Infoblox
CONTROL YOUR NETWORK

DEPLOYMENT GUIDE

Integration with Qualys

Outbound API

Contents

Introduction

Infoblox and Qualys: Supercharge Network Visibility and Automate Remediation
By combining Infoblox's DNS technology with the Qualys Cloud Platform, organizations can automate scanning when new devices join the network or when malicious activity is detected. Key capabilities include:

- **Asset Management**: Infoblox provides device discovery and a single source of truth for devices and networks, which Qualys can leverage for organizing new assets, automated tracking, and a detailed view of the network.
- **Visibility**: Infoblox delivers outbound notifications to Qualys to provide visibility into new networks, hosts, and IP-connected devices (IoT) joining the network, including contextual information such as where on the network an infected device is and to whom the device is assigned. This detailed context allows IT departments to prioritize response and remediation.
- **Malware and Data Exfiltration Threat Identification**: Infoblox uses advanced threat intelligence to detect and control malware communications at the DNS level by disrupting command-and-control communications to proactively control the spread of malware such as ransomware that uses DNS. These indicators of compromise can be easily shared with Qualys for further analysis and remediation.
- **Compliance and Audit**: Infoblox triggers Qualys when new devices join the network—physical, virtual, or cloud—to check for compliance.

Prerequisites

The following are prerequisites for the integration using Outbound API notifications:

- NIOS 8.1 or higher.
- Security Ecosystem license.
- Outbound API integration templates.
- Prerequisites for the templates (e.g. configured and set extensible attributes).
- Pre-configured services: DNS, DHCP, RPZ, Threat Analytics.

Limitations

Known limitations:

- Supported notifications: Object Change Network IPv4, Object Change Fixed Address IPv4, Object Change Host Address IPv4, Object Change Range IPv4, DHCP Leases, DNS RPZ and DNS Tunneling.

Best Practices

Outbound API templates can be found on the Infoblox community site (https://community.infoblox.com/). After registering an account, you can subscribe to the relevant groups and forums.

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

Although the pictures in this deployment guide depict a Infoblox NIOS version 8.2.1, everything can be performed in NIOS version 8.1 or higher.

Please refer to Infoblox's NIOS Administration 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 portal (https://support.infoblox.com/).

Configuration

Workflow

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

- Infoblox:
  - Install the Security Ecosystem license if it was not installed.
  - Check that the necessary services and features are properly configured and enabled, including DNS, RPZ, DHCP and Threat Analytics.
  - Create the required Extensible Attributes.
  - Download (or create your own) notification templates (delete_qualys.json, insert_qualys.json, qualys_dnsfw_tunnel_scan.json, qualys_host_reservation_lease_range_add.json, qualys_session.json) from the Infoblox community web-site.
  - Add the templates.
  - Add a REST API Endpoint:
  - Add Notifications.
  - Emulate an event, check Rest API debug log and/or verify changes on the grid.

Download templates from the Infoblox community web-site

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 with the NIOS releases (out-of-box). Templates are available on the Infoblox community web-site. Templates for the Qualys integration are located in the **"Partners Section"** forum. Other templates are also 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.

Other Relevant information

Create Extensible Attributes

Qualys templates use several extensible attributes to adjust the templates behavior. The supported extensible attributes are described in the table below and can be entered through the grid GUI at **"Administration"** → **"Extensible Attributes".**

Extensible Attribute	Description
Qualys_Asset_PC	"True or False": Defines if an asset should be created in Policy Compliance module. Used by "qualys_host_reservation_lease_range_add.json" template.
Qualys_Asset_VM	"True or False": Defines if an asset should be created in Vulnerability Management module. Used by "qualys_host_reservation_lease_range_add.json" template.
Qualys_Assets_Group	Defines a Qualys asset group for the object. If the assets group does not already exist, the assets group will be added to Qualys.
Qualys_LastScanTime	Internal attribute. Last time when an object* was scanned by Qualys.
Qualys_SNMP	Internal attribute. SNMP credentials id.

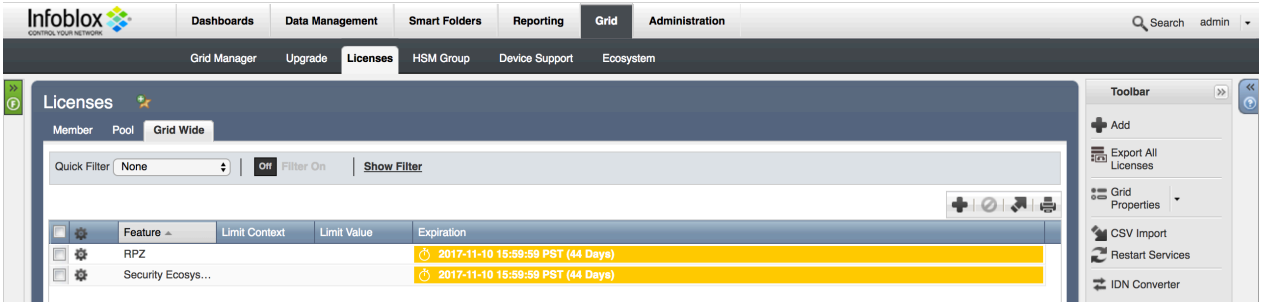
Qualys_Scan	"True or False": Defines if an object should be scanned as a response to a security event.
Qualys_Scan_On_Add	"True or False": Defines if an object should be scanned when it is added to Qualys.
Qualys_Scan_Option	Defines Qualys Scan option profile, which should be used.
Qualys_Scanner	Defines Qualys scanner appliance, which should be used.
Qualys_SyncTime	Internal attribute. Provides the time when an object* was synced with Qualys.
Qualys_Sync_Group	Internal attribute. Provies the the asset group an object was synced with in Qualys.
Qualys_UNIX	Internal attribute. Unix credentials id.
Qualys_User_SNMP	SNMP credentials which should be used to scan an object.
Qualys_User_Unix	Unix credentials which should be used to scan an object.

*NOTE: The objects referred to in the table above can include Host, IPv4Reservation, DHCP range, RPZ or Lease.

Infoblox NIOS configuration

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 go to **"Grid" → "Licenses" → "Grid Wide".**

Add/upload templates

- Navigate to **"Grid" → "Ecosystem" → "Templates"**, and press **"+"** or **"+ Add Template"** then the **"Add template"** window will open.

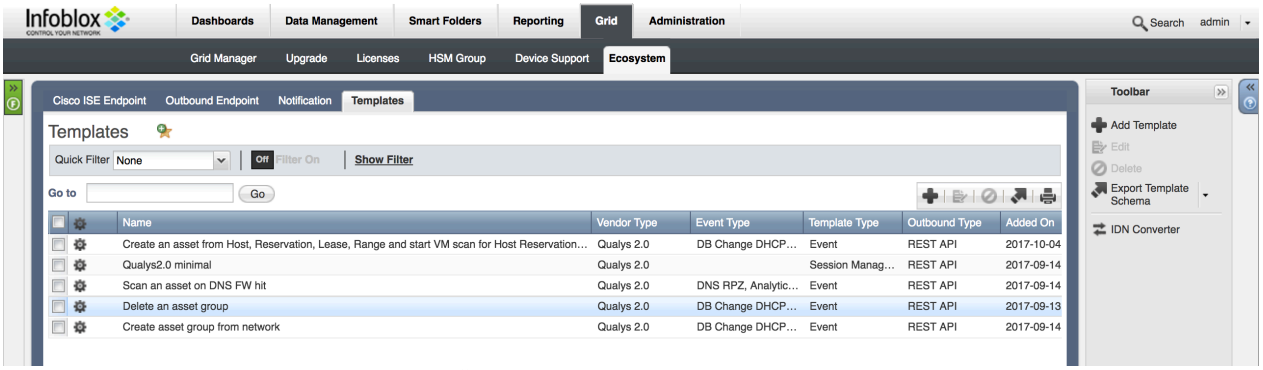
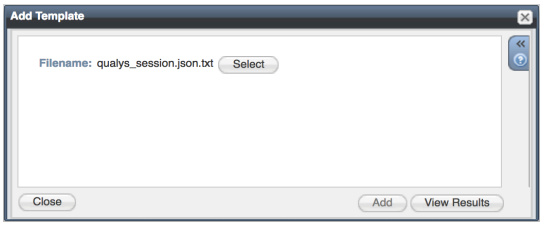
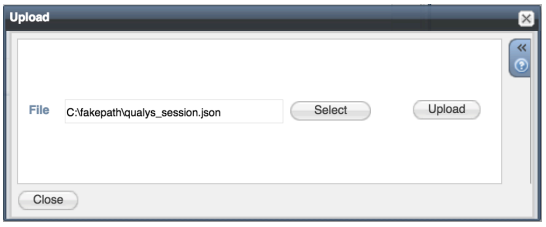
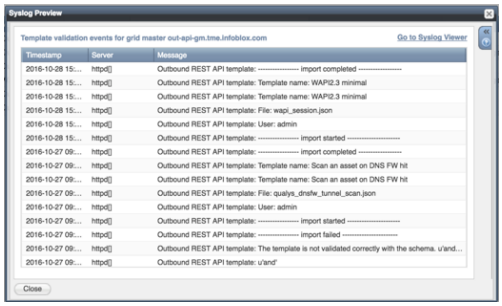


**Image 1: This image is in NIOS 8.2, NIOS 8.1 is slightly different.*

- Press the **"Select"** button on the **"Add template"** window.
- If a template was previously uploaded, press **"Yes"** to overwrite the template.
- Press the **"Select"** button on the **"Upload"** window. The standard file selection dialog will open.
- Select the file and press the **"Upload"** button on the **"Upload"** window.





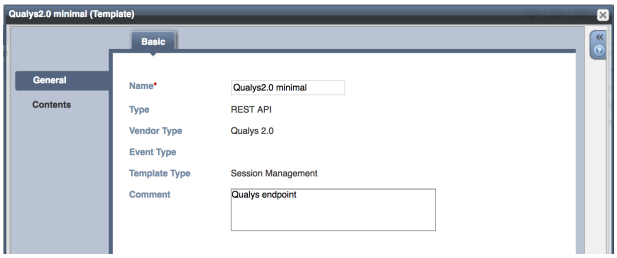


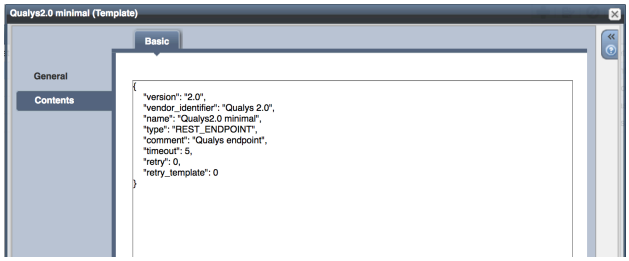
- Press the **"Add"** button and the template will be added/uploaded.
- You can review the uploaded results in the syslog or by pressing the **"View Results"** button.
- There is no difference between uploading session management and action templates.

Modifying Templates

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

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



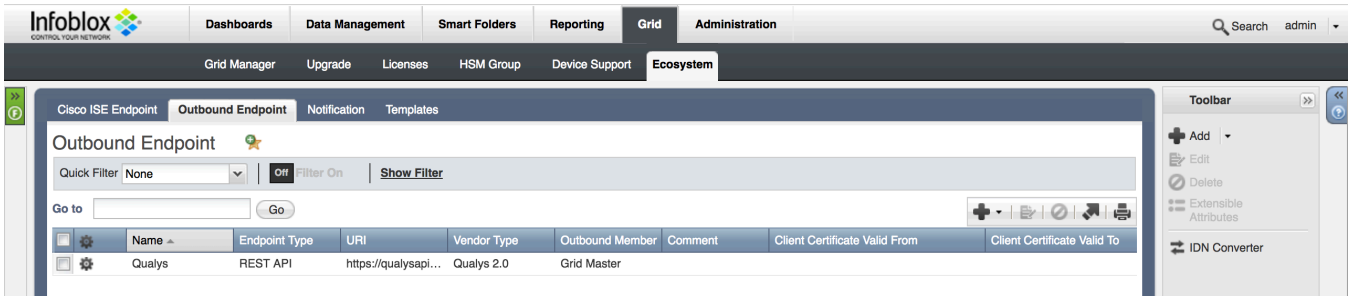


The template editor is a simple interface for making changes to templates. It is recommended to only use the template editor to make minor changes. You can also edit, cut and paste template snippets from the text editor of your choice.

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

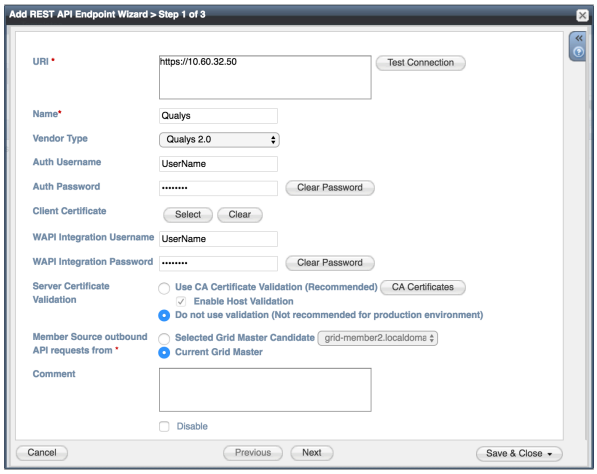
Add a REST API Endpoint

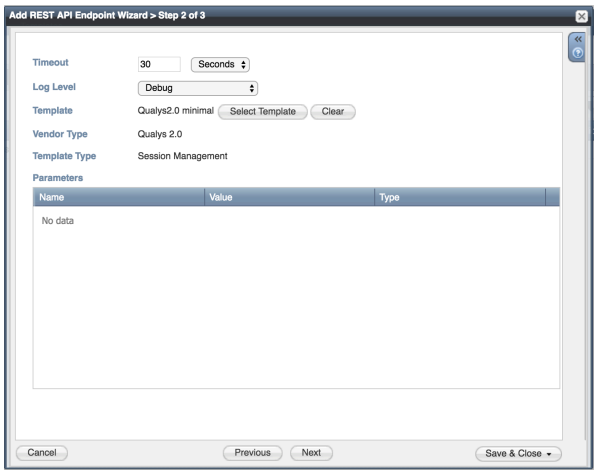
A **"REST API Endpoint"** is basically a remote system which should receive changes based on a notification and a configured template. A Grid, for example, can not only send notifications, it can also receive the notifications from itself (e.g. for testing purposes).



In order to add REST API Endpoints:

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





- The URI and Name fields are required.
- Specify **"Auth Username"**, **"Auth Password"** (Qualys Web Service account credentials), **"WAPI Integration Username"** and **"WAPI Integration Password"** (NIOS credentials).
- (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.

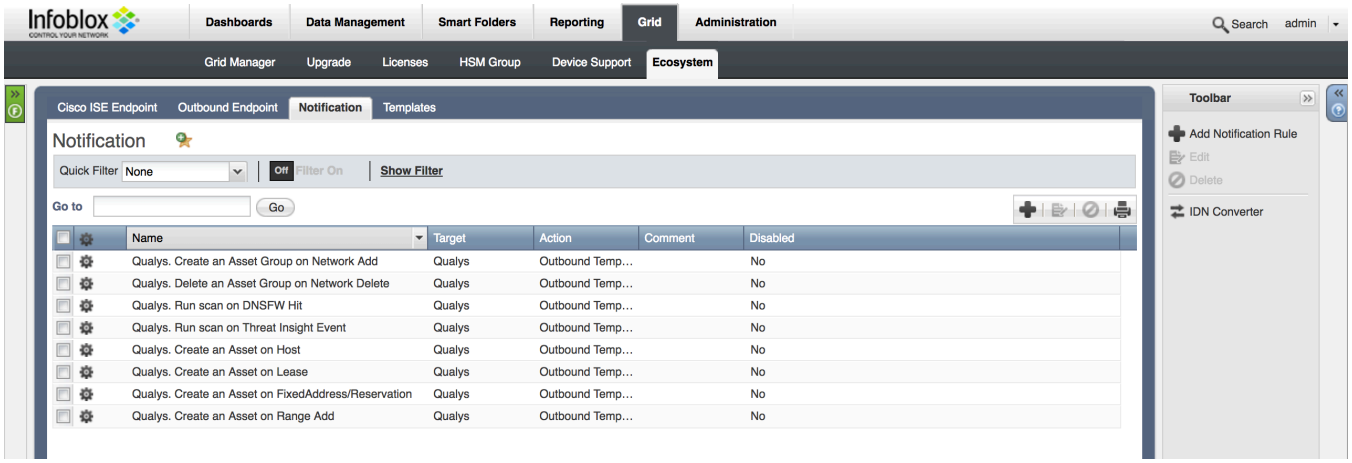
Please be aware that the "Test Connection" option only checks communication (establish TCP connection with a remote system) with the URI. This does not check the authentication/authorization credentials.

Note: "Test Connection" does not check if NIOS can authenticate with the provided credentials

Add a Notification

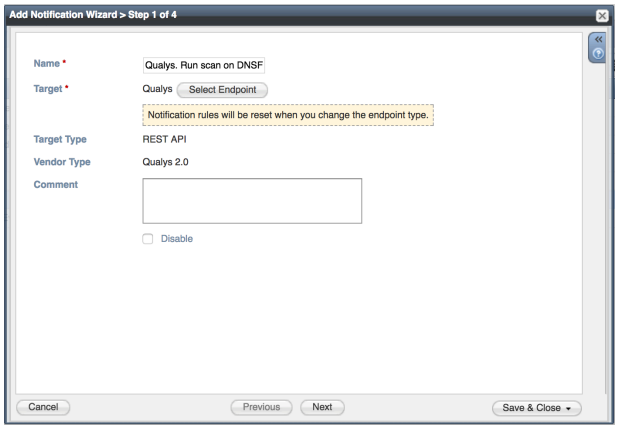
A notification can be considered as a "link" between a template, an endpoint and an event. In the notification properties, you define which event triggers the notification, which template is executed and with which API endpoint NIOS will establish the connection to. The Qualys templates support a subset 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 events and exclude a feed that is automatically populated by Threat Analytics.

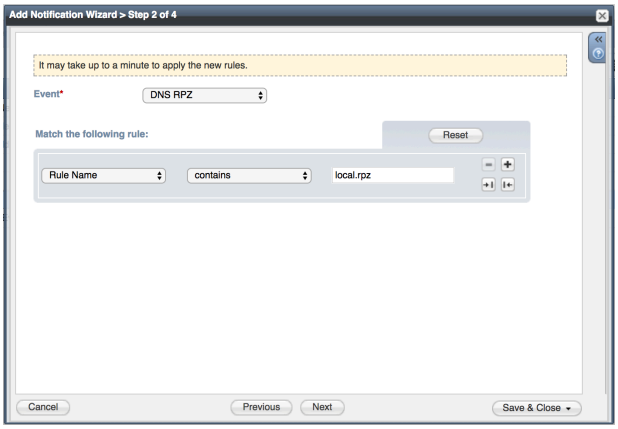
An endpoint and a template must be added before you can add a notification.



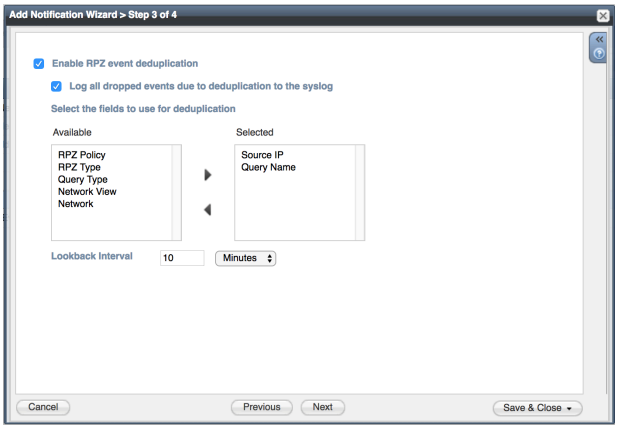
In order to add notifications:

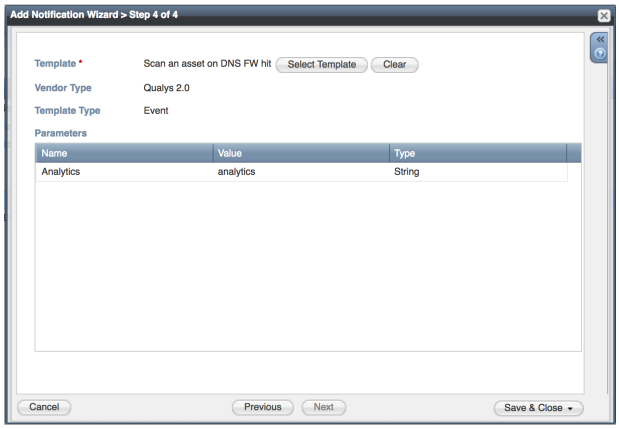
- Navigate to **"Grid" → "Ecosystem" → "Notification"** and press **"+"** or **"+ Add Notification Rule"** then the **"Add Notification Wizard"** window will open.





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

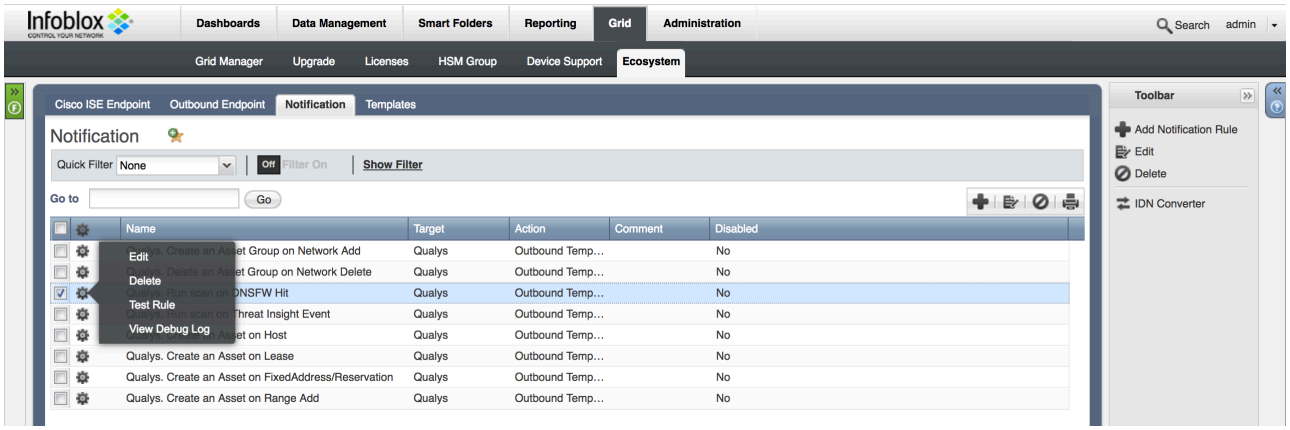




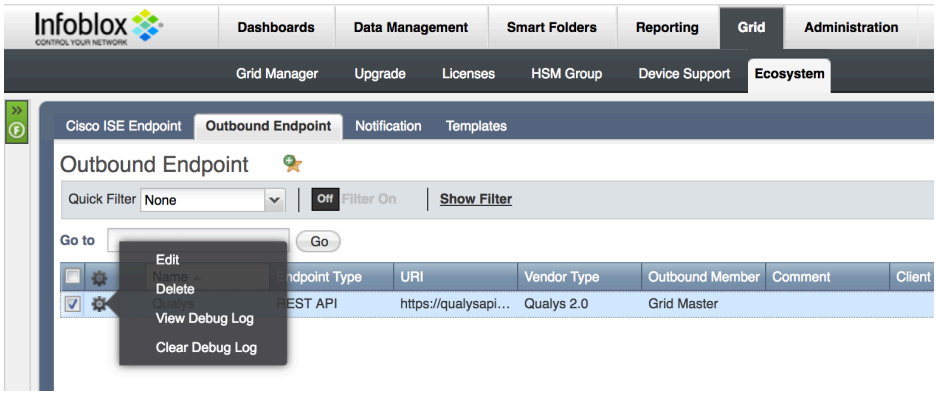
- (For RPZ notifications only) Check **"Enable RPZ event deduplication"** and specify relevant parameters. Click **"Next"**.
- Select a relevant template and specify the template's parameters if any are required. Click **"Save & Close"**.

Check the configuration

You can now emulate an event for which a notification was added (click on a gear icon next to the notification, and select **"Test Rule"**). E.g. create a host record. If you have the debug logging enabled, you can check it for any issues.



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



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