

Deployment Guide

# Infoblox Integration with Aruba ClearPass



# Table of Contents

<b>Introduction</b>	<b>2</b>
<b>Prerequisites</b>	<b>2</b>
<b>Known Limitations</b>	<b>2</b>
<b>Best Practices</b>	<b>3</b>
<b>Configuration</b>	<b>3</b>
Workflow	3
Before you get started	3
Download Templates from the Infoblox Community Website	3
Editing Instance Variables	4
Supported Notification	4
Infoblox Permissions	5
Aruba ClearPass Configuration	5
Adding Attributes	5
Adding Operator Profile (Permissions)	7
Adding API Client	9
Enable Insight	10
Infoblox NIOS Configuration	10
Verify that the Security Ecosystem License is installed	10
Heading Level 2	11

## 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”**.

The screenshot shows the Aruba ClearPass Policy Manager interface. The breadcrumb navigation is Administration » Dictionaries » Attributes. The page title is 'Attributes'. In the top right corner, there are buttons for 'Add', 'Import', and 'Export All', with the 'Add' button circled in red. Below the navigation is a filter section with a search box and 'Go' and 'Clear Filter' buttons. The main area contains a table of attributes:

#	Name	Entity	Data Type	Is Mandatory	Allow Multiple
1.	[airgroup_enable]	GuestUser	String	No	No
2.	[airgroup_shared]	GuestUser	String	No	No
3.	[airgroup_shared_group]	GuestUser	String	No	No
4.	[airgroup_shared_location]	GuestUser	String	No	No
5.	[airgroup_shared_role]	GuestUser	String	No	No
6.	[airgroup_shared_time]	GuestUser	String	No	No
7.	[airgroup_shared_user]	GuestUser	String	No	No
8.	[Blacklisted App]	Endpoint	Boolean	No	No

- 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**”.

**Add Attribute**

<b>Entity</b>	Endpoint	
<b>Name</b>	Infoblox Threat Severity	
<b>Data Type</b>	String	
<b>Is Mandatory</b>	<input type="radio"/> Yes <input checked="" type="radio"/> No	
<b>Allow Multiple</b>	<input type="radio"/> Yes <input checked="" type="radio"/> No	
<b>Default Value (optional)</b>	Unknown,Low,Medium,High,Critical	(Enter String without special characters e.g., firstfloor)

Add
Cancel

**ClearPass Policy Manager**
Support | Help | Logout  
admin (Super Administrator)

- Dashboard
- Monitoring
- Configuration
- Administration
- ClearPass Portal
- Users and Privileges
- Server Manager
- External Servers
- Certificates
- Dictionarys
- RADIUS
- RADIUS CoA Templates
- TACACS+ Services
- Fingerprints
- Attributes
- Applications
- Context Server Action
- Ingress Events

Administration » Dictionarys » Attributes

**Attributes**

Attribute Infoblox DHCP Fingerprint updated successfully

Filter: Name contains infoblox Go Clear Filter

#	Name	Entity	Data Type	Is Mandatory	Allow Multiple
1.	Infoblox DHCP Fingerprint	Endpoint	String	No	No
2.	Infoblox Last Known IP	Endpoint	String	No	No
3.	Infoblox Managed	Endpoint	Boolean	No	No
4.	Infoblox Threat Category	Endpoint	String	No	No
5.	Infoblox Threat Detection Device IP	Endpoint	String	No	No
6.	Infoblox Threat Name	Endpoint	String	No	No
7.	Infoblox Threat Severity	Endpoint	List	No	No
8.	Infoblox Threat Status	Endpoint	List	No	No

Showing 1-8 of 8

Export Delete

- 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 SStatus	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”.

The screenshot shows the Aruba ClearPass Guest Administration interface. The left sidebar contains a navigation menu with 'Administration' selected. Under 'Administration', 'Operator Logins' is selected, and 'Profiles' is highlighted. The main content area shows the 'Operator Profiles' page with a 'Create a new operator profile' button circled in red. Below the button is a table of existing operator profiles:

Name	Description
API Guest Operator	Operators with this profile can use the API to manage guest accounts.
BYOD Operator	Operators with this profile can view and manage their own provisioned devices.
Device Registration	Operators with this profile can self-provision their devices, for use with MAC authentication and AirGroup sharing.

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.

The screenshot shows the 'Operator Profile Editor' form. The 'Name' field is circled in red. Below it is the 'Description' field. The 'Access' section is expanded, showing 'Operator Privileges' with four items: 'Administrator', 'Advertising Services', 'AirGroup Services', and 'API Services'. Each item has a dropdown menu set to 'No Access', which is circled in red.

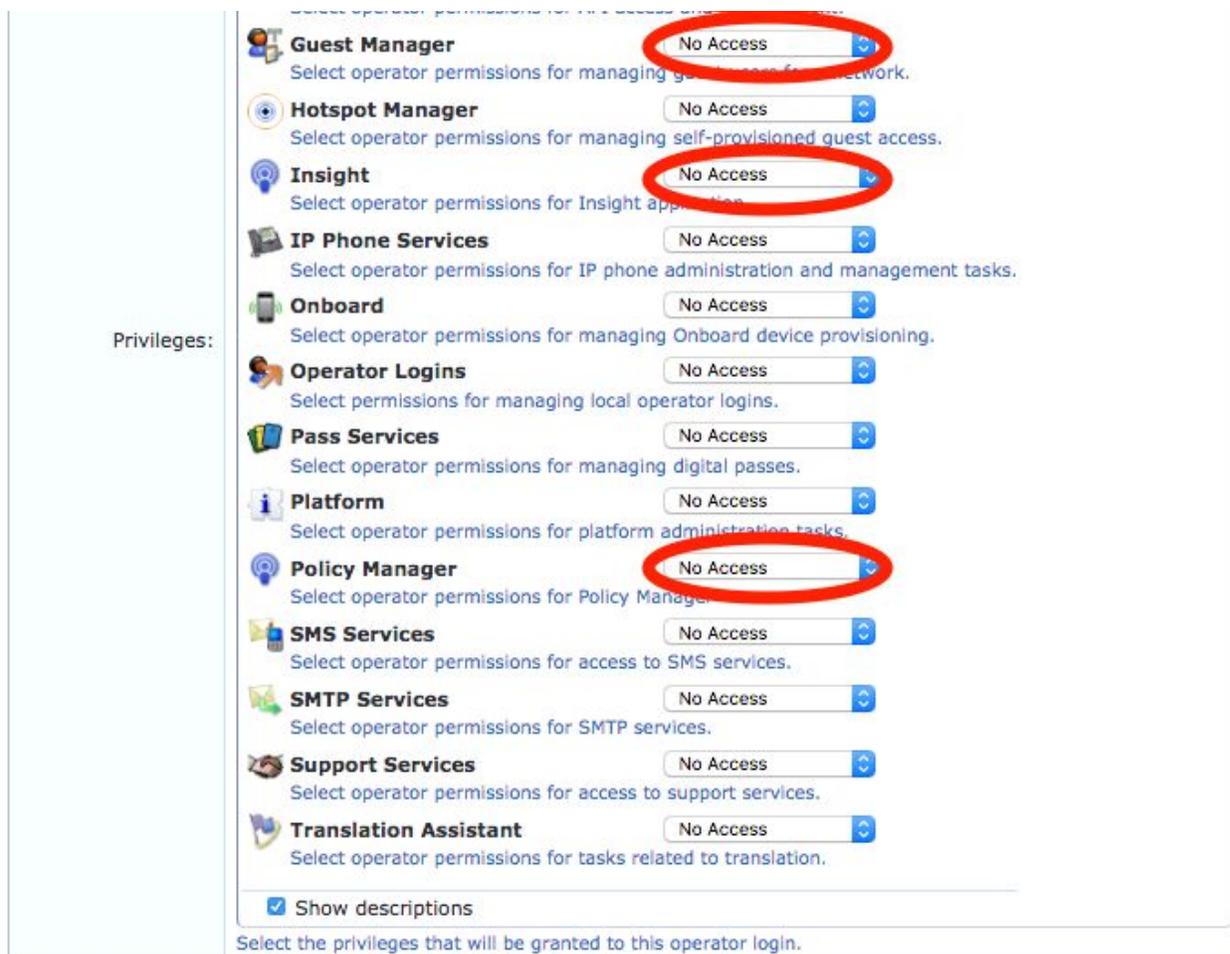


Table 5. Aruba Operator Privileges

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**.

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

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.

### Create API Client

<b>* Client ID:</b>	<input type="text" value="Infoblox"/> <small>The unique string identifying this API client. Use this value in the OAuth2 "client_id" parameter.</small>
<b>Description:</b>	<input style="width: 90%;" type="text" value="API Client for Infoblox - ClearPass Integration."/> <small>Use this field to store comments or notes about this API client.</small>
<b>Enabled:</b>	<input checked="" type="checkbox"/> Enable API client
<b>* Operator Profile:</b>	<input type="text" value="Infoblox_API_Access"/> <small>The operator profile applies role-based access control to authorized OAuth2 clients. This determines what API objects and methods are available for use.</small>
<b>* Grant Type:</b>	<input type="text" value="Client credentials (grant_type=client_credentials)"/> <small>Only the selected authentication method will be permitted for use with this client ID.</small>
<b>Client Secret:</b>	<input type="text" value="fMB16YHyd2ky0P13XePTtGRQU/qqpZ8P4oTYhA01K+YL"/> <small>Use this value in the OAuth2 "client_secret" parameter. NOTE: This value is encrypted when stored and cannot be displayed again.</small>
<b>Access Token Lifetime:</b>	<input type="text" value="1"/> <input type="text" value="hours"/> <small>Specify the lifetime of an OAuth2 access token.</small>

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.

The screenshot shows the Aruba ClearPass Policy Manager interface. The left sidebar contains a navigation menu with the following items: Dashboard, Monitoring, Configuration, Administration (circled in red), ClearPass Portal, Users and Privileges, Server Manager (circled in red), Server Configuration (circled in red), Log Configuration, Local Shared Folders, Licensing, External Servers, and Certificates. The main content area displays the path Administration » Server Manager » Server Configuration. Below this, there is a table of server configurations. The table has columns for #, Server Name, Management Port, Data Port, Zone, Insight, Cluster Sync, and Last Sync Time. The first row shows a server named 'clearpass.eco.tme.infoblox.com' with Management Port '10.60.32.77', Data Port '-', Zone 'default', Insight 'Enabled', and Cluster Sync 'Enabled'. Below the table are buttons for 'Collect Logs', 'Backup', 'Restore', 'Cleanup', 'Shutdown', and 'Reboot'.

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

The screenshot shows the 'System' tab configuration page in the Aruba ClearPass Policy Manager. The left sidebar is the same as in the previous screenshot. The main content area has tabs for System, Services Control, Service Parameters, System Monitoring, Network, and FIPS. The 'System' tab is active. The configuration fields are: Hostname: clearpass.eco.tme.infoblox.com; FQDN: (empty); Policy Manager Zone: default; Enable Performance Monitoring Display:  Enable this server for performance monitoring display; Insight Setting:  Enable Insight Current (circled in red),  Enable as Insight Master; Master: clearpass.eco.tme.infoblox.com(10.60.32.77); Enable Ingress Events Processing:  Enable Ingress Events processing on this server; Master Server in Zone: Primary master; Span Port: -- None --.

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”.

The screenshot shows the Infoblox NIOS interface. The top navigation bar has tabs for Dashboards, Data Management, Smart Folders, Grid, and Administration. Below this is a secondary navigation bar with tabs for Grid Manager, Upgrade, Licenses (selected), HSM Group, Device Support, and Ecosystem. The main content area is titled 'Licenses' and has a sub-navigation bar with tabs for Member, Pool, and Grid Wide (selected).

	FEATURE ▲	LIMIT CONTEXT	LIMIT VALUE	EXPIRATION
	RPZ			2020-06-30 16:59:59 PDT (67 Days)
	Security Ecosystem			2020-06-30 16:59:59 PDT (67 Days)

## Add/Upload Templates

In order to upload/add templates:

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

	NAME	VENDOR TYPE	EVENT TYPE	TEMPLATE TYPE
	Aruba ClearPass Login	Aruba ClearPass	Session	Event
	Aruba ClearPass Logout	Aruba ClearPass	Session	Event
	Aruba ClearPass Session	Aruba ClearPass		Session Manag...
	Aruba ClearPass Security	Aruba ClearPass	DNS RPZ, Analytics DNS Tunneling, Security ADP	Event
	Aruba ClearPass Discovery	Aruba ClearPass	DHCP Lease, DB Change DHCP Fixed Address IPv4, DB Cha...	Event
	Aruba ClearPass Assets	Aruba ClearPass	DHCP Lease, DB Change DHCP Fixed Address IPv4, DB Cha...	Event

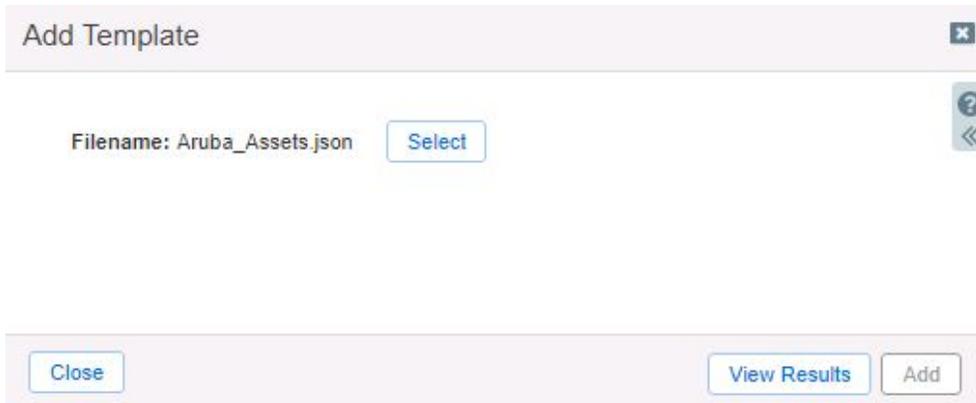
2. Press the “Select” button on the “Add template” window.

Filename: Aruba\_Assets.json

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.

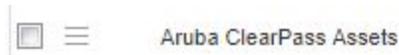


*Note: There is no difference between uploading session management and action templates.*

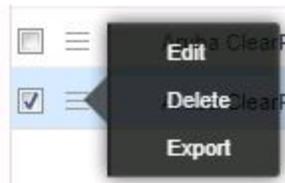
## Modifying Templates

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”.



- Then in the window that is revealed, click **“Contents”** in the left navigation panel

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:

- 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.

General  
Contents

```
{
  "vendor_identifier": "Aruba ClearPass",
  "version": "4.0",
  "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": {
    "Accept": "*/json"
  },
  "instance_variables": [
  ],
  "steps": [
    {
      "name": "Debug#0",
      "operation": "NOP",
      "body": "${XC:DEBUG:{H:}}${XC:DEBUG:{E:}}${XC:DEBUG:{I:}}${XC:DEBUG:{L:}}${XC:DEBUG:{S:}}${XC:DEBUG:{P:}}${XC:DEBUG:{R:}}${XC:DEBUG:{RH:}}${XC:DEBUG:{UT:}}",
    },
    {
      "name": "check if lease",
      "operation": "CONDITION",
      "condition": {
        "statements": [

```

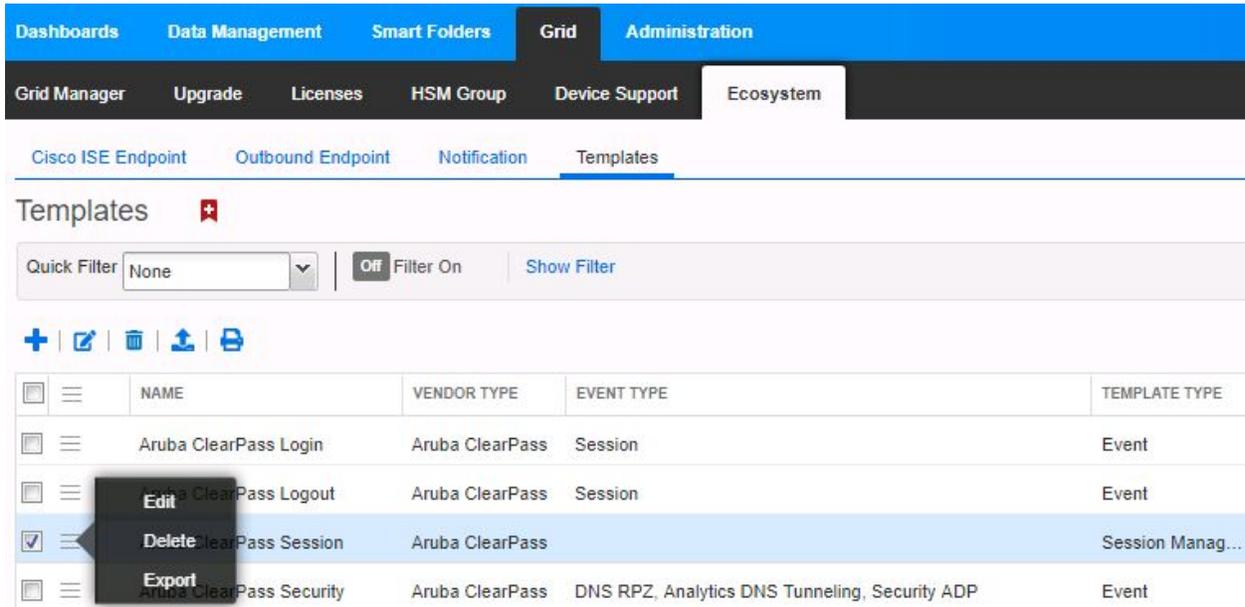
Cancel Save & Close

*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.

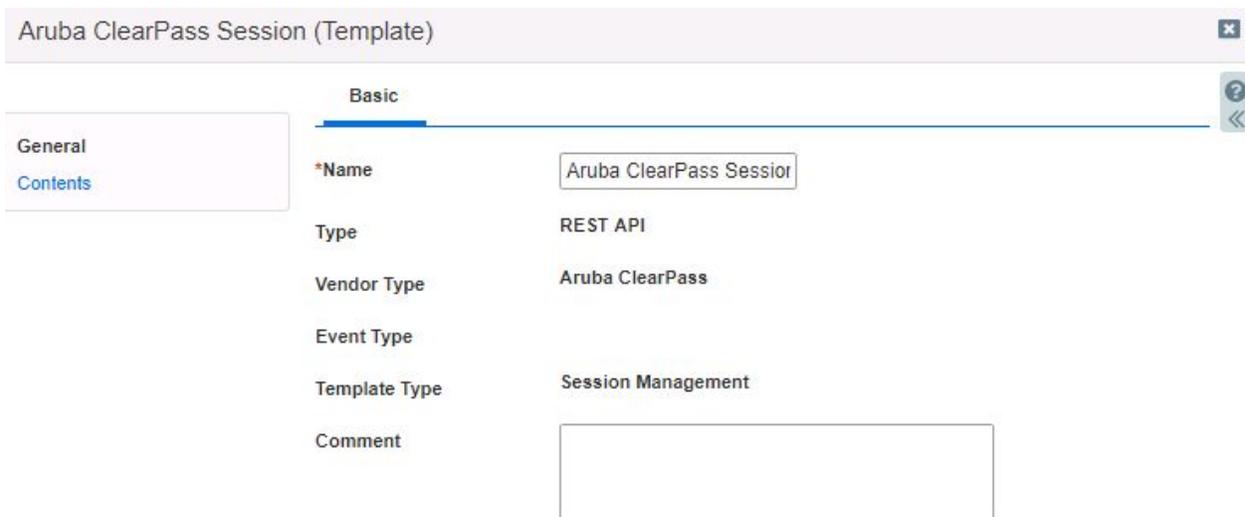
1. Navigate to “Grid” → “Ecosystem” → “Templates”. Then, click the ☰ hamburger icon associated with the **Aruba\_Session.json** template and click Edit to modify it.



The screenshot shows the Aruba ClearPass management console interface. The top navigation bar includes 'Dashboards', 'Data Management', 'Smart Folders', 'Grid', and 'Administration'. Below this, there are sub-menus for 'Grid Manager', 'Upgrade', 'Licenses', 'HSM Group', 'Device Support', and 'Ecosystem'. The 'Ecosystem' menu is expanded to show 'Cisco ISE Endpoint', 'Outbound Endpoint', 'Notification', and 'Templates'. The 'Templates' page is displayed, showing a table of templates. The 'Aruba ClearPass Session' template is selected, and a context menu is open over it, with the 'Edit' option highlighted.

	NAME	VENDOR TYPE	EVENT TYPE	TEMPLATE TYPE
<input type="checkbox"/>	Aruba ClearPass Login	Aruba ClearPass	Session	Event
<input type="checkbox"/>	Aruba ClearPass Logout	Aruba ClearPass	Session	Event
<input checked="" type="checkbox"/>	Aruba ClearPass Session	Aruba ClearPass		Session Manag...
<input type="checkbox"/>	Aruba ClearPass Security	Aruba ClearPass	DNS RPZ, Analytics DNS Tunneling, Security ADP	Event

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



The screenshot shows the configuration window for the 'Aruba ClearPass Session (Template)'. The left-hand panel has 'Contents' selected. The main area shows the 'Basic' configuration tab with the following fields:

- \*Name: Aruba ClearPass Sessior
- Type: REST API
- Vendor Type: Aruba ClearPass
- Event Type: Session Management
- Template Type: Session Management
- Comment: (empty text box)

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”.

General

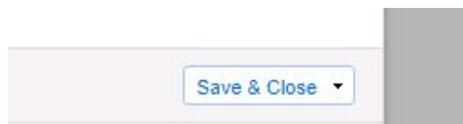
Contents

```

{
  "name": "Aruba ClearPass Session",
  "version": "3.0",
  "type": "REST_ENDPOINT",
  "inactivity_interval": 1000,
  "keepalive": true,
  "login_template": "Aruba ClearPass Login",
  "logout_template": "Aruba ClearPass Logout",
  "override_path": true,
  "path": "",
  "retry": 0,
  "retry_template": 0,
  "timeout": 60,
  "vendor_identifier": "Aruba ClearPass",
  "logout_only_at_template_end": true,
  "endpoint_variables": [
    {
      "name": "Client_ID",
      "type": "STRING",
      "value": "Infoblox_Client"
    },
    {
      "name": "KEY",
      "type": "STRING",
      "value": "YourKeyHere"
    }
  ]
}

```

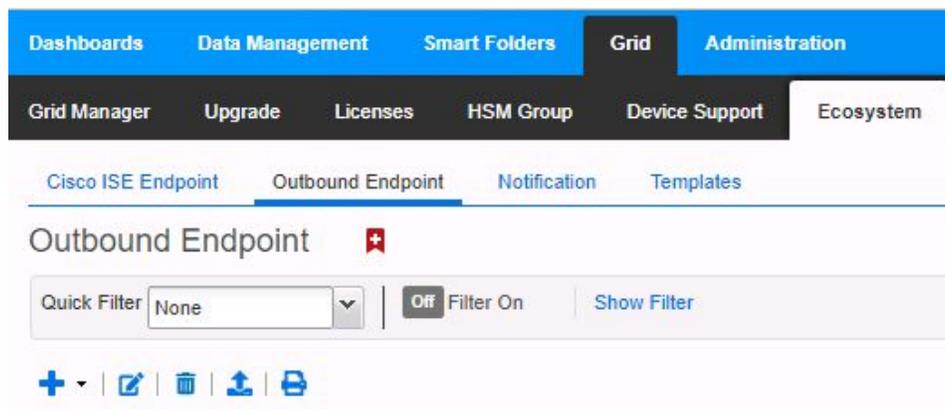
5. Click **Save & Close** to finalize all changes.



## 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.

Aruba ClearPass (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:
 

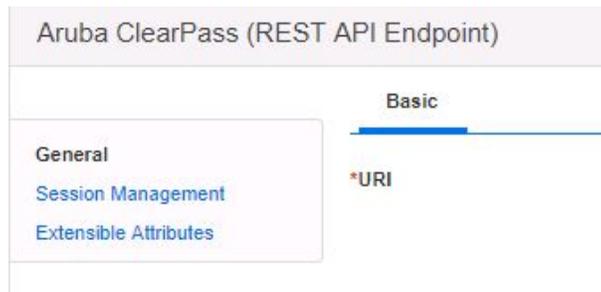
- Selected Grid Master Candidate
- Current Grid Master

Comment:

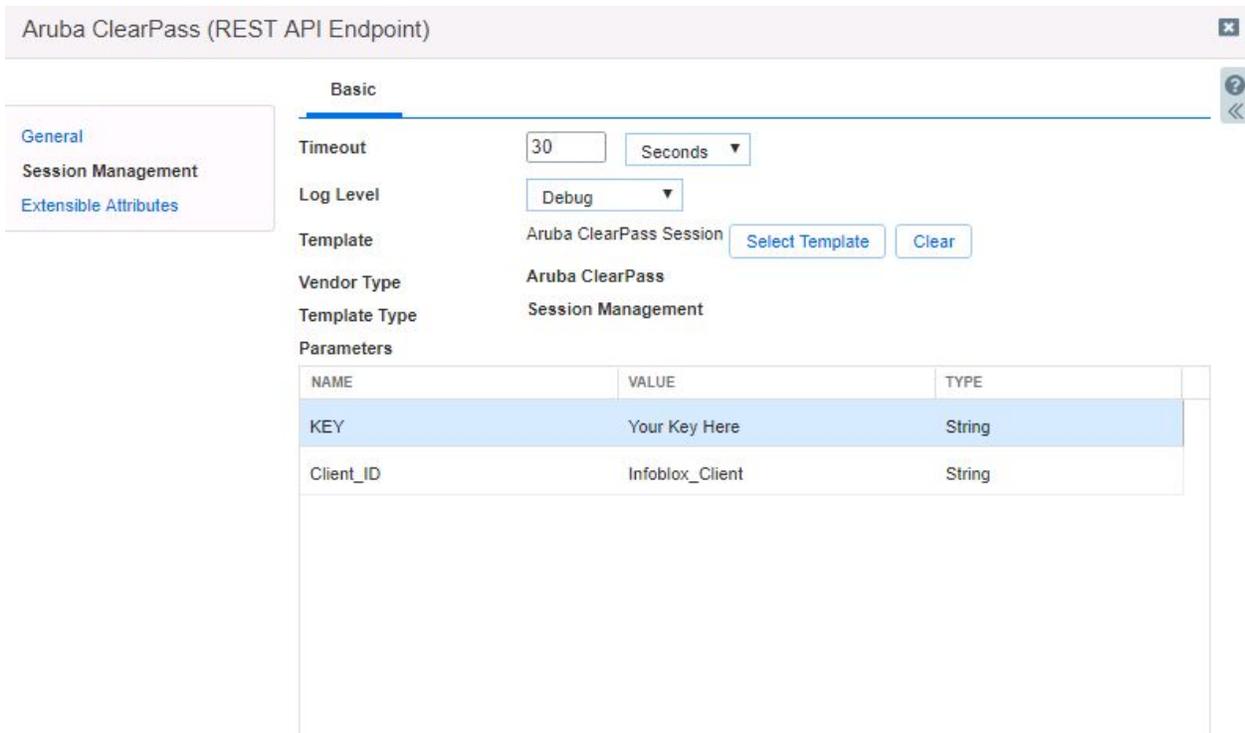
Disable

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

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



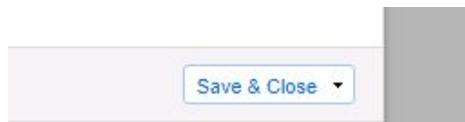
- In the Session Management settings of the Endpoint, add the **“Client\_ID”** and **“KEY”** to the value fields. *Note: The Client\_ID is case sensitive and specified on the Aruba ClearPass device as the API Client that was created earlier in this guide. KEY is case sensitive and the Client Secret that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



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



- 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**.

	NAME	TARGET	ACTION	COMMENT
<input type="checkbox"/>	Aruba_RPZ	Aruba ClearPass	Outbound Tem...	
<input type="checkbox"/>	Aruba_Tunneling	Aruba ClearPass	Outbound Tem...	
<input type="checkbox"/>	Aruba_ADP	Aruba ClearPass	Outbound Tem...	
<input type="checkbox"/>	Aruba_Discovery	Aruba ClearPass	Outbound Tem...	
<input type="checkbox"/>	Aruba_Lease	Aruba ClearPass	Outbound Tem...	
<input type="checkbox"/>	Aruba_Host_IPv4	Aruba ClearPass	Outbound Tem...	
<input type="checkbox"/>	Aruba_Host_IPv6	Aruba ClearPass	Outbound Tem...	
<input type="checkbox"/>	Aruba_Fixed_IPv4	Aruba ClearPass	Outbound Tem...	
<input type="checkbox"/>	Aruba_Fixed_IPv6	Aruba ClearPass	Outbound Tem...	

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

Add Notification Wizard > Step 1 of 4

\*Name

\*Target

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

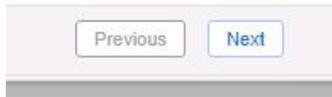
Target Type

Vendor Type

Comment

Disable

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.

\*Event DNS RPZ ▼

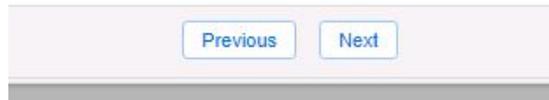
5. Apply a Filter to the Notification. *Note: for optimal performance it is best practice to make the filter as narrow as possible.*

Match the following rule:

Reset

Rule Name ▼ contains ▼ local.rpz - + ▶ ◀

6. Click **Next**.



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

Add Notification Wizard > Step 3 of 4 ✕

**Enable event deduplication**

Log all dropped events due to deduplication

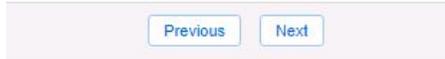
Select the fields to use for deduplication

Available	>	Selected
<p>RPZ Policy</p> <p>RPZ Type</p> <p>Query Type</p> <p>Network</p> <p>Network View</p>	<	<p>Source IP</p> <p>Query Name</p>

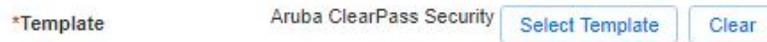
Lookback Interval 10 Minutes ▼

Cancel Previous Next Save & Close ▼

8. Click **“Next”**.



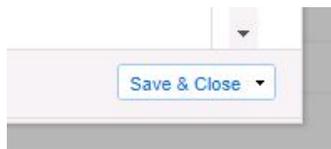
9. Click **Select Template** to select the relevant template.



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

Parameters		
NAME	VALUE	TYPE
ThreatSeverity	Low	String

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

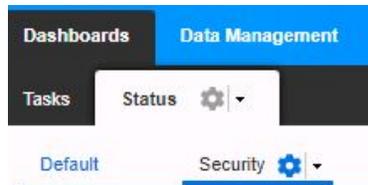


12. Create any other **Notifications** for other events as desired. All supported events for notifications are listed on Page 5.

### 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.

Dig Request

Run dig command on

Grid Master

Grid Member Select Member

Name Server to Query (Optional)

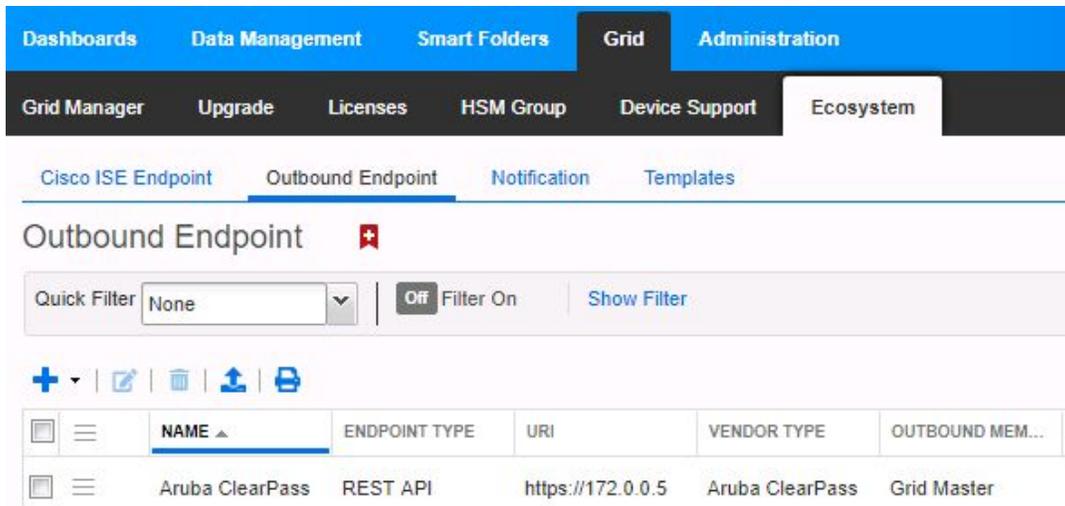
**For record type which is not part of drop down list, you must specify the record type**

Record Type

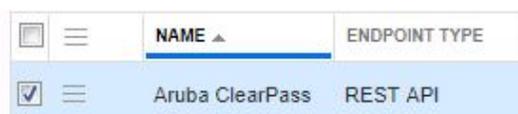
Send Recursive Query

Domain Name to Query  Perform Dig

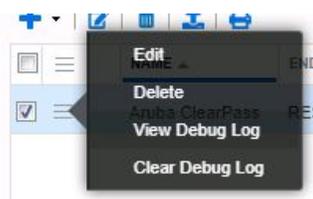
3. To view the results of the test, navigate to **“Grid”** → **“Ecosystem”** → **“Outbound Endpoint”**.



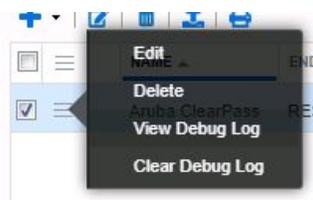
4. Click the  icon associated with the **Aruba ClearPass Outbound Endpoint**.



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.

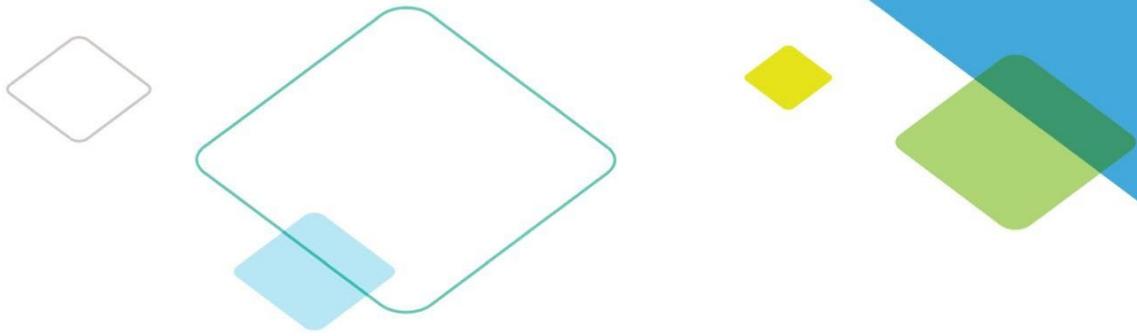
[https://www.arubanetworks.com/techdocs/ClearPass/6.7/PolicyManager/Content/CPPM\\_UserGuide/Admin/EndpointContextServersAdd\\_Infoblox.htm](https://www.arubanetworks.com/techdocs/ClearPass/6.7/PolicyManager/Content/CPPM_UserGuide/Admin/EndpointContextServersAdd_Infoblox.htm)

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](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>



Infoblox enables next level network experiences with its Secure Cloud-Managed Network Services. As the pioneer in providing the world's most reliable, secure and automated networks, we are relentless in our pursuit of network simplicity. A recognized industry leader, Infoblox has 50 percent market share comprised of 8,000 customers, including 350 of the Fortune 500.

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



© 2019 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).