Infoblox
NEXT LEVEL NETWORKING

Deployment Guide

Infoblox Integration with Aruba ClearPass

Table of Contents

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 integrated together you are able to automate your defense.
- **Certified secure. The best defense for wired and wireless connections:**

  Malware has become increasingly intelligent, using DNS in over 90% of attacks. With Infoblox and Aruba integrated together you are more protected than ever from DNS attacks like data exfiltration.
- **Identify what's on your multi-vendor wired and wireless network:**

  Automatic population of your Aruba ClearPass endpoints list with MAC addresses that are found by Infoblox so that you can see every network asset with unmatched clarity, context and insight.

This integration was developed in collaboration with HPE Aruba.

Prerequisites

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

- Infoblox
  - NIOS 8.3
  - 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.

Only assets with MAC addresses can be added, modified or deleted from Aruba ClearPass Policy Manager. All IPv6 assets require a MAC address acquired via Network Discovery.

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**"). As with any change to your network, it is also highly recommended to test all changes before implementing them into production.

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 Website

Outbound API templates are an essential part of the configuration. Templates fully control the integration and steps required to execute the outbound notifications. Detailed information on how to develop templates can be found in the NIOS Administrator's guide.

Infoblox does not distribute any templates (out-of-the-box) with the NIOS releases. Templates are available on the Infoblox community website. Templates for the 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
Aruba_LastSecurityEvent	Provides the last time a security event was sent to Aruba ClearPass.
Aruba_Location	Custom field. Determines the location field for the Aruba ClearPass endpoint upon creation.
Aruba_Secure	True or False. Defines if security attributes should be updated/added to an endpoint.
Aruba_Sync	True or False. Defines if an asset should be added to Aruba ClearPass.
Aruba_SyncedAt	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

Instance Variable	Description
ThreatSeverity	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

Notification	Description
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 or Deleted fixed/reserved IPv4 objects
Object Change Fixed Address IPv6	Added, Modified or Deleted fixed/reserved IPv6 objects
Object Change Host Address	Added, Modified or Deleted IPv4 Added/Modified Host IPv4 objects
Object Change Host Address	Added, Modified or Deleted IPv6 Added/Modified Host IPv6 objects
Security ADP	Advanced DNS Protection events
Network Discovery	Object Change Discovery Data

Infoblox Permissions

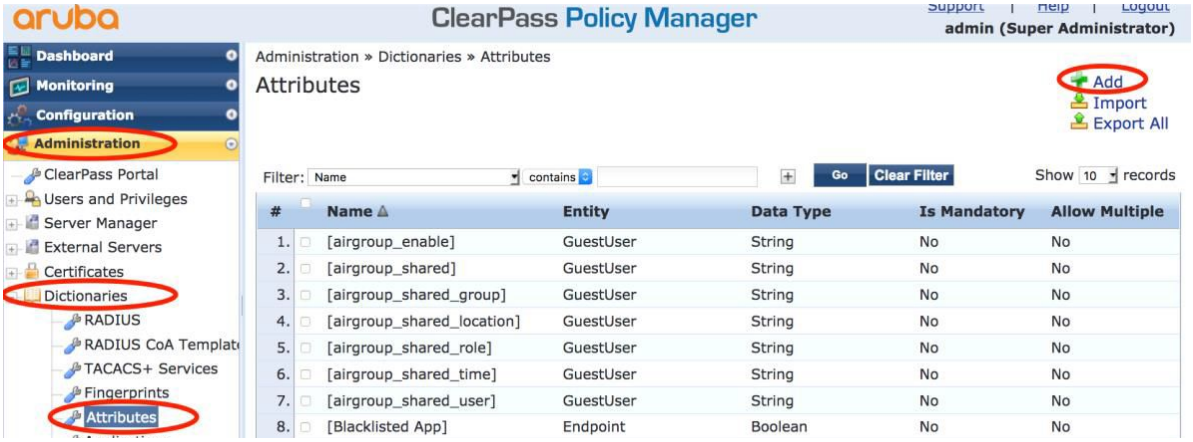
The Infoblox and Aruba ClearPass integration requires a few permission for the integration to work. Navigate to **"Administration"** → **"Administrators"** and add a **"Roles"**, **"Permissions"**, **"Groups"** and **"Admins"** to include permissions that are required for the integration. When creating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

Aruba ClearPass Configuration

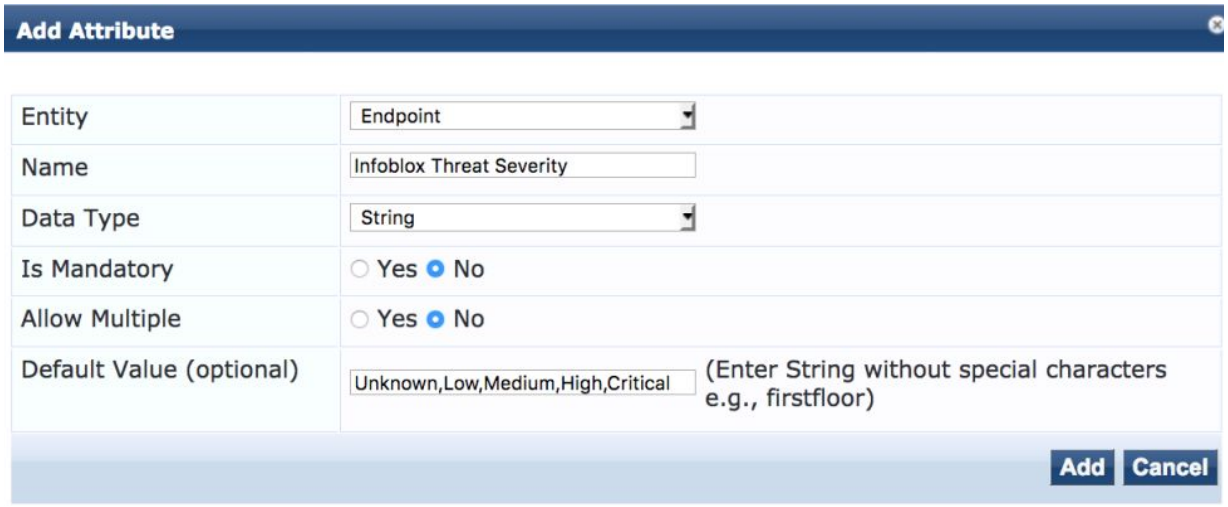
Adding Attributes

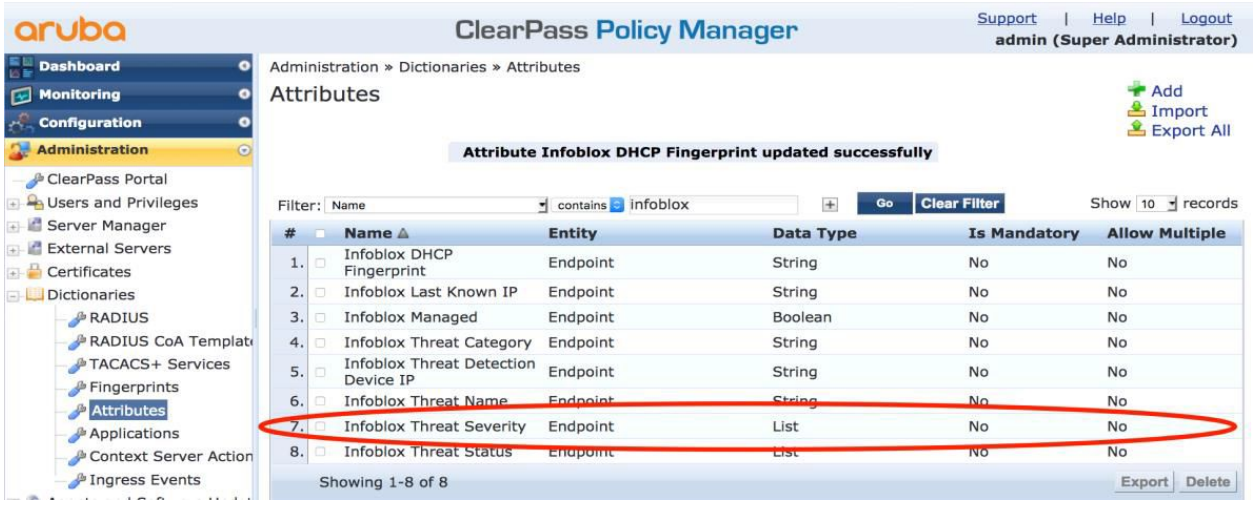
The Infoblox and Aruba ClearPass integration requires endpoint attributes that may not be already created. In order to add the attributes:

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"**.





3. Repeat Step 2 for each attribute from the table below:

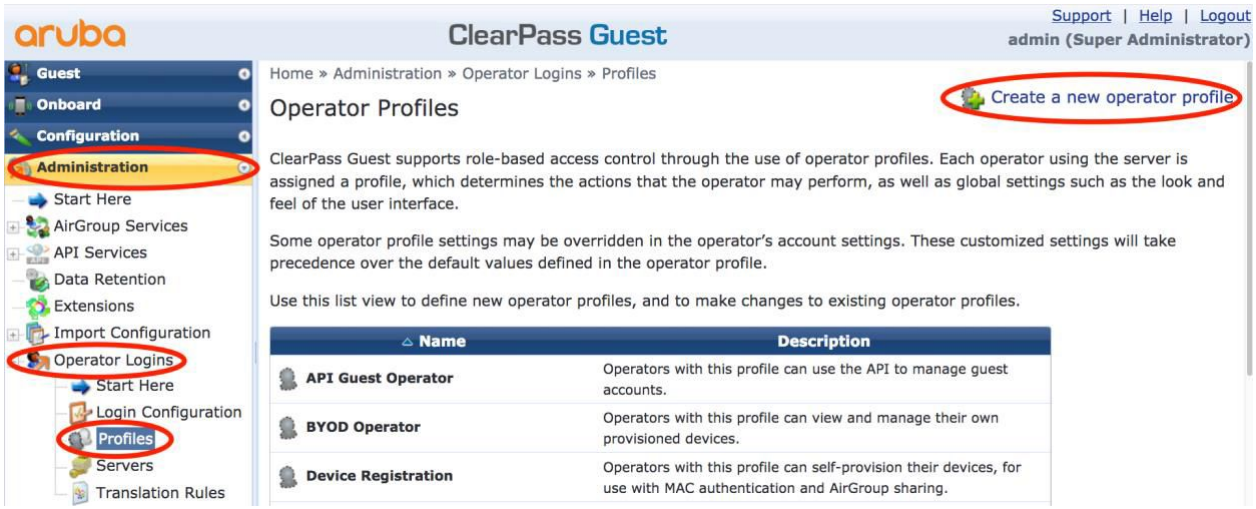
Table 4. Aruba Attributes

Field Name	Data Type	Description
Infoblox DHCP Fingerprint	String	DHCP fingerprint of the device if known
Infoblox Las 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

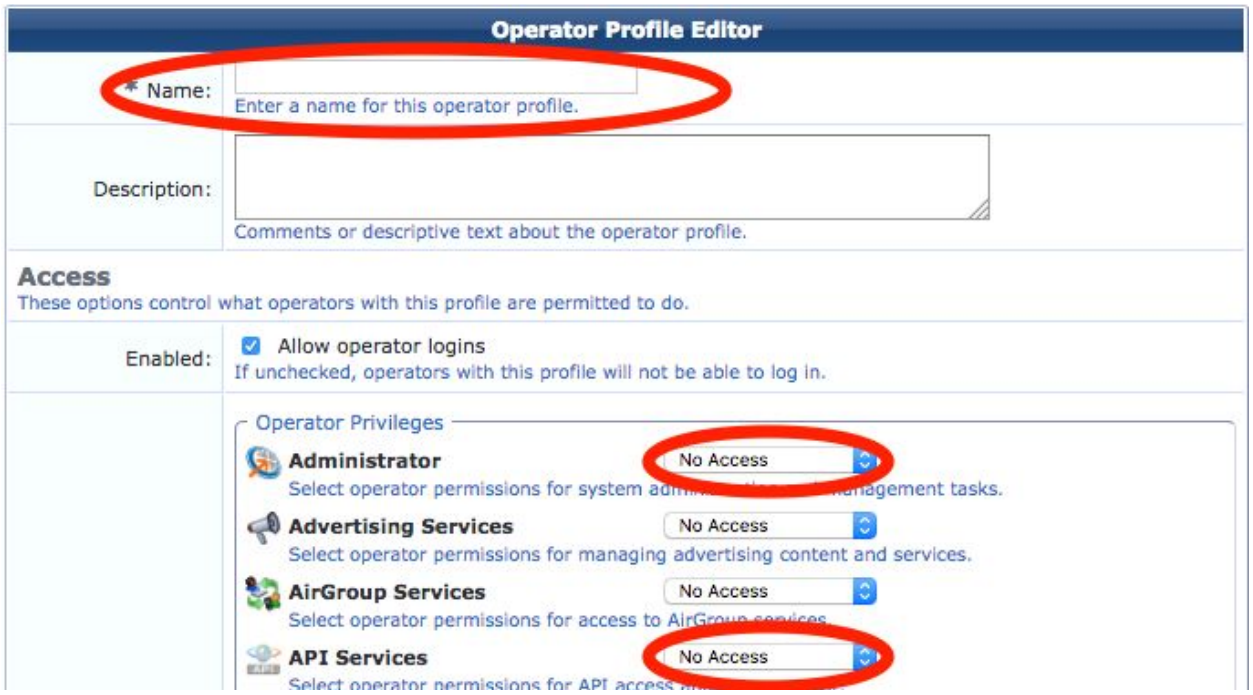
Infoblox Threat Severity	List	Severity of the incident
Infoblox Threat STatus	List	The current resolved/unresolved status of the threat
Infoblox RuleId	Integer	The ID of the rule
Infoblox RuleCategory	Text	The category to which the rule belongs

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.



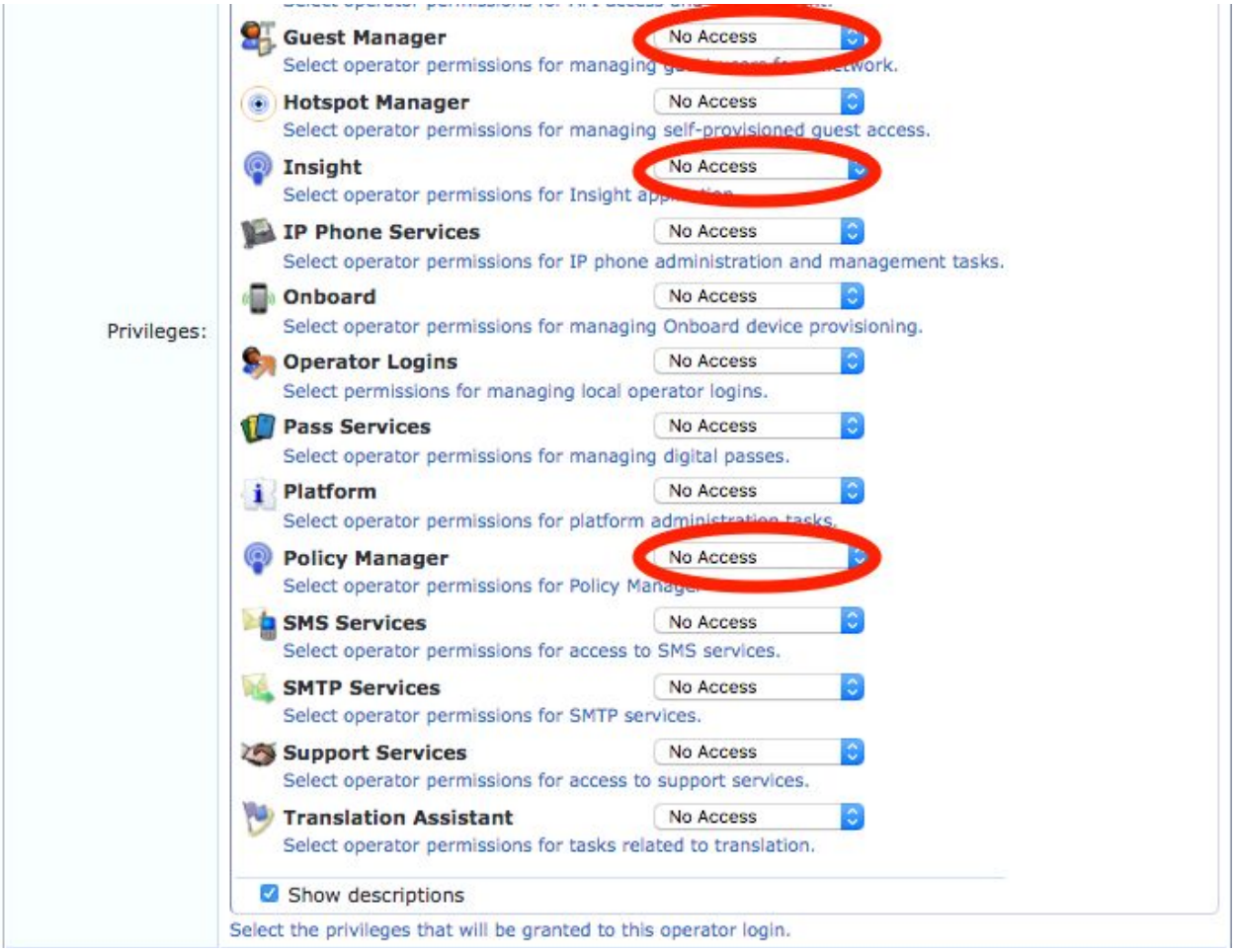
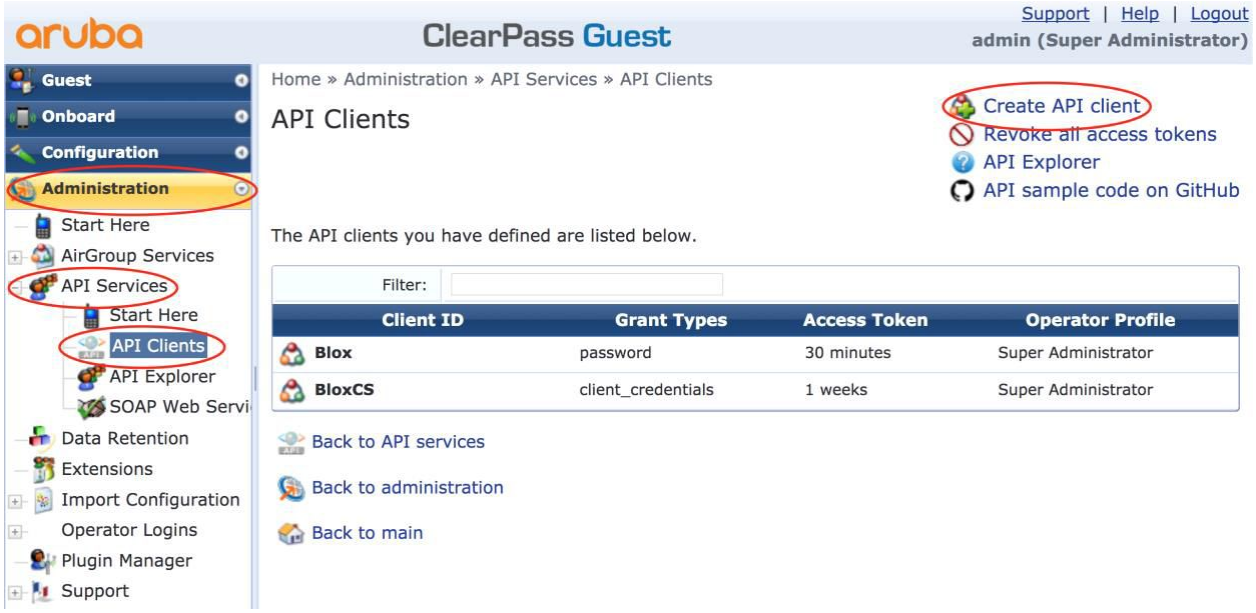


Table 5. Aruba Operator Privileges

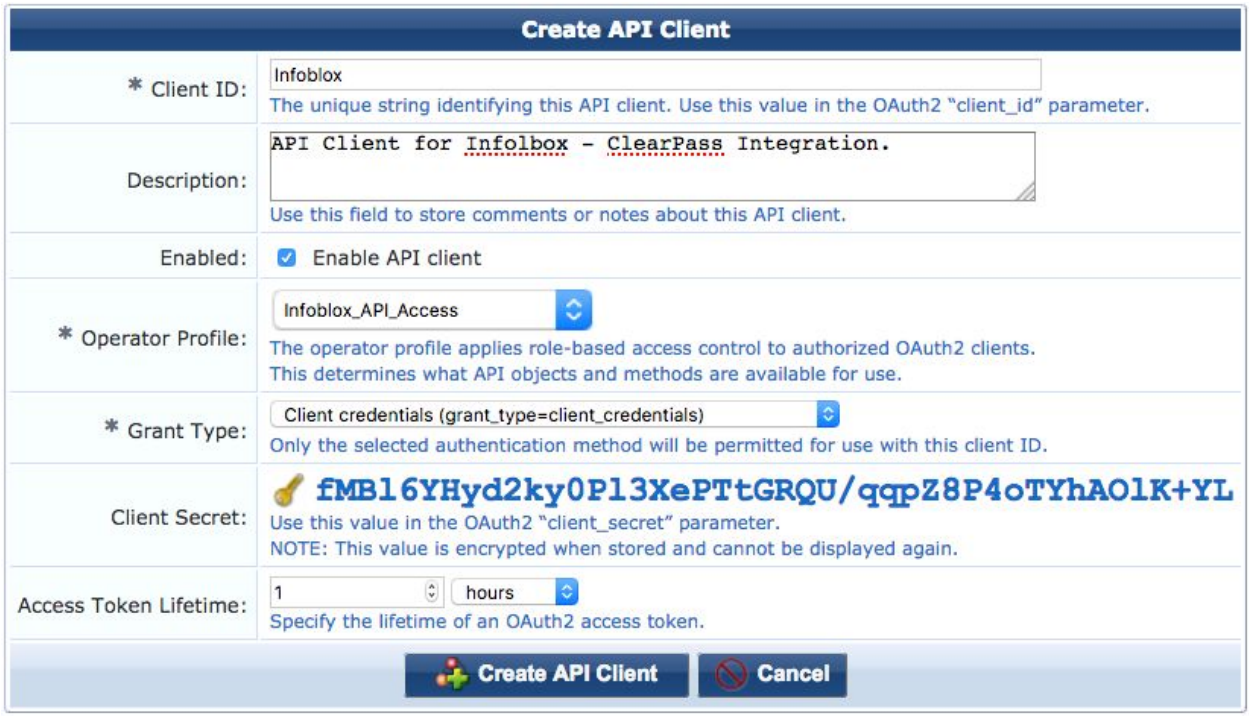
Privilege	Custom Name	Access
Administrator	Plugin Manager	Full
API services	Allow API Access Allow Access	Allow Access
Guest Manager	Active Sessions	Full
Guest Manager	Active Sessions History	Read Only
Guest Manager	Create Multiple Guest Accounts	Full
Guest Manager	Create New Guest Account	Read Only
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**.



2. 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.

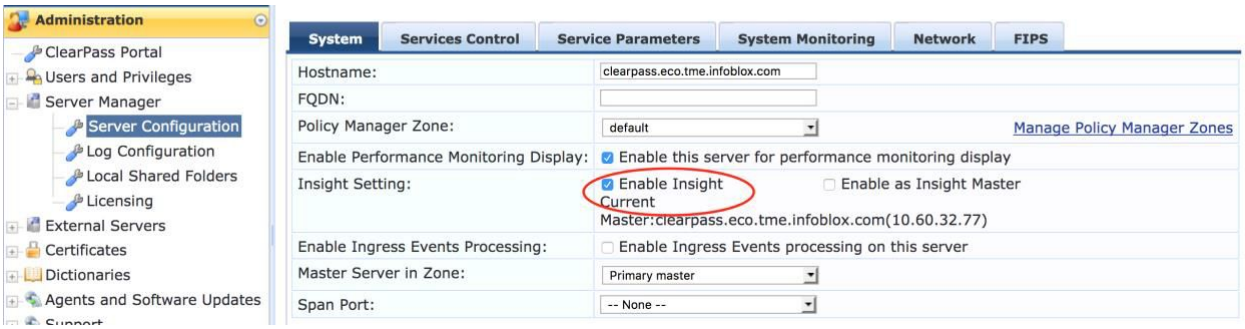


3. Click **“Create API Client”** when finished.

Enable Insight

1. 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”**.

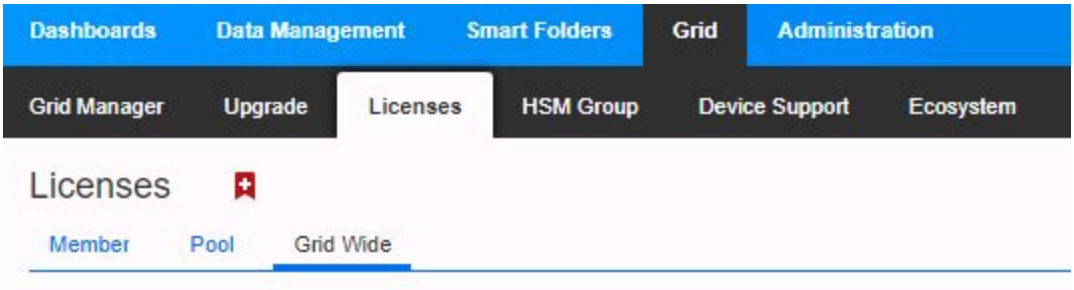


3. Click **Save** on the bottom right of the window to save the settings.
4. Lorem simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's
5. standard dummy text ever since the 1500s.

Infoblox NIOS Configuration

Verify that the Security Ecosystem License is installed

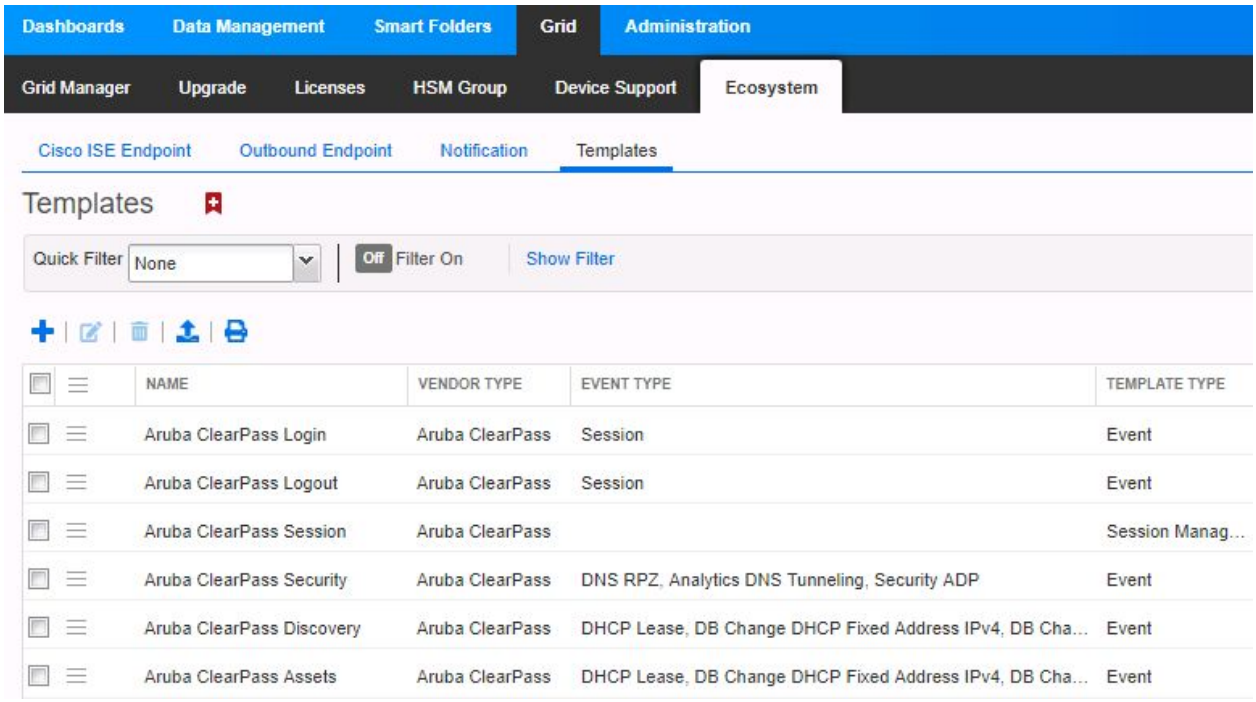
Security Ecosystem License is a “**Grid Wide**” License. Grid wide licenses activate services on all appliances in the same Grid. In order to check if the license was installed navigate to **“Grid”** → **“Licenses”** → **“Grid Wide”**.



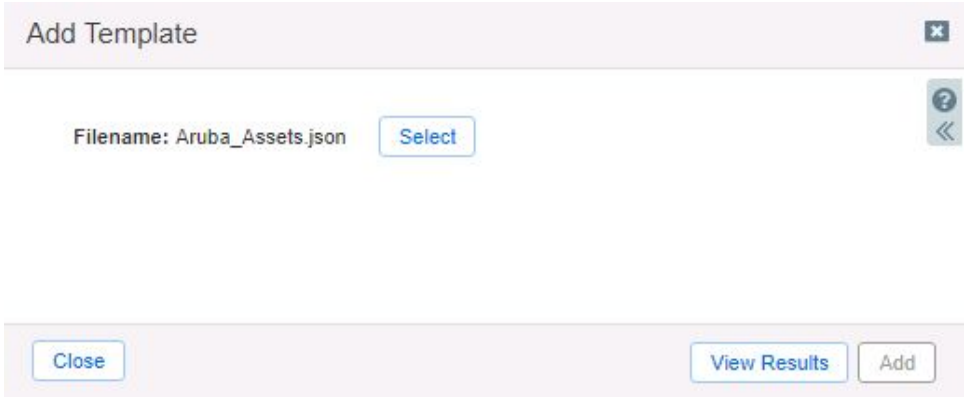
Add/Upload Templates

In order to upload/add templates:

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

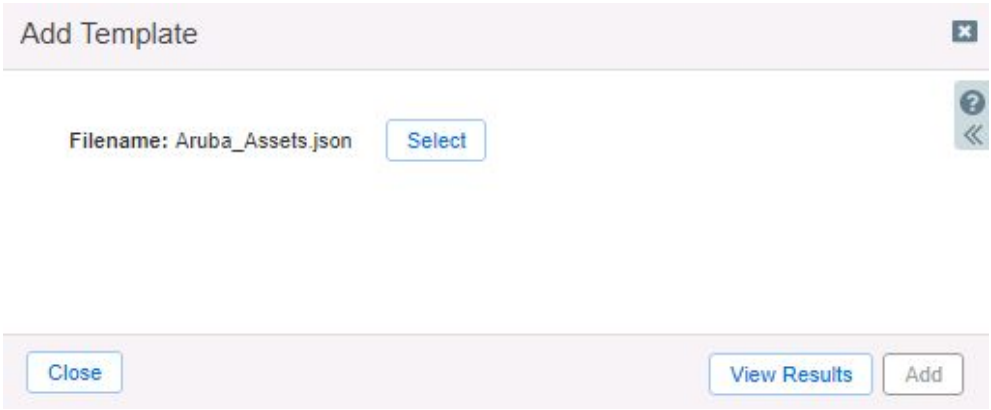


2. Press the **"Select"** button on the **"Add template"** window.



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

4. Click the **“Select”** button on the **“Upload”** window. The standard file selection dialog will open.
5. Select the file and click the **“Upload”** button on the **“Upload”** window.
6. click 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.



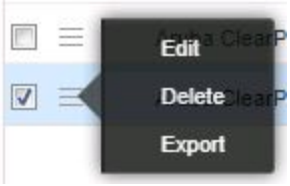
Note: There is no difference between uploading session management and action templates.

Modifying Templates

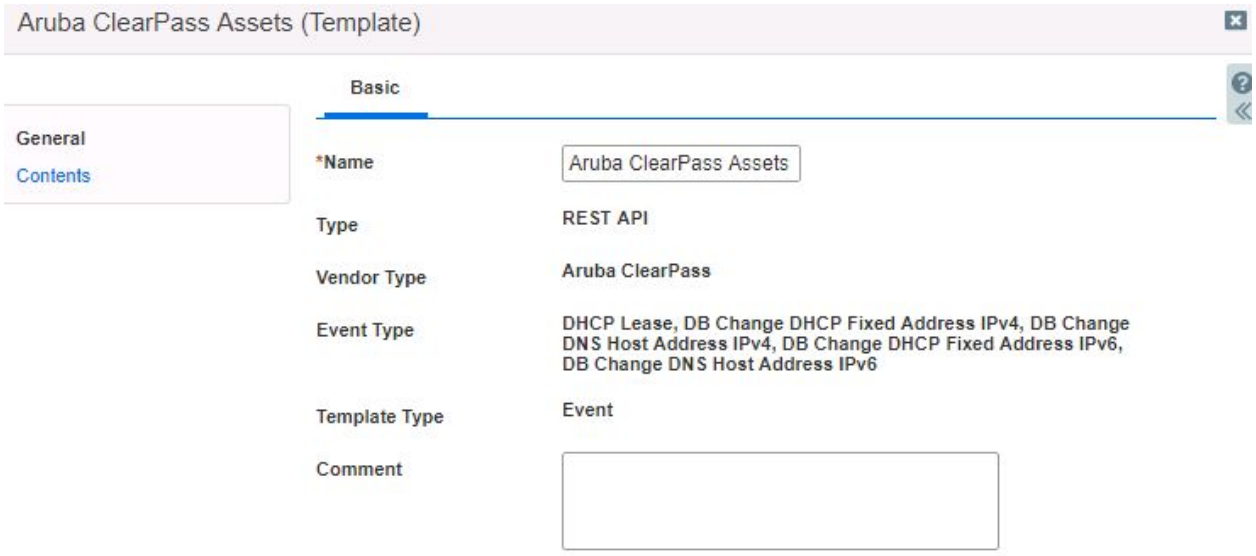
NIOS provides the facility to modify the templates via the web interface.

1. Navigate to **“Grid”** → **“Ecosystem”** → **“Templates”**. Then click the ☰ hamburger icon associated with the Template you would like to modify.

2. In the menu that is revealed, click **“Edit”**.



3. Then in the window that is revealed, click **"Contents"** in the left navigation panel



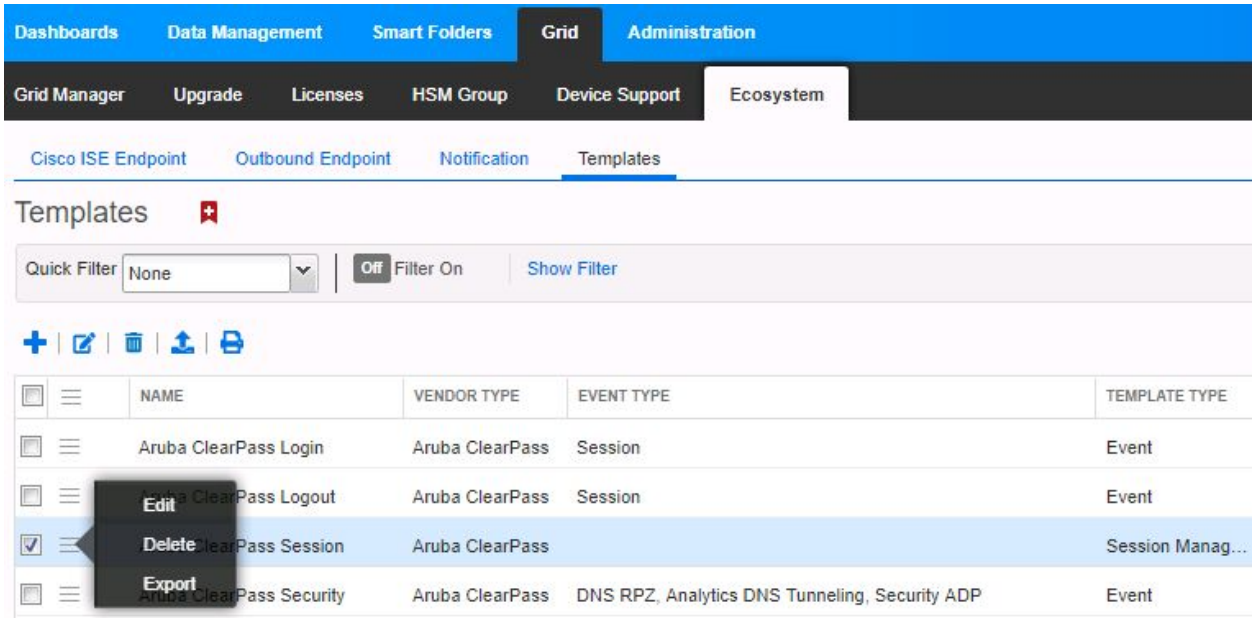
4. Shown is a simple text editor for making changes to the template. It is recommended to only use the built in template editor for minor edits. You may copy and paste to and from your favorite text editor if desired. To close the window click **"Cancel"** to discard any changes or click **"Save & Close"** to confirm any changes.

Note: you may not delete a template if it is used by an Outbound endpoint or a notification.

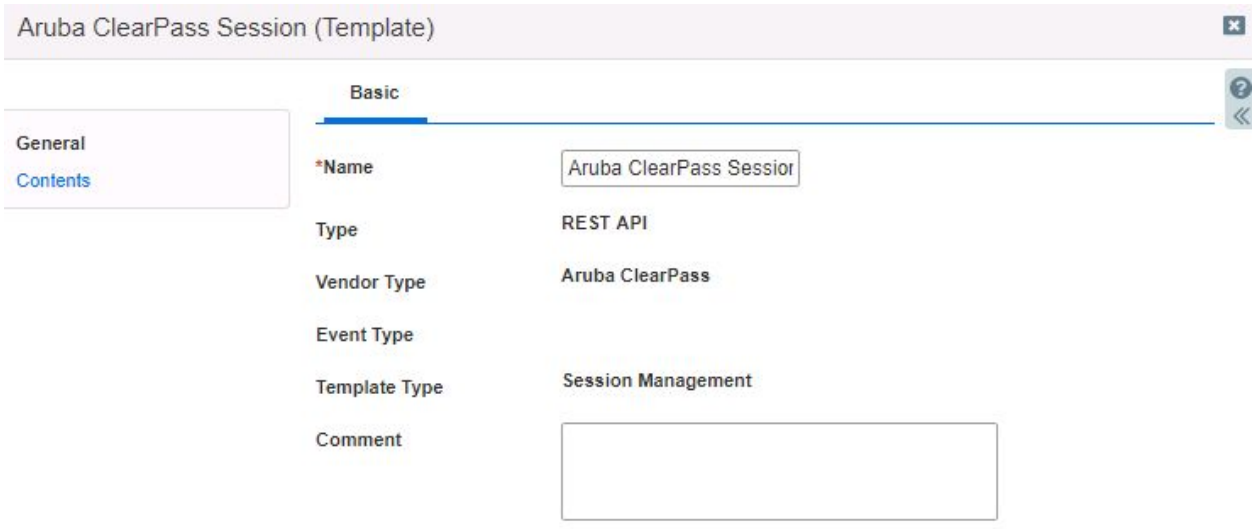
Adding Client Secret and Client ID

After adding all templates you must insert a Client ID specified on the Aruba ClearPass device, and a Client Secret that was acquired from the Aruba ClearPass device into the Session Management template.

1. Navigate to **"Grid" → "Ecosystem" → "Templates"**. Then, click the ☰ hamburger icon associated with the **Aruba_Session.json** template and click Edit to modify it.



2. Once inside the **Aruba ClearPass Session (Template)** window, click **Contents** in the left hand panel



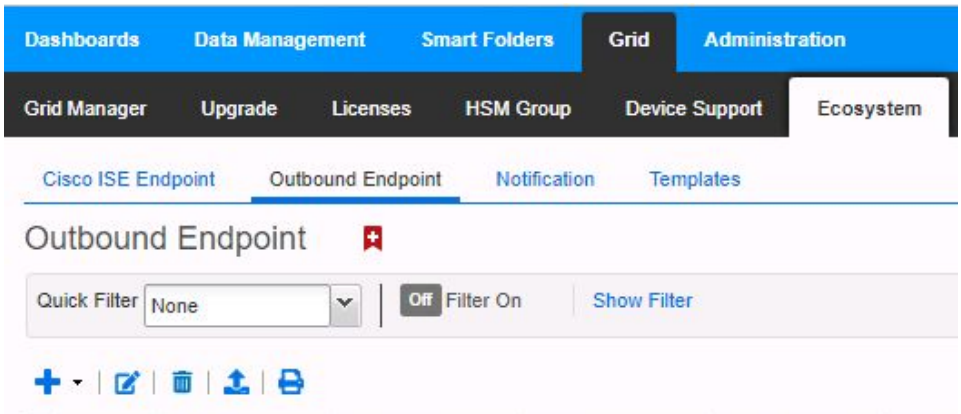
3. Inside the **“Aruba_Session.json”** template insert the **“Client Secret”** key into the **“value”** field of the **“endpoint_variables”** with the name **"KEY”**.
4. Inside the **“Aruba_Session.json”** template insert the **“Client ID”** value into the **“value”** field of the **“endpoint_variables”** with the name **"Client_ID”**.

5. Click **Save & Close** to finalize all changes.

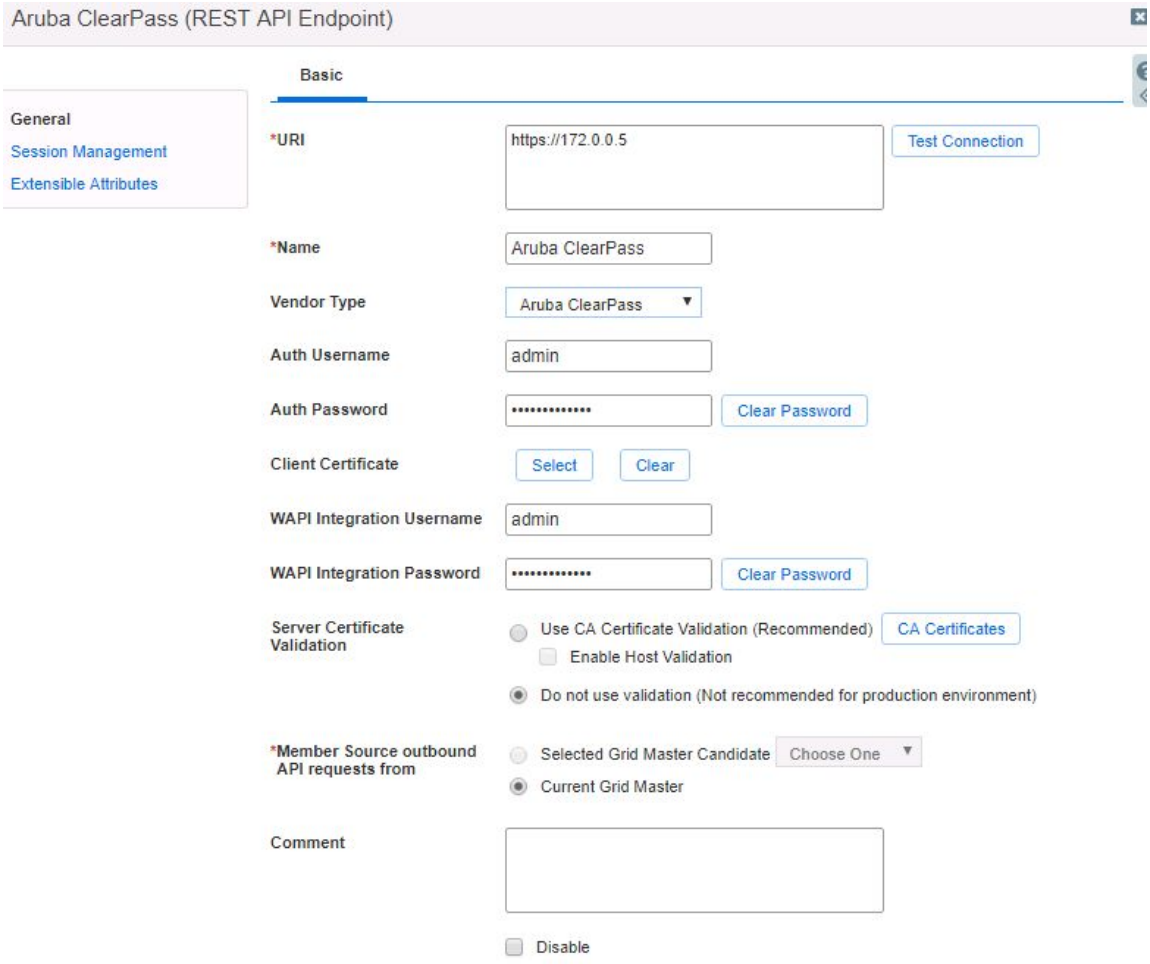
Add a REST API Endpoint

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).

1. Navigate to **“Grid”** → **“Ecosystem”** → **“Outbound Endpoints”** and click the **“+”** icon to begin adding a REST API Endpoint.

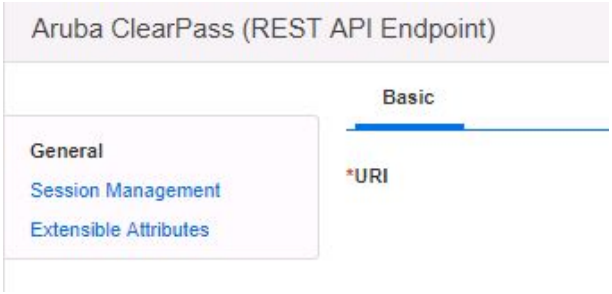


2. An Add REST API Endpoint Wizard will be revealed. Input the following Information:
    - **URI** must be the FQDN of the Aruba ClearPass device that Infoblox is integrating with.
    - **Name** must be filled, any value is acceptable.
    - **Vendor Type**, if the Vendor type is not specified select Aruba ClearPass from the drop-down menu
    - **Auth Username** is the user account used to access the API of the ClearPass device.
    - **Auth Password** is the API User's password used to access the API of the ClearPass device.
    - **WAPI Integration Username** is the NIOS user account used to access the NIOS API.
    - **WAPI Integration Password** is the NIOS user account's password used to access the NIOS API.
    - (Optional) **Client Certificate**, and **Server Certificate Validation** are used to encrypt communication between NIOS and Aruba ClearPass. If you wish to encrypt the data input your Certificates here.
    - (Optional) **Member Source outbound API requests from**. If desired, select another Grid Member to serve notifications to Aruba ClearPass.

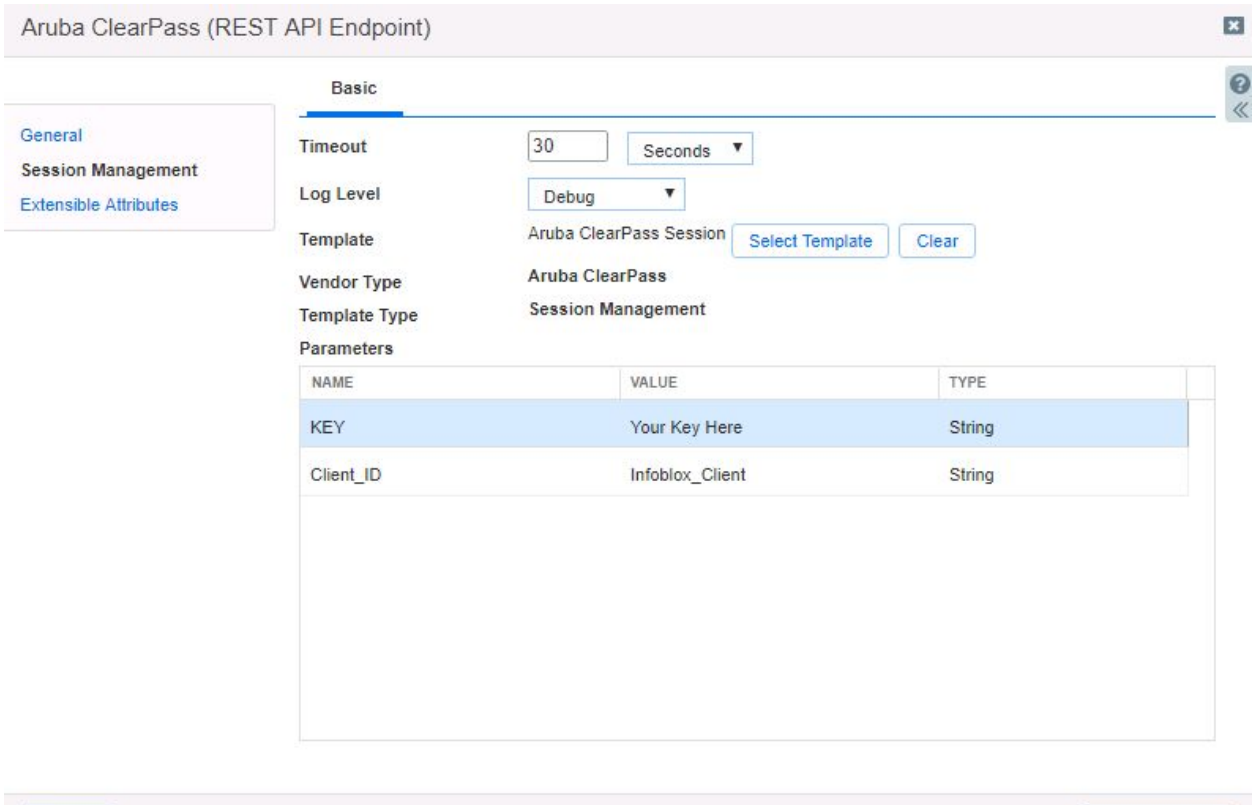


Note: When possible, it is recommended to send notifications from a Grid Master Candidate instead of from the Grid Master.

3. Click on **"Session Management"** in the top left panel of the **Aruba ClearPass (REST API Endpoint)** window.



4. In the Session Management settings of the Endpoint, add the **"Client_ID"** and **"KEY"** to the value fields. *Note: The Client_ID is case sensitive and specified on the Aruba ClearPass device as the API Client that was created earlier in this guide. KEY is case sensitive and the Client Secret that was acquired earlier in this guide.*



5. (Optional) Change the **Log Level** to **Debug** to view more information about the communication between Infoblox and Aruba ClearPass during testing.

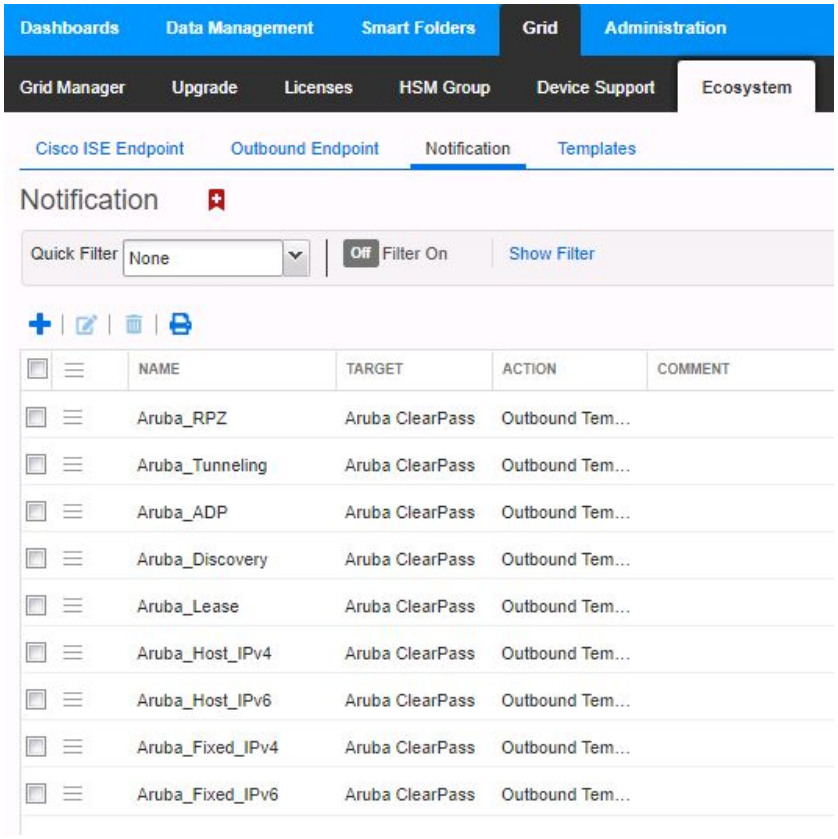
6. Click **Save & Close** to finalize all changes.

Add a Notification

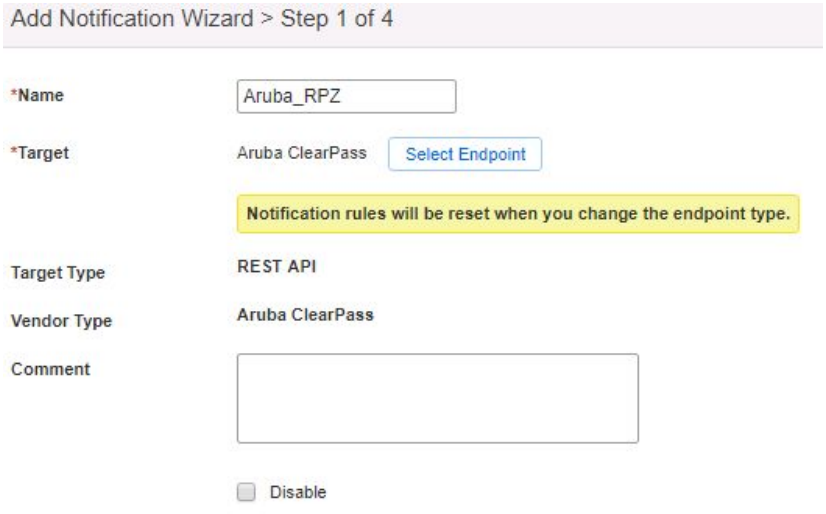
An endpoint and a template must be added before you can add a notification.

In order to add notifications follow the following steps:

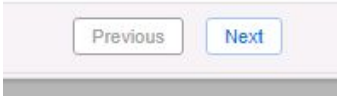
1. Navigate to **“Grid”** → **“Ecosystem”** → **“Notification”** and click the **“+”** icon to begin adding a **Notification**.



2. Specify the notification’s **Name**, and select a **Target** endpoint by clicking the **Select Endpoint** button.

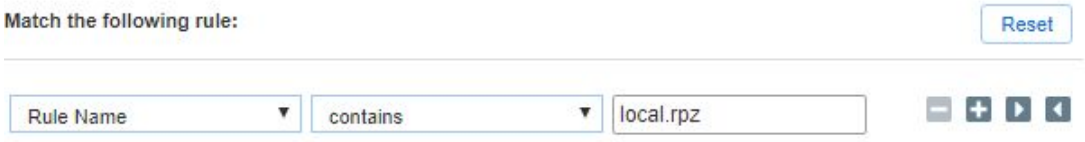


3. Click **Next**.

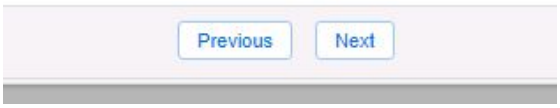


4. Select the relevant **Event** for the Notification by clicking on the Event dropdown. For a list of all supported Events view table 3 on page 5.

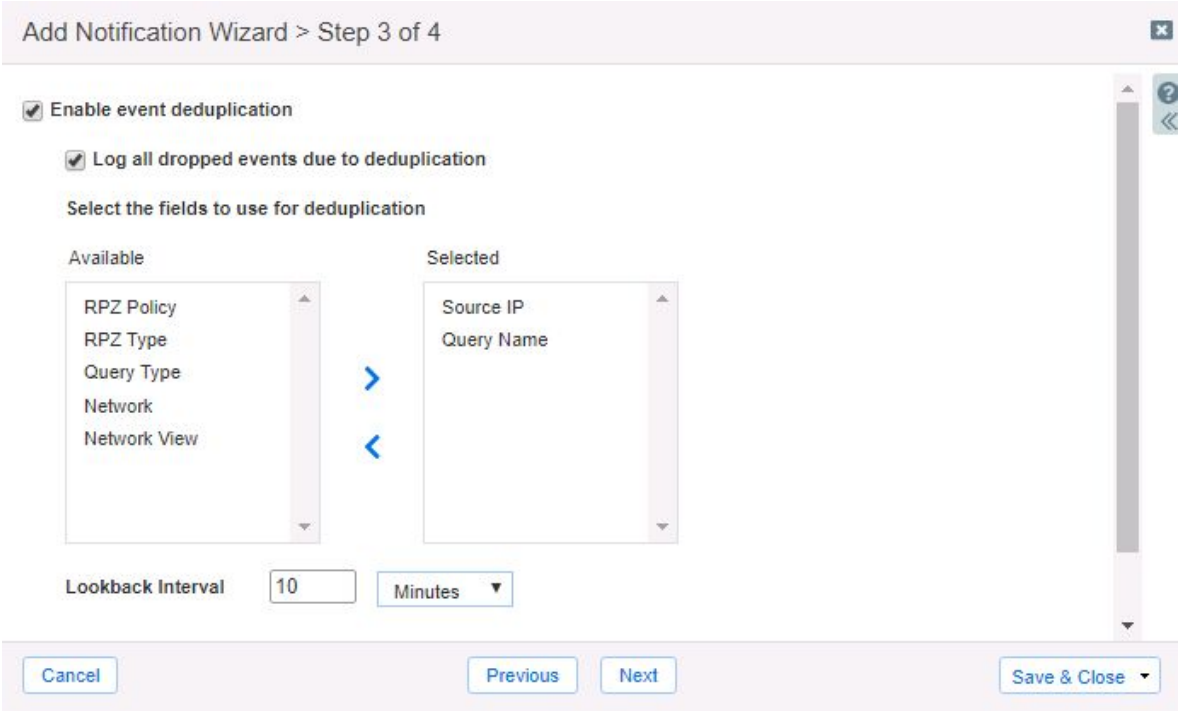
5. Apply a Filter to the Notification. *Note: for optimal performance it is best practice to make the filter as narrow as possible.*



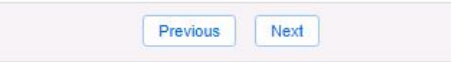
6. Click **Next**.



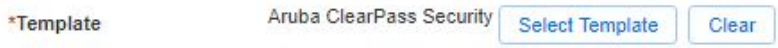
7. (For RPZ notifications only) Check **"Enable RPZ event deduplication"** and specify relevant parameters.



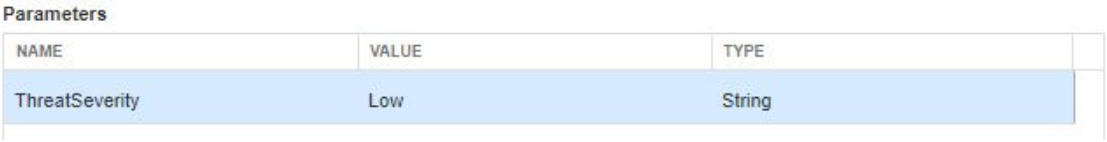
8. Click **"Next"**.



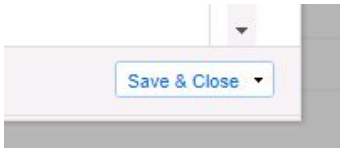
9. Click **Select Template** to select the relevant template.



10. (Optional) if desired specify the template's **Parameters**.



11. Click **Save & Close** to finalize the creation of the Notification.

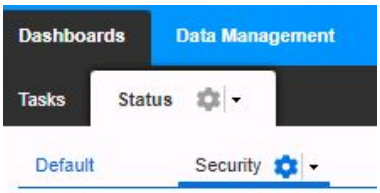


12. Create any other **Notifications** for other events as desired. All supported events for notifications are listed on Page 5.

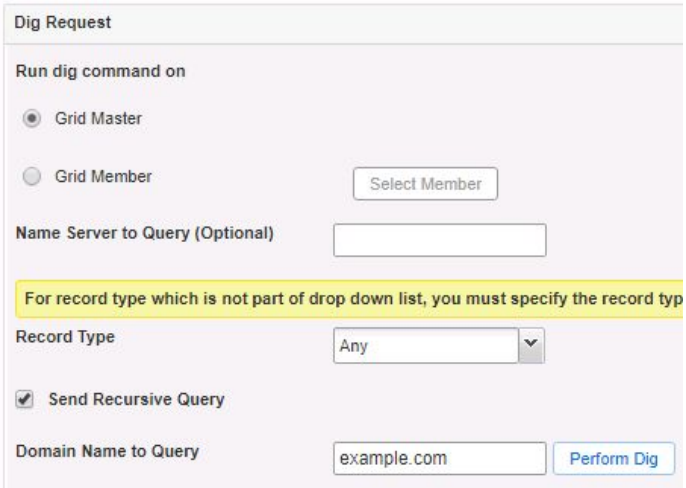
Check the Configuration

You can emulate an RPZ event to test the RPZ notification by performing the following steps:

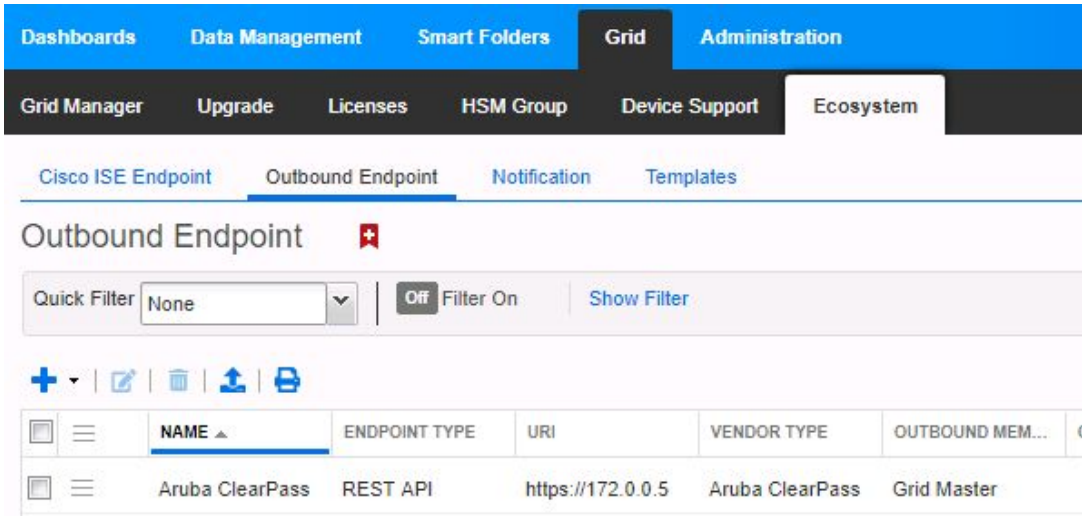
1. Navigate to **"Dashboards"** → **"Status"** → **"Security"**.



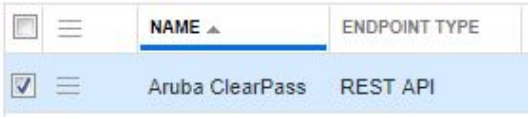
2. Input a domain that is blocked in the RPZ list that was included in a notification in the **"Domain Name to Query"** text field. Then click the **"Perform Dig"** button.



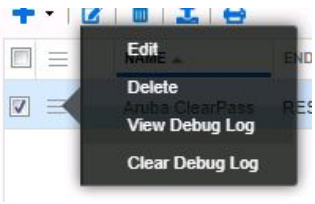
3. To view the results of the test, navigate to **"Grid"** → **"Ecosystem"** → **"Outbound Endpoint"**.



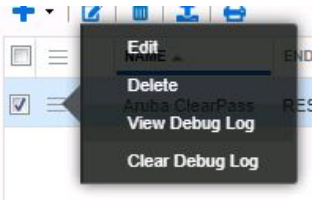
4. Click the ☰ hamburger icon associated with the **Aruba ClearPass Outbound Endpoint**.



5. Click **View Debug Log** in the menu that is revealed.



6. (Optional) To clear the Debug Log for other tests you may click **Clear Debug Log** instead.



Note: 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 Infoblox and Aruba ClearPass 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.

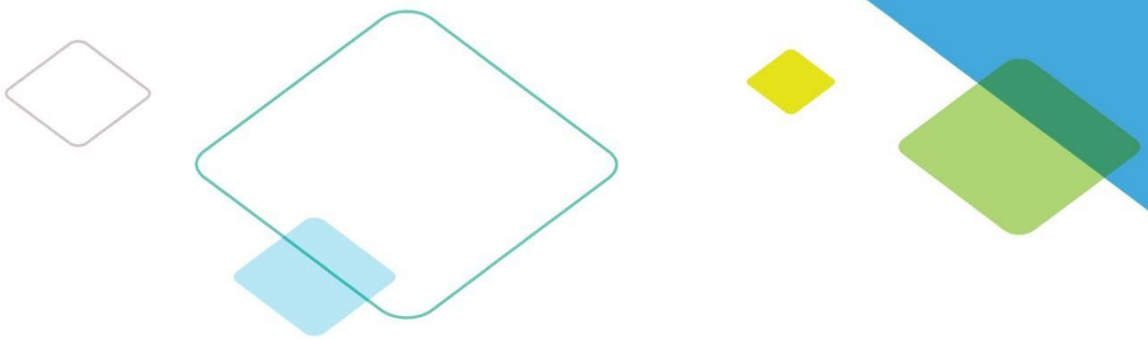
https://www.arubanetworks.com/techdocs/ClearPass/6.7/PolicyManager/Content/CPPM_UserGuide/Admin/EndpointContextServersAdd_Infoblox.htm

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

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



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