Validated Solution Guide

Aruba Solution TME

May 28, 2025

Table of Contents

ESP Policy Deploy

This guide is written to help IT professionals with prescriptive steps to deploy an effective policy enforcement solution for Orange Widget Logistics (OWL), a fictional enterprise described on the Reference Customer page.

The guide offers instructions for implementing the solution across corporate offices and remote branches using the following products:

- Aruba CX 6300 Series Switches
- Aruba 9000 Series Gateways
- Aruba 500 & 600 Series Access Points
- Aruba ClearPass Policy Manager
- Windows Server 2022 Active Directory Domain Services
- Microsoft Entra ID (Formerly Azure AD)
- VMWare vSphere

Document Conventions

Bold text indicates a command, navigational path, or a user interface element.

Examples:

- the **show port-access client** command
- Go to **Configuration > Identity > Role Mappings**

Italic text indicates important terminology or a value in a user interface field.

Examples:

- The *Enforcement Policy* determines ClearPass's authentication response based on its configured Rules list and is processed from the top down.
- **Name**: *RSVC-CP01*

Shaded blocks indicate variables for which you should substitute a value appropriate for your environment.

Example:

- VRRP VIP: `10.0.5.1`

NOTE:

For the most up-to-date information on ESP Policy solutions, please refer to the Validated Solution Guide Program

Introduction to Aruba Policy Enforcement

The Aruba Edge Services Platform (ESP) architecture provides the components needed to design and implement a comprehensive, zero-trust network across a modern enterprise. Aruba ESP enables consistent policy enforcement on the campus, across the WAN, within branches, and in the data center.

Purpose of This Guide

This deployment guide covers Policy enforcement in an Aruba Edge Services Platform (ESP) architecture. The guide provides guidance on design choices, with considerations for deploying effective security policies while interoperating with a commonly available user database such as Microsoft Active Directory.

Example reference designs illustrating the hardware, software, and logical workflow for this solution provide an example and aid in understanding the steps needed to secure edge switch ports and wireless access points for Orange Widget Logistics (OWL), the fictional customer described in the Reference Customer page.

Audience

This guide is written for IT professionals responsible for deploying an Aruba ESP campus network. These IT professionals perform a variety of roles:

- Systems engineers who require a standard set of procedures for implementing solutions
- Project managers who develop scopes of work for Aruba implementations
- Aruba partners who sell technology or create implementation documentation.

Not Covered in This Guide

This guide does not cover:

- Detailed VM host configuration
- Detailed Central WLAN configuration
- Detailed supplicant configuration
- Detailed Windows server configuration

Customer Use Case

Network access for OWL employees and guests currently consists of statically configured edge switch ports that rely on physical security to prevent unauthorized access. They offer no visibility to determine which authorized or unauthorized devices are physically connected to their network.

OWL's IT Infrastructure team is centralized at the Roseville, CA campus. Like many enterprise companies, OWL has no IT Network Engineering presence in other branches or remote office locations.

Campuses and Branches

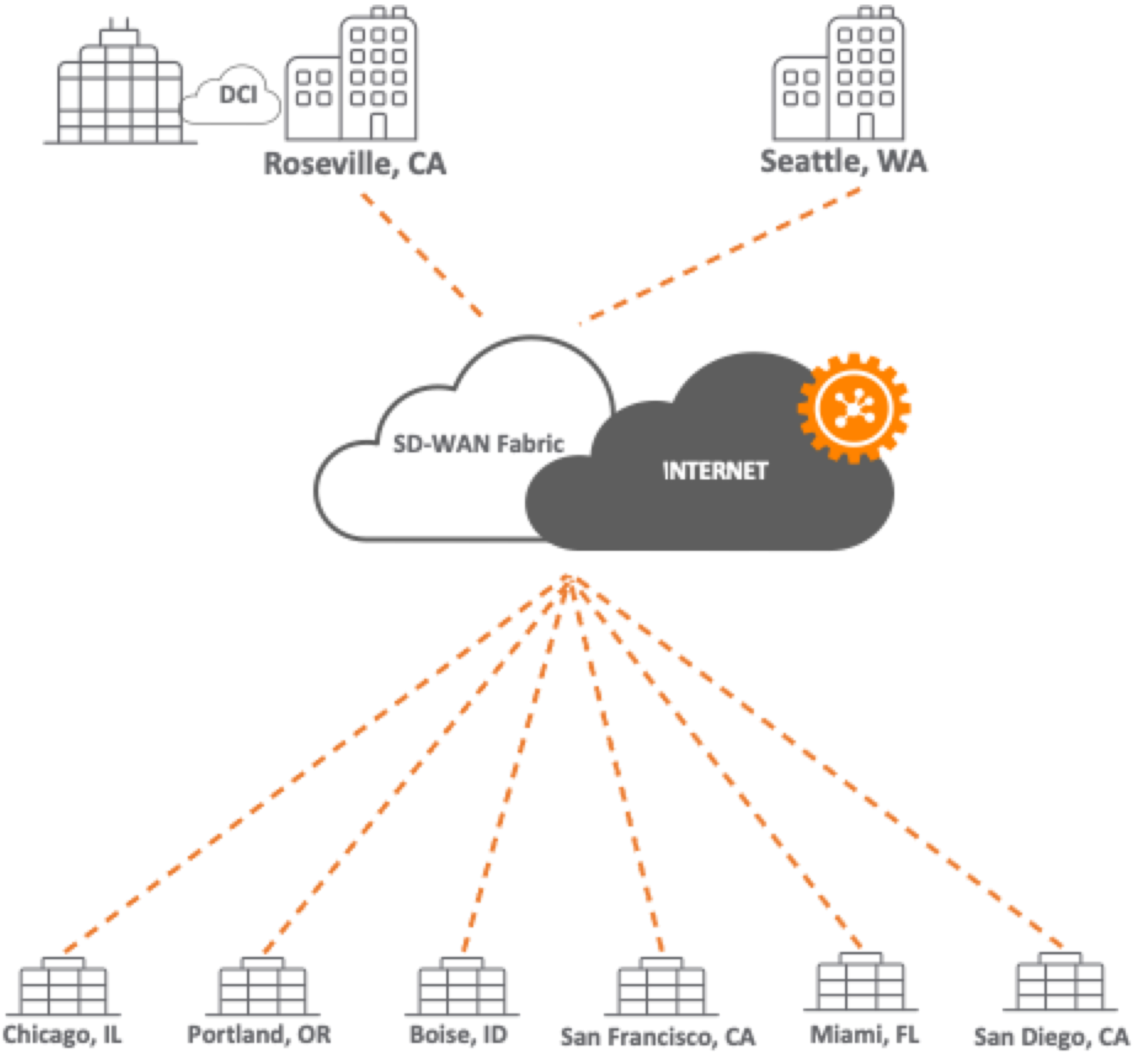


Figure 1: OWL Campuses and Branches

OWL's Roseville campus consists of three buildings totaling approximately 100,000 square feet of office and warehouse space. Building 1 contains a high concentration of conference rooms on the first floor; Building 2 houses IT, Finance, and other offices; and Building 3 is the R&D and Training department, as well as the distribution warehouse.

Roseville Campus

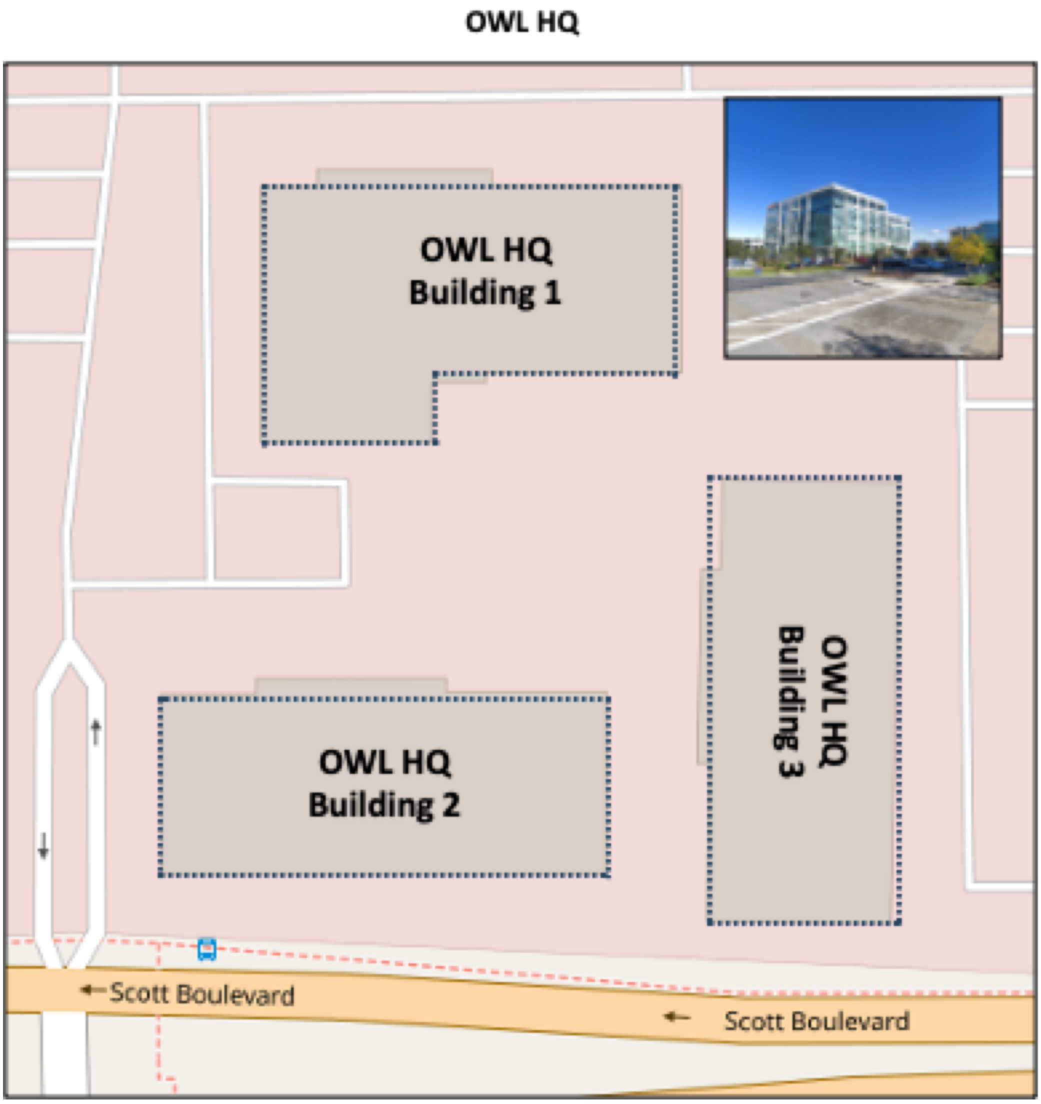


Figure 2: RSVCP Map

Reference Customer Environment

OWL's Roseville main headquarters campus is designed as a traditional 3-tier topology, with most data traffic carried within VLANs. Wireless traffic is tunneled within GRE to a gateway cluster for centralized policy enforcement. Wired traffic is bridged locally at the ingress switch port.

This design uses Layer 2 access with routed links between the aggregation and core switches.

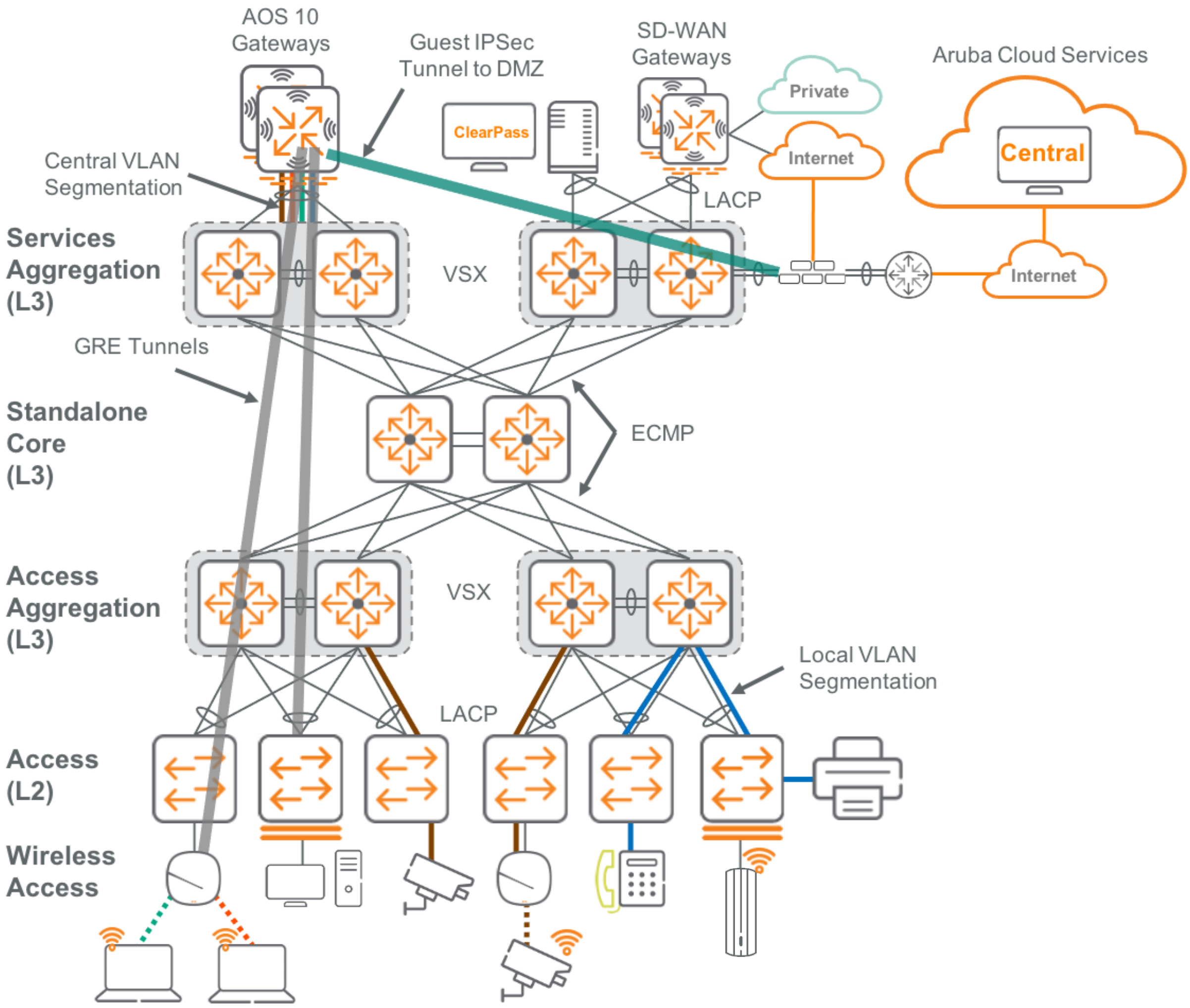


Figure 3: RSVCP

Policy enforcement occurs at the gateway cluster and at the Layer 2 access switch ports.

Reference Customer's Need for NAC

A recent incident at the company exposed a network security hole, prompting an IT leadership meeting that uncovered more incidents and highlighted the need for an effective NAC solution. OWL's documented incidents, which mirror challenges faced by other companies today, include:

- **Incident 1: Open Wi-Fi access to the corporate network:** After months of dealing with intermittent authentication failures at a branch, the branch manager installed a personal Wi-Fi router for his office laptop. Because the router connected to an access port configured for the laptop's docking station, all of the personal router's Wi-Fi clients were granted full access to the corporate network from inside and outside of the building.
- **Incident 2: Sales call center interrupted:** The sales call center moved floors without notifying IT. No resource was scheduled to configure the cubicle ports for the call center's VoIP phones.

- **Incident 3: Frustrated and embarrassed executives:** When the CEO and some of OWL's top customers visited a new branch, neither the CIO nor CEO could connect to the corporate network because the Wi-Fi and switchport configuration used local settings inconsistent with corporate policy. As a result, they spent an hour troubleshooting, in front of customers, with the IT director by phone, who guided them through configuring the supplicant correctly.
- **Incident 4: Weekend trip ruined for on-call network engineer:** A power supply failure in one of three switches caused Wi-Fi and wired network outages in a section of OWL's distribution center. With an outdated network drop list and no configuration backup, the on-call network engineer needed to drive onsite to trace cables and identify each client to determine the individual switchport configuration.
- **Incident 5: Reduced productivity and loss of revenue:** Internet service was disrupted at several sites across the company during the week of March Madness. The root cause: sales and distribution center staff circumvented Wi-Fi bandwidth restrictions by joining their phones and laptops to the dedicated handheld scanner SSID using a widely known "secret" PSK.

The Solution

OWL leadership has approved the implementation of Aruba ClearPass Policy Manager to eliminate or significantly reduce future incidents like the ones above by:

- **Preventing unauthorized access to the network to address Incident 1:** Aruba access switches, in conjunction with ClearPass, will enforce access policies that include rejecting unauthorized clients based on 802.1X or MAC authentication, thus preventing a home router from gaining access to OWL's network.
- **Eliminating the need for manual access switchport configuration to address Incidents 2 and 4**: Configuring port-access security on Aruba switches allows for colorless ports, which dynamically configure a switch port based on the identity of those connected, eliminating the need for manual switchport configuration every time staff moves to different desks or if devices must be moved due to a downed switch.
- **Eliminating network access frustrations for traveling employees to address Incident 3:** A properly configured corporate WLAN policy authenticated via CPPM across the organization ensures a consistent and secure user experience when connecting to OWL's corporate network across all sites.
- **Preventing users from oversubscribing an internet circuit to address Incident 5:** Using Aruba role-based access on the gateways and access switches enables OWL to enforce bandwidth throttling based on client identity, even on the handheld scanner SSID.

Project Requirements and Goals

The new ClearPass solution is developed based on a set of technical and business requirements that guide the decisions of ClearPass appliances' physical locations, high availability, and AAA configurations.

Technical Requirements

Primary technical objectives include:

- Secure wireless and wired edge ports using 802.1X and MAC authentication
- Identify all devices on the network through device profiling
- Configure switch ports dynamically based on device and user identity
- Centralize configuration management and monitoring from the cloud
- Implement a resilient network policy solution designed for High Availability.

Business Requirements

Business requirements are equally crucial:

- Prevent unauthorized access to the network
- Simplify and secure network access for IoT clients
- Provide a consistent network experience for users traveling between sites, whether connected over Wi-Fi or docked at a hoteling station.
- Reduce deployment timelines, complexity, and cost
- Provide easy guest access for visitors
- Provide appropriate access for contractors
- Improve the time to resolve authentication issues.

Together, these technical and business requirements form the foundation of the new ClearPass solution, ensuring that it is robust, user-friendly, and aligned with the organization's broader operational goals.

Deployment Overview

The selected solution for OWL is ClearPass Policy Manager due to its comprehensive set of flexible features that cater to the organization's requirements.

ClearPass Cluster

A *cluster* is a logical connection of any combination of Policy Manager hardware or virtual appliances. Policy Manager appliances can be deployed as dedicated hardware appliances or as virtual machines running on top of VMware vSphere Hypervisor or Microsoft Hyper-V. OWL uses VMWare.

Find additional information in the Cluster Configuration Options section of the CPPM User Guide.

Publisher/Subscriber Model

Policy Manager uses a Publisher/Subscriber model to provide multiple-box clustering. Another term for this model is *hub and spoke*, where the hub corresponds to the Publisher, and the spokes correspond to the Subscribers. For OWL, the design calls for a Publisher and Subscriber in the Roseville data center for this phase with a plan to deploy a second pair of servers, configured as Subscribers, in an offsite data center to support branch locations.

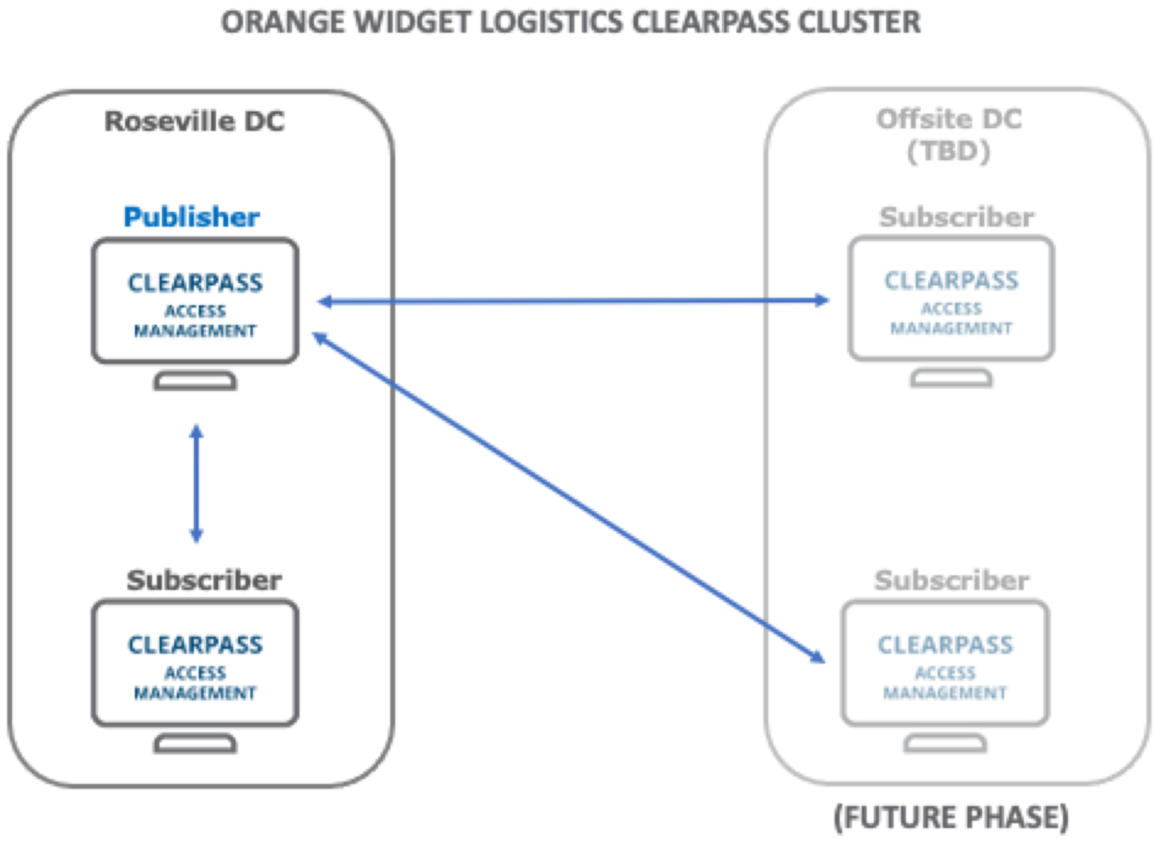

ORANGE WIDGET LOGISTICS CLEARPASS CLUSTER
Roseville DC
Publisher
CLEARPASS ACCESS MANAGEMENT
Subscriber
CLEARPASS ACCESS MANAGEMENT
Offsite DC (TBD)
Subscriber
CLEARPASS ACCESS MANAGEMENT
Subscriber
CLEARPASS ACCESS MANAGEMENT
(FUTURE PHASE)

Figure 4: OWL CPPM Cluster

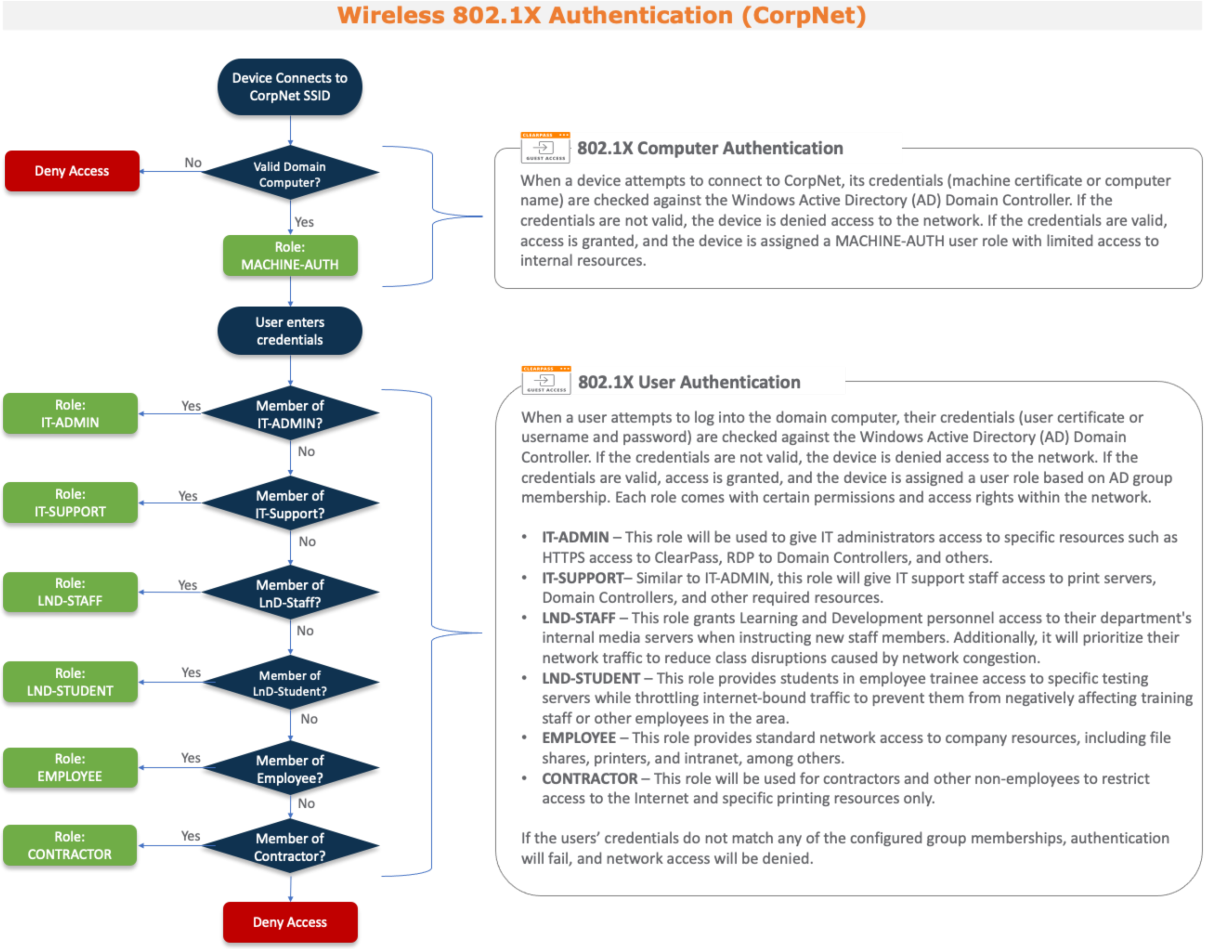
- The **Publisher server** functions as the conductor controller in the cluster. The Publisher is the central point of configuration, monitoring, and reporting, as well as database replication. The Publisher managed all databases.
  - This model include one active Publisher with a potentially unlimited number of Subscribers.
  - The Publisher server has full read/write access to the configuration database. All configuration changes must be made on the Publisher. The Publisher server sends configuration changes to each Subscriber server.
- The **Subscriber servers** are worker servers, managing all AAA load, all RADIUS requests, and policy decisions.
  - Subscriber servers maintain a local copy of the configuration database, and each Subscriber has read-only access to a local copy of the configuration database.

Authentication Logic

The policy solution aims to provide a secure network access and smooth authentication process for users, regardless if they are using a mobile device or working at their desks. Each time a device tries to connect to the network, through a wired or wireless connection, it is assigned the appropriate level of access based on a predetermined set of rules configured in ClearPass. Rules for each user role(s) are set up in Aruba Central are applied to both the Aruba CX switches and mobility gateways.

Wireless 802.1X Authentication

The flowchart below shows a high-level representation of the expected authentication logic used when a client device attempts to connect to OWL's new CorpNet SSID.



802.1X Computer Authentication

When a device attempts to connect to CorpNet, its credentials (machine certificate or computer name) are checked against the Windows Active Directory (AD) Domain Controller. If the credentials are not valid, the device is denied access to the network. If the credentials are valid, access is granted, and the device is assigned a MACHINE-AUTH user role with limited access to internal resources.

802.1X User Authentication

When a user attempts to log into the domain computer, their credentials (user certificate or username and password) are checked against the Windows Active Directory (AD) Domain Controller. If the credentials are not valid, the device is denied access to the network. If the credentials are valid, access is granted, and the device is assigned a user role based on AD group membership. Each role comes with certain permissions and access rights within the network.

- **IT-ADMIN** – This role will be used to give IT administrators access to specific resources such as HTTPS access to ClearPass, RDP to Domain Controllers, and others.
- **IT-SUPPORT**– Similar to IT-ADMIN, this role will give IT support staff access to print servers, Domain Controllers, and other required resources.
- **LND-STAFF** – This role grants Learning and Development personnel access to their department's internal media servers when instructing new staff members. Additionally, it will prioritize their network traffic to reduce class disruptions caused by network congestion.
- **LND-STUDENT** – This role provides students in employee trainee access to specific testing servers while throttling internet-bound traffic to prevent them from negatively affecting training staff or other employees in the area.
- **EMPLOYEE** – This role provides standard network access to company resources, including file shares, printers, and intranet, among others.
- **CONTRACTOR** – This role will be used for contractors and other non-employees to restrict access to the Internet and specific printing resources only.

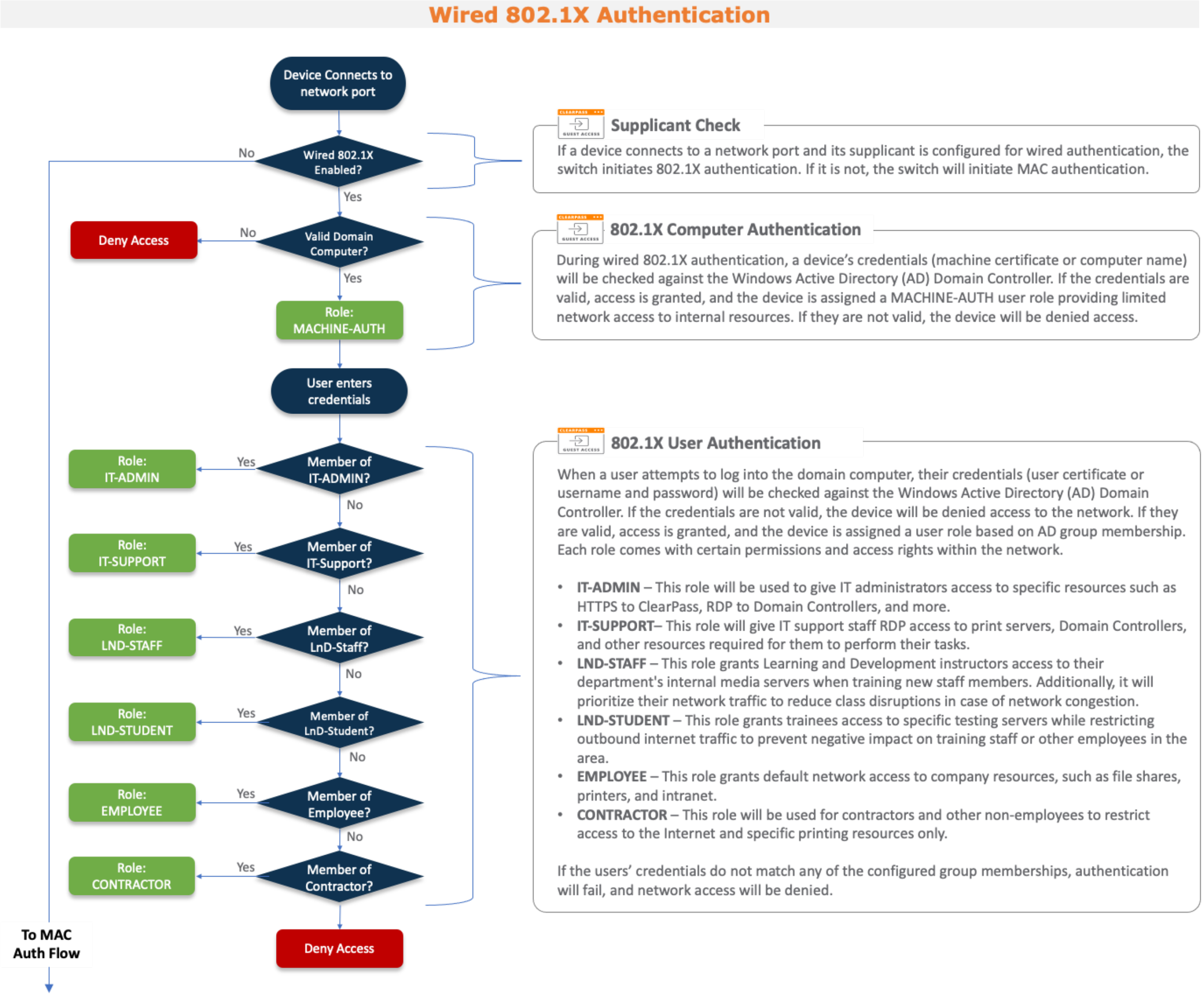
If the users' credentials do not match any of the configured group memberships, authentication will fail, and network access will be denied.

Figure 5: Wireless 802.1X Authentication

Wired 802.1X and MAC Authentication

The flowcharts below illustrate the authentication logic to expect when a client device is connected to a port configured for 802.1X and MAC authentication.

Wired 802.1X Authentication Flowchart



Supplicant Check

If a device connects to a network port and its supplicant is configured for wired authentication, the switch initiates 802.1X authentication. If it is not, the switch will initiate MAC authentication.

802.1X Computer Authentication

During wired 802.1X authentication, a device's credentials (machine certificate or computer name) will be checked against the Windows Active Directory (AD) Domain Controller. If the credentials are valid, access is granted, and the device is assigned a MACHINE-AUTH user role providing limited network access to internal resources. If they are not valid, the device will be denied access.

802.1X User Authentication

When a user attempts to log into the domain computer, their credentials (user certificate or username and password) will be checked against the Windows Active Directory (AD) Domain Controller. If the credentials are not valid, the device will be denied access to the network. If they are valid, access is granted, and the device is assigned a user role based on AD group membership. Each role comes with certain permissions and access rights within the network.

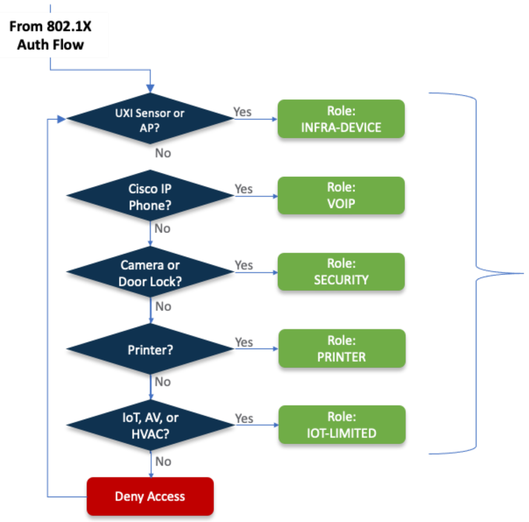
- **IT-ADMIN** – This role will be used to give IT administrators access to specific resources such as HTTPS to ClearPass, RDP to Domain Controllers, and more.
- **IT-SUPPORT**– This role will give IT support staff RDP access to print servers, Domain Controllers, and other resources required for them to perform their tasks.
- **LND-STAFF** – This role grants Learning and Development instructors access to their department's internal media servers when training new staff members. Additionally, it will prioritize their network traffic to reduce class disruptions in case of network congestion.
- **LND-STUDENT** – This role grants trainees access to specific testing servers while restricting outbound internet traffic to prevent negative impact on training staff or other employees in the area.
- **EMPLOYEE** – This role grants default network access to company resources, such as file shares, printers, and intranet.
- **CONTRACTOR** – This role will be used for contractors and other non-employees to restrict access to the Internet and specific printing resources only.

If the users' credentials do not match any of the configured group memberships, authentication will fail, and network access will be denied.

Figure 6: Wired 802.1X Authentication

Wired MAC Authentication Flowchart

Wired MAC Authentication



MAC Authentication

When a device lacks 802.1X support or its supplicant is not configured for it, the switch uses MAC authentication. During this process, the device's MAC address is checked against ClearPass's Endpoint Repository. Access will be granted to a device if it has been successfully profiled and matches one of the preconfigured rules in ClearPass's Role Mapping Policy. Based on the rules, the device will be assigned one of the roles listed below, each with specific permissions and access rights within the network.

- **INFRA-DEVICE** – This role will provide the required access for the connected UXI sensor to accomplish its monitoring tasks and for the AP to provide Wi-Fi access to clients. Additionally, the port will be configured as a trunk with a list of specific tagged VLANs and the network management VLAN set to native.
- **VOIP**– This role will place the phone on the voice VLAN, prioritize its traffic, and authenticate other devices connected to the phone's second Ethernet port.
- **SECURITY** – This role restricts these devices to only communicate with the security department's internal media and management servers.
- **PRINTER** – Devices assigned this role will be restricted to communicating with specific print servers on the internal network.
- **IOT-LIMITED** – This role restricts devices to specific traffic and destinations determined by IT.

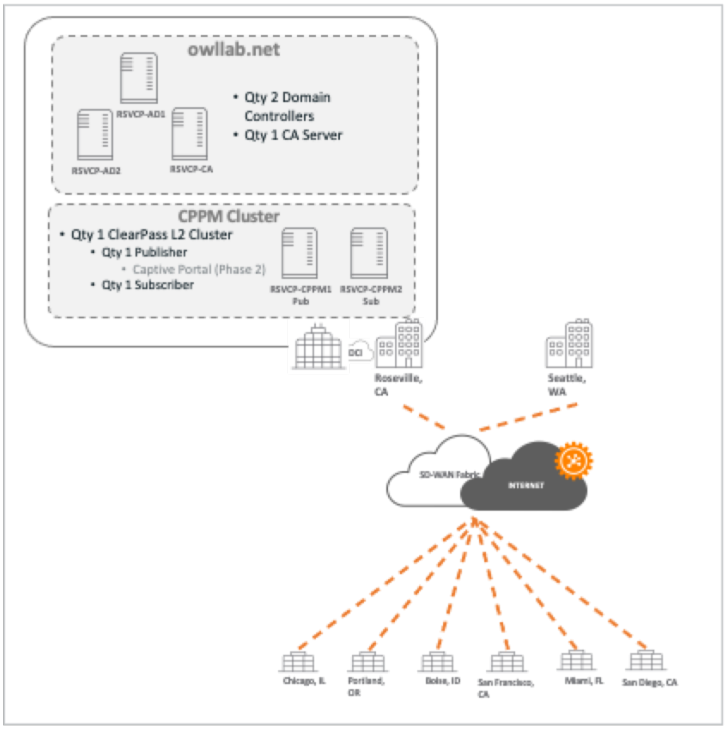
If the MAC address is not found in the Endpoint Repository, network access will be denied and the MAC auth process will restart after a specified quiet period.

Figure 7: Wired MAC Authentication

Deployment Overview

CPPM implementation is carried out in phases to help IT continue monitoring, administering, and supporting client access while also mitigating the risk of network service outages.

OWL CPPM Deployment Overview



Overview

- **Five (5) new VMs**
  - Qty 2 Domain Controllers
  - Qty 1 CA Server
  - Qty 2 ClearPass Servers
- **ClearPass Cluster**
  - L2 Redundant Pub/Sub
  - Authenticate wired & wireless Campus clients
- **AD DCs**
  - **Domain**: owllab.net
  - **OS**: WinSrvr2022
  - **DNS**
  - **DHCP**
- **CA Server**
  - **OS**: WInSrvr2022
- **Switches**
  - Roseville Campus access layer switches
    - **Building 1**
    - Building 2 (Phase 2)
    - Building 3 (Phase 2)
- **Gateways**
  - Roseville Campus Mobility Gateways
    - **SSID 1: CorpNet**
    - SSID 2: IoTNet (Phase 2)
    - SSID 3: GuestNet (Phase 2)

Figure 8: CPPM Deployment Overview

Deployment Outline

The outline below presents the high-level process used to deploy ClearPass Policy Manager for the reference customer OWL.

Note that that ClearPass is a versatile solution with many capabilities beyond the scope of this document. This deployment example serves as a guide for understanding the requirements for implementing CPPM.

Preparing for ClearPass Deployment

- Licensing
  - License gathering and activation
- Software download
- Infrastructure information gathering
  - From the network administrator:
    * Authentication servers, network devices, groups, and external authentication sources
  - For the VM server administrator:
    * ESXi virtual appliance software and requirements
  - From the VM server administrator:
    * Console access information
  - For the network administrator:
    * Network ports to permit and IP helper addresses
- Client device information gathering
  - User role/CPPM role and VLAN information

Appliances and Cluster Configuration

- Appliance configuration
  - Add/activate licenses with System Configuration Wizard
- Cluster configuration
  - Add subscribers, configure virtual IP addresses, join domain, enable insight, and update cluster software
- Configure certificates
  - Create Certificate Signing Request (CSR) and import certificates

Client Authentication Services Configuration

- Configure common components
  - Add AD authentication sources, network devices, and device groups
- Configure wireless 802.1X authentication service

- Configure wired 802.1X authentication service
- Configure wired MAC authentication service
- Configure switch in Aruba Central
- Organize services
- Configure wired client
- Validate authentication

In Scope for the Project (Not this Guide)

The last part of the outline lists steps required to implement ClearPass for the reference customer. Following these deployment steps provides the information necessary to fulfill the remainder of this NAC implementation process.

Pilot Deployment

Pilot IDF Rollout

- Select an IDF, floor, or select group of switcports for the pilot phase.
- Communicate rollout schedule and expectations to stakeholders.

Pilot Deployment and Monitoring

- Configure pilot switches in Aruba Central.
- Monitor system performance record user feedback.
- Adjust configuration based on observations and feedback.

Full-Scale Deployment

Production Switches Configuration

- Apply successful pilot configuration to production devices.
- Schedule phased deployment to minimize network disruptions.

Rollout Execution

- Execute the deployment phase on schedule.
- Continuously monitor network performance and security logs.

Staff Training and Documentation

- Train network staff on new configurations and troubleshooting.
- Update network documentation with new settings and policies.

Phased Rollout into Production

Required Equipment

Phase 1

- Enable AAA on port and configure them to fail to open

- Enable monitor mode

Phase 2

- Remove fail to open on the port
- Keep monitor mode

Phase 3

- Remove monitor mode
- Initiate full enforcement

For IT:

For Users:

High Level Design

Low Level Design

Key Terms

ClearPass

The guide assumes a completion of foundational ClearPass training and familiarity with the following related terms.

Hardware

- **Servers**
  - ClearPass
    - Cluster
    - Publisher
    - Subscriber
  - Microsoft Active Directory
    - Domain Controller (DC)
    - Domain Name Services (DNS)
    - Dynamic Host Configuration Protocol (DHCP)
    - Certificate Authority (CA)
- **Authenticators**
  - Gateway
  - Switch
  - Access Point (AP)
- **Supplicants**

  - Laptop
  - Printer
  - Desktop
  - IP Phone
  - Mobile Device

Software

-

  Configuration

  - AAA
  - VLAN
  - DHCP relay/IP helper
  - User roles
  - Redundancy
  - Virtual IP
  - CoA
  - MAC authentication
  - Web authentication
  - 802.1X
  - Identity store

Preparing for ClearPass Deployment

ClearPass deployment requires gathering specific information about infrastructure, client devices, and access levels, among others.

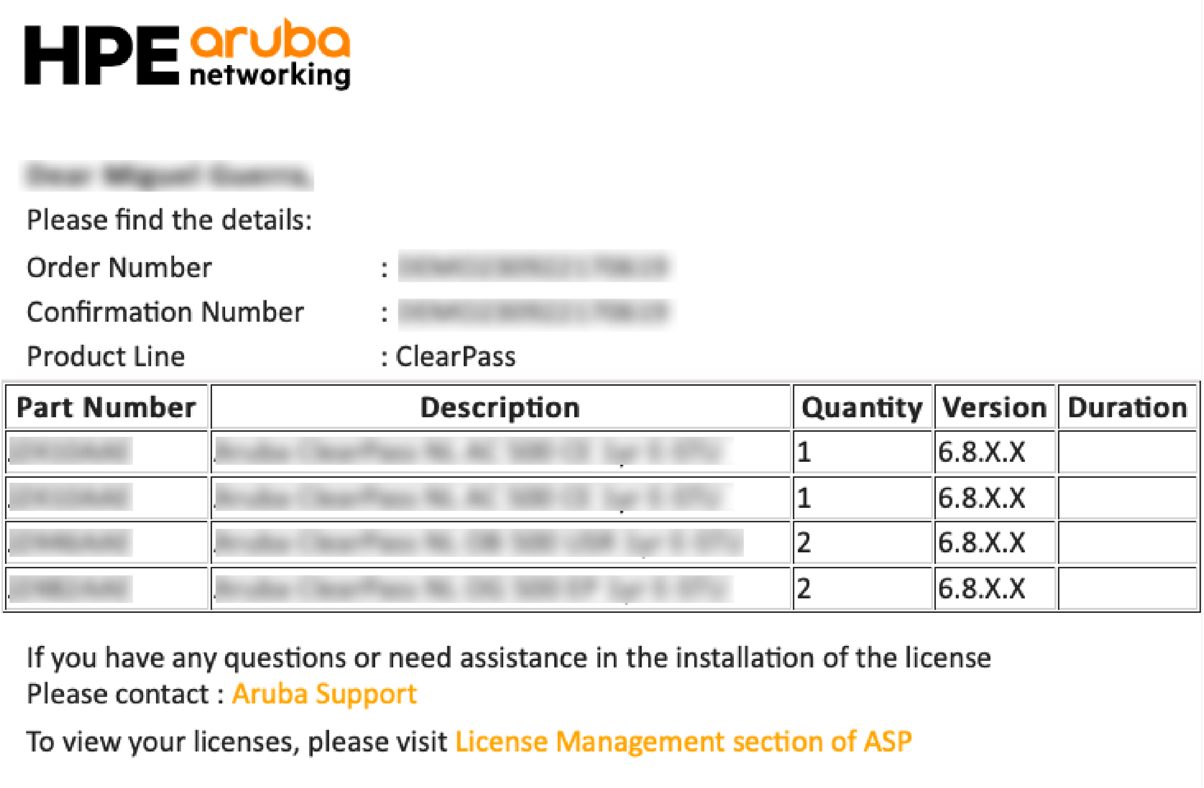
This chapter provides implementation details for IT administrators deploying the ClearPass solution at Orange Widget Logistics (OWL), a fictional customer described on the Reference Customer page.

Licensing

After a ClearPass Policy Manager (CPPM) purchase, Aruba Licensing Management sends licensing details to the customer email address provided in the ordering process.

Gather License

The licensing email is formatted like the sample below:



HPE aruba networking

[redacted]

Please find the details:

Order Number : [redacted]

Confirmation Number : [redacted]

Product Line : ClearPass

Part Number	Description	Quantity	Version	Duration
[redacted]	[redacted]	1	6.8.X.X	
[redacted]	[redacted]	1	6.8.X.X	
[redacted]	[redacted]	2	6.8.X.X	
[redacted]	[redacted]	2	6.8.X.X	

If you have any questions or need assistance in the installation of the license
Please contact : Aruba Support

To view your licenses, please visit License Management section of ASP

Figure 9: License Management Email

NOTE:

If the expected recipient does not receive the license email, contact the Aruba sales representative, partner account manager, or Aruba Support to request assistance.

The table below lists the licenses needed to deploy OWL's two-node ClearPass cluster with the ability to authenticate up to 1,000 concurrent endpoints. One VM-based license is used for each virtual appliance, and one 1,000-endpoint license is applied at the Publisher node and shared between both appliances when the cluster is created.

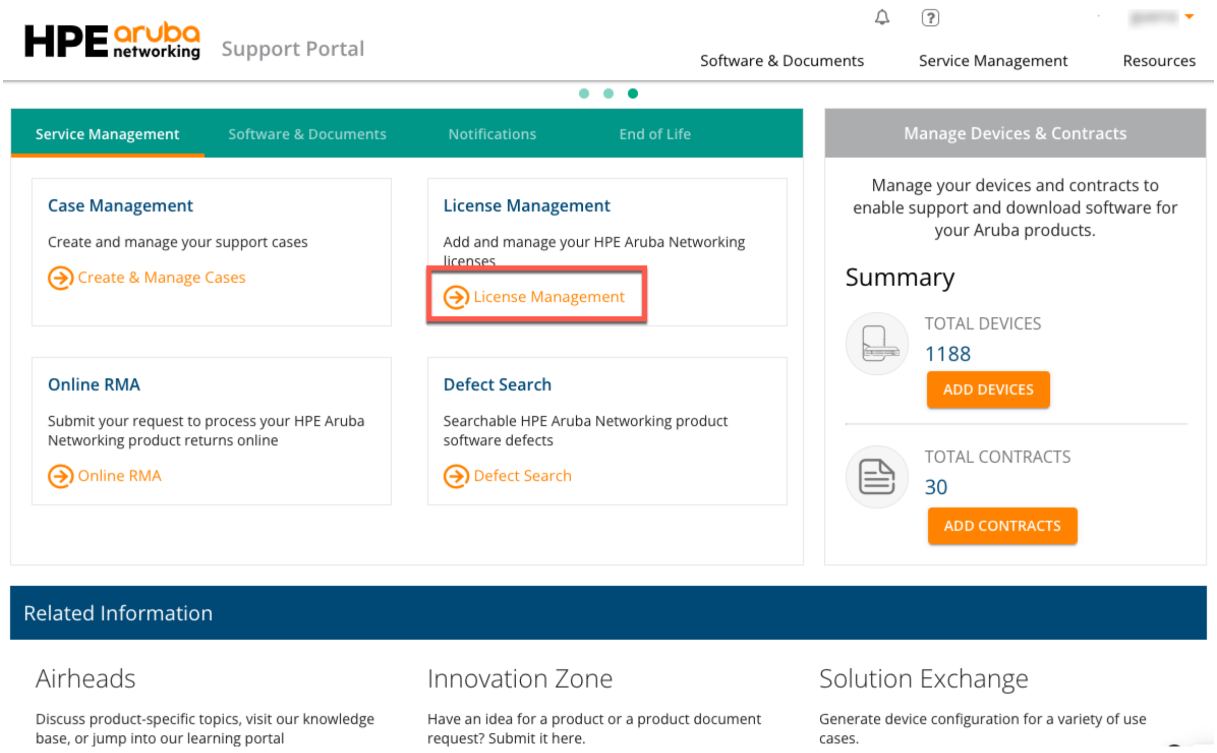
Part Number	Description	Quantity	Version
JZ399AAE	Aruba ClearPass Cx000V VM-Based Appliance E-LTU	2	6.8.X.X
JZ402AAE	Aruba ClearPass New Licensing Access 1K Concurrent Endpoints E-LTU	1	6.8.X.X

Activate License

After the proper license and order information is collected, use the steps below to activate the license.

Step 1 Open a web browser and log into the Aruba Support Portal.

Step 2 After log in, on the **Support Portal** page, click the **License Management** link in the center of the page. The **License Management** page appears.



Case Management

Create and manage your support cases

License Management

Add and manage your HPE Aruba Networking licenses

Online RMA

Submit your request to process your HPE Aruba Networking product returns online

Defect Search

Searchable HPE Aruba Networking product software defects

Manage your devices and contracts to enable support and download software for your Aruba products.

Summary

TOTAL DEVICES 1188

TOTAL CONTRACTS 30

Airheads

Discuss product-specific topics, visit our knowledge base, or jump into our learning portal

Innovation Zone

Have an idea for a product or a product document request? Submit it here.

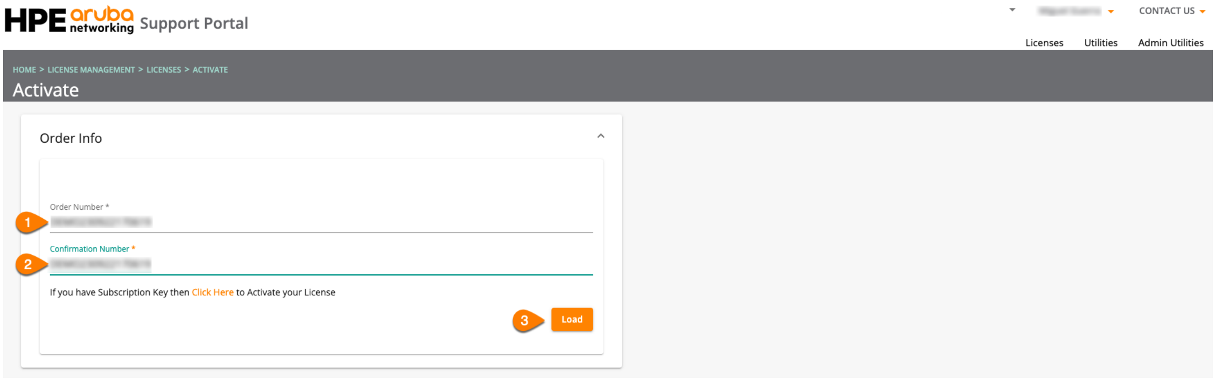
Solution Exchange

Generate device configuration for a variety of use cases.

Figure 10: ASP License Management

Step 3 On the **License Management** page, click the **Activate** button.

Step 4 On the **Activate** page, enter the order and confirmation number provided in the licensing email, then click the **Load** button.


HPE aruba networking Support Portal
[redacted]
CONTACT US
Licenses
Utilities
Admin Utilities
HOME > LICENSE MANAGEMENT > LICENSES > ACTIVATE
1
2
3

Activate

Order Info

Order Number * [redacted]

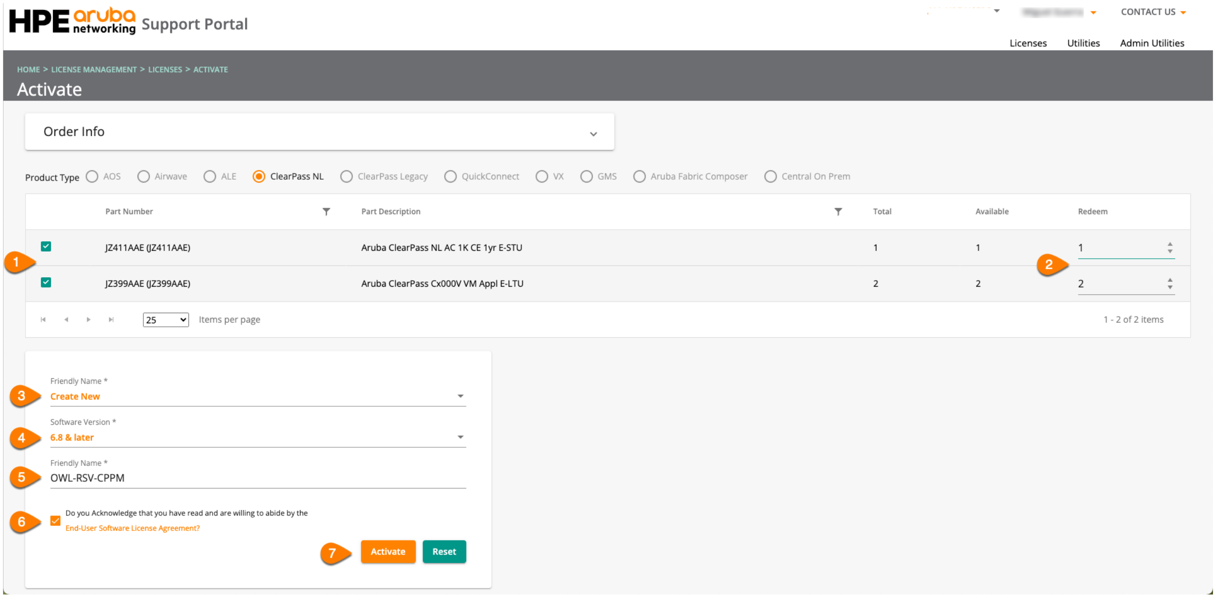
Confirmation Number * [redacted]

If you have Subscription Key then Click Here to Activate your License

Load

Figure 11: ASP License Activate

Step 5 When the order details appear, select the part numbers and quantities to be used. Enter the required information at the bottom of the page and click **Activate.**


HPE aruba networking Support Portal
[redacted]
CONTACT US
Licenses
Utilities
Admin Utilities
HOME > LICENSE MANAGEMENT > LICENSES > ACTIVATE
1
2
3
4
5
6
7

Activate

Order Info

Product Type ○ AOS ○ Airwave ○ ALE ● ClearPass NL ○ ClearPass Legacy ○ QuickConnect ○ VX ○ GMS ○ Aruba Fabric Composer ○ Central On Prem

	Part Number	Part Description	Total	Available	Redeem
☑	JZ411AAE (JZ411AAE)	Aruba ClearPass NL AC 1K CE 1yr E-STU	1	1	1
☑	JZ399AAE (JZ399AAE)	Aruba ClearPass Cx000V VM Appl E-LTU	2	2	2

25 Items per page 1 - 2 of 2 items

Friendly Name * Create New

Software Version * 6.8 & later

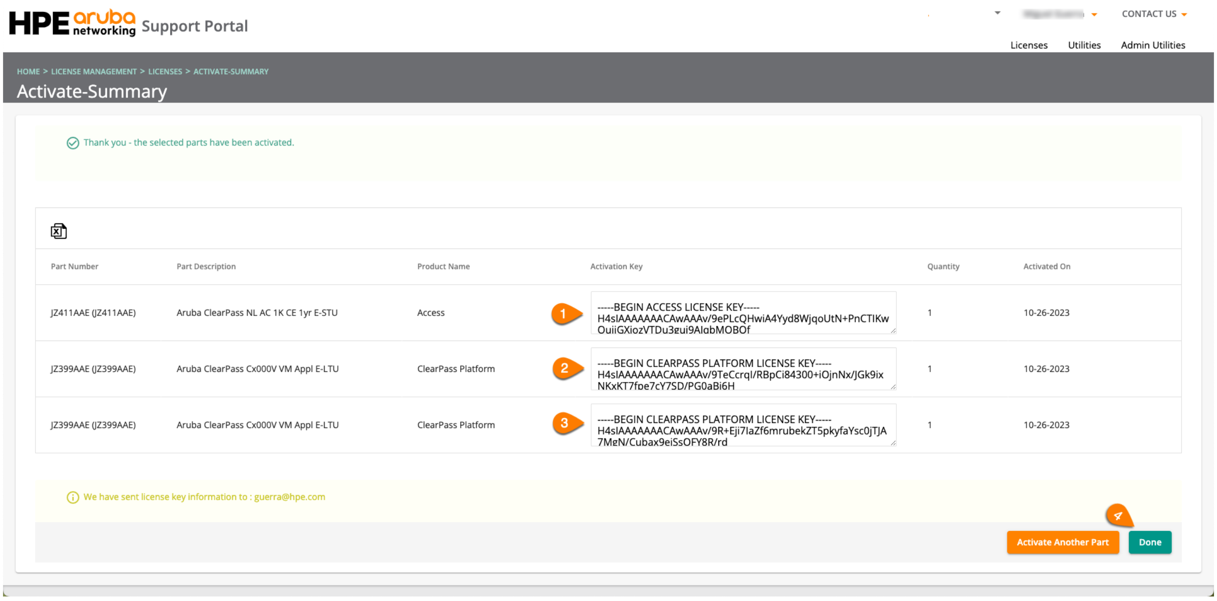
Friendly Name * OWL-RSV-CPPM

☑ Do you Acknowledge that you have read and are willing to abide by the End-User Software License Agreement?

Activate Reset

Figure 12: License Activation 2

Step 6 When the **Activate-Summary** page appears, save the **Activation Key** for each part number to apply later in the project and click the **Done** button.



HOME > LICENSE MANAGEMENT > LICENSES > ACTIVATE-SUMMARY

Activate-Summary

Thank you - the selected parts have been activated.

Part Number	Part Description	Product Name	Activation Key	Quantity	Activated On
JZ411AAE (JZ411AAE)	Aruba ClearPass NL AC 1K CE 1yr E-STU	Access	-----BEGIN ACCESS LICENSE KEY----- H4sIAAAAAAACAwAAAv/9ePLcQHwiA4Yyd8WjqoUtN+PnCTIKw OuiiGXiozVTDu3gui9AlqbMOBOf	1	10-26-2023
JZ399AAE (JZ399AAE)	Aruba ClearPass Cx000V VM Appl E-LTU	ClearPass Platform	-----BEGIN CLEARPASS PLATFORM LICENSE KEY----- H4sIAAAAAAACAwAAAv/9TeCcrql/RBpCi84300+iOjnNx/JGk9ix NKxKT7fpe7cY7SD/PG0aBi6H	1	10-26-2023
JZ399AAE (JZ399AAE)	Aruba ClearPass Cx000V VM Appl E-LTU	ClearPass Platform	-----BEGIN CLEARPASS PLATFORM LICENSE KEY----- H4sIAAAAAAACAwAAAv/9R+Eji7laZf6mrubekZT5pkyfaYsc0jTJA 7MgN/Cubax9eiSsOFY8R/rd	1	10-26-2023

We have sent license key information to : guerra@hpe.com

Figure 13: License Activation 3

Download Software

To download the software:

Step 1 Open a web browser and log into the Aruba Support Portal.

Step 2 After log in, on the **Support Portal** page, click the **Software & Documents** tab, then click the **ClearPass Policy Manager (CPPM)** link.

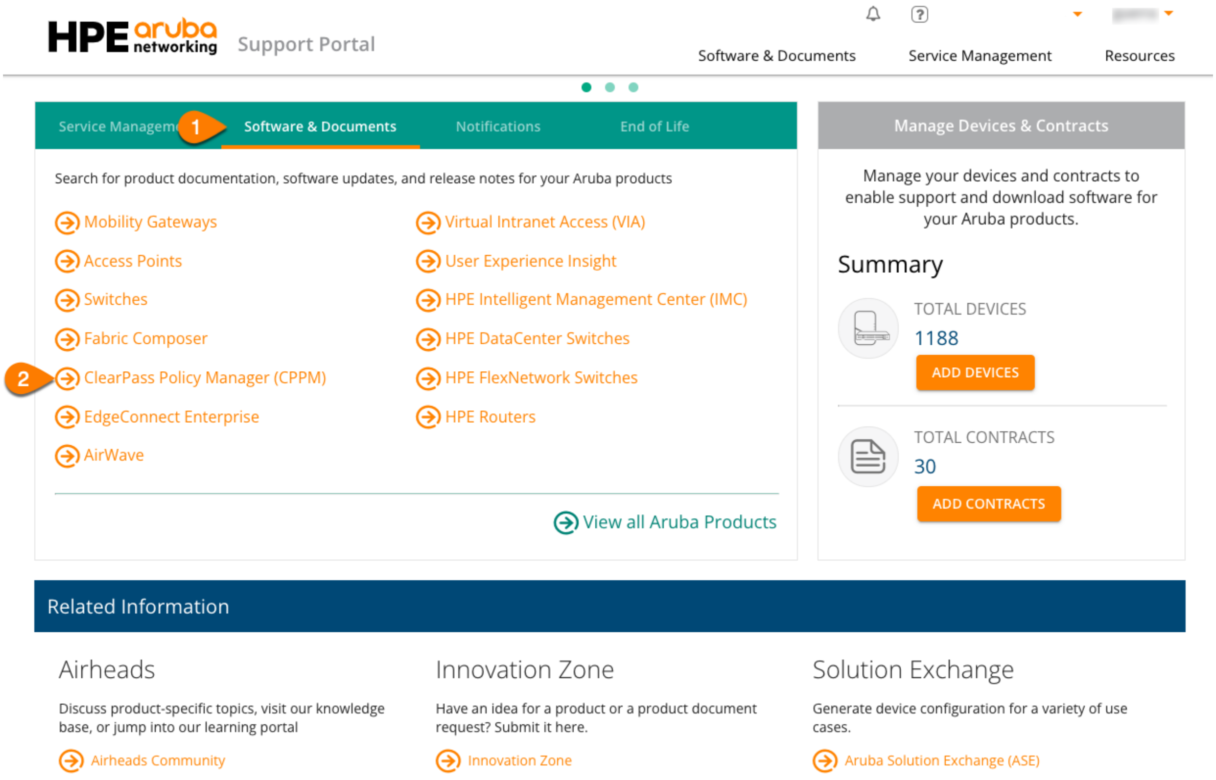

HPE aruba networking
Support Portal
Software & Documents
Service Management
Resources
Service Management
1
Software & Documents
Notifications
End of Life
Search for product documentation, software updates, and release notes for your Aruba products
Mobility Gateways
Access Points
Switches
Fabric Composer
2
ClearPass Policy Manager (CPPM)
EdgeConnect Enterprise
AirWave
Virtual Intranet Access (VIA)
User Experience Insight
HPE Intelligent Management Center (IMC)
HPE DataCenter Switches
HPE FlexNetwork Switches
HPE Routers
View all Aruba Products
Manage Devices & Contracts
Manage your devices and contracts to enable support and download software for your Aruba products.
Summary
TOTAL DEVICES
1188
ADD DEVICES
TOTAL CONTRACTS
30
ADD CONTRACTS
Related Information
Airheads
Discuss product-specific topics, visit our knowledge base, or jump into our learning portal
Airheads Community
Innovation Zone
Have an idea for a product or a product document request? Submit it here.
Innovation Zone
Solution Exchange
Generate device configuration for a variety of use cases.
Aruba Solution Exchange (ASE)

Figure 14: ASP Software Download

Step 3 When the **Software and Documents** page appears, use the **FILTERS** on the left to find the required image. Click the **Download** button at the right of the selected image.

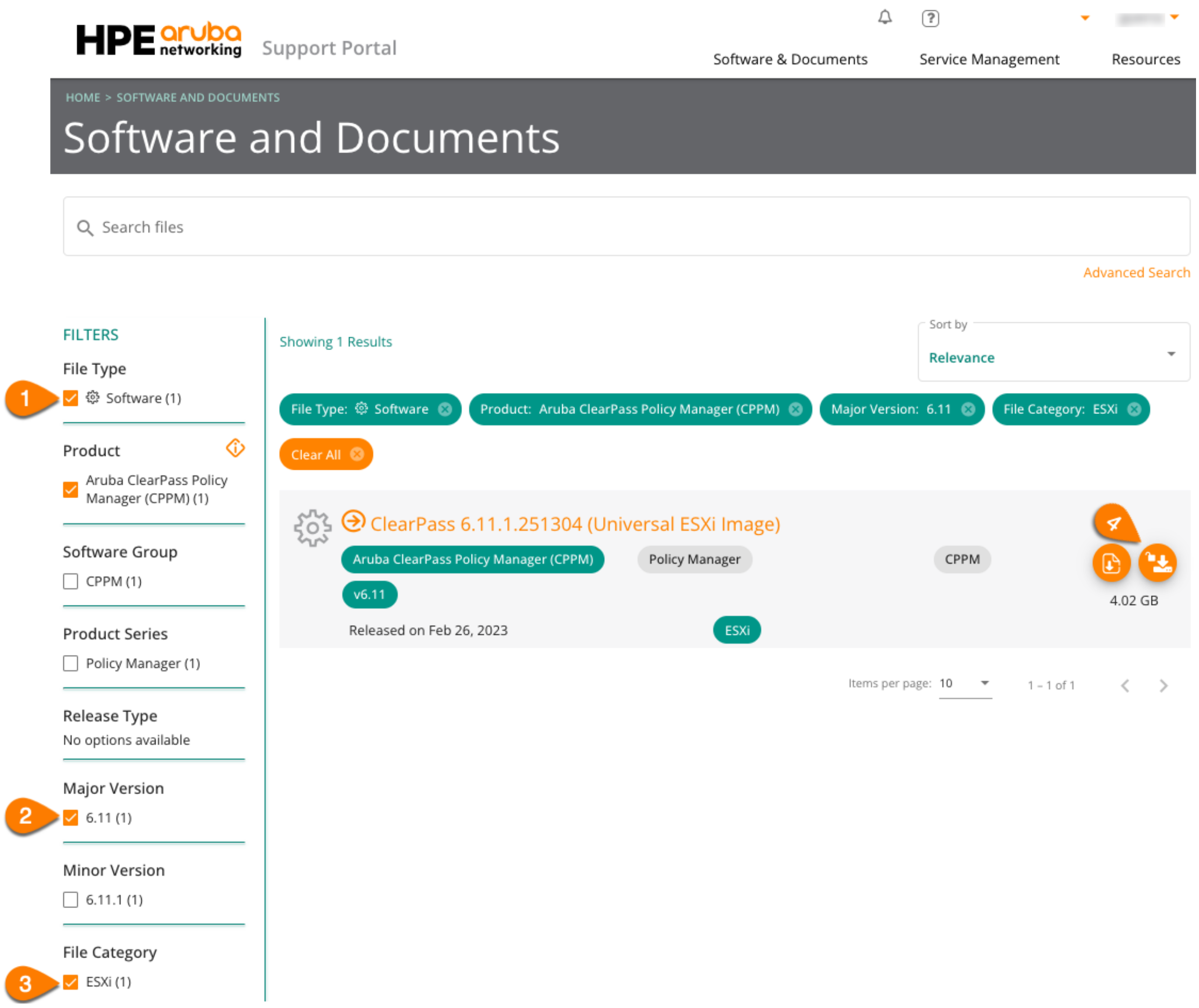


Figure 15: Software Download

Step 4 After the download is complete, proceed to **Information Sharing,** below.

Gather Infrastructure Information

This section outlines the information that must be gathered or shared with other parties. It is important to include all the details needed to prevent delays or service interruptions.

Network Administrator

As part of the discovery and design session, the information below is used implementation.

Authentication Servers (ClearPass Appliances)

The authentication servers in this deployment are the ClearPass appliances. The table lists information needed for initial configuration.

	Appliance 1	Appliance 2
Function	Publisher	Subscriber
Host Name	RSVCP-CPPM-1	RSVCP-CPPM-2
Management Port IP Address	10.2.120.195	10.2.120.194
Management Port Mask	255.255.255.0	255.255.255.0
Management Port Gateway	10.2.120.1	10.2.120.1
Virtual IP 1	10.2.120.192*	10.2.120.192
Virtual IP 2	10.2.120.193	10.2.120.193*
DNS Server 1	10.2.120.99	10.2.120.99
DNS Server 2	10.2.120.98	10.2.120.98
Administrator Password	Aruba123!	Aruba123!
NTP Server 1	10.2.120.99	10.2.120.99
NTP Server 2	10.2.120.98	10.2.120.98
Time Zone	Pacific Time	Pacific Time

**Indicates the appliance to be set as the primary node for that virtual IP.*

Network Devices (Authenticators)

The deployment calls for two types of authenticators: Aruba switches and gateways. ClearPass requires adding these devices to the **Network Devices** section in order to accept authentication requests sourced from them.

Individual Network Device Information

The table below lists information for each authenticator that must be added to **Network Devices** later in the implementation process.

Host Name	IP Address	Device Type
RSVCP-TEST-AC1	10.15.55.245	Aruba Switch
RSVCP-AG3-AC1	10.3.2.105	Aruba Switch
RSVCP-AG3-AC2	10.3.2.112	Aruba Switch
RSVCP-AG3-AC4	10.3.2.10	Aruba Switch
RSVCP-TEST-GW1	10.15.55.2	Aruba Gateway
RSVCP-SS2-CL1-1	10.6.15.11	Aruba Gateway
RSVCP-SS2-CL1-2	10.6.15.12	Aruba Gateway

NOTE:

ClearPass allows adding multiple devices simultaneously in the form of a subnet, or as individual IPs. For the reference customer list above, they are entered individually to allow greater control over the authentication requests that ClearPass accepts.

Common Network Device Information

The information below is the same across all devices listed in the table above. Both are needed when configuring the authenticators in the **Network Devices** list later in the implementation process.

- **RADIUS Shared Secret:** *Aruba123!*
- **TACACS+ Shared Secret:** *Aruba123!*
- **Vendor Name:** *Aruba*

Network Device Groups

Authentication requests are filtered using **Device Groups**, during **Services** configuration later in the implementation process. The table below lists the three groups to be created and the device types.

Device Groups	Devices (from Device Type column above)
Switches	Aruba Switch
Gateways	Aruba Gateway

External Authentication Sources

This deployment authenticates client devices against several authentication sources, including internal databases in ClearPass and in Windows Domain Controllers. Internal databases are created later in the process, Note the Windows Domain Controller information ahead of time:

	Domain Controller 1	Domain Controller 2
Host Name	rsvcp-ad1.owllab.net	rsvcp-ad2.owllab.net
Type	Active Directory	Active Directory
Bind DN	service@owllab.net	service@owllab.net
Bind Password	Aruba123!	Aruba123!

VM Server Administrator

ESXi Virtual Appliance Software and Requirements

The OWL must accommodate a maximum of 1,000 concurrent client devices in the first phase, with plans to increase to 5,000 in the second phase. As a result, the two virtual appliances are scoped as C2000V.

Provide the following information to the systems administrator responsible for deploying virtual appliances.

- OVF Zip files, downloaded earlier
- Sizing requirements for the project:

  C2000V (5K Virtual Appliance OVF)

  - 8 reserved virtual CPUs
    - The underlying CPU is recommended to have a PassMark® of 9600 or higher.
  - 16 GB RAM
  - Disk Space: 1000 GB disk space required (thick provisioned)
- Installing ClearPass on an ESX/ESXi Virtual Appliance
- VMware VSphere Hypervisor (ESXi) Requirements

NOTE:

Aruba ClearPass supports both physical and virtual appliance deployments. For complete details, refer to the ClearPass Installation Guide.

NOTE:

When a ClearPass cluster design requires configuring Virtual IP addresses in a virtual machine deployment, forged transmits must be enabled on the VMWare distributed virtual switch.

Network Administrator

Network Ports to Enable

The table below lists the network ports that must be open between the Publisher and Subscriber servers.

Port	Protocol	Description
80	HTTP	Internal Proxy
123	UDP	TNTP: Time synchronization
443	TCP	HTTPS: Internal proxy and server-to-server service

Port	Protocol	Description
5432	TCP	PostgreSQL: Database replication

Because any Subscriber server can be promoted as the Publisher server, all port/protocol combinations listed above should be:

- Bidirectional
- Open between any two servers in the cluster

IP Helper Addresses

To profile devices on the OWL network, ClearPass uses DHCP fingerprinting. To enable ClearPass to receive and collect DHCP request information, add the following IP Addresses as IP helper addresses to VLAN interfaces where client devices are present.

RSVCP-CPPM1: *10.2.120.194*

RSVCP-CPPM2: *10.2.120.195*

Gather Client Device Information

The client information below is used to configure services later in the implementation process.

User Role/CPPM Role Information

The table below contains user roles that switches, gateways, and ClearPass use to secure client devices.

Role Name	Description	Authorization Method
MACHINE-AUTH	OWL domain computers	Active Directory
EMPLOYEE	Default role for trusted employee users and computers	Active Directory
IT-SUPPORT	Read-only/Limited access to infrastructure devices	Active Directory
IT-ADMIN	Full access to infrastructure devices	Active Directory
INFRA-DEVICE	APs, UXI Sensors, and other infrastructure devices	Endpoint Repository
LND-STAFF	Learning & Development Staff	Active Directory
LND-STUDENT	Learning & Development Student	Active Directory

Role Name	Description	Authorization Method
VOIP	VoIP Phones	Endpoint Repository
PRINTER	Printers	Endpoint Repository
GUEST	OWL Guest	Guest User Repository
CONTRACTOR	Limited access to specific internal OWL resources and internet	Active Directory
SECURITY	Cameras, door locks, and other OWL security devices	Endpoint Repository
IOT-LIMITED	HVAC, lighting, A/V, and other OWL-owned headless devices	Guest Device Repository

VLAN Information

The table below contains VLAN information used to configure Enforcement Policies (where applicable) later in the implementation process.

VLAN ID	VLAN Name
10	Employee
20	Management
30	Voice
40	Printer
50	Guest
60	IoT

Virtual Appliance Console Access

The final step is to gather the required information to access the console of the two new ClearPass virtual appliances after the server administrator has created the VMs. This is needed to access the System Configuration Wizard. For physical appliances, this configuration is performed using a a physical console connection. For virtual appliances, a VM management interface is used.

After gathering all the information above, proceed to the **ClearPass Appliance and Cluster Configuration** chapter.

Configure ClearPass Appliances and Cluster

After gathering information cited in the previous chapter, continue with ClearPass appliance and cluster configuration.

This chapter outlines the steps to deploy one Aruba ClearPass Publisher and one Subscriber in a cluster for Orange Widget Logistics (OWL), the fictional customer described on the Reference Customer page. Although the instructions are specific to the scope of the sample deployment, they can be used as a reference point to deploy other ClearPass Policy Manager clusters.

Appliance Configuration

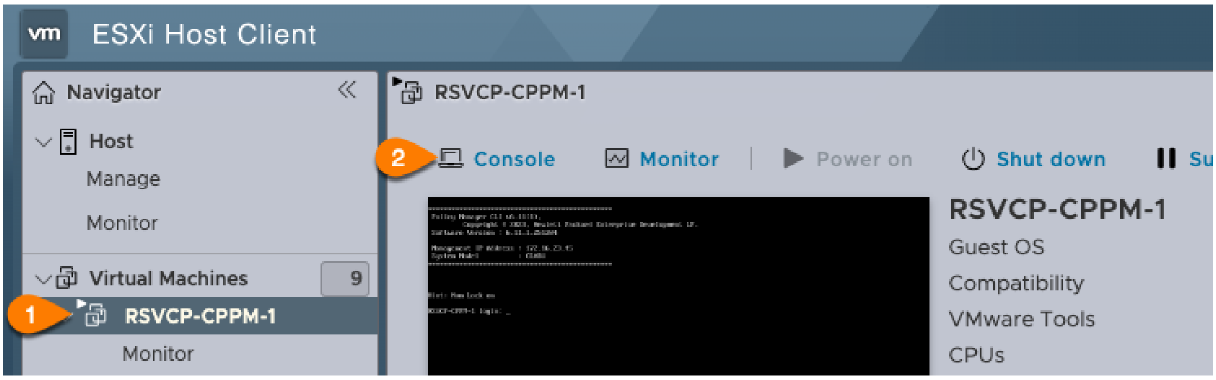
System Configuration Wizard

Follow the steps below to complete the initial setup of the new appliances and make them network-accessible.

> **NOTE:**
>
> The **System Configuration Wizard** steps in this subsection are the same for both physical and virtual appliances.

Step 1 With the virtual machine's management access information obtained in the last step of the previous chapter, open the command line interface (CLI) from the console of the first ClearPass appliance.

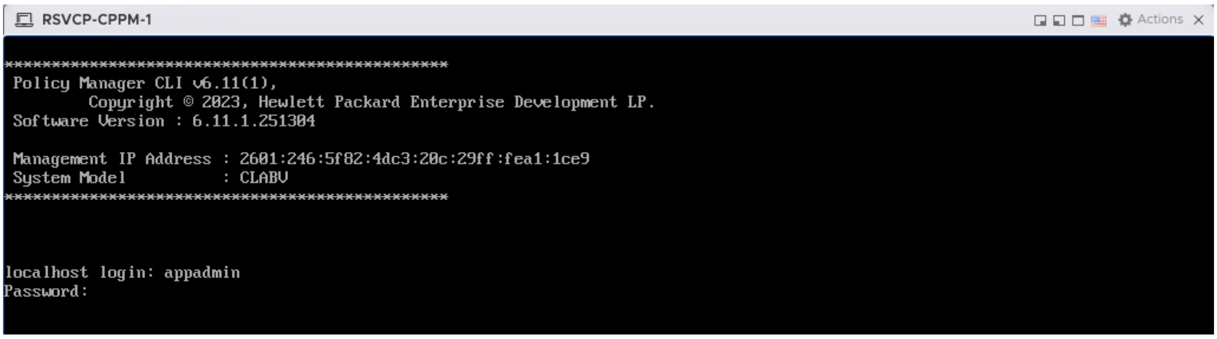
- In ESXi, go to **Virtual Machines > RSVCP-CPPM-1 > Console**



```
***********************************************************
 Policy Manager CLI [illegible]
        Copyright © [illegible] Hewlett Packard Enterprise Development LP.
 Software Version : [illegible]

 Management IP Address : [illegible]
 System Model          : [illegible]
***********************************************************



Hint: Num Lock on

RSVCP-CPPM-1 login: _
```

Figure 16: ESXI Console

Step 2 Log in using the following default credentials: - **User:** *appadmin* - **Password:** *eTIPS123*

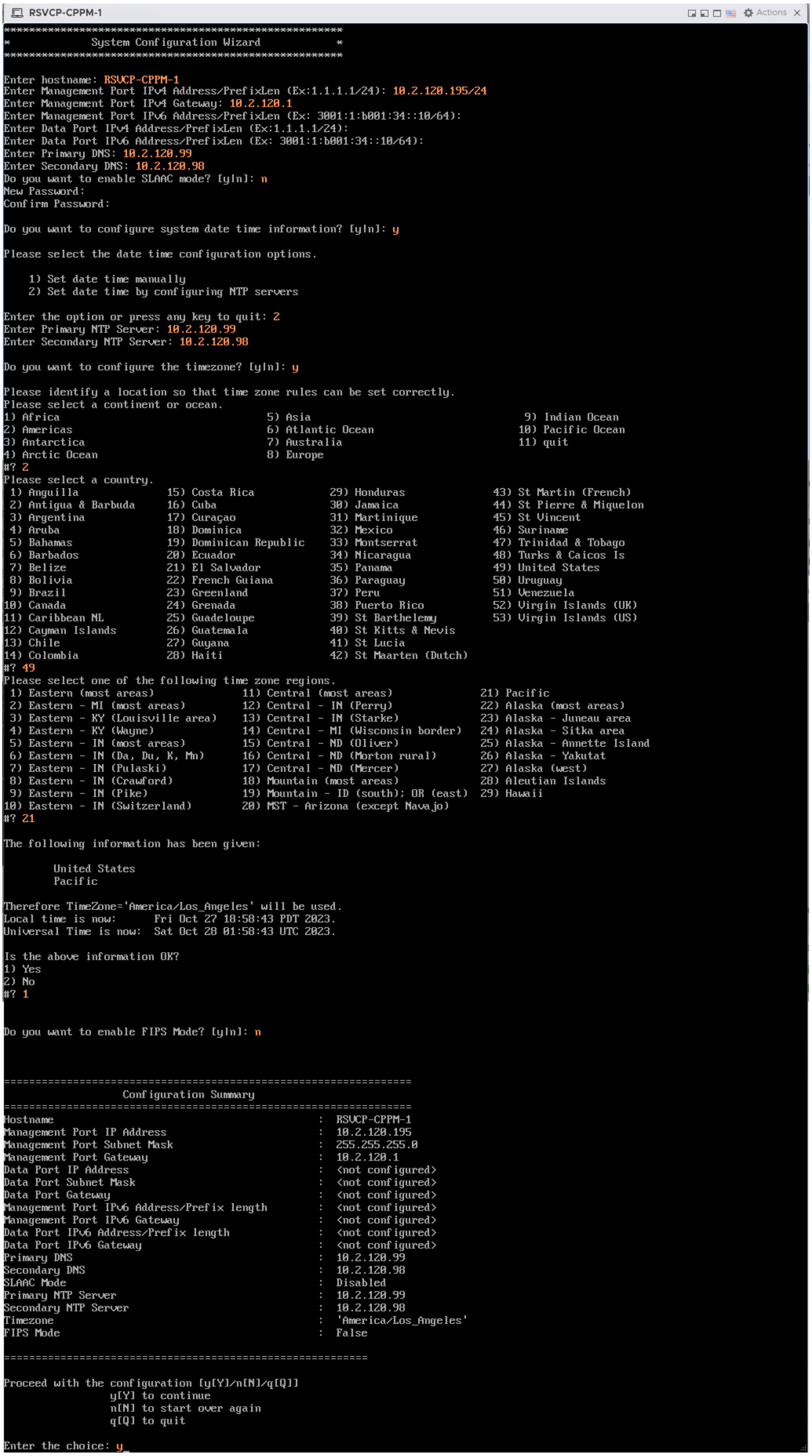


```
***********************************************
 Policy Manager CLI v6.11(1),
        Copyright © 2023, Hewlett Packard Enterprise Development LP.
 Software Version : 6.11.1.251304

 Management IP Address : 2601:246:5f82:4dc3:20c:29ff:fea1:1ce9
 System Model          : CLABV
***********************************************


localhost login: appadmin
Password:
```

Figure 17: Startup Config Login

Step 3 Enter the information for the first ClearPass server as prompted in the System Configuration Wizard. Remember that this is information collected in the **Authentication Servers (ClearPass Appliances)** section of the previous chapter. - **Enter hostname:** *RSVCP-CPPM-1* - **Enter Management Port IPv4 Address/PrefixLen (Ex: 1.1.1.1/24):** *10.2.120.195*/24 - **Enter Management Port IPv4 Gateway:** *10.2.120.1* - **Enter Management Port IPv6 Address/PrefixLen:** *Press ENTER to skip* - **Enter Data Port IPv4 Address/Prefix/Len:** *Press ENTER to skip* - **Enter Data Port IPv6 Address/PrefixLen:** *Press ENTER to skip* - **Enter Primary DNS:** *10.2.120.99* - **Enter Secondary DNS:** *10.2.120.98* - **Do you want to enable SLAAC mode?** *n* - **New Password:** *Aruba123!* - **Confirm Password:** *Aruba123!* - **Do you want to configure system date time information?** y - **Please select the date time configuration options**: 2 - **Enter Primary NTP Server:** *10.2.120.99* - **Enter Secondary NTP Server:** *10.2.120.98* - **Do you want to configure the timezone?** y - **Please select a continent or ocean:** 2 - **Please select a country:** 49 - **Please select one of the following time zone regions:** 21 - **Is the above information OK?** 1 - **Do you want to enable FIPS Mode?** n - **Proceed with the configuration. Enter the choice:** y

A sample console session is shown below. (Entered values appear in orange font for emphasis. The actual console session is monochrome.)



```
*******************************************************
*             System Configuration Wizard             *
*******************************************************

Enter hostname: RSVCP-CPPM-1
Enter Management Port IPv4 Address/PrefixLen (Ex:1.1.1.1/24): 10.2.120.195/24
Enter Management Port IPv4 Gateway: 10.2.120.1
Enter Management Port IPv6 Address/PrefixLen (Ex: 3001:1:b001:34::10/64):
Enter Data Port IPv4 Address/PrefixLen (Ex:1.1.1.1/24):
Enter Data Port IPv6 Address/PrefixLen (Ex: 3001:1:b001:34::10/64):
Enter Primary DNS: 10.2.120.99
Enter Secondary DNS: 10.2.120.98
Do you want to enable SLAAC mode? [y|n]: n
New Password:
Confirm Password:

Do you want to configure system date time information? [y|n]: y

Please select the date time configuration options.

    1) Set date time manually
    2) Set date time by configuring NTP servers

Enter the option or press any key to quit: 2
Enter Primary NTP Server: 10.2.120.99
Enter Secondary NTP Server: 10.2.120.98

Do you want to configure the timezone? [y|n]: y

Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
1) Africa                                 5) Asia                                   9) Indian Ocean
2) Americas                               6) Atlantic Ocean                        10) Pacific Ocean
3) Antarctica                             7) Australia                             11) quit
4) Arctic Ocean                           8) Europe
#? 2
Please select a country.
 1) Anguilla              15) Costa Rica             29) Honduras              43) St Martin (French)
 2) Antigua & Barbuda     16) Cuba                   30) Jamaica               44) St Pierre & Miquelon
 3) Argentina             17) Curaçao                31) Martinique            45) St Vincent
 4) Aruba                 18) Dominica               32) Mexico                46) Suriname
 5) Bahamas               19) Dominican Republic     33) Montserrat            47) Trinidad & Tobago
 6) Barbados              20) Ecuador                34) Nicaragua             48) Turks & Caicos Is
 7) Belize                21) El Salvador            35) Panama                49) United States
 8) Bolivia               22) French Guiana          36) Paraguay              50) Uruguay
 9) Brazil                23) Greenland              37) Peru                  51) Venezuela
10) Canada                24) Grenada                38) Puerto Rico           52) Virgin Islands (UK)
11) Caribbean NL          25) Guadeloupe             39) St Barthelemy         53) Virgin Islands (US)
12) Cayman Islands        26) Guatemala              40) St Kitts & Nevis
13) Chile                 27) Guyana                 41) St Lucia
14) Colombia              28) Haiti                  42) St Maarten (Dutch)
#? 49
Please select one of the following time zone regions.
 1) Eastern (most areas)               11) Central (most areas)              21) Pacific
 2) Eastern - MI (most areas)          12) Central - IN (Perry)              22) Alaska (most areas)
 3) Eastern - KY (Louisville area)     13) Central - IN (Starke)             23) Alaska - Juneau area
 4) Eastern - KY (Wayne)               14) Central - MI (Wisconsin border)   24) Alaska - Sitka area
 5) Eastern - IN (most areas)          15) Central - ND (Oliver)             25) Alaska - Annette Island
 6) Eastern - IN (Da, Du, K, Mn)       16) Central - ND (Morton rural)       26) Alaska - Yakutat
 7) Eastern - IN (Pulaski)             17) Central - ND (Mercer)             27) Alaska (west)
 8) Eastern - IN (Crawford)            18) Mountain (most areas)             28) Aleutian Islands
 9) Eastern - IN (Pike)                19) Mountain - ID (south); OR (east)  29) Hawaii
10) Eastern - IN (Switzerland)         20) MST - Arizona (except Navajo)
#? 21

The following information has been given:

        United States
        Pacific

Therefore TimeZone='America/Los_Angeles' will be used.
Local time is now:      Fri Oct 27 18:58:43 PDT 2023.
Universal Time is now:  Sat Oct 28 01:58:43 UTC 2023.

Is the above information OK?
1) Yes
2) No
#? 1


Do you want to enable FIPS Mode? [y|n]: n



==================================================================
                   Configuration Summary
==================================================================
Hostname                                           :  RSVCP-CPPM-1
Management Port IP Address                         :  10.2.120.195
Management Port Subnet Mask                        :  255.255.255.0
Management Port Gateway                            :  10.2.120.1
Data Port IP Address                               :  <not configured>
Data Port Subnet Mask                              :  <not configured>
Data Port Gateway                                  :  <not configured>
Management Port IPv6 Address/Prefix length         :  <not configured>
Management Port IPv6 Gateway                       :  <not configured>
Data Port IPv6 Address/Prefix length               :  <not configured>
Data Port IPv6 Gateway                             :  <not configured>
Primary DNS                                        :  10.2.120.99
Secondary DNS                                      :  10.2.120.98
SLAAC Mode                                         :  Disabled
Primary NTP Server                                 :  10.2.120.99
Secondary NTP Server                               :  10.2.120.98
Timezone                                           :  'America/Los_Angeles'
FIPS Mode                                          :  False

===========================================================

Proceed with the configuration [y[Y]/n[N]/q[Q]]
                 y[Y] to continue
                 n[N] to start over again
                 q[Q] to quit

Enter the choice: y
```

Figure 18: System Configuration Wizard

Step 4 After completing the last prompt to confirm the configuration, repeat the above steps for the second CPPM server.

Step 5 Wait for both servers to become available in the web browser, then move to the following section.

Licensing

The license activation keys collected during the **ClearPass Preparation** chapter are added in the following steps. The required keys are used in the following manner:

- Two (2) **Platform Licenses,** one for each virtual appliance.
- One (1) **Access License**, added to the first virtual appliance and shared between both nodes when the cluster is formed.

Add Licenses

First-time log in to a ClearPass virtual appliance's web interface generates a prompt for an appliance license key (collected in the prevous chapter). Follow the steps below to apply the licenses.

Step 1 Retrieve the license keys listed in the **License Gathering** steps in the **ClearPass Preparation** chapter.

Step 2 Open a web browser and connect to the first ClearPass appliance using its IP address.

Step 3 Click on **ClearPass Policy Manager** button

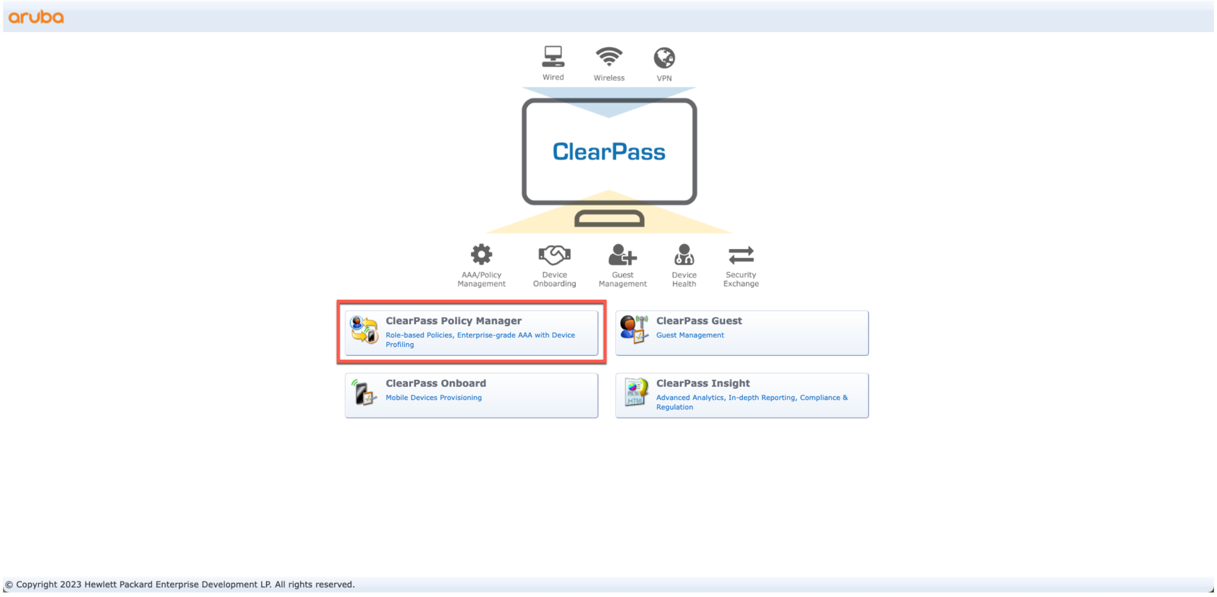
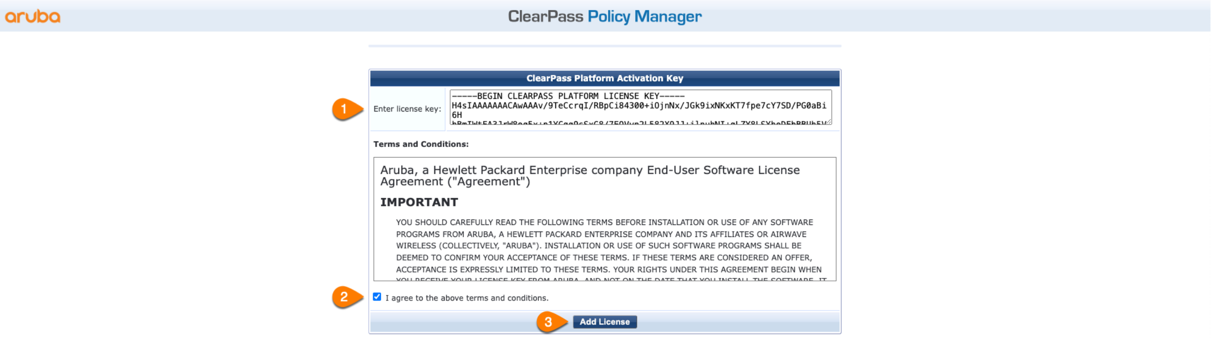

aruba
Wired
Wireless
VPN
ClearPass
AAA/Policy Management
Device Onboarding
Guest Management
Device Health
Security Exchange
ClearPass Policy Manager
Role-based Policies, Enterprise-grade AAA with Device Profiling
ClearPass Guest
Guest Management
ClearPass Onboard
Mobile Devices Provisioning
ClearPass Insight
Advanced Analytics, In-depth Reporting, Compliance & Regulation
© Copyright 2023 Hewlett Packard Enterprise Development LP. All rights reserved.

Figure 19: CPPM Welcome Screen

Step 4 On the next page, in the **Enter license key** text box, paste one of the two **ClearPass Platform** Activation Keys obtained previously, then click the **Add License** button.



ClearPass Platform Activation Key

Enter license key:

```
-----BEGIN CLEARPASS PLATFORM LICENSE KEY-----
H4sIAAAAAAACAwAAAv/9TeCcrqI/RBpCi84300+iOjnNx/JGk9ixNKxKT7fpe7cY7SD/PG0aBi
6H
```

Terms and Conditions:

Aruba, a Hewlett Packard Enterprise company End-User Software License Agreement ("Agreement")

IMPORTANT

YOU SHOULD CAREFULLY READ THE FOLLOWING TERMS BEFORE INSTALLATION OR USE OF ANY SOFTWARE PROGRAMS FROM ARUBA, A HEWLETT PACKARD ENTERPRISE COMPANY AND ITS AFFILIATES OR AIRWAVE WIRELESS (COLLECTIVELY, "ARUBA"). INSTALLATION OR USE OF SUCH SOFTWARE PROGRAMS SHALL BE DEEMED TO CONFIRM YOUR ACCEPTANCE OF THESE TERMS. IF THESE TERMS ARE CONSIDERED AN OFFER, ACCEPTANCE IS EXPRESSLY LIMITED TO THESE TERMS. YOUR RIGHTS UNDER THIS AGREEMENT BEGIN WHEN

☑ I agree to the above terms and conditions.

Add License

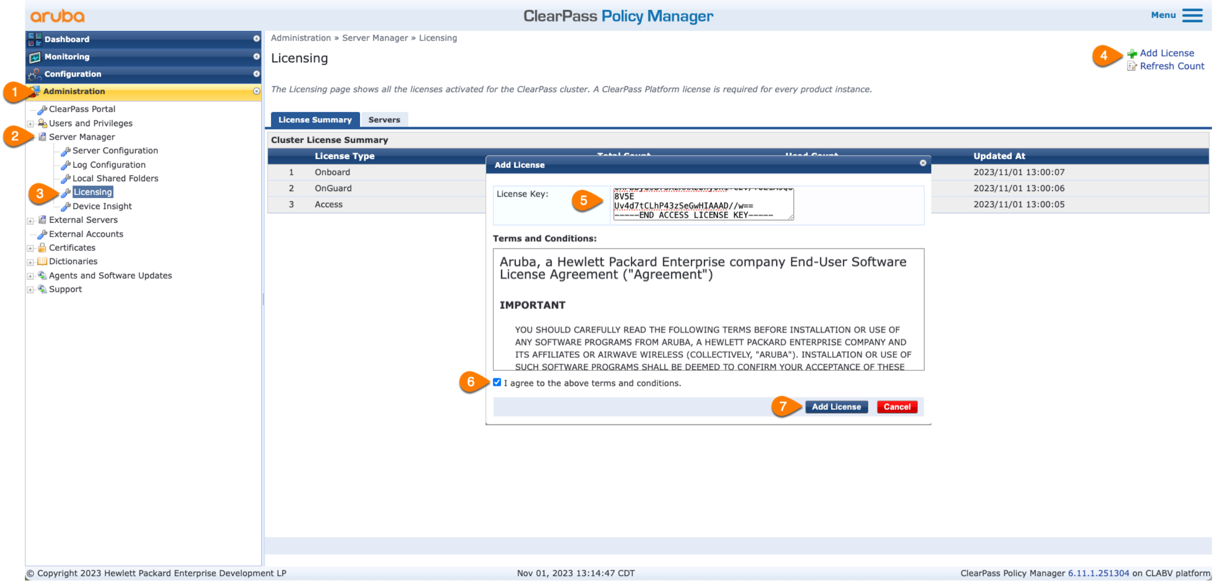
Figure 20: Platform Activation Key

Step 5 Log in with the password created in the **System Configuration Wizard** section earlier in this chapter. - **Username:** *admin* - **Password:** *Aruba123!*

NOTE:

The password generated during the **System Configuration Wizard** can be used to log in to both the web UI through either console or SSH. However, it is important to remember that the username for the web UI is *admin* and the username for the CLI is *appadmin*.

Step 6 After log in, go to **Administration** > **Server Manager** > **Licensing** and click the **Add License** link at the upper right. In the **Add License** window, paste the **Access** activation key obtained previously. Review and accept the terms and conditions, then click the **Add License** button.



Administration » Server Manager » Licensing

Licensing

The Licensing page shows all the licenses activated for the ClearPass cluster. A ClearPass Platform license is required for every product instance.

Cluster License Summary

	License Type	Total Count	Used Count	Updated At
1	Onboard			2023/11/01 13:00:07
2	OnGuard			2023/11/01 13:00:06
3	Access			2023/11/01 13:00:05

Add License

License Key:

```
8V5E
Uv4d7tCLhP43zSeGwHIAAAD//w==
-----END ACCESS LICENSE KEY-----
```

Terms and Conditions:

Aruba, a Hewlett Packard Enterprise company End-User Software License Agreement ("Agreement")

IMPORTANT

YOU SHOULD CAREFULLY READ THE FOLLOWING TERMS BEFORE INSTALLATION OR USE OF ANY SOFTWARE PROGRAMS FROM ARUBA, A HEWLETT PACKARD ENTERPRISE COMPANY AND ITS AFFILIATES OR AIRWAVE WIRELESS (COLLECTIVELY, "ARUBA"). INSTALLATION OR USE OF SUCH SOFTWARE PROGRAMS SHALL BE DEEMED TO CONFIRM YOUR ACCEPTANCE OF THESE

☑ I agree to the above terms and conditions.

Add License Cancel

© Copyright 2023 Hewlett Packard Enterprise Development LP

Nov 01, 2023 13:14:47 CDT

ClearPass Policy Manager 6.11.1.251304 on CLABV platform

Figure 21: Add Access License

Step 7 Confirm that the **Access** license total count increased to the amount expected. The total count is found in the **License Summary** tab of the **Licensing** page.

NOTE:

If the total license count is different than expected, check if additional keys must be added. Verify that the correct license quantities were selected during the activation process. Check if licenses were split into multiple line items: for example, two **NL AC 500** license keys are listed instead of one **NL AC 1K**.

Step 8 After applying the licenses to RSVCP-CPPM-1, repeat steps 1 to 5 above for RSVCP-CPPM-2.

NOTE:

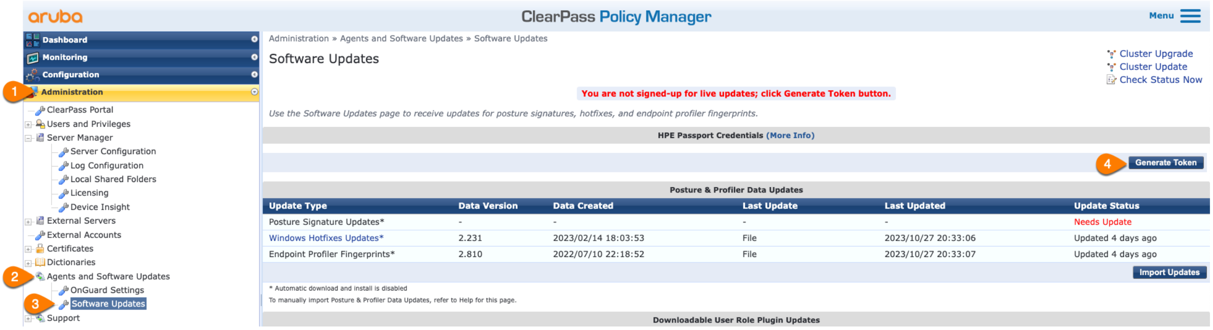
Step 6 is not performed for the second CPPM server. The Access license added in Step 6 is shared by both appliances when they form a cluster.

Configure HPE Passport Credentials

To activate licenses on the newly created ClearPass appliances, the HPE Passport Credentials must first be configured in the **Software Updates** section. Follow the steps below to complete activation.

Step 1 Open a web browser and connect to the first ClearPass appliance using its IP address.

Step 2 Go to **Administration** > **Agents and Software Updates** > **Software Updates** and click the **Generate Token** button on the upper right. Follow the prompts to enter the **HPE Passport Credentials**.



Administration » Agents and Software Updates » Software Updates

Software Updates

You are not signed-up for live updates; click Generate Token button.

Use the Software Updates page to receive updates for posture signatures, hotfixes, and endpoint profiler fingerprints.

HPE Passport Credentials (More Info)

Posture & Profiler Data Updates

Update Type	Data Version	Data Created	Last Update	Last Updated	Update Status
Posture Signature Updates*	-	-	-	-	Needs Update
Windows Hotfixes Updates*	2.231	2023/02/14 18:03:53	File	2023/10/27 20:33:06	Updated 4 days ago
Endpoint Profiler Fingerprints*	2.810	2022/07/10 22:18:52	File	2023/10/27 20:33:07	Updated 4 days ago

* Automatic download and install is disabled

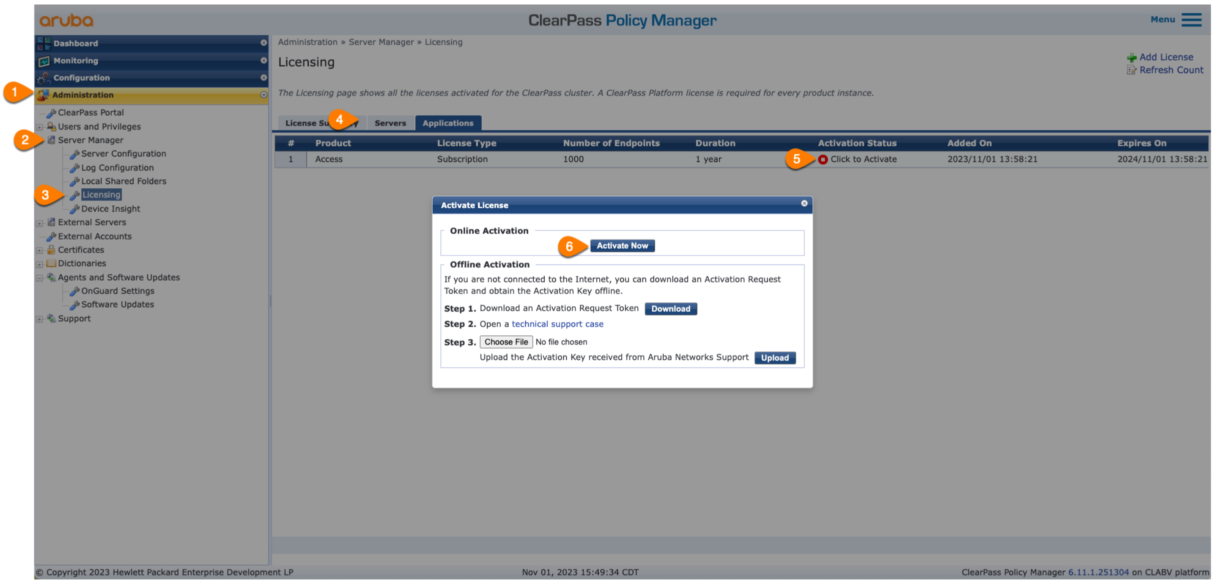
To manually import Posture & Profiler Data Updates, refer to Help for this page.

Downloadable User Role Plugin Updates

Figure 22: Generate Token

Activate Licenses

Step 1 After saving credentials for the ClearPass server, return to the **Administration** > **Server Manager** > **Licensing** > **Servers** tab. Click the red **Click to Activate** link. When the **Activate License** window appears, click the **Activate Now** button.



Administration » Server Manager » Licensing

Licensing

The Licensing page shows all the licenses activated for the ClearPass cluster. A ClearPass Platform license is required for every product instance.

#	Product	License Type	Number of Endpoints	Duration	Activation Status	Added On	Expires On
1	Access	Subscription	1000	1 year	Click to Activate	2023/11/01 13:58:21	2024/11/01 13:58:21

Activate License

Online Activation

Offline Activation

If you are not connected to the Internet, you can download an Activation Request Token and obtain the Activation Key offline.

Step 1. Download an Activation Request Token

Step 2. Open a technical support case

Step 3. No file chosen

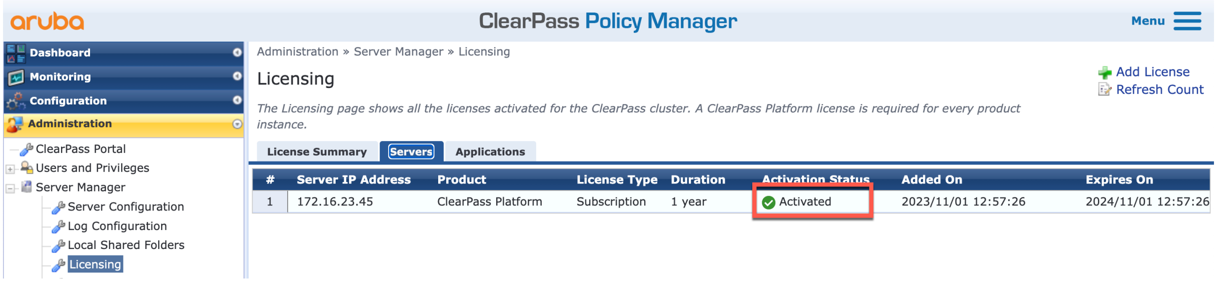
Upload the Activation Key received from Aruba Networks Support

© Copyright 2023 Hewlett Packard Enterprise Development LP Nov 01, 2023 15:49:34 CDT ClearPass Policy Manager 6.11.1.251304 on CLABV platform

Figure 23: Activate Now

Step 2 Repeat the previous step for the **Applications** tab to activate the Access license.

Step 3 Verify that activation is successful, click both the **Servers** and **Applications** tabs and verify the green and white checkmark icon in the **Activation Status** column.



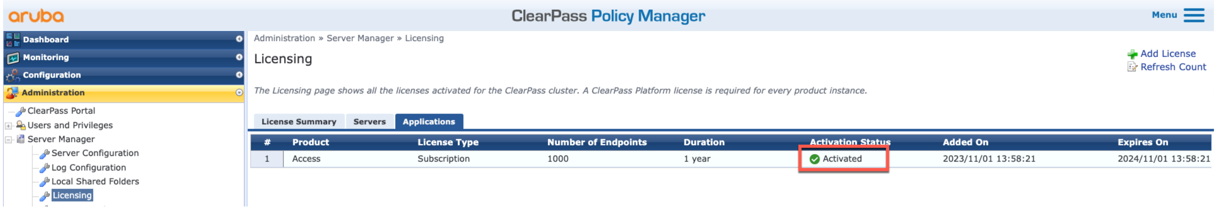
Administration » Server Manager » Licensing

Licensing

The Licensing page shows all the licenses activated for the ClearPass cluster. A ClearPass Platform license is required for every product instance.

#	Server IP Address	Product	License Type	Duration	Activation Status	Added On	Expires On
1	172.16.23.45	ClearPass Platform	Subscription	1 year	✓ Activated	2023/11/01 12:57:26	2024/11/01 12:57:26

Figure 24: Activated



Administration » Server Manager » Licensing

Licensing

The Licensing page shows all the licenses activated for the ClearPass cluster. A ClearPass Platform license is required for every product instance.

#	Product	License Type	Number of Endpoints	Duration	Activation Status	Added On	Expires On
1	Access	Subscription	1000	1 year	✓ Activated	2023/11/01 13:58:21	2024/11/01 13:58:21

Figure 25: Activated2

Step 4 With server and application licenses activated, repeat step 1 for ClearPass server 2.

Cluster Configuration

Deploying an Aruba ClearPass cluster requires creating a logical connection between any combination of ClearPass hardware or virtual appliances. This section outlinea the steps to deploy a two-node cluster consisting of one Publisher and one Subscriber.

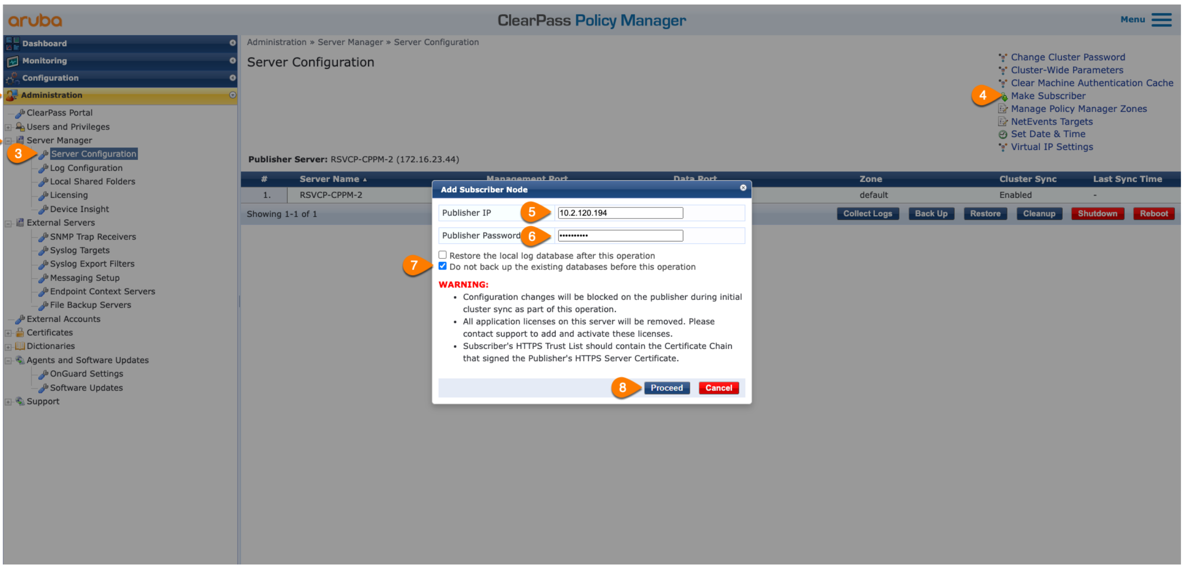
Add Subscriber

Configuring the cluster starts with RSVCP-CPPM-2, which acts as the subscriber to RSVCP-CPPM-1.

Step 1 Open a web browser and connect to RSVCP-CPPM-2.

Step 2 Log in using the admin credentials. - **Username:** *admin* - **Password:** *Aruba123!*

Step 3 From the CPPM Dashboard, go to **Administration** > **Server Manager** > **Server Configuration** and click the **Make Subscriber** link on the upper right of the window. When the **Add Subscriber Node** window appears, enter the IP address and admin password for RSVCP-CPPM-1, check the second checkbox, and click the **Proceed** button.



Publisher Server: RSVCP-CPPM-2 (172.16.23.44)

#	Server Name ▴	Management Port	Data Port	Zone	Cluster Sync	Last Sync Time
1.	RSVCP-CPPM-2			default	Enabled	-

Showing 1-1 of 1

Add Subscriber Node

Publisher IP: 10.2.120.194

Publisher Password: ••••••••••

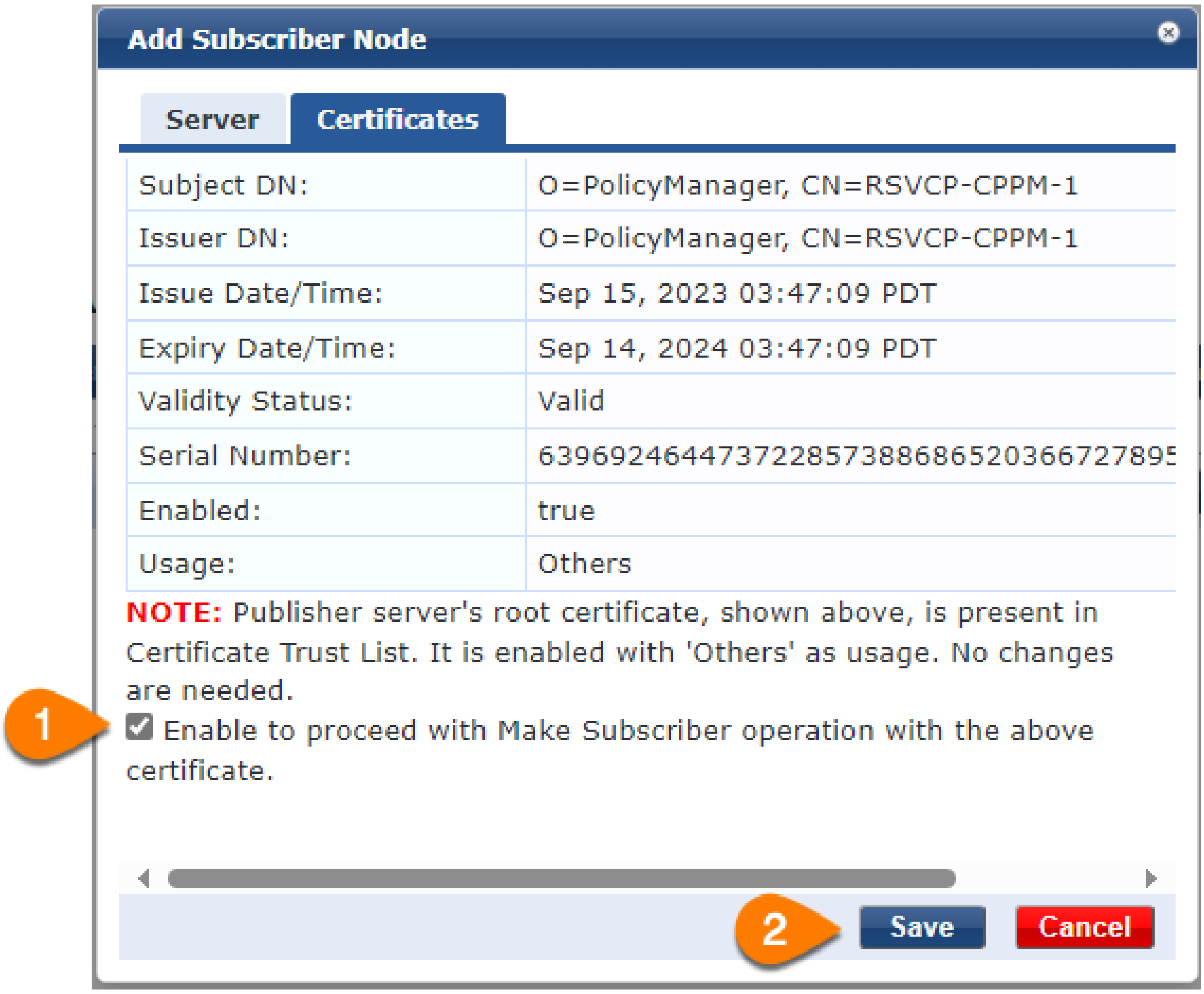
☐ Restore the local log database after this operation
☑ Do not back up the existing databases before this operation

WARNING:

- Configuration changes will be blocked on the publisher during initial cluster sync as part of this operation.
- All application licenses on this server will be removed. Please contact support to add and activate these licenses.
- Subscriber's HTTPS Trust List should contain the Certificate Chain that signed the Publisher's HTTPS Server Certificate.

Figure 26: Make Subscriber

Step 4 When prompted, click the “Enable..” checkbox, then click **Save** button as illustrated below.



Subject DN:	O=PolicyManager, CN=RSVCP-CPPM-1
Issuer DN:	O=PolicyManager, CN=RSVCP-CPPM-1
Issue Date/Time:	Sep 15, 2023 03:47:09 PDT
Expiry Date/Time:	Sep 14, 2024 03:47:09 PDT
Validity Status:	Valid
Serial Number:	639692464473722857388686520366727895
Enabled:	true
Usage:	Others

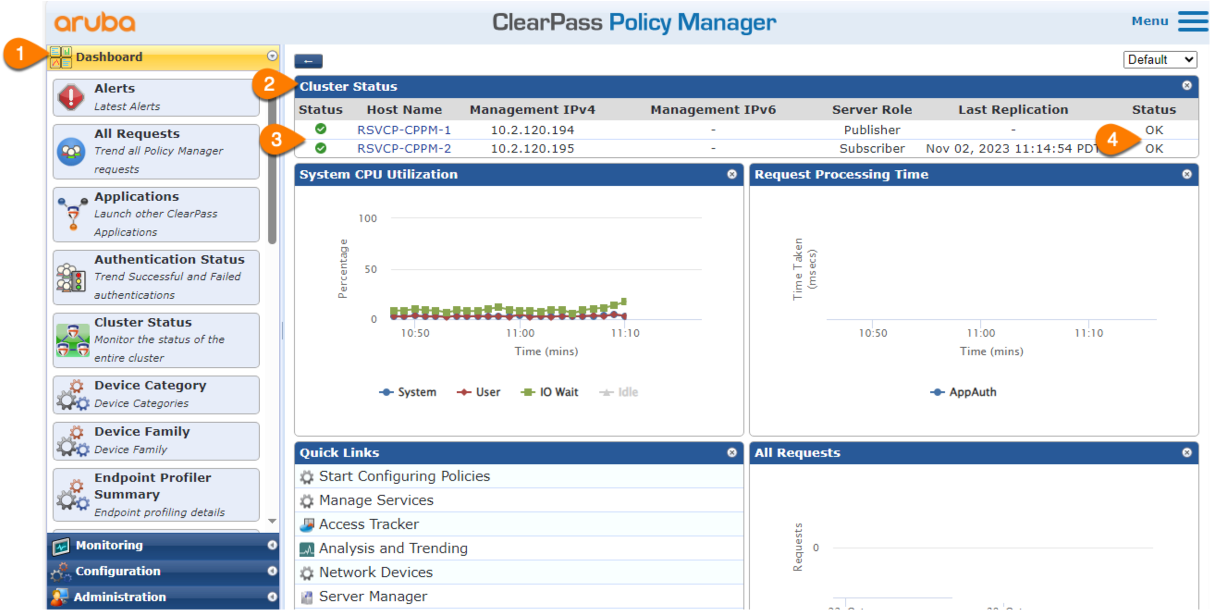
NOTE: Publisher server's root certificate, shown above, is present in Certificate Trust List. It is enabled with 'Others' as usage. No changes are needed.

☑ Enable to proceed with Make Subscriber operation with the above certificate.

Figure 27: Add Subscriber Node

Step 5 Allow activation time (typically 5-15 minutes), then log into RSVCP-CPPM-1's web UI.

Step 6 Verify that the cluster was formed. **Dashboard** > **Cluster Status** pane displays both servers with a green icon and a status of **OK** at the far right for each nodes.



Cluster Status

Status	Host Name	Management IPv4	Management IPv6	Server Role	Last Replication	Status
✓	RSVCP-CPPM-1	10.2.120.194	-	Publisher	-	OK
✓	RSVCP-CPPM-2	10.2.120.195	-	Subscriber	Nov 02, 2023 11:14:54 PDT	OK

Figure 28: Verify Cluster Status

Step 7 When the cluster is formed, proceed to next section.

NOTE:

After the cluster is formed, all subsequent configuration is performed using the Publisher node. See the Cluster Configuration Options page for more details.

Configure Virtual IP Addresses

Two nodes in a cluster can be configured to share one or more virtual IP addresss. Each virtual IP address is bound to the Primary node by default. The Secondary node takes over when the Primary node is unavailable. For OWL's ClearPass deployment, two virtual IPs are configured according to the following table.

Virtual IP	Primary Node	Secondary Node	Interface	Virtual Host ID
10.2.120.192	RSVCP-CPPM-1	RSVCP-CPPM-2	MGMT	1
10.2.120.193	RSVCP-CPPM-2	RSVCP-CPPM-1	MGMT	2

NOTE:

Although not required, this sample cluster is configured with two virtual IP addresses for load balancing. This is achieved by configuring one virtual IP address as the primary RADIUS server for switches and gateways from half of the sites and the other as the primary RADIUS server for the other half, ensuring that both ClearPass appliances actively serve clients at all times.

NOTE:

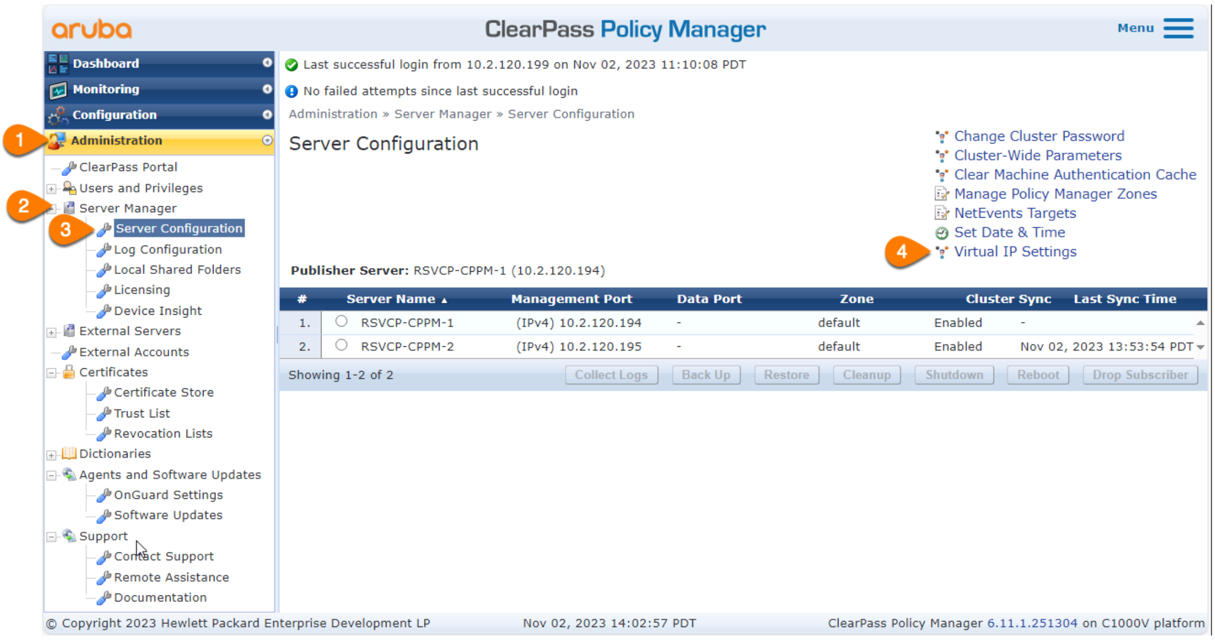
If a ClearPass cluster design requires configuring Virtual IP address(es) in a virtual machine deployment similar to this sample deployment, then “forged transmits” must be enabled on the VMWare distributed virtual switch to allow the Virtual IP feature.

Follow the steps below to configure the Virtual IP Settings.

Step 1 Open a web browser and connect to the publisher node, RSVCP-CPPM-1.

Step 2 Log in using the admin credentials. - **Username:** *admin* - **Password:** *Aruba123!*

Step 3 Go to **Administration** > **Server Manager** > **Server Configuration** and click the **Virtual IP Settings** link at the upper right area.



Last successful login from 10.2.120.199 on Nov 02, 2023 11:10:08 PDT

No failed attempts since last successful login

Administration » Server Manager » Server Configuration

Server Configuration

Publisher Server: RSVCP-CPPM-1 (10.2.120.194)

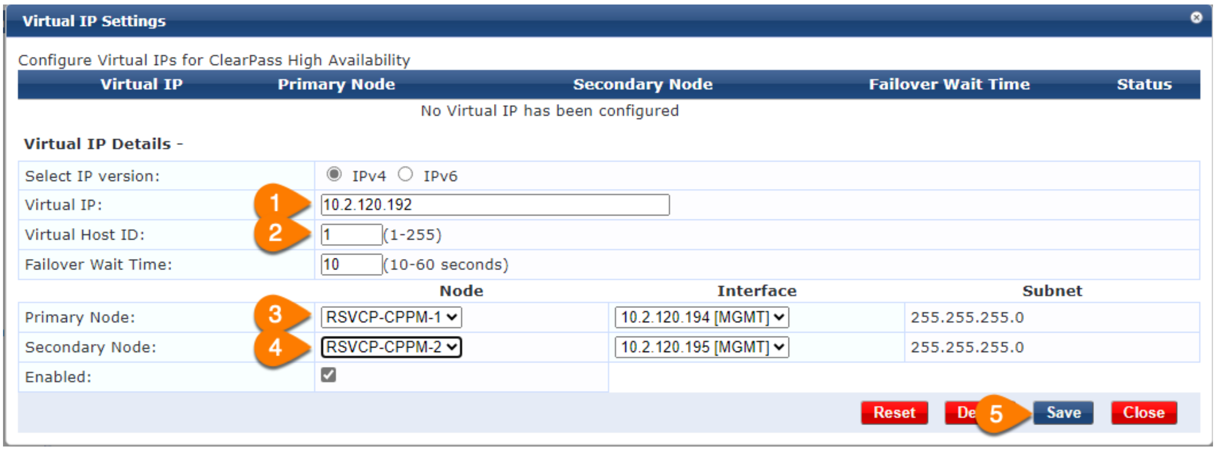
#	Server Name ▲	Management Port	Data Port	Zone	Cluster Sync	Last Sync Time
1.	○ RSVCP-CPPM-1	(IPv4) 10.2.120.194	-	default	Enabled	-
2.	○ RSVCP-CPPM-2	(IPv4) 10.2.120.195	-	default	Enabled	Nov 02, 2023 13:53:54 PDT

Showing 1-2 of 2

© Copyright 2023 Hewlett Packard Enterprise Development LP Nov 02, 2023 14:02:57 PDT ClearPass Policy Manager 6.11.1.251304 on C1000V platform

Figure 29: Virtual IP Settings 1

Step 4 In the **Virtual IP Settings** window, enter the first Virtual IP configuration using the table at the beginning of this subsection. Click the **Save** button.



Virtual IP Settings

Configure Virtual IPs for ClearPass High Availability

Virtual IP	Primary Node	Secondary Node	Failover Wait Time	Status
No Virtual IP has been configured				

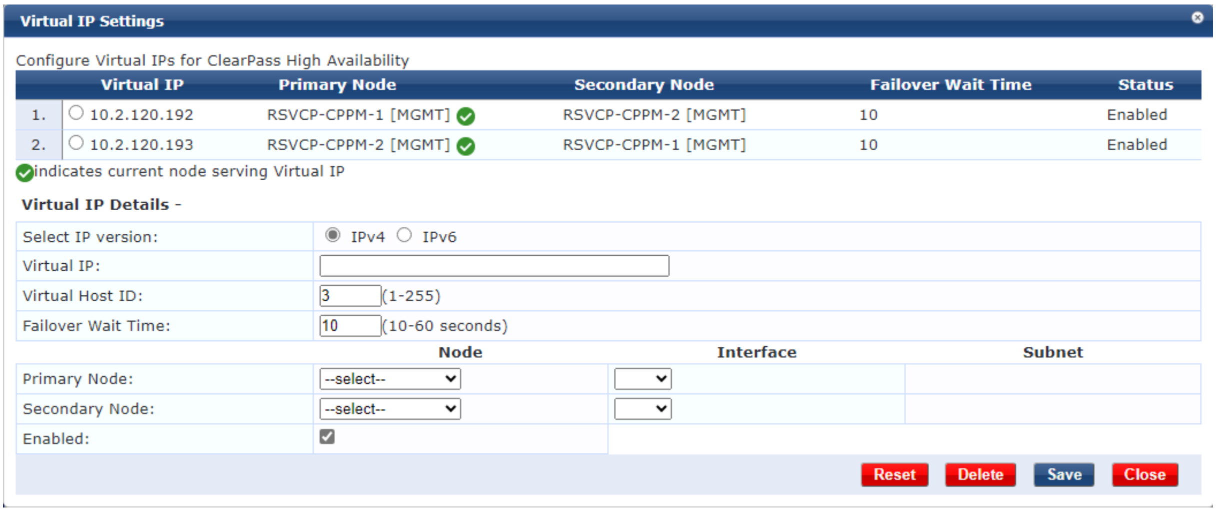
Virtual IP Details -

Select IP version:	● IPv4 ○ IPv6		
Virtual IP:	10.2.120.192		
Virtual Host ID:	1 (1-255)		
Failover Wait Time:	10 (10-60 seconds)		
	Node	**Interface**	**Subnet**
Primary Node:	RSVCP-CPPM-1	10.2.120.194 [MGMT]	255.255.255.0
Secondary Node:	RSVCP-CPPM-2	10.2.120.195 [MGMT]	255.255.255.0
Enabled:	☑		

Figure 30: Virtual IP Settings 2

Step 5 Repeat step 4 above for the second Virtual IP configuration.

Step 5 Click the **Close** button and re-open the **Virtual IP Settings** window to verify that both addresses show a **Status** of *Enabled* similar to the screenshot below.



Virtual IP Settings

Configure Virtual IPs for ClearPass High Availability

	Virtual IP	Primary Node	Secondary Node	Failover Wait Time	Status
1.	○ 10.2.120.192	RSVCP-CPPM-1 [MGMT] ✓	RSVCP-CPPM-2 [MGMT]	10	Enabled
2.	○ 10.2.120.193	RSVCP-CPPM-2 [MGMT] ✓	RSVCP-CPPM-1 [MGMT]	10	Enabled

✓indicates current node serving Virtual IP

Virtual IP Details -

Select IP version:	● IPv4 ○ IPv6		
Virtual IP:			
Virtual Host ID:	3 (1-255)		
Failover Wait Time:	10 (10-60 seconds)		
	Node	**Interface**	**Subnet**
Primary Node:	--select--		
Secondary Node:	--select--		
Enabled:	☑		

Figure 31: Virtual IP Settings 3

Join Domain

This procedure describes the steps to integrate Policy Manager and Microsoft Active Directory. For some use cases, Policy Manager is required to join the Active Directory, for example: 802.1X authentication with EAP-PEAP-MSCHAPv2. In other use cases, such as with Captive Portal authentication, joining Policy Manager to Active Directory is optional.

A one-time procedure to join Policy Manager to the domain must be performed from an account that has the ability to join a computer to the domain. For this deployment, use the credentials recorded in the **External Authentication Sources** subsection of the **ClearPass Preparation** page.

- **Username:** *olwservice@owllab .net*

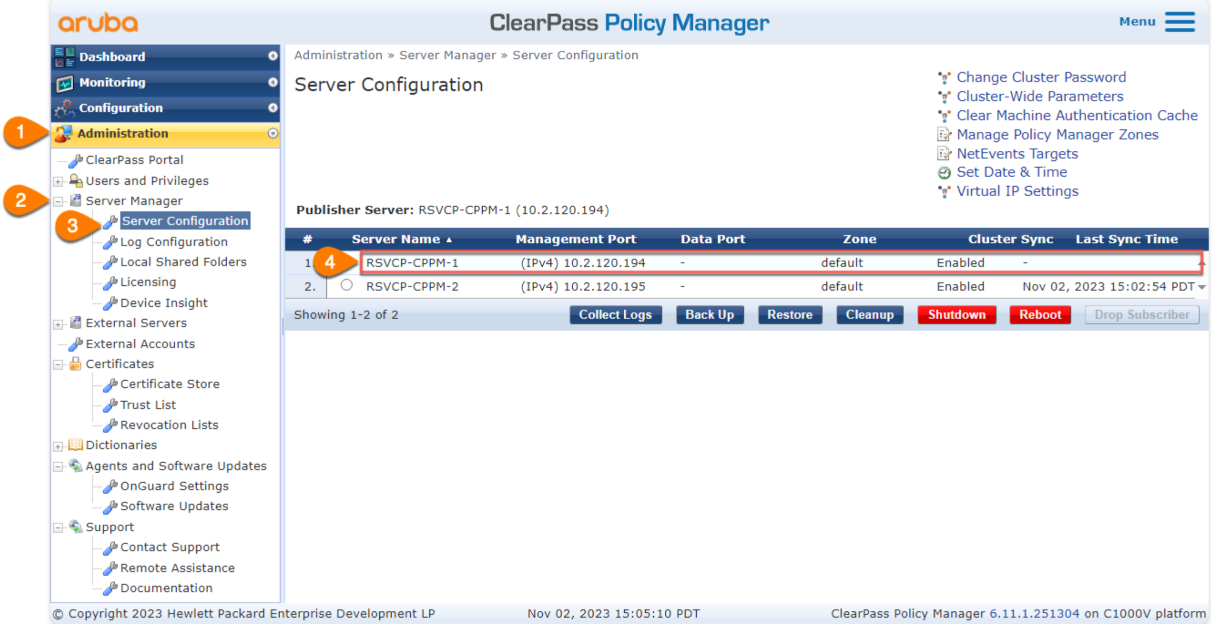
- **Password:** *Aruba123!*

Follow the steps below to join both ClearPass appliances to the domain.

Step 1 Open a web browser and connect to the publisher node, RSVCP-CPPM-1.

Step 2 Log in using the admin credentials. - **Username:** *admin* - **Password:** *Aruba123!*

Step 3 Go to **Administration** > **Server Manager** > **Server Configuration** and click anywhere along the line of RSVCP-CPPM-1 indicated by the red box below. Do not click the radio button next to the server name.



Administration » Server Manager » Server Configuration

Server Configuration

Publisher Server: RSVCP-CPPM-1 (10.2.120.194)

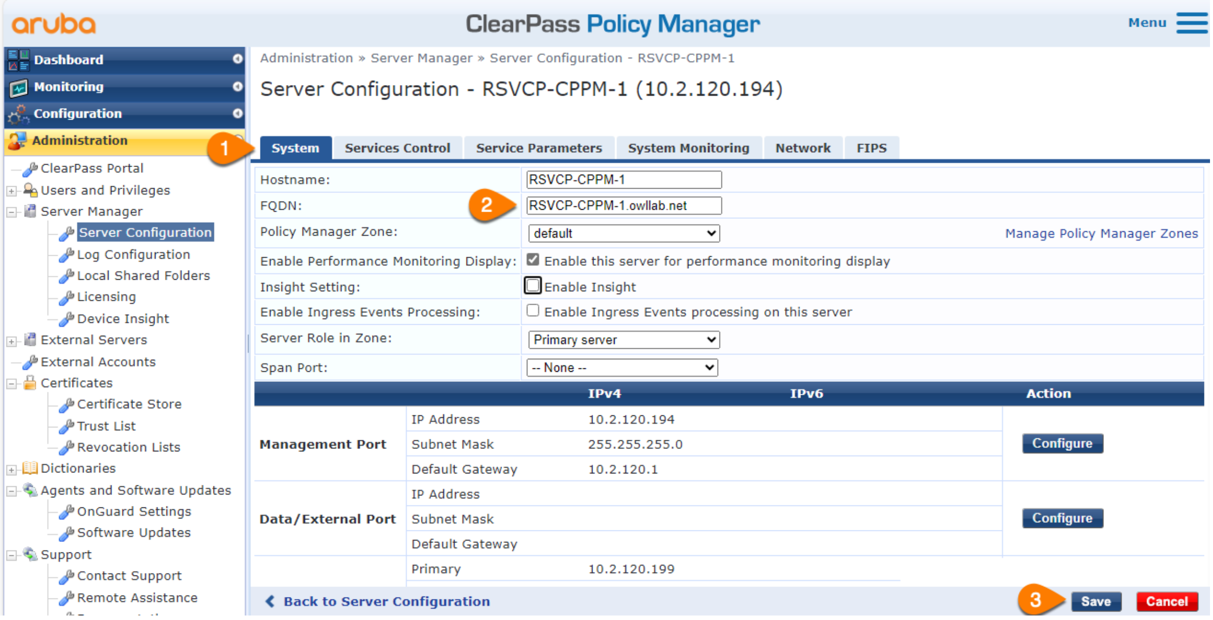
#	Server Name ▲	Management Port	Data Port	Zone	Cluster Sync	Last Sync Time
1	RSVCP-CPPM-1	(IPv4) 10.2.120.194	-	default	Enabled	-
2.	○ RSVCP-CPPM-2	(IPv4) 10.2.120.195	-	default	Enabled	Nov 02, 2023 15:02:54 PDT

Showing 1-2 of 2

© Copyright 2023 Hewlett Packard Enterprise Development LP Nov 02, 2023 15:05:10 PDT ClearPass Policy Manager 6.11.1.251304 on C1000V platform

Figure 32: Domain Join 1

Step 4 In the **Server Configuration** details page for RSVCP-CPPM-1, in the **System** tab, enter the fully qualified domain name for the appliance. Click the **Save** button.



Administration » Server Manager » Server Configuration - RSVCP-CPPM-1

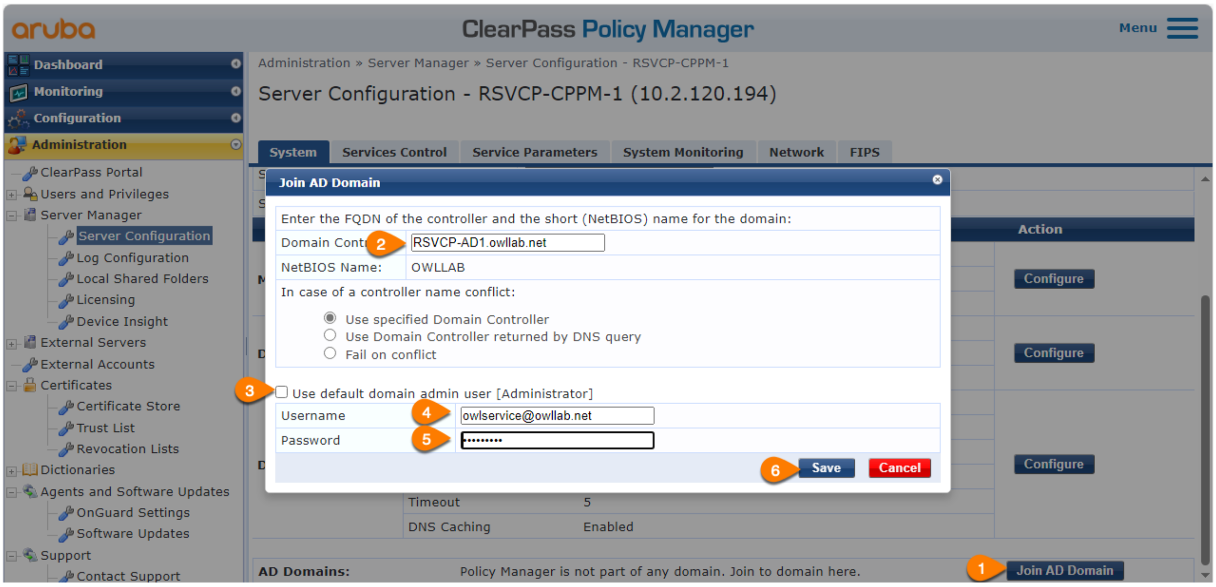
Server Configuration - RSVCP-CPPM-1 (10.2.120.194)

Hostname:	RSVCP-CPPM-1
FQDN:	RSVCP-CPPM-1.owllab.net
Policy Manager Zone:	default
Enable Performance Monitoring Display:	☑ Enable this server for performance monitoring display
Insight Setting:	□ Enable Insight
Enable Ingress Events Processing:	□ Enable Ingress Events processing on this server
Server Role in Zone:	Primary server
Span Port:	-- None --

		IPv4	IPv6	Action
Management Port	IP Address	10.2.120.194		Configure
	Subnet Mask	255.255.255.0		
	Default Gateway	10.2.120.1		
Data/External Port	IP Address			Configure
	Subnet Mask			
	Default Gateway			
	Primary	10.2.120.199		

Figure 33: Configure FQDN

Step 5 After saving the FQDN setting, scroll to the bottom of the page, click the **Join AD Domain** button on the lower right, and enter the required information in the **Join AD Domain** window. Click **Save** to close the window.



Administration » Server Manager » Server Configuration - RSVCP-CPPM-1

Server Configuration - RSVCP-CPPM-1 (10.2.120.194)

Join AD Domain

Enter the FQDN of the controller and the short (NetBIOS) name for the domain:

Domain Cont	RSVCP-AD1.owllab.net
NetBIOS Name:	OWLLAB

In case of a controller name conflict:

● Use specified Domain Controller
○ Use Domain Controller returned by DNS query
○ Fail on conflict

□ Use default domain admin user [Administrator]

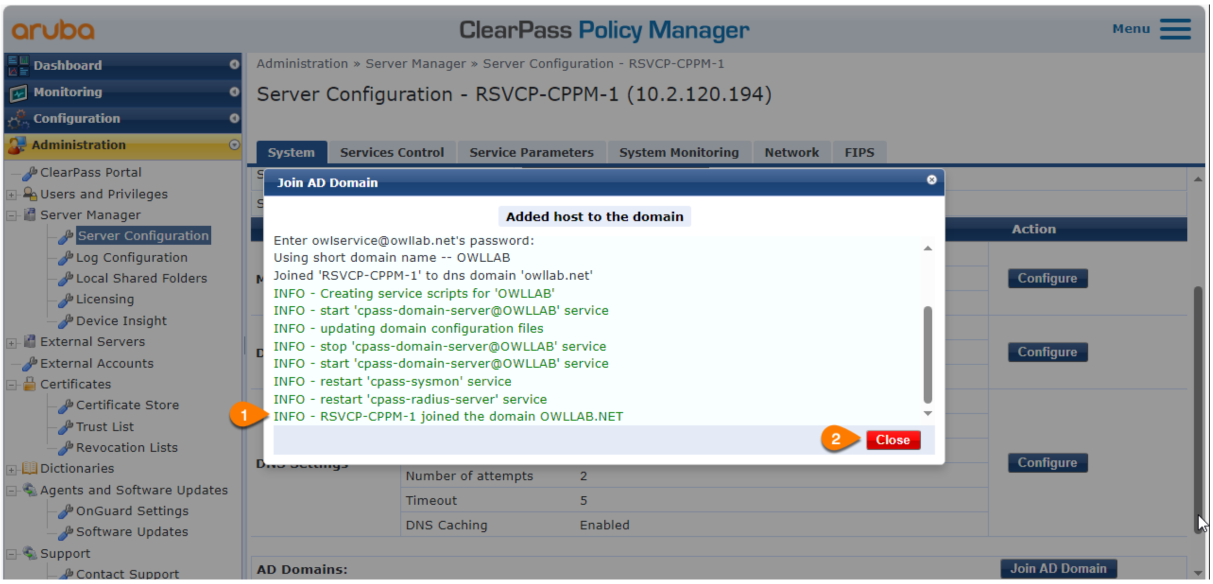
Username	owlservice@owllab.net
Password	•••••••••

Timeout	5
DNS Caching	Enabled

AD Domains: Policy Manager is not part of any domain. Join to domain here.

Figure 34: Join AD Domain

Step 6 Wait for the domain join process to finish and click the **Close** button.



Server Configuration - RSVCP-CPPM-1 (10.2.120.194)

Added host to the domain

```
Enter owlservice@owllab.net's password:
Using short domain name -- OWLLAB
Joined 'RSVCP-CPPM-1' to dns domain 'owllab.net'
INFO - Creating service scripts for 'OWLLAB'
INFO - start 'cpass-domain-server@OWLLAB' service
INFO - updating domain configuration files
INFO - stop 'cpass-domain-server@OWLLAB' service
INFO - start 'cpass-domain-server@OWLLAB' service
INFO - restart 'cpass-sysmon' service
INFO - restart 'cpass-radius-server' service
INFO - RSVCP-CPPM-1 joined the domain OWLLAB.NET
```

Number of attempts	2
Timeout	5
DNS Caching	Enabled

Figure 35: Domain Join Complete

Step 7 Repeat steps 3 to 6 for RSVCP-CPPM-2, then proceed to the next section.

Enable Insight

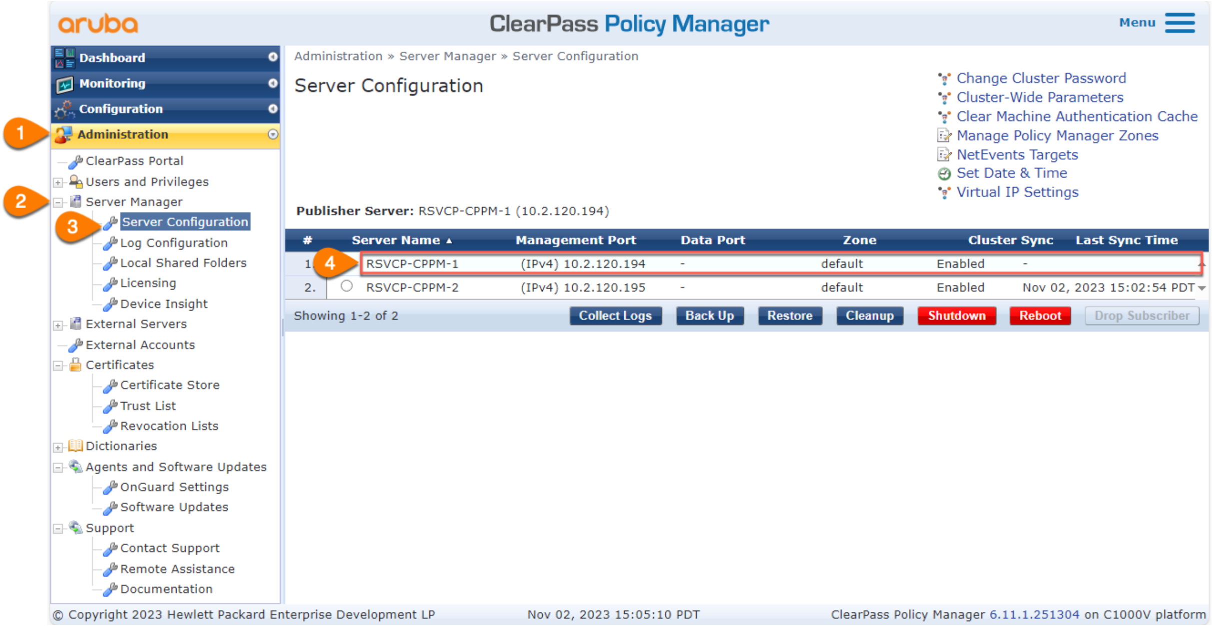
Multiple functions depend on Policy Manager Insight. For example, to use MAC caching, Policy Manager Insight must be enabled on at least one server within a cluster. Enabling Policy Manager Insight on at least two servers in a cluster is recommended. For more details, see the Policy Manager Insight section of the CPPM User Guide.

Follow the steps below to enable Policy Manager Insight.

Step 1 Open a web browser and connect to the publisher node, RSVCP-CPPM-1.

Step 2 Log in using the admin credentials. - **Username:** *admin* - **Password:** *Aruba123!*

Step 3 Go to **Administration** > **Server Manager** > **Server Configuration** and click anywhere along the line of RSVCP-CPPM-1 indicated by the red box below. Do not click the radio button next to the server name.



Administration » Server Manager » Server Configuration

Server Configuration

Publisher Server: RSVCP-CPPM-1 (10.2.120.194)

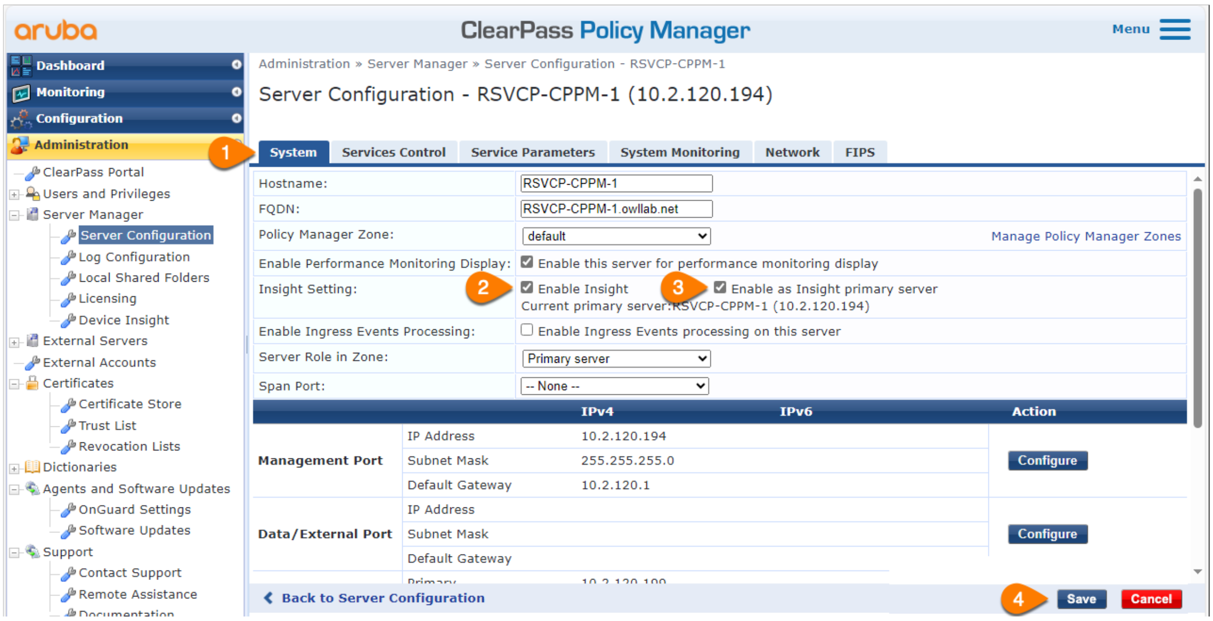
#	Server Name ▲	Management Port	Data Port	Zone	Cluster Sync	Last Sync Time
1.	RSVCP-CPPM-1	(IPv4) 10.2.120.194	-	default	Enabled	-
2.	○ RSVCP-CPPM-2	(IPv4) 10.2.120.195	-	default	Enabled	Nov 02, 2023 15:02:54 PDT

Showing 1-2 of 2

© Copyright 2023 Hewlett Packard Enterprise Development LP   Nov 02, 2023 15:05:10 PDT   ClearPass Policy Manager 6.11.1.251304 on C1000V platform

Figure 36: Insight 1

Step 4 In the **Server Configuration** details page for RSVCP-CPPM-1, in the **System** tab, check both boxes in the **Insight Setting** section and click the **Save** button to enable Insight for the publisher and set it as the primary Insight server.



Administration » Server Manager » Server Configuration - RSVCP-CPPM-1

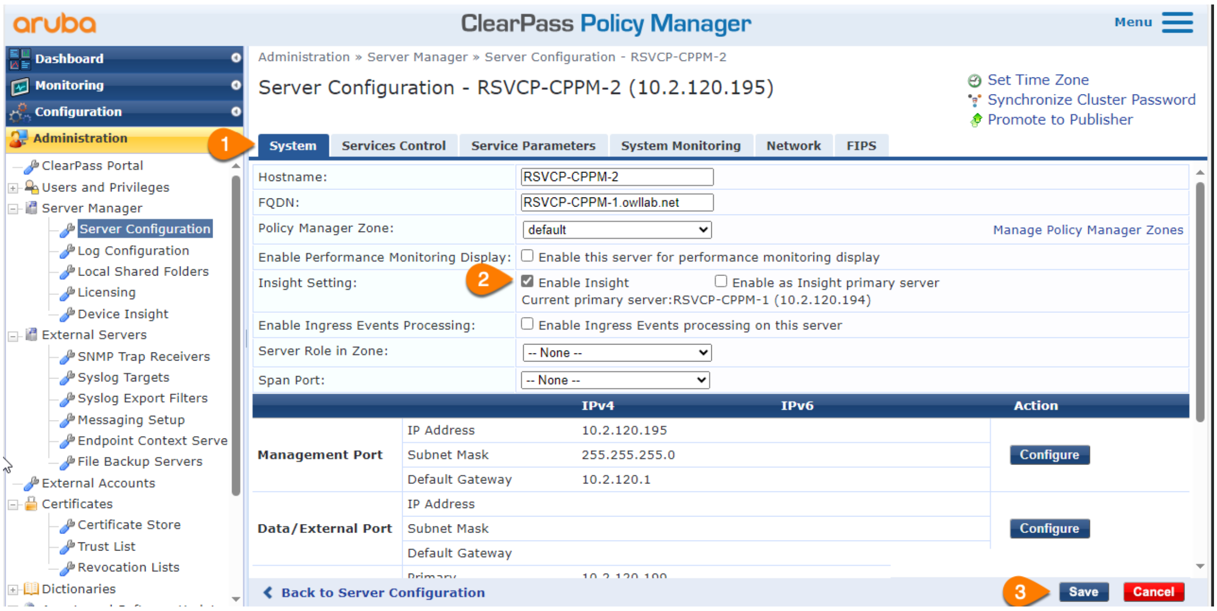
Server Configuration - RSVCP-CPPM-1 (10.2.120.194)

Hostname:	RSVCP-CPPM-1
FQDN:	RSVCP-CPPM-1.owllab.net
Policy Manager Zone:	default
Enable Performance Monitoring Display:	☑ Enable this server for performance monitoring display
Insight Setting:	☑ Enable Insight ☑ Enable as Insight primary server Current primary server:RSVCP-CPPM-1 (10.2.120.194)
Enable Ingress Events Processing:	□ Enable Ingress Events processing on this server
Server Role in Zone:	Primary server
Span Port:	-- None --

		IPv4	IPv6	Action
Management Port	IP Address	10.2.120.194		
	Subnet Mask	255.255.255.0		
	Default Gateway	10.2.120.1		
Data/External Port	IP Address			
	Subnet Mask			
	Default Gateway			
	Primary	10.2.120.100		

Figure 37: Enable Insight

Step 5 Repeat the steps above for RSVCP-CPPM-2, but do not check the box to set it as the primary Insight server as shown below.



Server Configuration - RSVCP-CPPM-2 (10.2.120.195)

Hostname:	RSVCP-CPPM-2
FQDN:	RSVCP-CPPM-1.owllab.net
Policy Manager Zone:	default
Enable Performance Monitoring Display:	☐ Enable this server for performance monitoring display
Insight Setting:	☑ Enable Insight ☐ Enable as Insight primary server Current primary server:RSVCP-CPPM-1 (10.2.120.194)
Enable Ingress Events Processing:	☐ Enable Ingress Events processing on this server
Server Role in Zone:	-- None --
Span Port:	-- None --

		IPv4	IPv6	Action
Management Port	IP Address	10.2.120.195		Configure
	Subnet Mask	255.255.255.0		
	Default Gateway	10.2.120.1		
Data/External Port	IP Address			Configure
	Subnet Mask			
	Default Gateway			
	Primary	10.2.120.100		

Figure 38: Enable Insight 2

Step 6 With Insight enabled on both nodes in this cluster, proceed to the next steps.

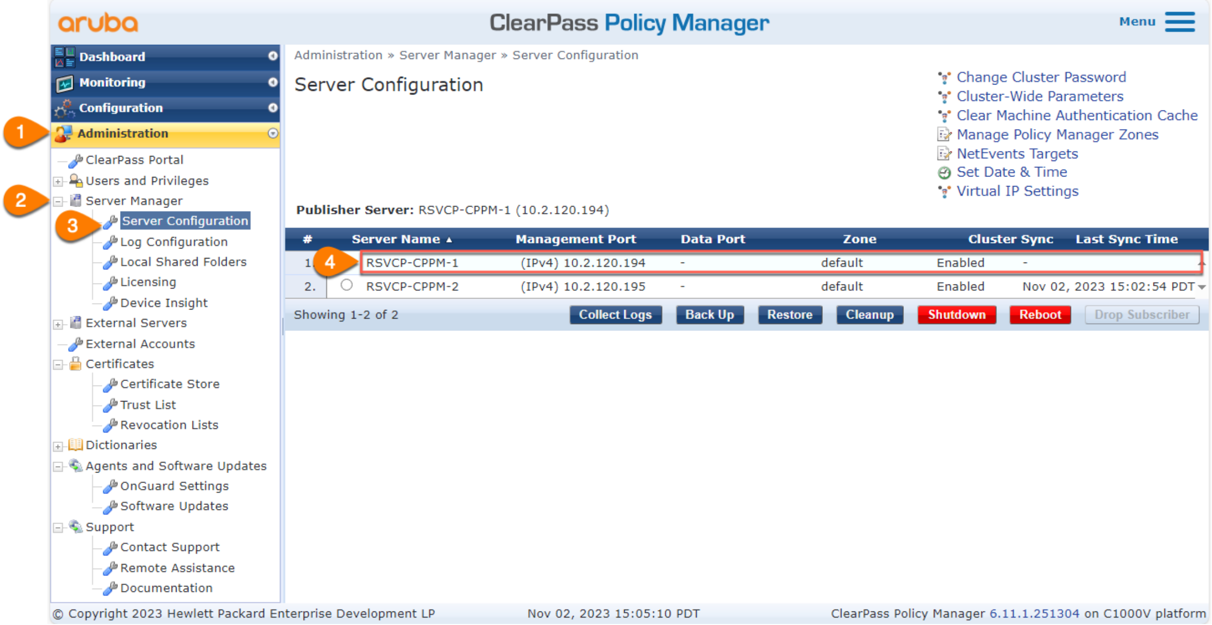
Enable Log Interim Accounting

Follow the steps below to enable ClearPass to collect more granular RADIUS accounting information.

Step 1 Open a web browser and connect to the publisher node, RSVCP-CPPM-1.

Step 2 Log in using the admin credentials. - **Username:** *admin* - **Password:** *Aruba123!*

Step 3 Go to **Administration** > **Server Manager** > **Server Configuration** and click anywhere along the line of RSVCP-CPPM-1 indicated by the red box below. Do not click the radio button next to the server name.



Administration » Server Manager » Server Configuration

Server Configuration

Publisher Server: RSVCP-CPPM-1 (10.2.120.194)

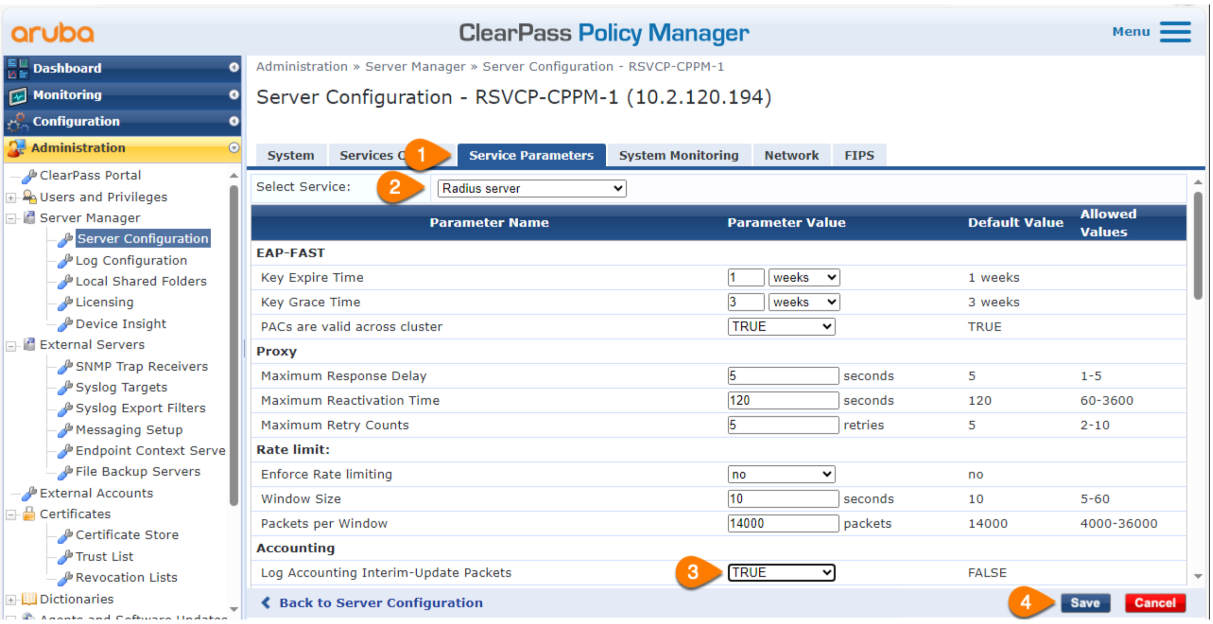
#	Server Name ▲	Management Port	Data Port	Zone	Cluster Sync	Last Sync Time
1.	RSVCP-CPPM-1	(IPv4) 10.2.120.194	-	default	Enabled	-
2. ○	RSVCP-CPPM-2	(IPv4) 10.2.120.195	-	default	Enabled	Nov 02, 2023 15:02:54 PDT

Showing 1-2 of 2

© Copyright 2023 Hewlett Packard Enterprise Development LP   Nov 02, 2023 15:05:10 PDT   ClearPass Policy Manager 6.11.1.251304 on C1000V platform

Figure 39: Insight 1

Step 4 In the **Server Configuration** details page for RSVCP-CPPM-1, in the **Service Parameters** tab, select the *Radius server* option from the **Select Service** dropdown. Scroll to the **Accounting** section, set the **Log Accounting Interim-Update Packets** option to *TRUE*, and click the **Save** button.



Administration » Server Manager » Server Configuration - RSVCP-CPPM-1

Server Configuration - RSVCP-CPPM-1 (10.2.120.194)

Select Service: Radius server

Parameter Name	Parameter Value		Default Value	Allowed Values
EAP-FAST				
Key Expire Time	1	weeks	1 weeks	
Key Grace Time	3	weeks	3 weeks	
PACs are valid across cluster	TRUE		TRUE	
Proxy				
Maximum Response Delay	5	seconds	5	1-5
Maximum Reactivation Time	120	seconds	120	60-3600
Maximum Retry Counts	5	retries	5	2-10
Rate limit:				
Enforce Rate limiting	no		no	
Window Size	10	seconds	10	5-60
Packets per Window	14000	packets	14000	4000-36000
Accounting				
Log Accounting Interim-Update Packets	TRUE		FALSE	

Figure 40: Log Interim Accounting

Step 5 Repeat the steps above for RSVCP-CPPM-2 and proceed to the next section.

Update Cluster Software

ClearPass Policy Manager regularly checks for available updates on the Policy Manager Webservice server. Appliances can be updated individually or as a cluster using **Cluster Update**. The **Cluster Update** page automates the process of updating a cluster. The Publisher is automatically updated first before selected Subscribers.

Follow the steps below to update the cluster. Find more information in the Software Updates section of the ClearPass User Guide.

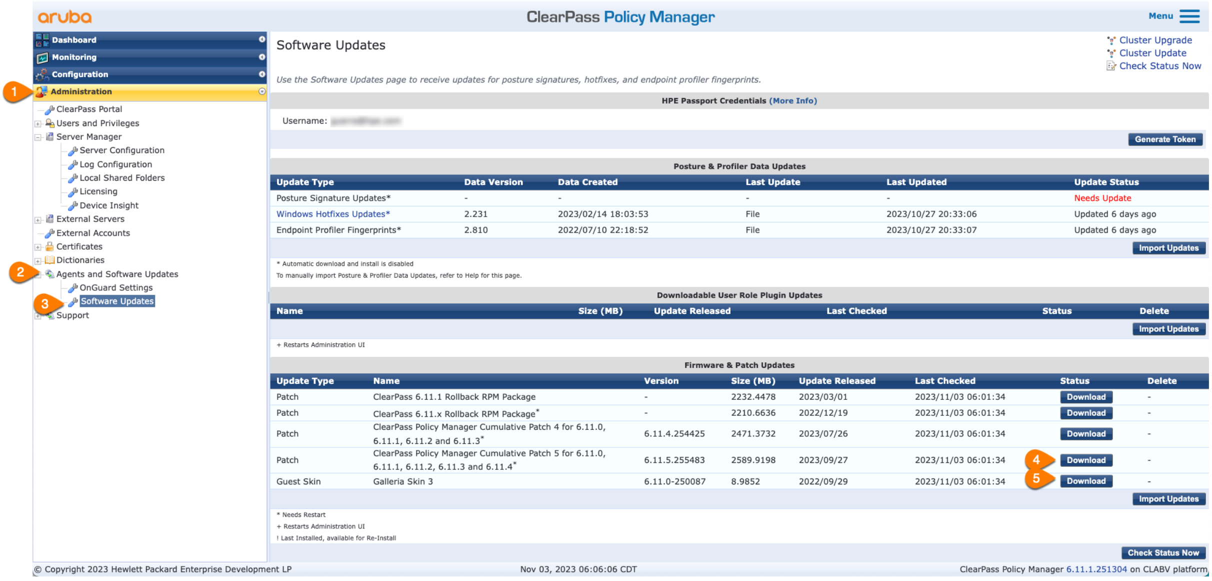
NOTE:

Valid HPE Passport Credentials must be configured to receive updates. Please refer to the **Configure HPE Passport Credentials** section earlier in this guide for details.

Step 1 Open a web browser and connect to the publisher node, RSVCP-CPPM-1.

Step 2 Log in using the admin credentials. - **Username:** *admin* - **Password:** *Aruba123!*

Step 3 Go to **Administration** > **Agents and Software Updates** > **Software Updates** > **Firmware & Patch Updates** and click the **Download** buttons for the required patches. The new guest skin and the latest patch are downloaded for this sample deployment.



Software Updates

Use the Software Updates page to receive updates for posture signatures, hotfixes, and endpoint profiler fingerprints.

HPE Passport Credentials (More Info)

Username: [redacted]

Posture & Profiler Data Updates

Update Type	Data Version	Data Created	Last Update	Last Updated	Update Status
Posture Signature Updates*	-	-	-	-	Needs Update
Windows Hotfixes Updates*	2.231	2023/02/14 18:03:53	File	2023/10/27 20:33:06	Updated 6 days ago
Endpoint Profiler Fingerprints*	2.810	2022/07/10 22:18:52	File	2023/10/27 20:33:07	Updated 6 days ago

* Automatic download and install is disabled
To manually import Posture & Profiler Data Updates, refer to Help for this page.

Downloadable User Role Plugin Updates

Name	Size (MB)	Update Released	Last Checked	Status	Delete

+ Restarts Administration UI

Firmware & Patch Updates

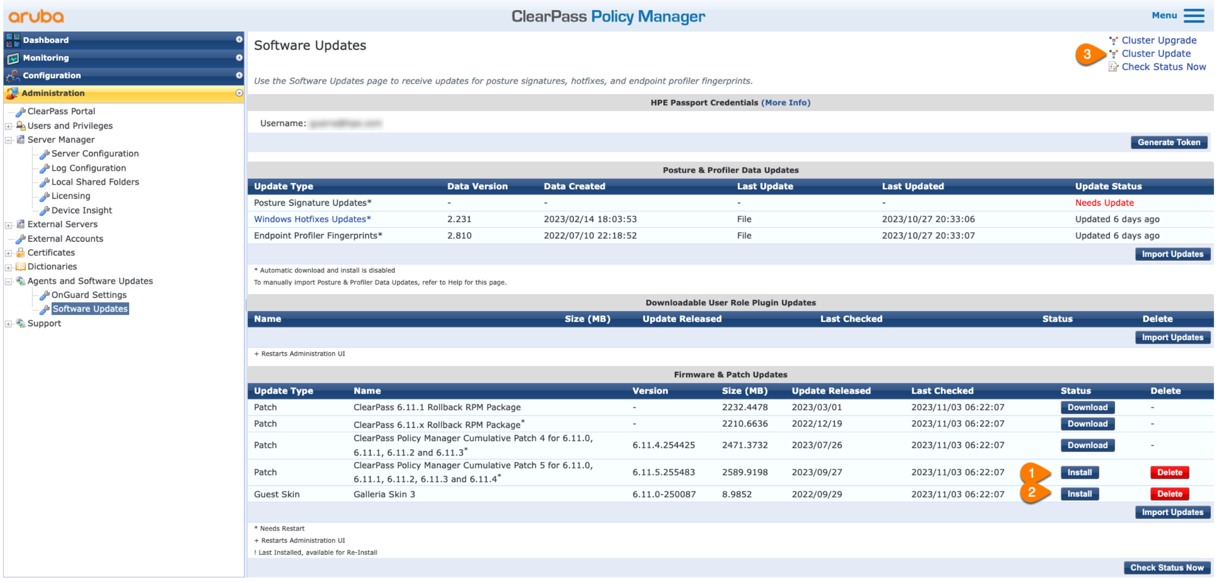
Update Type	Name	Version	Size (MB)	Update Released	Last Checked	Status	Delete
Patch	ClearPass 6.11.1 Rollback RPM Package	-	2232.4478	2023/03/01	2023/11/03 06:01:34	Download	-
Patch	ClearPass 6.11.x Rollback RPM Package*	-	2210.6636	2022/12/19	2023/11/03 06:01:34	Download	-
Patch	ClearPass Policy Manager Cumulative Patch 4 for 6.11.0, 6.11.1, 6.11.2 and 6.11.3*	6.11.4.254425	2471.3732	2023/07/26	2023/11/03 06:01:34	Download	-
Patch	ClearPass Policy Manager Cumulative Patch 5 for 6.11.0, 6.11.1, 6.11.2, 6.11.3 and 6.11.4*	6.11.5.255483	2589.9198	2023/09/27	2023/11/03 06:01:34	Download	-
Guest Skin	Galleria Skin 3	6.11.0-250087	8.9852	2022/09/29	2023/11/03 06:01:34	Download	-

* Needs Restart
+ Restarts Administration UI
! Last Installed, available for Re-Install

© Copyright 2023 Hewlett Packard Enterprise Development LP Nov 03, 2023 06:06:06 CDT ClearPass Policy Manager 6.11.1.251304 on CLABV platform

Figure 41: Download Updates

Step 4 After both updates are complete, verify that the **Download** buttons changed to **Install.** Click the **Cluster Update** link at the upper right.



Software Updates

Use the Software Updates page to receive updates for posture signatures, hotfixes, and endpoint profiler fingerprints.

HPE Passport Credentials (More Info)

Username: [redacted]

Generate Token

Posture & Profiler Data Updates

Update Type	Data Version	Data Created	Last Update	Last Updated	Update Status
Posture Signature Updates*	-	-	-	-	Needs Update
Windows Hotfixes Updates*	2.231	2023/02/14 18:03:53	File	2023/10/27 20:33:06	Updated 6 days ago
Endpoint Profiler Fingerprints*	2.810	2022/07/10 22:18:52	File	2023/10/27 20:33:07	Updated 6 days ago

Import Updates

* Automatic download and install is disabled
To manually import Posture & Profiler Data Updates, refer to Help for this page.

Downloadable User Role Plugin Updates

Name	Size (MB)	Update Released	Last Checked	Status	Delete

Import Updates

+ Restarts Administration UI

Firmware & Patch Updates

Update Type	Name	Version	Size (MB)	Update Released	Last Checked	Status	Delete
Patch	ClearPass 6.11.1 Rollback RPM Package	-	2232.4478	2023/03/01	2023/11/03 06:22:07	Download	-
Patch	ClearPass 6.11.x Rollback RPM Package*	-	2210.6636	2022/12/19	2023/11/03 06:22:07	Download	-
Patch	ClearPass Policy Manager Cumulative Patch 4 for 6.11.0, 6.11.1, 6.11.2 and 6.11.3*	6.11.4.254425	2471.3732	2023/07/26	2023/11/03 06:22:07	Download	-
Patch	ClearPass Policy Manager Cumulative Patch 5 for 6.11.0, 6.11.1, 6.11.2, 6.11.3 and 6.11.4*	6.11.5.255483	2589.9198	2023/09/27	2023/11/03 06:22:07	Install	Delete
Guest Skin	Galleria Skin 3	6.11.0-250087	8.9852	2022/09/29	2023/11/03 06:22:07	Install	Delete

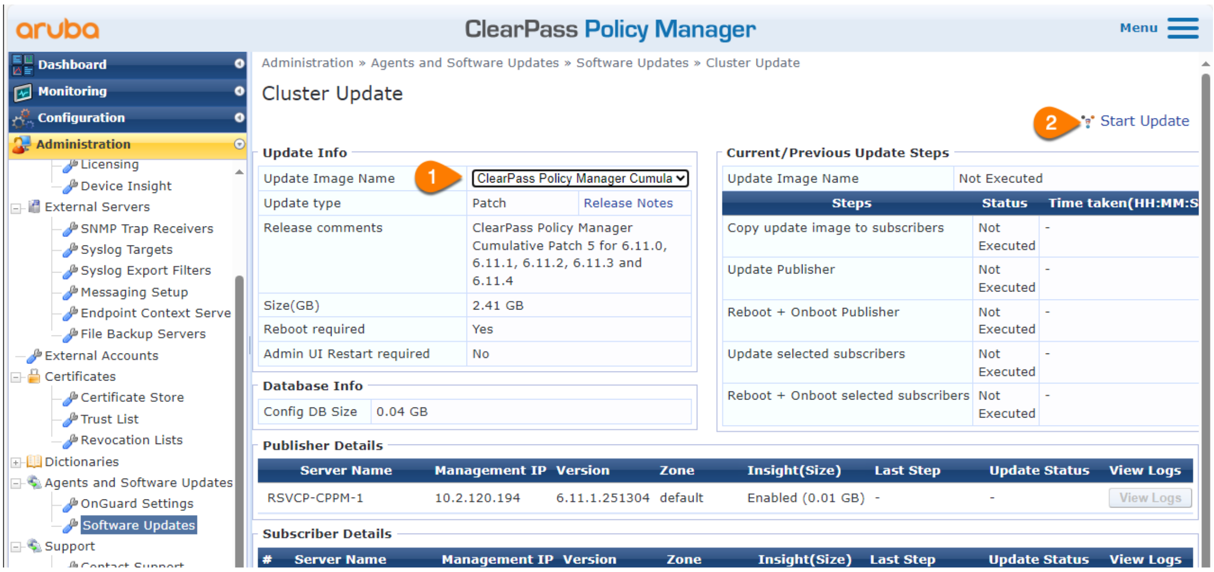
Import Updates

* Needs Restart
+ Restarts Administration UI
! Last Installed, available for Re-Install

Check Status Now

Figure 42: Cluster Update

Step 5 On the **Cluster Update** page, select the *Cumulative Patch* and click the **Start Update** link on the upper right to open the **Start Cluster Update** window.



Administration » Agents and Software Updates » Software Updates » Cluster Update

Cluster Update

Update Info

Update Image Name	ClearPass Policy Manager Cumula
Update type	Patch Release Notes
Release comments	ClearPass Policy Manager Cumulative Patch 5 for 6.11.0, 6.11.1, 6.11.2, 6.11.3 and 6.11.4
Size(GB)	2.41 GB
Reboot required	Yes
Admin UI Restart required	No

Database Info

Config DB Size	0.04 GB

Current/Previous Update Steps

Update Image Name	Not Executed	
Steps	**Status**	**Time taken(HH:MM:S**
Copy update image to subscribers	Not Executed	-
Update Publisher	Not Executed	-
Reboot + Onboot Publisher	Not Executed	-
Update selected subscribers	Not Executed	-
Reboot + Onboot selected subscribers	Not Executed	-

Publisher Details

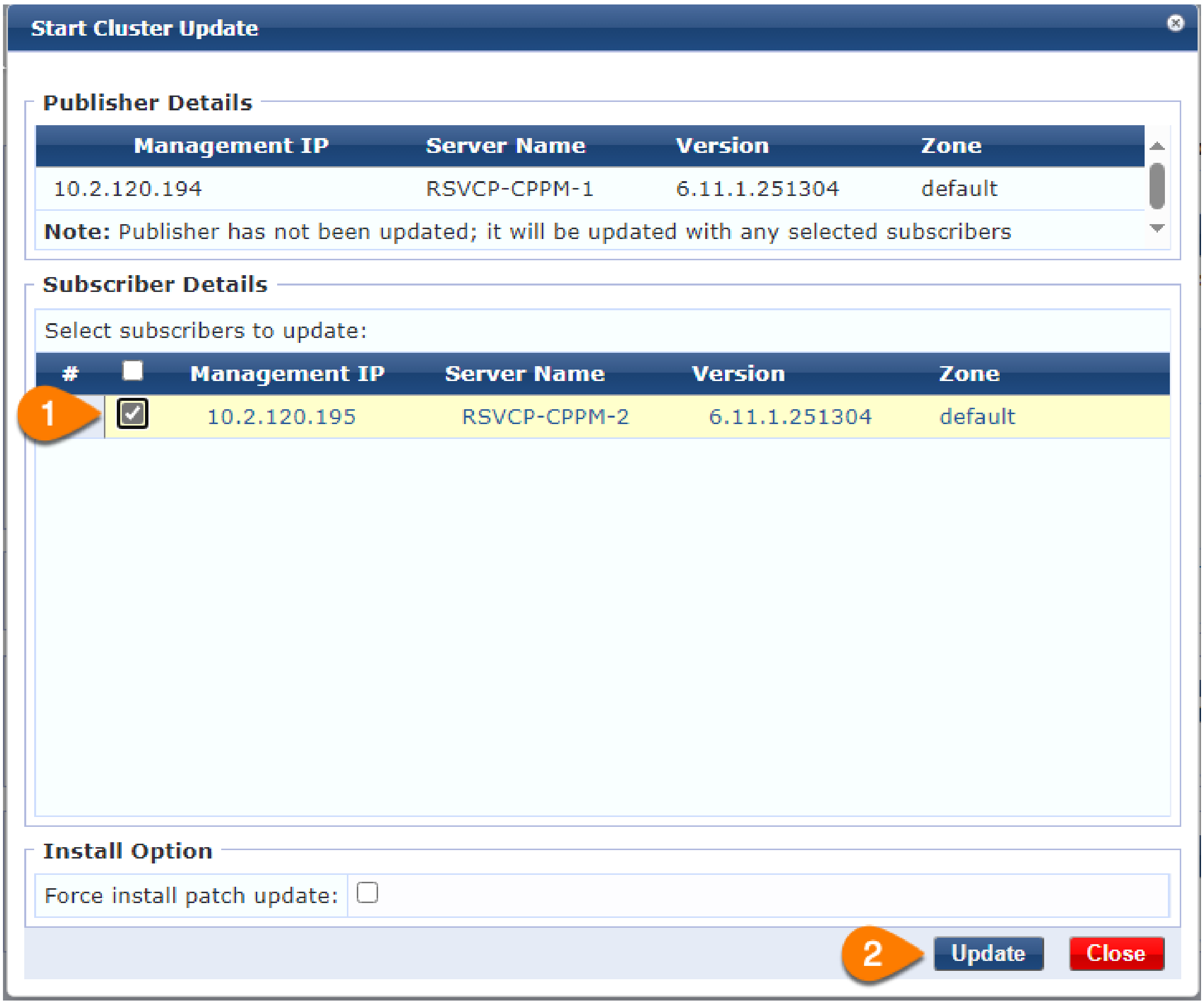
Server Name	Management IP	Version	Zone	Insight(Size)	Last Step	Update Status	View Logs
RSVCP-CPPM-1	10.2.120.194	6.11.1.251304	default	Enabled (0.01 GB)	-	-	View Logs

Subscriber Details

#	Server Name	Management IP	Version	Zone	Insight(Size)	Last Step	Update Status	View Logs

Figure 43: Cluster Update 2

Step 6 On the **Start Cluster Update** window, click the checkbox for the subscriber node, RSVCP-CPPM-2. Click the **Update** button.



Start Cluster Update

Publisher Details

Management IP	Server Name	Version	Zone
10.2.120.194	RSVCP-CPPM-1	6.11.1.251304	default

Note: Publisher has not been updated; it will be updated with any selected subscribers

Subscriber Details

Select subscribers to update:

#	□	Management IP	Server Name	Version	Zone
	☑	10.2.120.195	RSVCP-CPPM-2	6.11.1.251304	default

Install Option

Force install patch update: □

Figure 44: Start Cluster Update

Step 7 Allow time for updates to complete. For reference, OWL's two-node cluster took 90 minutes to install the Cumulative Patch on both appliances.

Step 8 Repeat steps 5 and 6 for the *Galleria Skin 3* update.

For more information about the **Cluster Update** page, see the Cluster Update and Upgrade section in the *ClearPass Policy Manager User Guide.*

NOTE:

When appliances are taken out of a cluster, for each resulting standalone appliance, you must go to **Administration > Agents and Software Updates > Software Updates** and use the **Generate Token** button to generate a new software updates token specific to that appliance.

Step 9 When all updates are complete, proceed to the next section.

Configure Certificates

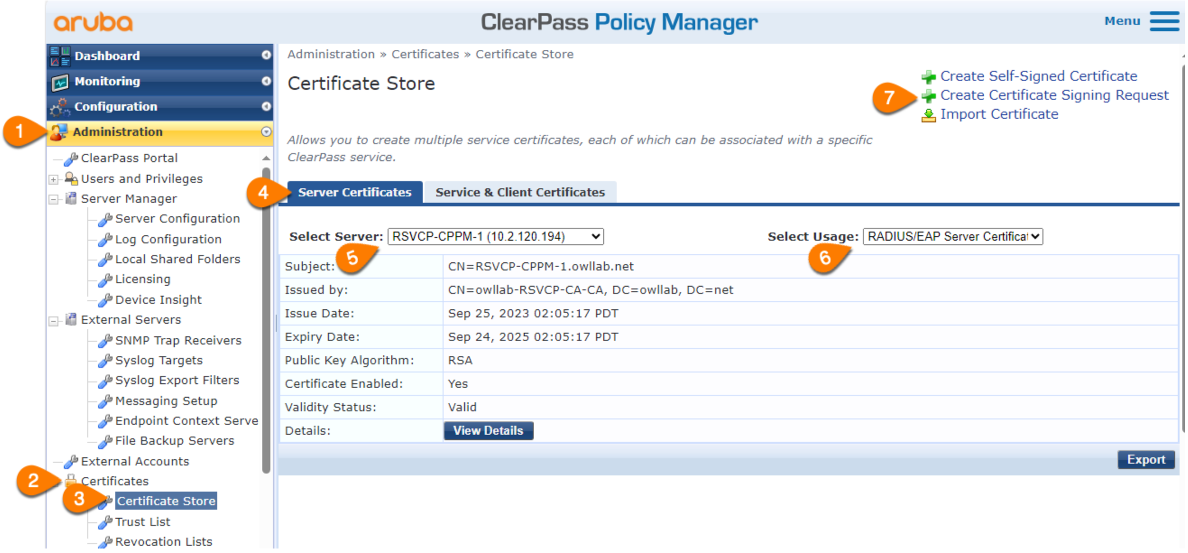
This section covers certificate-related tasks to obtain and install a signed server certificate from Active Directory for 802.1X authentication to support OWL's ClearPass deployment. Find more options and details in the Certificate Store section of the ClearPass User Guide.

Create Certificate Signing Request (CSR)

Step 1 Open a web browser and connect to the publisher node, RSVCP-CPPM-1.

Step 2 Log in using the admin credentials. - **Username:** *admin* - **Password:** *Aruba123!*

Step 3 Go to **Administration** > **Certificates** > **Certificate Store** > **Server Certificates** tab, choose *RSVCP-CPPM-1* from the **Select Server** dropdown, choose *RADIUS/EAP Server Certificate* from the **Select Usage** dropdown, then click the **Create Certificate Signing Request** link at the upper right of the window.



Certificate Store

Allows you to create multiple service certificates, each of which can be associated with a specific ClearPass service.

Select Server: RSVCP-CPPM-1 (10.2.120.194) **Select Usage:** RADIUS/EAP Server Certificat

Subject:	CN=RSVCP-CPPM-1.owllab.net
Issued by:	CN=owllab-RSVCP-CA-CA, DC=owllab, DC=net
Issue Date:	Sep 25, 2023 02:05:17 PDT
Expiry Date:	Sep 24, 2025 02:05:17 PDT
Public Key Algorithm:	RSA
Certificate Enabled:	Yes
Validity Status:	Valid
Details:	View Details

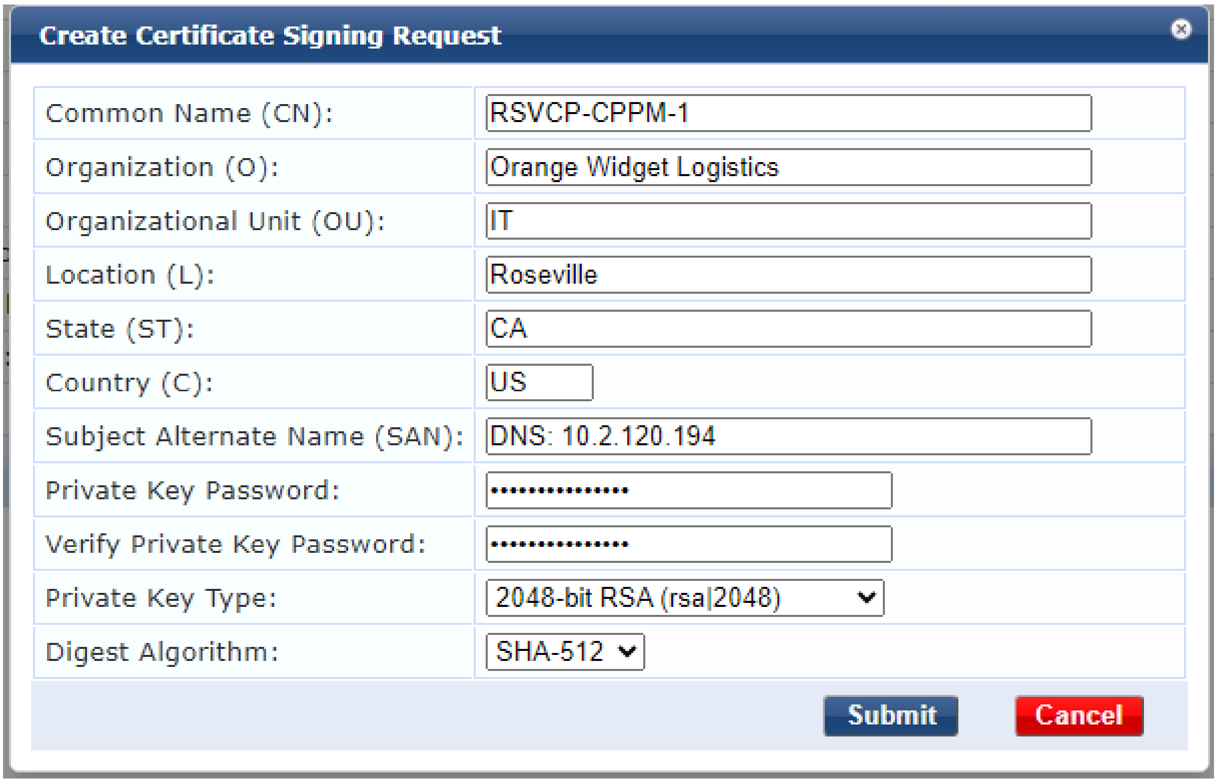
Figure 45: Generate CSR

Step 4 In the Create Certificate Signing Request window, enter the following information for RSVCP-CPPM-1, then click the **Submit** button:

- **Common Name (CN)**: *RSVCP-CPPM-1*
- ***Organization:*** Orange Widget Logistics*
- ***Organizational Unit (OU):*** IT*
- ***Location (L):*** Roseville*
- ***State (ST):*** CA*
- ***Country (C):*** US*
- ***Subject Alternate Name (SAN):*** DNS: 10.2.120.194*

- **Private Key Password:** *Aruba123!*
- **Verify Private Key Password:** *Aruba123!*
- **Private Key Type:** *2048-bit RSA*
- **Digest Algorithm:** *SHA-512*

I AM HERE!!!! **Optional*

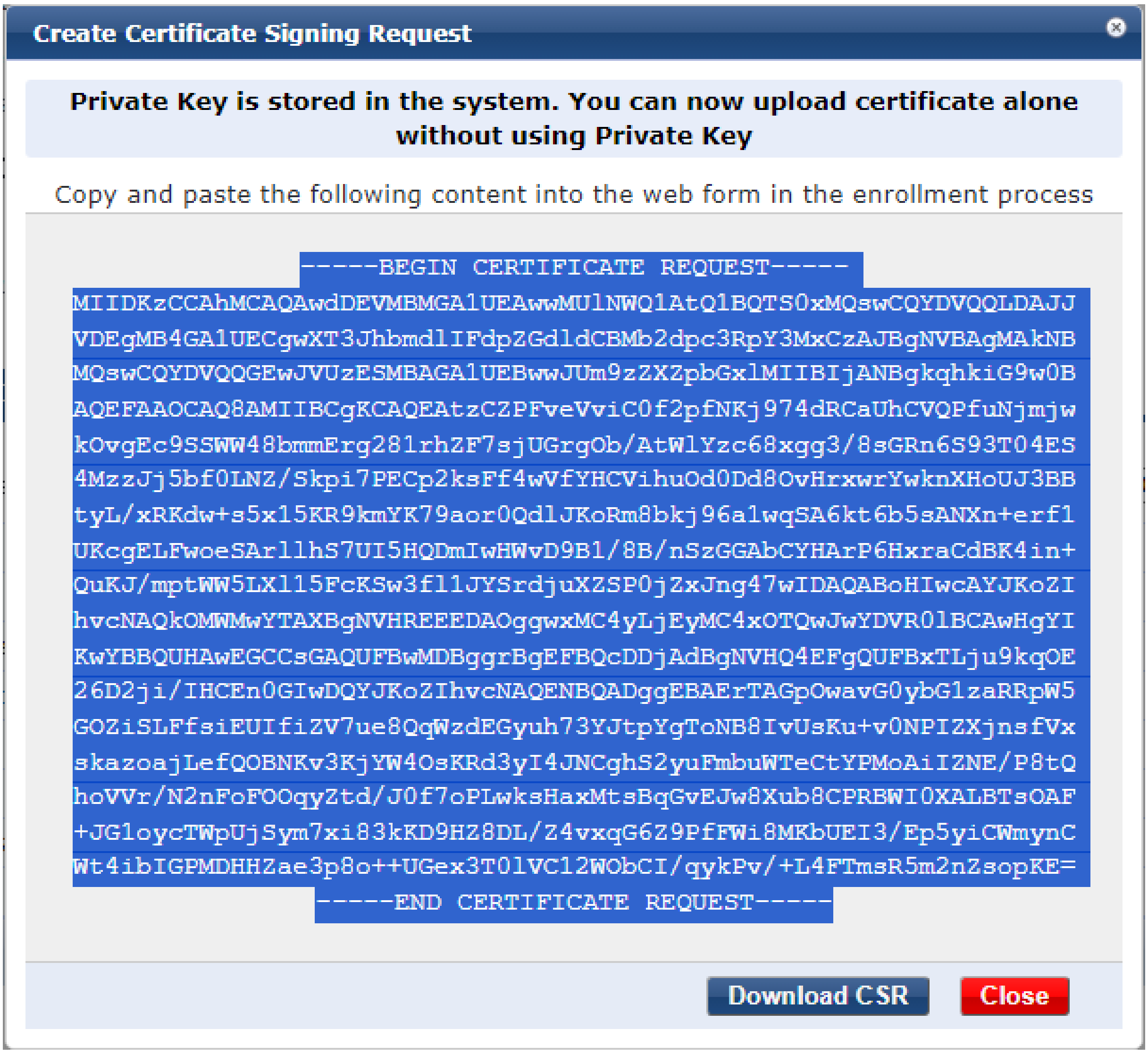


Create Certificate Signing Request

Common Name (CN):	RSVCP-CPPM-1
Organization (O):	Orange Widget Logistics
Organizational Unit (OU):	IT
Location (L):	Roseville
State (ST):	CA
Country (C):	US
Subject Alternate Name (SAN):	DNS: 10.2.120.194
Private Key Password:	••••••••••••••••
Verify Private Key Password:	••••••••••••••••
Private Key Type:	2048-bit RSA (rsa|2048)
Digest Algorithm:	SHA-512

Figure 46: Create CSR Window

Step 5 After clicking the **Submit** button, copy the CSR text that appears, paste it to a Notepad or email body, then click the **Download CSR** button.



Private Key is stored in the system. You can now upload certificate alone without using Private Key

Copy and paste the following content into the web form in the enrollment process

```
-----BEGIN CERTIFICATE REQUEST-----
MIIDKzCCAhMCAQAwdDEVMBMGA1UEAwwMU1NWQ1AtQ1BQTS0xMQswCQYDVQQLDAJJ
VDEgMB4GA1UECgwXT3JhbmdlIFdpZGdldCBMb2dpc3RpY3MxCzAJBgNVBAgMAkNB
MQswCQYDVQQGEwJVUzESMBAGA1UEBwwJUm9zZXZpbGxlMIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEAtzCZPFveVviC0f2pfNKj974dRCaUhCVQPfuNjmjw
kOvgEc9SSWW48bmmErg281rhZF7sjUGrgOb/AtWlYzc68xgg3/8sGRn6S93T04ES
4MzzJj5bf0LNZ/Skpi7PECp2ksFf4wVfYHCVihuOd0Dd8OvHrxwrYwknXHoUJ3BB
tyL/xRKdw+s5x15KR9kmYK79aor0QdlJKoRm8bkj96a1wqSA6kt6b5sANXn+erf1
UKcgELFwoeSArllhS7UI5HQDmIwHWvD9B1/8B/nSzGGAbCYHArP6HxraCdBK4in+
QuKJ/mptWW5LXl15FcKSw3fl1JYSrdjuXZSP0jZxJng47wIDAQABoHIwcAYJKoZI
hvcNAQkOMWMwYTAXBgNVHREEEDAOggwxMC4yLjEyMC4xOTQwJwYDVR0lBCAwHgYI
KwYBBQUHAwEGCCsGAQUFBwMDBggrBgEFBQcDDjAdBgNVHQ4EFgQUFBxTLju9kqOE
26D2ji/IHCEn0GIwDQYJKoZIhvcNAQENBQADggEBAErTAGpOwavG0ybG1zaRRpW5
GOZiSLFfsiEUIfiZV7ue8QqWzdEGyuh73YJtpYgToNB8IvUsKu+v0NPIZXjnsfVx
skazoajLefQOBNKv3KjYW4OsKRd3yI4JNCghS2yuFmbuWTeCtYPMoAiIZNE/P8tQ
hoVVr/N2nFoFOOqyZtd/J0f7oPLwksHaxMtsBqGvEJw8Xub8CPRBWI0XALBTsOAF
+JG1oycTWpUjSym7xi83kKD9HZ8DL/Z4vxqG6Z9PfFWi8MKbUEI3/Ep5yiCWmynC
Wt4ibIGPMDHHZae3p8o++UGex3T0lVC12WObCI/qykPv/+L4FTmsR5m2nZsopKE=
-----END CERTIFICATE REQUEST-----
```

Figure 47: CSR Key

Step 6 While still logged into the Publisher node, repeat steps 3 to 5 for RSVCP-CPPM-2's CSR, changing only the **Select Server** option in Step 3 and **CN** and **SAN** information in Step 4 with RSVCP-CPPM-2's information.

Step 7 Provide the copied text keys or the downloaded CSR files to the Windows server administrator and request the Root CA and RADIUS server certificates.

NOTE:

The Private Key is automatically stored on the current Policy Manager server. This allows for the upload (import) of the certificate without including the Private Key as part of the import process.

Step 8 When the certificates are received, proceed to the following section.

Import Certificates

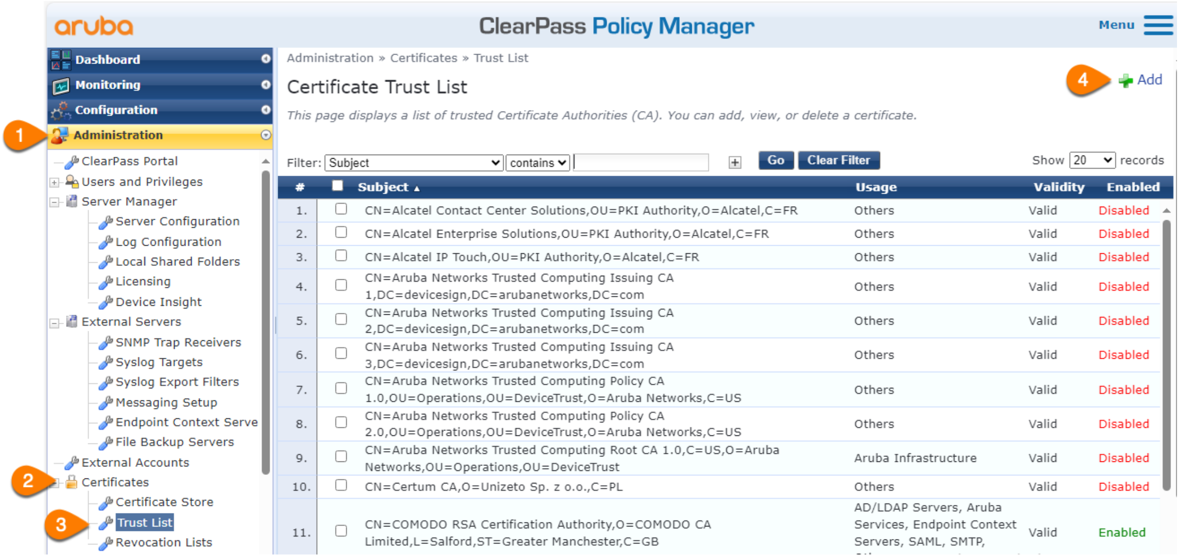
Root CA Certificate

Follow the steps below to import the server certificates for both ClearPass servers through the publisher's web UI.

Step 1 Open a web browser and connect to the publisher node, RSVCP-CPPM-1.

Step 2 Log in using the admin credentials. - **Username:** *admin* - **Password:** *Aruba123!*

Step 3 Go to **Administration** > **Certificates** > **Trust List** and click the **+Add** link at the upper right.



Administration » Certificates » Trust List

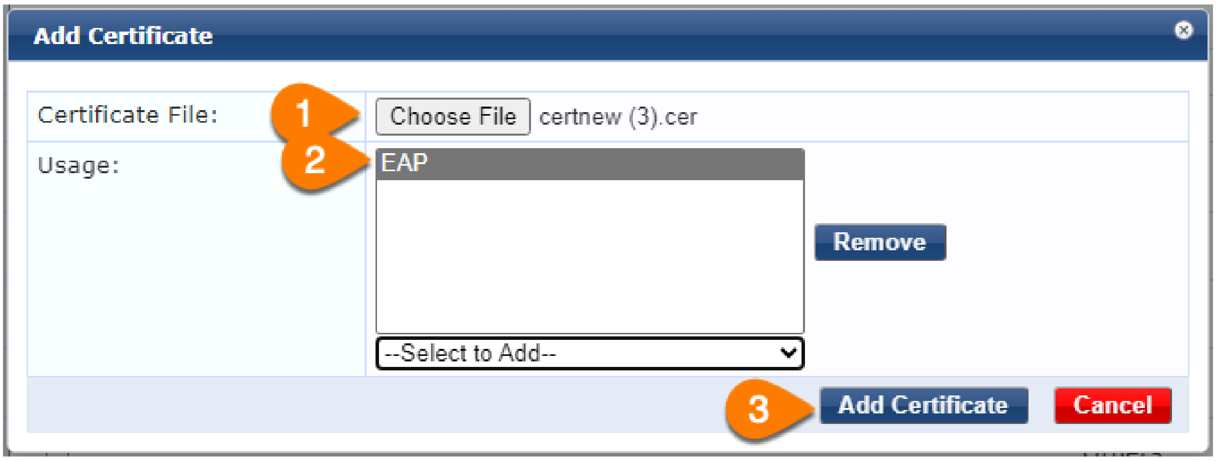
Certificate Trust List

This page displays a list of trusted Certificate Authorities (CA). You can add, view, or delete a certificate.

#	□	Subject ▴	Usage	Validity	Enabled
1.	□	CN=Alcatel Contact Center Solutions,OU=PKI Authority,O=Alcatel,C=FR	Others	Valid	Disabled
2.	□	CN=Alcatel Enterprise Solutions,OU=PKI Authority,O=Alcatel,C=FR	Others	Valid	Disabled
3.	□	CN=Alcatel IP Touch,OU=PKI Authority,O=Alcatel,C=FR	Others	Valid	Disabled
4.	□	CN=Aruba Networks Trusted Computing Issuing CA 1,DC=devicesign,DC=arubanetworks,DC=com	Others	Valid	Disabled
5.	□	CN=Aruba Networks Trusted Computing Issuing CA 2,DC=devicesign,DC=arubanetworks,DC=com	Others	Valid	Disabled
6.	□	CN=Aruba Networks Trusted Computing Issuing CA 3,DC=devicesign,DC=arubanetworks,DC=com	Others	Valid	Disabled
7.	□	CN=Aruba Networks Trusted Computing Policy CA 1.0,OU=Operations,OU=DeviceTrust,O=Aruba Networks,C=US	Others	Valid	Disabled
8.	□	CN=Aruba Networks Trusted Computing Policy CA 2.0,OU=Operations,OU=DeviceTrust,O=Aruba Networks,C=US	Others	Valid	Disabled
9.	□	CN=Aruba Networks Trusted Computing Root CA 1.0,C=US,O=Aruba Networks,OU=Operations,OU=DeviceTrust	Aruba Infrastructure	Valid	Disabled
10.	□	CN=Certum CA,O=Unizeto Sp. z o.o.,C=PL	Others	Valid	Disabled
11.	□	CN=COMODO RSA Certification Authority,O=COMODO CA Limited,L=Salford,ST=Greater Manchester,C=GB	AD/LDAP Servers, Aruba Services, Endpoint Context Servers, SAML, SMTP,	Valid	Enabled

Figure 48: Import Root CA Certificate

Step 4 In the **Add Certificate** window, select the *.cer* file for the **Root CA**, select *EAP* from the **Usage** dropdown, and click the **Add Certificate** button.



Certificate File: certnew (3).cer

Usage: EAP

Figure 49: Add Root CA Certificate

Step 5 After importing the Root CA certificate, proceed to the following section to import the RADIUS server certificates.

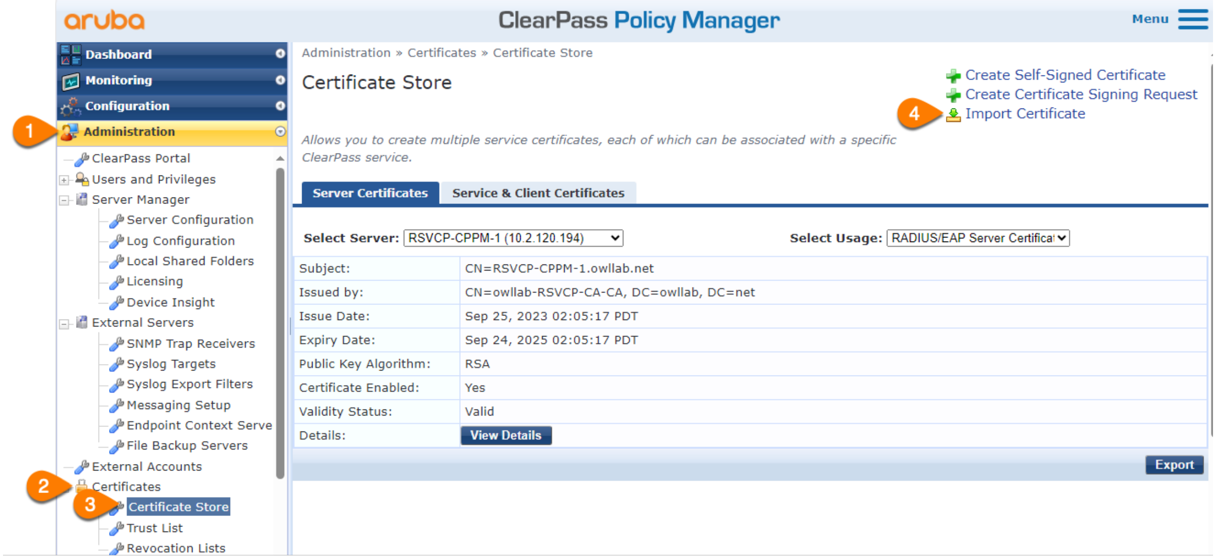
RADIUS Server Certificate

Follow the steps below to import the server certificates for both ClearPass servers through the publisher's web UI.

Step 1 Open a web browser and connect to the publisher node, RSVCP-CPPM-1.

Step 2 Log in using the admin credentials. - **Username:** *admin* - **Password:** *Aruba123!*

Step 3 Go to **Administration** > **Certificates** > **Certificate Store**, and click the **Create Certificate Signing Request** link at the upper right.



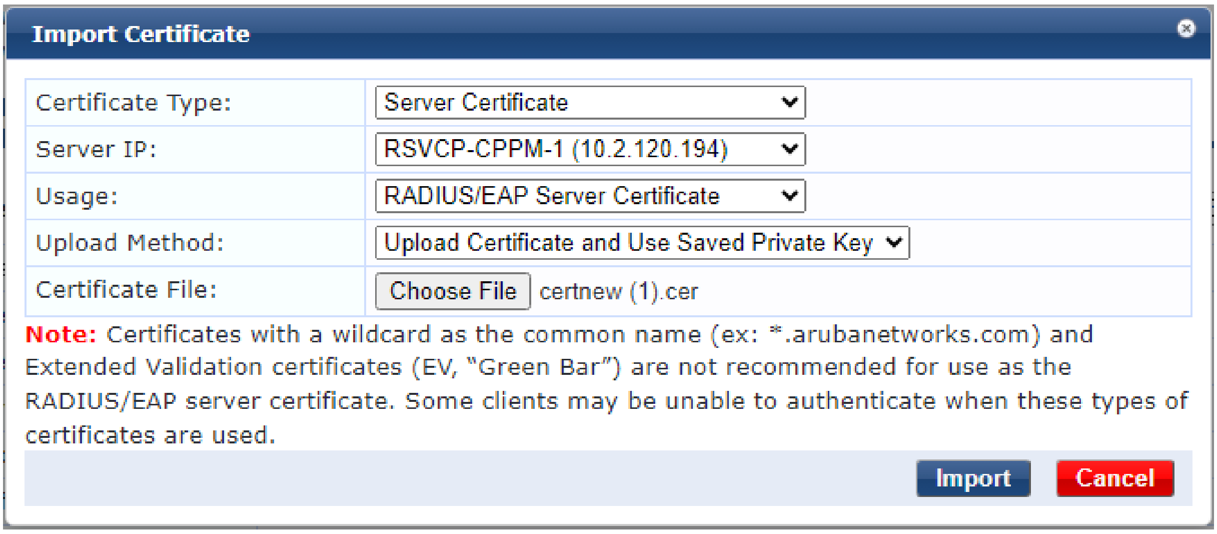
Allows you to create multiple service certificates, each of which can be associated with a specific ClearPass service.

Select Server: RSVCP-CPPM-1 (10.2.120.194)   Select Usage: RADIUS/EAP Server Certificat

Subject:	CN=RSVCP-CPPM-1.owllab.net
Issued by:	CN=owllab-RSVCP-CA-CA, DC=owllab, DC=net
Issue Date:	Sep 25, 2023 02:05:17 PDT
Expiry Date:	Sep 24, 2025 02:05:17 PDT
Public Key Algorithm:	RSA
Certificate Enabled:	Yes
Validity Status:	Valid
Details:	View Details

Figure 50: Import Server Certificate

Step 4 in the **Import Certificate** window, enter the following parameters for this deployment, then click the **Import** button. - **Certificate type:** *Server Certificate* - **Server IP:** *RSVCP-CPPM-1* - **Usage:** *RADIUS/EAP Server Certificate* - **Upload Method:** *Upload Certificate and Use Saved Private Key* - **Certificate File:** *Select the certificate file for RSVCP-CPPM-1 received from the Windows administrator*



Certificate Type:	Server Certificate
Server IP:	RSVCP-CPPM-1 (10.2.120.194)
Usage:	RADIUS/EAP Server Certificate
Upload Method:	Upload Certificate and Use Saved Private Key
Certificate File:	Choose File certnew (1).cer

Note: Certificates with a wildcard as the common name (ex: *.arubanetworks.com) and Extended Validation certificates (EV, "Green Bar") are not recommended for use as the RADIUS/EAP server certificate. Some clients may be unable to authenticate when these types of certificates are used.

Figure 51: Import Certificate File

Step 5 Repeat steps 3 and 4 and select certificate file RSVCP-CPPM-2 in step 4 to import the second certificate.

After completing these tasks, proceed to the **Configure WLAN and LAN Authentication** chapter.

Configure WLAN and LAN Authentication

This section provides steps to configure ClearPass Policy Manager (CPPM) for authentication and authorization of client devices. ClearPass includes a set of templates to help create services for common use cases. For Orange Widget Logistics (OWL), the fictional customer used in this reference design, service configuration involves templates and manual service creation.

A total of three authentication services are configured in this chapter:

- RADIUS service for 802.1X-enabled wireless SSID CorpNet
- RADIUS service for 802.1X-enabled wired switch ports
- RADIUS service for MAC authentication-enabled switch ports

Some of the services in this guide share components such as **Authentication Sources** and **Network Devices**. They are configured once before the individual service configuration instructions to reduce repetitive steps.

Configure Common Components

Authentication services in this guide share common steps. These include:

- **Authentication Sources** contain the identity store against which user devices are authenticated. In OWL's design, it includes Active Directory Domain Controllers.
- **Network Devices** must be configured with the Network Access Device (NAD) information so that ClearPass can accept authentication requests from the switches and gateways in this design.
- **Device Groups** are optional and can be used within service, role-mapping rules, or enforcement profiles. Administrators configure device groups at the global level. They can contain the members or IP addresses of a specified subnet, regular expression-based variation, or devices previously configured in the Policy Manager database. OWL's deployment involves using them in the enforcement policy, allowing ClearPass to send different responses based on request origin. For example, if the request is coming from an Aruba switch, ClearPass can return the user role. For requests coming from a non-Aruba switch, ClearPass can return the VLAN Name.

Follow the steps below to add the AD Domain Controllers, NADs, and Device Groups for OWL's ClearPass cluster.

Add AD Authentication Sources

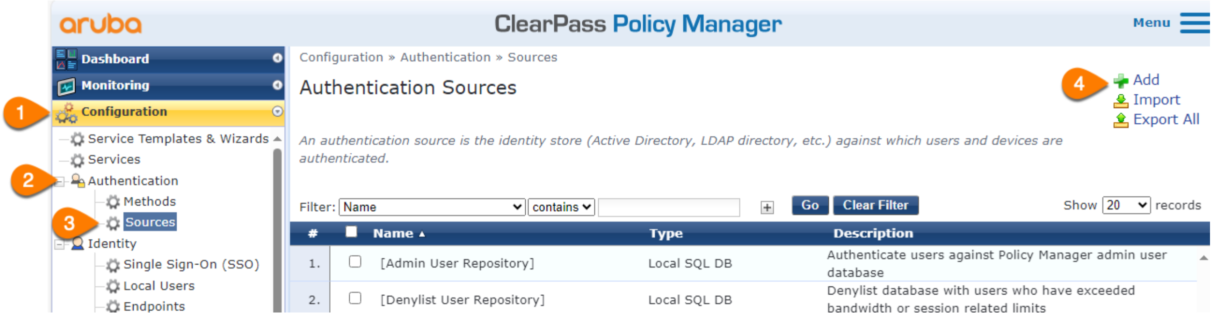
Follow the steps below to add the two Active Directory Domain Controllers to be queried by the ClearPass cluster.

Step 1 Open a web browser and connect to the publisher node, RSVCP-CPPM-1.

Step 2 Log in using the admin credentials. - **Username:** *admin* - **Password:** *Aruba123!*

Add First Domain Controller

Step 3 Go to **Configuration** > **Authentication** > **Sources** and click the **+Add** link at the upper right.



Configuration » Authentication » Sources

Authentication Sources

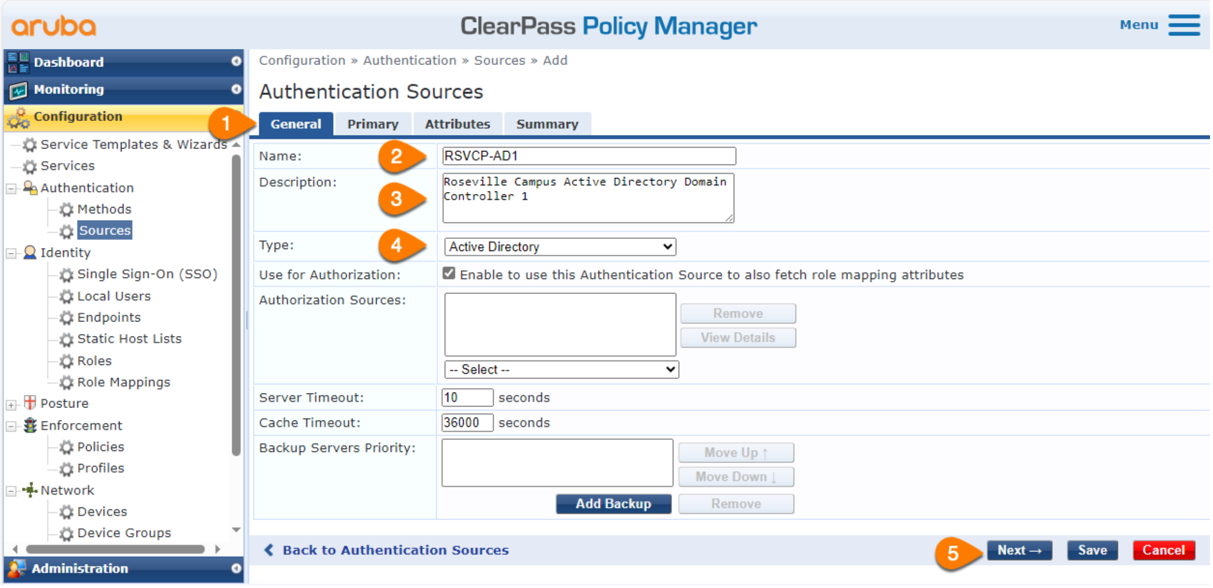
An authentication source is the identity store (Active Directory, LDAP directory, etc.) against which users and devices are authenticated.

#	Name	Type	Description
1.	[Admin User Repository]	Local SQL DB	Authenticate users against Policy Manager admin user database
2.	[Denylist User Repository]	Local SQL DB	Denylist database with users who have exceeded bandwidth or session related limits

Figure 52: Authentication Sources

Step 4 In the **General** tab, configure the following parameters, then click the **Next** button.

- **Name:** *RSVCP-AD1*
- **Description:** *Roseville Campus Active Directory Domain Controller 1*
- **Type:** *Active Directory*



Configuration » Authentication » Sources » Add

Authentication Sources

Name: RSVCP-AD1

Description: Roseville Campus Active Directory Domain Controller 1

Type: Active Directory

Use for Authorization: ☑ Enable to use this Authentication Source to also fetch role mapping attributes

Authorization Sources: -- Select --

Server Timeout: 10 seconds

Cache Timeout: 36000 seconds

Backup Servers Priority:

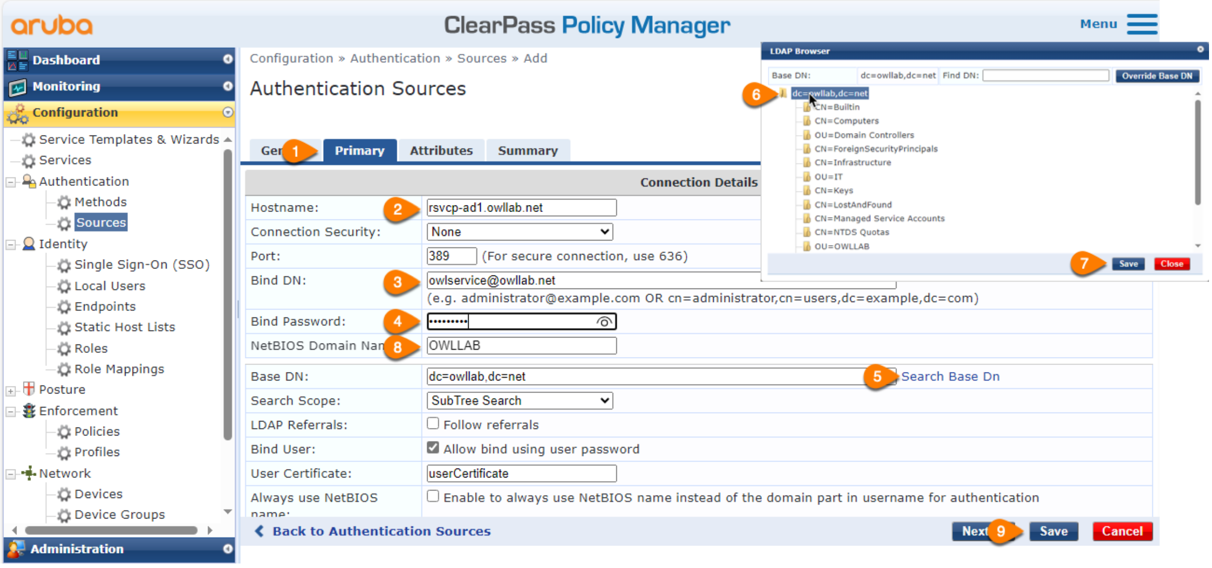
Figure 53: Add Active Directory DC 1 General Tab

Step 5 In the **Primary** Tab, configure the following parameters.

- **Hostname:** *rsvp-ad1.owllab.net*
- **Bind DN:** *owlservice@owllab .net*
- **Bind Password:** *Aruba123!*
  - **Base DN:** *(Click the **Search Base DN** link to verify that you can access the domain from the LDAP Browser window)*

  - * Click the **Save** button in the **LDAP Browser** window.

- Verify that **NetBIOS Domain Name** is populated
- Click the **Save** button



Hostname:	rsvcp-ad1.owllab.net
Connection Security:	None
Port:	389 (For secure connection, use 636)
Bind DN:	owlservice@owllab.net (e.g. administrator@example.com OR cn=administrator,cn=users,dc=example,dc=com)
Bind Password:	••••••••
NetBIOS Domain Nar	OWLLAB
Base DN:	dc=owllab,dc=net Search Base Dn
Search Scope:	SubTree Search
LDAP Referrals:	□ Follow referrals
Bind User:	☑ Allow bind using user password
User Certificate:	userCertificate
Always use NetBIOS name:	□ Enable to always use NetBIOS name instead of the domain part in username for authentication

LDAP Browser

Base DN: dc=owllab,dc=net Find DN:

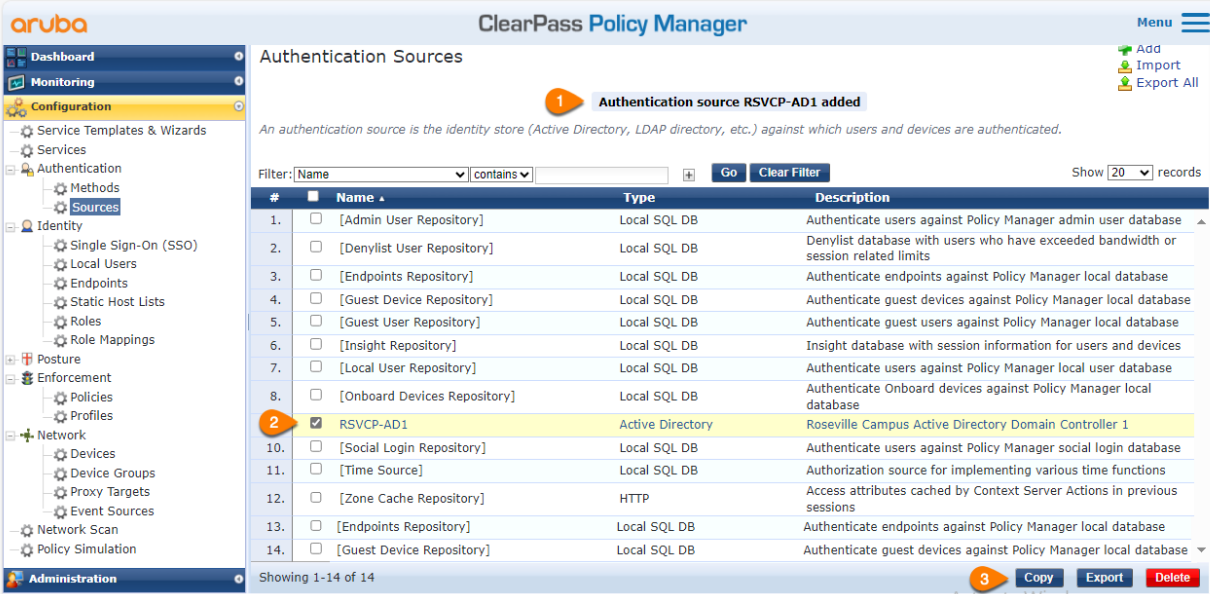
- dc=owllab,dc=net
  - CN=Builtin
  - CN=Computers
  - OU=Domain Controllers
  - CN=ForeignSecurityPrincipals
  - CN=Infrastructure
  - OU=IT
  - CN=Keys
  - CN=LostAndFound
  - CN=Managed Service Accounts
  - CN=NTDS Quotas
  - OU=OWLLAB

Figure 54: Add Active Directory DC 1 Primary Tab

Add Second Domain Controller

Continue from the steps above to configure the second AD Domain Controller using the **Copy** function.

Step 6 Return to the **Sources** window, click the checkbox next to the new entry for *RSVCP-AD1*, then click the **Copy** button at the lower right.



Authentication Sources

Authentication source RSVCP-AD1 added

An authentication source is the identity store (Active Directory, LDAP directory, etc.) against which users and devices are authenticated.

Filter: Name contains Show 20 records

#	□	Name ▴	Type	Description
1.	□	[Admin User Repository]	Local SQL DB	Authenticate users against Policy Manager admin user database
2.	□	[Denylist User Repository]	Local SQL DB	Denylist database with users who have exceeded bandwidth or session related limits
3.	□	[Endpoints Repository]	Local SQL DB	Authenticate endpoints against Policy Manager local database
4.	□	[Guest Device Repository]	Local SQL DB	Authenticate guest devices against Policy Manager local database
5.	□	[Guest User Repository]	Local SQL DB	Authenticate guest users against Policy Manager local database
6.	□	[Insight Repository]	Local SQL DB	Insight database with session information for users and devices
7.	□	[Local User Repository]	Local SQL DB	Authenticate users against Policy Manager local user database
8.	□	[Onboard Devices Repository]	Local SQL DB	Authenticate Onboard devices against Policy Manager local database
	☑	RSVCP-AD1	Active Directory	Roseville Campus Active Directory Domain Controller 1
10.	□	[Social Login Repository]	Local SQL DB	Authenticate users against Policy Manager social login database
11.	□	[Time Source]	Local SQL DB	Authorization source for implementing various time functions
12.	□	[Zone Cache Repository]	HTTP	Access attributes cached by Context Server Actions in previous sessions
13.	□	[Endpoints Repository]	Local SQL DB	Authenticate endpoints against Policy Manager local database
14.	□	[Guest Device Repository]	Local SQL DB	Authenticate guest devices against Policy Manager local database

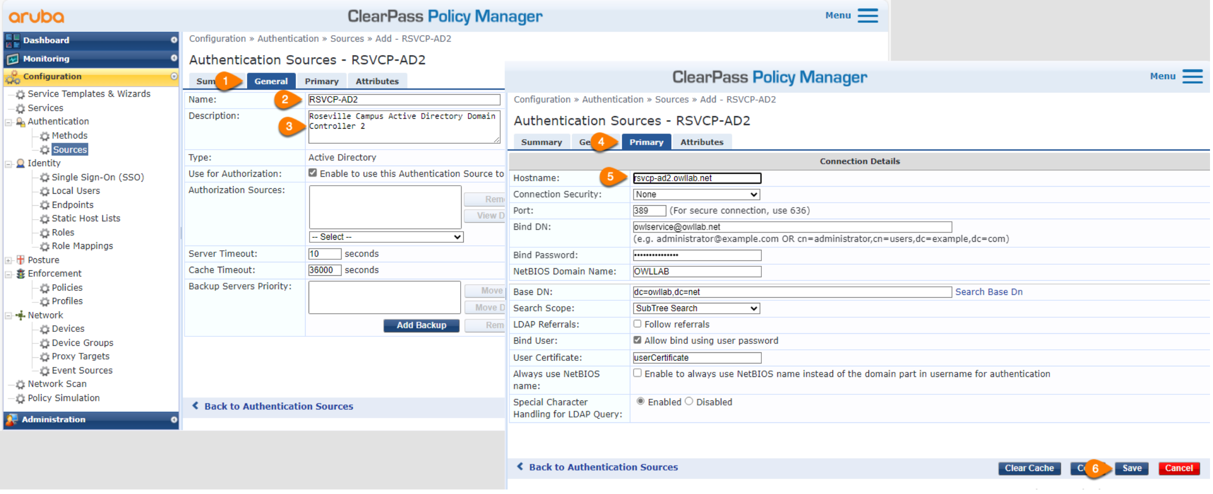
Showing 1-14 of 14

Figure 55: Create Copy of AD1

Step 7 Click the newly created *Copy_of_RSVCP-AD1* in the **Sources** list.

Step 8 When the details page appears, update the following, then click the **Save** button. - In the **General** tab: - **Name:** *RSVCP-AD2* - **Description:** *Roseville Campus Active Directory Domain Controller 2*

- In the **Primary** tab:
  - **Hostname:** *rsvcp-ad2.owllab.net*



Configuration » Authentication » Sources » Add - RSVCP-AD2

Authentication Sources - RSVCP-AD2

Name:	RSVCP-AD2
Description:	Roseville Campus Active Directory Domain Controller 2
Type:	Active Directory
Use for Authorization:	☑ Enable to use this Authentication Source to
Authorization Sources:	-- Select --
Server Timeout:	10 seconds
Cache Timeout:	36000 seconds
Backup Servers Priority:	

Configuration » Authentication » Sources » Add - RSVCP-AD2

Authentication Sources - RSVCP-AD2

Connection Details

Hostname:	rsvcp-ad2.owllab.net
Connection Security:	None
Port:	389 (For secure connection, use 636)
Bind DN:	owlservice@owllab.net (e.g. administrator@example.com OR cn=administrator,cn=users,dc=example,dc=com)
Bind Password:	•••••••••••••••
NetBIOS Domain Name:	OWLLAB
Base DN:	dc=owllab,dc=net
Search Scope:	SubTree Search
LDAP Referrals:	☐ Follow referrals
Bind User:	☑ Allow bind using user password
User Certificate:	userCertificate
Always use NetBIOS name:	☐ Enable to always use NetBIOS name instead of the domain part in username for authentication
Special Character Handling for LDAP Query:	● Enabled ○ Disabled

Figure 56: Edit Duplicate of AD1

Step 9 With both AD DCs added, proceed to the next section.

Add Network Devices (Authenticators)

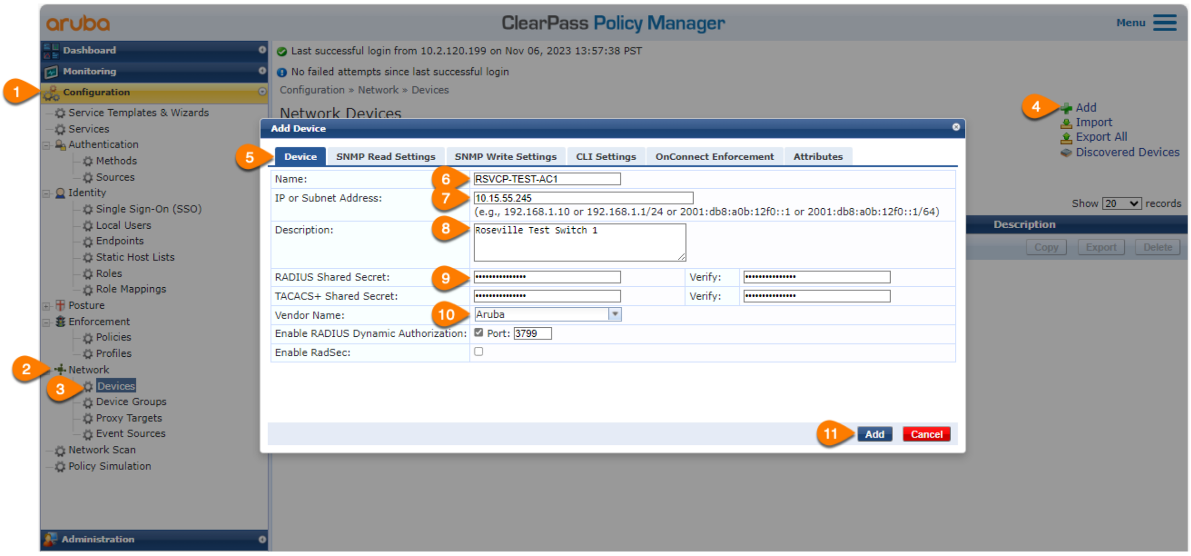
Network Devices are configured so ClearPass can accept authentication requests from switches and gateways in this design.

Follow the steps below to add the gateways and switches using the information from the **Network Devices (Authenticators)** section on the **ClearPass Preparation** page.

Step 1 Open a web browser and connect to the publisher node, RSVCP-CPPM-1.

Step 2 Log in using the admin credentials. - **Username:** *admin* - **Password:** *Aruba123!*

Step 3 Go to **Configuration** > **Network** > **Devices**, click the **Add** link at the upper right. Add the first device from the **Network Devices** table above.



Last successful login from 10.2.120.199 on Nov 06, 2023 13:57:38 PST

No failed attempts since last successful login

Configuration » Network » Devices

Network Devices

Add Device

Device | SNMP Read Settings | SNMP Write Settings | CLI Settings | OnConnect Enforcement | Attributes

Name:	RSVCP-TEST-AC1		
IP or Subnet Address:	10.15.55.245 (e.g., 192.168.1.10 or 192.168.1.1/24 or 2001:db8:a0b:12f0::1 or 2001:db8:a0b:12f0::1/64)		
Description:	Roseville Test Switch 1		
RADIUS Shared Secret:	•••••••••••••••	Verify:	•••••••••••••••
TACACS+ Shared Secret:	•••••••••••••••	Verify:	•••••••••••••••
Vendor Name:	Aruba		
Enable RADIUS Dynamic Authorization:	☑ Port: 3799		
Enable RadSec:	☐		

Add Cancel

Figure 57: Add Network Device 1

Step 4 After adding the first network device, repeat the step or use the **Copy** function to add the remaining network devices listed in the previous chapter, then proceed to the next section.

Add Network Device Groups

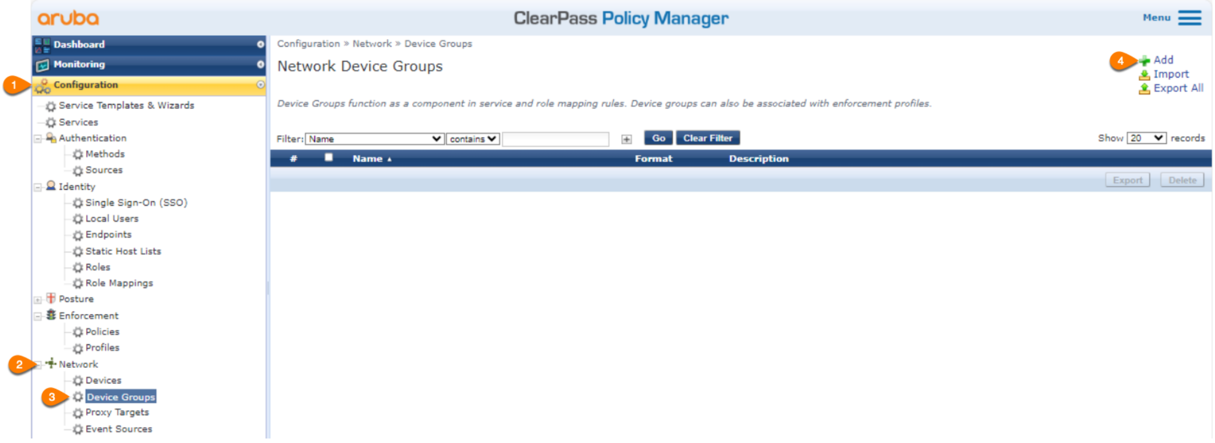
ClearPass can group devices into **Device Groups**, which are optional components in service and role-mapping rules. Administrators configure device groups at the global level. They can contain the members or IP addresses of a specified subnet, regular expression-based variation, or devices previously configured in the Policy Manager database. OWL's new cluster uses the third option with previously configured devices in a list format.

Follow the steps below to create the device groups.

Step 1 Open a web browser and connect to the publisher node, RSVCP-CPPM-1.

Step 2 Log in using the admin credentials. - **Username:** *admin* - **Password:** *Aruba123!*

Step 3 Go to **Configuration** > **Network** > **Device Groups** and click the **Add** link at the upper right.



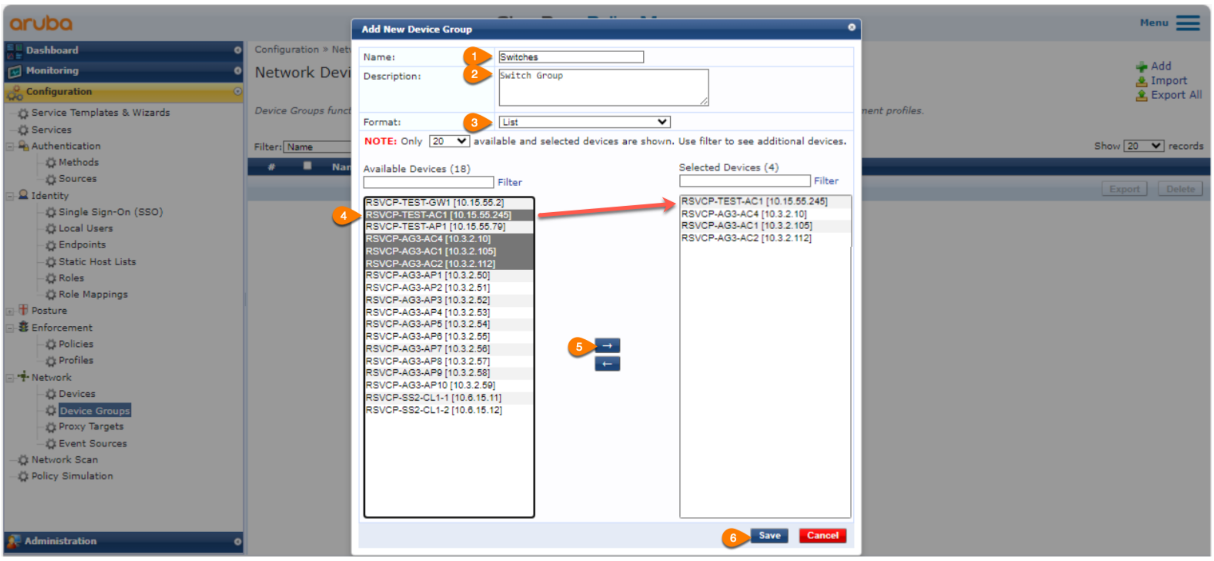
Device Groups function as a component in service and role mapping rules. Device groups can also be associated with enforcement profiles.

Figure 58: Add Network Device Group

Step 4 In the **Add New Device Group** window, configure the following parameters to add the switches to the list, then click the **Save** button. - **Name:** *Switches* - **Description:** *Switch Device Group* - **Format:** *List* - **Selected Devices:** *RSVCP-TEST-AC1, AG3-AC1, AG3-AC2, and AG3-AC4*

NOTE:

Press the SHIFT or CTRL key while clicking the list to select multiple devices and move them simultaneously.



Add New Device Group

Name: Switches

Description: Switch Group

Format: List

NOTE: Only 20 available and selected devices are shown. Use filter to see additional devices.

Available Devices (18)

RSVCP-TEST-GW1 [10.15.55.2]
RSVCP-TEST-AC1 [10.15.55.245]
RSVCP-TEST-AP1 [10.15.55.79]
RSVCP-AG3-AC4 [10.3.2.10]
RSVCP-AG3-AC1 [10.3.2.105]
RSVCP-AG3-AC2 [10.3.2.112]
RSVCP-AG3-AP1 [10.3.2.50]
RSVCP-AG3-AP2 [10.3.2.51]
RSVCP-AG3-AP3 [10.3.2.52]
RSVCP-AG3-AP4 [10.3.2.53]
RSVCP-AG3-AP5 [10.3.2.54]
RSVCP-AG3-AP6 [10.3.2.55]
RSVCP-AG3-AP7 [10.3.2.56]
RSVCP-AG3-AP8 [10.3.2.57]
RSVCP-AG3-AP9 [10.3.2.58]
RSVCP-AG3-AP10 [10.3.2.59]
RSVCP-SS2-CL1-1 [10.6.15.11]
RSVCP-SS2-CL1-2 [10.6.15.12]

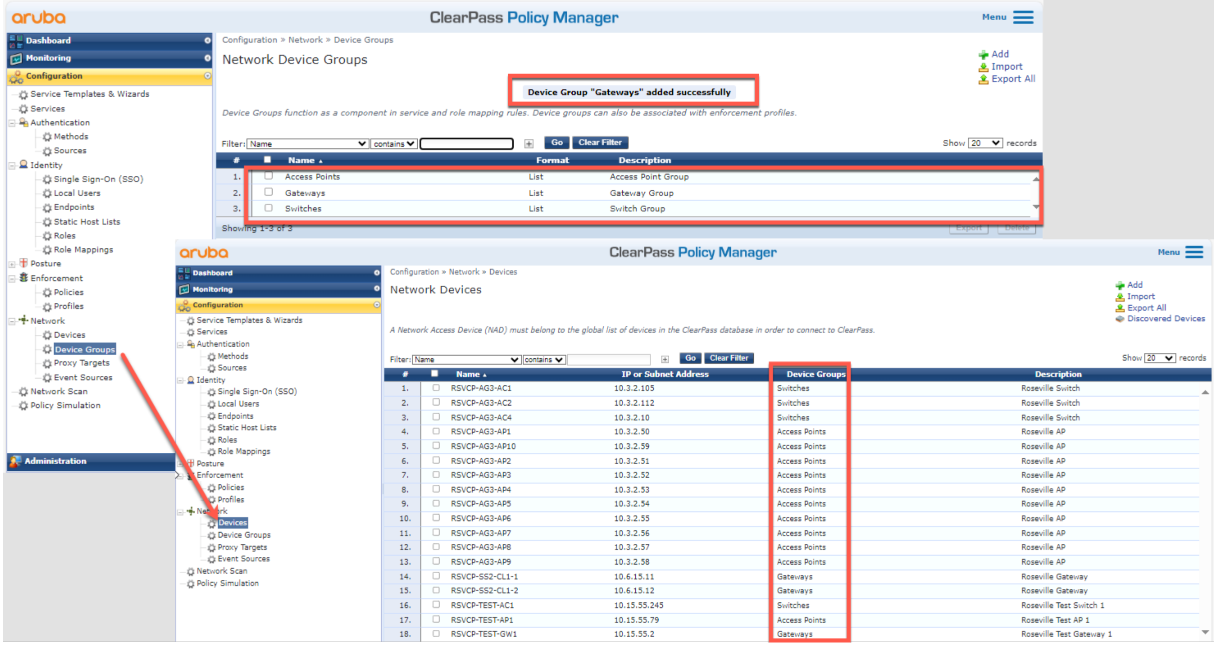
Selected Devices (4)

RSVCP-TEST-AC1 [10.15.55.245]
RSVCP-AG3-AC4 [10.3.2.10]
RSVCP-AG3-AC1 [10.3.2.105]
RSVCP-AG3-AC2 [10.3.2.112]

Figure 59: Add New Device Group Popup

Step 5 Repeat steps 3 and 4 to add the Gateway group.

Step 6 When complete, the groups are listed on the **Network Device Groups** page. They also appear in the **Device Groups** column on the **Network Devices** page, as shown below.



Configuration » Network » Device Groups

Network Device Groups

Device Group "Gateways" added successfully

Device Groups function as a component in service and role mapping rules. Device groups can also be associated with enforcement profiles.

Filter: Name contains — Show 20 records

#		Name	Format	Description
1.	□	Access Points	List	Access Point Group
2.	□	Gateways	List	Gateway Group
3.	□	Switches	List	Switch Group

Showing 1-3 of 3

Configuration » Network » Devices

Network Devices

A Network Access Device (NAD) must belong to the global list of devices in the ClearPass database in order to connect to ClearPass.

Filter: Name contains — Show 20 records

#		Name	IP or Subnet Address	Device Groups	Description
1.	□	RSVCP-AG3-AC1	10.3.2.105	Switches	Roseville Switch
2.	□	RSVCP-AG3-AC2	10.3.2.112	Switches	Roseville Switch
3.	□	RSVCP-AG3-AC4	10.3.2.10	Switches	Roseville Switch
4.	□	RSVCP-AG3-AP1	10.3.2.50	Access Points	Roseville AP
5.	□	RSVCP-AG3-AP10	10.3.2.59	Access Points	Roseville AP
6.	□	RSVCP-AG3-AP2	10.3.2.51	Access Points	Roseville AP
7.	□	RSVCP-AG3-AP3	10.3.2.52	Access Points	Roseville AP
8.	□	RSVCP-AG3-AP4	10.3.2.53	Access Points	Roseville AP
9.	□	RSVCP-AG3-AP5	10.3.2.54	Access Points	Roseville AP
10.	□	RSVCP-AG3-AP6	10.3.2.55	Access Points	Roseville AP
11.	□	RSVCP-AG3-AP7	10.3.2.56	Access Points	Roseville AP
12.	□	RSVCP-AG3-AP8	10.3.2.57	Access Points	Roseville AP
13.	□	RSVCP-AG3-AP9	10.3.2.58	Access Points	Roseville AP
14.	□	RSVCP-SS2-CL1-1	10.6.15.11	Gateways	Roseville Gateway
15.	□	RSVCP-SS2-CL1-2	10.6.15.12	Gateways	Roseville Gateway
16.	□	RSVCP-TEST-AC1	10.15.55.245	Switches	Roseville Test Switch 1
17.	□	RSVCP-TEST-AP1	10.15.55.79	Access Points	Roseville Test AP 1
18.	□	RSVCP-TEST-GW1	10.15.55.2	Gateways	Roseville Test Gateway 1

Figure 60: Added Device Groups

NOTE:

The Access Points and an Access Points Group in the image above were created for future use of Bridge mode and Mixed mode SSIDs but do not need to be added in this first phase of OWL's deployment, which is only using Tunnel Mode.

Step 7 Proceed to the next section.

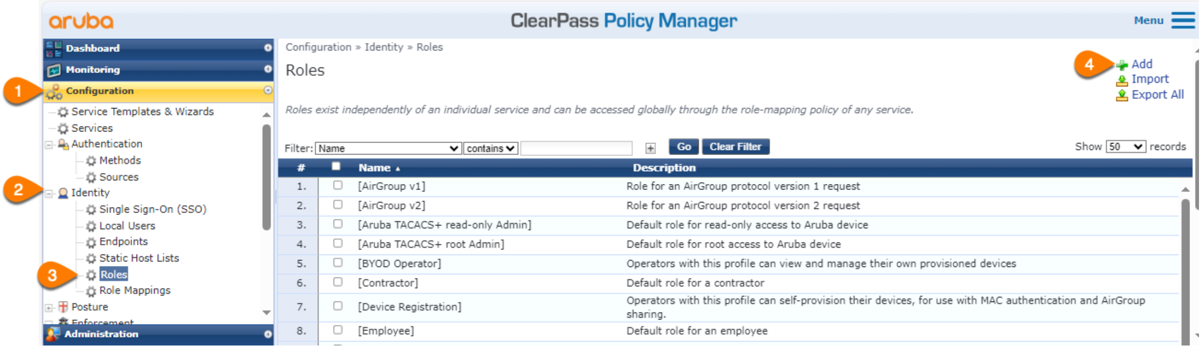
Configure Wireless 802.1X Authentication

The first service to configure is for **CorpNet** WLAN, that services trusted OWL-owned assets. It authenticates clients against Active Directory (AD) using the EAP-TLS authentication method and use AD user group memberships to grant different authorization levels.

Note that the workflow for this setup requires creating Role Mapping and Enforcement Policies before adding the actual service.

Configure ClearPass Roles for Role Mapping Policy

Step 1 Go to **Configuration** > **Identity** > **Roles** and click the **Add** link at the upper right.



Configuration » Identity » Roles

Roles

Roles exist independently of an individual service and can be accessed globally through the role-mapping policy of any service.

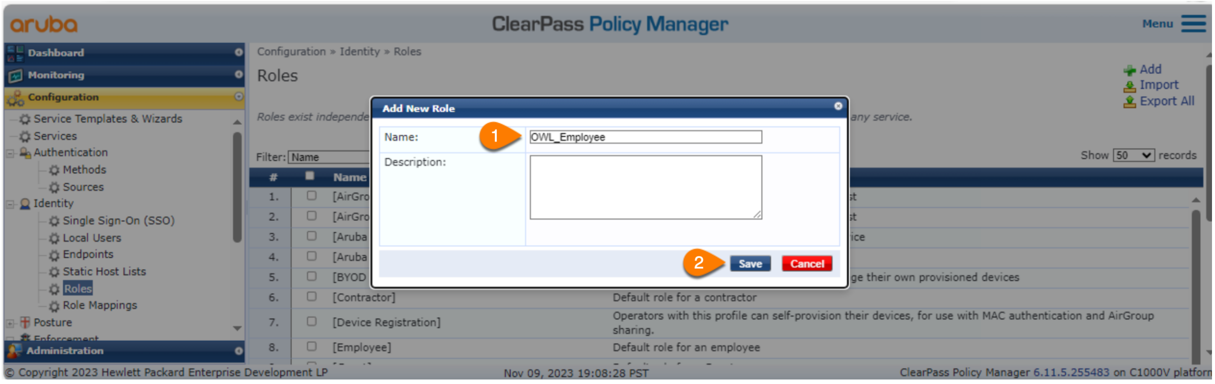
Filter: Name contains

Show 50 records

#		Name ▴	Description
1.	□	[AirGroup v1]	Role for an AirGroup protocol version 1 request
2.	□	[AirGroup v2]	Role for an AirGroup protocol version 2 request
3.	□	[Aruba TACACS+ read-only Admin]	Default role for read-only access to Aruba device
4.	□	[Aruba TACACS+ root Admin]	Default role for root access to Aruba device
5.	□	[BYOD Operator]	Operators with this profile can view and manage their own provisioned devices
6.	□	[Contractor]	Default role for a contractor
7.	□	[Device Registration]	Operators with this profile can self-provision their devices, for use with MAC authentication and AirGroup sharing.
8.	□	[Employee]	Default role for an employee

Figure 61: Add Roles

Step 2 In the **Add New Role** window, add the first role by matching the following info, then click the **Save** button. - **Name:** *OWL_Employee*



Add New Role

Name: OWL_Employee

Description:

© Copyright 2023 Hewlett Packard Enterprise Development LP Nov 09, 2023 19:08:28 PST ClearPass Policy Manager 6.11.5.255483 on C1000V platform

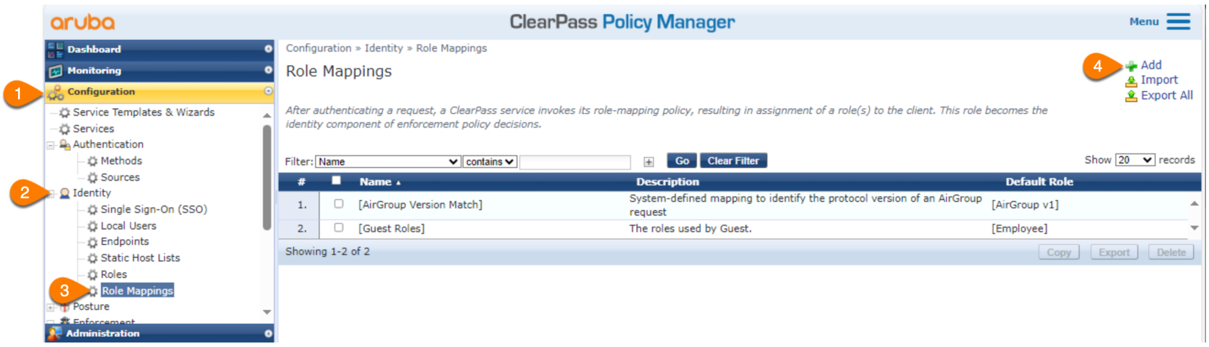
Figure 62: Create Role Mapping Role

Step 3 Repeat the step to add the following new roles: - OWL_IT-Support - OWL_IT-Admin - OWL_Infra-Device - OWL_LnD-Staff - OWL_LnD-Student - OWL_VoIP - OWL_Printer - OWL_Guest - OWL_Contractor - OWL_Security - OWL_IoT-Limited

Step 4 When complete, continue to the next section.

Configure Role Mapping Policy

Step 1 Go to **Configuration** > **Identity** > **Role Mappings** and click the **Add** link at the upper right.



Configuration » Identity » Role Mappings

Role Mappings

After authenticating a request, a ClearPass service invokes its role-mapping policy, resulting in assignment of a role(s) to the client. This role becomes the identity component of enforcement policy decisions.

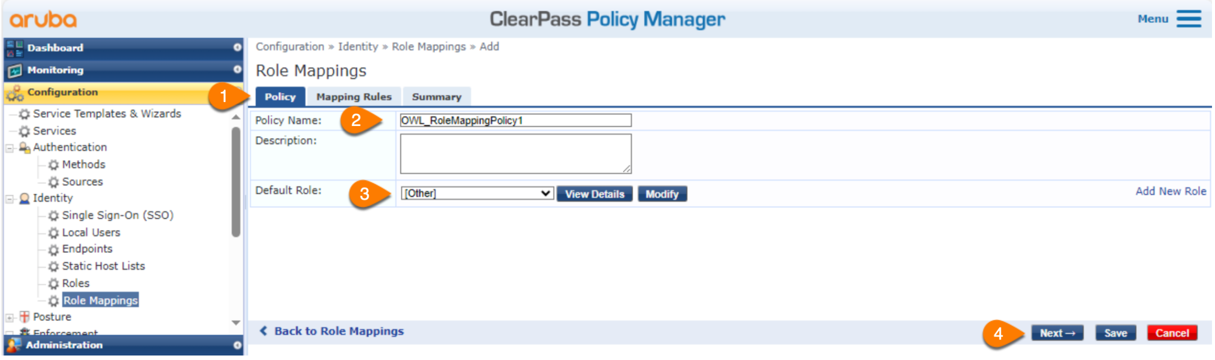
Filter: Name contains | Show 20 records

#	Name	Description	Default Role
1.	[AirGroup Version Match]	System-defined mapping to identify the protocol version of an AirGroup request	[AirGroup v1]
2.	[Guest Roles]	The roles used by Guest.	[Employee]

Showing 1-2 of 2

Figure 63: Add Role Mapping Policy

Step 2 In the **Role Mappings** window, on the **Policy** tab, configure the following, then click the **Next** button. - **Policy Name:** *OWL_RoleMappingPolicy1* - **Default Role:** *[Other]*



Configuration » Identity » Role Mappings » Add

Role Mappings

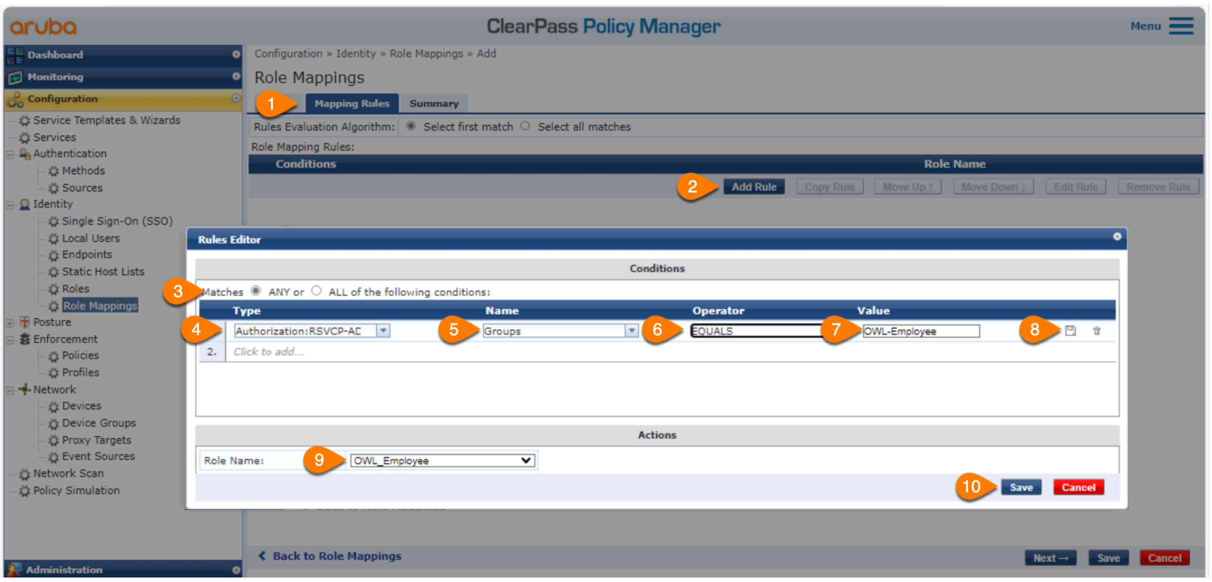
Policy Name: OWL_RoleMappingPolicy1

Description:

Default Role: [Other]

Figure 64: Role Mapping Policy Tab

Step 3 On the **Mapping Rules** tab, click the **Add Rule** button and configure the following on the **Rules Editor** window, then click the **Save** button. - **Matches:** *ANY* - **Type:** *Authorization:RSVCP-AD1* - **Name:** *Groups* - **Operator:** *EQUALS* - **Value:** *OWL-Employee* - **Role Name:** *OWL_Employee*



Configuration » Identity » Role Mappings » Add

Role Mappings

Rules Evaluation Algorithm: ● Select first match ○ Select all matches

Role Mapping Rules:

Conditions	Role Name

Rules Editor

Conditions

Matches ● ANY or ○ ALL of the following conditions:

	Type	Name	Operator	Value
1.	Authorization:RSVCP-AC	Groups	EQUALS	OWL-Employee
2.	Click to add...			

Actions

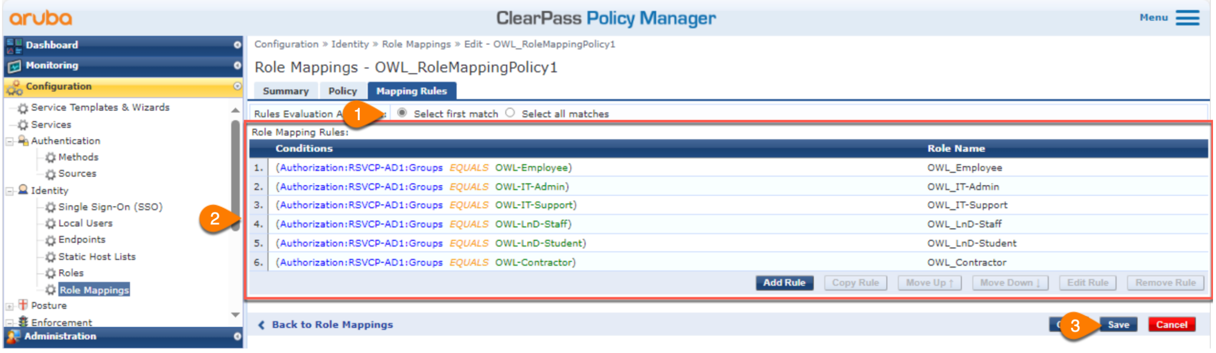
Role Name: OWL_Employee

Figure 65: Role Mapping Rules

Step 4 Repeat the step above until the following mapping rules are entered.

Type	Name	Operator	Value	Role Name
Authorization:RSVCP-AD1	Groups	EQUALS	OWL-Employee	OWL_Employee
Authorization:RSVCP-AD1	Groups	EQUALS	OWL-IT-Admin	OWL_IT-Admin
Authorization:RSVCP-AD1	Groups	EQUALS	OWL-IT-Support	OWL_IT-Support
Authorization:RSVCP-AD1	Groups	EQUALS	OWL-LnD-Staff	OWL_LnD-Staff
Authorization:RSVCP-AD1	Groups	EQUALS	OWL-LnD-Student	OWL_LnD-Student
Authorization:RSVCP-AD1	Groups	EQUALS	OWL-Contractor	OWL_Contractor

Step 5 Verify that the **Mapping Rules** look like the screenshot below, then click the **Save** button.



Configuration » Identity » Role Mappings » Edit - OWL_RoleMappingPolicy1

Role Mappings - OWL_RoleMappingPolicy1

Rules Evaluation A[illegible]: ● Select first match ○ Select all matches

Role Mapping Rules:

	Conditions	Role Name
1.	(Authorization:RSVCP-AD1:Groups EQUALS OWL-Employee)	OWL_Employee
2.	(Authorization:RSVCP-AD1:Groups EQUALS OWL-IT-Admin)	OWL_IT-Admin
3.	(Authorization:RSVCP-AD1:Groups EQUALS OWL-IT-Support)	OWL_IT-Support
4.	(Authorization:RSVCP-AD1:Groups EQUALS OWL-LnD-Staff)	OWL_LnD-Staff
5.	(Authorization:RSVCP-AD1:Groups EQUALS OWL-LnD-Student)	OWL_LnD-Student
6.	(Authorization:RSVCP-AD1:Groups EQUALS OWL-Contractor)	OWL_Contractor

Figure 66: Role Mapping Rules 2

Step 6 Proceed to the next section.

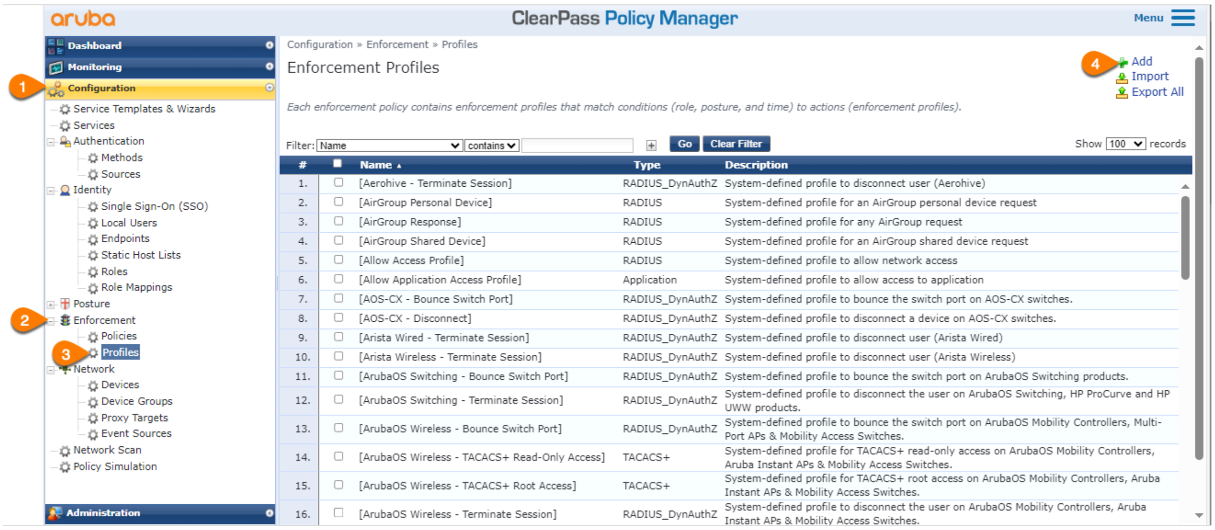
Configure Enforcement Profiles for Enforcement Policy

Follow the steps below to configure the Enforcement Profiles documented in the **User Role/Client Role Information** table in the **Preparing for ClearPass Deployment** chapter.

Step 1 Open a web browser and connect to the publisher node, RSVCP-CPPM-1.

Step 2 Log in using the admin credentials. - **Username:** *admin* - **Password:** *Aruba123!*

Step 3 Go to **Configuration** > **Enforcement** > **Profiles** and click the **Add** link at the upper right.



Enforcement Profiles

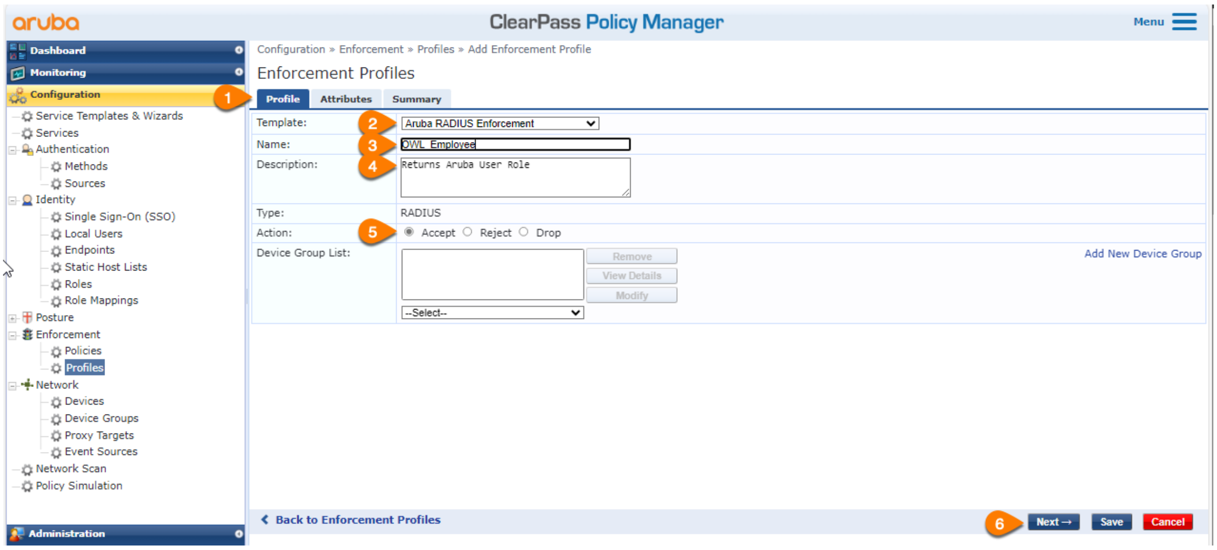
Each enforcement policy contains enforcement profiles that match conditions (role, posture, and time) to actions (enforcement profiles).

Filter: Name contains
Show 100 records

#	□	Name ▲	Type	Description
1.	□	[Aerohive - Terminate Session]	RADIUS_DynAuthZ	System-defined profile to disconnect user (Aerohive)
2.	□	[AirGroup Personal Device]	RADIUS	System-defined profile for an AirGroup personal device request
3.	□	[AirGroup Response]	RADIUS	System-defined profile for any AirGroup request
4.	□	[AirGroup Shared Device]	RADIUS	System-defined profile for an AirGroup shared device request
5.	□	[Allow Access Profile]	RADIUS	System-defined profile to allow network access
6.	□	[Allow Application Access Profile]	Application	System-defined profile to allow access to application
7.	□	[AOS-CX - Bounce Switch Port]	RADIUS_DynAuthZ	System-defined profile to bounce the switch port on AOS-CX switches.
8.	□	[AOS-CX - Disconnect]	RADIUS_DynAuthZ	System-defined profile to disconnect a device on AOS-CX switches.
9.	□	[Arista Wired - Terminate Session]	RADIUS_DynAuthZ	System-defined profile to disconnect user (Arista Wired)
10.	□	[Arista Wireless - Terminate Session]	RADIUS_DynAuthZ	System-defined profile to disconnect user (Arista Wireless)
11.	□	[ArubaOS Switching - Bounce Switch Port]	RADIUS_DynAuthZ	System-defined profile to bounce the switch port on ArubaOS Switching products.
12.	□	[ArubaOS Switching - Terminate Session]	RADIUS_DynAuthZ	System-defined profile to disconnect the user on ArubaOS Switching, HP ProCurve and HP UWW products.
13.	□	[ArubaOS Wireless - Bounce Switch Port]	RADIUS_DynAuthZ	System-defined profile to bounce the switch port on ArubaOS Mobility Controllers, Multi-Port APs & Mobility Access Switches.
14.	□	[ArubaOS Wireless - TACACS+ Read-Only Access]	TACACS+	System-defined profile for TACACS+ read-only access on ArubaOS Mobility Controllers, Aruba Instant APs & Mobility Access Switches.
15.	□	[ArubaOS Wireless - TACACS+ Root Access]	TACACS+	System-defined profile for TACACS+ root access on ArubaOS Mobility Controllers, Aruba Instant APs & Mobility Access Switches.
16.	□	[ArubaOS Wireless - Terminate Session]	RADIUS_DynAuthZ	System-defined profile to disconnect the user on ArubaOS Mobility Controllers, Aruba Instant APs & Mobility Access Switches.

Figure 67: Add Enforcement Profile

Step 4 In the **Add Enforcement Profile** window, match the following settings in the **Profile** tab, then click the **Save** button. - **Template:** *Aruba RADIUS Enforcement* - **Name:** *OWL_Employee* - **Description:** *Return Aruba User Role* - **Action:** *Accept*



Enforcement Profiles

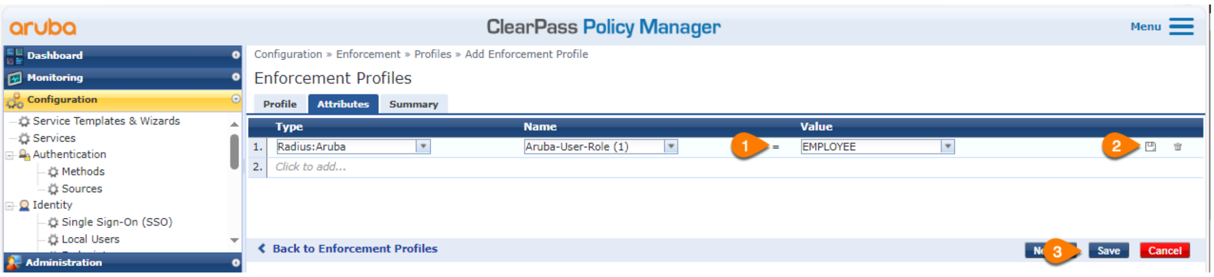
Template: Aruba RADIUS Enforcement
Name: OWL_Employee
Description: Returns Aruba User Role
Type: RADIUS
Action: ● Accept ○ Reject ○ Drop
Device Group List: --Select--

Figure 68: Enforcement Profile Tab

Step 5 In the **Attributes** tab, match the following settings, then click the **Save** icon next to the **Value**, followed by the **Next** button. - **Type:** *Radius:Aruba* - **Name:** *Aruba-User-Role (1)* - **Value:** *EMPLOYEE*

NOTE:

Make sure to match the letter case when configuring user roles. Case-sensitive Aruba switches, gateways, and APs ignore the role returned by ClearPass if the case does not match.



Configuration » Enforcement » Profiles » Add Enforcement Profile

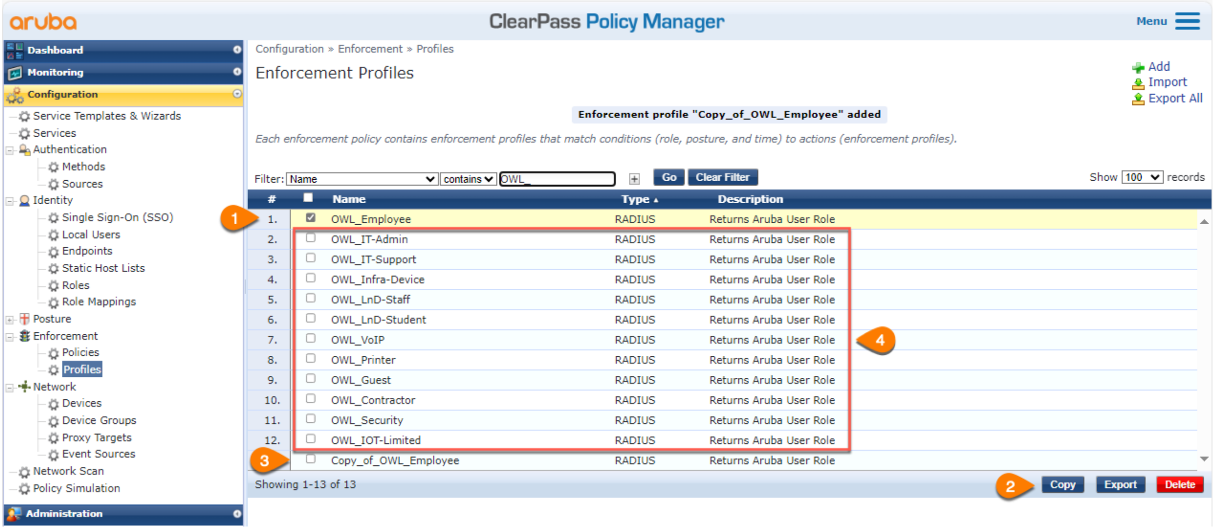
Enforcement Profiles

Profile | Attributes | Summary

	Type	Name		Value
1.	Radius:Aruba	Aruba-User-Role (1)	=	EMPLOYEE
2.	Click to add...			

Figure 69: Enforcement Attributes Tab

Step 6 After the first rule is saved, click the **Copy** button to create the second rule as follows: - Click the checkbox next to the newly created *OWL_Employee* profile - Click the **Copy** button - Click the newly created *Copy_of_OWL_Employee* profile



Configuration » Enforcement » Profiles

Enforcement Profiles

Enforcement profile "Copy_of_OWL_Employee" added

Each enforcement policy contains enforcement profiles that match conditions (role, posture, and time) to actions (enforcement profiles).

Filter: Name contains OWL_ Show 100 records

#		Name	Type	Description
1.	☑	OWL_Employee	RADIUS	Returns Aruba User Role
2.	□	OWL_IT-Admin	RADIUS	Returns Aruba User Role
3.	□	OWL_IT-Support	RADIUS	Returns Aruba User Role
4.	□	OWL_Infra-Device	RADIUS	Returns Aruba User Role
5.	□	OWL_LnD-Staff	RADIUS	Returns Aruba User Role
6.	□	OWL_LnD-Student	RADIUS	Returns Aruba User Role
7.	□	OWL_VoIP	RADIUS	Returns Aruba User Role
8.	□	OWL_Printer	RADIUS	Returns Aruba User Role
9.	□	OWL_Guest	RADIUS	Returns Aruba User Role
10.	□	OWL_Contractor	RADIUS	Returns Aruba User Role
11.	□	OWL_Security	RADIUS	Returns Aruba User Role
12.	□	OWL_IOT-Limited	RADIUS	Returns Aruba User Role
	□	Copy_of_OWL_Employee	RADIUS	Returns Aruba User Role

Showing 1-13 of 13

Figure 70: Enforcement Profiles All

Step 7 When the **Edit Enforcement Profile** page appears, update the following, then click the **Save** button. - In the **Profile** tab: - **Name:** *OWL_IT-Admin* - In the **Attributes** tab: - **Value:** *IT-ADMIN*

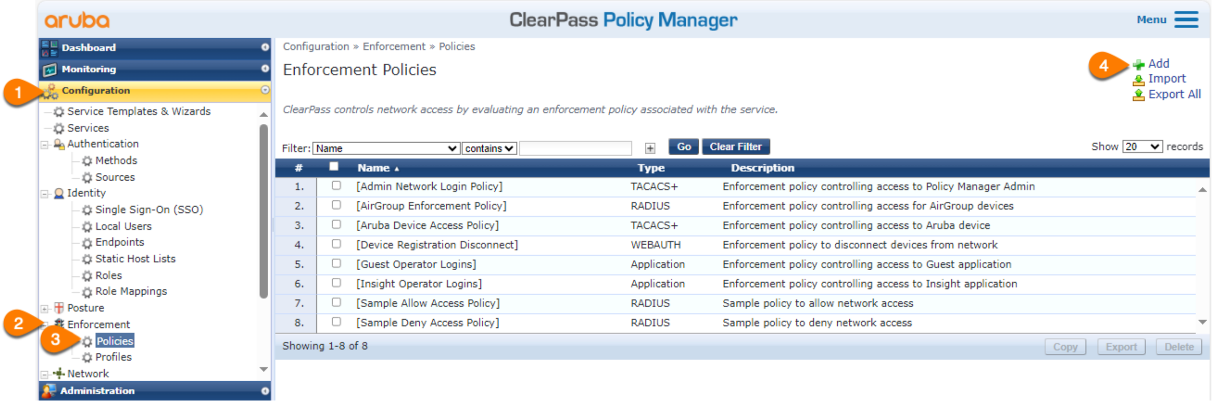
Step 8 Repeat the steps to create the rest of the profiles in the image above.

Step 9 When the remaining profiles are created, proceed to the next section.

Configure Enforcement Policy

Follow the steps below to configure the Enforcement Policy for the Wireless 802.1X service for CorpNet SSID.

Step 1 Go to **Configuration** > **Enforcement** > **Policies** and click the **Add** link at the upper right.



Enforcement Policies

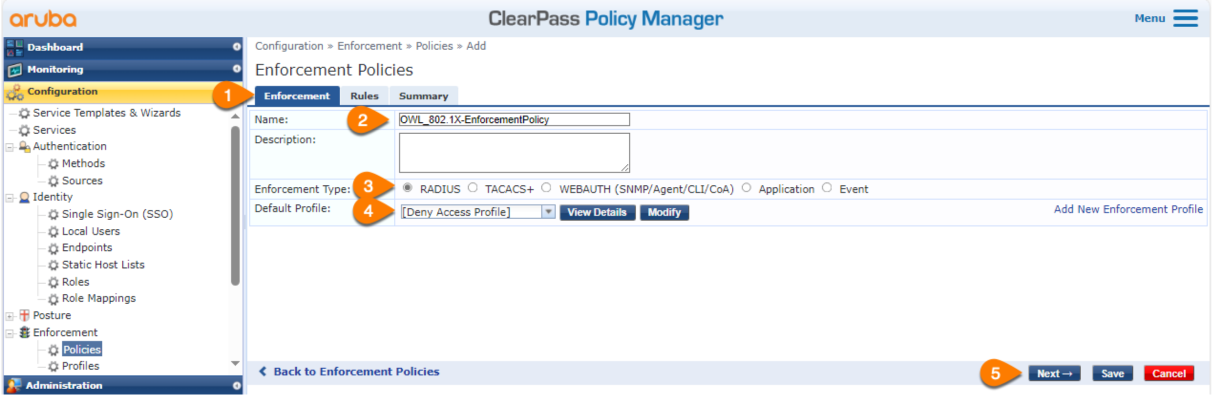
ClearPass controls network access by evaluating an enforcement policy associated with the service.

#		Name ▴	Type	Description
1.	□	[Admin Network Login Policy]	TACACS+	Enforcement policy controlling access to Policy Manager Admin
2.	□	[AirGroup Enforcement Policy]	RADIUS	Enforcement policy controlling access for AirGroup devices
3.	□	[Aruba Device Access Policy]	TACACS+	Enforcement policy controlling access to Aruba device
4.	□	[Device Registration Disconnect]	WEBAUTH	Enforcement policy to disconnect devices from network
5.	□	[Guest Operator Logins]	Application	Enforcement policy controlling access to Guest application
6.	□	[Insight Operator Logins]	Application	Enforcement policy controlling access to Insight application
7.	□	[Sample Allow Access Policy]	RADIUS	Sample policy to allow network access
8.	□	[Sample Deny Access Policy]	RADIUS	Sample policy to deny network access

Showing 1-8 of 8

Figure 71: Add Enforcement Policy

Step 2 In the **Add Enforcement Policies** screen, in the **Enforcement** tab, configure the following, then click the **Next** button. - **Name:** *OWL_802.1X-EnforcementPolicy* - **Enforcement Type:** *RADIUS* - **Default Profile:** *[Deny Access Policy]*



Enforcement Policies

Name: OWL_802.1X-EnforcementPolicy

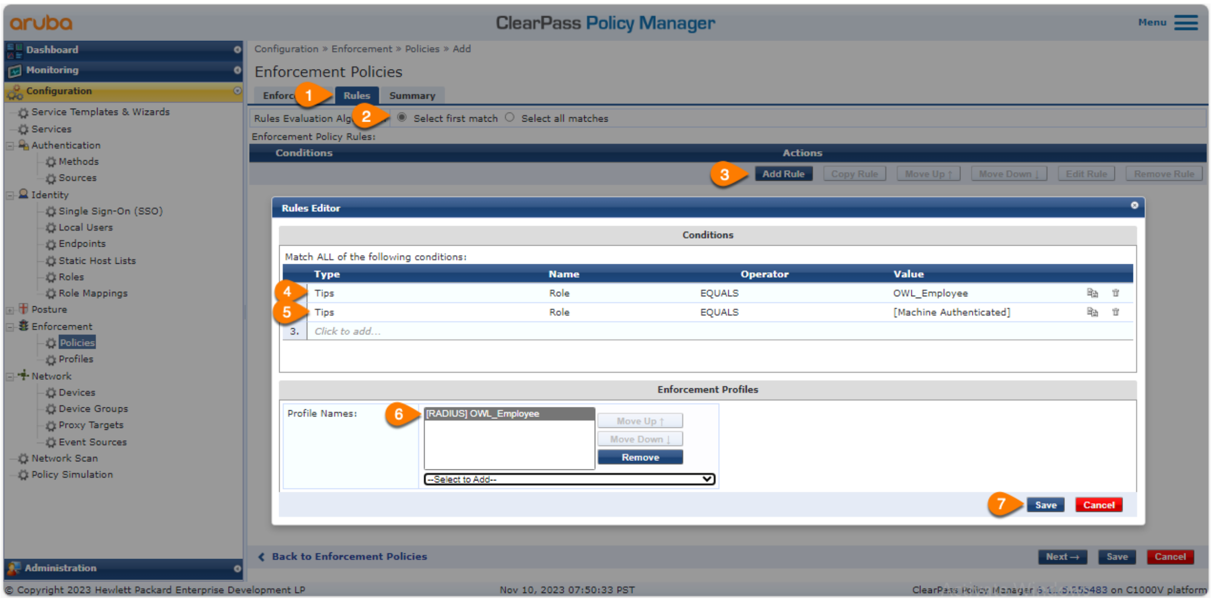
Description:

Enforcement Type: ● RADIUS ○ TACACS+ ○ WEBAUTH (SNMP/Agent/CLI/CoA) ○ Application ○ Event

Default Profile: [Deny Access Profile]

Figure 72: Enforcement Policy Enforcement Tab

Step 3 In the **Rules** tab, click the **Add Rule** button. In the **Rules Editor** window, configure the settings to match the image below, then click the **Save** button.



Rules Evaluation Algorithm: ● Select first match ○ Select all matches

Enforcement Policy Rules:

Conditions	Actions

Conditions

Match ALL of the following conditions:

	Type	Name	Operator	Value
	Tips	Role	EQUALS	OWL_Employee
	Tips	Role	EQUALS	[Machine Authenticated]
3.	Click to add...			

Enforcement Profiles

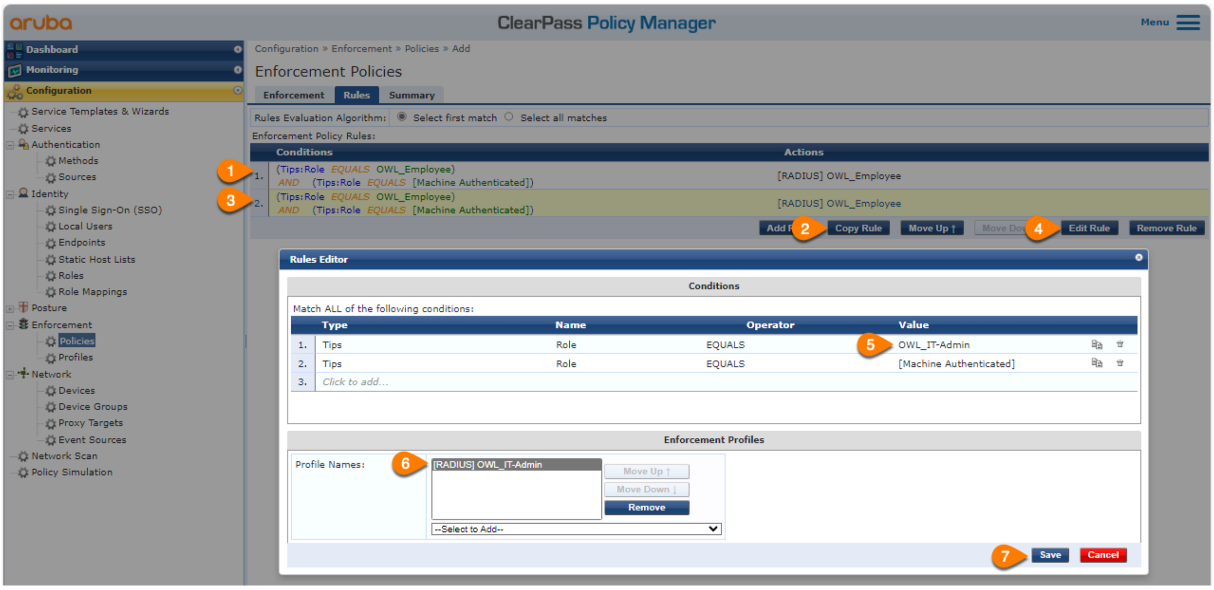
Profile Names: [RADIUS] OWL_Employee

--Select to Add--

© Copyright 2023 Hewlett Packard Enterprise Development LP Nov 10, 2023 07:50:33 PST ClearPass Policy Manager 6.11.5.255483 on C1000V platform

Figure 73: Enforcement Policy Rules Tab

Step 4 After the first rule is saved, click the **Copy Rule** button to create the second rule as follows: - Select the newly created rule for *OWL_Employee* - Click the **Copy Rule** button - Select the newly duplicated rule - Click the **Edit Rule** button - Change the **Value** column of the first rule to *OWL_IT-Admin* - Replace the **Profile Name** with *OWL_IT-Admin* - Click the **Save** button



Rules Evaluation Algorithm: ● Select first match ○ Select all matches

Enforcement Policy Rules:

	Conditions	Actions
1.	(Tips:Role EQUALS OWL_Employee) AND (Tips:Role EQUALS [Machine Authenticated])	[RADIUS] OWL_Employee
2.	(Tips:Role EQUALS OWL_Employee) AND (Tips:Role EQUALS [Machine Authenticated])	[RADIUS] OWL_Employee

Conditions

Match ALL of the following conditions:

	Type	Name	Operator	Value
1.	Tips	Role	EQUALS	OWL_IT-Admin
2.	Tips	Role	EQUALS	[Machine Authenticated]
3.	Click to add...			

Enforcement Profiles

Profile Names: [RADIUS] OWL_IT-Admin

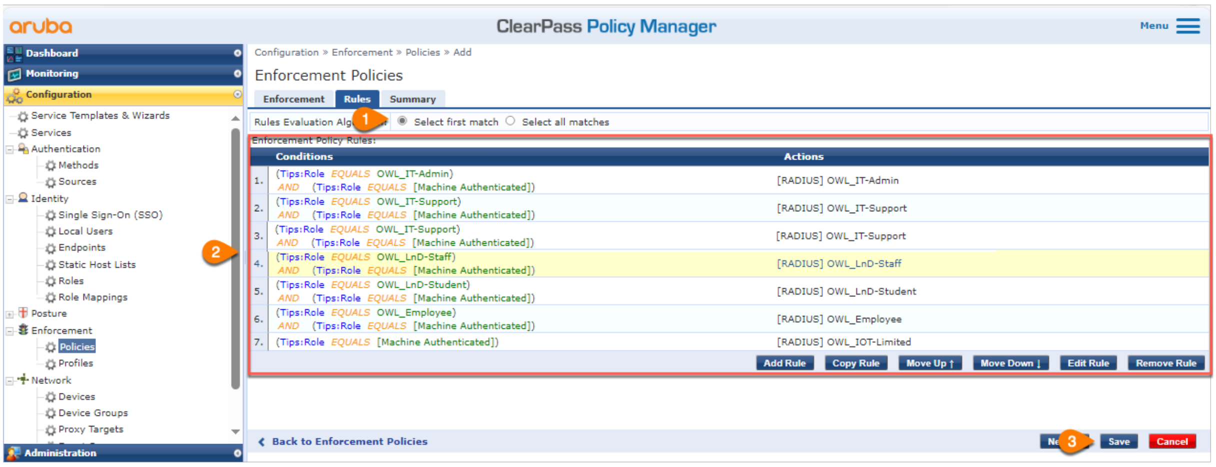
--Select to Add--

Figure 74: Enforcement Policy Copy Rule

Step 5 Repeat the last step until the enforcement rules below are created, then click the **Save** button.

Type	Profile Names
Tips Role equals OWL_Employee AND Tips Role equals [Machine Authenticated]	[RADIUS] OWL_Employee
Tips Role equals OWL_IT-Admin AND Tips Role equals [Machine Authenticated]	[RADIUS] OWL_IT-Admin
Tips Role equals OWL_IT-Support AND Tips Role equals [Machine Authenticated]	[RADIUS] OWL_IT-Support
Tips Role equals OWL_LnD-Staff AND Tips Role equals [Machine Authenticated]	[RADIUS] OWL_LnD-Staff
Tips Role equals OWL_LnD-Student AND Tips Role equals [Machine Authenticated]	[RADIUS] OWL_LnD-Student
Tips Role equals OWL_Contractor AND Tips Role equals [Machine Authenticated]	[RADIUS] OWL_Contractor
Tips Role equals [Machine Authenticated]	[RADIUS] OWL_Machine-Auth

Step 6 Verify that the **Enforcement Policy Rules** look like the screenshot below, then click the **Save** button.



Rules Evaluation Alg[...]: ● Select first match ○ Select all matches

Enforcement Policy Rules:

	Conditions	Actions
1.	(Tips:Role EQUALS OWL_IT-Admin) AND (Tips:Role EQUALS [Machine Authenticated])	[RADIUS] OWL_IT-Admin
2.	(Tips:Role EQUALS OWL_IT-Support) AND (Tips:Role EQUALS [Machine Authenticated])	[RADIUS] OWL_IT-Support
3.	(Tips:Role EQUALS OWL_IT-Support) AND (Tips:Role EQUALS [Machine Authenticated])	[RADIUS] OWL_IT-Support
4.	(Tips:Role EQUALS OWL_LnD-Staff) AND (Tips:Role EQUALS [Machine Authenticated])	[RADIUS] OWL_LnD-Staff
5.	(Tips:Role EQUALS OWL_LnD-Student) AND (Tips:Role EQUALS [Machine Authenticated])	[RADIUS] OWL_LnD-Student
6.	(Tips:Role EQUALS OWL_Employee) AND (Tips:Role EQUALS [Machine Authenticated])	[RADIUS] OWL_Employee
7.	(Tips:Role EQUALS [Machine Authenticated])	[RADIUS] OWL_IOT-Limited

Figure 75: Enforcement Policy Save Rule

Step 7 When complete, proceed to the next section.

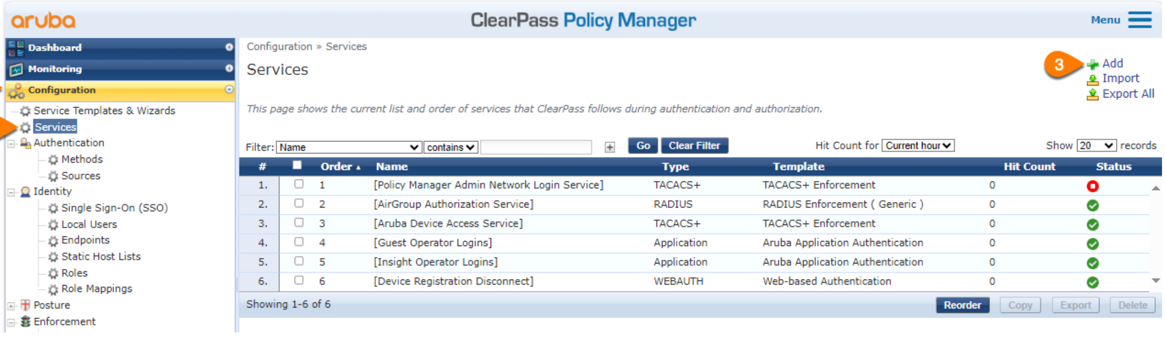
Configure Service

With the enforcement and role mapping policies created, follow the steps below to create the RADIUS service for CorpNet SSID.

Step 1 Open a web browser and connect to the publisher node, RSVCP-CPPM-1.

Step 2 Log in using the admin credentials. - **Username:** *admin* - **Password:** *Aruba123!*

Step 3 Go to **Configuration** > **Services** and click the **Add** link at the upper right.



Configuration » Services

Services

This page shows the current list and order of services that ClearPass follows during authentication and authorization.

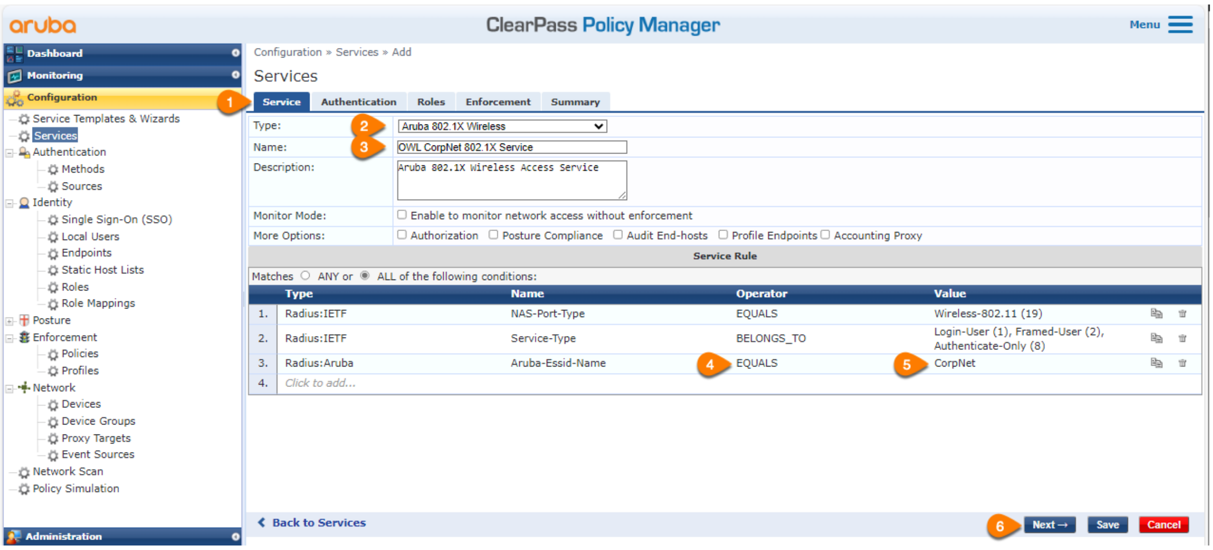
Filter: Name contains | Hit Count for Current hour | Show 20 records

#	☐	Order ▲	Name	Type	Template	Hit Count	Status
1.	☐	1	[Policy Manager Admin Network Login Service]	TACACS+	TACACS+ Enforcement	0	🟥
2.	☐	2	[AirGroup Authorization Service]	RADIUS	RADIUS Enforcement (Generic)	0	✓
3.	☐	3	[Aruba Device Access Service]	TACACS+	TACACS+ Enforcement	0	✓
4.	☐	4	[Guest Operator Logins]	Application	Aruba Application Authentication	0	✓
5.	☐	5	[Insight Operator Logins]	Application	Aruba Application Authentication	0	✓
6.	☐	6	[Device Registration Disconnect]	WEBAUTH	Web-based Authentication	0	✓

Showing 1-6 of 6

Figure 76: Add Wireless RADIUS Service

Step 4 In the new **Services** window, in the **Services** tab, configure the following, then click the **Next** button. - **Type:** *Aruba 802.1X Wireless* - **Name:** *OWL CorpNet 802.1X Service* - **Service Rule List > Rule No. 3:** - **Operator column:** Change to *EQUALS* - **Value column:** Change to *CorpNet*



Configuration » Services » Add

Services

Type: Aruba 802.1X Wireless

Name: OWL CorpNet 802.1X Service

Description: Aruba 802.1X Wireless Access Service

Monitor Mode: ☐ Enable to monitor network access without enforcement

More Options: ☐ Authorization ☐ Posture Compliance ☐ Audit End-hosts ☐ Profile Endpoints ☐ Accounting Proxy

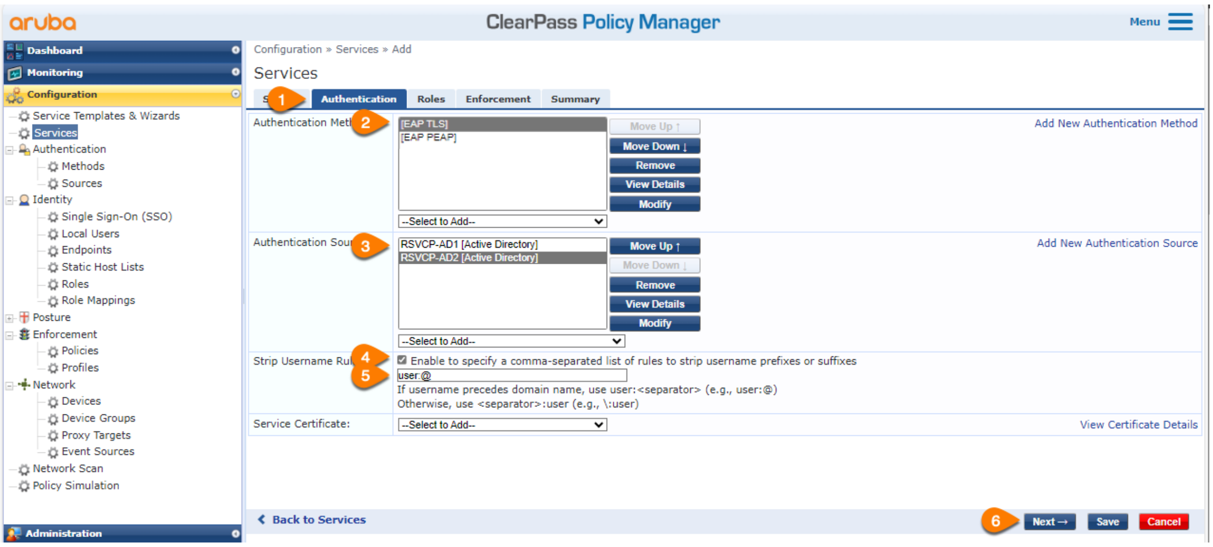
Service Rule

Matches ○ ANY or ● ALL of the following conditions:

	Type	Name	Operator	Value
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.	Radius:Aruba	Aruba-Essid-Name	EQUALS	CorpNet
4.	*Click to add...*			

Figure 77: Dot1X Wireless Service Tab

Step 5 In the **Authentication** tab, configure the following, then click the **Next** button. - **Authentication Methods:** - EAP-TLS - [EAP PEAP] - **Authentication Sources:** - *RSVCP-AD1* - *RSVCP-AD2* - **Strip Username Rules:** - (Check the box to enable) - *User:@*



Configuration » Services » Add

Services

Service | Authentication | Roles | Enforcement | Summary

Authentication Methods: [EAP TLS]
[EAP PEAP] --Select to Add--

Authentication Sources: RSVCP-AD1 [Active Directory]
RSVCP-AD2 [Active Directory] --Select to Add--

Strip Username Rules: ☑ Enable to specify a comma-separated list of rules to strip username prefixes or suffixes

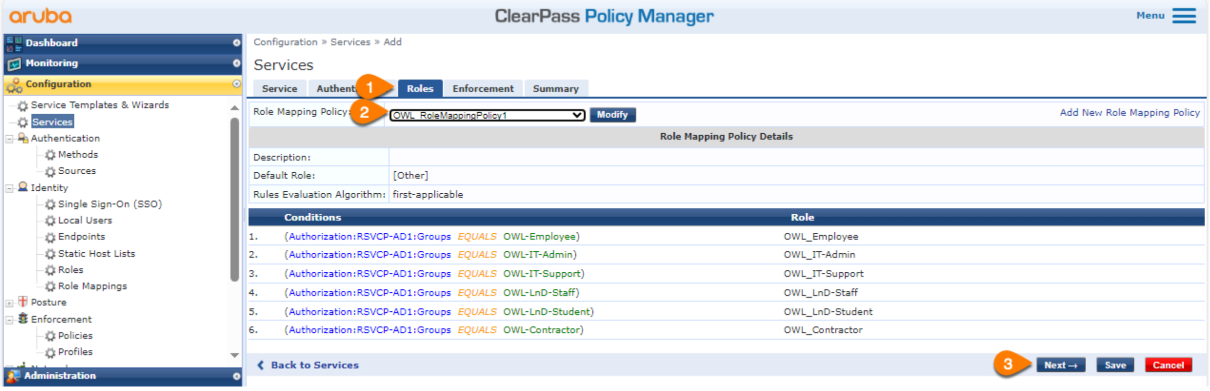
user:@

If username precedes domain name, use user:<separator> (e.g., user:@)
Otherwise, use <separator>:user (e.g., \:user)

Service Certificate: --Select to Add--

Figure 78: Dot1X Wireless Authentication Tab

Step 6 In the **Roles** tab, select *OWL_RoleMappingPolicy1* from the **Role Mapping Policy** dropdown, then click the **Next** button.



Configuration » Services » Add

Services

Service | Authentication | Roles | Enforcement | Summary

Role Mapping Policy: OWL_RoleMappingPolicy1

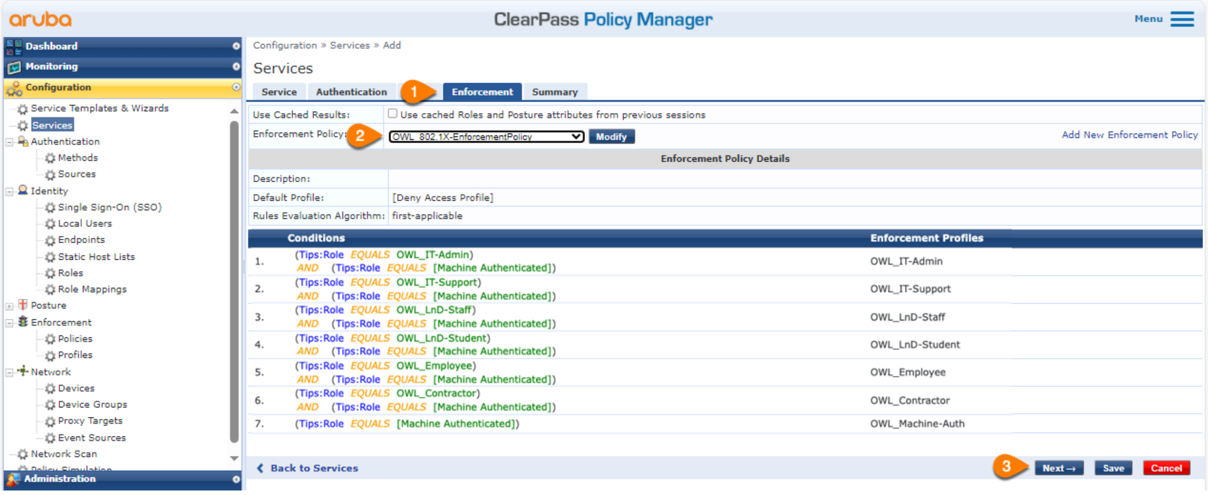
Role Mapping Policy Details

Description:
Default Role: [Other]
Rules Evaluation Algorithm: first-applicable

	Conditions	Role
1.	(Authorization:RSVCP-AD1:Groups EQUALS OWL-Employee)	OWL_Employee
2.	(Authorization:RSVCP-AD1:Groups EQUALS OWL-IT-Admin)	OWL_IT-Admin
3.	(Authorization:RSVCP-AD1:Groups EQUALS OWL-IT-Support)	OWL_IT-Support
4.	(Authorization:RSVCP-AD1:Groups EQUALS OWL-LnD-Staff)	OWL_LnD-Staff
5.	(Authorization:RSVCP-AD1:Groups EQUALS OWL-LnD-Student)	OWL_LnD-Student
6.	(Authorization:RSVCP-AD1:Groups EQUALS OWL-Contractor)	OWL_Contractor

Figure 79: Dot1X Wireless Roles Tab

Step 7 In the **Enforcement** tab, select *OWL_802.1X_EnforcementPolicy* from the **Enforcement Policy** dropdown, then click the **Save** button.



Use Cached Results: □ Use cached Roles and Posture attributes from previous sessions

Enforcement Policy: OWL_802.1X-EnforcementPolicy

Enforcement Policy Details

Description:	
Default Profile:	[Deny Access Profile]
Rules Evaluation Algorithm:	first-applicable

	Conditions	Enforcement Profiles
1.	(Tips:Role EQUALS OWL_IT-Admin) AND (Tips:Role EQUALS [Machine Authenticated])	OWL_IT-Admin
2.	(Tips:Role EQUALS OWL_IT-Support) AND (Tips:Role EQUALS [Machine Authenticated])	OWL_IT-Support
3.	(Tips:Role EQUALS OWL_LnD-Staff) AND (Tips:Role EQUALS [Machine Authenticated])	OWL_LnD-Staff
4.	(Tips:Role EQUALS OWL_LnD-Student) AND (Tips:Role EQUALS [Machine Authenticated])	OWL_LnD-Student
5.	(Tips:Role EQUALS OWL_Employee) AND (Tips:Role EQUALS [Machine Authenticated])	OWL_Employee
6.	(Tips:Role EQUALS OWL_Contractor) AND (Tips:Role EQUALS [Machine Authenticated])	OWL_Contractor
7.	(Tips:Role EQUALS [Machine Authenticated])	OWL_Machine-Auth

Figure 80: Dot1X Wireless Enforcement Tab

Step 8 When complete, proceed to next section.

Configure CorpNet WLAN in Aruba Central

Below are the primary settings for CorpNet WLAN. For prescriptive guidance on creating a new WLAN, please see the Campus Wireless Connectivity chapter of the Campus Deploy guide.

General

- **ESSID:** *CorpNet*
- **Band:** *all*

VLANs

- **Traffic forwarding mode:** *Tunnel*
- **Primary Gateway Cluster:** *CP-RSVWLAN:CL-RSVCP-S2*
- **VLAN ID:** *EMPLOYEE(103)*

Security

- **Key Management:** *WPA3-Enterprise*
- **Primary Server:** *rsvcp-cppm-1*
- **Secondary Server:** *rsvcp-cppm-2*

Access

- **Access Rules:** *Role Based*
- **Roles:** Ensure all Roles are configured
  - *MACHINE-AUTH*
  - *EMPLOYEE*

  - *IT-SUPPORT*
  - *IT-ADMIN*
  - *INFRA-DEVICE*
  - *LND-STAFF*
  - *LND-STUDENT*
  - *VOIP*
  - *PRINTER*
  - *GUEST*
  - *CONTRACTOR*
  - *SECURITY*
  - *IOT-LIMITED*

Configure Client

Below are the sample Windows client settings for CorpNet WLAN.

PEAP

- **SSID:** *CorpNet*
- **Security type:** *WPA3-Enterprise*
- **Encryption type:** *AES*
- **Authentication Method:** *PEAP/EAP-MSCHAP v2*
- **Authentication mode:** *User or computer authentication*

EAP-TLS

- **SSID:** *CorpNet*
- **Security type:** *WPA3-Enterprise*
- **Encryption type:** *AES*
- **Authentication Method:** *Microsoft Smart Card or other certificate (EAP-TLS)*
- **Authentication mode:** *User or computer authentication*

Validate Authentication

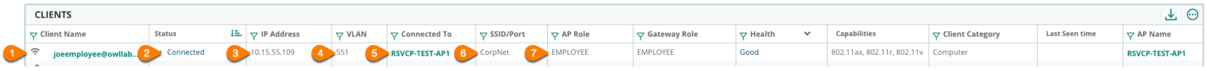
After connecting a client device to CorpNet, confirm successful authentication by reviewing the client, Aruba Central, and ClearPass Access Tracker. The following are examples from OWL's CorpNet test.

Windows Client

In Windows, view **Network & internet** > **Wi-Fi** > **CorpNet** and verify that IP address in the expected subnet and client is able to access the expected resources according to their user role or VLAN.

Aruba Central

In Aruba Central, go to **Groups** > **Clients** , find the test client, and review details. Example:



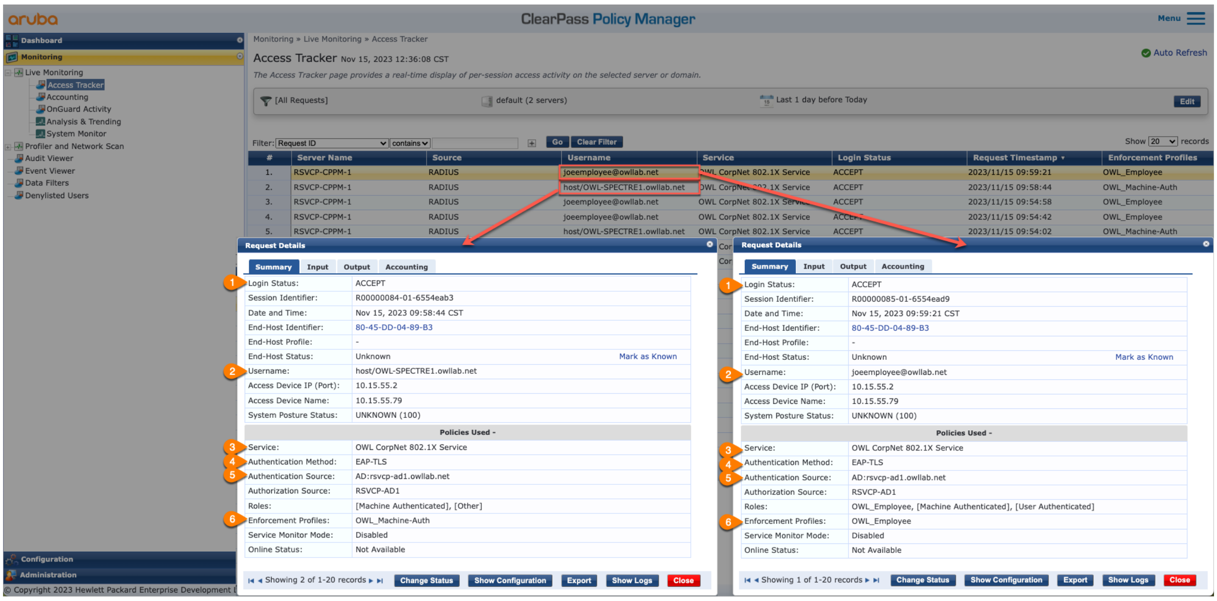
CLIENTS

Client Name	Status	IP Address	VLAN	Connected To	SSID/Port	AP Role	Gateway Role	Health	Capabilities	Client Category	Last Seen time	AP Name
joeemployee@owllab...	Connected	10.15.55.109	551	RSVCP-TEST-AP1	CorpNet	EMPLOYEE	EMPLOYEE	Good	802.11ax, 802.11r, 802.11v	Computer		RSVCP-TEST-AP1

Figure 81: Validate Central for CorpNet

ClearPass

In ClearPass, go to **Monitoring** > **Access Tracker**, find the authentication events and review details. Example:



Monitoring » Live Monitoring » Access Tracker

Access Tracker Nov 15, 2023 12:36:08 CST

The Access Tracker page provides a real-time display of per-session access activity on the selected server or domain.

[All Requests] default (2 servers) Last 1 day before Today

Filter: Request ID contains

Show 20 records

#	Server Name	Source	Username	Service	Login Status	Request Timestamp	Enforcement Profiles
1.	RSVCP-CPPM-1	RADIUS	joeemployee@owllab.net	OWL CorpNet 802.1X Service	ACCEPT	2023/11/15 09:59:21	OWL_Employee
2.	RSVCP-CPPM-1	RADIUS	host/OWL-SPECTRE1.owllab.net	OWL CorpNet 802.1X Service	ACCEPT	2023/11/15 09:58:44	OWL_Machine-Auth
3.	RSVCP-CPPM-1	RADIUS	joeemployee@owllab.net	OWL CorpNet 802.1X Service	ACCEPT	2023/11/15 09:54:58	OWL_Employee
4.	RSVCP-CPPM-1	RADIUS	joeemployee@owllab.net	OWL CorpNet 802.1X Service	ACCEPT	2023/11/15 09:54:42	OWL_Employee
5.	RSVCP-CPPM-1	RADIUS	host/OWL-SPECTRE1.owllab.net	OWL CorpNet 802.1X Service	ACCEPT	2023/11/15 09:54:02	OWL_Machine-Auth

Request Details

Login Status:	ACCEPT
Session Identifier:	R00000084-01-6554eab3
Date and Time:	Nov 15, 2023 09:58:44 CST
End-Host Identifier:	80-45-DD-04-89-B3
End-Host Profile:	-
End-Host Status:	Unknown Mark as Known
Username:	host/OWL-SPECTRE1.owllab.net
Access Device IP (Port):	10.15.55.2
Access Device Name:	10.15.55.79
System Posture Status:	UNKNOWN (100)
Policies Used -	
Service:	OWL CorpNet 802.1X Service
Authentication Method:	EAP-TLS
Authentication Source:	AD:rsvcp-ad1.owllab.net
Authorization Source:	RSVCP-AD1
Roles:	[Machine Authenticated], [Other]
Enforcement Profiles:	OWL_Machine-Auth
Service Monitor Mode:	Disabled
Online Status:	Not Available

Showing 2 of 1-20 records

Request Details

Login Status:	ACCEPT
Session Identifier:	R00000085-01-6554ead9
Date and Time:	Nov 15, 2023 09:59:21 CST
End-Host Identifier:	80-45-DD-04-89-B3
End-Host Profile:	-
End-Host Status:	Unknown Mark as Known
Username:	joeemployee@owllab.net
Access Device IP (Port):	10.15.55.2
Access Device Name:	10.15.55.79
System Posture Status:	UNKNOWN (100)
Policies Used -	
Service:	OWL CorpNet 802.1X Service
Authentication Method:	EAP-TLS
Authentication Source:	AD:rsvcp-ad1.owllab.net
Authorization Source:	RSVCP-AD1
Roles:	OWL_Employee, [Machine Authenticated], [User Authenticated]
Enforcement Profiles:	OWL_Employee
Service Monitor Mode:	Disabled
Online Status:	Not Available

Showing 1 of 1-20 records

© Copyright 2023 Hewlett Packard Enterprise Development l

Figure 82: Validate ClearPass for CorpNet

When validation is complete, proceed to next section.

Configure Wired Authentication for ArubaOS-CX Switches

For wired authentication, two separate services must be created. One is to authenticate OWL devices configured for wired 802.1X, and the second is to authenticate all wired headless devices via MAC authentication. Follow the steps below to configure both services.

Configure Wired 802.1X Authentication

The 802.1X service uses EAP-TLS authentication method with Active Directory (AD) user group memberships to provide different authorization levels for corporate users and computers.

Note that the workflow for this setup requires creating Role Mapping and Enforcement Policies before adding the actual service.

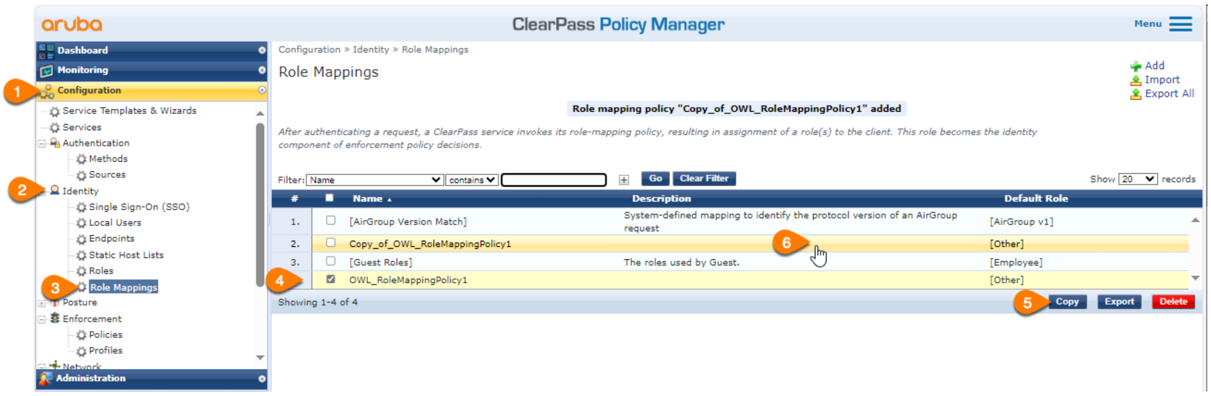
Configure ClearPass Roles for Role Mapping Policy

The ClearPass Roles created for the CorpNet Role Mapping Policy earlier in this chapter will be re-used for this configuration.

Configure Role Mapping Policy

Duplicate the Role Mapping Policy created for the Wireless 802.1X service earlier in this chapter to be able to manage them separately.

Step 1 Go to **Configuration** > **Identity** > **Role Mappings** > and check the box next to the previously created policy, then click the **Copy** button in the lower right of the page, and click on the new copy.



Configuration » Identity » Role Mappings

Role Mappings

Role mapping policy "Copy_of_OWL_RoleMappingPolicy1" added

After authenticating a request, a ClearPass service invokes its role-mapping policy, resulting in assignment of a role(s) to the client. This role becomes the identity component of enforcement policy decisions.

Filter: Name contains | Go | Clear Filter | Show 20 records

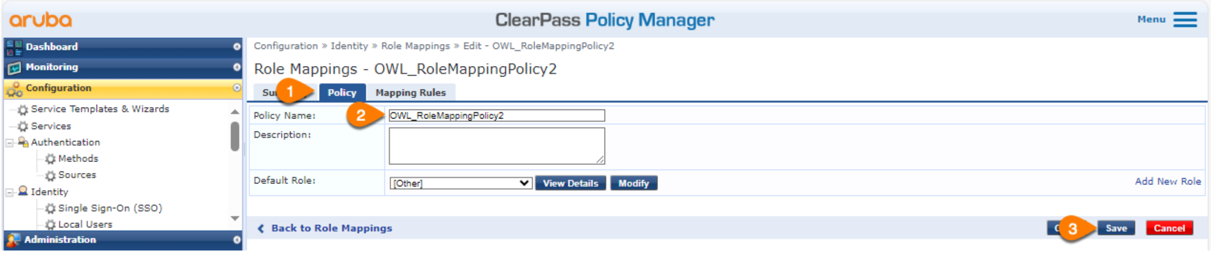
#	■	Name ▴	Description	Default Role
1.	□	[AirGroup Version Match]	System-defined mapping to identify the protocol version of an AirGroup request	[AirGroup v1]
2.	□	Copy_of_OWL_RoleMappingPolicy1		[Other]
3.	□	[Guest Roles]	The roles used by Guest.	[Employee]
	☑	OWL_RoleMappingPolicy1		[Other]

Showing 1-4 of 4

Figure 83: Duplicate Role Mapping Policy

Step 2 Click on the newly created *Copy_of_OWL_RoleMappingPolicy1*

Step 3 In the **Role Mappings** window, under the **Policy** tab, update the following, then click the **Save** button. - **Policy Name:** Rename to *OWL_RoleMappingPolicy2*



Configuration » Identity » Role Mappings » Edit - OWL_RoleMappingPolicy2

Role Mappings - OWL_RoleMappingPolicy2

Policy Name: OWL_RoleMappingPolicy2

Description:

Default Role: [Other]

Figure 84: Rename Copy of Role Mapping Policy

Step 4 With OWL_RoleMappingPolicy2 successfully created, proceed to the next section.

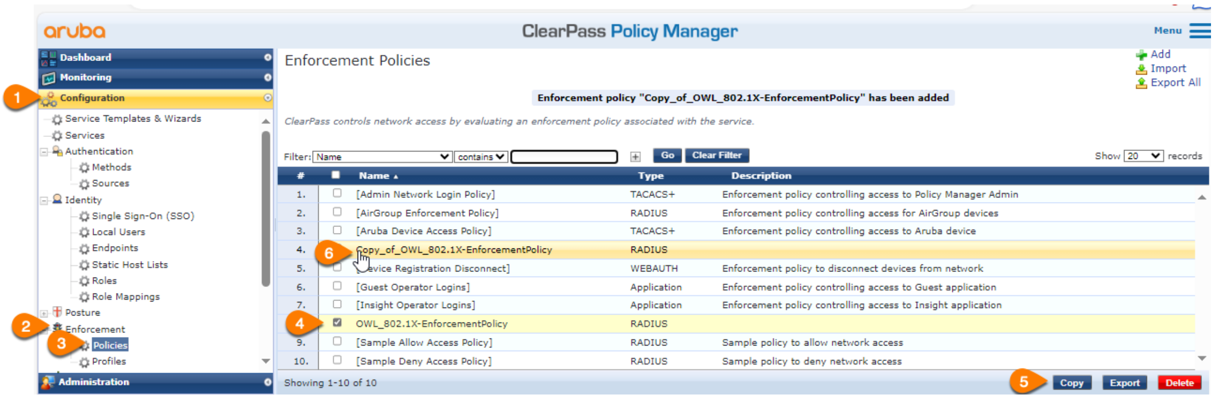
Configure Enforcement Profiles for Enforcement Policy

The Enforcement Profiles created for the CorpNet Enforcement Policy earlier in this chapter are used for this configuration.

Configure Enforcement Policy

Duplicate the Enforcement Policy created for the Wireless 802.1X service earlier in this chapter to be able to manage them separately.

Step 1 Go to **Configuration** > **Enforcement** > **Policies** > and check the box next to the previously created policy, then click the **Copy** button in the lower right of the page.



Enforcement Policies

Enforcement policy "Copy_of_OWL_802.1X-EnforcementPolicy" has been added

ClearPass controls network access by evaluating an enforcement policy associated with the service.

Filter: Name contains Show 20 records

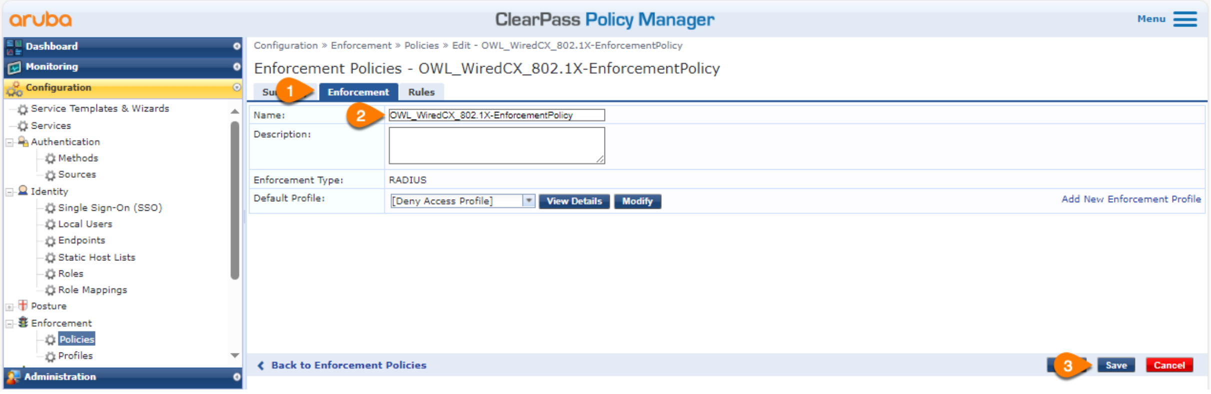
#	■	Name ▲	Type	Description
1.	□	[Admin Network Login Policy]	TACACS+	Enforcement policy controlling access to Policy Manager Admin
2.	□	[AirGroup Enforcement Policy]	RADIUS	Enforcement policy controlling access for AirGroup devices
3.	□	[Aruba Device Access Policy]	TACACS+	Enforcement policy controlling access to Aruba device
4.		Copy_of_OWL_802.1X-EnforcementPolicy	RADIUS	
5.	□	[Device Registration Disconnect]	WEBAUTH	Enforcement policy to disconnect devices from network
6.	□	[Guest Operator Logins]	Application	Enforcement policy controlling access to Guest application
7.	□	[Insight Operator Logins]	Application	Enforcement policy controlling access to Insight application
	☑	OWL_802.1X-EnforcementPolicy	RADIUS	
9.	□	[Sample Allow Access Policy]	RADIUS	Sample policy to allow network access
10.	□	[Sample Deny Access Policy]	RADIUS	Sample policy to deny network access

Showing 1-10 of 10

Figure 85: Duplicate Enforcement Policy

Step 2 Click on the newly created *Copy_of_OWL_802.1XEnforcementPolicy*

Step 3 In the **Enforcement Policies** window, under the **Enforcement** tab, update the following, then click the **Save** button. - **Name:** Rename to *OWL_WiredCX_802.1X-EnforcementPolicy*



Configuration » Enforcement » Policies » Edit - OWL_WiredCX_802.1X-EnforcementPolicy

Enforcement Policies - OWL_WiredCX_802.1X-EnforcementPolicy

Name: OWL_WiredCX_802.1X-EnforcementPolicy

Description:

Enforcement Type: RADIUS

Default Profile: [Deny Access Profile]

Figure 86: Rename Copy of Enforcement Policy

Step 4 With OWL_WiredCX_802.1X-EnforcementPolicy successfully created, proceed to the next section.

Configure Service

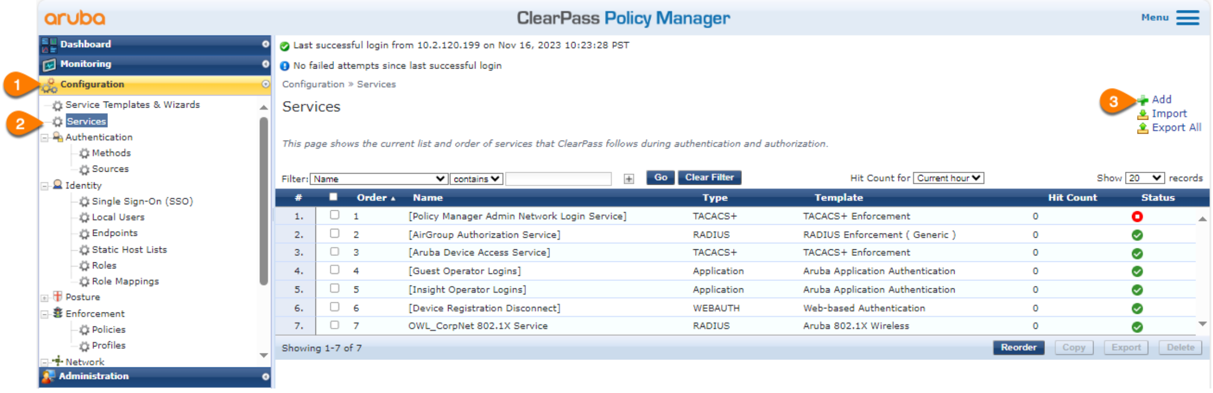
Follow the steps below to configure the wired 802.1X service for OWL's CX switches.

Step 1 Open a web browser and connect to the publisher node, RSVCP-CPPM-1.

Step 2 Log in using the admin credentials.

- **Username:** *admin*
- **Password:** *Aruba123!*

Step 3 Go to **Configuration** > **Services** and click the **Add** link at the upper right.



Last successful login from 10.2.120.199 on Nov 16, 2023 10:23:28 PST

No failed attempts since last successful login

Configuration » Services

Services

This page shows the current list and order of services that ClearPass follows during authentication and authorization.

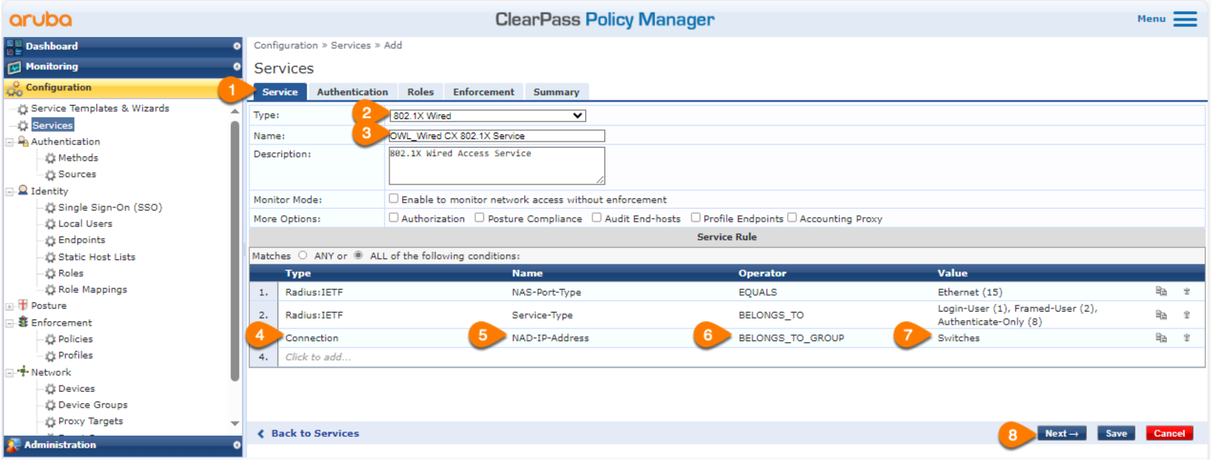
Filter: Name contains | Hit Count for Current hour | Show 20 records

#	☐	Order ▲	Name	Type	Template	Hit Count	Status
1.	☐	1	[Policy Manager Admin Network Login Service]	TACACS+	TACACS+ Enforcement	0	🟥
2.	☐	2	[AirGroup Authorization Service]	RADIUS	RADIUS Enforcement (Generic)	0	✓
3.	☐	3	[Aruba Device Access Service]	TACACS+	TACACS+ Enforcement	0	✓
4.	☐	4	[Guest Operator Logins]	Application	Aruba Application Authentication	0	✓
5.	☐	5	[Insight Operator Logins]	Application	Aruba Application Authentication	0	✓
6.	☐	6	[Device Registration Disconnect]	WEBAUTH	Web-based Authentication	0	✓
7.	☐	7	OWL_CorpNet 802.1X Service	RADIUS	Aruba 802.1X Wireless	0	✓

Showing 1-7 of 7

Figure 87: Add Wired CX RADIUS Service

Step 4 In the new **Services** screen, under the **Services** tab, configure the following, then click the **Next** button. - **Type:** *802.1X Wired* - **Name:** *OWL_Wired CX 802.1X Service* - Add **Service Rule 3:** - **Type:** *Connection* - **Name:** *NAD-IP-Address* - **Operator:** *BELONGS_TO_GROUP* - **Value:** *Switches*



Configuration » Services » Add

Services

Type: 802.1X Wired

Name: OWL_Wired CX 802.1X Service

Description: 802.1X Wired Access Service

Monitor Mode: ☐ Enable to monitor network access without enforcement

More Options: ☐ Authorization ☐ Posture Compliance ☐ Audit End-hosts ☐ Profile Endpoints ☐ Accounting Proxy

Service Rule

Matches ○ ANY or ● ALL of the following conditions:

	Type	Name	Operator	Value
1.	Radius:IETF	NAS-Port-Type	EQUALS	Ethernet (15)
2.	Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Framed-User (2), Authenticate-Only (8)
	Connection	NAD-IP-Address	BELONGS_TO_GROUP	Switches
4.	*Click to add...*			

Figure 88: Wired CX Service Tab

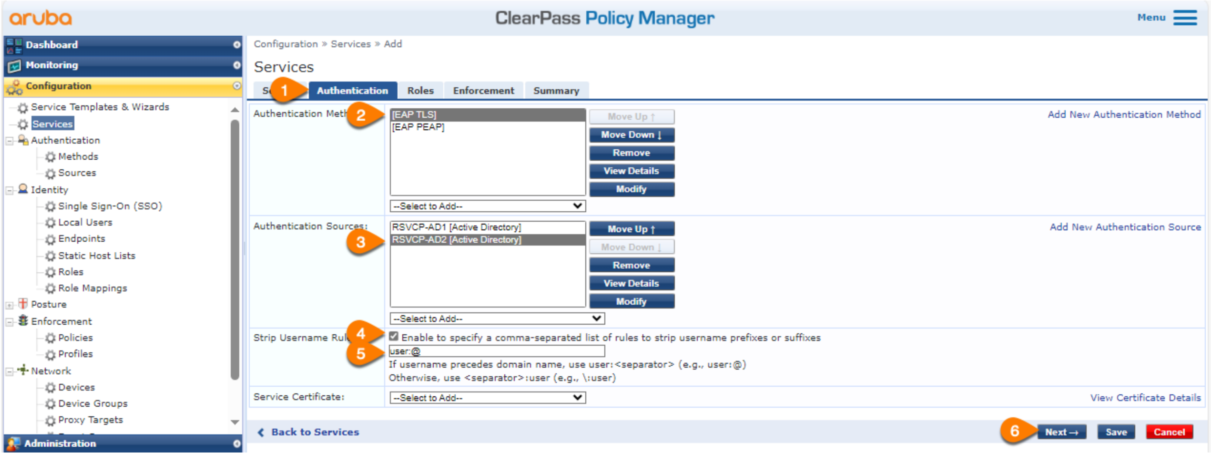
Step 5 In the **Authentication** tab, configure the following, then click the **Next** button.

- **Authentication Methods:**
  - EAP-TLS

  - [EAP PEAP]

- **Authentication Sources:**
  - *RSVCP-AD1*
  - *RSVCP-AD2*

- **Strip Username Rules:**
  - (Check the box to enable)
  - *User:@*



Authentication Meth: [EAP TLS] [EAP PEAP] --Select to Add--

Authentication Sources: RSVCP-AD1 [Active Directory] RSVCP-AD2 [Active Directory] --Select to Add--

Strip Username Rul: ☑ Enable to specify a comma-separated list of rules to strip username prefixes or suffixes

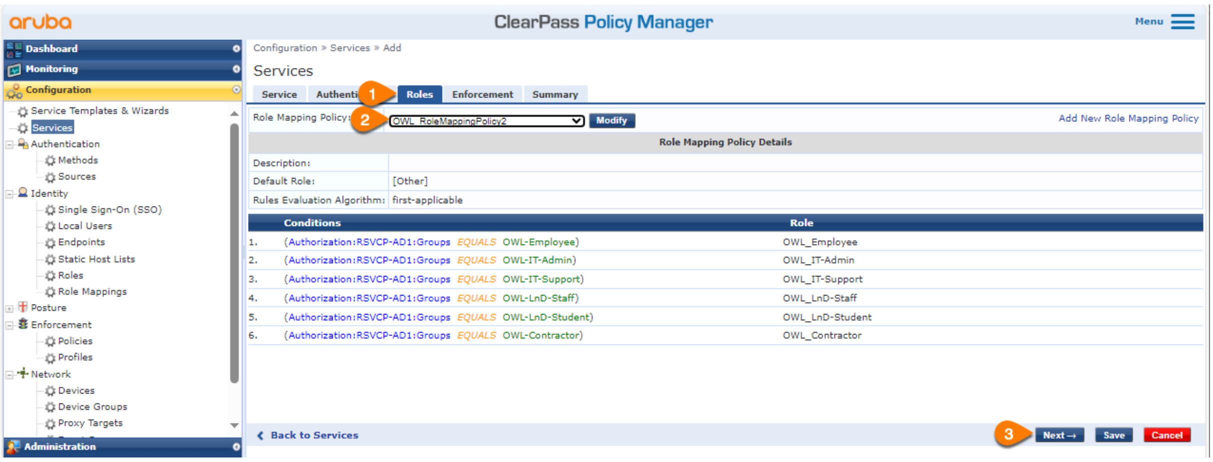
user:@

If username precedes domain name, use user:<separator> (e.g., user:@)
Otherwise, use <separator>:user (e.g., \:user)

Service Certificate: --Select to Add--

Figure 89: Wired CX Authentication Tab

Step 6 In the **Roles** tab, select *OWL_RoleMappingPolicy2* from the **Role Mapping Policy** dropdown, then click the **Next** button.



Role Mapping Policy: OWL_RoleMappingPolicy2

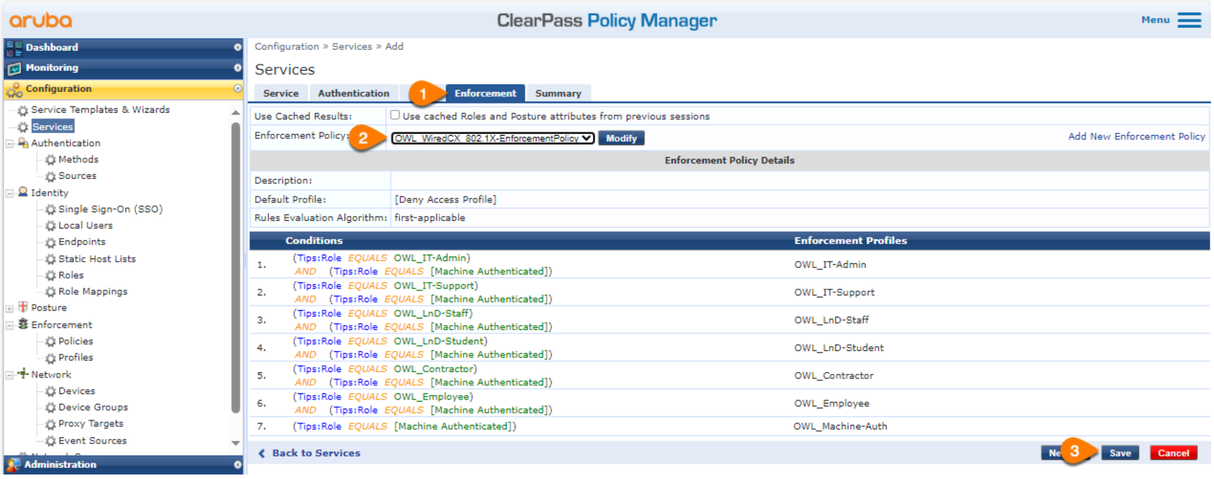
Role Mapping Policy Details

Description:	
Default Role:	[Other]
Rules Evaluation Algorithm:	first-applicable

	Conditions	Role
1.	(Authorization:RSVCP-AD1:Groups *EQUALS* OWL-Employee)	OWL_Employee
2.	(Authorization:RSVCP-AD1:Groups *EQUALS* OWL-IT-Admin)	OWL_IT-Admin
3.	(Authorization:RSVCP-AD1:Groups *EQUALS* OWL-IT-Support)	OWL_IT-Support
4.	(Authorization:RSVCP-AD1:Groups *EQUALS* OWL-LnD-Staff)	OWL_LnD-Staff
5.	(Authorization:RSVCP-AD1:Groups *EQUALS* OWL-LnD-Student)	OWL_LnD-Student
6.	(Authorization:RSVCP-AD1:Groups *EQUALS* OWL-Contractor)	OWL_Contractor

Figure 90: Wired CX Roles Tab

Step 7 In the **Enforcement** tab, select *OWL_WiredCX_802.1X_EnforcementPolicy* from the **Enforcement Policy** dropdown, then click the **Save** button.



Use Cached Results: □ Use cached Roles and Posture attributes from previous sessions

Enforcement Policy: OWL_WiredCX_802.1X-EnforcementPolicy

Enforcement Policy Details

Description:

Default Profile: [Deny Access Profile]

Rules Evaluation Algorithm: first-applicable

	Conditions	Enforcement Profiles
1.	(Tips:Role EQUALS OWL_IT-Admin) AND (Tips:Role EQUALS [Machine Authenticated])	OWL_IT-Admin
2.	(Tips:Role EQUALS OWL_IT-Support) AND (Tips:Role EQUALS [Machine Authenticated])	OWL_IT-Support
3.	(Tips:Role EQUALS OWL_LnD-Staff) AND (Tips:Role EQUALS [Machine Authenticated])	OWL_LnD-Staff
4.	(Tips:Role EQUALS OWL_LnD-Student) AND (Tips:Role EQUALS [Machine Authenticated])	OWL_LnD-Student
5.	(Tips:Role EQUALS OWL_Contractor) AND (Tips:Role EQUALS [Machine Authenticated])	OWL_Contractor
6.	(Tips:Role EQUALS OWL_Employee) AND (Tips:Role EQUALS [Machine Authenticated])	OWL_Employee
7.	(Tips:Role EQUALS [Machine Authenticated])	OWL_Machine-Auth

Figure 91: Wired CX Enforcement Tab

Step 8 When complete, proceed to next section.

Configure Wired MAC Authentication

In this deployment, the MAC Auth service uses the Endpoint Repository and DHCP profiling to provide different authorization levels for headless devices such as printers, phones, access points, and others.

Note that the workflow for this setup requires creating Role Mapping and Enforcement Policies before adding the actual service.

Follow the steps below to configure this service.

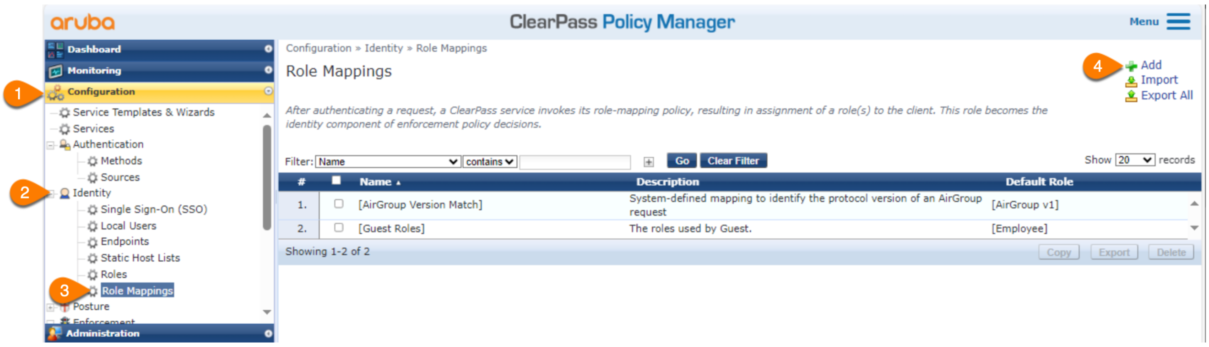
Configure ClearPass Roles for Role Mapping Policy

The ClearPass Roles created for the CorpNet Role Mapping Policy earlier in this chapter are used for this configuration.

Configure Role Mapping Policy

Configure a new Role Mapping Policy for the MAC authentication service.

Step 1 Go to **Configuration** > **Identity** > **Role Mappings** and click the **Add** link at the upper right.



Configuration » Identity » Role Mappings

Role Mappings

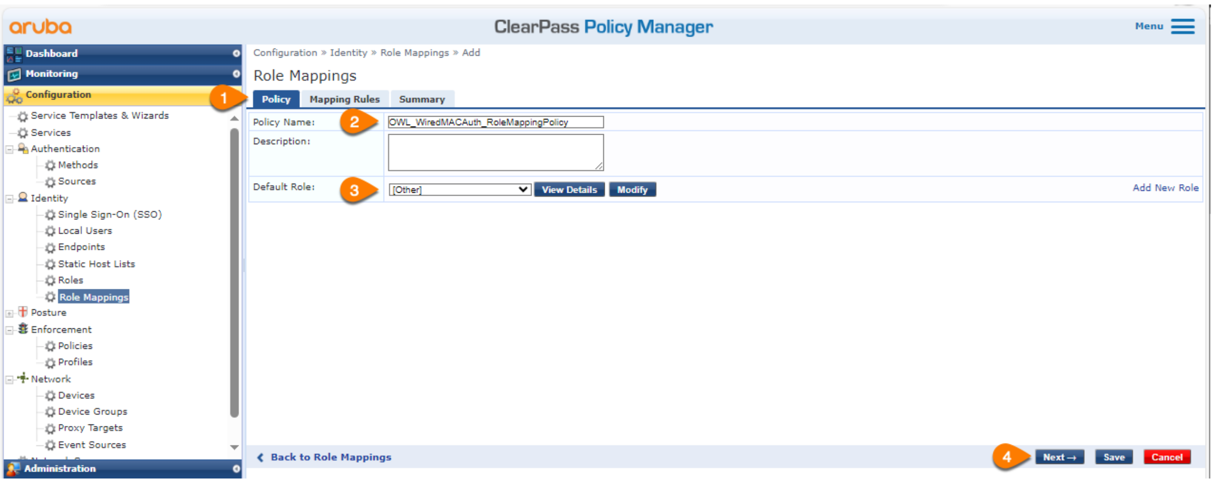
After authenticating a request, a ClearPass service invokes its role-mapping policy, resulting in assignment of a role(s) to the client. This role becomes the identity component of enforcement policy decisions.

#	☐	Name ▴	Description	Default Role
1.	☐	[AirGroup Version Match]	System-defined mapping to identify the protocol version of an AirGroup request	[AirGroup v1]
2.	☐	[Guest Roles]	The roles used by Guest.	[Employee]

Showing 1-2 of 2

Figure 92: Add Role Mapping Policy

Step 2 In the **Role Mappings** window, under the **Policy** tab, configure the following, then click the **Next** button. - **Policy Name:** *OWL_WiredMACAuth_RoleMappingPolicy* - **Default Role:** *[Other]*



Configuration » Identity » Role Mappings » Add

Role Mappings

Policy Name: OWL_WiredMACAuth_RoleMappingPolicy

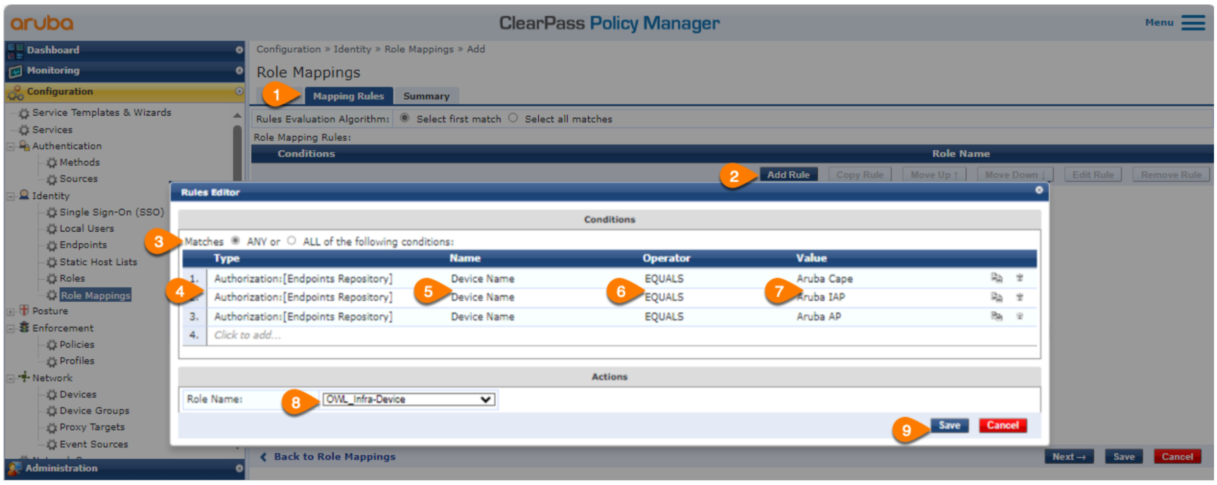
Description:

Default Role: [Other]

Figure 93: MAC Auth Role Mapping Policy Tab

Step 3 In the **Mapping Rules** tab, click the **Add Rule** button and configure the following on the **Rules Editor** window. - **Matches:** *ANY* - **Type:** *Authorization:[Endpoints Repository]* for all rules - **Name:** *Device Name* for all rules - **Operator:** *EQUALS* for all rules - **Value:** *Aruba Cape* for the first rule, *Aruba IAP* for the second, and Aruba AP for the third - **Role Name:** *OWL_Infra-Device*

Step 4 When all conditions and actions are configured similar to the image below, click **Save**.



Configuration » Identity » Role Mappings » Add

Role Mappings

Mapping Rules | Summary

Rules Evaluation Algorithm: ● Select first match ○ Select all matches

Role Mapping Rules:

Conditions	Role Name

Rules Editor

Conditions

Matches ● ANY or ○ ALL of the following conditions:

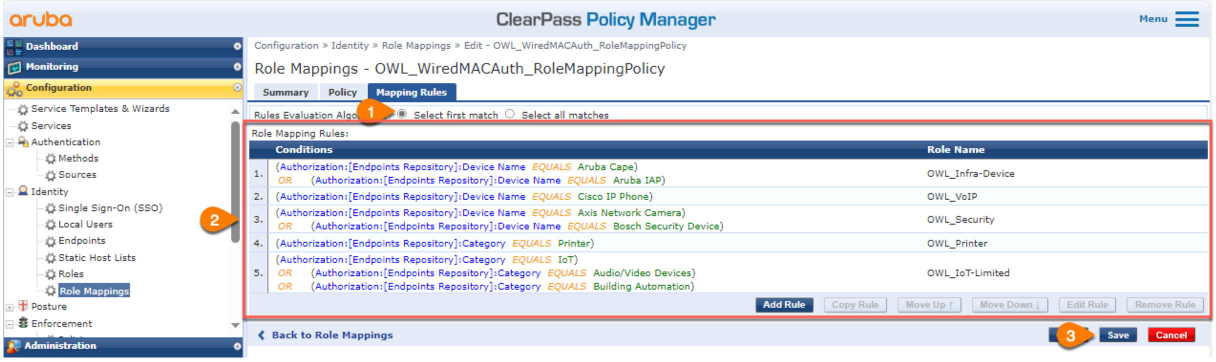
	Type	Name	Operator	Value
1.	Authorization:[Endpoints Repository]	Device Name	EQUALS	Aruba Cape
2.	Authorization:[Endpoints Repository]	Device Name	EQUALS	Aruba IAP
3.	Authorization:[Endpoints Repository]	Device Name	EQUALS	Aruba AP
4.	Click to add...			

Actions

Role Name: OWL_Infra-Device

Figure 94: MAC Auth Role Mapping Rules Tab

Step 5 Repeat the two previous steps until the Role Mapping Rules list matches the screenshot below.



Configuration » Identity » Role Mappings » Edit - OWL_WiredMACAuth_RoleMappingPolicy

Role Mappings - OWL_WiredMACAuth_RoleMappingPolicy

Summary | Policy | Mapping Rules

Rules Evaluation Algo ● Select first match ○ Select all matches

Role Mapping Rules:

	Conditions	Role Name
1.	(Authorization:[Endpoints Repository]:Device Name EQUALS Aruba Cape) OR (Authorization:[Endpoints Repository]:Device Name EQUALS Aruba IAP)	OWL_Infra-Device
2.	(Authorization:[Endpoints Repository]:Device Name EQUALS Cisco IP Phone)	OWL_VoIP
3.	(Authorization:[Endpoints Repository]:Device Name EQUALS Axis Network Camera) OR (Authorization:[Endpoints Repository]:Device Name EQUALS Bosch Security Device)	OWL_Security
4.	(Authorization:[Endpoints Repository]:Category EQUALS Printer)	OWL_Printer
5.	(Authorization:[Endpoints Repository]:Category EQUALS IoT) OR (Authorization:[Endpoints Repository]:Category EQUALS Audio/Video Devices) OR (Authorization:[Endpoints Repository]:Category EQUALS Building Automation)	OWL_IoT-Limited

Figure 95: MAC Auth Role Mapping Rules Tab 2

NOTE:

The Role Mapping Rules in this example and in the rest of this guide are specific for Orange Widget Logistics, the example customer in the VSG reference architecture. For additional configuration options, see the Adding and Modifying Role Mapping Policies section of the CPPM User Guide.

Step 6 Proceed to the next section.

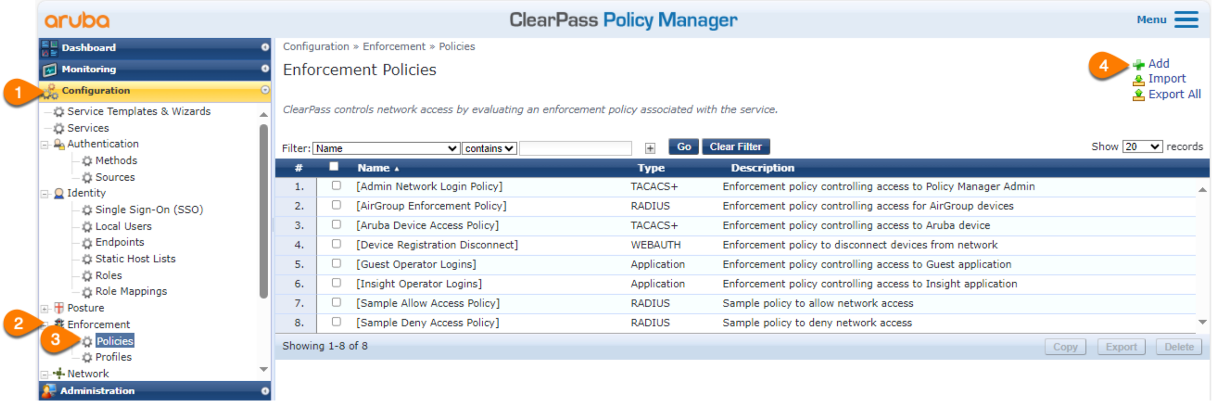
Configure Enforcement Profiles for Enforcement Policy

The Enforcement Profiles created for the CorpNet Enforcement Policy earlier in this chapter are used for this configuration.

Configure Enforcement Policy

Follow the steps below to configure the Enforcement Policy for the wired MAC authentication service.

Step 1 Go to **Configuration** > **Enforcement** > **Policies** and click the **Add** link at the upper right.



Configuration » Enforcement » Policies

Enforcement Policies

ClearPass controls network access by evaluating an enforcement policy associated with the service.

Filter: Name contains

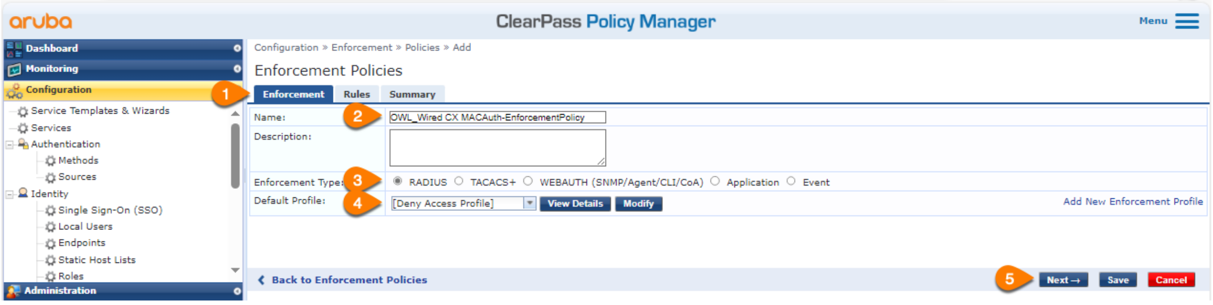
Show 20 records

#	☐	Name ▲	Type	Description
1.	☐	[Admin Network Login Policy]	TACACS+	Enforcement policy controlling access to Policy Manager Admin
2.	☐	[AirGroup Enforcement Policy]	RADIUS	Enforcement policy controlling access for AirGroup devices
3.	☐	[Aruba Device Access Policy]	TACACS+	Enforcement policy controlling access to Aruba device
4.	☐	[Device Registration Disconnect]	WEBAUTH	Enforcement policy to disconnect devices from network
5.	☐	[Guest Operator Logins]	Application	Enforcement policy controlling access to Guest application
6.	☐	[Insight Operator Logins]	Application	Enforcement policy controlling access to Insight application
7.	☐	[Sample Allow Access Policy]	RADIUS	Sample policy to allow network access
8.	☐	[Sample Deny Access Policy]	RADIUS	Sample policy to deny network access

Showing 1-8 of 8

Figure 96: Add Enforcement Policy

Step 2 In the **Add Enforcement Policies** window, in the **Enforcement** tab, configure the following, then click the **Next** button. - **Name:** *OWL_Wired CX MACAuth-EnforcementPolicy* - **Enforcement Type:** *RADIUS* - **Default Profile:** *[Deny Access Policy]*



Configuration » Enforcement » Policies » Add

Enforcement Policies

Name: OWL_Wired CX MACAuth-EnforcementPolicy

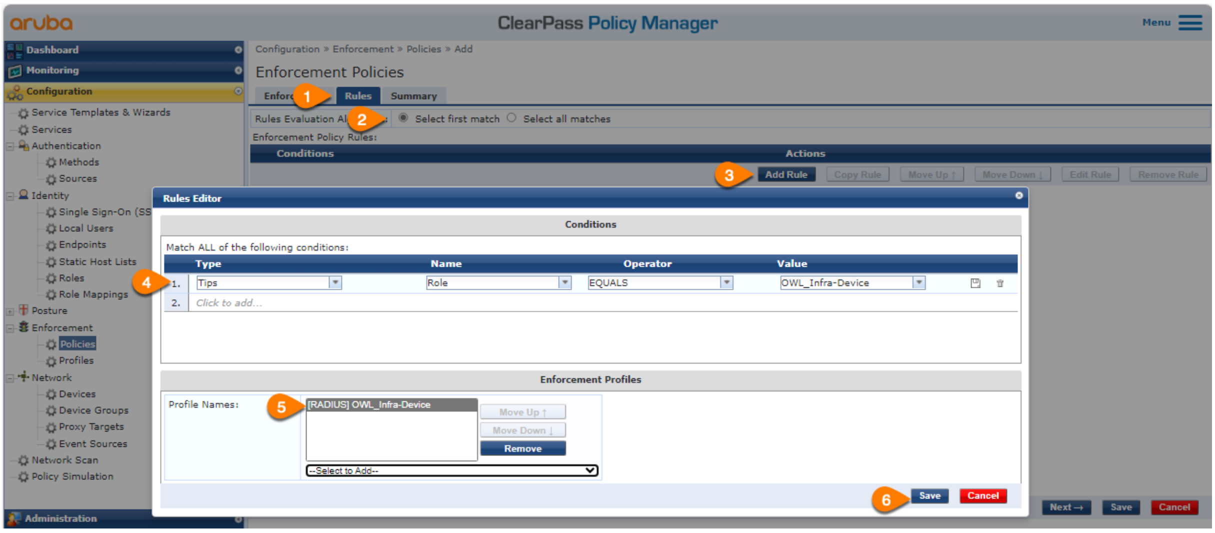
Description:

Enforcement Type: ● RADIUS ○ TACACS+ ○ WEBAUTH (SNMP/Agent/CLI/CoA) ○ Application ○ Event

Default Profile: [Deny Access Profile]

Figure 97: Wired MAC Auth Policy Enforcement Tab

Step 3 In the **Rules** tab, click the **Add Rule** button. In the **Rules Editor** window, configure the following, then click the **Save** button.



Configuration » Enforcement » Policies » Add

Enforcement Policies

Rules Evaluation Al: ● Select first match ○ Select all matches

Enforcement Policy Rules:

Conditions

Match ALL of the following conditions:

	Type	Name	Operator	Value
1.	Tips	Role	EQUALS	OWL_Infra-Device
2.	*Click to add...*			

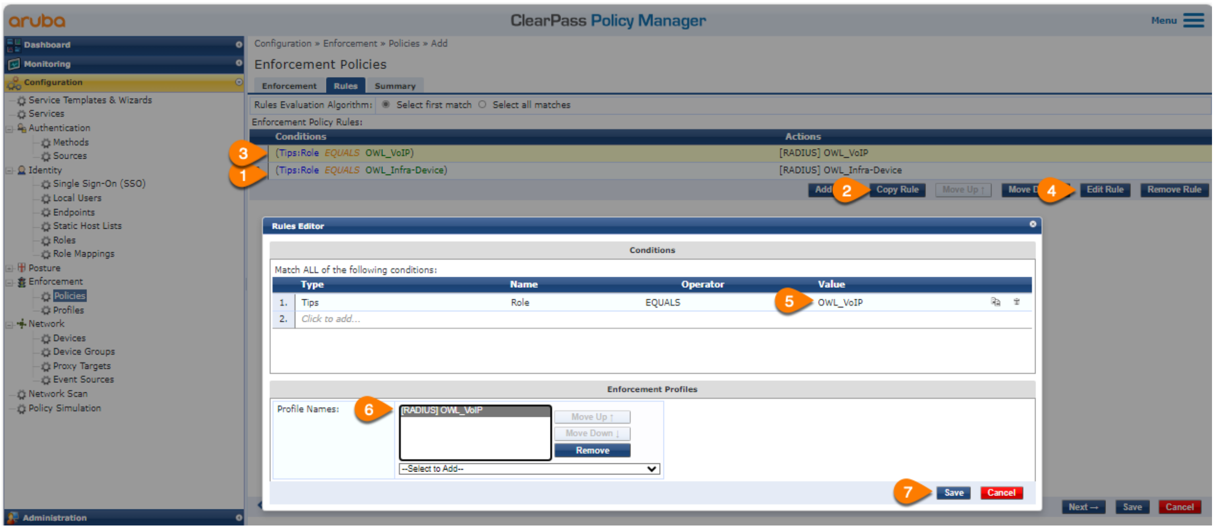
Enforcement Profiles

Profile Names: [RADIUS] OWL_Infra-Device

--Select to Add--

Figure 98: Enforcement Policy Rules Tab

Step 4 After the first rule is saved, click the **Copy Rule** button to create the second rule as follows: - Select the newly created rule for *OWL_Infra-Device* - Click the **Copy Rule** button - Select the newly duplicated rule - Click the **Edit Rule** button - Change the **Value** column condition 1 to *OWL_VoIP* - Replace the **Profile Name** with *OWL_VoIP* - Click the **Save** button



Rules Evaluation Algorithm: ● Select first match ○ Select all matches

Enforcement Policy Rules:

Conditions	Actions
(Tips:Role EQUALS OWL_VoIP)	[RADIUS] OWL_VoIP
(Tips:Role EQUALS OWL_Infra-Device)	[RADIUS] OWL_Infra-Device

Conditions

Match ALL of the following conditions:

	Type	Name	Operator	Value
1.	Tips	Role	EQUALS	OWL_VoIP
2.	Click to add...			

Enforcement Profiles

Profile Names: [RADIUS] OWL_VoIP

Figure 99: Enforcement Policy Copy Rule

Step 5 Repeat the previous step until the enforcement rules below are entered, then click the **Save** button.

Type	Profile Names
Tips Role equals OWL_VoIP	[RADIUS] OWL_VoIP
Tips Role equals OWL_Infra-Device	[RADIUS] OWL_Infra-Device
Tips Role equals OWL_Printer	[RADIUS] OWL_Printer
Tips Role equals OWL_IoT-Limited	[RADIUS] OWL_IoT-Limited
Tips Role equals OWL_Security	[RADIUS] OWL_Security

Step 6 When complete, proceed to the next section.

Configure Service

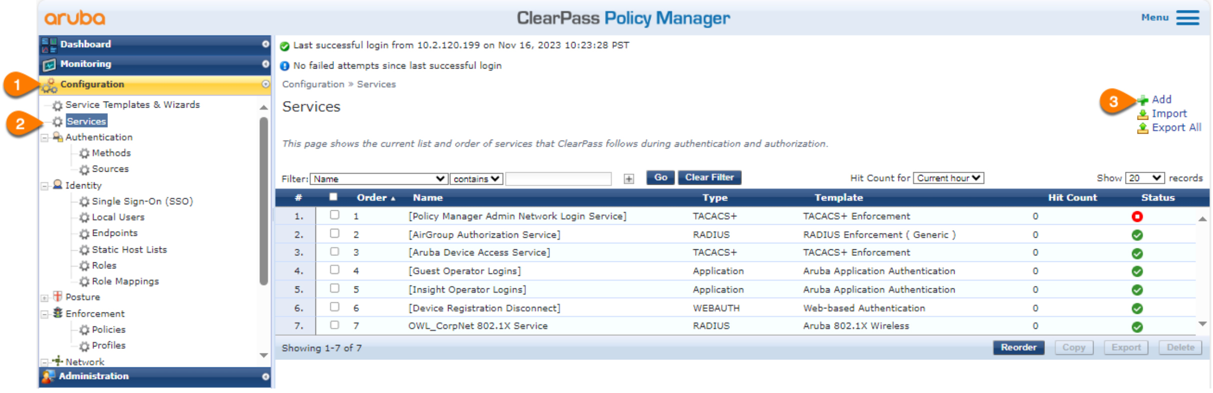
Follow the steps below to configure the wired MAC authentication service for OWL's CX switches.

Step 1 Open a web browser and connect to the publisher node, RSVCP-CPPM-1.

Step 2 Log in using the admin credentials.

- **Username:** *admin*
- **Password:** *Aruba123!*

Step 3 Go to **Configuration** > **Services** and click the **Add** link at the upper right.



Last successful login from 10.2.120.199 on Nov 16, 2023 10:23:28 PST

No failed attempts since last successful login

Configuration » Services

Services

This page shows the current list and order of services that ClearPass follows during authentication and authorization.

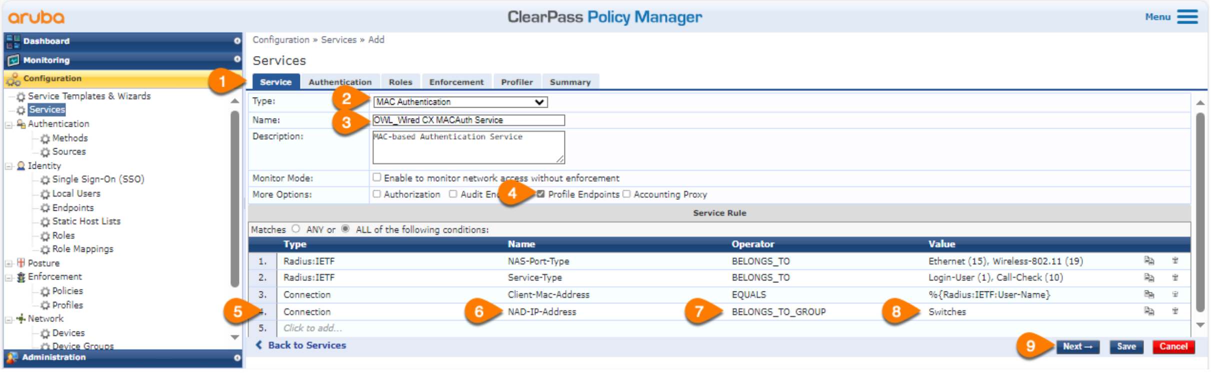
Filter: Name contains | Hit Count for Current hour | Show 20 records

#	☐	Order ▴	Name	Type	Template	Hit Count	Status
1.	☐	1	[Policy Manager Admin Network Login Service]	TACACS+	TACACS+ Enforcement	0	🟥
2.	☐	2	[AirGroup Authorization Service]	RADIUS	RADIUS Enforcement (Generic)	0	✓
3.	☐	3	[Aruba Device Access Service]	TACACS+	TACACS+ Enforcement	0	✓
4.	☐	4	[Guest Operator Logins]	Application	Aruba Application Authentication	0	✓
5.	☐	5	[Insight Operator Logins]	Application	Aruba Application Authentication	0	✓
6.	☐	6	[Device Registration Disconnect]	WEBAUTH	Web-based Authentication	0	✓
7.	☐	7	OWL_CorpNet 802.1X Service	RADIUS	Aruba 802.1X Wireless	0	✓

Showing 1-7 of 7

Figure 100: Add Wired CX RADIUS Service

Step 4 In the new **Services** window, in the **Services** tab, configure the following: - **Type:** *MAC Authentication* - **Name:** *OWL_Wired CX MACAuth Service* - Add **Service Rule 3:** - **Type:** *Connection* - **Name:** *NAD-IP-Address* - **Operator:** *BELONGS_TO_GROUP* - **Value:** *Switches* - Click the **Next** button



Configuration » Services » Add

Services

Type: MAC Authentication

Name: OWL_Wired CX MACAuth Service

Description: MAC-based Authentication Service

Monitor Mode: ☐ Enable to monitor network access without enforcement

More Options: ☐ Authorization ☐ Audit En ☑ Profile Endpoints ☐ Accounting Proxy

Service Rule

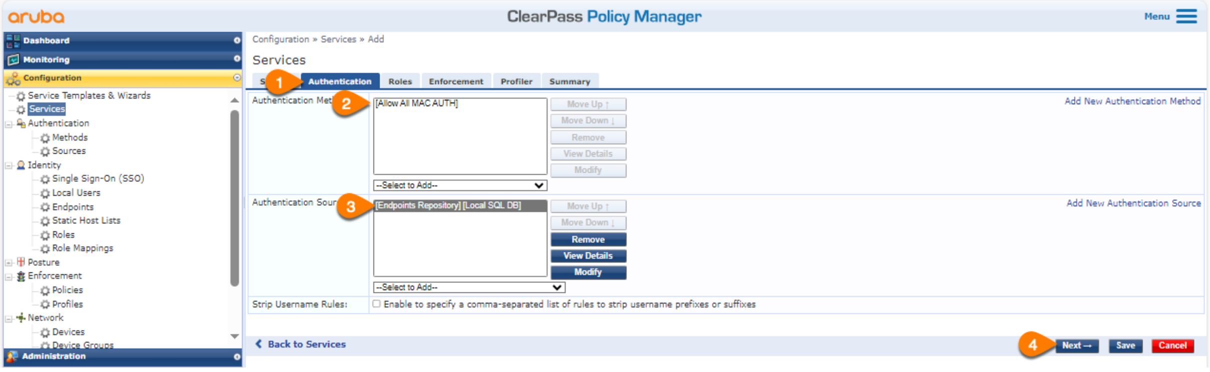
Matches ○ ANY or ● ALL of the following conditions:

	Type	Name	Operator	Value
1.	Radius:IETF	NAS-Port-Type	BELONGS_TO	Ethernet (15), Wireless-802.11 (19)
2.	Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Call-Check (10)
3.	Connection	Client-Mac-Address	EQUALS	%{Radius:IETF:User-Name}
4.	Connection	NAD-IP-Address	BELONGS_TO_GROUP	Switches
5.	*Click to add...*			

Figure 101: Wired CX MAC Auth Add

Step 5 In the **Authentication** tab, configure the following:

- **Authentication Methods:**
  - [Allow All MAC AUTH]
- **Authentication Sources:**
  - [Endpoints Repository] [Local SQL DB]
- Click the **Next** Button



Authentication Met: [Allow All MAC AUTH]

--Select to Add--

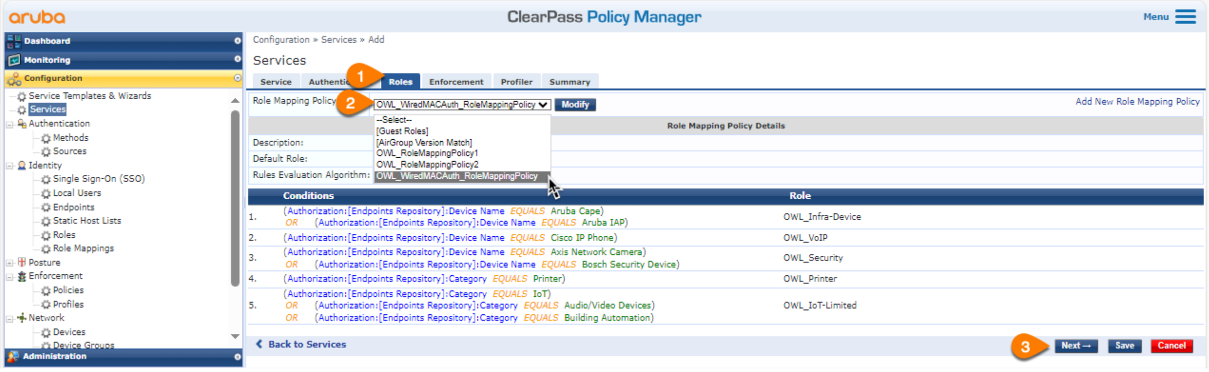
Authentication Sour: [Endpoints Repository] [Local SQL DB]

--Select to Add--

Strip Username Rules: □ Enable to specify a comma-separated list of rules to strip username prefixes or suffixes

Figure 102: Wired CX MAC Authentication Tab

Step 6 In the **Roles** tab, select *OWL_WiredMACAuth_RoleMappingPolicy* from the **Role Mapping Policy** dropdown, then click the **Next** button.



Role Mapping Policy: OWL_WiredMACAuth_RoleMappingPolicy

Role Mapping Policy Details

Description:

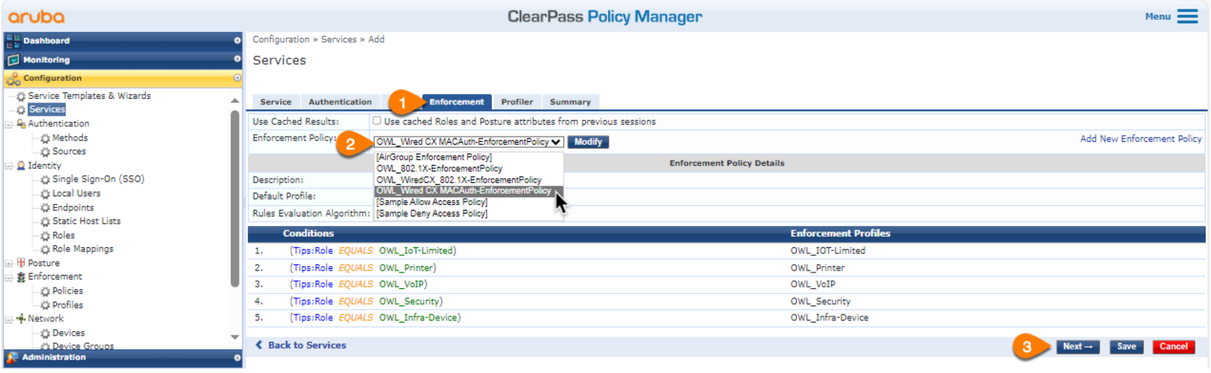
Default Role:

Rules Evaluation Algorithm:

	Conditions	Role
1.	(Authorization:[Endpoints Repository]:Device Name *EQUALS* Aruba Cape) *OR* (Authorization:[Endpoints Repository]:Device Name *EQUALS* Aruba IAP)	OWL_Infra-Device
2.	(Authorization:[Endpoints Repository]:Device Name *EQUALS* Cisco IP Phone)	OWL_VoIP
3.	(Authorization:[Endpoints Repository]:Device Name *EQUALS* Axis Network Camera) *OR* (Authorization:[Endpoints Repository]:Device Name *EQUALS* Bosch Security Device)	OWL_Security
4.	(Authorization:[Endpoints Repository]:Category *EQUALS* Printer)	OWL_Printer
5.	(Authorization:[Endpoints Repository]:Category *EQUALS* IoT) *OR* (Authorization:[Endpoints Repository]:Category *EQUALS* Audio/Video Devices) *OR* (Authorization:[Endpoints Repository]:Category *EQUALS* Building Automation)	OWL_IoT-Limited

Figure 103: Wired CX MAC Auth Roles Tab

Step 7 In the **Enforcement** tab, select *OWL_Wired CX MACAuth-EnforcementPolicy* from the **Enforcement Policy** dropdown, then click the **Next** button.



Use Cached Results: □ Use cached Roles and Posture attributes from previous sessions

Enforcement Policy: OWL_Wired CX MACAuth-EnforcementPolicy

Enforcement Policy Details

Description:

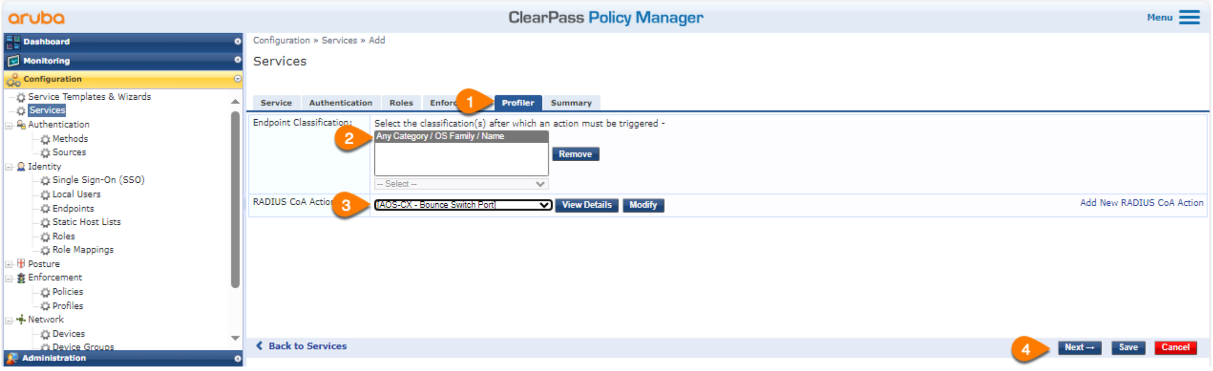
Default Profile:

Rules Evaluation Algorithm:

	Conditions	Enforcement Profiles
1.	(Tips:Role *EQUALS* OWL_IoT-Limited)	OWL_IOT-Limited
2.	(Tips:Role *EQUALS* OWL_Printer)	OWL_Printer
3.	(Tips:Role *EQUALS* OWL_VoIP)	OWL_VoIP
4.	(Tips:Role *EQUALS* OWL_Security)	OWL_Security
5.	(Tips:Role *EQUALS* OWL_Infra-Device)	OWL_Infra-Device

Figure 104: Wired CX MAC Auth Enforcement Tab

Step 8 In the **Profiler** tab, configure the following settings, then click the **Next** button: - **Endpoint Classification:** *Any Category/ OS Family/ Name* - **RADIUS CoA Action:** *[AOS-CX - Bounce Switch Port]*



Configuration » Services » Add

Services

Endpoint Classification: Select the classification(s) after which an action must be triggered - Any Category / OS Family / Name

-- Select --

RADIUS CoA Actio [AOS-CX - Bounce Switch Port]

Figure 105: Wired CX MAC Auth Profiler Tab

Step 9 Review the **Summary** tab, then proceed to next section.

Organize Services

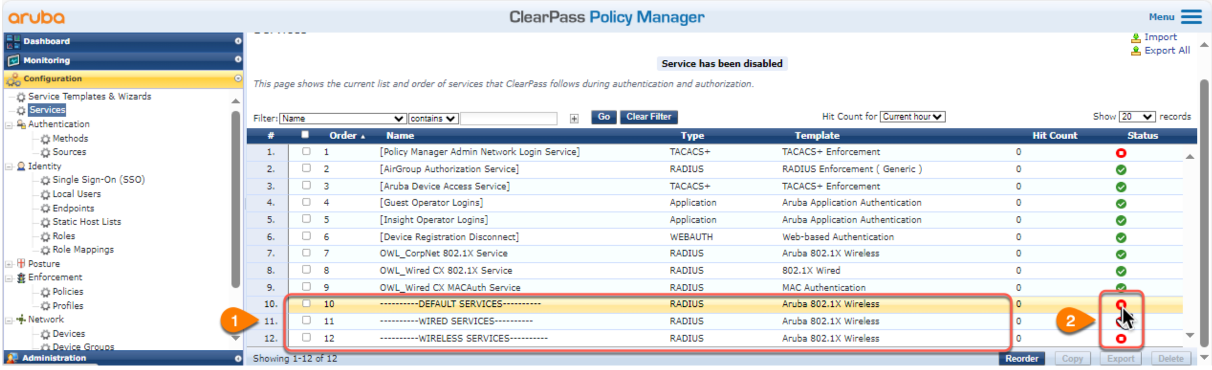
Because services process authentication requests from the top down, similar to an ACL, it is essential to organize them in a way that is most effective for the deployment. Although the order is not critical for the three services created in this sample deployment, it is important to begin with a well organized set of services to facilitate troubleshooting and expansion of services as more sites are deployed or new services are tested.

One method to organize services is to create service "separators," as described in the next section.

Create Service "Separators"

Separators optional, but recommended. They keep services grouped and make them easier to sort when troubleshooting.

Step 1 Pick any existin services and duplicate it with the **Copy** button. Then, rename it. Repeat until the three services below are created.



Service has been disabled

This page shows the current list and order of services that ClearPass follows during authentication and authorization.

Filter: Name contains   Hit Count for Current hour   Show 20 records

#	■	Order ▲	Name	Type	Template	Hit Count	Status
1.	□	1	[Policy Manager Admin Network Login Service]	TACACS+	TACACS+ Enforcement	0	○
2.	□	2	[AirGroup Authorization Service]	RADIUS	RADIUS Enforcement (Generic)	0	✓
3.	□	3	[Aruba Device Access Service]	TACACS+	TACACS+ Enforcement	0	✓
4.	□	4	[Guest Operator Logins]	Application	Aruba Application Authentication	0	✓
5.	□	5	[Insight Operator Logins]	Application	Aruba Application Authentication	0	✓
6.	□	6	[Device Registration Disconnect]	WEBAUTH	Web-based Authentication	0	✓
7.	□	7	OWL_CorpNet 802.1X Service	RADIUS	Aruba 802.1X Wireless	0	✓
8.	□	8	OWL_Wired CX 802.1X Service	RADIUS	802.1X Wired	0	✓
9.	□	9	OWL_Wired CX MACAuth Service	RADIUS	MAC Authentication	0	✓
10.	□	10	----------DEFAULT SERVICES----------	RADIUS	Aruba 802.1X Wireless	0	○
11.	□	11	----------WIRED SERVICES----------	RADIUS	Aruba 802.1X Wireless	0	○
12.	□	12	----------WIRELESS SERVICES----------	RADIUS	Aruba 802.1X Wireless	0	○

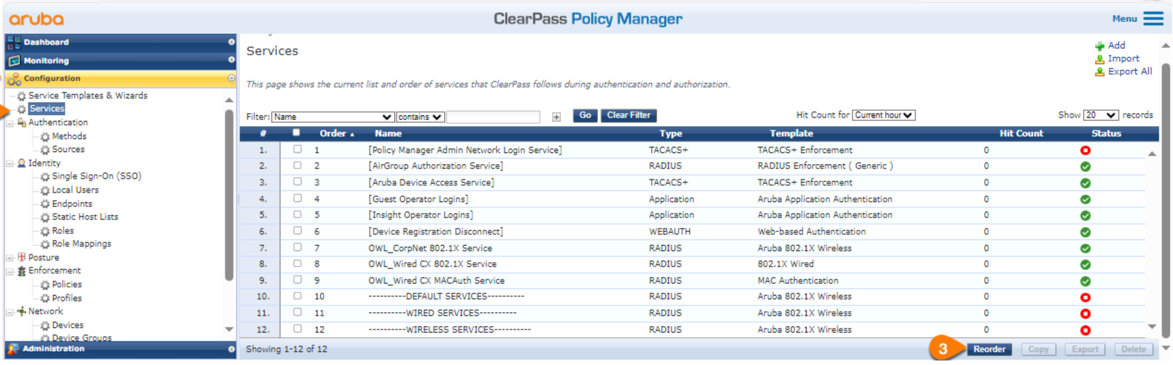
Showing 1-12 of 12

Figure 106: Service Separators

Step 2 Ensure that the newly created "separator" services are disabled, as shown in the image above, to prevent ClearPass from using them to process requests.

Reorder Services

Step 1 After the “separator” services are disabled, click the **Reorder** button at the lower right.



Services

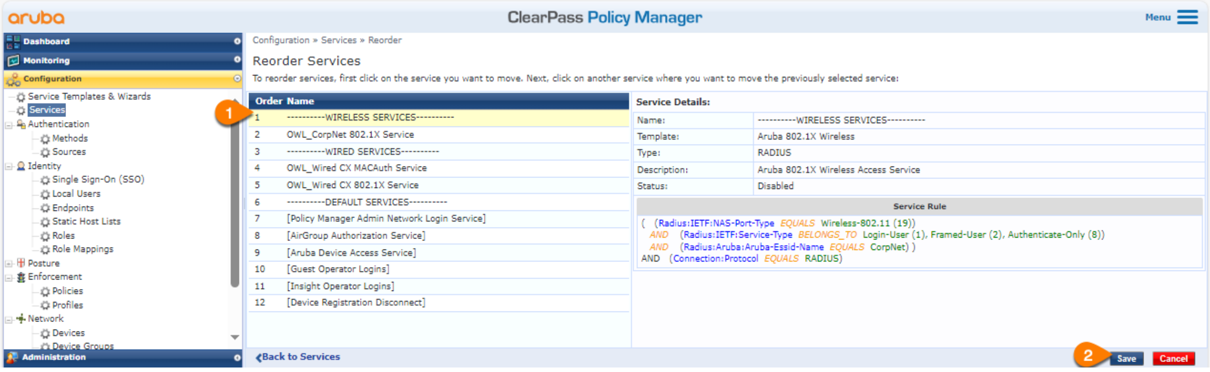
This page shows the current list and order of services that ClearPass follows during authentication and authorization.

#	■	Order ▲	Name	Type	Template	Hit Count	Status
1.	□	1	[Policy Manager Admin Network Login Service]	TACACS+	TACACS+ Enforcement	0	○
2.	□	2	[AirGroup Authorization Service]	RADIUS	RADIUS Enforcement (Generic)	0	✓
3.	□	3	[Aruba Device Access Service]	TACACS+	TACACS+ Enforcement	0	✓
4.	□	4	[Guest Operator Logins]	Application	Aruba Application Authentication	0	✓
5.	□	5	[Insight Operator Logins]	Application	Aruba Application Authentication	0	✓
6.	□	6	[Device Registration Disconnect]	WEBAUTH	Web-based Authentication	0	✓
7.	□	7	OWL_CorpNet 802.1X Service	RADIUS	Aruba 802.1X Wireless	0	✓
8.	□	8	OWL_Wired CX 802.1X Service	RADIUS	802.1X Wired	0	✓
9.	□	9	OWL_Wired CX MACAuth Service	RADIUS	MAC Authentication	0	✓
10.	□	10	----------DEFAULT SERVICES----------	RADIUS	Aruba 802.1X Wireless	0	○
11.	□	11	----------WIRED SERVICES----------	RADIUS	Aruba 802.1X Wireless	0	○
12.	□	12	----------WIRELESS SERVICES----------	RADIUS	Aruba 802.1X Wireless	0	○

Showing 1-12 of 12

Figure 107: Service Reoder

Step 2 In the **Reorder** window, left-click and release the first service to be moved, move the cursor to the desired location, and then click again to release the service in the intended place.



Configuration » Services » Reorder

Reorder Services

To reorder services, first click on the service you want to move. Next, click on another service where you want to move the previously selected service:

Order	Name
1	----------WIRELESS SERVICES----------
2	OWL_CorpNet 802.1X Service
3	----------WIRED SERVICES----------
4	OWL_Wired CX MACAuth Service
5	OWL_Wired CX 802.1X Service
6	----------DEFAULT SERVICES----------
7	[Policy Manager Admin Network Login Service]
8	[AirGroup Authorization Service]
9	[Aruba Device Access Service]
10	[Guest Operator Logins]
11	[Insight Operator Logins]
12	[Device Registration Disconnect]

Service Details:

Name:	----------WIRELESS SERVICES----------
Template:	Aruba 802.1X Wireless
Type:	RADIUS
Description:	Aruba 802.1X Wireless Access Service
Status:	Disabled

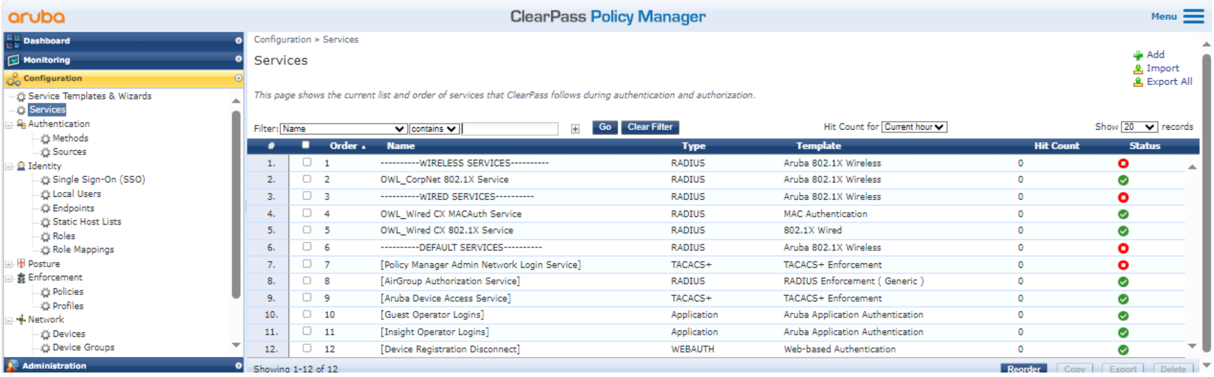
Service Rule

```
(  (Radius:IETF:NAS-Port-Type  EQUALS  Wireless-802.11 (19))
   AND  (Radius:IETF:Service-Type  BELONGS_TO  Login-User (1), Framed-User (2), Authenticate-Only (8))
   AND  (Radius:Aruba:Aruba-Essid-Name  EQUALS  CorpNet) )
AND  (Connection:Protocol  EQUALS  RADIUS)
```

Figure 108: Service Reorder 2

Step 3 Repeat this step until the order looks similar to the image above.

Step 4 When the reorder is complete, the services should look like the screenshot below.



Configuration » Services

Services

This page shows the current list and order of services that ClearPass follows during authentication and authorization.

#	■	Order ▲	Name	Type	Template	Hit Count	Status
1.	□	1	----------WIRELESS SERVICES----------	RADIUS	Aruba 802.1X Wireless	0	○
2.	□	2	OWL_CorpNet 802.1X Service	RADIUS	Aruba 802.1X Wireless	0	✓
3.	□	3	----------WIRED SERVICES----------	RADIUS	Aruba 802.1X Wireless	0	○
4.	□	4	OWL_Wired CX MACAuth Service	RADIUS	MAC Authentication	0	✓
5.	□	5	OWL_Wired CX 802.1X Service	RADIUS	802.1X Wired	0	✓
6.	□	6	----------DEFAULT SERVICES----------	RADIUS	Aruba 802.1X Wireless	0	○
7.	□	7	[Policy Manager Admin Network Login Service]	TACACS+	TACACS+ Enforcement	0	○
8.	□	8	[AirGroup Authorization Service]	RADIUS	RADIUS Enforcement (Generic)	0	✓
9.	□	9	[Aruba Device Access Service]	TACACS+	TACACS+ Enforcement	0	✓
10.	□	10	[Guest Operator Logins]	Application	Aruba Application Authentication	0	✓
11.	□	11	[Insight Operator Logins]	Application	Aruba Application Authentication	0	✓
12.	□	12	[Device Registration Disconnect]	WEBAUTH	Web-based Authentication	0	✓

Showing 1-12 of 12

Figure 109: Service Reorder 3

Step 5 Proceed to the next section.

Verify Switch Configuration

The following sections contain the base configuration expected for AOS-CX switches to authenticate wired clients against the RADIUS services configured in this guide. For instructions on configuring the switches, see the Configure RADIUS and UBT section of the Wired Access Configuration page in the Campus Deploy guide.

Global RADIUS Configuration

Verify that the following global RADIUS configuration exists.

```
radius-server host 10.2.120.192 key plaintext Aruba123!
radius-server host 10.2.120.193 key plaintext Aruba123!

aaa group server radius clearpass_radius_group
    server 10.2.120.192
    server 10.2.120.193

aaa accounting port-access start-stop interim 60 group clearpass_radius_group

radius dyn-authorization enable

radius dyn-authorization client 10.2.120.194 secret-key Aruba123!
radius dyn-authorization client 10.2.120.195 secret-key Aruba123!

aaa authentication port-access dot1x authenticator
    radius server-group clearpass_radius_group
    enable
aaa authentication port-access mac-auth
    radius server-group clearpass_radius_group
    enable
```

The table below provides brief descriptions of each configuration section above.

Configuration	Description
radius-server host 10.2.120.192 key plaintext Aruba123!radius-server host 10.2.120.193 key plaintext Aruba123!	Adds the RADIUS server virtual IP addresses along with shared secret.
aaa group server radius clearpass_radius_group server 10.2.120.192 server 10.2.120.193	Creates a AAA server group with name and adds the newly added RADIUS servers to it.
aaa accounting port-access start-stop interim 60 group clearpass_radius_group	Configures the new RADIUS server group to send accounting records at the beginning and end of each user/device session, as well as interim updates every 60 seconds.
radius dyn-authorization enable	Enables CoA

Configuration	Description
radius dyn-authorization client 10.2.120.194 secret-key Aruba123!radius dyn-authorization client 10.2.120.195 secret-key Aruba123!	Configures the switch to accept and process dynamic authorization requests sourced from the RADIUS servers' IP addresses (not VRRP virtual IPs).
aaa authentication port-access dot1x authenticator radius server-group clearpass_radius_group enable	Enables 802.1X authentication and configures authentication requests to be sent to RADIUS server group **clearpass_radius_group**
aaa authentication port-access mac-auth radius server-group clearpass_radius_group enable	Enables MAC authentication and configures authentication requests to be sent to RADIUS server group **clearpass_radius_group**

Switch Port Configuration

Verify that the following configuration exists on the ports expected to authenticate wired clients.

```
interface 1/1/1
    aaa authentcation port-access client-limit 3
    aaa authentication port-access onboarding-method concurrent enable
    aaa authentication port-access dot1x authenticator
        max-eapol-requests 1
        max-retries 1
        reauth
        enable
    aaa authentication port-access mac-auth
        cached-reauth
        cached-reauth-period 86400
        quiet-period 30
        enable
```

The table below provides brief descriptions of each configuration section above.

Configuration	Description
aaa authentcation port-access client-limit 3	Sets the port to authenticate a maximum of three clients
aaa authentication port-access onboarding-method concurrent enable	Configures the port to use 802.1X and MAC authentication simultaneously
aaa authentication port-access dot1x authenticator	Opens the configuration subsection for 802.1X
max-eapol-requests 1	Sets port to only send one EAPOL request to the client. If the client does not respond to the single request, the authentication process is considered failed.

Configuration	Description
max-retries 1	Sets the maximum number of times the switch reattempts the authentication process after a failure
reauth	Enables the switch to periodically reinitiate the authentication process to verify that the client should still be granted network access
enable	Enables 802.1X authentication on the port
aaa authentication port-access mac-auth	Opens the configuration subsection for MAC authentication
cached-reauth cached-reauth-period 86400	Configures the switch to cache the MAC address and use it to reauthenticate the client on the same port without going through full authentication if the device disconnects and reconnects during a period of 86400 seconds (24 hours).
quiet-period 30	Sets the duration during which the switch does not attempt to reauthenticate a device after a failed authentication attempt
enable	Enables MAC authentication on the port

This concludes ClearPass deployment guidance.

I AM HERE!!!!

aruba
a Hewlett Packard
Enterprise company

www.arubanetworks.com

3333 Scott Blvd. Santa Clara, CA 95054
1.844.472.2782 | T: 1.408.227.4500 | FAX: 1.408.227.4550