

# ONBOARD USING DIFFERENT SSID

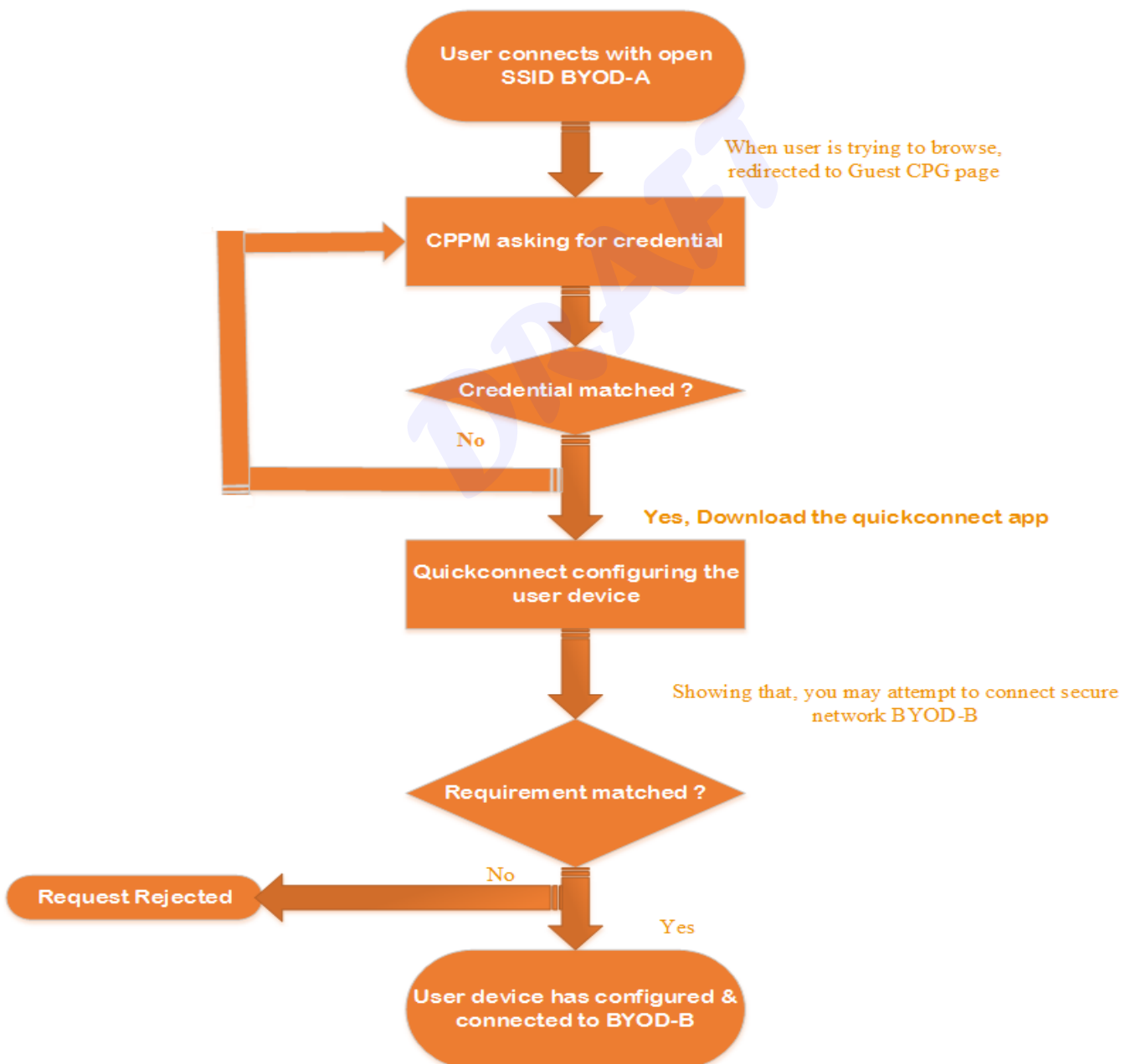
## Overview:

This topic is about Device onboard using two SSID. In this scenario I'll use two SSID. At first user device will connect to one SSID, which is open network, after that user will redirect to CPPM's captive portal page. When user complete the captive portal authentication, onboard will start to working. It will configure the user device and after completion user will automatically switch to 2<sup>nd</sup> SSID.

SSID used here

1. BYOD-A [Open network ]
2. BYOD-B [Secured with WPA2-AES]

## Flowchart:



**A. Log in to the CPPM and go to Home » Onboard + Workspace » Onboard/MDM Configuration » Network Settings**

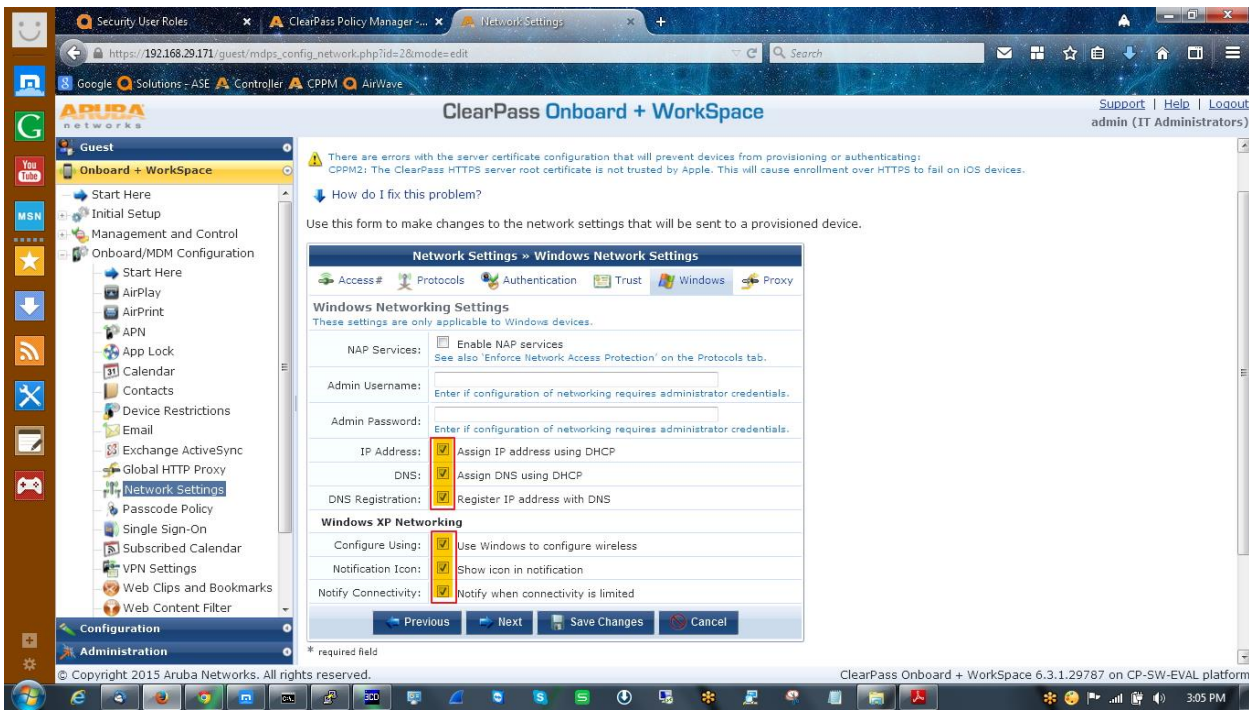
**Put the name of the 2<sup>nd</sup> ssid & select 'automatically join network'**

The screenshot shows the 'Network Settings' page in the ClearPass Onboard + Workspace interface. The left sidebar contains a navigation menu with options like 'Guest', 'Onboard + Workspace', 'Management and Control', and 'Configuration'. The main content area is titled 'Network Access' and 'Options for basic network access'. It includes fields for 'Name' (VFM Network), 'Description', 'Network Type' (Wireless only), and 'Security Type' (Enterprise (802.1X)). Below these are 'Wireless Network Settings' with 'Security Version' (WPA2 with AES), 'SSID' (BYOD-B), and 'Auto Join' (checked). The page footer indicates 'ClearPass Onboard + Workspace 6.3.1.29787 on CP-SW-EVAL platform'.

**B. Now go to next tab and configure as per your requirement.**

The screenshot shows the 'Enterprise Protocols' page in the ClearPass Onboard + Workspace interface. The left sidebar is the same as in the previous screenshot. The main content area is titled 'Enterprise Protocols' and 'Options for 802.1X protocols supported on the network'. It includes tabs for 'Access', 'Protocols', 'Authentication', 'Trust', 'Windows', and 'Proxy'. The 'Authentication' tab is selected, showing 'Accepted EAP Types' (TLS, PEAP, TTLS, EAP-FAST) and 'Authentication Protocols' (TLS, PEAP, TTLS, EAP-FAST). The page footer indicates 'ClearPass Onboard + Workspace 6.3.1.29787 on CP-SW-EVAL platform'.

**C. Open the windows tab**

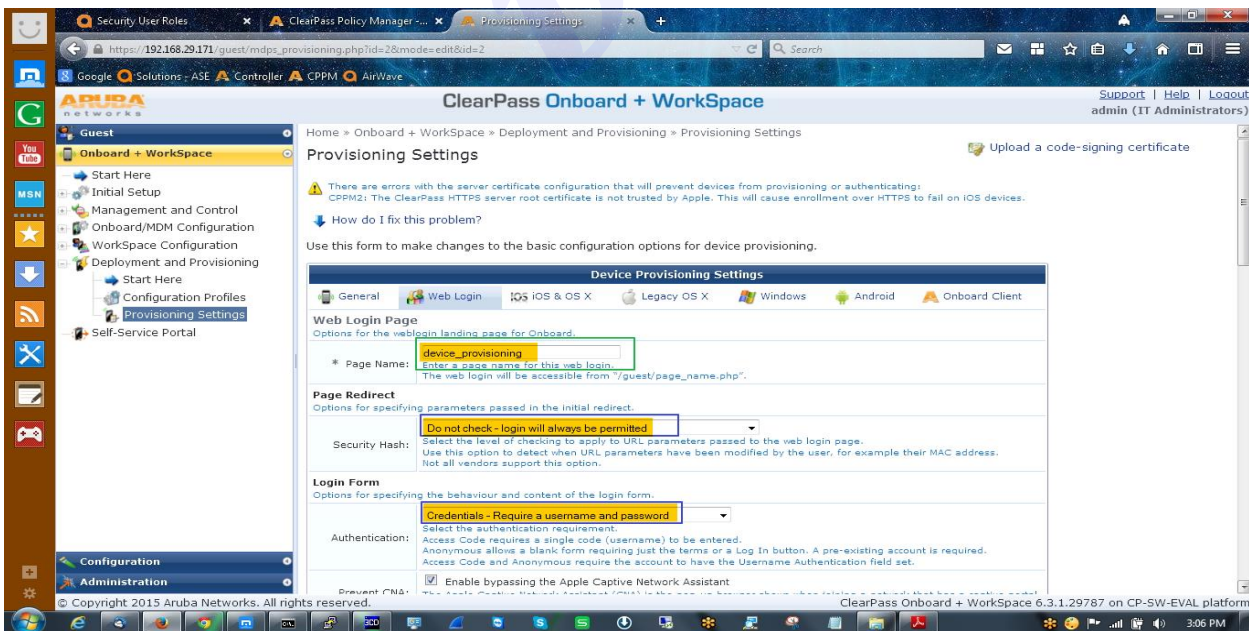


#### D. Follow this path Home » Onboard + Workspace » Deployment and Provisioning » Provisioning Settings

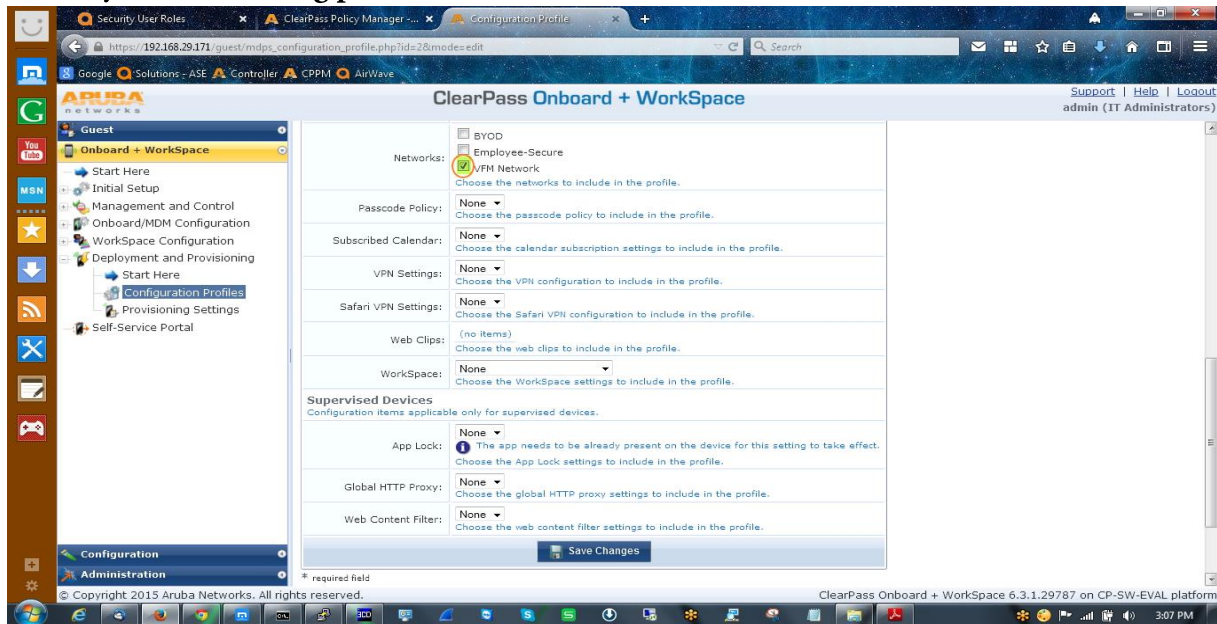
Careful about page name, because this name will be your captive portal log in page.

In here it is device provisioning, so the redirection page is

[http://192.168.29.171/guest/device\\_provisioning.php](http://192.168.29.171/guest/device_provisioning.php)

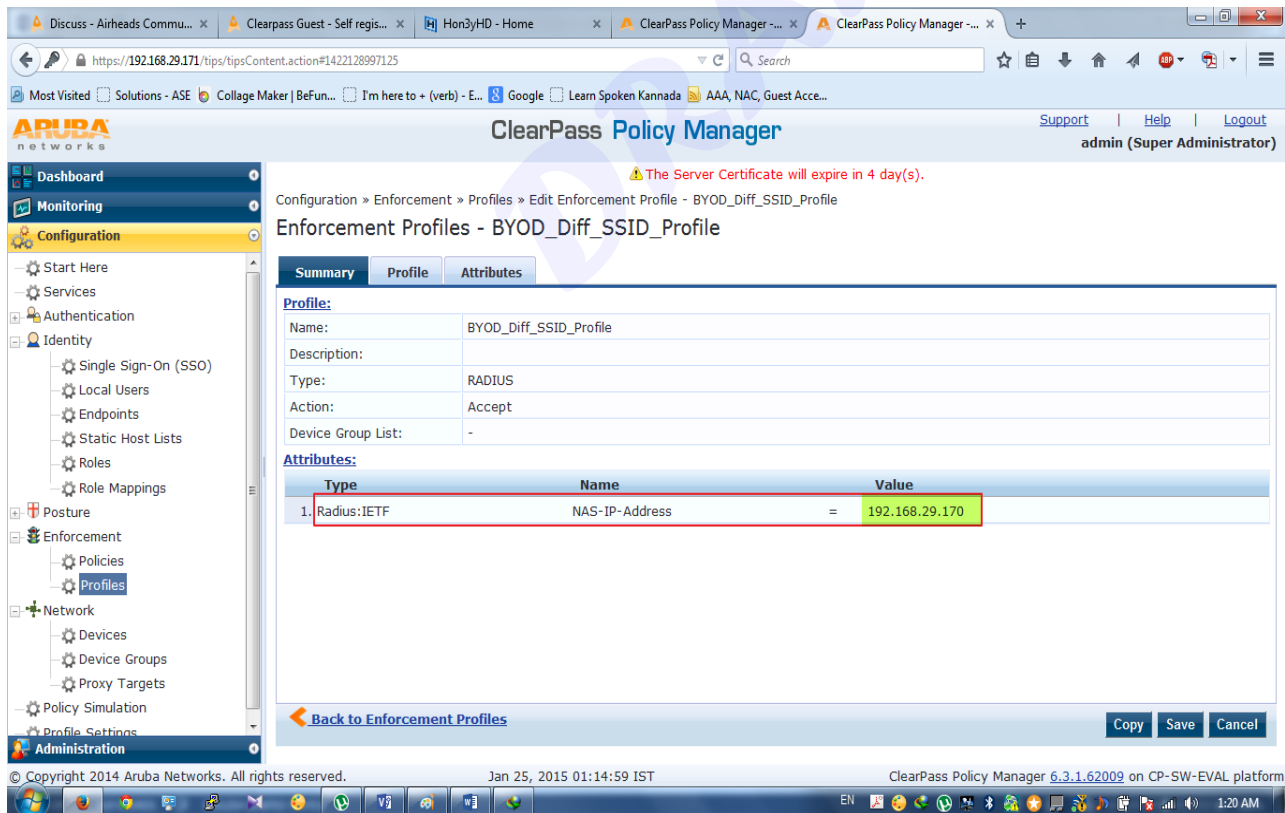


**E. Go to Home » Onboard + Workspace » Deployment and Provisioning » Configuration Profiles and choose you Provisioning profile.**



**F. Open Configuration » Enforcement » Profiles »**

**Here I'll configure one enforcement profile.**



**Now go to Configuration » Enforcement » Policies » to configure an enforcement policy & configure two authentication method, PAP & EAP-TLS.**



Discuss - Airheads Commu... x Clearpass Guest - Self regis... x Hon3yHD - Home x ClearPass Policy Manager ~... x ClearPass Policy Manager ~... x

https://192.168.29.171/tips/tipsContent.action#1422129227768

Most Visited Solutions - ASE Collage Maker | BeFun... I'm here to + (verb) - E... Google Learn Spoken Kannada AAA, NAC, Guest Ace...

**ARUBA networks** ClearPass Policy Manager [Support](#) | [Help](#) | [Logout](#) admin (Super Administrator)

The Server Certificate will expire in 4 day(s).

Configuration » Enforcement » Policies » Edit - BYOD\_Diff\_SSID\_Policy

### Enforcement Policies - BYOD\_Diff\_SSID\_Policy

**Summary** Enforcement Rules

**Enforcement:**

Name:	BYOD_Diff_SSID_Policy	
Description:		
Enforcement Type:	RADIUS	
Default Profile:	Denyall	

**Rules:**

Rules Evaluation Algorithm: Evaluate all

Conditions	Actions
1. (Authentication:OuterMethod EQUALS PAP)	BYOD_Diff_SSID_Profile
2. (Authentication:OuterMethod EQUALS EAP-TLS)	BYOD_Diff_SSID_Profile
3. (Tips:Role EQUALS [Employee])	BYOD_Diff_SSID_Profile

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

© Copyright 2014 Aruba Networks. All rights reserved. Jan 25, 2015 01:18:37 IST ClearPass Policy Manager 6.3.1.62009 on CP-SW-EVAL platform

**G. Switch to Configuration » Identity » Local Users and assign the same role as assign in policy.**

ClearPass Policy Manager ~... x Provisioning Settings x Install Add-on x

https://192.168.29.171/tips/tipsContent.action#1422035767719

Most Visited Solutions - ASE Facebook Cover | Alice ... Collage Maker | BeFun... I'm here to + (verb) - E... Google Live Match Video, Vide... Exodus Gods And King... Learn Spoken Kannada

**ARUBA networks** ClearPass Policy Manager [Support](#) | [Help](#) | [Logout](#) admin (Super Administrator)

Configuration » Identity » Local Users

### Edit Local User

User ID: suman  
Name: suman sinha  
Password: .....  
Verify Password: .....  
Enable User ☒ (Check to enable local user)  
Role: [Employee]  
access

**Attributes**

Attribute	Value
1. Click to add...	

[Save](#) [Cancel](#)

[Add](#) [Import](#) [Export All](#)

Show 10 records

Status	
read_Write_role	Enabled
_role	Enabled
uper_admin_access	Enabled
)	Enabled

[Export](#) [Delete](#)

https://192.168.29.171/tips/tipsContent.action# rights reserved. Jan 23, 2015 23:20:48 IST ClearPass Policy Manager 6.3.1.62009 on CP-SW-EVAL platform

**H. Open Configuration » Services » and configure a service**

Configuration > Services > Edit - BYOD\_Diff\_SSID\_Service

Services - BYOD\_Diff\_SSID\_Service

Summary Service Authentication Roles Enforcement

**Service:**

Name: BYOD\_Diff\_SSID\_Service  
 Description: Aruba 802.1X Wireless Access Service  
 Type: Aruba 802.1X Wireless  
 Status: Enabled  
 Monitor Mode: Disabled  
 More Options: -

**Service Rule**

Match ANY of the following conditions:

Type	Name	Operator	Value
1. Radius:Aruba	Aruba-Essid-Name	CONTAINS	BYOD-A
2. Radius:Aruba	Aruba-Essid-Name	CONTAINS	BYOD-B
3. Radius:IETF	NAS-IP-Address	EQUALS	192.168.29.170
4. Connection	Src-IP-Address	EQUALS	127.0.0.1
5. Radius:IETF	NAS-IP-Address	EQUALS	127.0.0.1
6. Radius:IETF	Service-Type	EQUALS	Authorize-Only (17)

**Authentication:**

Authentication Methods: 1. [PAP]  
 2. [EAP TLS]  
 Authentication Sources: [Local User Repository]  
 Strip Username Rules: -

Back to Services Disable Copy Save Cancel

Copyright 2014 Aruba Networks. All rights reserved. Jan 23, 2015 15:02:43 IST ClearPass Policy Manager 6.3.1.62009 on CP-SW-EVAL platform 3:08 PM

Here I added two SSID in service , so that the 2<sup>nd</sup> service is not required.

Check the configuration of rest of the service

Configuration > Services > Edit - BYOD\_Diff\_SSID\_Service

Services - BYOD\_Diff\_SSID\_Service

Summary Service Authentication Roles Enforcement

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

Authentication Sources: [Local User Repository] [Local SQL DB]  
 --Select to Add--

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

Back to Services Disable Copy Save Cancel

Copyright 2014 Aruba Networks. All rights reserved. Jan 23, 2015 15:02:52 IST ClearPass Policy Manager 6.3.1.62009 on CP-SW-EVAL platform 3:08 PM

Here I'm using only two authentication method because 1<sup>st</sup> time due to captive portal user will use PAP, & in meantime when using quickconnect app it'll complete another authentication using PAP, after that it will use EAP-TLS to complete onboarding.

Security User Roles | ClearPass Policy Manager | Configuration Profile

https://192.168.29.171/https/tipsContent.action#1422005886312

ClearPass Policy Manager

Support | Help | Logout  
admin (Super Administrator)

Configuration > Services > Edit - BYOD\_Diff\_SSID\_Service

Services - BYOD\_Diff\_SSID\_Service

Summary | Service | Authentication | Roles | Enforcement

Role Mapping Policy: Onboard Authorization Role Mapping [Modify](#) [Add new Role Mapping Policy](#)

Role Mapping Policy Details

Description: Maps RADIUS authorization attributes to a role for the Onboard device type

Default Role: [Employee]

Rules Evaluation Algorithm: first-applicable

Conditions	Role
1. (Radius:Aruba:Aruba-Mdps-Device-Name BEGINS_WITH Android)	[Onboard Android]
2. (Radius:Aruba:Aruba-Mdps-Device-Name BEGINS_WITH Windows)	[Onboard Windows]
3. OR (Radius:Aruba:Aruba-Mdps-Device-Product BEGINS_WITH iPad)	[Onboard iOS]
OR (Radius:Aruba:Aruba-Mdps-Device-Product BEGINS_WITH iPhone)	
4. (Radius:Aruba:Aruba-Mdps-Device-Product BEGINS_WITH iPod)	[Onboard Mac OS X]
OR (Radius:Aruba:Aruba-Mdps-Device-Product BEGINS_WITH MacBook)	

[Back to Services](#) [Disable](#) [Copy](#) [Save](#) [Cancel](#)

Copyright 2014 Aruba Networks. All rights reserved. Jan 23, 2015 15:02:57 IST ClearPass Policy Manager 6.3.1.62009 on CP-SW-EVAL platform 3:08 PM

Security User Roles | ClearPass Policy Manager | Configuration Profile

https://192.168.29.171/https/tipsContent.action#1422005886312

ClearPass Policy Manager

Support | Help | Logout  
admin (Super Administrator)

Configuration > Services > Edit - BYOD\_Diff\_SSID\_Service

Services - BYOD\_Diff\_SSID\_Service

Summary | Service | Authentication | Roles | Enforcement

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

Enforcement Policy: BYOD\_Diff\_SSID\_Policy [Modify](#) [Add new Enforcement Policy](#)

Enforcement Policy Details

Description:

Default Profile: Denyall

Rules Evaluation Algorithm: first-applicable

Conditions	Enforcement Profiles
1. (Authentication:OuterMethod EQUALS PAP)	BYOD_Diff_SSID_Profile
2. AND (Authentication:OuterMethod EQUALS EAP-TLS)	
(Tips:Role EQUALS [Employee])	BYOD_Diff_SSID_Profile

[Back to Services](#) [Disable](#) [Copy](#) [Save](#) [Cancel](#)

Copyright 2014 Aruba Networks. All rights reserved. Jan 23, 2015 15:03:03 IST ClearPass Policy Manager 6.3.1.62009 on CP-SW-EVAL platform 3:08 PM

1. Now log in to controller to configure WLAN profile.



Authentication Profiles | ClearPass Policy Manager | L2 Authentication | Portal Login

https://192.168.29.170:4343/screens/switch/config\_controller.html?mode=authprofiles

aruba MOBIILITY CONTROLLER | Aruba-3600

Dashboard Monitoring Configuration Diagnostics Maintenance Save Configuration

WIZARDS

- AP
- Controller
- Campus WLAN
- Remote AP
- WIP
- AirWave

NETWORK

- Controller
- VLANs
- Ports
- Cellular Profile
- IP

SECURITY

- Authentication
- Access Control

WIRELESS

- AP Configuration
- AP Installation

MANAGEMENT

- General
- Administration
- Certificates
- SNMP
- Logging
- Clock
- Guest Provisioning

Security > Authentication > Profiles

Servers AAA Profiles L2 Authentication L3 Authentication User Rules Advanced

AAA Profile > BYOD A-aaa\_prof

Initial role BYOD-A

MAC Authentication Default Role guest

802.1X Authentication Default Role Authenticated

Download Role from CPPM

L2 Authentication Fail Rules

IP Version	Source	Destination	Service/Application	Action	Log	Mirror	Queue
IPv4	user	CPPM	svc-http	permit			Low
IPv4	user	CPPM	svc-https	permit			Low
IPv4	user	any	svc-http	dst-nat 8080			Low
IPv4	user	any	svc-https	dst-nat 8081			Low
IPv4	user	any	svc-http-proxy1	dst-nat 8088			Low
IPv4	user	any	svc-http-proxy2	dst-nat 8088			Low
IPv4	user	any	svc-http-proxy3	dst-nat 8088			Low

User idle timeout

RADIUS Interim Acco

User derivation rules

Wired to Wireless Ro

SIP authentication ro

Device Type Classific

Enforce DHCP

PAN Firewall Integration

logon control [default]

captive portal

captive portal role

Authentication Profiles | ClearPass Policy Manager | Configuration Profile

https://192.168.29.170:4343/screens/switch/config\_controller.html?mode=authprofiles

aruba MOBIILITY CONTROLLER | Aruba-3600

Dashboard Monitoring Configuration Diagnostics Maintenance Save Configuration

WIZARDS

- AP
- Controller
- Campus WLAN
- Remote AP
- WIP
- AirWave

NETWORK

- Controller
- VLANs
- Ports
- Cellular Profile
- IP

SECURITY

- Authentication
- Access Control

WIRELESS

- AP Configuration
- AP Installation

MANAGEMENT

- General
- Administration
- Certificates
- SNMP
- Logging
- Clock
- Guest Provisioning

Security > Authentication > Profiles

Servers AAA Profiles L2 Authentication L3 Authentication User Rules Advanced

AAA Profile > BYOD B-aaa\_prof

Initial role BYODlogon

MAC Authentication Default Role guest

802.1X Authentication Default Role Authenticated

Download Role from CPPM

L2 Authentication Fail Through

Multiple Server Accounting

User idle timeout

RADIUS Interim Accounting

User derivation rules

Wired to Wireless Roaming

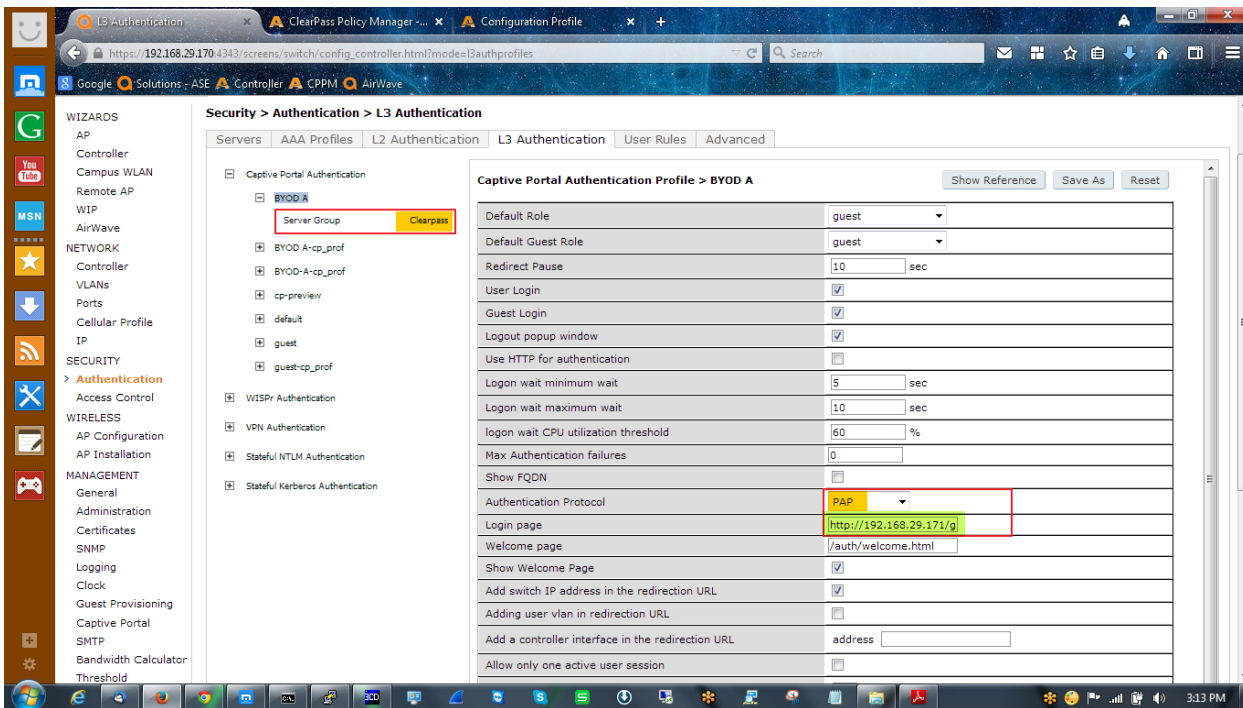
SIP authentication role

Device Type Classification

Enforce DHCP

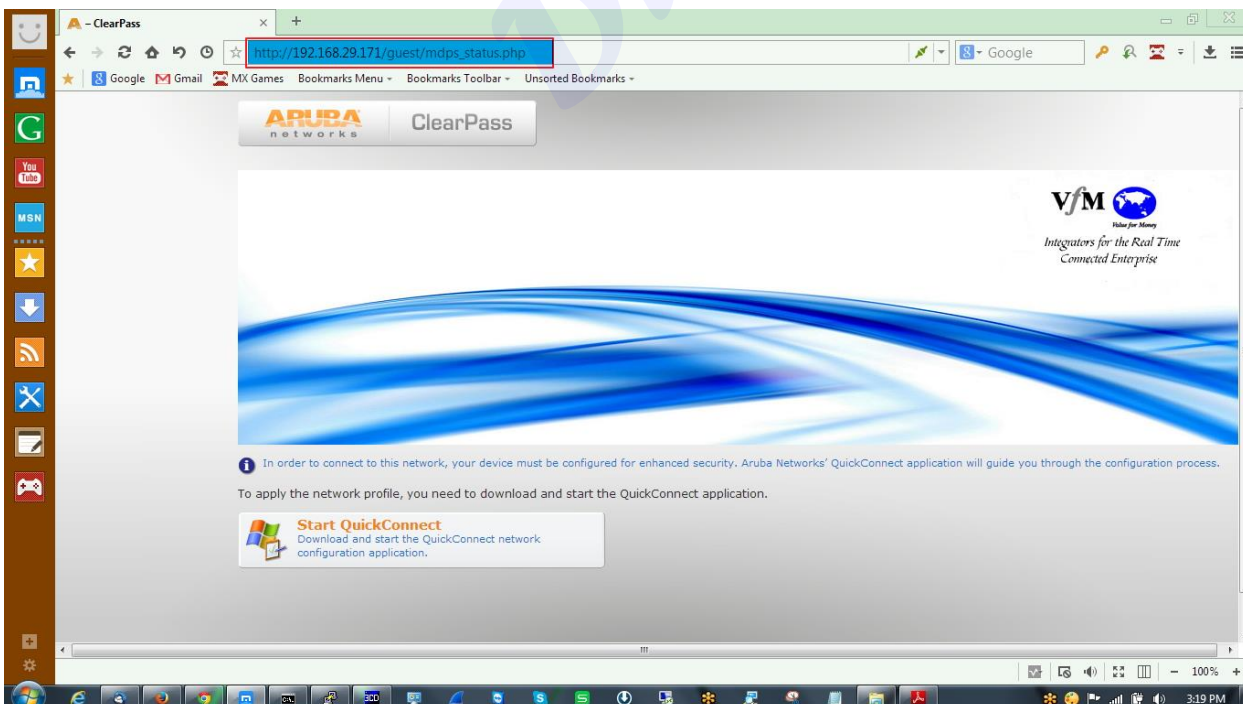
PAN Firewall Integration



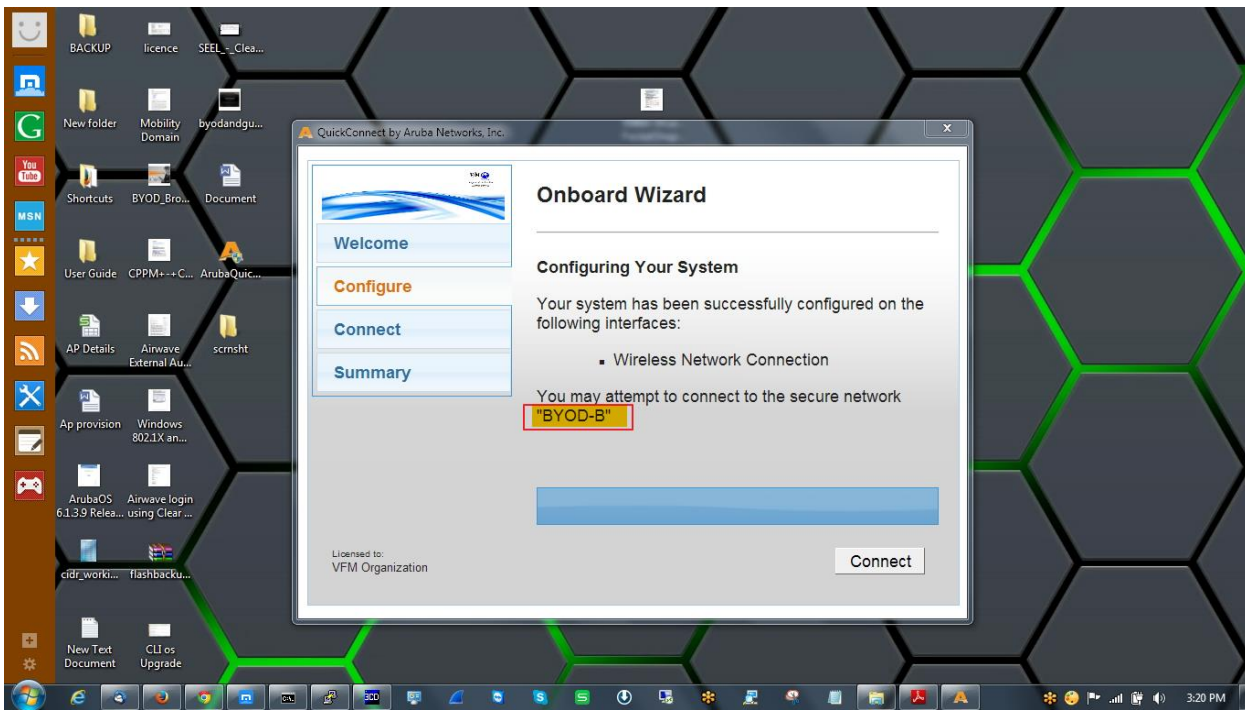


## THAT'S ALL, NOW I'LL CHECK OUTPUT

At first I'll connect to BYOD-A [open network]. You can see here my credential is correct so it gives me the quickconnect download link.



Here it's showing me warning that, you may attempt to connect to the secure network BYOD-B, that's what I want.



#	Server	Source	Username	Service	Login Status	Request Timestamp
1.	192.168.29.171	RADIUS	suman	BYOD_Diff_SSID_Servi	ACCEPT	2015/01/23 15:15:21
2.	192.168.29.171	RADIUS	suman	BYOD_Diff_SSID_Servi	ACCEPT	2015/01/23 15:13:49
3.	192.168.29.171	RADIUS	suman	BYOD_Diff_SSID_Servi	ACCEPT	2015/01/23 15:13:25
4.	192.168.29.171	RADIUS	byod	BYOD_Diff_SSID_Servi	REJECT	2015/01/23 15:13:14
5.	192.168.29.171	RADIUS	suman	BYOD_Diff_SSID_Servi	ACCEPT	2015/01/23 15:08:59
6.	192.168.29.171	RADIUS	suman	BYOD_Diff_SSID_Servi	ACCEPT	2015/01/23 15:08:53
7.	192.168.29.171	RADIUS	suman	BYOD_Diff_SSID_Servi	ACCEPT	2015/01/23 15:08:43
8.	192.168.29.171	RADIUS	suman	BYOD_Diff_SSID_Servi	ACCEPT	2015/01/23 14:58:12
9.	192.168.29.171	RADIUS	suman	BYOD_Diff_SSID_Servi	ACCEPT	2015/01/23 14:58:07
10.	192.168.29.171	RADIUS	suman	BYOD_Diff_SSID_Servi	ACCEPT	2015/01/23 14:57:57
11.	192.168.29.171	RADIUS	suman	Onboard Authorizatio	REJECT	2015/01/23 14:55:28
12.	192.168.29.171	RADIUS	suman	BYOD_Diff_SSID_Servi	ACCEPT	2015/01/23 14:55:20
13.	192.168.29.171	RADIUS	suman	Onboard Authorizatio	REJECT	2015/01/23 14:53:56
14.	192.168.29.171	RADIUS	suman	Onboard Authorizatio	REJECT	2015/01/23 14:53:37
15.	192.168.29.171	RADIUS	suman	Onboard Authorizatio	REJECT	2015/01/23 14:53:17
16.	192.168.29.171	RADIUS	suman	Onboard Authorizatio	REJECT	2015/01/23 14:53:06
17.	192.168.29.171	RADIUS	suman	BYOD_Diff_SSID_Servi	ACCEPT	2015/01/23 14:48:21
18.	192.168.29.171	RADIUS	suman	BYOD_Diff_SSID_Servi	ACCEPT	2015/01/23 14:45:53

*Thank you*