Deployment Guide

Integration with Tenable.io

TABLE OF CONTENTS

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 and Lease events only. The asset management template does not support delete or modify events and does not delete or modify IP's or Host's from Tenable.io due to limitations with Tenable.io API. If additional templates become available, they will be found on the Infoblox community site.

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 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_Assets.txt, Tenable_IO_Security.txt, Tenable_IO_Session.txt, Tenable_IO_Logout.txt, Tenable_IO_Login.txt) 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 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 (out-of-the-box) with the NIOS releases. Templates are available on the Infoblox community web-site. Templates for the Tenable.io 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 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	Defines if a host should be synced with Tenable.io using a hostname. The hostname should be resolvable by Tenable.io.	List (true, false)
TNBL_IO_Last_Scan	Contains a date when an asset was scanned last time by a request from Infoblox	String
TNBL_IO_Scan	Defines if an asset should be scanned if RPZ, ADP or DNS Tunneling events are triggered	List (true, false)
TNBL_IO_Scan_On_Add	Defines if an asset should be scanned immediately after creation	List (true, false)
TNBL_IO_Scan_Template	Defines a Tenable.io active scan which should be used for scans initiated by Infoblox. List of possible values should match active scan names on Tenable.io.	String
TNBL_IO_Sync	Defines if an object should be synced with Tenable.io.	List (true, false)
TNBL_IO_Sync_Time	Contains date/time when the object was synchronized.	String
TNBL_IO_Target_Group	Defines a target group in Tenable.io that holds the assets to be scanned by Tenable.io.	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

Add_Discovery_Data	true or false. Defines if a Discovered device should be added to Tenable.io
Scan_Discovery_Data	true or false. Defines if a Discovered device should be scanned when added to Tenable.io
Discovery_Scan_Template	Defines a Tenable.io active scan which should be used for scans initiated by Infoblox for Discovery events.
Discovery_Target_Group	Defines a target group in Tenable.io that holds the assets to be scanned by Tenable.io

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 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 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.

Infoblox Permissions

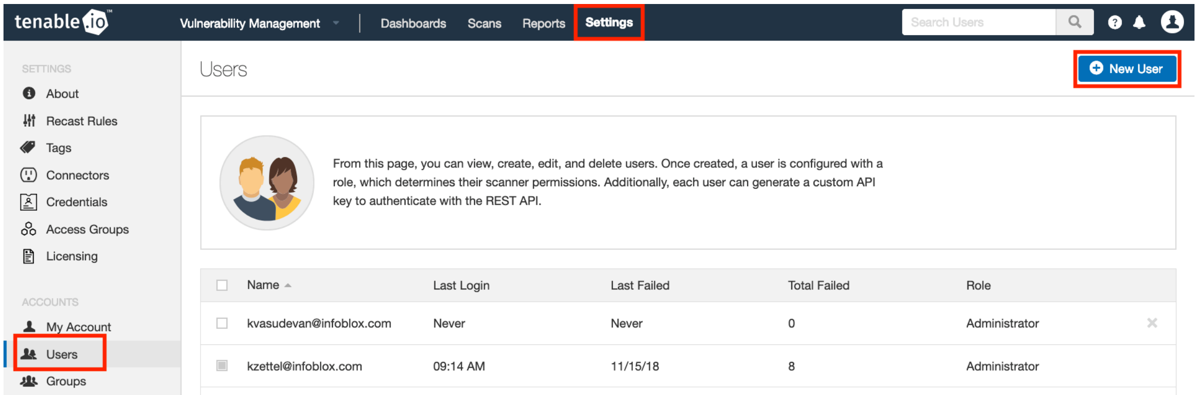
The Infoblox and Tenable.io integration requires a few permissions for the integration to work. Navigate to **“Administration”** → **“Administrators”** and add a **“Roles”**, **“Permissions”**, **“Groups”** and **“Admins”** to include permissions that are required for the integrations. When creating 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”**.

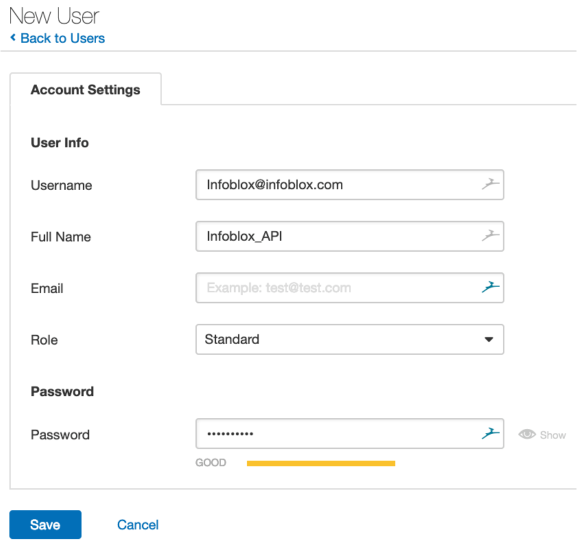


Users

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.

□	Name	Last Login	Last Failed	Total Failed	Role
□	kvasudevan@infoblox.com	Never	Never	0	Administrator
□	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

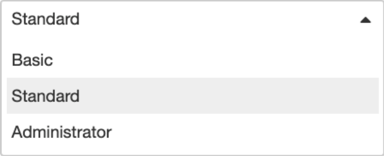
User Info

Username	Infoblox@infoblox.com
Full Name	Infoblox_API
Email	Example: test@test.com
Role	Standard

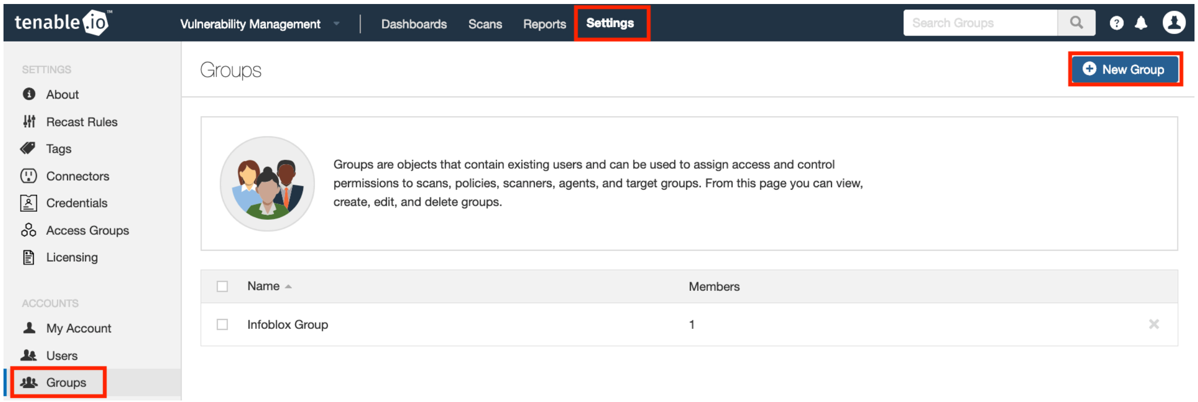
Password

Password	••••••••••

GOOD



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

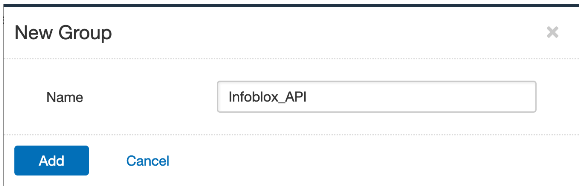


Groups

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

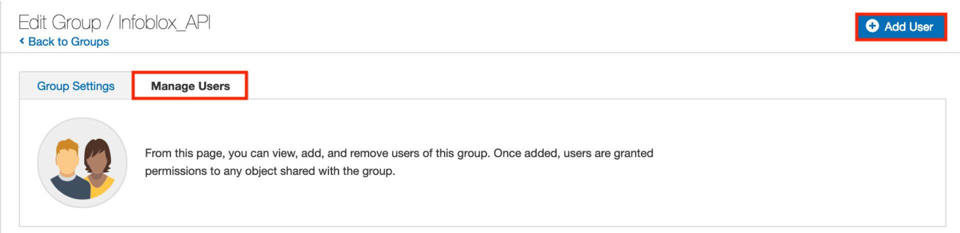
4. Enter a name for a Group that is not currently being used and click **“Add”**.



New Group

Name: Infoblox_API

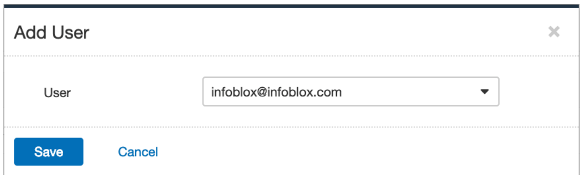
5. Inside the Created Group select **“Manage Users”** and then click **“Add Users”**.



Edit Group / Infoblox_API

From this page, you can view, add, and remove users of this group. Once added, users are granted permissions to any object shared with the group.

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

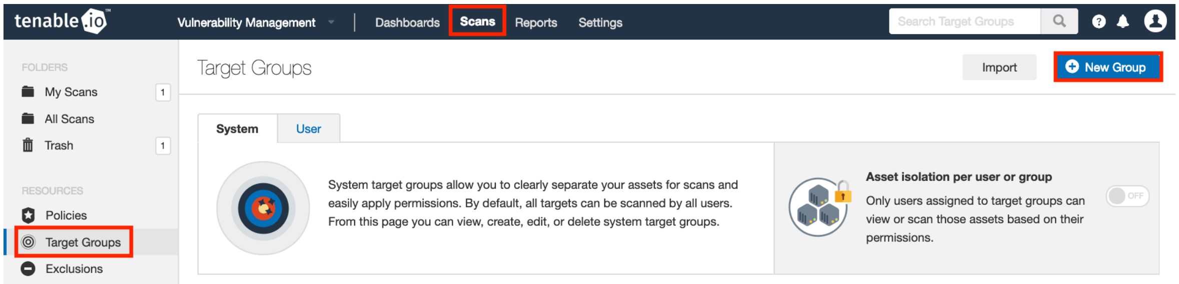


Add User

User infoblox@infoblox.com

Create a Target Group

7. Navigate to **“Scans”** → **“Target Groups”** and select **“New Group”**.



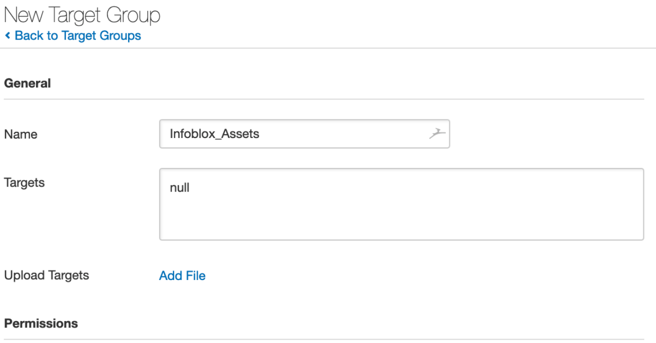
Target Groups

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 view or scan those assets based on their permissions.

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



New Target Group

General

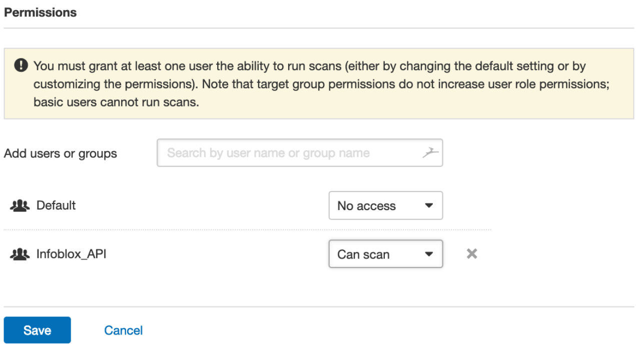
Name: Infoblox_Assets

Targets: null

Upload Targets: Add File

Permissions

9. 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: Search by user name or group name

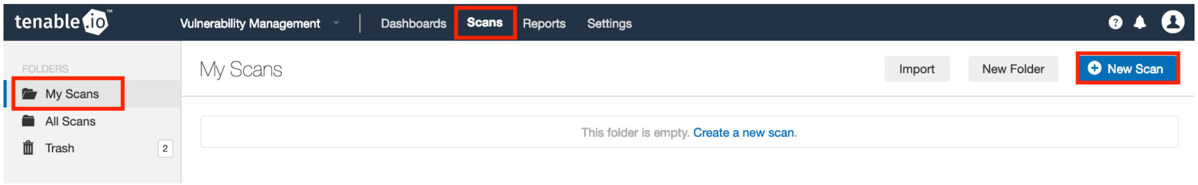
Default: No access

Infoblox_API: Can scan

Create a Scan Template

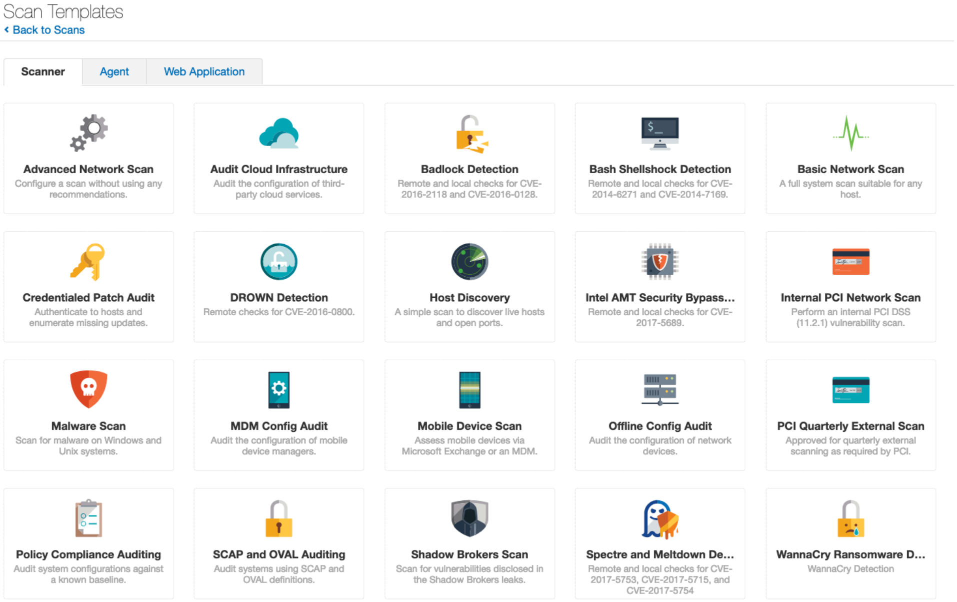
In order to create a scan template:

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



This folder is empty. Create a new scan.

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



Advanced Network Scan: Configure a scan without using any recommendations.

Audit Cloud Infrastructure: Audit the configuration of third-party cloud services.

Badlock Detection: Remote and local checks for CVE-2016-2118 and CVE-2016-0128.

Bash Shellshock Detection: Remote and local checks for CVE-2014-6271 and CVE-2014-7169.

Basic Network Scan: A full system scan suitable for any host.

Credentialed Patch Audit: Authenticate to hosts and enumerate missing updates.

DROWN Detection: Remote checks for CVE-2016-0800.

Host Discovery: A simple scan to discover live hosts and open ports.

Intel AMT Security Bypass…: Remote and local checks for CVE-2017-5689.

Internal PCI Network Scan: Perform an internal PCI DSS (11.2.1) vulnerability scan.

Malware Scan: Scan for malware on Windows and Unix systems.

MDM Config Audit: Audit the configuration of mobile device managers.

Mobile Device Scan: Assess mobile devices via Microsoft Exchange or an MDM.

Offline Config Audit: Audit the configuration of network devices.

PCI Quarterly External Scan: Approved for quarterly external scanning as required by PCI.

Policy Compliance Auditing: Audit system configurations against a known baseline.

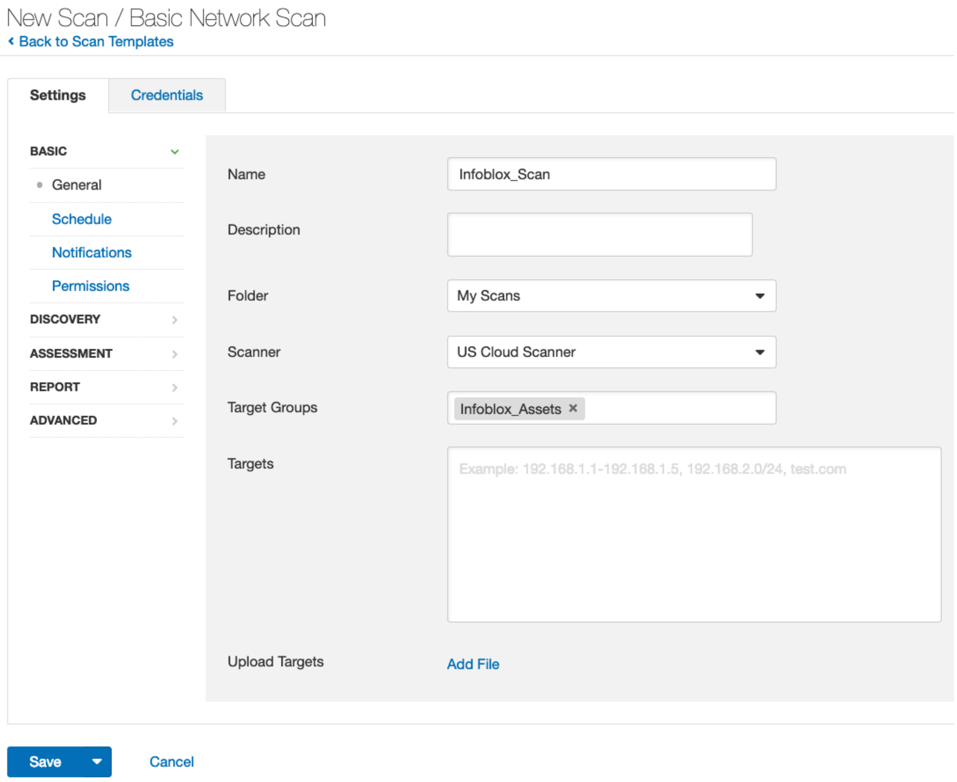
SCAP and OVAL Auditing: Audit systems using SCAP and OVAL definitions.

Shadow Brokers Scan: Scan for vulnerabilities disclosed in the Shadow Brokers leaks.

Spectre and Meltdown De…: Remote and local checks for CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754

WannaCry Ransomware D…: WannaCry Detection

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

Name: Infoblox_Scan

Description:

Folder: My Scans

Scanner: US Cloud Scanner

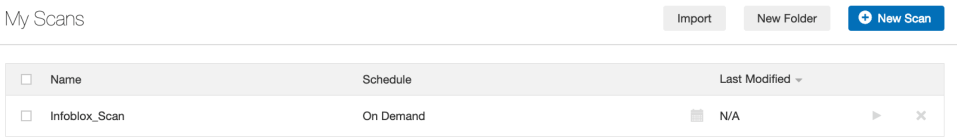
Target Groups: Infoblox_Assets ×

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

Upload Targets: Add File

Note: you can configure any other setting as needed.

4. Click Save when you are finished configuring the scan template.



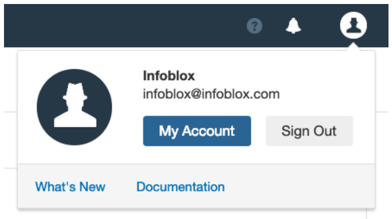
My Scans

□	Name	Schedule	Last Modified
□	Infoblox_Scan	On Demand	N/A

Generate API Keys

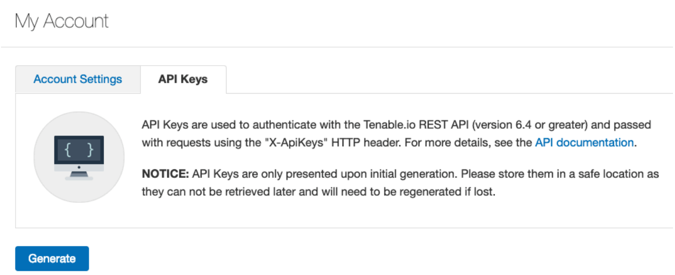
In order to Generate API Keys:

1. Navigate to the image for your profile and select **“My Account”**.



Infoblox
infoblox@infoblox.com

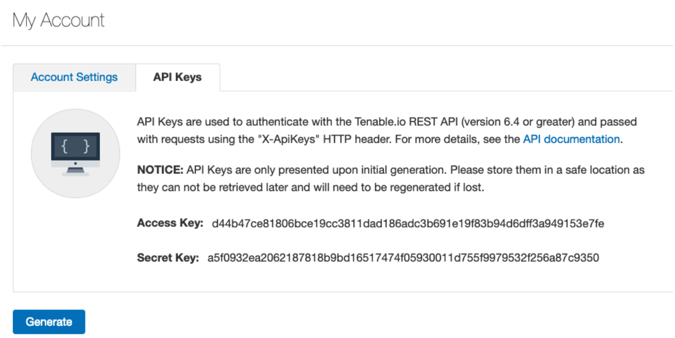
2. Navigate to **“API Keys”** and click **“Generate”**.



API Keys are used to authenticate with the Tenable.io REST API (version 6.4 or greater) and passed with requests using the "X-ApiKeys" HTTP header. For more details, see the API documentation.

NOTICE: API Keys are only presented upon initial generation. Please store them in a safe location as they can not be retrieved later and will need to be regenerated if lost.

3. Here you will find the **"Access Key"** and the **"Secret Key"**.



API Keys are used to authenticate with the Tenable.io REST API (version 6.4 or greater) and passed with requests using the "X-ApiKeys" HTTP header. For more details, see the API documentation.

NOTICE: API Keys are only presented upon initial generation. Please store them in a safe location as they can not be retrieved later and will need to be regenerated if lost.

Access Key: d44b47ce81806bce19cc3811dad186adc3b691e19f83b94d6dff3a949153e7fe

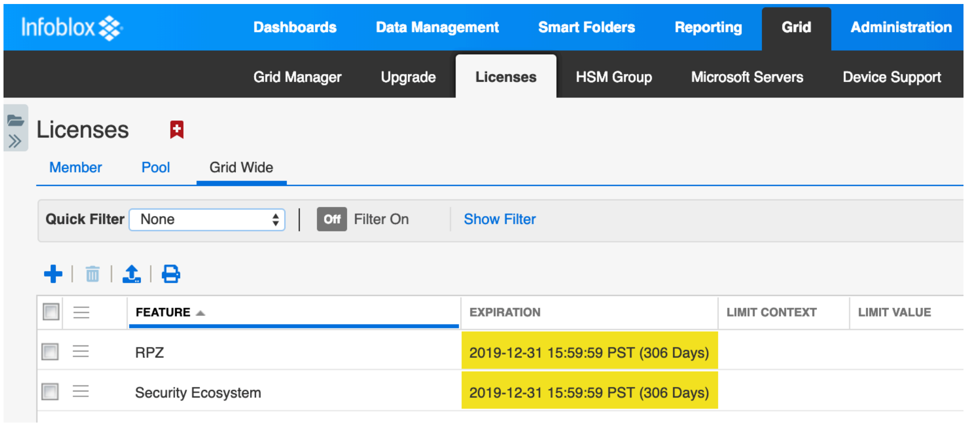
Secret Key: a5f0932ea2062187818b9bd16517474f05930011d755f9979532f256a87c9350

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"**.



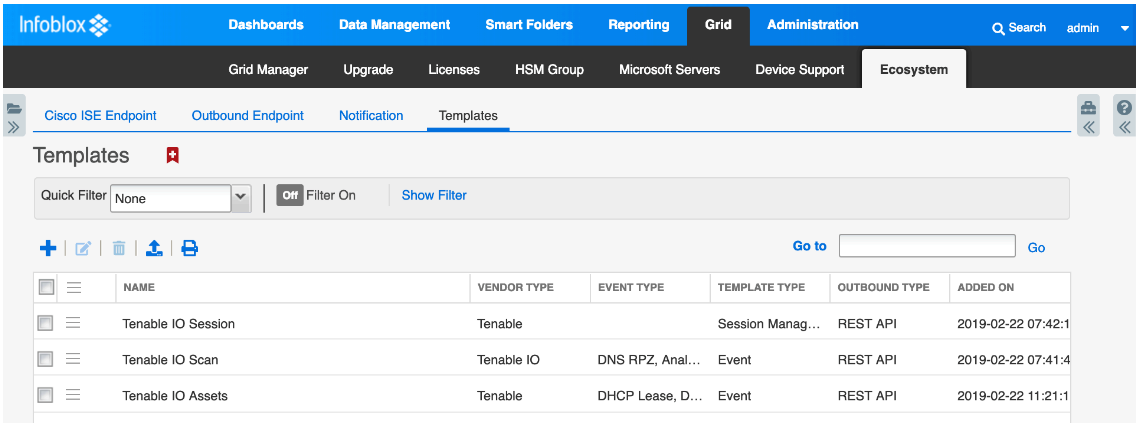
Quick Filter: None

FEATURE	EXPIRATION	LIMIT CONTEXT	LIMIT VALUE
RPZ	2019-12-31 15:59:59 PST (306 Days)		
Security Ecosystem	2019-12-31 15:59:59 PST (306 Days)		

Add/Upload Templates

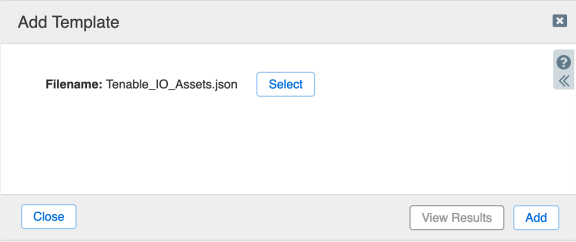
In order to upload/add templates:

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



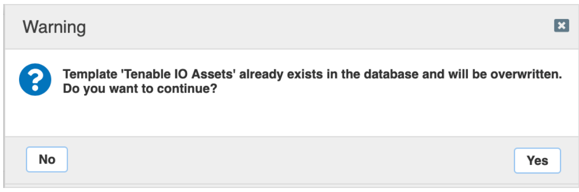
	NAME	VENDOR TYPE	EVENT TYPE	TEMPLATE TYPE	OUTBOUND TYPE	ADDED ON
□	Tenable IO Session	Tenable		Session Manag…	REST API	2019-02-22 07:42:1
□	Tenable IO Scan	Tenable IO	DNS RPZ, Anal…	Event	REST API	2019-02-22 07:41:4
□	Tenable IO Assets	Tenable	DHCP Lease, D…	Event	REST API	2019-02-22 11:21:1

2. Click the **“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.



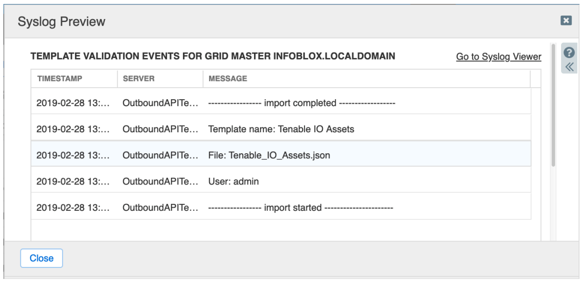
Filename: Tenable_IO_Assets.json

6. If a template was previously uploaded, click **“Yes”** to overwrite the template.



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

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



TEMPLATE VALIDATION EVENTS FOR GRID MASTER INFOBLOX.LOCALDOMAIN

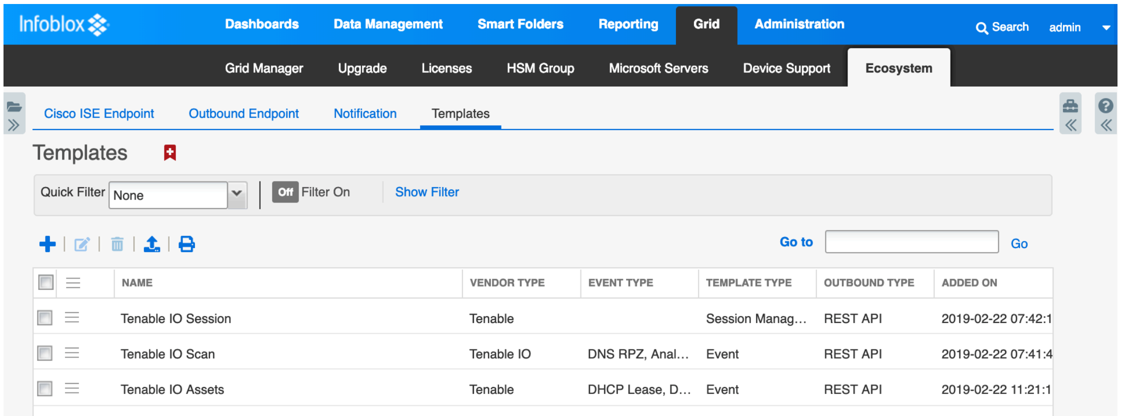
```
TIMESTAMP          SERVER            MESSAGE
2019-02-28 13:...  OutboundAPITe...  ---------------- import completed -----------------
2019-02-28 13:...  OutboundAPITe...  Template name: Tenable IO Assets
2019-02-28 13:...  OutboundAPITe...  File: Tenable_IO_Assets.json
2019-02-28 13:...  OutboundAPITe...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

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

Modifying Templates

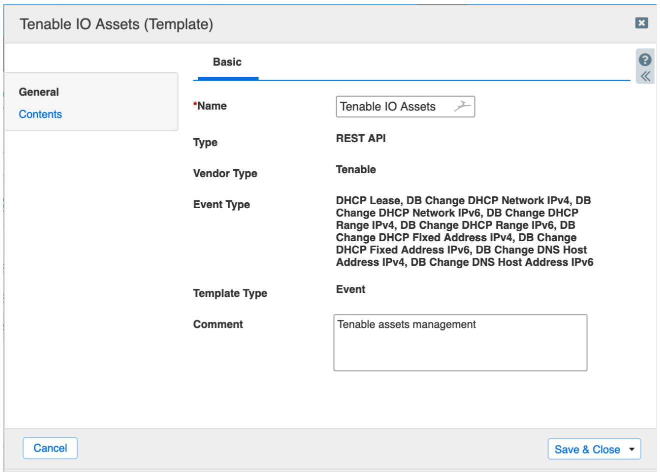
NIOS provides the facility to modify the templates via the web-interface.

1. Navigate to **“Grid”** → **“Ecosystem”** → **“Templates”**, and then click the gear icon next to the template you want to modify.



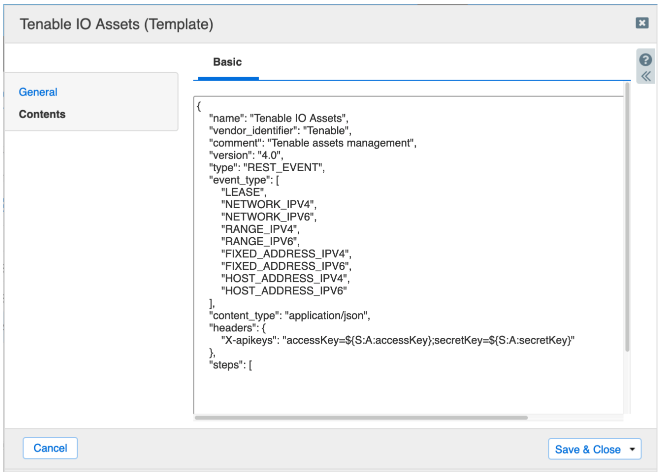
NAME	VENDOR TYPE	EVENT TYPE	TEMPLATE TYPE	OUTBOUND TYPE	ADDED ON
Tenable IO Session	Tenable		Session Manag…	REST API	2019-02-22 07:42:1
Tenable IO Scan	Tenable IO	DNS RPZ, Anal…	Event	REST API	2019-02-22 07:41:4
Tenable IO Assets	Tenable	DHCP Lease, D…	Event	REST API	2019-02-22 11:21:1

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



*Name	Tenable IO Assets
Type	REST API
Vendor Type	Tenable
Event Type	DHCP Lease, DB Change DHCP Network IPv4, DB Change DHCP Network IPv6, DB Change DHCP Range IPv4, DB Change DHCP Range IPv6, 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 assets management

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



```
{
    "name": "Tenable IO Assets",
    "vendor_identifier": "Tenable",
    "comment": "Tenable assets management",
    "version": "4.0",
    "type": "REST_EVENT",
    "event_type": [
        "LEASE",
        "NETWORK_IPV4",
        "NETWORK_IPV6",
        "RANGE_IPV4",
        "RANGE_IPV6",
        "FIXED_ADDRESS_IPV4",
        "FIXED_ADDRESS_IPV6",
        "HOST_ADDRESS_IPV4",
        "HOST_ADDRESS_IPV6"
    ],
    "content_type": "application/json",
    "headers": {
        "X-apikeys": "accessKey=${S:A:accessKey};secretKey=${S:A:secretKey}"
    },
    "steps": [
```

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.

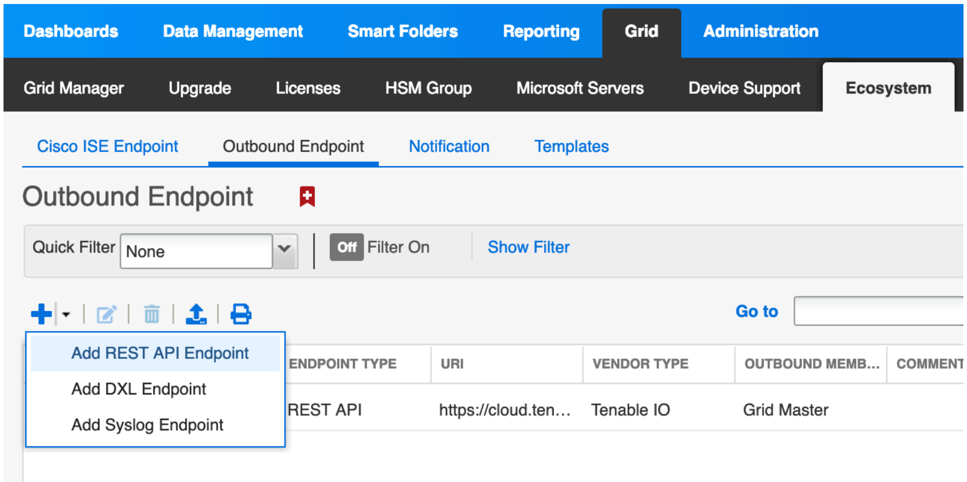
Note: You cannot delete a template if it is used by an endpoint or by a notification.

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).

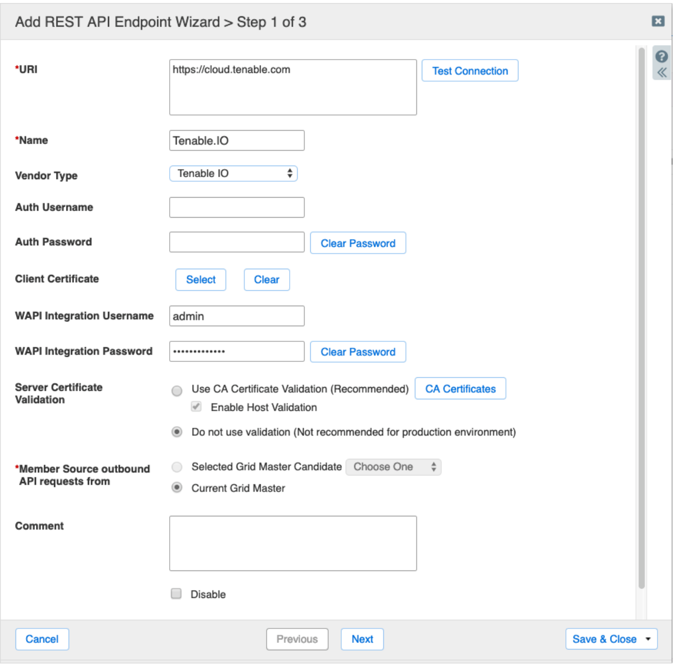
In order to add REST API Endpoints:

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



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

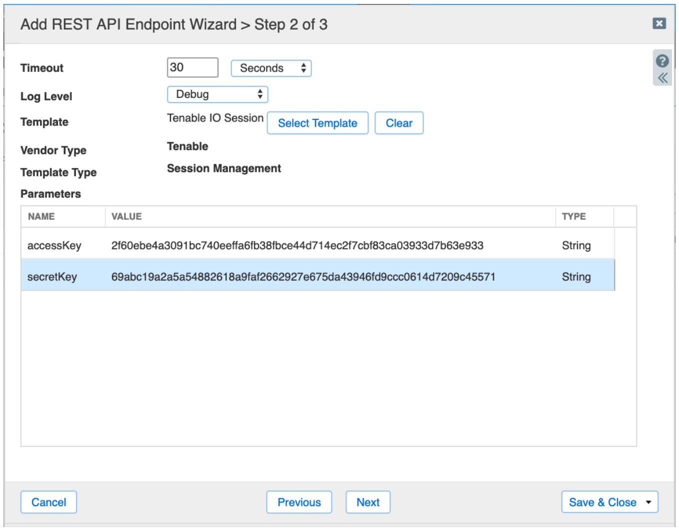
2. The URI and Name for the appliance you are integrating with are required.
3. The URI should be the IP/FQDN of the appliance you are integrating with, with the correct URI scheme.
4. Specify **"WAPI Integration Username"** and **"WAPI Integration Password"** (NIOS credentials).



Add REST API Endpoint Wizard > Step 1 of 3

*URI	https://cloud.tenable.com
*Name	Tenable.IO
Vendor Type	Tenable IO
Auth Username	
Auth Password	
Client Certificate	
WAPI Integration Username	admin
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 Choose One ● Current Grid Master
Comment	
	□ Disable

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



Add REST API Endpoint Wizard > Step 2 of 3

Timeout	30 Seconds
Log Level	Debug
Template	Tenable IO Session
Vendor Type	Tenable
Template Type	Session Management

Parameters

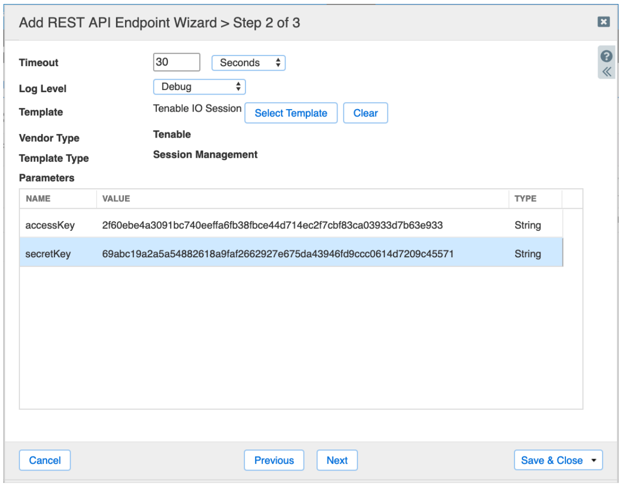
NAME	VALUE	TYPE
accessKey	2f60ebe4a3091bc740eeffa6fb38fbce44d714ec2f7cbf83ca03933d7b63e933	String
secretKey	69abc19a2a5a54882618a9faf2662927e675da43946fd9ccc0614d7209c45571	String

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

- 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

Vendor Type: Tenable

Template Type: Session Management

Parameters

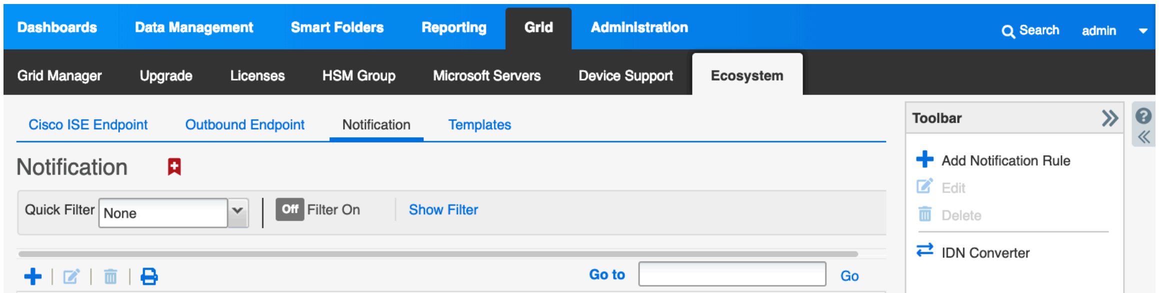
NAME	VALUE	TYPE
accessKey	2f60ebe4a3091bc740eeffa6fb38fbce44d714ec2f7cbf83ca03933d7b63e933	String
secretKey	69abc19a2a5a54882618a9faf2662927e675da43946fd9ccc0614d7209c45571	String

Add a Notification

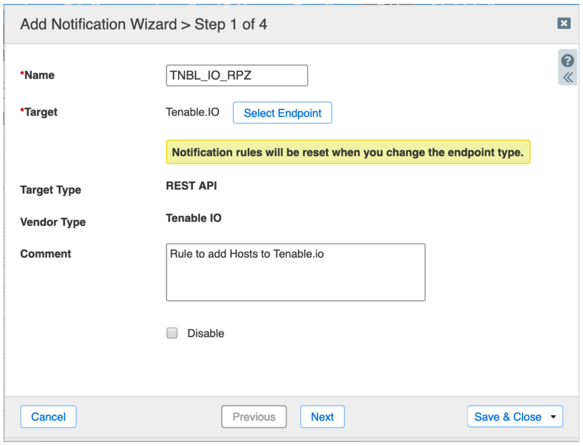
An endpoint and a template must be added before you can add a notification.

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.



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

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

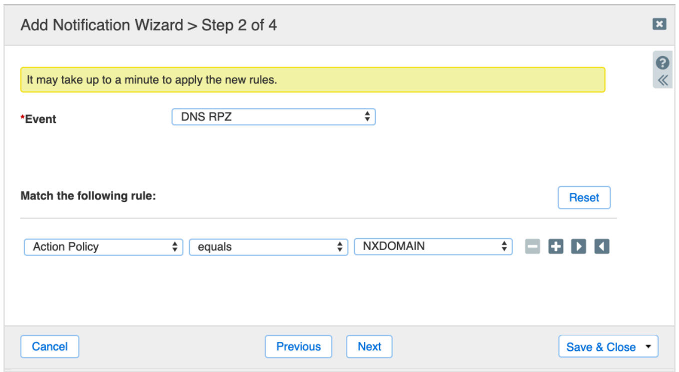
Target Type: REST API

Vendor Type: Tenable IO

Comment: Rule to add Hosts to Tenable.io

□ Disable

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

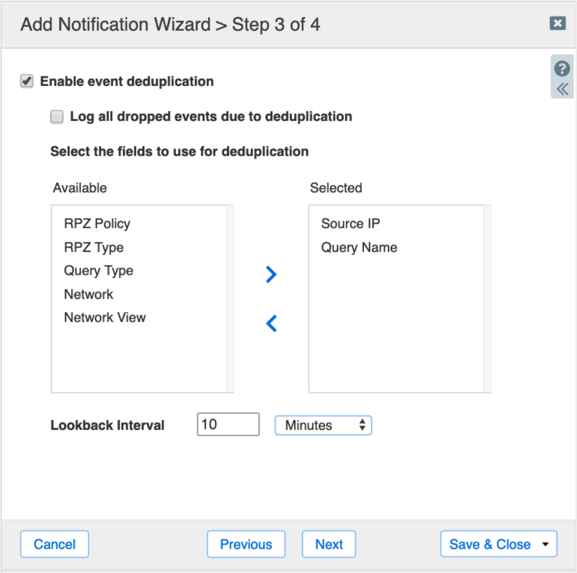
It may take up to a minute to apply the new rules.

*Event: DNS RPZ

Match the following rule:

Action Policy | equals | NXDOMAIN

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

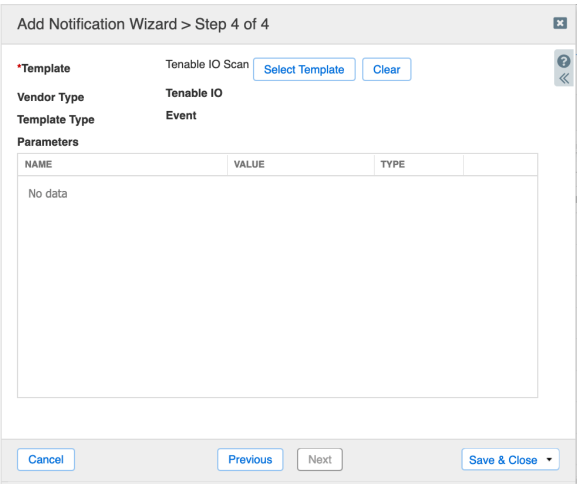
□ Log all dropped events due to deduplication

Select the fields to use for deduplication

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

Lookback Interval: 10 Minutes

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

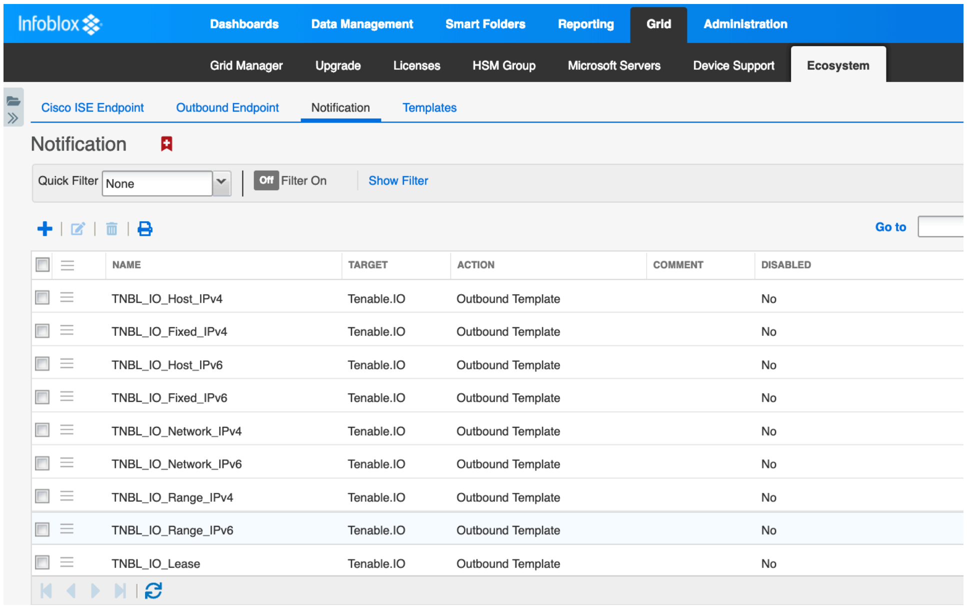
Vendor Type: Tenable IO

Template Type: Event

Parameters

NAME	VALUE	TYPE
No data		

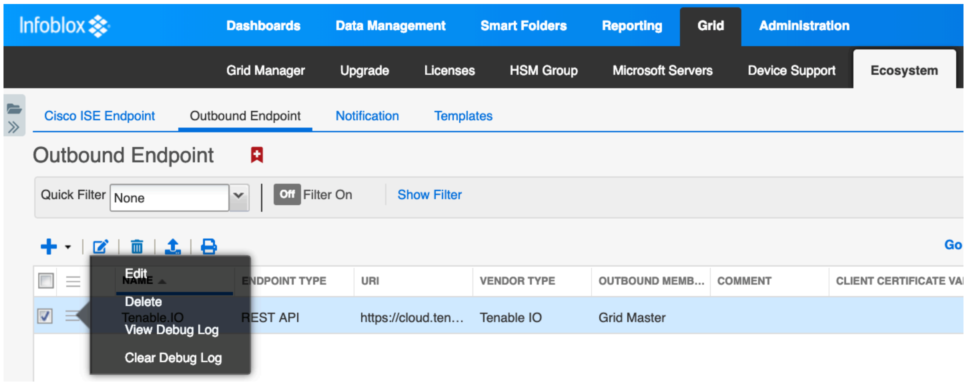
6. Similarly add rules for other events as well.



NAME	TARGET	ACTION	COMMENT	DISABLED
TNBL_IO_Host_IPv4	Tenable.IO	Outbound Template		No
TNBL_IO_Fixed_IPv4	Tenable.IO	Outbound Template		No
TNBL_IO_Host_IPv6	Tenable.IO	Outbound Template		No
TNBL_IO_Fixed_IPv6	Tenable.IO	Outbound Template		No
TNBL_IO_Network_IPv4	Tenable.IO	Outbound Template		No
TNBL_IO_Network_IPv6	Tenable.IO	Outbound Template		No
TNBL_IO_Range_IPv4	Tenable.IO	Outbound Template		No
TNBL_IO_Range_IPv6	Tenable.IO	Outbound Template		No
TNBL_IO_Lease	Tenable.IO	Outbound Template		No

Check the Configuration

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

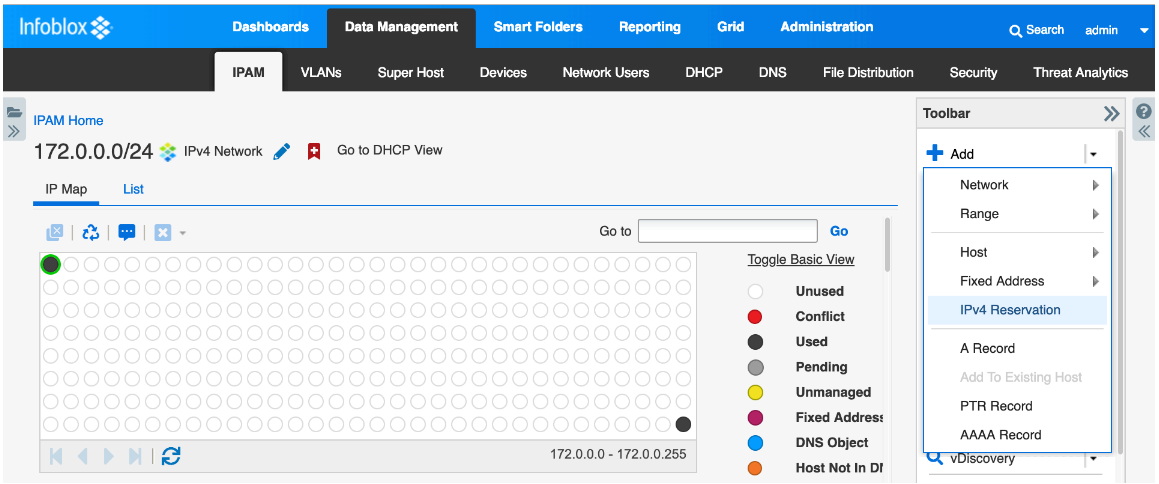


NAME	ENDPOINT TYPE	URI	VENDOR TYPE	OUTBOUND MEMB...	COMMENT	CLIENT CERTIFICATE VA
Tenable.IO	REST API	https://cloud.ten…	Tenable IO	Grid Master		

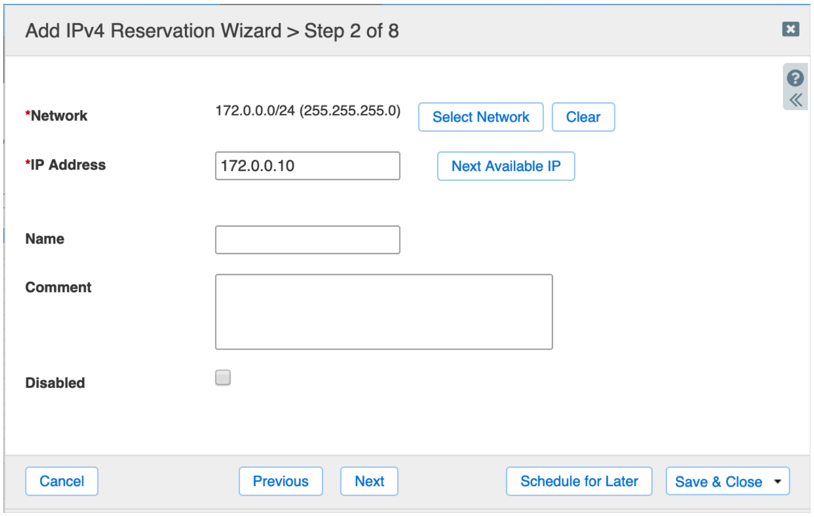
Address Object Management Test

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

1. To create an IPv4 reservation, navigate to **"Data Management" → "IPAM"**. Select an IPv4 network here (say 172.0.0.0/24).
2. Click the drop down next to the **“+ Add”** button under the toolbar and choose **“IPv4 Reservation”**.

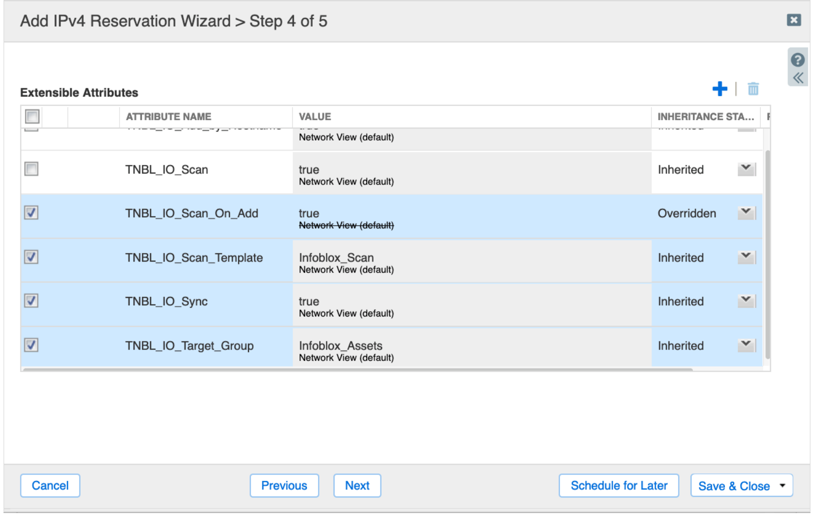


3. Click **“Next”**, then insert the IP **“172.0.0.10”** into the **“IP Address”** field.


Add IPv4 Reservation Wizard > Step 2 of 8

***Network**	172.0.0.0/24 (255.255.255.0)
***IP Address**	172.0.0.10
Name	
Comment	
Disabled	□

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

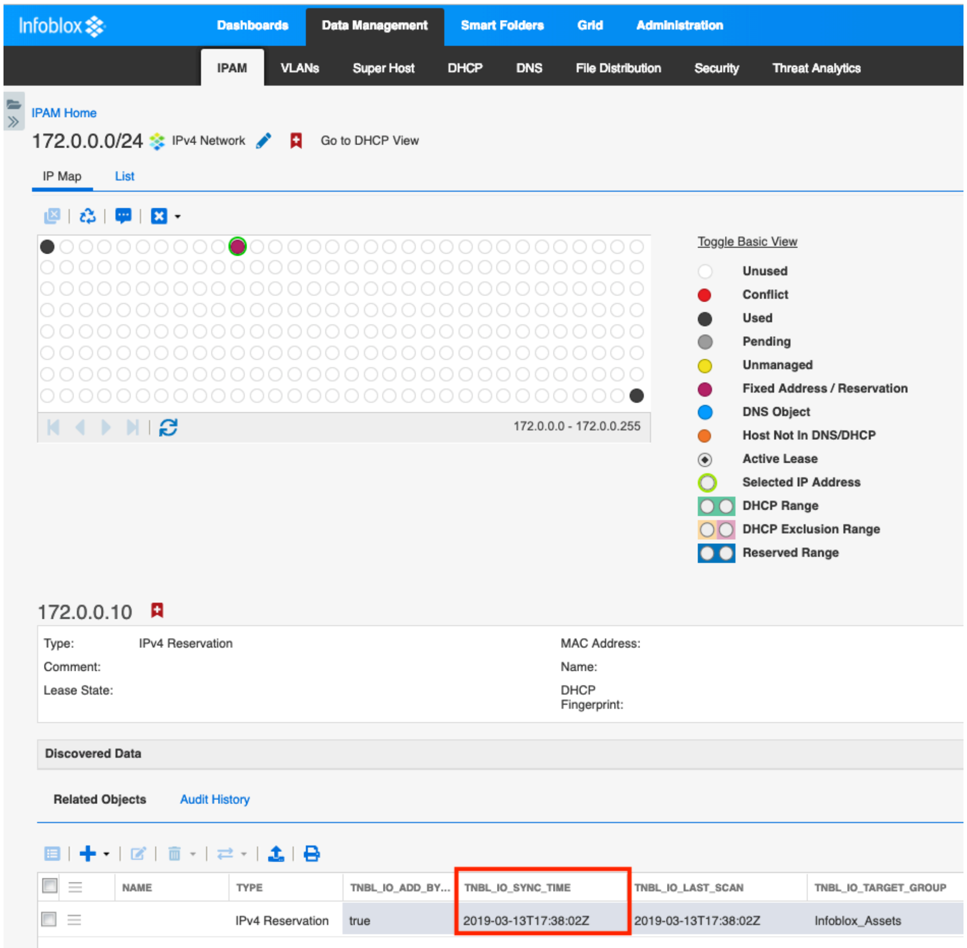

Add IPv4 Reservation Wizard > Step 4 of 5

Extensible Attributes

□	ATTRIBUTE NAME	VALUE	INHERITANCE STA...
		Network View (default)	
□	TNBL_IO_Scan	true Network View (default)	Inherited
☑	TNBL_IO_Scan_On_Add	true ~~Network View (default)~~	Overridden
☑	TNBL_IO_Scan_Template	Infoblox_Scan Network View (default)	Inherited
☑	TNBL_IO_Sync	true Network View (default)	Inherited
☑	TNBL_IO_Target_Group	Infoblox_Assets Network View (default)	Inherited

5. Click **“Save & Close”**.

6. Select the IP and refresh. The **“TNBL_IO_SYNC_TIME”** EA is now updated.



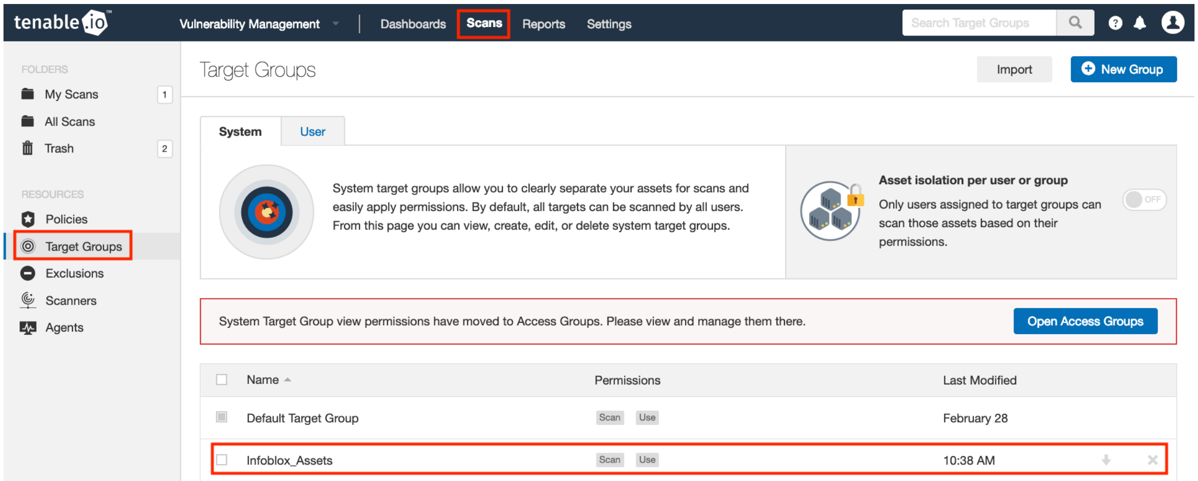
172.0.0.0/24 IPv4 Network Go to DHCP View

172.0.0.10

Type:	IPv4 Reservation
Comment:	
Lease State:	
MAC Address:	
Name:	
DHCP Fingerprint:	

NAME	TYPE	TNBL_IO_ADD_BY...	TNBL_IO_SYNC_TIME	TNBL_IO_LAST_SCAN	TNBL_IO_TARGET_GROUP
	IPv4 Reservation	true	2019-03-13T17:38:02Z	2019-03-13T17:38:02Z	Infoblox_Assets

7. In the Tenable.io, navigate to **“Scans”** **→** **“Target Groups”** then select the target group you sent the asset to. The **“172.0.0.10”** address reservation has been added to the **“Targets”** list. Refresh the page if necessary.



Target Groups

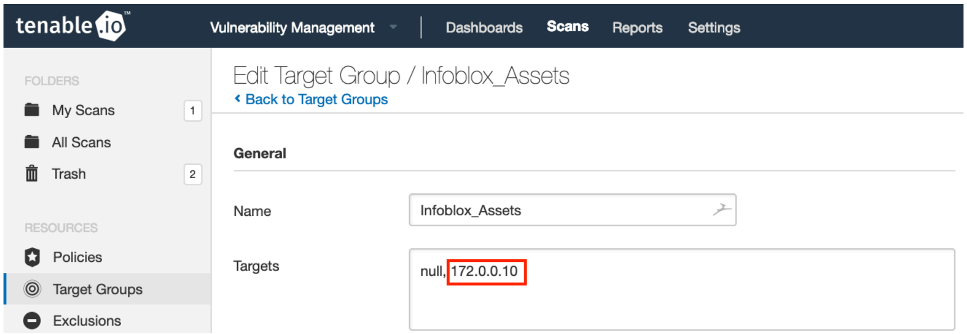
System target groups allow you to clearly separate your assets for scans and easily apply permissions. By default, all targets can be scanned by all users. From this page you can view, create, edit, or delete system target groups.

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.

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



Edit Target Group / Infoblox_Assets

General

Name: Infoblox_Assets

Targets: null, 172.0.0.10

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

NEXT LEVEL NETWORKING

Infoblox is leading the way to next-level DDI with its Secure Cloud-Managed Network Services. Infoblox brings next-level security, reliability and automation to on-premises, cloud and hybrid networks, setting customers on a path to a single pane of glass for network management. Infoblox is a recognized leader with 50 percent market share comprised of 8,000 customers, including 350 of the Fortune 500.

Corporate Headquarters | 3111 Coronado Dr. | Santa Clara, CA | 95054
+1.408.986.4000 | 1.866.463.6256 (toll-free, U.S. and Canada) | info@infoblox.com | www.infoblox.com