Infoblox
CONTROL YOUR NETWORK

Deployment Guide

Integration with Extreme Networks Extreme Management Center

Outbound API

Contents

Introduction

Integration between Infoblox and Extreme Networks allows customers to share data on devices, which helps them in prioritizing threats. This integration allows customers to break silos between network and security tools and improve ROI for the security investments already made.

Prerequisites

- Infoblox:
    - NIOS 8.3 or higher.
    - Security Ecosystem License.
    - Outbound Notification integration templates.
    - Prerequisites for the templates (e.g. configured and set extensible attributes).
    - Pre-configured services: DNS, DHCP, RPZ, Threat Analytics and ADP.
    - NIOS API user with the following permissions (access via API only):
        - All Host – RW.
        - All IPv4 DHCP Fixed Addresses/Reservations – RW.
        - IPv6 DHCP Fixed Addresses/Reservations – RW.
- Extreme Networks:
    - Extreme Management Center 8.1 or higher
    - Extreme Management Center API user with the following permissions:
        - Read/Write access to the NAC System Web Services APIs
        - Read/Write access to the NAC Services API

Known Limitations

The current templates support DNS Firewall (RPZ), Threat Insight (DNS Tunneling), Advanced DNS Protection (ADP) Host IPv4, Host IPv6, Fixed address IPv4, Fixed address IPv6, Discovery Data and lease events only. The asset management template does not support IPAM DB DELETE events and does not delete endpoints from Extreme Management Center. It is possible to modify the template and add support for DELETE event.

Fixed events will only updated Extreme Management Center when the ends system group extensible attribute, location extensible attribute or IP address is updated. Discovered events will only updated Extreme Management Center when IP or MAC address changes.

Only assets with MAC address can be synchronized to Extreme Networks Management Center for asset events, however security events can still be added based on IP.

Best Practices

Outbound Notification templates can be found on the Infoblox community site on the partners integration page. After registering an account, you can subscribe to the relevant groups and forums. If additional templates come out they will be found on the community site.

For production systems, it is highly recommended to set the log level for an end-point to **“Info”** or higher (**“Warning”**, **“Error”**).

Please refer to the Infoblox NIOS Administrator's Guide about other best practices, limitations and any detailed information on how to develop notification templates. The NIOS Administrator's Guide can be found through the Help panel in your Infoblox GUI, or on the Infoblox Support Center.

Configuration

Workflow

- Extreme Networks:
    1 Add End-System Groups
    2 Configure Distributed IPS
- Infoblox:
    1 Install the Security Ecosystem license if it was not installed.
    2 Check that the necessary services and features are properly configured and enabled, including DNS, RPZ and Threat Analytics.
    3 Create the required Extensible Attributes.
    4 Download (or create your own) notification templates (EN_Security.json, EN_Assets.json) from the Infoblox community web-site.
    5 Add the templates.
    6 Add a REST API Endpoint.
    7 Add Notifications.
    8 Emulate an event, check Rest API debug log and/or verify changes on the grid.

Before you get Started

Download Templates from the Infoblox Community Website

Outbound Notification templates are an essential part of the configuration. Templates fully control the integration and steps required to execute the outbound notifications. Detailed information on how to develop templates can be found in the NIOS Administrator's guide.

Infoblox does not distribute any templates (out-of-the-box) with the NIOS releases. Templates "**EN_Assets**" and "**EN_Security**" are available on the Infoblox community web-site. Templates for the Extreme Networks integration will be located in the **"**Partners Integrations**"**. You can find other templates posted in the **"**API & Integration**"** forum.

Templates may require additional extensible attributes, parameters or WAPI credentials to be created or defined. The required configuration should be provided with a template. Don't forget to apply any changes required by the template before testing a notification.

Extensible Attributes

Table 1. Extensible Attributes

Extensible Attributes	Description
XMC_End_System_Group	Custom field. Determines the End-System Group to add assets to for non-security events.
XMC_Location	Custom field. Determines the location field for the Extreme Networks End-System Entry custom field upon creation.
XMC_RemediateGroup	Custom field. Determines the End-System Group to add assets to for security events.
XMC_RemediateOnEvent	True or False. Defines if security event or log should be added to Extreme Networks.
XMC_RemediatedAt	Provides the last time a security event was sent to Extreme Networks.
XMC_Sync	True or False. Defines if devices should be updated/added to End-System Group.
XMC_SyncAt	Provides the last time an asset was added/modified on Extreme Networks.

Instance Variables

Extreme Network templates use an instance variable to adjust the templates' behavior. Instance variables can be entered through the grid GUI at **"Grid" → "Ecosystem" → "Notification"** and then selecting the notification you created at **"Edit" → "Templates"**.

Table 2. Instance Variables

Instance Variable	Description
Default_End_System_Group	Determines the End-System Group to add assets into if the extensible attribute "XMC_End_System_Group" isn't defined.
Default_Remediate_Group	Determines the End-System Group to add assets into for security events if the extensible attribute "XMC_RemediateGroup" isn't defined.
Only_Managed_Assets	True or False. Determines if unmanaged devices should be added to Extreme Networks.

Supported Notification

A notification can be considered as a **"link"** between a template, an endpoint and an event. In the notification properties, you define which event triggers the notification, which template is executed and with which API endpoint NIOS will establish the connection to. The Extreme networks templates support a subset of available notifications

(refer to the limitations chapter in this guide for more details). In order to simplify the deployment, only create required notifications and use the relevant filters. It is highly recommended to configure deduplication for RPZ and ADP events and exclude a feed that is automatically populated by Threat Analytics.

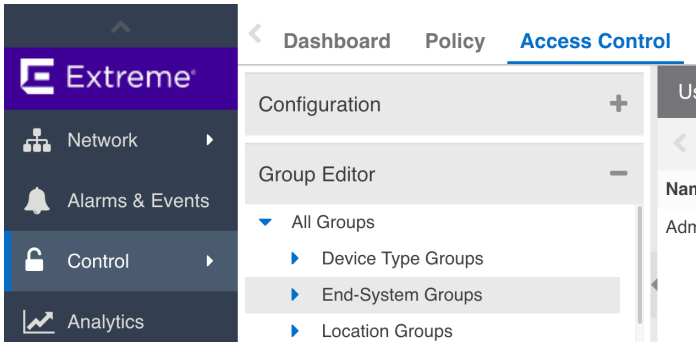
Table 3. Supported Notifications

Notification	Description
DNS RPZ	DNS queries that are Malicious or unwanted.
DNS Tunneling	Data exfiltration that occurs on the network.
Security ADP	Potential DOS attacks that occur on the network.
DHCP Leases	Lease events that occur on the network.
Object Change Fixed Address IPv4	Added/Modified fixed/reserved IPv4 objects.
Object Change Fixed Address IPv6	Added/Modified fixed/reserved IPv6 objects.
Object Change Host Address IPv4	Added/Modified Host IPv4 objects.
Object Change Host Address IPv6	Added/Modified Host IPv6 objects.
Object Change Discovery Data	Discovered Database objects.

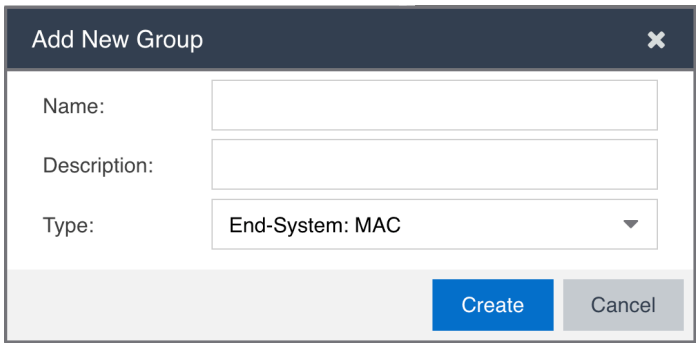
Extreme Networks Configuration

Create End-System Groups

1. Navigate to **"Control" → "Access Control" → "Group Editor" → "End-System Groups"**, and click **"Add…"**.

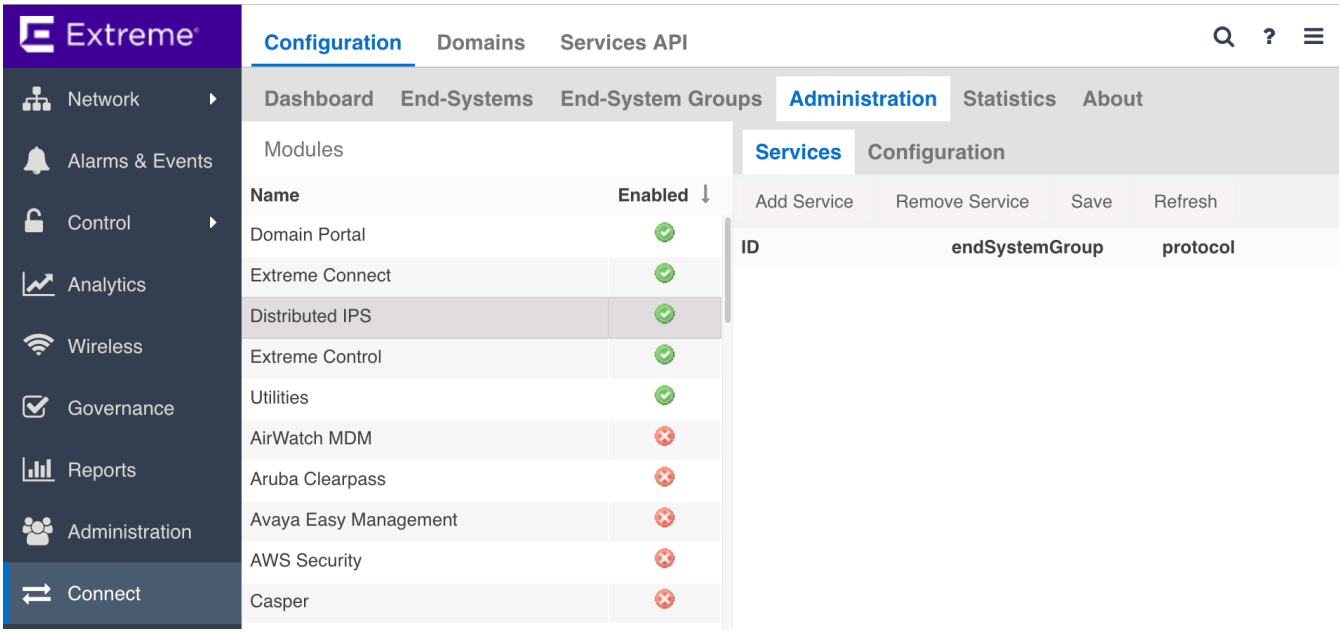


2. Enter the **"Name"** and **"Type"** for the end system group the click **"Create"**.
   - **"End-System: Mac"** is used when the MAC address is known.
   - **"End-System: IP"** is used when the MAC address isn't known on security events.



Configure Distributed IPS

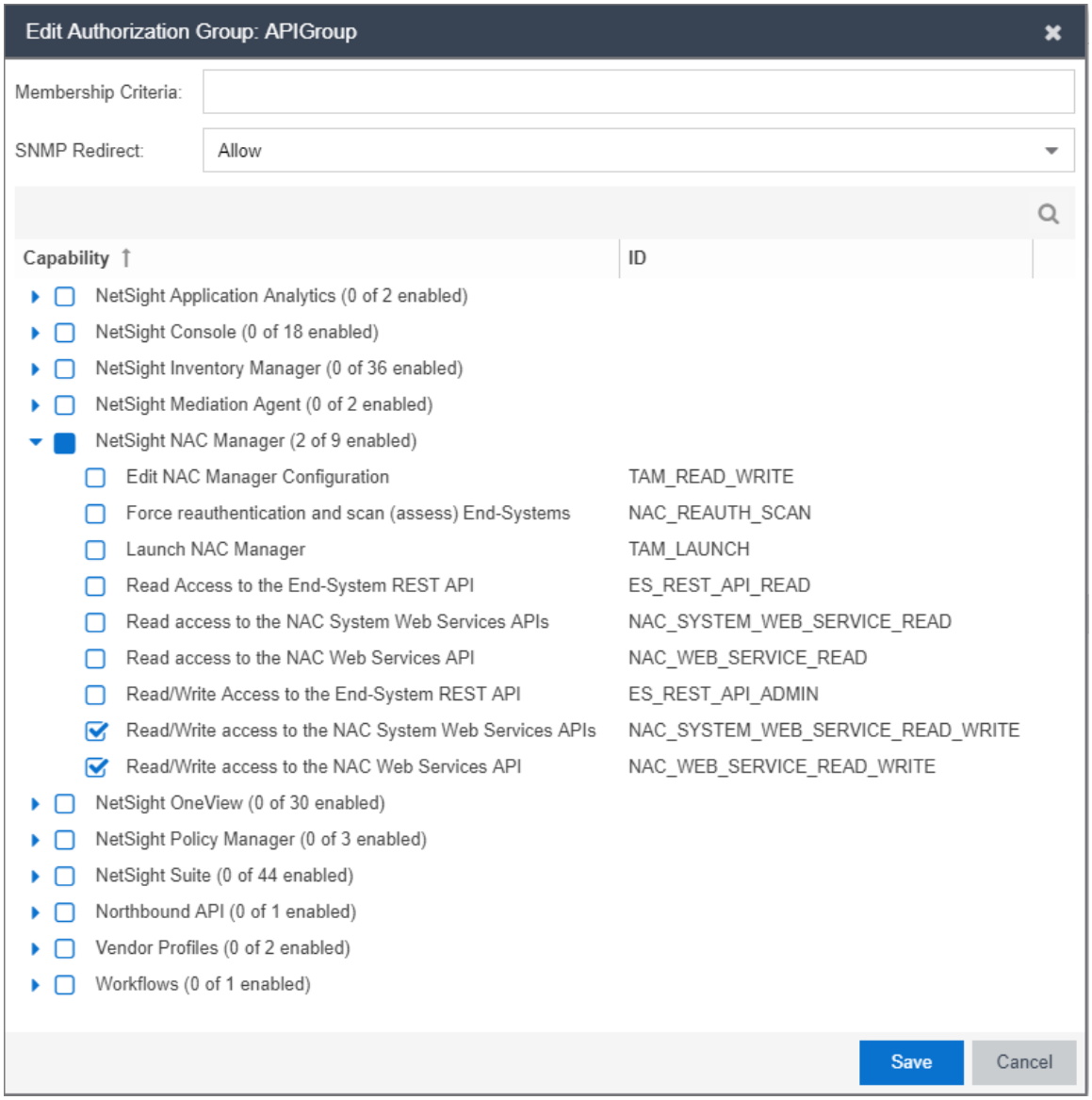
1. Navigate to **"Connect"** → **"Configuration"** → **"Administration"** → **"Services"** → **"Distributed IPS"**, and click **"Add Service"**.



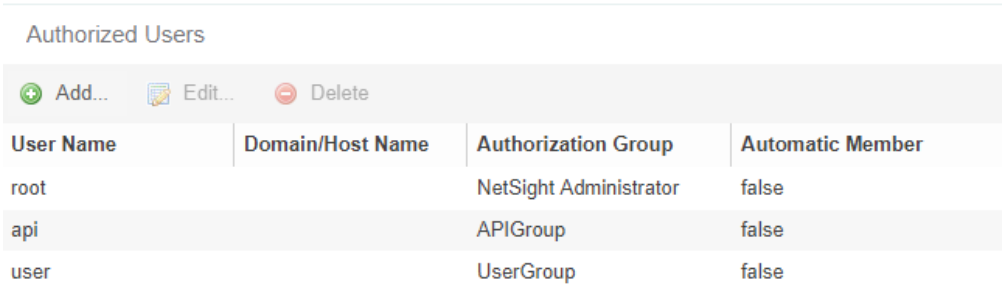
2. Enter the **"End-System Group",** created in step 2, into the **"endSystemGroup"** field, enter the regex **"Infoblox:.+?-threatIpAddress.$threatIpAddress.+?-threatName.$threatName"** into the **"regex"** field and enter the **"endSystemGroupType"** to add assets to the **"End-System Group"** if the MAC address isn't known.
    - If Infoblox doesn't know the MAC address and an "IP" end-system group is selected, then the IP will be added to the to the "IP" end-system group.
    - If the Extreme Management Center knows the MAC and a "MAC" end-system group is selected, then the asset will be added to the "MAC" end-system group.

Configure API User

1. Create an API user:
    a. If Extreme Management Center doesn't use AD/Radius backend:
        i. SSH to the Management Center and create a user with password (adduser)
    b. If the Management Center is using AD or Radius:
        i. Create API user in your AD or Radius backend.
2. Navigate to **"Administration"** → **"Users"** and create an **"Authorization Group"** with minimum privileges (Extreme Management Center version 8.1.4+):
    a. Note: Older versions require the user is part of NetSight Administrator



3. Add the API user to the API Group:
    a. If the Management Center does not use AD/Radius backend or if you do not want to use automatic assignment Add the API user to the API Group
    b. If the Management Center does use AD/Radius backend you can configure Membership Criteria for the automatic mapping of AD/Radius attributes to the group.



Infoblox NIOS Configuration

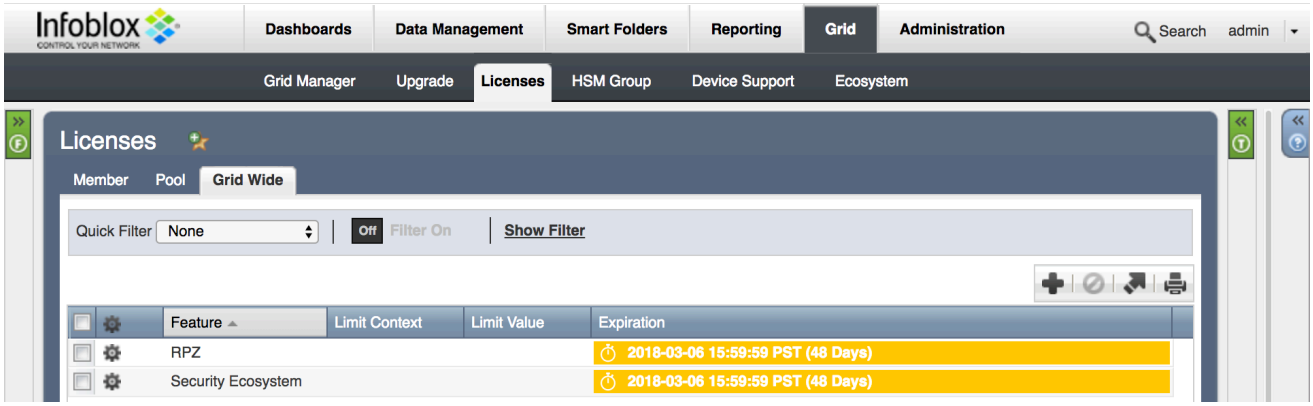
Infoblox Permissions

The Infoblox and Extreme Networks integration requires a few permissions for the integration to work. Navigate to **"Administration" → "Administrators"** and add a **"Roles"**, **"Permissions"**, **"Groups"** and **"Admins"** to include permissions that are required for the integrations. When creating a new group, under the **"Groups"** tab, select the **"API"** interface under the **"Roles" → "Allowed Interfaces"** category.

Check if the Security Ecosystem License is Installed

Security Ecosystem License is a "**Grid Wide**" License. Grid wide licenses activate services on all appliances in the same Grid.

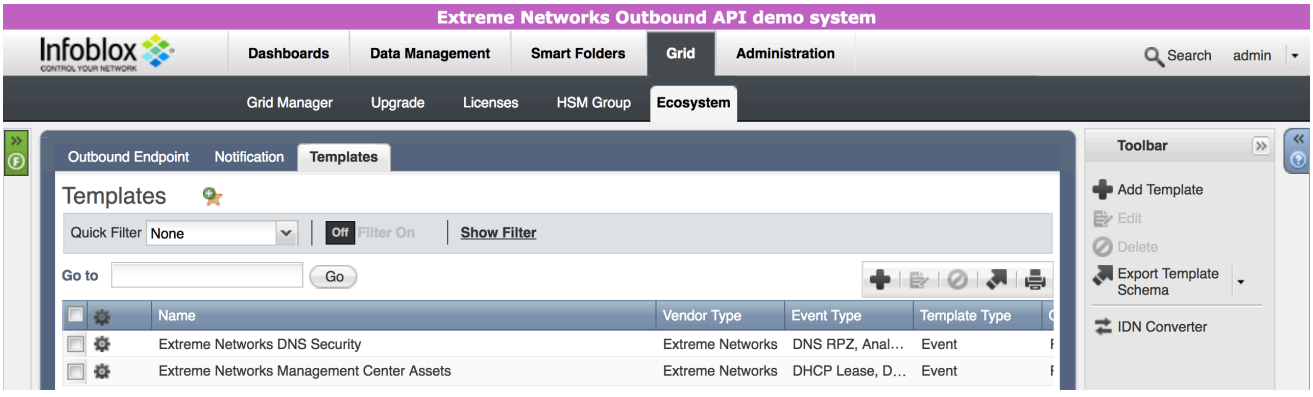
In order to check if the license was installed navigate to **"Grid" → "Licenses" → "Grid Wide"**.



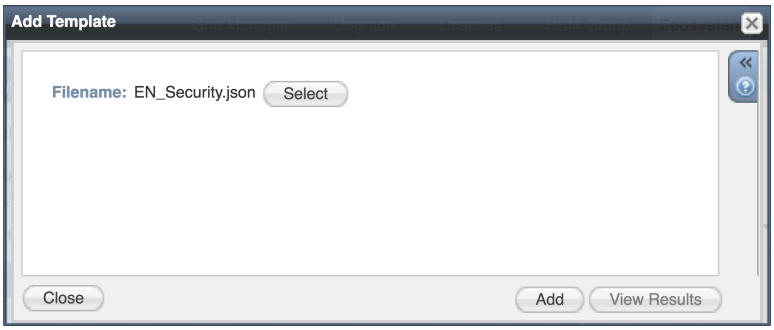
Add/Upload Templates

In order to upload/add templates:

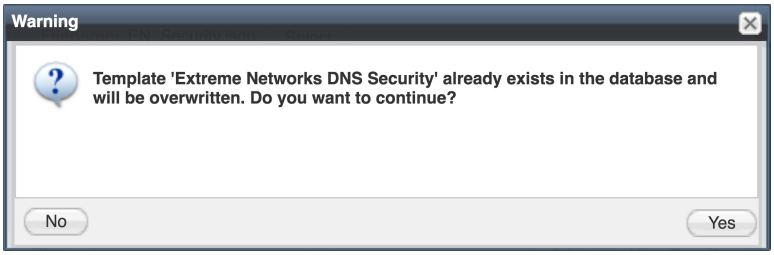
1. Navigate to **"Grid" → "Ecosystem" → "Templates"**, and press **"+"** or **"+ Add Template"**.



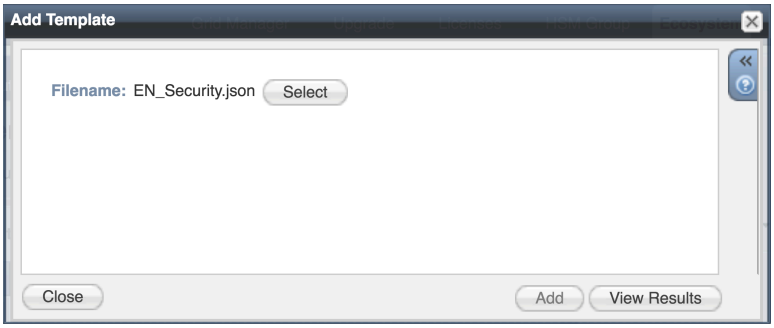
2. Press the **"Select"** button on the **"Add template"** window.

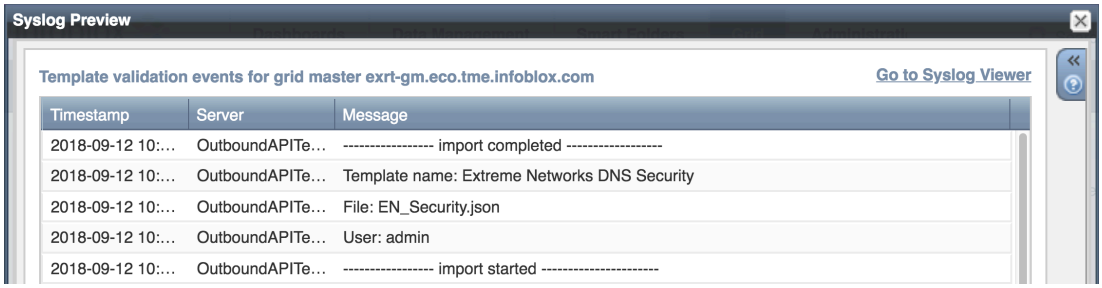


3. If a template was previously uploaded, press **"Yes"** to overwrite the template.



4. Pres the **"Select"** button on the **"Upload"** window. The standard file selection dialog will open.
5. Select the file and press the **"Upload"** button on the **"Upload"** window.
6. Press the **"Add"** button and the template will be added/uploaded.
7. You can review the uploaded results in the syslog or by pressing the **"View Results"** button.



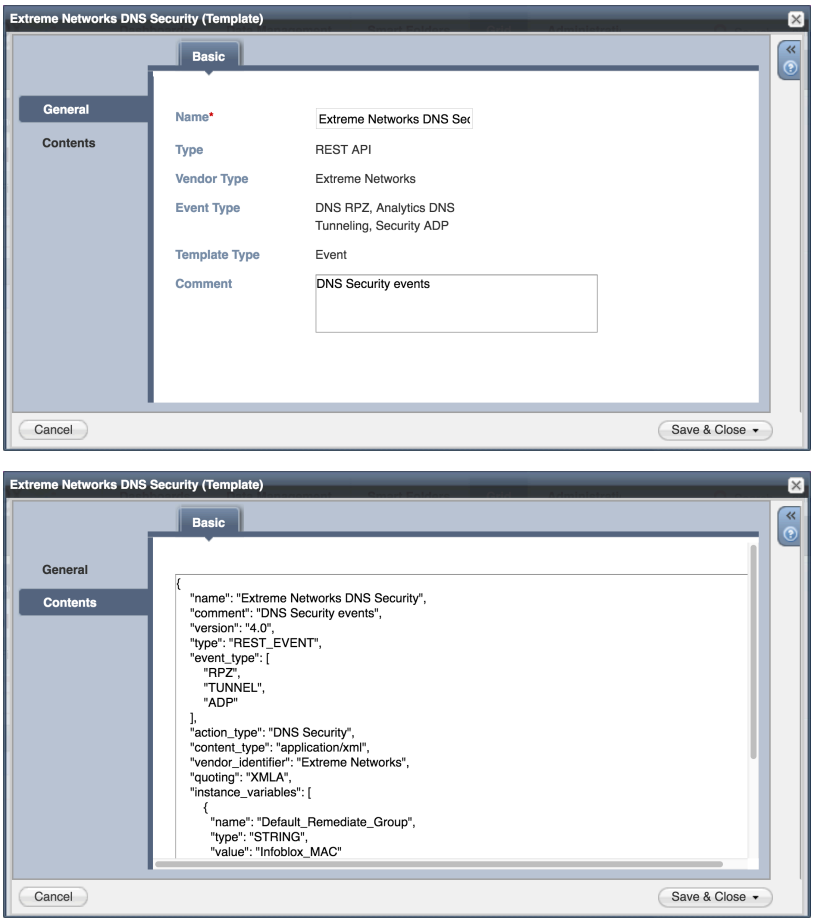


8. There is no difference between uploading session management and action templates.

Modifying Templates

NIOS provides the facility to modify the templates via the web-interface.

1. Navigate to **"Grid"** → **"Ecosystem"** → **"Templates"**, and then press the gear icon next to the template you want to modify.
2. Press the **"Edit"** button to open up the **"Template"** window.



The template editor is a simple interface for making changes to templates. It is recommended to only use the template editor to make minor changes. You can also edit, cut and paste template snippets from a text editor of your choice.

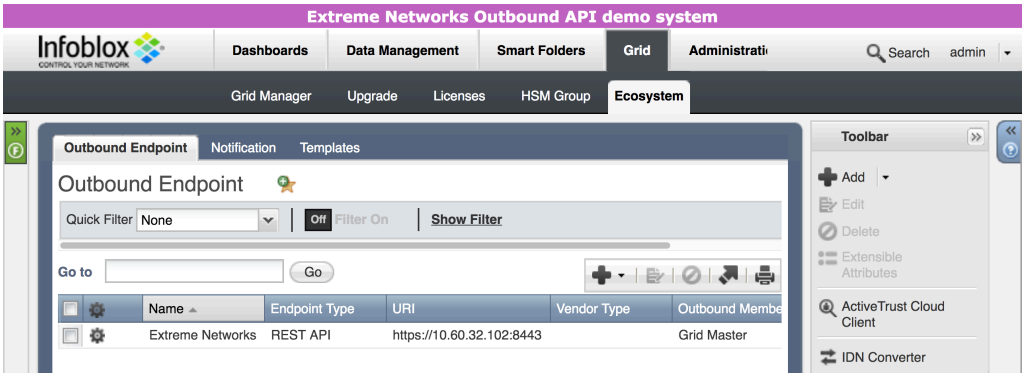
Note: You cannot delete a template if it is used by an endpoint or by a notification.

Add a Rest API Endpoint

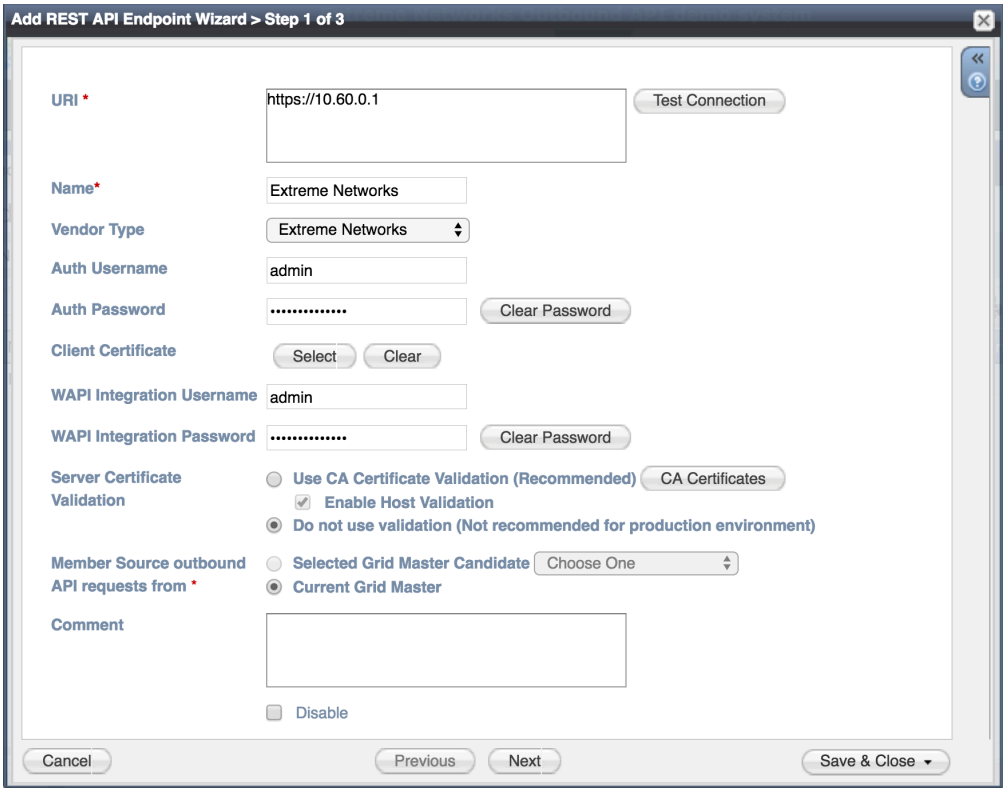
A **"REST API Endpoint"** is basically a remote system which should receive changes based on a notification and a configured template. A Grid, for example, can not only send notifications, it can also receive the notifications from itself (e.g. for testing purposes).

In order to add REST API Endpoints:

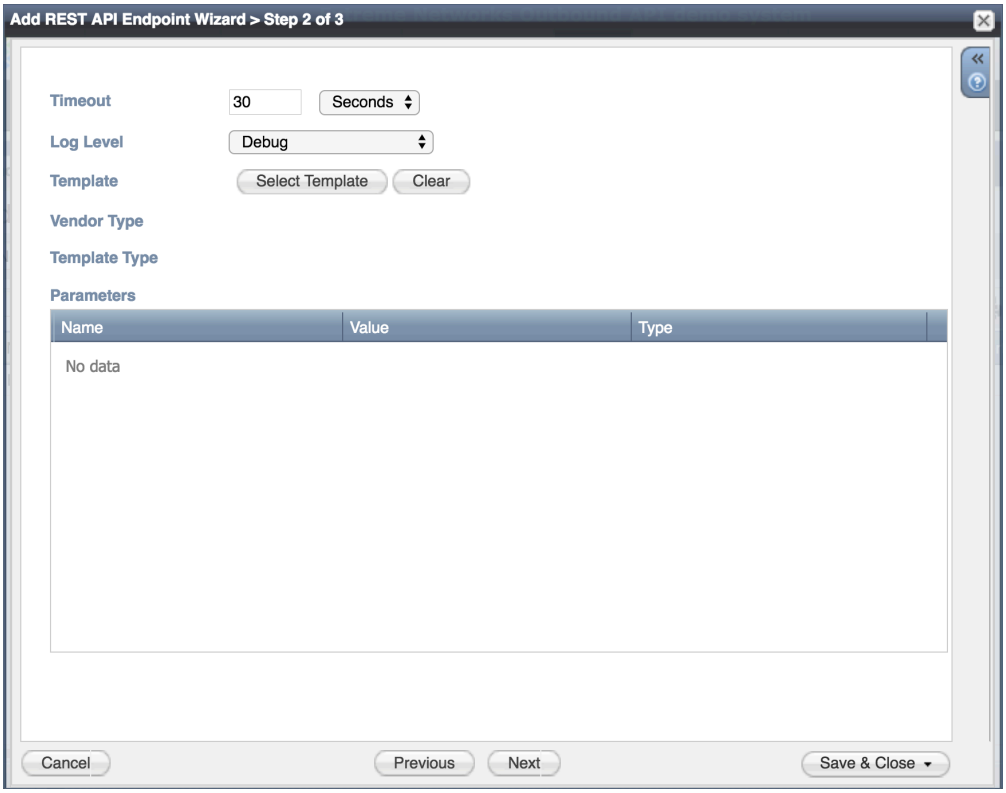
1. Navigate to "Grid" → "Ecosystem" → "Outbound Endpoints" and press "+" or "+ Add REST API Endpoint" buttons. The "Add REST API Endpoint Wizard" window will open.



2. The URI and Name for the appliance you are integrating with are required.
3. The URI should be the IP of the appliance you are integrating with, with the correct URI scheme.
4. Specify **"Auth Username"**, **"Auth Password"** (Extreme Networks Web Service account credentials), **"WAPI Integration Username"** and **"WAPI Integration Password"** (NIOS credentials).



5. (Optional) For debug purposes only: Under **"Session Management"**, set **"Log Level"** to **"Debug"**.



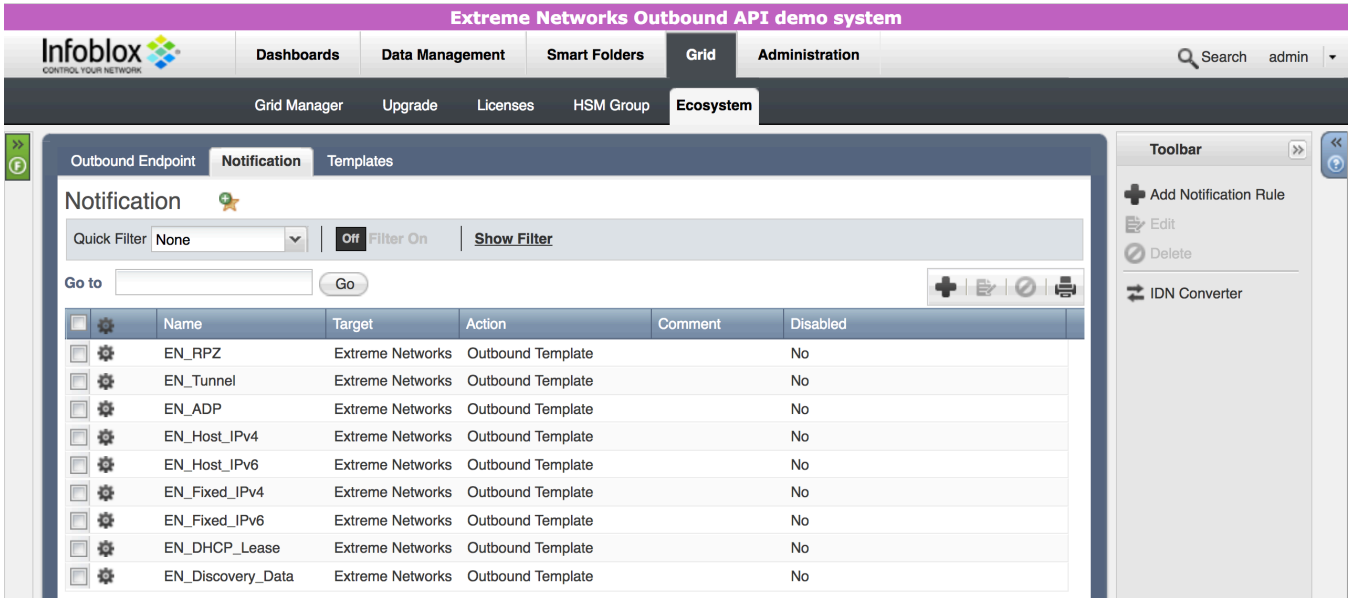
When possible, it is recommended to send notifications from a Grid Master Candidate instead of from the Grid Master.

Add a Notification

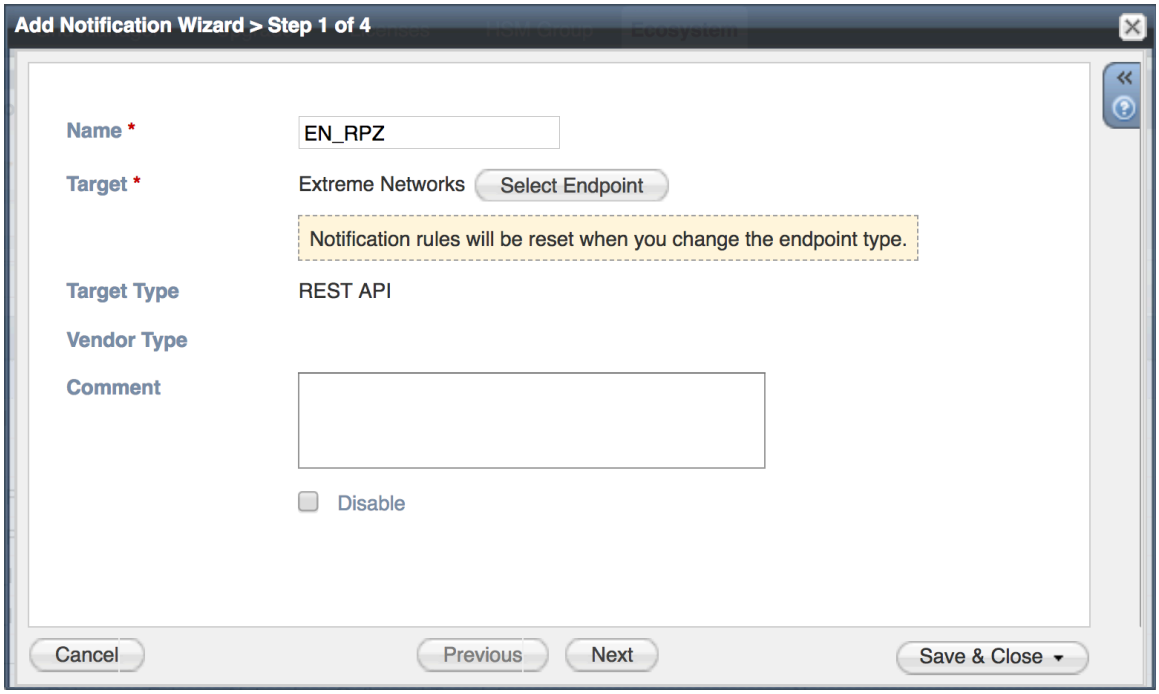
An endpoint and a template must be added before you can add a notification.

In order to add notifications:

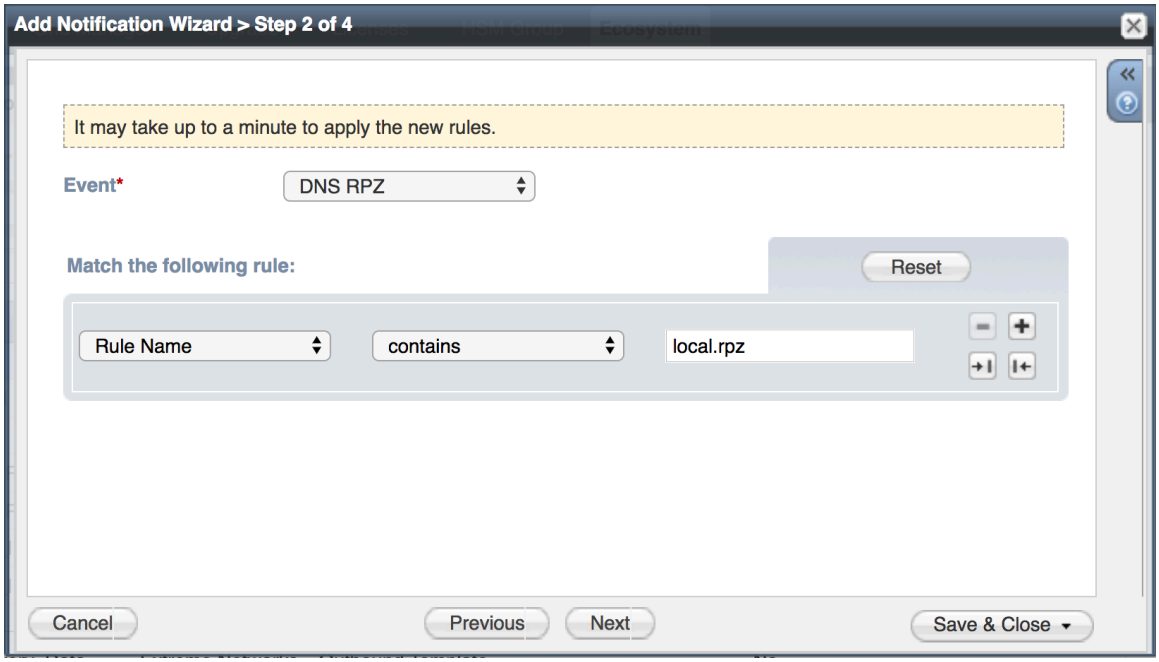
1. Navigate to **"Grid" → "Ecosystem" → "Notification"** and press **"+"** or **"+ Add Notification Rule"** then the **"Add Notification Wizard"** window will open.



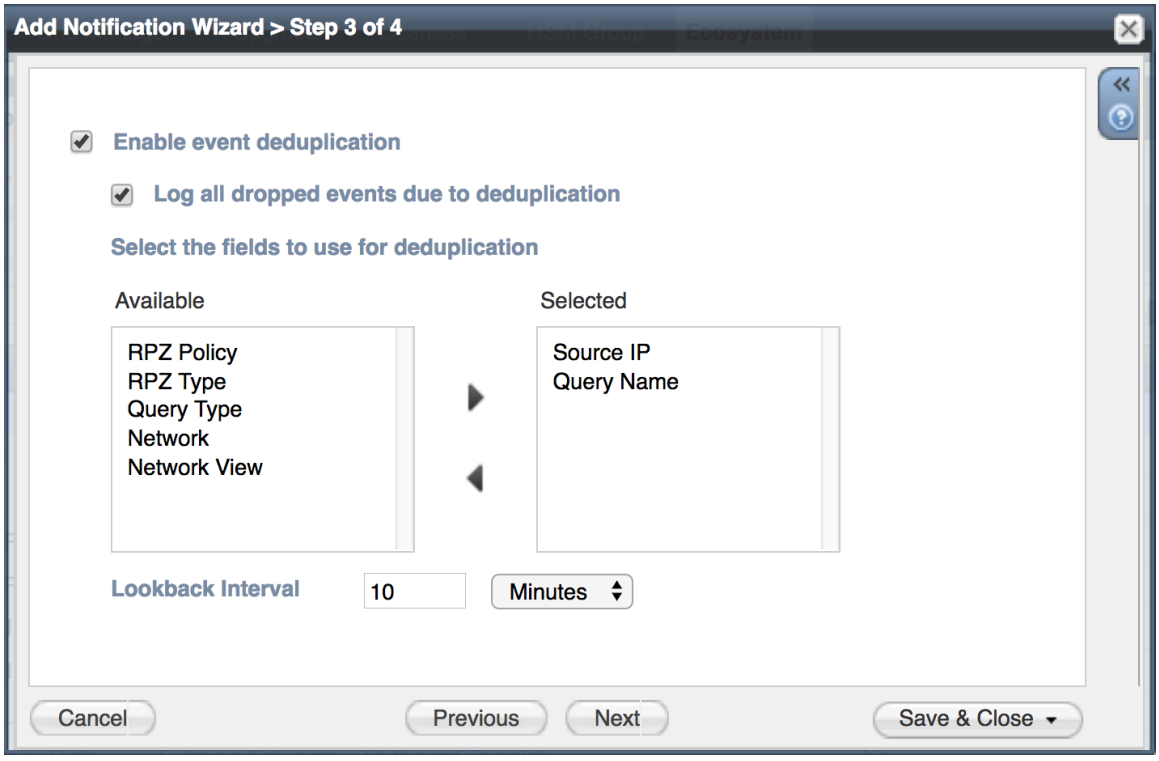
2. Specify the notification's name and select an endpoint (Target), click **"Next"**.



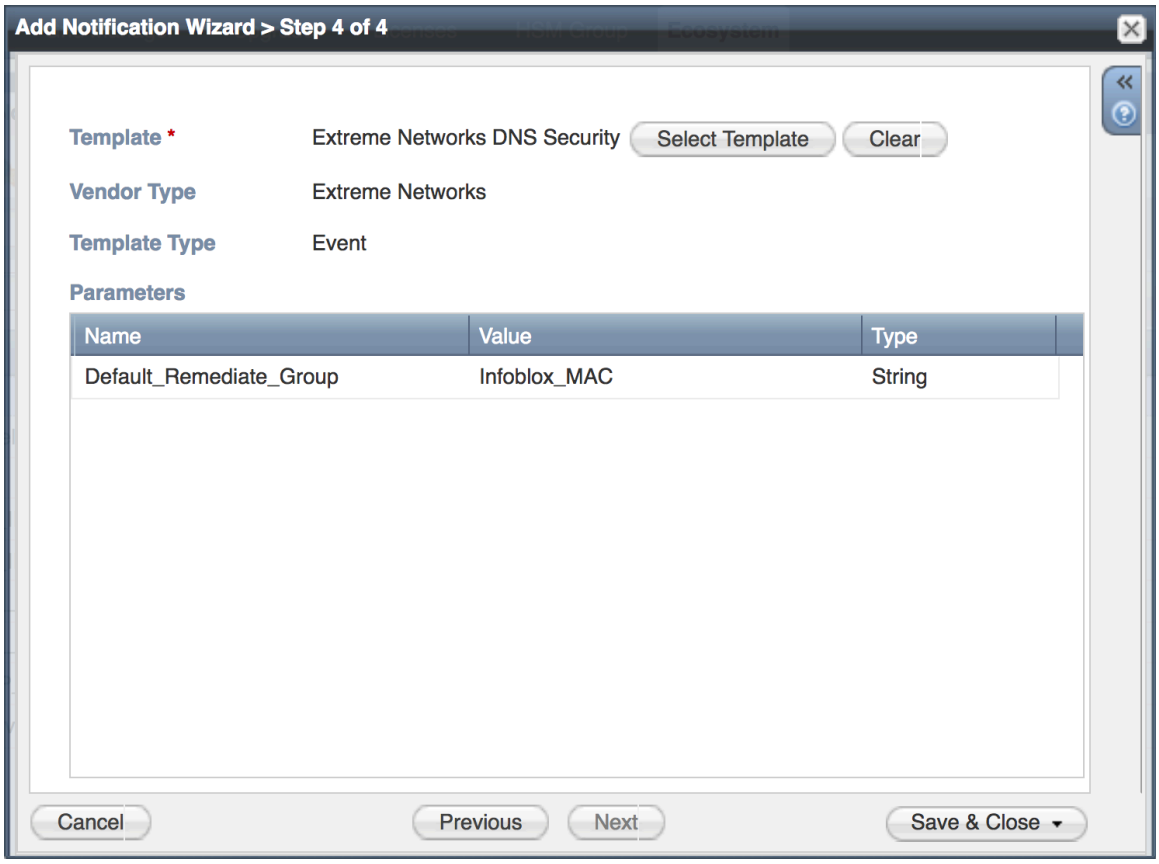
3. Select an event type and define a filter. Note: For optimal performance, it is best practice to make the filter as narrow as possible. Click **"Next"**.



4. (For RPZ notifications only) Check **"Enable RPZ event deduplication"** and specify relevant parameters. Click **"Next"**.

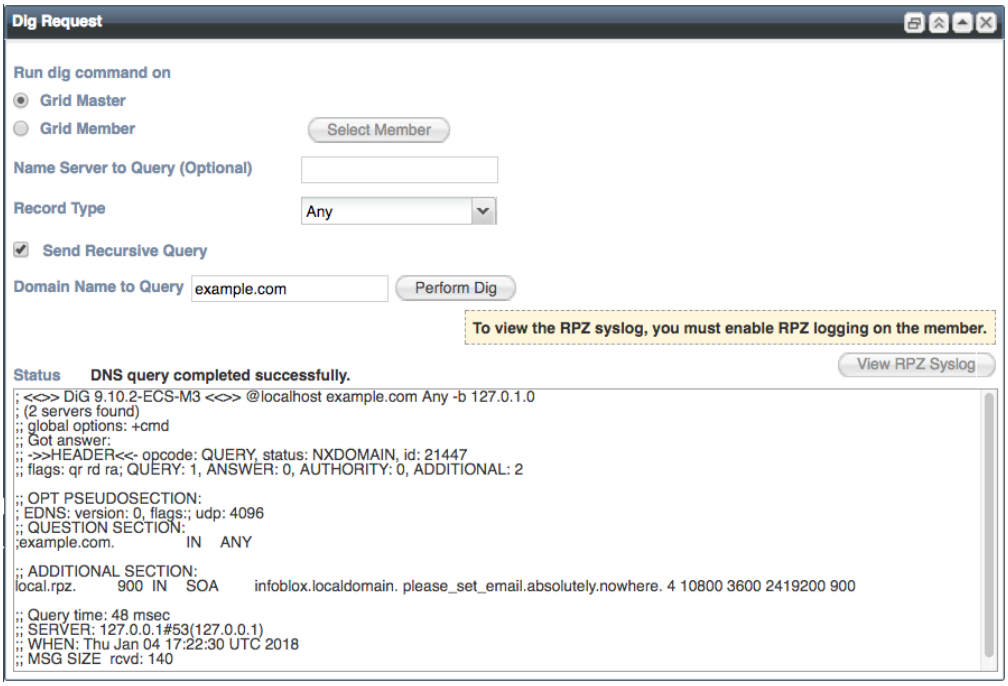


5. Select a relevant template and specify the template's parameters if any are required. Click **"Save & Close"**.

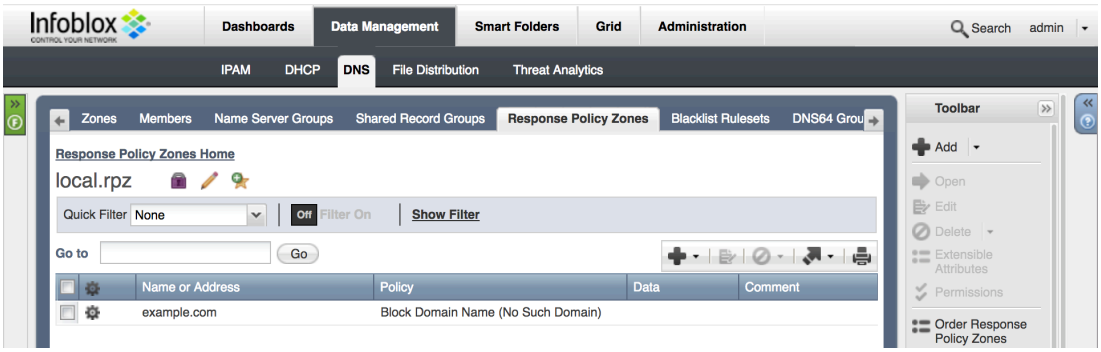


Check the Configuration

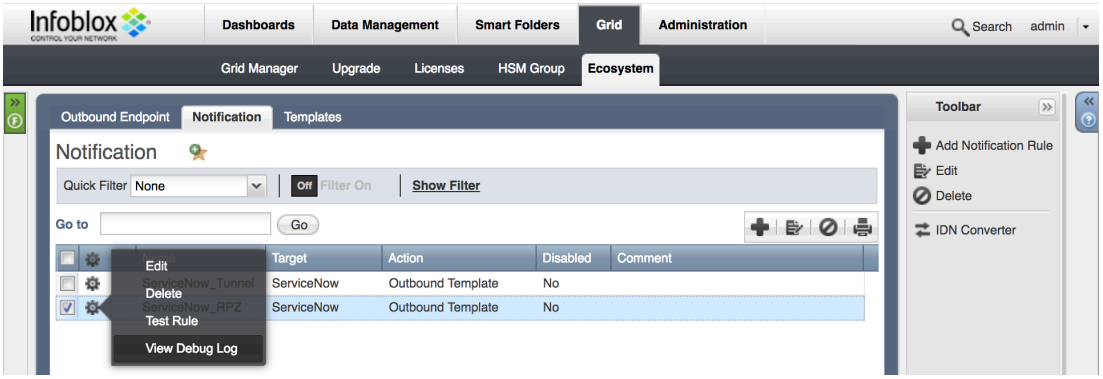
You can emulate an event for which a notification was added by going to **"Dashboards"** → **"Status"** → **"Security"** then on the **"Dig Request"** panel, fill in the **"Domain Name to Query"** text box and click the **"Perform Dig"** button.



When performing the dig request above, make sure that the **"Domain Name to Query"** is blocked by your RPZ. To check this, navigate to **"Data Management"** → **"DNS"** → **"Response Policy Zone"**. You can export a RPZ feed or check the content of a local RPZ.



To check a debug log for an endpoint, go to **"Grid"** → **"Ecosystem"** → **"Notification"**, click on the gear wheel and select **"View Debug Log"**.



Depending on a browser, the debug log will be downloaded or opened in a new tab. You may need to check your popup blocker or download settings.

Summary

Integration between Infoblox and Extreme Networks allows customers to share data on devices, which helps them in prioritizing threats. This integration allows customers to break silos between network and security tools and improve ROI for the security investments already made.

Additional Integrations

- When a client connects to a network managed by Extreme Management Center, information about the client is collected by Extreme Management Center and the shared with Infoblox.

  https://github.com/extremenetworks/Integrations/tree/master/Infoblox/ext_attributes

- Extreme Management Center knows the mac address of all the clients on the network and shares this information with Infoblox which can then use this information to stop unwanted or malicious leases.

  https://github.com/extremenetworks/Integrations/tree/master/Infoblox/dhcp

- When Infoblox detects DNS tunneling from an infected client, Infoblox informs Extreme Management Center which then disconnects the infected user.

  https://github.com/extremenetworks/Integrations/tree/master/Infoblox/dips