DEPLOYMENT GUIDE

Enabling and Configuring Outbound API Notifications

Table of Contents

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. Various 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 (eg.: 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, testing all changes before implementing them into production is highly recommended.

Please refer to the Infoblox NIOS Administrator's Guide for any other best practices, limitations and 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.

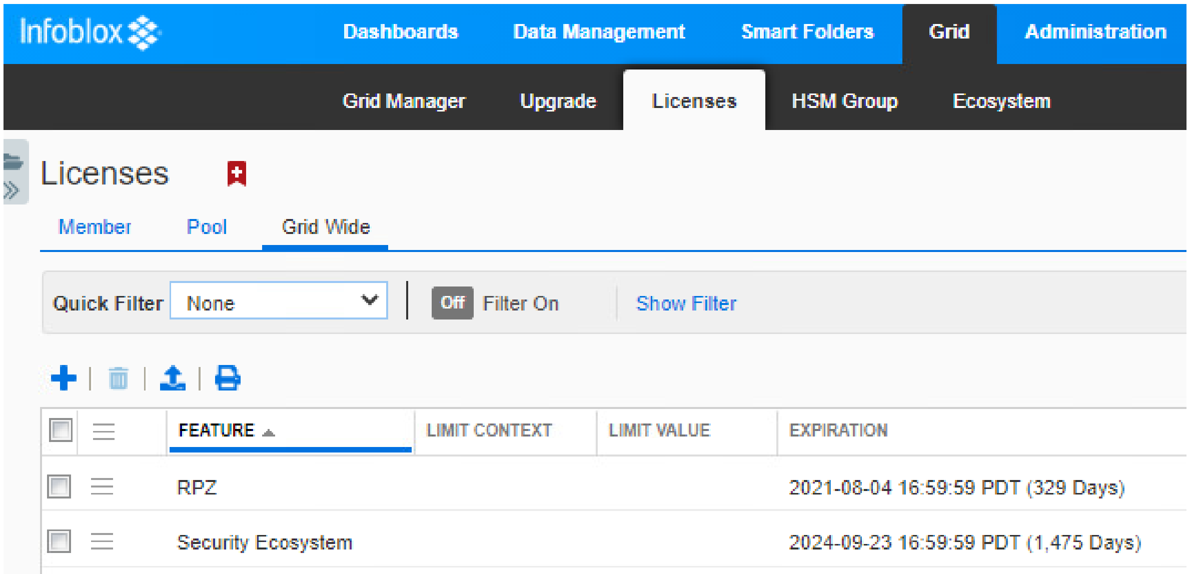
6. Add a REST API Endpoint.

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.



Quick Filter: None

Off Filter On

FEATURE	LIMIT CONTEXT	LIMIT VALUE	EXPIRATION
RPZ			2021-08-04 16:59:59 PDT (329 Days)
Security Ecosystem			2024-09-23 16:59:59 PDT (1,475 Days)

Create or Download Templates from the Infoblox Community Website

Outbound API templates are essential to the configuration. Templates fully control the integration and steps required to execute the outbound notifications. Detailed information on developing templates can be found in the NIOS Administrator's guide.

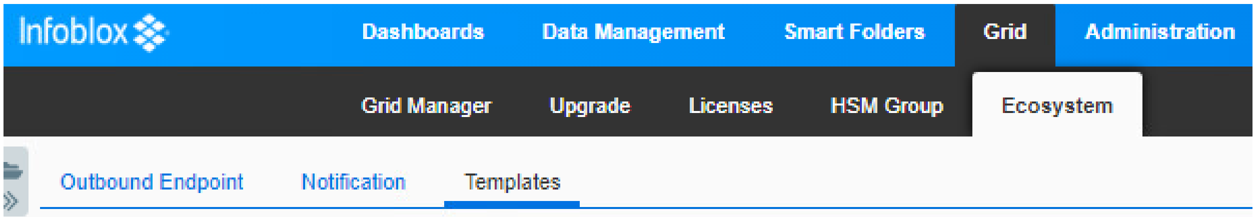
Infoblox does not distribute any templates (out-of-the-box) with the NIOS releases. Templates are available on the Infoblox community website. Community created Templates will be located in Partners Integrations, you can also find other templates posted in the API & Integration forum.

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.

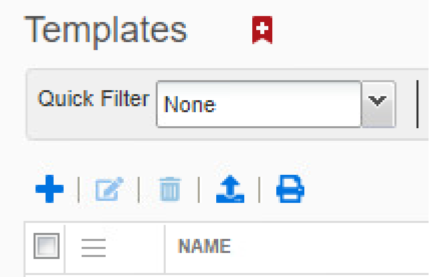
Add/Upload Templates

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

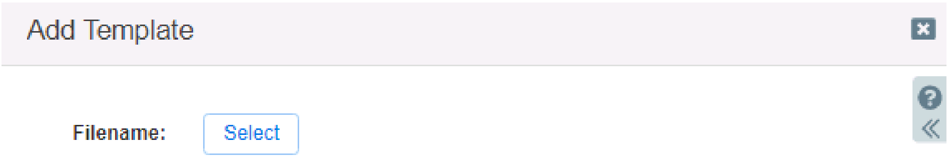
1. Navigate to **Grid** → **Ecosystem** → **Templates**.



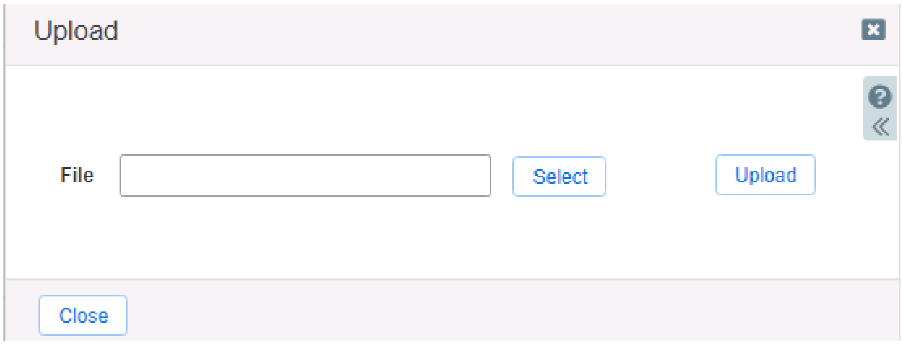
2. Press the **+** icon located above the table of Templates.



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

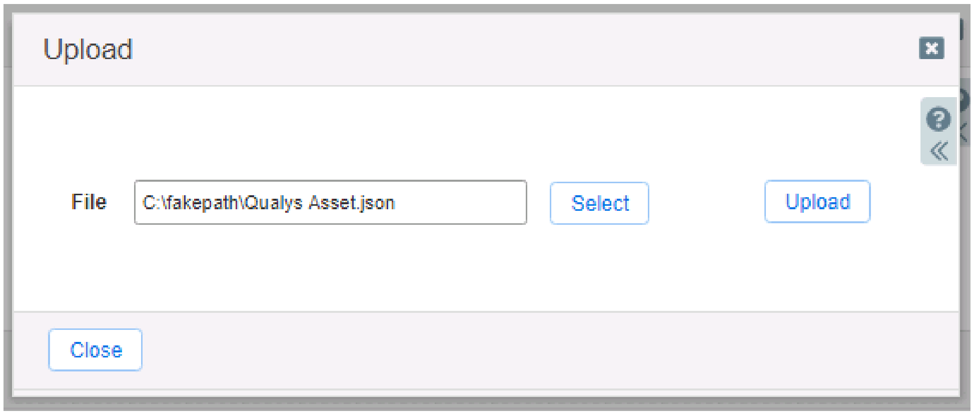


4. Click the **Select** button in the revealed Upload dialog box.



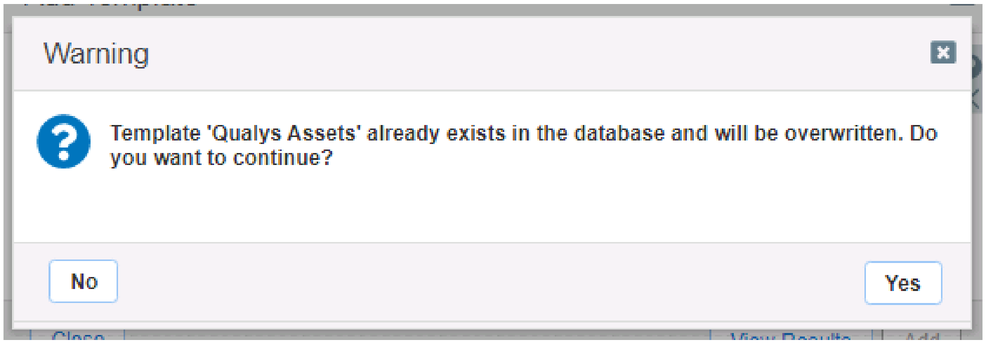
5. Locate and select the Template you would like to upload. Or, input the full path of the file in the File text box.

6. Once the File has been selected, click **Upload**.



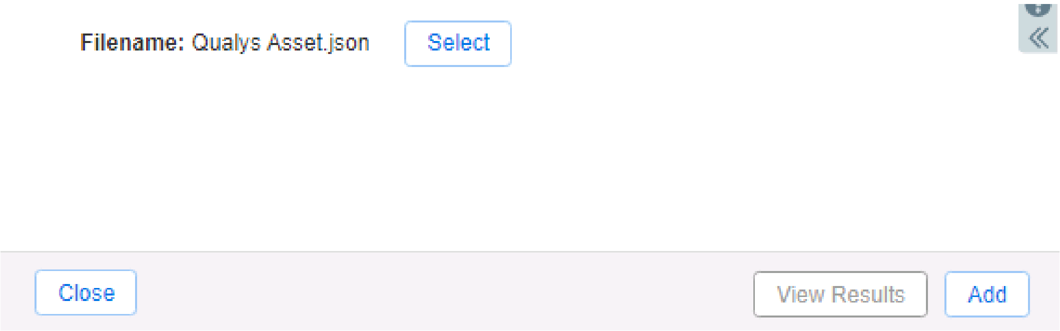
File C:\fakepath\Qualys Asset.json

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


Warning

Template 'Qualys Assets' already exists in the database and will be overwritten. Do you want to continue?

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


Filename: Qualys Asset.json

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

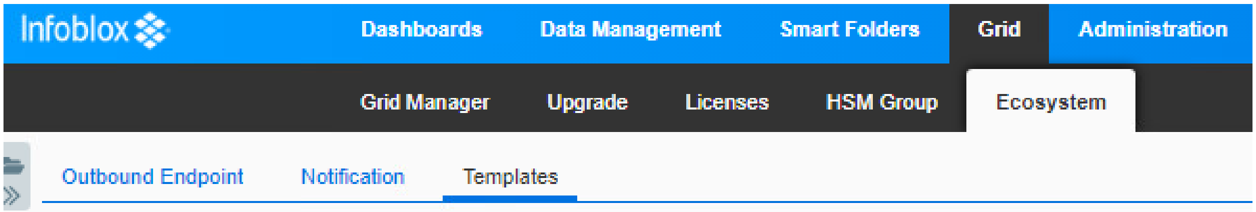
10. Repeat steps 2-8 for any other templates you intend to upload.

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

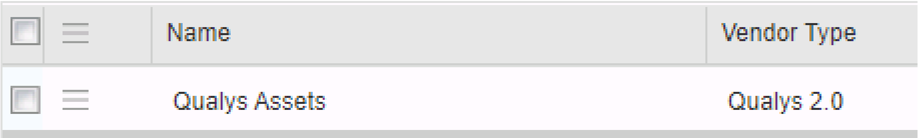
Modifying Templates

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**.

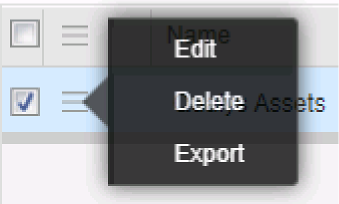


2. Click the ≡ hamburger icon associated with the Template you would like to modify.

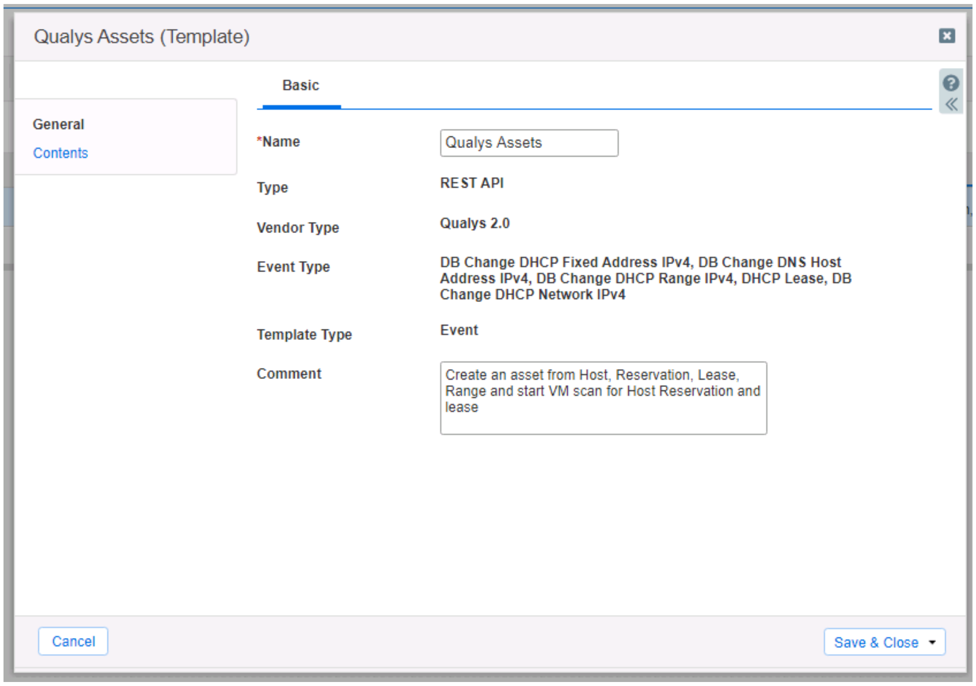


□	≡	Name	Vendor Type
□	≡	Qualys Assets	Qualys 2.0

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



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



*Name: Qualys Assets

Type: REST API

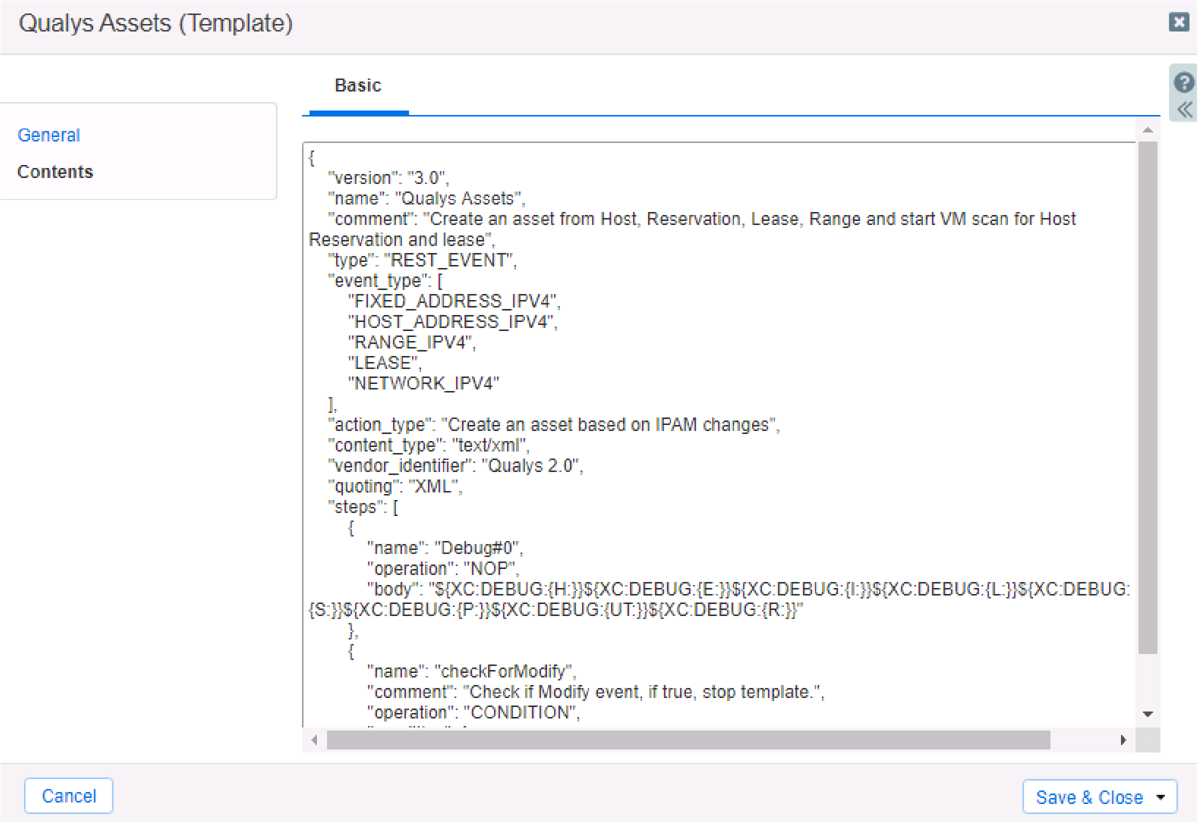
Vendor Type: Qualys 2.0

Event Type: DB Change DHCP Fixed Address IPv4, DB Change DNS Host Address IPv4, DB Change DHCP Range IPv4, DHCP Lease, DB Change DHCP Network IPv4

Template Type: Event

Comment: Create an asset from Host, Reservation, Lease, Range and start VM scan for Host Reservation and lease

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**.



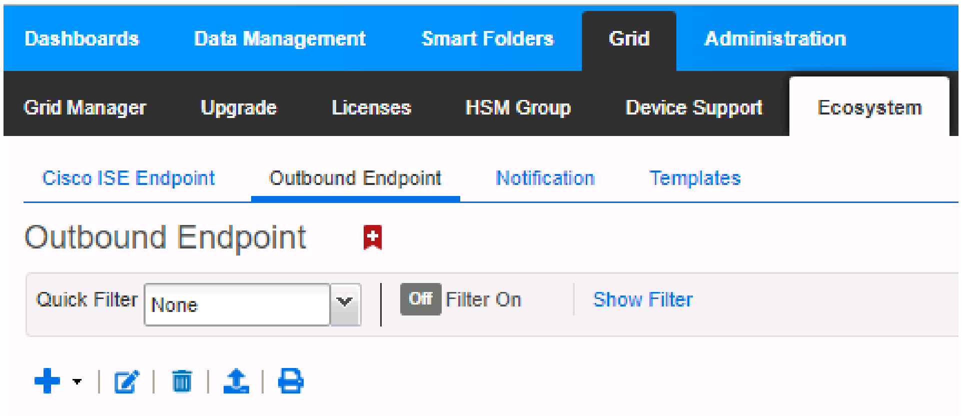
```
{
   "version": "3.0",
   "name": "Qualys Assets",
   "comment": "Create an asset from Host, Reservation, Lease, Range and start VM scan for Host
Reservation and lease",
   "type": "REST_EVENT",
   "event_type": [
      "FIXED_ADDRESS_IPV4",
      "HOST_ADDRESS_IPV4",
      "RANGE_IPV4",
      "LEASE",
      "NETWORK_IPV4"
   ],
   "action_type": "Create an asset based on IPAM changes",
   "content_type": "text/xml",
   "vendor_identifier": "Qualys 2.0",
   "quoting": "XML",
   "steps": [
      {
         "name": "Debug#0",
         "operation": "NOP",
         "body": "${XC:DEBUG:{H:}}${XC:DEBUG:{E:}}${XC:DEBUG:{I:}}${XC:DEBUG:{L:}}${XC:DEBUG:
{S:}}${XC:DEBUG:{P:}}${XC:DEBUG:{UT:}}${XC:DEBUG:{R:}}"
      },
      {
         "name": "checkForModify",
         "comment": "Check if Modify event, if true, stop template.",
         "operation": "CONDITION",
```

Note: You may not delete a template if an Outbound endpoint or a notification uses it.

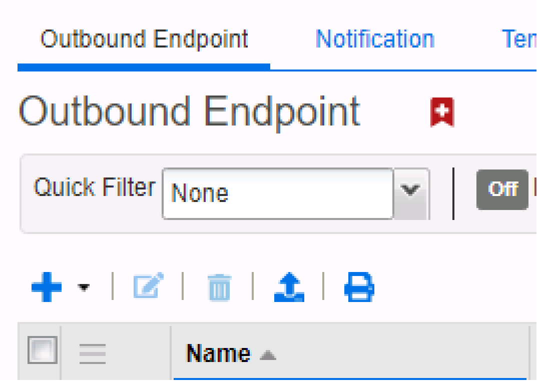
Add a REST API Endpoint

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 but also receive the notifications from itself (e.g., for testing purposes).

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

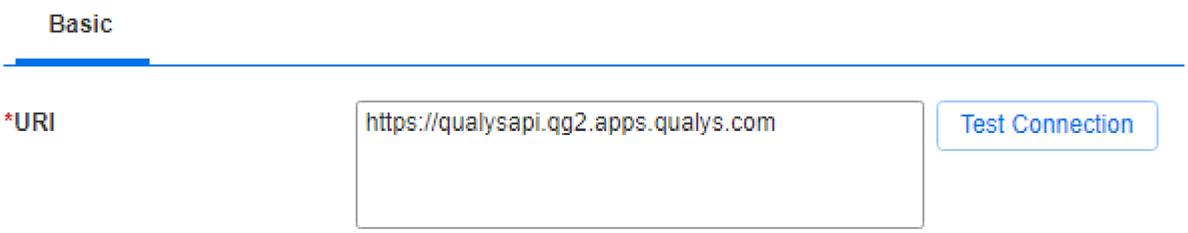


2. Click the **+** icon located above the list of Outbound Endpoints.



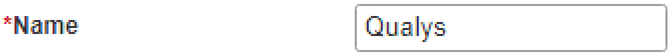
3. An Add REST API Endpoint Wizard will be revealed. Input the following information:

   - **URI**, the URI is the API address associated with the Outbound Endpoint. For information on acquiring this address, refer to the API documentation of the external device.



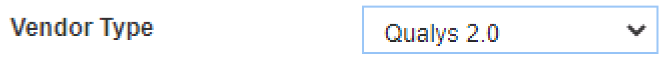
*URI https://qualysapi.qg2.apps.qualys.com

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



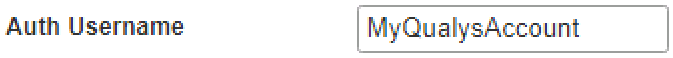
*Name Qualys

   - **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.



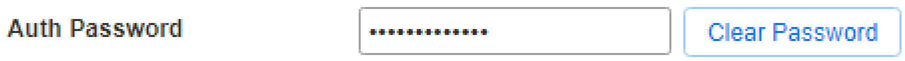
Vendor Type Qualys 2.0

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



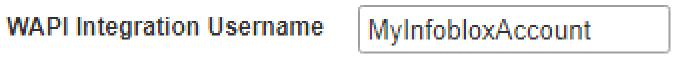
Auth Username MyQualysAccount

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



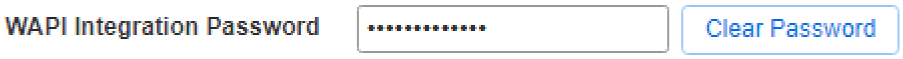
Auth Password ••••••••••••••

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



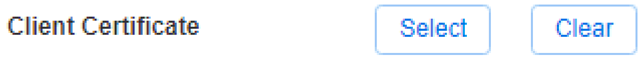
WAPI Integration Username MyInfobloxAccount

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



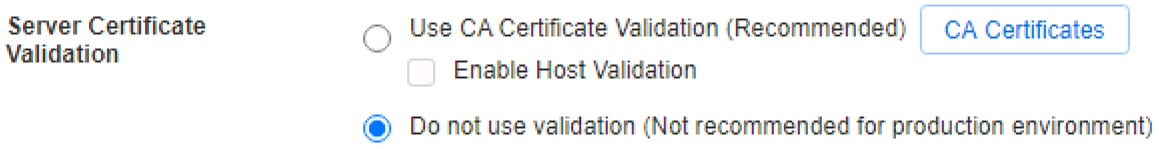
WAPI Integration Password ••••••••••••••

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



Client Certificate

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



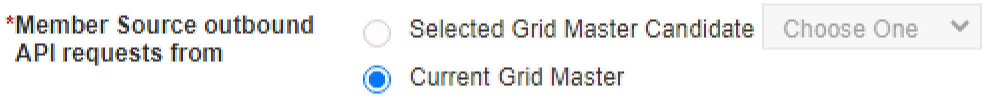
Server Certificate Validation

○ Use CA Certificate Validation (Recommended)

□ Enable Host Validation

● Do not use validation (Not recommended for production environment)

- (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.

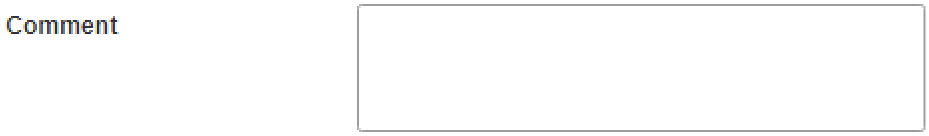


*Member Source outbound API requests from

○ Selected Grid Master Candidate Choose One

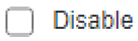
● Current Grid Master

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



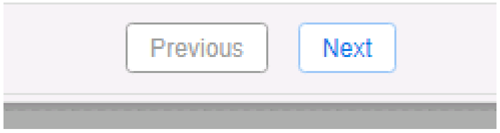
Comment

- (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.



□ Disable

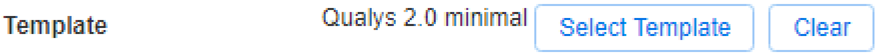
4. Click **Next,** located at the bottom of the Add REST API Endpoint Wizard.



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

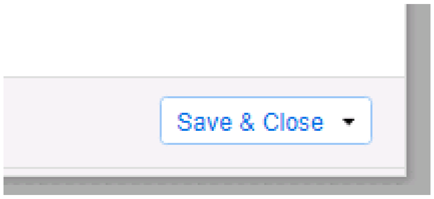
Log Level: Debug

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.



Template: Qualys 2.0 minimal

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



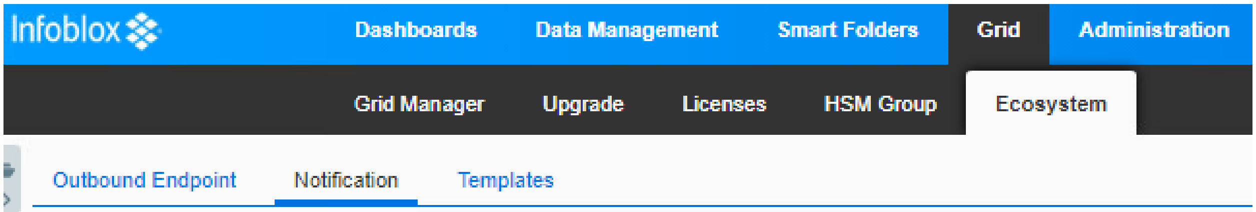
Add a Notification

A notification can be considered 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.

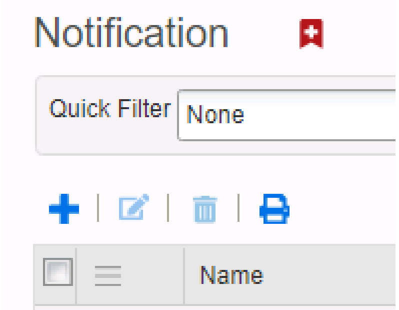
Note: An endpoint and a template must be added before you can add a notification.

To add notifications, follow the following steps:

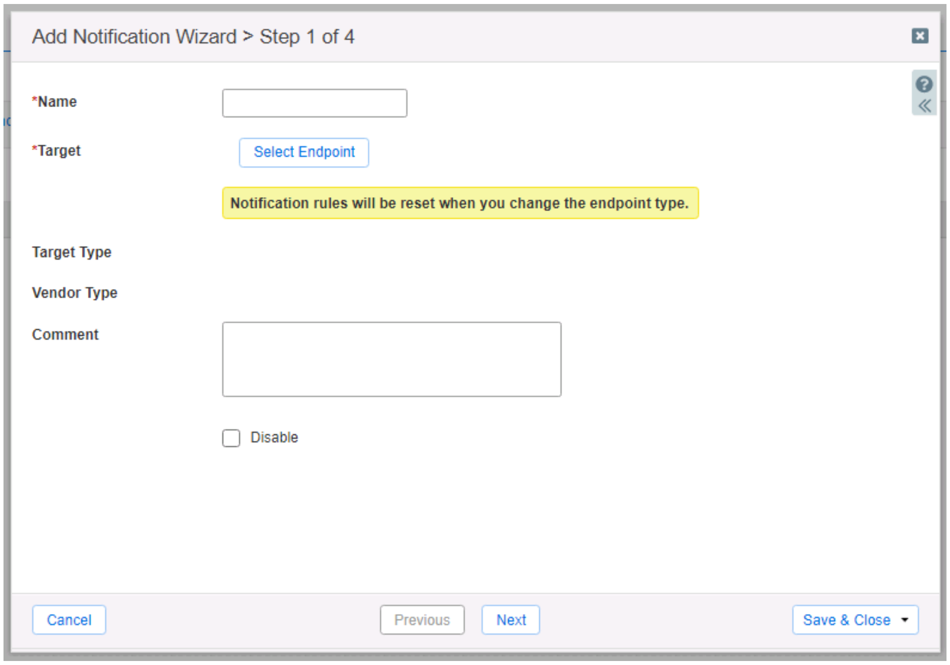
1. Navigate to **Grid** → **Ecosystem** → **Notification**.



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



3. An Add Notification Wizard will be revealed.



Add Notification Wizard > Step 1 of 4

*Name

*Target

Notification rules will be reset when you change the endpoint type.

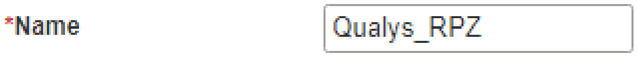
Target Type

Vendor Type

Comment

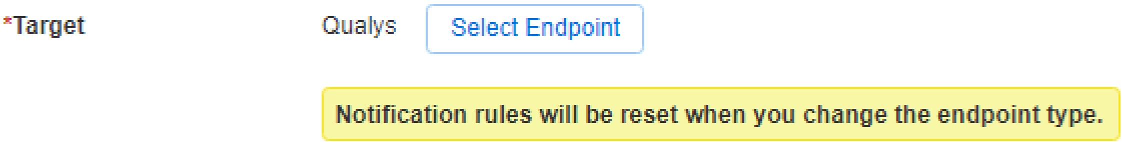
□ Disable

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



*Name: Qualys_RPZ

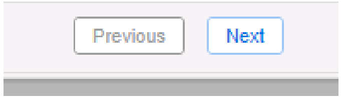
- Select a **Target** endpoint by clicking the **Select Endpoint** button.



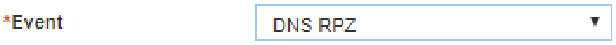
*Target: Qualys

Notification rules will be reset when you change the endpoint type.

4. Click **Next**.

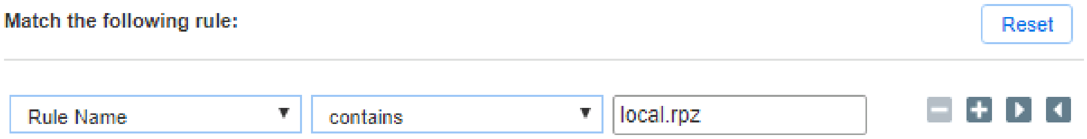


5. Select the relevant Event for the Notification by clicking on the **Event** dropdown.



*Event: DNS RPZ

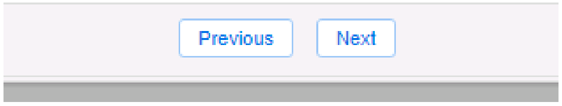
6. Apply a Filter to the Notification. Note: It is best practice to make the filter as narrow as possible for optimal performance.



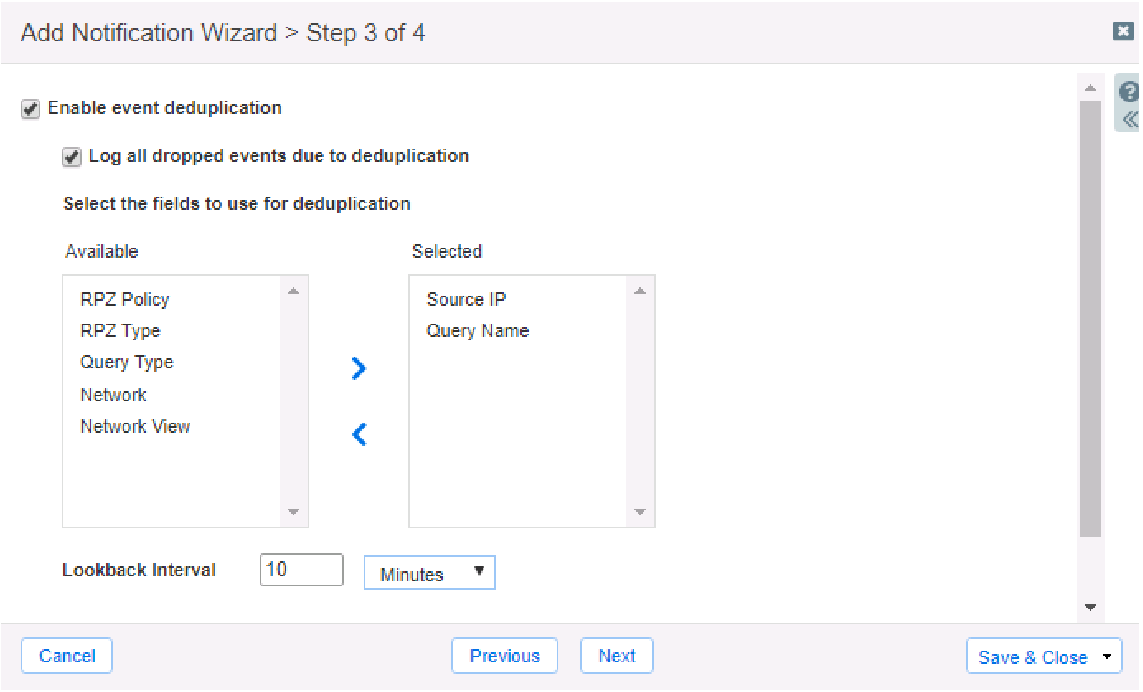
Match the following rule:

Rule Name ▾ contains ▾ local.rpz

7. Click **Next**.



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



Add Notification Wizard > Step 3 of 4

☑ Enable event deduplication

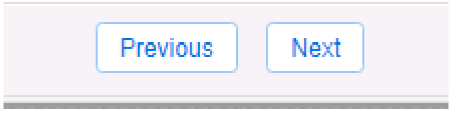
☑ Log all dropped events due to deduplication

Select the fields to use for deduplication

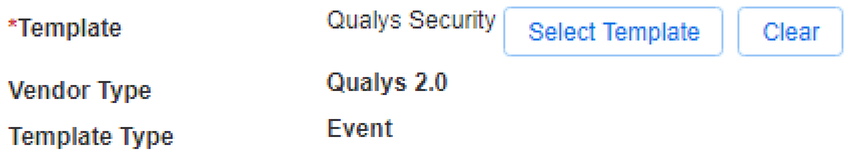
Available	Selected
RPZ Policy	Source IP
RPZ Type	Query Name
Query Type	
Network	
Network View	

Lookback Interval 10 Minutes ▾

9. Click **Next**.



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

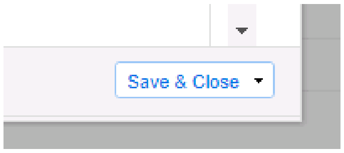


*Template: Qualys Security

Vendor Type: Qualys 2.0

Template Type: Event

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



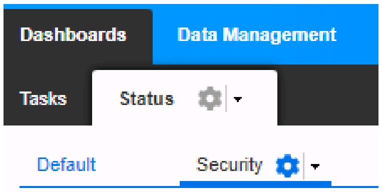
12. Create any other Notifications for other events as desired.

Check the Configuration

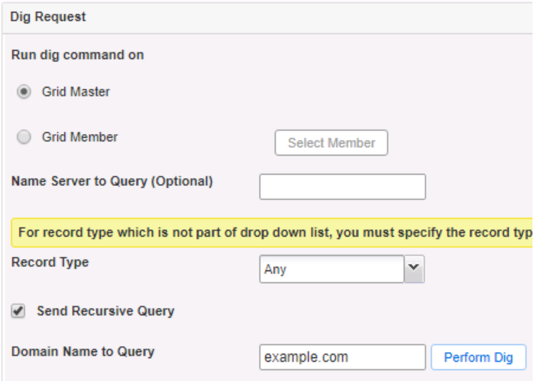
Emulate an RPZ Event

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 selected domain is contained in the RPZ included in the notification created earlier in this document. Then, click the **Perform Dig** button.



Dig Request

Run dig command on

● Grid Master

○ Grid Member

Name Server to Query (Optional):

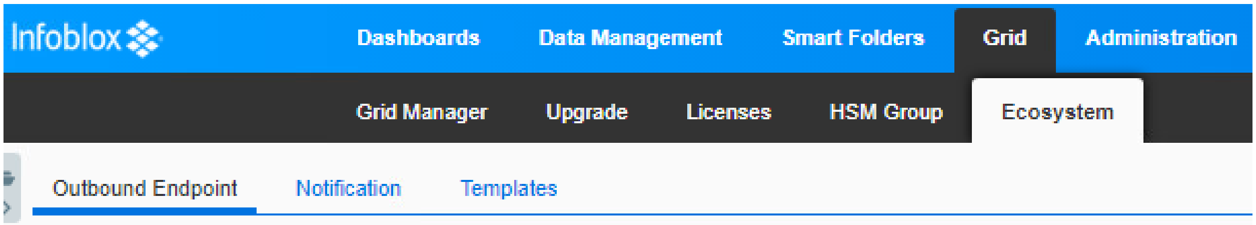
For record type which is not part of drop down list, you must specify the record typ

Record Type: Any

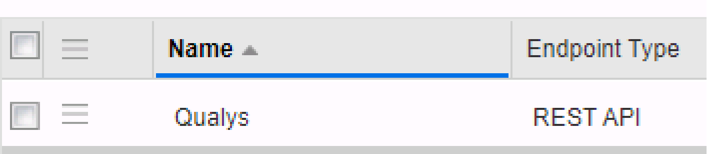
☑ Send Recursive Query

Domain Name to Query: example.com

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

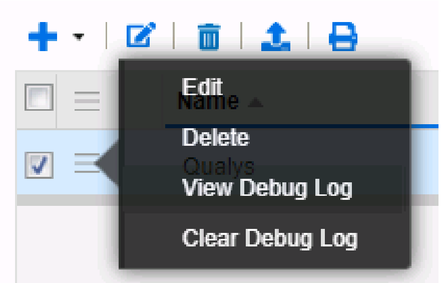


4. Click the ☰ hamburger icon associated with the REST API Endpoint.

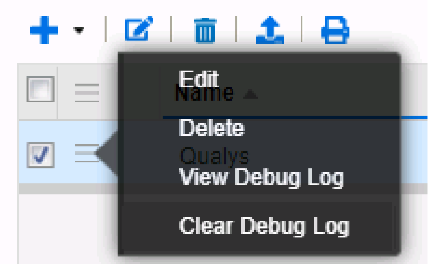


□	☰	Name ▲	Endpoint Type
□	☰	Qualys	REST API

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



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

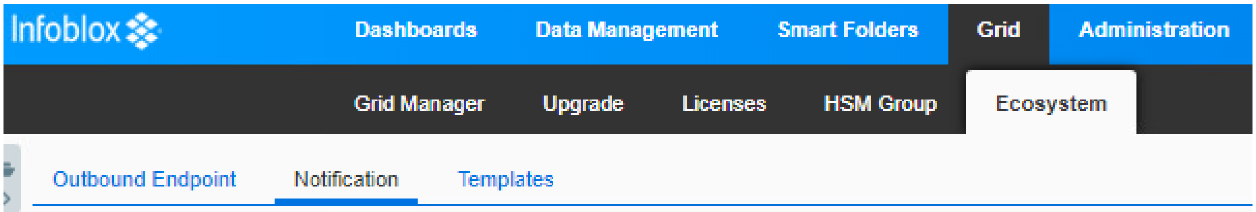


Note: Depending on a browser, the debug log will be downloaded or opened in a new tab. You may need to check your popup blocker or download settings.

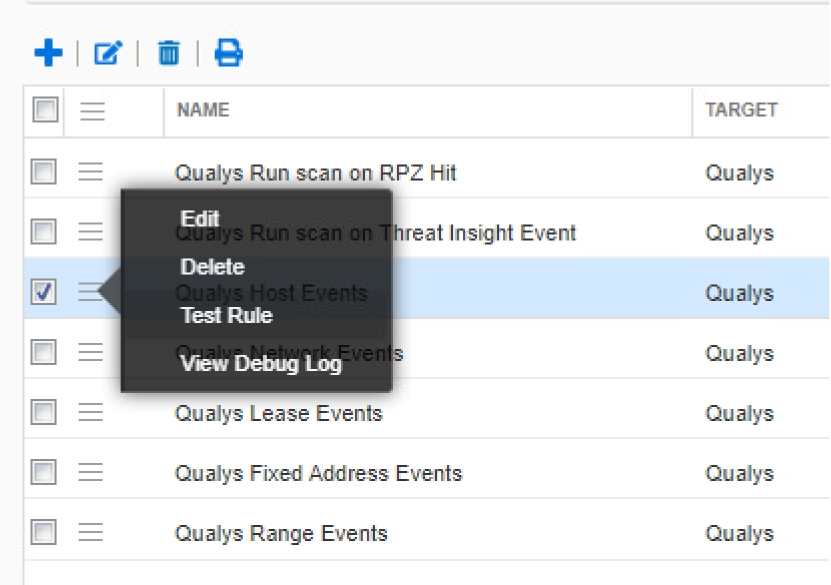
Test a Notification

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

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

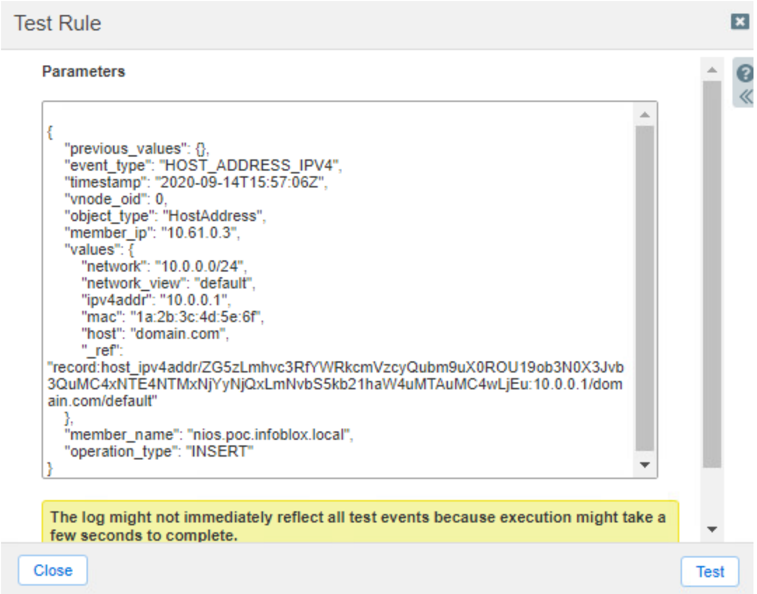


2. Click the ☰ hamburger icon associated with the Notification you want to test. Then, click **Test Rule** in the menu that is revealed.



		NAME	TARGET
□	☰	Qualys Run scan on RPZ Hit	Qualys
□	☰	Qualys Run scan on Threat Insight Event	Qualys
☑	☰	Qualys Host Events	Qualys
□	☰	Qualys Network Events	Qualys
□	☰	Qualys Lease Events	Qualys
□	☰	Qualys Fixed Address Events	Qualys
□	☰	Qualys Range Events	Qualys

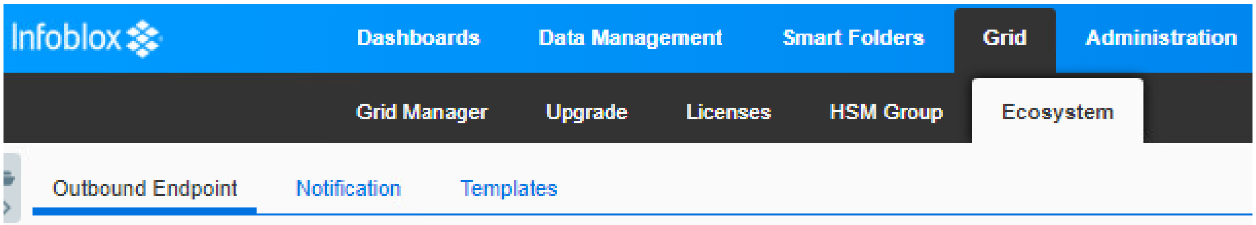
3. A Test Rule window will be revealed. If needed, modify the test parameters so that they will trigger the notification. Then, click **Test**.



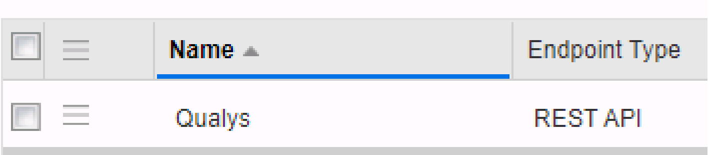
```
{
   "previous_values": {},
   "event_type": "HOST_ADDRESS_IPV4",
   "timestamp": "2020-09-14T15:57:06Z",
   "vnode_oid": 0,
   "object_type": "HostAddress",
   "member_ip": "10.61.0.3",
   "values": {
      "network": "10.0.0.0/24",
      "network_view": "default",
      "ipv4addr": "10.0.0.1",
      "mac": "1a:2b:3c:4d:5e:6f",
      "host": "domain.com",
      "_ref":
"record:host_ipv4addr/ZG5zLmhvc3RfYWRkcmVzcyQubm9uX0ROU19ob3N0X3Jvb
3QuMC4xNTE4NTMxNjYyNjQxLmNvbS5kb21haW4uMTAuMC4wLjEu:10.0.0.1/dom
ain.com/default"
   },
   "member_name": "nios.poc.infoblox.local",
   "operation_type": "INSERT"
}
```

The log might not immediately reflect all test events because execution might take a few seconds to complete.

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

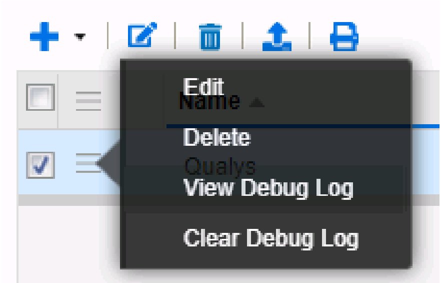


5. Click the ☰ hamburger icon associated with the REST API Endpoint.

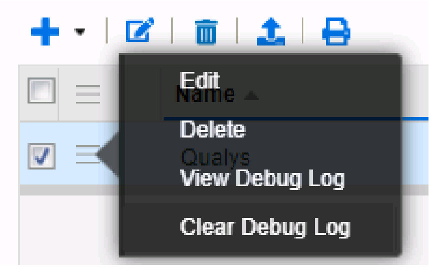


□	☰	Name ▲	Endpoint Type
□	☰	Qualys	REST API

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/

infoblox.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054
+1.408.986.4000
www.infoblox.com