Aruba ClearPass NAC Configuration

**1. Aruba ClearPass 802.1X**

Policies, Profiling, Policy Enforcement, Segmentation, and Posture Assessment

**a. Service Configuration**

* **CORP-WiFi**:
  + **Authentication Method**: EAP-TLS
  + **Authorization Source**: Active Directory
  + **Enforcement Profile**: Assign VLAN 10 and full intranet access
  + **Authentication Method**: PEAP-MSCHAPv2
  + **Authorization Source**: Active Directory
  + **Enforcement Profile**: Assign VLAN 20, Internet access, and MDM compliance check
* **Guest**:
  + **Authentication Method**: Captive Portal with RADIUS
  + **Enforcement Profile**: Assign VLAN 30 and Internet-only access
* **IoT**:
  + **Authentication Method**: MAC Authentication (MAB) or Certificate-based
  + **Enforcement Profile**: Assign VLAN 40 and restricted access

**b. Profiling**

Enable device profiling to identify device types and apply appropriate policies.

**c. Policy Enforcement**

Use role-based access control to enforce policies based on user roles and device types.

**d. Segmentation**

Implement VLAN assignments and access control lists (ACLs) to segment network traffic appropriately.

**e. Posture Assessment**

Integrate with MDM solutions like Intune to assess device posture and compliance status.

**2. RADIUS Server Settings**

* **Configuration Steps**:
  1. Navigate to **Administration > Server Manager > Server Configuration**.
  2. Select the Policy Manager server.
  3. Under the **Service Parameters** tab, choose **RADIUS Server**.
  4. Configure parameters such as **Request Expire Time** (e.g., 60 seconds) to accommodate authentication processing times.

**3. Certificate Requirements**

ClearPass requires two primary certificates:

**RADIUS Server Certificate**: Used for EAP authentication.

1. **HTTPS Web Server Certificate**: Used for the WebGUI and captive portal access.

Ensure that these certificates are signed by a trusted Certificate Authority (CA) and are properly installed on the ClearPass server.

**4. Active Directory Configuration to Support NAC**

* **Integration Steps**:
  1. Navigate to **Configuration > Authentication > Sources**.
  2. Add a new authentication source of type **Active Directory**.
  3. Provide the necessary domain information and credentials.
  4. Test the connection to ensure successful integration.

This integration allows ClearPass to authenticate users and retrieve group membership information for policy enforcement.

**5. Intune Configuration for Device Compliance**

* **Integration Steps**:
  1. Install the ClearPass Intune Extension.
  2. Configure the extension to communicate with Microsoft Intune.
  3. Ensure that device certificates include the Intune device ID in the Subject Alternative Name (SAN) field.
  4. Set up periodic synchronization to retrieve compliance data from Intune.

This setup enables ClearPass to enforce access policies based on device compliance status reported by Intune.

**6. AP Network Architecture: Centralized and Distributed Models**

**a. Centralized Model**

* **Use Case Fit**: University campuses, medium/large enterprise headquarters, research institutions.
* **Architecture**:
  + Deploy Aruba Mobility Controllers to manage APs centrally.
  + Use ClearPass for centralized authentication and policy enforcement.
  + Implement VLANs and roles to segment traffic.

**b. Distributed Model**

* **Use Case Fit**: Retail branches, distributed enterprise sites, regional offices, small campuses.
* **Architecture**:
  + Deploy Instant APs (IAPs) managed via Aruba Central.
  + Use ClearPass for authentication and policy enforcement.
  + Implement local VLANs and roles at each site.

**Aruba ClearPass Configuration Output for Enterprise NAC**

**1. Aruba ClearPass Policies**

**Service Configuration (802.1X)**

services:

* name: CORP-WiFi-802.1X type: 802.1X Wireless authentication\_method: EAP-TLS enforcement\_policy: Corp-Access-Enforcement role\_mapping\_policy: Corp-Role-Mapping
* name: BYOD-802.1X type: 802.1X Wireless authentication\_method: PEAP-MSCHAPv2 enforcement\_policy: BYOD-Enforcement posture\_policy: BYOD-Posture role\_mapping\_policy: BYOD-Role-Mapping
* name: Guest-Access type: Captive Portal authentication\_method: Web Login + RADIUS enforcement\_policy: Guest-Enforcement
* name: IoT-Devices type: MAC Authentication authentication\_method: MAB or Certificate enforcement\_policy: IoT-Enforcement

**Enforcement Profiles**

enforcement\_profiles:

* name: Corp-VLAN10 type: VLAN vlan: 10
* name: BYOD-VLAN20 type: VLAN vlan: 20
* name: Guest-VLAN30 type: VLAN vlan: 30
* name: IoT-VLAN40 type: VLAN vlan: 40

**Enforcement Policies**

enforcement\_policies:

* name: Corp-Access-Enforcement rules:
  + condition: [TLS Certificate Valid, AD Group = 'CorpUsers'] action: [Corp-VLAN10, Permit Full Access]
* name: BYOD-Enforcement rules:
  + condition: [MDM Compliant, AD Group = 'BYOD'] action: [BYOD-VLAN20, Internet Access Only]
* name: Guest-Enforcement rules:
  + condition: [Guest Web Login Success] action: [Guest-VLAN30, NAT Access]
* name: IoT-Enforcement rules:
  + condition: [MAC in IoT Device DB] action: [IoT-VLAN40, Restricted ACL]

**Role Mapping Policies**

role\_mapping\_policies:

* name: Corp-Role-Mapping mapping:
  + condition: [AD Group = 'CorpUsers'] role: Corp-User
* name: BYOD-Role-Mapping mapping:
  + condition: [AD Group = 'BYOD'] role: BYOD-User

**2. RADIUS Server Settings**

radius: shared\_secret: auth\_ports: [1812] acct\_ports: [1813] retries: 3 timeout: 5 NAS-IP-Address: Dynamic Authorization Support: Enabled (CoA)

**3. Certificate Requirements**

certificates: server\_cert: issuer: Public CA or Enterprise PKI SAN: clearpass.company.com key\_usage: DigitalSignature, KeyEncipherment ext\_key\_usage: ServerAuth client\_cert: issuer: Intune / SCEP / Internal CA key\_usage: DigitalSignature, KeyEncipherment ext\_key\_usage: ClientAuth

**4. AD Configuration for NAC**

active\_directory: bind\_dn: CN=ClearPassService, OU=ServiceAccounts,DC=company,DC=com bind\_password: base\_dn: DC=company,DC=com join\_domain: true group\_lookup:

- name: CorpUsers

- name: BYOD

- name: Admins

authentication\_source: name: AD-Source type: Active Directory servers:

- ad1.company.com

- ad2.company.com

**5. Intune Configuration**

intune\_integration: tenant\_id: client\_id: client\_secret: api\_scope: <https://graph.microsoft.com/.default> compliance\_check: endpoint\_attribute: compliant action: Allow or Redirect to Remediate integration\_type: REST API (ClearPass Extensions)

**6. AP Network Architecture**

**Centralised**

centralised\_ap\_design: controller: Aruba Mobility Master (Cloud) ap\_model: Aruba AP-515 roaming: L2/L3 with Fast Transition (802.11r/k/v) ssid\_configs:

- name: CORP-WiFi

auth: 802.1X (EAP-TLS)

vlan: 10

qos: WMM, DSCP EF

- name: BYOD

auth: 802.1X (PEAP)

vlan: 20

posture: Enabled

- name: GUEST

auth: Captive Portal

vlan: 30

- name: IOT

auth: MAC Auth

vlan: 40

**Distributed**

**Use case: Retail branches or regional sites**

distributed\_ap\_design: controller: None (Aruba Instant APs or Meraki APs) cloud\_dashboard: Aruba Central / Meraki Dashboard radius\_proxy: SecureW2 or Portnox Cloud RADIUS ssid\_configs:

- name: CORP-WiFi

auth: EAP-TLS

vlan: 10

- name: BYOD

auth: PEAP-MSCHAPv2

vlan: 20

- name: GUEST

auth: Splash or NAT

vlan: 30

- name: IOT

auth: MAC-Based

vlan: 40

Aruba ClearPass, **Posture Assessment integrated with Microsoft Intune**

[ **ClearPass' built-in integration with Intune via Microsoft Graph API**. This enables real-time compliance checks and policy decisions based on device health and posture status as reported by Intune.]

Real-Time Intune Integration for Posture

**1. API Integration Setup**

* ClearPass uses **OAuth 2.0 and Microsoft Graph API** to query Intune.
* You register **ClearPass as an enterprise application** in Azure AD.
* Permissions required typically include:
  + DeviceManagementManagedDevices.Read.All
  + Device.Read.All
  + Directory.Read.All

**2. Azure App Registration (Steps in Azure Portal)**

* Register a new app in Azure AD.
* Generate a **Client ID**, **Client Secret**, and **Tenant ID**.
* Grant appropriate API permissions.
* Add admin consent for the permissions.
* Configure **redirect URI** if needed.

**3. ClearPass Configuration**

* Navigate to **Administration > External Servers > Endpoint Context Servers**.
* Add **Microsoft Intune as a context server**:
  + Use https://graph.microsoft.com as the API base.
  + Input Azure app credentials (Client ID, Secret, Tenant ID).
* Enable **Endpoint Context Servers in the Posture Policy settings**.

**4. Posture Evaluation in Policy Flow**

* When a device connects to the network (e.g., 802.1X):
  + ClearPass uses the MAC address or user identity to **query Microsoft Graph**.
  + It fetches **real-time device compliance status** from Intune (e.g., compliant, not compliant).
* ClearPass evaluates this data in the **Role Mapping and Enforcement Policies**:
  + Example: Assign “Quarantine VLAN” if device is **non-compliant**.
  + Or allow full access for **compliant** and domain-joined devices.

**Example Policy Usage**

If Device OS is Windows AND Intune Compliance = False THEN assign VLAN 50 (Remediation)

If Device OS is iOS AND Intune Compliance = True THEN assign VLAN 10 (Trusted)

**Additional Considerations**

* **Latency**: Queries are in near real-time (~seconds).
* **Caching**: You can configure how long posture data is cached in ClearPass.
* **Scalability**: Scales well in large environments due to API-based pull model.
* **Fallback**: Design fallback behavior in case API fails (e.g., default to guest or deny access).

**How Intune Compliance Is Used in ClearPass Policy Flow**

**1. Role Mapping Policy**

This is where ClearPass **evaluates context** (like Intune compliance) and assigns roles based on conditions.

**Example Role Mapping Rule:**

Condition: Endpoint Posture Source = Intune AND Compliance Status = NonCompliant

Action: Assign Role = Intune\_NonCompliant

Other conditions can include:

* Device OS
* Endpoint category (e.g., BYOD, corporate)
* AD group membership
* MDM status from Intune

**2. Enforcement Policy**

This is where ClearPass **applies the action** — like assigning VLANs, downloadable ACLs, or triggering redirection.

**Example Enforcement Rule:**

Condition: Role = Intune\_NonCompliant

Action: VLAN Assignment = Quarantine\_VLAN (e.g., VLAN 50)

Other actions can include:

* Send CoA (Change of Authorization) to the switch/AP
* Trigger captive portal
* Deny access
* Redirect to remediation URL

**Integration Summary**

* **Intune API** → provides posture info (e.g., compliant, non-compliant).
* **ClearPass Role Mapping** → uses this info to classify the device.
* **ClearPass Enforcement** → takes action based on the assigned role.

**Aruba ClearPass Role Mapping Policy** and **Enforcement Policy** that integrates **Intune compliance posture** for conditional access.

This YAML format assumes usage of **ClearPass REST API (v6.9+)** compatible fields. Tailor object IDs and names as per your environment.

Intune\_posture\_policy.yaml needs to be structured with keys like role\_mapping\_policies, enforcement\_profiles, and enforcement\_policies

**Intune-integrated Posture Assessment**, **Role Mapping**, and **Policy Enforcement**:

* **Role Mapping** uses Endpoint:Posture-Status which is populated from the **Intune Compliance API via ClearPass Extension/REST integration**.
* **Enforcement Profiles** apply VLANs and roles based on mapped posture status.
* **Enforcement Policy** chooses the correct action/profile based on the assigned role from Role Mapping.

📄 intune\_posture\_policy.yaml

role\_mapping\_policies:

- name: "Intune\_Posture\_Classification"

description: "Assign roles based on Intune compliance posture"

rules:

- condition:

- type: "Endpoint Posture"

attribute: "MDM Compliance Status"

operator: "EQUALS"

value: "Compliant"

role: "Intune\_Compliant"

- condition:

- type: "Endpoint Posture"

attribute: "MDM Compliance Status"

operator: "EQUALS"

value: "NonCompliant"

role: "Intune\_NonCompliant"

- condition:

- type: "Endpoint Posture"

attribute: "MDM Compliance Status"

operator: "EQUALS"

value: "Unknown"

role: "Intune\_Unknown"

enforcement\_policies:

- name: "Enforce\_Access\_Based\_On\_Intune\_Posture"

description: "Policy enforcement based on Intune roles"

rules:

- condition:

- type: "Role"

operator: "EQUALS"

value: "Intune\_Compliant"

action:

type: "Allow Access"

vlan: 10

enforcement\_profile: "Permit-Full-Access"

- condition:

- type: "Role"

operator: "EQUALS"

value: "Intune\_NonCompliant"

action:

type: "Quarantine"

vlan: 50

enforcement\_profile: "Deny-Or-Redirect"

- condition:

- type: "Role"

operator: "EQUALS"

value: "Intune\_Unknown"

action:

type: "Guest-Access"

vlan: 30

enforcement\_profile: "Redirect-To-Onboarding"

enforcement\_profiles:

- name: "Permit-Full-Access"

description: "Grants full network access"

type: "RADIUS Accept"

attributes:

- key: "Tunnel-Private-Group-ID"

value: "10"

- key: "Tunnel-Type"

value: "VLAN"

- key: "Tunnel-Medium-Type"

value: "IEEE-802"

- name: "Deny-Or-Redirect"

description: "Redirects to remediation portal"

type: "RADIUS Reject with Redirect"

attributes:

- key: "Aruba-User-Role"

value: "remediation"

- name: "Redirect-To-Onboarding"

description: "Redirects unknown clients to onboarding"

type: "RADIUS Accept with URL Redirect"

attributes:

- key: "Aruba-User-Role"

value: "onboard"

**Integration Steps Summary:**

1. **Intune API Integration**: Set up via ClearPass Extension > Intune Extension.
2. **Posture Source Mapping**: Ensure posture data appears in endpoint context.
3. **Roles**: Configure Intune\_Compliant, Intune\_NonCompliant, etc.
4. **Enforcement Profiles**: Must be predefined or imported.
5. **Policy Upload**: Use ClearPass API or import manually via GUI (CSV/XML/YAML supported).

Aruba ClearPass NAC Operational Guide

# 1. Runbook: Aruba ClearPass NAC Day 0, Day 1, and Day 2 Tasks

## Day 0 – Planning and Initial Configuration

- Rack and stack ClearPass appliance or deploy VM.  
- IP addressing and hostname assignment.  
- DNS, NTP, and default gateway configuration.  
- Install licenses and verify subscription status.  
- Set up RADIUS and TACACS shared secrets.  
- Create initial admin users and roles.  
- Configure integration with Active Directory.  
- Upload server certificates (RADIUS and HTTPS).  
- Backup system after base configuration.

## Day 1 – Service and Policy Deployment

- Configure RADIUS services (802.1X, MAB, Guest, BYOD).  
- Define authentication sources (AD, Local, Endpoint Repository).  
- Set up profiling methods (DHCP, HTTP, SNMP, etc.).  
- Create enforcement policies (role-based, VLAN assignments).  
- Integrate with MDM/UEM (e.g., Intune) for posture and compliance.  
- Create and assign roles for different device types.  
- Verify authentication and access control using test clients.  
- Enable logging, alerts, and syslog forwarding.

## Day 2 – Operational Maintenance and Monitoring

- Daily: Monitor live sessions, policy matches, system health.  
- Weekly: Review authentication logs and enforcement trends.  
- Monthly: Review posture compliance, update firmware if needed.  
- Quarterly: Validate backups and export configurations.  
- As Needed: Troubleshoot failed authentications, renew expiring certs, refine profiling fingerprints.

# 2. Ansible Playbook: ClearPass Configuration and Operational Backup

Below is an example Ansible playbook that connects to ClearPass API to export configuration and operational backups.

---  
- name: Backup ClearPass Configuration and Operational Data  
 hosts: localhost  
 gather\_facts: no  
 vars:  
 cppm\_host: "clearpass.example.com"  
 cppm\_username: "api\_user"  
 cppm\_password: "secure\_password"  
 backup\_path: "/backups/clearpass/"  
 tasks:  
 - name: Get Access Token  
 uri:  
 url: "https://{{ cppm\_host }}/api/oauth"  
 method: POST  
 body: "grant\_type=password&username={{ cppm\_username }}&password={{ cppm\_password }}"  
 headers:  
 Content-Type: "application/x-www-form-urlencoded"  
 return\_content: yes  
 validate\_certs: no  
 register: auth\_response  
  
 - name: Download Configuration Backup  
 uri:  
 url: "https://{{ cppm\_host }}/api/backup/config"  
 method: GET  
 headers:  
 Authorization: "Bearer {{ auth\_response.json.access\_token }}"  
 dest: "{{ backup\_path }}/cppm\_config\_backup.tar.gz"  
 validate\_certs: no  
  
 - name: Download Operational Backup  
 uri:  
 url: "https://{{ cppm\_host }}/api/backup/operational"  
 method: GET  
 headers:  
 Authorization: "Bearer {{ auth\_response.json.access\_token }}"  
 dest: "{{ backup\_path }}/cppm\_operational\_backup.tar.gz"  
 validate\_certs: no

# 3. ClearPass CLI Output: Policy Sets

Below is a sample CLI-style output of policy sets based on your customer environment:

Policy Set: CORP-WiFi  
---------------------------------  
Authentication Method : EAP-TLS  
Authentication Source : Active Directory  
Role Mapping : Employee, Trusted Device  
Enforcement Profile : VLAN 10, Access Role: corp\_full\_access  
  
Policy Set: BYOD-Secure  
---------------------------------  
Authentication Method : PEAP-MSCHAPv2  
Authentication Source : Active Directory  
Role Mapping : Employee, Non-Compliant  
Enforcement Profile : VLAN 20, Access Role: internet\_only  
  
Policy Set: Guest  
---------------------------------  
Authentication Method : Captive Portal (ClearPass)  
Authentication Source : Local Guest Repository  
Role Mapping : Guest  
Enforcement Profile : VLAN 30, Access Role: guest\_internet  
  
Policy Set: IoT  
---------------------------------  
Authentication Method : MAC Authentication / Certificate  
Authentication Source : Endpoint Repository  
Role Mapping : IoT Device  
Enforcement Profile : VLAN 40, Access Role: restricted  
  
Profiling Enabled: Yes (DHCP Fingerprinting, SNMP, HTTP User-Agent)  
Posture Assessment: Integrated with Intune via API, Real-time device compliance checks.  
Segmentation: VLAN assignment + ACLs enforced at edge (wired/wireless)