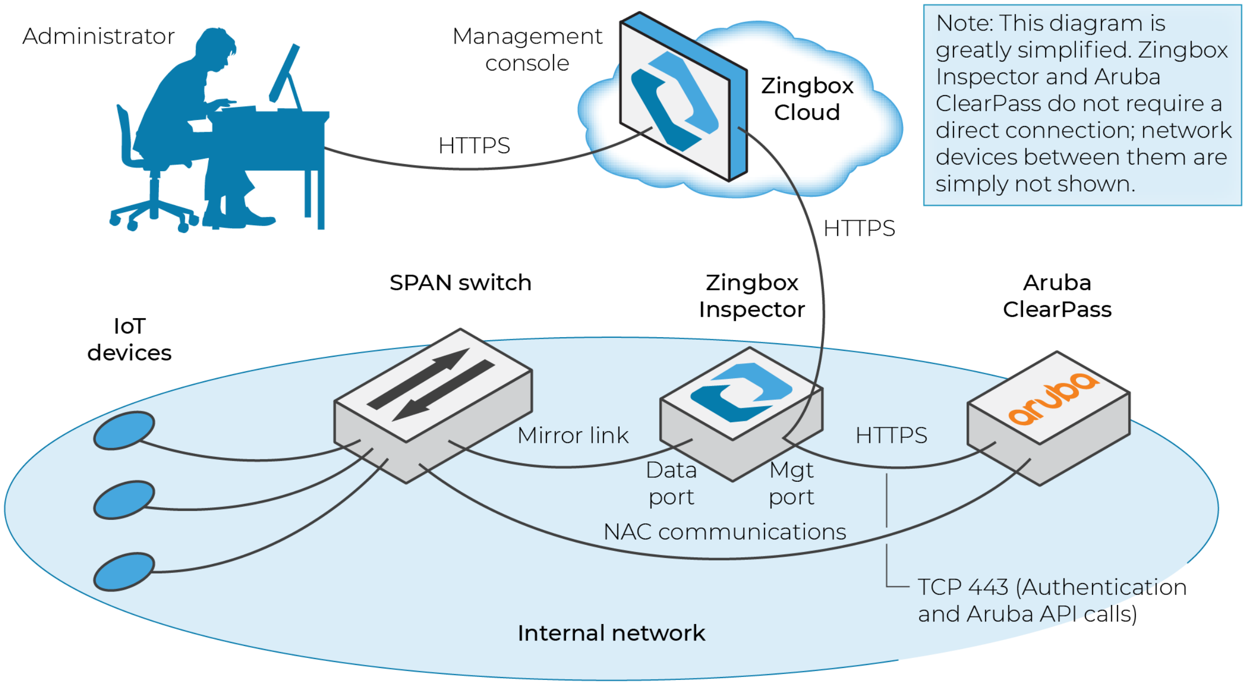
Zingbox IoT Guardian – Aruba ClearPass Integration Guide

Through a Zingbox-Aruba integration, Zingbox IoT Guardian can provide Aruba ClearPass with accurate IoT device identities and notify it whenever a security threat arises and device behavior veers from what is expected and safe. IoT Guardian does this by discovering IoT devices on the network, identifying and profiling them, and then reporting them to your ClearPass system. IoT Guardian also checks for security risks and anomalous behavior, and when it discovers any, it sends alerts to ClearPass for automated policy enforcement,

Through integration, IoT Guardian populates custom endpoint attributes on your ClearPass instance with Zingbox-learned device context and alerts. ClearPass can then use this context in NAC (network access control) policies to segment endpoints into VLANs for reduced risk exposure. In addition, with just a couple of clicks from the IoT Guardian management console, you can manually quarantine compromised devices identified by Zingbox alerts and later remove them from quarantine through ClearPass.

Make sure Zingbox Inspector can form an HTTPS connection to your ClearPass instance on TCP port 443.



Note: This diagram is greatly simplified. Zingbox Inspector and Aruba ClearPass do not require a direct connection; network devices between them are simply not shown.

Figure 1: Zingbox IoT Guardian and Aruba ClearPass integration

Aruba ClearPass

Note: These instructions are based on Aruba ClearPass 6.7.0. They should remain valid with later versions of ClearPass although it's possible that some elements in the GUI might change in the future.

1. Create an operator profile

You must use an operator profile that has full access to API services, ClearPass Insight, and ClearPass Policy Manager. If you already have such a profile, you can use that when configuring the RESTful API client. Otherwise, create a new profile as described here:

1. Log in to ClearPass Guest, click Administration > Operator Logins > Profiles > Create a new operator profile.
2. Enter the following in the *Operator Profile Editor* that appears, leave the other settings at their default values, and then click Save Changes:

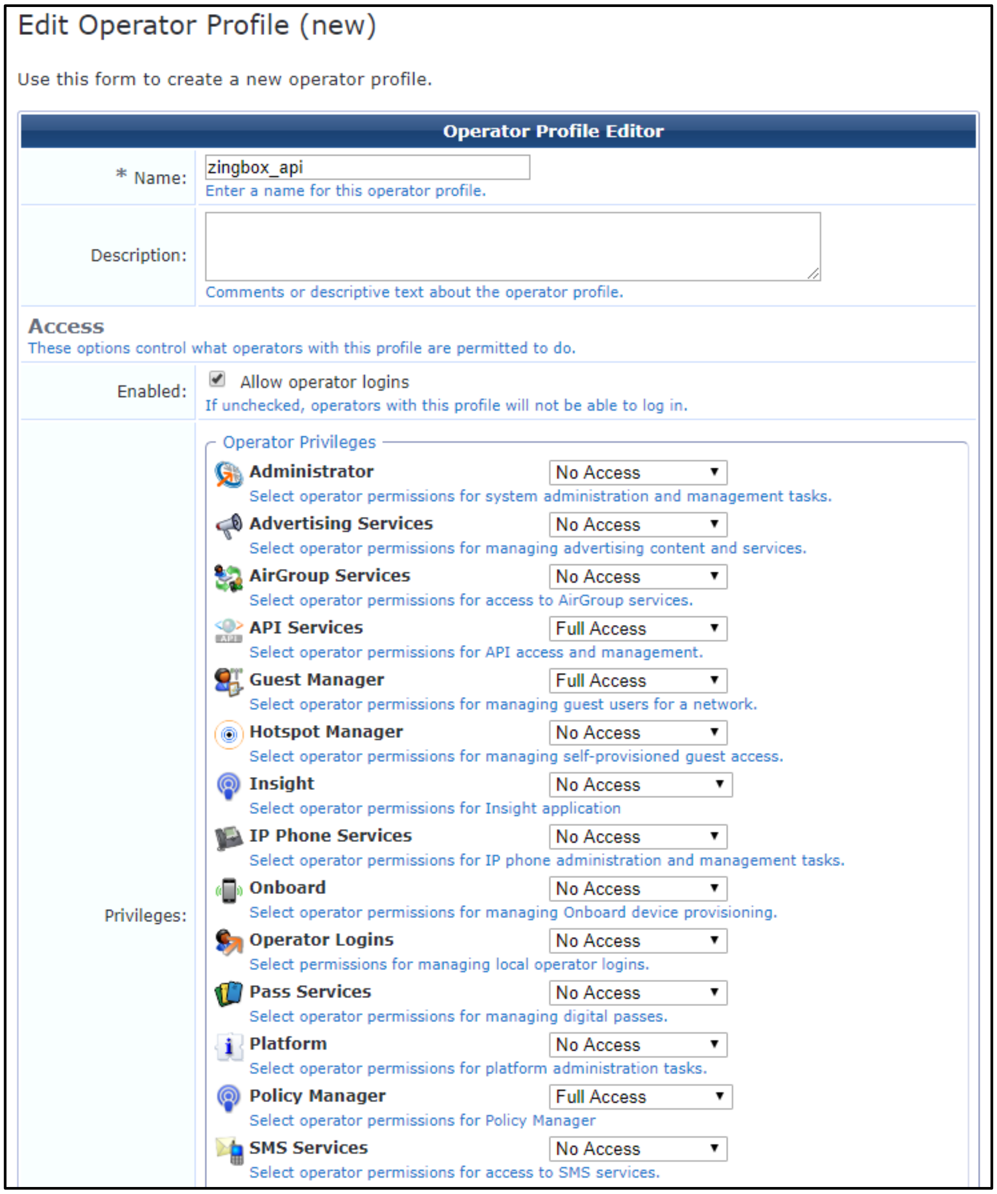
   Name: Enter a name for the profile, such as zingbox_api.

   Operator Privileges

      API Services: Full Access

      Insight: Full Access

      Policy Manager: Full Access



Edit Operator Profile (new)

Use this form to create a new operator profile.

Operator Profile Editor

* Name: zingbox_api
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:

Operator Privileges

Administrator — No Access
Select operator permissions for system administration and management tasks.

Advertising Services — No Access
Select operator permissions for managing advertising content and services.

AirGroup Services — No Access
Select operator permissions for access to AirGroup services.

API Services — Full Access
Select operator permissions for API access and management.

Guest Manager — Full Access
Select operator permissions for managing guest users for a network.

Hotspot Manager — No Access
Select operator permissions for managing self-provisioned guest access.

Insight — No Access
Select operator permissions for Insight application

IP Phone Services — No Access
Select operator permissions for IP phone administration and management tasks.

Onboard — No Access
Select operator permissions for managing Onboard device provisioning.

Operator Logins — No Access
Select permissions for managing local operator logins.

Pass Services — No Access
Select operator permissions for managing digital passes.

Platform — No Access
Select operator permissions for platform administration tasks.

Policy Manager — Full Access
Select operator permissions for Policy Manager

SMS Services — No Access
Select operator permissions for access to SMS services.

Figure 2: Aruba ClearPass Guest – Operator Profile Editor

2. Add a RESTful API client

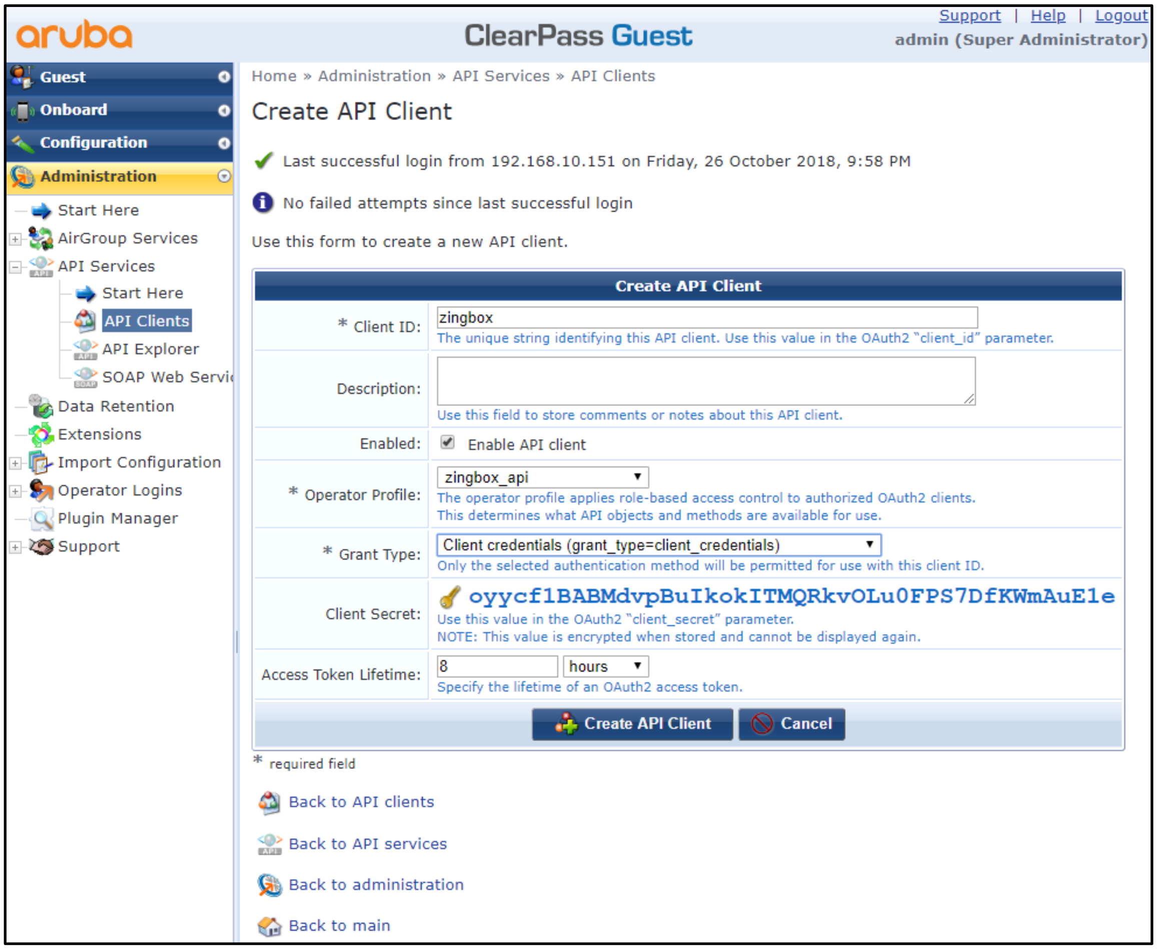
Define a client for the Zingbox Inspector to use when accessing the Aruba ClearPass API. There are two important settings that you must record so that you can enter them later when setting up Zingbox IoT Guardian: the client ID and client secret. The client uses the operator profile that you created in the previous step.

1. While still logged in to Aruba ClearPass Guest, click **Administration > API Services > API Clients > Create API Client**.
2. Enter the following in the *Create API Client* dialog box, leave the other settings at their default values, and then click **Create API Client**:

   Client ID: Enter a unique text string for the client ID. Note what it is so that you can enter it later when configuring the integration settings in the IoT Guardian management console.

   Operator Profile: Choose the operator profile you configured in the previous section; for example, **zingbox_api**.

   Grant Type: **Client credentials (grant_type=client_credentials)** When you choose this, ClearPass Guest automatically generates a client secret and displays it. Record the client secret for later use when configuring IoT Guardian.



Home » Administration » API Services » API Clients

Create API Client

✓ Last successful login from 192.168.10.151 on Friday, 26 October 2018, 9:58 PM

ℹ No failed attempts since last successful login

Use this form to create a new API client.

Create API Client

* Client ID:	zingbox 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:	zingbox_api ▾ 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:	Client credentials (grant_type=client_credentials) ▾ Only the selected authentication method will be permitted for use with this client ID.
Client Secret:	oyycf1BABMdvpBuIkokITMQRkvOLu0FPS7DfKWmAuE1e Use this value in the OAuth2 "client_secret" parameter. NOTE: This value is encrypted when stored and cannot be displayed again.
Access Token Lifetime:	8 hours ▾ Specify the lifetime of an OAuth2 access token.

Create API Client | Cancel

* required field

Back to API clients

Back to API services

Back to administration

Back to main

Figure 3: Aruba ClearPass Guest – Create API Client dialog box

3. Create a Zingbox endpoint attribute

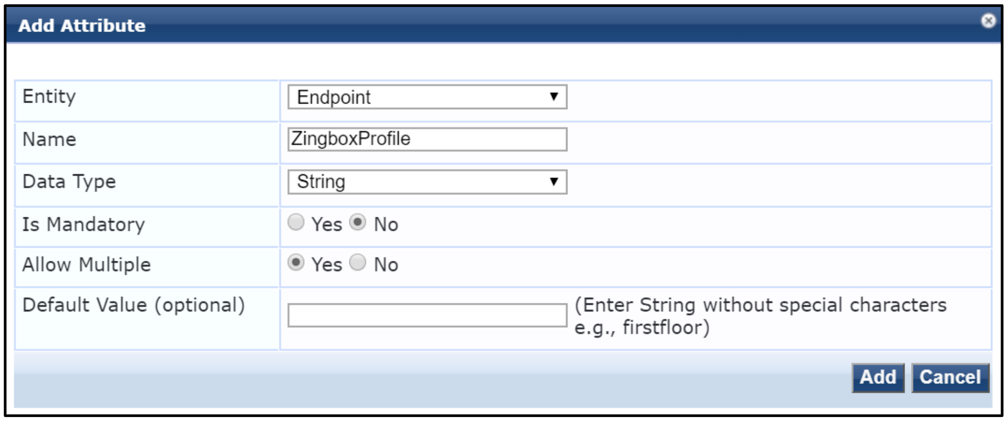
Create an endpoint attribute that Zingbox Inspector can populate with device profiles it learns and alerts it detects.

1. Log in to ClearPass Policy Manager and then click Administration > Dictionaries > Attributes > Add.
2. In the *Add Attributes* dialog box that appears, enter the following, leave the other values at their default settings, and then click Add:

   Entity: Endpoint

   Name: ZingboxProfile

   Data Type: String



Add Attribute

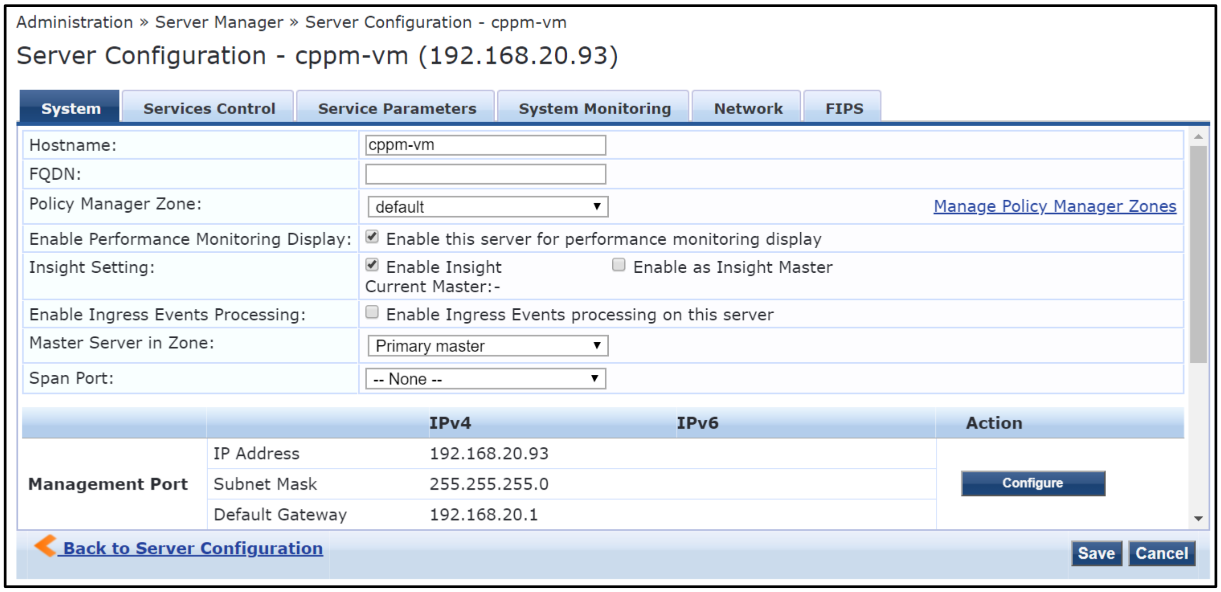
Entity	Endpoint ▾
Name	ZingboxProfile
Data Type	String ▾
Is Mandatory	○ Yes ● No
Allow Multiple	● Yes ○ No
Default Value (optional)	(Enter String without special characters e.g., firstfloor)

Figure 4: Aruba ClearPass Policy Manager – Add Attribute dialog box

4. Enable Insight

By enabling Insight, Zingbox Inspector can enrich the device characteristics it learns from monitoring network traffic with data from ClearPass.

1. While logged in to ClearPass Policy Manager, click Administration > Server Manager > Server Configuration, and then click your server name.
2. On the *System* tab, select Enable Insight, leave the other settings as they are, and then click Save.



Administration » Server Manager » Server Configuration - cppm-vm

Server Configuration - cppm-vm (192.168.20.93)

Hostname:	cppm-vm
FQDN:	
Policy Manager Zone:	default ▾ Manage Policy Manager Zones
Enable Performance Monitoring Display:	☑ Enable this server for performance monitoring display
Insight Setting:	☑ Enable Insight ☐ Enable as Insight Master Current Master:-
Enable Ingress Events Processing:	☐ Enable Ingress Events processing on this server
Master Server in Zone:	Primary master ▾
Span Port:	-- None -- ▾

		IPv4	IPv6	Action
Management Port	IP Address	192.168.20.93		Configure
	Subnet Mask	255.255.255.0		
	Default Gateway	192.168.20.1		

Figure 5: Aruba ClearPass Policy Manager – Server Configuration System tab

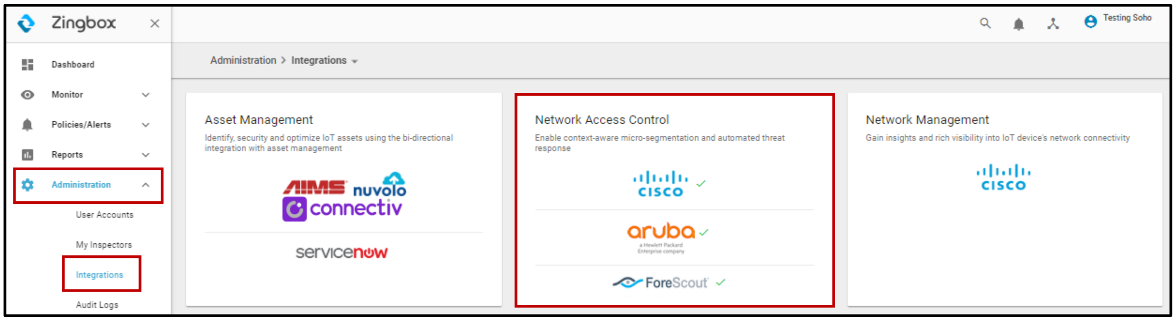
5. Configure policies and profiles

Once Zingbox IoT Guardian and Aruba ClearPass are integrated, IoT Guardian provides ClearPass with device profiles that you can then use to create security groups for defining network segments and access policies.

1. In ClearPass Policy Manager, click Configuration > Enforcement and add policies to segment IoT devices into VLANs based on ZingboxProfile attribute values.
2. While in the same *Enforcement* section, add enforcement profiles to isolate and quarantine devices based on alert-triggered notifications.

Zingbox IoT Guardian

1. From the IoT Guardian management console, click **Administration** > **Integrations** > **Network Access Control**.



Identify, security and optimize IoT assets using the bi-directional integration with asset management

Enable context-aware micro-segmentation and automated threat response

Gain insights and rich visibility into IoT device's network connectivity

Figure 6: Zingbox IoT Guardian - Integrations page

2. To configure Aruba ClearPass integration settings, click the **Edit** icon in the *ISE Integration* panel.

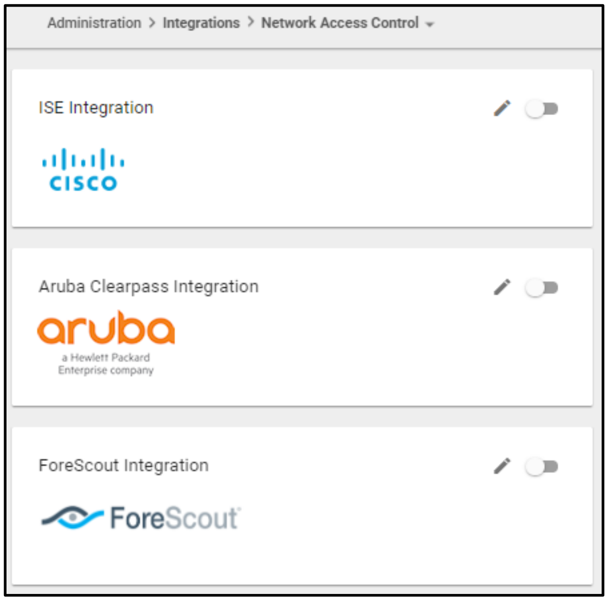

Administration > Integrations > Network Access Control
ISE Integration
cisco
Aruba Clearpass Integration
aruba
a Hewlett Packard Enterprise company
ForeScout Integration
ForeScout

Figure 7: Zingbox IoT Guardian - Network Access Control panel

3. Enter the following information in the form that appears:

   Host: Enter the IP address or host name of the Aruba ClearPass server with which the selected Zingbox Inspector will connect.

   Client ID: Enter the name of the client ID that you created earlier when configuring ClearPass. This is the ID that the Inspector will use when connecting to it.

   Client Secret: Enter the client secret that you recorded earlier when adding a RESTful API client to the ClearPass configuration.

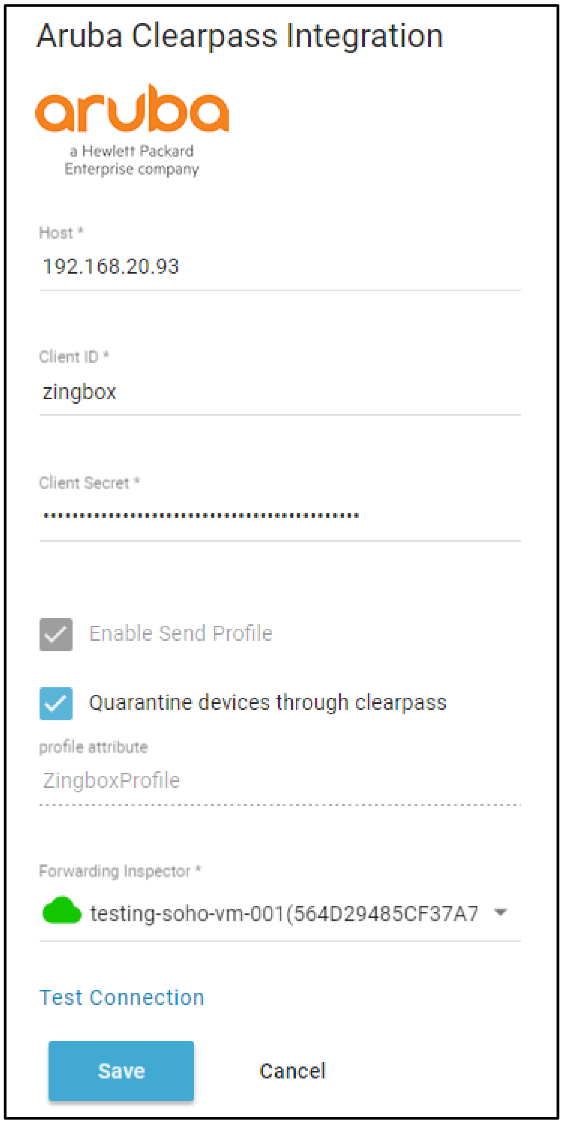
Enable Send Profile: (read only; always enabled)

Profile Attribute: ZingboxProfile (read only)

Quarantine devices through ClearPass: Select to enable an IoT Guardian administrator or owner to send commands to ClearPass to quarantine devices and remove devices from quarantine. Clear the check box to disable this option.

Forwarding Inspector: Choose an Inspector to interact with Aruba ClearPass and make sure the Inspector can reach it from its management interface.

Test Connection: Click to perform a one-time connection test between the chosen Inspector and the configured ClearPass system. (After you save the configuration, Zingbox Inspector automatically performs a periodic connection test with the ClearPass system in the background every ten minutes.)



Aruba Clearpass Integration

Host *
192.168.20.93

Client ID *
zingbox

Client Secret *
••

☑ Enable Send Profile

☑ Quarantine devices through clearpass

profile attribute
ZingboxProfile

Forwarding Inspector *
testing-soho-vm-001(564D29485CF37A7

Figure 8: Zingbox IoT Guardian – Aruba ClearPass Integration form

4. Click the Save button.

After you configure Aruba ClearPass and IoT Guardian, the chosen Zingbox inspector will start populating the ClearPass server with IoT device profiles and retrieving device data from ClearPass through Insight.

Put a device in quarantine

To put a device in quarantine through ClearPass from the IoT Guardian management console:

1. Click **Policies/Alerts > Alerts**, expand an alert policy based on machine learning, and select one of the alerts.
2. Click the **More** icon (···), click **Quarantine through ClearPass**, and then click **OK** when prompted to confirm the action.

Zingbox Inspector sends ClearPass a command to assign it to a quarantine VLAN. The device remains in quarantine while you investigate the cause of the alert. Once it's resolved, you can then use the "Release from quarantine via ClearPass" option.

Release a device from quarantine

Removing a device from quarantine is the same procedure as putting it in quarantine except that you select **Release from quarantine via ClearPass**. Zingbox Inspector sends ClearPass a command to clear the "Quarantine" status and ClearPass disconnects the device. When it reconnects, it is put in its normally assigned VLAN.

Conclusion

You've successfully configured both sides of an IoT Guardian and Aruba ClearPass integration and optionally configured them to work together to quarantine devices.