Infoblox
NEXT LEVEL NETWORKING

Deployment Guide

Enabling and Configuring Outbound API Notifications

Table of Contents

Introduction 2

Prerequisites 2

Known Limitations 2

Best Practices 2

Workflow 2

Verify that the Security Ecosystem License is installed 3

Create or Download Templates from the Infoblox Community Website 3

Add/Upload Templates 3

Modifying Templates 5

Add a REST API Endpoint 7

Add a Notification 10

Check the Configuration 13

Emulate an RPZ Event 13

Test a Notification 14

Additional Resources 17

Introduction

Infoblox's Outbound REST API offers a robust framework that can be leveraged to integrate Infoblox with many third-party devices. The Outbound API can send REST API calls to any device that can receive REST API calls. A variety of integrations already exist on the Infoblox Community Website at https://community.infoblox.com

Prerequisites

The following are prerequisites for Outbound API notifications:

- Infoblox Grid running NIOS 8.0 or higher.
- Security Ecosystem License.
- Pre-configured services that will be used with Outbound Notifications (example: DNS, DHCP, RPZ, Threat Analytics, Threat Protection, and ADP).
- Pre-Configured third party services that will be used with Outbound Notifications such as McAfee DXL.

Known Limitations

For potential limitations please view the NIOS Administrator Guide. Or, if you are deploying templates that have already been created, view the associated deployment guide.

Best Practices

Outbound API 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. Integrations are developed and updated regularly, templates and template updates can 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**"). As with any change to your network, it is also highly recommended to test all changes before implementing them into production.

Please refer to the Infoblox NIOS Administrator's Guide for any 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 portal.

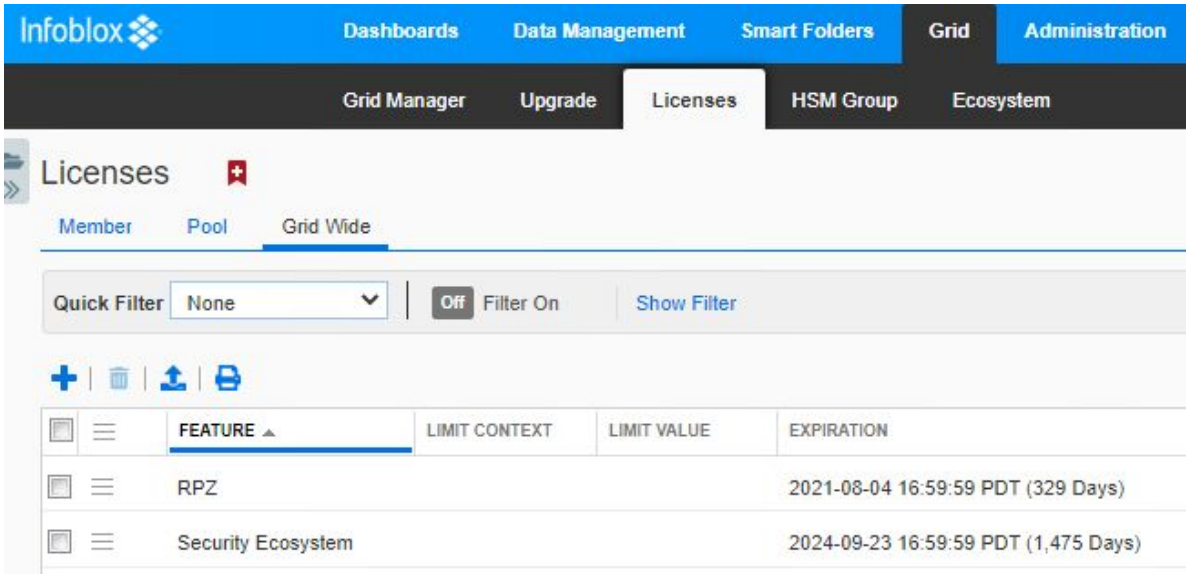
Workflow

Use the following workflow to enable, configure, and test outbound notifications:

1. Verify that the Security Ecosystem license is installed.
2. Check that desired services and features are properly configured and enabled.
3. (Optional) Create Extensible Attributes.
4. Create templates or download templates from the Infoblox Community Website.
5. Add the templates to NIOS.
6. Add a REST API Endpoint.
7. Add a Notification.
8. Emulate an event, check the Rest API debug log and verify changes on the REST API Endpoint.

Verify that the Security Ecosystem License is installed

The 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 is installed log in to the web interface of your Grid Master. Then, navigate to **Grid** → **Licenses** → **Grid Wide**. Verify that the license exists, and that it has not expired.



Create or Download Templates from the Infoblox Community Website

Outbound API 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.

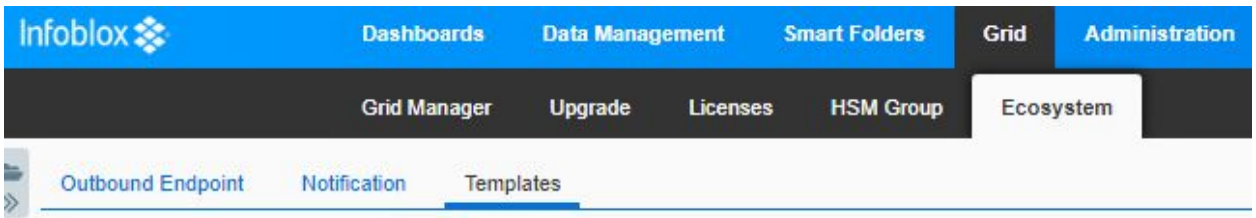
Infoblox does not distribute any templates (out-of-the-box) with the NIOS releases. Templates are available on the Infoblox community website. Community created Templates will be located in **Partners Integrations**, you can also find other templates posted in the **API & Integration** forum.

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

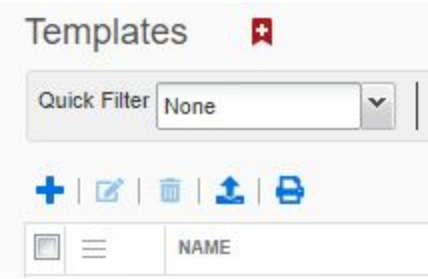
Add/Upload Templates

In order to add/upload templates perform the following steps:

1. Navigate to **Grid** → **Ecosystem** → **Templates**.



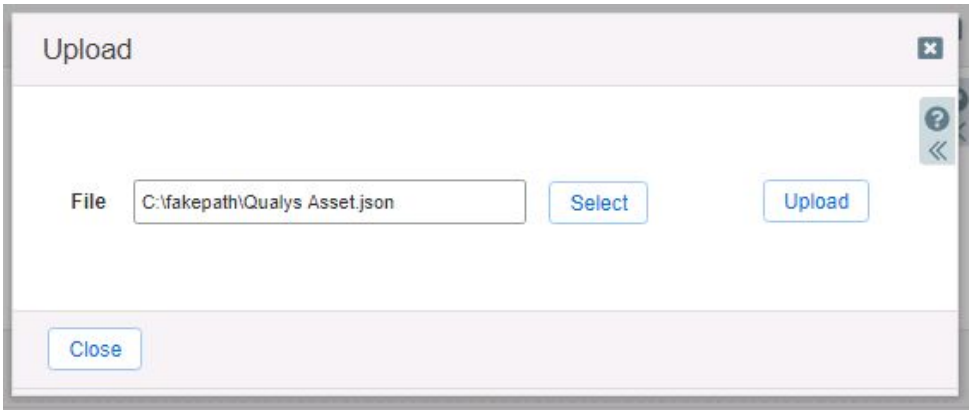
2. Press the **+** icon located above the table of Templates.



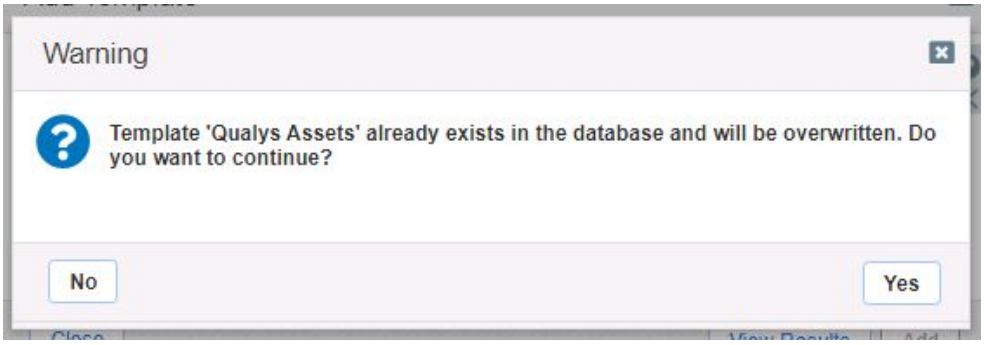
3. Press the **Select** button in the **Add Template** dialog that is revealed.

4. Click the Select button in the **Upload** dialog box that is revealed.

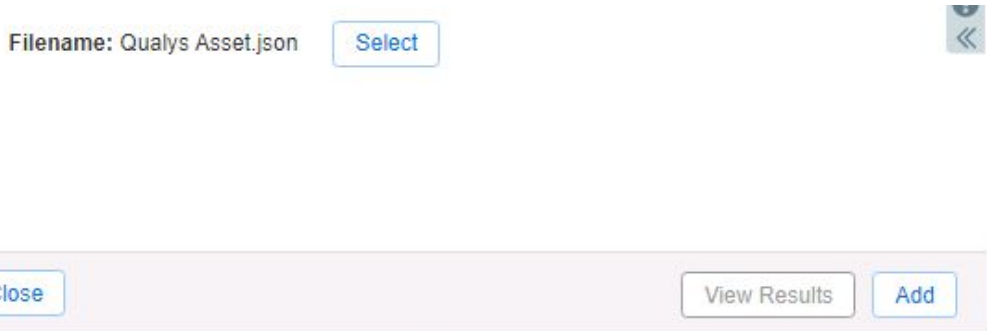
5. Locate and select the **Template** you would like to upload. Or, input the full path of the file in the **File** text box.
6. Once the File has been selected, click **Upload**.



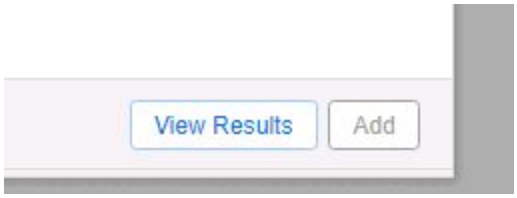
7. If a template was previously uploaded, press **Yes** to overwrite the template.



8. Click the **Add** button and the template to begin the file upload.



9. (Optional) You may review the results of the file upload in the syslog, or by pressing the **View Results** button.



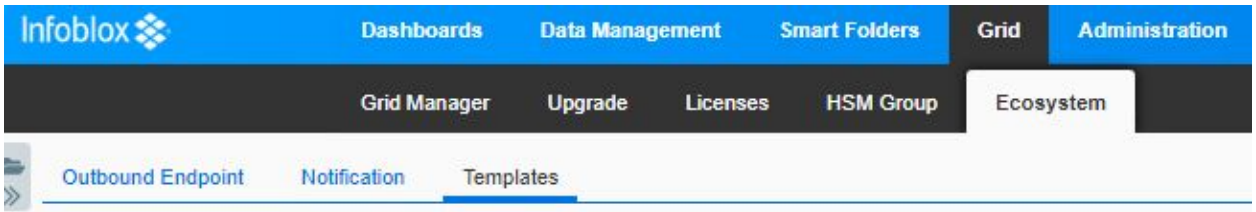
10. Repeat steps **2-8** for any other templates you intend to upload.

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

Modifying Templates

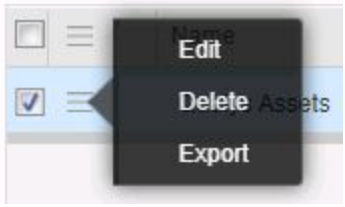
NIOS provides the ability to modify the templates via a simple text editor in the web interface. To modify templates perform the following steps:

1. Navigate to **Grid** → **Ecosystem** → **Templates**.

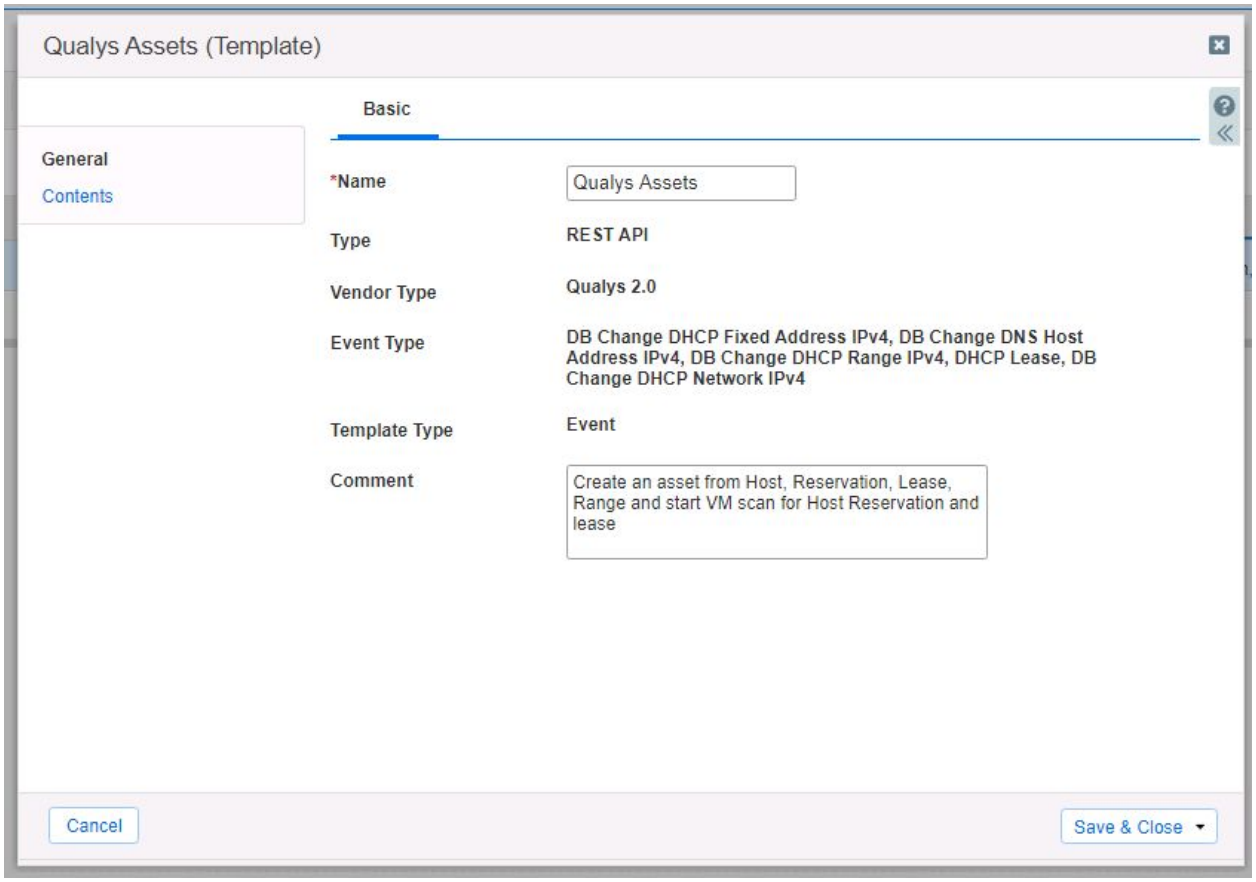


2. Click the ☰ **hamburger icon** associated with the Template you would like to modify.

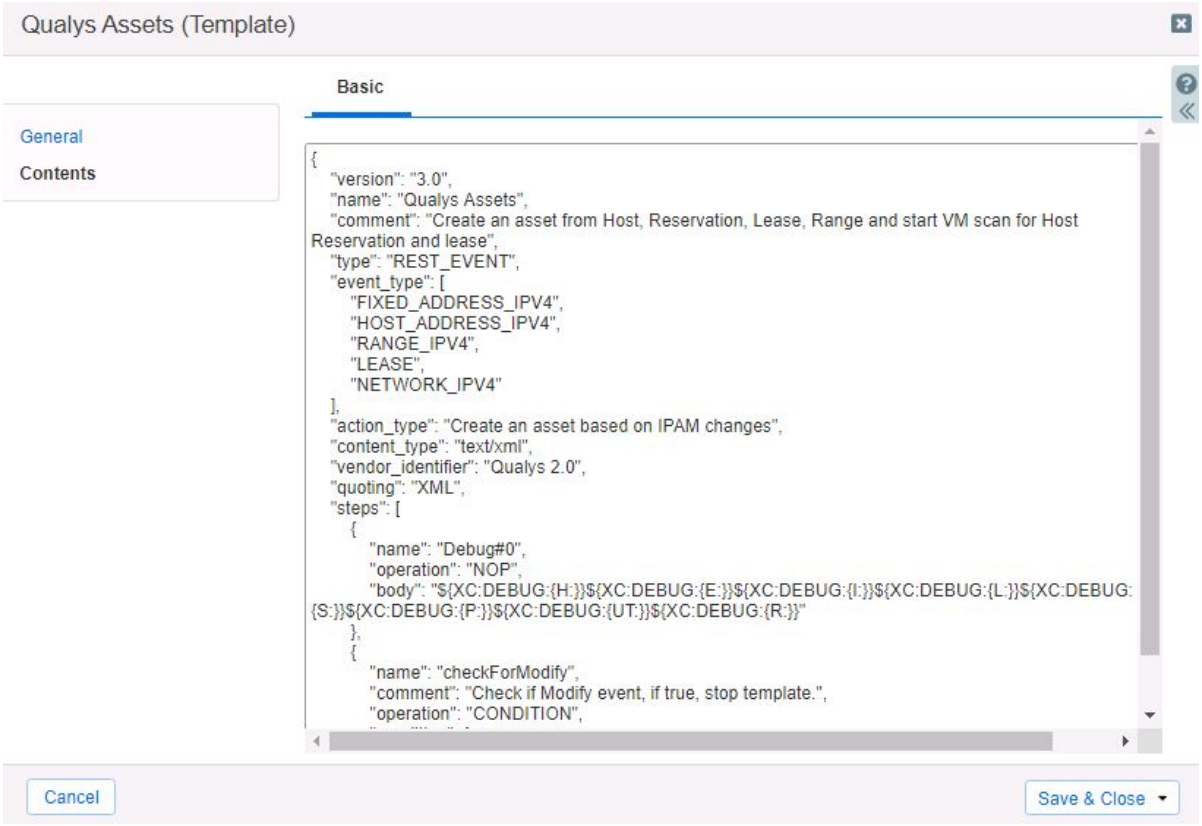
3. In the menu that is revealed, click **Edit**.



4. In the window that is revealed, click **Contents** in the left navigation panel.



5. A simple text editor will be revealed. This text editor allows for changes to be made to the template. It is recommended to only use the built-in template editor for minor edits. If desired, you may copy and paste from this text editor to an external text editor. To close the window without saving any changes, click **Cancel**. Or, to save any changes click **Save & Close**.

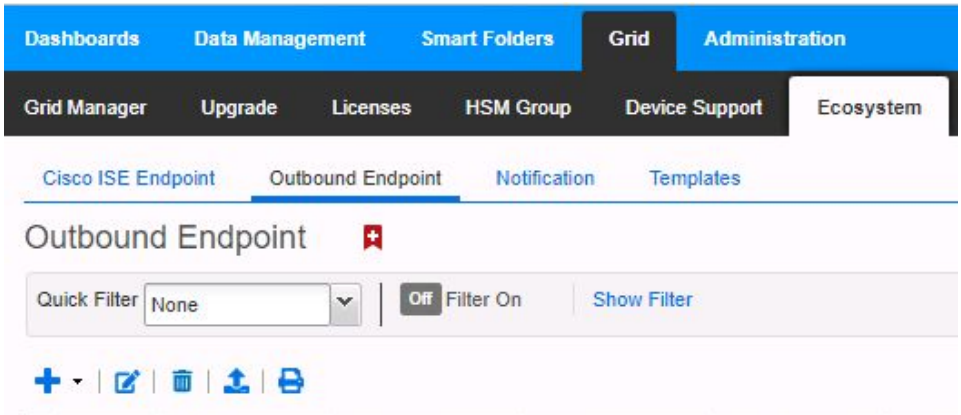


*Note: you may **not** delete a template if it is used by an Outbound endpoint or a notification.*

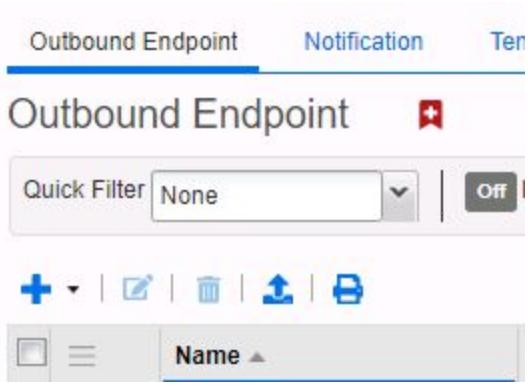
Add a REST API Endpoint

A **REST API Endpoint** can be viewed as a remote system which can 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).

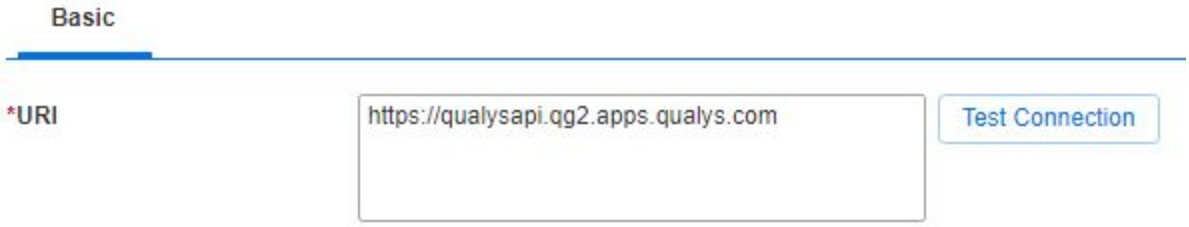
1. Navigate to **Grid** → **Ecosystem** → **Outbound Endpoint**.



2. Click the **+** icon located above the list of Outbound Endpoints.



3. An **Add REST API Endpoint Wizard** will be revealed. Input the following Information:
    - **URI**, the URI is the API address associated with the Outbound Endpoint. For information on how to acquire this address refer to the API documentation of the external device.



    - **Name**, Input a name for the Outbound Endpoint. *Note: this name is only used for backend organization purposes.*

    - **Vendor Type**, Select the vendor type from the drop-down menu. *Note: This value is sourced from any templates that have been uploaded to NIOS.*

    - **Auth Username** is the user account used to access the API of the Outbound Endpoint.

    - **Auth Password** is the API User's password used to access the API of the Outbound Endpoint.

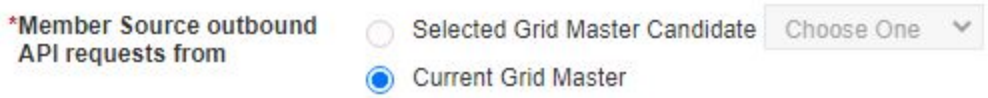
    - **WAPI Integration Username** is the NIOS user account used to access the NIOS API.

- **WAPI Integration Password** is the NIOS user account password used to access the NIOS API.

- (Optional) **Client Certificate** here is where you can upload a certificate for the Endpoint.

- (Optional) **Server Certificate Validation** is used to assist with encrypting traffic between NIOS the Outbound Endpoint. If you wish to encrypt the data input your certificates here.

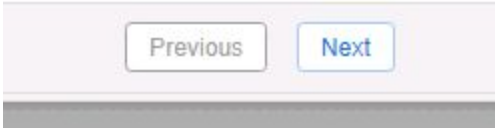
- (Optional) **Member Source outbound API requests from**. If desired, select another Grid Member to serve notifications to an external device. *Note: When possible, it is recommended to send notifications from a Grid Master Candidate instead of from the Grid Master.*



- (Optional) **Comment**. If desired you may input a comment for the Outbound Endpoint.

- (Optional) **Disable**. If desired you can disable the Outbound Endpoint by using this checkbox. *Note: that this only disables the Outbound Endpoint configuration, it does not disable any Notifications, or Templates that may be associated with this Endpoint.*

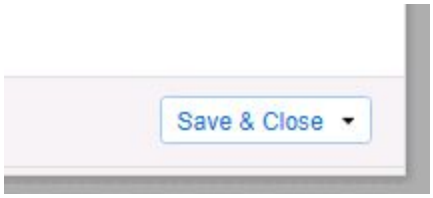
4. Click **Next** located at the bottom of the **Add REST API Endpoint Wizard**.



5. (Optional) Change the **Log Level** to **Debug** to view more information about the communication between Infoblox and an external device during testing.

6. (Optional) On **Step 2 of 3** of the **Add REST API Endpoint Wizard**, click the **Select Template** button to select a Session template for the external device.

7. Click **Save & Close** to confirm the creation of the REST API Endpoint.



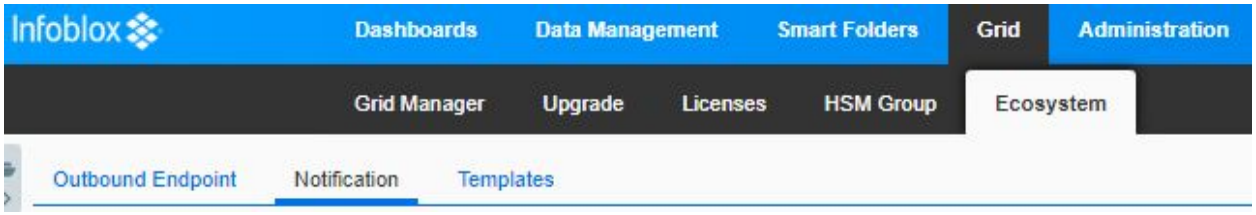
Add a Notification

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, the template which is executed and the API endpoint to which NIOS will establish the connection. The templates can support a variety of notifications. In order to simplify the deployment, only create required notifications, and use relevant filters. It is highly recommended to configure deduplication for ADP and RPZ events, and exclude a feed that is automatically populated by Threat Analytics.

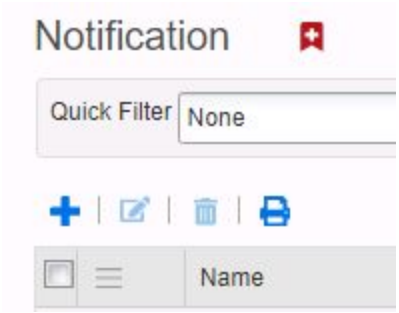
Note: An endpoint and a template must be added before you can add a notification.

In order to add notifications follow the following steps:

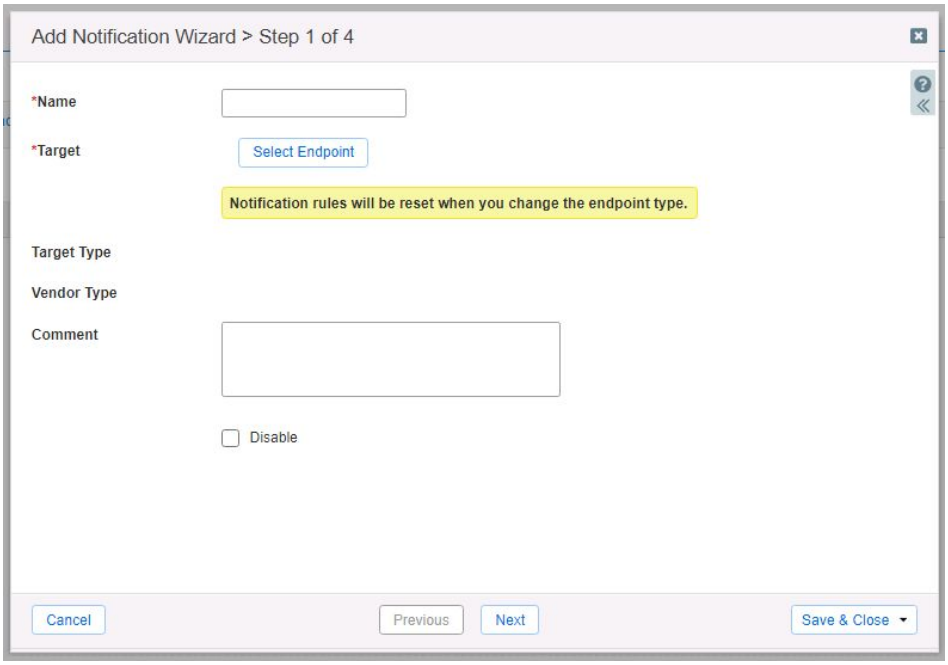
1. Navigate to **Grid** → **Ecosystem** → **Notification**.



2. Click the **+** icon located above the Notification list to begin adding a new **Notification**.

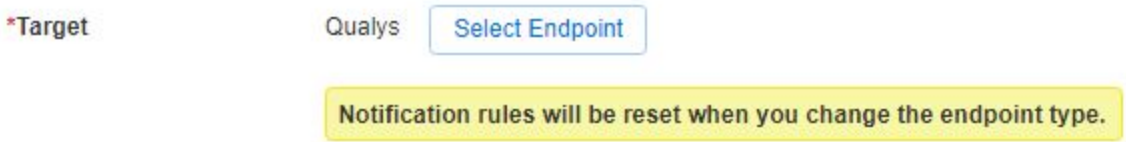


3. An **Add Notification Wizard** will be revealed.

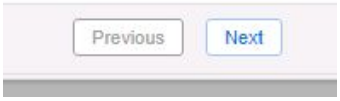


   - Specify the **Name** of the notification.

   - Select a **Target** endpoint by clicking the **Select Endpoint** button.

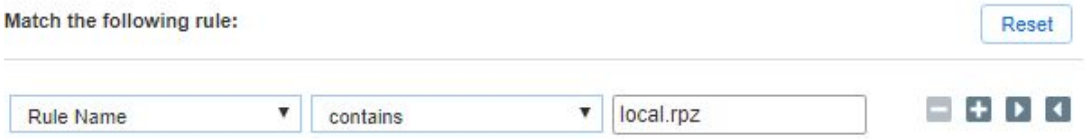


4. Click **Next**.



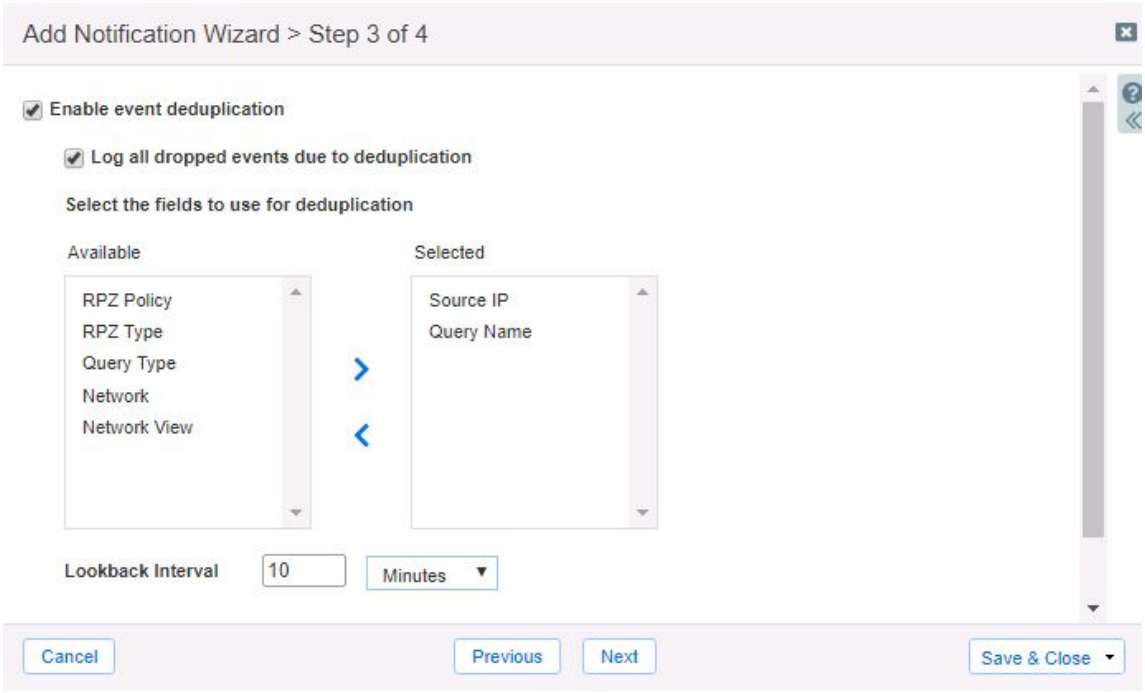
5. Select the relevant **Event** for the Notification by clicking on the Event dropdown.

6. Apply a Filter to the Notification. *Note: for optimal performance it is best practice to make the filter as narrow as possible.*

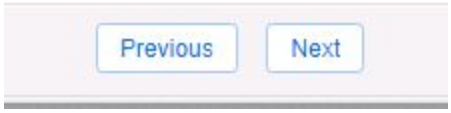


7. Click **Next**.

8. (For RPZ, and ADP notifications only) Click the Checkbox for **Enable event deduplication** and specify relevant parameters.

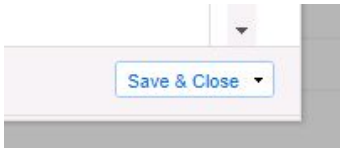


9. Click **Next**.



10. Click **Select Template** to select the relevant template.

11. Click **Save & Close** to finalize the creation of the Notification.



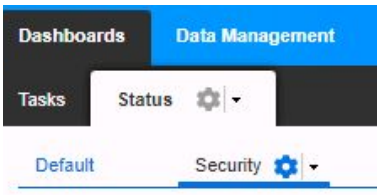
12. Create any other **Notifications** for other events as desired.

Check the Configuration

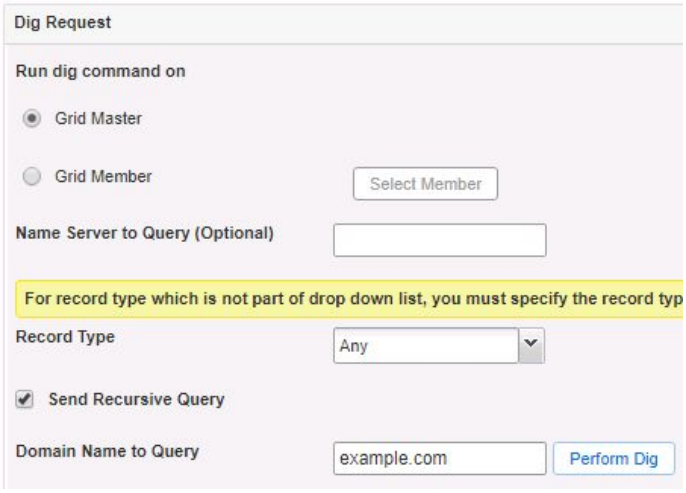
Emulate an RPZ Event

You can emulate an RPZ event to test a RPZ notification by performing the following steps:

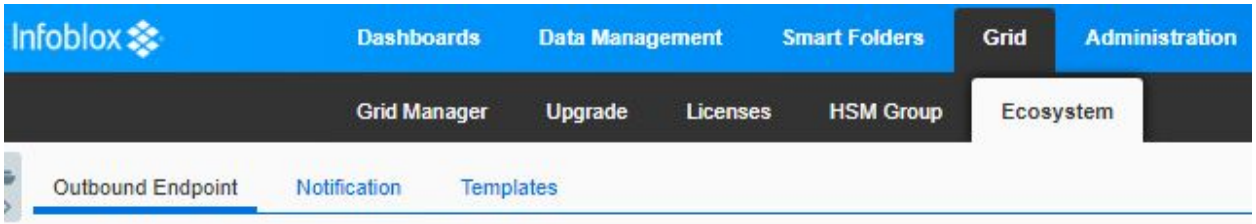
1. Navigate to **Dashboards** → **Status** → **Security**.



2. Input a domain in the **Domain Name to Query** text field**.** Ensure that the domain selected is contained in the RPZ that was included in the notification that was created earlier in this document. Then, click the **Perform Dig** button.

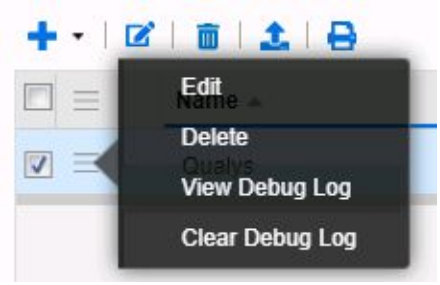


3. To view the results of the test, navigate to **Grid** → **Ecosystem** → **Outbound Endpoint**.

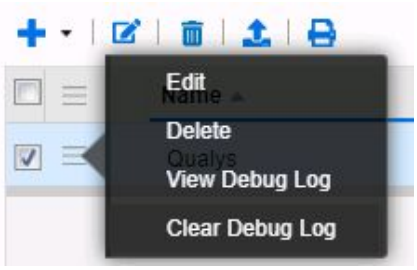


4. Click the ☰ hamburger icon associated with the **REST API Endpoint**.

5. Click **View Debug Log** in the menu that is revealed.



6. (Optional) To clear the Debug Log for other tests you may click **Clear Debug Log** instead.

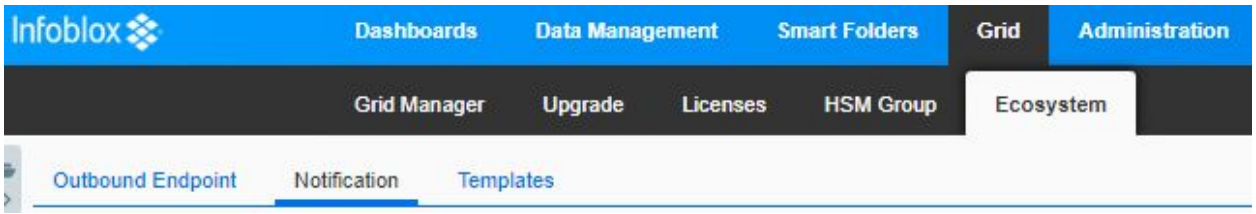


Note: Depending on a browser, the debug log will be downloaded or opened in a new tab. You may need to check your popup blocker or download settings.

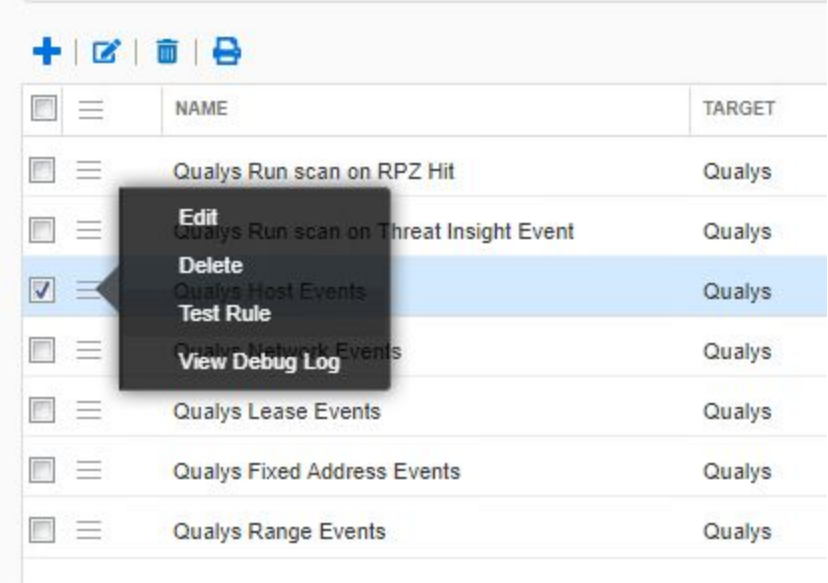
Test a Notification

For specific event types, you may test a Notification via the Test Rule function.

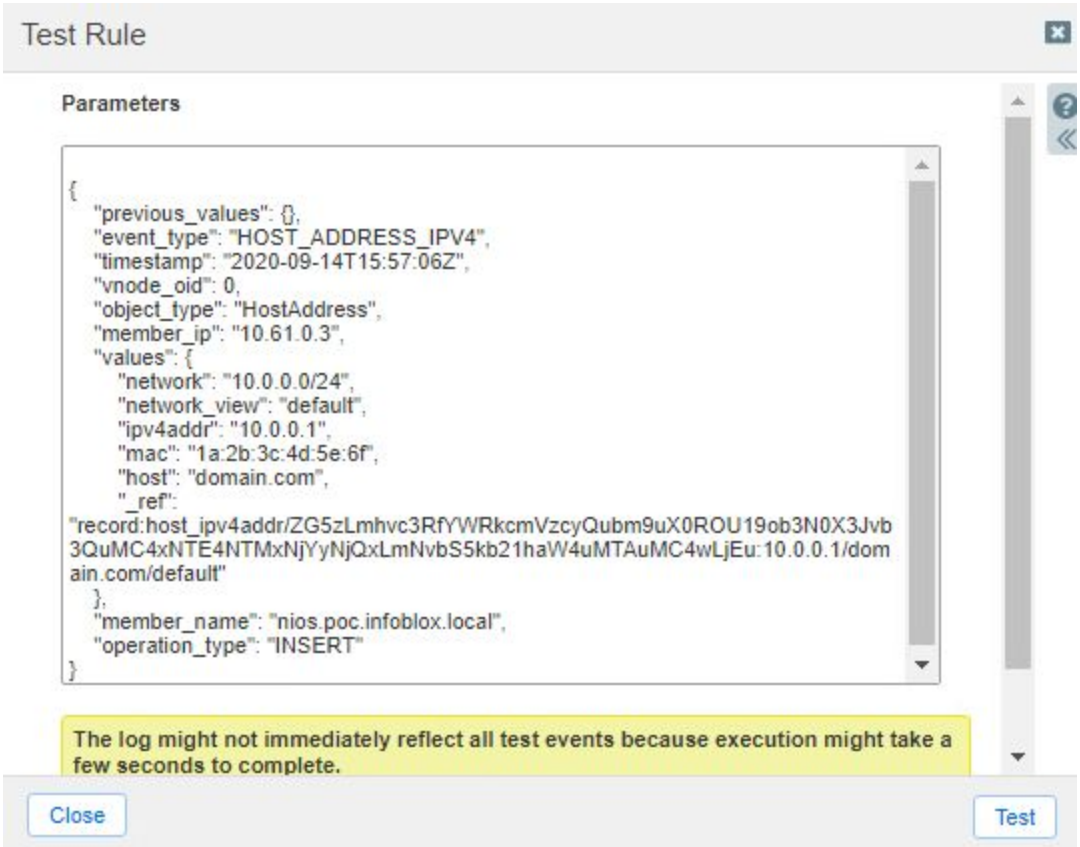
1. To test a notification, navigate to **Grid** → **Ecosystem** → **Notification**.



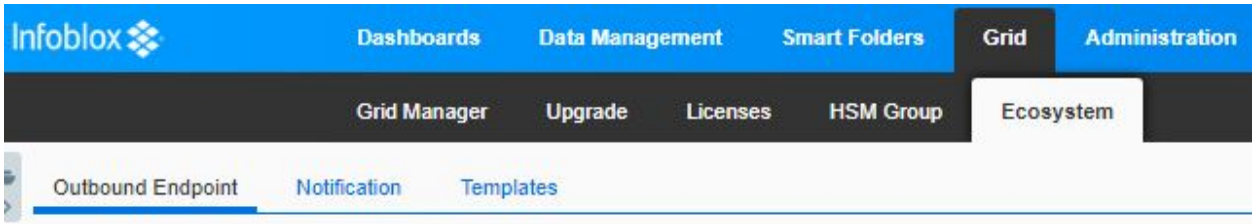
2. Click the ☰ **hamburger icon** associated with the Notification you would like to test. Then, click **Test Rule** in the menu that is revealed.



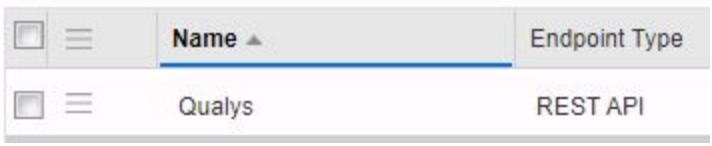
3. A Test Rule window will be revealed. If needed, modify the test parameters so that they will trigger the notification. Then, click **Test**.



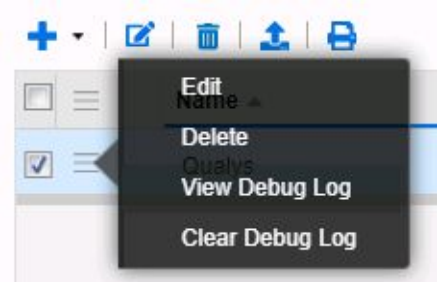
4. To view the results of the test, navigate to **Grid → Ecosystem → Outbound Endpoint**.



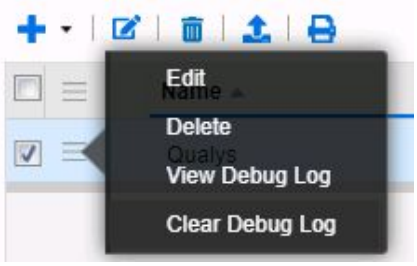
5. Click the ☰ hamburger icon associated with the **REST API Endpoint**.



6. Click **View Debug Log** in the menu that is revealed.



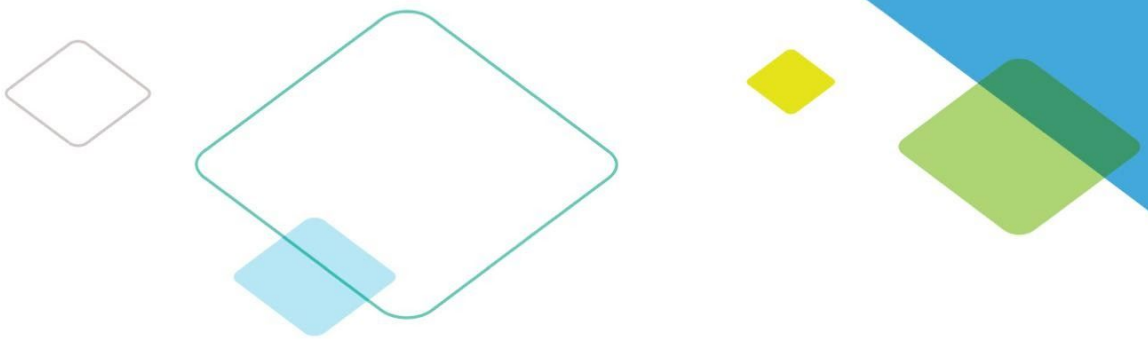
7. (Optional) To clear the Debug Log for other tests you may click **Clear Debug Log** instead. *Note: this will clear any contents in the debug log, when a log is cleared, there is no way to recover it.*



Additional Resources

For more information regarding Infoblox or the Infoblox Outbound API, 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/



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