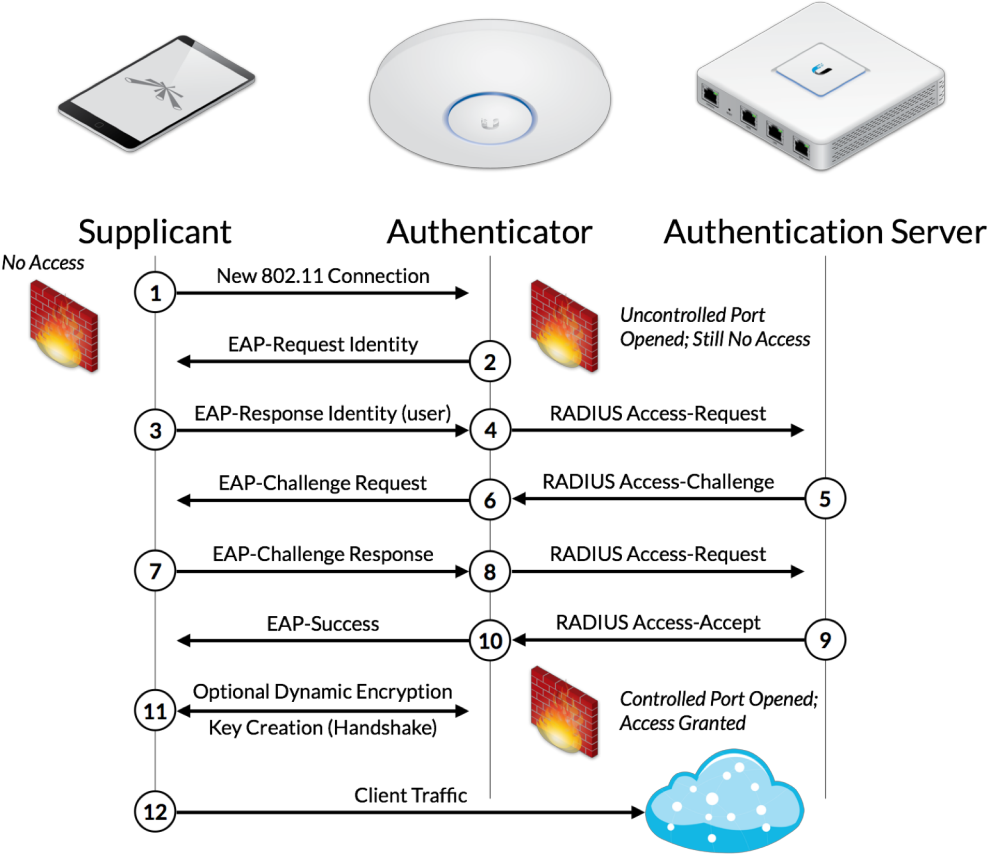


# Aruba CPPM (Clearpass Policy Manager)



# 802.1X Authentication (EAP & RADIUS)



# Configuring ClearPass for Mist as Radius Client



1) Adding Mist as the Radius Client in Aruba  
Configuration >> Network >> Devices

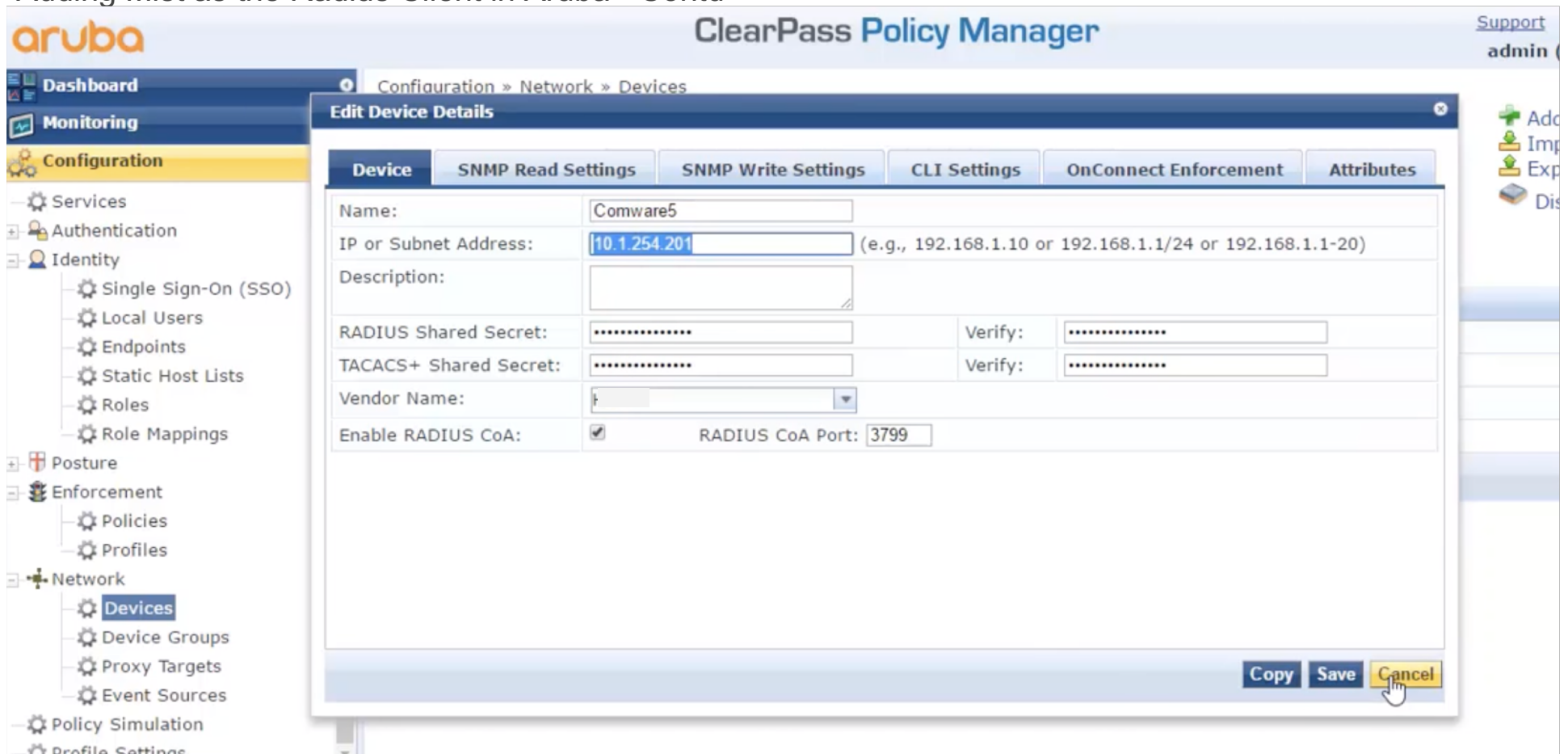
The screenshot shows the Aruba ClearPass Policy Manager interface. The left sidebar contains a navigation menu with categories: Dashboard, Monitoring, Configuration (selected), Services, Authentication, Identity, Posture, Enforcement, Network, and Policy Simulation. Under Configuration, the 'Network' folder is expanded, and 'Devices' is selected. The main content area displays 'Network Devices' with a breadcrumb trail 'Configuration > Network > Devices'. A filter bar at the top allows searching by Name, with a dropdown set to 'contains'. Below the filter is a table with 4 records:

| #  | <input type="checkbox"/> | Name ▲             | IP or Subnet Address | Description |
|----|--------------------------|--------------------|----------------------|-------------|
| 1. | <input type="checkbox"/> | AccessSwitch       | 10.1.254.100         |             |
| 2. | <input type="checkbox"/> | Comware5           | 10.1.254.201         |             |
| 3. | <input type="checkbox"/> | Comware7           | 10.1.254.202         |             |
| 4. | <input type="checkbox"/> | WirelessController | 10.1.254.31          |             |

Below the table, it says 'Showing 1-4 of 4'. At the bottom right of the table area are buttons for 'Copy', 'Export', and 'Delete'. On the right side of the interface, there are action buttons: 'Add', 'Import', 'Export All', and 'Discovered Devices'. The top right corner shows 'Support | Help | Logout' and the user 'admin (Super Administrator)'.

# Configuring ClearPass for Mist as Radius Client

Adding Mist as the Radius Client in Aruba - Contd



The screenshot displays the Aruba ClearPass Policy Manager interface. The left sidebar shows the navigation menu with 'Configuration' selected. The main content area shows the 'Edit Device Details' form for a device named 'Comware5'. The form includes fields for Name, IP or Subnet Address (10.1.254.201), Description, RADIUS Shared Secret, TACACS+ Shared Secret, Vendor Name, and Enable RADIUS CoA (checked). The RADIUS CoA Port is set to 3799. The form is divided into tabs: Device, SNMP Read Settings, SNMP Write Settings, CLI Settings, OnConnect Enforcement, and Attributes. The 'Device' tab is active. At the bottom right of the form, there are buttons for 'Copy', 'Save', and 'Cancel'.

| Device                 | SNMP Read Settings  | SNMP Write Settings | CLI Settings | OnConnect Enforcement | Attributes |
|------------------------|---|---------------------|--------------|-----------------------|------------|
| Name:                  | Comware5  |                     |              |                       |            |
| IP or Subnet Address:  | 10.1.254.201 (e.g., 192.168.1.10 or 192.168.1.1/24 or 192.168.1.1-20) |                     |              |                       |            |
| Description:           |   |                     |              |                       |            |
| RADIUS Shared Secret:  | .....   | Verify:             | .....        |                       |            |
| TACACS+ Shared Secret: | .....   | Verify:             | .....        |                       |            |
| Vendor Name:           | [Dropdown]  |                     |              |                       |            |
| Enable RADIUS CoA:     | <input checked="" type="checkbox"/>                                   | RADIUS CoA Port:    | 3799         |                       |            |

# Creating Roles in ClearPass

## 2) Adding a Role In Aruba

Configuration -> Identity -> Roles

Configuration » Identity » Roles

### Roles

Filter:

| #  | <input type="checkbox"/> | Name ▲             |
|----|--------------------------|--------------------|
| 1. | <input type="checkbox"/> | staff-role-aruba   |
| 2. | <input type="checkbox"/> | staff-role-cisco   |
| 3. | <input type="checkbox"/> | student-role-aruba |
| 4. | <input type="checkbox"/> | student-role-cisco |

Showing 1-4 of 4

# Tie Role to the Group (AD)

## 3) Mapping AD Group to a Role In Aruba

Configuration -> Identity -> Roles Mappings -> Add

Configuration » Identity » Role Mappings » Add

### Role Mappings

Policy Mapping Rules Summary

Rules Evaluation Algorithm:  Select first match  Select all matches

Role Mapping Rules:

| Conditions   | Role Name          |
|--|--------------------|
| 1. (Authorization:AD:memberOf CONTAINS StaffGroup)<br>AND (Connection:NAD-IP-Address BELONGS_TO_GROUP aruba-device)            | staff-role-aruba   |
| 2. (Authorization:AD:memberOf CONTAINS StaffGroup)<br>AND (Connection:NAD-IP-Address BELONGS_TO_GROUP cisco-wireless-device)   | staff-role-cisco   |
| 3. (Authorization:AD:memberOf CONTAINS StudentGroup)<br>AND (Connection:NAD-IP-Address BELONGS_TO_GROUP aruba-device)          | student-role-aruba |
| 4. (Authorization:AD:memberOf CONTAINS StudentGroup)<br>AND (Connection:NAD-IP-Address BELONGS_TO_GROUP cisco-wireless-device) | student-role-cisco |

Add Rule Move Up Move Down

# AVP tied to a Enforcement Profile



4) Add relevant attributes to the Enforcement Profile  
(In this case, Airespace-ACL-Name and Airespace-Interface-Name)

Configuration -> Enforcement -> Profiles -> Edit Enforcement Profile

| Summary             | Profile                  | Attributes    |
|---------------------|--------------------------|---------------|
| <b>Profile:</b>     |                          |               |
| Name:               | secure-staff-cisco       |               |
| Description:        |                          |               |
| Type:               | RADIUS                   |               |
| Action:             | Accept                   |               |
| Device Group List:  | -                        |               |
| <b>Attributes:</b>  |                          |               |
| Type                | Name                     | Value         |
| 1. Radius:Airespace | Airespace-ACL-Name       | = secure_user |
| 2. Radius:Airespace | Airespace-Interface-Name | = staff_wifi  |

# Policy Enforcement

## 5) Add Policy

Configuration -> Enforcement -> Policies -> Add

| Enforcement                 | Rules                                 | Summary                       |
|-----------------------------|---------------------------------------|-------------------------------|
| <b>Enforcement:</b>         |                                       |                               |
| Name:                       | secure wireless enforcement policy    |                               |
| Description:                |                                       |                               |
| Enforcement Type:           | RADIUS                                |                               |
| Default Profile:            | [Deny Access Profile]                 |                               |
| <b>Rules:</b>               |                                       |                               |
| Rules Evaluation Algorithm: | First applicable                      |                               |
| Conditions                  |                                       | Actions                       |
| 1.                          | (Tips:Role EQUALS staff-role-aruba)   | [RADIUS] secure-staff-aruba   |
| 2.                          | (Tips:Role EQUALS staff-role-cisco)   | [RADIUS] secure-staff-cisco   |
| 3.                          | (Tips:Role EQUALS student-role-aruba) | [RADIUS] secure-student-aruba |
| 4.                          | (Tips:Role EQUALS student-role-cisco) | [RADIUS] secure-student-cisco |



# Bring it all together as a service



6) Configure Service to reflect the profile and policy  
Configuration -> Services-> Add

| Service                                | Authentication   | Authorization | Roles           | Enforcement  | Summary |
|--|--|---------------|-----------------|--|---------|
| <b>Service:</b>                        |  |               |                 |  |         |
| Type:                                  | 802.1X Wireless  |               |                 |  |         |
| Name:                                  | secure wireless service  |               |                 |  |         |
| Description:                           | 802.1X Wireless Access Service                                       |               |                 |  |         |
| Monitor Mode:                          | Disabled   |               |                 |  |         |
| More Options:                          | Authorization  |               |                 |  |         |
| <b>Service Rule</b>                    |  |               |                 |  |         |
| Match ALL of the following conditions: |  |               |                 |  |         |
|  | <b>Type</b>  | <b>Name</b>   | <b>Operator</b> | <b>Value</b>   |         |
| 1.                                     | Radius:IETF  | NAS-Port-Type | EQUALS          | Wireless-802.11 (19)                                   |         |
| 2.                                     | Radius:IETF  | Service-Type  | BELONGS_TO      | Login-User (1), Framed-User (2), Authenticate-Only (8) |         |
| 3.                                     | Connection   | SSID          | CONTAINS        | secure   |         |
| <b>Authentication:</b>                 |  |               |                 |  |         |
| Authentication Methods:                | 1. [EAP PEAP]<br>2. [EAP TLS]  |               |                 |  |         |
| Authentication Sources:                | AD [Active Directory]  |               |                 |  |         |
| Strip Username Rules:                  | -  |               |                 |  |         |
| <b>Authorization:</b>                  |  |               |                 |  |         |
| Authorization Details:                 | 1. [Endpoints Repository] [Local SQL DB]<br>2. AD [Active Directory] |               |                 |  |         |
| <b>Roles:</b>                          |  |               |                 |  |         |
| Role Mapping Policy:                   | secure wireless role mapping   |               |                 |  |         |
| <b>Enforcement:</b>                    |  |               |                 |  |         |
| Use Cached Results:                    | Disabled   |               |                 |  |         |
| Enforcement Policy:                    | secure wireless enforcement policy                                   |               |                 |  |         |