

# MACHINE AND USER AUTHENTICATION IN WINDOWS WITH CLEARPASS

Sometimes we need more than just user authentication, in this document I will share the configuration steps needed to enforce machine and user authentication and also put per user based role.

## SCENARIO:

1. If a user complete USER+MACHINE both authentication, then the user will get 'authenticated' role along with VLAN1
2. If a user complete only any of the above authentication [USER or MACHINE], the user will get 'guest' role along with VLAN2.

## INTRODUCTION:

The following was completed using Clearpass 6.4.1, a windows 2012, a 3600 running 6.4.2.4 and AP-93.

Clearpass is joined to domain and able to access the server.

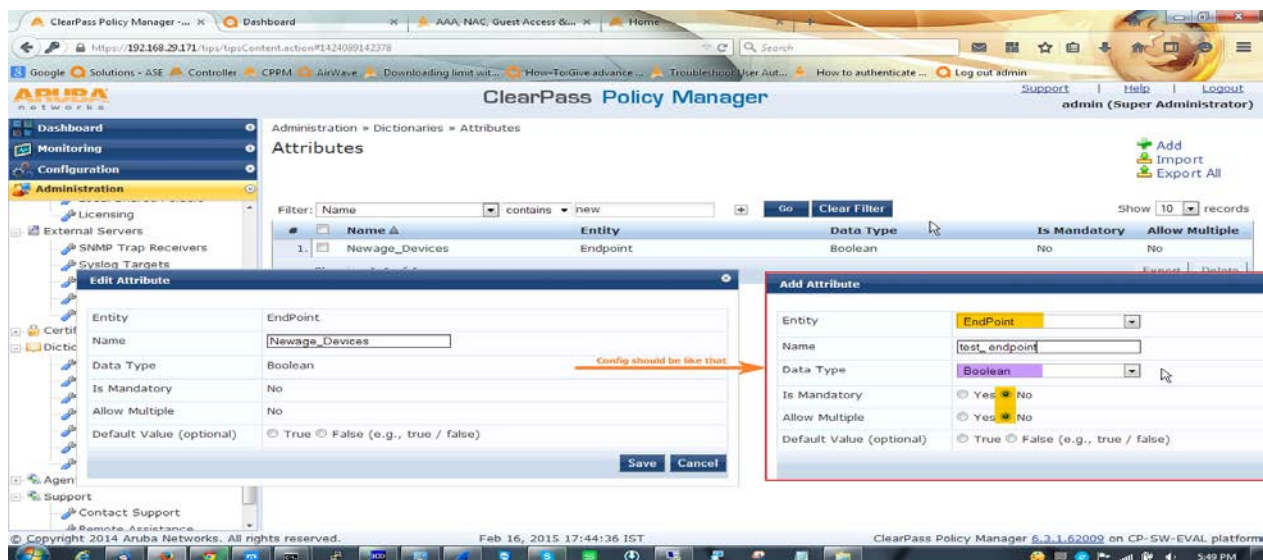
You can find another good guide on the same in

[How-to-Machine-AND-User-Authentication-in-Windows-with-Clearpass](#)

## CONFIGURATION:

A. At first we will create one custom endpoint attribute, it will validate our valid device.

Go to Administration » Dictionaries » Attributes and in right left corner click on add to add a custom attribute. The attribute should be endpoint attribute and boolean.



B. Now we will configure enforcement profile. For this scenario we need three enforcement profile.

Open Configuration » Enforcement » Profiles. Follow this screenshot.

First enforcement profile is a post auth profile to enforce the attribute, for this we will select **Clearpass entity update enforcement** template.

The screenshot shows the ClearPass Policy Manager interface. The left sidebar has a tree view with 'Configuration' expanded, and 'Profiles' selected under 'Enforcement'. The main content area shows the 'Edit Enforcement Profile' page for 'Mach\_and\_User\_Auth\_Entty\_Updte\_Prof'. The 'Profile' tab is active, displaying the following details:

- Profile:**
  - Name: Mach\_and\_User\_Auth\_Entty\_Updte\_Prof
  - Description:
  - Type: Post\_Authentication
  - Action:
  - Device Group List: -
- Attributes:**

Type	Name	Value
1. Endpoint	Newage_Devices	= true

Now 2<sup>nd</sup> one for authenticated users. In here we will give the user 'authenticated' role and after that assigned them to VLAN1.

The screenshot shows the ClearPass Policy Manager interface. The left sidebar has a tree view with 'Configuration' expanded, and 'Profiles' selected under 'Enforcement'. The main content area shows the 'Edit Enforcement Profile' page for 'Newage\_Mach\_and\_User\_Auth\_Profile'. The 'Profile' tab is active, displaying the following details:

- Profile:**
  - Name: Newage\_Mach\_and\_User\_Auth\_Profile
  - Description:
  - Type: RADIUS
  - Action: Accept
  - Device Group List: -
- Attributes:**

Type	Name	Value
1. Radius:Aruba	Aruba-User-Role	= authenticated
2. Radius:Aruba	Aruba-User-Vlan	= 1

3<sup>rd</sup> profile for the user, who completed only one authentication. Here we will give the user 'guest' role along with VLAN2

The screenshot displays the ClearPass Policy Manager web interface. The left sidebar shows the navigation menu with categories: Identity, Posture, Enforcement, Network, and Administration. The 'Enforcement' category is expanded, and the 'Profiles' sub-item is selected. The main content area shows the 'Edit Enforcement Profile - Guest' page. The 'Summary' tab is active, displaying the profile details: Name: Guest, Description: (empty), Type: RADIUS, Action: Accept, and Device Group List: -. Below this, the 'Attributes' section shows a table with two attributes:

Type	Name	Value
1. Radius:Aruba	Aruba-User-Role	= guest
2. Radius:Aruba	Aruba-User-Vlan	= 2

At the bottom of the page, there is a 'Back to Enforcement Profiles' link and buttons for 'Copy', 'Save', and 'Cancel'. The footer of the interface shows the copyright notice '© Copyright 2014 Aruba Networks. All rights reserved.', the date 'Feb 16, 2015 17:46:22 IST', and the version 'ClearPass Policy Manager 6.3.1.62009 on CP-SW-EVAL platform'.

C. After configuring enforcement profile we have to configure enforcement policy which will bundle all the three enforcement profile.

Open Configuration » Enforcement » Policies

ClearPass Policy Manager - Dashboard

Configuration » Enforcement » Policies » Edit - Newage\_Mach\_and\_User\_Auth\_Policy

### Enforcement Policies - Newage\_Mach\_and\_User\_Auth\_Policy

Summary Enforcement Rules

**Enforcement:**

Name: Newage\_Mach\_and\_User\_Auth\_Policy

Description:

Enforcement Type: RADIUS

Default Profile: [Deny Access Profile]

**Rules:**

Rules Evaluation Algorithm: First applicable

Conditions	Actions
1. (Tips:Role MATCHES_ALL [Machine Authenticated]) [User Authenticated]	Newage_Mach_and_User_Auth_Profile, Mach_and_User_Auth_Entty_Updte_Prof
2. (Tips:Role EQUALS [Machine Authenticated])	Guest
3. (Tips:Role EQUALS [User Authenticated])	Guest

[Back to Enforcement Policies](#) [Copy](#) [Save](#) [Cancel](#)

© Copyright 2014 Aruba Networks. All rights reserved. Feb 16, 2015 17:46:44 IST ClearPass Policy Manager 6.3.1.62009 on CP-SW-EVAL platform

D. Now we have to configure one role mapping policy to tag information in the request so later we can use it in enforcement profile. Also create one role to map this.

Go to Configuration » Identity » Role Mapping

ClearPass Policy Manager - Dashboard

Configuration » Identity » Role Mappings » Edit - Newage\_Mach\_and\_User\_Auth\_Role\_Mapping

### Role Mappings - Newage\_Mach\_and\_User\_Auth\_Role\_Mapping

Summary Policy Mapping Rules

**Policy:**

Policy Name: Newage\_Mach\_and\_User\_Auth\_Role\_Mapping

Description:

Default Role: [Guest]

**Mapping Rules:**

Rules Evaluation Algorithm: Evaluate all

Conditions	Role Name
1. (Endpoint:Newage_Devices EQUALS true) AND (Authorization:Phoenix:UserDN ENDS_WITH CN=Users,DC=newage,DC=com)	Newage_Mach_and_User_Auth_Role

[Back to Role Mappings](#) [Copy](#) [Save](#) [Cancel](#)

© Copyright 2014 Aruba Networks. All rights reserved. Feb 16, 2015 17:47:23 IST ClearPass Policy Manager 6.3.1.62009 on CP-SW-EVAL platform

This role mapping will place the validate user in desired roles, User auth

E. Now the most important things, we have to configure one service.

Check the summary tab of the service. Remember to enable authorization source in service tab.

The screenshot displays the ClearPass Policy Manager web interface. The left sidebar shows the navigation menu with 'Configuration' selected. The main content area shows the 'Services - Newage\_Mach\_and\_User\_Auth\_Service' configuration page. The 'Summary' tab is active, displaying the following details:

- Service:**
  - Name: Newage\_Mach\_and\_User\_Auth\_Service
  - Description: Aruba 802.1X Wireless Access Service
  - Type: Aruba 802.1X Wireless
  - Status: Enabled
  - Monitor Mode: Disabled
  - More Options: [Authorization](#)
- Service Rule**
  - Match ALL of the following conditions:
  - | Type            | Name             | Operator | Value          |
|-----------------|------------------|----------|----------------|
| 1. Radius:Aruba | Aruba-Essid-Name | EQUALS   | Corp-Network   |
| 2. Radius:IETF  | NAS-IP-Address   | EQUALS   | 192.168.29.170 |
| 3. Connection   | Protocol         | EQUALS   | RADIUS         |
- Authentication:**
  - Authentication Methods: 1. [EAP PEAP], 2. [EAP MSCHAPv2]
  - Authentication Sources: Phoenix

At the bottom of the configuration page, there are buttons for 'Back to Services', 'Disable', 'Copy', 'Save', and 'Cancel'. The footer of the interface shows the copyright information: '© Copyright 2014 Aruba Networks. All rights reserved.' and the version: 'ClearPass Policy Manager 6.3.1.62009 on CP-SW-EVAL platform'.

Open authentication tab and select AD as a authentication source, EAP-PEAP and EAP-MSCHAPV2 as authentication method [this two is enough to handle the AAA process but if you want or if you have legacy device you always can configure other authentication method].



ClearPass Policy Manager - ... x Dashboard x AAA, NAC, Guest Access &... x Home x

https://192.168.29.171/tips/tipsContent.action#1424089391239

Google Solutions - ASE Controller CPPM AirWave Downloading limit wit... How-To-Give advance ... Troubleshoot User Aut... How to authenticate ... Log out admin

ARUBA networks

# ClearPass Policy Manager

Support | Help | Logout  
admin (Super Administrator)

Configuration » Services » Edit - Newage\_Mach\_and\_User\_Auth\_Service

## Services - Newage\_Mach\_and\_User\_Auth\_Service

Summary Service Authentication Authorization Roles Enforcement

Authentication Methods:

- [EAP PEAP]
- [EAP MSCHAPv2]

--Select to Add--

Authentication Sources:

- Phoenix [Active Directory]

--Select to Add--

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

Back to Services

Disable Copy Save Cancel

© Copyright 2014 Aruba Networks. All rights reserved. Feb 16, 2015 17:48:17 IST ClearPass Policy Manager 6.3.1.62009 on CP-SW-EVAL platform

ClearPass Policy Manager - ... x Dashboard x AAA, NAC, Guest Access &... x Home x

https://192.168.29.171/tips/tipsContent.action#1424089391239

Google Solutions - ASE Controller CPPM AirWave Downloading limit wit... How-To-Give advance ... Troubleshoot User Aut... How to authenticate ... Log out admin

ARUBA networks

# ClearPass Policy Manager

Support | Help | Logout  
admin (Super Administrator)

Configuration » Services » Edit - Newage\_Mach\_and\_User\_Auth\_Service

## Services - Newage\_Mach\_and\_User\_Auth\_Service

Summary Service Authentication Authorization Roles Enforcement

Authorization Details:

Authorization sources from which role mapping attributes are fetched (for each Authentication Source)

Authentication Source	Attributes Fetched From
1. Phoenix [Active Directory]	Phoenix [Active Directory]

Additional authorization sources from which to fetch role-mapping attributes -

- [Endpoints Repository] [Local SQL DB]

--Select to Add--

Back to Services

Disable Copy Save Cancel

© Copyright 2014 Aruba Networks. All rights reserved. Feb 16, 2015 17:48:22 IST ClearPass Policy Manager 6.3.1.62009 on CP-SW-EVAL platform

ClearPass Policy Manager - ... Dashboard AAA, NAC, Guest Access &... Home

https://192.168.29.171/tips/tipsContent.action#1424089391239

Google Solutions - ASE Controller CPM AirWave Downloading limit wit... How-To-Give advance ... Troubleshoot User Aut... How to authenticate ... Log out admin

ARUBA networks ClearPass Policy Manager Support Help Logout admin (Super Administrator)

Configuration » Services » Edit - Newage\_Mach\_and\_User\_Auth\_Service

Services - Newage\_Mach\_and\_User\_Auth\_Service

Summary Service Authentication Authorization Roles Enforcement

Role Mapping Policy: Newage\_Mach\_and\_User\_Auth\_Role\_Mappin Modify Add new Role Mapping Policy

Role Mapping Policy Details

Description:

Default Role: [Guest]

Rules Evaluation Algorithm: evaluate-all

Conditions	Role
1. (Endpoint:Newage_Devices EQUALS true) AND (Authorization:Phoenix:UserDN ENDS_WITH CN=Users,DC=newage,DC=com)	Newage_Mach_and_User_Auth_Role

Back to Services Disable Copy Save Cancel

© Copyright 2014 Aruba Networks. All rights reserved. Feb 16, 2015 17:48:27 IST ClearPass Policy Manager 6.3.1.62009 on CP-SW-EVAL platform 5:53 PM

ClearPass Policy Manager - ... Dashboard AAA, NAC, Guest Access &... Home

https://192.168.29.171/tips/tipsContent.action#1424089391239

Google Solutions - ASE Controller CPM AirWave Downloading limit wit... How-To-Give advance ... Troubleshoot User Aut... How to authenticate ... Log out admin

ARUBA networks ClearPass Policy Manager Support Help Logout admin (Super Administrator)

Configuration » Services » Edit - Newage\_Mach\_and\_User\_Auth\_Service

Services - Newage\_Mach\_and\_User\_Auth\_Service

Summary Service Authentication Authorization Roles Enforcement

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

Enforcement Policy: Newage\_Mach\_and\_User\_Auth\_Policy 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 MATCHES_ALL [Machine Authenticated]) [User Authenticated])	Newage_Mach_and_User_Auth_Profile, Mach_and_User_Auth_Entty_Updte_Prof
2. (Tips:Role EQUALS [Machine Authenticated])	Guest
3. (Tips:Role EQUALS [User Authenticated])	Guest

Back to Services Disable Copy Save Cancel

© Copyright 2014 Aruba Networks. All rights reserved. Feb 16, 2015 17:48:32 IST ClearPass Policy Manager 6.3.1.62009 on CP-SW-EVAL platform 5:53 PM

The screenshot displays the ClearPass Policy Manager web interface. The left sidebar shows the navigation menu with categories like Dashboard, Monitoring, Configuration, Identity, Posture, Enforcement, Network, and Administration. The main content area is titled 'Configuration » Services » Edit - Newage\_Mach\_and\_User\_Auth\_Service'. Below this, there are tabs for Summary, Service, Authentication, Authorization, Roles, and Enforcement. The 'Enforcement' tab is active, showing the 'Enforcement Policy' dropdown set to 'Newage\_Mach\_and\_User\_Auth\_Policy'. Below this, the 'Enforcement Policy Details' section shows the 'Default Profile' as '[Deny Access Profile]' and the 'Rules Evaluation Algorithm' as 'first-applicable'. A table lists the conditions and enforcement profiles:

Conditions	Enforcement Profiles
1. (Tips:Role MATCHES_ALL [Machine Authenticated]) [User Authenticated])	Newage_Mach_and_User_Auth_Profile, Mach_and_User_Auth_Entty_Updte_Prof
2. (Tips:Role EQUALS [Machine Authenticated])	Guest
3. (Tips:Role EQUALS [User Authenticated])	Guest

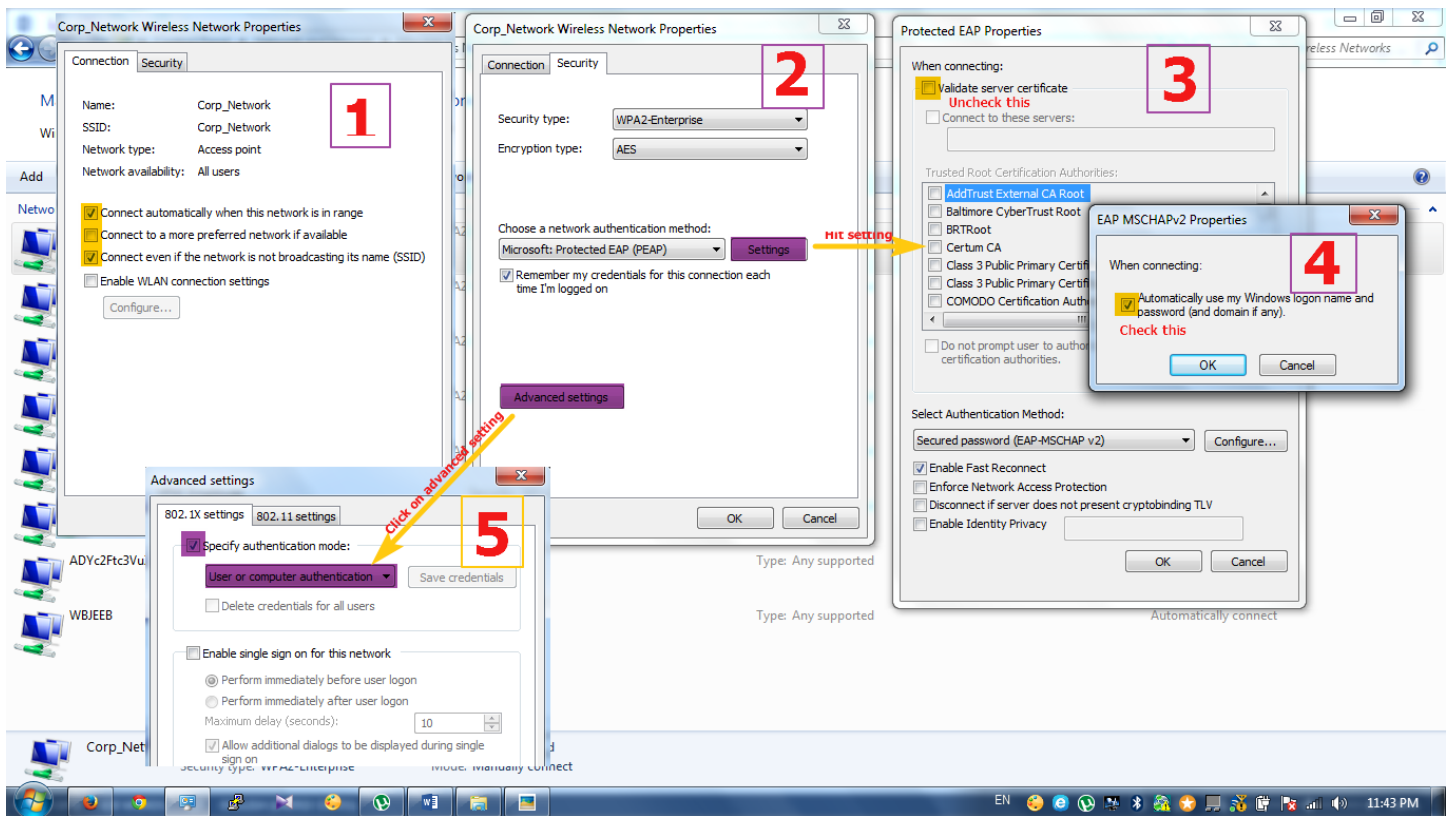
At the bottom of the interface, there are buttons for 'Back to Services', 'Disable', 'Copy', 'Save', and 'Cancel'. The footer shows the copyright information for Aruba Networks and the current date and time.

In controller side nothing to do, just make sure that you have the VLAN and Role configured in controller, because what are you defining[VLAN & Role] here will take effect from the controller.

We need to configure our wireless ssid profile to make the both authentication work. Below are the configuration steps.

Go to **Control Panel\Network and Internet\Manage Wireless Networks** click add and add your desired network and go to the setting.





**That's all. Now it's time to check output**

The screenshot displays the ClearPass Policy Manager web interface. The 'Request Details' section is active, showing a summary of the request. The 'Summary' tab is selected, displaying the following information:

Summary	Input	Output	Accounting
Session Identifier:	R00000084-01-54e1da17		
Date and Time:	Feb 16, 2015 17:22:55 IST		
End-Host Identifier:	0026B6BDF559		
Username:	NEWAGE\sumansinha		
Access Device IP/Port:	192.168.29.170:0		
System Posture Status:	UNKNOWN (100)		
<b>Policies Used -</b>			
Service:	Newage_Mach_and_User_Auth_Service		
Authentication Method:	EAP-PEAP,EAP-MSCHAPv2		
Authentication Source:	AD:phoenix.newage.com		
Authorization Source:	[Endpoints Repository], Phoenix		
Roles:	Newage_Mach_and_User_Auth_Role, [Machine Authenticated], [User Authenticated]		
Enforcement Profiles:	Mach_and_User_Auth_Entty_Updte_Prof, Newage_Mach_and_User_Auth_Profile		
Service Monitor Mode:	Disabled		
Online Status:	Offline		

The 'Summary & output' section on the right shows the 'RADIUS Response' with the following details:

Summary	Input	Output	Accounting
Enforcement Profiles:	Mach_and_User_Auth_Entty_Updte_Prof, Newage_M		
System Posture Status:	UNKNOWN (100)		
Audit Posture Status:	UNKNOWN (100)		
<b>RADIUS Response</b>			
Endpoint:	Newage_Devices	true	
Radius:	Aruba:Aruba-User-Role	authenticated	
Radius:	Aruba:Aruba-User-Vlan	1	

The bottom section of the interface shows a table of request logs with columns for ID, IP, Username, Service, Status, and Time.

In above user has completed both authentication so it's got authenticated role along with VLAN1.

ClearPass Policy Manager

admin (Super Administrator)

Request Details

Summary	Input	Output	Accounting
Session Identifier:	R00000091-01-54e23c81		
Date and Time:	Feb 17, 2015 00:22:49 IST		
End-Host Identifier:	C0188528A50E		
Username:	sumansinha		
Access Device IP/Port:	192.168.29.170:0		
System Posture Status:	UNKNOWN (100)		
Policies Used -			
Service:	Newage_Mach_and_User_Auth_Service		
Authentication Method:	EAP-PEAP,EAP-MSCHAPv2		
Authentication Source:	AD:phoenix.newage.com		
Authorization Source:	[Endpoints Repository], Phoenix		
Roles:	[Guest], [User Authenticated]		
Enforcement Profiles:	Guest		
Service Monitor Mode:	Disabled		
Online Status:	Online		

Summary & output

Request Details

Summary	Input	Output	Accounting
Enforcement Profiles:	Guest		
System Posture Status:	UNKNOWN (100)		
Audit Posture Status:	UNKNOWN (100)		
RADIUS Response			
Radius:Aruba:Aruba-User-Role	guest		
Radius:Aruba:Aruba-User-Vlan	2		

Showing 1 of 1-90 records

Change Status Export

Configuration Administration

Copyright 2014 Aruba Networks. All rights reserved. Feb 17, 2015 00:23:21 IST ClearPass Policy Manager 6.3.1.62009 on CP-SW-EVAL platform

ClearPass Policy Manager

admin (Super Administrator)

Request Details

Summary	Input	Output	Accounting
Session Identifier:	R00000085-01-54e1da5a		
Date and Time:	Feb 16, 2015 17:24:03 IST		
End-Host Identifier:	0026B6BDF559		
Username:	host/sumansinha.newage.com		
Access Device IP/Port:	192.168.29.170:0		
System Posture Status:	UNKNOWN (100)		
Policies Used -			
Service:	Newage_Mach_and_User_Auth_Service		
Authentication Method:	EAP-PEAP,EAP-MSCHAPv2		
Authentication Source:	AD:phoenix.newage.com		
Authorization Source:	[Endpoints Repository], Phoenix		
Roles:	[Guest], [Machine Authenticated]		
Enforcement Profiles:	Guest		
Service Monitor Mode:	Disabled		
Online Status:	Offline		

Summary & output

Request Details

Summary	Input	Output	Accounting
Enforcement Profiles:	Guest		
System Posture Status:	UNKNOWN (100)		
Audit Posture Status:	UNKNOWN (100)		
RADIUS Response			
Radius:Aruba:Aruba-User-Role	guest		
Radius:Aruba:Aruba-User-Vlan	2		

Showing 17 of 1-88 records

Change Status Export Show Logs

Configuration Administration

https://192.168.29.171/tips/tipsContent.action# rights reserved. Feb 17, 2015 00:13:22 IST ClearPass Policy Manager 6.3.1.62009 on CP-SW-EVAL platform

In above users has completed only one authentication so it's got **guest** role along with VLAN2.