Wired Policy Enforcement

a Hewlett Packard Enterprise company

ClearPass

Solution Guide

Copyright

Change Log

Version	Date	Modified By	Comments
2018-01	2/9/18	Tim Cappalli Aruba Security Group	**MAJOR CHANGES** - [CW7] Added ClearPass OnConnect section - [CW7] Updated dynamic authorization references to use new H3C templates in 6.7 **MINOR CHANGES** - [AOS-S] corrected ordering of some commands - [AOS-S] added addr-limit config - [AOS-S] added SNMP server trap source - [AOS-S] updated DUR section to include standard mode added in 6.7 - [AOS-S] updated web auth service to use new page name attribute added in 6.7 - [Cisco] Added note about LAN base image - [Cisco] updated web auth service to use new page name attribute added in 6.7 - [CW7] updated web auth service to use new page name attribute added in 6.7
2017-02	7/31/17	Tim Cappalli Aruba Security Group	Added ArubaOS-Switch 16.04 features (downloadable user roles and per-user tunneled-node)
2017-01 (1.0)	6/2/17	Tim Cappalli Aruba Security Group	Initial release. ArubaOS-Switch 16.02, Comware 7, Cisco IOS 12/15 w/ IBNS1

Contents

The Building Blocks for Secure Access

There are four fundamental elements for building a secure, dynamic wired edge: Profiling, Authentication, Authorization and Posture.

Profiling

Understanding which devices are connecting to the network and what each of their capabilities are is critical to building a secure network policy. For example, Windows, macOS and most Linux distros have robust and flexible 802.1X supplicants that support secure user and device authentication, whereas most printers, media players, building controls, sensors and other headless devices do not support any interactive authentication methods.

Device profile information is also important for detecting unauthorized access to the network. If a user were to change the MAC address of their laptop to match a previously authenticated device, like a printer, for example, ClearPass will detect a profile change and trigger a conflict state.

Authentication

User and/or device identification enables dynamic network policies based on properties such as group, department, organizational structure, or owner. Authentication solutions can range from simplistic to complex, but flexible enough to meet the needs of an organization's security policy.

Authorization

The authorization phase is where most of the magic happens, regardless of the authentication method. Contextual information from all corners of the network and infrastructure can be evaluated to help make a policy decision. Some examples of contextual data sources include the user identity store, enterprise mobility management solutions, endpoint security solutions, asset management tools, the ClearPass device profile information, as well as nearly anything that has a SQL or API-based interface. The possibilities are endless and allow for robust, dynamic network security policies.

Posture

Posture can mean many different things in different environments. In a traditional "NAC" sense of the word, posture often refers to device health using some form of agent, whether persistent, dissolvable or embedded. This agent validates a predefined health policy that is used as part of authorization for network access. As more and more organizations deploy Enterprise Mobility Management (EMM) solutions for both corporate and personal assets, posture has evolved to included device data from these solutions.

In environments where traditional health status is not required for security or business requirements, profiling data can be viewed as a type of posture for the device. For example, a device that starts as a printer and becomes a Mac laptop creates a conflict condition which indicates some type of device posture change.

Technologies and Components

Standards and Technologies

802.1X

802.1X is a framework for port-based access control which is most commonly used with 802.3 Ethernet networks and 802.11 wireless LANs. There are three entities: supplicant (client device), authenticator (network device), and the authentication server (commonly a RADIUS server).

Additional information: http://www.ieee802.org/1/pages/802.1x-2010.html

EAP

EAP is the Extensible Authentication Protocol and is a framework for various authentication methods (known as EAP methods). EAP operates as part of the 802.1X framework at layer 2 prior to IP address assignment.

Additional information: https://tools.ietf.org/html/rfc3748

Common EAP Methods

There are over 40 EAP methods in the wild but the most popular and widely supported methods are EAP-TLS, PEAP and EAP-TTLS.

EAP-TLS (Transport Layer Security) is the gold standard in network authentication and uses mutual authentication with both server and client certificates. EAP-TLS is recommended for secure network authentication.

Additional information: https://tools.ietf.org/html/rfc5216

PEAP (Protected EAP) encapsulates other EAP methods inside a TLS tunnel and uses a server-side certificate for authentication server validation by the supplicant. Common inner methods include EAP-MSCHAPv2 and EAP-GTC. Due to wide OS supplicant support, PEAPv0/EAP-MSCHAPv2 is the most widely used EAP method but suffers from security issues related to man-in-the-middle attacks when the supplicant is not pre-configured.

Additional information: https://tools.ietf.org/html/draft-kamath-pppext-peapv0-00

EAP-TTLS (Tunneled Transport Layer Security) is similar to PEAP and uses a server side certificate with supplicant validation. This EAP method is commonly used in non-Active Directory environments where username/password based authentication is desired. EAP-TTLS is supported on a wide range of platforms but may require an administrative configuration profile and/or manual configuration which can add to deployment overhead and complexity. The EAP method also suffers from the same man-in-the-middle attack concerns as PEAP with a supplicant that is not pre-configured.

Additional information: https://tools.ietf.org/html/rfc5281

RADIUS

The RADIUS protocol is used for Authentication, Authorization and Accounting (AAA) communication between authenticators (network access devices) and the authentication server (RADIUS server). Attribute Value Pairs (AVPs) are used to pass information between the authenticator and authentication server in both directions.

EAP messages are encapsulated in RADIUS packets between the authenticator (network device) and the authentication server (RADIUS server).

Additional information: https://tools.ietf.org/html/rfc2138

SNMP

Simple Network Management Protocol is most commonly used for monitoring devices but can also be used for setting configuration elements on the device.

SNMP traps are used to notify a management/monitoring platform of an event, similar to a push notification.

Additional information: http://www.snmp.com/protocol/

Switch Requirements for Colorless Ports

ClearPass is a multi-vendor product that leverages standards-based protocols and technologies along with the flexibility to support vendor-specific switch features for policy enforcement. Below are the basic switch feature sets required for various policy enforcement workflows. These technologies and features will be discussed throughout this document.

RADIUS-based Enforcement

Feature	Role	Primary Use
802.1X IEEE-802.1X	Secure port access via EAPoL	Standard AAA
MAC Authentication Bypass	Fallback for headless devices and guests	Standard AAA, Guest
Dynamic Authorization RFC 5176 (replaced RFC 3576)	Session lifecycle: change of user or device posture/behavior/status	Standard AAA, Guest, Onboard, OnGuard
External Captive Portal Redirect	Guest registration and login, device onboarding, informational splash pages	Guest, Onboard, OnGuard

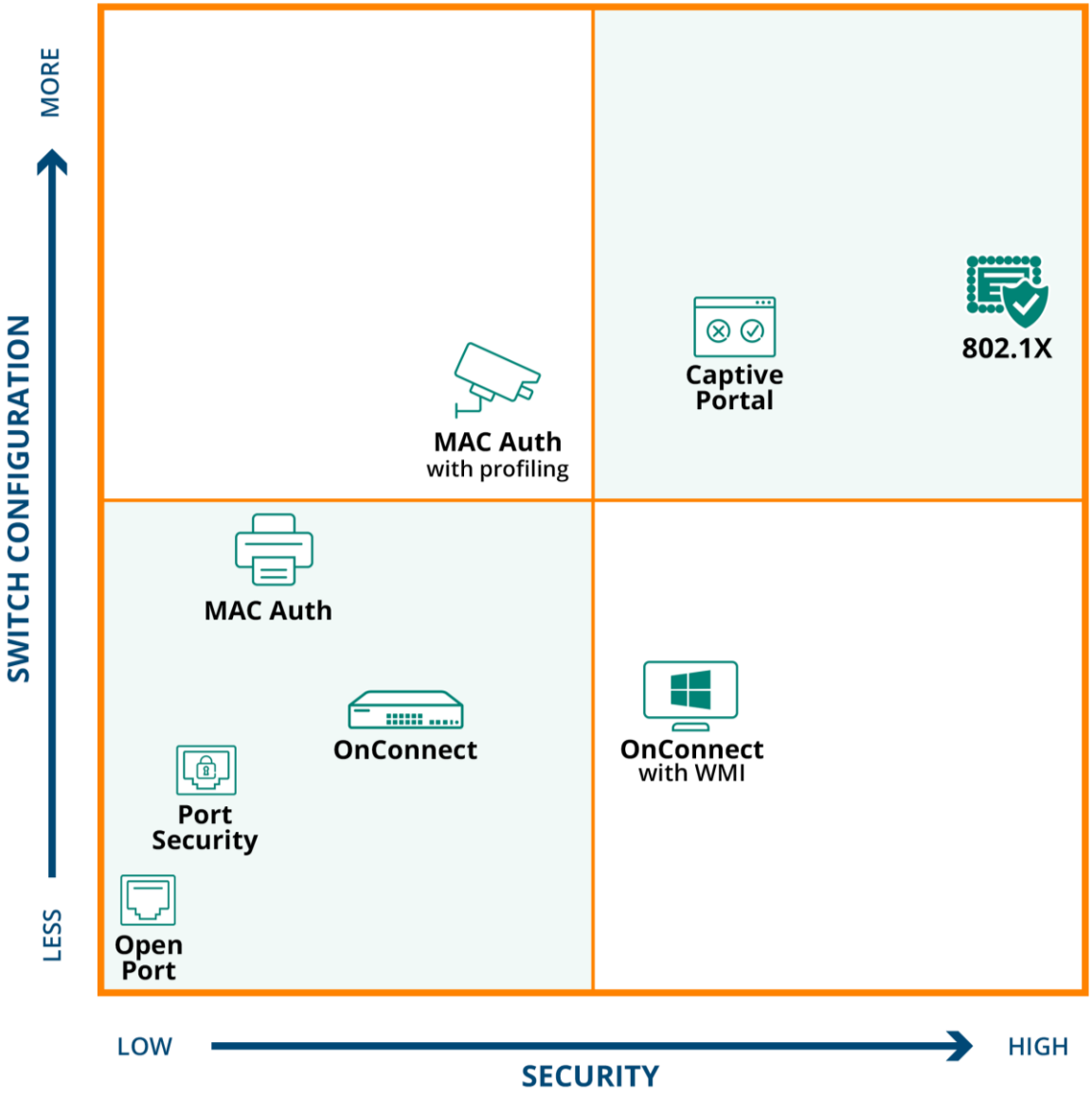
SNMP-based Enforcement

Feature	Role
SNMP Trap: Link Status	Informs ClearPass of a link state change to trigger policy evaluation
SNMP Trap: MAC Notification	Informs ClearPass of the MAC address(es) detected on the port for use in policy evaluation.
SNMP Write: VLAN	Provides the ability for ClearPass to enforce VLAN assignment based on policy evaluation
NOTE: These are the base level requirements for SNMP-based enforcement on the switch side. ClearPass OnConnect must also support the switch. As of ClearPass 6.7.0, OnConnect currently supports ArubaOS-Switch, HPE FlexNetwork (Comware 7) and Cisco Catalyst switches.	

Enforcement Options

There are many different ways to enforce policy on the wired edge. ClearPass offers the capability to enforce policy using standards-based technologies which allow for robust, multi-vendor policy creation and enforcement.

The diagram below offers a 10,000-foot view of the different enforcement methodologies and how they compare from a network security versus a switch configuration complexity point of view. As will be explained throughout this document, many of these are layered together to form the golden colorless port.



RADIUS-based Enforcement

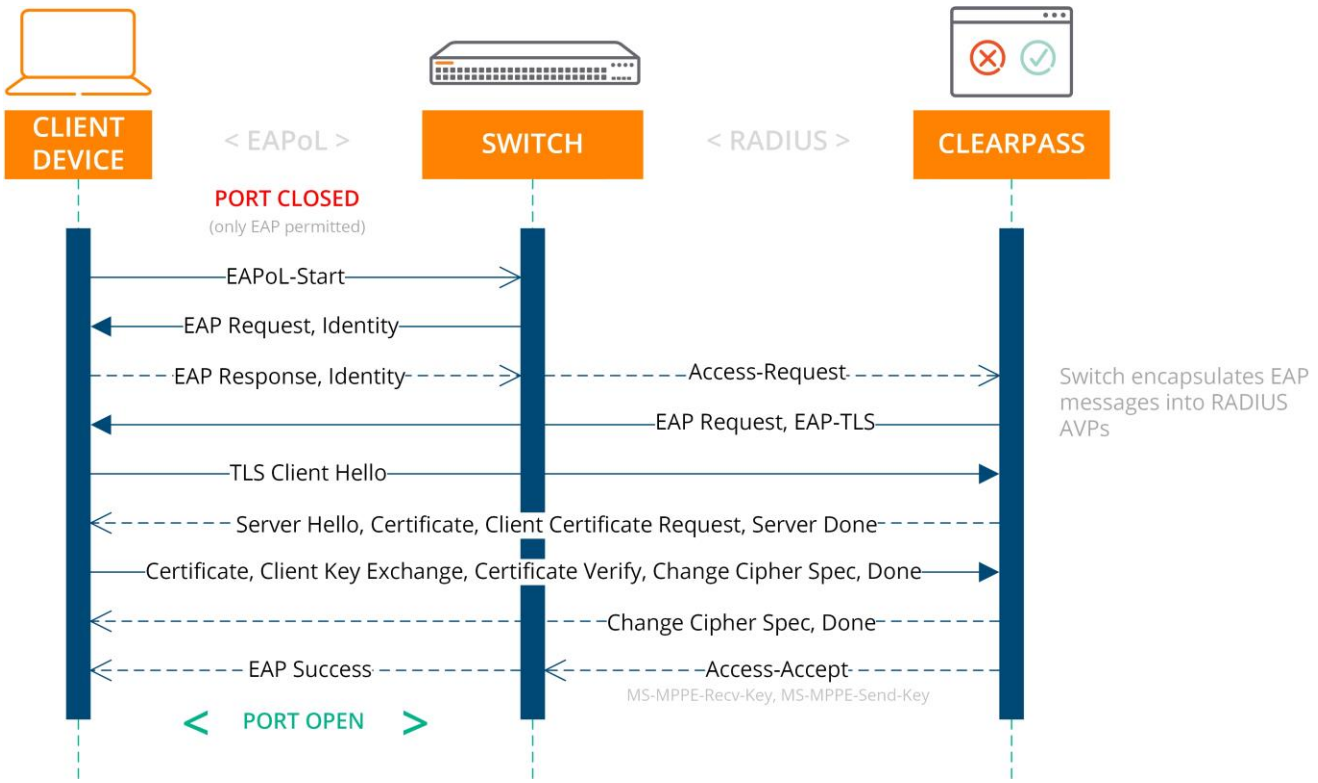
Often times "enabling AAA on the switch" is equated with 802.1X, but that's not the case. AAA can mean 802.1X, MAC Authentication, web authentication or any combination depending on the switch's capabilities.

802.1X

The gold framework for secure port-based access control is defined in the 802.1X standard. The framework offers the best possible mix of flexibility, security, user and device identification and dynamic policy changes.

EAP-based authentication is used within the 802.1X framework to provide multiple different methods of authenticating to the network. As explained earlier, the three most popular EAP methods are EAP-TLS, PEAP, and EAP-TTLS.

The sequence diagram below is an example of a basic EAP-TLS authentication.



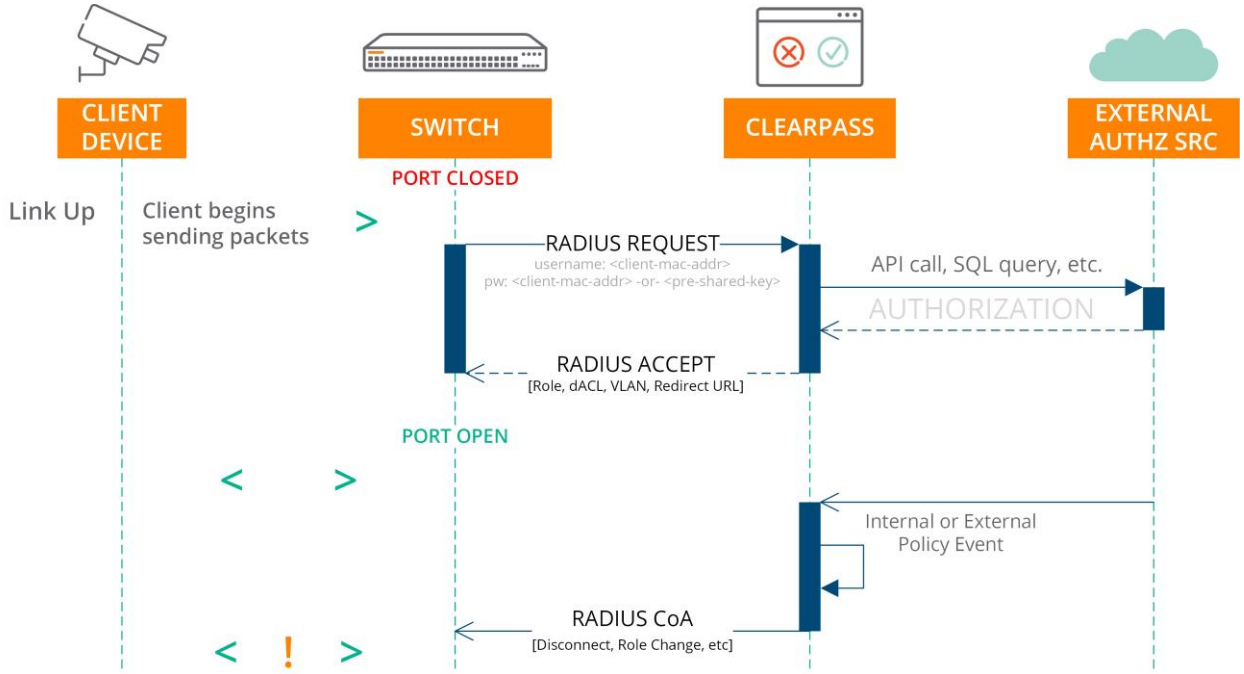
Common examples of wired devices capable of 802.1X authentication:

- Laptops and desktops running:
- Windows
- macOS
- Most Linux distributions
- Newer printers
- VoIP devices
- Aruba access points

MAC Authentication

MAC authentication, sometimes referred to as MAC Auth Bypass (MAB), is commonly used as a fail-through for headless, non-802.1X capable and legacy devices as well as guest users. MAB is often combined with 802.1X and Captive Portal as part of a colorless port configuration supporting every user and device type with a single port configuration.

MAC authentication occurs between the switch and the RADIUS server by sending the client MAC address as the username and either the MAC address or a pre-shared key as the password.



Because MAC Authentication occurs between the switch and the RADIUS server, no client-side configuration or interaction is necessary. Due to this simplicity, MAC authentication is often deployed as a first step in the network authentication journey with the eventual goal of moving to 802.1X. It is then used as a fallback for non-802.1X capable and guest devices.

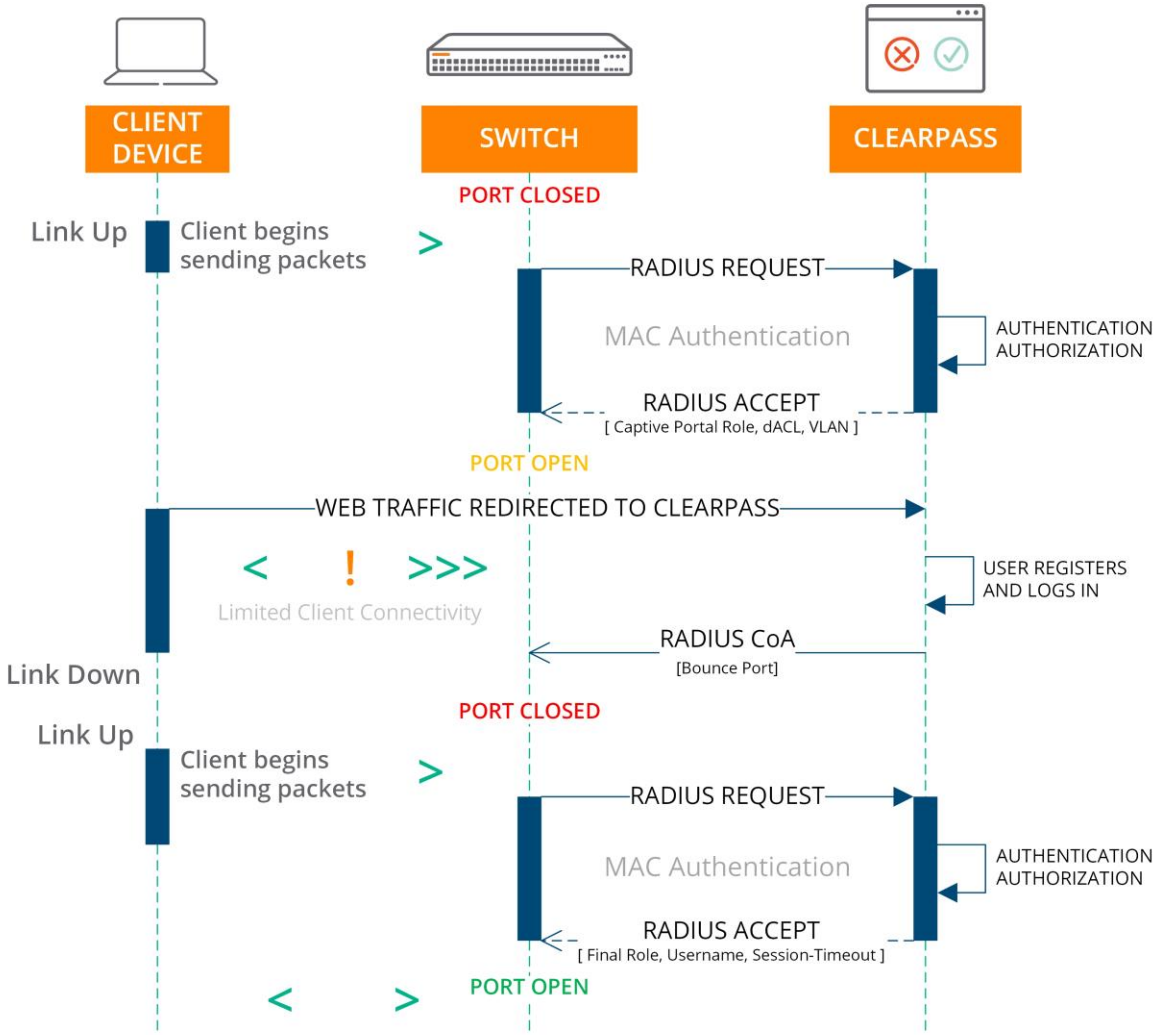
One thing to be aware of is that MAC addresses can be spoofed. MAC authentication should only be used in combination with other authorization components like device profiling. ClearPass has a built-in "conflict" state that is triggered when the category of a device changes. For example, if a printer is suddenly re-profiled as a computer, there is likely reason for concern.

Common examples of devices authorized using MAC address:

- Building controls (HVAC, door access, etc)
- Game consoles and media players
- IP cameras
- Older printers
- Patient care medical devices

Captive Portal

Web-based authentication using captive portals is often associated with guest networks. Their usage has evolved to include other functions such as device onboarding, multi-factor authentication and splash pages for user notifications.



Centralized Enforcement Using Per-Port Tunneled-Node

For the highest level of security, visibility and control, Aruba switches and Aruba Mobility Controllers can be used together to offer stateful firewall processing, application visibility and bandwidth restrictions, and centralized policy enforcement using the Per-Port Tunneled-Node (PPTN) feature.

Overview

Per-Port Tunneled-Node (PPTN) is a unique feature, introduced in ArubaOS-Switch version 16.02 and supported on Mobility Controllers running ArubaOS 6.5 and higher, which allows for all wired traffic entering a switch port to be GRE encapsulated and sent up to an Aruba Mobility Controller for processing; like the tunnel forwarding mode in the Aruba wireless architecture.

When a port is configured for PPTN, it is placed into a dead-end VLAN locally on the switch. This VLAN must also exist on the controller but cannot be tagged throughout the network. It must match on both sides and cannot have an IP address or be tagged on an interface. This VLAN is used on the inside of the GRE tunnel to transport the traffic between the switch and controller.

Once the tunnel is established, the controller handles all AAA functions and places the device into the appropriate user role. All firewall policies, bandwidth contracts and other traffic restrictions are enforced by the controller. The traffic flow is nearly identical to a wireless client connected to a tunneled SSID.

Sample Use Cases

- Branch scenarios where all wired and wireless traffic is processed by a Mobility Controller
- Regulatory or high-risk environments where all wired traffic must traverse a firewall
- Providing access to a centrally defined network that does not traverse the entire infrastructure
- Areas with high numbers of headless/IoT devices like building infrastructure head-ends or maintenance facilities
- Temporarily providing access during an event using an unmanaged switch

Dynamic Segmentation and Enforcement Using Per-User Tunneled-Node

Overview

Per-User Tunneled-Node (PUTN), introduced with ArubaOS-Switch 16.04 and supported on Mobility Controllers running ArubaOS 8.1 and higher, adds the ability for a ClearPass policy decision to tell an Aruba switch whether a device's traffic should be processed locally or tunneled to a Mobility Controller. This enables stateful firewall processing of traffic and advanced application control at the controller when you need it, and traditional stateless processing at the switch when you don't.

Per-User Tunneled-Node can take advantage of new ArubaOS 8 features such as dynamic load balancing of users in a cluster. Tunneling is enabled in the Aruba user role and can be combined with the Downloadable User Role (DUR) feature for dynamic and flexible policy enforcement and segmentation.

Sample Use Cases

As an example, a typical edge network consists of employee desktops and laptops, visitor or contractor laptops, access points, security cameras, desk and conference phones, building controls and headless meeting room equipment.

Type	Enforcement	Notes
Access Point	Local	Local infrastructure device
Voice / Video Device	Local	Desk and conference phones, security cameras, room media systems
Employee on Managed Device	Local	Users connecting from a healthy, managed device can stay local to the switch
Employee on Unmanaged Device	Tunnel	Users connecting from an unmanaged, potentially untrusted device can be tunneled
New/Unknown Device	Tunnel	Tunnel new or unknown , potentially untrusted devices for profiling, potential onboarding, guest registration or and/or quarantine
Guest User	Tunnel	Tunnel guest users to DMZ guest network
Contractor	Tunnel	Contractors may need more access than a traditional guest user
Change in User/Device Posture	Tunnel	User or device goes from a healthy to unhealthy state (OnGuard checks, IntroSpect notification, Ingress Event Engine Notification)

SNMP-based Enforcement with ClearPass OnConnect

ClearPass OnConnect is a new feature added in ClearPass 6.6.1 which utilizes SNMP for non-authenticated, basic VLAN enforcement at the edge and is included in the base ClearPass license!

Technical Overview

Profiling

Profiling is a very important piece of OnConnect because there is no traditional authentication phase.

Just like RADIUS-based enforcement, traditional passive profiling data, like DHCP fingerprints, can be leveraged as part of an OnConnect policy evaluation. Active methods such as Enterprise Mobility Management (EMM) platform data can also be leveraged to build policy.

OnConnect also supports a new method of active profiling that leverages the Windows Management Instrumentation (WMI) protocol for domain-joined Windows devices. ClearPass can send a WMI request to the device to request the active logged in user on a Windows domain-joined device. ClearPass can then run an authorization query against Active Directory to pull in directory information about the user such as group membership, OU and department. These directory attributes can then be used as part of an OnConnect enforcement just like in a RADIUS role mapping and/or enforcement policy.

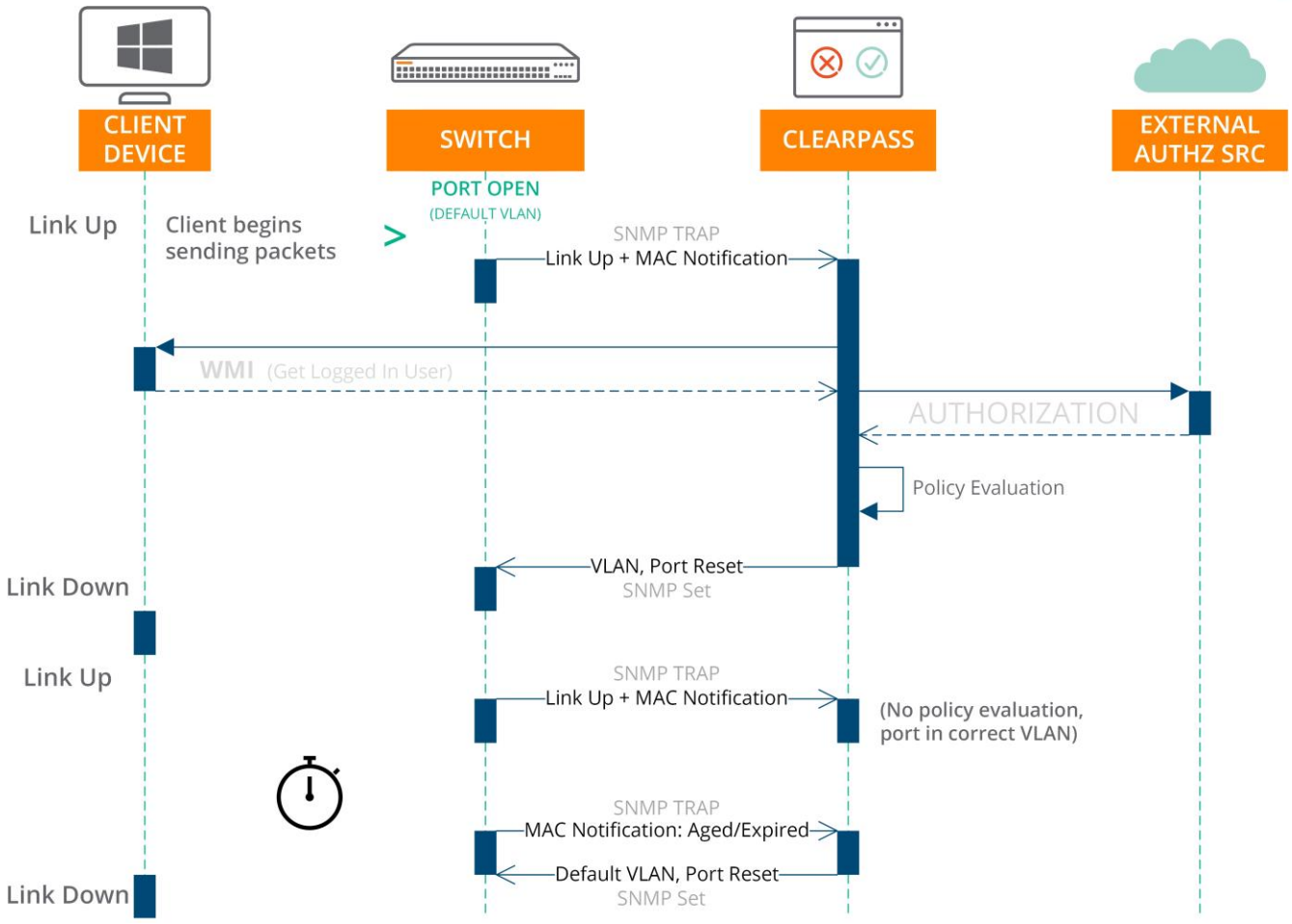
How It Works

Switches are configured to send link change (up/down) and MAC notification SNMP traps to ClearPass. When a new device connects, and the switch has sent the trap(s), Policy Manager will verify that the switch and port have been configured for OnConnect enforcement and then proceed with policy evaluation. Note that during this time, the device will be in the default VLAN as configured on the switch port.

If WMI credentials have been defined in ClearPass, a WMI request will be sent to the client requesting the currently logged in user. If a username is returned and authorization to Active Directory is enabled in the service, Policy Manager will query AD for the user properties. Any additional authorization sources, such as the Endpoint Repository, Guest Device Repository (device registration) or even an external SQL database, will be queried as well.

Three SNMP enforcement actions are available: VLAN Change, Port Bounce, and Session Timer. In many cases, all 3 will be combined as part of an enforcement. For example, if a logged in AD user is detected on the device, you may want to change the VLAN, reset the port (so the device can re-DHCP in the correct VLAN) and also set a session timer to trigger re-authentication at a later time.

In the Policy Enforcement section of this guide, full configuration examples will be provided.



Sample Use Cases

- Legacy switching that lacks reliable 802.1X and/or MAC authentication support
- Varying versions of switch code across the environment
- Existing network/helpdesk support team knowledge, comfort level and expertise with SNMP vs RADIUS.

Policy Enforcement Configuration

The remainder of this document will cover configuration of some common scenarios utilizing the technologies discussed earlier.

These examples are just that, examples. They're designed to show different ways to build policy on both the network device and in ClearPass. Not every unique scenario or combination will be covered but the goal is to highlight key concepts and features that can be adapted into other scenarios.

ArubaOS-Switch Enforcement

RADIUS-based Enforcement

Policy Enforcement

Similar to an Aruba wireless controller, ArubaOS-Switch uses the concept of user roles to simplify configuration and policy creation and increase visibility and control.

User Roles

An ArubaOS-Switch user role can contain:

- VLAN-ID or VLAN name
- reauthentication interval
- user policy
- captive portal profile

A user policy is composed of one or more traffic classes to match specified packets. The class defines the ACL to match traffic and the policy combines multiple classes together with enforcement actions.

Here's an example of a complete user role configuration with dependencies:

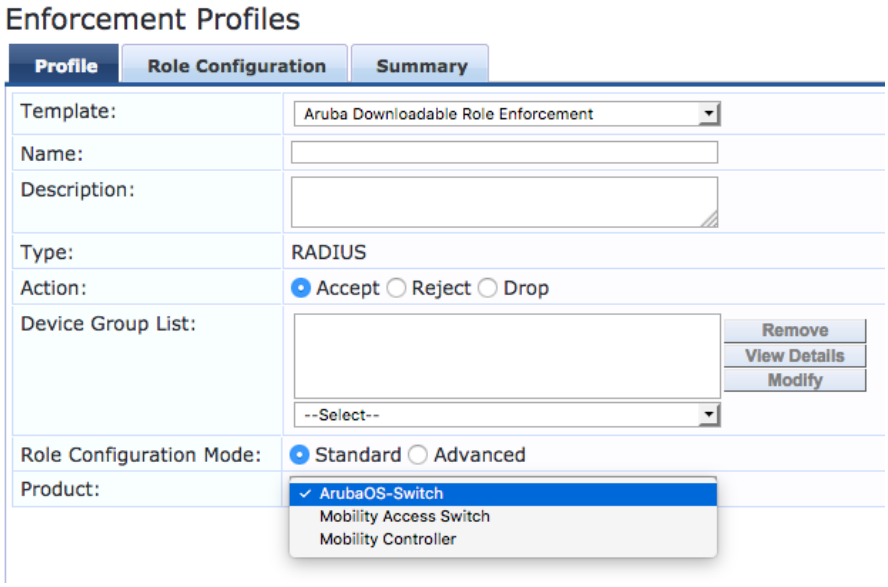
```
class ipv4 "IP-ANY-ANY"
     match ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
   exit

policy user "PERMIT-ALL"
     class ipv4 "IP-ANY-ANY" action permit
   exit

aaa authorization user-role name "SECURE"
     policy "PERMIT-ALL"
     reauth-period 28800
     vlan-name "EDGE_SECURE"
   exit
```

A user role defined locally on the switch itself is known as a local user role (LUR).

Downloadable User Roles (DURs)

Downloadable user roles (available on Aruba Mobility Controllers, Aruba Mobility Access Switches and ArubaOS-Switches) enable ClearPass to act as a centralized policy and enforcement definition point. This allows an intelligent edge with greater flexibility and dynamic security while simplifying local configuration.

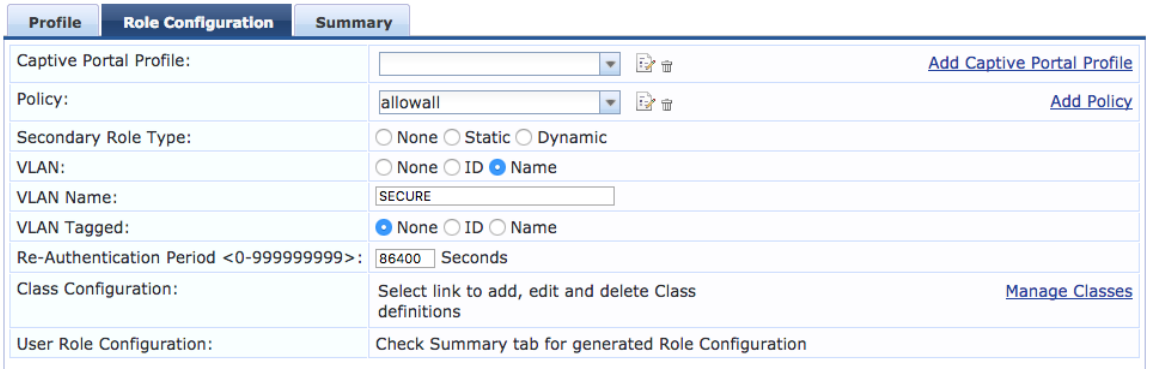
ClearPass has a special enforcement profile template for DUR called **`Aruba Downloadable Role Enforcement`**. This template supports all 3 Aruba products (ArubaOS-Switch, Mobility Access Switch and Mobility Controller).



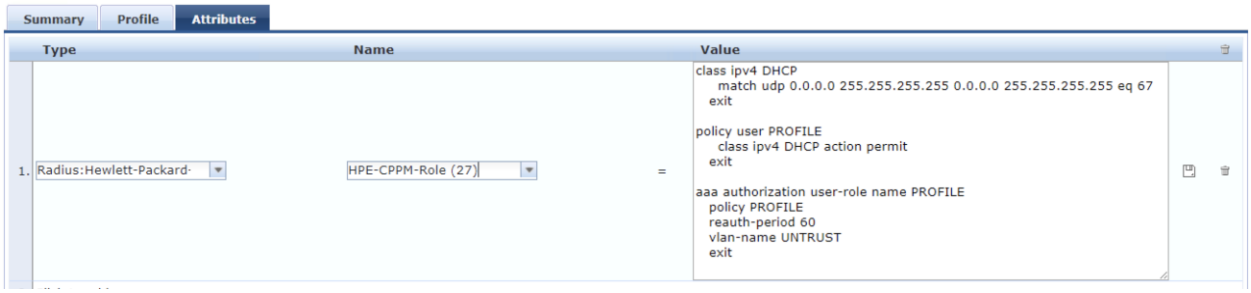
Two configuration modes are available for Downloadable User Roles, Standard and Advanced.

NOTE: ArubaOS-Switch 16.04+ and ClearPass 6.6.7+ are required to use Downloadable User Roles and standard mode is only available in ClearPass 6.7.0+.

Standard mode uses a GUI editor to build out the role elements like VLAN assignment, classes and policy.



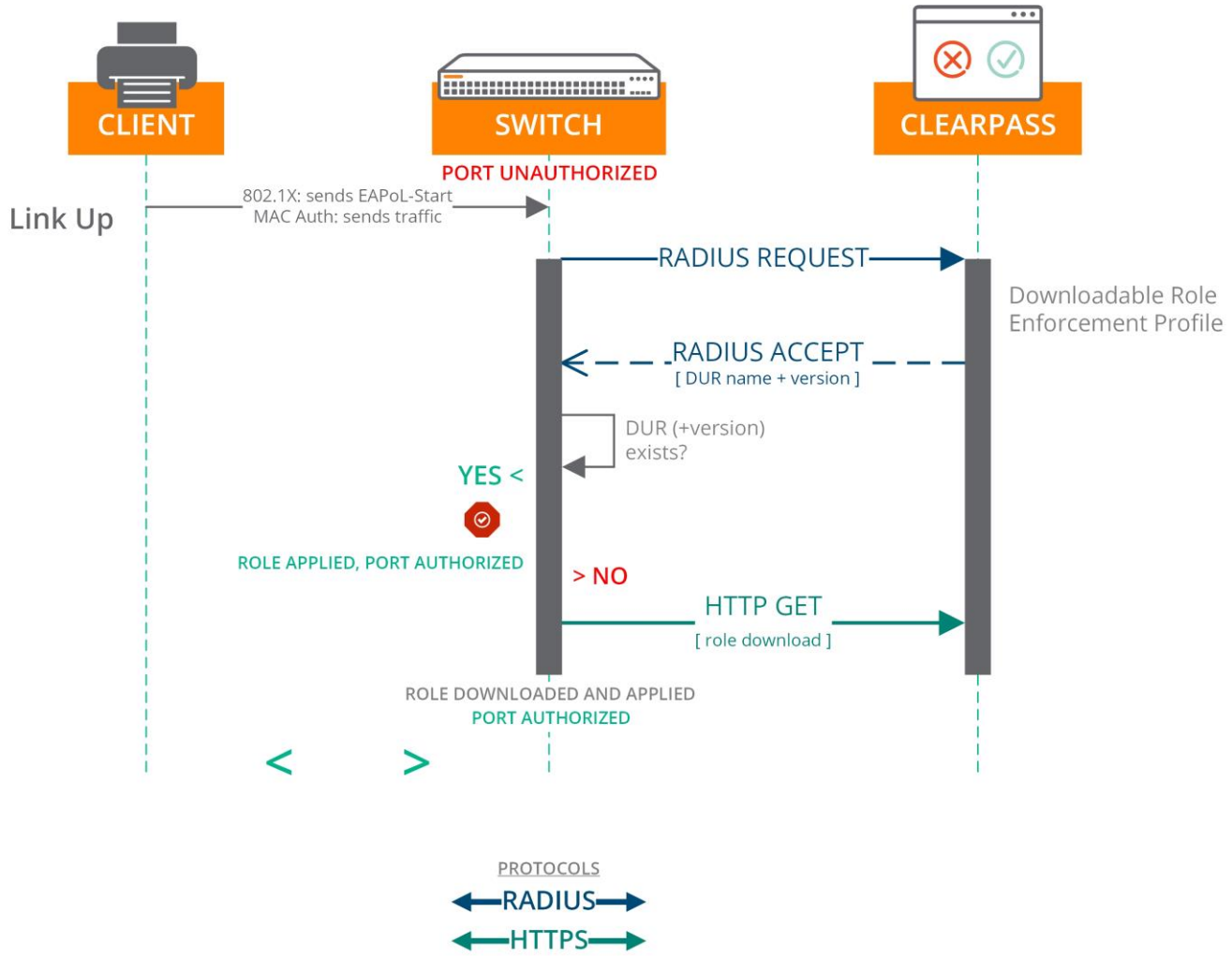
Advanced mode allows for direct input of all required user role configuration elements as the **`Value`** for the **`HPE-CPPM-Role`** attribute.



Each DUR has a version number that is automatically generated by ClearPass and dynamically appended to the name in the background. This allows the switch to determine if role elements have changed and download a new version of the role for use with subsequent authentications. This also prevents the switch from downloading the same role for every new device.

When a downloadable user role name is returned in the RADIUS access-accept, the switch checks to see if the DUR + version combination already exists. If present, the switch's cached version of the role is applied to the user. If the role is not present, or if the version number has changed, the switch initiates an HTTP GET to ClearPass to download the updated role elements. Existing authenticated users will continue to use the older role version until they reauthenticate. This process is illustrated in the sequence diagram below.

NOTE: HTTPS (TCP 443) must be permitted between the switch's management IP and ClearPass. The request is sourced from the same interface/IP as RADIUS.



Dynamic Authorization

ArubaOS-Switch supports the following Disconnect and Change of Authorization commands:

- **Terminate Session**: traditional disconnect message; reinitializes authenticator state
- **Bounce Host Port**: bounces the port by disabling and re-enabling the port
- **Disable Host Port:** administratively disables the port
- **Change User Role:** dynamically change the user role without disconnecting the user

Configuration Overview

Here are the hardware and software combinations used for this configuration:

- Aruba 2930F switch running ArubaOS-Switch 16.04.008
- ClearPass Policy Manager 6.6.7

This configuration has been tested on the Aruba 3810M and 2930F. The minimum version of ArubaOS-Switch required for this configuration is 16.04.008.

Switch Configuration

The configuration snippets below assume that components like VLANs, uplinks, NTP and other basics have already been configured.

Key basic components:

- NTP is required as accurate time plays a critical role in network authentication
- To support captive portal redirection, the client VLAN(s) must have an IP address assigned on the switch (ex: `vlan 812 ip address 100.81.2.252/24`). It is recommended to use the authorized-managers feature to restrict access to switch management functions on these interfaces.

Enable global functions and configurations:

`ip client-tracker trusted`	provides IP visibility for AAA-enabled ports
`ip source-interface radius vlan 810`	set RADIUS source interface

Define the ClearPass server(s) as RADIUS server(s) and dynamic authorization client(s):

`radius-server host 100.65.30.42 key Aruba123!`	define ClearPass as RADIUS server
`radius-server host 100.65.30.42 dyn-authorization`	enable dynamic authorization (CoA)
`radius-server host 100.65.30.42 time-window plus-or-minus-time-window 30`	time difference permitted for CoA packet (seconds)
`aaa server-group radius CLEARPASS host 100.65.30.42`	assign to server-group

To support downloadable user roles, the signing CA (intermediate) of the ClearPass HTTPS certificate must be added to the switch and marked as trusted.

For example, `clearpass-demo.arubaboston.com` (server certificate) is signed by `COMODO RSA Domain Validation Secure Server CA` (intermediate / signing CA) which is signed by `COMODO RSA Certification Authority` (root CA).

The ***`COMODO RSA Domain Validation Secure Server CA`*** should be added to the switch.

`crypto pki ta-profile CLEARPASS`	create new trust profile
`copy <sftp|tftp> ta-certificate CLEARPASS <sftp|tftp server> <ca-cert-filename>`	copy the signing CA certificate to the switch via SFTP or TFTP

DURs also require a ClearPass read-only user account to download the user role configuration. Configure the expected username and password for the account.

`radius-server cppm identity aoss-dur key R!!y5tr0ngpw`	ClearPass DUR account

Enable AAA functions:

`aaa authentication port-access eap-radius server-group CLEARPASS`	enable EAP-based authentication
`aaa authentication mac-based chap-radius server-group CLEARPASS`	enabled MAC authentication
`aaa accounting network start-stop radius server-group CLEARPASS`	enable RADIUS accounting
`aaa accounting update periodic 5`	set interim-accounting update interval (minutes)
`aaa authentication captive-portal enable`	enable captive-portal redirect
`aaa authorization user-role enable`	enable user roles
`aaa authorization user-role enable download`	enable DUR

Port configuration:

`aaa port-access authenticator active`	enable port authentication
`aaa port-access authenticator 1-12 client-limit 10`	permit up to 10 active clients per port
`aaa port-access mac-based 1-12`	enable MAC authentication on ports 1-12
`aaa port-access mac-based 1-12 addr-limit 10`	permit up to 10 authenticated MACs per port
`aaa port-access authenticator 1-12`	enable EAP-based authentication on ports 1-12
`aaa port-access authenticator 1-12 supplicant-timeout 10`	supplicant timeout period (seconds)
`aaa port-access authenticator 1-12 tx-period 10`	EAP Request-Identity waiting period (seconds)

Define traffic classes to match packets for use in policy:

```
class ipv4 DNS
     match udp any any eq 53
class ipv4 DHCP
     match udp any any eq 67
class ipv4 INTERNAL
     match ip any 100.64.0.0/10
class ipv4 IP-ANY-ANY
     match ip any any
class ipv4 WEB-TRAFFIC
     match tcp any any eq 80
     match tcp any any eq 443
class ipv4 CLEARPASS-WEB
     match tcp any host 100.65.30.42 eq 80
     match tcp any host 100.65.30.42 eq 443
```

Create user policies to take action on the traffic classes:

policy user CLEARPASS-REDIRECT class ipv4 DNS action permit class ipv4 DHCP action permit class ipv4 CLEARPASS-WEB action permit class ipv4 WEB-TRAFFIC action redirect captive-portal	permit DNS, DHCP and web traffic destined for ClearPass, redirect all other web traffic
policy user DENY-INTERNAL class ipv4 DNS action permit class ipv4 DHCP action permit class ipv4 INTERNAL action deny class ipv4 IP-ANY-ANY action permit	permit DNS and DHCP, deny all internal subnets, permit everything else
policy user PERMIT-ALL class ipv4 IP-ANY-ANY action permit	permit everything

Here are a few examples of user role configurations:

aaa authorization user-role name BYOD policy PERMIT-ALL reauth-period 43200 vlan-name EDGE_GUEST	BYOD role, allow all reauthenticate every 12 hours EDGE_GUEST VLAN
aaa authorization user-role name GUEST policy DENY-INTERNAL reauth-period 14400 vlan-name EDGE_GUEST	GUEST role, deny internal IPs reauthenticate every 4 hours EDGE_GUEST VLAN
aaa authorization user-role name VOICE policy PERMIT-ALL reauth-period 86400 vlan-name EDGE_VOICE	VOICE role, allow all reauthenticate every 24 hours EDGE_VOICE VLAN
aaa authorization user-role name SPLASH captive-portal-profile use-radius-vsa policy CLEARPASS-REDIRECT vlan-name EDGE_GUEST	SPLASH role, redirect to ClearPass Use URL from RADIUS response EDGE_GUEST VLAN This is the “fail through” role
aaa authorization user-role name PROFILE captive-portal-profile use-radius-vsa policy CLEARPASS-REDIRECT reauth-period 180 vlan-name EDGE_GUEST	PROFILE role, redirect to ClearPass Use URL from RADIUS response Reauthenticate every 3 minutes EDGE_GUEST VLAN, this role is used to profile unknown devices.

ClearPass: Basics

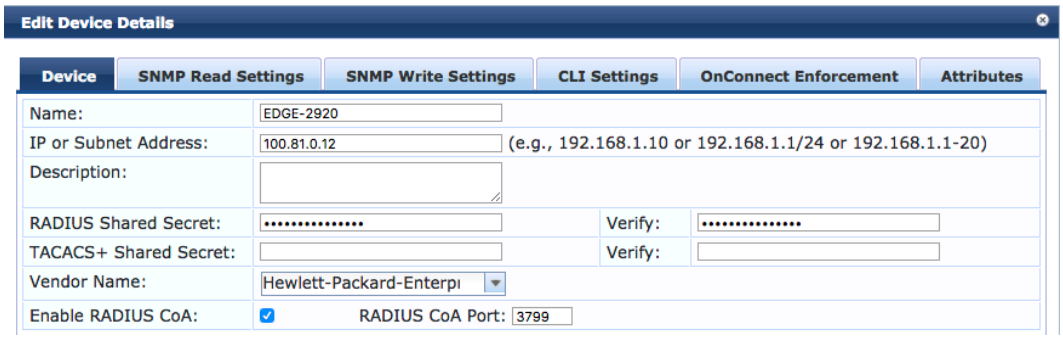
ArubaOS-Switch uses the `Hewlett-Packard-Enterprise` RADIUS dictionary and two new vendor-specific attributes (VSAs) were added to support the local user role and downloadable user role features.

The minimum supported ClearPass release for the downloadable user role feature is 6.6.7 which includes the two new VSAs.

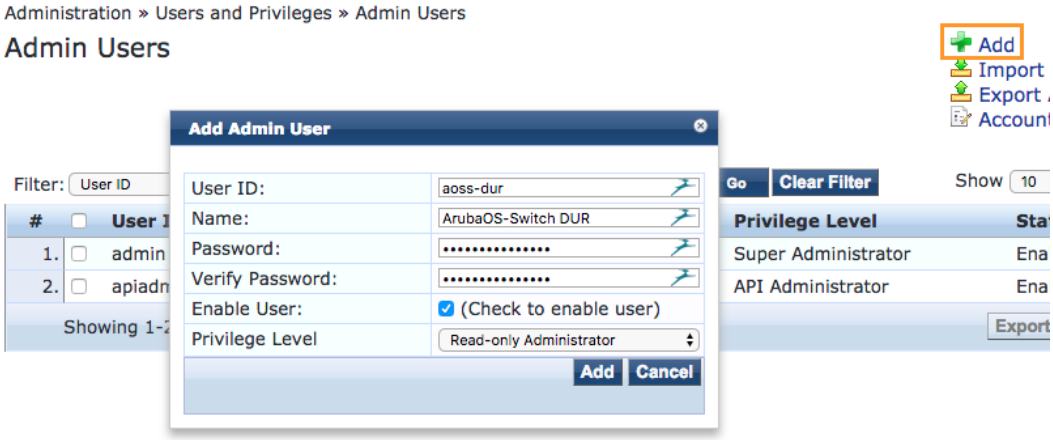
If only local user roles will be used with ClearPass prior to 6.6.7, verify that the `Hewlett-Packard-Enterprise` dictionary in your ClearPass cluster has attribute #25, **`HPE-User-Role`**. If it's missing, download and import the latest dictionary file from support.arubanetworks.com > Download Software > ClearPass > Tools > RADIUS Dictionaries.

Instructions for importing a new or updated RADIUS dictionary can be found in the ClearPass User Guide.

Define your switch(es) as a network device(s) under **`Configuration » Network » Devices`**. At a minimum, configure **`Name`**, **`IP or Subnet Address`**, **`RADIUS Shared Secret`** and **`Vendor Name`**.



To utilize the downloadable user role feature, a read-only administrator account must be created in ClearPass so the switch can download the role information. Navigate to **`Administration » Users and Privileges » Admin Users » Add`**. The username and password should match the account defined on the switch in the previous section. For **`Privilege Level`**, select **`Read-Only Administrator`**.



ClearPass: MAC Authentication

Overview

The MAC Authentication service will handle headless devices like printers, phones, access points and others as well as provide the redirect URL for unknown devices and users to allow for a captive portal authentication.

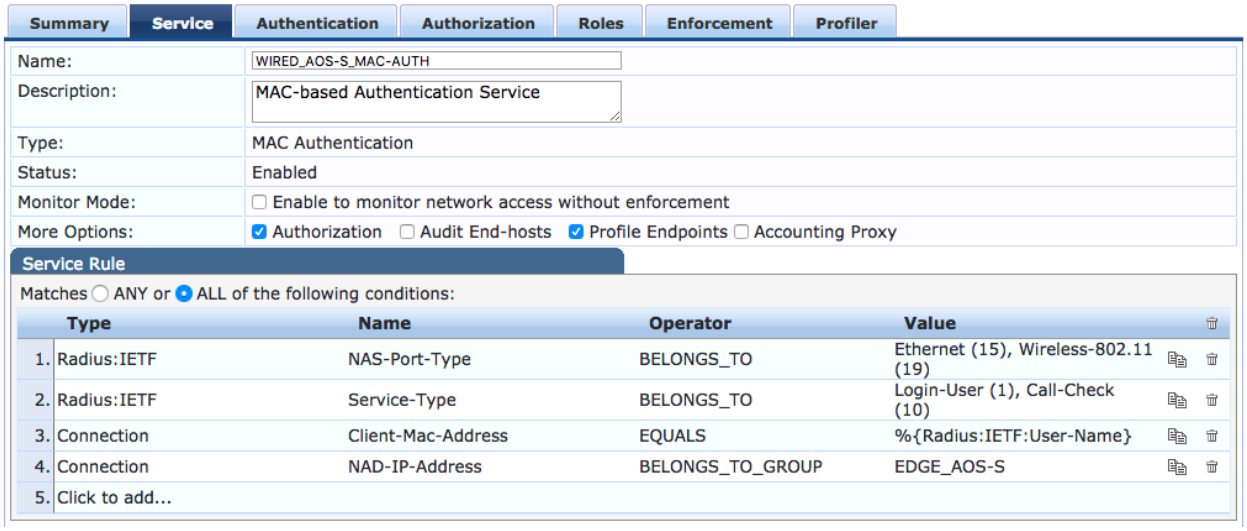
In this scenario, we're leveraging the Guest Device Repository and Device Registration portal to allow end-users and IT staff to register headless and non-802.1X capable devices. These devices can be assigned a role and account lifetime.

Service Configuration

Start with a new service of type **`MAC Authentication`**.

Under More Options, check the **`Authorization`** and **`Profile Endpoints`** boxes. This will enable two new tabs. The default service rules will work with an ArubaOS-Switch.

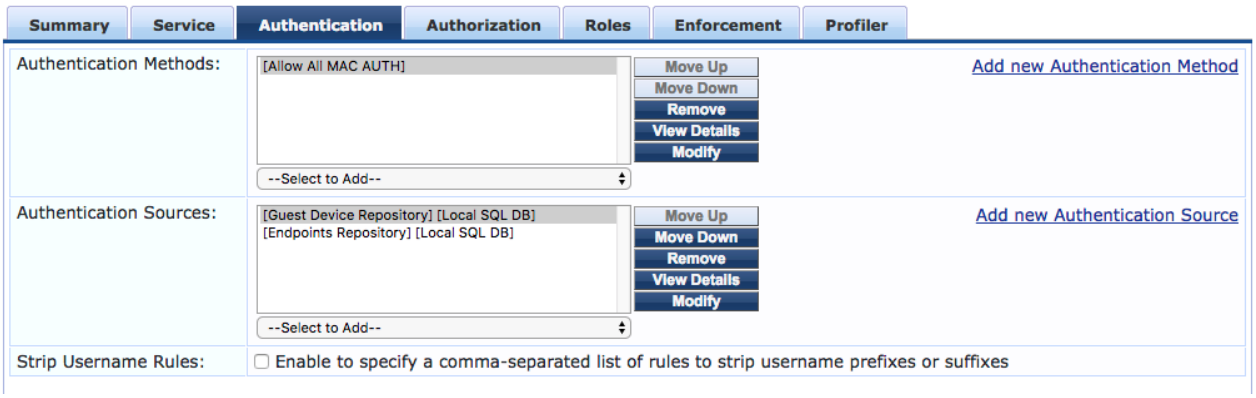
If there is a need to restrict the service to a particular set of switches, you can use a **`Connection`** | **`NAD-IP-Address`** | **`BELONGS_TO_GROUP`** rule to reference a NAD group as seen in rule 4 below.



Authentication

On the authentication tab, remove **[MAC Auth]** under Authentication Methods and add **[Allow All MAC Auth]**.

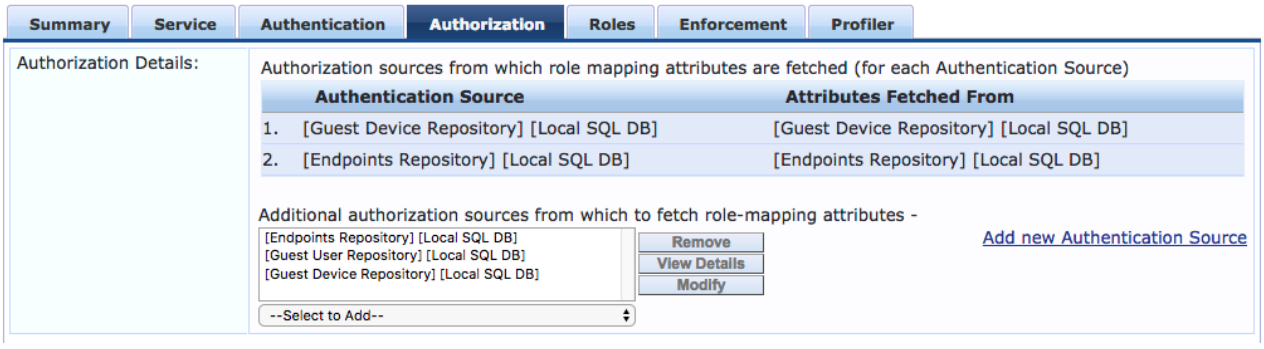
For Authentication Sources, you'll add **[Guest Device Repository] [Local SQL DB]** and move it above **[Endpoints Repository] [Local SQL DB]**.



Authorization

On the Authorization tab, add the **[Endpoints Repository]**, **[Guest User Repository]** and **[Guest Device Repository]** to the "Additional authorization sources..." list as shown below.

By default, authorization data is only fetched from the authentication source where the user/device was found.

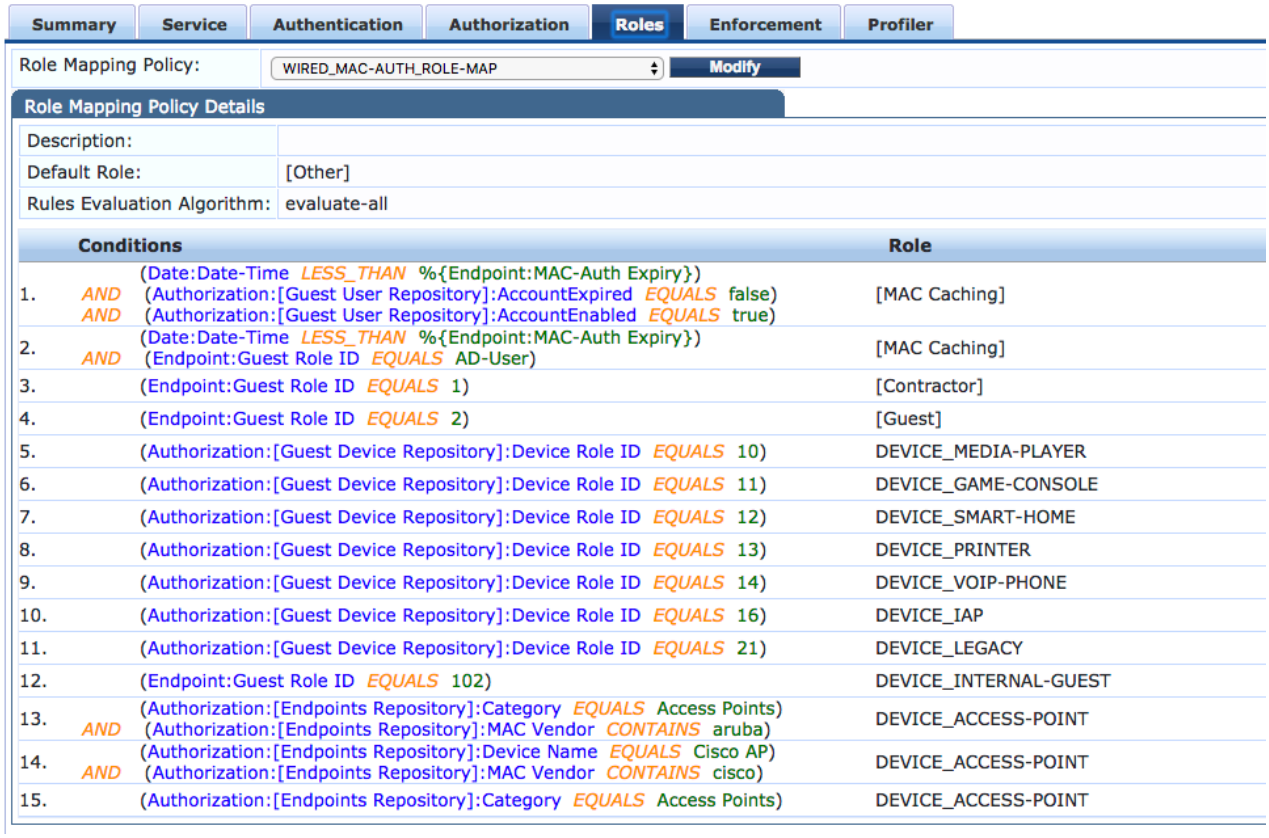


So, for example, say a guest user's device is re-authenticating to the network within their account expiration window, you'll find the MAC address in the `[Endpoints Repository]` with some data like guest role and expiration time but we also want to check with ClearPass Guest to make sure an administrator hasn't disabled the account.

Roles

Role mapping is used to tag devices and users with as much information as possible for use in a policy decision. This role map is an example of a typical MAC authentication scenario

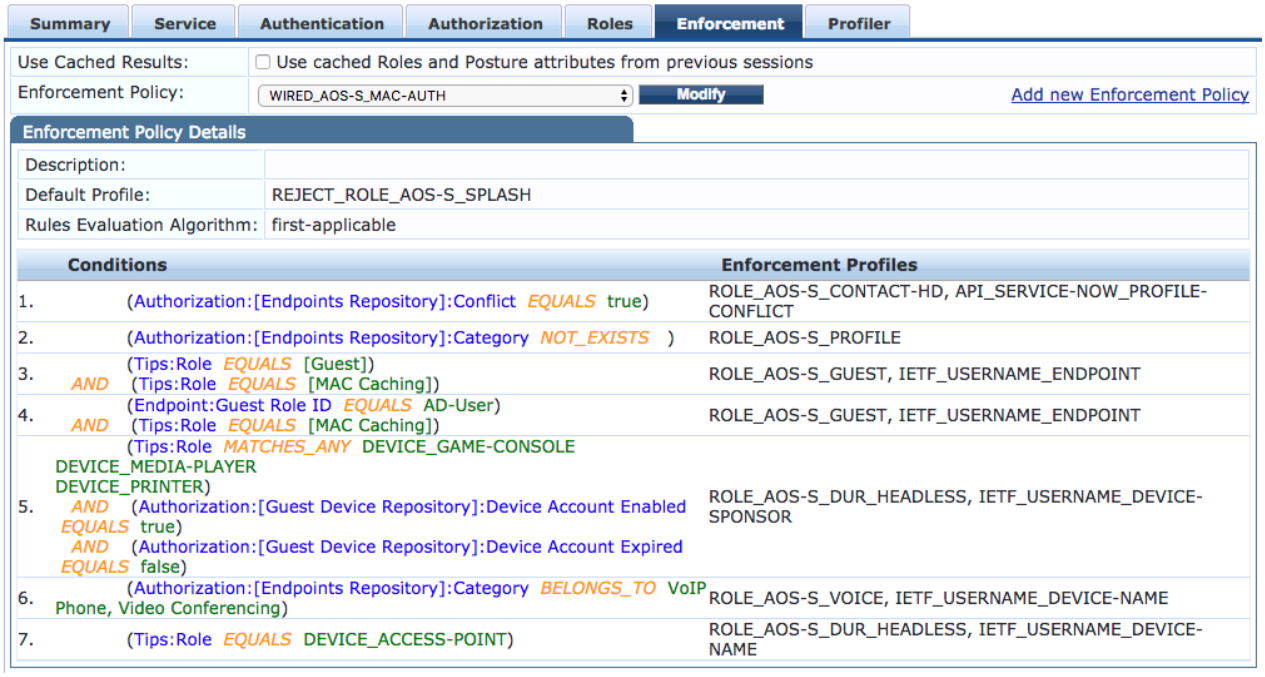
- Rule 1 and 2 are checking to see that a guest user account is still valid and returning the [MAC Caching] tag / TIPS role
- Rules 3-12 map user and device role IDs to tags / TIPS roles for use in policy
- Rules 13-15 map profiling data to a tag / TIPS role for use in policy



Enforcement

For the default policy, the captive portal "splash" role is specified. This is used when a request falls through the policy with no match.

Let's take apart the enforcement rules one by one:



Summary | Service | Authentication | Authorization | Roles | Enforcement | Profiler

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

Enforcement Policy: WIRED_AOS-S_MAC-AUTH [Modify] Add new Enforcement Policy

Enforcement Policy Details

Description:	
Default Profile:	REJECT_ROLE_AOS-S_SPLASH
Rules Evaluation Algorithm:	first-applicable

	Conditions	Enforcement Profiles
1.	(Authorization:[Endpoints Repository]:Conflict *EQUALS* true)	ROLE_AOS-S_CONTACT-HD, API_SERVICE-NOW_PROFILE-CONFLICT
2.	(Authorization:[Endpoints Repository]:Category *NOT_EXISTS*)	ROLE_AOS-S_PROFILE
3.	(Tips:Role *EQUALS* [Guest]) *AND* (Tips:Role *EQUALS* [MAC Caching])	ROLE_AOS-S_GUEST, IETF_USERNAME_ENDPOINT
4.	(Endpoint:Guest Role ID *EQUALS* AD-User) *AND* (Tips:Role *EQUALS* [MAC Caching])	ROLE_AOS-S_GUEST, IETF_USERNAME_ENDPOINT
5.	(Tips:Role *MATCHES_ANY* DEVICE_GAME-CONSOLE DEVICE_MEDIA-PLAYER DEVICE_PRINTER) *AND* (Authorization:[Guest Device Repository]:Device Account Enabled *EQUALS* true) *AND* (Authorization:[Guest Device Repository]:Device Account Expired *EQUALS* false)	ROLE_AOS-S_DUR_HEADLESS, IETF_USERNAME_DEVICE-SPONSOR
6.	(Authorization:[Endpoints Repository]:Category *BELONGS_TO* VoIP Phone, Video Conferencing)	ROLE_AOS-S_VOICE, IETF_USERNAME_DEVICE-NAME
7.	(Tips:Role *EQUALS* DEVICE_ACCESS-POINT)	ROLE_AOS-S_DUR_HEADLESS, IETF_USERNAME_DEVICE-NAME

1

(Authorization:[Endpoints Repository]:Conflict *EQUALS* true)	ROLE_AOS-S_CONTACT-HD, API_SERVICE-NOW_PROFILE-CONFLICT

If a device's profiled category changes, ClearPass triggers the `Conflict` attribute.

Here we're saying if the Conflict attribute is `true`, put the device into a captive portal redirect to let them know to contact the help desk and also send an API call over to ServiceNow to open a ticket.

2

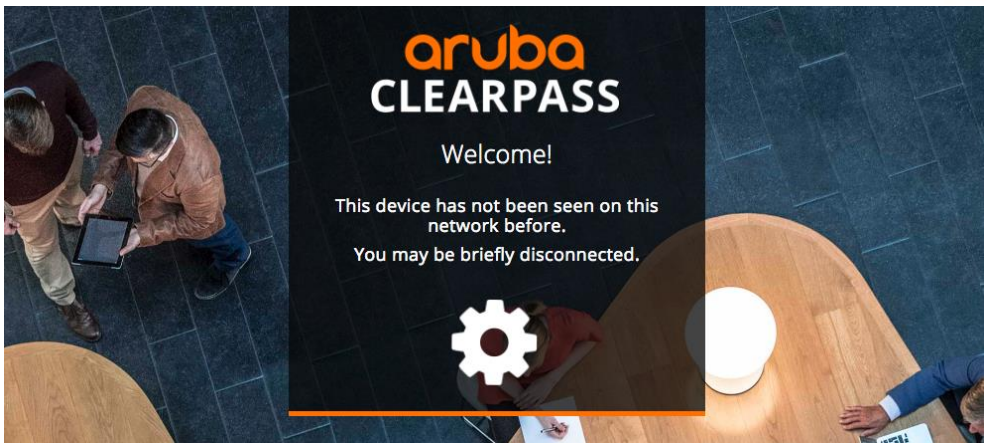
(Authorization:[Endpoints Repository]:Category *NOT_EXISTS*)	ROLE_AOS-S_PROFILE

This rule evaluates whether the profile `Category` exists for the authenticating endpoint.

If it does not exist, the device has not been profiled and a captive portal redirect URL and **`PROFILE`** user role are returned to the switch.

	Type	Name		Value
1.	Radius:Hewlett-Packard-Enterprise	HPE-User-Role	=	PROFILE
2.	Radius:Hewlett-Packard-Enterprise	HPE-Captive-Portal-URL	=	https://clearpass-demo.arubaboston.com/guest/wired_profiling.php

---



NOTE: Captive portal redirect is not required for profiling. It's simply an example of leveraging features to improve user experience.

3

(Tips:Role *EQUALS* [Guest]) *AND* (Tips:Role *EQUALS* [MAC Caching])	ROLE_AOS-S_GUEST, IETF_USERNAME_ENDPOINT

During role mapping, we were able to determine that the device should still be MAC Cached based on its expiration and the user's account status.

The **GUEST** user role and the guest's username/email will be returned.

4

(Endpoint:Guest Role ID *EQUALS* AD-User) *AND* (Tips:Role *EQUALS* [MAC Caching])	ROLE_AOS-S_GUEST, IETF_USERNAME_ENDPOINT

This rule is similar to rule 3, but instead of checking for a Guest role, we're checking for the custom AD-User role which is configured for temporary guest access with valid AD credentials.

The **GUEST** user role and the user's AD username will be returned in the RADIUS response.

5

(Tips:Role *MATCHES_ANY* DEVICE_GAME-CONSOLE DEVICE_MEDIA-PLAYER DEVICE_PRINTER) *AND* (Authorization:[Guest Device Repository]:Device Account Enabled *EQUALS* true) *AND* (Authorization:[Guest Device Repository]:Device Account Expired *EQUALS* false)	ROLE_AOS-S_DUR_HEADLESS, IETF_USERNAME_DEVICE-SPONSOR

Many headless devices have been registered via the Device Registration portal. Here we're validating whether the authenticating device was registered as a game console, media player or printer and that the device account is enabled and hasn't expired.

This is an example of using a downloadable user role. The sponsor's username is also returned.

Radius:Hewlett-Packard-Enterprise	HPE-CPPM-Role	=	class ipv4 DHCP match udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 67 exit class ipv4 DNS match udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 53 exit class ipv4 HTTPS-ANY match tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 443 exit class ipv4 WLC-ANY match ip 0.0.0.0 255.255.255.255 100.66.10.0 255.255.255.0 exit policy user HEADLESS class ipv4 DHCP action permit class ipv4 DNS action permit class ipv4 HTTPS-ANY action permit class ipv4 WLC-ANY action permit exit aaa authorization user-role name HEADLESS policy HEADLESS reauth-period 86400 vlan-name EDGE_HEADLESS exit

6

(Authorization:[Endpoints Repository]:Category *BELONGS_TO* VoIP Phone, Video Conferencing)	ROLE_AOS-S_VOICE, IETF_USERNAME_DEVICE-NAME

Based on profiling data, we're authorizing devices categorized as VoIP Phone and Video Conferencing by sending back a **VOICE** user role along with the profiled device name as the username (as an example).

	Type	Name		Value
1.	Radius:IETF	User-Name	=	%{Authorization:[Endpoints Repository]:Device Name}

7

(Tips:Role *EQUALS* DEVICE_ACCESS-POINT)	ROLE_AOS-S_DUR_HEADLESS, IETF_USERNAME_DEVICE-NAME

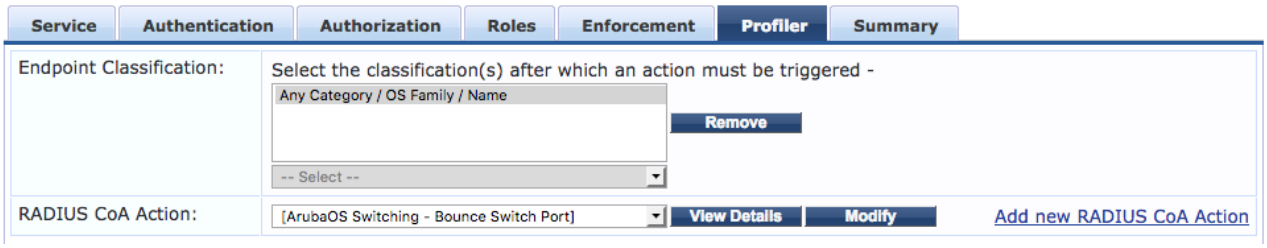
The last rule checks for a TIPS role/tag of DEVICE_ACCESS-POINT from the role mapping and assigns the **HEADLESS** downloadable user role and returns the device name as the username like in rule 5.

Profiler

The Profiler function allows for an unknown device to be automatically disconnected from the network once profile data has been collected and evaluated. This prevents a device from being "stuck" in a limited access role. During the second authentication, the new profile data can be used in the policy decision. This is a very common feature for MAC Authentication services.

Since we may want to drop a newly profiled device into a new user role with a different VLAN, the port will need to be bounced to force the device to re-DHCP.

Use caution in voice environments where client devices are connected behind a voice device. Bouncing a port after profiling a new device connected behind the voice device could result in interruption of voice service.



NOTE: In ClearPass 6.6.X, this enforcement profile is called **[HPE Bounce Host-Port]**. It was renamed to **[ArubaOS Switching – Bounce Switch Port]** in the 6.7.0 release.

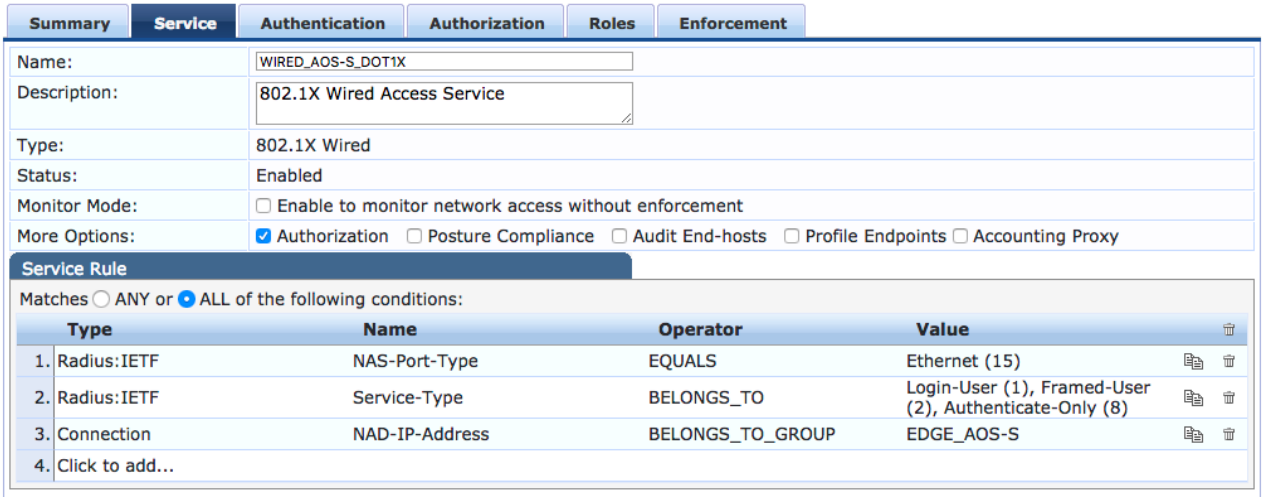
ClearPass: 802.1X

Service Configuration

Create a new service of type **802.1X Wired**.

Under More Options, check the **Authorization** boxes. The default service rules will work with an ArubaOS-Switch.

If there is a need to restrict the service to a particular group of switches, you can use a **Connection** | **NAD-IP-Address** | **BELONGS_TO_GROUP** rule to reference a NAD group as seen in rule 3 below.



Authentication

This service will be supporting both secure certificate-based authentication (EAP-TLS) and traditional, legacy username and password authentication (PEAPv0/EAP-MSCHAPv2).

The username and password-based authentication will be used for two purposes:

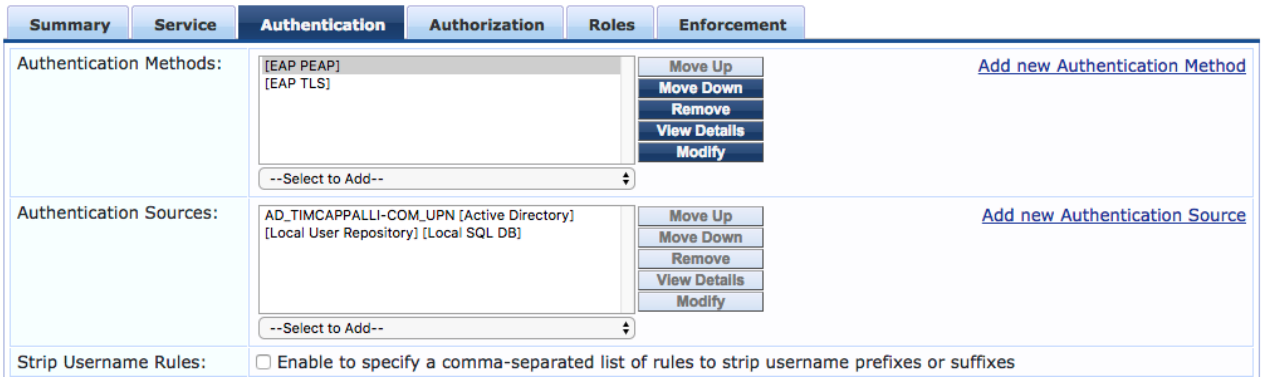
1) Allow a BYOD device to initially connect and kick off the Onboard process to allow a certificate to be issued
2) Allow for domain-joined assets to use their computer/machine account to authenticate to the network as well as support machine + user workflows

Based on the above requirements, remove all the default EAP methods from the Authentication Methods list on the Authentication tab except for **[EAP PEAP]** and **[EAP TLS]**.

> **NOTE:** The default **[EAP TLS]** method does not have OCSP authorization configured and is being used here solely as an example. OCSP is used to check real-time validity of a certificate and enabling it is highly recommended. Special care should be taken when authenticating certificates from different certificate authorities. This is outside the scope of this document.

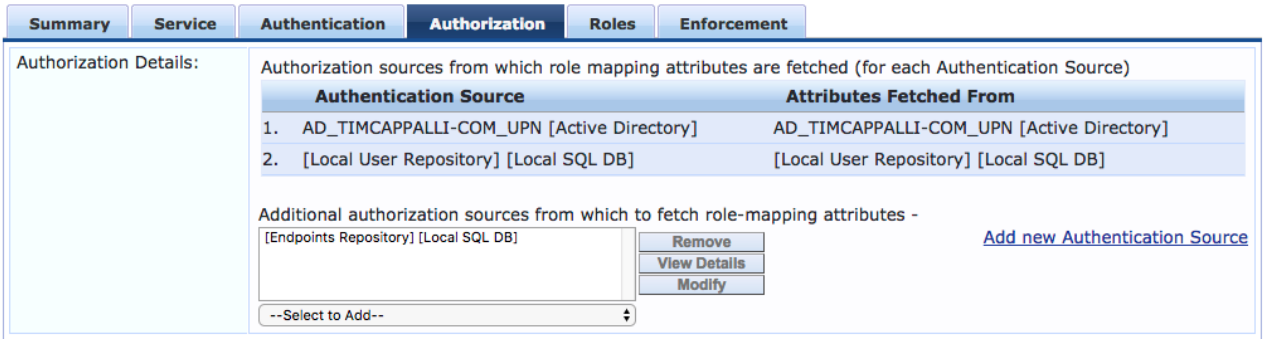
For Authentication Sources, you'll add our Active Directory identity store and also the **`[Local User Repository]`**. Authentication sources will vary in your environment.

The Local User Repository will be used in the example for infrastructure accounts like having an access point or VoIP phone authenticate securely to the network using the 802.1X framework.



Authorization

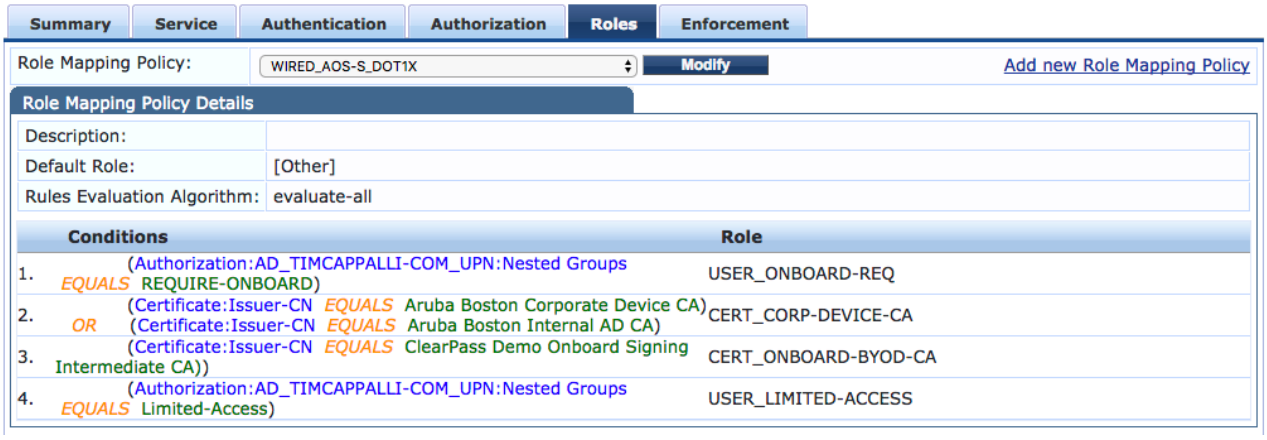
Since device profile information will be leveraged in policy, add the **`[Endpoints Repository]`** to the "Additional authorization sources…" list as shown below.



Roles

Role mapping is used to tag devices and users with as much prevalent information as possible for use in a policy decision.

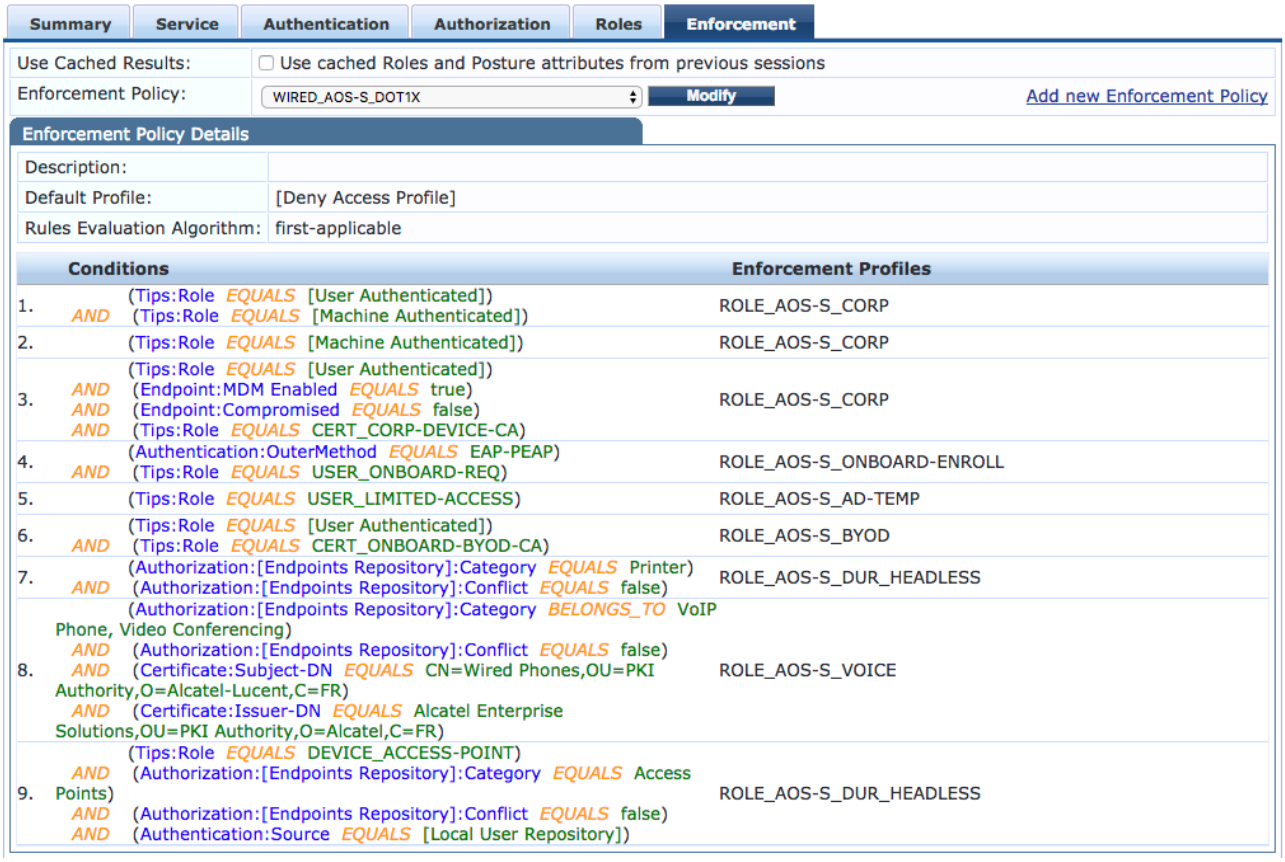
These rules and tags will vary greatly by environment, but below you'll find examples of device and user tagging.



- Rules 1 and 4 are checking group membership from Active Directory
- Rules 2-3 are matching on the common name of the issuing CA for the authenticating certificate

Enforcement

Let's take apart this enforcement policy rule by rule:



Summary | Service | Authentication | Authorization | Roles | Enforcement

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

Enforcement Policy: WIRED_AOS-S_DOT1X [Modify] Add new Enforcement Policy

Enforcement Policy Details

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

	Conditions	Enforcement Profiles
1.	(Tips:Role *EQUALS* [User Authenticated]) *AND* (Tips:Role *EQUALS* [Machine Authenticated])	ROLE_AOS-S_CORP
2.	(Tips:Role *EQUALS* [Machine Authenticated])	ROLE_AOS-S_CORP
3.	(Tips:Role *EQUALS* [User Authenticated]) *AND* (Endpoint:MDM Enabled *EQUALS* true) *AND* (Endpoint:Compromised *EQUALS* false) *AND* (Tips:Role *EQUALS* CERT_CORP-DEVICE-CA)	ROLE_AOS-S_CORP
4.	(Authentication:OuterMethod *EQUALS* EAP-PEAP) *AND* (Tips:Role *EQUALS* USER_ONBOARD-REQ)	ROLE_AOS-S_ONBOARD-ENROLL
5.	(Tips:Role *EQUALS* USER_LIMITED-ACCESS)	ROLE_AOS-S_AD-TEMP
6.	(Tips:Role *EQUALS* [User Authenticated]) *AND* (Tips:Role *EQUALS* CERT_ONBOARD-BYOD-CA)	ROLE_AOS-S_BYOD
7.	(Authorization:[Endpoints Repository]:Category *EQUALS* Printer) *AND* (Authorization:[Endpoints Repository]:Conflict *EQUALS* false)	ROLE_AOS-S_DUR_HEADLESS
8.	(Authorization:[Endpoints Repository]:Category *BELONGS_TO* VoIP Phone, Video Conferencing) *AND* (Authorization:[Endpoints Repository]:Conflict *EQUALS* false) *AND* (Certificate:Subject-DN *EQUALS* CN=Wired Phones,OU=PKI Authority,O=Alcatel-Lucent,C=FR) *AND* (Certificate:Issuer-DN *EQUALS* Alcatel Enterprise Solutions,OU=PKI Authority,O=Alcatel,C=FR)	ROLE_AOS-S_VOICE
9.	(Tips:Role *EQUALS* DEVICE_ACCESS-POINT) *AND* (Authorization:[Endpoints Repository]:Category *EQUALS* Access Points) *AND* (Authorization:[Endpoints Repository]:Conflict *EQUALS* false) *AND* (Authentication:Source *EQUALS* [Local User Repository])	ROLE_AOS-S_DUR_HEADLESS

1

	(Tips:Role *EQUALS* [User Authenticated])	
AND	(Tips:Role *EQUALS* [Machine Authenticated])	ROLE_AOS-S_CORP

When a Windows device authenticates to the network using its Active Directory computer account, the `[Machine Authenticated]` tag/TIPS role is added to the session automatically.

If both a machine and user authentication have occurred, then return the `CORP` user role.

This is commonly used to validate that the user is using a corporate asset.

2

	(Tips:Role *EQUALS* [Machine Authenticated])	ROLE_AOS-S_CORP

This checks for a Machine-only authentication. These typically occur when the device is sitting at the Windows logon screen and connectivity is required for updates, remote access or for new users to log in.

3

	(Tips:Role *EQUALS* [User Authenticated])	
AND	(Endpoint:MDM Enabled *EQUALS* true)	
AND	(Endpoint:Compromised *EQUALS* false)	ROLE_AOS-S_CORP
AND	(Tips:Role *EQUALS* CERT_CORP-DEVICE-CA)	

This is a typical rule to deal with a non-Windows corporate-managed asset that is managed by an EMM solution.

The two endpoint attributes have been synced down from the EMM solution via ClearPass Exchange. In this case, the rule is evaluating whether the device has its device management enabled and that no compromise has occurred.

The last condition checks for the tag/TIPS role from our role mapping to verify the certificate used to authenticate was issued from the Corporate Device CA.

4

	(Authentication:OuterMethod *EQUALS* EAP-PEAP)	
AND	(Tips:Role *EQUALS* USER_ONBOARD-REQ)	ROLE_AOS-S_ONBOARD-ENROLL

Most personal devices will perform Onboarding through the captive portal workflow after 802.1X fails, but some users may authenticate via PEAPv0/EAP-MSCHAPv2 when prompted by their device.

This rule will catch those users who need to be using EAP-TLS authentication via ClearPass Onboard.

The user role **ONBOARD-ENROLL** and the Onboard enrollment URL are being returned to the switch.

	Type	Name		Value
1.	Radius:Hewlett-Packard-Enterprise	HPE-User-Role	=	ONBOARD-ENROLL
2.	Radius:Hewlett-Packard-Enterprise	HPE-Captive-Portal-URL	=	https://clearpass-demo.arubaboston.com/onboard/wired_onboard_1.php

---

5

	(Tips:Role *EQUALS* USER_LIMITED-ACCESS)	ROLE_AOS-S_AD-TEMP

This is a basic rule as an example of a security exception for a group of users. These devices are dropped into the **AD-TEMP** role.

6

	(Tips:Role *EQUALS* [User Authenticated])	
AND	(Tips:Role *EQUALS* CERT_ONBOARD-BYOD-CA)	ROLE_AOS-S_BYOD

After a device has been onboarded, subsequent authentications will occur via EAP-TLS. Rule 6 uses the tag from the role mapping to check the common name of the issuing CA. These devices will be dropped into a **BYOD** role.

7

```
(Authorization:[Endpoints Repository]:Category EQUALS Printer)
AND (Authorization:[Endpoints Repository]:Conflict EQUALS false)        ROLE_AOS-S_DUR_HEADLESS
```

Here the device category of Printer is being evaluated along with a check of the **`Conflict`** flag. Username/password vs certificate authentication in this case is irrelevant, however, an additional condition could easily be added similar to rules 8 and 9 below.

This example uses the **`HEADLESS`** downloadable user role.

```
Radius:Hewlett-Packard-Enterprise   HPE-CPPM-Role   =   class ipv4 DHCP
                                                       match udp 0.0.0.0 255.255.255.255 0.0.0.0
                                                       255.255.255.255 eq 67
                                                       exit
                                                       class ipv4 DNS
                                                       match udp 0.0.0.0 255.255.255.255 0.0.0.0
                                                       255.255.255.255 eq 53
                                                       exit
                                                       class ipv4 HTTPS-ANY
                                                       match tcp 0.0.0.0 255.255.255.255 0.0.0.0
                                                       255.255.255.255 eq 443
                                                       exit
                                                       class ipv4 WLC-ANY
                                                       match ip 0.0.0.0 255.255.255.255 100.66.10.0
                                                       255.255.255.0
                                                       exit

                                                       policy user HEADLESS
                                                       class ipv4 DHCP action permit
                                                       class ipv4 DNS action permit
                                                       class ipv4 HTTPS-ANY action permit
                                                       class ipv4 WLC-ANY action permit
                                                       exit

                                                       aaa authorization user-role name HEADLESS
                                                       policy HEADLESS
                                                       reauth-period 86400
                                                       vlan-name EDGE_HEADLESS
                                                       exit
```

8

```
(Authorization:[Endpoints Repository]:Category BELONGS_TO
VoIP Phone, Video Conferencing)
  AND (Authorization:[Endpoints Repository]:Conflict EQUALS false)
  AND (Certificate:Subject-DN EQUALS CN=Wired Phones,OU=PKI        ROLE_AOS-S_VOICE
Authority,O=Alcatel-Lucent,C=FR)
  AND (Certificate:Issuer-DN EQUALS Alcatel Enterprise
Solutions,OU=PKI Authority,O=Alcatel,C=FR)
```

Many voice devices come from the factory with an embedded certificate that can be used for network authentication. The phone's factory cert is being leveraged for EAP-TLS combined with profiling data. The **`VOICE`** user role is being passed back for these devices.

9

```
(Tips:Role EQUALS DEVICE_ACCESS-POINT)
  AND (Authorization:[Endpoints Repository]:Category EQUALS Access
Points)                                                  ROLE_AOS-S_DUR_HEADLESS
  AND (Authorization:[Endpoints Repository]:Conflict EQUALS false)
  AND (Authentication:Source EQUALS [Local User Repository])
```

As discussed during the authentication section, a local user account was created in ClearPass for use by access points to authenticate. Rule 9 is comparing the tag/TIPS role, category, conflict status and verifying the authentication source was the **`[Local User Repository]`**. The **`HEADLESS`** downloadable user role is being used like in rule 7.

ClearPass: Web Authentication

The Web Authentication service handles captive portal-based authentications with server-initiated workflows.

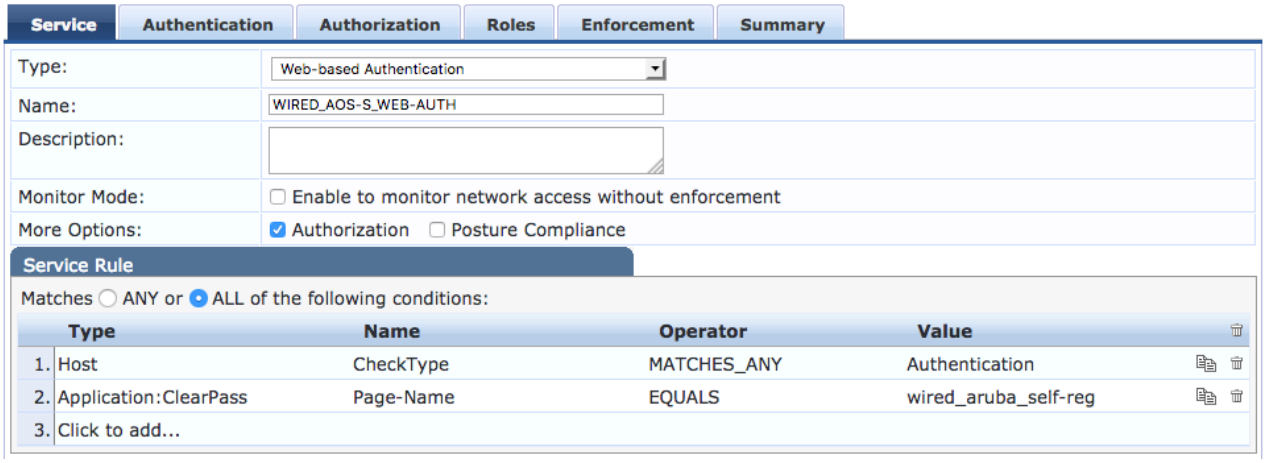
Service Configuration

Create a new service of type **`Web-based Authentication`**.

Check the **`Authorization`** box and select **`Matches ALL`** under Service Rule.

Add a second service rule with **`Application:ClearPass`** | **`Page-Name`** | **`EQUALS`** and then the page name.

For example: if the full page URL is `https://<fqdn>/guest/wired_aruba_self-reg.php`, then the page name is: `wired_aruba_self-reg`.

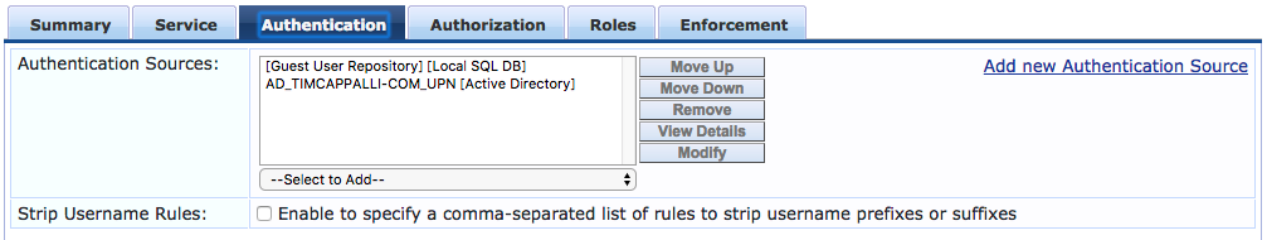


NOTE: The Page-Name attribute was added in ClearPass 6.7.0. Skip if using ClearPass 6.6.X.

Authentication

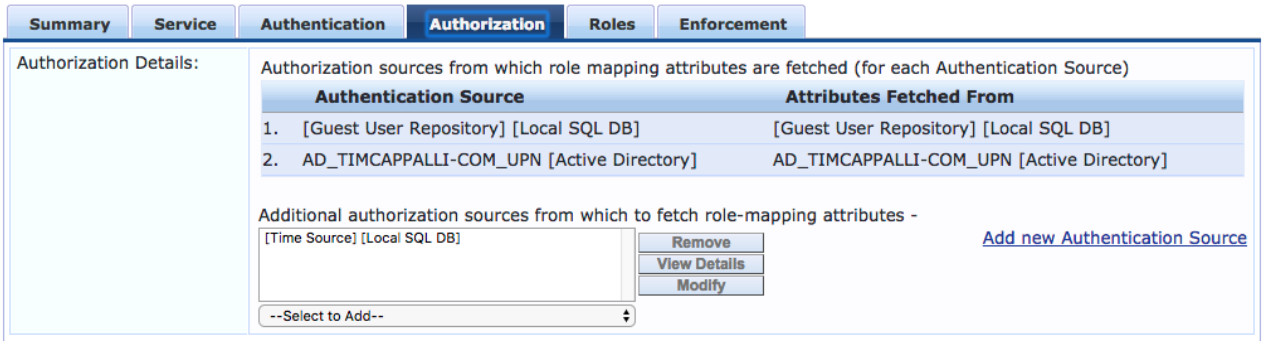
This service will be supporting both guest and Active Directory users for captive portal login.

For Authentication Sources, you'll add the **`[Guest User Repository]`** and also our Active Directory identity store. Authentication sources will vary in your environment.



Authorization

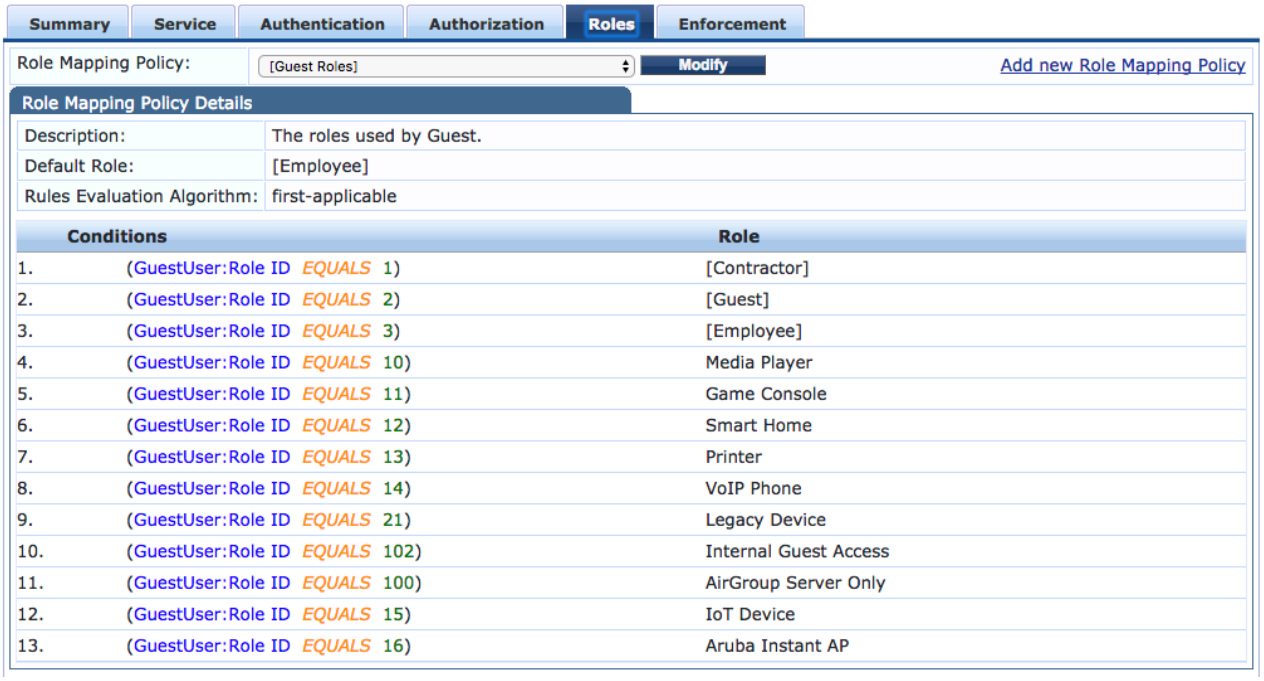
We will need to assign a manual expiration time to AD users. This time is calculated by the **[Time Source]** so it will need to be added as an additional authorization source.



Roles

In this scenario, guests and contractors will go through a standard self-registration process and any employee who authenticates with their corporate credentials will get a temporary guest role. Since there is no specific mapping of AD group, you'll use the generic **[Guest Roles]** role map.

If different enforcement actions will be taken for different groups or classifications of users, create a new role map like the in 802.1X configuration.



Enforcement

Because the server-initiated workflow is used with ArubaOS-Switch, the enforcement policy for the WEBAUTH service is very simple. The goal is to update the device endpoint record with attributes from the user authentication that will be stored and used for subsequent authentications and then bounce the port to trigger a reauthentication event.

> **Note:** If a VLAN change is not required, a Terminate Session disconnect message can be used instead of a port bounce.

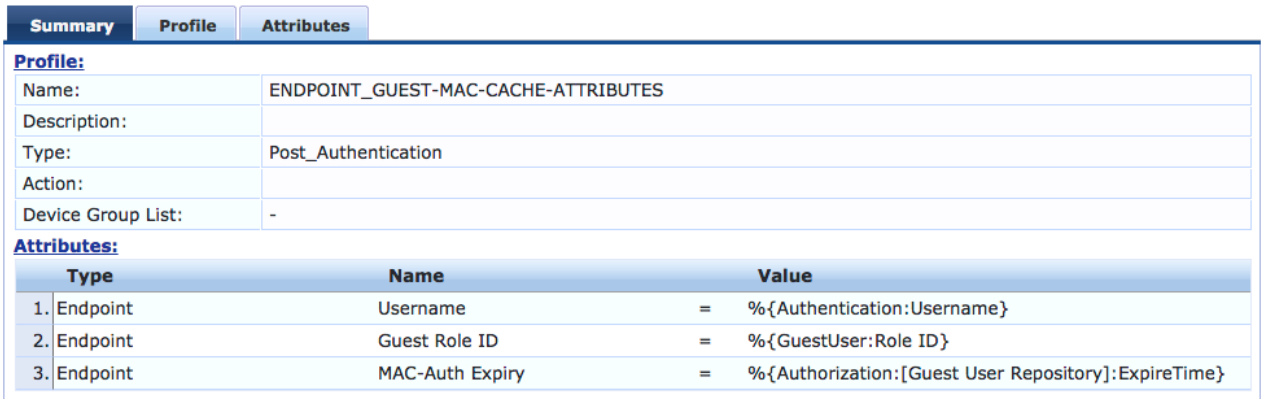
In this example, both guest and Active Directory accounts are being used.

For the guest accounts, a basic enforcement profile for MAC caching the user needs to be set up so when they re-authenticate after the port bounce, the user will not be prompted to authenticate again until their account expires.

Before creating the enforcement policy, create a new enforcement profile for the guest users (**`Configuration » Enforcement » Profiles » Add Enforcement Profile`**).

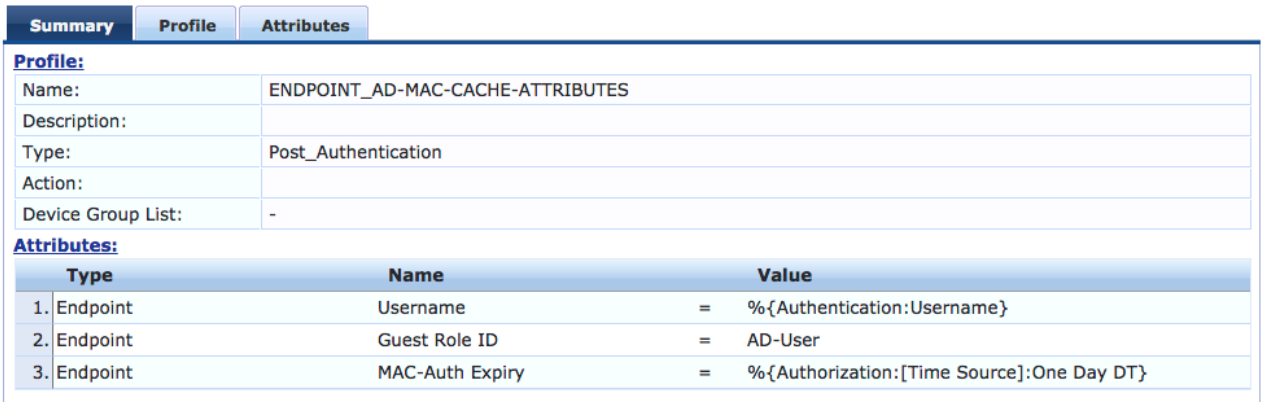
1. Select `ClearPass Entity Update Enforcement` from the Template dropdown
2. Give the profile a name
3. On the attributes tab, add the 3 entries below and then save.
   Note that the value field will require manual entry (copy and paste the values below).

TYPE	NAME	VALUE
Endpoint	`Username`	`%{Authentication:Username}`
Endpoint	`Guest Role ID`	`%{GuestUser:Role ID}`
Endpoint	`MAC-Auth Expiry`	`%{Authorization:[Guest User Repository]:ExpireTime}`

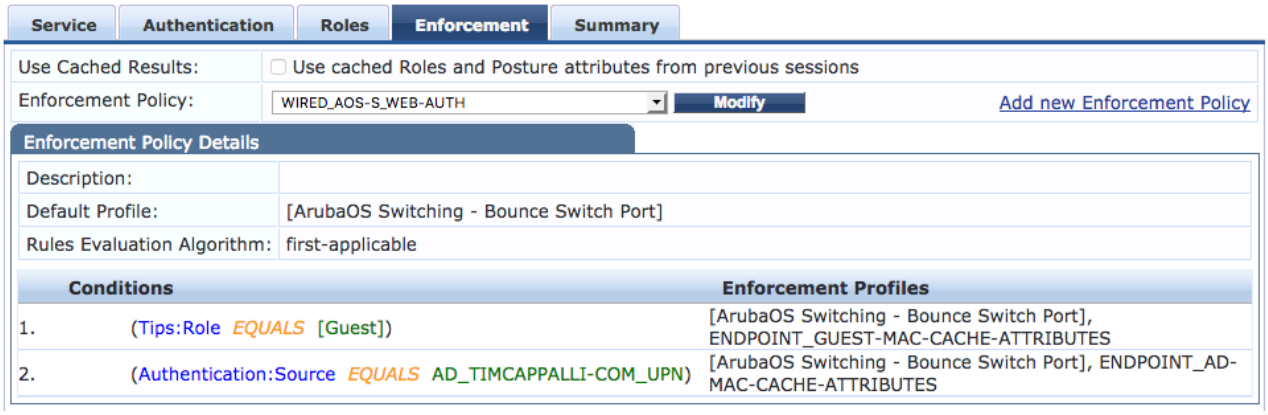


Next, create an enforcement profile for the AD users following a similar process. Since captive portal-based access should only be temporary for employees, a manual expiration of one day will be used via **[Time Source]**, a pre-built authentication source

TYPE	NAME	VALUE
Endpoint	Username	%{Authentication:Username}
Endpoint	Guest Role ID	AD-User
Endpoint	MAC-Auth Expiry	%{Authorization:[Time Source]:One Day DT}



Now, create a very basic enforcement policy. The first rule checks for a TIPS role / tag of **[Guest]**. The second rule checks that the Authentication Source is Active Directory. Both rules issue a CoA bounce switch port and then perform the appropriate endpoint update.

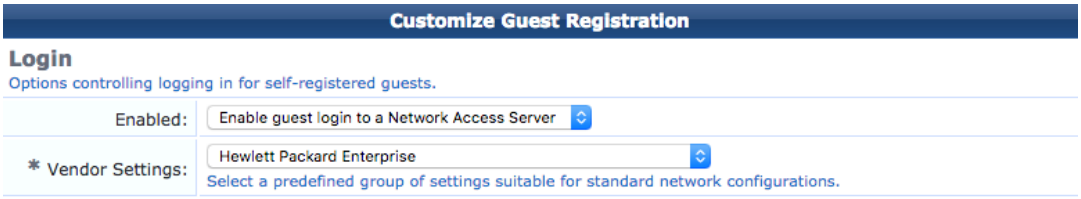


NOTE: In ClearPass 6.6.X, the enforcement profile **[HPE Bounce Host-Port]** is used.

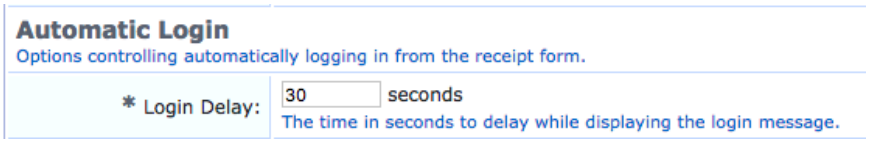
ClearPass: Guest

Configuring a self-registration workflow in Guest is outside the scope of the document. For the purposes of this guide, the only relevant settings on the guest side are the **NAS Vendor Settings** and the **Login Delay**.

Under **NAS Vendor Settings**, be sure the **Vendor Settings** are set to **Hewlett Packard Enterprise**. This will tell Guest to use a server-initiated login and which will craft a `WEBAUTH` request which is handled by the service we previously created.



Under **Login Delay**, set the value to a minimum of 30 seconds. This is required with server-initiated workflows because you don't want the user to attempt to browse while the port is still down or their device is re-authenticating. You may need to adjust this value in your environment.



Useful Switch Troubleshooting Commands and Tips

show port-access config

This is a very useful command that shows you the AAA functions enabled globally and on each port.

```
Port Access Status Summary

  Port-access authenticator activated [No] : Yes
  Allow RADIUS-assigned dynamic (GVRP) VLANs [No] : No
  Dot1x2010 Mode [Disabled] : Disabled              Use LLDP data to authenticate [No] : No

        802.1X  802.1X   Web      Mac      LMA   Cntrl Mixed    Speed
  Port  Supp    Auth     Auth     Auth     Auth  Dir   Mode     VSA   MBV
  ----- ------- -------- -------- -------- ----- ----- -------- ----- ---
  1     No      Yes      No       Yes      No    both  No       No    Yes
  2     No      Yes      No       Yes      No    both  No       No    Yes
  3     No      Yes      No       Yes      No    both  No       No    Yes
  4     No      Yes      No       Yes      No    both  No       No    Yes
  5     No      Yes      No       Yes      No    both  No       No    Yes
  6     No      Yes      No       Yes      No    both  No       No    Yes
  7     No      Yes      No       Yes      No    both  No       No    Yes
  8     No      Yes      No       Yes      No    both  No       No    Yes
  9     No      Yes      No       Yes      No    both  No       No    Yes
  10    No      Yes      No       Yes      No    both  No       No    Yes
  11    No      Yes      No       Yes      No    both  No       No    Yes
  12    No      Yes      No       Yes      No    both  No       No    Yes
  13    No      No       No       No       No    both  No       No    Yes
  14    No      No       No       No       No    both  No       No    Yes
```

show user-role

```
EDGE-2920# show user-role

 User Roles

  Enabled       : Yes
  Initial Role  : denyall

  Type       Name
  ---------- ------------------------------------------------------
  local      BYOD
  local      CORP
  local      GUEST
  local      VOICE
  local      SPLASH
  local      AD-TEMP
  local      PROFILE
  predefined denyall
  local      HEADLESS
  local      CONTACT-HD
  local      ONBOARD-ENROLL
  downloaded *ROLE_AOS_S_DUR_HEADLESS-3180-5
  downloaded *ROLE_AOS_S_DUR_T__AUTHENTICATED-3164-4
```

show user-role <role-name> detailed

```
EDGE-2920# show user-role SPLASH detailed

 User Role Information

   Name                            : SPLASH
   Type                            : local
   Reauthentication Period (seconds) : 0
   Untagged VLAN                   : EDGE_GUEST
   Captive Portal Profile          : use-radius-vsa
     URL                           : (use RADIUS VSA)
   Policy                          : CLEARPASS-REDIRECT

Statements for policy "CLEARPASS-REDIRECT"
policy user "CLEARPASS-REDIRECT"
     10 class ipv4 "DNS" action permit
     20 class ipv4 "DHCP" action permit
     30 class ipv4 "CLEARPASS-WEB" action permit
     40 class ipv4 "WEB-TRAFFIC" action redirect captive-portal
   exit

Statements for class IPv4 "DNS"
class ipv4 "DNS"
     10 match udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 53
   exit

Statements for class IPv4 "DHCP"
class ipv4 "DHCP"
     10 match udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 67
   exit

Statements for class IPv4 "CLEARPASS-WEB"
class ipv4 "CLEARPASS-WEB"
     10 match tcp 0.0.0.0 255.255.255.255 100.65.30.42 0.0.0.0 eq 80
     20 match tcp 0.0.0.0 255.255.255.255 100.65.30.42 0.0.0.0 eq 443
   exit

Statements for class IPv4 "WEB-TRAFFIC"
class ipv4 "WEB-TRAFFIC"
     10 match tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 80
     20 match tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 443
   exit
```

show port-access clients

Similar to `show user-table` on ArubaOS

```
EDGE-2920# show port-access clients

 Port Access Client Status

  Port  Client Name   MAC Address   IP Address      User Role         Type  VLAN
  ----- ------------- ------------- --------------- ----------------- ----- ----
  2     darth.vade... 00e04c-363b99 n/a             HEADLESS          MAC   815
  3     host/win10... 90e2ba-692d5a n/a             CORP              8021X 811
  6     HP IP Phone   2c4138-7fc880 100.81.3.10     VOICE             MAC   813
  7     Aruba AP      d8c7c8-cb497a n/a             HEADLESS          MAC   815
```

If ClearPass returned a user role, but the device is in a **denyall** role, there is likely a configuration issue with the user role. Run **show log -r** to display the system logs which should indicate an issue.

```
W 04/19/17 13:30:10 05208 dca: Failed to apply user role SPLASH to macAuth
            client 90E2BA692D5A on port 3: required CAPTIVE-PORTAL-URL VSA was
            not sent.
```

In this case, the role was configured to look for the captive portal redirect URL in the RADIUS response (use-radius-vsa) but the VSA was not present.

show port-access clients detailed <port>

```
EDGE-2920# show port-access clients detailed 3

 Port Access Client Status Detail

  Client Base Details :
   Port            : 3                    Authentication Type : 802.1x
   Client Status   : authenticated        Session Time        : 265 seconds
   Client name     : TIMCAPPALLI\tim      Session Timeout     : 86400 seconds
   MAC Address     : 90e2ba-692d5a
   IP              : 100.81.1.11

 User Role Information

   Name                            : CORP
   Type                            : local
   Reauthentication Period (seconds) : 86400
   Untagged VLAN                   : 811
   Tagged
VLANs                      :
   Captive Portal Profile          :
   Policy                          : PERMIT-ALL

Statements for policy "PERMIT-ALL"
policy user "PERMIT-ALL"
     10 class ipv4 "IP-ANY-ANY" action permit
   exit

Statements for class IPv4 "IP-ANY-ANY"
class ipv4 "IP-ANY-ANY"
     10 match ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
   exit
```

show user-role downloaded

```
EDGE-2930# show user-role downloaded
Downloaded user roles are preceded by *

 Downloaded User Roles

  Enabled       : Yes
  Type       Name
  ---------- ----------------------------------------------------
  downloaded *ROLE_AOS_S_DUR_PROFILE-3160-2
  downloaded *ROLE_AOS_S_DUR_HEADLESS-3180-5
  downloaded *ROLE_AOS_S_DUR_T__AUTHENTICATED-3164-4
```

show user-role downloaded detailed
show user-role <NAME> downloaded detailed

```
EDGE-2930# show user-role downloaded detailed
Downloaded user roles are preceded by *

 User Role Information

   Name                            : *ROLE_AOS_S_DUR_PROFILE-3160-2
   Type                            : downloaded
   Reauthentication Period (seconds) : 60
   Untagged VLAN                   : UNTRUST
   Tagged VLAN                     :
   Captive Portal Profile          :
   Policy                          : PROFILE_ROLE_AOS_S_DUR_PROFILE-3160-2

Statements for policy "PROFILE_ROLE_AOS_S_DUR_PROFILE-3160-2"
policy user "PROFILE_ROLE_AOS_S_DUR_PROFILE-3160-2"
     10 class ipv4 "DHCP_ROLE_AOS_S_DUR_PROFILE-3160-2" action permit
   exit


Statements for class IPv4 "DHCP_ROLE_AOS_S_DUR_PROFILE-3160-2"
class ipv4 "DHCP_ROLE_AOS_S_DUR_PROFILE-3160-2"
     10 match udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 67
   exit

   Tunnelednode Server Redirect    : Disabled
   Secondary Role Name             :

 User Role Information

   Name                            : *ROLE_AOS_S_DUR_HEADLESS-3180-5
   Type                            : downloaded
   Reauthentication Period (seconds) : 86400
   Untagged VLAN                   : SECURE-A
   Tagged VLAN                     :
   Captive Portal Profile          :
   Policy                          : HEADLESS_ROLE_AOS_S_DUR_HEADLESS-3180-5
```

SNMP-based Enforcement

Policy Enforcement

VLAN assignment via SNMP is the primary enforcement method with OnConnect. VLAN access control lists (ACLs) are commonly used to control traffic in this scenario.

Configuration Overview

Here are the hardware and software combinations used for this configuration:

- Aruba 2920 switch running ArubaOS-Switch 16.03.0003 (no version dependency, but 16.01 or greater is recommended)
- ClearPass Policy Manager 6.6.4 (required: 6.6.1+)

This configuration example uses SNMP v2c. SNMPv3 is also supported for OnConnect.

Quirks and Limitations

- Active user visibility is available for Windows domain-joined machines only
- OnConnect enforcement takes an average of 60 seconds with WMI enabled

Switch Configuration

Global switch configuration:

`snmp-server community OnConnectRO operator`	create SNMP ro community for ClearPass
`snmp-server community OnConnectRW operator unrestricted`	create SNMP rw community for ClearPass
`snmp-server host 4.3.2.1 community ClearPassOnConnect trap-level all`	set ClearPass as the snmp trap destination
`snmp-server trap-source 1.2.3.4`	set the SNMP trap source address
`snmp-server enable traps mac-notify`	enable MAC notify traps globally

Interface configuration:

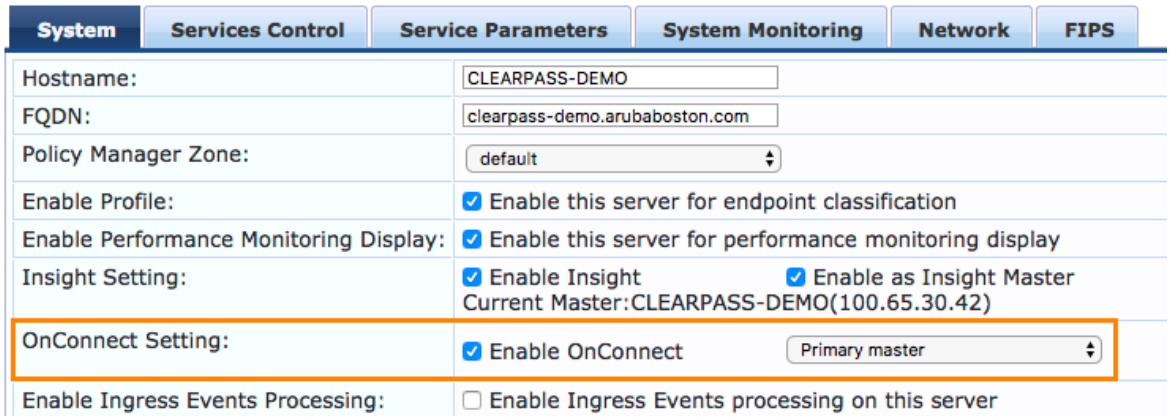
`snmp-server enable traps link-change 17-20`	enable link state traps for OnConnect interfaces
`interface 17-20 mac-notify traps learned` `interface 17-20 mac-notify traps removed`	enable MAC notifications for OnConnect interfaces
`Interface 17-20 untagged vlan 812`	set default untrusted VLAN

ClearPass: Basics

Server Configuration

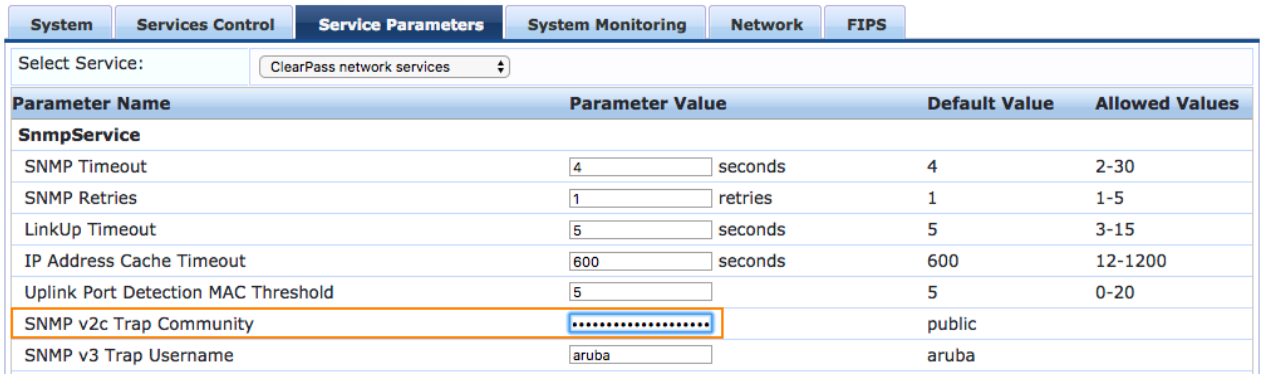
Enable OnConnect under Server Configuration (**`Administration » Server Manager » Server Configuration`**)

> **NOTE:** This is only required in ClearPass 6.6.X



Configure the **`SNMP v2c Trap Community`** under **`Administration » Server Manager » Server Configuration, Service Parameters, ClearPass network services`**.

This should match the community string defined in this switch configuration element: *`snmp-server host 100.65.30.42 community ClearPassOnConnect trap-level all`*



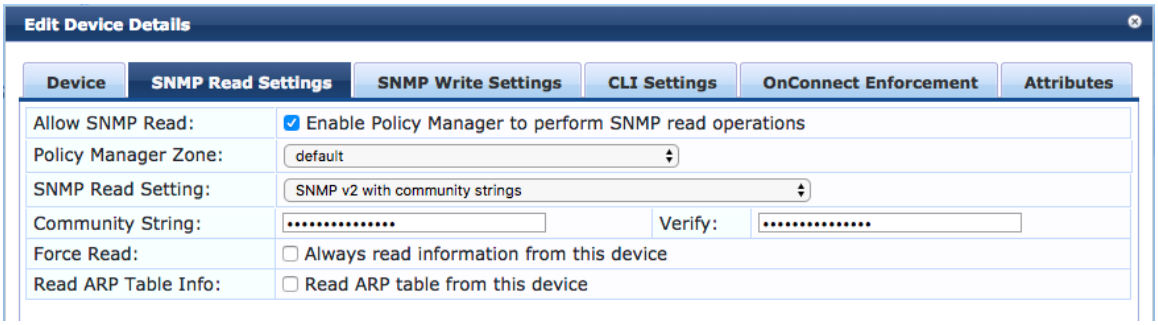
After changing the trap community, the **`System auxiliary services`** service needs to be restarted.

Navigate to **`Administration » Server Manager » Server Configuration, Services Control`** and locate **`System auxiliary services.`**

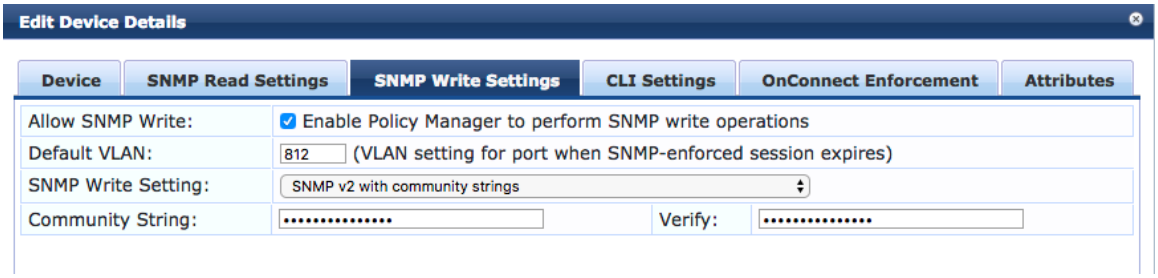
Click **Stop**. Once the service has stopped, click **Start** to restart the service.

Network Device

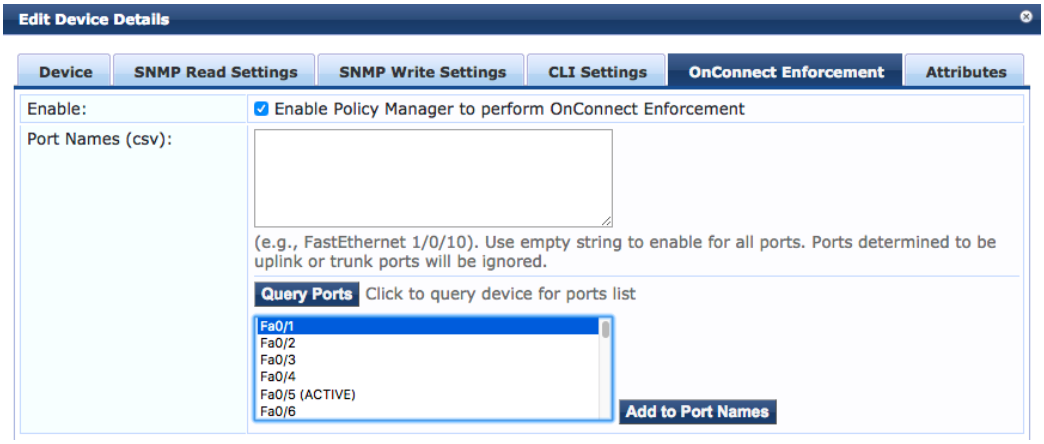
Enable SNMP Read and configure the community strings for the device:



Enable SNMP Write and configure the community strings for the device. Also, configure the Default VLAN (generally this will be the guest or untrusted VLAN):



Enable Policy Manager to perform OnConnect Enforcement:



Use the **`Query Ports`** button to test the SNMP configuration. The list will be populated with the switch ports if all is working correctly. Individual interfaces can also be enabled for OnConnect enforcement by selecting them in the list and clicking **`Add to Port Names`** (or by manually adding them to the Port Names list).

Windows Management Instrumentation (WMI) Overview

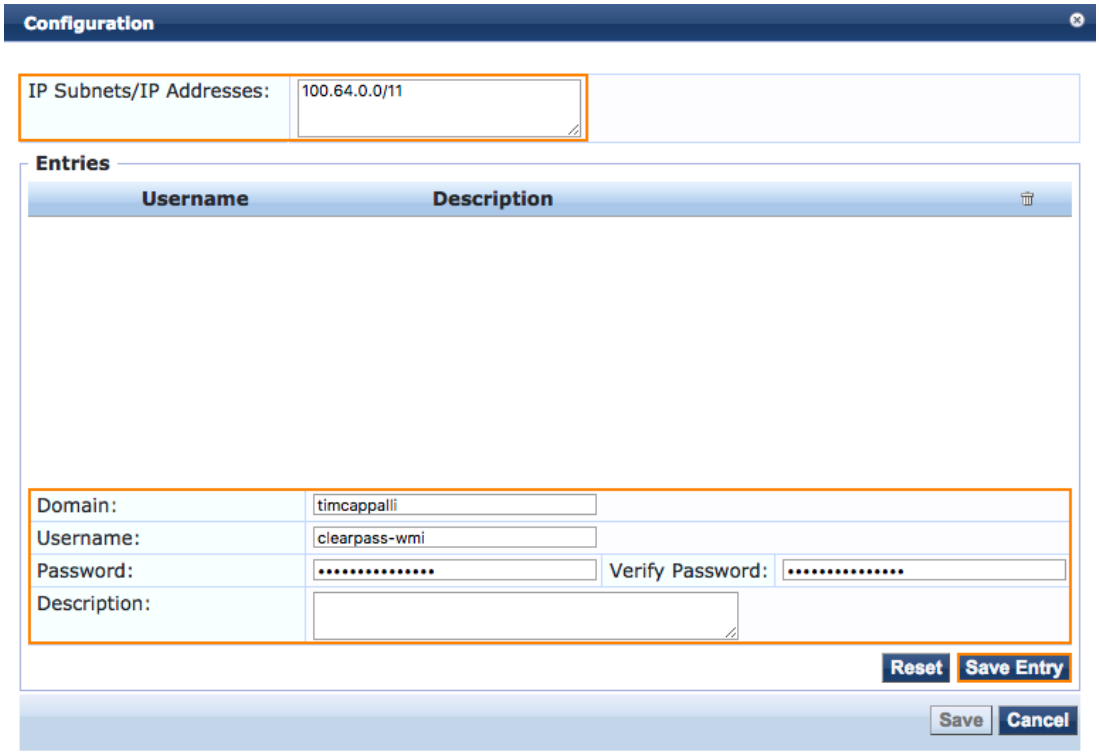
During a port status change, ClearPass can query domain-joined Windows devices for the current logged in user. This information can then be compared with user account information in Active Directory during authorization.

Requirements:

- Active Directory user account with WMI remote access privileges
- Windows firewall must allow inbound access to WMI from ClearPass

WMI Configuration: ClearPass

Inside ClearPass, map the WMI credentials to the edge subnets under **`Configuration » Profile Settings » WMI Configuration`**.

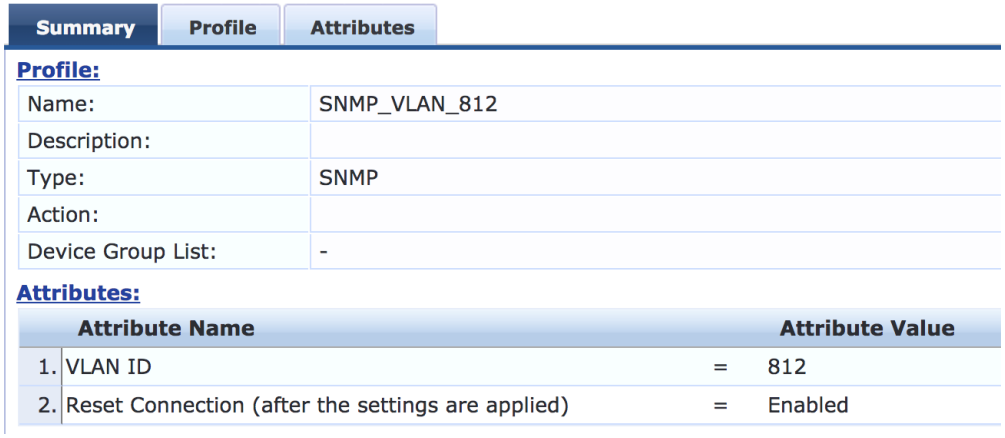


ClearPass: Enforcement Profiles

Enforcement profiles for OnConnect are very basic.

For each enforcement VLAN, create a new SNMP Based Enforcement profile. Navigate to **`Configuration » Enforcement » Profiles » Add Enforcement Profile`**. Select **`SNMP Based Enforcement`** from the template dropdown.

Add the **`VLAN ID`** and **`Reset Connection`** attributes. You can also optionally add the **`Session Timeout`** attribute to trigger a re-evaluation of policy after a certain amount of time.



Summary | Profile | Attributes

Profile:

Name:	SNMP_VLAN_812
Description:	
Type:	SNMP
Action:	
Device Group List:	-

Attributes:

	Attribute Name		Attribute Value
1.	VLAN ID	=	812
2.	Reset Connection (after the settings are applied)	=	Enabled

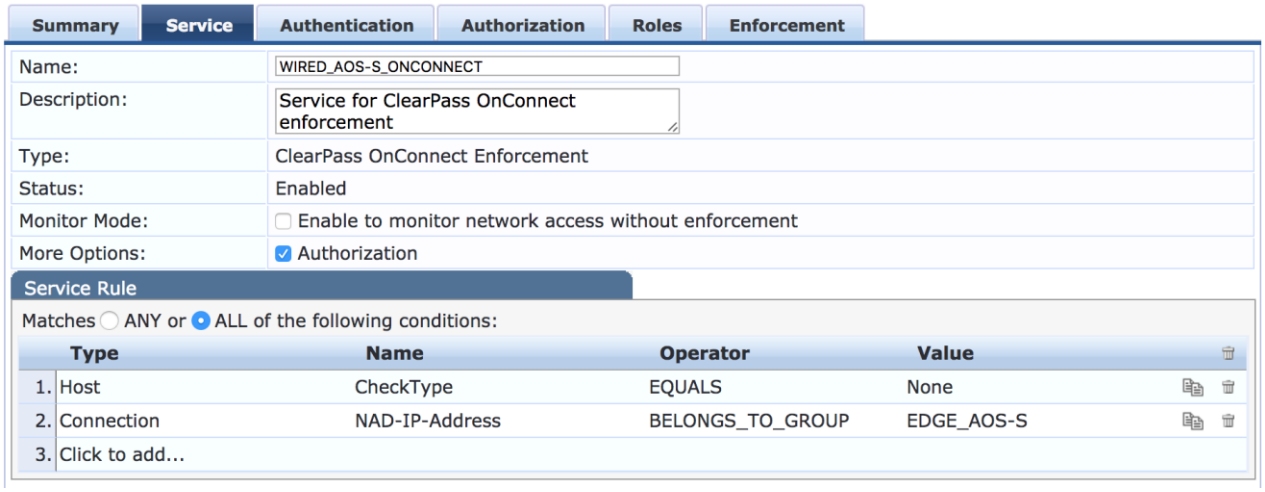
ClearPass: OnConnect Service

Service Configuration

Start with a new service of type **`ClearPass OnConnect Enforcement`**.

Under More Options, check the **`Authorization`**. This will enable the Authorization tab. The default service rules will work with an ArubaOS-Switch.

If there is a need to restrict the service to a particular set of switches, you can use a **`Connection`** | **`NAD-IP-Address`** | **`BELONGS_TO_GROUP`** service rule to reference a NAD group as seen in rule 2 below.



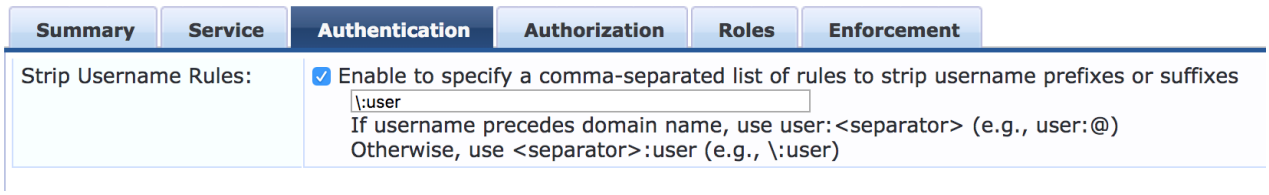
Authentication

Since OnConnect does not do any traditional user or device authentication, the only option available on the Authentication tab is the Strip Username Rules configuration.

If you are not planning to use WMI, nothing has to be configured on the Authentication tab.

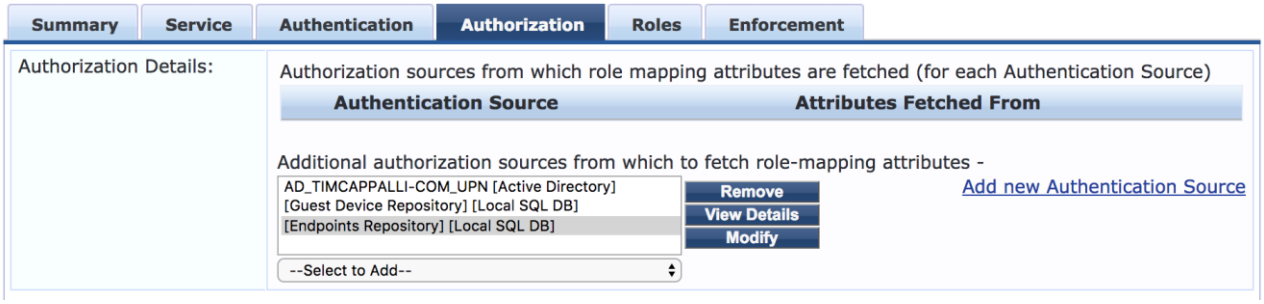
If you are planning to use WMI to grab the currently logged in user, the Strip Username Rules will need to be configured. WMI returns the username in down-level logon format (REALM\username) so the REALM will need to be stripped off before an authorization check can be done against Active Directory.

Use the **`\:user`** rule to strip the REALM from the down-level logon username.



Authorization

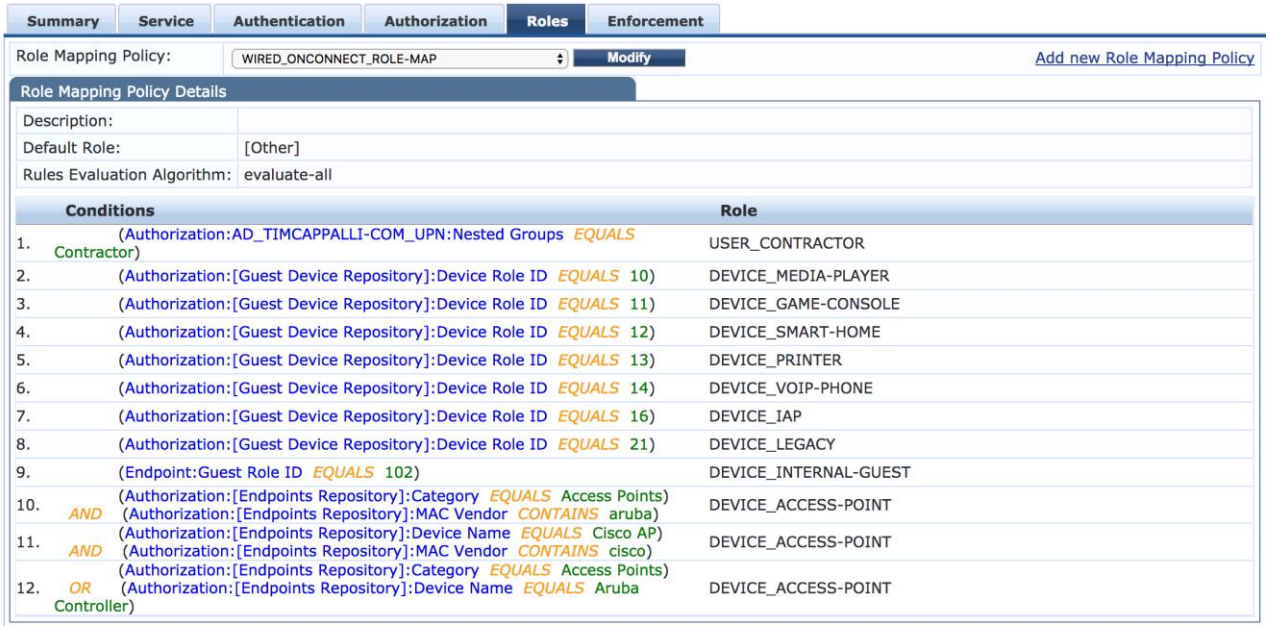
On the Authorization tab, add the **[Endpoints Repository]** and **[Guest Device Repository]** to the "Additional authorization sources…" list as shown below. If WMI-based authorization will be used, also add your Active Directory authentication source to the list so user properties can be evaluated.



Roles

Role mapping is used to tag devices and users with as much information as possible for use in a policy decision.

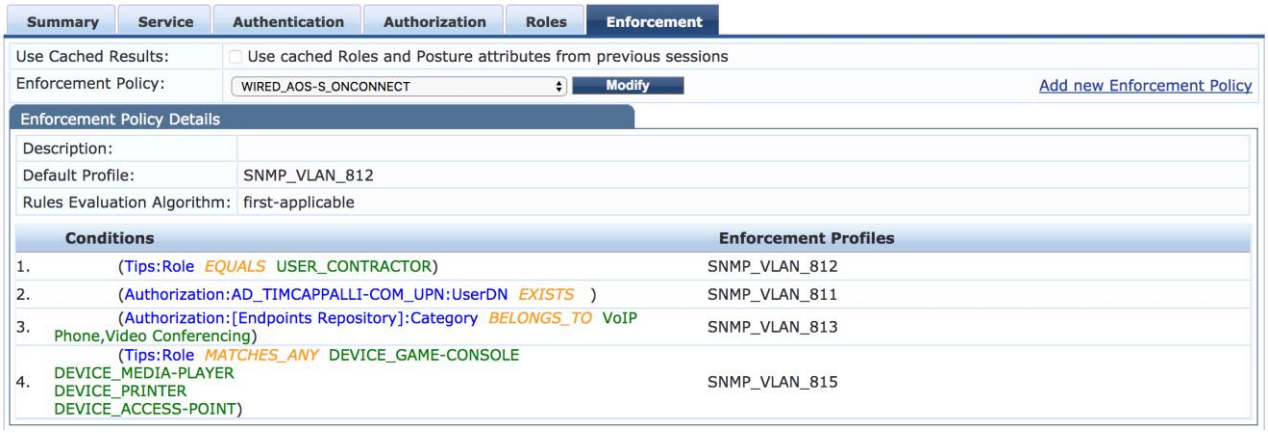
This *example* role map covers both headless devices and user mapping based off AD group membership. Headless devices are mapped using a mix of device registrations and raw profile data.



Enforcement

For the default policy, the default guest VLAN profile is specified. This is used when a request falls through the policy with no match which would be a guest in this case.

Let's take apart the enforcement rules one by one:



1

(Tips:Role *EQUALS* USER_CONTRACTOR)	SNMP_VLAN_812

If the logged in user is a member of the "Contractor" AD group, the `USER_CONTRACTOR` tag/TIPS Role is mapped. This device is then given the GUEST VLAN, 812 in this example.

2

(Authorization:AD_TIMCAPPALLI-COM_UPN:UserDN *EXISTS*)	SNMP_VLAN_811

This rule just checks that the logged in user is a domain user. All domain users will have a **`UserDN`** attribute. These devices will be placed into the "SECURE" VLAN, 811 in this case.

3

(Authorization:[Endpoints Repository]:Category *BELONGS_TO* VoIP Phone,Video Conferencing)	SNMP_VLAN_813

Profile data is being leveraged in rule 3 to drop voice devices into VLAN 813, the voice VLAN.

4

(Tips:Role *MATCHES_ANY* DEVICE_GAME-CONSOLE DEVICE_MEDIA-PLAYER DEVICE_PRINTER DEVICE_ACCESS-POINT)	SNMP_VLAN_815

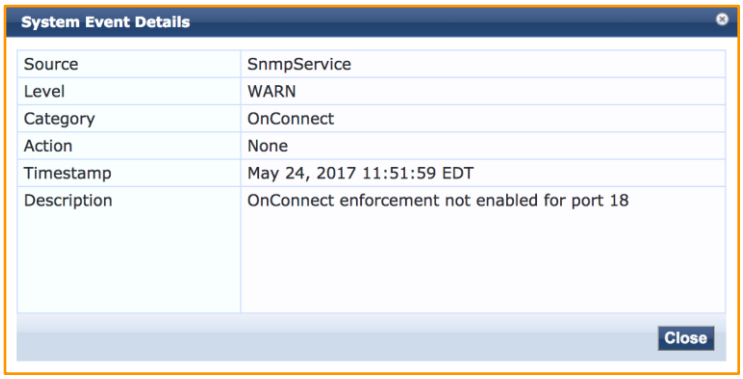
These tags/TIPS roles are mapped based on the role assigned during Device Registration. These registered devices will be dropped into the "HEADLESS" VLAN, 815 in this case.

Useful Troubleshooting Commands and Tips

ClearPass

If OnConnect requests are not appearing in Access Tracker, take a look in Event Viewer. Below are some common error messages.

- Traps are being sent by the switch, but the network device definition in ClearPass does not have the port listed for OnConnect enforcement.



- The SNMP trap community is mismatched

Switch

show snmp-server traps

This command will give you a summary of the switch's SNMP configuration.

```
Trap Receivers

  Link-Change Traps Enabled on Ports [All] : All

  Traps Category                          Current Status
  ____________________________________  __________________
  SNMP Authentication                   : Extended
  Password change                       : Enabled
  Login failures                        : Enabled
  Port-Security                         : Enabled
  Authorization Server Contact          : Enabled
  DHCP-Snooping                         : Enabled
  DHCPv6-Snooping Out of Resource       : Enabled
  DHCPv6-Snooping Errant Replies        : Enabled
  Dynamic ARP Protection                : Enabled
  Dynamic IP Lockdown                   : Enabled
  Dynamic IPv6 Lockdown Out of Resource : Enabled
  Dynamic IPv6 Lockdown Violations      : Enabled
  Startup Config change                 : Disabled
  Running Config Change                 : Disabled
  MAC address table changes             : Enabled

  DHCP-Server                           : Enabled
  NTP-Client                            : Disabled

  ND Snooping Out of Resources Traps    : Enabled

  Address               Community              Events   Type   Retry   Timeout
  --------------------- ---------------------- -------- ------ ------- -------
  100.65.30.42          ClearPassOnConnect     All      trap   3       15
```

show vlan port <X> detail

```
EDGE-2920# show vlan port 18 detail

 Status and Counters - VLAN Information - for ports 18

  Port name: ONCONNECT
  VLAN ID Name                | Status     Voice Jumbo Mode
  ------- ------------------- + ---------- ----- ----- --------
  812     EDGE_GUEST          | Port-based No    No    Untagged
```

debug snmp
debug destination session

Debug commands can be used for more advanced troubleshooting and to verify that the switch is sending traps to ClearPass. **debug snmp** enables all SNMP debugging and **debug destination session** will echo all of the debug text to the current session. To disable, use **no debug snmp**.

Per-Port Tunneled-Node (PPTN)

Policy Enforcement

Per-Port Tunneled-Node allows for the same enforcement options as a wireless client. This includes stateful session processing, deep packet inspection, URL filtering and bandwidth contracts.

Configuration Overview

The hardware and software requirements for Per-Port Tunneled-Node are:

- Aruba switch running ArubaOS-Switch 16.02 or greater:
  - 5400R
  - 3810M / 3800
  - 2930F / 2930M
  - 2920

  * Please refer to switch documentation for scalability numbers

- Aruba hardware mobility controller for tunnel termination running either ArubaOS 6.5+ or 8.1+
- ClearPass Policy Manager (no version dependency, but 6.6.4+ is recommended)

Here are the hardware and software combinations used for this example configuration:

- Aruba 2920 switch running ArubaOS-Switch 16.03.0003
- Aruba 7005 mobility controller (both ArubaOS 6.5.2 and 8.1.0.1 are used in the example)
- ClearPass Policy Manager 6.6.4

Because Per-Port Tunneled-Node uses the same guest configuration (client-initiated) as a wireless client, that portion will not be covered in this section.

Quirks and Limitations

- PPTN has a limit of 32 MAC addresses per port
- Each switch stack requires a unique VLAN for transport

Switch Configuration

Configuring Per-Port Tunneled-Node (PPTN) on an ArubaOS-Switch is very easy and only requires a few extra configuration elements.

`vlan 4013 name TN-TRANSPORT`	define tunneled-node transport VLAN (see explanation below)
`tunneled-node-server controller-ip 100.66.1.100`	enable dynamic authorization (CoA)
`papi-security key-value <key>`	*optional, only required if PAPI security is enabled on controller
`interface 13-16 tunneled-node-server`	enable tunneled-node on the appropriate ports
`interface 13-16 untagged vlan 4013`	assign same ports to TN transport VLAN

The tunneled-node transport VLAN is essentially a locally significant VLAN that needs to be defined on both the switch and controller. This VLAN does not have an L3 interface and should not be tagged upstream in the network. It is solely used inside the GRE tunnel.

With tunneled-node, the client device's VLAN is assigned and enforced by the controller. In a tunneled-node only deployment, no client device access networks need to be configured at the edge switch layer.

Aruba Controller Overview

From the controller perspective, tunneled-node traffic can leverage the same, pre-existing user roles and policies from a wireless deployment. You can even leverage the same client access VLANs.

For example: if the guest/open SSID uses a specific guest VLAN on the controller, that same VLAN can be used for wired guests via tunneled-node.

Another note: tunneled-node AAA configuration uses the same as a wired access interface on the controller. If your environment is already configured for authentication of the controller's switch ports, the existing configuration will work for tunneled-node client devices. The only configuration required in that case would be the TN transport VLAN.

Licensing

Per-Port Tunneled-Node is licensed in the same way as an access point and consumes 1 license set per switch stack. For centralized policy enforcement and visibility with PPTN, only AP and PEF licenses are required. If web filtering is required, WebCC would also be needed.

If the controller itself has all 4 licenses installed (AP, PEF, WebCC and RFProtect), one of each license will be consumed per switch stack, just like an access point.

For more information on ArubaOS 6.5 licensing, please see the ArubaOS 6.5 User Guide.

Aruba Controller Configuration

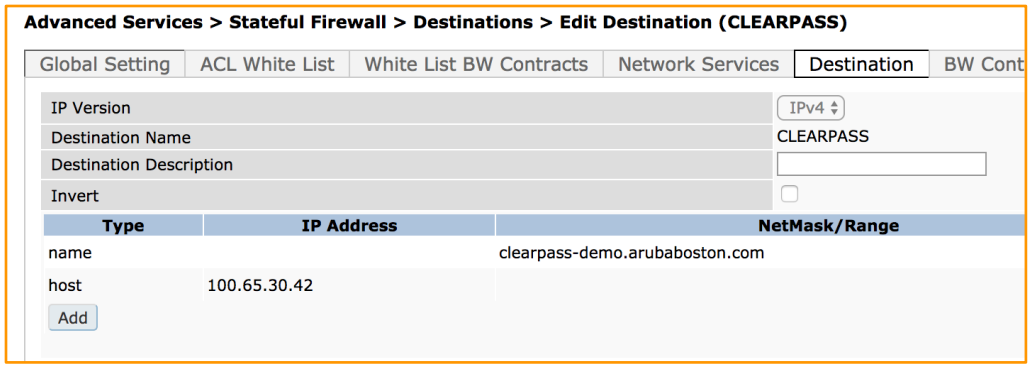
This section will cover ArubaOS 6.5. The configuration for ArubaOS 8 is nearly identical, it just uses the new hierarchical configuration model. This section also assumes your controller has already been configured with the basics (VLANs, IPs, NTP, licenses etc) and also that ClearPass has been defined as a RADIUS server and been placed into a RADIUS server group.

NOTE: If the controller you're working with is already configured to support wireless policy and the goal is to build a consistent policy across wired and wireless access, there is no need to configure new roles. The example below assumes there are no existing role or policy configurations on the controller.

Roles and Policies

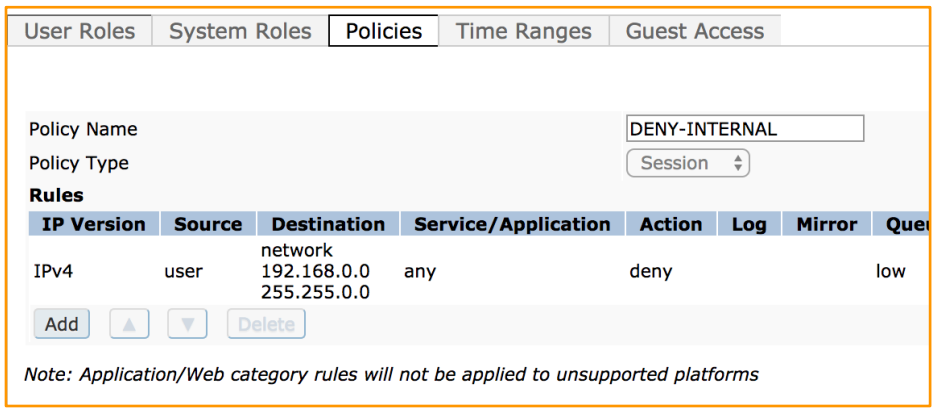
For this example, 7 roles will be created in the controller: `PROFILE`, `GUEST-ACCESS`, `SPLASH`, `HEADLESS`, `SECURE`, `ONBOARD-ENROLL` and `QUARANTINE`. Each of these roles will have an attached firewall policy.

First, create netdestination with entries for your ClearPass server(s):
`Configuration > Advanced Services > Stateful Firewall > Destinations`




```
netdestination CLEARPASS
 no description
 no invert
  name clearpass-demo.arubaboston.com position 1
  host 100.65.30.42 position 2
```

Next create a new policy that denies access to internal networks:
`Configuration > Security > Access Control > Policies > Add`




```
ip access-list session DENY-INTERNAL
alias user network 192.168.0.0 255.255.0.0 any deny
```

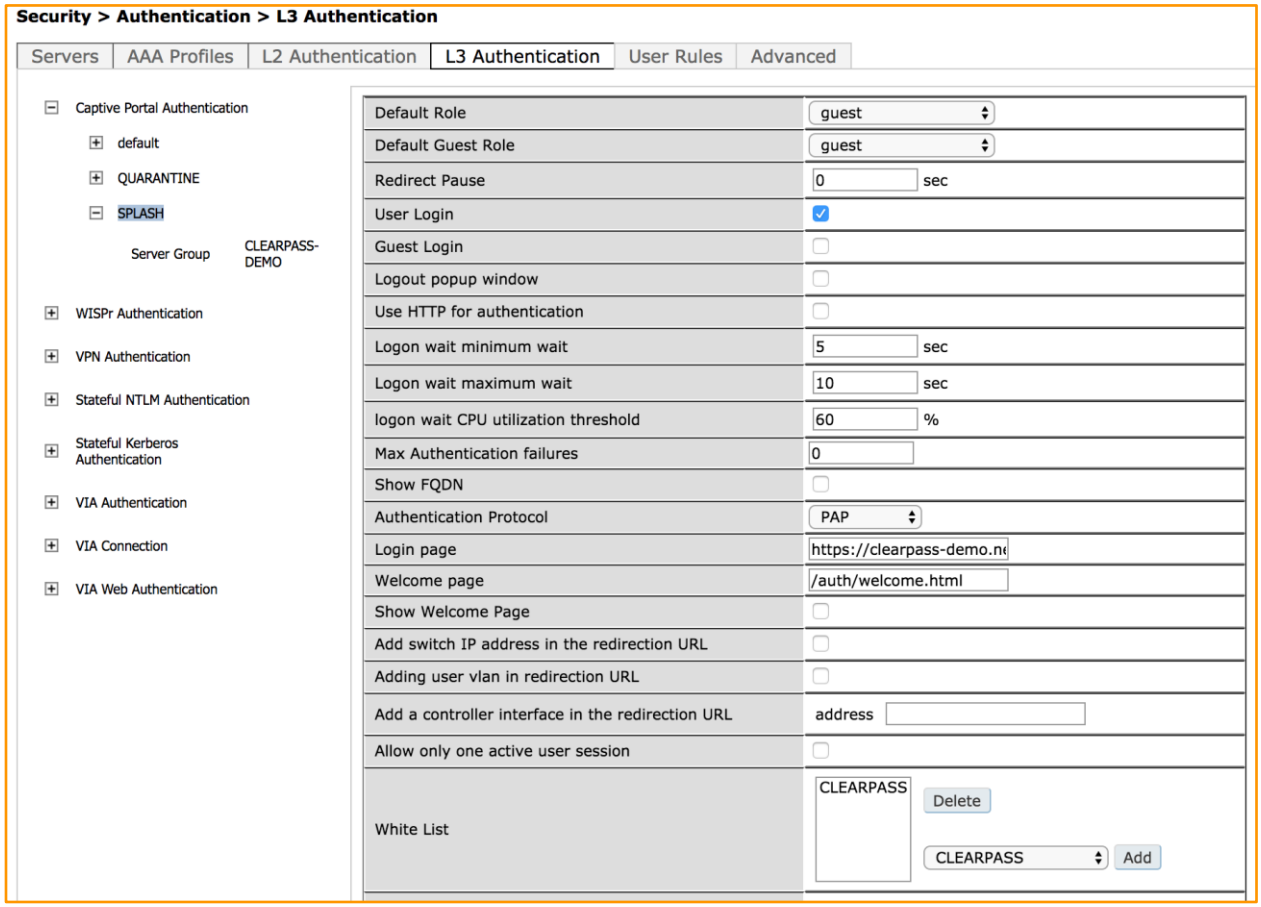
Also, create a policy that permits both DNS and DHCP.

```
ip access-list session DNS-DHCP
  any any svc-dhcp permit
  user any svc-dns permit
'
```

Now a captive portal profile: **`Configuration > Security > Authentication > L3 Authentication > Captive Portal Authentication > Add`**

- Set the Redirect Pause to 0
- Uncheck Logout popup window
- Set the **`Login page`** URL to the ClearPass guest self-registration page.
- Uncheck Show Welcome Page
- Add your ClearPass netdestination to the **`White List`**

Apply the config and then set the **`Server Group`** to the ClearPass RADIUS server group.



Now click back on the profile name and click **`Save As`** and call the new profile **`QUARANTINE.`**

- Uncheck User Login
- Change the **`Login page`** URL to the quarantine page

Repeat one more time for the **`ONBOARD-ENROLL`** profile.

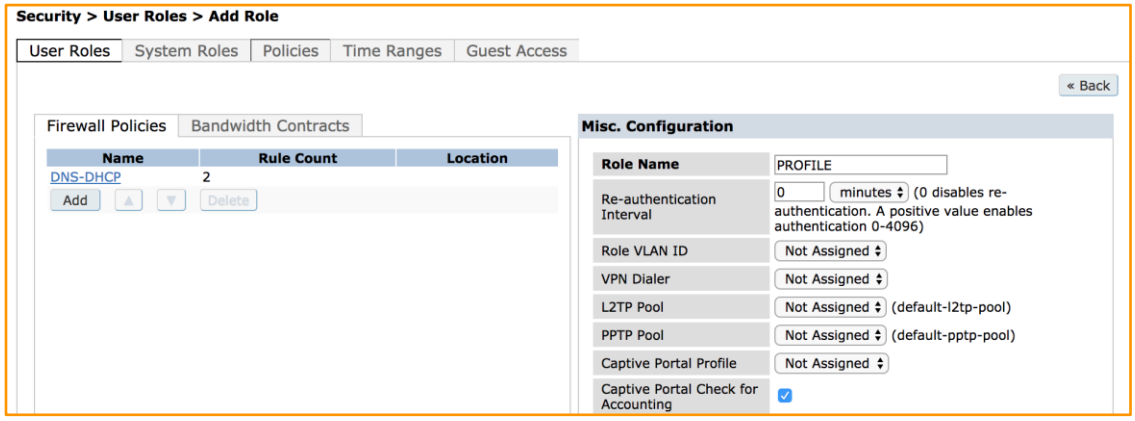
```
aaa authentication captive-portal SPLASH
  server-group CLEARPASS-DEMO
  redirect-pause 0
  no logout-popup-window
  login-page https://clearpass-demo.net.arubaboston.com/guest/wired_aruba_self-reg_pptn.php
  no enable-welcome-page
  white-list CLEARPASS
aaa authentication captive-portal QUARANTINE
      server-group CLEARPASS-DEMO
      no user-logon
  redirect-pause 0
  no logout-popup-window
  login-page https://clearpass-demo.net.arubaboston.com/guest/wired_aruba_self-reg_pptn.php
  no enable-welcome-page
  white-list CLEARPASS
```

Now create the 6 user roles. Only the first two roles will have a screenshot example.

`Configuration > Security > Access Control > User Roles > Add.`

PROFILE

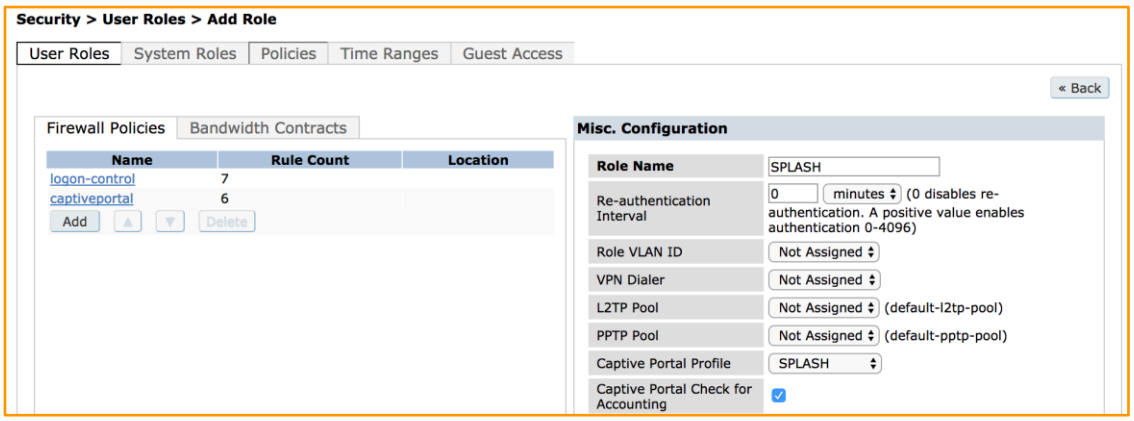
- Firewall Policies: **`DNS-DHCP`**




```
user-role PROFILE
access-list session DNS-DHCP
```

SPLASH

- Firewall Policies: logon-control, captiveportal
- Captive Portal Profile: **SPLASH**




```
user-role SPLASH
access-list session logon-control
access-list session captiveportal
 captive-portal SPLASH
```

ONBOARD-ENROLL

- Firewall Policies: logon-control, captiveportal
- Captive Portal Profile: **ONBOARD-ENROLL**

```
user-role ONBOARD-ENROLL
access-list session logon-control
access-list session captiveportal
 captive-portal ONBOARD-ENROLL
```

QUARANTINE

- Firewall Policies: logon-control, captiveportal
- Captive Portal Profile: **QUARANTINE**

```
user-role QUARANTINE
access-list session logon-control
access-list session captiveportal
 captive-portal QUARANTINE
```

GUEST-ACCESS

- Firewall Policies: logon-control, DENY-INTERNAL, allowall

```
user-role GUEST-ACCESS
access-list session logon-control
access-list session DENY-INTERNAL
access-list session allowall
```

SECURE

- Firewall Policies: **`allowall`**

```
user-role SECURE
access-list session allowall
```

HEADLESS

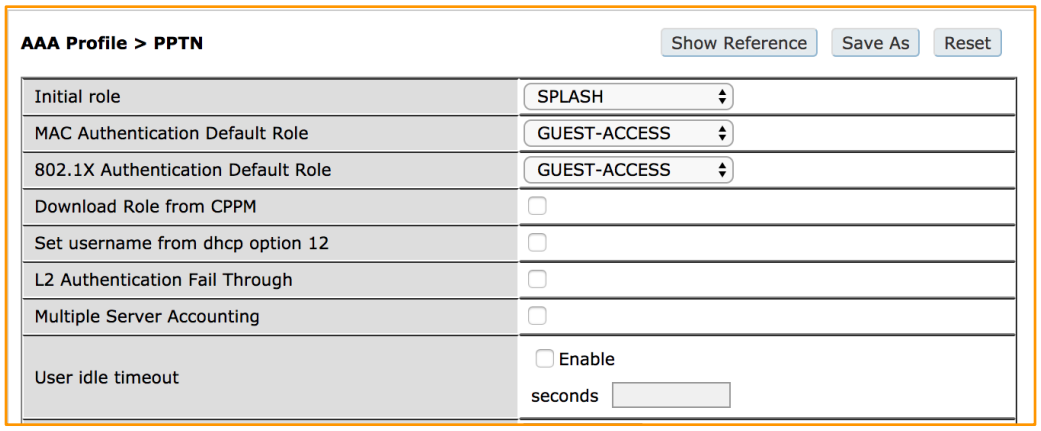
- Firewall Policies: **`allowall`**

```
user-role HEADLESS
access-list session allowall
```

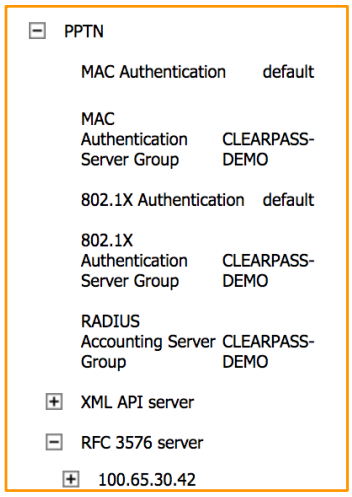
AAA Configuration

Create a new AAA profile under **Configuration > Security > Authentication > AAA Profiles**

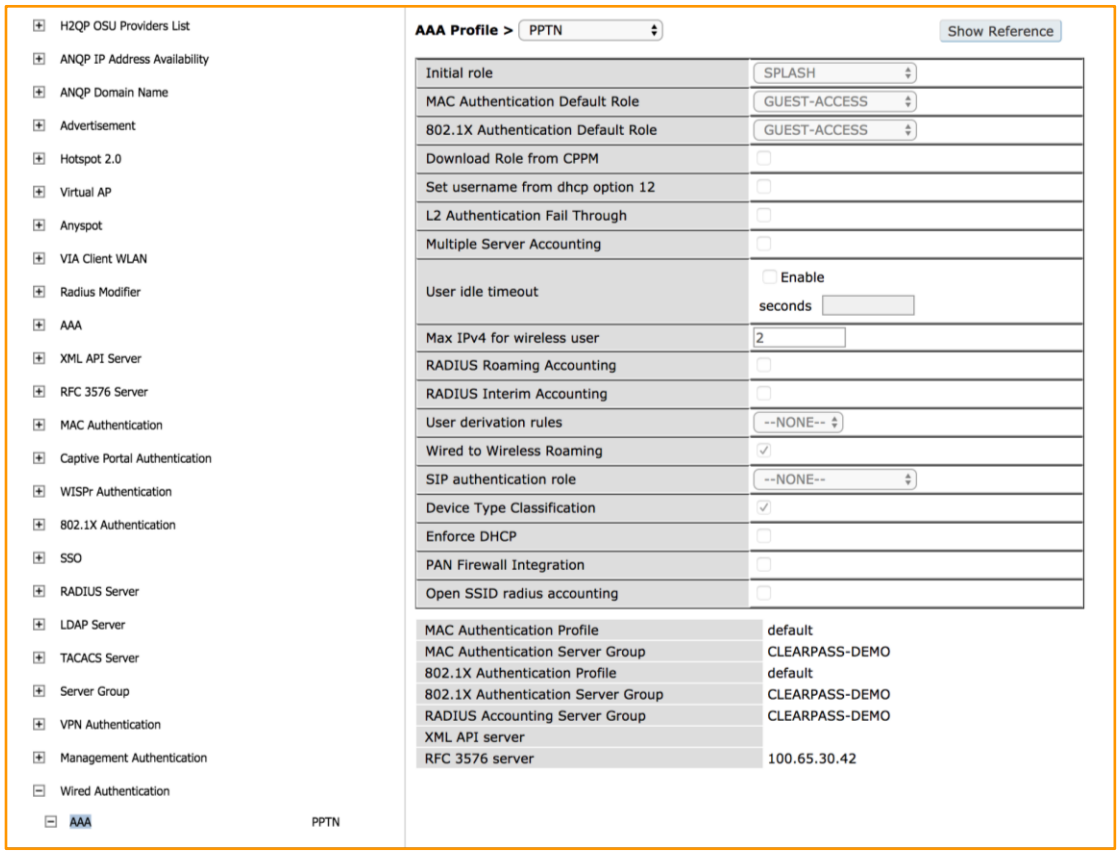
Assign **SPLASH** as the initial role and **GUEST-ACCESS** as the default 802.1X and MAC Authentication roles as ClearPass will be sending back the role name after authentication.



Now assign the various authentication profiles and server groups. Default can be used for both MAC Authentication and 802. 1X Authentication. The server groups should be configured for ClearPass.



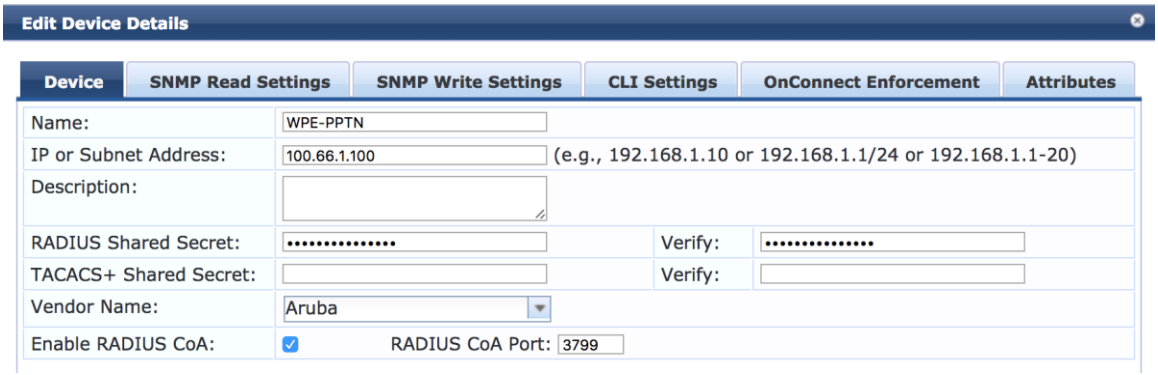
To enable wired authentication, navigate to **`Configuration > Advanced Services > All Profiles > Wireless LAN > Wired Authentication`**, click **AAA** and select the PPTN profile.




```
aaa authentication wired
 profile PPTN
```

ClearPass: Basics

Define your controller(s) as a network device(s) under **`Configuration » Network » Devices`**. At a minimum, configure **`Name`**, **`IP or Subnet Address`**, **`RADIUS Shared Secret`** and **`Vendor Name`**.



ClearPass: MAC Authentication

Overview

The MAC Authentication service will handle headless devices like printers, phones, access points and others as well as provide the redirect URL for unknown devices and users to allow for a captive portal authentication.

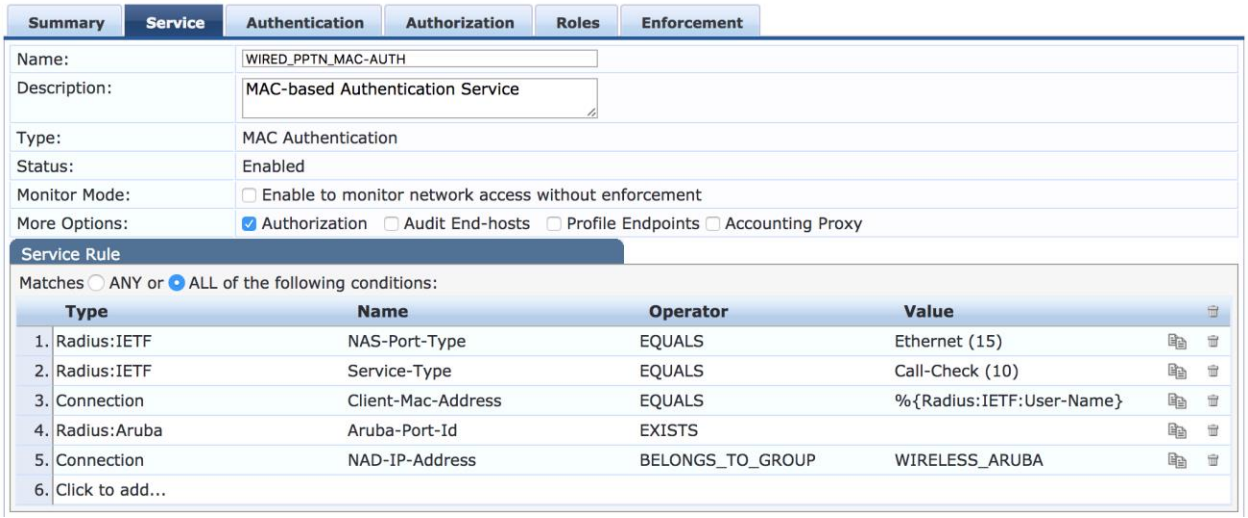
In this scenario, we're leveraging the Guest Device Repository and Device Registration portal to allow end-users and IT staff to register headless and non-802.1X capable devices. These devices can be assigned a role and account lifetime.

Service Configuration

Start with a new service of type **`MAC Authentication`**.

Under More Options, check the **`Authorization`** box. This will enable a new tab. Be sure to follow the screenshot below. Notice that **`NAS-Port-Type`** and **`Service-Type`** are different than a traditional wireless service with an Aruba controller. These values are used to isolate the request as a wired MAC authentication coming from the controller.

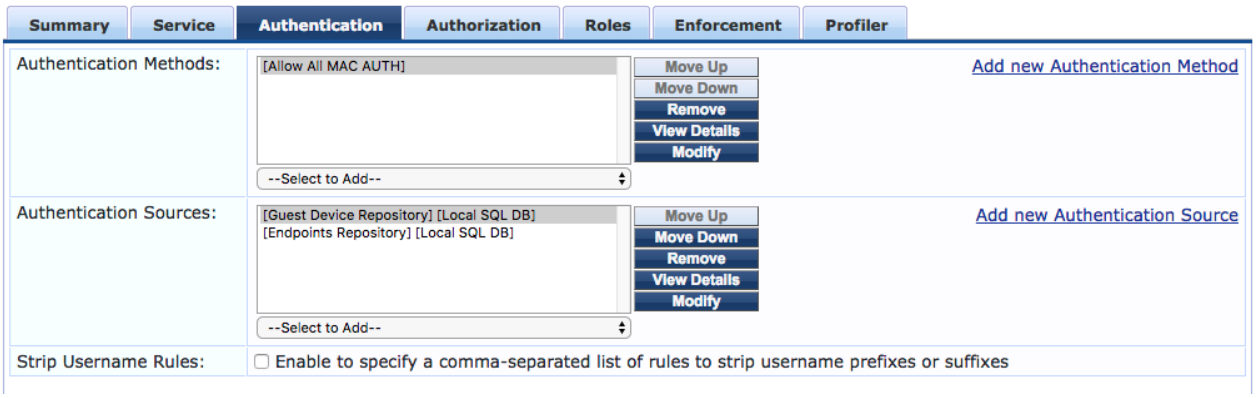
If there is a need to restrict the service to a particular set of switches, you can use a **`Connection`** | **`NAD-IP-Address`** | **`BELONGS_TO_GROUP`** rule to reference a NAD group as seen in rule 5 below.



Authentication

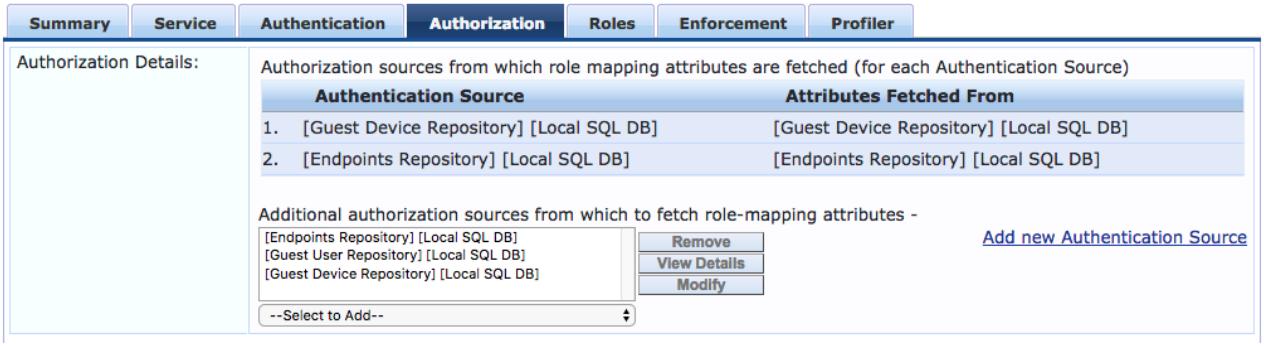
On the authentication tab, remove **[MAC Auth]** under Authentication Methods and add **[Allow All MAC Auth]**.

For Authentication Sources, you'll add **[Guest Device Repository] [Local SQL DB]** and move it above **[Endpoints Repository] [Local SQL DB]**.



Authorization

On the Authorization tab, add the **[Endpoints Repository]**, **[Guest User Repository]** and **[Guest Device Repository]** to the "Additional authorization sources..." list as shown below.

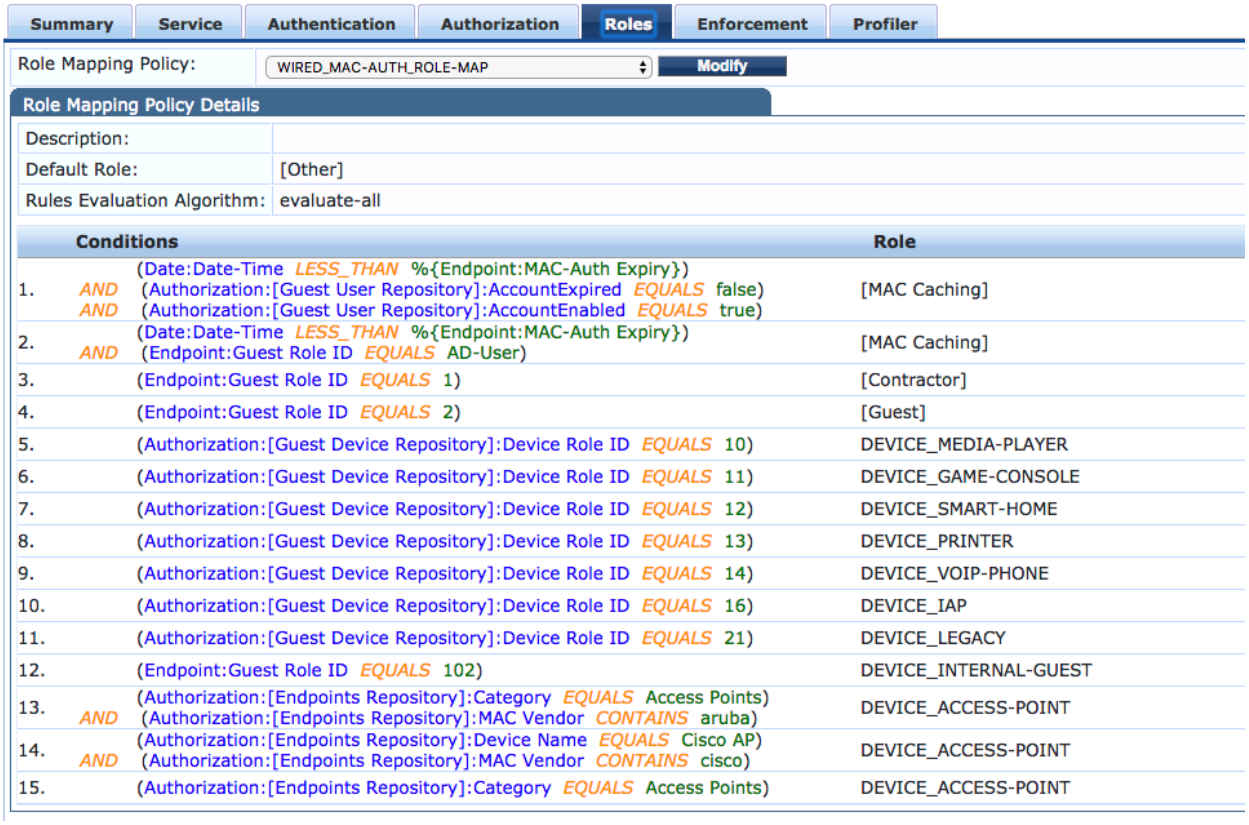


By default, authorization data is only fetched from the authentication source where the user/device was found. So, for example, let's say a guest user's device is re-authenticating to the network within their account expiration window, you'll find the MAC address in the [Endpoints Repository] with some data like guest role and expiration time but we also want to check with ClearPass Guest to make sure an administrator hasn't disabled the account.

Roles

Role mapping is used to tag devices and users with as much information as possible for use in a policy decision.

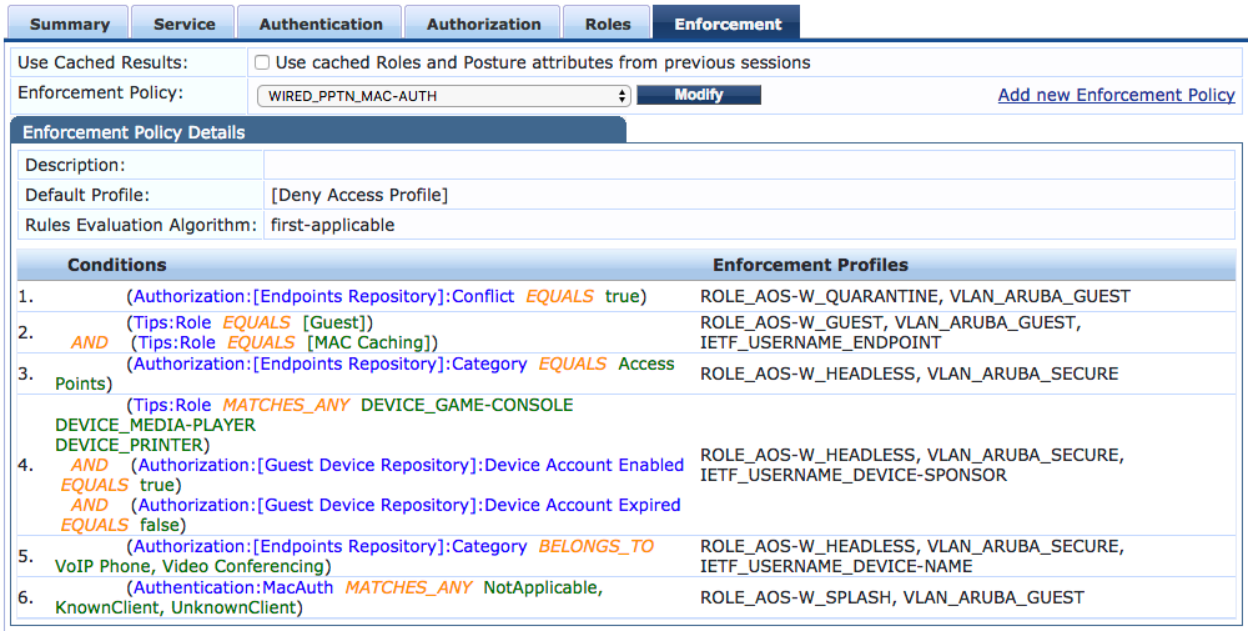
- Rule 1 and 2 are checking to see that a guest user account is still valid and returning the [MAC Caching] tag / TIPS role
- Rules 3-12 map user and device role IDs to tags / TIPS roles for use in policy
- Rules 13-15 map profiling data to a tag / TIPS role for use in policy



Enforcement

For the default policy, the captive portal "splash" role is specified. This is used when a request falls through the policy with no match.

Let's take apart the enforcement rules one by one:



Summary | Service | Authentication | Authorization | Roles | Enforcement

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

Enforcement Policy: WIRED_PPTN_MAC-AUTH [Modify] Add new Enforcement Policy

Enforcement Policy Details

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

	Conditions	Enforcement Profiles
1.	(Authorization:[Endpoints Repository]:Conflict *EQUALS* true)	ROLE_AOS-W_QUARANTINE, VLAN_ARUBA_GUEST
2.	(Tips:Role *EQUALS* [Guest]) *AND* (Tips:Role *EQUALS* [MAC Caching])	ROLE_AOS-W_GUEST, VLAN_ARUBA_GUEST, IETF_USERNAME_ENDPOINT
3.	(Authorization:[Endpoints Repository]:Category *EQUALS* Access Points)	ROLE_AOS-W_HEADLESS, VLAN_ARUBA_SECURE
4.	(Tips:Role *MATCHES_ANY* DEVICE_GAME-CONSOLE DEVICE_MEDIA-PLAYER DEVICE_PRINTER) *AND* (Authorization:[Guest Device Repository]:Device Account Enabled *EQUALS* true) *AND* (Authorization:[Guest Device Repository]:Device Account Expired *EQUALS* false)	ROLE_AOS-W_HEADLESS, VLAN_ARUBA_SECURE, IETF_USERNAME_DEVICE-SPONSOR
5.	(Authorization:[Endpoints Repository]:Category *BELONGS_TO* VoIP Phone, Video Conferencing)	ROLE_AOS-W_HEADLESS, VLAN_ARUBA_SECURE, IETF_USERNAME_DEVICE-NAME
6.	(Authentication:MacAuth *MATCHES_ANY* NotApplicable, KnownClient, UnknownClient)	ROLE_AOS-W_SPLASH, VLAN_ARUBA_GUEST

1

(Authorization:[Endpoints Repository]:Conflict *EQUALS* true)	ROLE_AOS-W_QUARANTINE, VLAN_ARUBA_GUEST

If a device's profiled category changes, ClearPass triggers the `Conflict` attribute.

In this rule, if the Conflict attribute is `true`, the device is being placed into a captive portal redirect to let them know to contact the help desk. Also, the **`GUEST`** named VLAN is being returned using the `Aruba-Name-User-Vlan` VSA.

	Type	Name		Value
1.	Radius:Aruba	Aruba-Named-User-Vlan	=	GUEST

2

(Tips:Role *EQUALS* [Guest]) *AND* (Tips:Role *EQUALS* [MAC Caching])	ROLE_AOS-W_GUEST, VLAN_ARUBA_GUEST, IETF_USERNAME_ENDPOINT

During role mapping, it was determined that the device should still be MAC Cached based on its expiration and the user's account status.

The **`GUEST`** user role and name VLAN as well as the guest's username/email will be returned to the controller.

3

(Authorization:[Endpoints Repository]:Category *EQUALS* Access Points)	ROLE_AOS-W_HEADLESS, VLAN_ARUBA_SECURE

Using profile data, access points will be assigned the **HEADLESS** role in the **SECURE** VLAN.

4

(Tips:Role *MATCHES_ANY* DEVICE_GAME-CONSOLE DEVICE_MEDIA-PLAYER DEVICE_PRINTER) *AND* (Authorization:[Guest Device Repository]:Device Account Enabled *EQUALS* true) *AND* (Authorization:[Guest Device Repository]:Device Account Expired *EQUALS* false)	ROLE_AOS-W_HEADLESS, VLAN_ARUBA_SECURE, IETF_USERNAME_DEVICE-SPONSOR

Many headless devices have been registered via the Device Registration portal. This rule evaluates whether the authenticating device was registered as a game console, media player or printer and that the device account is enabled and hasn't expired.

The **HEADLESS** user role, **SECURE** VLAN name and the sponsor/owner's username are being returned to the controller for these devices.

5

(Authorization:[Endpoints Repository]:Category *BELONGS_TO* VoIP Phone, Video Conferencing)	ROLE_AOS-W_HEADLESS, VLAN_ARUBA_SECURE, IETF_USERNAME_DEVICE-NAME

Based on profiling data, devices categorized as VoIP Phone and Video Conferencing are being authorized by sending back a **VOICE** user role along with the profiled device name as the username (as an example) and the **SECURE** VLAN name.

	Type	Name		Value
1.	Radius:IETF	User-Name	=	%{Authorization:[Endpoints Repository]:Device Name}

6

(Authentication:MacAuth *MATCHES_ANY* NotApplicable, KnownClient, UnknownClient)	ROLE_AOS-W_SPLASH, VLAN_ARUBA_GUEST

The last rule is the catch all rule and drops the device/user into the captive portal splash page for registration and/or authentication before continuing.

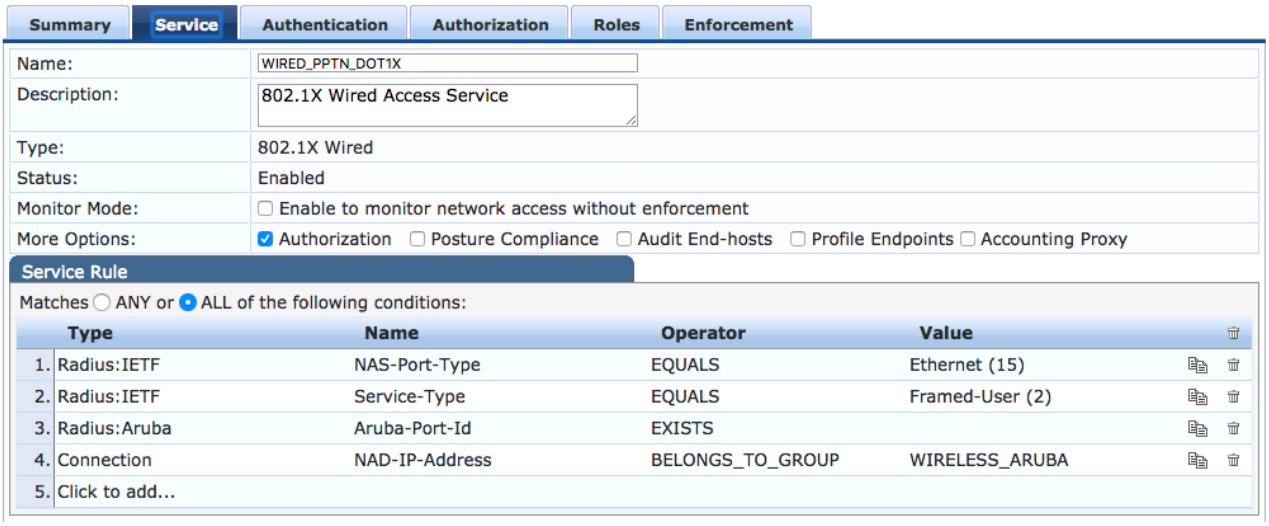
ClearPass: 802.1X

Service Configuration

Create a new service of type **802.1X Wired**.

Under More Options, check the **Authorization** boxes. Be sure to follow the screenshot below. Notice that **Service-Type** is different than a traditional wired service. This value is used to isolate the request as a wired 802.1X request coming from the Aruba controller.

If there is a need to restrict the service to a particular group of switches, you can use a **Connection** | **NAD-IP-Address** | **BELONGS_TO_GROUP** rule to reference a NAD group as seen in rule 4 below.



Authentication

This service will be supporting both secure certificate-based authentication (EAP-TLS) and traditional, legacy username and password authentication (PEAPv0/EAP-MSCHAPv2).

The username and password-based authentication will be used for two purposes:

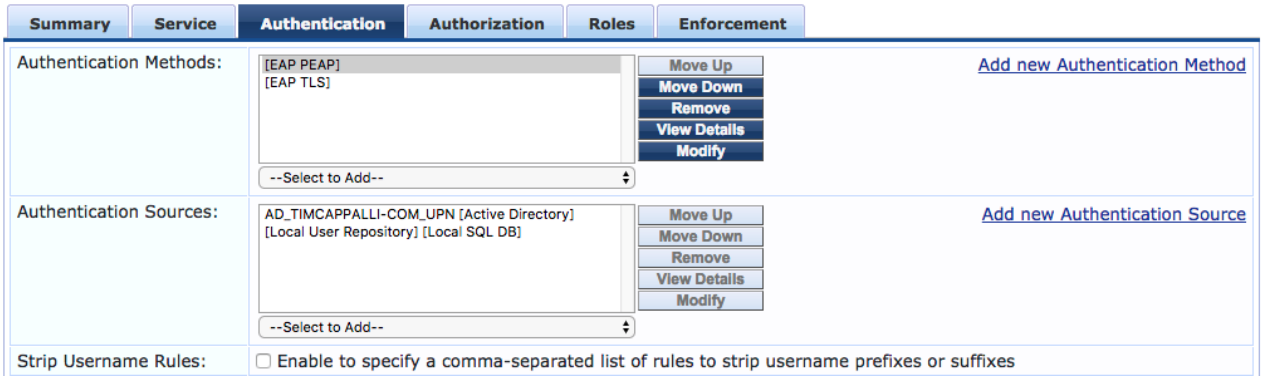
3) Allow a BYOD device to initially connect and kick off the Onboard process to allow a certificate to be issued
4) Allow for domain-joined assets to use their computer/machine account to authenticate to the network as well as support machine + user workflows

Based on the above requirements, remove all the default EAP methods from the Authentication Methods list on the Authentication tab except for **[EAP PEAP]** and **[EAP TLS]**.

NOTE: The default `[EAP TLS]` method does not have OCSP authorization configured and is being used here solely as an example. OCSP is used to check real-time validity of a certificate and enabling it is highly recommended. Special care should be taken when authenticating certificates from different certificate authorities. This is outside the scope of this document.

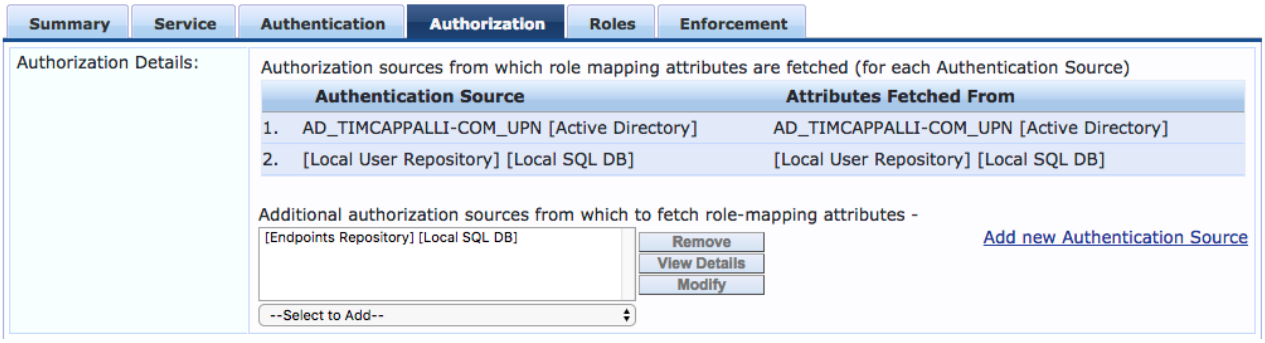
For Authentication Sources, you'll add our Active Directory identity store and also the **`[Local User Repository]`**. Authentication sources will vary in your environment.

The Local User Repository will be used in the example for infrastructure accounts like having an access point or VoIP phone authenticate securely to the network using the 802.1X framework.



Authorization

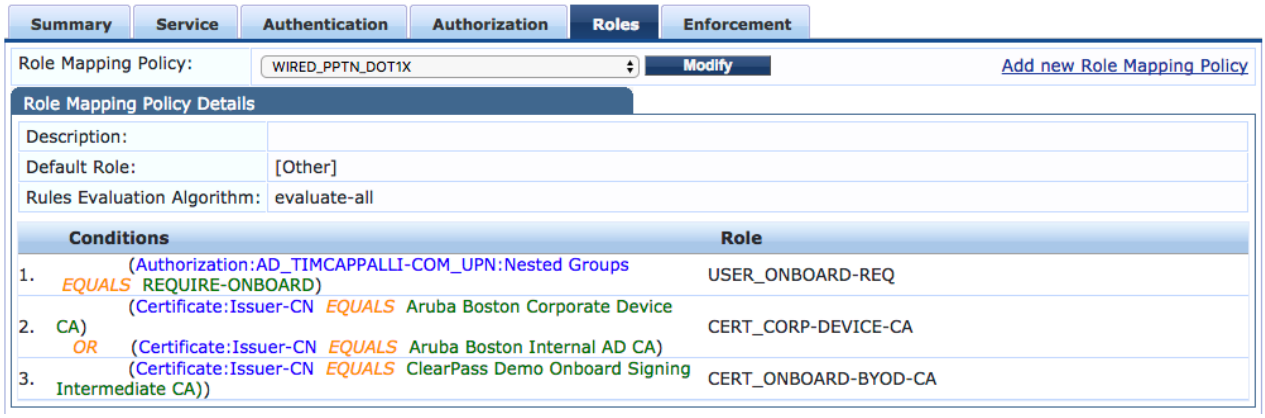
Since device profile information will be leveraged in policy, add the **`[Endpoints Repository]`** to the "Additional authorization sources…" list as shown below.



Roles

Role mapping is used to tag devices and users with as much prevalent information as possible for use in a policy decision.

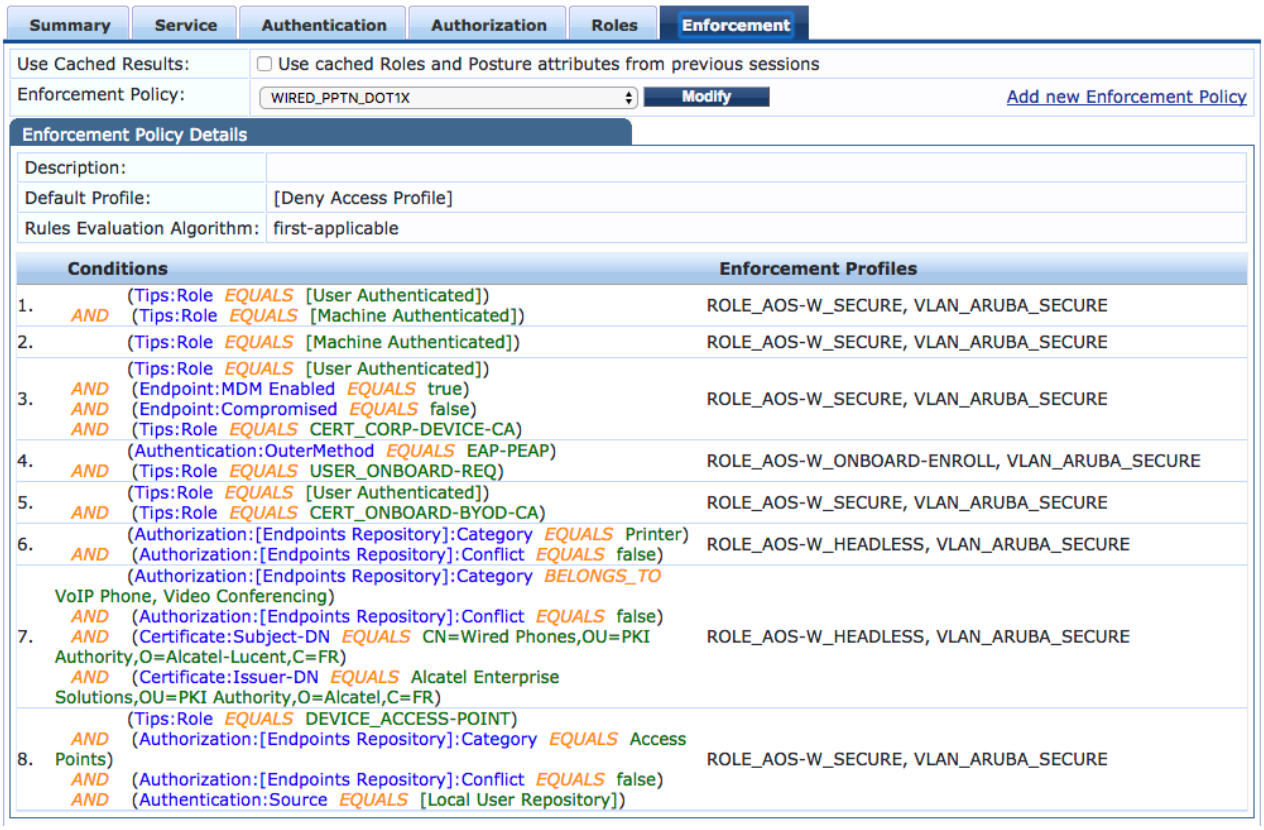
These rules and tags will vary greatly by environment, but below you'll find examples of device and user tagging.



- Rules 1 and 4 are checking group membership from Active Directory
- Rules 2-3 are matching on the common name of the issuing CA for the authenticating certificate

Enforcement

Let's take apart this enforcement policy rule by rule:



Summary | Service | Authentication | Authorization | Roles | Enforcement

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

Enforcement Policy: WIRED_PPTN_DOT1X [Modify] Add new Enforcement Policy

Enforcement Policy Details

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

	Conditions	Enforcement Profiles
1.	(Tips:Role *EQUALS* [User Authenticated]) *AND* (Tips:Role *EQUALS* [Machine Authenticated])	ROLE_AOS-W_SECURE, VLAN_ARUBA_SECURE
2.	(Tips:Role *EQUALS* [Machine Authenticated])	ROLE_AOS-W_SECURE, VLAN_ARUBA_SECURE
3.	(Tips:Role *EQUALS* [User Authenticated]) *AND* (Endpoint:MDM Enabled *EQUALS* true) *AND* (Endpoint:Compromised *EQUALS* false) *AND* (Tips:Role *EQUALS* CERT_CORP-DEVICE-CA)	ROLE_AOS-W_SECURE, VLAN_ARUBA_SECURE
4.	(Authentication:OuterMethod *EQUALS* EAP-PEAP) *AND* (Tips:Role *EQUALS* USER_ONBOARD-REQ)	ROLE_AOS-W_ONBOARD-ENROLL, VLAN_ARUBA_SECURE
5.	(Tips:Role *EQUALS* [User Authenticated]) *AND* (Tips:Role *EQUALS* CERT_ONBOARD-BYOD-CA)	ROLE_AOS-W_SECURE, VLAN_ARUBA_SECURE
6.	(Authorization:[Endpoints Repository]:Category *EQUALS* Printer) *AND* (Authorization:[Endpoints Repository]:Conflict *EQUALS* false)	ROLE_AOS-W_HEADLESS, VLAN_ARUBA_SECURE
7.	(Authorization:[Endpoints Repository]:Category *BELONGS_TO* VoIP Phone, Video Conferencing) *AND* (Authorization:[Endpoints Repository]:Conflict *EQUALS* false) *AND* (Certificate:Subject-DN *EQUALS* CN=Wired Phones,OU=PKI Authority,O=Alcatel-Lucent,C=FR) *AND* (Certificate:Issuer-DN *EQUALS* Alcatel Enterprise Solutions,OU=PKI Authority,O=Alcatel,C=FR)	ROLE_AOS-W_HEADLESS, VLAN_ARUBA_SECURE
8.	(Tips:Role *EQUALS* DEVICE_ACCESS-POINT) *AND* (Authorization:[Endpoints Repository]:Category *EQUALS* Access Points) *AND* (Authorization:[Endpoints Repository]:Conflict *EQUALS* false) *AND* (Authentication:Source *EQUALS* [Local User Repository])	ROLE_AOS-W_SECURE, VLAN_ARUBA_SECURE

1

	(Tips:Role *EQUALS* [User Authenticated])	ROLE_AOS-W_SECURE, VLAN_ARUBA_SECURE
AND	(Tips:Role *EQUALS* [Machine Authenticated])	

When a Windows device authenticates to the network using its Active Directory computer account, the `[Machine Authenticated]` tag/TIPS role is added to the session automatically.

If both a machine and user authentication have occurred, then return the `SECURE` user role and VLAN name.

This is commonly used to validate that the user is using a corporate asset.

2

	(Tips:Role *EQUALS* [Machine Authenticated])	ROLE_AOS-W_SECURE, VLAN_ARUBA_SECURE

Rule 2 is for a machine-only authentication. These typically occur when the device is sitting at the Windows logon screen and connectivity is required for updates, remote access or for new users to login.

3

```
      (Tips:Role  EQUALS  [User Authenticated])
AND   (Endpoint:MDM Enabled  EQUALS  true)
AND   (Endpoint:Compromised  EQUALS  false)
AND   (Tips:Role  EQUALS  CERT_CORP-DEVICE-CA)
```

ROLE_AOS-W_SECURE, VLAN_ARUBA_SECURE

This is a typical rule to deal with a non-Windows corporate-managed asset that is managed by an EMM solution.

The two endpoint attributes have been synced down from the EMM solution via ClearPass Exchange. In this case, the rule is evaluating whether the device has its device management enabled and that no compromise has occurred.

The last condition checks for the tag/TIPS role from our role mapping to verify the certificate used to authenticate was issued from the Corporate Device CA.

4

```
      (Authentication:OuterMethod  EQUALS  EAP-PEAP)
AND   (Tips:Role  EQUALS  USER_ONBOARD-REQ)
```

ROLE_AOS-W_ONBOARD-ENROLL, VLAN_ARUBA_SECURE

Most personal devices will perform Onboarding through the captive portal workflow after 802.1X fails, but some users may authenticate via PEAPv0/EAP-MSCHAPv2 when prompted by their device. This rule will catch those users who need to be using certificate-based authentication (EAP-TLS) via ClearPass Onboard.

The user role **ONBOARD-ENROLL** and **SECURE** VLAN name are returned to the controller.

5

```
      (Tips:Role  EQUALS  [User Authenticated])
AND   (Tips:Role  EQUALS  CERT_ONBOARD-BYOD-CA)
```

ROLE_AOS-W_SECURE, VLAN_ARUBA_SECURE

After a device has been onboarded, subsequent authentications will occur via EAP-TLS. Rule 6 uses the tag from the role mapping to check the common name of the issuing CA. These devices will be dropped into a **SECURE** role and VLAN.

6

```
      (Authorization:[Endpoints Repository]:Category  EQUALS  Printer)
AND   (Authorization:[Endpoints Repository]:Conflict  EQUALS  false)
```

ROLE_AOS-W_HEADLESS, VLAN_ARUBA_SECURE

This rule uses the device category of Printer combined with a check of the **Conflict** flag. The authentication method (username/password vs certificate) does not really matter in this case, however, an additional condition could easily be added similar to rules 7 and 8 below.

7

```
      (Authorization:[Endpoints Repository]:Category  BELONGS_TO
VoIP Phone, Video Conferencing)
  AND   (Authorization:[Endpoints Repository]:Conflict  EQUALS  false)
  AND   (Certificate:Subject-DN  EQUALS  CN=Wired Phones,OU=PKI
Authority,O=Alcatel-Lucent,C=FR)
  AND   (Certificate:Issuer-DN  EQUALS  Alcatel Enterprise
Solutions,OU=PKI Authority,O=Alcatel,C=FR)
```

ROLE_AOS-W_HEADLESS, VLAN_ARUBA_SECURE

Many voice devices come from the factory with an embedded certificate that can be used for network authentication. The factory cert is being leveraged for EAP-TLS combined with profiling data. The **HEADLESS** user role and **SECURE** VLAN name are being passed back for these devices.

8

```
        (Tips:Role  EQUALS  DEVICE_ACCESS-POINT)
  AND   (Authorization:[Endpoints Repository]:Category  EQUALS  Access
Points)                                                  ROLE_AOS-W_SECURE, VLAN_ARUBA_SECURE
  AND   (Authorization:[Endpoints Repository]:Conflict  EQUALS  false)
  AND   (Authentication:Source  EQUALS  [Local User Repository])
```

As discussed during the authentication section, a local user account was created in ClearPass for use by access points to authenticate. Rule 8 is comparing the tag/TIPS role, category, conflict status and verifying the authentication source was the **`[Local User Repository]`**

ClearPass: Web Authentication

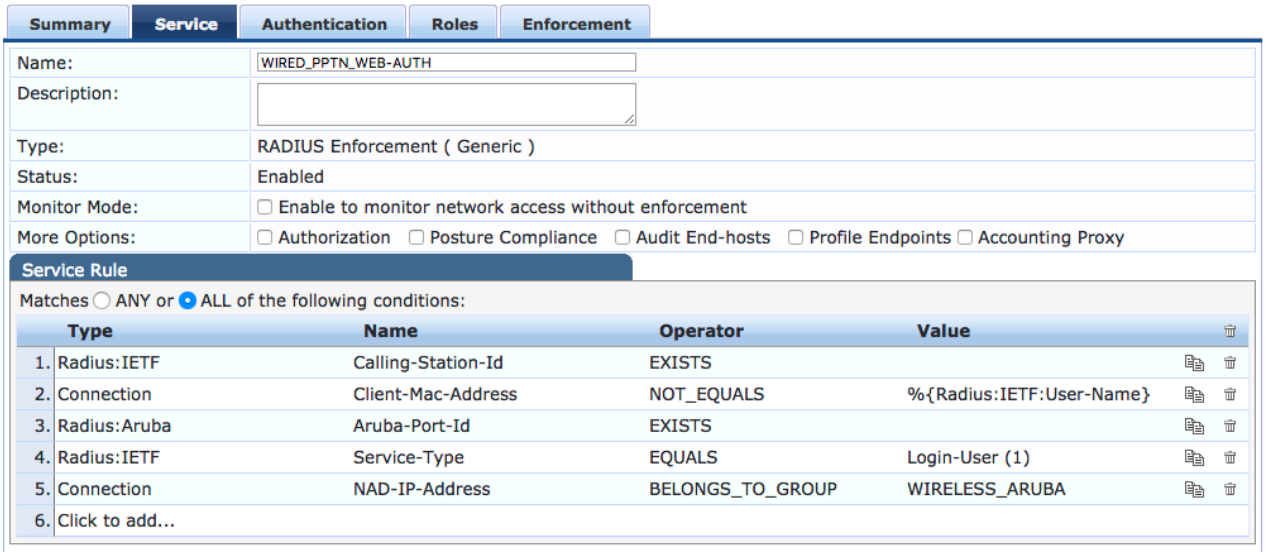
The Web Authentication service handles captive portal-based authentications with server-initiated workflows.

Service Configuration

Create a new service of type **`RADIUS Based Enforcement (Generic)`**.

Be sure to follow the screenshot below. Notice that **`Service-Type`** is set to **`Login-User (1)`** and **`Aruba-Port-Id`** just needs to be present in the request, regardless of value. These values are used isolate the request as a wired, RADIUS-based web authentication request coming from the Aruba controller.

If there is a need to restrict the service to a particular group of switches, you can use a **`Connection`** | **`NAD-IP-Address`** | **`BELONGS_TO_GROUP`** rule to reference a NAD group as seen in rule 5 below.



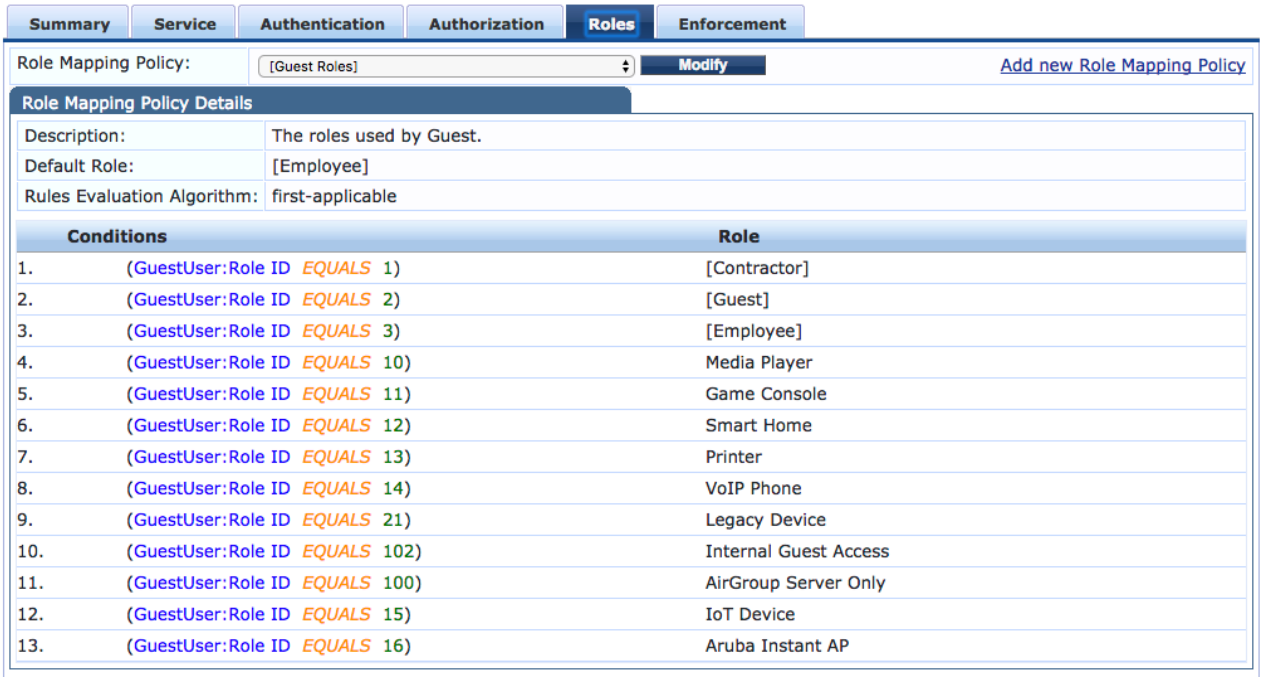
Authentication

This service will be supporting both guest and Active Directory users for captive portal login.

For Authentication Sources, you'll add the **`[Guest User Repository]`** and also our Active Directory identity store. Authentication sources will vary in your environment.

Roles

In this scenario, guests will go through a standard self-registration process. Since no custom role mapping is being used, you'll select the generic **`[Guest Roles]`** role map.



Summary | Service | Authentication | Authorization | Roles | Enforcement

Role Mapping Policy: [Guest Roles] Modify — Add new Role Mapping Policy

Role Mapping Policy Details

Description:	The roles used by Guest.
Default Role:	[Employee]
Rules Evaluation Algorithm:	first-applicable

	Conditions	Role
1.	(GuestUser:Role ID *EQUALS* 1)	[Contractor]
2.	(GuestUser:Role ID *EQUALS* 2)	[Guest]
3.	(GuestUser:Role ID *EQUALS* 3)	[Employee]
4.	(GuestUser:Role ID *EQUALS* 10)	Media Player
5.	(GuestUser:Role ID *EQUALS* 11)	Game Console
6.	(GuestUser:Role ID *EQUALS* 12)	Smart Home
7.	(GuestUser:Role ID *EQUALS* 13)	Printer
8.	(GuestUser:Role ID *EQUALS* 14)	VoIP Phone
9.	(GuestUser:Role ID *EQUALS* 21)	Legacy Device
10.	(GuestUser:Role ID *EQUALS* 102)	Internal Guest Access
11.	(GuestUser:Role ID *EQUALS* 100)	AirGroup Server Only
12.	(GuestUser:Role ID *EQUALS* 15)	IoT Device
13.	(GuestUser:Role ID *EQUALS* 16)	Aruba Instant AP

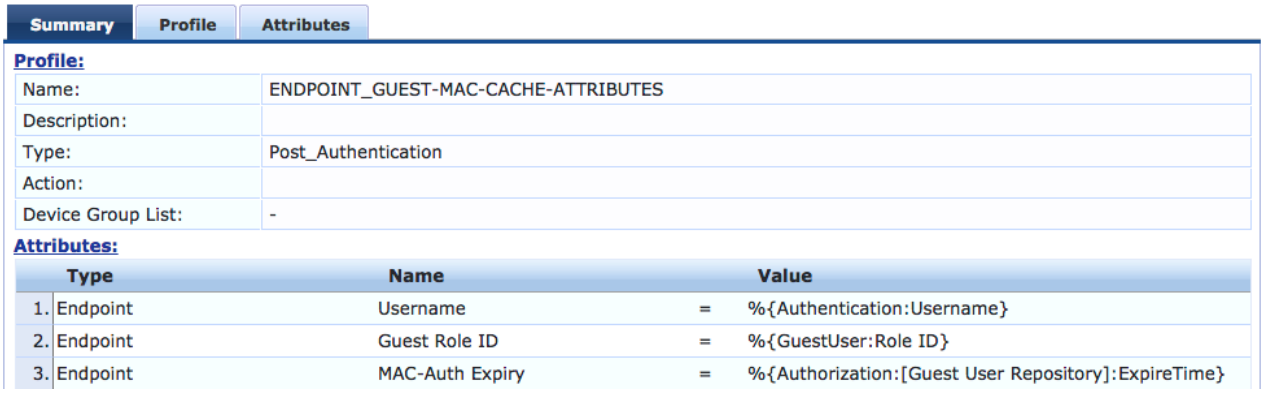
Enforcement

Although the client device is wired, the web authentication will be processed just like a wireless client using a **`controller-initiated`** login, meaning that the client browser submits the credentials to the controller's web server and the controller in turn makes a RADIUS request to ClearPass.

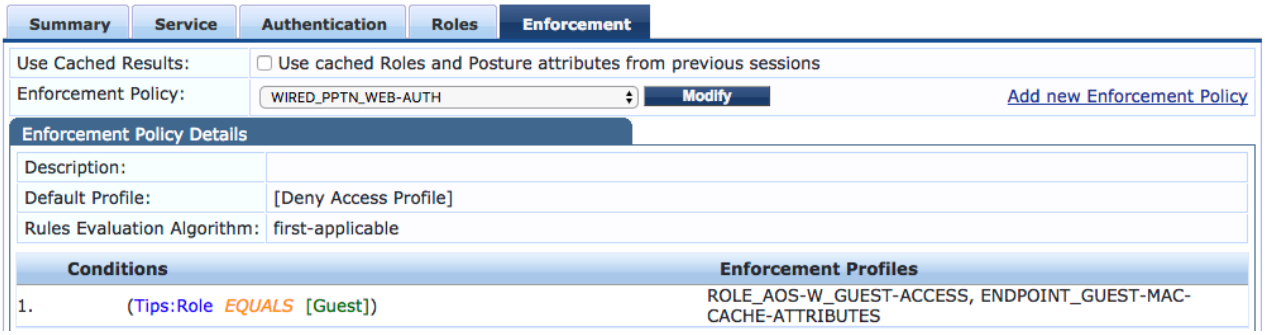
Before creating the enforcement policy, create a new enforcement profile for the guest users (**`Configuration » Enforcement » Profiles » Add Enforcement Profile`**).

1. Select `ClearPass Entity Update Enforcement` from the Template dropdown
2. Give the profile a name
3. On the attributes tab, add the 3 entries below and then save. Note that the value field will require manual entry (copy and paste the values below).

TYPE	NAME	VALUE
Endpoint	`Username`	`%{Authentication:Username}`
Endpoint	`Guest Role ID`	`%{GuestUser:Role ID}`
Endpoint	`MAC-Auth Expiry`	`%{Authorization:[Guest User Repository]:ExpireTime}`



Now, create a very basic enforcement policy. The rule checks for a TIPS role / tag of **`[Guest]`** and returns the **`GUEST-ACCESS`** role in the RADIUS response and writes the username, role ID and expiration time to the end-point database for use with MAC caching on subsequent authentications.



Useful Troubleshooting Commands and Tips

Controller

show tunneled-node config

```
Tunneled node Server:Enabled
Tunnel Loop Prevention:Disabled
```

show tunneled-node state

```
Tunneled Node State
-------------------
IP           MAC                port  state     vlan  tunnel  inactive-time
--           ---                ----  -----     ----  ------  -------------
100.81.0.12  5c:b9:01:14:0a:00  13    complete  4013  9       0
100.81.0.12  5c:b9:01:14:0a:00  16    complete  4013  10      0
100.81.0.12  5c:b9:01:14:0a:00  15    complete  4013  11      0
```

show tunneled-node database

```
Tunneled node database
----------------------
IP           #Tunnels
--           --------
100.81.0.12  3
```

Switch

show tunneled-node-server state

```
Tunneled Node Port State

 Active Controller IP Address  : 100.66.1.100

 Port   State
 ------ ------------------------
 13     Complete
 14     Port down
 15     Port down
 16     Port down
```

Per-User Tunneled-Node (PUTN)

Policy Enforcement

Per-User Tunneled-Node (PUTN) allows for dynamic tunneling of user traffic to a mobility controller based on a policy decision. For example, devices like access points, printers and voice devices can stay locally switched, while a new unknown device, guest user or device with questionable posture can be tunneled to an Aruba mobility controller. Each device connected to a switch port is assigned a user role and in turn can stay local or be tunneled.

A new user role configuration element was added in ArubaOS-Switch 16.04 named **`tunneled-node-server-redirect secondary-role`**. The existing controller role that will be enforced for the tunneled client is defined as this secondary role. The switch will pass this secondary role name up to the controller where it will be enforced.

```
aaa authorization user-role name "T--QUARANTINE"
   vlan-id 603      <<< controller VLAN ID (must also be defined on the switch)
   tunneled-node-server-redirect secondary-role quarantine    <<< controller user role
   exit
```

In this example, **`T--QUARANTINE`** is returned as the `HPE-User-Role` from ClearPass. This local user role has a secondary role defined which instructs the switch to tunnel this user to the active switch anchor controller in the defined VLAN. All of the client's traffic is then processed by the mobility controller.

The switch is in full control of authentication, authorization and accounting. ClearPass disconnect messages and change of authorization (CoA) requests are sent from ClearPass to the switch for enforcement.

With PUTN, the controller is a stateful, deep packet inspection and processing engine with enhanced visibility and control. All tunneled users appear in both the switch and controller user tables.

SWITCH

```
EDGE-2930# show port-access clients
Downloaded user roles are preceded by *

 Port Access Client Status

  Port  Client Name   MAC Address       IP Address      User Role         Type  VLAN
  ----- ------------- ----------------- --------------- ----------------- ----- ----
  5     darth.vade... 90e2ba-692d5a     100.66.3.16     T--QUARANTINE     8021X 603
```

MOBILITY CONTROLLER

(some columns removed for readability)

```
(BOS-7010-1) *#show user-table role QUARANTINE

Users
-----
    IP            MAC            Name     Role        Age(d:h:m)  AP name    Roaming  User Type
----------   ------------       ------    ----        ----------  -------    -------  ---------
100.66.3.16  90:e2:ba:69:2d:5a            quarantine  00:00:01    tunnel 26  Wired    TUNNELED USER
```

Configuration Overview

The hardware and software requirements for Per-User Tunneled-Node are:

- Compatible Aruba switch running ArubaOS-Switch 16.04 or greater:
  - 5400R
  - 3810M / 3800
  - 2930F / 2930M

  * Please refer to switch documentation for latest feature support and scalability numbers

- Aruba hardware mobility controller for tunnel termination running ArubaOS 8.1+
- ClearPass Policy Manager (no version dependency unless downloadable user roles are in use which requires 6.6.7+)

Here are the hardware and software combinations used for this example configuration:

- Aruba 2930F switch running ArubaOS-Switch 16.04.0008
- Aruba Virtual Mobility Master (VMM) running ArubaOS 8.1.0.1
- Aruba 7010 mobility controller running ArubaOS 8.1.0.1
- ClearPass Policy Manager 6.6.7

Quirks and Limitations

- Switch tunneled-node mode is global: per-user OR per-port
- PUTN has a limit of 32 MAC addresses per port
- Client VLANs defined on the controller must also be defined on the switch, but they should not be tagged through the network

Switch Configuration

This section will only cover configuration elements unique to Per-User Tunneled-Node (PUTN). The previous sections cover the full AAA configuration for 802.1X, MAC authentication, web authentication and user roles.

Define the controller VLANs where tunneled users will be assigned. These VLAN IDs must match the controller but the VLAN name can be different.

NOTE: These VLANs should only be created/defined. No IP address should be added and the VLAN should not be tied to any port.

`vlan 602 name TN-SECURE`	controller VLAN for trusted users
`vlan 603 name TN-GUEST`	controller VLAN for guest users
`vlan 604 name TN-UNTRUST`	controller VLAN for untrusted users

Define the switch anchor controller and globally enable role-based tunneled node (per-user).

`tunneled-node-server`	enter into TN global config
`  controller-ip 100.66.1.11`	TN controller
`  mode role-based`	globally enable role-based TN

Create local user roles with the secondary-role attribute.

NOTE: The secondary-role name is case-sensitive and ArubaOS 8.x stores everything as lowercase. The secondary-role definition on the switch must be lowercase.

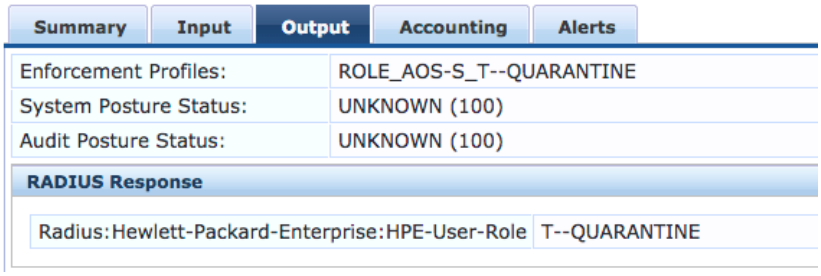
`aaa authorization user-role name T--QUARANTINE`	define the LUR
`  vlan-id 604`	assign controller's client access VLAN
`  tunneled-node-server-redirect secondary-role quarantine`	assign controller user role

ClearPass Configuration

Local User Roles (LURs)

When using a local user role (LUR) with PUTN, the ClearPass configuration remains the same as any other user role enforcement.

A user role name is simply returned to the switch using the `HPE-User-Role` VSA.



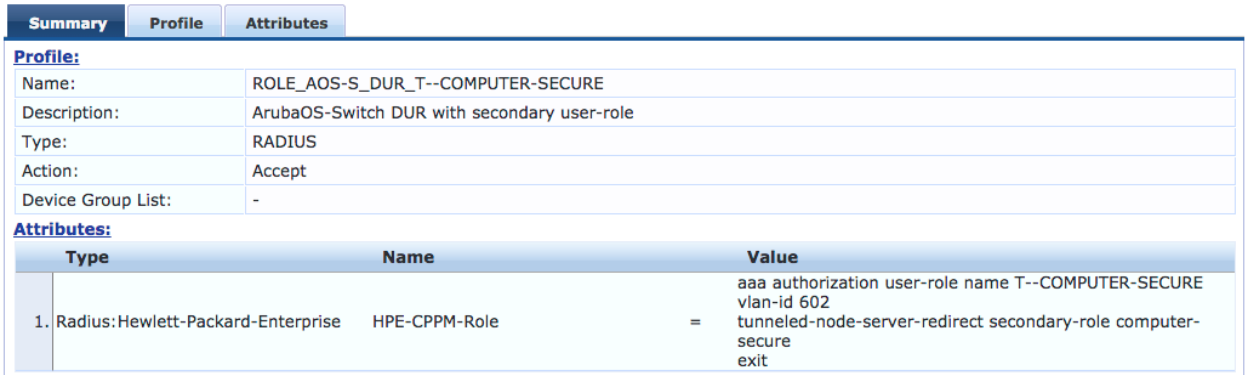
Downloadable User Roles (DURs)

From the role definition standpoint, downloadable user roles with PUTN use the same `Aruba Downloadable Role Enforcement` template and configuration with the addition of the `tunneled-node-server-redirect secondary-role` statement. See the Downloadable User Roles (DURs) section earlier in this document for more details and configuration requirements for DURs.

Below are two examples of DURs with PUTN.

NOTE: VLAN name can be used with PUTN for flexibility as long as the VLAN ID with this name on the switch is the same VLAN ID that will be used for client access on the controller.

For example, if VLAN 603 is the client access VLAN on the controller, the VLAN name defined on the switch must be for VLAN 603.



Summary | Profile | Attributes

Profile:

Name:	ROLE_AOS-S_DUR_T--PROFILE
Description:	ArubaOS-Switch DUR with secondary user-role for centralized device profiling
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Radius:Hewlett-Packard-Enterprise	HPE-CPPM-Role	=	aaa authorization user-role name T--PROFILE vlan-name TN-UNTRUST tunneled-node-server-redirect secondary-role profile exit

Role and Enforcement Profile Naming

Role and profile naming conventions can greatly assist with policy creation as well as reporting. The ability to quickly determine that a downloadable tunneled role was used instead of a local user role just from the name is invaluable.

For the PUTN examples used in this guide, all switch user roles with a secondary-role definition use the naming convention **T--{CONTROLLER-ROLE-NAME}**.

```
EDGE-2930# show user-role
Downloaded user roles are preceded by *

 User Roles

  Enabled       : Yes
  Initial Role  : denyall

  Type       Name
  ---------- ----------------------------------------------------
  local      VOICE             <<< user/traffic stays local
  local      SECURE            <<< user/traffic stays local
  predefined denyall
  local      T--SECURE         <<< user/traffic tunneled, controller role = SECURE
  local      T--PROFILE        <<< user/traffic tunneled, controller role = PROFILE
  local      T--HEADLESS       <<< user/traffic tunneled, controller role = HEADLESS
  local      T--QUARANTINE     <<< user/traffic tunneled, controller role = QUARANTINE
  local      COMPUTER-SECURE   <<< user/traffic stays local
```

Along the same lines for downloadable user roles, DUR enforcement profile examples in this guide use the naming convention **ROLE_AOS-S_DUR_{ROLE-NAME}.**

#	Name ▲	Type	Description
1.	ROLE_AOS-S_DUR_HEADLESS	RADIUS	ArubaOS-Switch DUR
2.	ROLE_AOS-S_DUR_PROFILE	RADIUS	ArubaOS-Switch DUR
3.	ROLE_AOS-S_DUR_SPLASH	RADIUS	ArubaOS-Switch DUR
4.	ROLE_AOS-S_DUR_T--COMPUTER-SECURE	RADIUS	ArubaOS-Switch DUR with secondary user-role
5.	ROLE_AOS-S_DUR_T--PROFILE	RADIUS	ArubaOS-Switch DUR with secondary user-role for centralized device profiling
6.	ROLE_AOS-S_GAME-CONSOLE	RADIUS	ArubaOS-Switch Local User Role
7.	ROLE_AOS-S_GUEST	RADIUS	ArubaOS-Switch Local User Role

Useful Troubleshooting Commands and Tips

show tunneled-node-server state

```
EDGE-2930# show tunneled-node-server state

 Local Master Server (LMS) State

 LMS Type     IP Address       State        Capability Role
 Primary   :  100.66.1.11      Complete     Per User   Operational Primary

 Switch Anchor Controller (SAC) State

               IP Address       Mac Address             State
 SAC         : 100.66.1.11      000b86-dd4a40           Registered

 User Anchor Controller (UAC) : 100.66.1.11
 User              Port       VLAN       State       Bucket ID
 90e2ba-692d5a     5          603        Registered  30
```

show tunneled-node-user all

```
EDGE-2930# show tunneled-node-user all

PORT    MAC-ADDRESS     TUNNEL-STATUS   SECONDARY-USERROLE     FAILURE-REASON
5       90e2ba-692d5a   UP              quarantine
```

HPE FlexNetwork (Comware v7) Enforcement

RADIUS-based Enforcement

Policy Enforcement

Access Control Lists (ACLs)

HPE Comware 7-based switches use locally defined ACLs that can be referenced via RADIUS.

ACLs are defined locally on the switch and can be returned as part of a RADIUS response or added directly to a switch port or VLAN interface.

VLAN Enforcement

VLANs in CW7 can be referenced by VLAN-ID or VLAN name. Although it is an optional configuration, VLAN name is highly recommended in a colorless port deployment as it removes the need for ClearPass to maintain a VLAN to function mapping for each switch. This simplifies policy creation, management and troubleshooting.

For example, each switch might use a different VLAN-ID for “secure access”. Instead of having to write complex policy in ClearPass to return the correct VLAN-ID for each switch, we just give the appropriate VLAN-ID a name on each switch; “SECURE” for example. Now in your ClearPass policy, you simply return a VLAN enforcement with “SECURE” as the VLAN-ID and each switch will use the appropriate VLAN-ID mapped locally on the switch.

Dynamic Authorization

CW7 switches support the following dynamic authorization commands:

- **Terminate Session**: traditional disconnect message; reinitializes authenticator state
- **Bounce Host Port**: bounces the port by disabling and re-enabling the port
- **Disable Host Port:** administratively disables the port

NOTE: In ClearPass 6.6.X and earlier, the pre-defined Cisco dynamic authorization enforcement profiles need to be used with CW7 switches. In ClearPass 6.7.X+, use the pre-built H3C dynamic authorization enforcement profiles.

Configuration Overview

Here are the hardware and software combinations used for this configuration:

- HPE 5130 EI switch running Comware 7.10.R3115P07
- ClearPass Policy Manager 6.6.4 (there are no ClearPass version dependencies for this configuration)

This configuration has been tested on the HPE 5130EI, 5130HI and 5510HI. The minimum versions of Comware 7 required for this configuration are:

- 5130_EI_7.10.R3113P02
- 5130_HI_7.10.R1308
- 5510_HI_7.10.R1308

Quirks and Limitations

- Comware 7 will not accept an ACL name via the RADIUS **`filter-id`** or **`url-redirect`** attributes. The ACL number must be sent. If you do not send an ACL in the RADIUS response and there is no ACL statically configured on the port, all traffic is permitted for that session.

Switch Configuration

The configuration snippets below assume that components like VLANs, uplinks, NTP and other basics have already been configured. Note that NTP is required as accurate time plays a critical role in network authentication.

CW7 uses the concept of authentication domains and schemes. You first create a scheme for the protocol (RADIUS in this case) and then map the authentication scheme to the domain. Then enable the newly created authentication domain as the global default.

```
radius scheme clearpass
 primary authentication 100.65.30.42 key simple L0ng&Compl5x$ecret!
 primary accounting 100.65.30.42 key simple L0ng&Compl5x$ecret!
 accounting-on enable
 user-name-format keep-original
#

domain clearpass
 authentication lan-access radius-scheme clearpass
 authorization lan-access radius-scheme clearpass
 accounting lan-access radius-scheme clearpass
#

domain default enable clearpass
#
```

Set the NAS-IP to the RADIUS source address (usually the switch's management IP) and configure your ClearPass server(s) as a RADIUS dynamic authorization client(s) to support Change of Authorization.

```
radius nas-ip 100.81.0.11
#

radius dynamic-author server
 client ip 100.65.30.42 key simple L0ng&Compl5x$ecret!
#
```

Enable global functions and configurations:

`port-security enable` `port-security mac-move permit`	enable port authentication
`dhcp snooping enable`	provides IP visibility
`dot1x authentication-method eap`	enable EAP-based 802.1X
`dot1x timer supp-timeout 10` `dot1x timer tx-period 10`	set 802.1X timers

Define access control entries:

`acl number 3900 name ALLOWALL`
` rule permit ip`
`#`
	allow all

`acl number 3902 name PROFILE`
` rule permit udp destination-port eq bootps`
` rule permit udp destination-port eq dns`
`#`
	unknown endpoint profiling

`acl number 3910 name CLEARPASS-REDIRECT`
` description CLEARPASS-REDIRECT`
` rule permit tcp destination 100.65.30.42 0 destination-port eq 443`
` rule permit tcp destination 100.65.30.42 0 destination-port eq www`
` rule permit tcp destination 100.65.30.42 0 destination-port eq 6658`
` rule permit udp destination-port eq dns`
` rule permit udp destination-port eq bootps`
`#`
	captive portal redirect + OnGuard Agent communication

`acl number 3911 name INTERNET-ONLY`
` rule permit udp destination-port eq bootps`
` rule permit udp destination-port eq dns`
` rule deny ip destination 100.64.0.0 0.31.255.255`
` rule permit ip`
`#`
	deny internal access

`acl number 3912 name BYOD`
` rule permit udp destination-port eq bootps`
` rule permit udp destination-port eq dns`
` rule deny ip destination 100.65.0.0 0.0.255.255`
` rule permit ip`
`#`
	deny restricted networks for personal devices

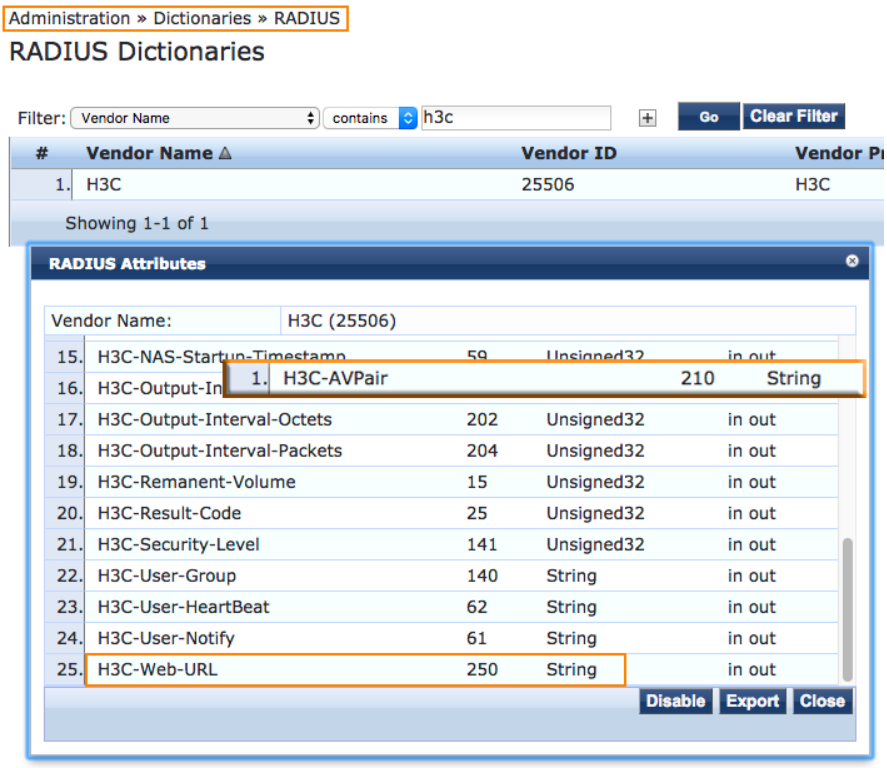
Configure end-user ports:

`interface GigabitEthernet1/0/1`	
`port link-type hybrid`	supports VoIP devices with clients behind them
`port hybrid vlan 813 tagged` `port hybrid vlan 1 untagged`	set voice VLAN as tagged set dead-end VLAN as untagged
`undo voice-vlan mode auto`	disable OUI based voice VLAN
`voice-vlan 813 enable`	voice VLAN
`mac-vlan enable`	MAC to VLAN mapping
`undo dot1x handshake`	not needed, see CW7 docs

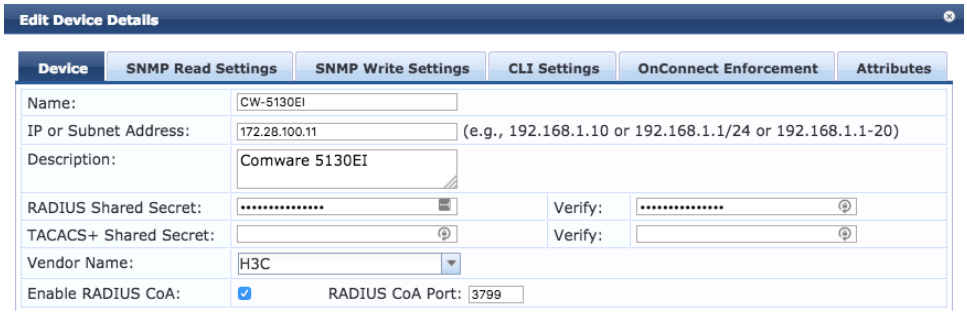
`dot1x mandatory-domain clearpass`	use 'clearpass' domain for 1X
`undo dot1x multicast-trigger`	disable, can cause issues with VoIP phones
`dot1x unicast-trigger`	^ unicast EAP Request to unknown MAC
`dot1x re-authenticate`	allow periodic reauthentication
`dot1x re-authenticate server-unreachable keep-online`	keeps authenticated 802.1X users online when server not reachable for 802.1X reauthentication
`mac-authentication max-user 10`	max number of MA users connected to port
`mac-authentication domain clearpass`	use 'clearpass' domain for MA
`mac-authentication timer auth-delay 15`	wait 15 seconds before initiating MA
`mac-authentication re-authenticate server-unreachable keep-online`	keeps authenticated MA users online when server not reachable for MAC reauthentication
`mac-authentication host-mode multi-vlan`	allows multiple MAC-VLAN mappings per port
`mac-authentication parallel-with-dot1x`	initiate 802.1X and MA simultaneously
`mac-authentication re-authenticate`	allow periodic reauthentication
`port-security port-mode userlogin-secure-or-mac-ext`	allow authentication of multiple 802.1X and/or MA users
`dhcp snooping binding record`	add snooping entry to table

ClearPass: Basics

Comware 7 uses the H3C RADIUS dictionary and new RADIUS VSAs were added to support some new features like captive portal redirect. In ClearPass 6.7.X, Verify that the dictionary in your ClearPass instance has attribute #210, **`H3C-AVPair`** and attribute #250, **`H3C-Web-URL`**. If either of these are missing (ClearPass 6.6.X and earlier), download and import the latest dictionary file from support.arubanetworks.com. Instructions for importing a new or updated RADIUS dictionary can be found in the ClearPass User Guide.



Define your switch(es) as a network device(s) under **`Configuration » Network » Devices`**. At a minimum, configure **`Name`**, **`IP or Subnet Address`**, **`RADIUS Shared Secret`** and **`Vendor Name`**.



NOTE: If ClearPass 6.6.X or earlier is in use, define the vendor as Cisco. Dynamic authorization templates for H3C (used with Comware) were added in ClearPass 6.7.0.

ClearPass: MAC Authentication

Overview

The MAC Authentication service will handle headless devices like printers, phones, access points and others as well as provide the redirect URL for unknown devices and users to allow for a captive portal authentication.

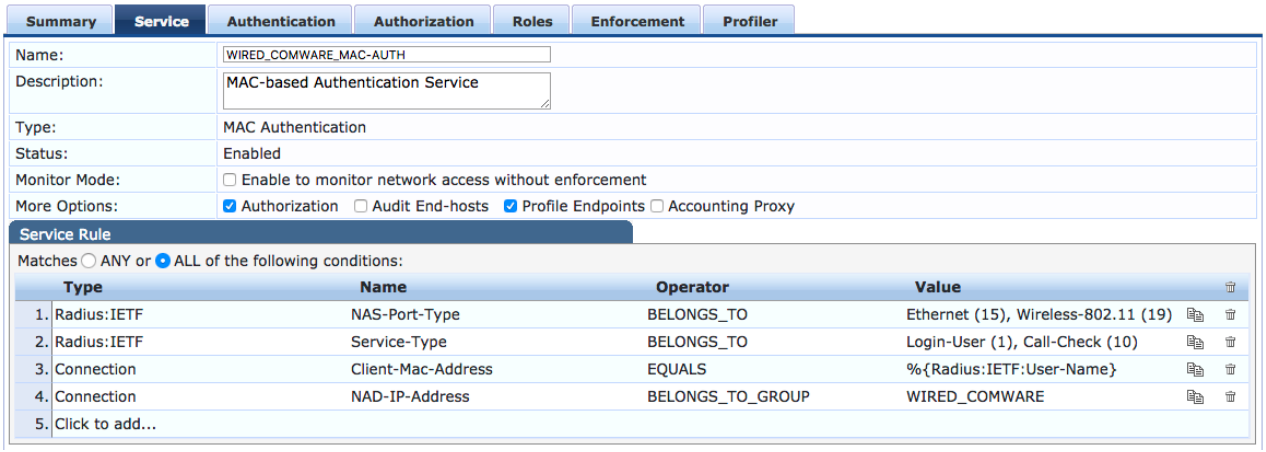
In this scenario, we're leveraging the Guest Device Repository and Device Registration Portal to allow end-users and IT staff to register headless and non-802.1X capable devices. These devices can be assigned a role and account lifetime.

Service Configuration

Start with a new service of type **`MAC Authentication`**.

Under More Options, check the **`Authorization`** and **`Profile Endpoints`** boxes. This will enable two new tabs. The default service rules will work with a CW7 switch.

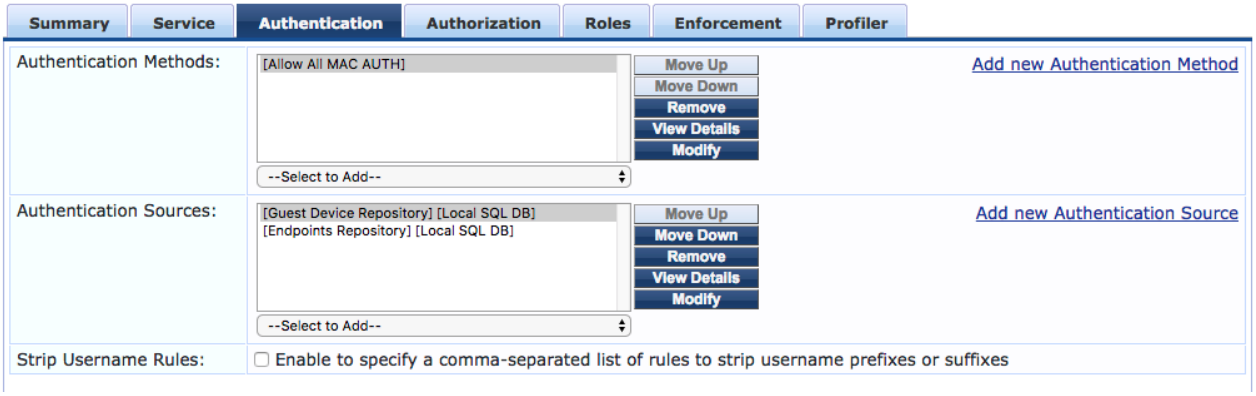
If there is a need to restrict the service to a particular set of switches, you can use a Connection | NAD-IP-Address | BELONGS_TO_GROUP rule to reference a NAD group as seen in rule 4 below.



Authentication

On the authentication tab, remove **[MAC Auth]** under Authentication Methods and add **[Allow All MAC Auth]**.

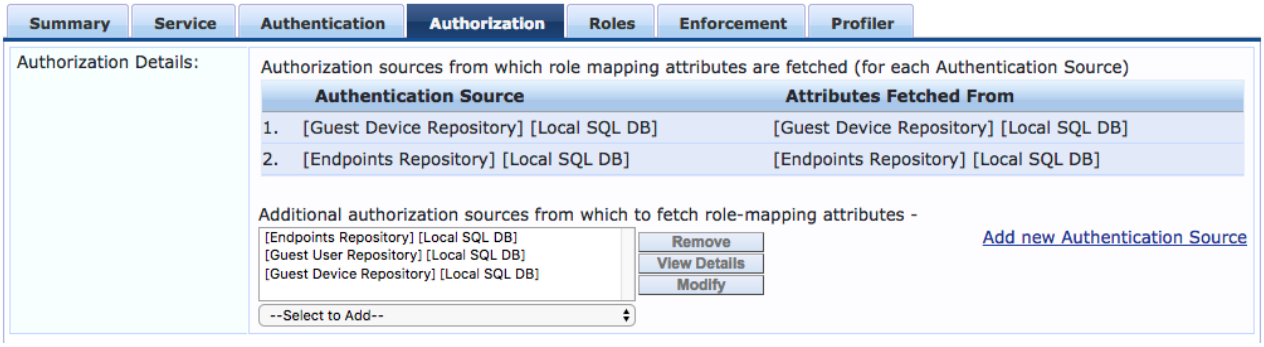
For Authentication Sources, you'll add **[Guest Device Repository] [Local SQL DB]** and move it above **[Endpoints Repository] [Local SQL DB]**.



Authorization

On the Authorization tab, add the **[Endpoints Repository], [Guest User Repository]** and **[Guest Device Repository]** to the "Additional authorization sources…" list as shown below.

By default, authorization data is only fetched from the authentication source where the user/device was found.

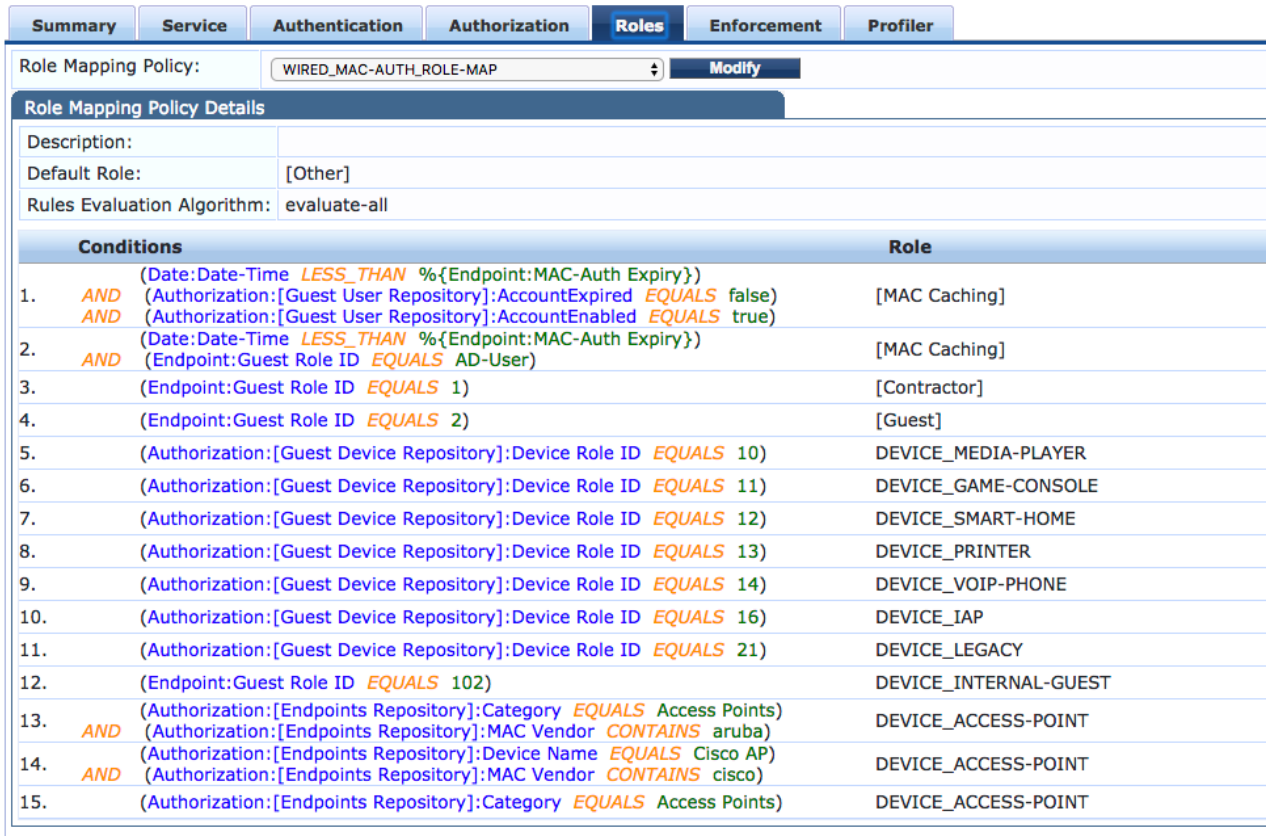


So, for example, let's say a guest user's device is re-authenticating to the network within their account expiration window, you'll find the MAC address in the [Endpoints Repository] with some data like guest role and expiration time but we also want to check with ClearPass Guest to make sure an administrator hasn't disable the account.

Roles

Role mapping is used to tag devices and users with as much information as possible for use in a policy decision.

- Rule 1 and 2 are checking to see that a guest user account is still valid and returning the [MAC Caching] tag / TIPS role
- Rules 3-12 map user and device role IDs to tags / TIPS roles for use in policy
- Rules 13-15 map profiling data to a tag / TIPS role for use in policy



Summary | Service | Authentication | Authorization | Roles | Enforcement | Profiler

Role Mapping Policy: WIRED_MAC-AUTH_ROLE-MAP [Modify]

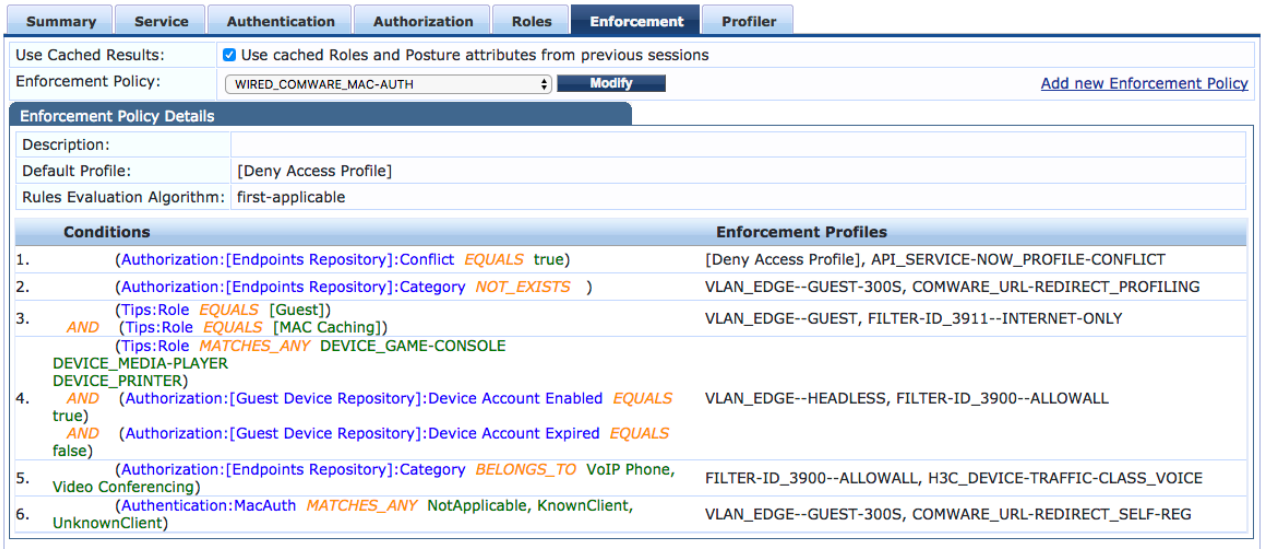
Role Mapping Policy Details

Description:	
Default Role:	[Other]
Rules Evaluation Algorithm:	evaluate-all

	Conditions	Role
1.	(Date:Date-Time *LESS_THAN* %{Endpoint:MAC-Auth Expiry}) *AND* (Authorization:[Guest User Repository]:AccountExpired *EQUALS* false) *AND* (Authorization:[Guest User Repository]:AccountEnabled *EQUALS* true)	[MAC Caching]
2.	(Date:Date-Time *LESS_THAN* %{Endpoint:MAC-Auth Expiry}) *AND* (Endpoint:Guest Role ID *EQUALS* AD-User)	[MAC Caching]
3.	(Endpoint:Guest Role ID *EQUALS* 1)	[Contractor]
4.	(Endpoint:Guest Role ID *EQUALS* 2)	[Guest]
5.	(Authorization:[Guest Device Repository]:Device Role ID *EQUALS* 10)	DEVICE_MEDIA-PLAYER
6.	(Authorization:[Guest Device Repository]:Device Role ID *EQUALS* 11)	DEVICE_GAME-CONSOLE
7.	(Authorization:[Guest Device Repository]:Device Role ID *EQUALS* 12)	DEVICE_SMART-HOME
8.	(Authorization:[Guest Device Repository]:Device Role ID *EQUALS* 13)	DEVICE_PRINTER
9.	(Authorization:[Guest Device Repository]:Device Role ID *EQUALS* 14)	DEVICE_VOIP-PHONE
10.	(Authorization:[Guest Device Repository]:Device Role ID *EQUALS* 16)	DEVICE_IAP
11.	(Authorization:[Guest Device Repository]:Device Role ID *EQUALS* 21)	DEVICE_LEGACY
12.	(Endpoint:Guest Role ID *EQUALS* 102)	DEVICE_INTERNAL-GUEST
13.	(Authorization:[Endpoints Repository]:Category *EQUALS* Access Points) *AND* (Authorization:[Endpoints Repository]:MAC Vendor *CONTAINS* aruba)	DEVICE_ACCESS-POINT
14.	(Authorization:[Endpoints Repository]:Device Name *EQUALS* Cisco AP) *AND* (Authorization:[Endpoints Repository]:MAC Vendor *CONTAINS* cisco)	DEVICE_ACCESS-POINT
15.	(Authorization:[Endpoints Repository]:Category *EQUALS* Access Points)	DEVICE_ACCESS-POINT

Enforcement

Let's take apart this enforcement policy rule by rule:



1 (Authorization:[Endpoints Repository]:Conflict EQUALS true) [Deny Access Profile], API_SERVICE-NOW_PROFILE-CONFLICT

If a device's profiled category changes, ClearPass triggers a Conflict attribute.

If the `Conflict` attribute is `true`, deny access to the network and also send an API call over to ServiceNow to open a ticket.

Other options could include a captive portal redirect to notify the user, text message to the user, etc.

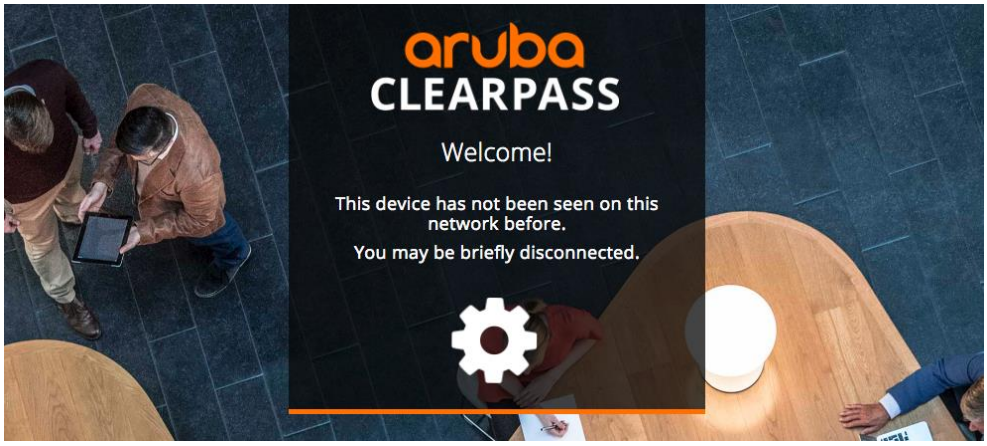
2

(Authorization:[Endpoints Repository]:Category *NOT_EXISTS*)	VLAN_EDGE--GUEST-300S, COMWARE_URL-REDIRECT_PROFILING

This rule evaluates whether the profile `Category` exists for the authenticating endpoint.

If it does not exist, the device has not been profiled and a redirect URL, ACL number, short session-timeout and a VLAN assignment are returned to the switch.

	Type	Name		Value
1.	Radius:H3C	H3C-AVPair	=	url-redirect-acl=3910
2.	Radius:H3C	H3C-AVPair	=	url-redirect=https://clearpass-demo.net.arubaboston.com/guest/wired_profiling.php?mac=%{Connection:Client-Mac-Address-Colon}
3.	Radius:IETF	Session-Timeout	=	60



NOTE: Captive portal is not required for profiling. It's simply an example of leveraging features to improve user experience.

3

(Tips:Role *EQUALS* [Guest]) *AND* (Tips:Role *EQUALS* [MAC Caching])	VLAN_EDGE--GUEST, FILTER-ID_3911--INTERNET-ONLY

During role mapping, we were able to determine that the device should still be MAC Cached based on its expiration and the user's account status.

The **`EDGE_GUEST`** VLAN and the ACL number for internet only access will be returned.

4

(Tips:Role *MATCHES_ANY* DEVICE_GAME-CONSOLE DEVICE_MEDIA-PLAYER DEVICE_PRINTER) *AND* (Authorization:[Guest Device Repository]:Device Account Enabled *EQUALS* true) *AND* (Authorization:[Guest Device Repository]:Device Account Expired *EQUALS* false)	VLAN_EDGE--HEADLESS, FILTER-ID_3900--ALLOWALL

Many headless devices have been registered via the Device Registration portal. Here we're validating whether the authenticating device was registered as a game console, media player or printer and that the device account is enabled and hasn't expired.

The **`EDGE_HEADLESS`** VLAN is being returned along with the ACL number for `ALLOWALL`.

5

(Authorization:[Endpoints Repository]:Category *BELONGS_TO* VoIP Phone, Video Conferencing)	FILTER-ID_3900--ALLOWALL, H3C_DEVICE-TRAFFIC-CLASS_VOICE

Based on profiling data, devices categorized as VoIP Phone and Video Conferencing are authorized by sending back a filter-id and device-traffic-class.

	Type	Name		Value
1.	Radius:H3C	H3C-AVPair	=	device-traffic-class=voice

This `device-traffic-class=voice` attribute/value pair tells the switch that this device should be treated as a voice device. Since the ports are configured as hybrid and a voice VLAN is mapped, the voice VLAN will be tagged down to the voice device.

```
<EDGE-5130EI>dis mac-authentication connection interface GigabitEthernet 1/0/3
Total connections: 1

Slot ID: 1
User MAC address: 2c41-387f-c880
Access interface: GigabitEthernet1/0/3
Username: 2c41387fc880
Authentication domain: clearpass
Initial VLAN: 813
Authorization untagged VLAN: N/A
Authorization tagged VLAN: 813
Authorization ACL ID: 3900
Authorization user profile: N/A
Authorization URL:  N/A
Termination action: Default
Session timeout period: N/A
Online from: 2017/04/03 01:42:42
Online duration: 0h 5m 56s
```

6

(Authentication:MacAuth *MATCHES_ANY* NotApplicable, KnownClient, UnknownClient)	VLAN_EDGE--GUEST-300S, COMWARE_URL-REDIRECT_SELF-REG

The last rule is effectively a “catch all” which handles unknown devices.

Enforcement action #1 uses the **`url-redirect-acl`** H3C-AVPair to tell the switch to use ACL number 3910 on the switch for redirection to the captive portal.

Action #2 provides the redirect URL to the switch using the **`url-redirect`** H3C-AVPair. Notice that we added a variable to dynamically appended the client MAC address to the URL. This is required for many guest workflows.

	Type	Name		Value
1.	Radius:H3C	H3C-AVPair	=	url-redirect-acl=3910
2.	Radius:H3C	H3C-AVPair	=	url-redirect=https://clearpass-demo.net.arubaboston.com/guest/wired_comware_self-reg.php?mac=%{Connection:Client-Mac-Address-Colon}

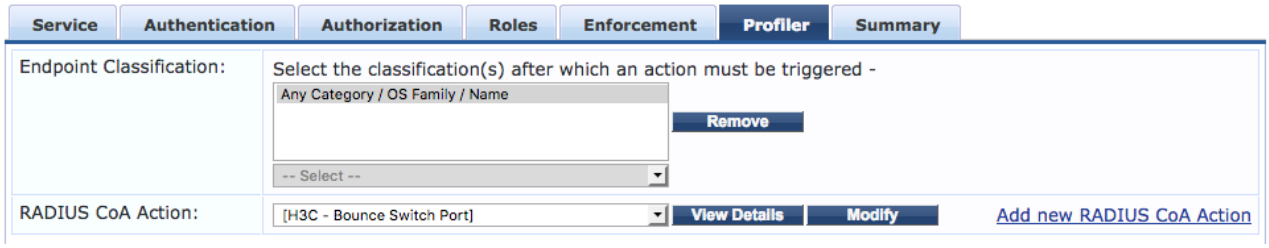
The second enforcement profile returns the **`EDGE_GUEST`** VLAN and a session-timeout which cause the device to be reauthenticated every 5 minutes until registered.

Profiler

The Profiler function allows for an unknown device to be automatically disconnected from the network once profile data has been collected and evaluated. This prevents a device from being "stuck" in a limited access role. During the second authentication, the new profile data can be used in the policy decision. This is a very common feature for MAC Authentication services.

Since we may want to drop a newly profile device into a new VLAN, the port will need to be bounced to force the device to re-DHCP.

Use caution in voice environments where client devices are connected behind a voice device. Bouncing a port after profiling a client device connected behind the voice device could result in interruption of voice service.



NOTE: In ClearPass 6.6.X and earlier, use the `[Cisco - Bounce-Host-Port]` enforcement profile.

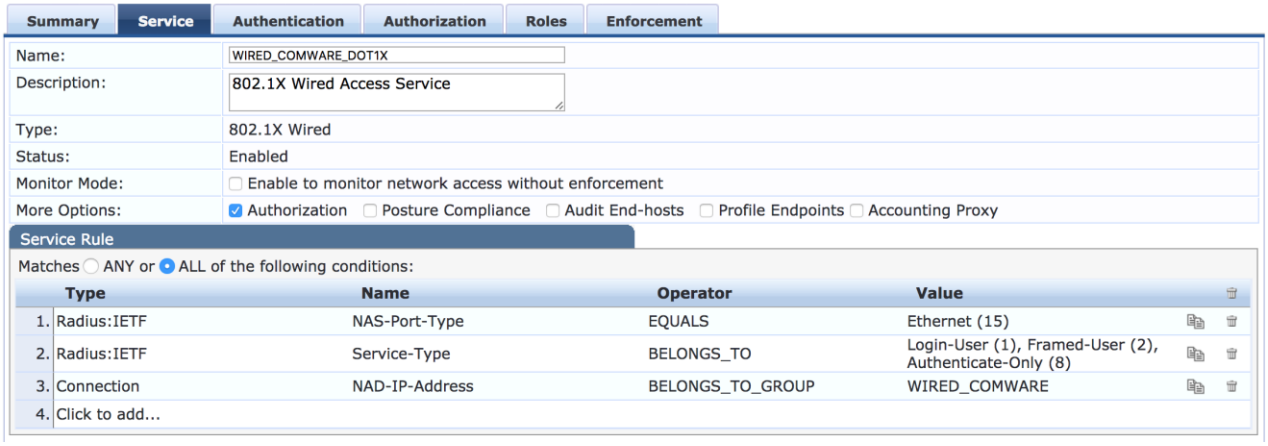
ClearPass: 802.1X

Service Configuration

Create a new service of type **`802.1X Wired`**.

Under More Options, check the **`Authorization`** boxes. The default service rules will work with an ArubaOS-Switch.

If there is a need to restrict the service to a particular group of switches, you can use a `Connection | NAD-IP-Address | BELONGS_TO_GROUP` rule to reference a NAD group as seen in rule 3 below.



Authentication

This service will be supporting both secure certificate-based authentication (EAP-TLS) and traditional, legacy username and password authentication (PEAPv0/EAP-MSCHAPv2).

The username and password-based authentication will be used for two purposes:

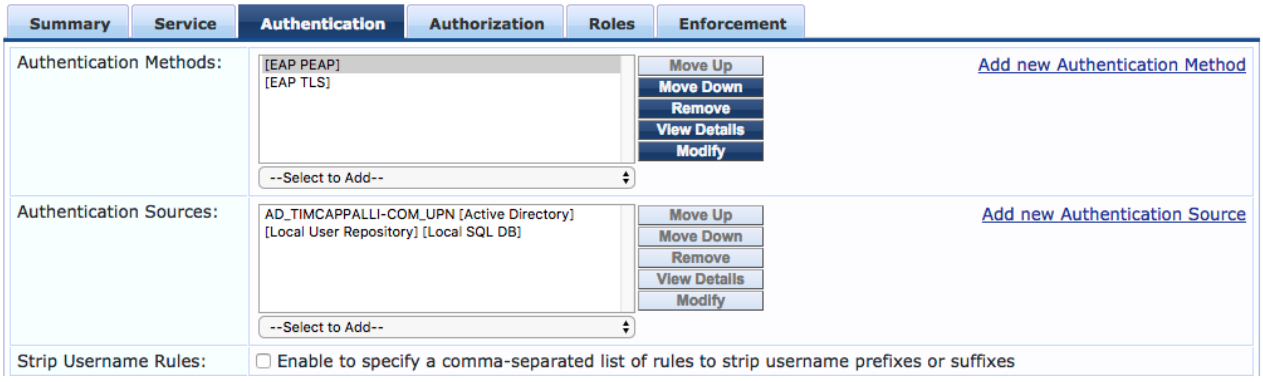
1) Allow a BYOD device to initially connect and kick off the Onboard process to allow a certificate to be issued
2) Allow for domain-joined assets to use their computer/machine account to authenticate to the network as well as support machine + user workflows

Based on the above requirements, remove all the default EAP methods from the Authentication Methods list on the Authentication tab except for **`[EAP PEAP]`** and **`[EAP TLS]`**.

> **NOTE:** The default **`[EAP TLS]`** method does not have OCSP authorization configured and is being used here solely as an example. OCSP is used to check real-time validity of a certificate and enabling it is highly recommended. Special care should be taken when authenticating certificates from different certificate authorities. This is outside the scope of this document.

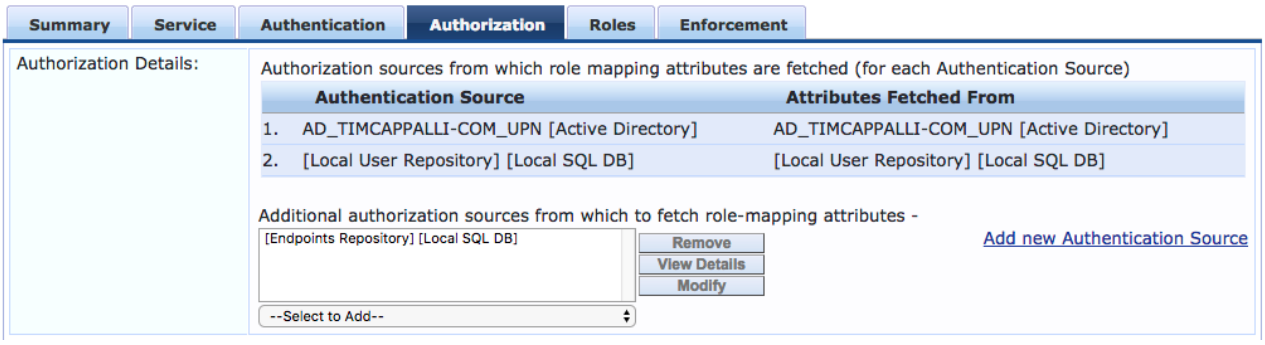
For Authentication Sources, you'll add our Active Directory identity store and also the **`[Local User Repository]`**. Authentication sources will vary in your environment.

The Local User Repository will be used in the example for infrastructure accounts like having an access point or VoIP phone authenticate securely to the network using the 802.1X framework.



Authorization

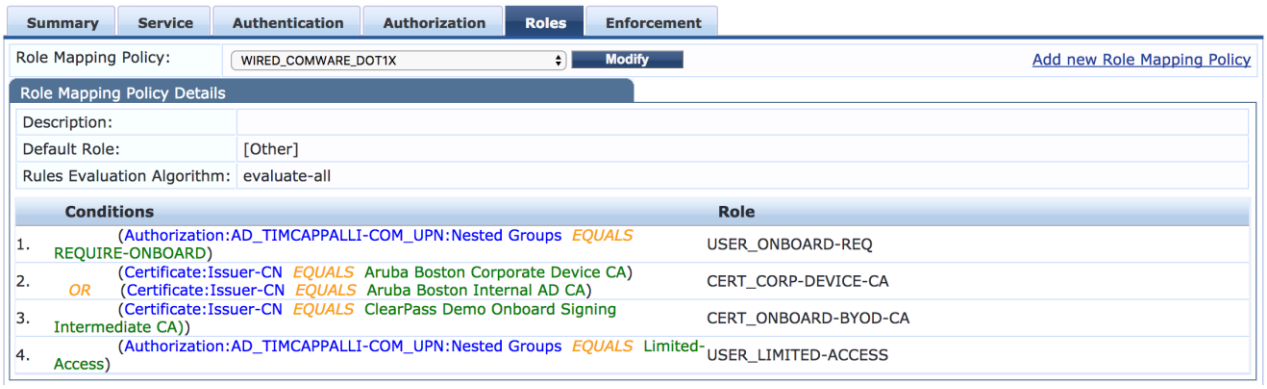
Since device profile information will be leveraged in policy, add the **`[Endpoints Repository]`** to the "Additional authorization sources…" list as shown below.



Roles

Role mapping is used to tag devices and users with as much prevalent information as possible for use in a policy decision.

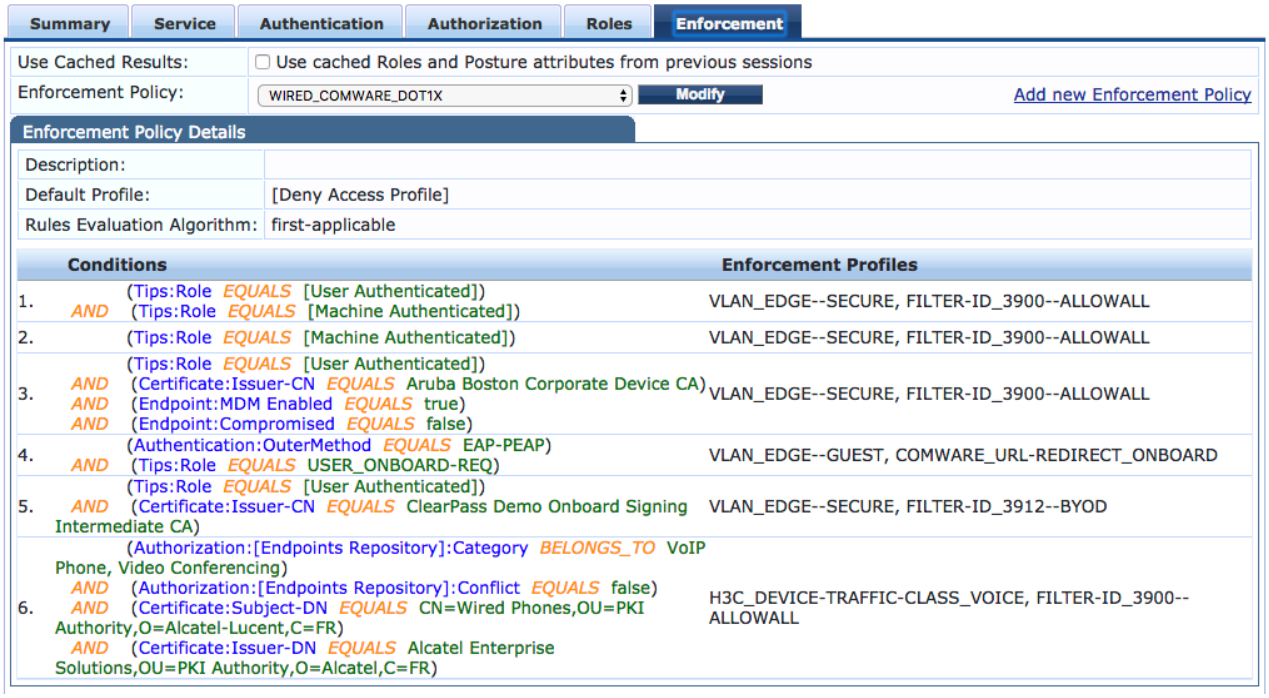
These rules and tags will vary greatly by environment, but below you'll find examples of device and user tagging.



- Rules 1 and 4 are checking group membership from Active Directory
- Rules 2-3 are matching on the common name of the issuing CA for the authenticating certificate

Enforcement

Let's take apart this enforcement policy rule by rule:



Summary | Service | Authentication | Authorization | Roles | Enforcement

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

Enforcement Policy: WIRED_COMWARE_DOT1X [Modify] Add new Enforcement Policy

Enforcement Policy Details

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

	Conditions	Enforcement Profiles
1.	(Tips:Role EQUALS [User Authenticated]) AND (Tips:Role EQUALS [Machine Authenticated])	VLAN_EDGE--SECURE, FILTER-ID_3900--ALLOWALL
2.	(Tips:Role EQUALS [Machine Authenticated])	VLAN_EDGE--SECURE, FILTER-ID_3900--ALLOWALL
3.	(Tips:Role EQUALS [User Authenticated]) AND (Certificate:Issuer-CN EQUALS Aruba Boston Corporate Device CA) AND (Endpoint:MDM Enabled EQUALS true) AND (Endpoint:Compromised EQUALS false)	VLAN_EDGE--SECURE, FILTER-ID_3900--ALLOWALL
4.	(Authentication:OuterMethod EQUALS EAP-PEAP) AND (Tips:Role EQUALS USER_ONBOARD-REQ)	VLAN_EDGE--GUEST, COMWARE_URL-REDIRECT_ONBOARD
5.	(Tips:Role EQUALS [User Authenticated]) AND (Certificate:Issuer-CN EQUALS ClearPass Demo Onboard Signing Intermediate CA)	VLAN_EDGE--SECURE, FILTER-ID_3912--BYOD
6.	(Authorization:[Endpoints Repository]:Category BELONGS_TO VoIP Phone, Video Conferencing) AND (Authorization:[Endpoints Repository]:Conflict EQUALS false) AND (Certificate:Subject-DN EQUALS CN=Wired Phones,OU=PKI Authority,O=Alcatel-Lucent,C=FR) AND (Certificate:Issuer-DN EQUALS Alcatel Enterprise Solutions,OU=PKI Authority,O=Alcatel,C=FR)	H3C_DEVICE-TRAFFIC-CLASS_VOICE, FILTER-ID_3900--ALLOWALL

1

	(Tips:Role EQUALS [User Authenticated])	
AND	(Tips:Role EQUALS [Machine Authenticated])	VLAN_EDGE--SECURE, FILTER-ID_3900--ALLOWALL

When a Windows device authenticates to the network using its Active Directory computer account, the `[Machine Authenticated]` tag/TIPS role is added to the session automatically.

If both a machine and user authentication have occurred, then return the **`EDGE_SECURE`** VLAN name and filter-ID **`3900`** which matches an allowall ACL locally on the switch.

This is commonly used to validate that the user is using a corporate asset.

2

	(Tips:Role EQUALS [Machine Authenticated])	VLAN_EDGE--SECURE, FILTER-ID_3900--ALLOWALL

Rule 2 is for a machine-only authentication. These typically occur when the device is sitting at the Windows logon screen and connectivity is required for updates, remote access or for new users to login.

3

(Tips:Role *EQUALS* [User Authenticated]) *AND* (Certificate:Issuer-CN *EQUALS* Aruba Boston Corporate Device CA) *AND* (Endpoint:MDM Enabled *EQUALS* true) *AND* (Endpoint:Compromised *EQUALS* false)	VLAN_EDGE--SECURE, FILTER-ID_3900--ALLOWALL

This is a typical rule to deal with a non-Windows corporate-managed asset that is managed by an EMM solution. The two endpoint attributes have been synced down from the EMM solution via ClearPass Exchange. In this case, the rule is evaluating whether the device has its device management enabled and that no compromise has occurred. The last condition checks for the tag/TIPS role from our role mapping to verify the certificate used to authenticate was issued from the Corporate Device CA.

4

(Authentication:OuterMethod *EQUALS* EAP-PEAP) *AND* (Tips:Role *EQUALS* USER_ONBOARD-REQ)	VLAN_EDGE--GUEST, COMWARE_URL-REDIRECT_ONBOARD

Most personal devices will perform Onboarding through the captive portal workflow after 802.1X fails, but some users may authenticate via PEAPv0/EAP-MSCHAPv2 when prompted by their device. This rule will catch those users who need to be using certificate-based authentication (EAP-TLS) via ClearPass Onboard.

A **`url-redirect-acl`** number is returned to the switch along with the Onboard enrollment URL via the H3C-AVPair attributes. This ACL was configured locally on the switch earlier.

	Type	Name		Value
1.	Radius:H3C	H3C-AVPair	=	url-redirect-acl=3910
2.	Radius:H3C	H3C-AVPair	=	url-redirect=https://clearpass-demo.net.arubaboston.com/onboard/wired_onboard_1.php?mac=%{Connection:Client-Mac-Address-Colon}

5

(Tips:Role *EQUALS* [User Authenticated]) *AND* (Certificate:Issuer-CN *EQUALS* ClearPass Demo Onboard Signing Intermediate CA)	VLAN_EDGE--SECURE, FILTER-ID_3912--BYOD

After a device has been onboarded, subsequent authentications will occur via EAP-TLS. Rule 5 uses the tag from the role mapping to check the common name of the issuing CA. These devices will be dropped into the **`EDGE_SECURE`** VLAN with 3912 returned as a filter-ID which is the BYOD ACL locally defined on the switch.

6

(Authorization:[Endpoints Repository]:Category *BELONGS_TO* VoIP Phone, Video Conferencing) *AND* (Authorization:[Endpoints Repository]:Conflict *EQUALS* false) *AND* (Certificate:Subject-DN *EQUALS* CN=Wired Phones,OU=PKI Authority,O=Alcatel-Lucent,C=FR) *AND* (Certificate:Issuer-DN *EQUALS* Alcatel Enterprise Solutions,OU=PKI Authority,O=Alcatel,C=FR)	H3C_DEVICE-TRAFFIC-CLASS_VOICE, FILTER-ID_3900--ALLOWALL

Many voice devices come from the factory with an embedded certificate that can be used for network authentication. Here we're leveraging the factory cert for EAP-TLS combined with profiling data.

This **`device-traffic-class=voice`** attribute/value pair tells the switch that this device should be treated as a voice device. Since the ports are configured as hybrid and a voice VLAN is mapped, the voice VLAN will be tagged down to the voice device. The ACL number for allowall is also passed as a filter-id.

ClearPass: Web Authentication

The Web Authentication service handles captive portal-based authentications with server-initiated workflows.

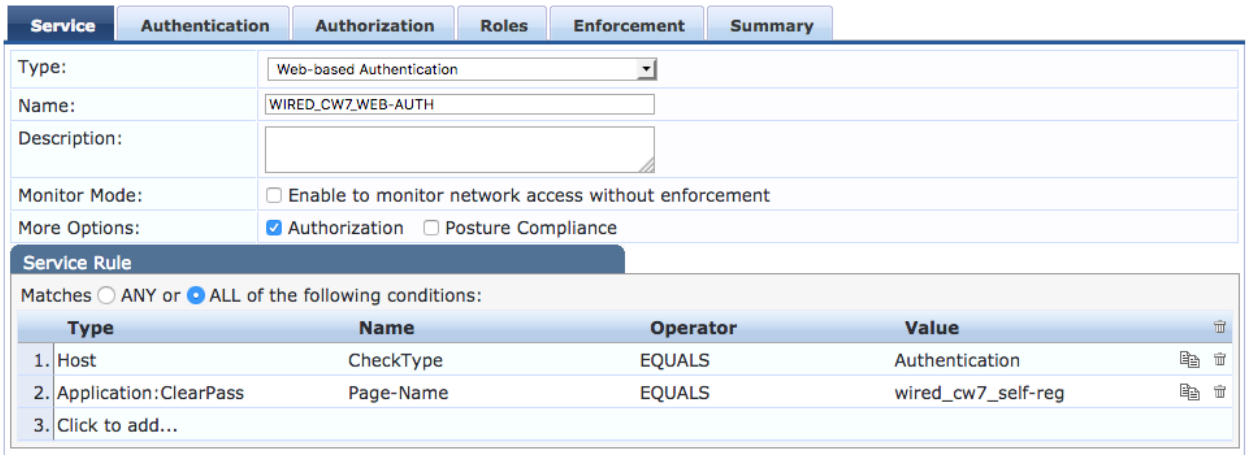
Service Configuration

Create a new service of type **`Web-based Authentication`**.

Check the **`Authorization`** box and select **`Matches ALL`** under Service Rule.

Add a second service rule with **`Application:ClearPass`** | **`Page-Name`** | **`EQUALS`** and then the page name.

For example: if the full page URL is `https://<fqdn>/guest/wired_cw7_self-reg.php`, then the page name is: `wired_cw7_self-reg`.

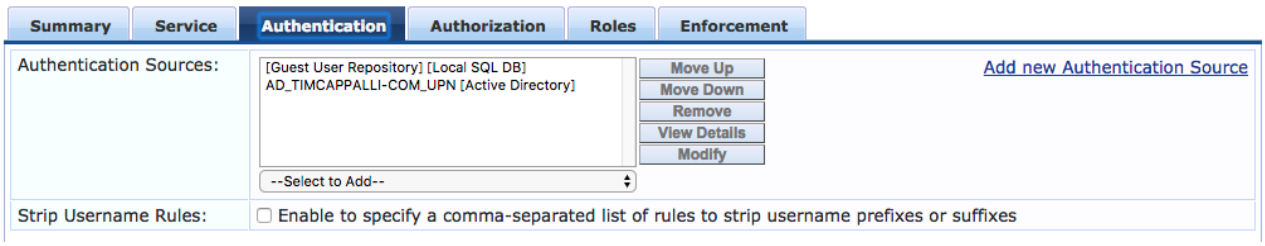


NOTE: The Page-Name attribute was added in ClearPass 6.7.0. Skip if using ClearPass 6.6.X.

Authentication

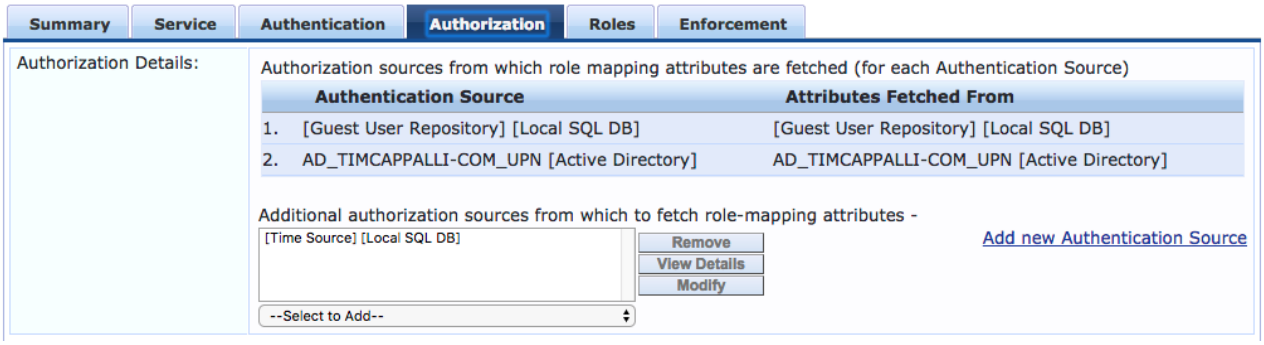
This service will be supporting both guest and Active Directory users for captive portal login.

For Authentication Sources, you'll add the **`[Guest User Repository]`** and also our Active Directory identity store. Authentication sources will vary in your environment.



Authorization

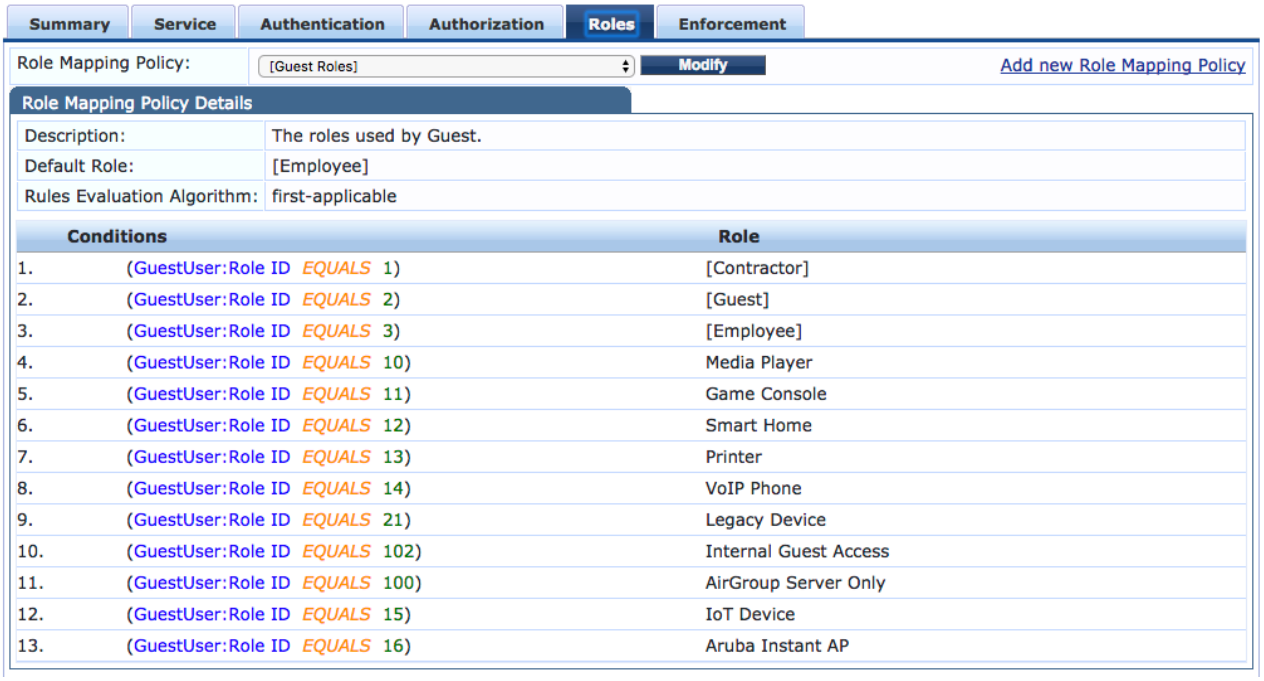
We will need to assign a manual expiration time to AD users. This time is calculated by the **[Time Source]** so it will need to be added as an additional authorization source.



Roles

In this scenario, guests and contractors will go through a standard self-registration process and any employee who authenticates with their corporate credentials will get a temporary guest role. Since there is no specific mapping of AD group, you'll use the generic **[Guest Roles]** role map.

If different enforcement actions will be taken for different groups or classifications of users, create a new role map like the in 802.1X configuration.



Enforcement

Because the server-initiated workflow is used with Comware 7, the enforcement policy for the WEBAUTH service is very simple. The goal is to update the device endpoint record with attributes from the user authentication that will be stored and used for subsequent authentications and then bounce the port to trigger a reauthentication event.

> **Note:** If a VLAN change is not required, a Terminate Session disconnect message can be used instead of a port bounce.

In this example, only guest users are permitted.

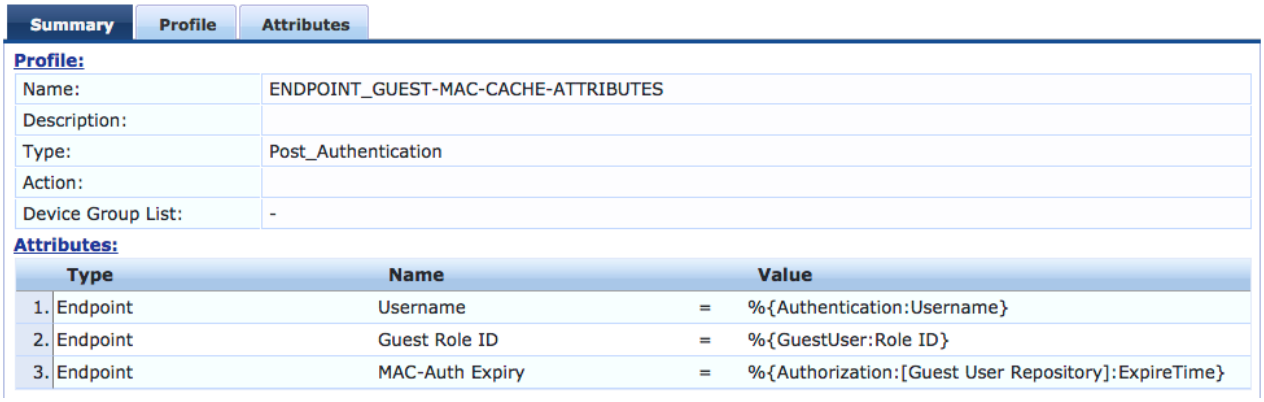
A basic enforcement profile for MAC caching the device is used so when re-authenticating after the port bounce, the user will not be prompted to authenticate again until their account expires.

Before creating the enforcement policy, create a new enforcement profile for the guest users (**`Configuration » Enforcement » Profiles » Add Enforcement Profile`**).

- Select `ClearPass Entity Update Enforcement` from the Template dropdown
- Give the profile a name
- On the attributes tab, add the 3 entries below and then save

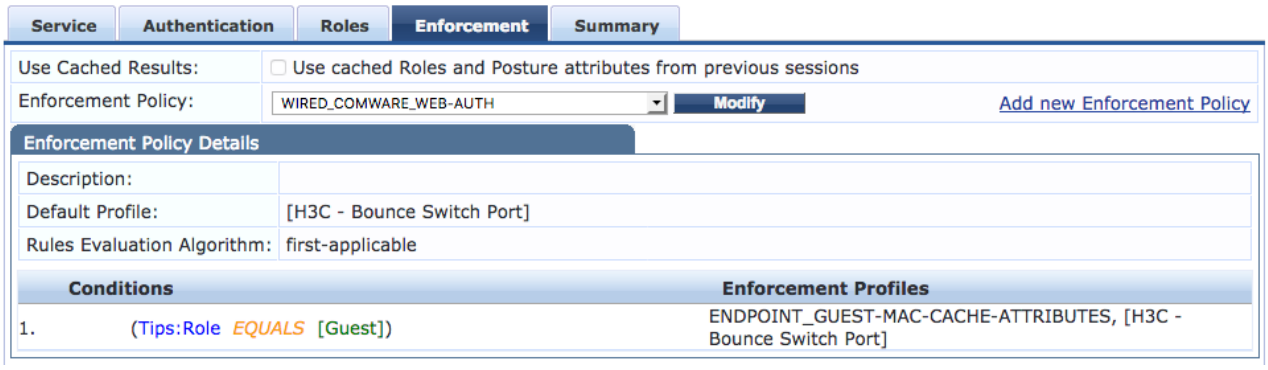
  Note that the value field will require manual entry (copy and paste the values below)

TYPE	NAME	VALUE
Endpoint	`Username`	`%{Authentication:Username}`
Endpoint	`Guest Role ID`	`%{GuestUser:Role ID}`
Endpoint	`MAC-Auth Expiry`	`%{Authorization:[Guest User Repository]:ExpireTime}`



Now, create a very basic enforcement policy with a single rule which checks for the TIPS roles / tags **[Guest]** and **[MAC Caching]**. The enforcement profiles will be **[H3C – Bounce Switch Port]** and the endpoint update profile that you just created.

The **Default Profile** for the Enforcement Policy can be set to **[H3C – Bounce Switch Port]**.

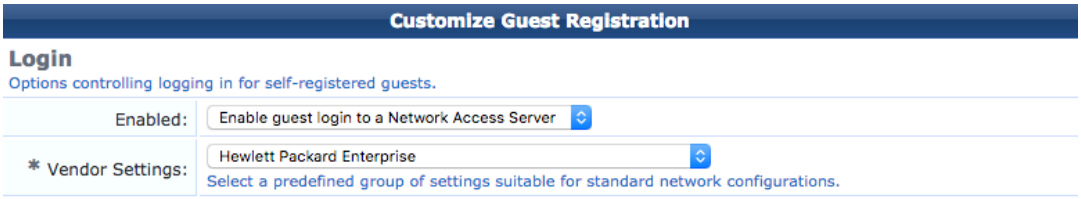


NOTE: In ClearPass 6.6.X and earlier, use the `[Cisco - Bounce-Host-Port]` enforcement profile.

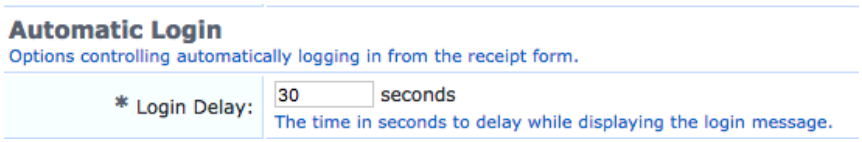
ClearPass: Guest

Configuring a self-registration workflow in Guest is outside the scope of the document. For the purposes of this guide, the only relevant settings on the guest side are the **NAS Vendor Settings** and the **Login Delay**.

Under **NAS Vendor Settings**, be sure the **Vendor Settings** are set to **Hewlett Packard Enterprise** which should automatically set the **Login Method** to **Server-initiated**. This is what tells Guest to craft a WEBAUTH request which we just built the service for.



Under **Login Delay**, set the value to a minimum of 30 seconds. This is required with server-initiated workflows because we don't want the user to attempt to browse while the port is still down or their device is re-authenticating. You may need to adjust this value in your environment.



Useful Switch Troubleshooting Commands

display dot1x sessions
display dot1x sessions interface <interface>

```
<EDGE-5130EI>dis dot1x sessions
 GigabitEthernet1/0/1  is link-down
   Online 802.1X users: 0
 GigabitEthernet1/0/2  is link-down
   Online 802.1X users: 0
 GigabitEthernet1/0/3  is link-up
   Online 802.1X users: 0
 GigabitEthernet1/0/4  is link-down
   Online 802.1X users: 0
 GigabitEthernet1/0/5  is link-down
   Online 802.1X users: 0
 GigabitEthernet1/0/6  is link-up
   Online 802.1X users: 1
          MAC address       Auth state
          90e2-ba69-2d5a    Authenticated
 GigabitEthernet1/0/7  is link-up
   Online 802.1X users: 0
GigabitEthernet1/0/8  is link-down
  Online 802.1X users: 0
```

display dot1x connection
display dot1x connection interface <interface>
display dot1x connection user-name <username>
display dot1x connection user-mac <MAC>

```
<EDGE-5130EI>display dot1x connection
Total connections: 1

Slot ID: 1
User MAC address: 90e2-ba69-2d5a
Access interface: GigabitEthernet1/0/6
Username: kylo.ren@timcappalli.com
Authentication domain: clearpass
IPv4 address: 100.81.1.12
Authentication method: EAP
Initial VLAN: 1
Authorization untagged VLAN: 811
Authorization tagged VLAN list: N/A
Authorization ACL ID: 3900
Authorization user profile: N/A
Authorization URL:  N/A
Termination action: Radius-request
Session timeout period: 43200 s
Online from: 2017/04/03 02:05:30
Online duration: 0h 8m 12s
```

display mac-authentication interface <interface>

```
<EDGE-5130EI>dis mac-authentication interface GigabitEthernet 1/0/3
Global MAC authentication parameters:
   MAC authentication     : Enabled
   User name format       : MAC address in lower case(xxxxxxxxxxxx)
           Username       : mac
           Password       : mac
   Offline detect period  : 300 s
   Quiet period           : 60 s
   Server timeout         : 100 s
   Reauth period          : 3600 s
   Authentication domain  : Not configured, use default domain
 Max MAC-auth users       : 4294967295 per slot
 Online MAC-auth users    : 1

GigabitEthernet1/0/3  is link-up
   MAC authentication         : Enabled
   Carry User-IP              : Disabled
   Authentication domain      : clearpass
   Auth-delay timer           : Enabled
   Auth-delay period          : 15 s
   Periodic reauth            : Enabled
   Reauth period              : N/A
   Re-auth server-unreachable : Online
   Guest VLAN                 : Not configured
   Guest VLAN auth-period     : 30
   Critical VLAN              : Not configured
   Critical voice VLAN        : Disabled
   Host mode                  : Multiple VLAN
   Offline detection          : Enabled
   Authentication order       : Parallel

   Max online users           : 10
   Authentication attempts    : successful 21, failed 0
   Current online users       : 1
          MAC address       Auth state
          2c41-387f-c880    Authenticated
```

display mac-authentication connection
display mac-authentication connection interface <interface>
display mac-authentication connection user-mac|user-name <MAC>|<username>

```
<EDGE-5130EI>dis mac-authentication connection interface GigabitEthernet 1/0/3
Total connections: 1
Slot ID: 1
User MAC address: 2c41-387f-c880
Access interface: GigabitEthernet1/0/3
Username: 2c41387fc880
Authentication domain: clearpass
Initial VLAN: 813
Authorization untagged VLAN: N/A
Authorization tagged VLAN: 813
Authorization ACL ID: 3900
Authorization user profile: N/A
Authorization URL:  N/A
Termination action: Default
Session timeout period: N/A
Online from: 2017/04/03 01:42:42
Online duration: 0h 5m 56s
```

SNMP-based Enforcement

Policy Enforcement

VLAN assignment via SNMP is the primary enforcement method with OnConnect. VLAN access control lists (ACLs) are commonly used to control traffic in this scenario.

Configuration Overview

Here are the hardware and software combinations used for this configuration:

- HPE 5130EI switch running code version 7.10.R3115P07 (no version dependency)
- ClearPass Policy Manager 6.7.1 (required: 6.7.1+)

This configuration example uses SNMP v2c. SNMPv3 is also supported for OnConnect.

Quirks and Limitations

- Active user visibility is available for Windows domain-joined machines only
- OnConnect enforcement takes an average of 60 seconds with WMI enabled

Switch Configuration

Global switch configuration:

`snmp-agent`	enable SNMP agent
`snmp-agent community read C0mw@re!`	define SNMP ro community for ClearPasss
`snmp-agent community write C!earP@ss0nConn5ct`	define SNMP rw community for ClearPass
`snmp-agent target-host trap address udp-domain 100.65.30.52 params securityname C!earP@ss0nConn5ct v2c`	set ClearPass as the snmp trap destination

`snmp-agent trap enable mac-address`
`snmp-agent trap enable arp`
`snmp-agent trap if-mib link extended`
	enable SNMP traps

Interface configuration:

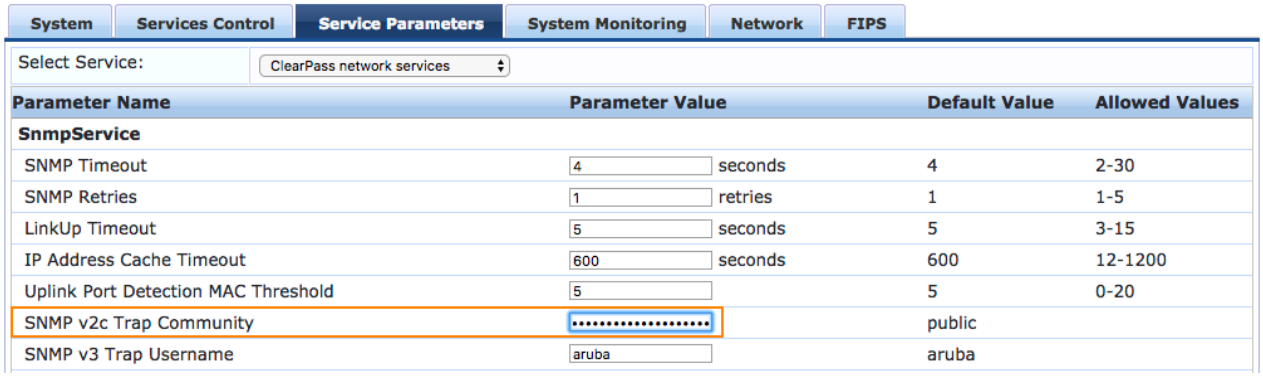
`interface range GigabitEthernet 1/0/1 to GigabitEthernet 1/0/12`
 	
`port access vlan 2101`
	set default untrusted VLAN

ClearPass: Basics

Server Configuration

Configure the **SNMP v2c Trap Community** under **Administration » Server Manager » Server Configuration, Service Parameters, ClearPass network services**.

This should match the community string defined in this switch configuration element: *snmp-server host 100.65.30.42 community ClearPassOnConnect trap-level all*



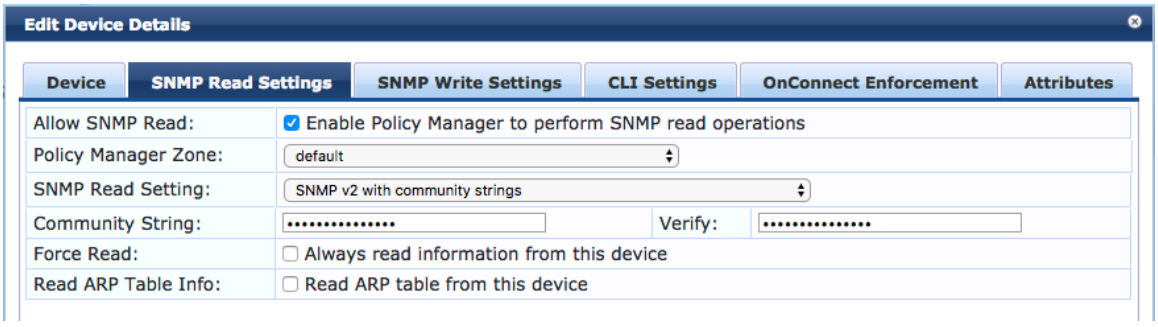
After changing the trap community, the **System auxiliary services** service needs to be restarted.

Navigate to **Administration » Server Manager » Server Configuration, Services Control** and locate **System auxiliary services.**

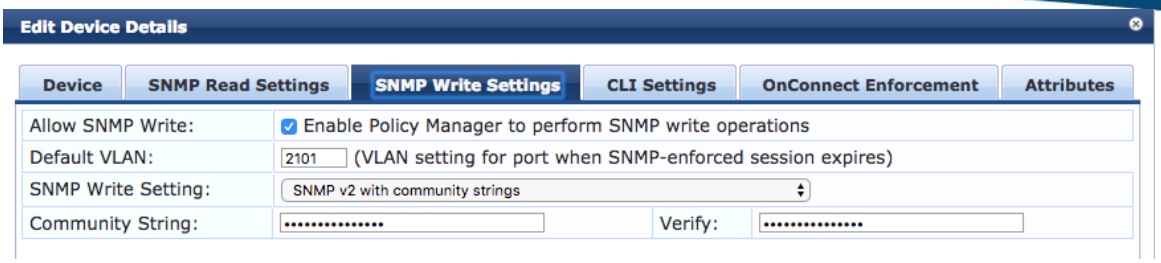
Click **Stop**. Once the service has stopped, click **Start** to restart the service.

Network Device

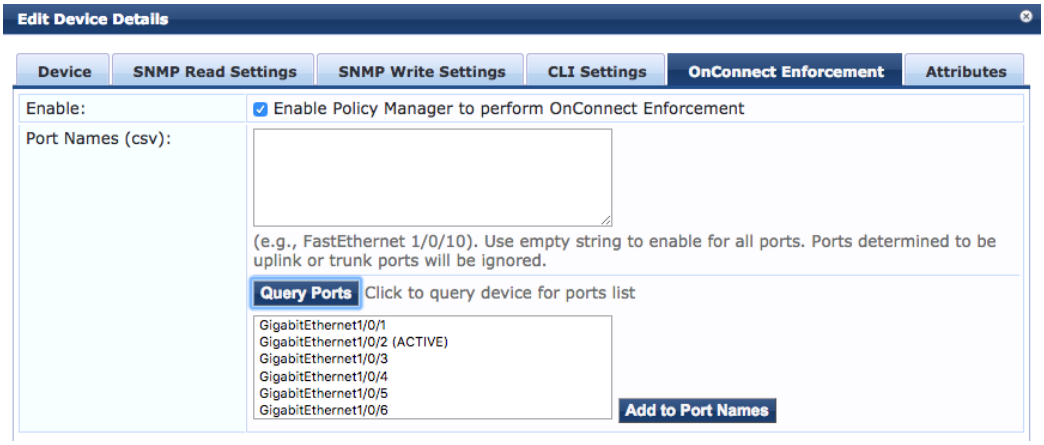
Enable SNMP Read and configure the community strings for the device:



Enable SNMP Write and configure the community strings for the device. Also, configure the Default VLAN (generally this will be the guest or untrusted VLAN):



Enable Policy Manager to perform OnConnect Enforcement.



Use the **`Query Ports`** button to test the SNMP configuration. The list will be populated with the switch ports if all is working correctly.

Individual interfaces can also be enabled for OnConnect enforcement by selecting them in the list and clicking **`Add to Port Names`** (or by manually adding them to the Port Names list).

Windows Management Instrumentation (WMI) Overview

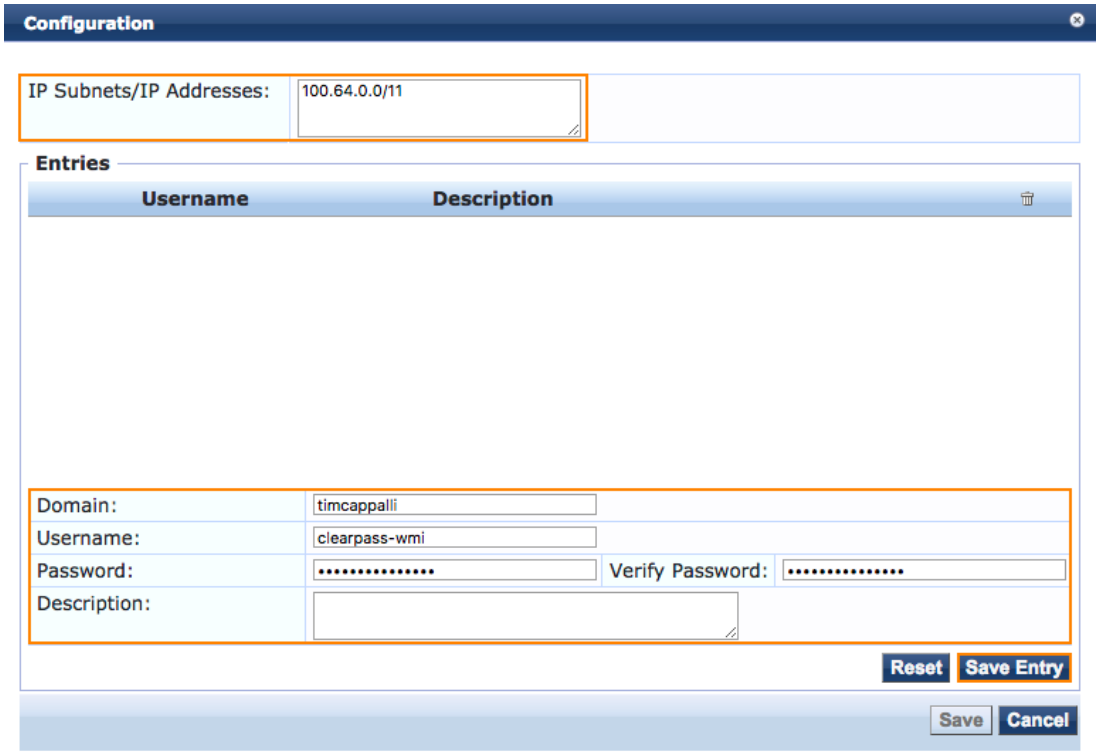
During a port status change, ClearPass can query domain-joined Windows devices for the current logged in user. This information can then be compared with user account information in Active Directory during authorization.

Requirements:

- Active Directory user account with WMI remote access privileges
- Windows firewall must allow inbound access to WMI from ClearPass

WMI Configuration: ClearPass

Inside ClearPass, map the WMI credentials to the edge subnets under **`Configuration » Profile Settings » WMI Configuration`**.

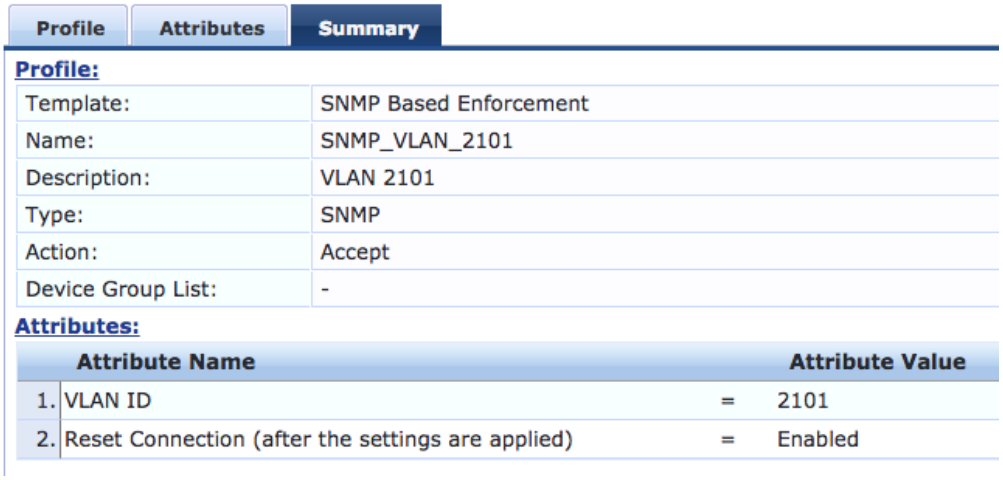


ClearPass: Enforcement Profiles

Enforcement profiles for OnConnect are very basic.

For each enforcement VLAN, create a new SNMP Based Enforcement profile. Navigate to **`Configuration » Enforcement » Profiles » Add Enforcement Profile`**. Select **`SNMP Based Enforcement`** from the template dropdown.

Add the **`VLAN ID`** and **`Reset Connection`** attributes. You can also optionally add the **`Session Timeout`** attribute to trigger a re-evaluation of policy after a certain amount of time.



Profile | Attributes | Summary

Profile:

Template:	SNMP Based Enforcement
Name:	SNMP_VLAN_2101
Description:	VLAN 2101
Type:	SNMP
Action:	Accept
Device Group List:	-

Attributes:

	Attribute Name		Attribute Value
1.	VLAN ID	=	2101
2.	Reset Connection (after the settings are applied)	=	Enabled

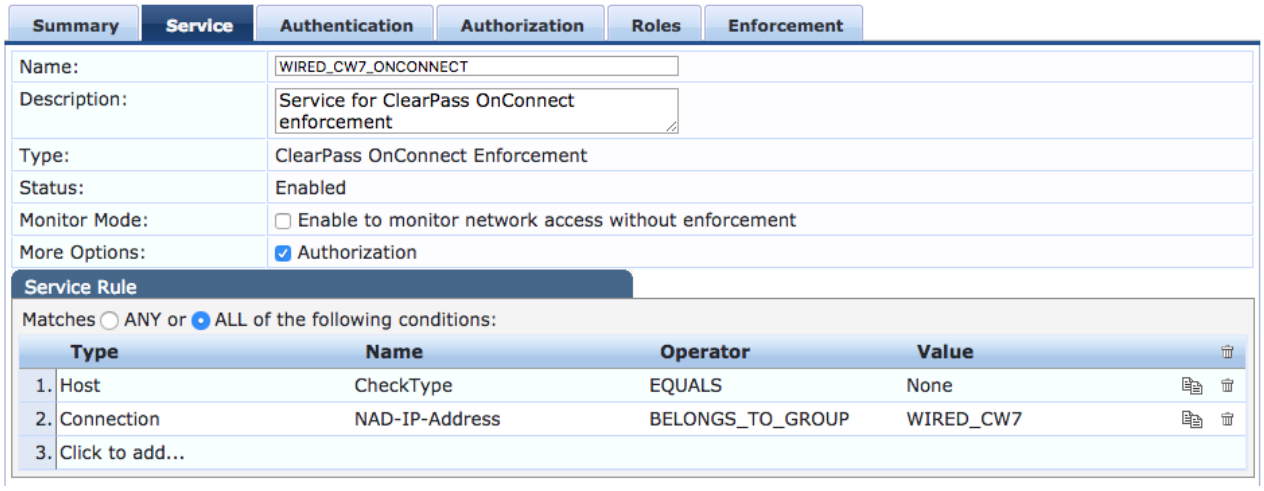
ClearPass: OnConnect Service

Service Configuration

Start with a new service of type **`ClearPass OnConnect Enforcement`**.

Under More Options, check the **`Authorization`**. This will enable the Authorization tab. The default service rules will work with a Comware 7 switch.

If there is a need to restrict the service to a particular set of switches, you can use a **`Connection`** | **`NAD-IP-Address`** | **`BELONGS_TO_GROUP`** service rule to reference a NAD group as seen in rule 2 below.



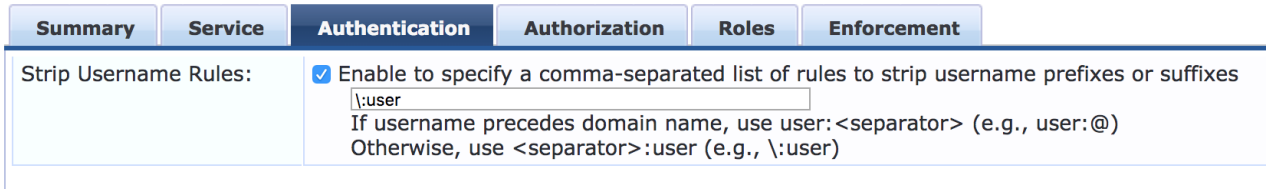
Authentication

Since OnConnect does not do any traditional user or device authentication, the only option available on the Authentication tab is the Strip Username Rules configuration.

If you are not planning to use WMI, nothing has to be configured on the Authentication tab.

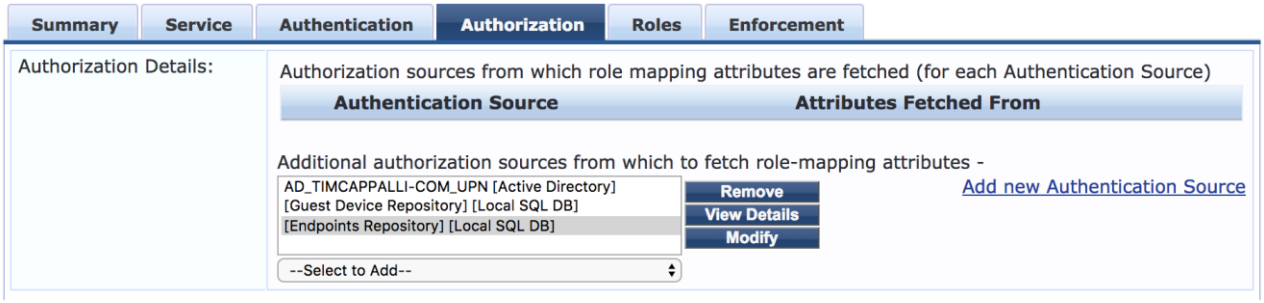
If you are planning to use WMI to grab the currently logged in user, the Strip Username Rules will need to be configured. WMI returns the username in down-level logon format (REALM\username) so the REALM will need to be stripped off before an authorization check can be done against Active Directory.

Use the **`\:user`** rule to strip the REALM from the down-level logon username.



Authorization

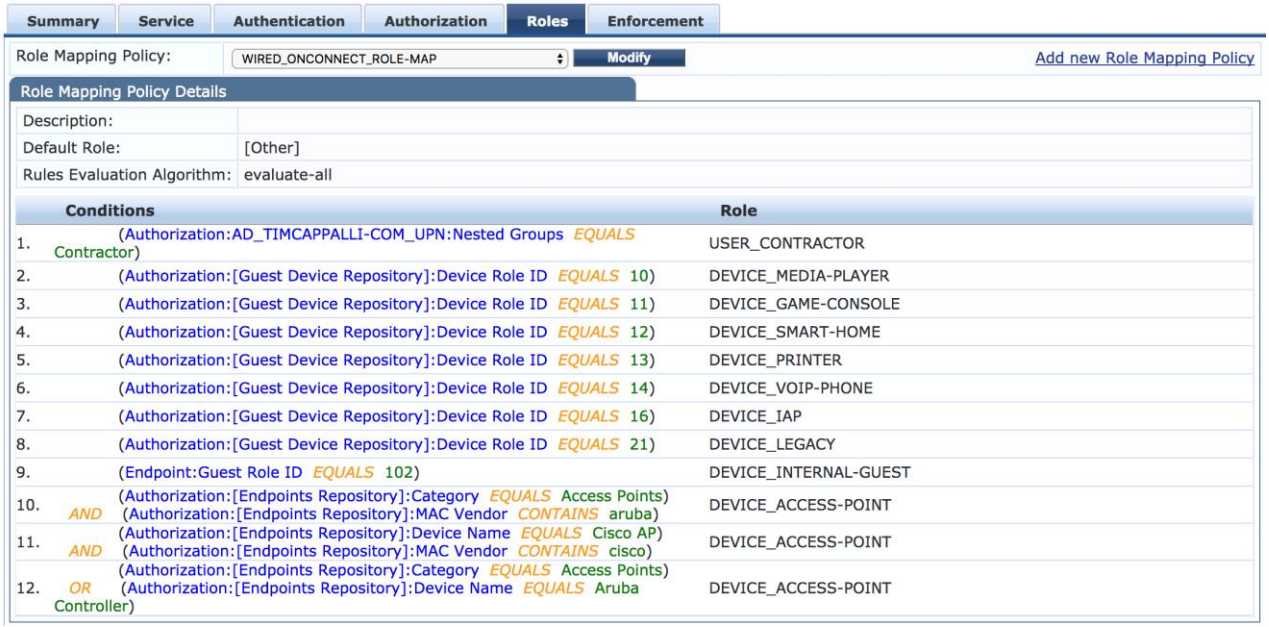
On the Authorization tab, add the **[Endpoints Repository]** and **[Guest Device Repository]** to the "Additional authorization sources…" list as shown below. If WMI-based authorization will be used, also add your Active Directory authentication source to the list so user properties can be evaluated.



Roles

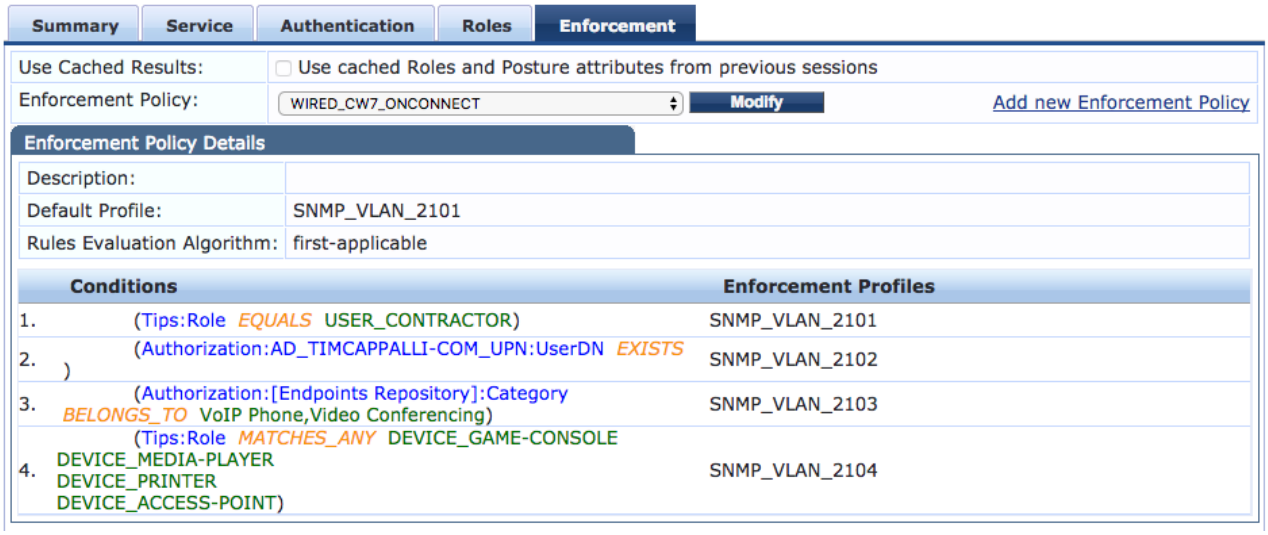
Role mapping is used to tag devices and users with as much information as possible for use in a policy decision.

This *example* role map covers both headless devices and user mapping based off AD group membership. Headless devices are mapped using a mix of device registrations and raw profile data.



Enforcement

For the default policy, the default guest VLAN profile is specified. This is used when a request falls through the policy with no match. Let's take apart the enforcement policy, rule by rule.



1 (Tips:Role *EQUALS* USER_CONTRACTOR) SNMP_VLAN_2101

If the logged in user is a member of the "Contractor" AD group, the `USER_CONTRACTOR` tag/TIPS Role is mapped. This device is then given the GUEST VLAN, 2101 in this example.

2 (Authorization:AD_TIMCAPPALLI-COM_UPN:UserDN *EXISTS*) SNMP_VLAN_2102

This rule just checks that the logged in user is a domain user. All domain users will have a **`UserDN`** attribute. These devices will be placed into the "SECURE" VLAN, 2102 in this case.

3 (Authorization:[Endpoints Repository]:Category *BELONGS_TO* VoIP Phone,Video Conferencing) SNMP_VLAN_2103

Profile data is being leveraged in rule 3 to drop voice devices into VLAN 2103, for voice.

4 (Tips:Role *MATCHES_ANY* DEVICE_GAME-CONSOLE DEVICE_MEDIA-PLAYER DEVICE_PRINTER DEVICE_ACCESS-POINT) SNMP_VLAN_2104

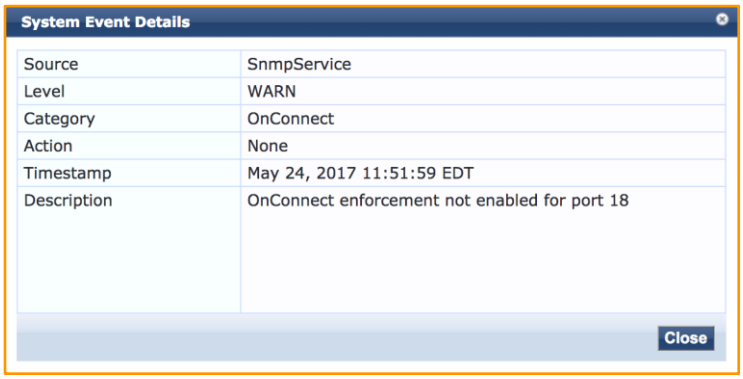
These tags/TIPS roles are mapped based on the role assigned during Device Registration. These registered devices will be dropped into the "HEADLESS" VLAN, 2104 in this case.

Useful Troubleshooting Commands and Tips

ClearPass

If OnConnect requests are not appearing in Access Tracker, take a look in Event Viewer. Below are some common error messages.

- Traps are being sent by the switch, but the network device definition in ClearPass does not have the port listed for OnConnect enforcement.



- The SNMP trap community is mismatched

Switch

display snmp-agent trap-list

This command will give you a summary of the switch's SNMP trap configuration.

```
[CW-5130EI] dis snmp-agent trap-list
   arp notification is disabled.
   configuration notification is enabled.
   mac-address notification is enabled.
   radius notification is disabled.
   standard notification is enabled.
   stp notification is disabled.
   system notification is enabled.

   Enabled notifications: 4; Disabled notifications: 3
```

debugging snmp agent packet receive
debugging snmp trap packet

Debug commands can be used for more advanced troubleshooting and to verify that the switch is sending traps to ClearPass. Sample debug output is shown below.

Link change trap

```
%Feb  5 14:53:26:598 2018 CW-5130EI IFNET/5/LINK_UPDOWN: Line protocol on the interface
GigabitEthernet1/0/2 is down.
*Feb  5 14:53:26:602 2018 CW-5130EI SNMP/7/TRAP_PACKET:
   linkDown trap<v2> send to: 100.65.30.52
   Request ID: 1954667472
   Error status: 0
   Error index: 0
   UDP port: 162
   Trap successfully sent*Feb  5 14:53:26:603 2018 CW-5130EI SNMP/7/VBLIST:
   snmpTrapOID.0: 1.3.6.1.6.3.1.1.5.3
*Feb  5 14:53:26:603 2018 CW-5130EI SNMP/7/VBLIST:
   ifIndex.2: 2
*Feb  5 14:53:26:603 2018 CW-5130EI SNMP/7/VBLIST:
   ifAdminStatus.2: 2
*Feb  5 14:53:26:603 2018 CW-5130EI SNMP/7/VBLIST:
   ifOperStatus.2: 2
*Feb  5 14:53:26:603 2018 CW-5130EI SNMP/7/VBLIST:
   ifDescr.2: GigabitEthernet1/0/2
```

VLAN Enforcement and reset

```
*Feb  5 15:08:21:327 2018 CW-5130EI SNMP/7/PACKET:
   Set request
   Request ID: 1950334484
   Error status: 0
   Error index: 0
*Feb  5 15:08:21:327 2018 CW-5130EI SNMP/7/VBLIST:
   ifAdminStatus.1: 1
```

Cisco Catalyst (IOS) Enforcement

RADIUS-based Enforcement

Policy Enforcement

Access Control Lists (ACLs)

Cisco Catalyst switches can leverage two types of ACLs as part of policy enforcement.

Traditional ACLs are defined locally on the switch and can be returned as part of a RADIUS response or added directly to a switch port or VLAN interface.

Downloadable ACLs (dACLs) are defined centrally on the RADIUS server. When a client authenticates in this scenario, a dACL name is returned back to the switch. The switch then sends a second RADIUS request to pull down the contents of the dACL.

RADIUS	2c41387fc880	2c41387fc880	WIRED_CISCO_MAC-AUTH	ACCEPT	VLAN_EDGE--GUEST-300S, DACL_CISCO_DHCP-DNS	< Initial auth
RADIUS	#ACSACL#-IP-DACL_CISCO_DHCP_DNS-3001-2		Cisco Downloadable ACL	ACCEPT	DACL_CISCO_DHCP-DNS	< dACL request

VLAN Enforcement

A VLAN in Cisco IOS can be referenced by VLAN-ID or VLAN name. Although it is an optional configuration, VLAN name is highly recommended in a colorless port deployment as it removes the need for ClearPass to maintain a VLAN to function mapping for each switch. This simplifies policy creation, management and troubleshooting.

For example, each switch might use a different VLAN-ID for “secure access”. Instead of having to write complex policy in ClearPass to return the correct VLAN-ID for each switch, we just give the appropriate VLAN-ID a name on each switch; “SECURE” for example. Now in your ClearPass policy, you simply return a VLAN enforcement with “SECURE” as the VLAN-ID and each switch will use the appropriate VLAN-ID mapped locally on the switch.

Dynamic Authorization

Cisco Catalyst switches support the following dynamic authorization commands:

- **Terminate Session**: traditional disconnect message; reinitializes authenticator state
- **Bounce Host Port**: bounces the port by disabling and re-enabling the port
- **Disable Host Port:** administratively disables the port
- **Reauthenticate Host:** initiates a re-authentication event

ClearPass includes all 4 of these dynamic authorization enforcement profiles in Policy Manager.

NOTE: The switch can be configured to ignore Bounce Host Port and Disable Host Port commands using the following commands:

```
authentication command bounce-port ignore
authentication command disable-port ignore
```

Configuration Overview

Here are the hardware and software combinations used for this configuration:

- Cisco Catalyst 2960 switch running Cisco IOS 15.0(2)SE10a with LAN base image
- ClearPass Policy Manager 6.6.4 (there are no ClearPass version dependencies for this configuration)

This section covers Cisco's Identity Based Networking Services (IBNS) **version 1** configuration model. A future update to this document will add IBNS 2.

NOTE: IBNS 2 requires Catalyst 3850 or 3650 running IOS 15.2(1)E+ or IOS-XE 03.05.00E+, Catalyst C6500 running IOS 15.2(1)SY+, or Sup8E running IOS-XE 03.06.00E+

Quirks and Limitations

On older Cisco Catalyst switches, each port can have only one VLAN assignment except in the case of a client device connected behind a VoIP device (in that scenario, the VoIP device is tagged and the device behind it is untagged).

These limitations were removed for the following switches and versions and VLANs can be assigned by authentication session:

- Catalyst 2960X, IOS 15.2(2)E
- Catalyst 3850, IOS-XE 03.03.00SE
- Catalyst 3650, IOS-XE 03.03.00SE

Switch Configuration

The configuration snippets below assume that components like VLANs, uplinks, NTP and other basics have already been configured. Note that NTP is required as accurate time plays a critical role in network authentication.

Define the ClearPass server(s) as RADIUS server(s) and dynamic authorization client(s):

```
radius server CLEARPASS-PROD
 address ipv4 10.65.30.42 auth-port 1812 acct-port 1813
 key L0ng&Compl5x$ecret!
!
aaa server radius dynamic-author
 client 10.65.30.42 server-key L0ng&Compl5x$ecret!
 port 3799
 auth-type all
!
```

Enable AAA functions:

`aaa new-model` `aaa session-id common`	
`ip device tracking`	tracks client IPs (required for dACLs)

`aaa authentication dot1x default group radius`
`aaa authorization network default group radius`
`aaa accounting dot1x default start-stop group radius`
	enable each of the AAA functions and map server group

`dot1x system-auth-control`	globally enable port-based access control
`radius-server vsa send accounting` `radius-server vsa send authentication`	send Cisco VSA in authentication and accounting messages
`radius-server attribute 11 default direction in`	accept IETF 'filter-id' to assign ACLs

Define access control entries:

`ip access-list extended CLEARPASS-REDIRECT`
` deny ip any host 10.65.30.42`
` permit tcp any any eq www`
` permit tcp any any eq 443`
	ACL used to control traffic redirection to captive portal

`ip access-list extended default_port_acl` ` permit icmp any any`	default port ACL

permit udp any eq bootpc any eq bootps permit udp any any eq domain permit tcp any host 10.65.30.42 eq www permit tcp any host 10.65.30.42 eq 443 permit tcp any host 10.65.30.42 eq 6658 deny ip any any	
ip access-list extended ALLOWALL permit ip any any	allow all ACL used after successful authN/authZ

Configure end-user ports:

interface FastEthernet0/1 description COLORLESS-PORT	
switchport access vlan 111 switchport mode access	assign a dead-end VLAN as default (optional security recommendation)
switchport voice vlan 813	set the voice VLAN if using VoIP devices
ip access-group default_port_acl in	default ACL applied to the port
authentication host-mode multi-domain	support both voice and data device on same port
authentication order dot1x mab	set the authentication sequence
authentication priority dot1x mab	set the priority for auth methods
authentication port-control auto	enable authentication on port
authentication timer reauthenticate server	accept reauth-interval from ClearPass
mab	enable MAC Auth Bypass
dot1x pae authenticator	set the port as an authenticator
dot1x timeout tx-period 10	EAP Request-Identity waiting period
dot1x timeout supp-timeout 15	supplicant timeout period
dot1x max-reauth-req 1	number of additional times EAP Req-ID is sent

ClearPass: Basics

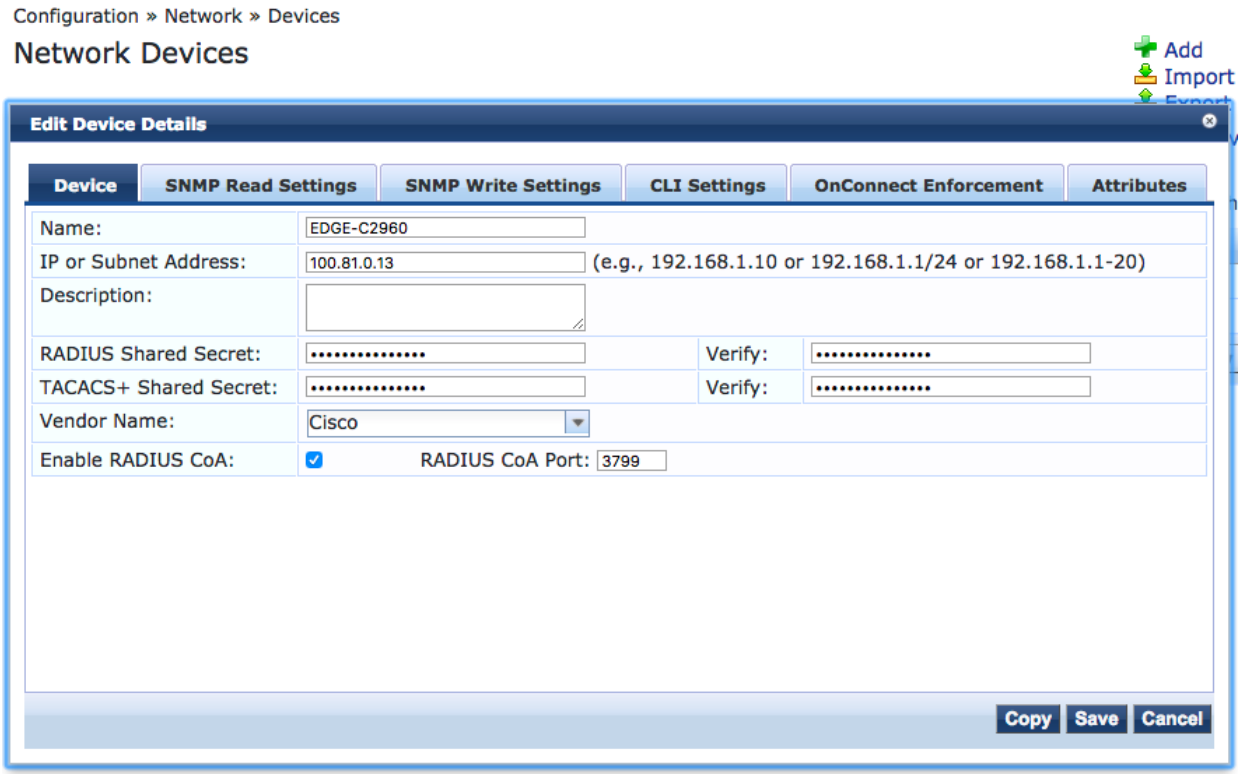
Define Switch(es)

In order for ClearPass to service RADIUS requests, switches need to be added to ClearPass as Network Devices.

They can be defined individually (security best practice) or they can be added by range or subnet. For example, in a layer 2 deployment, all switches may have a management address in the same subnet. If all switches share the same RADIUS (and TACACS+) shared secrets, the subnet can be defined instead of each switch individually. You can also define a smaller range.

To add network devices, navigate to **Configuration » Network » Devices** and click **Add**.

At a minimum, give the device (or subnet/range) a name, add the IP address, subnet with mask or range, define the RADIUS Shared Secret and select Cisco as the Vendor Name. CoA is automatically enabled.



ClearPass: MAC Authentication

Overview

The MAC Authentication service will handle headless devices like printers, phones, access points and others as well as provide the redirect URL for unknown devices to allow for a captive portal authentication. A mix of dACLs and filter-id-based enforcement will be used to show the different options.

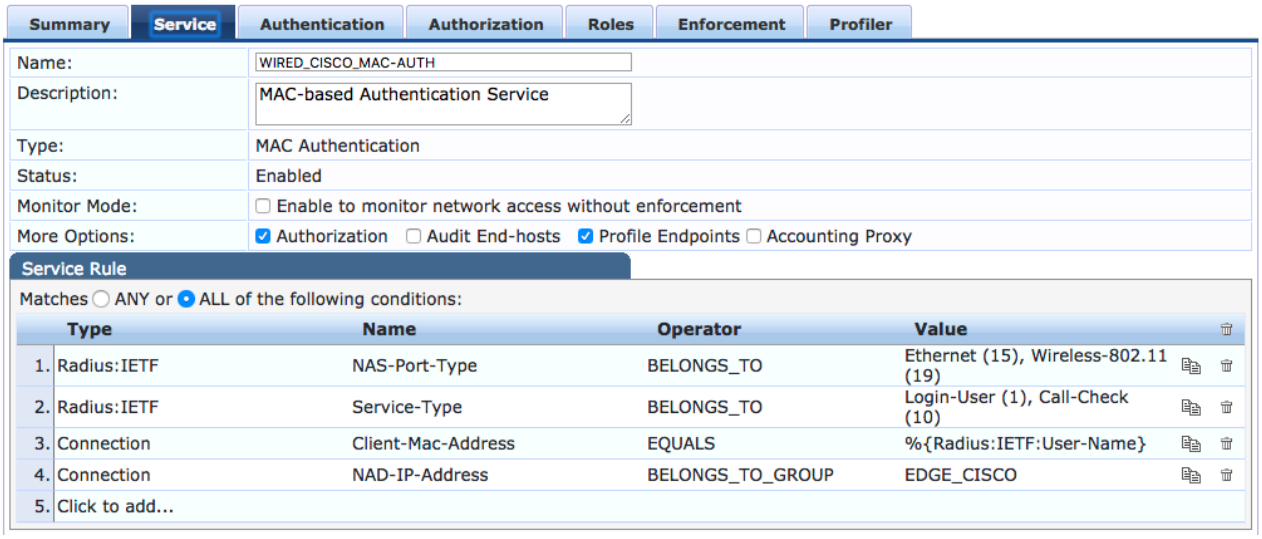
In this scenario, we're leveraging the Guest Device Repository and Device Registration Portal to allow end-users and IT staff to register headless and non-802.1X capable devices. These devices can be assigned a role and account lifetime. Device Registration Portal configuration will not be covered.

Service Configuration

Start with a new service of type **`MAC Authentication`**.

Under More Options, check the **`Authorization`** and **`Profile Endpoints`** boxes. This will enable two new tabs. The default service rules will work with a Cisco switch.

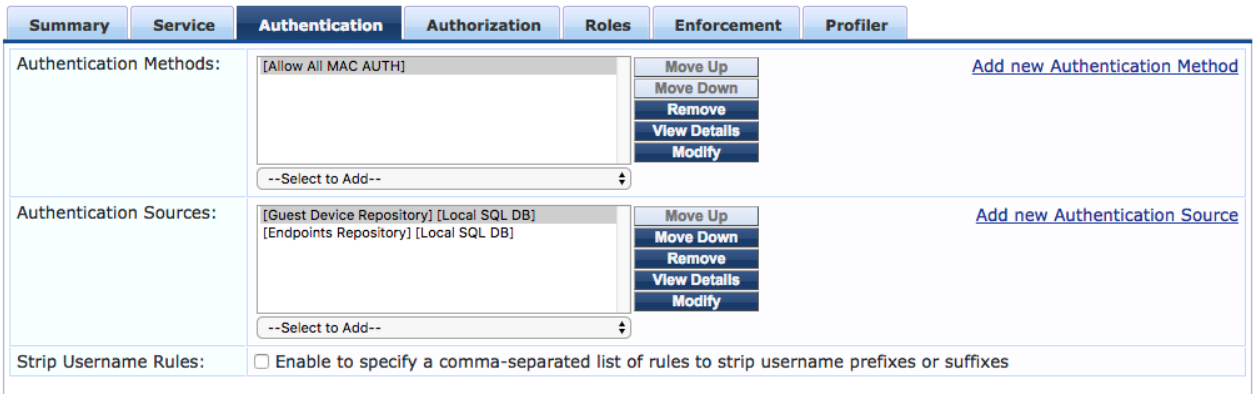
If there is a need to restrict the service to a particular group of switches, you can use a **`Connection`** | **`NAD-IP-Address`** | **`BELONGS_TO_GROUP`** rule to reference a NAD group as seen in rule 4 below.



Authentication

On the authentication tab, remove **[MAC Auth]** under Authentication Methods and add **[Allow All MAC Auth]**.

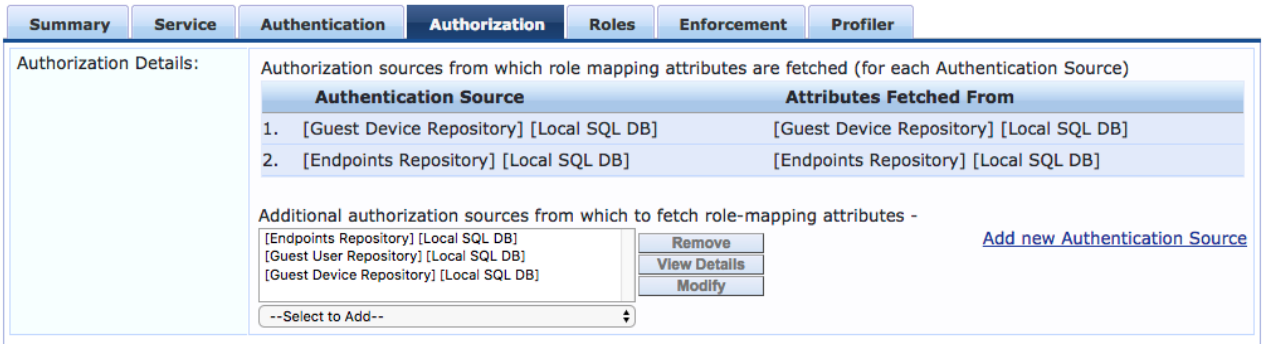
For Authentication Sources, you'll add **[Guest Device Repository] [Local SQL DB]** and move it above **[Endpoints Repository].**



Authorization

On the Authorization tab, add the **[Endpoints Repository], [Guest User Repository]** and **[Guest Device Repository]** to the "Additional authorization sources…" list as shown below.

By default, authorization data is only fetched from the authentication source where the user/device was found.



So, for example, let's say a guest user's device is re-authenticating to the network within their account expiration window, you'll find the MAC address in the [Endpoints Repository] with some data like guest role and expiration time but we also want to check with ClearPass Guest to make sure an administrator hasn't disabled the account.

Roles

Role mapping is used to tag devices and users with as much prevalent information as possible for use in a policy decision.

This role map is an example of a typical MAC Authentication:

Summary | Service | Authentication | Authorization | Roles | Enforcement | Profiler

Role Mapping Policy: WIRED_MAC-AUTH_ROLE-MAP Modify

Role Mapping Policy Details

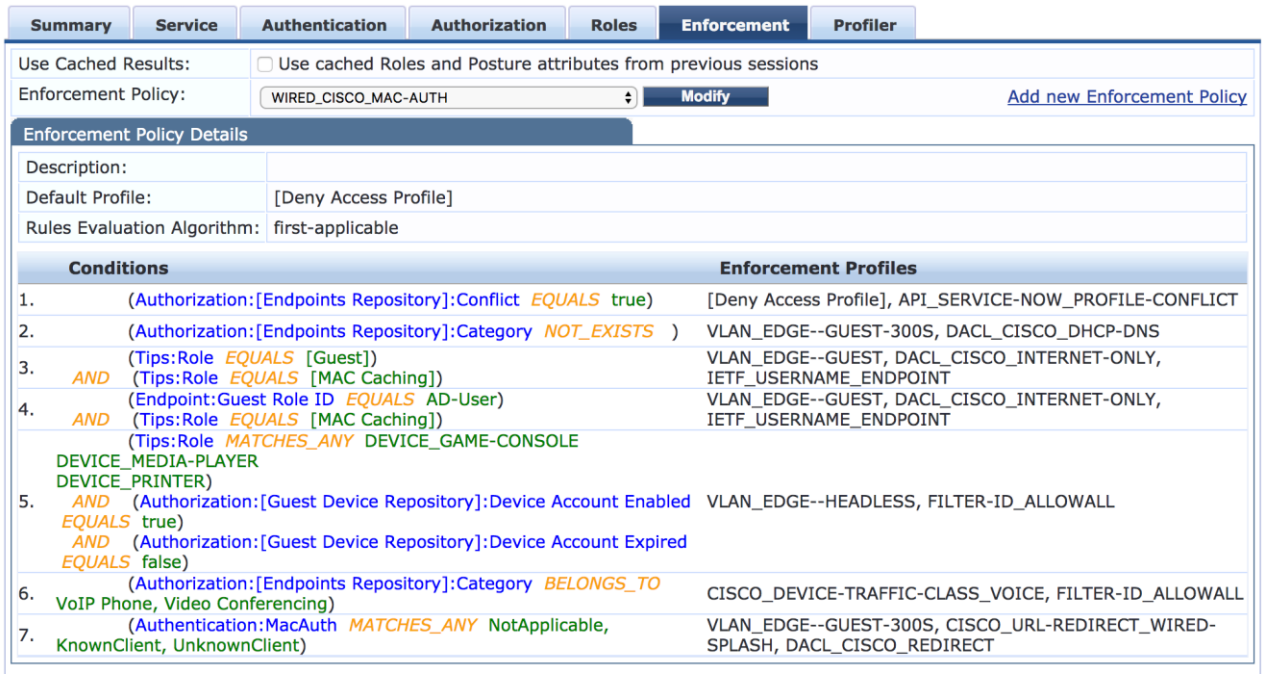
Description:	
Default Role:	[Other]
Rules Evaluation Algorithm:	evaluate-all

	Conditions	Role
1.	(Date:Date-Time *LESS_THAN* %{Endpoint:MAC-Auth Expiry}) *AND* (Authorization:[Guest User Repository]:AccountExpired *EQUALS* false) *AND* (Authorization:[Guest User Repository]:AccountEnabled *EQUALS* true)	[MAC Caching]
2.	(Date:Date-Time *LESS_THAN* %{Endpoint:MAC-Auth Expiry}) *AND* (Endpoint:Guest Role ID *EQUALS* AD-User)	[MAC Caching]
3.	(Endpoint:Guest Role ID *EQUALS* 1)	[Contractor]
4.	(Endpoint:Guest Role ID *EQUALS* 2)	[Guest]
5.	(Authorization:[Guest Device Repository]:Device Role ID *EQUALS* 10)	DEVICE_MEDIA-PLAYER
6.	(Authorization:[Guest Device Repository]:Device Role ID *EQUALS* 11)	DEVICE_GAME-CONSOLE
7.	(Authorization:[Guest Device Repository]:Device Role ID *EQUALS* 12)	DEVICE_SMART-HOME
8.	(Authorization:[Guest Device Repository]:Device Role ID *EQUALS* 13)	DEVICE_PRINTER
9.	(Authorization:[Guest Device Repository]:Device Role ID *EQUALS* 14)	DEVICE_VOIP-PHONE
10.	(Authorization:[Guest Device Repository]:Device Role ID *EQUALS* 16)	DEVICE_IAP
11.	(Authorization:[Guest Device Repository]:Device Role ID *EQUALS* 21)	DEVICE_LEGACY
12.	(Endpoint:Guest Role ID *EQUALS* 102)	DEVICE_INTERNAL-GUEST
13.	(Authorization:[Endpoints Repository]:Category *EQUALS* Access Points) *AND* (Authorization:[Endpoints Repository]:MAC Vendor *CONTAINS* aruba)	DEVICE_ACCESS-POINT
14.	(Authorization:[Endpoints Repository]:Device Name *EQUALS* Cisco AP) *AND* (Authorization:[Endpoints Repository]:MAC Vendor *CONTAINS* cisco)	DEVICE_ACCESS-POINT
15.	(Authorization:[Endpoints Repository]:Category *EQUALS* Access Points)	DEVICE_ACCESS-POINT

- Conditions 1 and 2 are checking to see that a guest user account is still valid and returning the [MAC Caching] tag / TIPS role
- Conditions 3-12 map user and device role IDs to tags / TIPS roles for use in policy
- Conditions 13-15 map profiling data to a tag / TIPS role for use in policy

Enforcement

Let's take apart this enforcement policy rule by rule:



Summary | Service | Authentication | Authorization | Roles | Enforcement | Profiler

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

Enforcement Policy: WIRED_CISCO_MAC-AUTH [Modify] Add new Enforcement Policy

Enforcement Policy Details

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

	Conditions	Enforcement Profiles
1.	(Authorization:[Endpoints Repository]:Conflict *EQUALS* true)	[Deny Access Profile], API_SERVICE-NOW_PROFILE-CONFLICT
2.	(Authorization:[Endpoints Repository]:Category *NOT_EXISTS*)	VLAN_EDGE--GUEST-300S, DACL_CISCO_DHCP-DNS
3.	(Tips:Role *EQUALS* [Guest]) *AND* (Tips:Role *EQUALS* [MAC Caching])	VLAN_EDGE--GUEST, DACL_CISCO_INTERNET-ONLY, IETF_USERNAME_ENDPOINT
4.	(Endpoint:Guest Role ID *EQUALS* AD-User) *AND* (Tips:Role *EQUALS* [MAC Caching])	VLAN_EDGE--GUEST, DACL_CISCO_INTERNET-ONLY, IETF_USERNAME_ENDPOINT
5.	(Tips:Role *MATCHES_ANY* DEVICE_GAME-CONSOLE DEVICE_MEDIA-PLAYER DEVICE_PRINTER) *AND* (Authorization:[Guest Device Repository]:Device Account Enabled *EQUALS* true) *AND* (Authorization:[Guest Device Repository]:Device Account Expired *EQUALS* false)	VLAN_EDGE--HEADLESS, FILTER-ID_ALLOWALL
6.	(Authorization:[Endpoints Repository]:Category *BELONGS_TO* VoIP Phone, Video Conferencing)	CISCO_DEVICE-TRAFFIC-CLASS_VOICE, FILTER-ID_ALLOWALL
7.	(Authentication:MacAuth *MATCHES_ANY* NotApplicable, KnownClient, UnknownClient)	VLAN_EDGE--GUEST-300S, CISCO_URL-REDIRECT_WIRED-SPLASH, DACL_CISCO_REDIRECT

1

(Authorization:[Endpoints Repository]:Conflict *EQUALS* true) [Deny Access Profile], API_SERVICE-NOW_PROFILE-CONFLICT

If a device's profiled category changes, ClearPass triggers the **`Conflict`** attribute.

If the **`Conflict`** attribute is `true`, deny access to the network and also initiate an API call over to ServiceNow to open a ticket.

Other options could include a captive portal redirect to notify the user, text message to the user, etc.

2

(Authorization:[Endpoints Repository]:Category *NOT_EXISTS*) VLAN_EDGE--GUEST-300S, DACL_CISCO_DHCP-DNS

This rule evaluates whether the profile Category exists for the authenticating endpoint.

If it does not exist, the device has not been profiled and a dACL and VLAN assignment are returned to the switch. The dACL allows both DHCP and DNS:

1.	Radius:Cisco	Cisco-IP-Downloadable-ACL	=	permit udp any any eq bootps permit udp any any eq domain

3

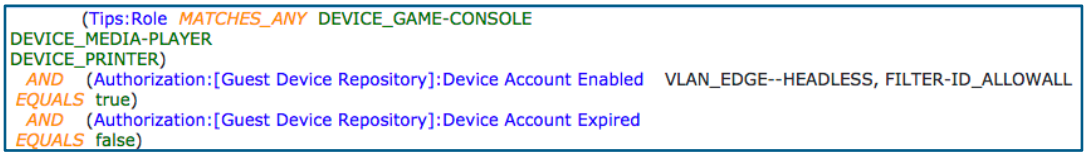
During role mapping, it was calculated that the device should still be MAC cached based on its expiration and the user's account status.

The **EDGE_GUEST** VLAN, internet-only dACL and the guest's username will be returned to the switch.

4

Like the previous rule, the **Guest Role ID** attribute is being checked for AD-User and the expiration time is being compared to the current time.

5



Many headless devices have been registered via the Device Registration portal. This rule evaluates whether the authenticating device was registered as a game console, media player or printer and that the device account is enabled and hasn't expired.

The **EDGE_HEADLESS** VLAN is being returned along with **Filter-ID = ALLOWALL** which references the local ACL on the switch of the same name.

6

Based on profiling data, we're authorizing devices categorized as VoIP Phone and Video Conferencing by sending back a `filter-id` and `device-traffic-class`.

This **device-traffic-class=voice** attribute/value pair tells the switch that this device should be treated as a voice device. Since the port's host-mode is configured for multi-domain, the switch will tag the voice VLAN configured on the port down to the voice device.

	Type	Name		Value
1.	Radius:Cisco	Cisco-AVPair	=	device-traffic-class=voice

```
EDGE-C2960#show authentication sessions interface fastEthernet 0/2
            Interface:  FastEthernet0/2
          MAC Address:  2c41.387f.c880
           IP Address:  100.81.3.10
            User-Name:  2c41387fc880
               Status:  Authz Success
               Domain:  VOICE
      Oper host mode:  multi-domain
```

7	(Authentication:MacAuth *MATCHES_ANY* NotApplicable, KnownClient, UnknownClient)	VLAN_EDGE--GUEST-300S, CISCO_URL-REDIRECT_WIRED-SPLASH, DACL_CISCO_REDIRECT

The last rule is effectively a “catch all” which handles unknown devices.

Enforcement action #1 uses the **`url-redirect-acl`** Cisco-AVPair to tell the switch to use the local **`CLEARPASS-REDIRECT`** **ACL** to control which traffic is redirected the captive portal.

Action #2 provides the redirect URL to the switch using the **`url-redirect`** Cisco-AVPair. Notice that we added a variable to dynamically appended the client MAC address to the URL. This is required for many guest workflows.

	Type	Name		Value
1.	Radius:Cisco	Cisco-AVPair	=	url-redirect-acl=CLEARPASS-REDIRECT
2.	Radius:Cisco	Cisco-AVPair	=	url-redirect=https://clearpass-demo.arubaboston.com/guest/wired_cisco_self-reg.php?mac=%{Connection:Client-Mac-Address-Colon}

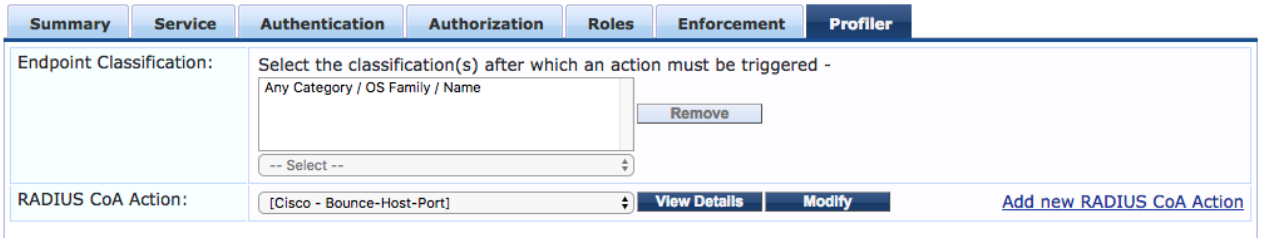
The second enforcement profile returns a dACL to control access during this captive portal pre-authentication state. We need to allow DNS and DHCP as well as HTTP and HTTPS traffic so that the switch will redirect all web traffic to ClearPass.

	Type	Name		Value
1.	Radius:Cisco	Cisco-IP-Downloadable-ACL	=	permit tcp any any eq www permit tcp any any eq 443 permit udp any any eq domain permit udp any any eq bootps deny ip any any

Profiler

The Profiler function allows for an unknown device to be automatically disconnected from the network once profile data has been collected and evaluated. This prevents a device from being "stuck" in a limited access role. During the second authentication, the new profile data can be used in the policy decision. This is a very common feature for MAC Authentication services.

In this case, we want to bounce the port for any type of new device because of rule 2 in the enforcement policy. Since this is a Cisco switch, the RADIUS CoA Action is **`[Cisco – Bounce-Host-Port]`**.



NOTE: Use caution in voice environments where client devices are connected behind a VoIP device. Bouncing a port after profiling a new device connected behind the VoIP device could result in interruption of voice service.

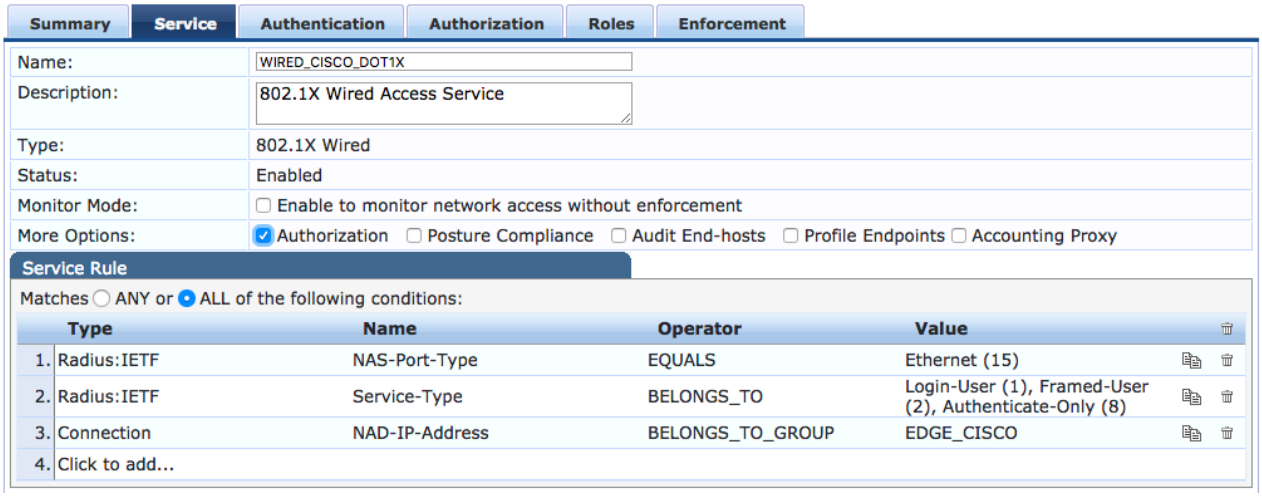
ClearPass: 802.1X

Service Configuration

Create a new service of type **`802.1X Wired`**.

Under More Options, check the **`Authorization`** boxes. The default service rules will work with a Cisco switch.

If there is a need to restrict the service to a particular group of switches, you can use a Connection | NAD-IP-Address | BELONGS_TO_GROUP rule to reference a NAD group as seen in rule 3 below.



Authentication

This service will be supporting both secure certificate-based authentication (EAP-TLS) and traditional, legacy username and password authentication (PEAPv0/EAP-MSCHAPv2).

The username and password based authentication will be used for two purposes:

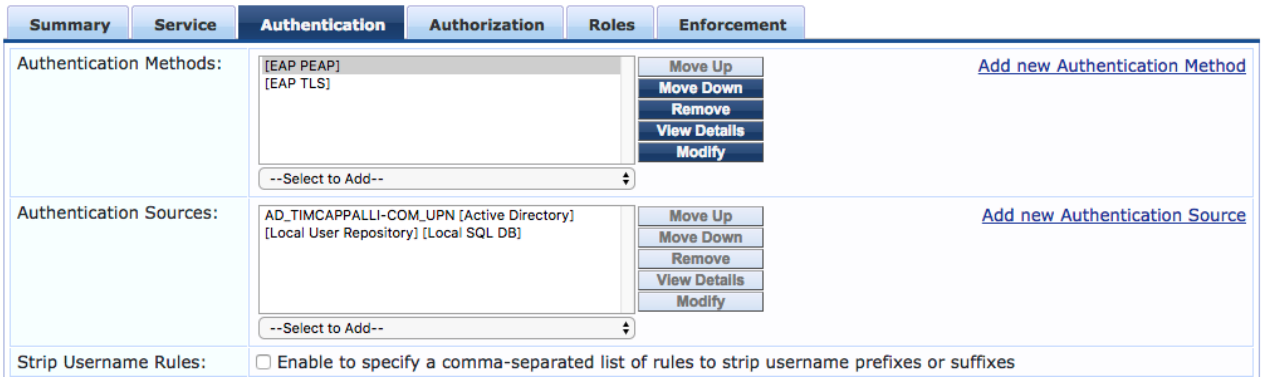
3) Allow a BYOD device to initially connect and kick off the Onboard process to issue them a certificate
4) Allow for domain-joined assets to use their computer/machine account to authenticate to the network as well as support machine + user workflows

Based on the above requirements, remove all the default EAP methods from the Authentication Methods list on the Authentication tab except for **`[EAP PEAP]`** and **`[EAP TLS]`.**

> **NOTE:** The default **`[EAP TLS]`** method does not have OCSP authorization configured. OCSP is used to check real-time validity of a certificate and enabling it is highly recommended. Special care should be taken when authenticating certificates from different certificate authorities. This is outside the scope of this document.

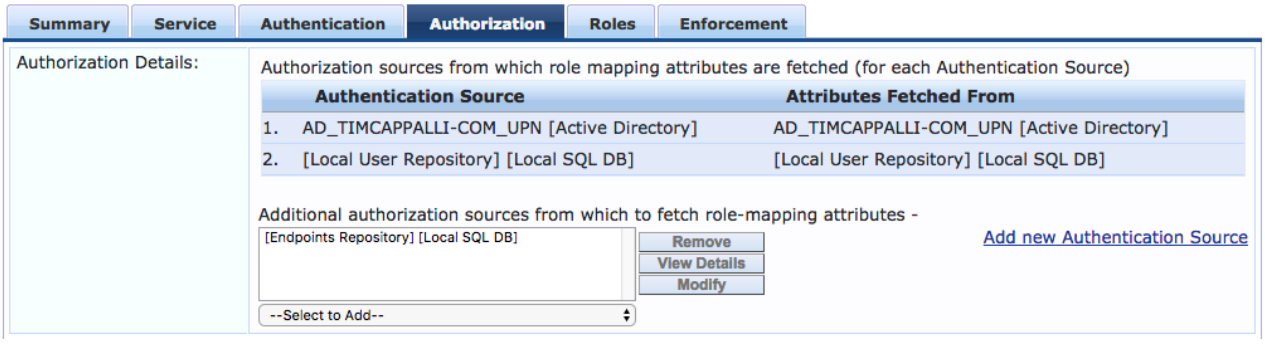
For Authentication Sources, you'll add our Active Directory identity store and also the **`[Local User Repository]`**. Authentication sources will vary in your environment.

The Local User Repository will be used in the example for infrastructure accounts like having an access point or VoIP phone authenticate securely to the network using the 802.1X framework.



Authorization

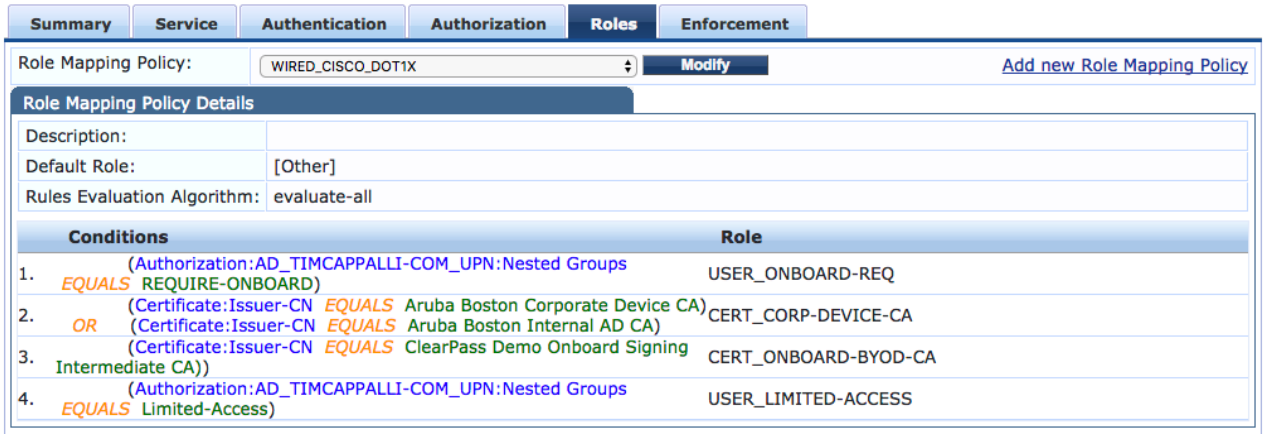
Since device profile information will be leveraged in policy, add the **`[Endpoints Repository]`** to the "Additional authorization sources…" list as shown below.



Roles

Role mapping is used to tag devices and users with as much prevalent information as possible for use in a policy decision.

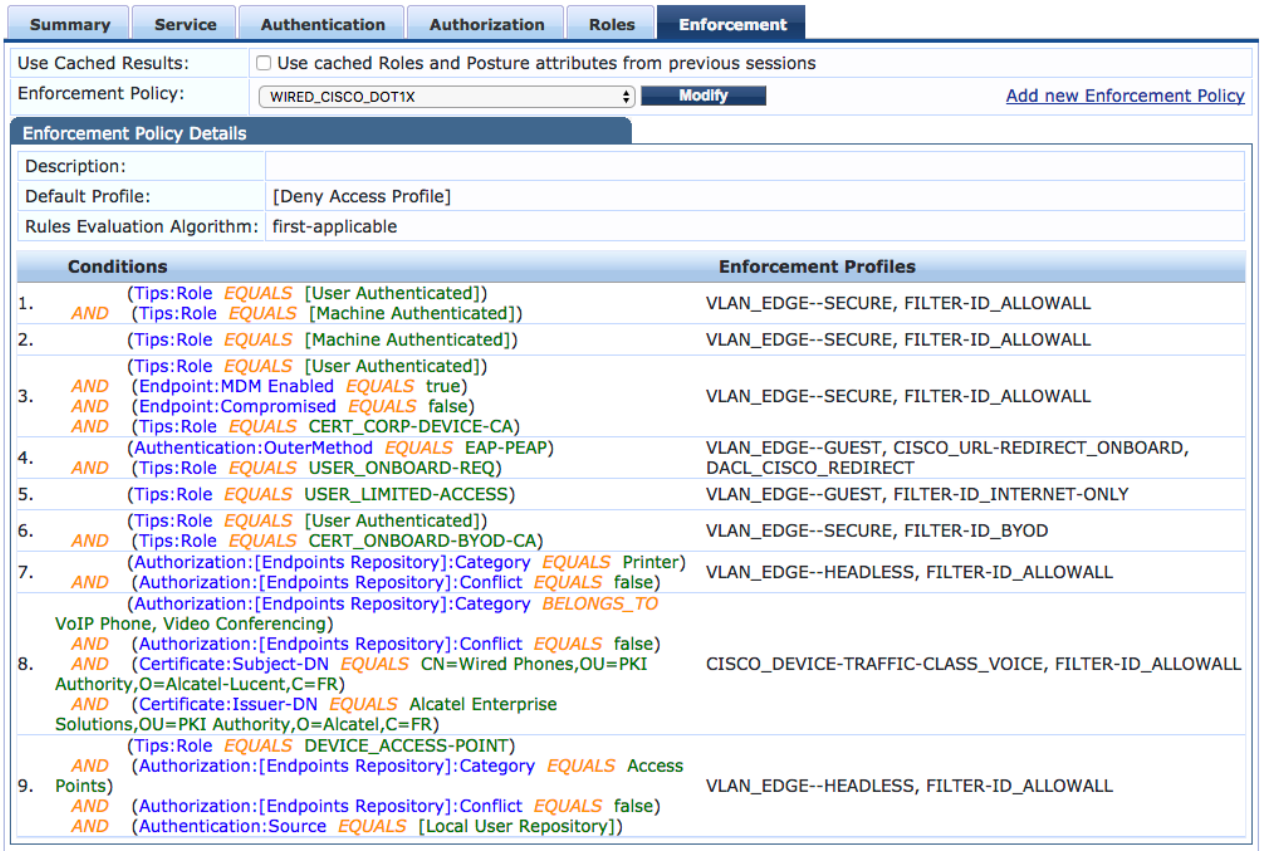
These rules and tags will vary greatly by environment, but below you'll find examples of device and user tagging.



- Rules 1 and 4 are checking group membership from Active Directory
- Rules 2-3 are matching on the common name of the issuing CA for the authenticating certificate

Enforcement

Let's take apart this enforcement policy rule by rule:



Summary | Service | Authentication | Authorization | Roles | Enforcement

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

Enforcement Policy: WIRED_CISCO_DOT1X [Modify] Add new Enforcement Policy

Enforcement Policy Details

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

	Conditions	Enforcement Profiles
1.	(Tips:Role EQUALS [User Authenticated]) AND (Tips:Role EQUALS [Machine Authenticated])	VLAN_EDGE--SECURE, FILTER-ID_ALLOWALL
2.	(Tips:Role EQUALS [Machine Authenticated])	VLAN_EDGE--SECURE, FILTER-ID_ALLOWALL
3.	(Tips:Role EQUALS [User Authenticated]) AND (Endpoint:MDM Enabled EQUALS true) AND (Endpoint:Compromised EQUALS false) AND (Tips:Role EQUALS CERT_CORP-DEVICE-CA)	VLAN_EDGE--SECURE, FILTER-ID_ALLOWALL
4.	(Authentication:OuterMethod EQUALS EAP-PEAP) AND (Tips:Role EQUALS USER_ONBOARD-REQ)	VLAN_EDGE--GUEST, CISCO_URL-REDIRECT_ONBOARD, DACL_CISCO_REDIRECT
5.	(Tips:Role EQUALS USER_LIMITED-ACCESS)	VLAN_EDGE--GUEST, FILTER-ID_INTERNET-ONLY
6.	(Tips:Role EQUALS [User Authenticated]) AND (Tips:Role EQUALS CERT_ONBOARD-BYOD-CA)	VLAN_EDGE--SECURE, FILTER-ID_BYOD
7.	(Authorization:[Endpoints Repository]:Category EQUALS Printer) AND (Authorization:[Endpoints Repository]:Conflict EQUALS false)	VLAN_EDGE--HEADLESS, FILTER-ID_ALLOWALL
8.	(Authorization:[Endpoints Repository]:Category BELONGS_TO VoIP Phone, Video Conferencing) AND (Authorization:[Endpoints Repository]:Conflict EQUALS false) AND (Certificate:Subject-DN EQUALS CN=Wired Phones,OU=PKI Authority,O=Alcatel-Lucent,C=FR) AND (Certificate:Issuer-DN EQUALS Alcatel Enterprise Solutions,OU=PKI Authority,O=Alcatel,C=FR)	CISCO_DEVICE-TRAFFIC-CLASS_VOICE, FILTER-ID_ALLOWALL
9.	(Tips:Role EQUALS DEVICE_ACCESS-POINT) AND (Authorization:[Endpoints Repository]:Category EQUALS Access Points) AND (Authorization:[Endpoints Repository]:Conflict EQUALS false) AND (Authentication:Source EQUALS [Local User Repository])	VLAN_EDGE--HEADLESS, FILTER-ID_ALLOWALL

1

	(Tips:Role EQUALS [User Authenticated])	
AND	(Tips:Role EQUALS [Machine Authenticated])	VLAN_EDGE--SECURE, FILTER-ID_ALLOWALL

When a Windows device authenticates to the network using its Active Directory computer account, the **[Machine Authenticated]** tag/TIPS role is added to the session automatically.

If both a machine and user authentication have occurred, then return the **EDGE_SECURE** VLAN and the **allowall** filter-ID.

This is commonly used to validate that the user is connecting from a corporate asset.

2

(Tips:Role EQUALS [Machine Authenticated])	VLAN_EDGE--SECURE, FILTER-ID_ALLOWALL

Rule 2 is for a machine-only authentication. These typically occur when the device is sitting at the Windows logon screen and connectivity is required for updates, remote access or for new users to login.

3

	(Tips:Role *EQUALS* [User Authenticated])	
AND	(Endpoint:MDM Enabled *EQUALS* true)	VLAN_EDGE--SECURE, FILTER-ID_ALLOWALL
AND	(Endpoint:Compromised *EQUALS* false)	
AND	(Tips:Role *EQUALS* CERT_CORP-DEVICE-CA)	

This is a typical rule to deal with a non-Windows corporate-managed asset that is managed by an EMM solution.

The two endpoint attributes have been synced down from the EMM solution. In this case, the rule is evaluating whether the device has its device management enabled and that no compromise has occurred.

The last condition checks for the tag/TIPS role from our role mapping to verify the certificate used to authenticate was issued from the Corporate Device CA.

4

	(Authentication:OuterMethod *EQUALS* EAP-PEAP)	VLAN_EDGE--GUEST, CISCO_URL-REDIRECT_ONBOARD,
AND	(Tips:Role *EQUALS* USER_ONBOARD-REQ)	DACL_CISCO_REDIRECT

Most personal devices will perform Onboarding through the captive portal workflow after 802.1X fails, but some users may authenticate via PEAPv0/EAP-MSCHAPv2 when prompted by their device.

This rule will catch those users who need to be using EAP-TLS authentication via ClearPass Onboard.

Enforcement action #1 returns the **`EDGE_GUEST`** VLAN name.

Enforcement action #2 uses the **`url-redirect-acl`** Cisco-AVPair to tell the switch to use the local **`CLEARPASS-REDIRECT`** ACL to control which traffic is redirected the captive portal.

Rule number 2 provides the redirect URL to the switch using the **`url-redirect`** Cisco-AVPair. Notice that we added a variable to dynamically appended the client MAC address to the URL.

	Type	Name		Value
1.	Radius:Cisco	Cisco-AVPair	=	url-redirect-acl=CLEARPASS-REDIRECT
2.	Radius:Cisco	Cisco-AVPair	=	url-redirect=https://clearpass-demo.net.arubaboston.com/onboard/wired_onboard_1.php?mac=%{Connection:Client-Mac-Address-Colon}

Enforcement action #3 returns a dACL to control access during this captive portal pre-authentication state. DNS and DHCP as well as HTTP and HTTPS traffic need to be allowed so that the switch will redirect all web traffic to ClearPass.

	Type	Name		Value
1.	Radius:Cisco	Cisco-IP-Downloadable-ACL	=	permit tcp any any eq www permit tcp any any eq 443 permit udp any any eq domain permit udp any any eq bootps deny ip any any

5

(Tips:Role *EQUALS* USER_LIMITED-ACCESS)	VLAN_EDGE--GUEST, FILTER-ID_INTERNET-ONLY

This is a basic rule as an example of a security exception for a group of users. These devices are dropped into the **`EDGE_GUEST`** VLAN with the **`INTERNET-ONLY`** ACL.

6

(Tips:Role *EQUALS* [User Authenticated]) *AND* (Tips:Role *EQUALS* CERT_ONBOARD-BYOD-CA)	VLAN_EDGE--SECURE, FILTER-ID_BYOD

After a device has been Onboarded, it will authenticate via EAP-TLS. Rule 6 uses the tag from the role mapping to check the common name of the issuing CA. These devices will be dropped into the **`EDGE_SECURE`** VLAN with the **`BYOD`** ACL.

7

(Authorization:[Endpoints Repository]:Category *EQUALS* Printer) *AND* (Authorization:[Endpoints Repository]:Conflict *EQUALS* false)	VLAN_EDGE--HEADLESS, FILTER-ID_ALLOWALL

This rule uses the device category of Printer combined with a check of the `Conflict` flag. The authentication method (username/password vs certificate) does not really matter in this case, however, an additional condition could easily be added similar to rules 8 and 9 below.

8

(Authorization:[Endpoints Repository]:Category *BELONGS_TO* VoIP Phone, Video Conferencing) *AND* (Authorization:[Endpoints Repository]:Conflict *EQUALS* false) *AND* (Certificate:Subject-DN *EQUALS* CN=Wired Phones,OU=PKI Authority,O=Alcatel-Lucent,C=FR) *AND* (Certificate:Issuer-DN *EQUALS* Alcatel Enterprise Solutions,OU=PKI Authority,O=Alcatel,C=FR)	CISCO_DEVICE-TRAFFIC-CLASS_VOICE, FILTER-ID_ALLOWALL

Many voice devices come from the factory with an embedded certificate that can be used for network authentication. The factory cert is being leveraged for EAP-TLS combined with profiling data. The **`device-traffic-class=voice`** Cisco-AVPair and **`allowall`** filter-id are being passed back.

This **`device-traffic-class=voice`** attribute/value pair tells the switch that this device should be treated as a voice device. Since the port's host-mode is configured for multi-domain, the switch will tag the voice VLAN configured on the port down to the voice device.

	Type	Name		Value
1.	Radius:Cisco	Cisco-AVPair	=	device-traffic-class=voice

9

(Tips:Role *EQUALS* DEVICE_ACCESS-POINT) *AND* (Authorization:[Endpoints Repository]:Category *EQUALS* Access Points) *AND* (Authorization:[Endpoints Repository]:Conflict *EQUALS* false) *AND* (Authentication:Source *EQUALS* [Local User Repository])	VLAN_EDGE--HEADLESS, FILTER-ID_ALLOWALL

As discussed during the authentication section, a local user account was created in ClearPass for use by access points to authenticate. Rule 9 is comparing the tag/TIPS role, category, conflict status and verifying the authentication source was the **`[Local User Repository]`**

ClearPass: Web Authentication

The Web Authentication service handles captive portal-based authentications with server-initiated workflows.

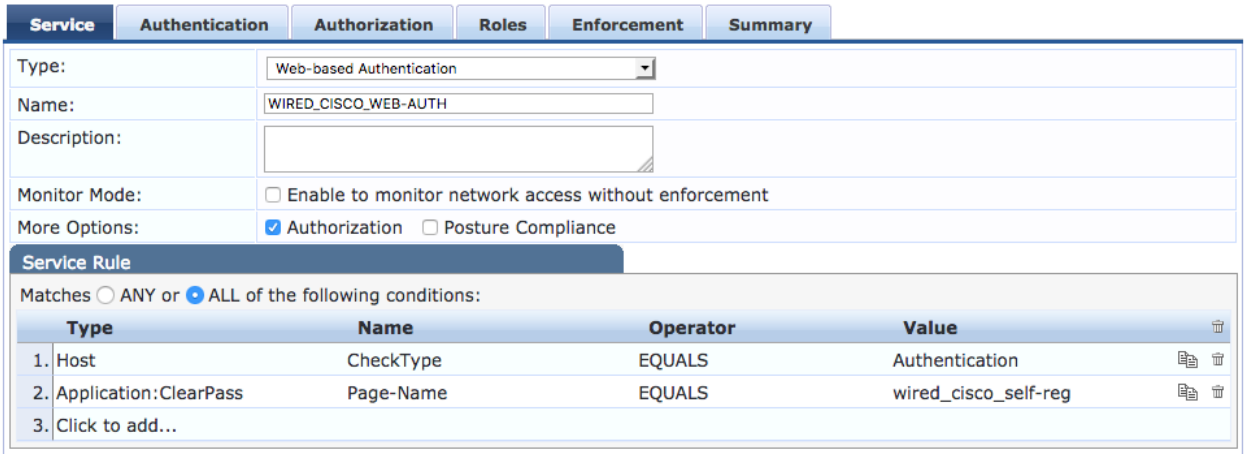
Service Configuration

Create a new service of type **`Web-based Authentication`**.

Check the **`Authorization`** box and select **`Matches ALL`** under Service Rule.

Add a second service rule with **`Application:ClearPass`** | **`Page-Name`** | **`EQUALS`** and then the page name.

For example: if the full page URL is `https://<fqdn>/guest/wired_cisco_self-reg.php`, then the page name is: `wired_cisco_self-reg`.

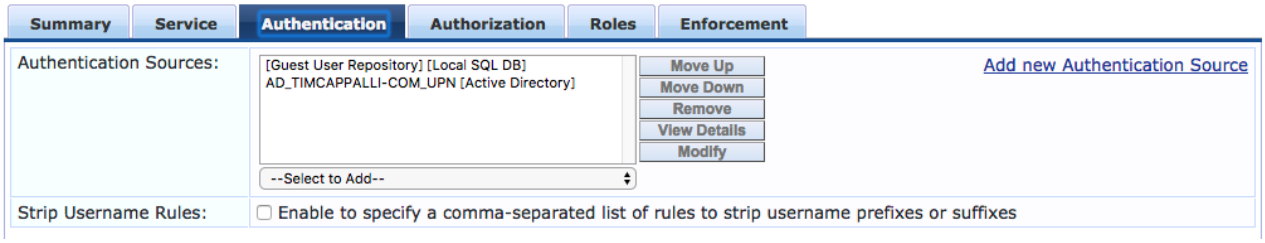


NOTE: The Page-Name attribute was added in ClearPass 6.7.0. Skip if using ClearPass 6.6.X.

Authentication

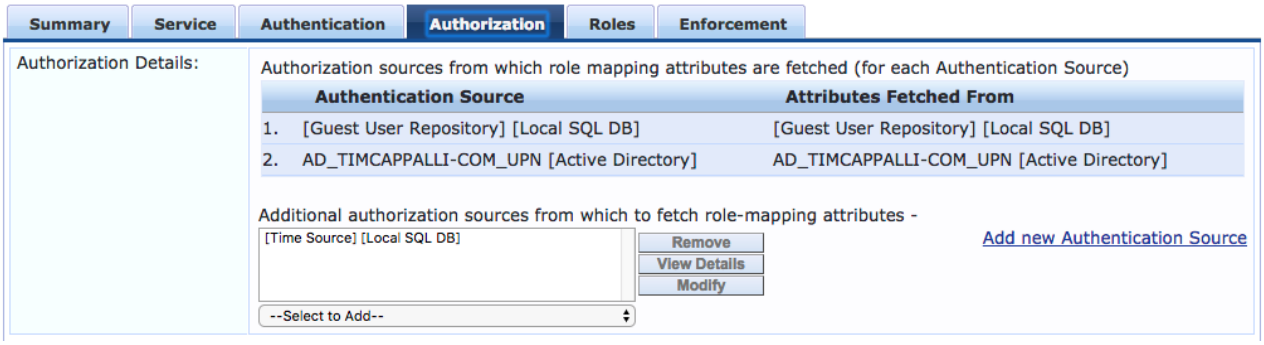
This service will be supporting both guest and Active Directory users for captive portal login.

For Authentication Sources, you'll add the **`[Guest User Repository]`** and also our Active Directory identity store. Authentication sources will vary in your environment.



Authorization

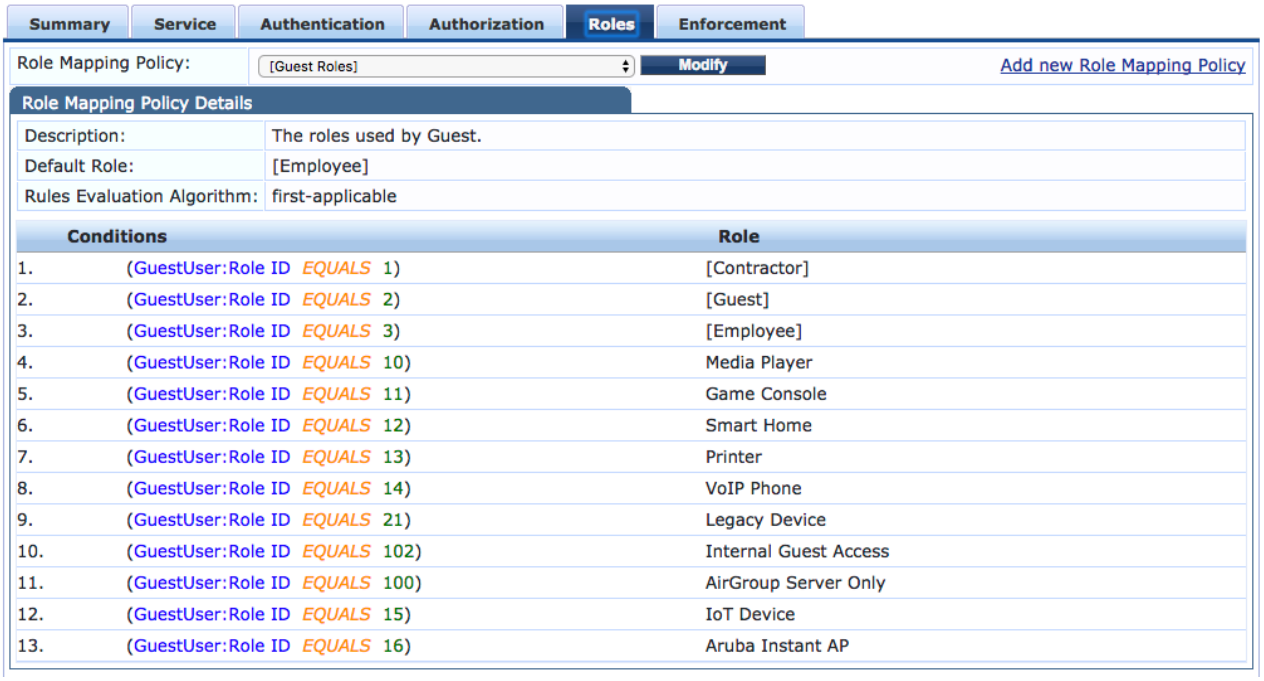
We will need to assign a manual expiration time to AD users. This time is calculated by the `[Time Source]` so it will need to be added as an additional authorization source.



Roles

In this scenario, guests and contractors will go through a standard self-registration process and any employee who authenticates with their corporate credentials will get a temporary guest role. Since there is no specific mapping of AD group, you'll use the **`[Guest Roles]`** role map.

If different enforcement actions will be taken for different groups or classifications of users, create a new role map like the in 802.1X configuration.



Enforcement

Because the server-initiated workflow is used with Cisco switching, the enforcement policy for the WEBAUTH service is very simple. The goal is to update the device endpoint record with attributes from the user authentication that will be stored and used for subsequent authentications and then bounce the port to trigger a reauthentication event. Note that if a VLAN change is not required, a re-authenticate session CoA can be used instead.

In this example, we're authenticating both guest and Active Directory accounts.

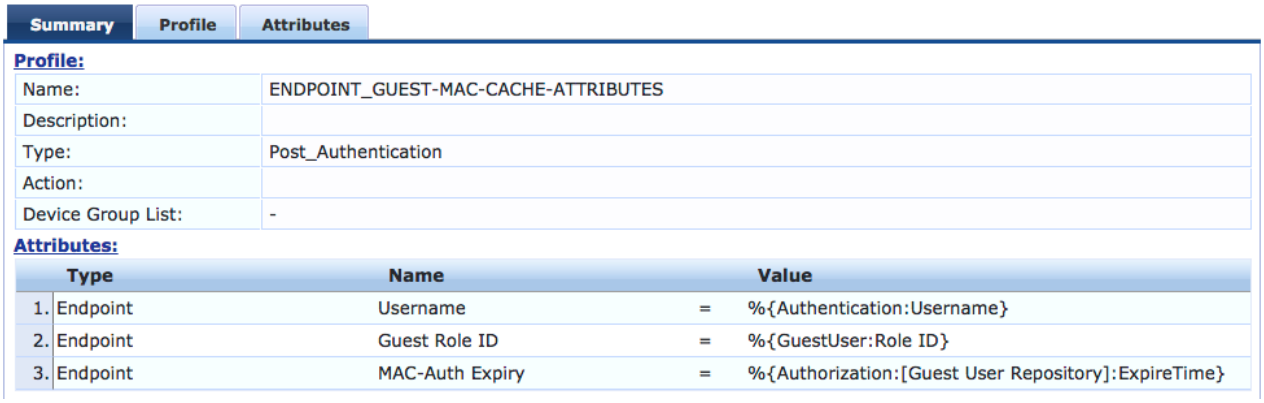
For the guest accounts, we need to set up a basic enforcement profile for MAC caching the user so when they re-authenticate after the port bounce, the user will not be prompted to authenticate again until their account expires.

Create a new enforcement profile for the guest users (**`Configuration » Enforcement » Profiles » Add Enforcement Profile`**).

- Select `ClearPass Entity Update Enforcement` from the Template dropdown
- Give the profile a name
- On the attributes tab, add the 3 entries below and then save

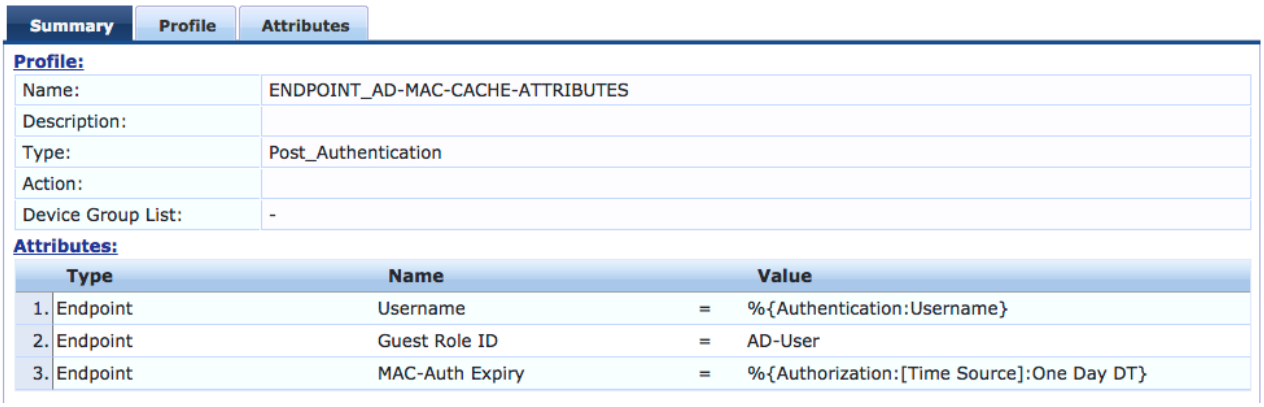
- Note that the value field will require manual entry (copy and paste the values below)

TYPE	NAME	VALUE
Endpoint	`Username`	`%{Authentication:Username}`
Endpoint	`Guest Role ID`	`%{GuestUser:Role ID}`
Endpoint	`MAC-Auth Expiry`	`%{Authorization:[Guest User Repository]:ExpireTime}`



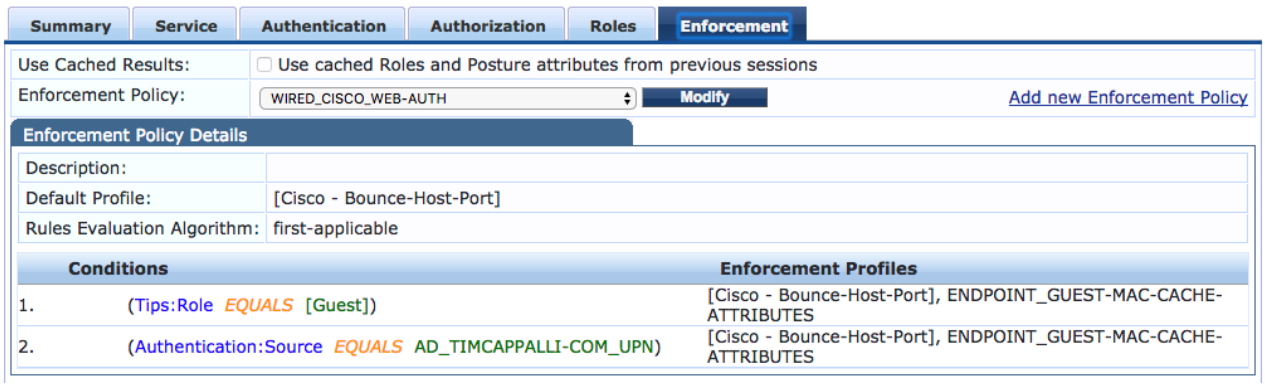
Next, create an enforcement profile for the AD users following a similar process. Since captive portal-based access should only be temporary for employees, you'll use a manual expiration of one day by using **[Time Source],** a pre-built information source. (**Configuration » Authentication » Sources » [Time Source]**).

TYPE	NAME	VALUE
Endpoint	Username	%{Authentication:Username}
Endpoint	Guest Role ID	AD-User
Endpoint	MAC-Auth Expiry	%{Authorization:[Time Source]:One Day DT}



The enforcement policy is very basic. The first rule checks for a TIPS role / tag of **[Guest]**.

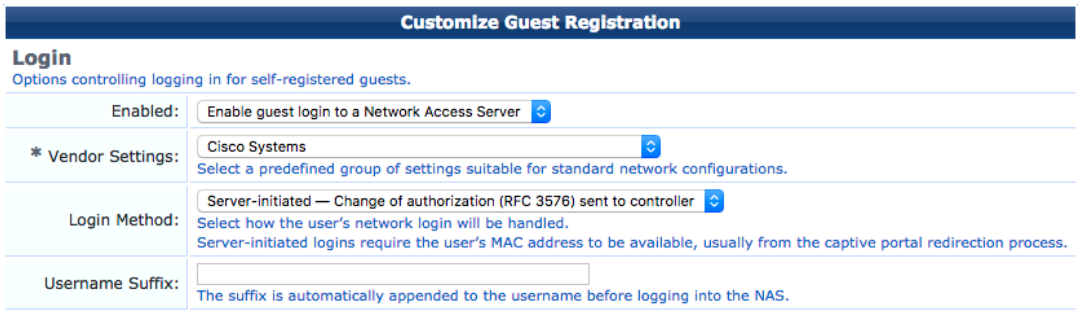
The second rule checks that the Authentication Source is Active Directory and then issues a CoA bounce port and the endpoint update enforcement profile that was created.



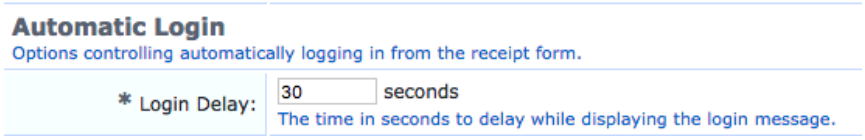
ClearPass: Guest

Configuring a self-registration workflow in Guest is outside the scope of the document. For the purposes of this guide, the only relevant settings on the guest side are the **NAS Vendor Settings** and the **Login Delay**.

Under **NAS Vendor Settings**, be sure the **Vendor Settings** are set to **Cisco Systems** which should automatically set the **Login Method** to **Server-initiated**. This is what tells Guest to craft a WEBAUTH request which we just built the service for.



Under **Login Delay**, set the value to a minimum of 30 seconds. This is required with server-initiated workflows because we don't want the user to attempt to browse while the port is still down or their device is re-authenticating. You may need to adjust this value in your environment.



Useful Switch Troubleshooting Commands

show authentication sessions

```
EDGE-C2960#show authentication sessions

Interface  MAC Address     Method   Domain   Status         Session ID
Fa0/4      0015.177b.b0d7  dot1x    DATA     Authz Success  6451000D0000010569EC4085
Fa0/1      90e2.ba69.2d5a  mab      DATA     Authz Success  6451000D0000010469E9CAC0
Fa0/5      0004.f21e.f64a  mab      VOICE    Authz Success  6451000D0000010669EF6C3F
```

show authentication sessions interface <x>

```
EDGE-C2960#show authentication sessions interface fastEthernet 0/1
            Interface:  FastEthernet0/1
          MAC Address:  90e2.ba69.2d5a
           IP Address:  100.81.2.10
            User-Name:  90e2ba692d5a
               Status:  Authz Success
               Domain:  DATA
       Oper host mode:  multi-domain
     Oper control dir:  both
        Authorized By:  Authentication Server
          Vlan Policy:  812
              ACS ACL:  xACSACLx-IP-DACL_CISCO_REDIRECT-3007-5
     URL Redirect ACL:  CLEARPASS-REDIRECT
         URL Redirect:  https://clearpass-
demo.arubaboston.com/guest/wired_cisco_self-reg.php?mac=90:e2:ba:69:2d:5a
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  6451000D0000010469E9CAC0
      Acct Session ID:  0x00000139
               Handle:  0x54000105

Runnable methods list:
       Method   State
       dot1x    Failed over
       mab      Authc Success
```

show dot1x interface <x> details

```
EDGE-C2960#show dot1x interface fastEthernet 0/4 details

Dot1x Info for FastEthernet0/4
-----------------------------------
PAE                       = AUTHENTICATOR
QuietPeriod               = 60
ServerTimeout             = 0
SuppTimeout               = 15
ReAuthMax                 = 1
MaxReq                    = 2
TxPeriod                  = 10

Dot1x Authenticator Client List
------------------------------
EAP Method                = (25)
Supplicant                = 0015.177b.b0d7
Session ID                = 6451000D0000010569EC4085
    Auth SM State         = AUTHENTICATED
    Auth BEND SM State    = IDLE
```

show epm session interface <x>

```
EDGE-C2960#show epm session interface fastEthernet 0/1
 Legend:
 Admission Method        : (a)authproxy (e)eou (d)dot1x (m)mab (c)cts
 Authorization Policies  : (a)acl (s)sgt (u)url (r)urlacl (q)qos
 Interface            Admission Method    Authorization
 ------------------------------------------------------
 FastEthernet0/1           d          aur
```

show ip device tracking all

```
EDGE-C2960#show ip device tracking all
IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30
IP Device Tracking Probe Delay Interval = 0
-----------------------------------------------------------------------
  IP Address     MAC Address   Vlan  Interface               STATE
-----------------------------------------------------------------------
100.81.2.13     90e2.ba69.2d5a  812  FastEthernet0/5          INACTIVE
100.81.3.10     0004.f21e.f64a  813  FastEthernet0/5          ACTIVE
100.81.2.10     90e2.ba69.2d5a  812  FastEthernet0/1          INACTIVE
100.81.2.10     2c41.387f.c880  812  FastEthernet0/2          INACTIVE
100.81.1.10     90e2.ba69.2d5a  811  FastEthernet0/7          INACTIVE
100.81.1.11     0015.177b.b0d7  811  FastEthernet0/4          ACTIVE

Total number interfaces enabled: 8
Enabled interfaces:
  Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5, Fa0/7, Fa0/9,
  Fa0/11
```

SNMP-based Enforcement

Policy Enforcement

VLAN assignment via SNMP is the primary enforcement method with OnConnect. VLAN access control lists (ACLs) are commonly used to control traffic in this scenario.

Configuration Overview

Here are the hardware and software combinations used for this configuration:

- Cisco Catalyst 2960 switch running Cisco IOS 15.0(2)SE10a with LAN base image
- ClearPass Policy Manager 6.6.4 (required: 6.6.1+)

Quirks and Limitations

- Active user visibility is available for Windows domain-joined machines only
- OnConnect enforcement takes an average of 60 seconds with WMI enabled

Switch Configuration

Global switch configuration:

`snmp-server community OnC0nnect@Cisco2960RO! ro`	create SNMP ro community for ClearPass
`snmp-server community OnC0nnect@Cisco2960RW! rw`	create SNMP rw community for ClearPass

`snmp-server enable traps snmp linkdown linkup`
`snmp-server enable traps mac-notification`
`snmp-server enable traps entity`
`snmp-server enable traps bridge newroot topologychange`
`snmp-server enable traps vlan-membership`
	enable traps

`snmp-server trap link ietf` `snmp-server trap timeout 5`	trap settings
`snmp-server host 100.65.30.42 trap version 2c Cle@rPass0nConnect! snmp mac-notification`	set ClearPass as the snmp-server and set trap community

`mac address-table notification change interval 1`
`mac address-table notification threshold`
`mac address-table notification change`
	MAC notifications configuration

Interface configuration:

`interface FastEthernet0/1`	

`switchport mode access`
`switchport access vlan 10`
`switchport mode access`
	assign default VLAN and access mode

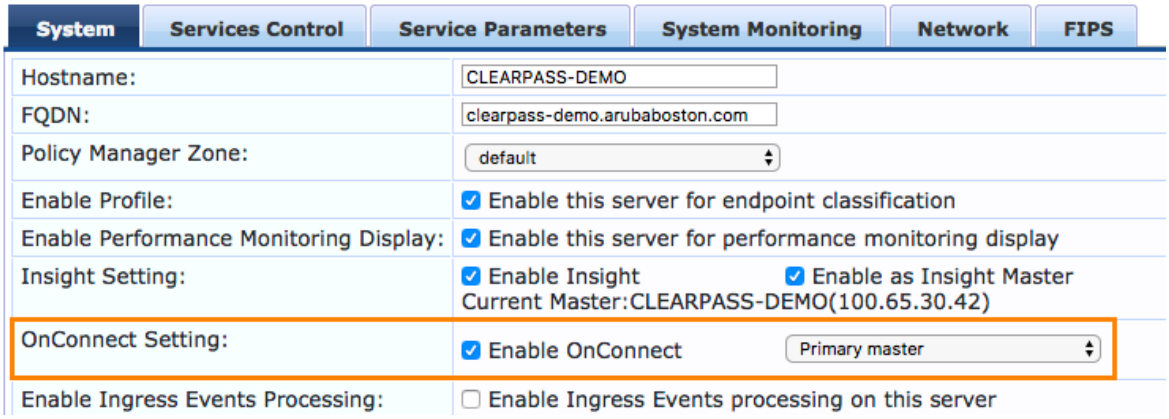
`snmp trap mac-notification change added` `snmp trap mac-notification change removed`	Enable MAC notifications

ClearPass: Basics

Server Configuration

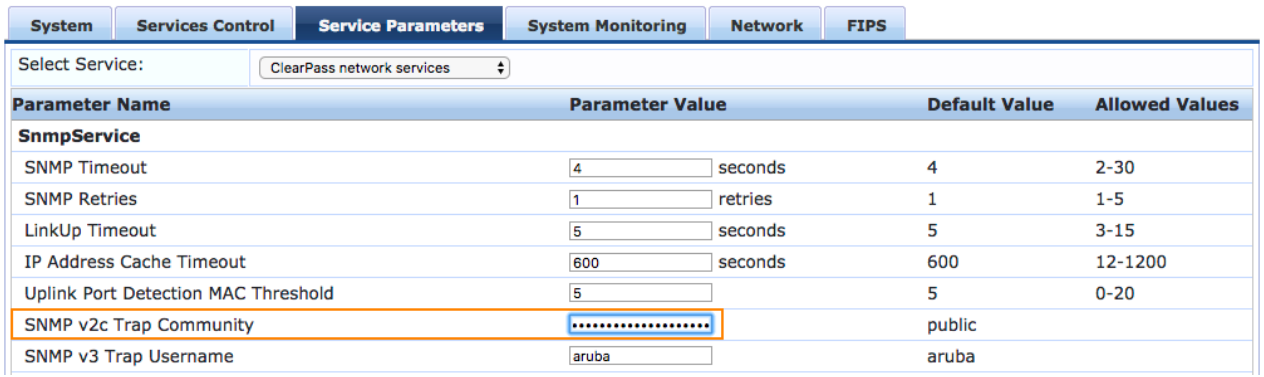
Enable OnConnect under Server Configuration (**`Administration » Server Manager » Server Configuration`**)

> **NOTE:** This is only required in ClearPass 6.6.X



Configure the SNMP v2c Trap community string for under **`Administration » Server Manager » Server Configuration, Service Parameters, ClearPass network services`**.

This should match the community string define in this switch configuration element:
`snmp-server host 100.65.30.42 trap version 2c` **`Cle@rPass0nConnect!`** `snmp mac-notification`



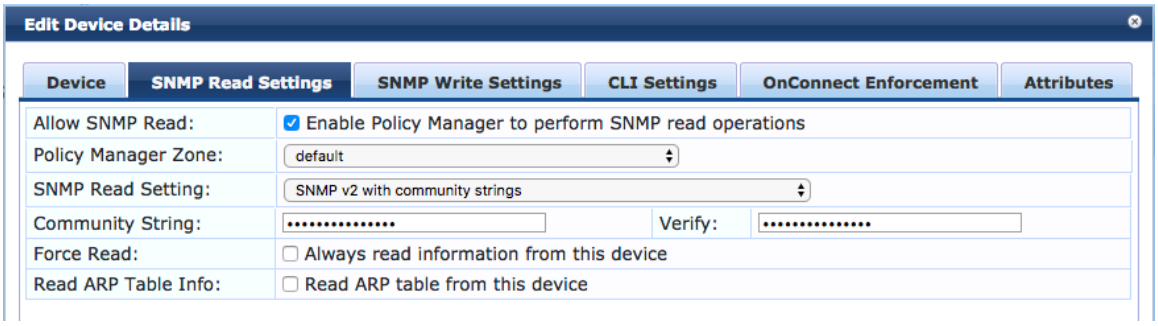
After changing the trap community, the **`System auxiliary services`** service needs to be restarted.

Navigate to **`Administration » Server Manager » Server Configuration, Services Control`** and locate **`System auxiliary services.`**

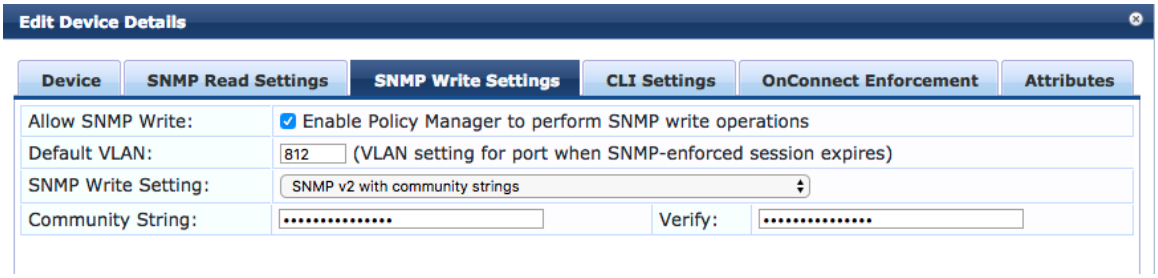
Click **Stop**. Once the service has stopped, click **Start** to restart the service.

Network Device

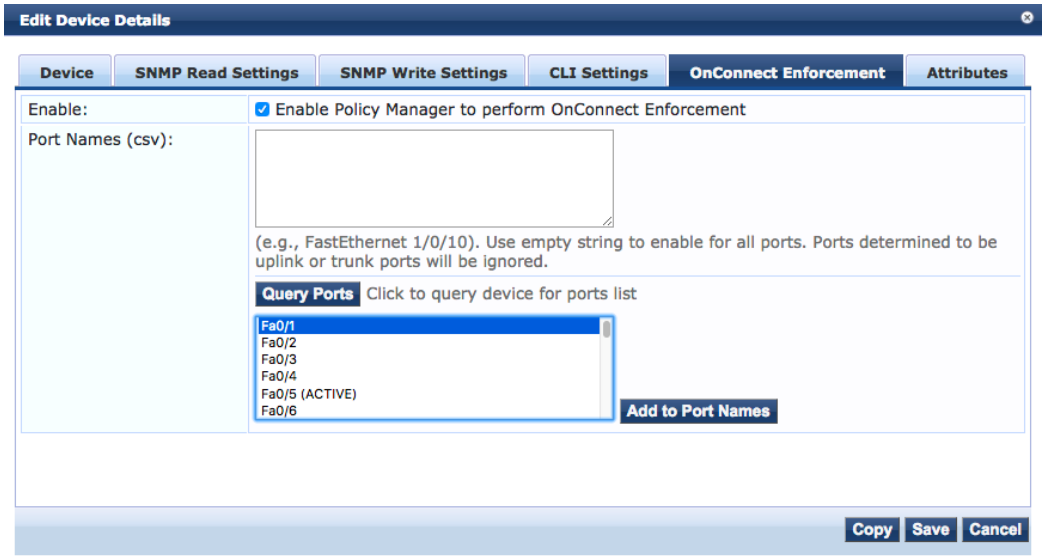
Enable SNMP Read and configure the community strings for the device:



Enable SNMP Write and configure the community strings for the device:



Enable Policy Manager to perform OnConnect Enforcement.



Use the **`Query Ports`** button to test the SNMP configuration. The list will be populated with the switch ports if all is working correctly.

Individual interfaces can also be enabled for OnConnect enforcement by selecting them in the list and clicking **`Add to Port Names`** (or by manually adding them to the Port Names list).

Windows Management Instrumentation (WMI) Overview

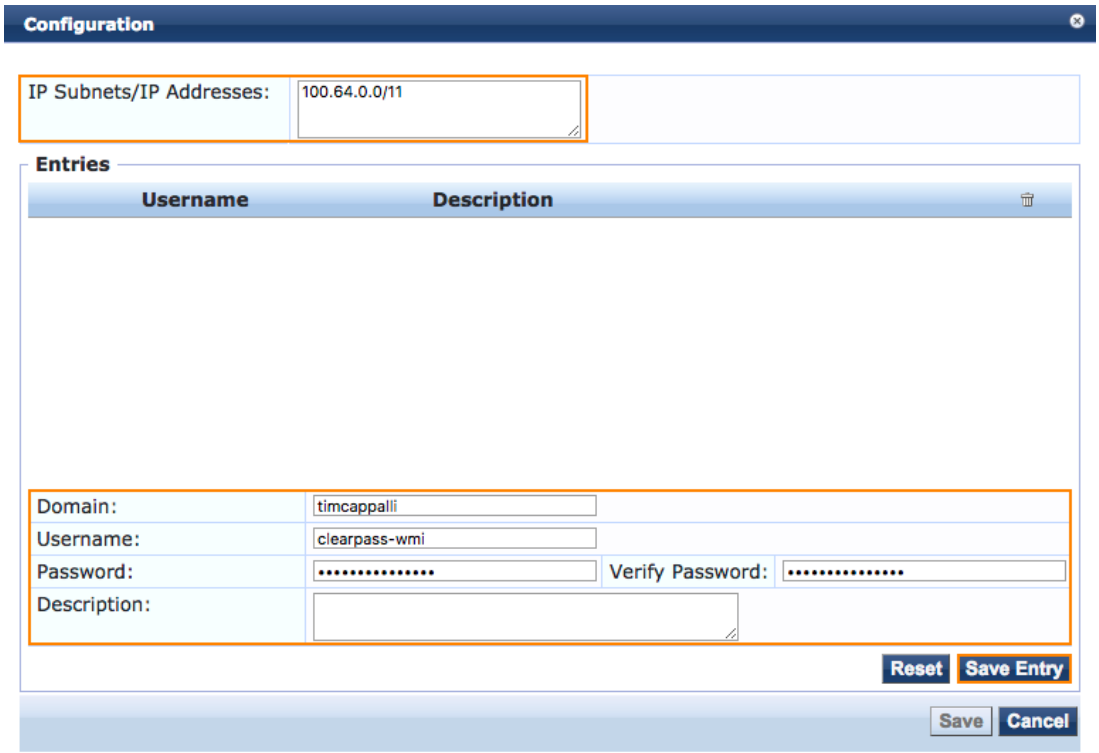
During a port status change, ClearPass can query domain-joined Windows devices for the current logged in user. This information can then be compared with user account information in Active Directory during authorization.

Requirements:

- Active Directory user account with WMI remote access privileges
- Windows firewall must allow inbound access to WMI from ClearPass

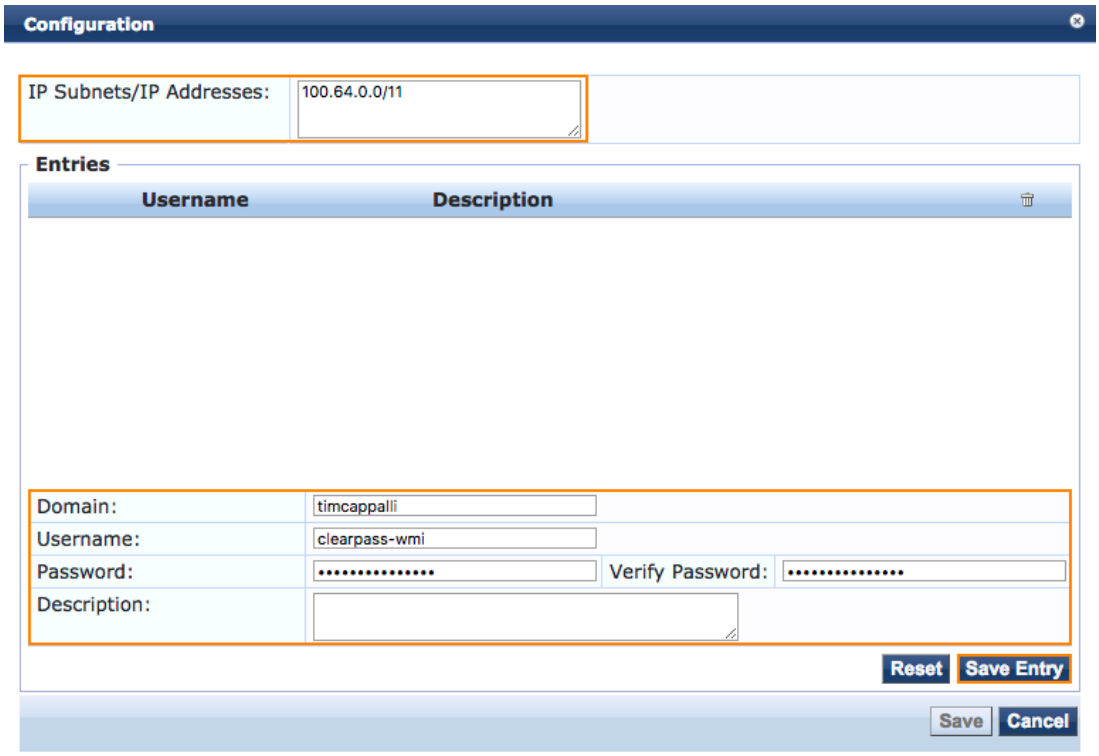
WMI Configuration: ClearPass

Inside ClearPass, map the WMI credentials to the edge subnets under Configuration » Profile Settings » WMI Configuration.



WMI Configuration: ClearPass

Inside ClearPass, map the WMI credentials to the edge subnets under **`Configuration » Profile Settings » WMI Configuration`**.

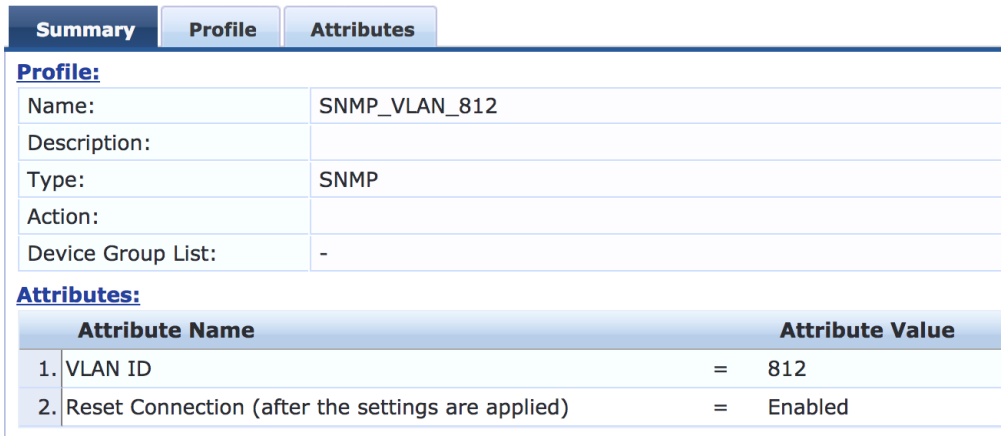


ClearPass: Enforcement Profiles

Enforcement profiles for OnConnect are very basic.

For each enforcement VLAN, create a new SNMP Based Enforcement profile. Navigate to **`Configuration » Enforcement » Profiles » Add Enforcement Profile`**. Select **`SNMP Based Enforcement`** from the template dropdown.

Add the **`VLAN ID`** and **`Reset Connection`** attributes. You can also optionally add the **`Session Timeout`** attribute to trigger a re-evaluation of policy after a certain amount of time.



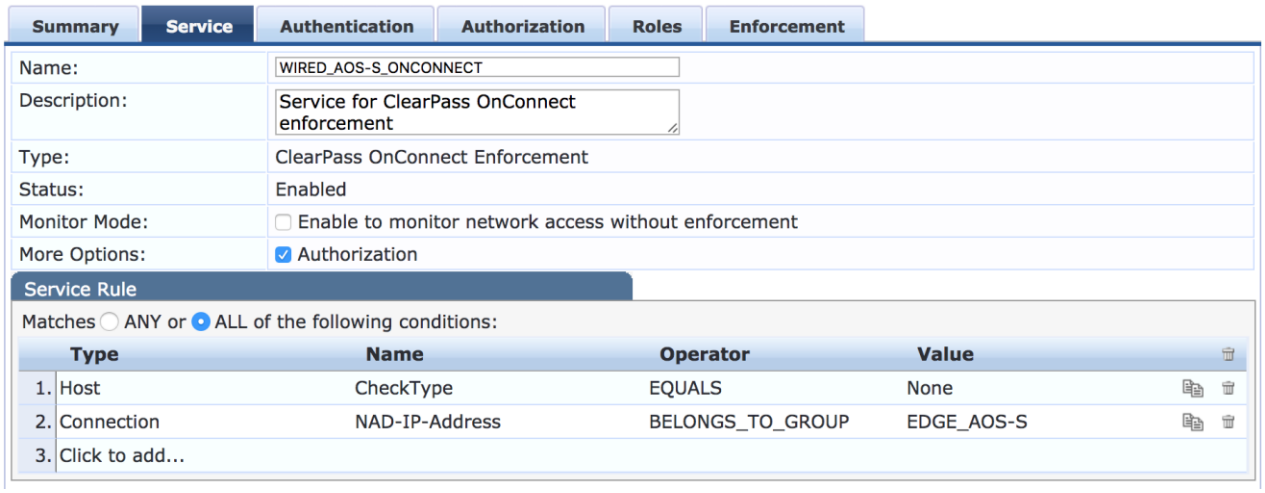
ClearPass: OnConnect Service

Service Configuration

Start with a new service of type **`ClearPass OnConnect Enforcement`**.

Under More Options, check the **`Authorization`**. This will enable the Authorization tab. The default service rules will work with an ArubaOS-Switch.

If there is a need to restrict the service to a particular set of switches, you can use a **`Connection`** | **`NAD-IP-Address`** | **`BELONGS_TO_GROUP`** service rule to reference a NAD group as seen in rule 2 below.



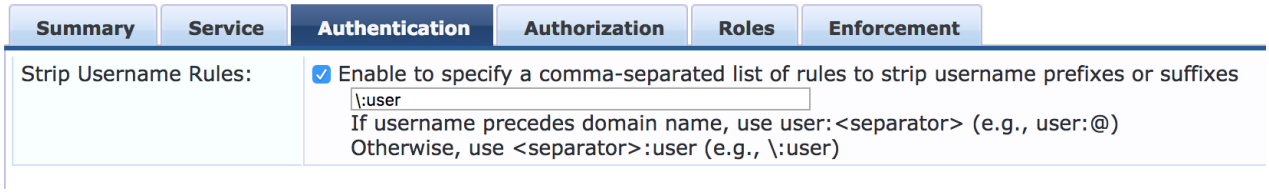
Authentication

Since OnConnect does not do any traditional user or device authentication, the only option available on the Authentication tab is the Strip Username Rules configuration.

If you are not planning to use WMI, nothing has to be configured on the Authentication tab.

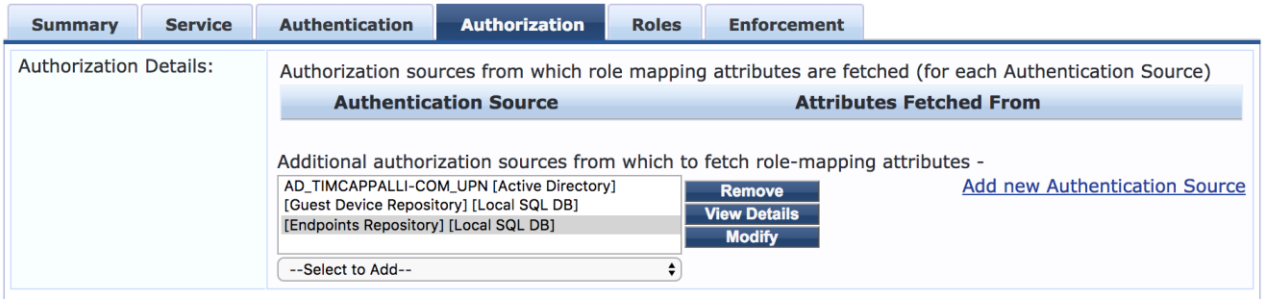
If you are planning to use WMI to grab the currently logged in user, the Strip Username Rules will need to be configured. WMI returns the username in down-level logon format (REALM\username) so the REALM will need to be stripped off before an authorization check can be done against Active Directory.

Use the **`\:user`** rule to strip the REALM from the down-level logon username.



Authorization

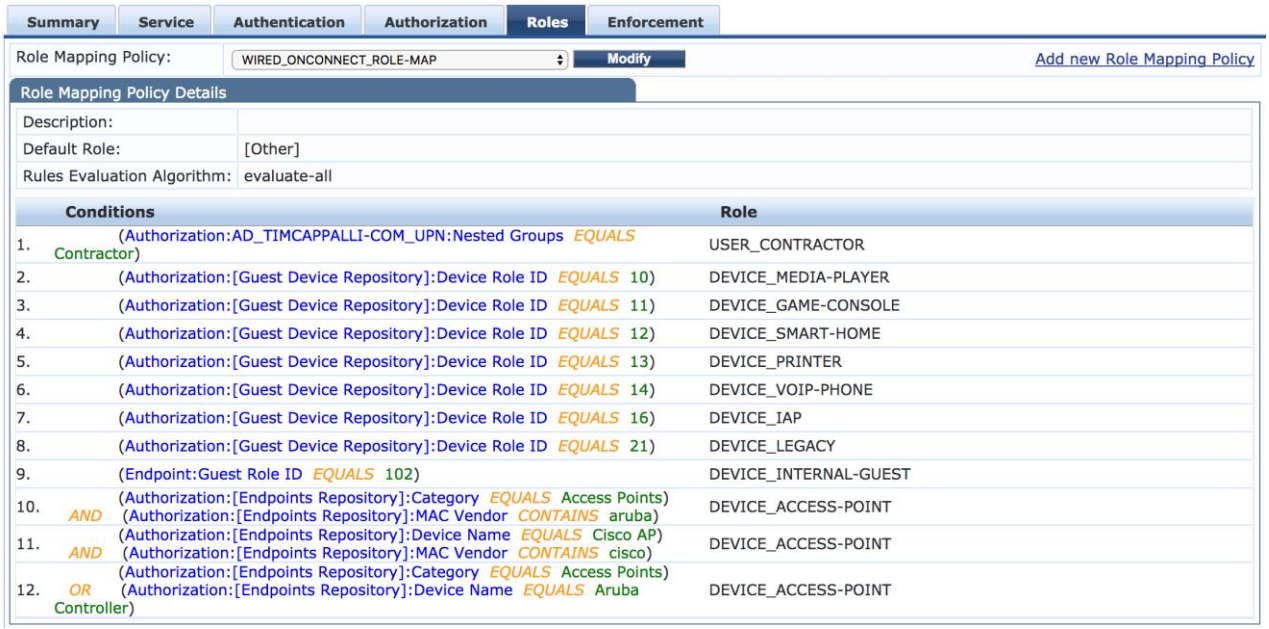
On the Authorization tab, add the **[Endpoints Repository]** and **[Guest Device Repository]** to the "Additional authorization sources…" list as shown below. If WMI-based authorization will be used, also add your Active Directory authentication source to the list so user properties can be evaluated.



Roles

Role mapping is used to tag devices and users with as much information as possible for use in a policy decision.

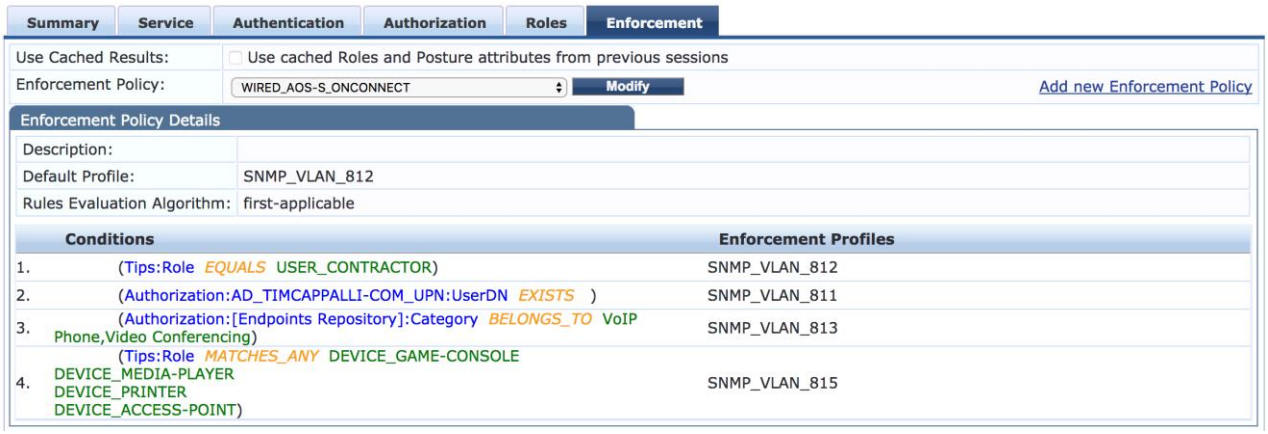
This *example* role map covers both headless devices and user mapping based off AD group membership. Headless devices are mapped using a mix of device registrations and raw profile data.



Enforcement

For the default policy, the default guest VLAN profile is specified. This is used when a request falls through the policy with no match which would be a guest in this case.

Let's take apart the enforcement rules one by one:



1

(Tips:Role EQUALS USER_CONTRACTOR) SNMP_VLAN_812

If the logged in user is in the "Contractor" group, the `USER_CONTRACTOR` tag/TIPS Role is mapped. This device is then given the GUEST VLAN, 812 in this example.

2

(Authorization:AD_TIMCAPPALLI-COM_UPN:UserDN EXISTS) SNMP_VLAN_811

This rule just checks that the logged in user is a domain user. All domain users will have a `UserDN` attribute. These devices will be placed into the "SECURE" VLAN, 811 in this case.

3

(Authorization:[Endpoints Repository]:Category BELONGS_TO VoIP Phone,Video Conferencing) SNMP_VLAN_813

Profile data is being leverage in rule 3 to drop voice devices into VLAN 813, the voice VLAN.

4

(Tips:Role MATCHES_ANY DEVICE_GAME-CONSOLE DEVICE_MEDIA-PLAYER DEVICE_PRINTER DEVICE_ACCESS-POINT) SNMP_VLAN_815

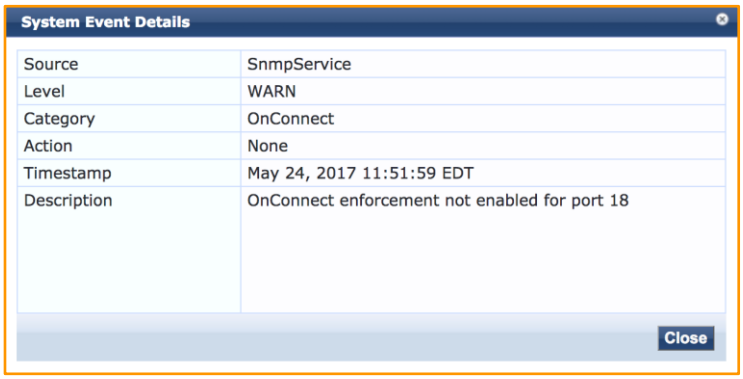
These tags/TIPS roles are mapped based on the role assigned during Device Registration. These registered devices will be dropped into the "HEADLESS" VLAN, 815 in this case.

Useful Troubleshooting Commands and Tips

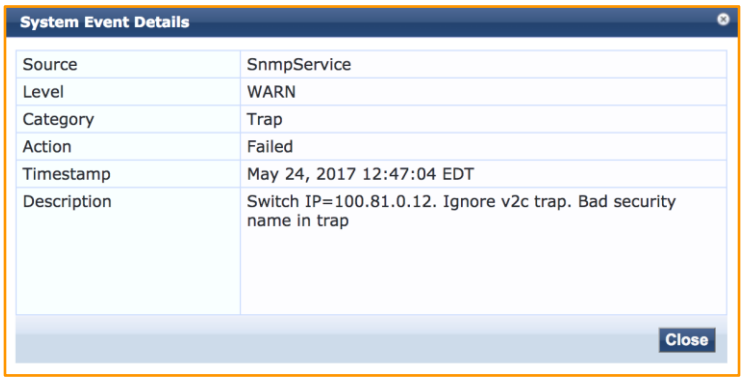
ClearPass

If OnConnect requests are not appearing in Access Tracker, take a look in Event Viewer. Below are some common error messages.

- Traps are being sent by the switch, but the network device definition in ClearPass does not have the port listed for OnConnect enforcement.



- The SNMP trap community is mismatched



Switch

`debug snmp packets`

www.arubanetworks.com
3333 Scott Blvd
Santa Clara, CA 95054
Phone: 1-800-WIFI-LAN (+800-943-4526)
Fax 408.227.4550