ONBOARD USING DIFFERENT SSID

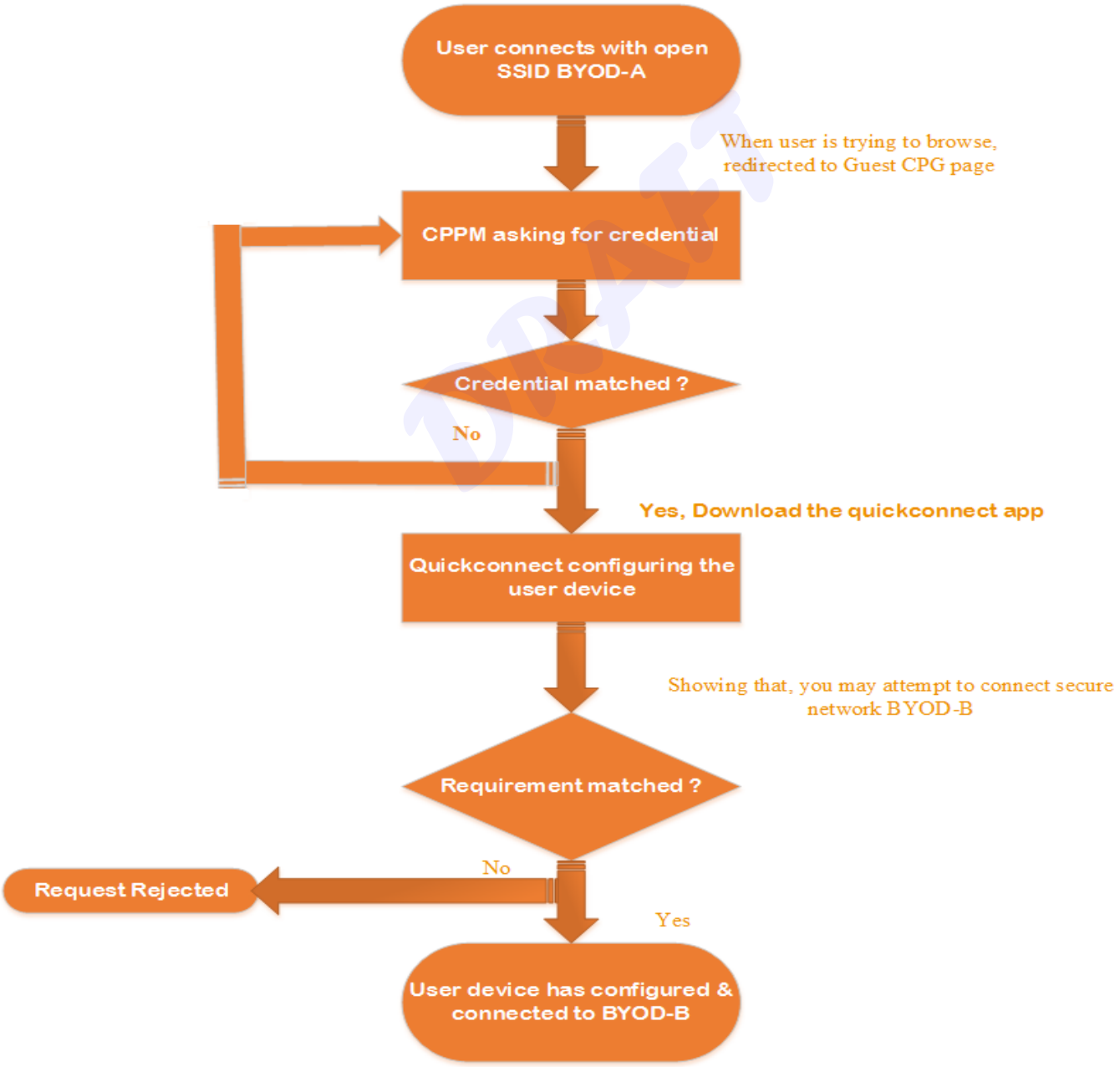
Overview:

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 2nd SSID.

SSID used here

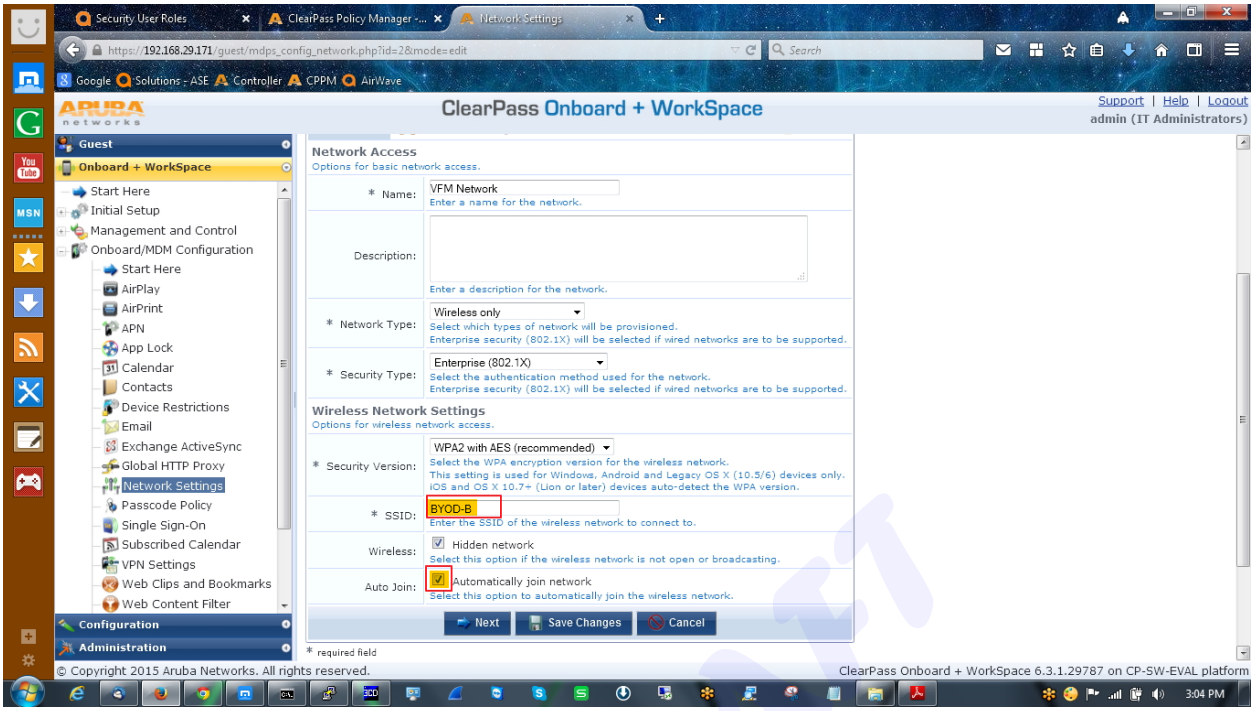
1. BYOD-A [Open network]
2. BYOD-B [Secured with WPA2-AES]

Flowchart:

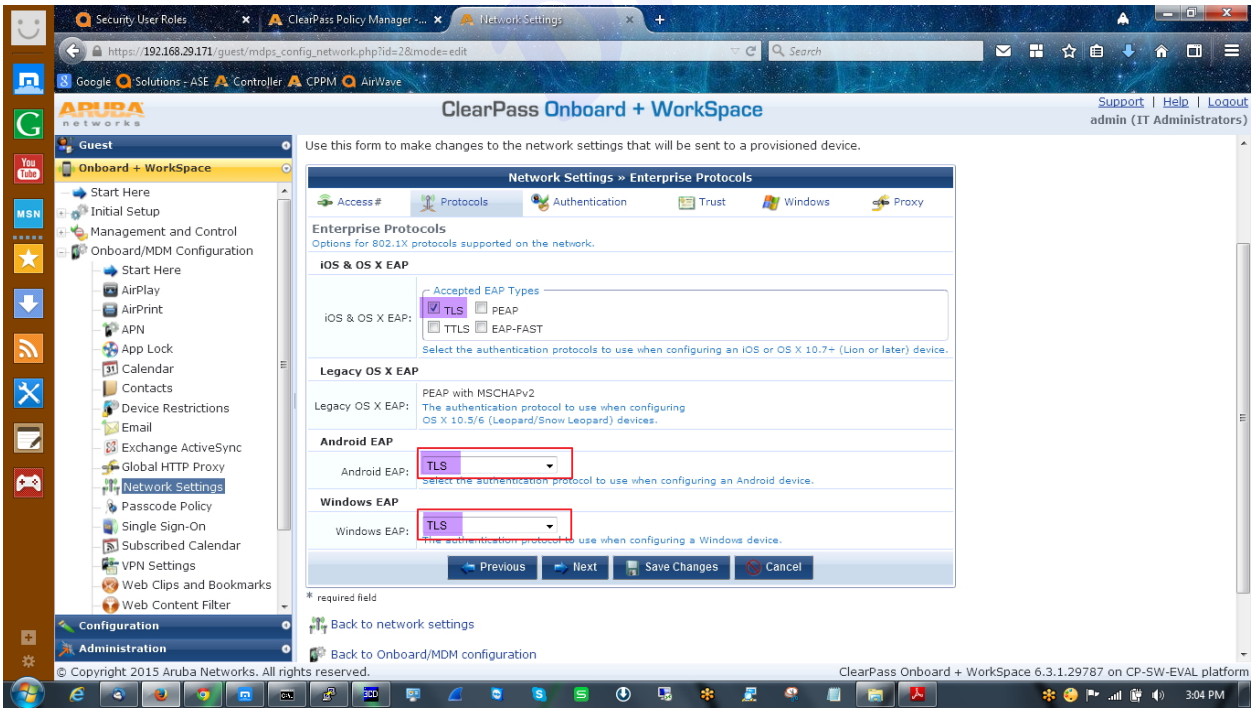


A. **Log in to the CPPM and go to Home » Onboard + Workspace » Onboard/MDM Configuration » Network Settings**

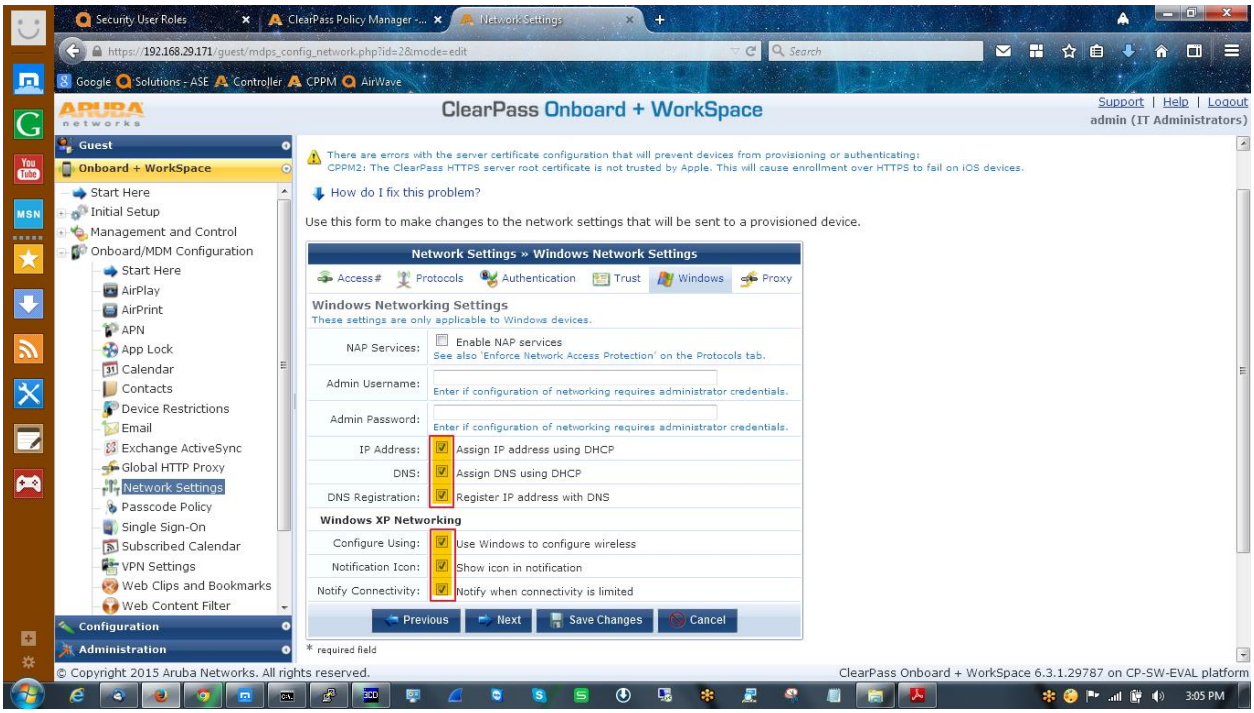
Put the name of the 2nd ssid & select 'automatically join network'



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



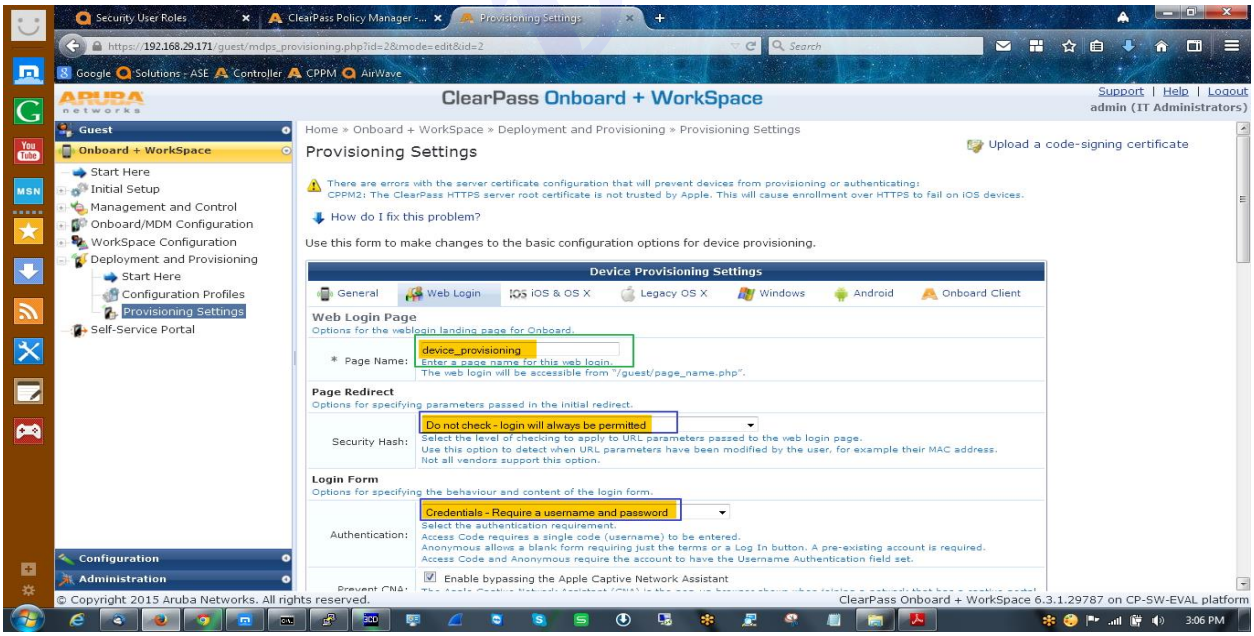
C. **Open the windows tab**



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.

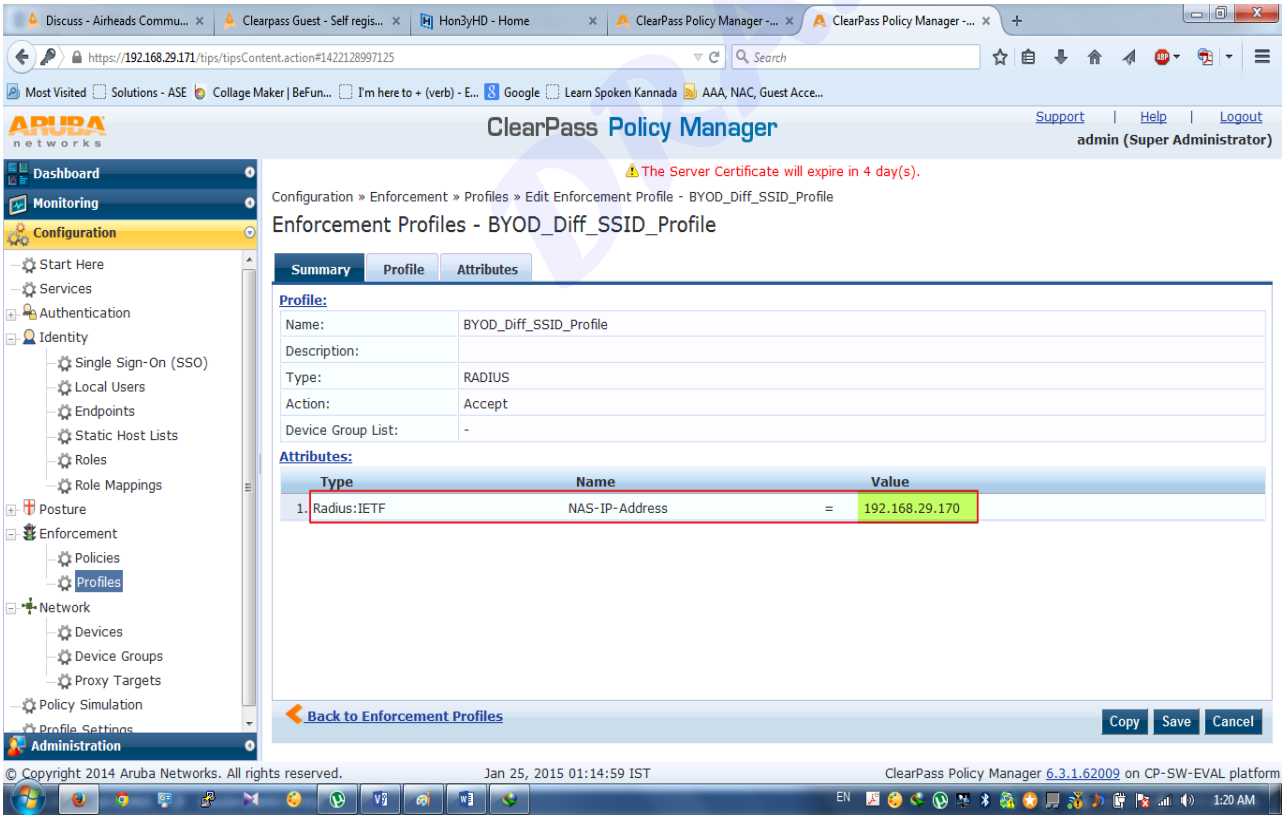
In here it is device provisioning, so the redirection page is
http://192.168.29.171/guest/device_provisioning.php



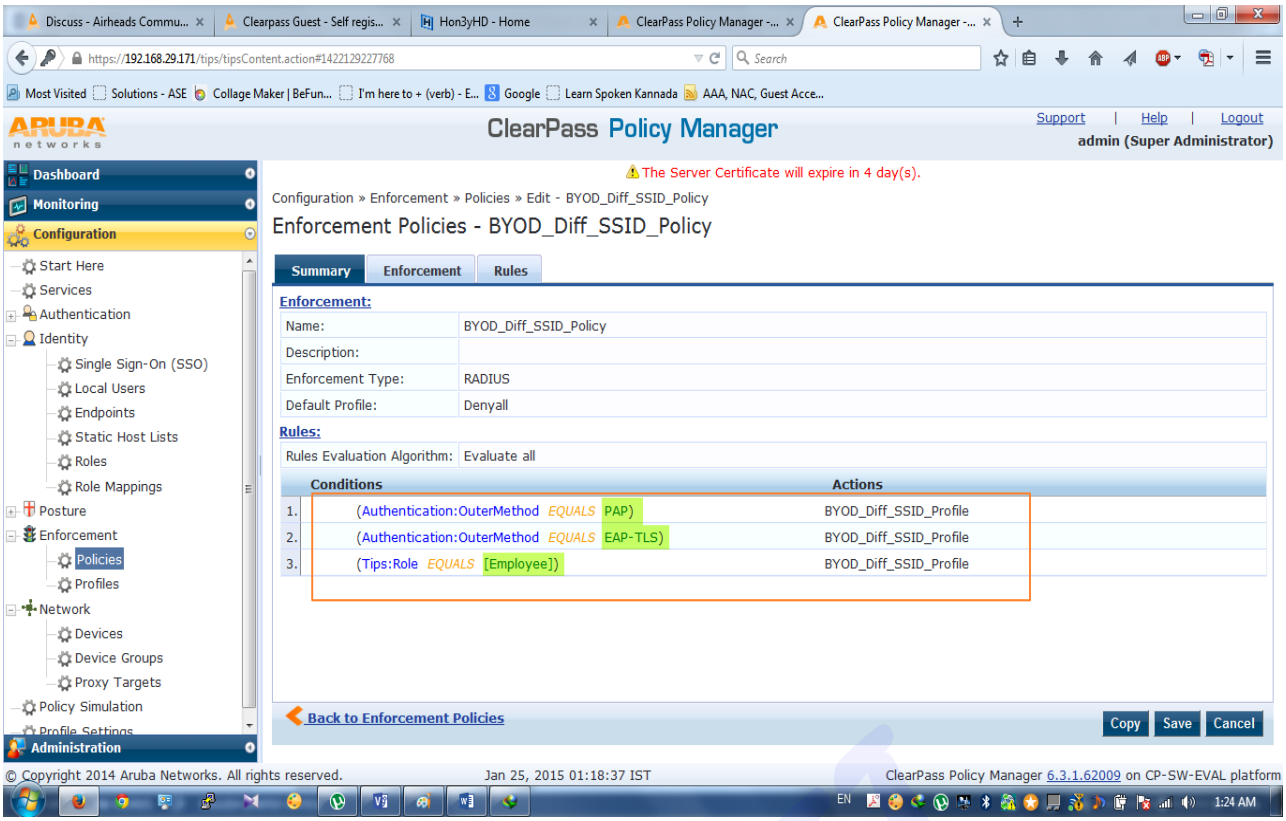
E. Go to Home » Onboard + Workspace » Deployment and Provisioning » Configuration Profiles and choose you Provisioning profile.

F. Open Configuration » Enforcement » Profiles »

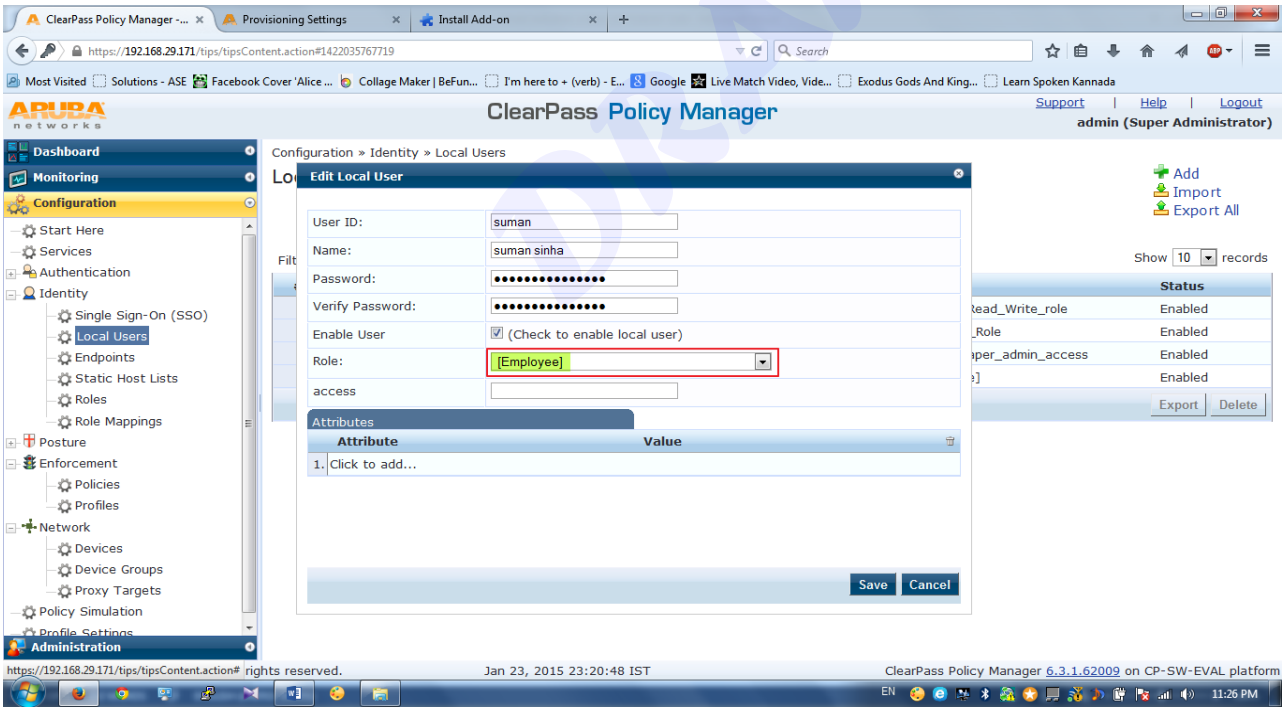
Here I'll configure one enforcement profile.



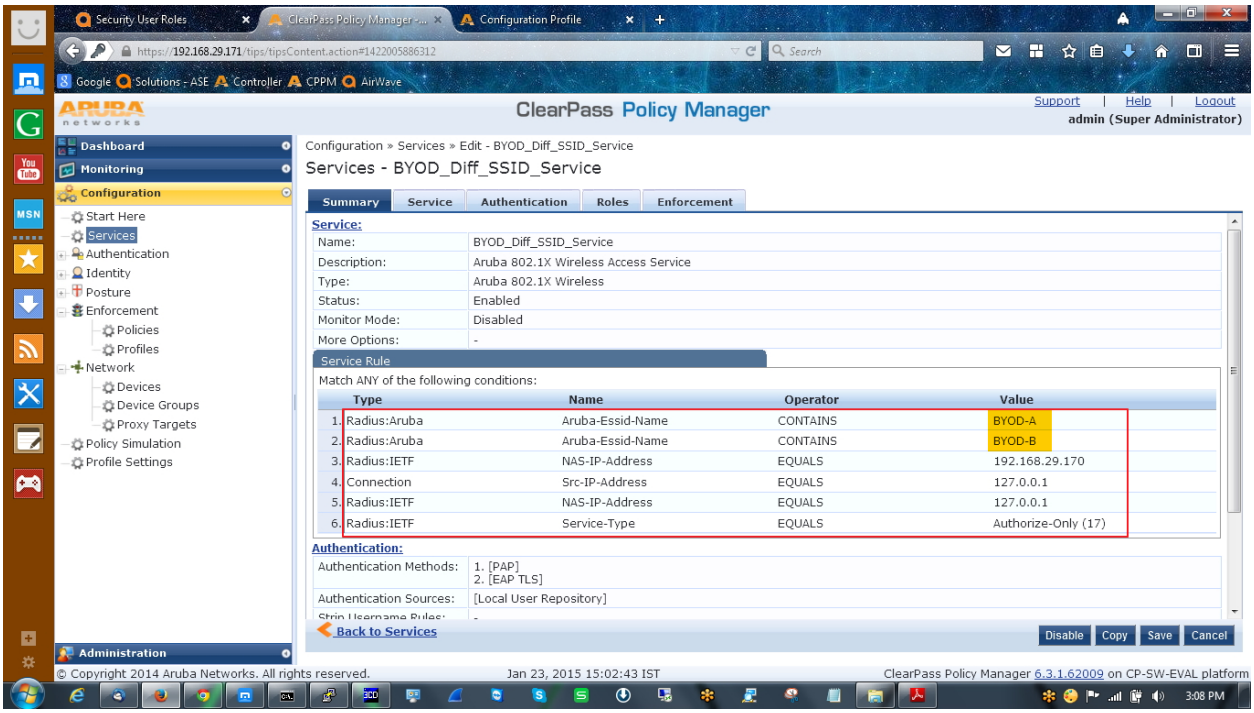
Now go to Configuration » Enforcement » Policies » to configure an enforcement policy & configure two authentication method, PAP & EAP-TLS.



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

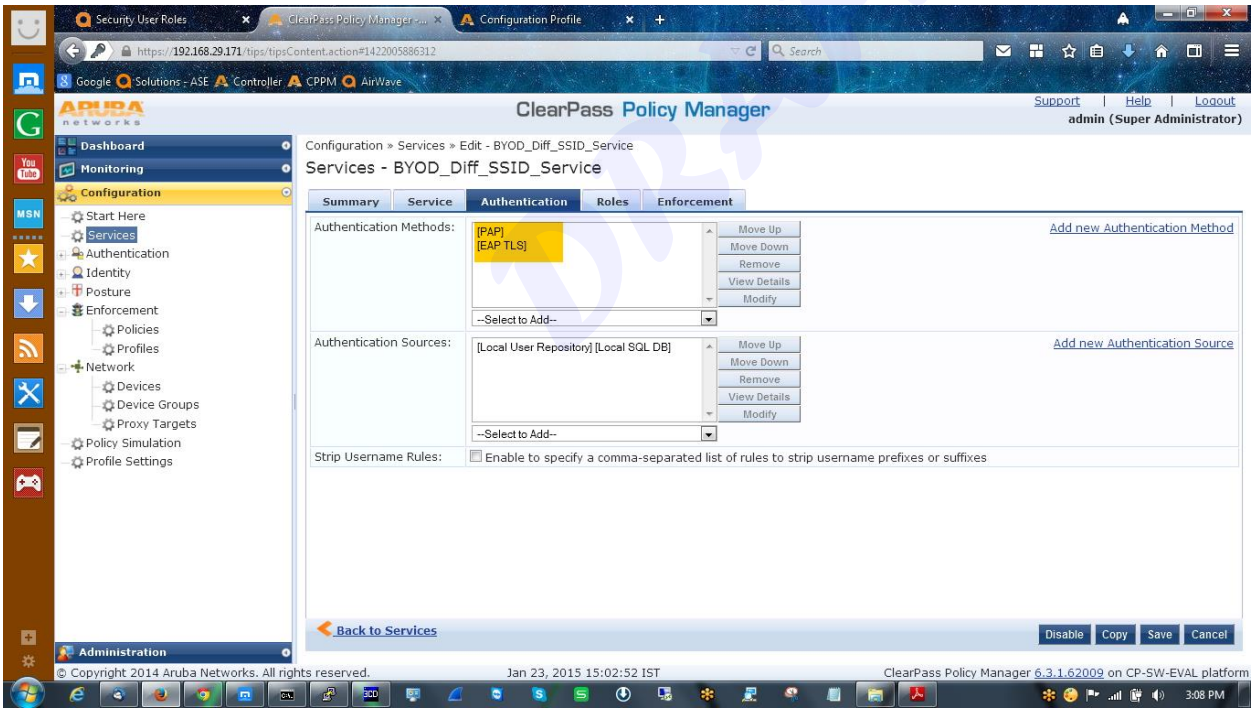


H. Open Configuration » Services » and configure a service

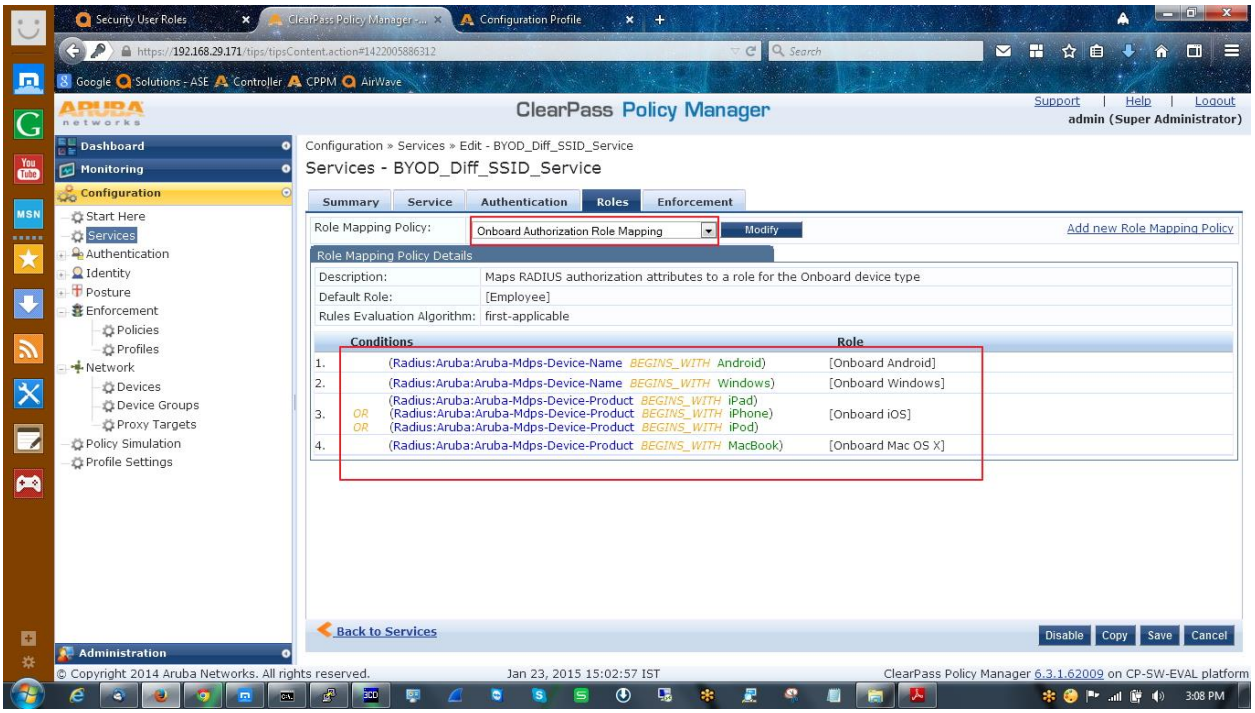


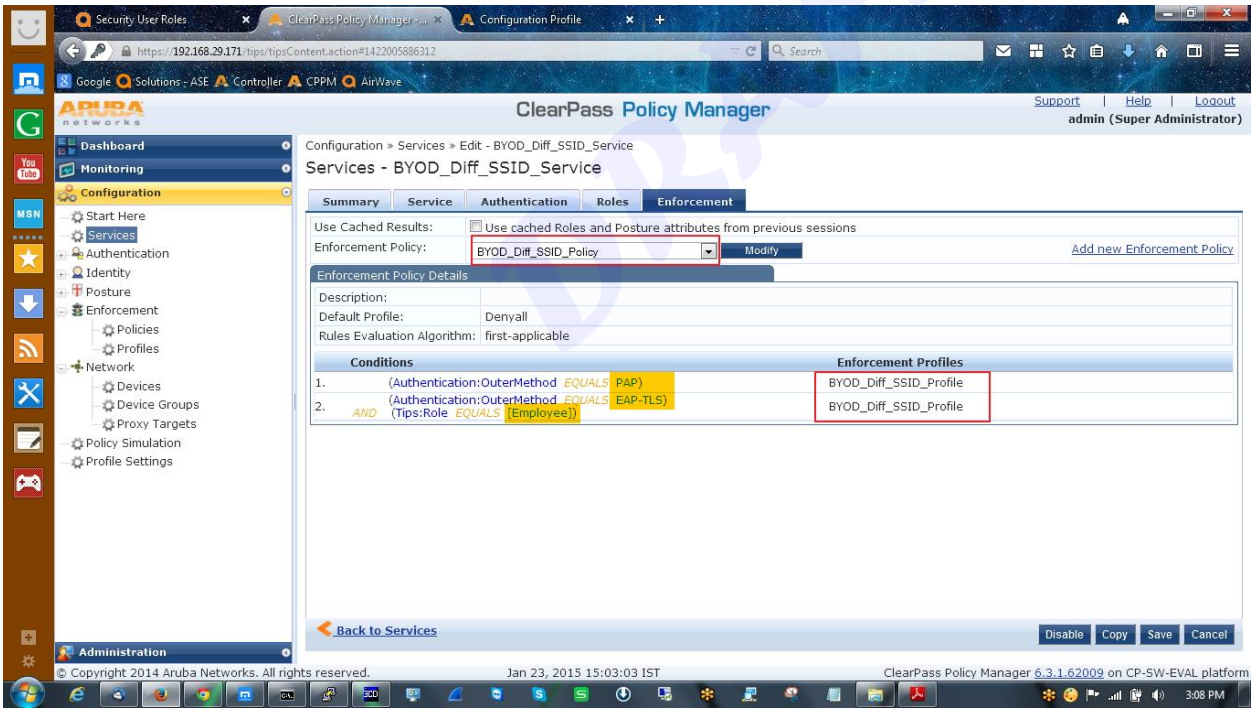
Here I added two SSID in service , so that the 2nd service is not required.

Check the configuration of rest of the service

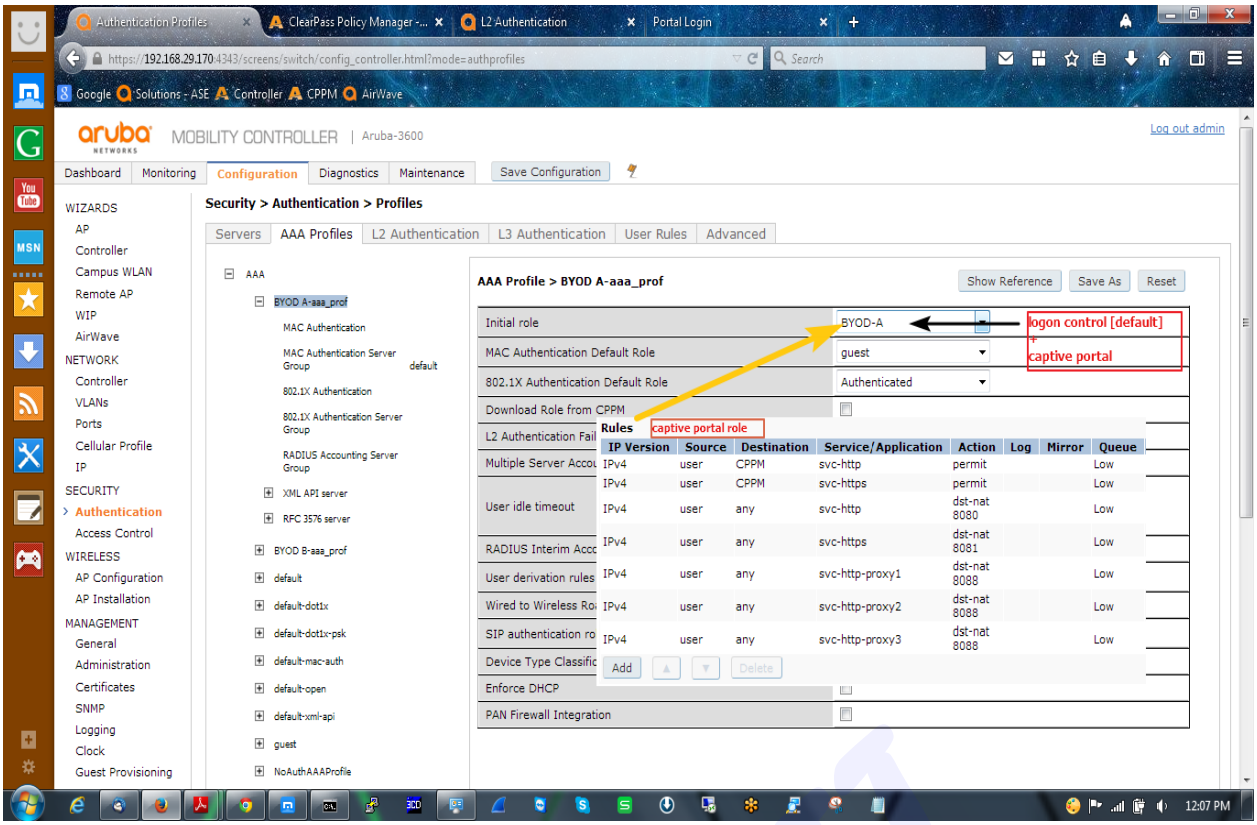


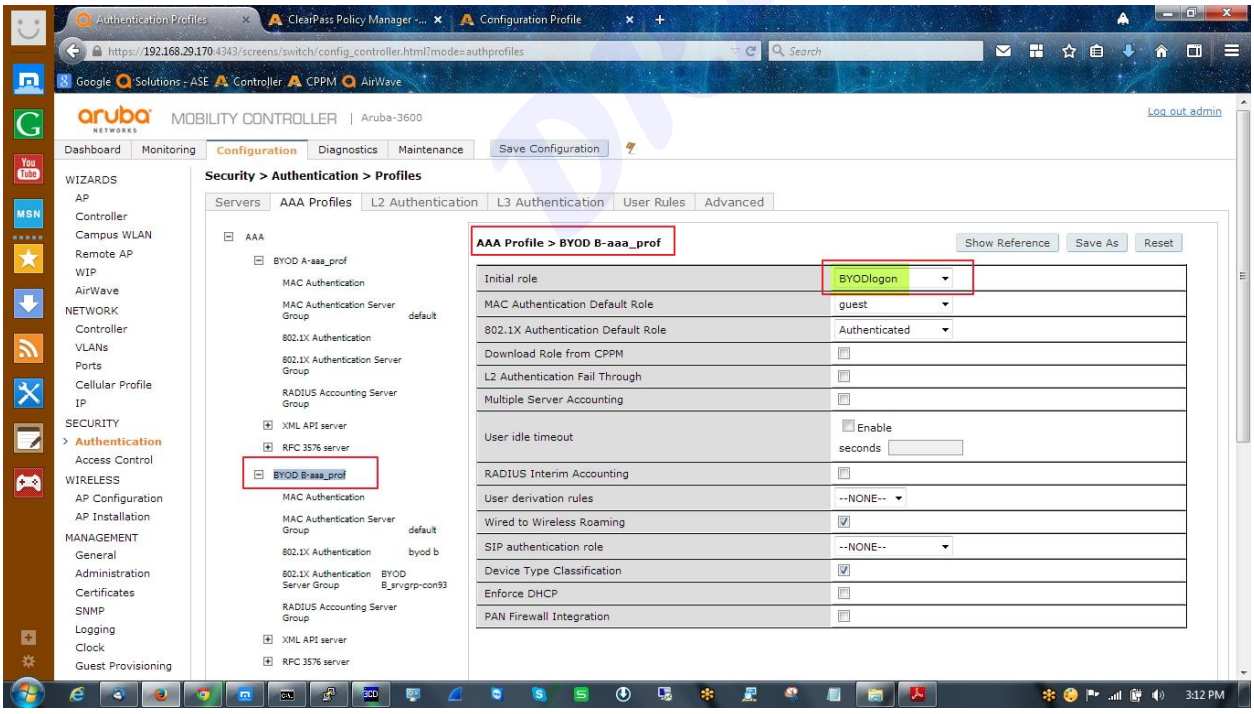
Here I'm using only two authentication method because 1st time due to captive portal user will use PAP, & in meantime when using quickconnect app it'll complete another authentication using PAP, after that it will use EAP-TLS to complete onboarding.

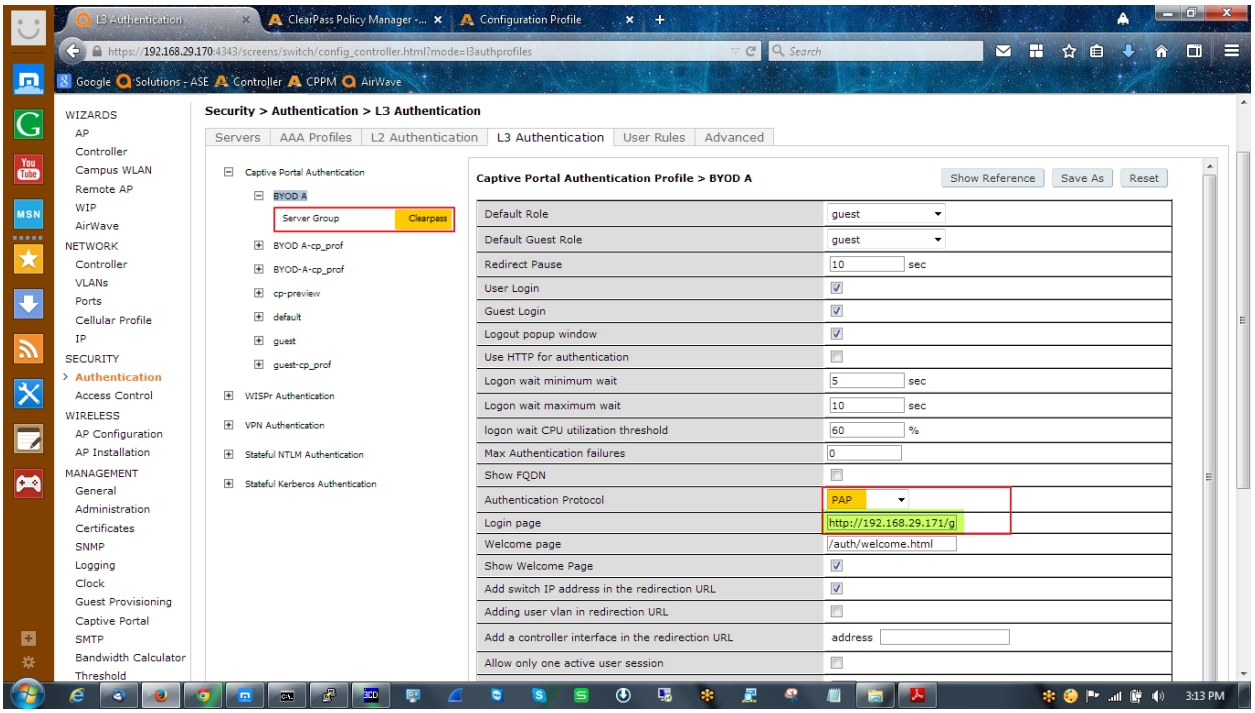




1. **Now log in to controller to configure WLAN profile.**

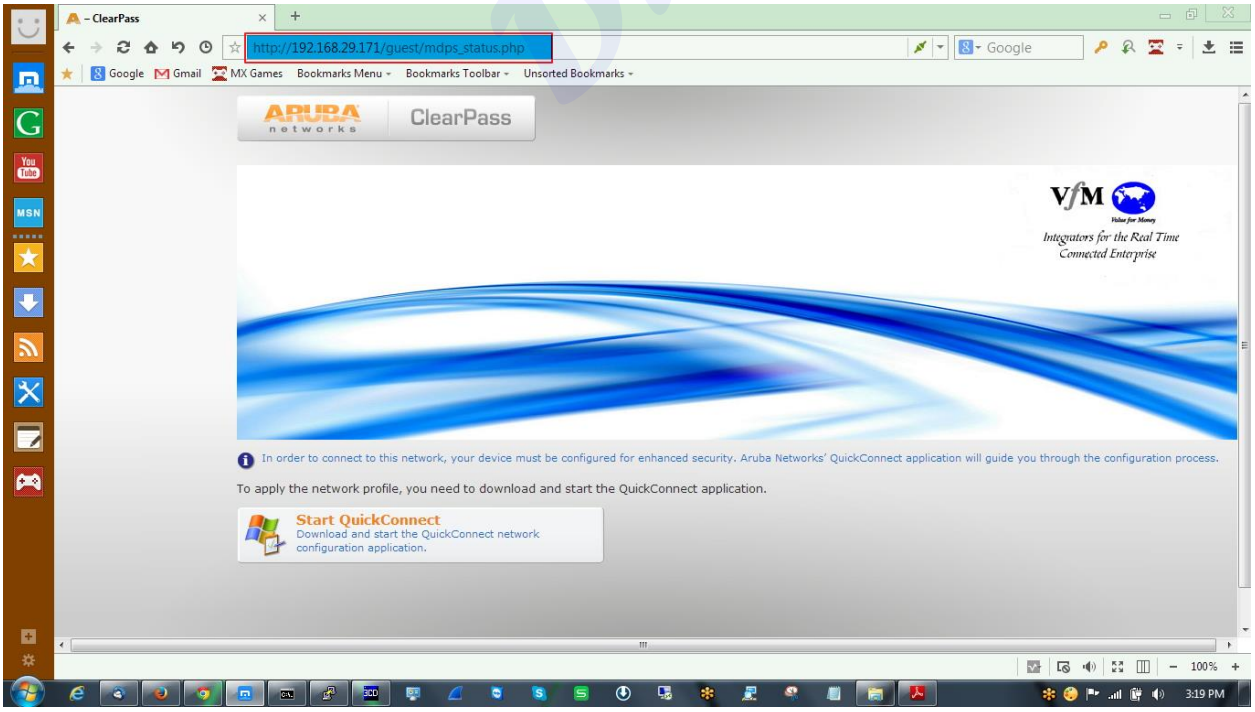

Authentication Profiles
ClearPass Policy Manager -...
L2 Authentication
Portal Login
https://192.168.29.170:4343/screens/switch/config_controller.html?mode=authprofiles
MOBILITY CONTROLLER | Aruba-3600
Log out admin
Dashboard
Monitoring
Configuration
Diagnostics
Maintenance
Save Configuration
Security > Authentication > Profiles
Servers
AAA Profiles
L2 Authentication
L3 Authentication
User Rules
Advanced
AAA Profile > BYOD A-aaa_prof
Show Reference
Save As
Reset
Initial role
BYOD-A
logon control [default]
+
captive portal
MAC Authentication Default Role
guest
802.1X Authentication Default Role
Authenticated
Download Role from CPPM
Rules
captive portal role
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
Add
Delete
Enforce DHCP
PAN Firewall Integration
12:07 PM


Authentication Profiles
ClearPass Policy Manager -...
Configuration Profile
https://192.168.29.170:4343/screens/switch/config_controller.html?mode=authprofiles
MOBILITY CONTROLLER | Aruba-3600
Log out admin
Dashboard
Monitoring
Configuration
Diagnostics
Maintenance
Save Configuration
Security > Authentication > Profiles
Servers
AAA Profiles
L2 Authentication
L3 Authentication
User Rules
Advanced
AAA Profile > BYOD B-aaa_prof
Show Reference
Save As
Reset
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
Enable
seconds
RADIUS Interim Accounting
User derivation rules
--NONE--
Wired to Wireless Roaming
SIP authentication role
--NONE--
Device Type Classification
Enforce DHCP
PAN Firewall Integration
BYOD B-aaa_prof
3:12 PM

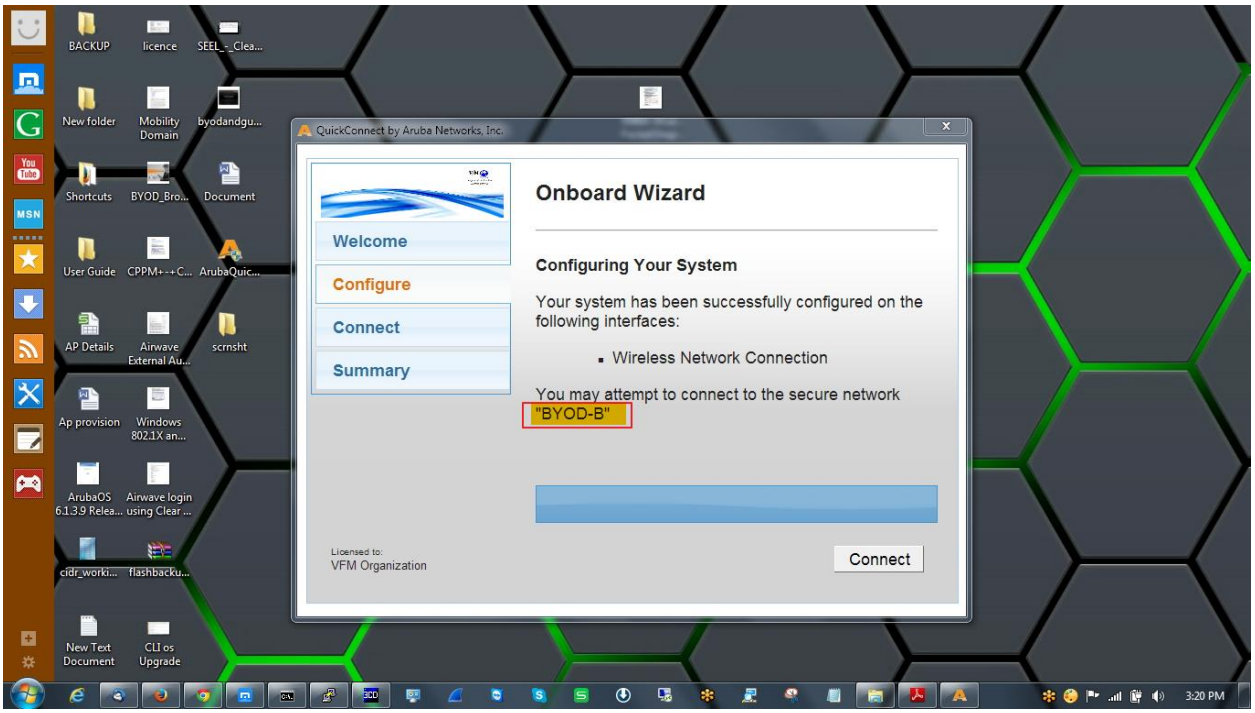


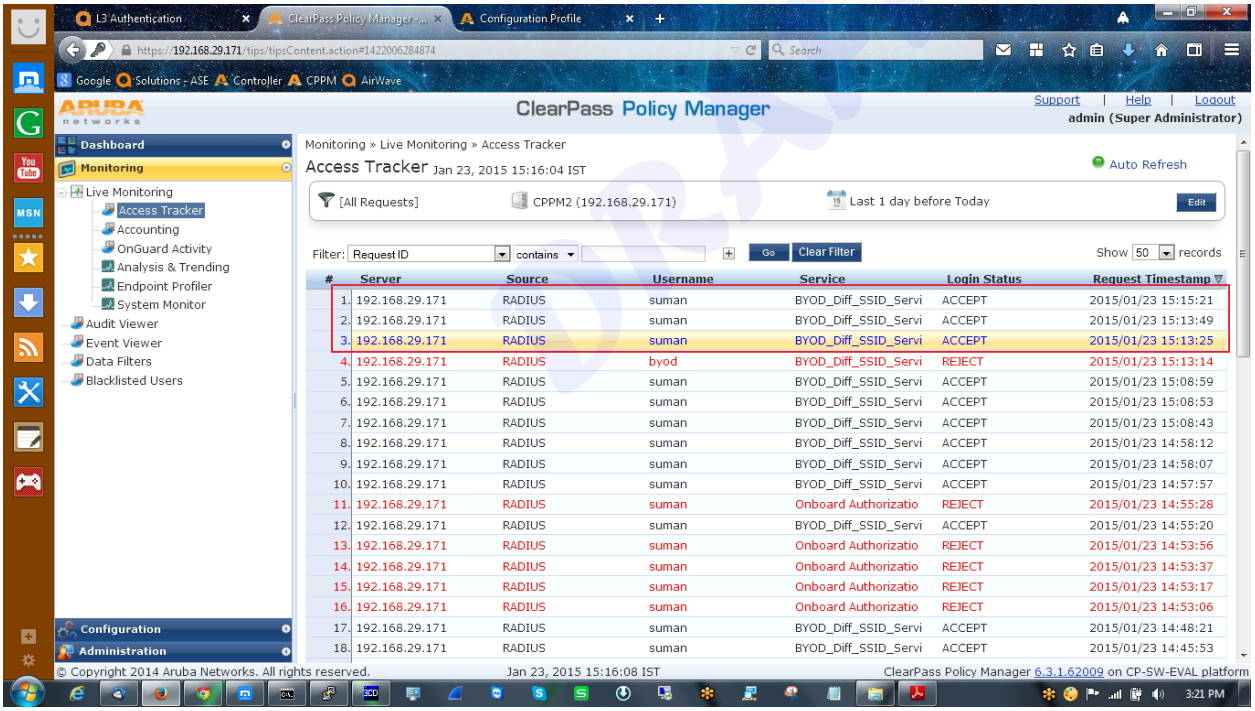
THAT'S ALL, NOW I'LL CHECK OUTPUT

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.


QuickConnect by Aruba Networks, Inc.
Onboard Wizard
Welcome
Configure
Connect
Summary
Configuring Your System
Your system has been successfully configured on the following interfaces:
Wireless Network Connection
You may attempt to connect to the secure network
"BYOD-B"
Licensed to:
VFM Organization
Connect


ClearPass Policy Manager
Access Tracker Jan 23, 2015 15:16:04 IST
Auto Refresh
Monitoring » Live Monitoring » Access Tracker
admin (Super Administrator)
Support | Help | Logout
Dashboard
Monitoring
Live Monitoring
Access Tracker
Accounting
OnGuard Activity
Analysis & Trending
Endpoint Profiler
System Monitor
Audit Viewer
Event Viewer
Data Filters
Blacklisted Users
Configuration
Administration
[All Requests]
CPPM2 (192.168.29.171)
Last 1 day before Today
Edit
Filter: Request ID contains Go Clear Filter
Show 50 records
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
© Copyright 2014 Aruba Networks. All rights reserved.
Jan 23, 2015 15:16:08 IST
ClearPass Policy Manager 6.3.1.62009 on CP-SW-EVAL platform

Thank you