DEPLOYMENT GUIDE

Infoblox Integration with Qualys

Table of Contents

Introduction 2

Prerequisites 2

Known Limitations 3

Best Practices 3

Configuration 4

- Workflow 4
- Before you get started 4
  - Download Templates from the Infoblox Community Website 4
  - Supported Notifications 5
  - Infoblox Permissions 6
- Qualys Configuration 6
  - Add a Qualys user with API Permissions 6
  - Acquire an API Address from your QualysGuard Account 8
- Infoblox NIOS Configuration 10
  - Verify that the Security Ecosystem License is installed 10
  - Add/Upload Templates 11
  - Modifying Templates 13
  - Add a REST API Endpoint 15
  - Add a Notification 18
  - Check the Configuration 21
- Additional Resources 23

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, automate tracking, and create a detailed view of a 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:

- Infoblox
  - NIOS 8.3
  - 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, Threat Protection, and ADP.
  - NIOS API user with the following permissions (access via API only):
    - All Network Views - RW

        - All Host - RW
        - All IPv4 DHCP Fixed Addresses/Reservations - RW
        - All IPv4 Networks - RW
- Qualys
    - Qualys API 2.0 or higher
    - Qualys user account with API permissions:
        - User Role of Manager or Unit Manager
        - Manage Asset Groups
        - Launch maps and scans
        - Launch compliance scans

Known Limitations

The current templates support Object Change Network IPv4, Object Change Fixed Address IPv4, Object Change Host Address IPv4, Object Change Range IPv4, DHCP Leases, RPZ (On-Prem, and from the BloxOne Threat Defense Cloud), Threat Insight (DNS Tunneling), and Advanced DNS protection (ADP). All other event types are not currently supported. Please note that the extensible attribute Qualys_Assets_Group does not support blank text or any other prohibited URL characters. This is a limitation from how asset groups are added via the Qualys API. Additionally, the deletion of self assigned asset groups (i.e. Asset-Group-For-Network-172.0.0.0/24) for Networks is the only form of deletion that is supported by the templates.

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. 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”). 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 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.

Configuration

Workflow

Qualys:

1. Add a Qualys user with API Permissions
2. Acquire an API Address from your QualysGuard Account.

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, DHCP, RPZ, Threat Analytics, and Threat Protection.
3. Create the required Extensible Attributes.
4. Download (or create your own) notification templates (Qualys Assets.json, Qualys Security.json, Qualys 2.0 Minimal.json) from the Infoblox community website.
5. Add the templates to NIOS.
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 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. Templates for the Qualys 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 details should be provided with a template. Don't forget to apply any changes required by the template before testing a notification.

Table 1. Extensible Attributes

Extensible Attributes	Description
Qualys_Asset_PC	True or False. Defines if an asset should be created in the Qualys Policy Compliance Module.
Qualys_Asset_VM	True or False. Defines if an asset should be created in the Qualys Vulnerability Management Module.
Qualys_Assets_Group	Defines which Qualys Asset Group the network object belongs to. If the group does not exist it will be automatically generated by Infoblox.
Qualys_LastScanTime	Defines the last time an asset was scanned by Qualys.
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 to be used.
Qualys_Scanner	Defined Qualys scanner appliance to be used.
Qualys_SyncTime	Internal attribute. Provides the time when an object was synced with Qualys
Qualys_User_SNMP	SNMP credentials to be used to scan an object.
Qualys_User_Unix	Unix Credentials used to scan an object.

Supported Notifications

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 Qualys templates support a subset of available notifications (refer to the limitations portion in this guide for more details). 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.

Table 3. Supported Notifications

Notification	Description
DNS RPZ	DNS queries that are malicious or unwanted
DNS Tunneling	Data exfiltration that occurs on the network
DHCP Lease	Lease events that occur on the network
Object Change Fixed Address IPv4	Add a fixed, or reserved IPv4 object
Object Change Host Address IPv4	Add a host IPv4 object
Object Change Network IPv4	Add, or delete a IPv4 Network
Security ADP	Advanced DNS Protection events

Infoblox Permissions

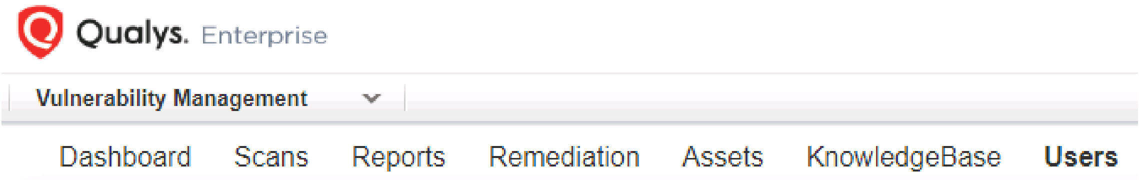
The Infoblox and Qualys integration require a few permissions for the integration to work. Navigate to Administration → Administrators and add Roles, Permissions, Groups and Admins to include permissions that are required for the integration. When creating a new group, under the Groups tab, select the API interface under the Allowed Interfaces category. For more information on how to manage permissions, please refer to the NIOS Admin Guide.

Qualys Configuration

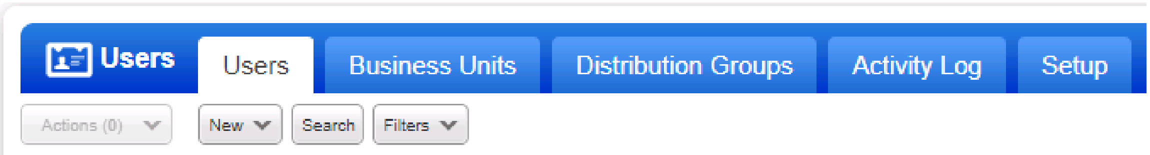
Add a Qualys user with API Permissions

The Infoblox and Qualys integration requires a Qualys user that has API permissions. Perform the following steps to create an API user:

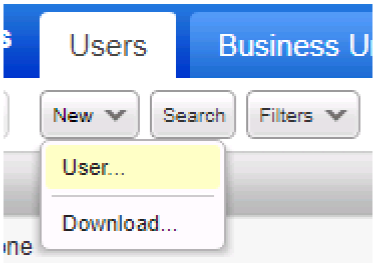
1. On the QualysGuard website, click **Users** on the navigation bar.



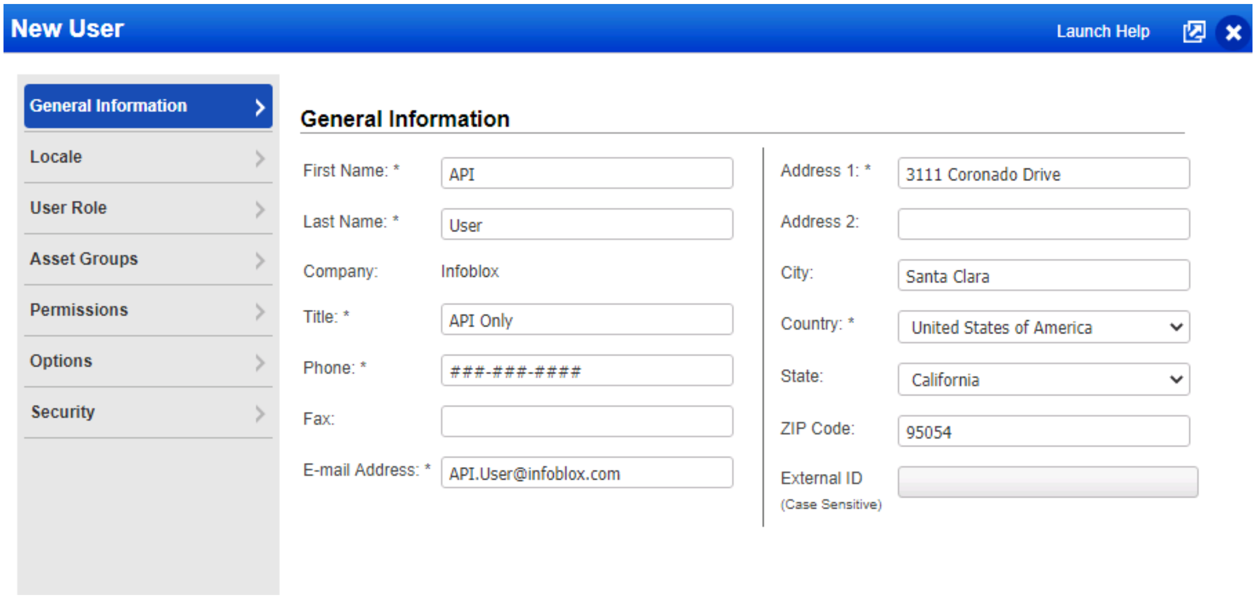
2. In the Users page, click the **Users** tab located near the top left of the page.



3. Below the Users Tab click **New**. Then, click **User…** in the list that is revealed.



4. Input all required information for the API User. Once all text boxes with an asterisk have been filled out, click **User Role** in the left navigation bar. Note, ensure that you or an associate has access to the E-mail Address entered to create required credentials that will be used later.



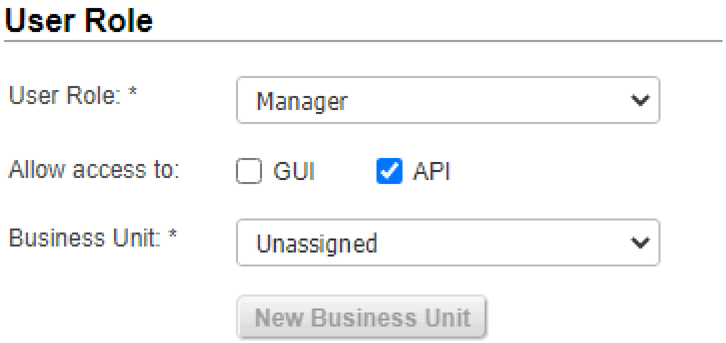
General Information

First Name: *	API	Address 1: *	3111 Coronado Drive
Last Name: *	User	Address 2:	
Company:	Infoblox	City:	Santa Clara
Title: *	API Only	Country: *	United States of America
Phone: *	###-###-####	State:	California
Fax:		ZIP Code:	95054
E-mail Address: *	API.User@infoblox.com	External ID (Case Sensitive)	

5. Select the desired **User Role** for the API user, and click the **checkbox** associated with API.

   ○ Note for the full use of the integration it is suggested to select the user role Manager for the API user.

   ○ Optionally, you may use the User Role Scanner, or Unit Manager however this will require manual assignment of permissions to any Qualys Asset Group you would like Infoblox to add IPs to. Additionally, you will need to manually add IPs each time a new Asset Group is created via the Infoblox API. The asset group will be created by the user, but IPs cannot be assigned at the time of Asset Group creation due to permission limitations. For more information access the Qualys documentation located here: User Roles and Permissions for VM/VMDR, PC, SCA



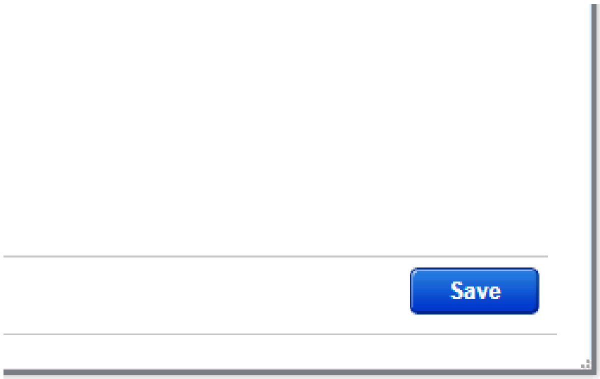
User Role

User Role: * Manager

Allow access to: □ GUI ☑ API

Business Unit: * Unassigned

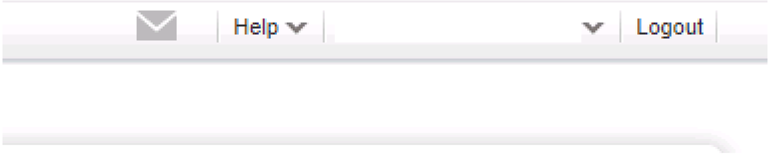
6. Once you are done configuring the new user, click **Save** on the bottom right of the window.



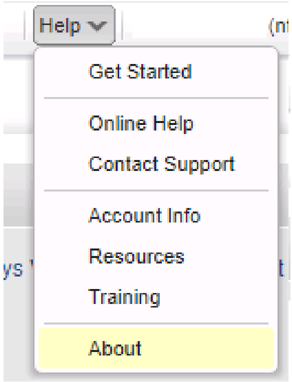
Acquire an API Address from your QualysGuard Account

In order for Infoblox to send API calls to Qualys, you must acquire the correct FQDN from your QualysGuard Account.

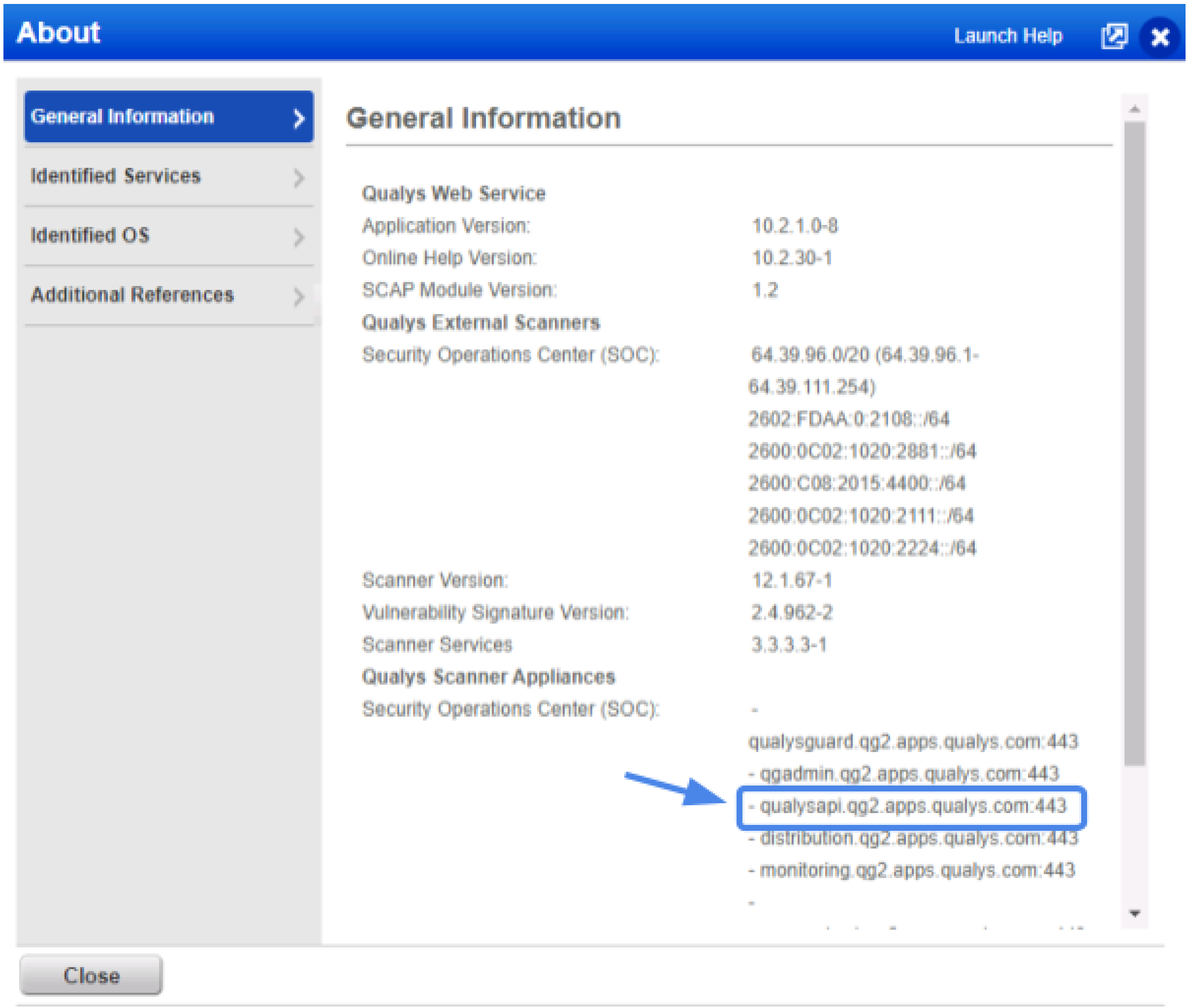
1. On the QualysGuard website click the **Help** dropdown button.



2. In the dropdown menu that is revealed, click **About**.



3. In the About window that is revealed, locate the Qualys API address located in the General Information panel. Save this address for use later in the deployment. In the screenshot qualysapi.qg2.apps.qualys.com:443 is the correct address, the correct address will always start with qualysapi. *Note: The address you see may be different than what is represented in the screenshot.*



General Information

Qualys Web Service

Application Version:	10.2.1.0-8
Online Help Version:	10.2.30-1
SCAP Module Version:	1.2

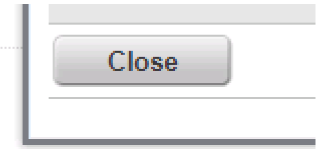
Qualys External Scanners

Security Operations Center (SOC):	64.39.96.0/20 (64.39.96.1-64.39.111.254) 2602:FDAA:0:2108::/64 2600:0C02:1020:2881::/64 2600:C08:2015:4400::/64 2600:0C02:1020:2111::/64 2600:0C02:1020:2224::/64
Scanner Version:	12.1.67-1
Vulnerability Signature Version:	2.4.962-2
Scanner Services	3.3.3.3-1

Qualys Scanner Appliances

Security Operations Center (SOC):	- qualysguard.qg2.apps.qualys.com:443 - qgadmin.qg2.apps.qualys.com:443 - qualysapi.qg2.apps.qualys.com:443 - distribution.qg2.apps.qualys.com:443 - monitoring.qg2.apps.qualys.com:443 -

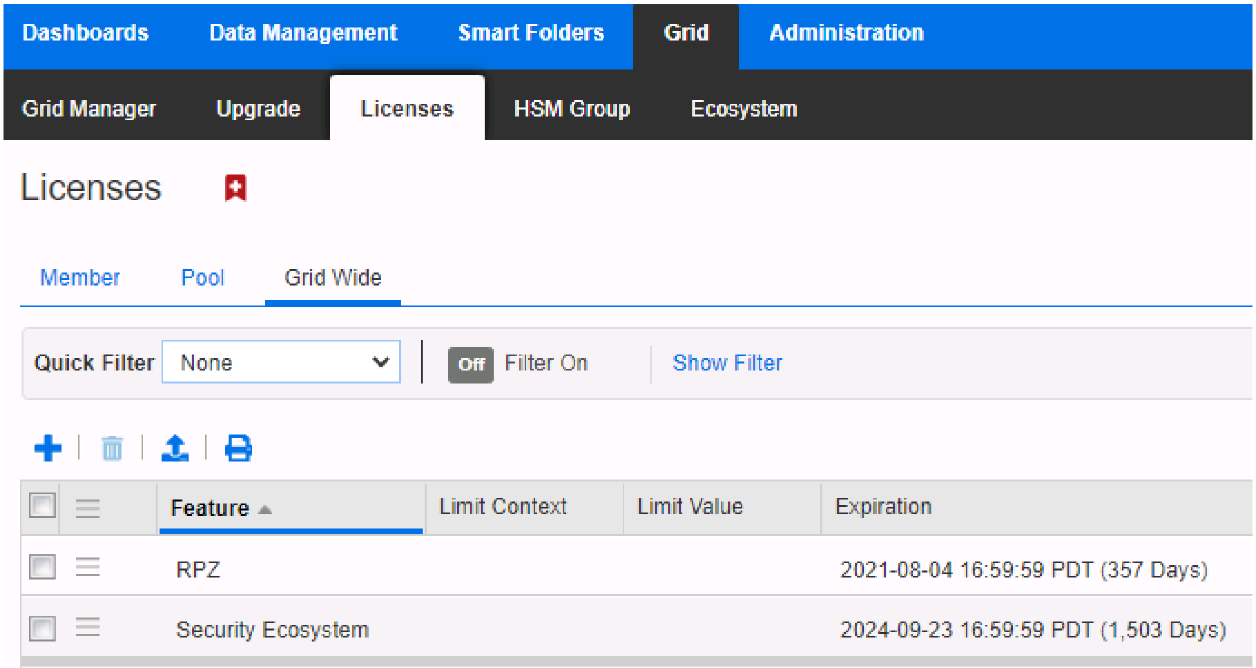
4. When you are done viewing the About window, click **Close** located near the bottom left of the window.



Infoblox NIOS Configuration

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 the Grid Master you intend to integrate with Qualys. Then, navigate to Grid → Licenses → Grid Wide. Verify that the license exists, and that it has not expired.

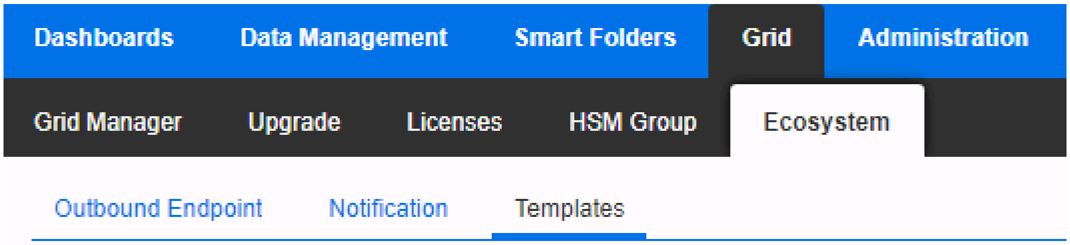


Feature	Limit Context	Limit Value	Expiration
RPZ			2021-08-04 16:59:59 PDT (357 Days)
Security Ecosystem			2024-09-23 16:59:59 PDT (1,503 Days)

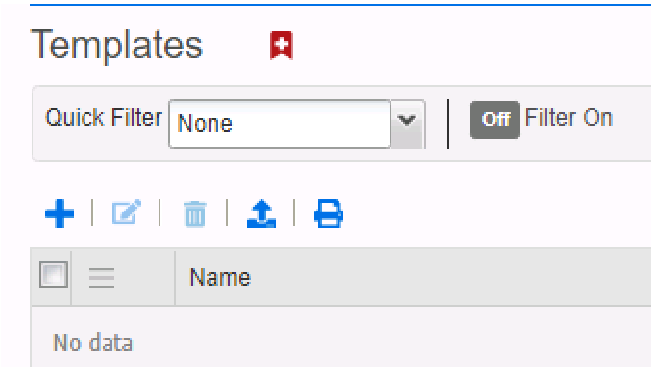
Add/Upload Templates

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

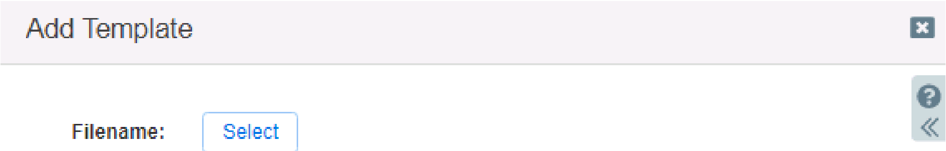
1. Navigate to **Grid** → **Ecosystem** → **Templates**.



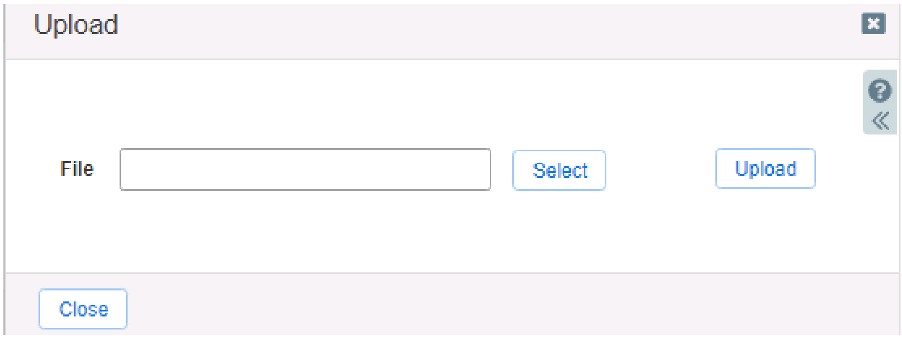
2. Press the **+** icon located above the table of Templates.



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

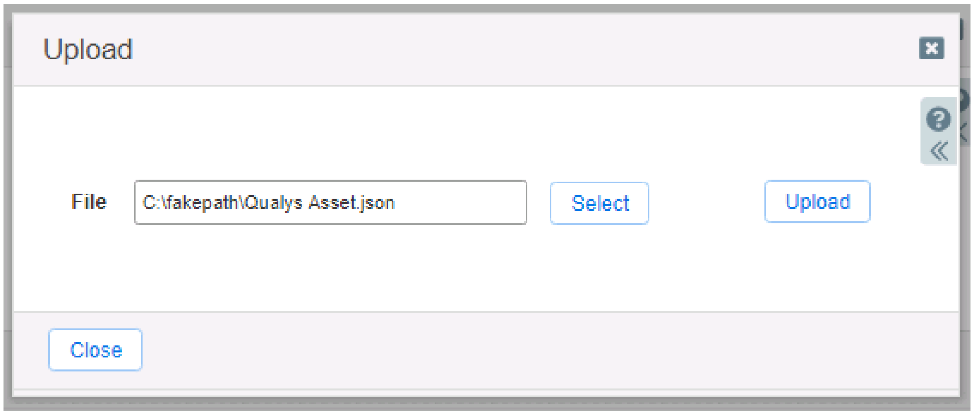


4. Click the **Select** button in the Upload dialog box that is revealed.

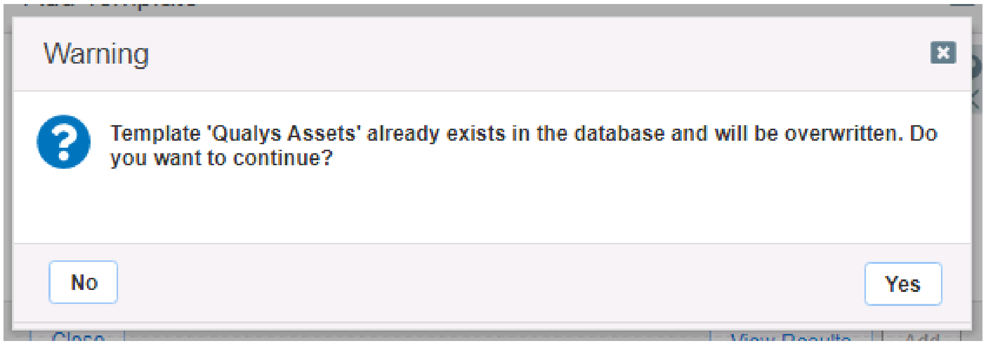


5. Locate and select the Template you would like to upload. Or, input the full path of the file in the File text box.

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

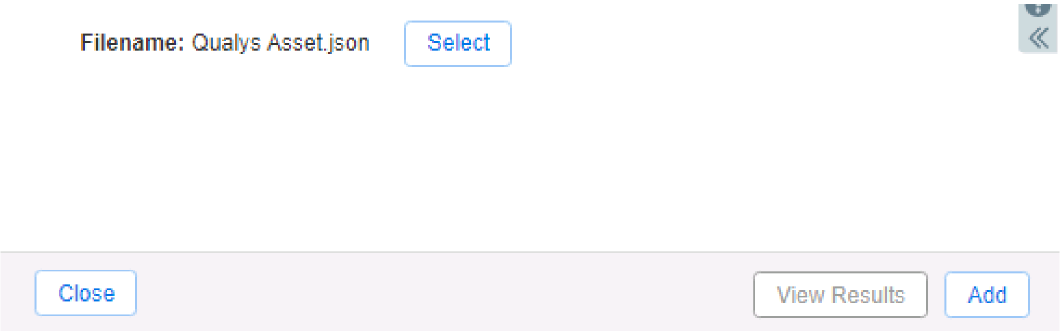


7. If a template was previously uploaded, press **Yes** to overwrite the template.

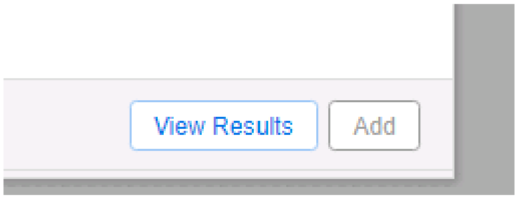

Warning

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.



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



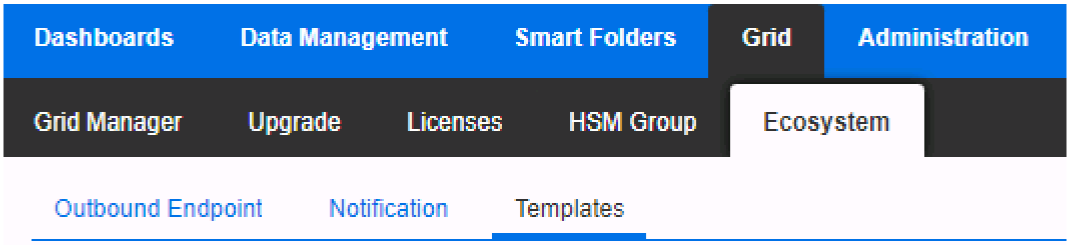
10. Repeat steps 2-8 for any other templates you intend to upload.

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

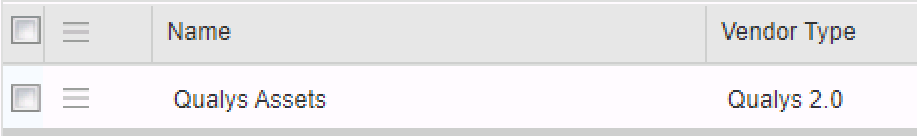
Modifying Templates

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**.



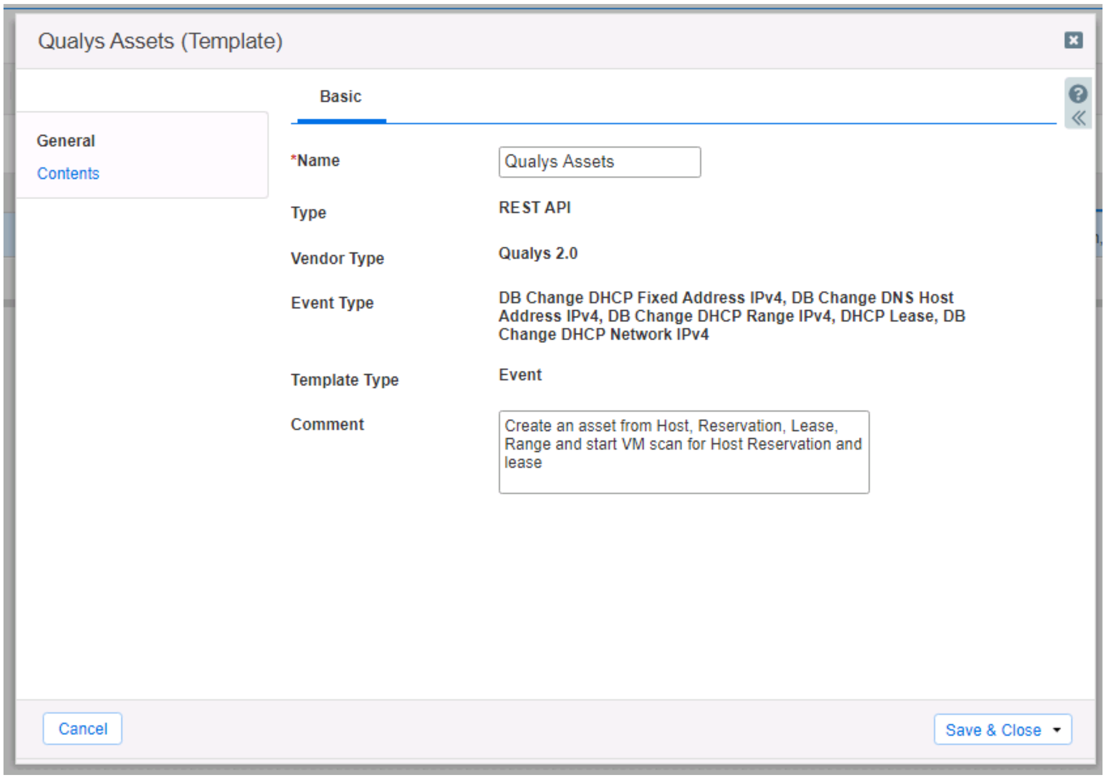
2. Click the ≡ hamburger icon associated with the Template you would like to modify.



□	≡	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



Qualys Assets (Template)

*Name: Qualys Assets

Type: REST API

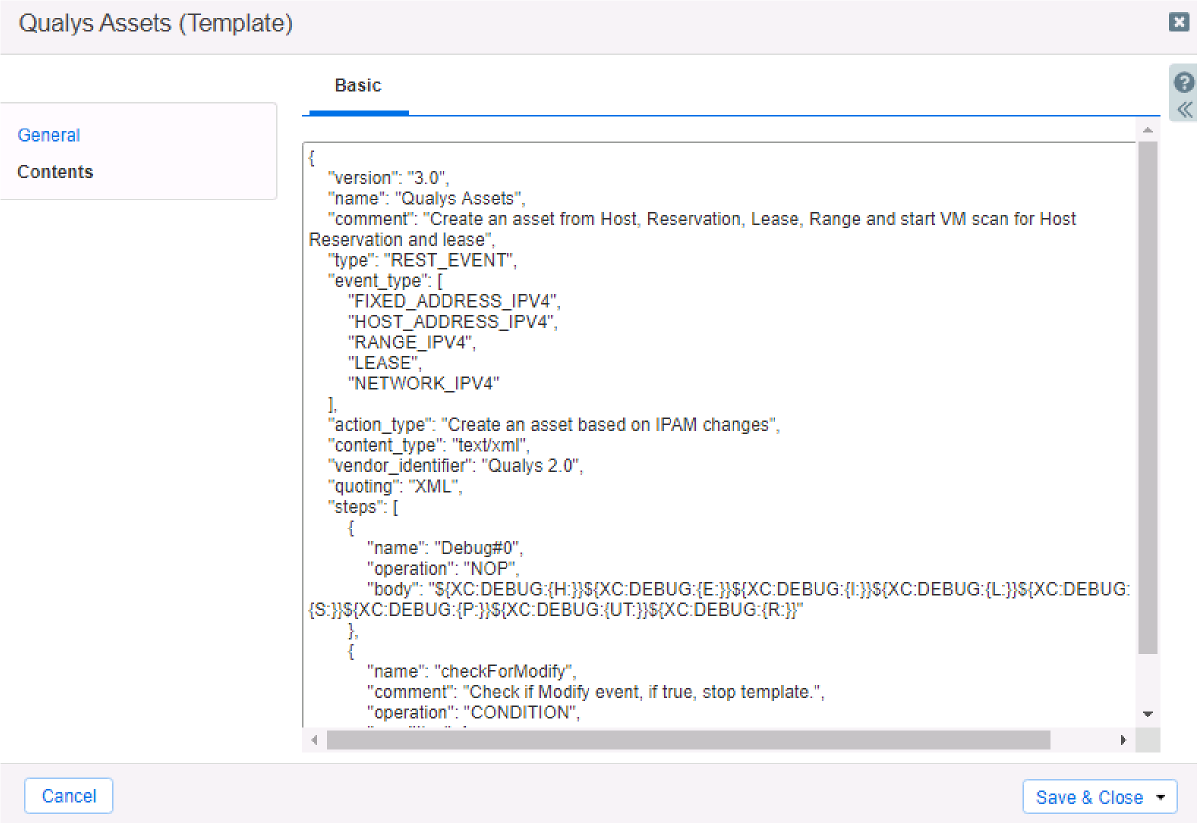
Vendor Type: Qualys 2.0

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**.



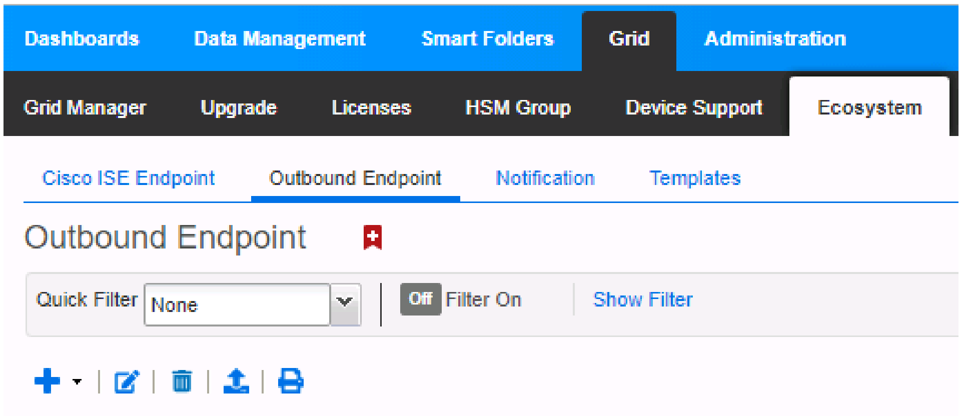
```
{
    "version": "3.0",
    "name": "Qualys Assets",
    "comment": "Create an asset from Host, Reservation, Lease, Range and start VM scan for Host
Reservation and lease",
    "type": "REST_EVENT",
    "event_type": [
        "FIXED_ADDRESS_IPV4",
        "HOST_ADDRESS_IPV4",
        "RANGE_IPV4",
        "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 it is used by an Outbound endpoint or a notification.

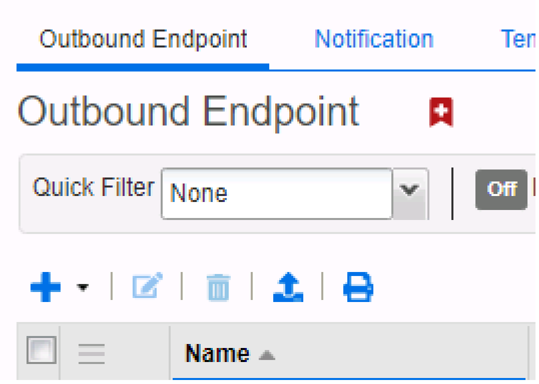
Add a REST API Endpoint

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**.

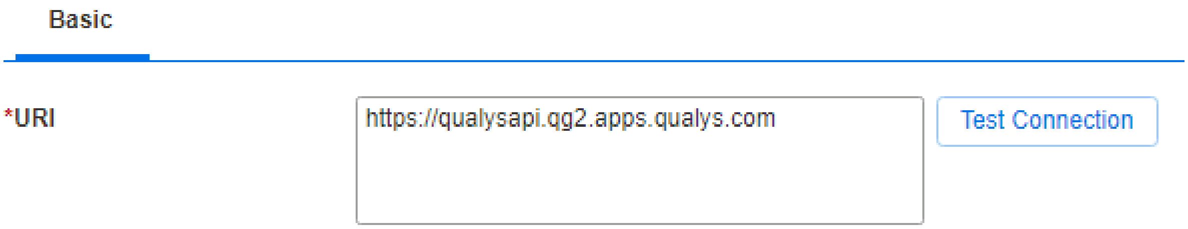


2. Click the **+** icon located above the list of Outbound Endpoints.



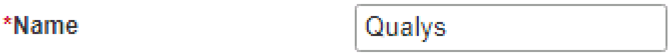
3. An Add REST API Endpoint Wizard will be revealed. Input the following Information:

   - **URI**, the URI is the API address associated with your Qualysguard account. Information on how to acquire this address is on page 8.



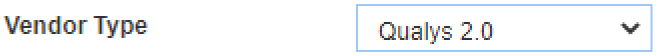
*URI https://qualysapi.qg2.apps.qualys.com

   - **Name**, Input a name for the Endpoint.



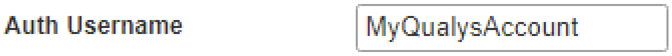
*Name Qualys

   - **Vendor Type**, Select Qualys 2.0 from the drop-down menu



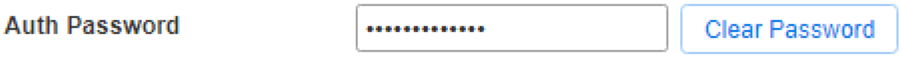
Vendor Type: Qualys 2.0

- **Auth Username** is the user account used to access the Qualys API.



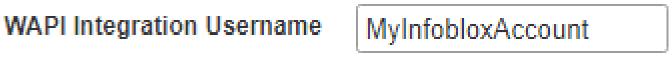
Auth Username: MyQualysAccount

- **Auth Password** is the API User's password used to access Qualys.



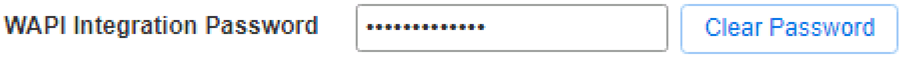
Auth Password: •••••••••••••

- **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.



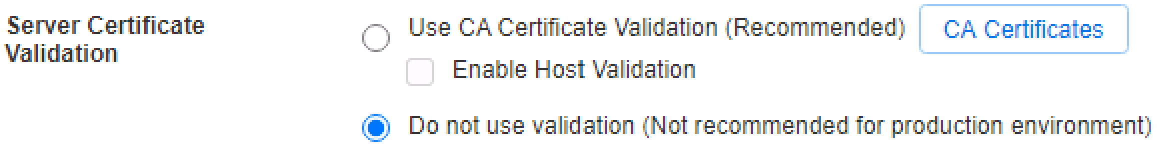
WAPI Integration Password: •••••••••••••

- (Optional) **Client Certificate** is used to assist with encrypting traffic between NIOS and Qualys. If you wish to encrypt the data input your Certificates here.

Client Certificate

Select
Clear

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



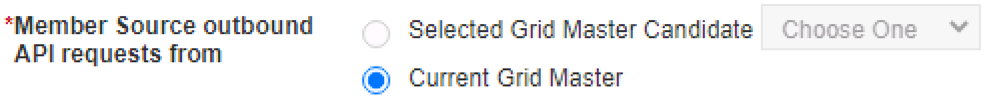
Server Certificate Validation

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

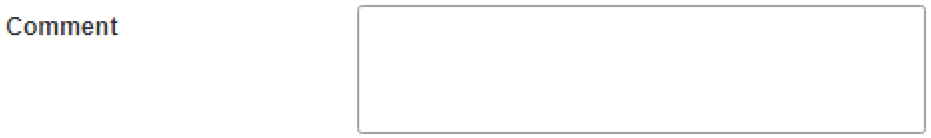


*Member Source outbound API requests from

○ Selected Grid Master Candidate

● Current Grid Master

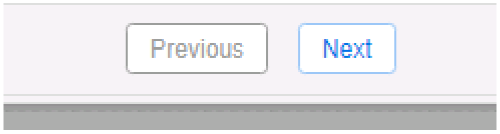
- (Optional) **Comment**. If desired you may input a comment for the Rest API Endpoint.



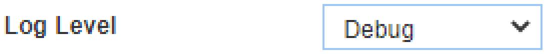
- (Optional) **Disable**. If desired you can disable the Rest API Endpoint by using this checkbox.

□ Disable

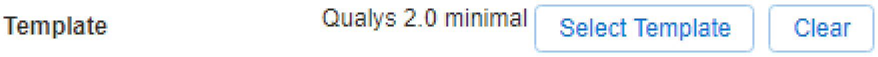
4. Click **Next** located at the bottom of the Add REST API Endpoint Wizard.



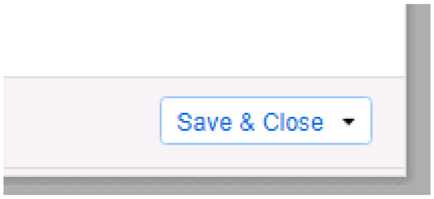
5. (Optional) Change the Log Level to Debug to view more information about the communication between Infoblox and Qualys during testing.


Log Level: Debug

6. On Step 2 of 3 of the Add REST API Endpoint Wizard, click the Select Template button to select a Session template for Qualys.


Template: Qualys 2.0 minimal

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

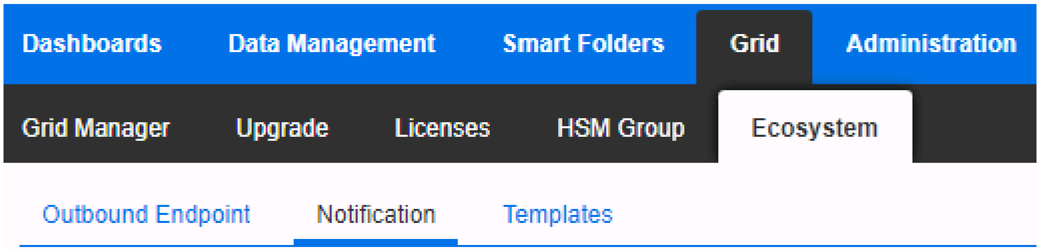


Add a Notification

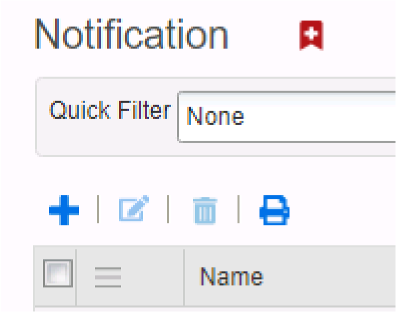
An endpoint and a template must be added before you can add a notification.

In order to add notifications follow the following steps:

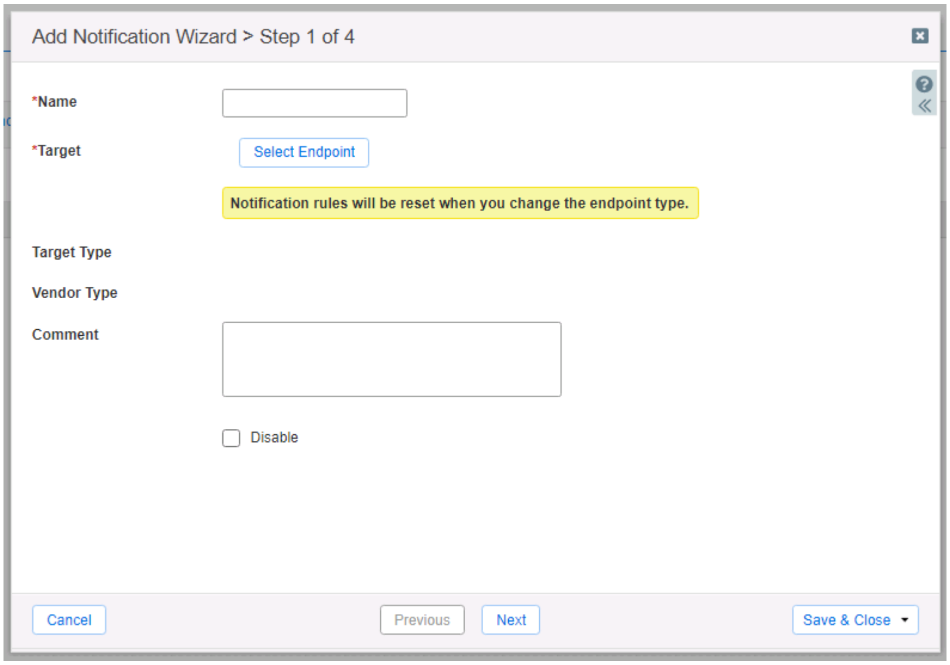
1. Navigate to **Grid** → **Ecosystem** → **Notification**.



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



3. An Add Notification Wizard will be revealed.


Add Notification Wizard > Step 1 of 4

*Name

*Target Select Endpoint

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

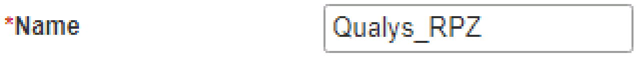
Target Type

Vendor Type

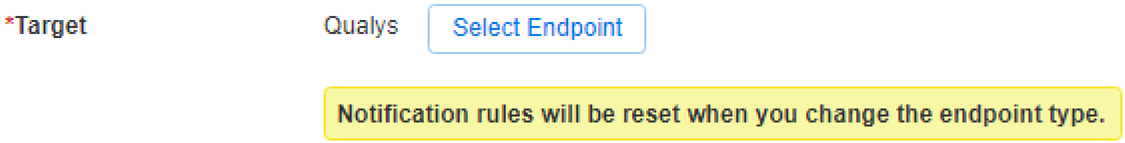
Comment

□ Disable

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


*Name Qualys_RPZ

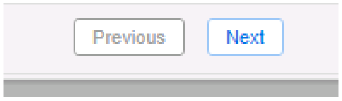
- Select a **Target endpoint** by clicking the **Select Endpoint** button.



*Target Qualys

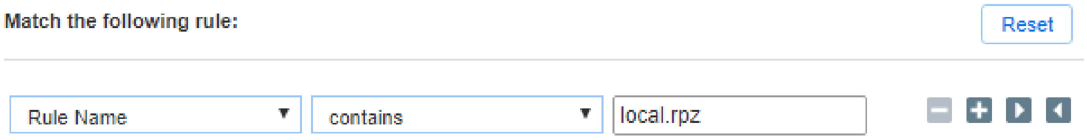
Notification rules will be reset when you change the endpoint type.

4. Click **Next**.



5. Select the relevant Event for the Notification by clicking on the **Event** dropdown. For a list of all supported Events view table 3 on page 5.

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

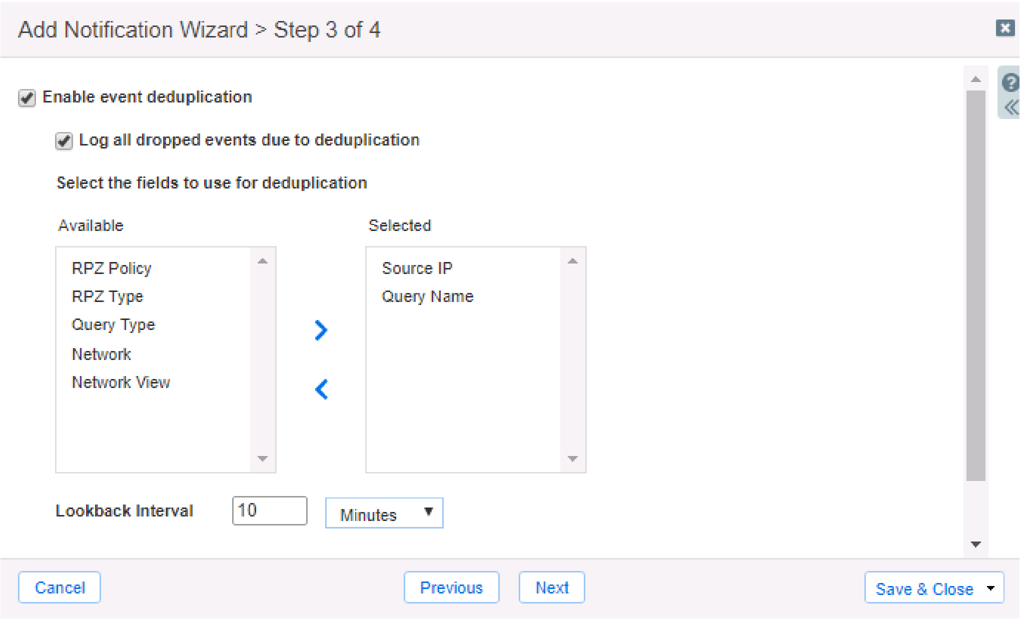


Match the following rule:

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

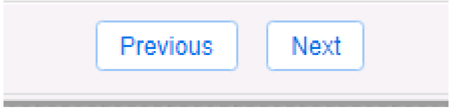
☑ Log all dropped events due to deduplication

Select the fields to use for deduplication

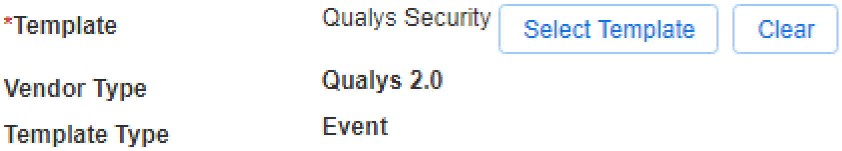
Available	Selected
RPZ Policy	Source IP
RPZ Type	Query Name
Query Type	
Network	
Network View	

Lookback Interval: 10 Minutes

9. Click **Next**.

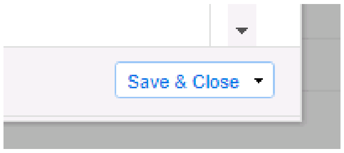


10. Click **Select Template** to select the relevant template.



*Template	Qualys Security
Vendor Type	Qualys 2.0
Template Type	Event

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



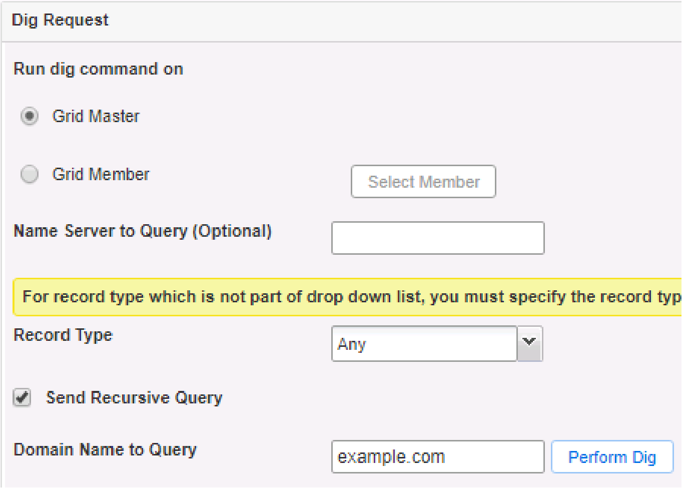
12. Create any other Notifications for other events as desired. All supported events for notifications are listed on Page 5.

Check the Configuration

You can emulate an RPZ event to test the 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 blocked by the RPZ list that was included in the notification that was created earlier. Then, click the **Perform Dig** button.



Dig Request

Run dig command on

● Grid Master

○ Grid Member — Select Member

Name Server to Query (Optional)

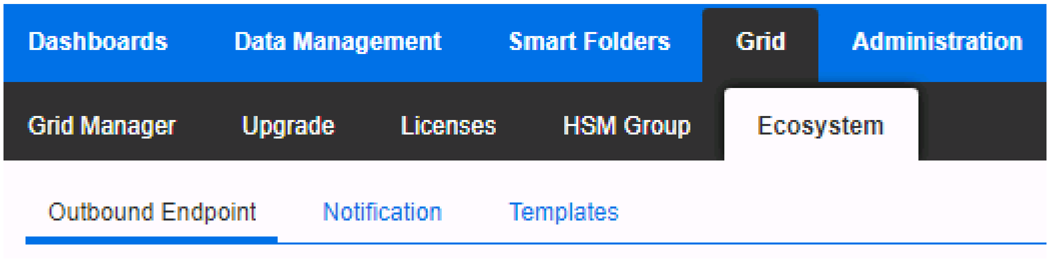
For record type which is not part of drop down list, you must specify the record typ

Record Type: Any

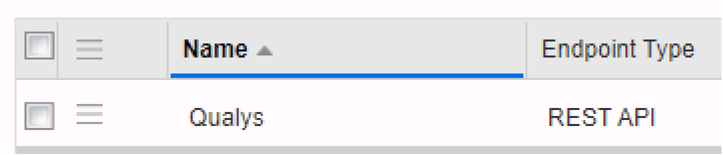
☑ Send Recursive Query

Domain Name to Query: example.com — Perform Dig

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

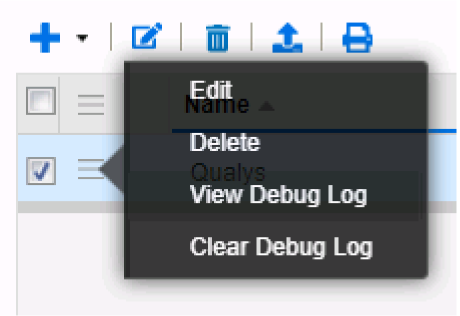


4. Click the ☰ hamburger icon associated with the Qualys REST API Endpoint.

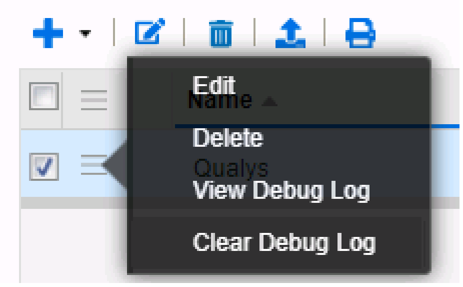


□	☰	Name ▲	Endpoint Type
□	☰	Qualys	REST API

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.

Additional Resources

For more information regarding Infoblox or Qualys, access these websites:

1. Infoblox Documentation Portal
2. Infoblox Website
3. Infoblox Community
4. Qualys API (VM, PC) User Guide
5. User Roles and Permissions for VM/VMDR, PC, SCA
6. Qualys Website

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