

DEPLOYMENT GUIDE

Tenable.io + Infoblox NIOS Outbound API Integration

Table of Contents

Introduction.....	2
Prerequisites.....	2
Known Limitations.....	3
Best practices.....	3
Configuration.....	3
Workflow.....	3
Before you get Started.....	4
Download Templates from the Infoblox Community Website.....	4
Extensible Attributes.....	4
Editing Instance Variables.....	5
Editing Session Variables.....	6
Supported Notifications.....	6
Infoblox Permissions.....	7
Tenable.io Configuration.....	7
Configure Permissions.....	7
Create a Target Group.....	9
Create a Scan Template.....	10
Generate API Keys.....	11
Infoblox NIOS Configuration.....	12
Check if the Security Ecosystem License is Installed.....	12
Add/Upload Templates.....	13
Modifying Templates.....	14
Add a Rest API Endpoint.....	16
Adding Token.....	18
Add a Notification.....	18
Check the Configuration.....	21
Address Object Management Test.....	21
Summary.....	25

Introduction

Infoblox and Tenable.io together help empower actionable insight into your entire infrastructure's security risks, allowing for you to quickly and accurately identify, investigate, and prioritize vulnerabilities and misconfigurations in your modern IT environment.

Infoblox provides Tenable.io with resources such as IP addresses, Hosts, and potential threats and in exchange Tenable.io gets improved management on assets and the ability to automatically trigger scans when security events occur. The integration with Infoblox and Tenable.io allows for quicker remediation and more insight into the entire network. *Note that all Images in this document were taken in NIOS 8.4*

Prerequisites

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

Infoblox:

- Infoblox:
 - NIOS 8.3 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, ADP and Threat Analytics.
 - NIOS API user with the following permissions (access via API only):
 - All Network Views – RW.
 - All Hosts – RW.
 - All IPv4 Networks – RW.
 - All IPv6 Networks – RW.
 - All IPv4 Ranges – RW.
 - All IPv6 Ranges – RW.

- All IPv4 DHCP Fixed Addresses/Reservations – RW.
- All IPv6 DHCP Fixed Addresses/Reservations – RW.
- Tenable.io
 - Account with standard permissions

Known Limitations

The current templates support DNS Firewall (RPZ), Threat Insight (DNS Tunneling), Advanced DNS Protection, Network IPv4, Network IPv6, Range IPv4, Range IPv6, Host IPv4, Host IPv6, Fixed address IPv4, Fixed address IPv6, Discovery and Lease events only. If additional templates become available, they will be found on the Infoblox community site.

Note that editing the device type of an IPv4 or IPv6 fixed address is not supported.

Note that for Host and Fixed events, manually adding, editing or deleting objects multiple times within a short span of time may cause unexpected results.

Best practices

Outbound API templates can be found on the Infoblox community site on the Partner Integrations 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 Infoblox community site.

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

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

Tenable.io:

1. Configure Permissions
2. Create a Target Group
3. Create a Scan template.
4. Generate API Keys

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, ADP and Threat Analytics.
3. Create the required Extensible Attributes.
4. Download (or create your own) notification templates (Tenable IO Session, Tenable IO Scan, Tenable IO Discovery, Tenable IO Lease, Tenable IO Assets, Tenable IO Network & Range) from the Infoblox community website.
5. Add the templates.
6. Add a REST API Endpoint.
7. Add Notifications.
8. Emulate an event, check Rest API Endpoint 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 Tenable.io integration are located in the Partner 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 should be provided with a template. Don't forget to apply any changes required by the template before testing a notification

Extensible Attributes

For this integration, the following Extensible Attributes need to be created on the grid.

Table 1. Extensible Attributes

Extensible Attributes	Description	Type
TNBL_IO_Add_by_Hostname	Whether or not using a host's name as the target name is desired (otherwise will use its IP as the target name). The hostname	List (true, false)

	should be resolvable by Tenable.io.	
TNBL_IO_Last_Scan	Timestamp when target was last scanned by Tenable.io.	String
TNBL_IO_Scan_On_Add	Whether or not a target will be scanned upon creation.	List (true, false)
TNBL_IO_Scan	Whether or not a target will be scanned after a security event.	List (true, false)
TNBL_IO_Sync	Whether or adding the target to the Target Group list of targets is desired.	List (true, false)
TNBL_IO_Scan_Template	Name of the scan that will scan the target. It must match an active scan on Tenable.io.	String
TNBL_IO_Asset_Sync	Whether or not syncing asset events with Tenable.io is desired.	List (true, false)
TNBL_IO_Sync_Time	Timestamp when the asset was added to Tenable.io.	String
TNBL_IO_Target_Group	A target group allows you to set permissions on which targets (FQDNs, CIDR notations, ranges, or IP addresses) users can scan.	String

Editing Instance Variables

Tenable.io templates use instance variables to adjust the templates' behavior. Instance variables can be entered through the grid GUI at Grid → Ecosystem → Notification and then selecting the notification you created at Edit → Templates.

Table 2. Instance Variables

Instance Variable	Description	Type
Add_Discovery_Data	Whether or adding the target to the Target Group list of targets is desired.	String (true, false)
Scan_Discovery_Data	Whether or not a target will be scanned upon creation.	String (true, false)
Discovery_Asset_Sync	Whether or not syncing asset events with Tenable.io is desired.	String (true, false)
Discovery_Scan_Template	Name of the scan that will scan the target. It must match an	String

	active scan on Tenable.io.	
Discovery_Target_Group	A target group allows you to set permissions on which targets (FQDNs, CIDR notations, ranges, or IP addresses) users can scan.	String

Editing Session Variables

The Tenable_IO_Session template uses two session variables to login to the Tenable.io instance. Session variables can be entered through the grid GUI at **Grid** → **Ecosystem** → **Outbound Endpoint** and then selecting the endpoint you created at **Edit** → **Session Management**.

Table 3. Session Variables

Session Variable	Description
accessKey	A Token that is required to leverage the Tenable.io API.
secretKey	A Token that is required to leverage the Tenable.io API.

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, which template is executed and with which API endpoint NIOS will establish the connection to. The Tenable.io 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.

Table 4. Supported Notifications

Notification	Description
DNS RPZ	DNS queries that are malicious or unwanted
DNS Tunneling	Data exfiltration that occurs on the network
ADP	DNS queries that are malicious or unwanted
DHCP Leases	Lease events that occur on the network
Object Change Network IPv4	Added/Deleted IPv4 network objects
Object Change Network IPv6	Added/Deleted network IPv6 objects

Object Change Range IPv4	Added/Deleted Host IPv4 objects
Object Change Range IPv6	Added/Deleted Host IPv6 objects
Object Change Fixed Address IPv4	Added/Deleted fixed/reserved IPv4 objects
Object Change Fixed Address IPv6	Added/Deleted fixed/reserved IPv6 objects
Object Change Host Address IPv4	Added/Deleted Host IPv4 objects
Object Change Host Address IPv6	Added/Deleted Host IPv6 objects
Object Change Discovery Data	Discovery data

Infoblox Permissions

The Infoblox and Tenable.io integration requires 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 integrations. When creating a new group, under the Groups tab, select the API interface under the Allowed Interfaces category.

Tenable.io Configuration

Configure Permissions

In order to configure permissions:

1. Navigate to **Settings** → **Users** and click **New User**.

From this page, you can view, create, edit, and delete users. Once created, a user is configured with a role, which determines their scanner permissions. Additionally, each user can generate a custom API key to authenticate with the REST API.

<input type="checkbox"/>	Name ^	Last Login	Last Failed	Total Failed	Role	
<input type="checkbox"/>	kvasudevan@infoblox.com	Never	Never	0	Administrator	✕
<input checked="" type="checkbox"/>	kzettel@infoblox.com	09:14 AM	11/15/18	8	Administrator	

2. Insert the **name** and **password** and enter the Role with permissions levels set to Standard or higher.

New User
[← Back to Users](#)

Account Settings

User Info

Username

Full Name

Email

Role

Password

Password [Show](#)

GOOD

[Save](#) [Cancel](#)

Standard

Basic

Standard

Administrator

3. Navigate to **Settings** → **Groups** and click **New Group**.

tenable.io Vulnerability Management Dashboards Scans Reports **Settings** Search Groups

SETTINGS

- About
- Recast Rules
- Tags
- Connectors
- Credentials
- Access Groups
- Licensing

ACCOUNTS

- My Account
- Users
- Groups**

Groups [New Group](#)

Groups are objects that contain existing users and can be used to assign access and control permissions to scans, policies, scanners, agents, and target groups. From this page you can view, create, edit, and delete groups.

Name	Members
Infoblox Group	1

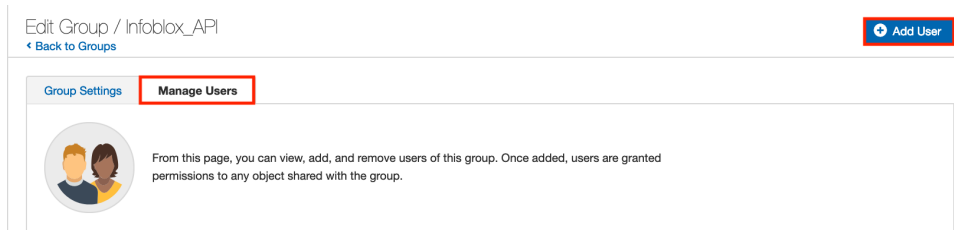
4. Enter a name for a Group that is not currently being used and click **Add**.

New Group

Name

[Add](#) [Cancel](#)

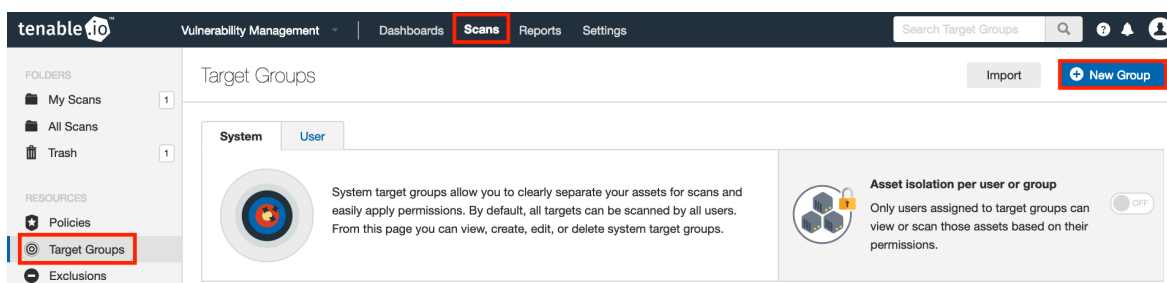
5. Inside the Created Group select **Manage Users** and then click **Add Users**.



6. Click the **User** dropdown and select the user created for the API.

Create a Target Group

1. Navigate to **Scans** → **Target Groups** and select **New Group**.



2. Enter a name for a target group that isn't being used and for Targets enter any default value for a place holder.

3. Under permissions add a group with at least standard permissions and click the drop down next to the user and choose Can scan then click **Save**.

Permissions

! You must grant at least one user the ability to run scans (either by changing the default setting or by customizing the permissions). Note that target group permissions do not increase user role permissions; basic users cannot run scans.

Add users or groups

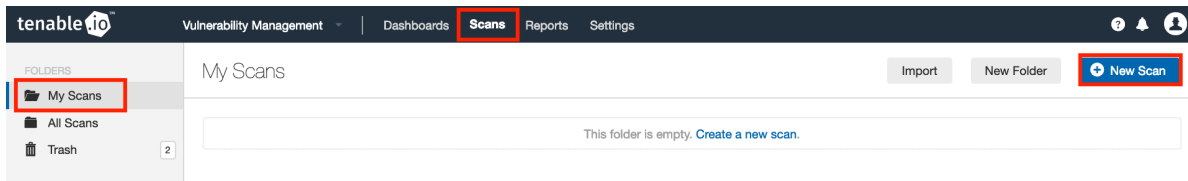
Default	No access
Infoblox_API	Can scan

[Save](#) [Cancel](#)

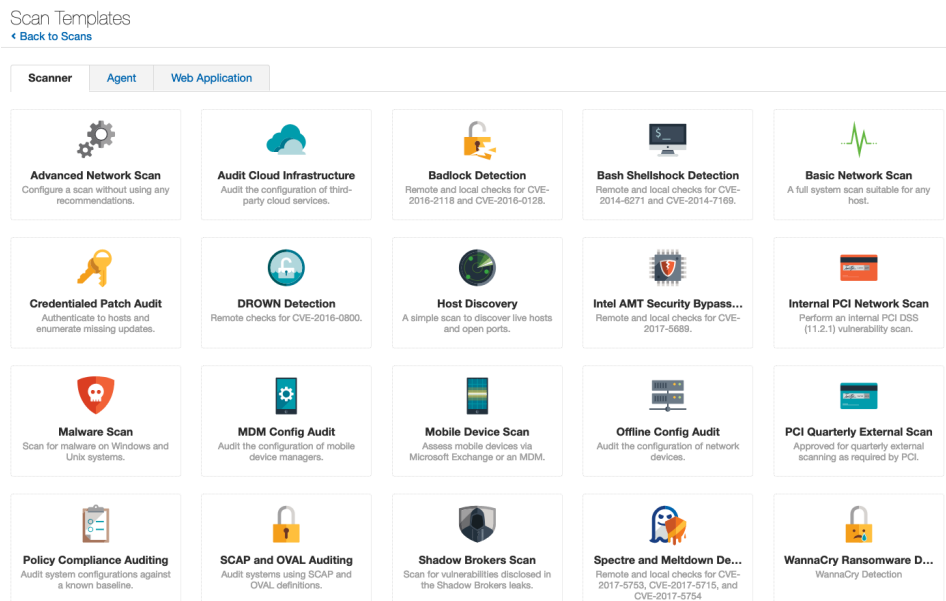
Create a Scan Template

In order to create a scan template:

1. Navigate to **Scans** → **My Scans** and select **New Scan**.



2. On the Scan Templates page select the appropriate Scanner template you wish to use.



3. Insert a name that isn't being used and choose the Target Group you created to add assets from Infoblox to.

New Scan / Basic Network Scan

[Back to Scan Templates](#)

Settings

Credentials

BASIC

General

Schedule

Notifications

Permissions

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name

Description

Folder

Scanner

Target Groups

Targets

Upload Targets

Infoblox_Scan

My Scans

US Cloud Scanner

TargetGroup_Test

Example: 192.168.1.1-192.168.1.5, 192.168.2.0/24, test.com

Add File

Save

Cancel

Note: you can configure any other setting as needed.

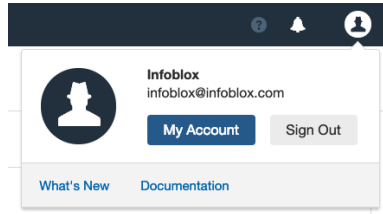
- Click **Save** when you are finished configuring the scan template.

My Scans			Import	New Folder	New Scan
<input type="checkbox"/>	Name	Schedule	Last Modified		
<input type="checkbox"/>	Infoblox_Scan	On Demand	N/A		

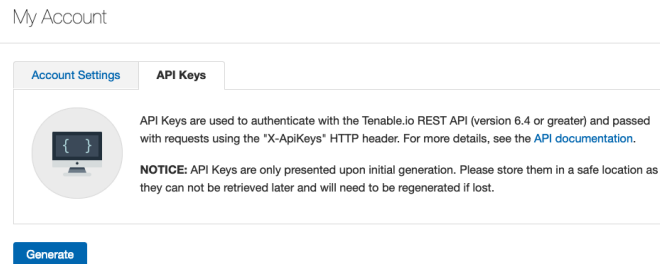
Generate API Keys

In order to Generate API Keys:

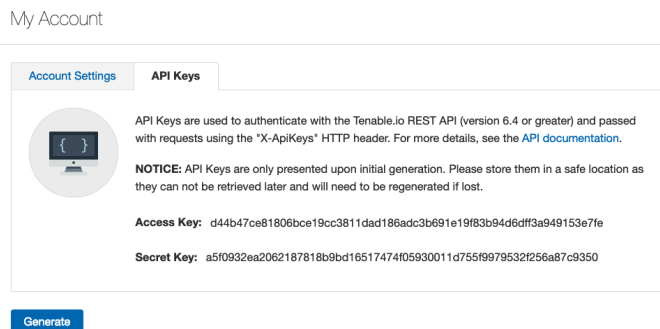
- Navigate to the image for your profile and select **My Account**.



2. Navigate to API Keys and click **Generate**.



3. Here you will find the Access Key and the Secret Key. You will need these for creating the Outbound Endpoint later in Infoblox.

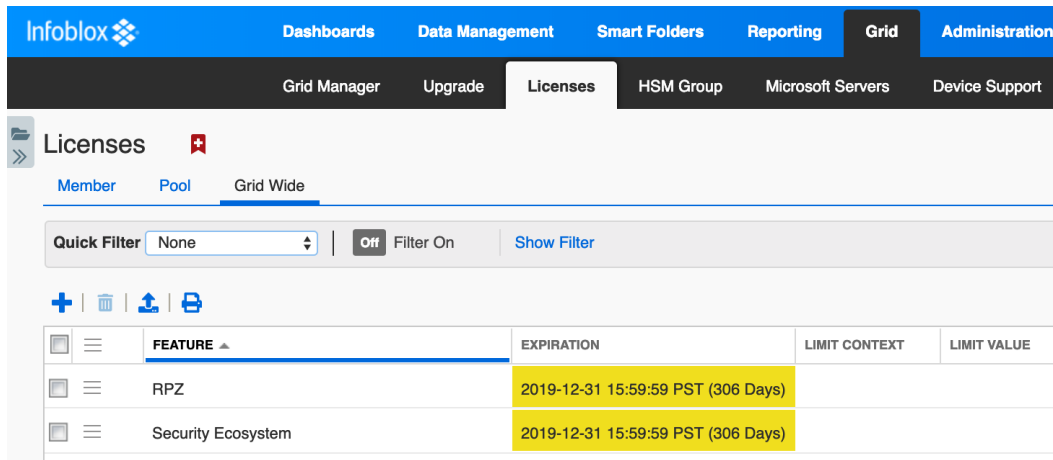


Infoblox NIOS Configuration

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.

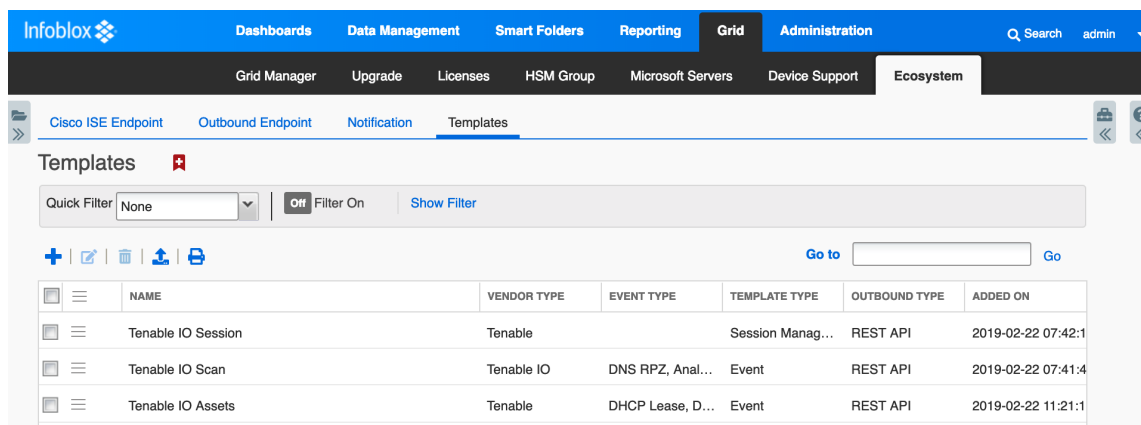
In order to check if the license was installed navigate to **Grid → Licenses → Grid Wide**.



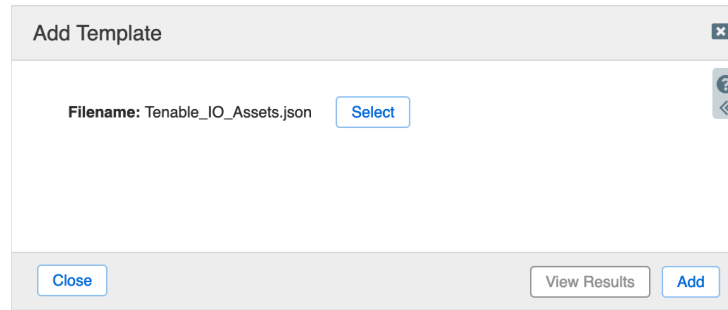
Add/Upload Templates

In order to upload/add templates:

1. Navigate to **Grid** → **Ecosystem** → **Templates** and click + or + **Add Template**.



2. Click the **Select** button on the Add template window.
3. Click the **Select** button on the Upload window. The standard file selection dialog will open.
4. Select the file and Click the **Upload** button on the Upload window.
5. Click the **Add** button and the template will be added/uploaded.

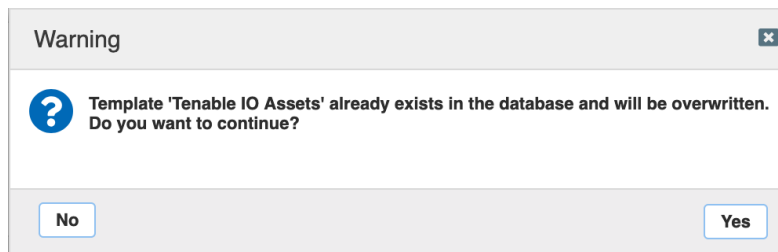


Add Template

Filename: Tenable_IO_Assets.json [Select](#)

[Close](#) [View Results](#) [Add](#)

- If a template was previously uploaded, click **Yes** to overwrite the template.

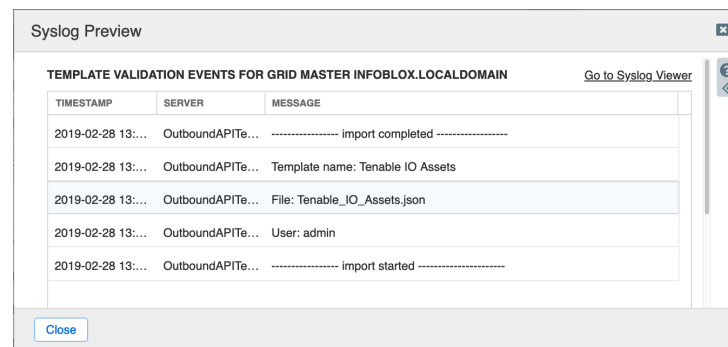


Warning

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

[No](#) [Yes](#)

- You can review the uploaded results in the syslog or by clicking the **View Results** button.



Syslog Preview

TEMPLATE VALIDATION EVENTS FOR GRID MASTER INFOBLOX.LOCALDOMAIN [Go to Syslog Viewer](#)

TIMESTAMP	SERVER	MESSAGE
2019-02-28 13:...	OutboundAPITe...	----- import completed -----
2019-02-28 13:...	OutboundAPITe...	Template name: Tenable IO Assets
2019-02-28 13:...	OutboundAPITe...	File: Tenable_IO_Assets.json
2019-02-28 13:...	OutboundAPITe...	User: admin
2019-02-28 13:...	OutboundAPITe...	----- import started -----

[Close](#)

Note: 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 click the **gear** icon next to the template you want to modify.

Infoblox

Dashboards

Data Management

Smart Folders

Reporting

Grid

Administration

Grid Manager

Upgrade

Licenses

HSM Group

Microsoft Servers

Device Support

Ecosystem

Cisco ISE Endpoint

Outbound Endpoint

Notification

Templates

Templates

Quick Filter

None

Off

Filter On

Show Filter

+

Go to

Go

	NAME	VENDOR TYPE	EVENT TYPE	TEMPLATE TYPE	OUTBOUND TYPE	ADDED ON
	Tenable IO Session	Tenable		Session Manag...	REST API	2019-02-22 07:42:1
	Tenable IO Scan	Tenable IO	DNS RPZ, Anal...	Event	REST API	2019-02-22 07:41:4
	Tenable IO Assets	Tenable	DHCP Lease, D...	Event	REST API	2019-02-22 11:21:1

2. Click the **Edit** button to open up the Template window.

Tenable IO Assets (Template)

Basic

General

Contents

Name

Tenable IO Assets

Type

REST API

Vendor Type

Tenable IO

Event Type

DB Change DHCP Fixed Address IPv4, DB Change DHCP Fixed Address IPv6, DB Change DNS Host Address IPv4, DB Change DNS Host Address IPv6

Template Type

Event

Comment

Tenable IO Assets management

Cancel

Save & Close

3. Click on the **Contents** tab to view/edit the template.

Tenable IO Assets (Template)

Basic

General

Contents

```
{
  "name": "Tenable IO Assets",
  "vendor_identifier": "Tenable IO",
  "comment": "Tenable IO Assets management",
  "version": "5.0",
  "type": "REST_EVENT",
  "event_type": [
    "FIXED_ADDRESS_IPV4",
    "FIXED_ADDRESS_IPV6",
    "HOST_ADDRESS_IPV4",
    "HOST_ADDRESS_IPV6"
  ],
  "content_type": "application/json",
  "quoting": "XMLA",
  "headers": {
    "X-apikeys": "accessKey=${S:A.accessKey};secretKey=${S:A.secretKey}"
  },
  "steps": [
    {
      "name": "DebugStart",
      "operation": "NOP",
      "body": "${X:C:DEBUG:(H)}${X:C:DEBUG:(F)}${X:C:DEBUG:(I)}${X:C:DEBUG:(L)}${X:C:DEBUG:(...)}"
    }
  ]
}
```

Cancel

Save & Close

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 a 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:

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

The screenshot displays the 'Outbound Endpoint' configuration page in the Infoblox NIOS interface. The top navigation bar includes 'Dashboards', 'Data Management', 'Smart Folders', 'Reporting', 'Grid', and 'Administration'. The 'Grid' tab is selected, and the 'Ecosystem' sub-tab is active. The 'Outbound Endpoint' section is highlighted, with sub-tabs for 'Cisco ISE Endpoint', 'Outbound Endpoint', 'Notification', and 'Templates'. Below the tabs, there's a 'Quick Filter' dropdown set to 'None', a 'Filter On' button, and a 'Show Filter' link. A 'Go to' search bar is also present. A dropdown menu is open, showing three options: 'Add REST API Endpoint' (highlighted), 'Add DXL Endpoint', and 'Add Syslog Endpoint'. Below the menu, a table lists existing endpoints:

ENDPOINT TYPE	URI	VENDOR TYPE	OUTBOUND MEMB...	COMMENT
REST API	https://cloud.ten...	Tenable IO	Grid Master	

2. The **URI** and **Name** for the appliance you are integrating with are required.
3. The URI should be the IP/FQDN of the appliance you are integrating with, with the correct URI scheme.
4. Specify **WAPI Integration Username** and **WAPI Integration Password** (NIOS credentials).

Add REST API Endpoint Wizard > Step 1 of 3

*URI: [Test Connection](#)

*Name:

Vendor Type:

Auth Username:

Auth Password: [Clear Password](#)

Client Certificate: [Select](#) [Clear](#)

WAPI Integration Username:

WAPI Integration Password: [Clear Password](#)

Server Certificate Validation:

- ☐ Use CA Certificate Validation (Recommended) [CA Certificates](#)
 - ☒ Enable Host Validation
- ☐ Do not use validation (Not recommended for production environment)

*Member Source outbound API requests from:

- ☐ Selected Grid Master Candidate [Choose One](#)
- ☒ Current Grid Master

Comment:

☐ Disable

[Cancel](#) [Previous](#) [Next](#) [Save & Close](#)

5. (Optional) For debug purposes only: Under Session Management, set Log Level to **Debug**.

Tenable IO (REST API Endpoint)

Basic

General

Session Management

Extensible Attributes

Timeout: [Seconds](#)

Log Level: [Debug](#)

Template: Tenable IO Session [Select Template](#) [Clear](#)

Vendor Type: Tenable IO

Template Type: Session Management

Parameters

NAME	VALUE	TYPE
accessKey	xxx	String
secretKey	xxx	String

[Cancel](#) [Save & Close](#)

6. The accessKey and secretKey can be found when you create the API keys for the user.

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

Adding Token

1. Navigate to the Session Management tab and add the **Token** to the value fields.

Add REST API Endpoint Wizard > Step 2 of 3

Timeout: 30 Seconds

Log Level: Debug

Template: Tenable IO Session [Select Template] [Clear]

Vendor Type: Tenable

Template Type: Session Management

NAME	VALUE	TYPE
accessKey	2f60ebe4a3091bc740eeffa6fb38fbc44d714ec2f7cbf83ca03933d7b63e933	String
secretKey	69abc19a2a5a54882618a9faf2662927e675da43946fd9ccc0614d7209c45571	String

[Cancel] [Previous] [Next] [Save & Close]

Add a Notification

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

In order to add notifications:

1. Navigate to **Grid** → **Ecosystem** → **Notification** and click + or + **Add Notification Rule** then the Add Notification Wizard window will open.

Dashboards Data Management Smart Folders Reporting Grid Administration

Grid Manager Upgrade Licenses HSM Group Microsoft Servers Device Support Ecosystem

Cisco ISE Endpoint Outbound Endpoint Notification Templates

Notification

Quick Filter: None [Filter On] [Show Filter]

[Add] [Edit] [Delete] [Duplicate] [Go to] [Go]

Toolbar: [Add Notification Rule] [Edit] [Delete] [IDN Converter]

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

Add Notification Wizard > Step 1 of 4

*Name: TNBL_IO_RPZ

*Target: Tenable IO [Select Endpoint](#)

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

Target Type: REST API

Vendor Type: Tenable IO

Comment:

☐ Disable

[Cancel](#) [Previous](#) [Next](#) [Save & Close](#)

3. 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**.

Add Notification Wizard > Step 2 of 4

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

*Event: DNS RPZ

Match the following rule: [Reset](#)

Action Policy equals NXDOMAIN

[Cancel](#) [Previous](#) [Next](#) [Save & Close](#)

4. (For Security related notifications only) Check Enable event deduplication and specify relevant parameters. Click **Next**.

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

- RPZ Policy
- RPZ Type
- Query Type
- Network
- Network View

Selected

- Source IP
- Query Name

Lookback Interval: 10 Minutes

Cancel Previous Next Save & Close

5. Select a relevant template and specify the template's parameters if any are required. Click **Save & Close**.

Add Notification Wizard > Step 4 of 4

*Template: Tenable IO Scan [Select Template](#) [Clear](#)

Vendor Type: Tenable IO

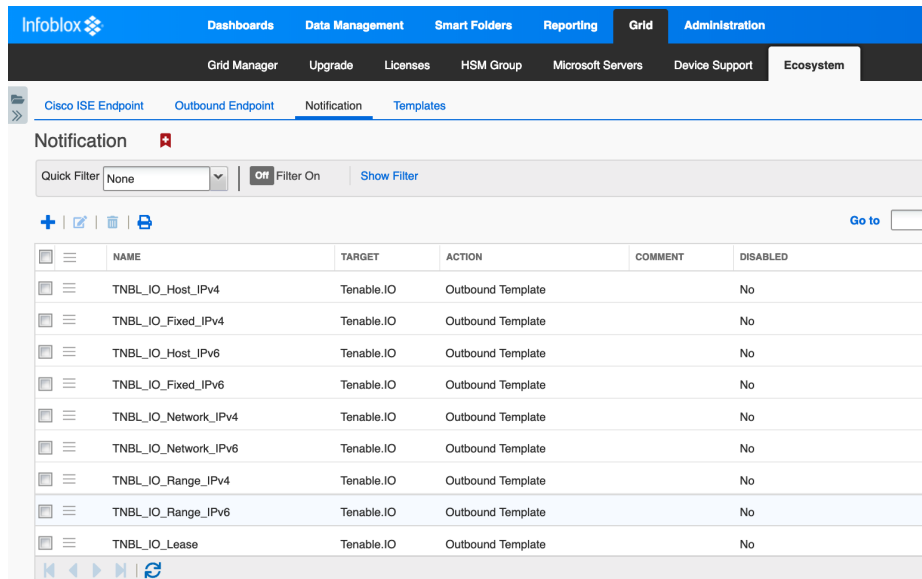
Template Type: Event

Parameters

NAME	VALUE	TYPE
No data		

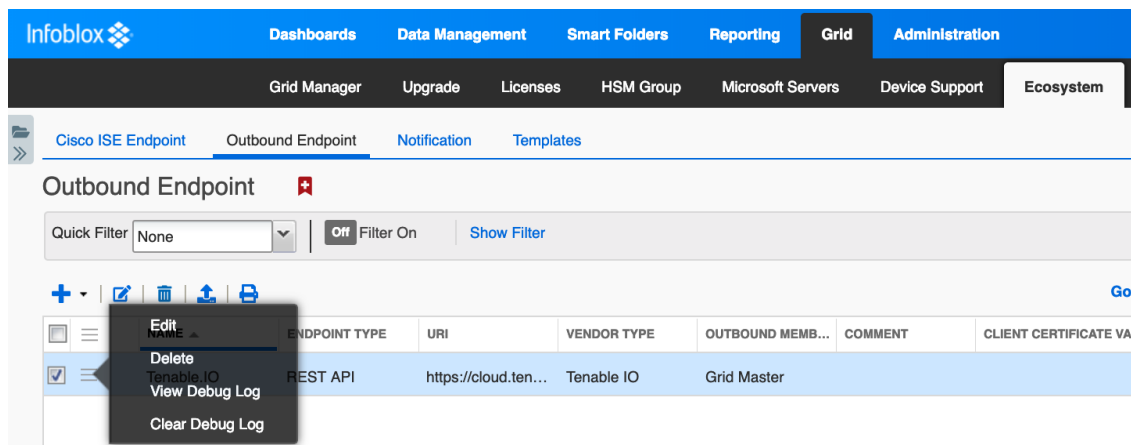
Cancel Previous Next Save & Close

6. Add rules for other events as well.



Check the Configuration

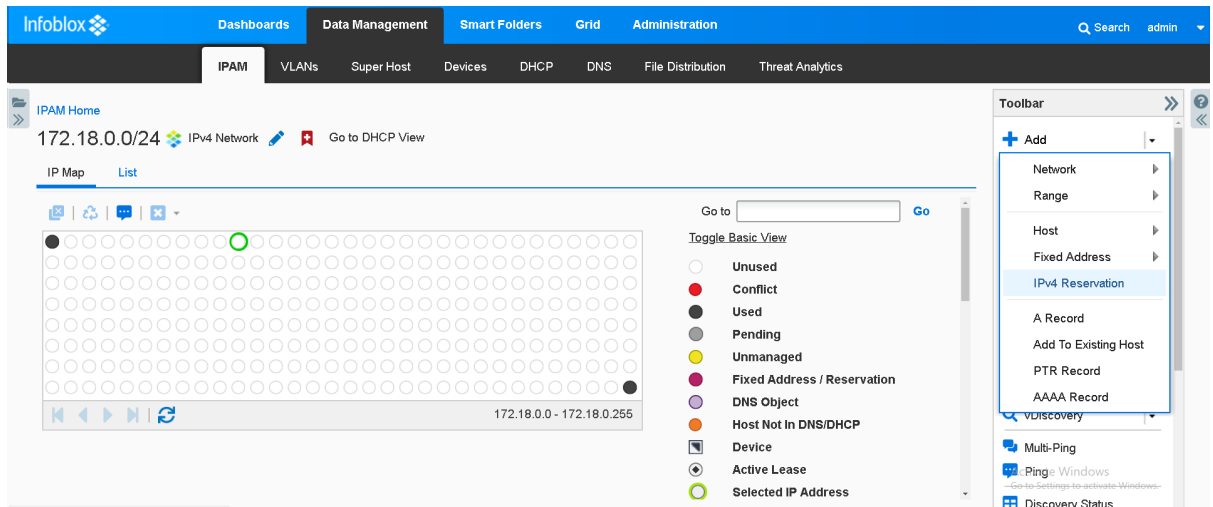
(Optional) On the Infoblox grid, navigate to **Grid** → **Ecosystem** → **Outbound Endpoint**, select Tenable.io endpoint, click on the hamburger icon and select Clear Debug Log.



Address Object Management Test

The templates support IPv4/IPv6 Hosts, IPv4/IPv6 Fixed IP/Reservations, IPv4/IPv6 Networks, IPv4/IPv6 Ranges, Discovery, and DHCP lease events. This use case demonstrates how to manage IP addresses on Tenable.io.

1. To create an IPv4 reservation, navigate to **Data Management** → **IPAM**. Select an IPv4 network here (i.e 172.18.0.0/24).
2. Click the **drop down** next to the + Add button under the toolbar and choose IPv4 Reservation.



3. Click **Next**, then insert the IP **172.18.0.10** into the IP Address field.

Add IPv4 Reservation Wizard > Step 2 of 8

*Network 172.18.0.0/24 (255.255.255.0) [Select Network](#) [Clear](#)

*IP Address [Next Available IP](#)

Name

Comment

Disabled ☐

[Cancel](#) [Previous](#) [Next](#) [Schedule for Later](#) [Save & Close](#)

4. Click on **Next** until you reach the Extensible Attributes window. If the Extensible Attributes have not already been inherited from the network, set them.

Add Host Wizard > Step 5 of 6

Extensible Attributes

	ATTRIBUTE NAME	VALUE	INHERITANCE STA...	REQUIRED
<input type="checkbox"/>	TNBL_IO_Add_by_Hostname	true Network View (default)	Inherited	No
<input type="checkbox"/>	TNBL_IO_Asset_Sync	true Network View (default)	Inherited	No
<input type="checkbox"/>	TNBL_IO_Scan	true Network View (default)	Inherited	No
<input type="checkbox"/>	TNBL_IO_Scan_On_Add	true Network View (default)	Inherited	No
<input type="checkbox"/>	TNBL_IO_Scan_Template	Infoblox_Scan Network View (default)	Inherited	No
<input type="checkbox"/>	TNBL_IO_Sync	true	Inherited	No

Cancel
Previous
Next
Schedule for Later
Save & Close

5. Click **Save & Close**.

6. Select the IP and refresh. The **TNBL_IO_Sync_Time** and **TNBL_IO_Last_Scan EA** are now updated.

Related Objects Audit History

	NAME	TYPE	TNBL_IO_SYNC_TIME ▲	TNBL_IO_LAST_SCAN
	ipv4res_test	IPv4 Reservation	2019-08-09T19:58:05Z	2019-08-09T19:58:05Z

7. In Tenable.io, navigate to **Scans** → **Target Groups** then select the target group you sent the asset to. The 172.18.0.10 address reservation has been added to the Targets list. Refresh the page if necessary.

tenable.io

Vulnerability Management

Dashboards

Scans

Reports

Settings

Search Target Groups

FOLDERS

My Scans 1

All Scans

Trash 2

RESOURCES

Policies

Target Groups

Exclusions

Scanners

Agents

Target Groups

Import

New Group

System

User

System target groups allow you to clearly separate your assets for scans and easily apply permissions. By default, all targets can be scanned by all users. From this page you can view, create, edit, or delete system target groups.

Asset isolation per user or group
Only users assigned to target groups can scan those assets based on their permissions.

System Target Group view permissions have moved to Access Groups. Please view and manage them there.

Open Access Groups

Name ▲	Permissions	Last Modified
Default Target Group	Scan Use	February 28
Infoblox_Assets	Scan Use	10:38 AM

Edit Target Group / Infoblox_Assets

[← Back to Target Groups](#)

General

Name:

Targets:

Upload Targets [Add File](#)

8. Navigate to **Scans** → **My Scans**. The address has been scanned and its timestamp is visible.

tenable.io Vulnerability Management | Dashboards **Scans** Reports Settings

Search Scans [Advanced](#) ?

FOLDERS Hide

- My Scans 1
- All Scans
- Trash 39

RESOURCES

- Policies
- Target Groups
- Exclusions
- Scanners
- Agents

My Scans

[Import](#) [New Folder](#) [New Scan](#)

<input type="checkbox"/>	Name	Schedule	Last Modified		
<input type="checkbox"/>	Infoblox Scan for 172.18.0.10 on 2019-07-30T17:24...	On Demand	✓ July 30	▶	✕
<input type="checkbox"/>	Infoblox_Scan	On Demand	N/A	▶	✕

9. Navigate to **Dashboards** → **Assets**. The object has been added as an Asset.

tenable.io Vulnerability Management | **Dashboards** Scans Reports Settings [New Interface](#)

Advanced Search Assets ?

WORKBENCH Hide

- Vulnerabilities
- Assets**
- Web Applications
- Health & Status

ANALYTICS

- My Dashboards

Assets

ALL ASSETS: 1 LAST UPDATED: 11:14 AM

<input type="checkbox"/>	Name	Address	OS	Last Seen	Source	
<input type="checkbox"/>	ipv4res_test	172.18.0.10	NIOS	11:14 AM		✕

10. In NIOS, navigate to **Data Management**→**IPAM**→**172.18.0.0/24** and select the IPv4 Reservation object just created. Scroll down and click the **garbage can** icon.

		NAME	TYPE	TNBL_IO_SYNC_TIME	TNBL_IO_LAST_SCAN
		ipv4res_test	IPv4 Reservation	2019-08-09T19:58:05Z	2019-08-09T19:58:05Z

11. In Tenable.io, navigate to **Dashboards** → **Assets**. The asset has been deleted.

Summary

Infoblox and Tenable.io together help empower actionable insight into your entire infrastructure's security risks, allowing for you to quickly and accurately identify, investigate, and prioritize vulnerabilities and misconfigurations in your modern IT environment.



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