

Deployment Guide

# Integration with Aruba ClearPass

Outbound API

## Contents

Introduction .....	3
Prerequisites .....	3
Known Limitations .....	3
Best Practices.....	3
Configuration .....	4
Workflow .....	4
Before you get Started .....	4
Download Templates from the Infoblox Community Web-Site .....	4
Editing Instance Variables.....	5
Supported Notification .....	5
Infoblox Permissions .....	5
Aruba ClearPass Configuration .....	6
Adding Attributes .....	6
Adding Operator Profile (Permissions).....	7
Adding API Client .....	8
Enable Insight.....	9
Infoblox NIOS Configuration .....	10
Check if the Security Ecosystem License is Installed .....	10
Add/Upload Templates.....	10
Modifying Templates .....	12
Adding Client Secret and Client ID.....	13
Add a Rest API Endpoint.....	14
Add a Notification .....	15
Check the Configuration .....	17
Summary .....	19
Additional Integrations.....	19

## Introduction

### Infoblox and Aruba ClearPass: Securing Network Access Control

From IoT to an always-on mobile workforce, organizations face increasingly complex IT infrastructures that are more exposed to attacks than ever before. By combining Infoblox's DNS security and network visibility with Aruba's control on the network, users can automate their network.

- **Visibility, Control, Response:**  
Malicious insiders and IoT-based attacks continue to grow, bypassing your perimeter security defenses. With Infoblox and Aruba integration you are able to automate the defense.
- **Certified secure. The best defense for wired and wireless connections:**  
Malware have become increasingly intelligent, using the DNS in over 90% of its campaigns. With Infoblox and Aruba integration you are more protected then ever from DNS attacks and data exfiltration via DNS.
- **Identify what's on your multi-vendor wired and wireless network:**  
Automatic population of your Aruba ClearPass endpoints list with Mac address's that are found by Infoblox so that you can see every network asset with unmatched clarity, context, and insight.

The integration was developed in collaboration with HPE Aruba.

## Prerequisites

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

- 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, Threat Analytics, Threat Protection, Network Discovery.
  - NIOS API user with the following permissions (access via API only):
    - All Host – RW.
    - All IPv4 DHCP Fixed Addresses/Reservations – RW.
    - IPv6 DHCP Fixed Addresses/Reservations – RW.
- Aruba
  - Aruba ClearPass 6.7 or higher.
  - Configured API client with client credentials.
  - Enable Insight

## Known Limitations

The current templates support DNS Firewall (RPZ), Advanced DNS Protection (ADP), Network Discovery, Threat Insight (DNS Tunneling), Host IPv4, Host IPv6, Fixed address IPv4, Fixed address IPv6, and lease events only. The asset management template does not support IPAM DB DELETE events and does not delete endpoints from Aruba ClearPass. It is possible to modify the template and add support for DELETE event.

Only assets with MAC address can be synchronized to Aruba ClearPass Policy Manager.

## Best Practices

Outbound API templates can be found on the Infoblox community site on the partners integration page. After registering an account, you can subscribe to the relevant groups and forums. If additional templates come out they will be found on the community site.

For production systems, it is highly recommended to set the log level for an end-point to **“Info”** or higher (**“Warning”**, **“Error”**).

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

- Aruba:
  1. Add Aruba ClearPass Attributes.
  2. Add an API Client.
  3. Enable Insight.
- 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, RPZ, Threat Analytics, Threat Protection and Discovery.
  3. Create the required Extensible Attributes.
  4. Download (or create your own) notification templates (Aruba\_Security.json, Aruba\_Assets.json, Aruba\_Login.json, Aruba\_Logout.json, Aruba\_Session.json) from the Infoblox community web-site.
  5. Add the templates.
  6. Add a REST API Endpoint.
  7. Add Notifications.
  8. Emulate an event, check Rest API debug log and/or verify changes on the grid.

### Before you get Started

#### Download Templates from the Infoblox Community 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 Aruba 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.

*Table 1. Extensible Attributes*

Extensible Attributes	Description
<b>Aruba_LastSecurityEvent</b>	Provides the last time a security event was sent to Aruba ClearPass.
<b>Aruba_Location</b>	Custom field. Determines the location field for the Aruba ClearPass endpoint upon creation.
<b>Aruba_Secure</b>	True or False. Defines if security attributes should be updated/added to an endpoint.
<b>Aruba_Sync</b>	True or False. Defines if an asset should be added to Aruba ClearPass.

<b>Aruba_SyncedAt</b>	Provides the last time an asset was added/modified on Aruba ClearPass.
-----------------------	--

### Editing Instance Variables

Aruba ClearPass templates use an instance variable 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*

<b>Instance Variable</b>	<b>Description</b>
<b>ThreatSeverity</b>	Defines the severity of threats on endpoints on Aruba ClearPass. Possible values: Unknown, Low, Medium, High, Critical

### 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, the template which is executed and the API endpoint to which NIOS will establish the connection. The Aruba ClearPass 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 3. Supported Notifications*

<b>Notification</b>	<b>Description</b>
DNS RPZ	DNS queries that are Malicious or unwanted
DNS Tunneling	Data exfiltration that occurs on the network
DHCP Leases	Lease events that occur on the network
Object Change Fixed Address IPv4	Added/Modified fixed/reserved IPv4 objects.
Object Change Fixed Address IPv6	Added/Modified fixed/reserved IPv6 objects.
Object Change Host Address IPv4	Added/Modified Host IPv4 objects.
Object Change Host Address IPv6	Added/Modified Host IPv6 objects.
Security ADP	Advanced DNS Protection events
Network Discovery	Object Change Discovery Data

### Infoblox Permissions

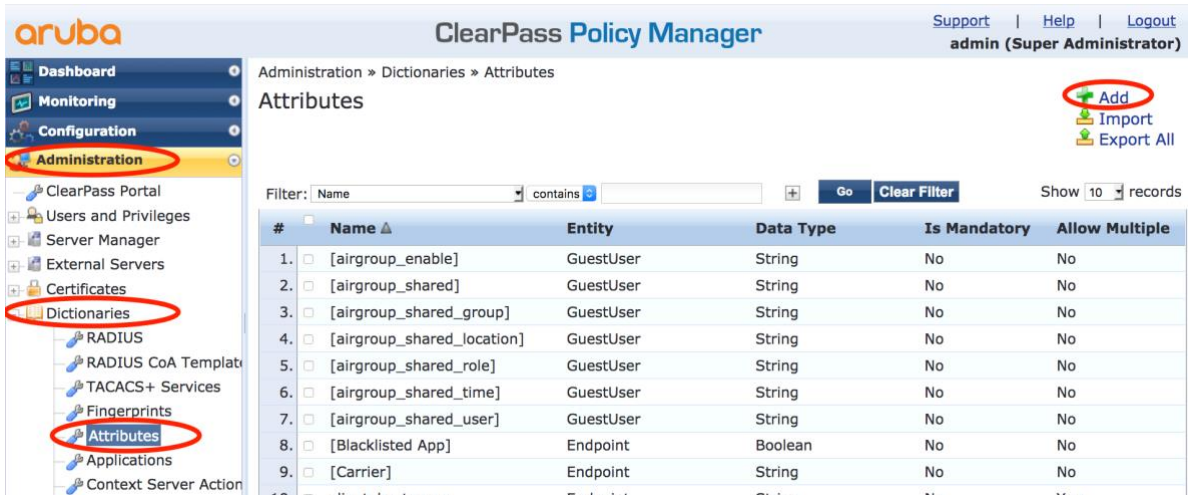
The Infoblox and Aruba ClearPass integration requires a few permissions for the integration to work. Navigate to **"Administration" → "Administrators"** and add a **"Roles"**, **"Permissions"**, **"Groups"** and **"Admins"** to include permissions that are required for the integrations. When creating a new group, under the **"Groups"** tab, select the **"API"** interface under the **"Allowed Interfaces"** category.

# Aruba ClearPass Configuration

## Adding Attributes

The Infoblox and Aruba ClearPass integration requires endpoint attributes that may not be already created. In order to add the attributes:

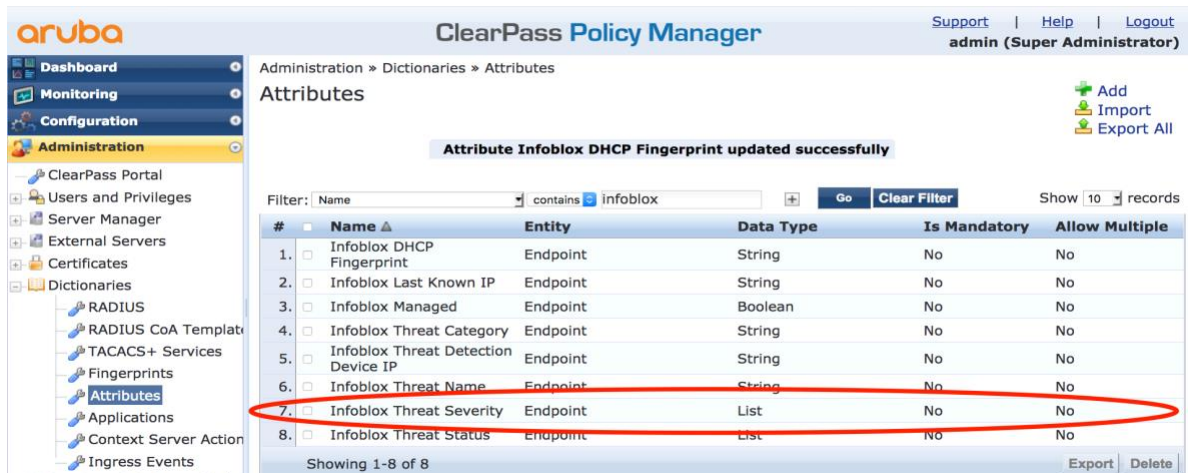
1. Navigate to **“Administration”** → **“Dictionaries”** → **“Attributes”**, then click Add.



2. In the **“Add Attribute”** window, set the Entity field to Endpoint, add the correct name to the Attribute, select the correct **“Data Type”**, set **“Is Mandatory”** to **“No”**, set the Allow Multiple to **“No”**, Enter the Default Values and then click **“Add”**.

The 'Add Attribute' form is shown with the following values:

- Entity: Endpoint
- Name: Infoblox Threat Severity
- Data Type: String
- Is Mandatory: No
- Allow Multiple: No
- Default Value (optional): Unknown,Low,Medium,High,Critical (Enter String without special characters e.g., firstfloor)



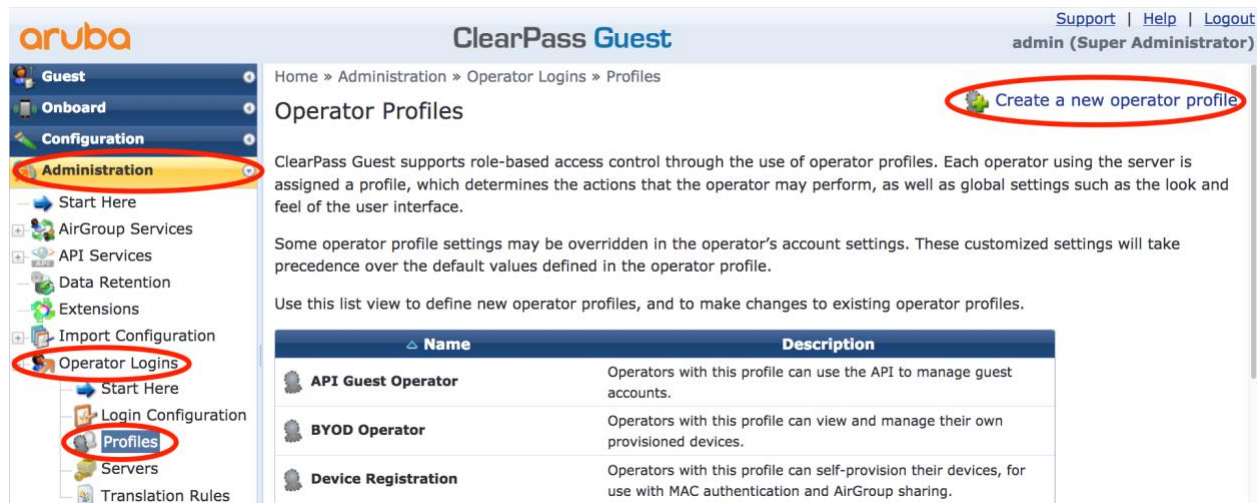
Repeat the above step and add the attributes from the table below.

Table 4. Aruba Attributes

Field Name	Data Type	Description
Infoblox DHCP Fingerprint	String	DHCP fingerprint of the device if known
Infoblox Last Known IP	String	IP address registered in IPAM
Infoblox Managed	Boolean	IPAM management status: managed or unmanaged.
Infoblox Threat Category	String	Threat type that occurred on the device.
Infoblox Threat Detection Device IP	String	IP of the DNS server that detected the threat.
Infoblox Threat Name	String	Requested domain name
Infoblox Threat Severity	List	Severity of the incident
Infoblox Threat Status	List	The current resolved/unresolved status of the threat.
Infoblox RuleId	Integer	The ID of the rule
Infoblox RuleCategory	Text	The category to which the rule belongs.

### Adding Operator Profile (Permissions)

1. Inside the ClearPass Guest Manager navigate to “Administration” → “Operator Logins” → “Profiles” and click “Create a new operator profile”.



2. Enter the name of the operator profile and then select the “Custom” option from the drop down of the operator privileges that are found in the list below.

**Operator Profile Editor**

Name:  Enter a name for this operator profile.

Description:  Comments or descriptive text about the operator profile.

**Access**  
These options control what operators with this profile are permitted to do.

Enabled:  Allow operator logins  
If unchecked, operators with this profile will not be able to log in.

**Privileges:**

- Administrator** No Access
- Advertising Services** No Access
- AirGroup Services** No Access
- API Services** No Access
- Guest Manager** No Access
- Hotspot Manager** No Access
- Insight** No Access
- IP Phone Services** No Access
- Onboard** No Access
- Operator Logins** No Access
- Pass Services** No Access
- Platform** No Access
- Policy Manager** No Access
- SMS Services** No Access
- SMTP Services** No Access
- Support Services** No Access
- Translation Assistant** No Access

Show descriptions

Table 5. Aruba Operator Privileges

Privilege	Custom Name	Access
Administrator	Plugin Manager	Full
API Services	Allow API Access	Allow Access
Guest Manager	Active Sessions	Full
Guest Manager	Active Sessions History	Read Only
Guest Manager	Create Multiple Guest Accounts	Full
Guest Manager	Create New Guest Account	Read Only
Guest Manager	Full User Control	Read Only
Insight	Administration	Read
Policy Manager	Identity – Endpoints	Read, Write

### Adding API Client

1. Inside the ClearPass Guest Manager navigate to **“Administration”** → **“API Services”** → **“API Clients”** and click Create API client.



aruba ClearPass Guest [Support](#) | [Help](#) | [Logout](#)  
admin (Super Administrator)

Home » Administration » API Services » API Clients

**API Clients**

The API clients you have defined are listed below.

Client ID	Grant Types	Access Token	Operator Profile
Blox	password	30 minutes	Super Administrator
BloxCS	client_credentials	1 weeks	Super Administrator

[Create API client](#)  
[Revoke all access tokens](#)  
[API Explorer](#)  
[API sample code on GitHub](#)

[Back to API services](#)  
[Back to administration](#)  
[Back to main](#)

Administration  
 Start Here  
 AirGroup Services  
 API Services  
 Start Here  
 API Clients  
 API Explorer  
 SOAP Web Servi  
 Data Retention  
 Extensions  
 Import Configuration  
 Operator Logins  
 Plugin Manager  
 Support

- On the “**Create API Client**” form, add the “**Client ID**”, set the “**Operator Profile**” to a “**Profile**” with the correct permissions, set the “**Grant Type**” to “**Client credentials (grant\_type=client\_credentials)**” and Remember the “**Client Secret**” key for later.

**Create API Client**

\* Client ID:   
The unique string identifying this API client. Use this value in the OAuth2 "client\_id" parameter.

Description:   
Use this field to store comments or notes about this API client.

Enabled:  Enable API client

\* Operator Profile:   
The operator profile applies role-based access control to authorized OAuth2 clients. This determines what API objects and methods are available for use.

\* Grant Type:   
Only the selected authentication method will be permitted for use with this client ID.

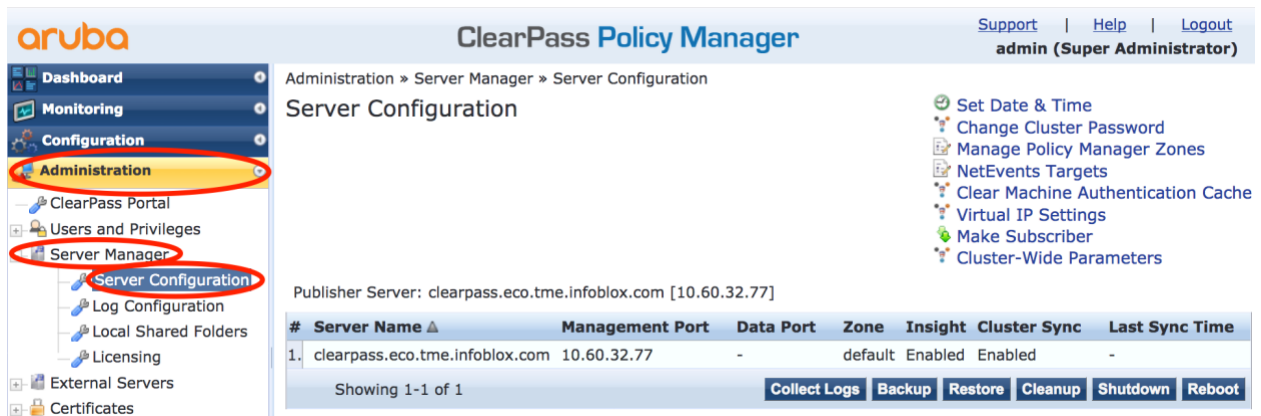
Client Secret: **fMB16YHyd2ky0P13XePTtGRQU/qqpZ8P4oTYhAO1K+YL**  
Use this value in the OAuth2 "client\_secret" parameter.  
NOTE: This value is encrypted when stored and cannot be displayed again.

Access Token Lifetime:    
Specify the lifetime of an OAuth2 access token.

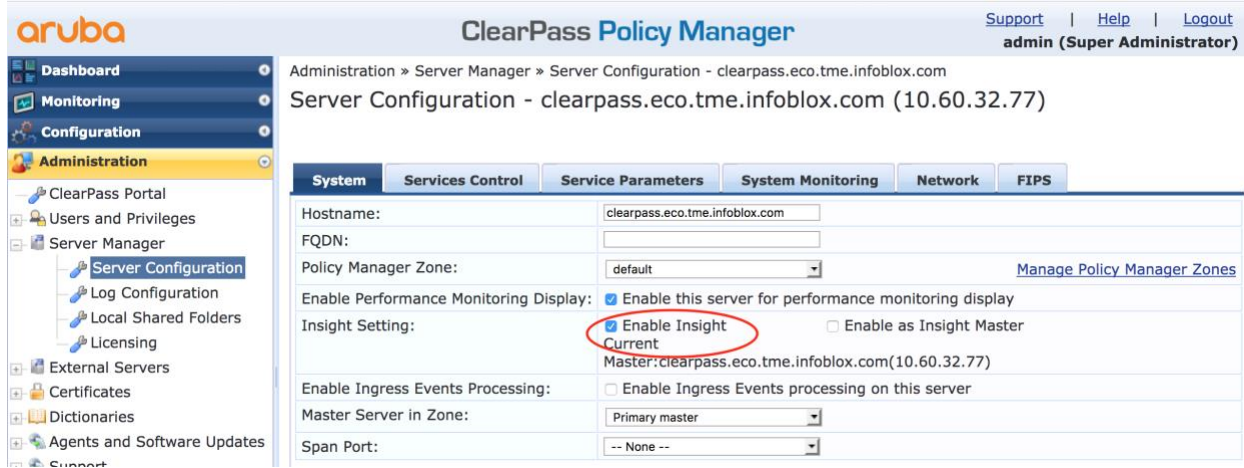
- Click “**Create API Client**” when finished.

### Enable Insight

- Inside the ClearPass Policy Manager navigate to “**Administration**” → “**Server Manager**” → “**Server Configuration**” and click the Aruba ClearPass server name to edit it.



2. On the “System” tab click the check box to “Enable Insight Current”.



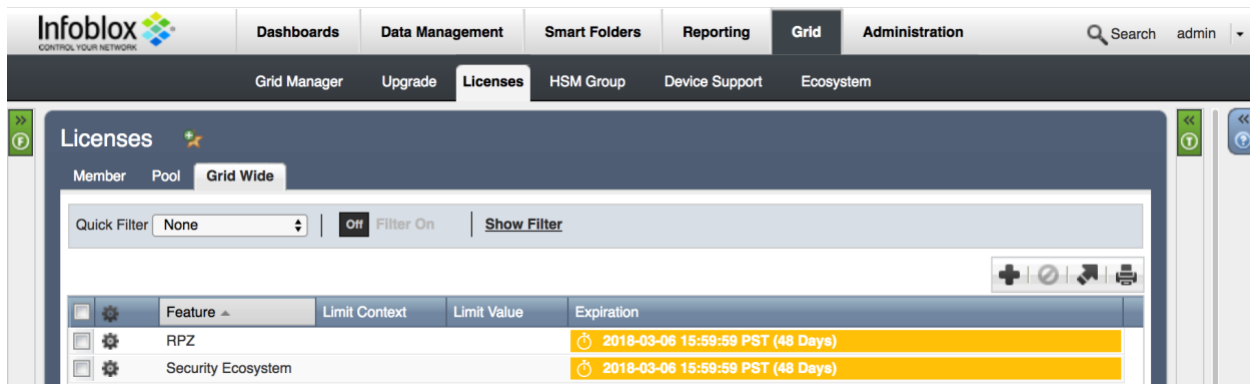
3. Click save on the bottom right of the window to save the settings.

## 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.

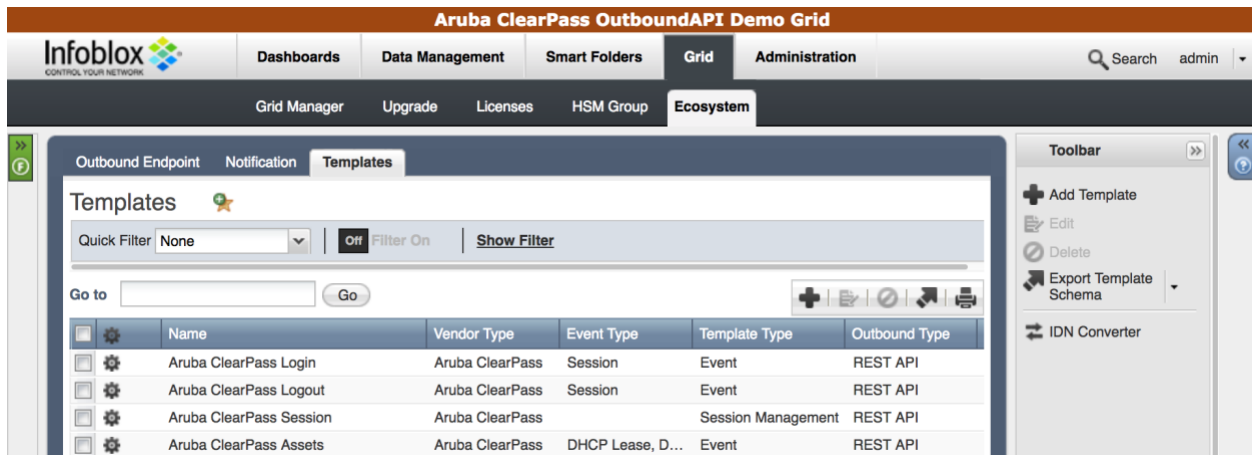
In order to check if the license was installed navigate to “**Grid**” → “**Licenses**” → “**Grid Wide**”.



## Add/Upload Templates

In order to upload/add templates:

1. Navigate to “Grid” → “Ecosystem” → “Templates”, and press “+” or “+ Add Template”.



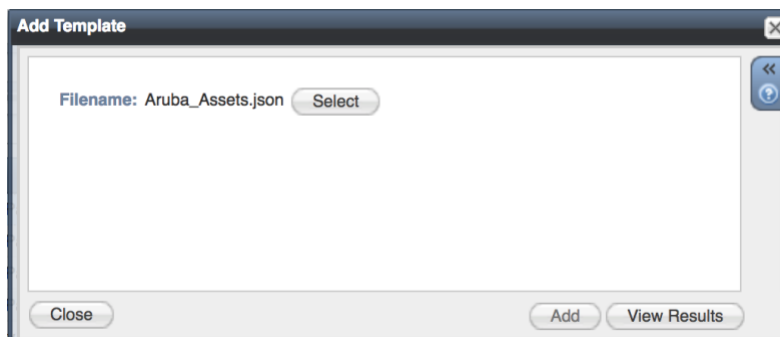
2. Press the “Select” button on the “Add template” window.



3. If a template was previously uploaded, press “Yes” to overwrite the template.



4. Press the “Select” button on the “Upload” window. The standard file selection dialog will open.
5. Select the file and press the “Upload” button on the “Upload” window.
6. Press the “Add” button and the template will be added/uploaded.
7. You can review the uploaded results in the syslog or by pressing the “View Results” button.



Syslog Preview

Template validation events for grid master infoblox.localdomain Go to Syslog Viewer

Timestamp	Server	Message
2018-02-27 07:...	OutboundAPI...	----- import completed -----
2018-02-27 07:...	OutboundAPI...	Template name: Aruba ClearPass Security
2018-02-27 07:...	OutboundAPI...	File: Aruba_Security.json
2018-02-27 07:...	OutboundAPI...	User: admin
2018-02-27 07:...	OutboundAPI...	----- import started -----
2018-02-27 07:...	OutboundAPI...	----- import completed -----
2018-02-27 07:...	OutboundAPI...	Template name: Aruba ClearPass Assets
2018-02-27 07:...	OutboundAPI...	File: Aruba_Assets.json
2018-02-27 07:...	OutboundAPI...	User: admin
2018-02-27 07:...	OutboundAPI...	----- import started -----
2018-02-27 07:...	OutboundAPI...	----- import completed -----
2018-02-27 07:...	OutboundAPI...	Template name: Aruba ClearPass Logout
2018-02-27 07:...	OutboundAPI...	File: Aruba_Logout.json
2018-02-27 07:...	OutboundAPI...	User: admin
2018-02-27 07:...	OutboundAPI...	----- import started -----

Close

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

## Modifying Templates

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

1. Navigate to **“Grid”** → **“Ecosystem”** → **“Templates”**, and then press the gear icon next to the template you want to modify.
2. Press the **“Edit”** button to open up the **“Template”** window.

Aruba ClearPass Assets (Template)

Basic

General

Contents

Name\* Aruba ClearPass Assets

Type REST API

Vendor Type Aruba ClearPass

Event Type DHCP Lease, DB Change  
DHCP Fixed Address IPv4,  
DB Change DNS Host  
Address IPv4, DB Change  
DHCP Fixed Address IPv6,  
DB Change DNS Host  
Address IPv6

Template Type Event

Comment

Cancel Save & Close

Aruba ClearPass Assets (Template)

Basic

General

Contents

```
{
  "vendor_identifier": "Aruba ClearPass",
  "version": "3.0",
  "name": "Aruba ClearPass Assets",
  "content_type": "application/json",
  "type": "REST_EVENT",
  "event_type": [
    "LEASE",
    "FIXED_ADDRESS_IPV4",
    "HOST_ADDRESS_IPV4",
    "FIXED_ADDRESS_IPV6",
    "HOST_ADDRESS_IPV6"
  ],
  "headers": {
    "Authorization": "Bearer ${S:A:SESSIONID}",
    "Accept": ""
  },
  "instance_variables": [
  ],
  "steps": [
    {
      "name": "Debug#0",
      "operation": "NOP"
    }
  ]
}
```

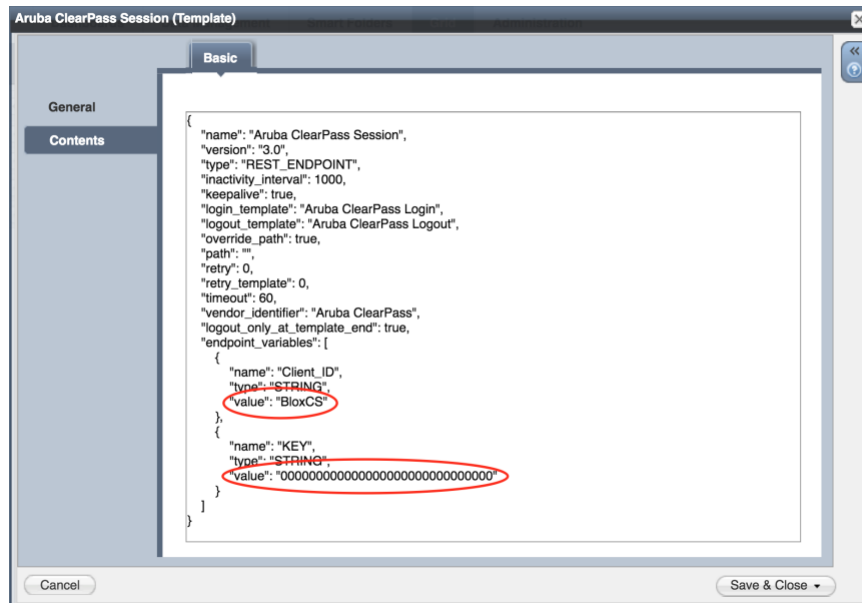
Cancel Save & Close

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.

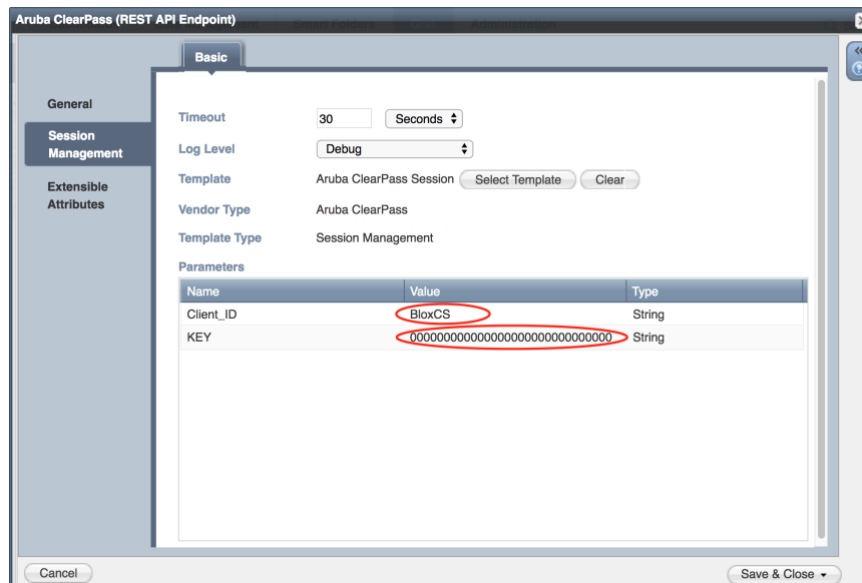
**Note: You cannot delete a template if it is used by an endpoint or by a notification.**

### Adding Client Secret and Client ID

1. Navigate to **“Grid”** → **“Ecosystem”** → **“Templates”** and then press the gear icon next to the **“Aruba\_Session.json”** template and click edit to modify it.
2. Inside the **“Aruba\_Session.json”** template insert the **“Client Secret”** key into the **“value”** field of the **“endpoint\_variables”** with the name **“KEY”**.
3. Inside the **“Aruba\_Session.json”** template insert the **“Client ID”** value into the **“value”** field of the **“endpoint\_variables”** with the name **“Client\_ID”**.



4. (NIOS 8.3 or later) Navigate to **“Grid”** → **“Ecosystem”** → **“Outbound Endpoint”** and click on the Aruba ClearPass endpoint and click **“Edit”**.
5. (NIOS 8.3 or later) Navigate to the **“Session Management”** tab and add the **“Client\_ID”** and **“KEY”** to the value fields.

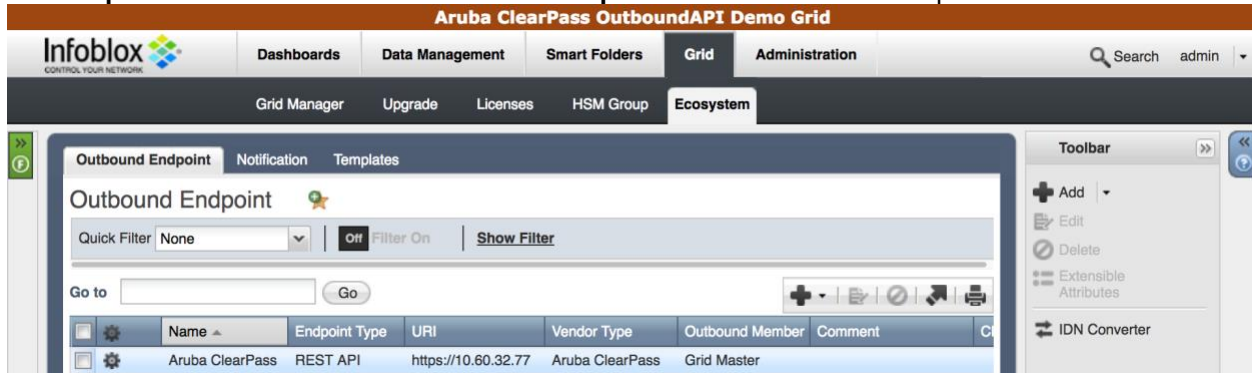


## Add a Rest API Endpoint

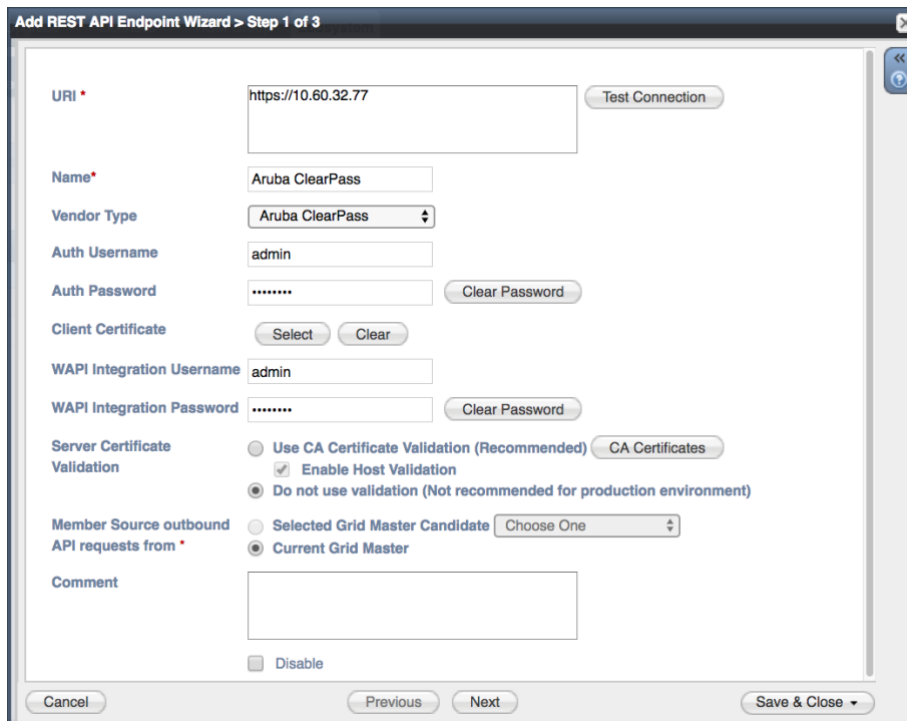
A **“REST API Endpoint”** is basically a remote system which should receive changes based on a notification and a configured template. A Grid, for example, can not only send notifications, it can also receive the notifications from itself (e.g. for testing purposes).

In order to add REST API Endpoints:

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



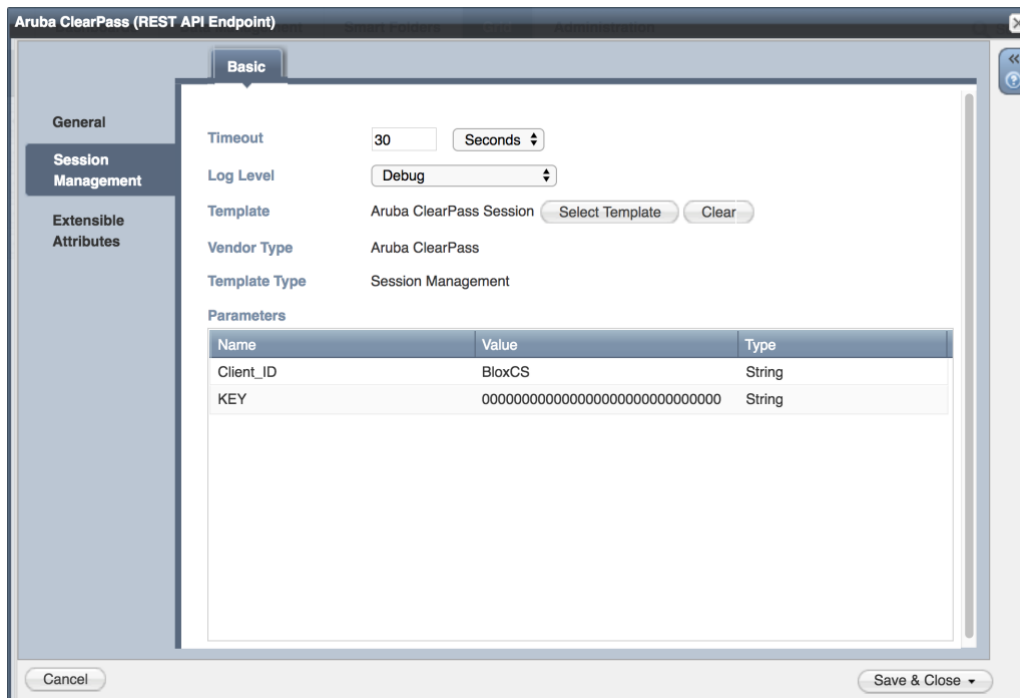
2. The URI and Name for the appliance you are integrating with are required.
3. The URI should be the IP of the appliance you are integrating with, with the correct URI scheme.
4. Specify **“Auth Username”**, **“Auth Password”** (Aruba Web Service account credentials), **“WAPI Integration Username”** and **“WAPI Integration Password”** (NIOS credentials).

The screenshot shows the 'Add REST API Endpoint Wizard - Step 1 of 3' dialog box. It contains the following fields and options:

- URI \***: https://10.60.32.77 (with a 'Test Connection' button)
- Name \***: Aruba ClearPass
- Vendor Type**: Aruba ClearPass (dropdown)
- Auth Username**: admin
- Auth Password**: masked with dots (with a 'Clear Password' button)
- Client Certificate**: Select and Clear buttons
- WAPI Integration Username**: admin
- WAPI Integration Password**: masked with dots (with a 'Clear Password' button)
- 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 (dropdown)
  - Current Grid Master
- Comment**: empty text area
- Disable

At the bottom are 'Cancel', 'Previous', 'Next', and 'Save & Close' buttons.

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



6. The Client\_ID and the KEY can be found when you create the Aruba ClearPass API client.

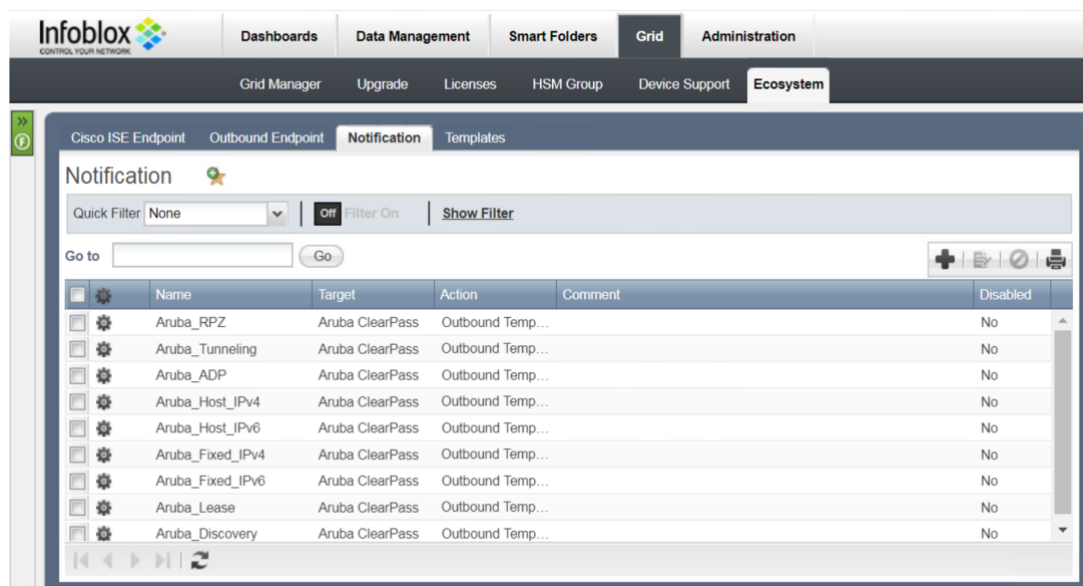
When possible, it is recommended to send notifications from a Grid Master Candidate instead of from the Grid Master.

### 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 press **“+”** 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 \*** Aruba\_RPZ

**Target \*** Aruba ClearPass

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

**Target Type** REST API

**Vendor Type** Aruba ClearPass

**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

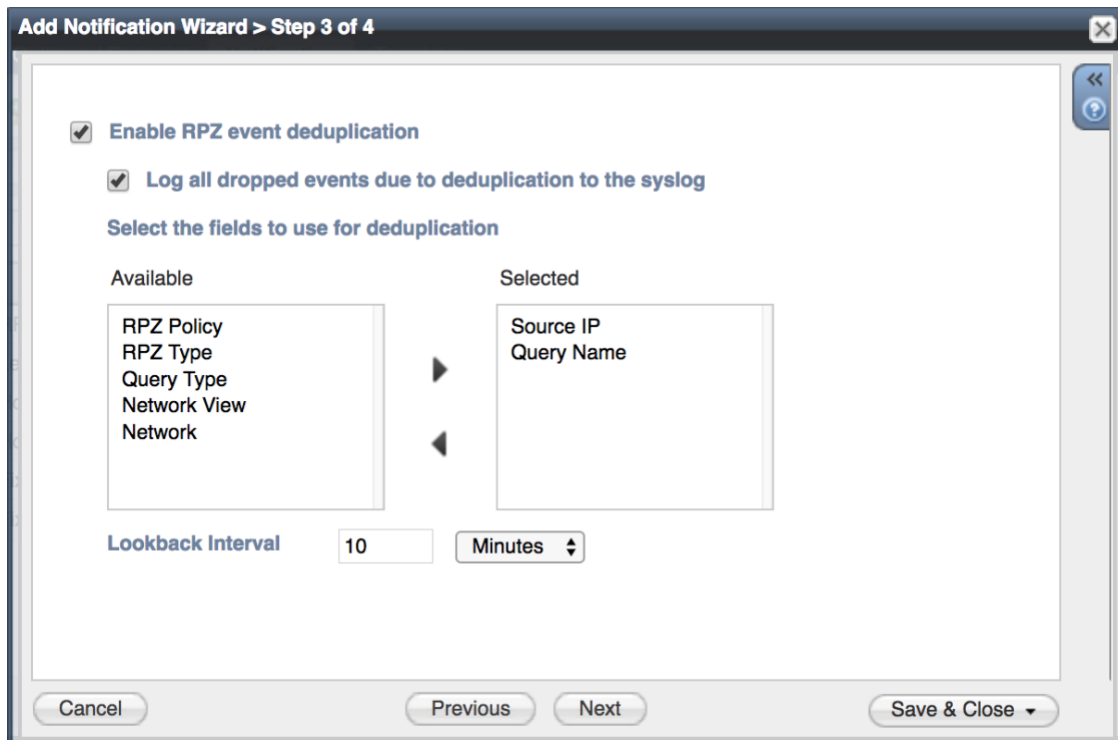
**Match the following rule:**

Rule Name contains local.rpz

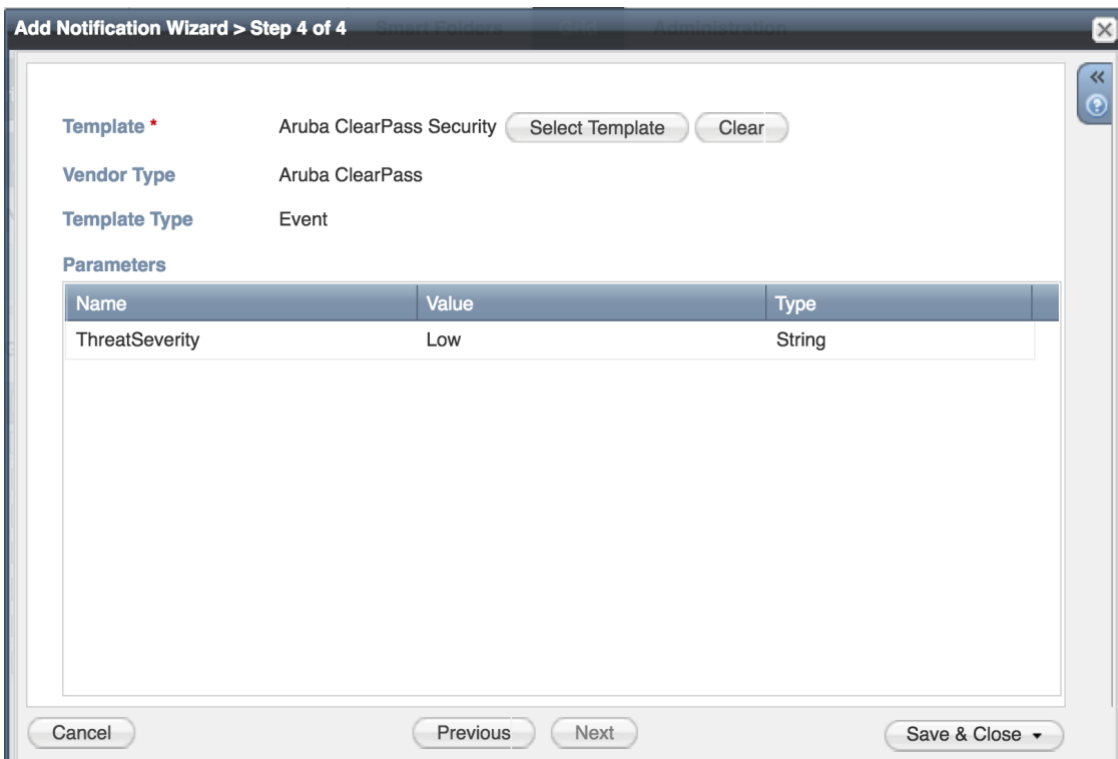
Cancel Previous Next Save & Close ▾

4. (For RPZ notifications only) Check **“Enable RPZ event deduplication”** and specify relevant parameters. Click **“Next”**.



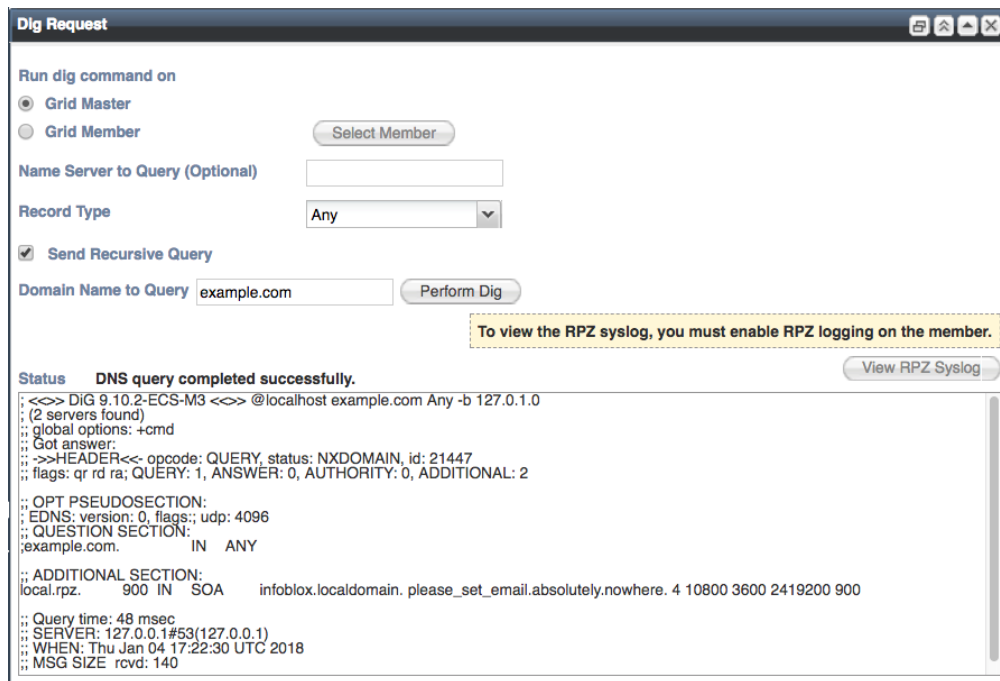


5. Select a relevant template and specify the template's parameters if any are required. Click **“Save & Close”**.

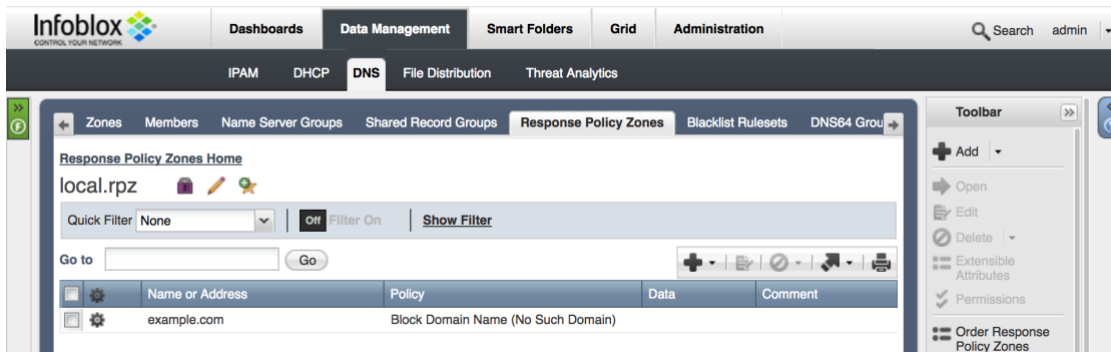


### Check the Configuration

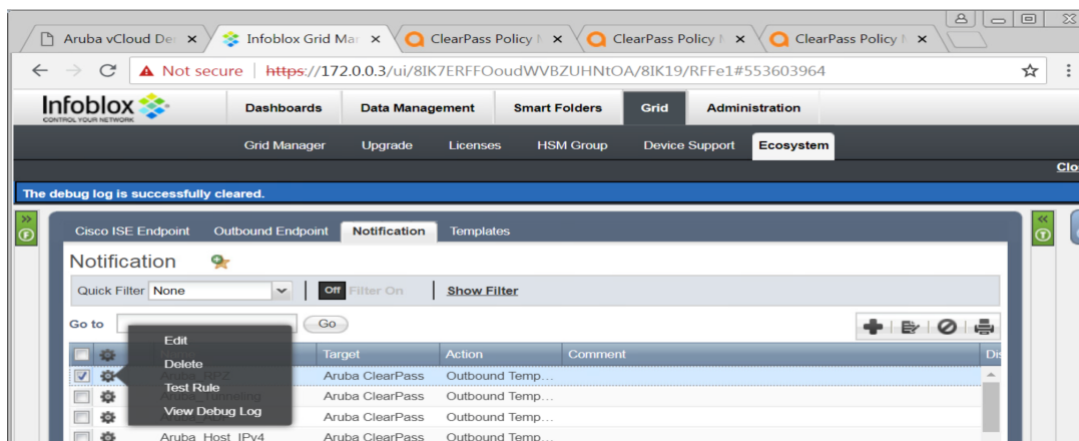
You can emulate an event for which a notification was added by going to **“DashBoards”** → **“Status”** → **“Security”** then on the **“Dig Request”** panel, fill in the **“Domain Name to Query”** text box and click the **“Perform Dig”** button.



When performing the dig request above, make sure that the “Domain Name to Query” is blocked by your RPZ. To check this, navigate to “Data Management” → “DNS” → “Response Policy Zone”. You can export a RPZ feed or check the content of a local RPZ.



To check a debug log for an endpoint, go to “Grid” → “Ecosystem” → “Notification”, click on the gear wheel and select “View Debug Log”.



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

## Summary

The integration solution from Infoblox and Aruba ClearPass Modernizes your IT service by giving increased Visibility, control, and responses with the best defense for wired and wireless devices and Increased Identification on what on your multivendor wired and wireless network.

## Additional Integrations

1. Integrating ClearPass with Infoblox typically tags the username context, as well as the external device being authenticated, along with its respective MAC address, which further simplifies IP address management on the Infoblox side.

[http://www.arubanetworks.com/techdocs/ClearPass/6.7/PolicyManager/Content/CPPM\\_UserGuide/Admin/EndPointContextServersAdd\\_Infoblox.htm](http://www.arubanetworks.com/techdocs/ClearPass/6.7/PolicyManager/Content/CPPM_UserGuide/Admin/EndPointContextServersAdd_Infoblox.htm)

2. This integration allows ClearPass to send Username and Mac Address mapping information to Infoblox's Mac Address Filters.

[https://community.arubanetworks.com/aruba/attachments/aruba/ForoenEspanol/1861/1/ClearPass\\_Exchange\\_Integration\\_Tech\\_Note\\_Infoblox\\_Mac\\_Address\\_Filter\\_Updates.pdf](https://community.arubanetworks.com/aruba/attachments/aruba/ForoenEspanol/1861/1/ClearPass_Exchange_Integration_Tech_Note_Infoblox_Mac_Address_Filter_Updates.pdf)

3. This integration authenticates a device on Aruba ClearPass and then based on data received from Infoblox through an enforcement profile puts the device onto a chosen network.

<https://github.com/aruba/clearpass-exchange-snippets/tree/master/ipam/infoblox-authz>