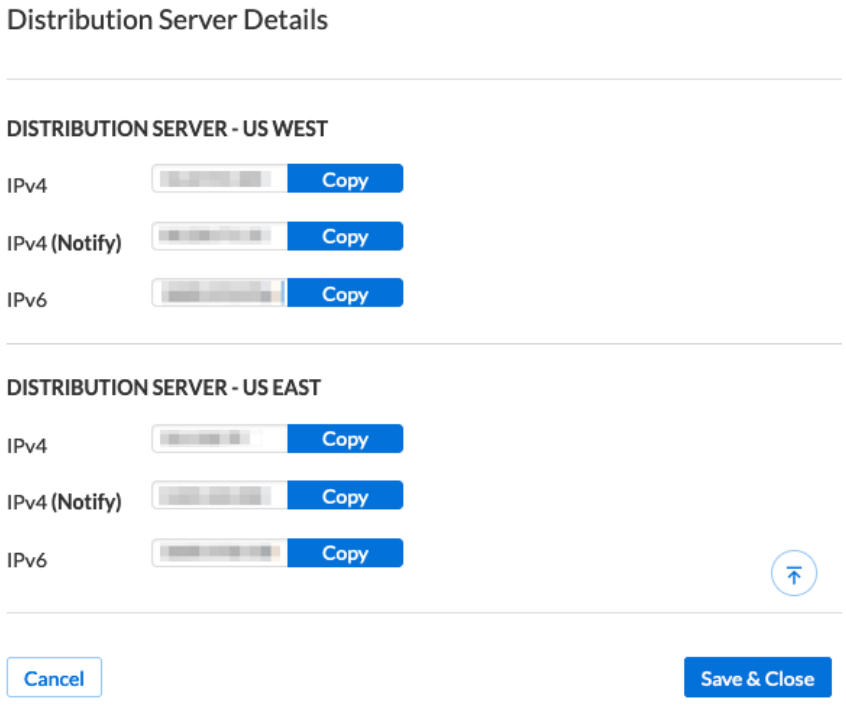
3. In the Threat Feed Details list, locate the first feed you will configure. Refer to the table in the Replacement Feed Mapping section for recommended feeds.
4. Click the **Copy** button for the desired feed. *Note: Paste this and other configuration data copied in this section into a text file for easy retrieval when configuring the feeds in NIOS.*



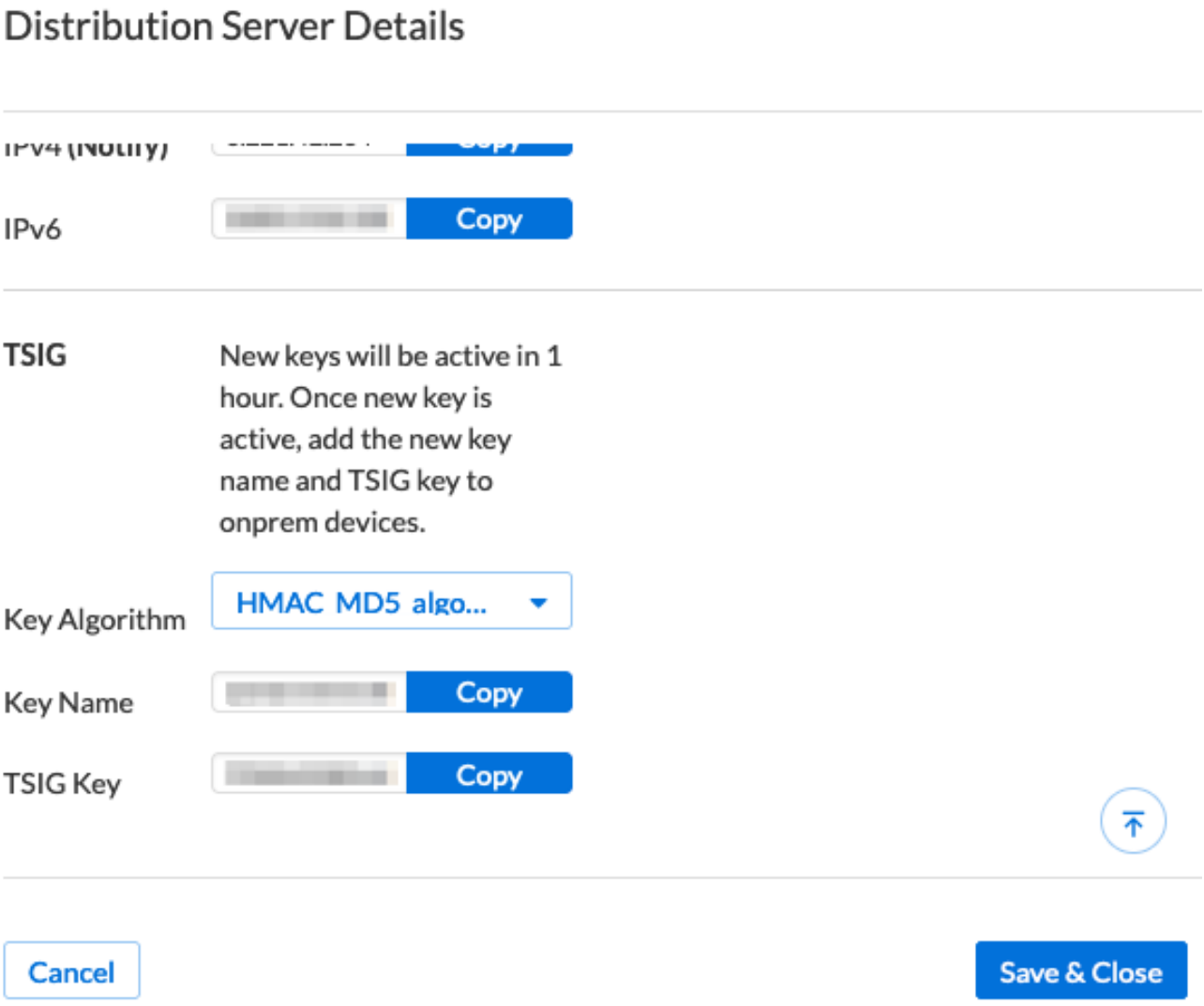
5. Repeat steps 3 and 4 for each feed. Refer to the table in the Replacement Feed Mapping section for recommended feeds.
6. Click **Close**.
7. Click on **Distribution Server Configuration Values**.



8. Scroll down to locate the Distribution Server you will use and click the **Copy** button for the IPv4 or IPv6 address. *Note: Paste this and other configuration data copied in this section into a text file for easy retrieval when configuring the feeds in NIOS.*



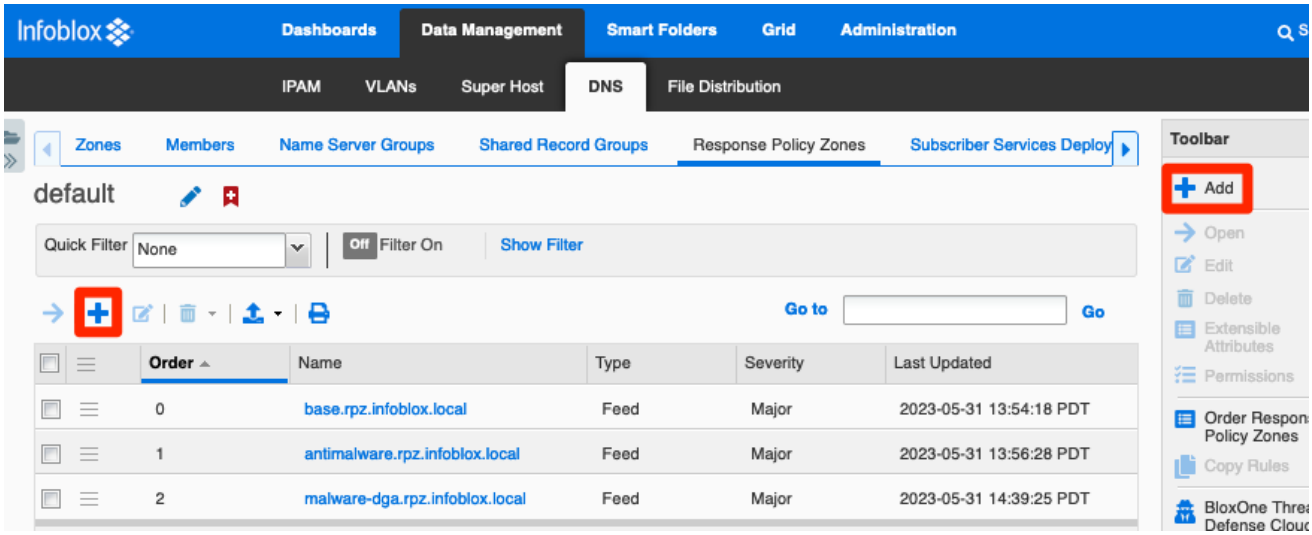
9. Scroll down to the TSIG section.
10. Note the Key Algorithm that is configured.
11. **Copy** the Key Name. *Note: Paste this and other configuration data copied in this section into a text file for easy retrieval when configuring the feeds in NIOS.*
12. **Copy** the TSIG Key. *Note: Paste this and other configuration data copied in this section into a text file for easy retrieval when configuring the feeds in NIOS.*
13. Click **Cancel** to exit the Distribution Server Details.



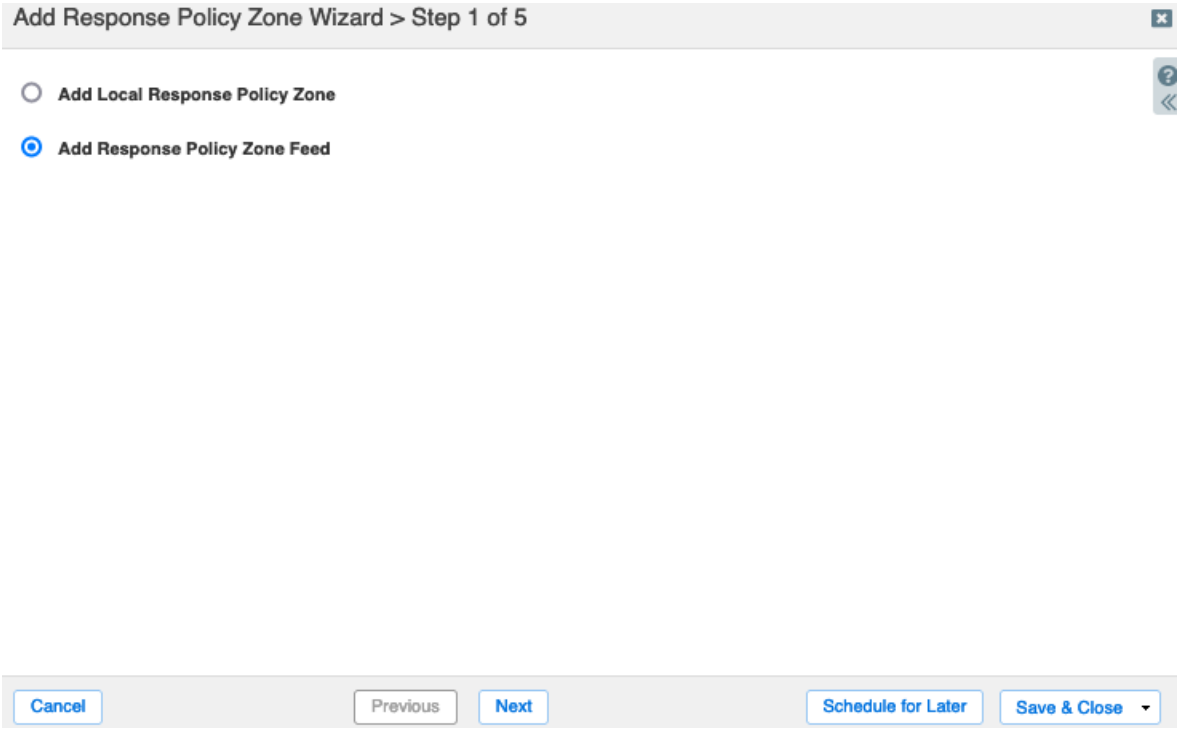
Add RPZ Feeds in NIOS

This section describes the process to add RPZ feeds in NIOS using the configuration data retrieved in the previous section.

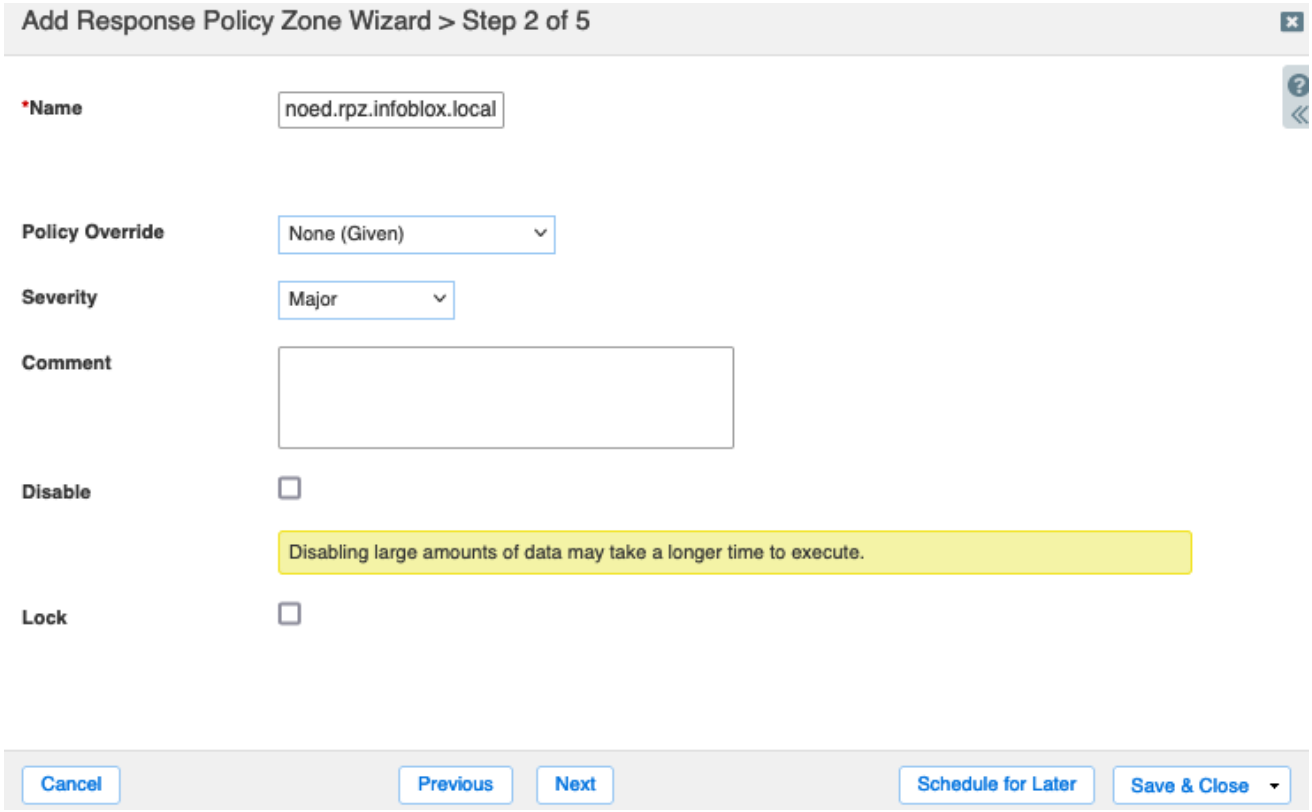
1. In NIOS Grid Manager, navigate to **Data Management** → **DNS** → **Response Policy Zones**.
2. Click the ✚ (add icon) or the **Add** button in the Toolbar.



3. On Step 1 of the Add Response Policy Zone Wizard, select **Add Response Policy Zone Feed**.
4. Click **Next**.



5. On Step 2, paste the **Name** of the feed, as copied from CSP.
6. Optionally, adjust **Policy Override** and **Severity**. Note: *This should reflect the policy used on the SURBL feeds being replaced.*
7. Click **Next**.

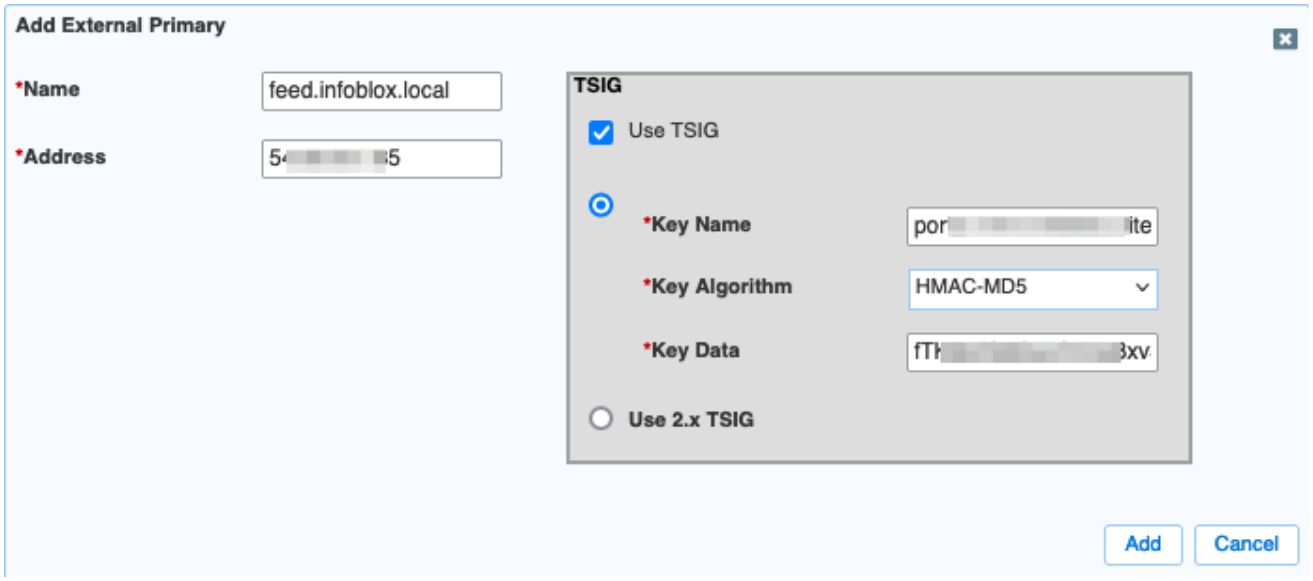


8. On Step 3, use the Add button dropdown to select **External Primary**.

Note: To save time, you can instead use a nameserver group configured with the external primary and any Grid secondaries to be used for all RPZs. Refer to [NIOS Documentation] for additional information on creating nameserver groups.

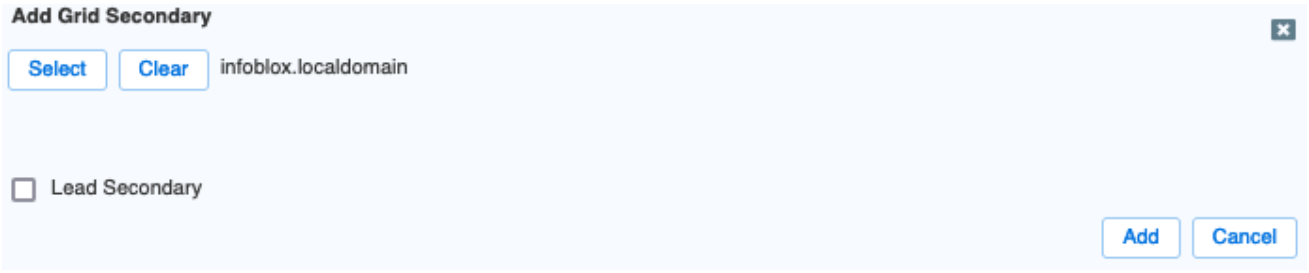
9. Enter a **Name**. *Note: This field is for reference purpose only, use any name you choose.*

10. Enter the **Address** of the distribution server as copied from the CSP.
11. Select the box for **Use TSIG**.
12. Enter the **Key Name** as copied from the CSP.
13. Select the **Key Algorithm** as noted from the CSP.
14. Enter the **Key Data** as copied from CSP.
15. Click **Add**.

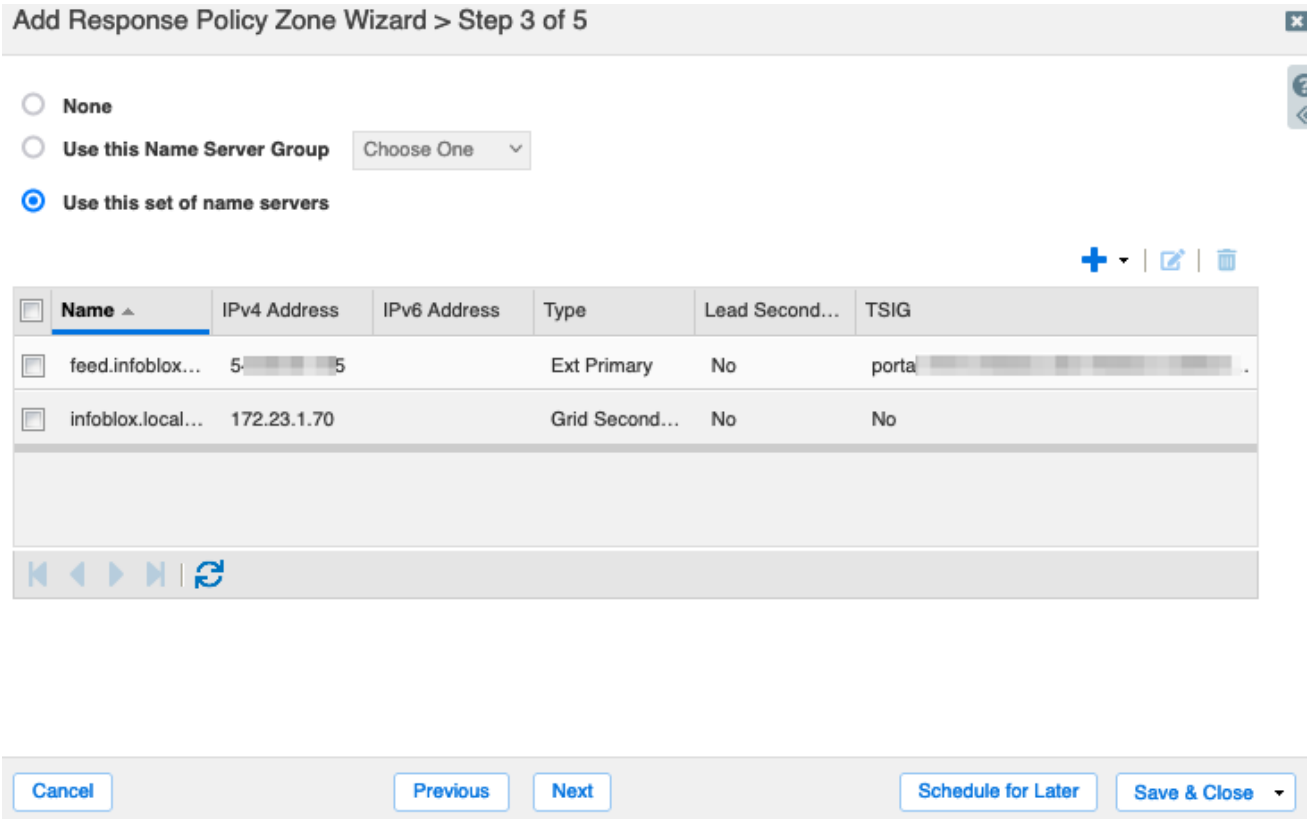


16. Use the Add button dropdown to select **Grid Secondary**.

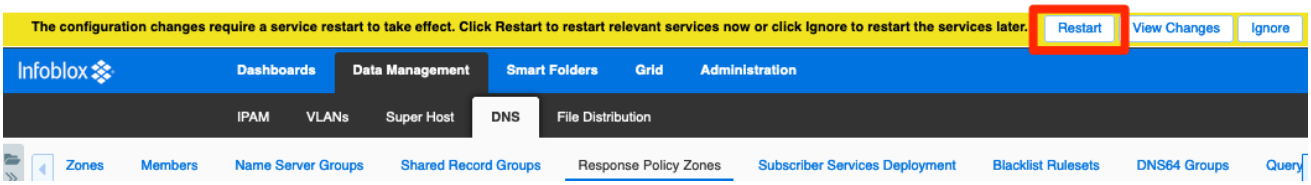
17. Click **Select** and choose the NIOS member to use. *Note: You can configure a single secondary to be "Lead Secondary". If you select this, that member will be the only one to reach out to the external primary. The feed is then redistributed between members using zone transfers.*
18. Click **Add**.



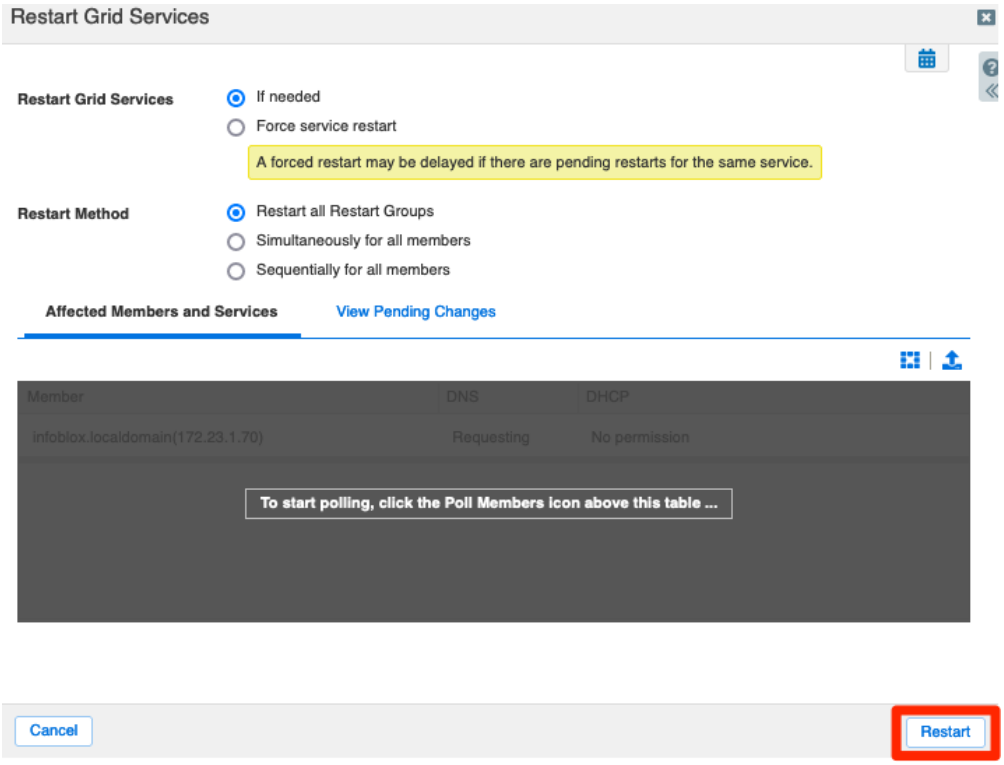
19. (Optional) Repeat Steps 17 and 18 to add additional NIOS appliances as secondaries.
20. **Save & Close**.



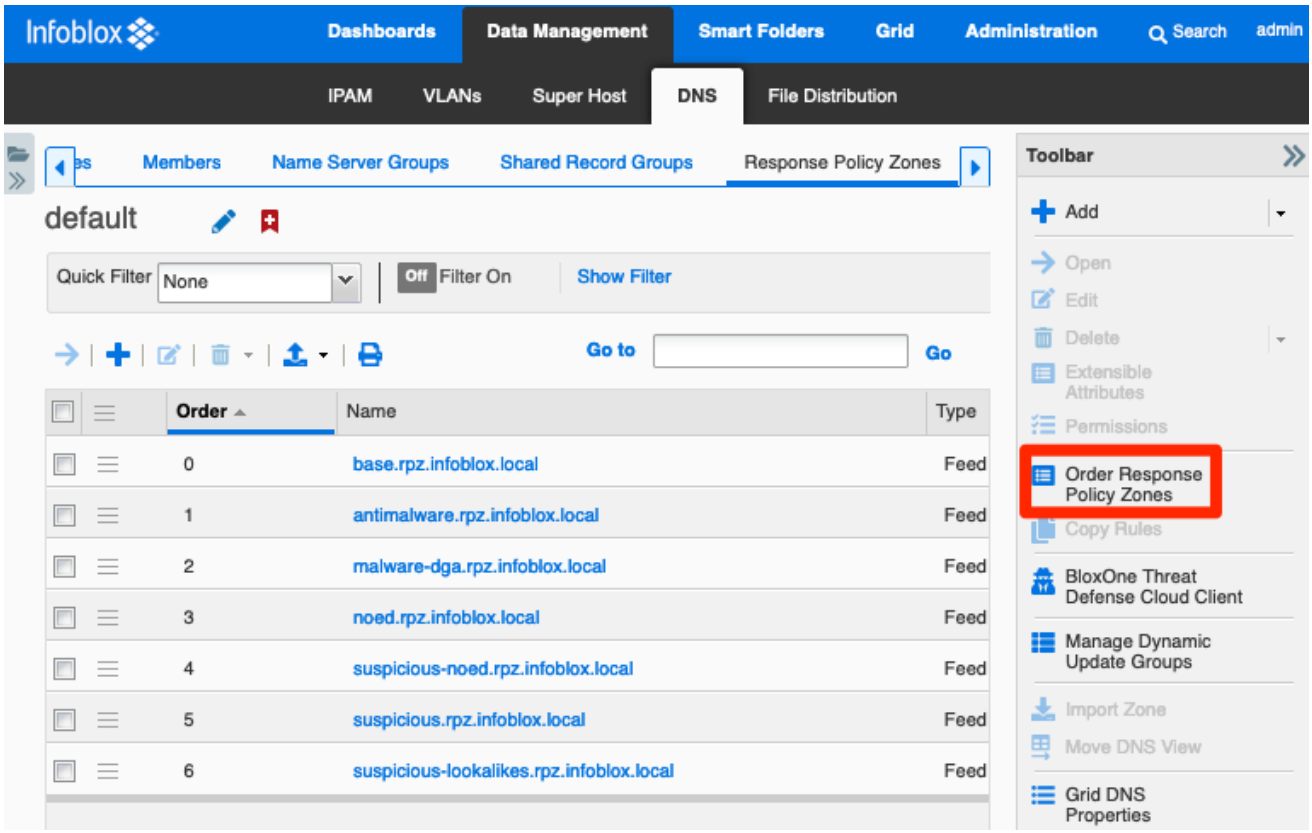
21. Repeat steps 2-20 for each feed you are adding.
22. When adding an RPZ a service restart is required. In the banner at the top of the Grid Manager window, click on **Restart**.



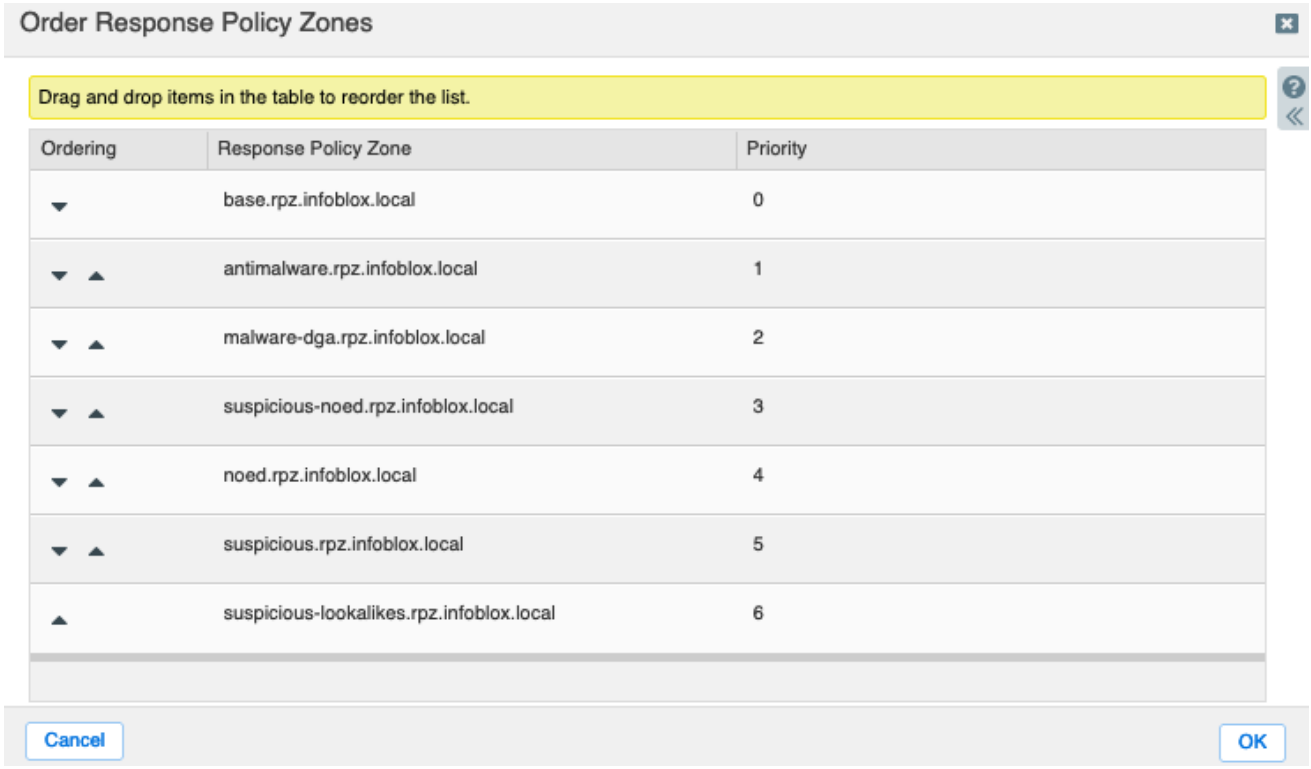
23. In the Restart Grid Services dialog, adjust Restart Method if desired and click **Restart**.



24. (Optional) Once you have added all feeds, use the **Order Response Policy Zones** button in the Toolbar to change the order feeds are applied.



25. In the Order Response Policy Zones dialog, use the arrows to change the order.
26. Click **OK** when complete.



27. Changing the order of RPZs requires a service restart to take effect. In the banner at the top of the Grid Manager window, click on **Restart**.
28. In the Restart Grid Services dialog, adjust Restart Method if desired and click **Restart**.

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