Infoblox®
CONTROL YOUR NETWORK

DEPLOYMENT GUIDE

Integration with Tenable Security Center

Outbound API

Contents

Introduction

Infoblox Outbound REST API integration framework is a new way to update both, IPAM data (networks, hosts, leases) and DNS threat data, into additional ecosystem solutions. Infoblox and Tenable Security Center (Tenable SC) together enable security and incident response teams to leverage the integration of vulnerability scanners, IPAM and DNS security to enhance visibility, manage assets, ease compliance and automate remediation. Thus, improving your security posture while maximizing your ROI in both products.

Prerequisites

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

- Infoblox:
    1. NIOS 8.2 or higher
    2. Security Ecosystem License
    3. Outbound API integration templates
    4. Prerequisites for the templates (e.g. configured and set extensible attributes)
- Tenable Security Center:
    1. "Static IP List" and "DNS Name List" assets
    2. "Active Scan" which will be used as a scan template

Limitations

Known limitations:

- IPv6 networks and addresses can be added to Tenable SC by the assets. However, Tenable SC does not support direct scanning of IPv6 addresses.
- The provided templates do not support assets removal.

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”).

Please refer to the Infoblox NIOS Administrator’s Guide for other best practices, limitations and detailed information for developing notification templates. The NIOS Administrator’s Guide can be found through the Help panel in the Infoblox Grid Manager GUI, or on the Infoblox Support portal (https://support.infoblox.com).

Configuration

Workflow

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

- Tenable Security Center:
    - Create "Static IP List" and "DNS Name List" assets.
    - Create "Active Scan".
- Infoblox:
    - Install the Security Ecosystem license if not already installed.
    - Check that the DHCP, DNS, RPZ and Threat Analytics services are properly configured and enabled.
    - Create the required Extensible Attributes (refer to the list provided below).

    - Download (or create your own) notification templates (TenableSession.json, TenableLogin.json, TenableLogout.json, TenableAsset.json, TenableScan.json) from Infoblox community web-site.
    - Add/upload the notification templates.
    - Add an Outbound Endpoint "Tenable SC".
    - Add Notifications.
- Emulate an event, check Outbound debug log and/or verify changes on Tenable SC side.

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 developing templates can be found in the NIOS Administrator guide.

Templates are not included in NIOS releases (out-of-box). These are available on the Infoblox community web-site. Templates for integration with Tenable Security Center are in the Tenable group (https://community.infoblox.com/t5/Tenable/gp-p/TENABLE). Other templates are posted in the “API & Integration” forum (https://community.infoblox.com/t5/API-Integration/bd-p/API_Integration).

Templates may require additional extensible attributes to be created, and parameters or WAPI credentials to be defined. The required configuration should be provided with a template. Remember to apply changes, required by the template, before testing a notification.

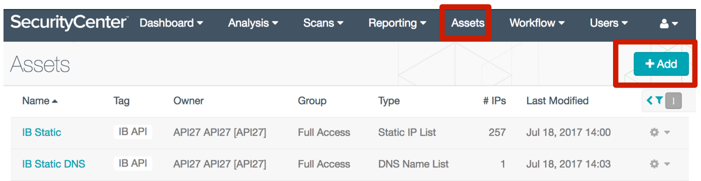
Tenable Security Center configuration

At least one static IP list, one DNS Name list and one active scan must be configured in Tenable Security Center. Existing assets and scans can be reused.

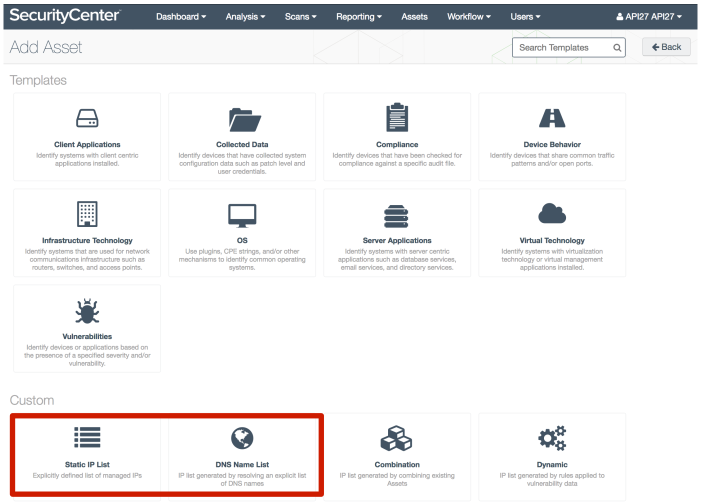
Assets creation

To create an asset:

1. On the "**Assets**" page, click the "**+Add**" button.
2. Select an appropriate template ("Static IP List" or "DNS Name List").
3. Specify "*Name*" and either "*IP*" or "*DNS Names*" (depending on the template) fields. The initial IP-address and/or DNS Name can be fake.
4. Click "**Submit**" to save the new asset.



Name	Tag	Owner	Group	Type	# IPs	Last Modified
IB Static	IB API	API27 API27 [API27]	Full Access	Static IP List	257	Jul 18, 2017 14:00
IB Static DNS	IB API	API27 API27 [API27]	Full Access	DNS Name List	1	Jul 18, 2017 14:03



Client Applications
Identify systems with client centric applications installed.

Collected Data
Identify devices that have collected system configuration data such as patch level and user credentials.

Compliance
Identify devices that have been checked for compliance against a specific audit file.

Device Behavior
Identify devices that share common traffic patterns and/or open ports.

Infrastructure Technology
Identify systems that are used for network communications infrastructure such as routers, switches, and access points.

OS
Use plugins, CPE strings, and/or other mechanisms to identify common operating systems.

Server Applications
Identify systems with server centric applications such as database services, email services, and directory services.

Virtual Technology
Identify systems with virtualization technology or virtual management applications installed.

Vulnerabilities
Identify devices or applications based on the presence of a specified severity and/or vulnerability.

Static IP List
Explicitly defined list of managed IPs

DNS Name List
IP list generated by resolving an explicit list of DNS names

Combination
IP list generated by combining existing Assets

Dynamic
IP list generated by rules applied to vulnerability data

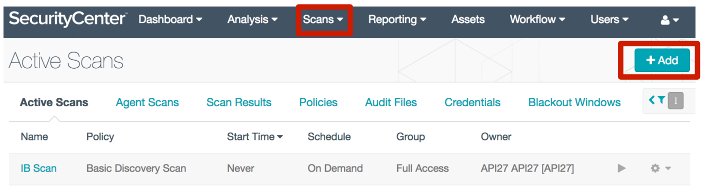
Active Scan creation

To create an active scan:

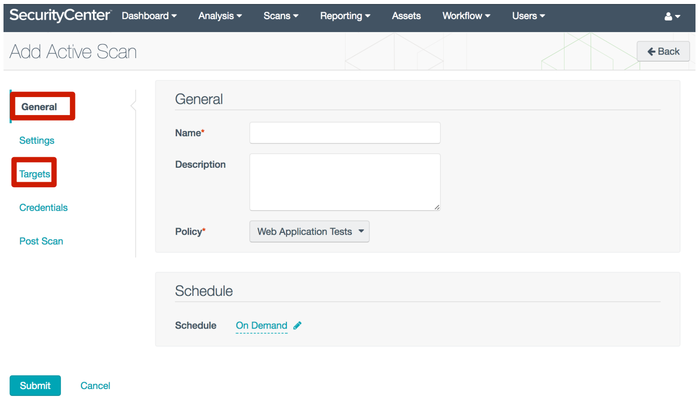
1. In the "**Scans**" drop-down menu select the "**Active Scans**" option.
2. Click on the "**+Add**" button.
3. On the "**General**" tab, set the "*Name*" and "*Policy*" fields.
4. Schedule must be configured "On Demand".
5. On the "Targets" tab, select "Target Type" as "**IP/DNS Name**" and specify any IP or domain

Note: during template execution, this object will be replaced

6. Specify other parameters as required.
7. Click on the "**Submit**" button to save the new Active Scan policy



Name	Policy	Start Time	Schedule	Group	Owner
IB Scan	Basic Discovery Scan	Never	On Demand	Full Access	API27 API27 [API27]



Name*

Description

Policy* Web Application Tests

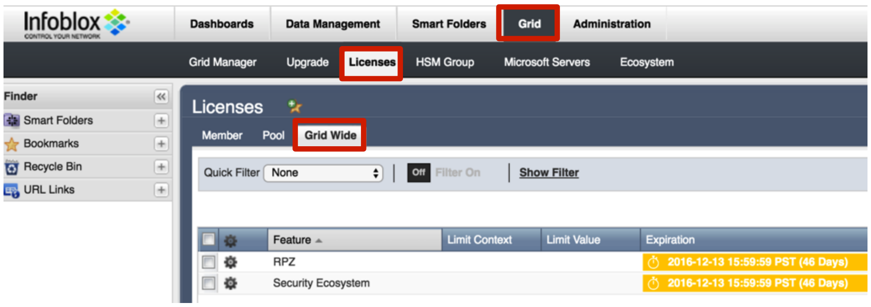
Schedule On Demand

Infoblox NIOS configuration

Check if the Security Ecosystem license is installed

The **Security Ecosystem** license is a Grid Wide license. Grid wide licenses activate services on all compatible appliances within the same Grid.

To check if the license was installed, navigate to **Grid** → **Licenses** → **Grid Wide**.



Quick Filter None | Off Filter On

Feature	Limit Context	Limit Value	Expiration
RPZ			2016-12-13 15:59:59 PST (46 Days)
Security Ecosystem			2016-12-13 15:59:59 PST (46 Days)

Create Extensible Attributes

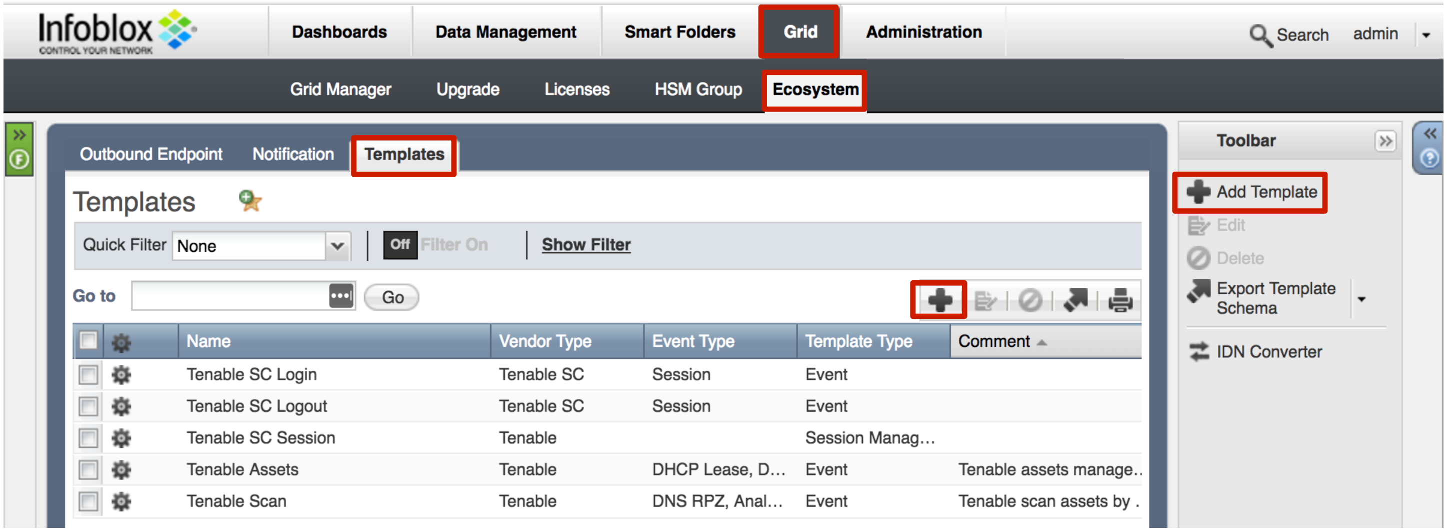
Tenable SC Outbound API notification templates use several Extensible Attributes to adjust the templates behavior. You can download and use the provided php-script, or create them manually. These extensible attributes are described in the table below.

Extensible Attribute	Description
TNBL_Sync	Defines if an object should be synced with Tenable SC. Possible values: true, false
TNBL_SyncTime	Contains date/time when the object was synchronized, updated by the assets management template
TNBL_AddNet	Defines if a network should be added to assets. Possible values: true, false. If TNBL_AddNet is false but TNBL_Sync is true, TNBL_AssetIPID and TNBL_AssetHostID will be updated.
TNBL_AddRange	Defines if a range should be added to assets. Possible values: true, false. If TNBL_AddNet is false but TNBL_Sync is true, TNBL_AssetIPID and TNBL_AssetHostID will be updated.
TNBL_ScanOnEvnt	Defines if an asset should be scanned if RPZ or DNS Tunneling events were triggered
TNBL_ScanOnAdd	Defines if an asset should be scanned immediately after creation
TNBL_ScanTemplate	Defines a Tenable SC active scan which should be used for scans initiated by Infoblox. List of possible values should match active scan names on Tenable SC.
TNBL_ScanTemplateID	Internal attribute, which is used to store an active scan id.
TNBL_AssetIP	Defines a Static IP List name. List of possible values should match names of static IP lists on Tenable SC.
TNBL_AssetIPID	Internal attribute, which is used to store a static IP list id.
TNBL_AssetHost	Defines a Static DNS Names List name. List of possible values should match names of static DNS Names lists on Tenable SC.
TNBL_AssetHostID	Internal attribute, which is used to store a static DNS Name list id.
TNBL_ScanTime	Contains a date when an asset was scanned last time by a request from Infoblox
TNBL_AddByHostname	Defines if a host should be synced with Tenable SC using a hostname. Possible values: true, false

Add/upload templates

To add/upload templates:

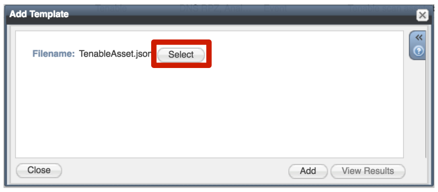
1. Navigate to **Grid → Ecosystem → Templates**, and press “**+**” or “**+ Add Template**”. The “**Add template**” window will open.



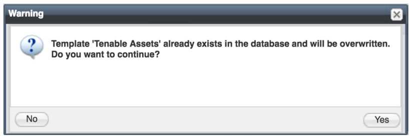
Templates

Name	Vendor Type	Event Type	Template Type	Comment
Tenable SC Login	Tenable SC	Session	Event	
Tenable SC Logout	Tenable SC	Session	Event	
Tenable SC Session	Tenable		Session Manag…	
Tenable Assets	Tenable	DHCP Lease, D…	Event	Tenable assets manage..
Tenable Scan	Tenable	DNS RPZ, Anal…	Event	Tenable scan assets by .

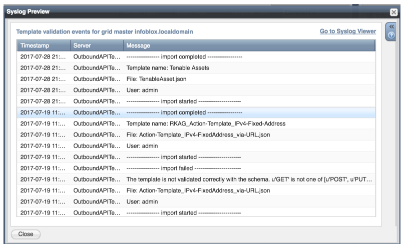
2. Press the “**Select**” button on the “**Add template**” window.
3. If the template was previously uploaded, press "**Yes**" to overwrite the template.
4. Press the “**Select**” button on the “**Upload**” window.
5. The standard file selection dialog will be opened. Select the file and press the “**Upload**” button.



Filename: TenableAsset.json



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



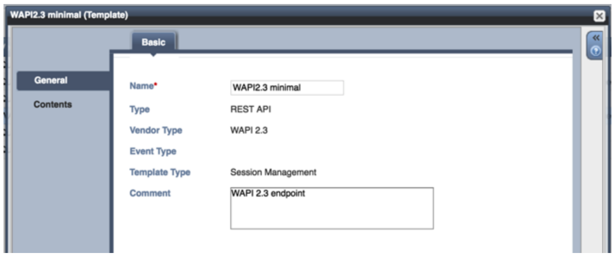
Template validation events for grid master infoblox.localdomain

Timestamp	Server	Message
2017-07-28 21:...	OutboundAPITe...	---------------- import completed -----------------
2017-07-28 21:...	OutboundAPITe...	Template name: Tenable Assets
2017-07-28 21:...	OutboundAPITe...	File: TenableAsset.json
2017-07-28 21:...	OutboundAPITe...	User: admin
2017-07-28 21:...	OutboundAPITe...	---------------- import started --------------------
2017-07-19 11:...	OutboundAPITe...	---------------- import completed -----------------
2017-07-19 11:...	OutboundAPITe...	Template name: RKAG_Action-Template_IPv4-Fixed-Address
2017-07-19 11:...	OutboundAPITe...	File: Action-Template_IPv4-FixedAddress_via-URL.json
2017-07-19 11:...	OutboundAPITe...	User: admin
2017-07-19 11:...	OutboundAPITe...	---------------- import started --------------------
2017-07-19 11:...	OutboundAPITe...	---------------- import failed ----------------------
2017-07-19 11:...	OutboundAPITe...	The template is not validated correctly with the schema. u'GET' is not one of [u'POST', u'PUT...
2017-07-19 11:...	OutboundAPITe...	File: Action-Template_IPv4-FixedAddress_via-URL.json
2017-07-19 11:...	OutboundAPITe...	User: admin
2017-07-19 11:...	OutboundAPITe...	---------------- import started --------------------

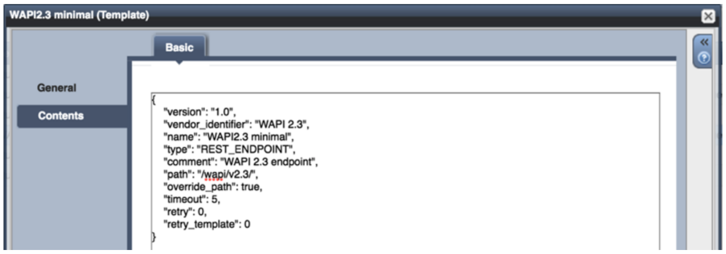
6. Press the “**Add**” button and the template will be added/uploaded.
7. You can review the uploaded results in the syslog or by pressing the “**View Results**” button.
8. There is no difference between uploading session management and action templates.

Modifying Templates

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



Name* WAPI2.3 minimal
Type REST API
Vendor Type WAPI 2.3
Event Type
Template Type Session Management
Comment WAPI 2.3 endpoint



```
{
 "version": "1.0",
 "vendor_identifier": "WAPI 2.3",
 "name": "WAPI2.3 minimal",
 "type": "REST_ENDPOINT",
 "comment": "WAPI 2.3 endpoint",
 "path": "/wapi/v2.3/",
 "override_path": true,
 "timeout": 5,
 "retry": 0,
 "retry_template": 0
}
```

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

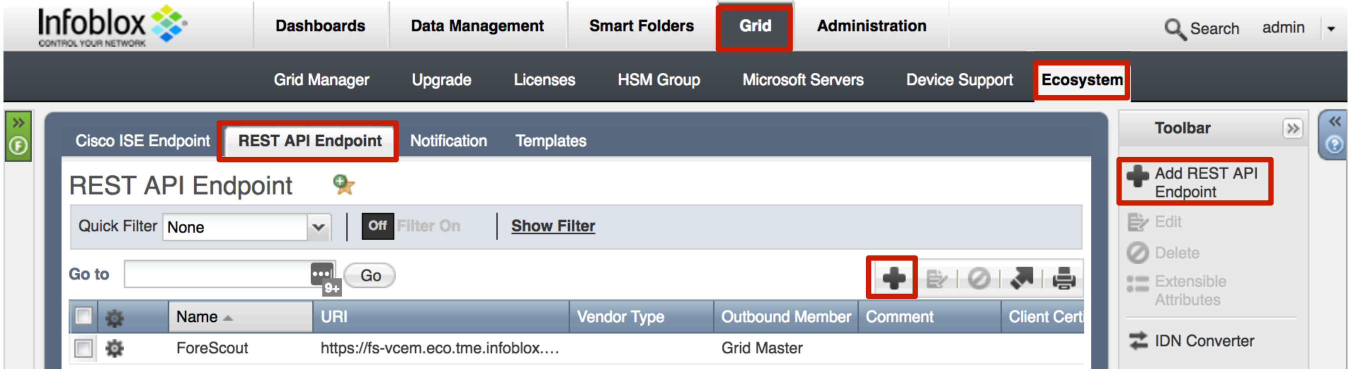
Note: You cannot delete a template if it is used by an endpoint or by a notification.

Add an Outbound Endpoint

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

To add an Outbound Endpoint:

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

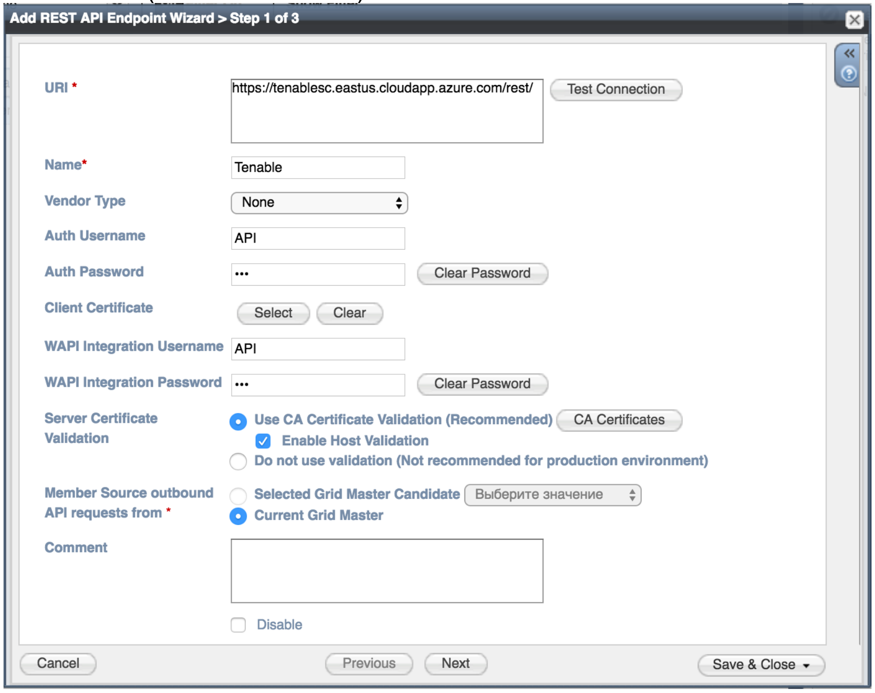


REST API Endpoint

Quick Filter: None

Name	URI	Vendor Type	Outbound Member	Comment	Client Cert
ForeScout	https://fs-vcem.eco.tme.infoblox.…		Grid Master		

2. The URI and Name fields are required.
3. Specify "***Auth Username***", "***Auth Password***", "***WAPI Integration Username***" and "***WAPI Integration Password***" (NIOS credentials). Click on the "**Next**" button.



Add REST API Endpoint Wizard > Step 1 of 3

URI *	https://tenablesc.eastus.cloudapp.azure.com/rest/
Name*	Tenable
Vendor Type	None
Auth Username	API
Auth Password	•••
Client Certificate	
WAPI Integration Username	API
WAPI Integration Password	•••
Server Certificate Validation	● Use CA Certificate Validation (Recommended) ☑ Enable Host Validation ○ Do not use validation (Not recommended for production environment)
Member Source outbound API requests from *	○ Selected Grid Master Candidate Выберите значение ● Current Grid Master
Comment	
	□ Disable

4. Specify "**Template**" (Session management template must be uploaded). **For debug purposes only** set "Log Level" to "**Debug**". Click on the "**Save & Close**" button.

It is recommended to send notifications from a Grid Master Candidate, if there is one available, instead of Grid Master.

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

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

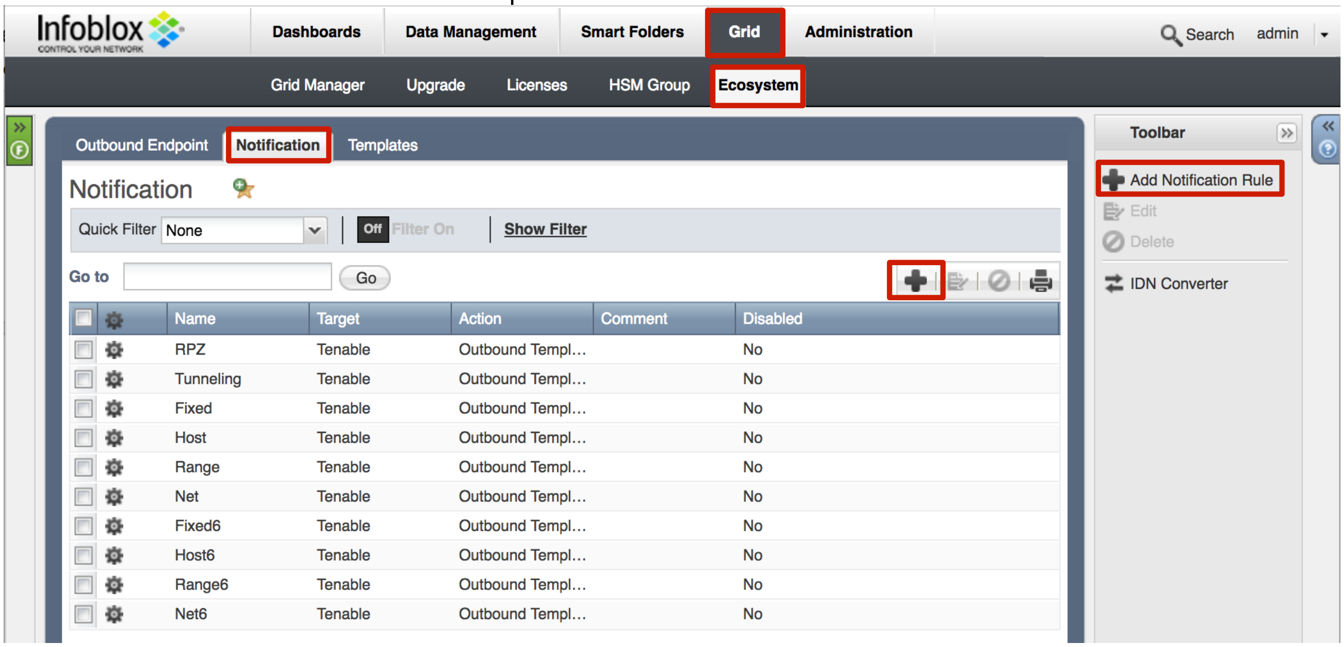
Add a Notification

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 the NIOS will establish its connection. To simplify the deployment, only create the required notifications and use relevant filters. It is highly recommended to configure deduplication for RPZ events and exclude RPZ feeds that are automatically populated by Threat Analytics.

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

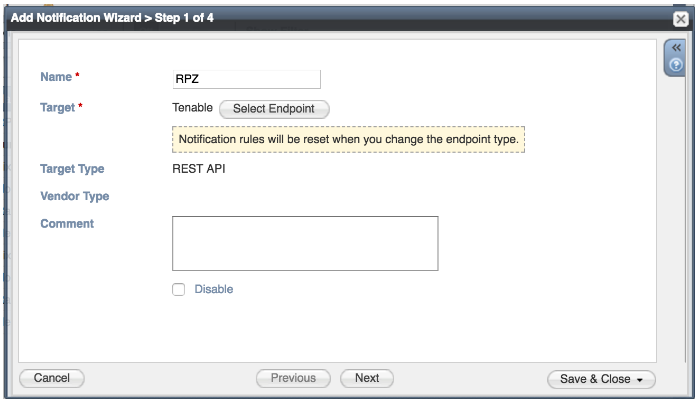
To add notifications:

1. Navigate to **Grid** → **Ecosystem** → **Notification** and press “**+**” or “**+ Add Notification Rule**”. The “**Add Notification Wizard**” window will open.



Name	Target	Action	Comment	Disabled
RPZ	Tenable	Outbound Templ...		No
Tunneling	Tenable	Outbound Templ...		No
Fixed	Tenable	Outbound Templ...		No
Host	Tenable	Outbound Templ...		No
Range	Tenable	Outbound Templ...		No
Net	Tenable	Outbound Templ...		No
Fixed6	Tenable	Outbound Templ...		No
Host6	Tenable	Outbound Templ...		No
Range6	Tenable	Outbound Templ...		No
Net6	Tenable	Outbound Templ...		No

2. Specify the notification’s name and select an endpoint (Target). Click "**Next**".
3. Select an event type and define a filter. From the performance perspective, it is best practice to make the filter as narrow as possible. Click "**Next**".



Add Notification Wizard > Step 1 of 4

Name * RPZ

Target * Tenable

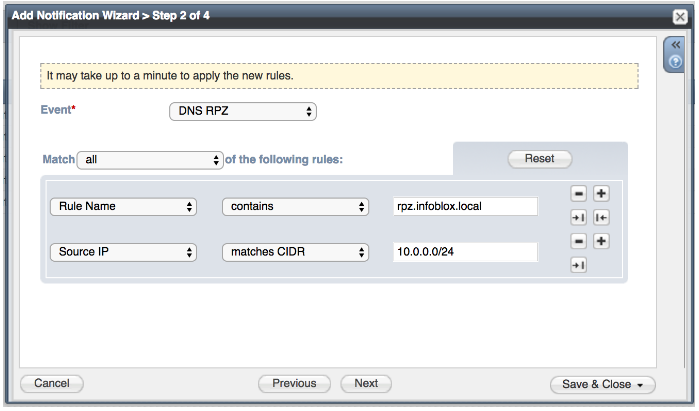
Notification rules will be reset when you change the endpoint type.

Target Type REST API

Vendor Type

Comment

□ Disable



Add Notification Wizard > Step 2 of 4

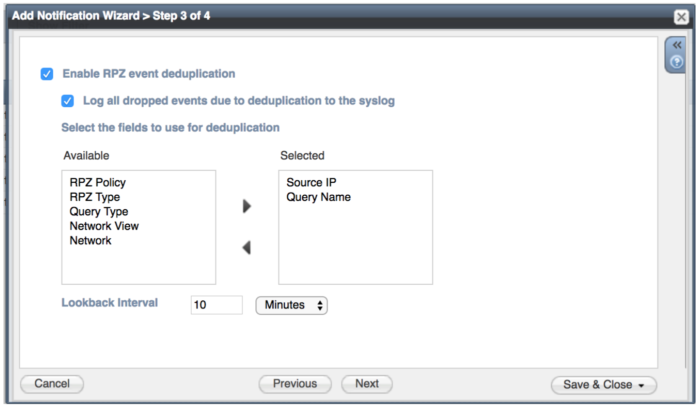
It may take up to a minute to apply the new rules.

Event* DNS RPZ

Match all of the following rules:

Rule Name	contains	rpz.infoblox.local
Source IP	matches CIDR	10.0.0.0/24

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



Add Notification Wizard > Step 3 of 4

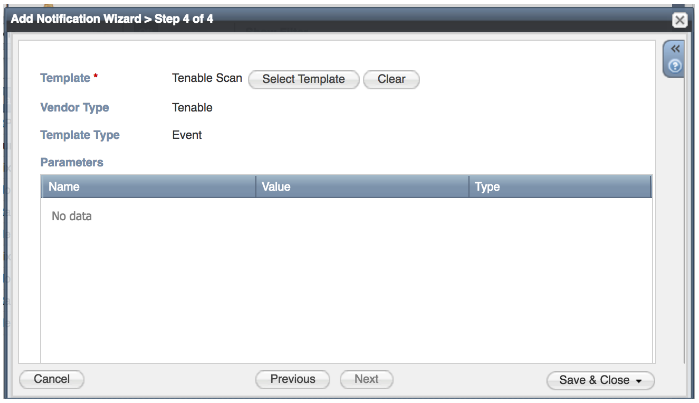
☑ Enable RPZ event deduplication

☑ Log all dropped events due to deduplication to the syslog

Select the fields to use for deduplication

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

Lookback Interval: 10 Minutes



Add Notification Wizard > Step 4 of 4

Template *: Tenable Scan

Vendor Type: Tenable

Template Type: Event

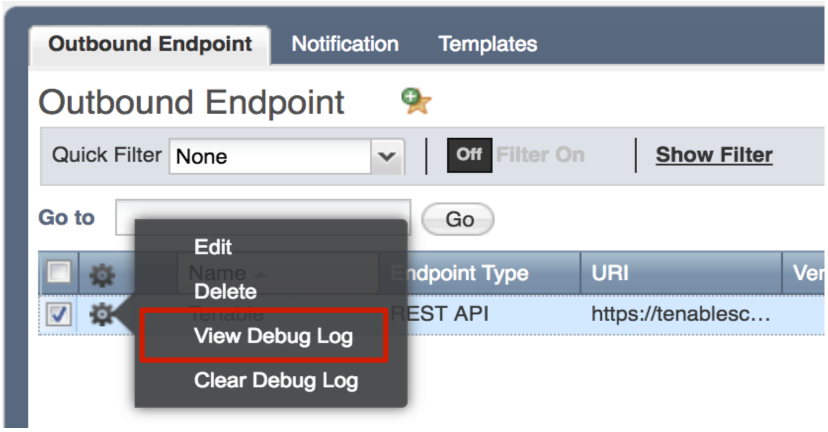
Parameters

Name	Value	Type
No data		

Check the configuration

You can emulate an event from where a notification was added by clicking on the gear icon next to the notification, and selecting "Test Rule". For example, create a host record, or add a DHCP lease. If you have the debug log 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 icon and select "**View Debug Log**".



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

Relevant action (e.g. a new asset) should be performed on Tenable Service Center side.