

DEPLOYMENT GUIDE

# PAN Firewall & Infoblox NIOS Outbound API Integration

JUNE 2021



# Table of Contents

<b>Introduction</b>	<b>2</b>
<b>Prerequisites</b>	<b>2</b>
Infoblox	2
PAN Firewall	2
<b>Static and Dynamic Address Groups</b>	<b>2</b>
Supported Events for Static Address Groups	3
Supported Events for Dynamic Address Groups	3
<b>Known Limitations</b>	<b>3</b>
<b>Best Practices</b>	<b>3</b>
<b>Workflow</b>	<b>3</b>
<b>Infoblox Community Website Templates</b>	<b>3</b>
<b>Extensible Attributes</b>	<b>4</b>
<b>Session Variables</b>	<b>4</b>
<b>Supported Notifications</b>	<b>4</b>
<b>PAN Firewall Configuration for Static Address Groups</b>	<b>5</b>
<b>PAN Firewall Config for Dynamic Address Groups</b>	<b>10</b>
<b>Infoblox NIOS Configuration</b>	<b>15</b>
Verify Security Ecosystem License is Installed	15
Add/Upload Templates	15
Modify Templates	16
Add a Rest API Endpoint	17
Add Notifications	19
Validate Configuration	21
<b>Appendix</b>	<b>22</b>
Dynamic Address Groups commands	22
Static Address Groups commands	22

## Introduction

The Outbound REST API integration framework from Infoblox provides a mechanism to create updates for both IPAM data (networks, hosts, leases) and DNS threat data into additional ecosystem solutions. Infoblox and Palo Alto Firewall together enable security and incident response teams to leverage the integration of vulnerability scanners 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 Outbound API notifications:

### Infoblox

1. NIOS 8.4 or higher
2. Security Ecosystem license
3. Outbound API integration templates
  - o Available for free download on the Infoblox [community site](#) after creating an account
4. Prerequisites for templates
  - o ex. Configured and set extensible attributes
5. Preconfigured required services
  - o DNS
  - o DHCP
  - o RPZ
  - o Threat Analytics
6. NIOS API user with the following permissions (access via API only)
  - o All Host – R-W
  - o All DHCP Fixed Addresses/Reservations – R-W
  - o All IPv4 Networks – R-W

### PAN Firewall

1. Installed and configured PAN Firewall
  - o Tested with PAN 8.1, 9, and 10
2. User credentials for the PAN Firewall
  - o User requires access to Address and Address group objects within PAN

## Static and Dynamic Address Groups

To simplify the creation of security policies, addresses that require the same security settings can be combined into address groups. An address group can be static or dynamic. Depending on your needs, you may decide that one is better for you (or both). A static address group can include address objects that are static, other dynamic address groups, or both. A dynamic address group populates its members dynamically via tag-based filters.

## Supported Events for Static Address Groups

ADP, RPZ and DNS Tunneling security events are supported (IPv4 only).

Insertion and deletion of IPv4 Fixed, Host, Lease, Reservation and Network events are supported (IPv4 only).

Insertion of Discovery events are supported (IPv4 only).

## Supported Events for Dynamic Address Groups

ADP, RPZ and DNS Tunneling security events are supported (IPv4 & IPv6).

Insertion and deletion of IPv4 and IPv6 Fixed, Host, Lease, and Reservation events are supported (IPv4 & IPv6).

Asset tag EA modification of an address is supported (IPv4 & IPv6).

## Known Limitations

When force rebooting the firewall, it may cause IP to tag mappings loss (Dynamic).

## Best Practices

Outbound API templates are available on the Infoblox [community site](#). 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 NIOS Administration guide about other best practices, limitations, and any detailed information on how to develop notification templates.

## Workflow

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

1. Install the Security Ecosystem license if not already installed.
2. Check that necessary services DHCP, DNS, RPZ, Threat Analytics are configured.
3. Create Extensible Attributes.
4. Create or download appropriate templates from the Infoblox community website: *Palo Alto Dynamic Assets*, *Palo Alto Dynamic Security*, *Palo Alto Static Assets*, *Palo Alto Static Security*, *PaloAlto\_login*, *PaloAlto\_logout*, and *Palo Alto Session*.
5. Add/upload the notification templates.
6. Add a REST API Endpoint.
7. Add Notifications.
8. Emulate an event, then check the debug log and/or verify changes on the REST API Endpoint.

## Infoblox Community Website Templates

Outbound API notifications template is 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 guide. Infoblox does not distribute any templates with the NIOS releases (out-of-box). Templates are available on the Infoblox community website. Templates may

require additional extensible attributes to be created, parameters, or WAPI credentials defined. The required configuration should be provided with a template. Do not forget to apply changes required by the template before testing a notification.

## Extensible Attributes

<i>Name</i>	<i>Description</i>	<i>Type</i>
<i>PaloAlto_Asset_Sync</i>	Serves as toggle to turn on/off sync for Asset Events.	List (true, false)
<i>PaloAlto_Security_Sync</i>	Serves as toggle to turn on/off sync for Security Events	List (true, false)
<i>PaloAlto_Asset_SyncedAt</i>	Update timestamp on an asset event. This attribute is created on the specific IP by the WAPIcall when not present.	String
<i>PaloAlto_Security_SyncedAt</i>	Update timestamp on a security event. This attribute is created on the specific IP by the WAPIcall when not present.	String
<i>PaloAlto_Asset_Tag</i>	[Dynamic Only] - Tag that attaches to an IP in a Dynamic Address Group.	String
<i>PaloAlto_Security_Tag</i>	[Dynamic Only] - Tag that attaches to an IP in a Dynamic Address Group	String
<i>PaloAlto_Timeout</i>	[Dynamic Only] - Starting with PAN-OS 9.0 a tag can contain an optional timeout attribute. Default is 0 (never expires) or a timeout value in seconds for the tag. Maximum timeout is 2592000 (30 days). In older versions of PAN-OS, this attribute cannot be accessed and IPs never timeout.	Integer

## Session Variables

<i>Name</i>	<i>Description</i>
<i>Host_Allow</i>	The static address group object which needs to be populated on the firewall for allowed hosts. This should be the same as the address group object created through the Palo Alto configuration. Set a default value (lbox_Host_Allow).
<i>Host_Deny</i>	The static address group object which needs to be populated on the firewall for denied hosts. This should be the same as the address group object created through the Palo Alto configuration. Set a default value (lbox_Host_Deny).

## Supported Notifications

A notification can be considered as a link between a template, an endpoint, and an event. In the notification properties, you can define the event triggers for the notification, the template to execute, and the external endpoint. The templates support a subset of available notifications. To simplify the deployment, create required notifications and use relevant filters. It is highly recommended to configure deduplication for RPZ events and

exclude a feed that is automatically populated by Threat Analytics. Supported modification events that occur in real time are editing the *PaloAlto\_Asset\_Tag* of an IP. This will remove the old tag from the IP and map the new tag to the IP.

<i>Notification</i>	<i>Description</i>
<i>DNS RPZ</i>	Malicious or unwanted DNS queries
<i>DNS Tunneling</i>	Data exfiltration occurring on the network
<i>Security ADP</i>	Malicious or unwanted DNS queries (via ADP)
<i>Object Change Fixed Address IPv4</i>	Added/Deleted fixed/reserved IPv4 objects
<i>Object Change Host Address IPv4</i>	Added/Deleted host IPv4 objects
<i>Object Change Fixed Address IPv6</i>	[Dynamic Only] - Added/Deleted fixed/reserved IPv6 objects
<i>Object Change Host Address IPv6</i>	[Dynamic Only] - Added/Deleted host IPv6 objects
<i>Object Change Network IPv4</i>	[Static Only] - Added/Deleted network IPv4 objects
<i>Object Change Discovery Data</i>	[Static Only] - Added IPAM Discovery events (via Network Insight)
<i>DHCP Leases</i>	DHCP lease events

## PAN Firewall Configuration for Static Address Groups

A static address group can include address objects that are static, dynamic address groups, or it can be a combination of both address objects and dynamic address groups.

Create appropriate policies in the firewall to allow or deny hosts. A policy requires an existing address group object as part of the policy creation process. Let's create two Static Address Groups for allowing and denying hosts access to the firewall.

1. Login to the PAN Firewall.



- For a Static Address Group, you will need to create a dummy address to fill it with initially. Navigate to **Objects** → **Addresses**. Click **+ Add** at the bottom of the screen.
  - Enter a name, such as the IP. Set the type to **IP Netmask**. Enter **10.0.0/24** for the IP address.

Address

Name

Description

Type   [Resolve](#)

Enter an IP address or a network using the slash notation (Ex. 192.168.80.150 or 192.168.80.0/24). You can also enter an IPv6 address or an IPv6 address with its prefix (Ex. 2001:db8:123:1::1 or 2001:db8:123:1::/64)

Tags

- Create the two Static Address Groups that will hold hosts you wish to either allow or deny firewall access. Let's create the allow group. Navigate to **Objects** → **Address Groups**. Click **+ Add** at the bottom of the screen.
  - Give the Address Group a comprehensible name, such as **lbox\_Host\_Allow**. Set the type to **Static**. Click **+ Add** and select the dummy address you just created. Click **OK**.

Address Group

Name

Description

Type

Addresses  ADDRESS ^  
 10.0.0.0

Tags

4. Now create the deny group. Navigate to **Objects** → **Address Groups**. Click **+ Add** at the bottom of the screen.
  - a) Give the Address Group a comprehensible name, such as **lblox\_Host\_Deny**. Set the type to **Static**. Click **+ Add** and select the dummy address you just created. Click **OK**.

The screenshot shows the 'Address Group' configuration window. The 'Name' field is filled with 'lblox\_Host\_Deny'. The 'Description' field is empty. The 'Type' dropdown is set to 'Static'. The 'Addresses' section shows a table with two rows: one with a checkbox and the text 'ADDRESS ^' and another with a checkbox and the IP address '10.0.0.0'. Below the table are buttons for 'Browse', '+ Add', and '- Delete'. At the bottom of the window are 'OK' and 'Cancel' buttons.

5. Create one policy for each of the Static Address Groups we just created so that PAN knows how to handle inbound hosts. Let's create the policy that will allow Infoblox hosts. Navigate to **Policies** → **Security**. Click **+ Add** at the bottom of the screen.
  - a) Under the **General** tab, name the policy.

The screenshot shows the 'Security Policy Rule' configuration window. The 'Name' field is filled with 'lblox\_AllowHosts'. The 'Rule Type' dropdown is set to 'universal (default)'. The 'Description' field is empty. The 'Tags' dropdown is empty. The 'Group Rules By Tag' dropdown is set to 'None'. The 'Audit Comment' field is empty. At the bottom of the window are 'OK' and 'Cancel' buttons.

- b) Under the **Source** tab, check the **Any** box above the SOURCE ZONE and SOURCE ADDRESS areas. Select **any** from the dropdown above the SOURCE USER and SOURCE DEVICE areas.

The screenshot shows the 'Security Policy Rule' configuration window with the 'Source' tab selected. The 'SOURCE ZONE' and 'SOURCE ADDRESS' fields have a checked 'Any' box above them. The 'SOURCE USER' and 'SOURCE DEVICE' dropdown menus are both set to 'any'. At the bottom, there are 'Add' and 'Delete' buttons for each field, and a 'Negate' checkbox which is unchecked. 'OK' and 'Cancel' buttons are at the bottom right.

- c) Under the **Destination** tab, select **any** from the dropdown above the DESTINATION ZONE and DESTINATION DEVICE areas. Click the **Add** button under the DESTINATION ADDRESS area and select the **Iblox\_Host\_Allow** Address Group created earlier for allowed hosts.

The screenshot shows the 'Security Policy Rule' configuration window with the 'Destination' tab selected. The 'DESTINATION ZONE' and 'DESTINATION DEVICE' dropdown menus are both set to 'any'. The 'DESTINATION ADDRESS' field contains the selected address group 'Iblox\_Host\_Allow'. 'Add' and 'Delete' buttons are visible below each field, and the 'Negate' checkbox is unchecked. 'OK' and 'Cancel' buttons are at the bottom right.

- d) Under the **Actions** tab, set the Action Setting Action to **Allow**. Click **OK**.

The screenshot shows the 'Security Policy Rule' configuration window with the 'Actions' tab selected. Under 'Action Setting', the 'Action' dropdown is set to 'Allow'. Under 'Log Setting', 'Log at Session End' is checked. Under 'Other Settings', 'Profile Type', 'Schedule', and 'QoS Marking' are all set to 'None'. 'Disable Server Response Inspection' is unchecked. 'OK' and 'Cancel' buttons are at the bottom right.

6. Let's create the policy that will deny Infoblox hosts. Navigate to **Policies** → **Security**. Click **+ Add** at the bottom of the screen.

a) Under the **General** tab, name the policy.

Security Policy Rule

General | Source | Destination | Application | Service/URL Category | Actions | Usage

Name: Iblox\_DenyHosts

Rule Type: universal (default)

Description:

Tags:

Group Rules By Tag: None

Audit Comment:

[Audit Comment Archive](#)

OK Cancel

b) Under the **Source** tab, check the **Any** box above the SOURCE ZONE and SOURCE ADDRESS areas. Select **any** from the dropdown above the SOURCE USER and SOURCE DEVICE areas.

Security Policy Rule

General | **Source** | Destination | Application | Service/URL Category | Actions | Usage

Any

SOURCE ZONE ^

Any

SOURCE ADDRESS ^

any

SOURCE USER ^

any

SOURCE DEVICE ^

+ Add - Delete

+ Add - Delete

+ Add - Delete

+ Add - Delete

Negate

OK Cancel

c) Under the **Destination** tab, select **any** from the dropdown above the DESTINATION ZONE and DESTINATION DEVICE areas. Click the **+ Add** button under the DESTINATION ADDRESS area and select the **Iblox\_Host\_Deny** Address Group created earlier for denied hosts.

Security Policy Rule

General | Source | **Destination** | Application | Service/URL Category | Actions | Usage

any

DESTINATION ZONE ^

Any

DESTINATION ADDRESS ^

Iblox\_Host\_Deny

any

DESTINATION DEVICE ^

+ Add - Delete

+ Add - Delete

+ Add - Delete

Negate

OK Cancel

d) Under the **Actions** tab, set the Action Setting Action to **Deny**. Click **OK**.

The screenshot shows the 'Security Policy Rule' configuration window with the 'Actions' tab selected. The 'Action Setting' section has 'Deny' selected in the 'Action' dropdown and 'Send ICMP Unreachable' unchecked. The 'Profile Setting' section has 'None' selected in the 'Profile Type' dropdown. The 'Log Setting' section has 'Log at Session Start' unchecked, 'Log at Session End' checked, and 'Log Forwarding' set to 'None'. The 'Other Settings' section has 'Schedule' set to 'None', 'QoS Marking' set to 'None', and 'Disable Server Response Inspection' unchecked. 'OK' and 'Cancel' buttons are at the bottom right.

7. Click  **Commit** in the upper right corner of the screen. This will activate your newly created Address, Address Groups and Policies on the running configuration of the firewall.

## PAN Firewall Config for Dynamic Address Groups

A dynamic address group populates its members dynamically using tag-based filters. Dynamic address groups are very useful if you have an extensive virtual infrastructure where changes in virtual machine location/IP address are frequent. For example, you have a sophisticated failover setup or provision new virtual machines frequently and would like to apply policy to traffic from or to the new machine without modifying the configuration/rules on the firewall.

Create appropriate policies in the firewall to allow or deny IP addresses. A policy requires an existing address group object as part of the policy creation process. Let's create two Dynamic Address Groups for allowing and denying hosts access to the firewall.

1. Login to the PAN Firewall.
2. Create the two Dynamic Address Groups that will hold hosts you wish to either allow or deny firewall access. Let's create the allow group. Navigate to **Objects** → **Address Groups**. Click  **Add** at the bottom of the screen.
  - a) Give the Address Group a comprehensible name, such as **DynamicAllow**. Set the type to **Dynamic**. To add match criteria, you can either click on  **Add Match Criteria** and select existing static Tags to match the group with (you can create these under **Objects** → **Tags**), or you can type them in manually by putting single quotes around each criterion and separating with terms *and* or *or*. Enter '**allow**' for the match criteria. Click **OK**.

The screenshot shows the 'Address Group' configuration window. The 'Name' field contains 'DynamicAllow'. The 'Description' field contains 'This group allows dynamic IPs.'. The 'Type' dropdown is set to 'Dynamic'. The 'Match' field contains the text ''allow' or 'hello' and 'criteria''. Below the 'Match' field is a blue '+ Add Match Criteria' button. The 'Tags' dropdown is empty. At the bottom right are 'OK' and 'Cancel' buttons.

3. Now create the deny group. Navigate to **Objects → Address Groups**. Click **+ Add** at the bottom of the screen.
  - a) Give the Address Group a comprehensible name, such as **DynamicDeny**. Set the type to **Dynamic**. To add match criteria, you can either click on **+ Add Match Criteria** and select existing static Tags to match the group with (you can create these under **Objects → Tags**), or you can type them in manually by putting single quotes around each criterion and separating with terms *and* or *or*. Enter **'deny'** for the match criteria. Click **OK**.

The screenshot shows the 'Address Group' configuration window. The 'Name' field contains 'DynamicDeny'. The 'Description' field contains 'This group denies dynamic IPs.'. The 'Type' dropdown is set to 'Dynamic'. The 'Match' field contains the text ''deny''. Below the 'Match' field is a blue '+ Add Match Criteria' button. The 'Tags' dropdown is empty. At the bottom right are 'OK' and 'Cancel' buttons.

4. Create one policy for each of the Dynamic Address Groups we just created so that PAN knows how to handle inbound hosts. Let's create the policy that will allow Infoblox hosts. Navigate to **Policies** → **Security**. Click **+ Add** at the bottom of the screen.

a) Under the **General** tab, name the policy.

The screenshot shows the 'Security Policy Rule' configuration window with the 'General' tab selected. The 'Name' field is set to 'DynamicAllow'. The 'Rule Type' is 'universal (default)'. The 'Description' field is empty. The 'Tags' field is empty. The 'Group Rules By Tag' is set to 'None'. The 'Audit Comment' field is empty. There is a link for 'Audit Comment Archive'. At the bottom right, there are 'OK' and 'Cancel' buttons.

b) Under the **Source** tab, check the **Any** box above the SOURCE ZONE and SOURCE ADDRESS areas. Select **any** from the dropdown above the SOURCE USER and SOURCE DEVICE areas.

The screenshot shows the 'Security Policy Rule' configuration window with the 'Source' tab selected. There are four columns for source selection: SOURCE ZONE, SOURCE ADDRESS, SOURCE USER, and SOURCE DEVICE. Each column has a 'Any' checkbox checked. Below each column are 'Add' and 'Delete' buttons. A 'Negate' checkbox is at the bottom. At the bottom right, there are 'OK' and 'Cancel' buttons.

- c) Under the **Destination** tab, select **any** from the dropdown above the DESTINATION ZONE and DESTINATION DEVICE areas. Click the **+ Add** button under the DESTINATION ADDRESS area and select the **Dynamic Allow** Address Group created earlier for allowed hosts.

The screenshot shows the 'Security Policy Rule' configuration window with the 'Destination' tab selected. The 'DESTINATION ZONE' dropdown is set to 'any'. The 'DESTINATION ADDRESS' area has a '+ Add' button and a list containing 'DynamicAllow'. The 'DESTINATION DEVICE' dropdown is also set to 'any'. At the bottom, there are 'Add', 'Delete', and 'Negate' buttons, and 'OK' and 'Cancel' buttons.

- d) Under the **Actions** tab, set the Action Setting Action to **Allow**. Click **OK**.

The screenshot shows the 'Security Policy Rule' configuration window with the 'Actions' tab selected. The 'Action Setting' section has 'Action' set to 'Allow' and 'Send ICMP Unreachable' unchecked. The 'Profile Setting' section has 'Profile Type' set to 'None'. The 'Log Setting' section has 'Log at Session Start' unchecked, 'Log at Session End' checked, and 'Log Forwarding' set to 'None'. The 'Other Settings' section has 'Schedule' and 'QoS Marking' set to 'None', and 'Disable Server Response Inspection' unchecked. At the bottom, there are 'OK' and 'Cancel' buttons.

5. Let's create the policy that will deny Infoblox hosts. Navigate to **Policies** → **Security**. Click **+ Add** at the bottom of the screen.

- a) Under the **General** tab, name the policy.

The screenshot shows the 'Security Policy Rule' configuration window with the 'General' tab selected. The 'Name' field is 'DynamicDeny', 'Rule Type' is 'universal (default)', and 'Description' is empty. The 'Tags' dropdown is empty, 'Group Rules By Tag' is 'None', and 'Audit Comment' is empty. At the bottom, there are 'OK' and 'Cancel' buttons.

- b) Under the **Source** tab, check the **Any** box above the SOURCE ZONE and SOURCE ADDRESS areas. Select **any** from the dropdown above the SOURCE USER and SOURCE DEVICE areas.

- c) Under the **Destination** tab, select **any** from the dropdown above the DESTINATION ZONE and DESTINATION DEVICE areas. Click the **Add** button under the DESTINATION ADDRESS area and select the **DynamicDeny** Address Group created earlier for denied hosts.

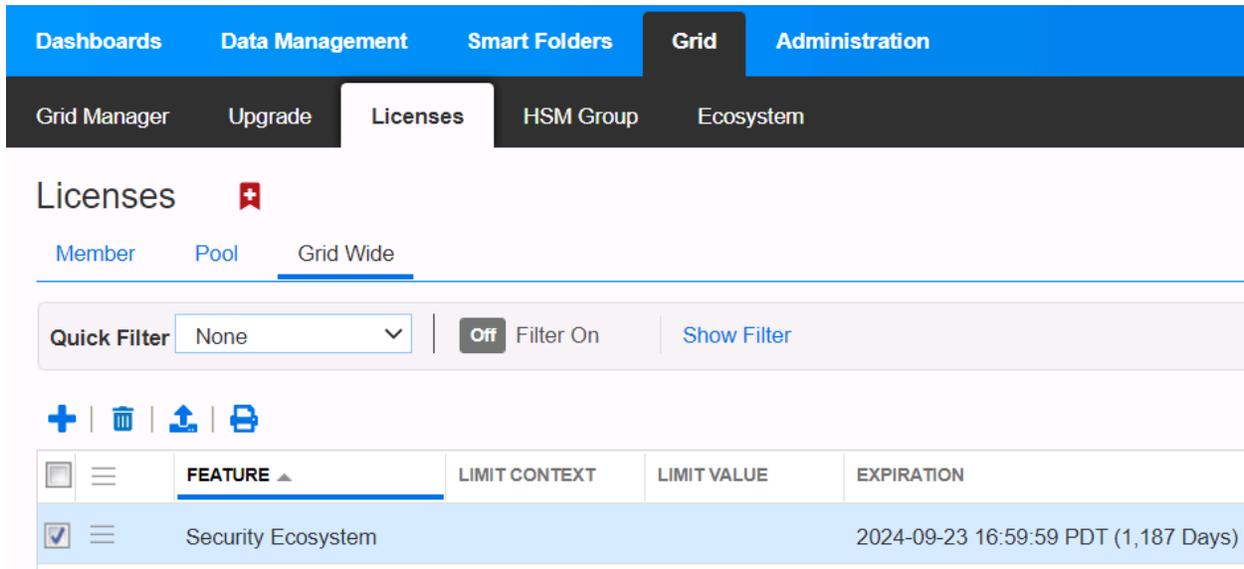
- d) Under the **Actions** tab, set the Action Setting Action to **Deny**. Click **OK**.

- Click  **Commit** in the upper right corner of the screen. This will activate your newly created Address, Address Groups and Policies on the running configuration of the firewall.

## Infoblox NIOS Configuration

### Verify 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. To verify if the license is installed, navigate to **Grid → Licenses → Grid Wide**.



The screenshot shows the Infoblox NIOS interface. The top navigation bar includes 'Dashboards', 'Data Management', 'Smart Folders', 'Grid', and 'Administration'. Under 'Grid', there are sub-menus for 'Grid Manager', 'Upgrade', 'Licenses', 'HSM Group', and 'Ecosystem'. The 'Licenses' page is active, showing tabs for 'Member', 'Pool', and 'Grid Wide'. A 'Quick Filter' dropdown is set to 'None', and a 'Filter On' toggle is set to 'Off'. Below the filter is a table with columns: 'FEATURE', 'LIMIT CONTEXT', 'LIMIT VALUE', and 'EXPIRATION'. The table contains one entry: 'Security Ecosystem' with an expiration date of '2024-09-23 16:59:59 PDT (1,187 Days)'.

	FEATURE ▲	LIMIT CONTEXT	LIMIT VALUE	EXPIRATION
<input checked="" type="checkbox"/>	Security Ecosystem			2024-09-23 16:59:59 PDT (1,187 Days)

### Add/Upload Templates

Add the correct templates from the Infoblox [community site](#).

For all features of PAN Dynamic Address Groups to work, you'll need these templates:

- Palo Alto Dynamic Assets
- Palo Alto Dynamic Security
- PaloAlto\_login
- PaloAlto\_logout
- Palo Alto Session

For all features of PAN Static Address Groups to work, you'll need these templates:

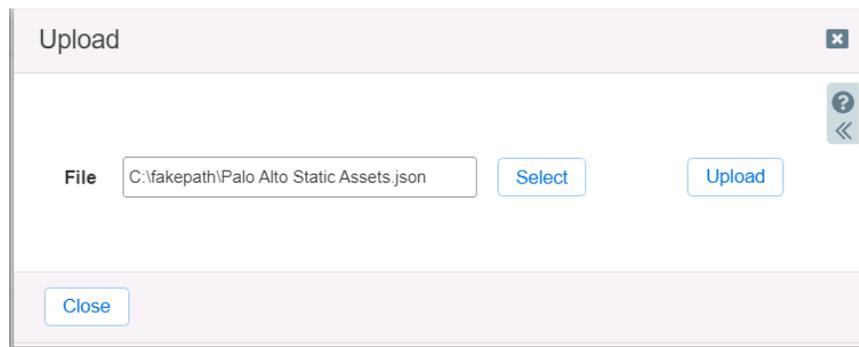
- Palo Alto Static Assets
- Palo Alto Static Security
- PaloAlto\_login
- PaloAlto\_logout
- Palo Alto Session

You can use one or both types of Address Groups simultaneously.

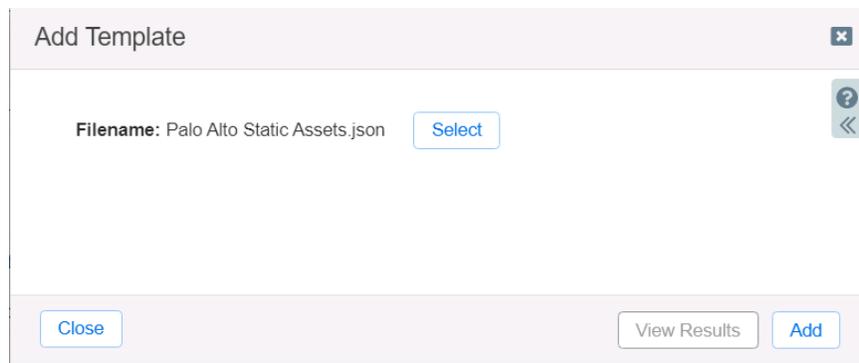
1. Navigate to **Grid → Ecosystem → Templates**. Click **+ Add Template** in the Toolbar or the **+ Add** button.
2. In the *Add Template* window that appears, click **Select**.



3. Click **Select** again in the *Upload* window that appears and browse for the template file you wish to add (.json or .txt). Click **Upload**.



4. Click **Add** again in the *Add Template* window.

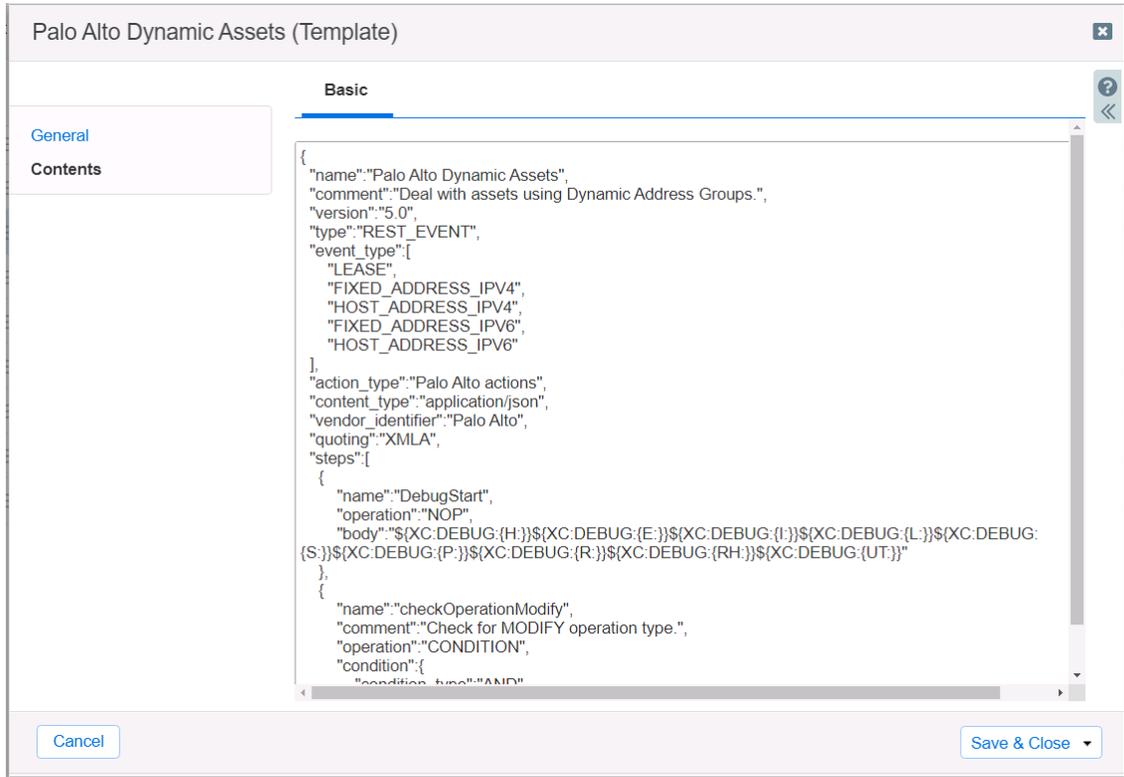


5. Repeat steps 1-4 for all other desired templates.

## Modify Templates

NIOS provides the ability to modify the templates via the web interface. 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. Copy the text into a text editor of your choice for major editing. **NOTE: You cannot delete a template if it is used by an endpoint or by a notification.**

1. Navigate to **Grid → Ecosystem → Templates**. Click the  hamburger button next to the name of the template you wish to modify then click **Edit**, or select it and click the  edit button.
2. Edit the template as you wish.



## Add a Rest API Endpoint

A REST API Endpoint is a remote system which receives 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 (ex. for testing purposes).

In this integration, the PAN Firewall is the endpoint. Let's add the endpoint.

1. Navigate to **Grid → Ecosystem → Outbound Endpoint**. Click the  **Add** button and select **Add REST API Endpoint**.
2. Fill in all the fields as required.  
*NOTE: The **Auth Username** and **Auth Password** are the credentials of the PAN Firewall. The **WAPI Integration Username** and **WAPI Integration Password** are the credentials of your NIOS grid.*
3. Click **Test Connection**.  
*NOTE: This only checks TCP communication with the URI. It does not verify authentication.*

Palo Alto Networks (REST API Endpoint)

**Basic**

General  
Session Management  
Extensible Attributes

\*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 
  
 Current Grid Master

Comment:

Disable

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

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

- Under the Session Management tab, set the Log Level to **Debug** for debug purposes during initial configuration.

Palo Alto Networks (REST API Endpoint)

**Basic**

General  
**Session Management**  
Extensible Attributes

Timeout:

Log Level:

Template:  [Select Template](#) [Clear](#)

Vendor Type: **Palo Alto**

Template Type: **Session Management**

Parameters

NAME	VALUE	TYPE
Host_Deny	lbox_Host_Deny	String
Host_Allow	lbox_Host_Allow	String

## Add Notifications

A notification is a link between a template, an endpoint, and an event. In the notification you define the event which triggers the notification, executed template, and the API endpoint of which the Grid will establish a connection. To simplify deployment, create only required notifications and use relevant filters. It is highly recommended to configure deduplication for RPZ events and exclude a feed automatically populated by Threat Analytics. **NOTE: when using Test Rule, rules for that notification apply.**

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

1. Navigate to **Grid → Ecosystem → Notification**. Click **+ Add Notification Rule** in the Toolbar or the **+ Add** button.
2. Enter a **Name** and select the **Target Endpoint**. You cannot change the name later. Click **Next**.

Add Notification Wizard > Step 1 of 4

\*Name: PAN\_Host\_IPv4\_Static

\*Target: Palo Alto Networks [Select Endpoint](#)

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

Target Type: REST API

Vendor Type: Palo Alto

Comment:

Disable

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

3. Select the **Event** and define **rules** that will trigger the Outbound API template to execute. Rules act as a filter in which only when they are satisfied will the template execute. You can choose to match all rules or any of multiple. Click **Next**. **NOTE: For optimal performance, it is best practice to make the rule filter as narrow as possible.**

Add Notification Wizard > Step 2 of 4

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

\*Event

Match the following rule:

4. Select **Enable event deduplication** if desired and applicable. Click **Next**.
5. Select the desired/applicable template to execute. Click **Save & Close**.

Add Notification Wizard > Step 4 of 4

\*Template

Vendor Type

Template Type

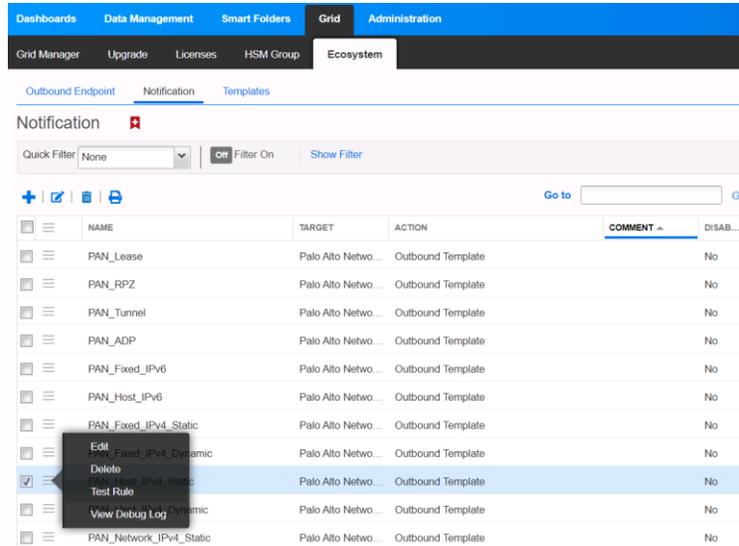
Parameters

NAME	VALUE	TYPE
No data		

## Validate Configuration

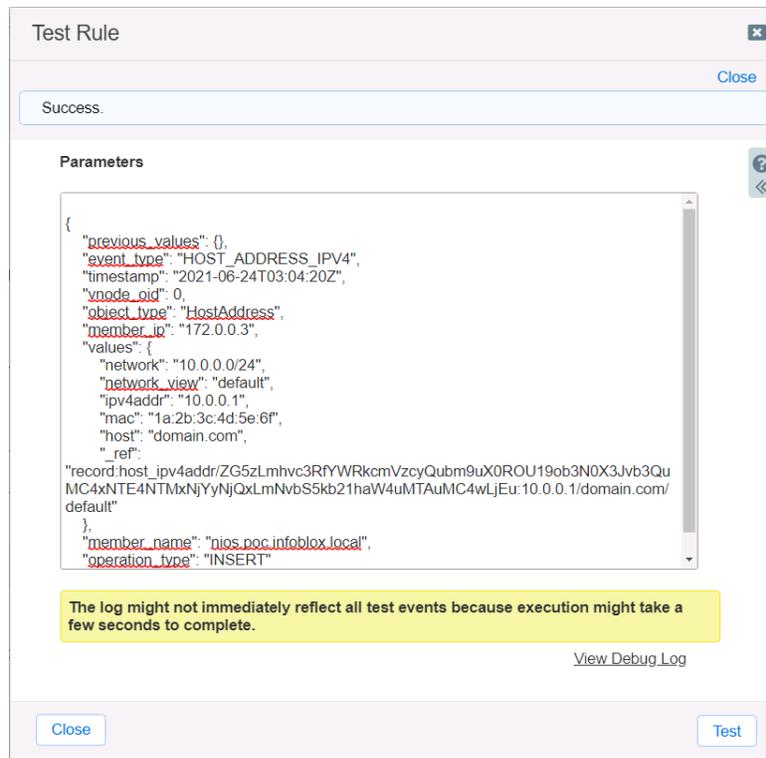
NIOS provides the ability to simulate an event for which a notification was created for. Let's test a notification.

1. Navigate to **Grid** → **Ecosystem** → **Notification**. Click the  hamburger button next to the name of the notification you wish to verify then click **Test Rule**.



	NAME	TARGET	ACTION	COMMENT	DISAB...
<input type="checkbox"/>	PAN_Lease	Palo Alto Netwo...	Outbound Template		No
<input type="checkbox"/>	PAN_RPZ	Palo Alto Netwo...	Outbound Template		No
<input type="checkbox"/>	PAN_Tunnel	Palo Alto Netwo...	Outbound Template		No
<input type="checkbox"/>	PAN_ADP	Palo Alto Netwo...	Outbound Template		No
<input type="checkbox"/>	PAN_Fixed_IPv6	Palo Alto Netwo...	Outbound Template		No
<input type="checkbox"/>	PAN_Host_IPv6	Palo Alto Netwo...	Outbound Template		No
<input type="checkbox"/>	PAN_Fixed_IPv4_Static	Palo Alto Netwo...	Outbound Template		No
<input type="checkbox"/>	Edit PAN_Fixed_IPv4_Dynamic	Palo Alto Netwo...	Outbound Template		No
<input checked="" type="checkbox"/>	Delete PAN_Fixed_IPv4_Static	Palo Alto Netwo...	Outbound Template		No
<input type="checkbox"/>	View Debug Log PAN_Fixed_IPv4_Dynamic	Palo Alto Netwo...	Outbound Template		No
<input type="checkbox"/>	PAN_Network_IPv4_Static	Palo Alto Netwo...	Outbound Template		No

2. Modify test parameters as desired. Click **Test**. Click **View Debug Log** to view the debug log and verify the event was successful. **NOTE: You may not see the event reflect in PAN if the appropriate parameters are not set, such as the EAs. Test with a real event to fully validate the whole configuration.**



```
{
  "previous_values": {},
  "event_type": "HOST_ADDRESS_IPV4",
  "timestamp": "2021-06-24T03:04:20Z",
  "vnode_oid": 0,
  "object_type": "HostAddress",
  "member_ip": "172.0.0.3",
  "values": {
    "network": "10.0.0.0/24",
    "network_view": "default",
    "ipv4addr": "10.0.0.1",
    "mac": "1a:2b:3c:4d:5e:6f",
    "host": "domain.com",
    "ref": ""
  },
  "record_host_ipv4addr/ZG5zLmhvc3RfYWVRkcmVzcyQubm9uX0ROU19ob3N0X3Jvb3QuMC4xNTE4NTMxNjYyNjQxLmNvbS5kb21haW4uMTAuMC4wLjEu:10.0.0.1/domain.com/default",
  "member_name": "nios.poc.infoblox.local",
  "operation_type": "INSERT"
}
```

The log might not immediately reflect all test events because execution might take a few seconds to complete.

[View Debug Log](#)

## Appendix

Alternatively curl commands can be used to create Palo Alto objects.

### Dynamic Address Groups commands

1. Command to register tag to an IP:

```
curl -k https://[firewall]/api/?key=[key]&type=user-id&cmd=<uid-  
message><version>2.0</version><type>update</type><payload><register><entry  
ip="[addressIP]"><tag><member>[tag]</member></tag></entry></register></payload></uid-message>
```

#### **For example:**

```
https://172.0.0.10/api/?key=xxxxx&type=user-id&cmd=<uid-  
message><version>2.0</version><type>update</type><payload><register><entry  
ip="10.0.0.1"><tag><member>allow</member></tag></entry></register></payloa  
d></uid-message>
```

2. Command to unregister tag from an IP:

```
curl -k https://[firewall]/api/?key=[key]&type=user-id&cmd=<uid-  
message><version>2.0</version><type>update</type><payload><unregister><e  
ntry ip="[IP-  
address]"><tag><member>[tag]</member></tag></entry></unregister></payload  
></uid-message>
```

### Static Address Groups commands

1. Command to add address to list of addresses:

```
curl -k  
https://[firewall]/api/?key=[key]&type=config&action=set&xpath=/config/shared/addr  
ess/entry[@name=' [address name]'&element=<ip-netmask>[addressIP]</ip-netmask>
```

#### **For example:**

```
https://172.0.0.10/api/?key=xxxxx&type=config&action=set&xpath=/config/shared/address/  
entry[@name='10.0.0.0']& element=<ip-netmask>10.0.0.0</ip-netmask>
```

2. Commands to add address to static address group:

```
curl -k https://[firewall]/api/?key=[key]&action=set&xpath=/config/shared/address-  
group/entry[@name=' [address group  
name]'&element=<static><member>[addressIP]</member></static>
```

```
curl -k https://172.0.0.10/api/?key=xxxxx&action=set&xpath=/config/shared/address-  
group/entry[@name='IBlox_Host_Allow']&element=<static><member>10.0.0.0 </member></static>
```

3. Commit to firewall:

```
curl -k https://[firewall]/api/?key=[key]& type=commit&cmd=<commit><force></force></commit>
```



Infoblox is the leader in modern, cloud-first networking and security services. Through extensive integrations, its solutions empower organizations to realize the full advantages of cloud networking today, while maximizing their existing infrastructure investments. Infoblox has over 12,000 customers, including 70% of the Fortune 500.

Corporate Headquarters | 2390 Mission College Boulevard, Ste. 501 | Santa Clara, CA | 95054  
+1.408.986.4000 | [info@infoblox.com](mailto:info@infoblox.com) | [www.infoblox.com](http://www.infoblox.com)



© 2021 Infoblox, Inc. All rights reserved. Infoblox logo, and other marks appearing herein are property of Infoblox, Inc. All other marks are the property of their respective owner(s).