APJ Workshop Lab Exercises – 2013Q4

by Aruba Networks

Table of Content

0. Initial Setup

Controller + AP

1. Basic deployment: a) Controller Initial setup & b) AP Provisioning
2. Complete Access-list
3. Complete User Roles
4. Complete AAA profiles
5. AAA Captive Portal profiles
6. VAP and SSID Profiles

ClearPass

1. Load ClearPass v6.1 VM
   1.1. Deploy ClearPass v6.1 OVF
   1.2. Turn-on Pre-Built Windows Server 2008 VM
2. Join AD Domain

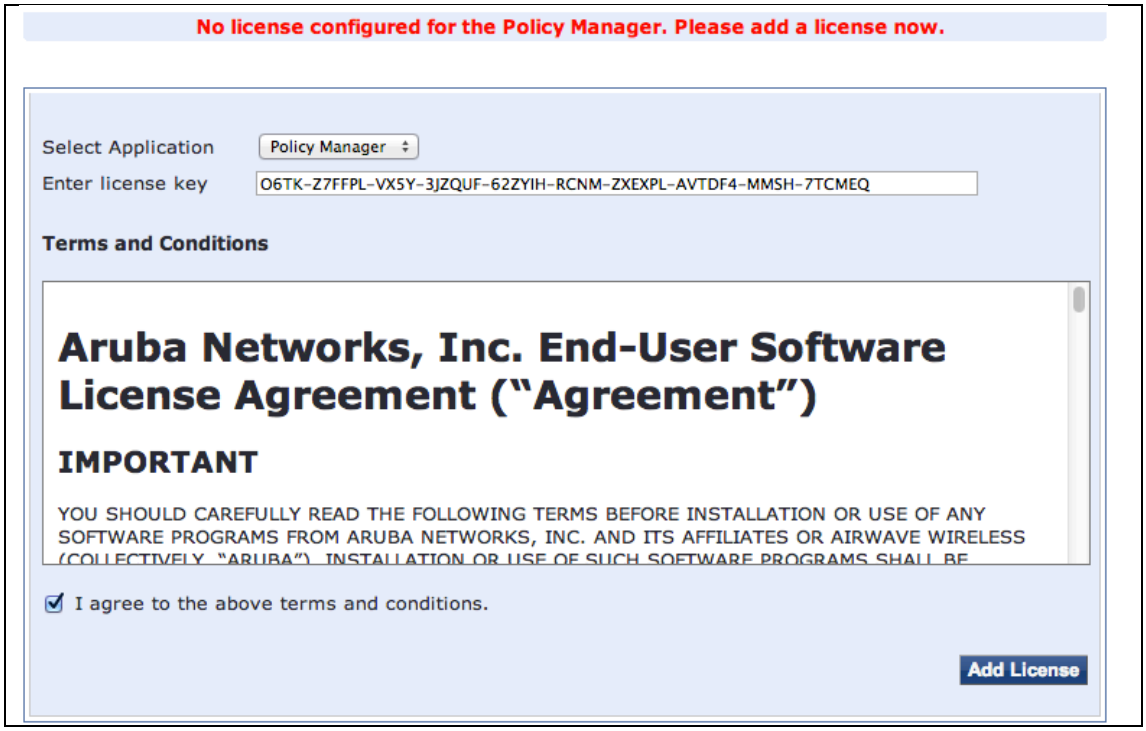
CPPM Initial setup
1. Login as "appadmin" & password "eTIPS123" -- (default password)
2. After login to CPPM system, System Configuration Wizard will start
3. Enter below information:
3.1. Enter hostname: cppmXX.workshop
3.2. Enter Management Port IP Address: 192.168.10.2XX
3.3. Enter Management Port Subnet Mask: 255.255.255.0
3.4. Enter Management Port Gateway: 192.168.10.254
3.5. Enter Data Port IP Address: *<Press Enter for skip>*
3.6. Enter Primary DNS: 192.168.10.30 (*AD Domain Server*)
3.7. Enter Secondary DNS: 192.168.10.254
3.8. New Password: aruba123
3.9. Confirm Password: aruba123
3.10. Do you wat to configure system date time information? [y|n]: Y
3.11. Enter "1" for Set date time manually
3.12. Follow instruction to enter System Date & Time
3.13. Enter "Y" for configure the timezone
3.14. Enter "5" for Asia, and "13" for Hong Kong
3.15. Enter "1" for confirm System Date & Time configuration
3.16. Enter "Y" for confirm System Configuration
3.17. Initial setup complete and CPPM will restart

Note:
For disable “Data” Port, type as below command at CLI:

```
network reset data
```

4. Access WebUI, and CPPM will asking for license. Enter Eval License:

O6TK-Z7FFPL-VX5Y-3JZQUF-62ZYIH-RCNM-ZXEXPL-AVTDF4-MMSH-7TCMEQ



Check the checkbox of "I agree to the above terms and conditions." & Click "Add License" button.

You will have 90 day(s) evaluation period

5. Login as "admin" and password "eTIPS123" -- default password
6. Goto ClearPass Policy Manger > Administration > Agents and Software Updates > Software Updates
6.1. Enter the Subscription ID:

m2xp3v-m5p2dy-5z3ysx-kpd8yh-v0mbn3

& click "Save" button

0.1. Install CPPM Patch - CLI

1. login to CPPM CLI, either using "putty" or "ssh"
1.1 e.g.: ssh appadmin@192.168.10.2XX & enter password: aruba123
2. at the CLI, check update patch installed on the system; type "system update -l"
3. at the CLI, install update patch; type "system update -i candidate@192.168.10.29:/home/candidate/CPPM-x86_64-20130418-admin-hang-fix-patch.bin"
< --- example --- >

```
appadmin@cppmv61.workshop]# system update -i
candidate@192.168.10.29:/home/candidate/CPPM-x86_64-20130418-admin-hang-
fix-patch.bin

The authenticity of host '192.168.10.29 (192.168.10.29)' can't be
established.
RSA key SHA1 fingerprint is
32:bb:f2:9a:b0:bd:86:ed:f8:94:7b:d0:d4:38:dc:e1:45:4b:c6:9d.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.10.29' (RSA) to the list of known
hosts.
candidate@192.168.10.29's password:
CPPM-x86_64-20130418-admin-hang-fix-patch.bin
100%   37MB  36.7MB/s   00:01

Installing patch from=CPPM-x86_64-20130418-admin-hang-fix-patch.bin
Extracting patch...
INFO: Preparing ...
INFO: Running pre-install scripts ...
INFO: Applying patch ...
INFO: Recording patch ...
INFO: Running post-install scripts ...

INFO: Updating Policy Manager admin server in a while...

INFO: Do not reboot the server until Policy Manager admin is accessible
after the updates

INFO: Patching complete with status - 0
Exiting with 0
```

< --- end example --- >

4. Verify the patch, type: "system update -l"
< --- example --- >

```
[appadmin@cppmv61.workshop]# system update -
l
Update         : 20130418-admin-hang-fix
Installed Date : Tue May 14 12:17:25 2013

Description    : Fix for ClearPass Admin hang issue
Packages       : tips-admin
Affects        : tips-admin-server

1 installed updates.
```

< --- end example --- >

```
syntax as below:
```

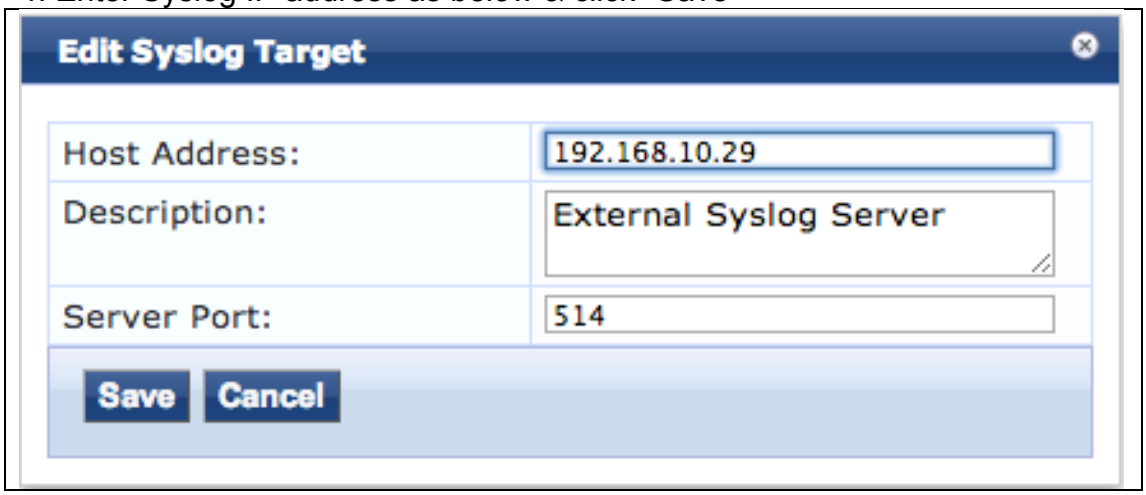
```
Usage:

    system update -i <user@hostname:/<filename> |
http://hostname/<filename> | <filename> >
    system update -l
Where,
    -i              --  Install the update on the system
    -l              --  List the updates installed on the system
```

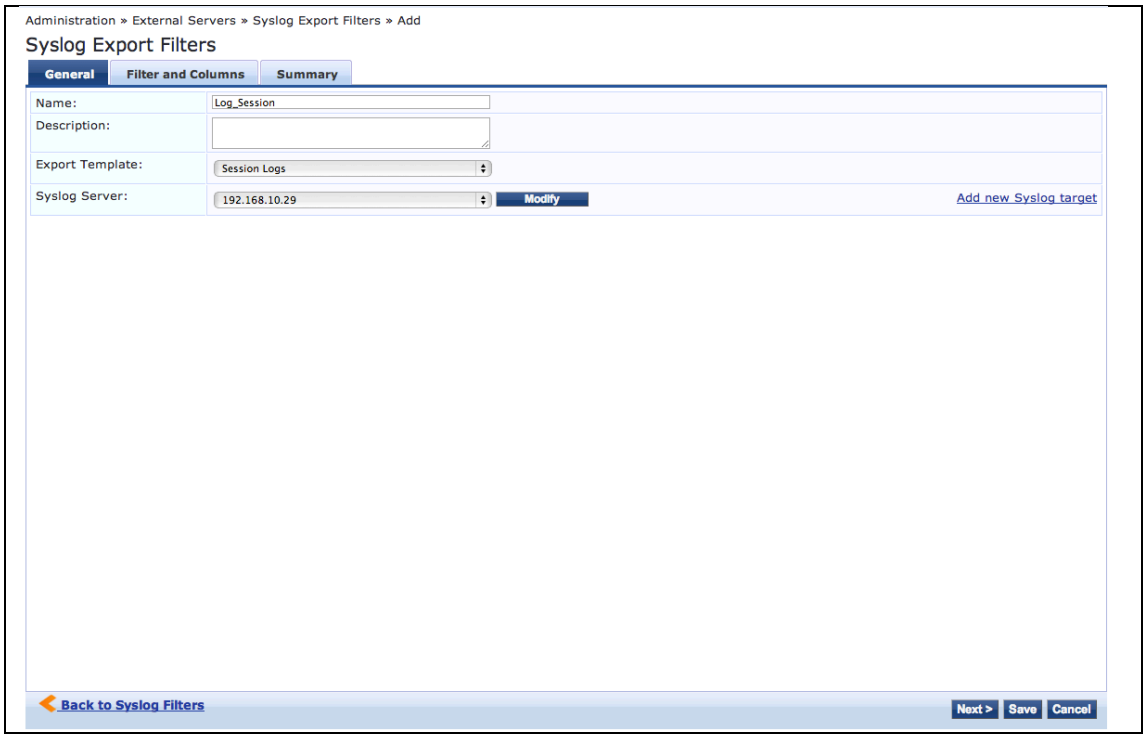
0.2. Add External Syslog Server

1. Login to CPPM WebUI by administrative account
2. At ClearPass Policy Manager, goto Administration > External Servers > Syslog Targets
3. Click "Add Syslog Target"

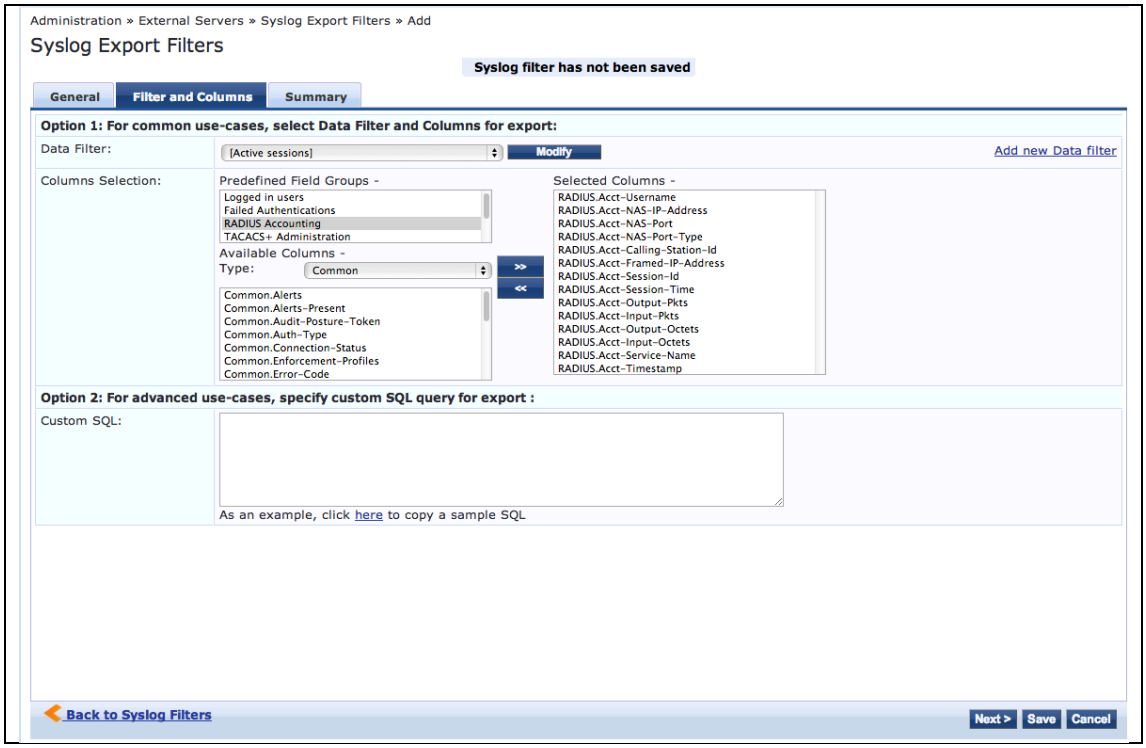
4. Enter Syslog IP address as below & click "Save"



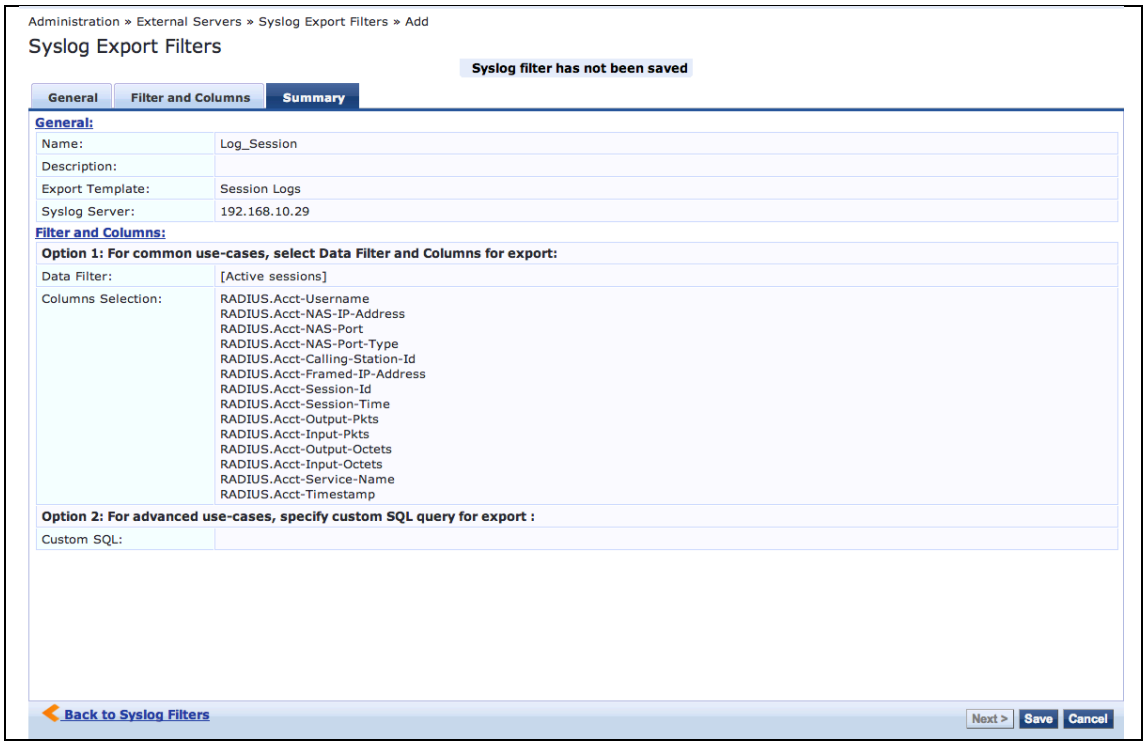
5. For export syslog out to external syslog server; goto Administration > External Servers > Syslog Export Filters
For example: send out session log, select "Session Logs" at export template field & click "Next" button



6. Select what session data/column would like to send out

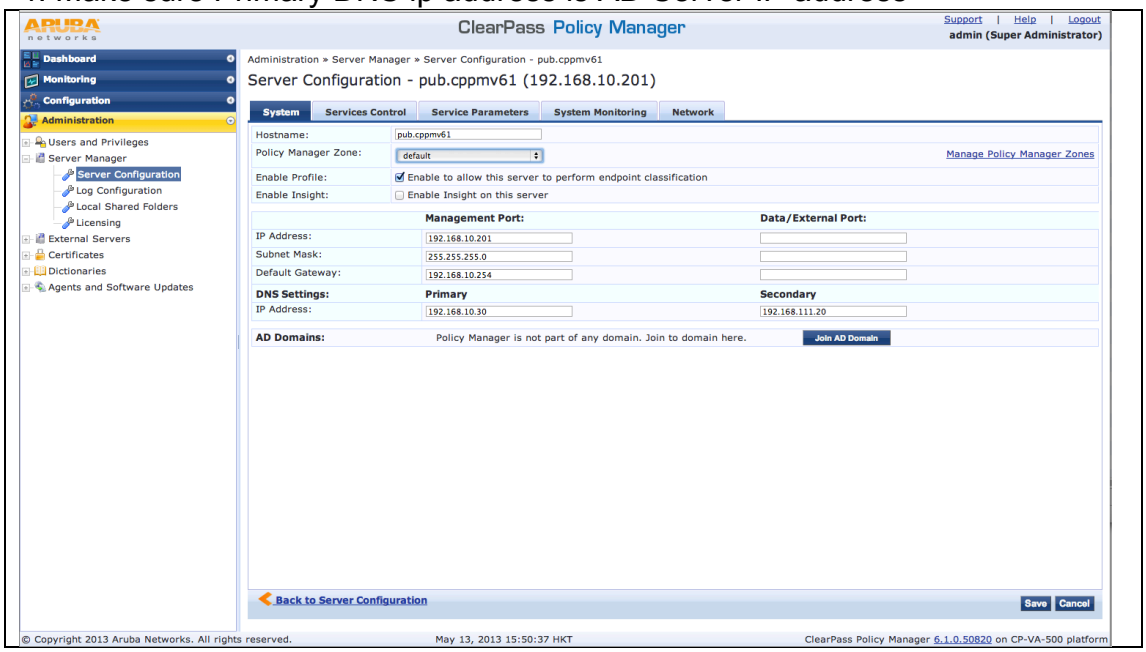


7. After confirm which column/field would like to send out, click "Next" and then "Save" button for complete

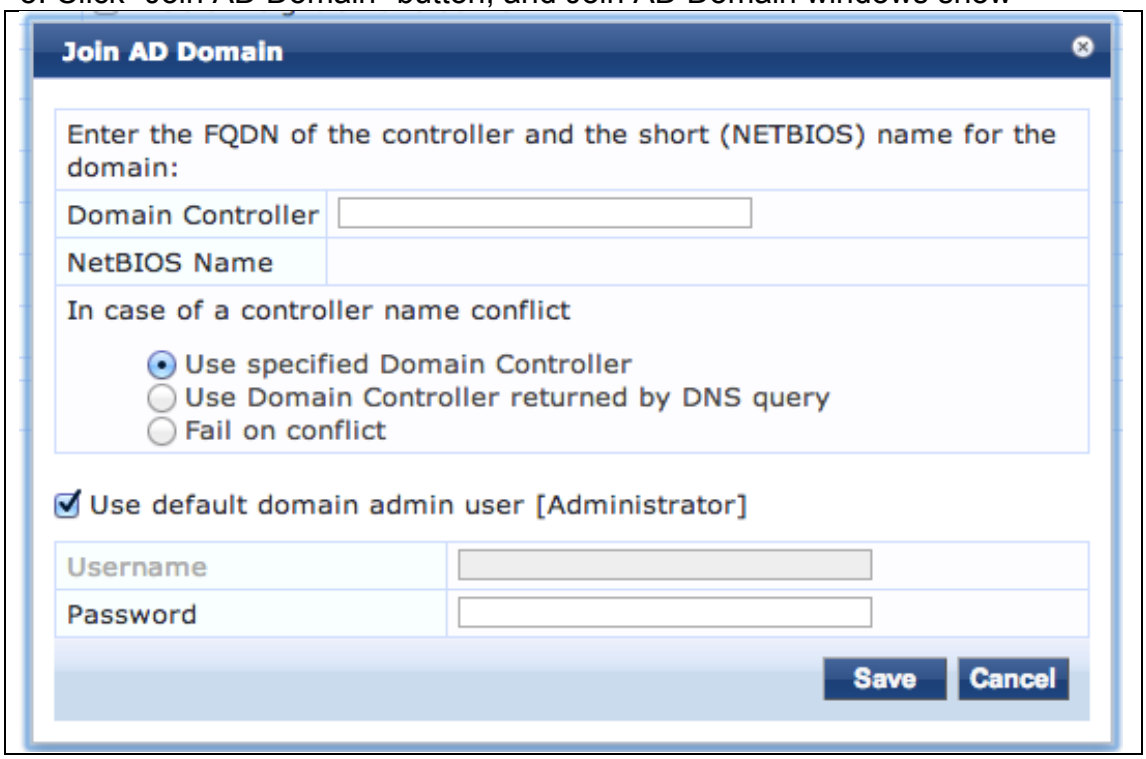

Administration » External Servers » Syslog Export Filters » Add
Syslog Export Filters
Syslog filter has not been saved
General
Filter and Columns
Summary
General:
Name: Log_Session
Description:
Export Template: Session Logs
Syslog Server: 192.168.10.29
Filter and Columns:
Option 1: For common use-cases, select Data Filter and Columns for export:
Data Filter: [Active sessions]
Columns Selection: RADIUS.Acct-Username
RADIUS.Acct-NAS-IP-Address
RADIUS.Acct-NAS-Port
RADIUS.Acct-NAS-Port-Type
RADIUS.Acct-Calling-Station-Id
RADIUS.Acct-Framed-IP-Address
RADIUS.Acct-Session-Id
RADIUS.Acct-Session-Time
RADIUS.Acct-Output-Pkts
RADIUS.Acct-Input-Pkts
RADIUS.Acct-Output-Octets
RADIUS.Acct-Input-Octets
RADIUS.Acct-Service-Name
RADIUS.Acct-Timestamp
Option 2: For advanced use-cases, specify custom SQL query for export :
Custom SQL:
Back to Syslog Filters
Next >
Save
Cancel

0.3. Join AD Domain

1. Login to CPPM WebUI
2. userid: admin ; password: aruba123
3. Goto Administration > Server manager > Server Configuration, select CPPM server
4. Make sure Primary DNS ip address is AD Server IP address



5. Click "Join AD Domain" button, and Join AD Domain windows show



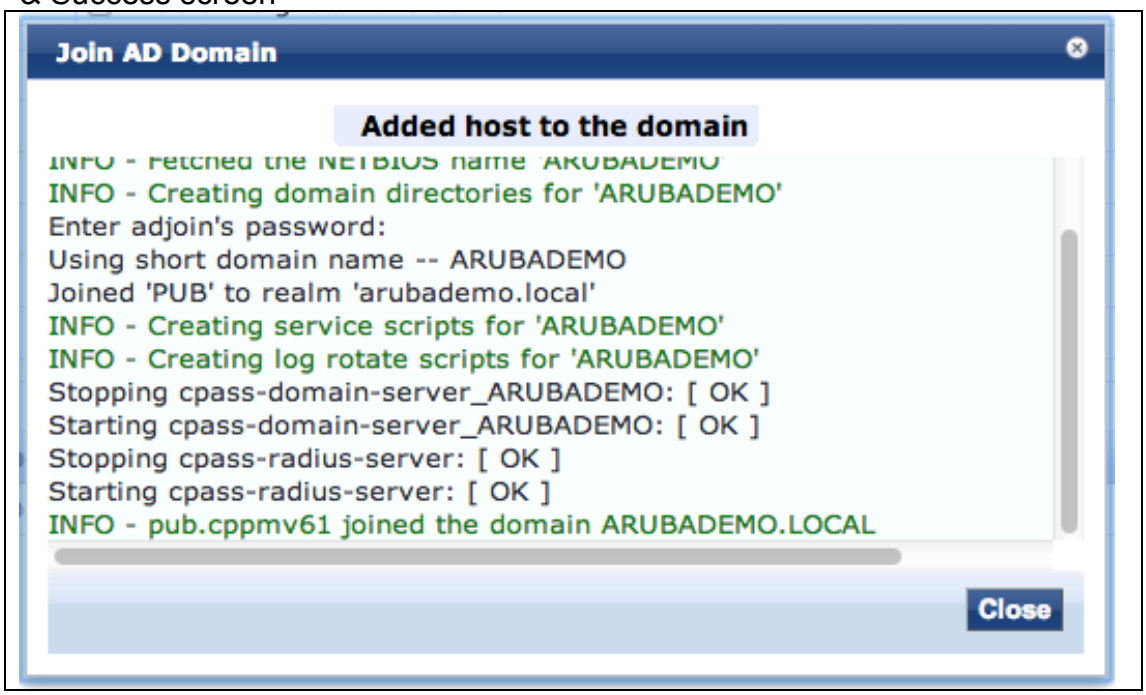
6. Enter below information:
 - Domain Controller: <*The hostname / IP Address of AD Domain Server*>
 - Domain Admin User ID: <*Domain Administrative User ID*>

- Password: <*Domain Administrator password*>

e.g.:

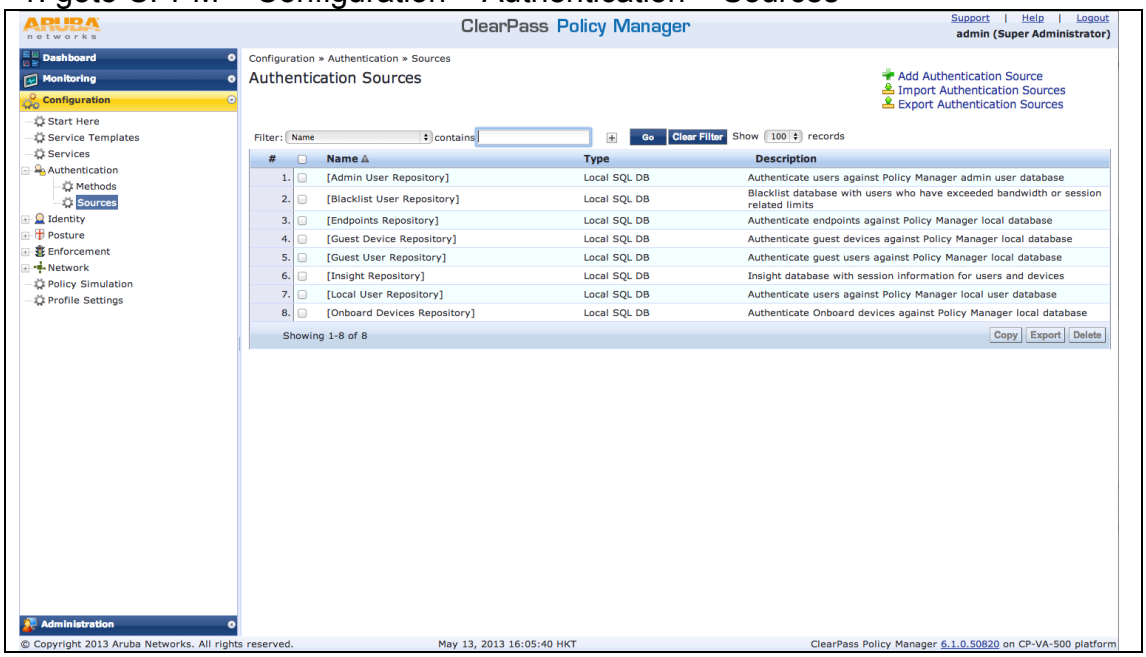
- Domain Controller: ad.arubademo.local
- Domain Admin User: adjoin
- Password: aruba123

& Success screen

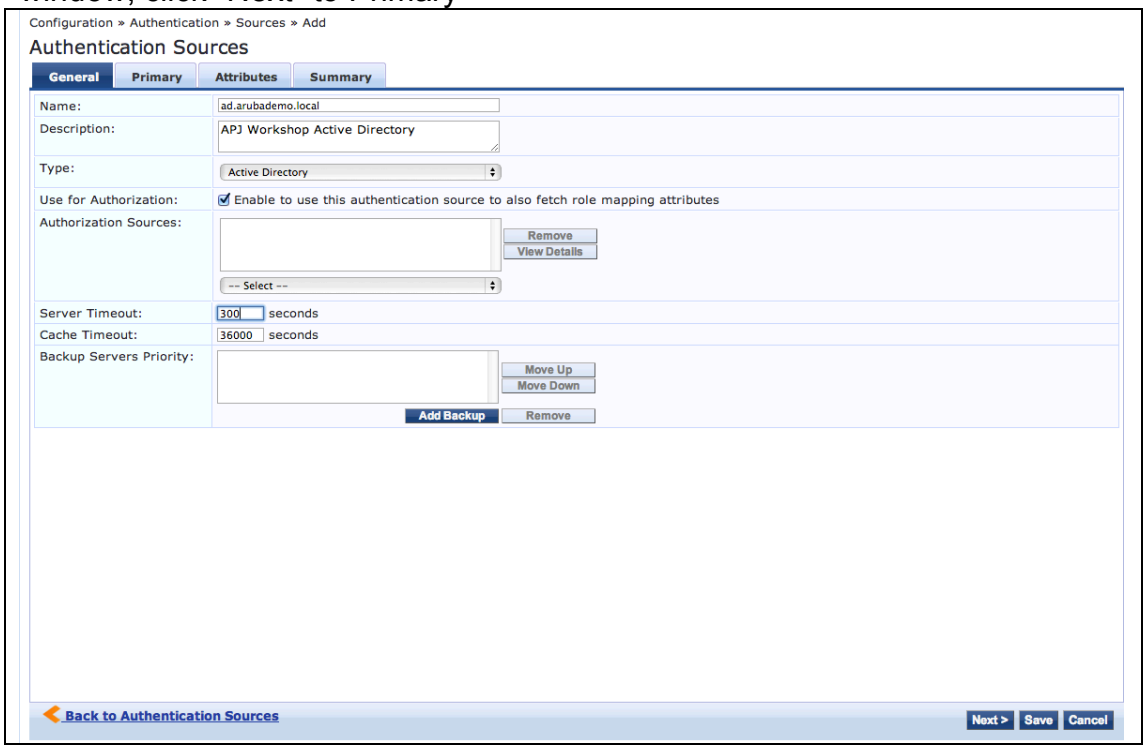


0.4. Add Authentication Sources

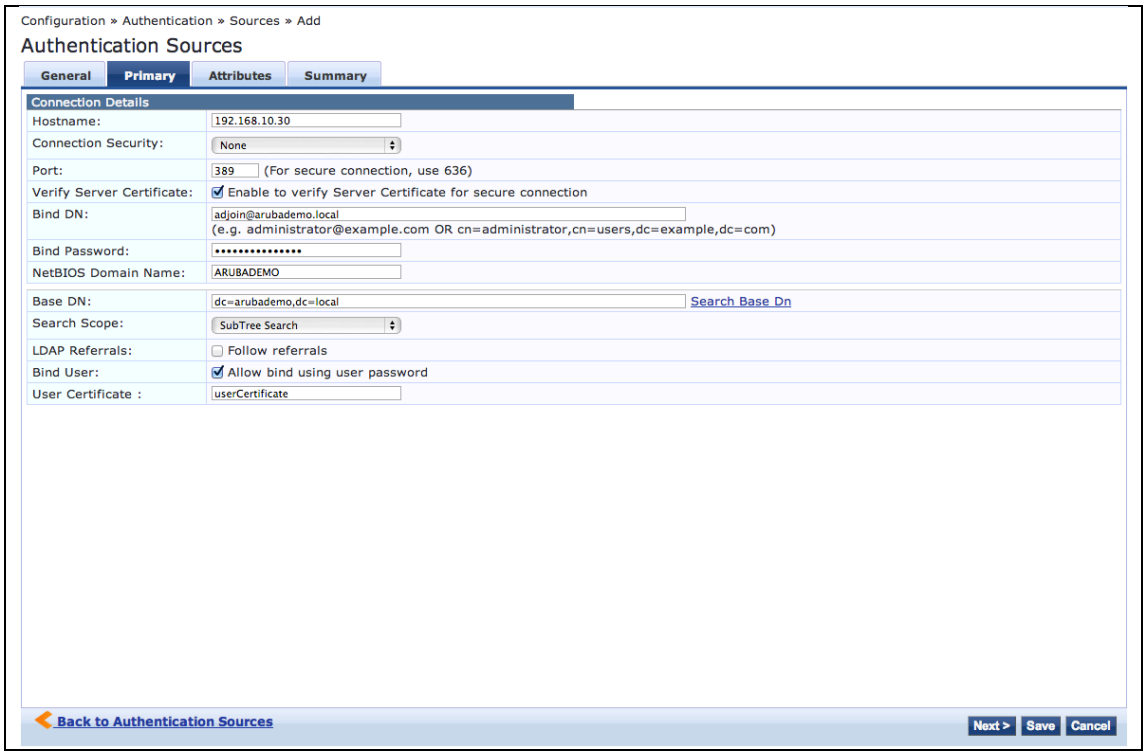
1. goto CPPM > Configuration > Authentication > Sources



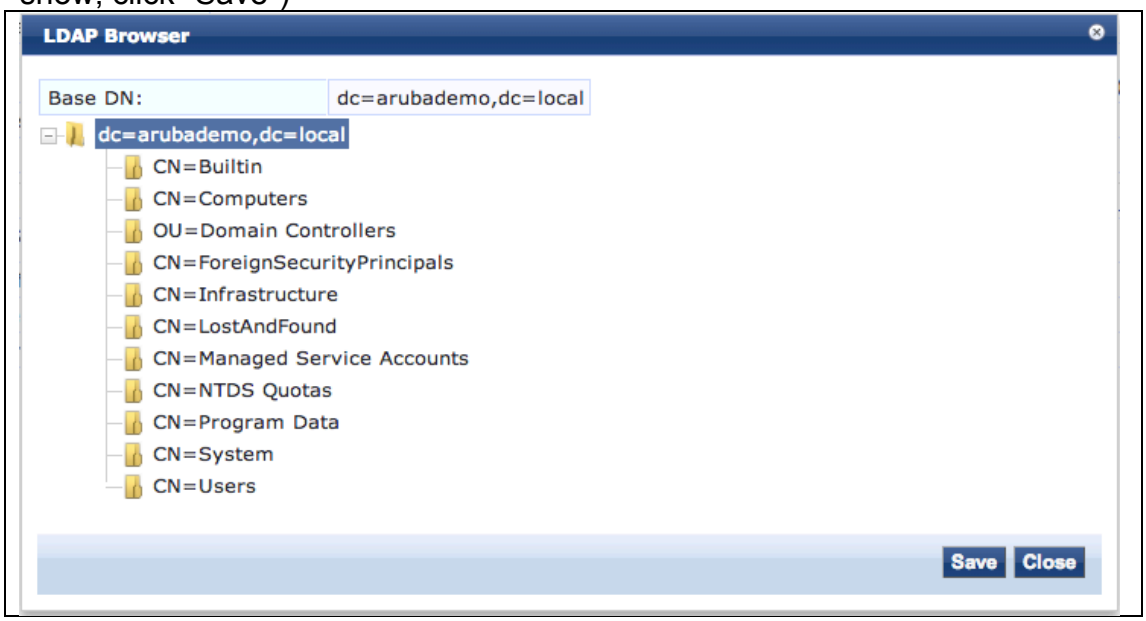
2. Click "Add Authentication Source", and goto Authentication Sources window; click "Next" to Primary



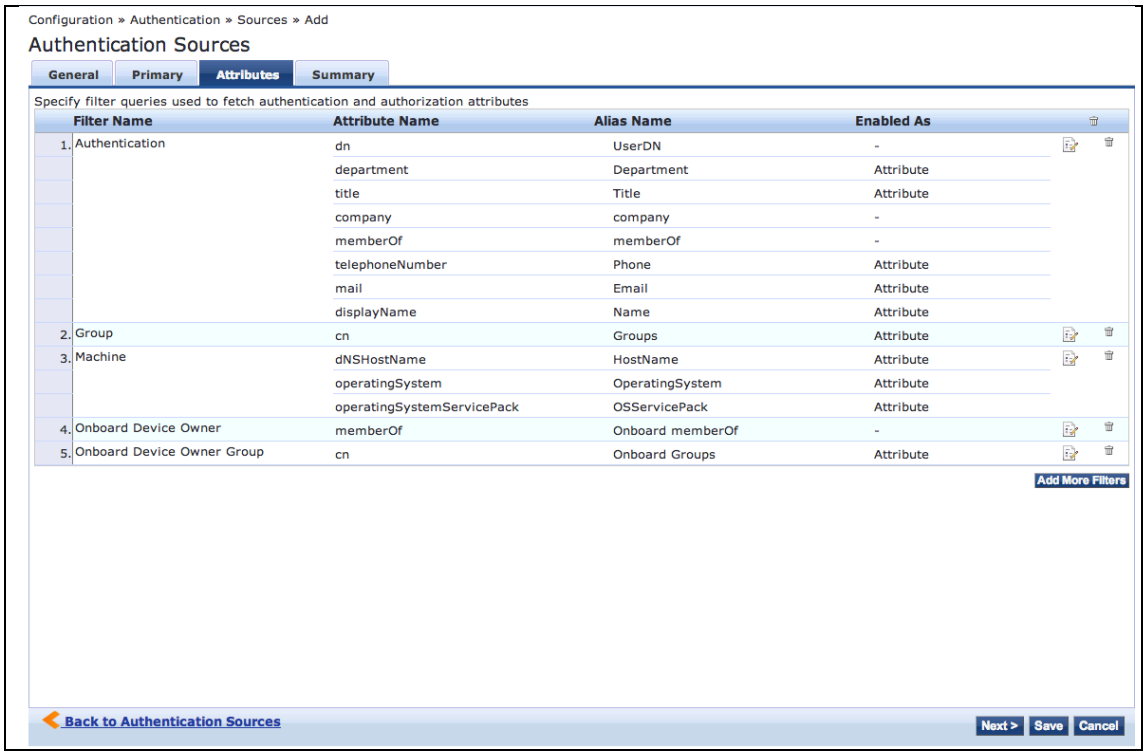
3. At Primary tab, enter as below:



e.g.:
Hostname: 192.168.10.30
Bind DN: adjoin@arubademo.local
Bind Password: aruba123
NetBIOS Domain Name: ARUBADEMO (default will auto filled)
Base DN: dc=arubademo,dc=local (click Search Base Dn, and information will show; click "Save")



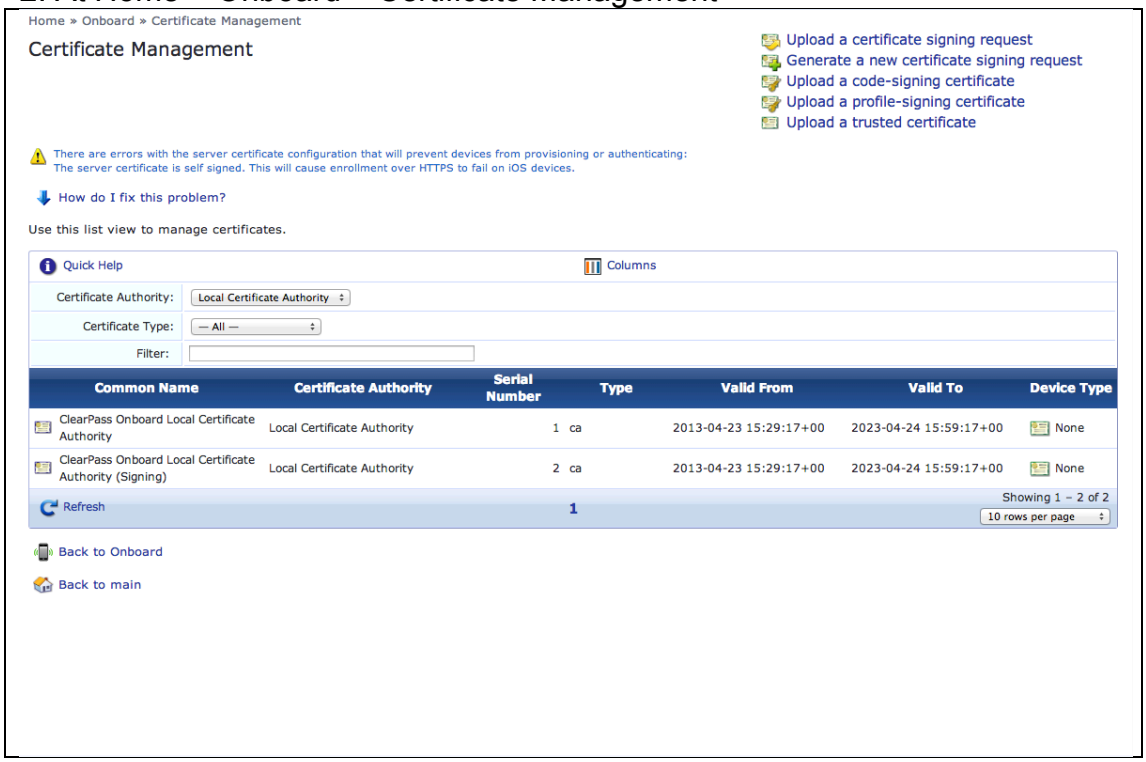
4. At Attributes tab, nothing need to add / change; click Next & Save



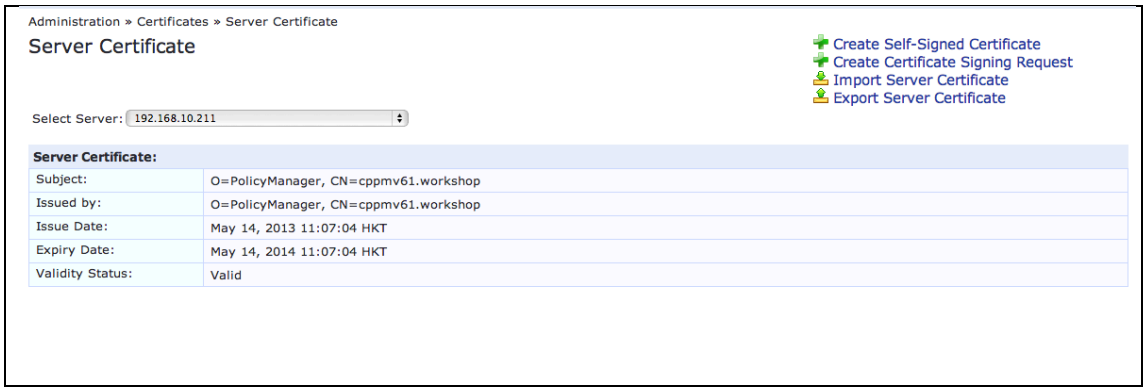
	Filter Name	Attribute Name	Alias Name	Enabled As
1.	Authentication	dn	UserDN	-
		department	Department	Attribute
		title	Title	Attribute
		company	company	-
		memberOf	memberOf	-
		telephoneNumber	Phone	Attribute
		mail	Email	Attribute
		displayName	Name	Attribute
2.	Group	cn	Groups	Attribute
3.	Machine	dNSHostName	HostName	Attribute
		operatingSystem	OperatingSystem	Attribute
		operatingSystemServicePack	OSServicePack	Attribute
4.	Onboard Device Owner	memberOf	Onboard memberOf	-
5.	Onboard Device Owner Group	cn	Onboard Groups	Attribute

0.5. Create Self-Signed Certificate for unit credentials

1. Click Dashboard > Quick Links > ClearPass Onboard
2. At Home > Onboard > Certificate Management

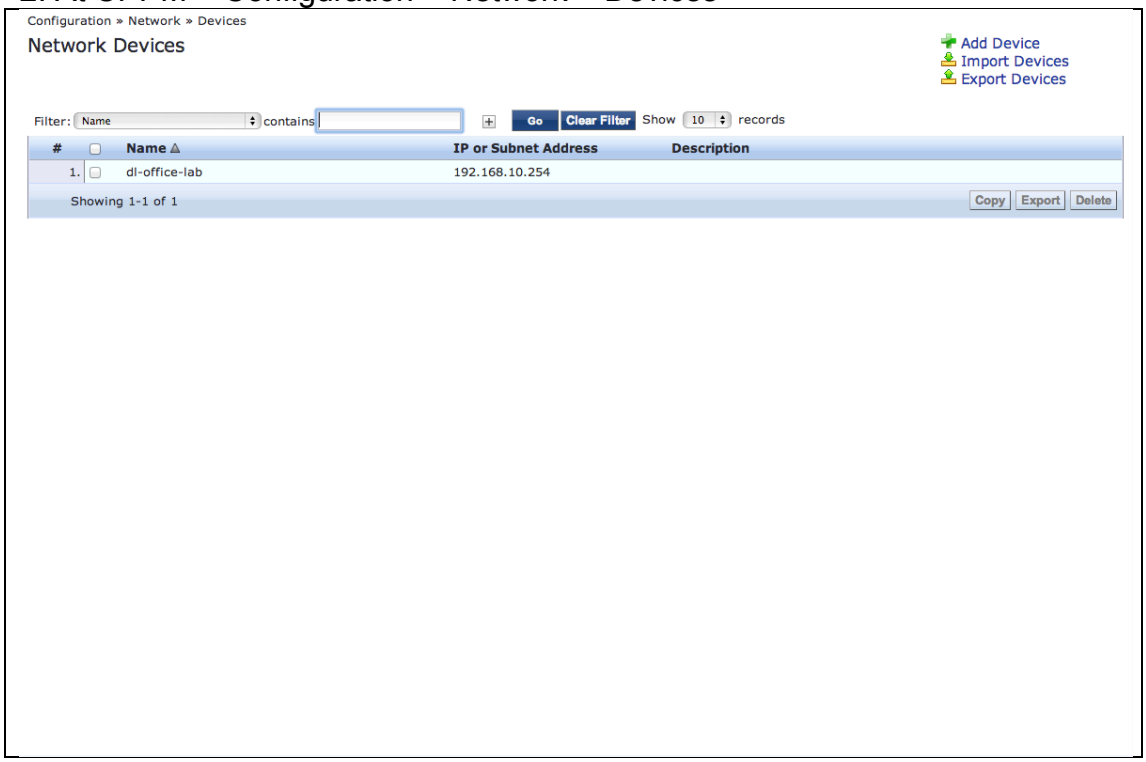


3. Those self-signed certificate is already in place.
4. Default ClearPass Server Certificate at ClearPass Policy Manager > Administration > Certificates > Server Certificate

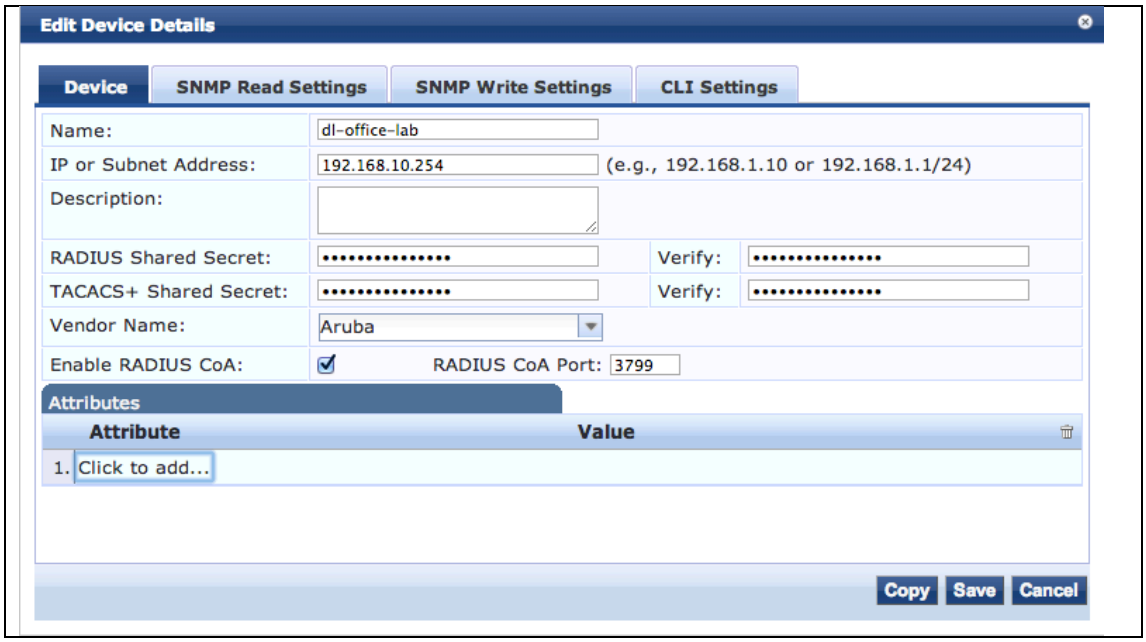


0.6. Add Network Access Device

1. Add Aruba Controller int o CPPM as NAD
2. At CPPM > Configuration > Network > Devices



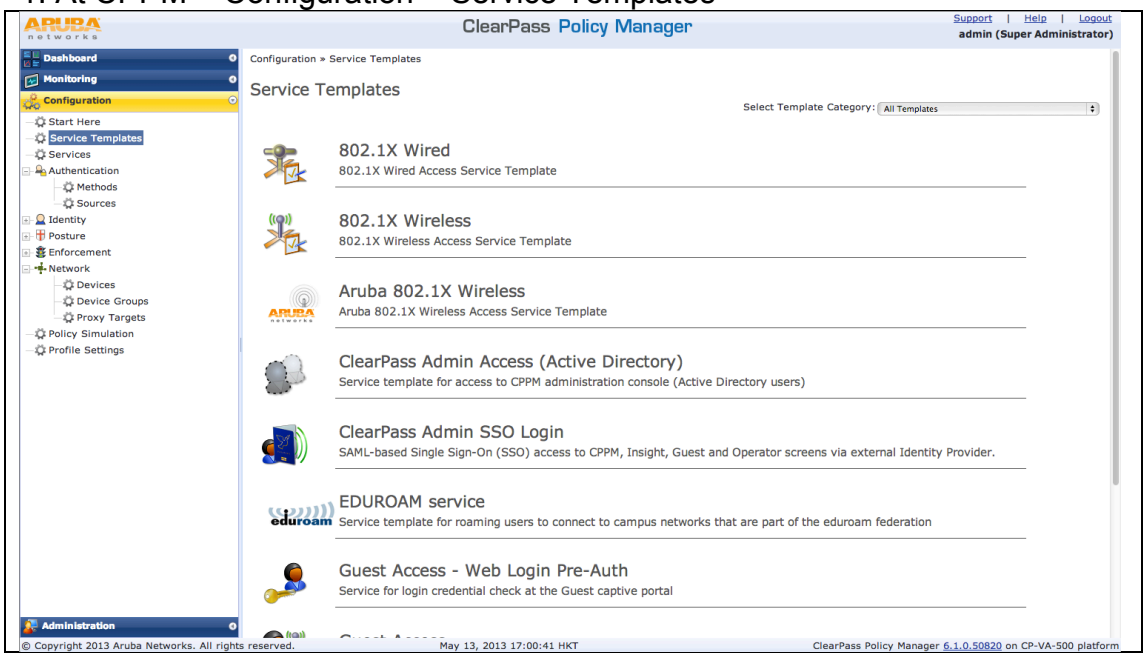
3. Enter Aruba Controller information:
 - Name: *<Controller Device name>*
 - IP/Subnet Address: *<Controller Device IP Address>*
 - RADIUS Shared Secret: *<Pre Shared Phase>*
 - Vendor Name: **Aruba**
 - Enable RADIUS CoA: click enable box



1.0. Basic ClearPass Confirguration Workshop

1.1. Create CPPM ClearPass Admin Services using Service Templates

1. At CPPM > Configuration > Service Templates



2. Select "ClearPass Admin Access (Active Directory)"
3. Enter below information:
 - Name Prefix: APJ-WS
 - Select AD: ad.arubademo.local
 - Role Mapping Detail:
   - Name: netadmin
   - Description: Network Administrator (optional)
   - Attribute name: memberOf
   - Super Admin Condition: Network Admins
   - Attribute name: memberOf
   - Read Only Admin Condition: Engineering
   - Attribute name: memberOf
   - Help Desk Condition: Help Desk

Configuration » Service Templates

Service Templates - ClearPass Admin Access (Active Directory)

Service that authenticates users against Active Directory (AD) and uses AD attributes to determine appropriate privilege level for ClearPass Policy Manager admin access.

Name Prefix:	APJ-WS

Authentication

Select AD*:	ad.arubademo	
AD Name*:	ad.arubademo	
Description:	APJ Workshop Active Driectory	
Server*:	192.168.10.30	
Identity*:	adjoin@arubademo.local	(e.g., administrator@example.com OR cn=administrator,cn=users,dc=example,dc=com)
NETBIOS*:	ARUBADEMO	
Base DN*:	dc=arubademo,dc=local	(e.g., CN=Users,DC=example,DC=example,DC=com)
Password*:	••••••••••••••••	
Port*:	389	(For secure connection, use port 636)

Role Mapping

Name*:	netadmin	Description:	Network Administrator
Attribute Name*:	memberOf	Super Admin Condition*:	Network Admins (e.g., Enter AD group name for super admin users)
Attribute Name*:	memberOf	Read Only Admin Condition*:	Engineering (e.g., Enter AD group name for read only users)
Attribute Name*:	memberOf	Help Desk Condition*:	Help Desk (e.g., Enter AD group name for help desk users)

Add Service Cancel

Result as below:

Configuration » Services » Edit - CPPM Admin ClearPass Admin Access (Active Directory)

Services - CPPM Admin ClearPass Admin Access (Active Directory)

Summary | Service | Authentication | Roles | Enforcement

Service:

Name:	CPPM Admin ClearPass Admin Access (Active Directory)
Description:	Service template for access to CPPM administration console (Active Directory users)
Type:	TACACS+ Enforcement
Status:	Enabled
Monitor Mode:	Disabled
More Options:	-

Service Rule

Match ANY of the following conditions:

	Type	Name	Operator	Value
1.	Connection	NAD-IP-Address	EQUALS	127.0.0.1

Authentication:

Authentication Sources:	ad.arubademo [Active Directory]
Strip Username Rules:	-

Roles:

Role Mapping Policy:	netadmin

Enforcement:

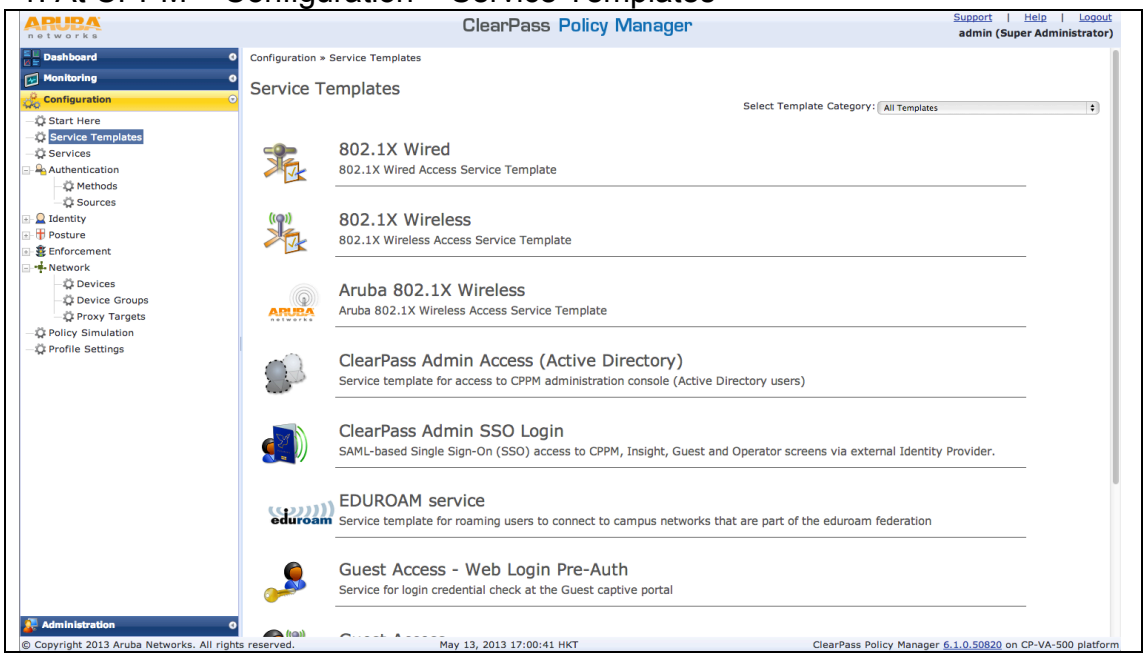
Use Cached Results:	Disabled
Enforcement Policy:	[Admin Network Login Policy]

Back to Services

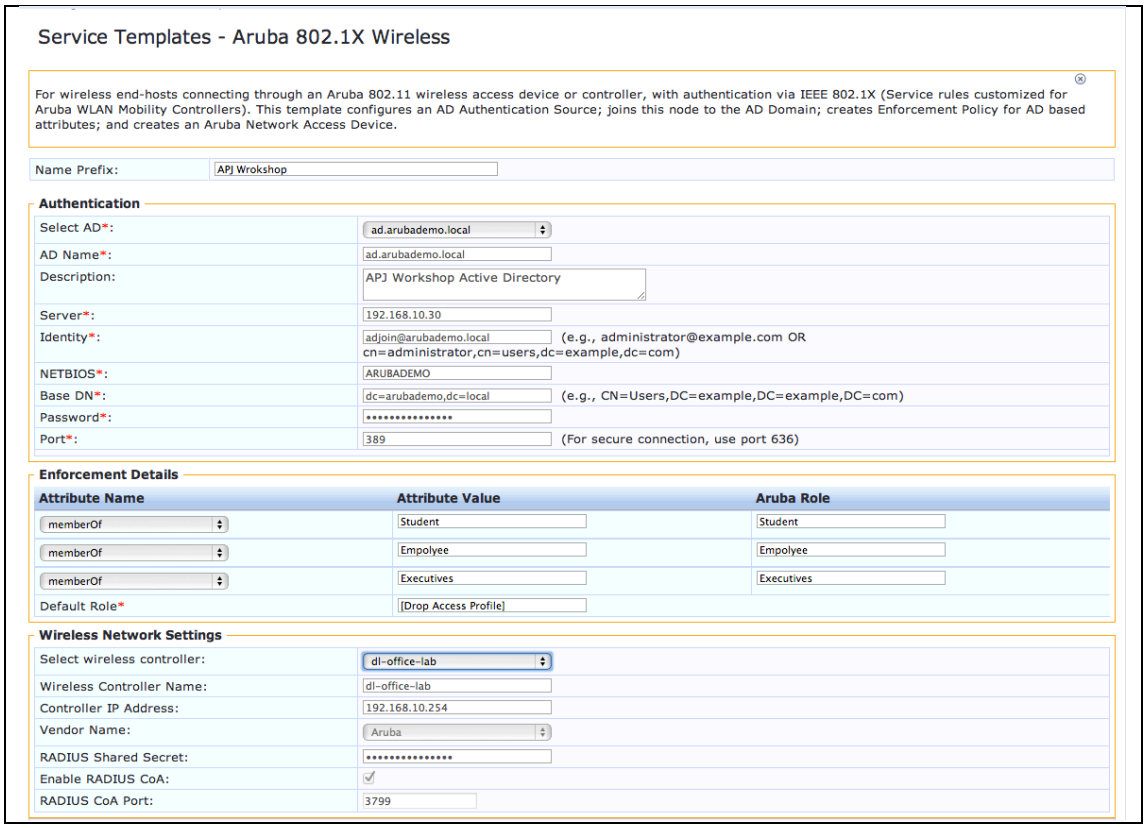
Disable Copy Save Cancel

1.2. Create CPPM dot1X Services using Service Templates

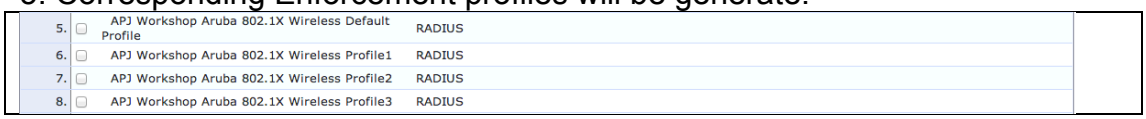
1. At CPPM > Configuration > Service Templates



2. Select "Aruba 802.1X Wireless"
3. Enter below information:
 - Name Prefix: APJ Workshop
 - Select AD: ad.arubademo.local
 - Enforcement Detail:
   - Attribute name: memberOf
   - Attribute Value: Student
   - Aruba Role: Student
 - Wireless Network Settings > Select wireless controller: dl-office-lab



4. Click "Add Service"
5. Corresponding Enforcement profiles will be generate:



5.	APJ Workshop Aruba 802.1X Wireless Default Profile	RADIUS
6.	APJ Workshop Aruba 802.1X Wireless Profile1	RADIUS
7.	APJ Workshop Aruba 802.1X Wireless Profile2	RADIUS
8.	APJ Workshop Aruba 802.1X Wireless Profile3	RADIUS

6. Add Roles at ClearPass Policy, goto Configuration > Identity > Roles

Configuration » Identity » Roles

Roles

Role Student_BYOD updated successfully

Add Roles
Import Roles
Export Roles

Filter: Name contains Go Clear Filter Show 100 records

#	Name	Description
1.	[AirGroup Administrator]	Operators with this role can manage multiple devices that are shared with all users
2.	[AirGroup Operator]	Operators with this role can self-provision devices within their personal WLAN
3.	[Aruba TACACS read-only Admin]	Default role for read-only access to Aruba device
4.	[Aruba TACACS root Admin]	Default role for root access to Aruba device
5.	[Contractor]	Default role for a contractor
6.	Employee	APJ Workshop
7.	[Employee]	Default role for an employee
8.	Executives	APJ Workshop
9.	Executives_BYOD	APJ Workshop
10.	[Guest]	Default role for a Guest
11.	[MAC Caching]	Default role applied during MAC caching
12.	[MACTrac Operator]	Operators with this role can create MAC accounts which could get authenticated
13.	[Onboard Android]	Role for an Android device being provisioned
14.	[Onboard iOS]	Role for an iOS device being provisioned
15.	[Onboard Mac OS X]	Role for a Mac OS X device being provisioned
16.	[Onboard Windows]	Role for a Windows device being provisioned
17.	[Other]	Default role for another user or device
18.	Staff	APJ Workshop
19.	Staff_BYOD	APJ Workshop
20.	Student	APJ Workshop
21.	Student_BYOD	APJ Workshop
22.	[TACACS API Admin]	API administrator role for Policy Manager Admin
23.	[TACACS Help Desk]	Help desk role for Policy Manager Admin
24.	[TACACS Network Admin]	Network administrator role for Policy Manager Admin
25.	[TACACS Read-only Admin]	Read-only administrator role for Policy Manager Admin

7. Click "Add Roles", and enter roles as below:
   Executives - for executive employees
   Executives_BYOD - for executive employees BYOD
   Staff - for staff empolyee
   Staff_BYOD - for staff member BYOD
   Student - for student
   Student_BYOD - for student BYOD

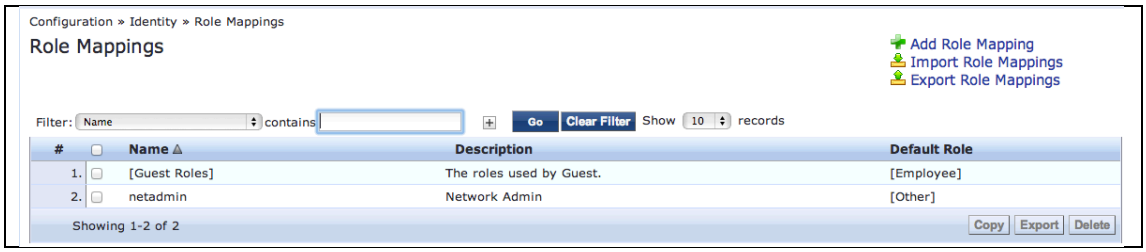
Edit Role

Name: Staff

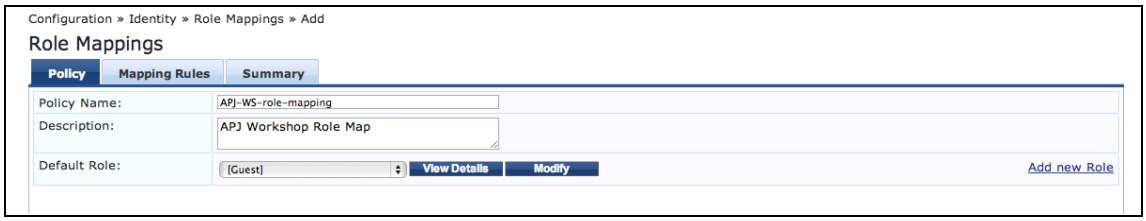
Description: APJ Workshop

Save Cancel

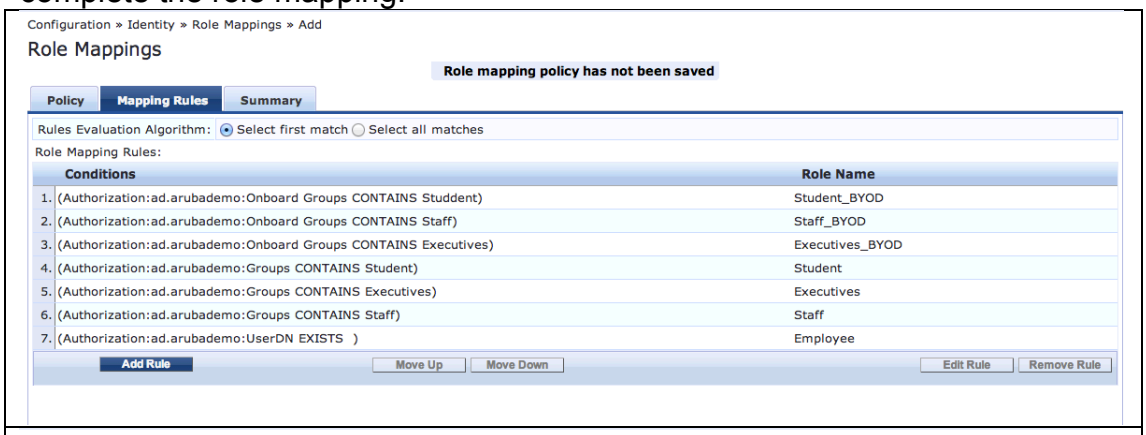
8. Add new role mapping at Configuration > Identity > Role Mappings; click "Add Role mapping"

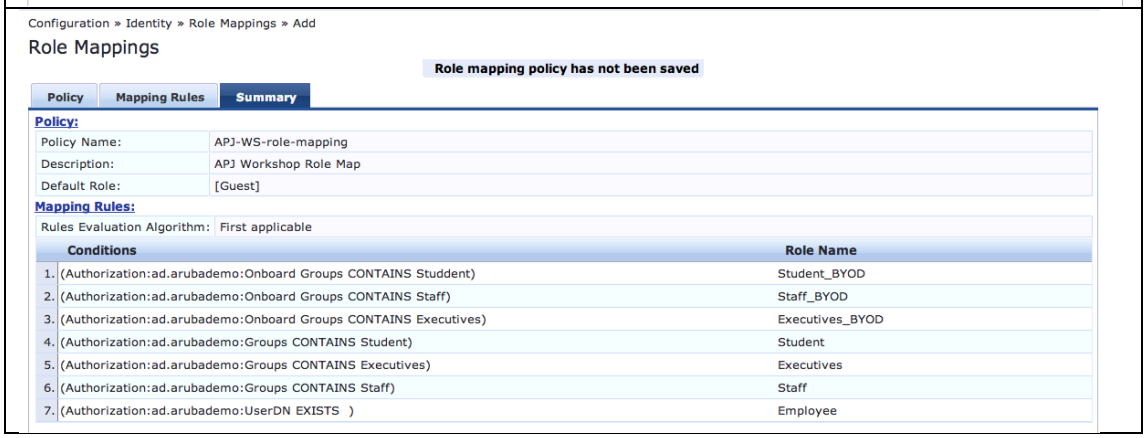


9. At Policy tab, enter Policy Name & Default Role as below & click "Next" button:

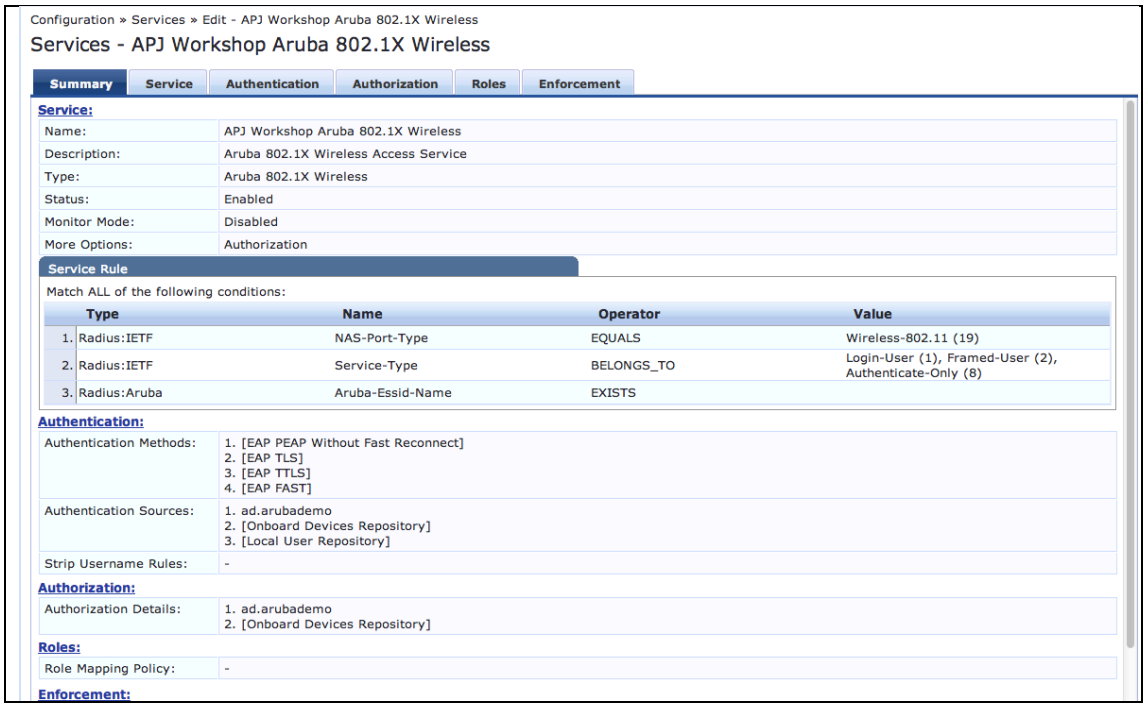


10. At Mapping Rules, enter as below; and click "Next" & "Save" button for complete the role mapping:

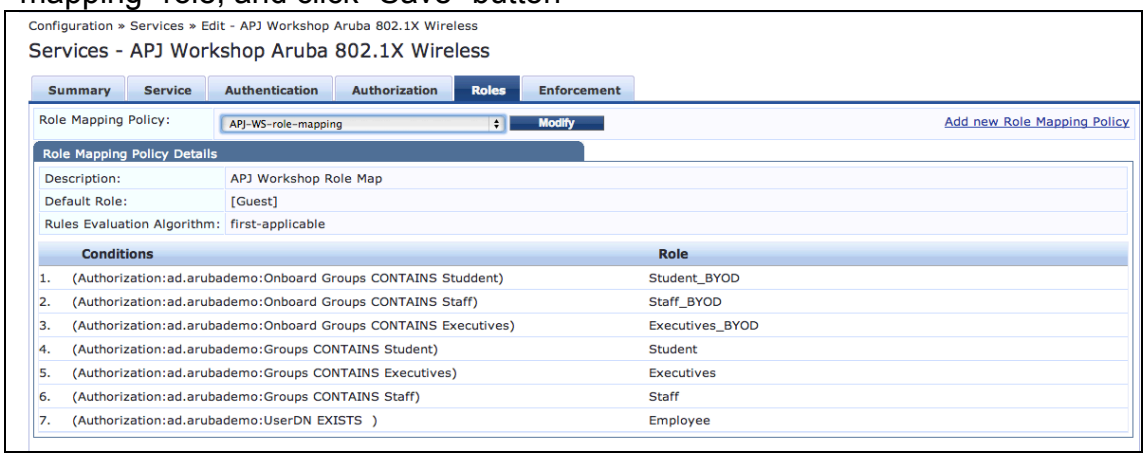




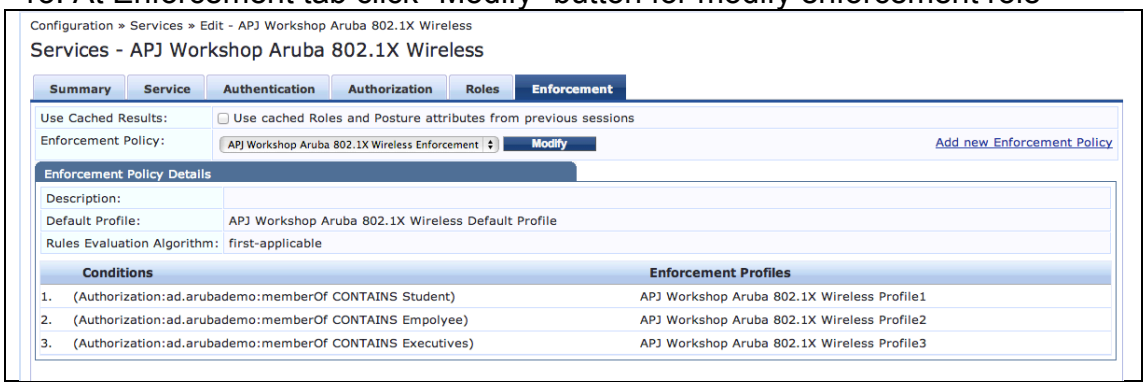
11. Go to Configuration > Services and select "APJ Workshop Aruba 802.1X Wireless" to edit



12. Goto Roles tab, at "Role mapping Policy" field select "APJ-WS-role-mapping" role; and click "Save" button



13. At Enforcement tab click "Modify" button for modify enforcement role

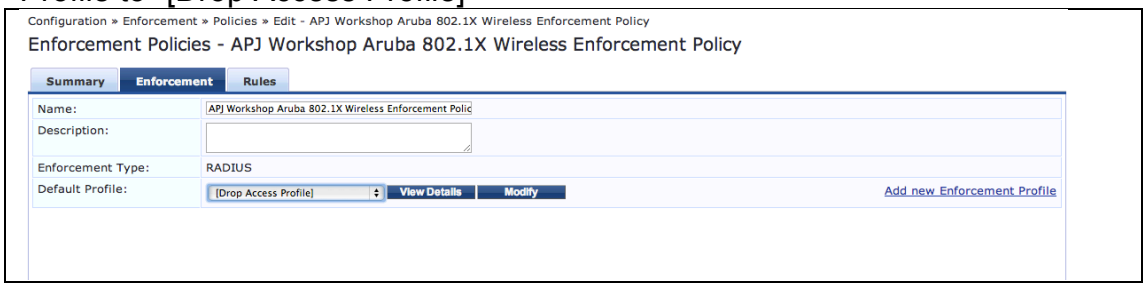


14.Add Enforcement Profiles,

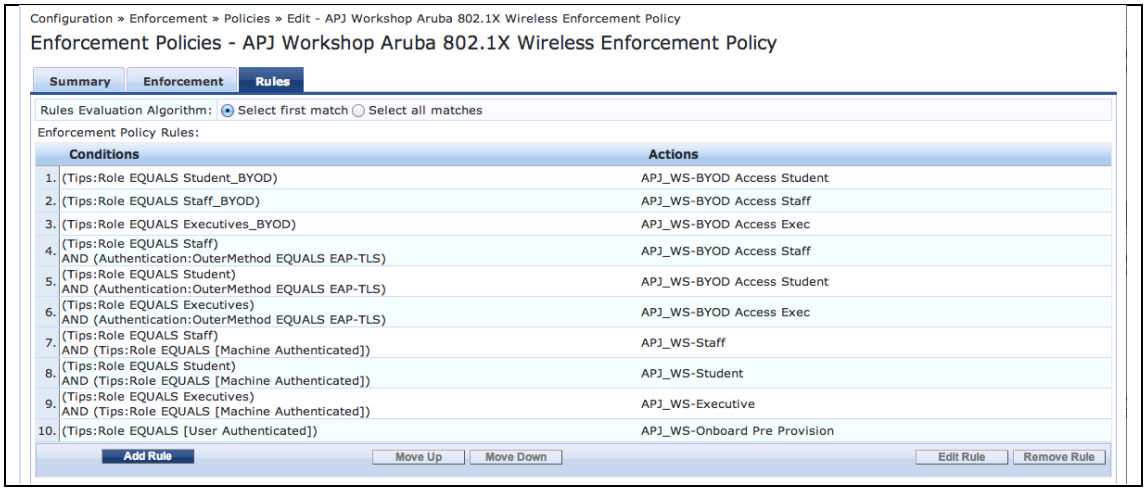
Enforcement Profile	Type	Name	Value

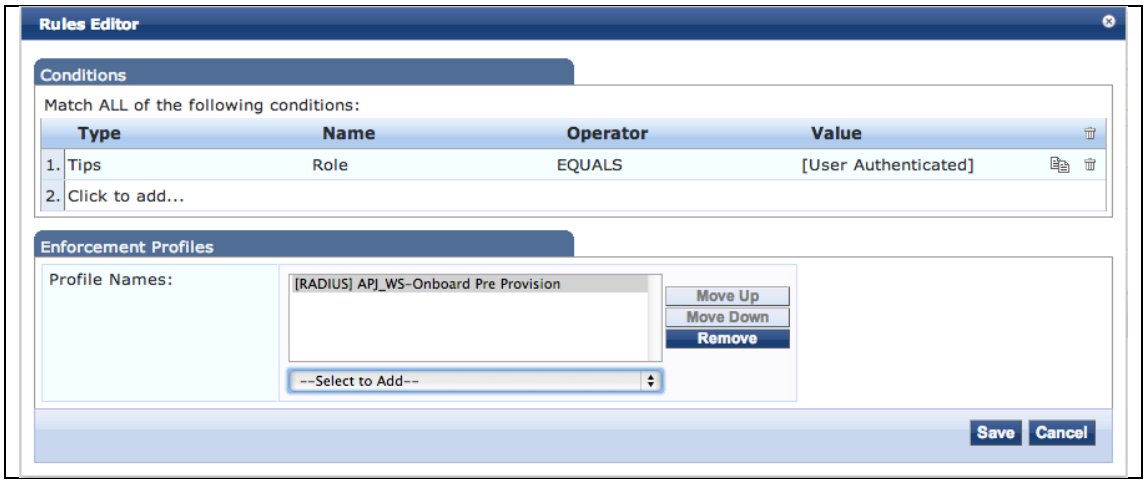
BYOD Access Exec	Radius:Aruba	Aruba-User-Role	Exec_BYOD
BYOD Access Staff	Radius:Aruba	Aruba-User-Role	Staff_BYOD
BYOD Access Student	Radius:Aruba	Aruba-User-Role	Student_BYOD
Executive	Radius:Aruba	Aruba-User-Role	Executive
Staff	Radius:Aruba	Aruba-User-Role	Staff
Student	Radius:Aruba	Aruba-User-Role	Student
Onboard Pre provisioning Aruba	Radius:Aruba	Aruba-User-Role	BYOD-Provision

15. At Enforcement tab, Configuration > Enforcement > Policies > Edit - "APJ Workshop Aruba 802.1X Wireless Enforcement Policy", change the Default Profile to "[Drop Access Profile]"



16. At Rules tab, Configuration > Enforcement > Policies > Edit - "APJ Workshop Aruba 802.1X Wireless Enforcement Policy", Add/Edit rules as below:





1.3. Aruba Controller

The followings are the sample of Aruba Controller configuration:

1. Access-list:

```
!
netdestination Apple
  name www.apple.com
!
netdestination CP6
  host 192.168.0.95
!
netdestination Google-Play
name android.clients.google.com !
ip access-list session captiveportal
user alias controller svc-https dst-nat 8081 user alias CP6 svc-http
permit
user alias CP6 svc-https permit
user any svc-http dst-nat 8080
user any svc-https dst-nat 8081
user any svc-http-proxy1 dst-nat 8088 user any svc-http-proxy2 dst-
nat 8088 user any svc-http-proxy3 dst-nat 8088
!
```

2. User Roles:

```
!
user-role logon
access-list session logon-control access-list session captiveportal
access-list session vpnlogon access-list session v6-logon-control
access-list session captiveportal6
!
user-role Executive
 access-list session allowall
!
user-role Exec_BYOD
 access-list session allowall
!
user-role Staff
 access-list session allowall
!
user-role Staff_BYOD
 access-list session allowall
!
```

```
user-role Student
 access-list session allowall
!
user-role Student_BYOD
 access-list session allowall
!
user-role Employee_BYOD
 access-list session allowall
!
user-role BYOD-Provision
captive-portal "byod-cp-prof" access-list session captiveportal
access-list session logon-control
!
```

3. AAA Profiles

```
!
aaa authentication-server radius "CP6-RADIUS"
   host "192.168.0.95"
   key aruba123
nas-identifier "Aruba651"
   nas-ip 192.168.0.254
   source-interface vlan 192
!
aaa server-group "CP60_group"
 auth-server CP6-RADIUS
 set role condition role value-of
!
aaa profile "CP6-aaa-dot1x-prof" authentication-dot1x "default"
dot1x-server-group "CP60_group" radius-accounting "CP60_group"
radius-interim-accounting rfc-3576-server "192.168.0.95"
!
```

4. AAA Captive Portal Profiles

```
!
aaa authentication captive-portal "byod-cp-prof"
   server-group "CP60_group"
   redirect-pause 1
   no logout-popup-window
   protocol-http
login-page "http://192.168.0.95/guest/device_provisioning.php"
switchip-in-redirection-url
white-list "Apple"
white-list "Google-Play"
!
```

5. VAP and SSID Profiles

```
!
wlan ht-ssid-profile "Edu-1"
!
wlan ssid-profile "corp-ssid-prof"
essid "Corp"
opmode wpa-tkip wpa-aes wpa2-aes wpa2-tkip local-probe-req-thresh 25
ht-ssid-profile "Edu-1"
!
wlan virtual-ap "corp-cp6-vap-prof"
```

```
aaa-profile "CP6-aaa-dot1x-prof" ssid-profile "corp-ssid-prof" vlan 1
band-steering
!
ap-group "default"
virtual-ap "corp-cp6-vap-prof" !
```

1.4. Testing Script

1. Connect to SSID: “Crop” by candidate’s laptops; e.g. Windows XP, Windows 7, etc.
2. Test login as below account
    - staff1
    - exec1
    - student1

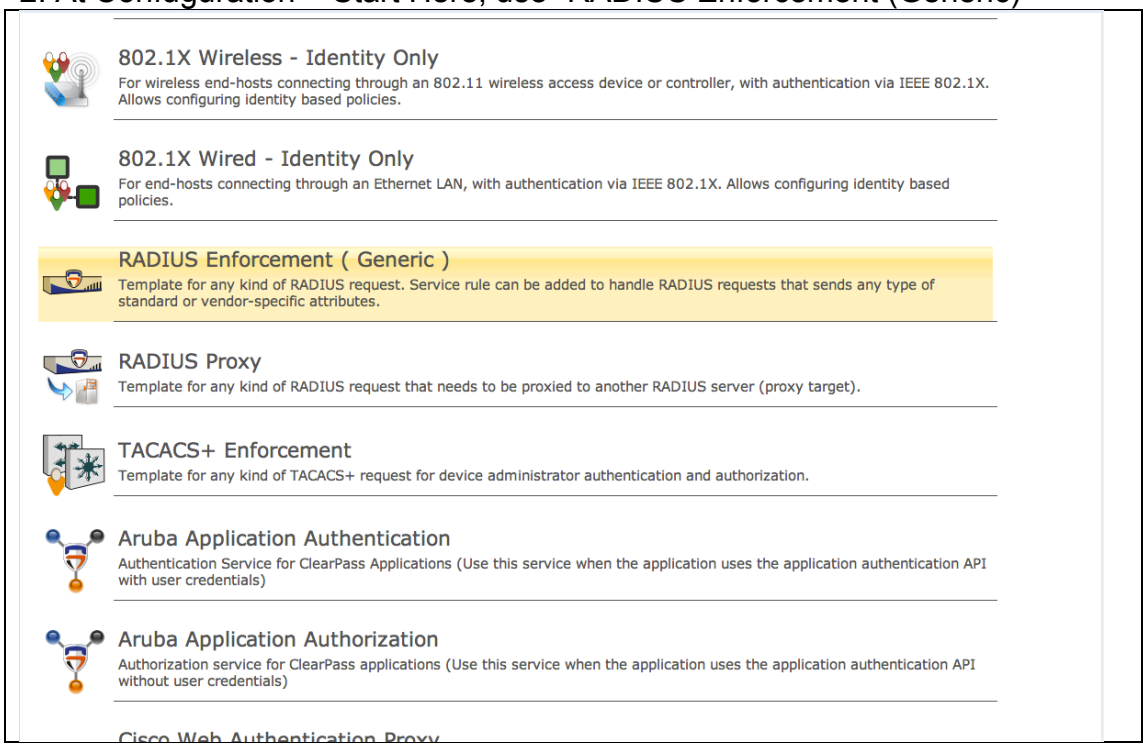
3. Verify the result !!
4. Connect to SSID: “Crop” by candidate’s mobile devices; e.g. iPad, iPhone, Android Phone, Android Tablet, etc.
5. Test login as below account
    - staff1
    - exec1
    - student1

6. Verify the result !!

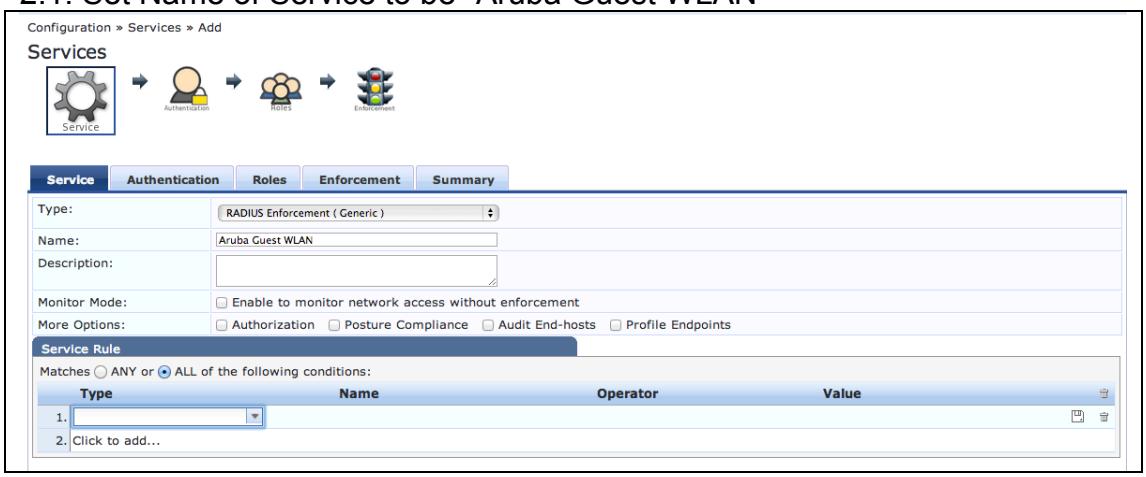
2.0. Advance ClearPass Confirguration Workshop

2.1. ClearPass – Guest -- Setup basic Guest WLAN Service to Aruba Controller

1. Configure Authentication Service on ClearPass Policy Manager
2. At Confuguration > Start Here, use “RADIUS Enforcement (Generic)”

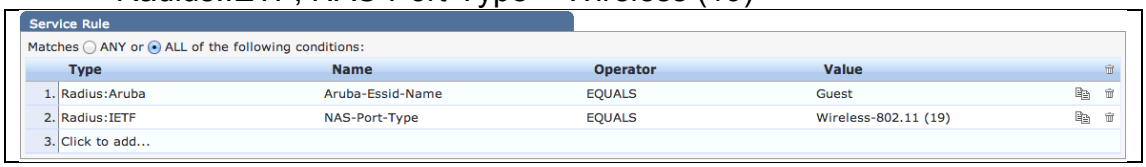


2.1. Set Name of Service to be "Aruba Guest WLAN"



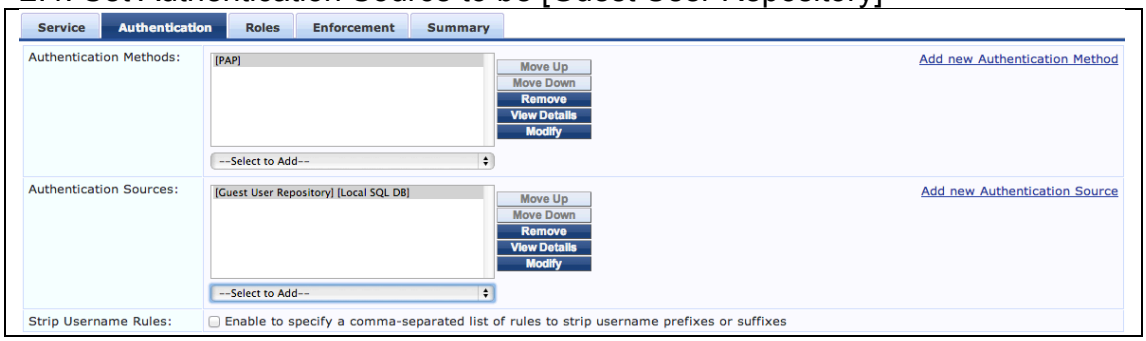
2.2. Set the following in Service Rules:

- Radius:Aruba, Aruba-ESSID-Name = “Guest-X”
- Radius:IETF, NAS-Port-Type = Wireless (19)



2.3. Set [PAP] as Authentication Method

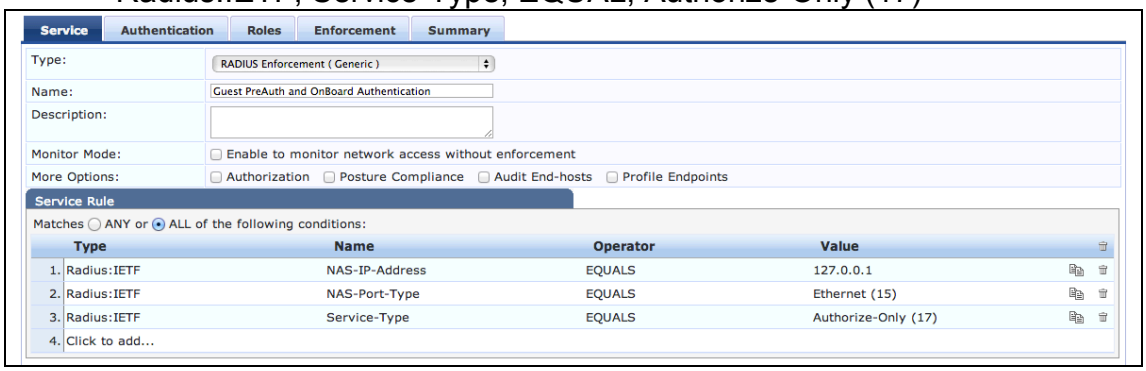
2.4. Set Authentication Source to be [Guest User Repository]



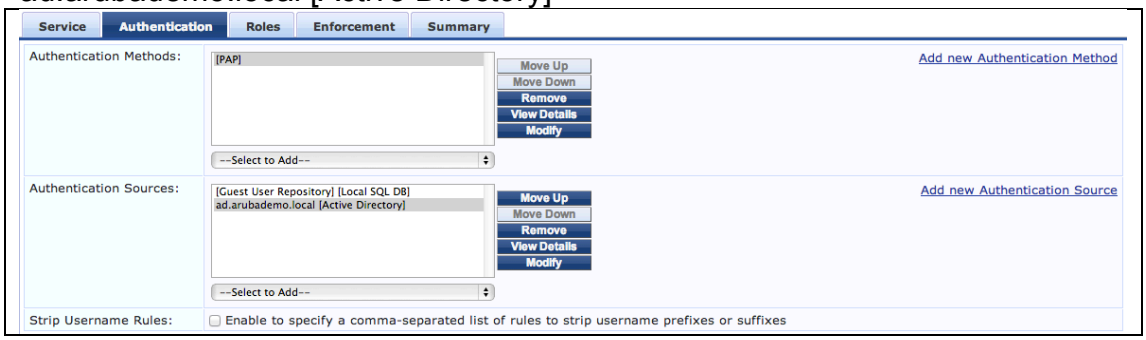
2.5. Click “Save”

3. Configure Pre-Authentication Service
3.1. Set Name of Service to be "Guest PreAuth and OnBoard Authentication"
3.2. Set the following in Service Rules:

- Radius:IETF, NAS-IP-Address, EQUAL, “127.0.0.1”
- Radius:IETF, NAS-Port-Type, EQUAL, Ethernet (15)
- Radius:IETF, Service-Type, EQUAL, Authorize-Only (17)

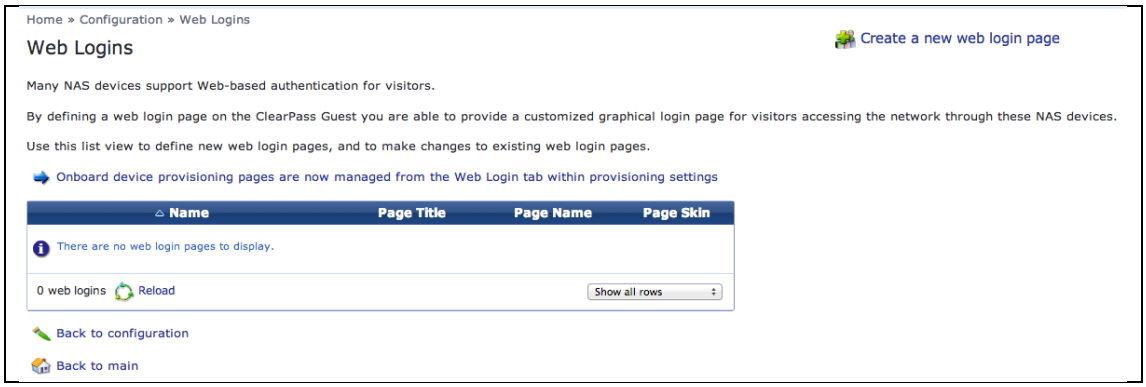


3.3. Set [PAP] as Authentication Method
3.4. Set Authentication Source to be [Guest User Repository] and ad.arubademo.local [Active Directory]

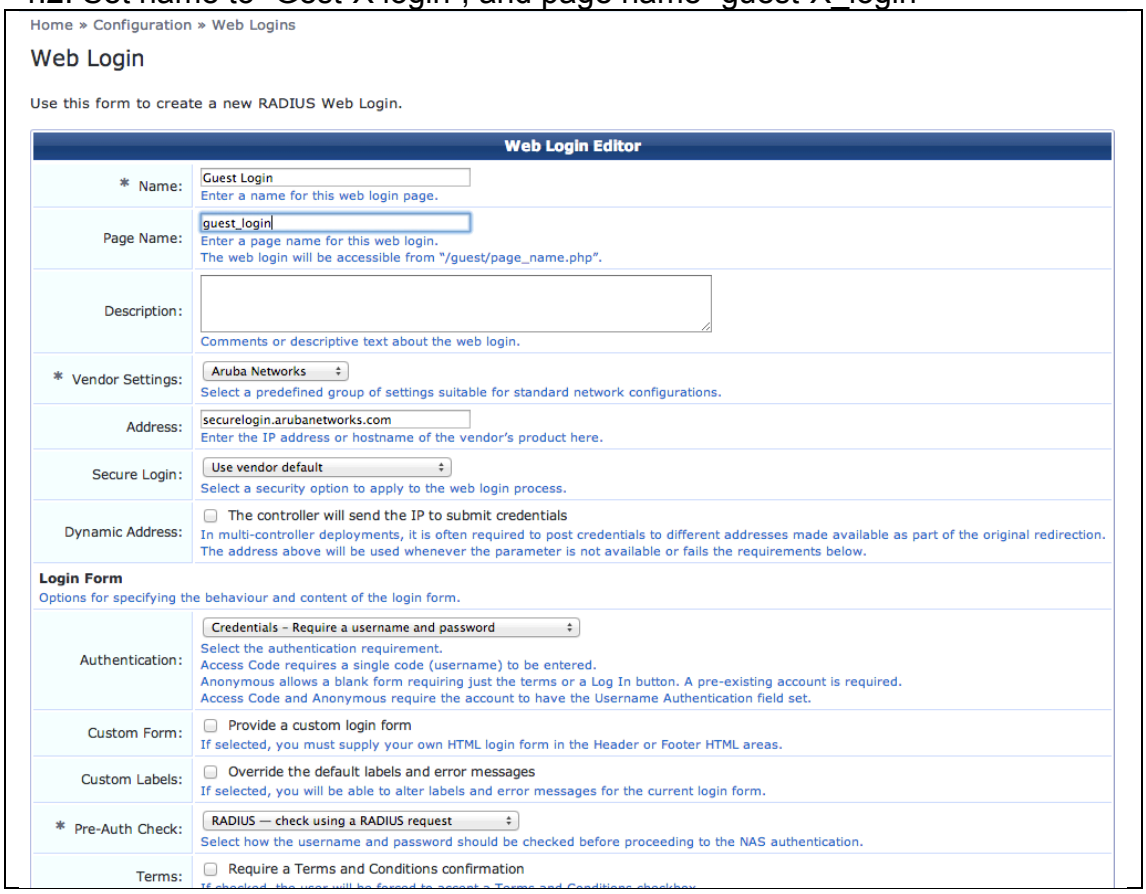


3.5. Click “Save”

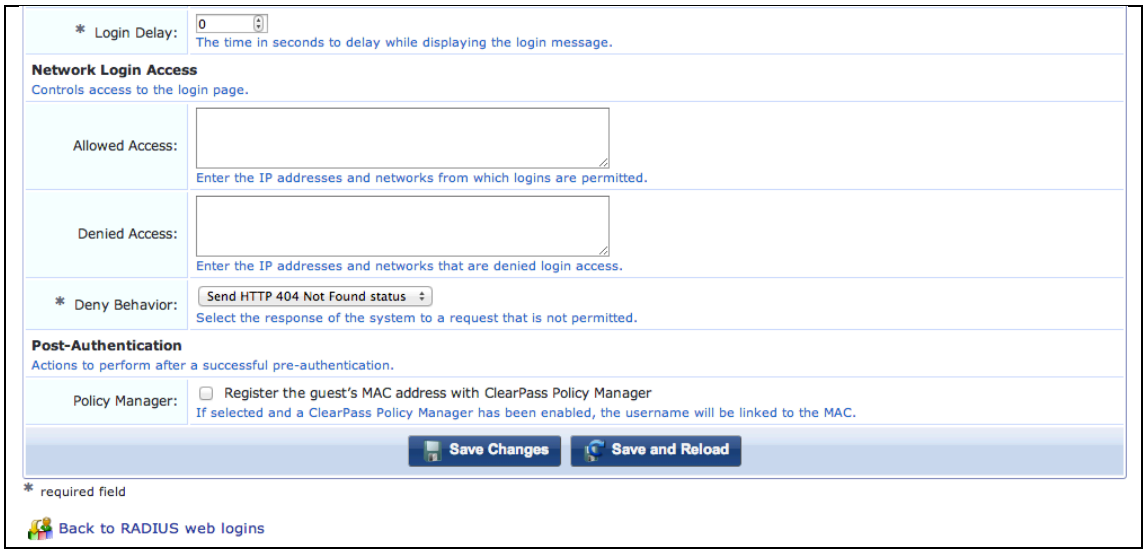
4. Configure ClearPass Guest
4.1. At ClearPass Guest > Configuration > Web Logins, and click “Create new WebLogin page”



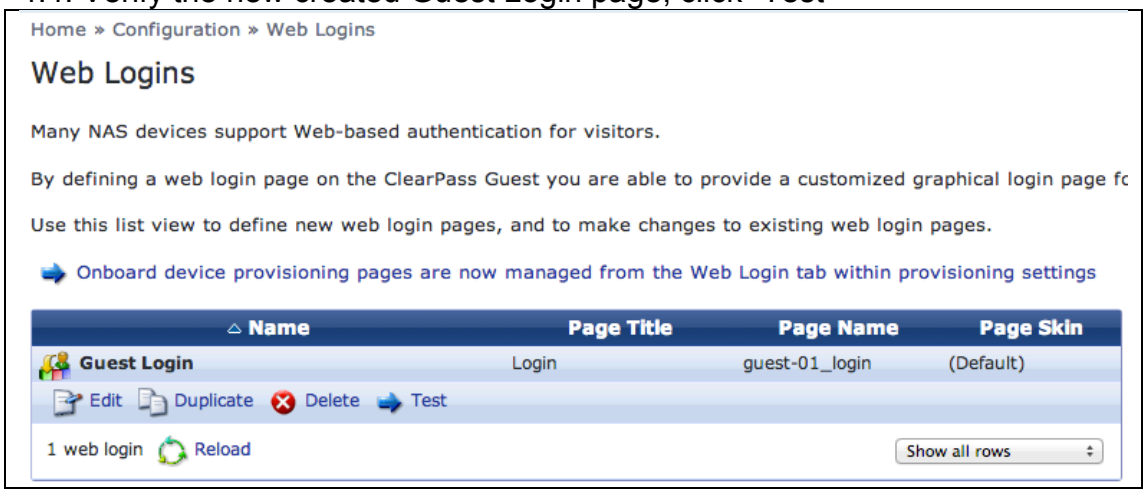
4.2. Set name to “Gest-X login”, and page name “guest-X_login”



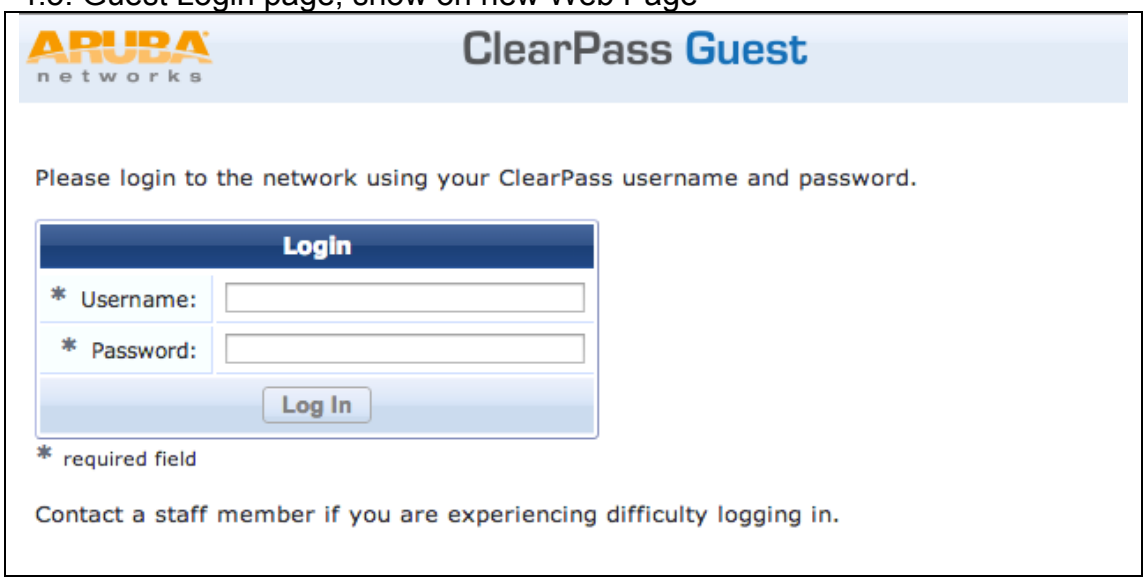
4.3. Keep use defaults values, click “Save and Reload” button & “Back to RADIUS web logins”



4.4. Verify the new created Guest Login page, click "Test"



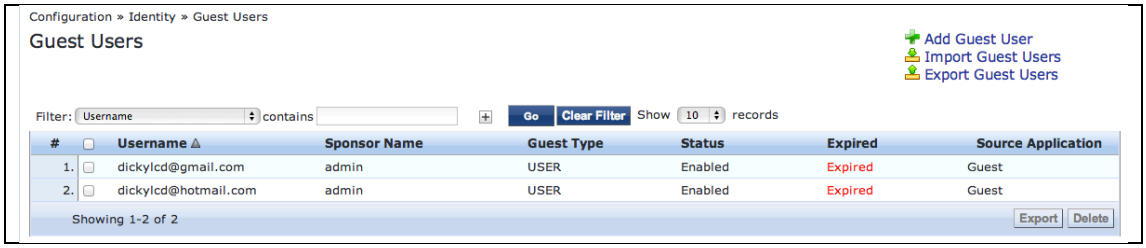
4.5. Guest Login page, show on new Web Page



5. Create New Guest User for Testing

5.1. At ClearPass Policy Manager, Configuration > Identity > Guest User

5.2. Click “Add Guest User”

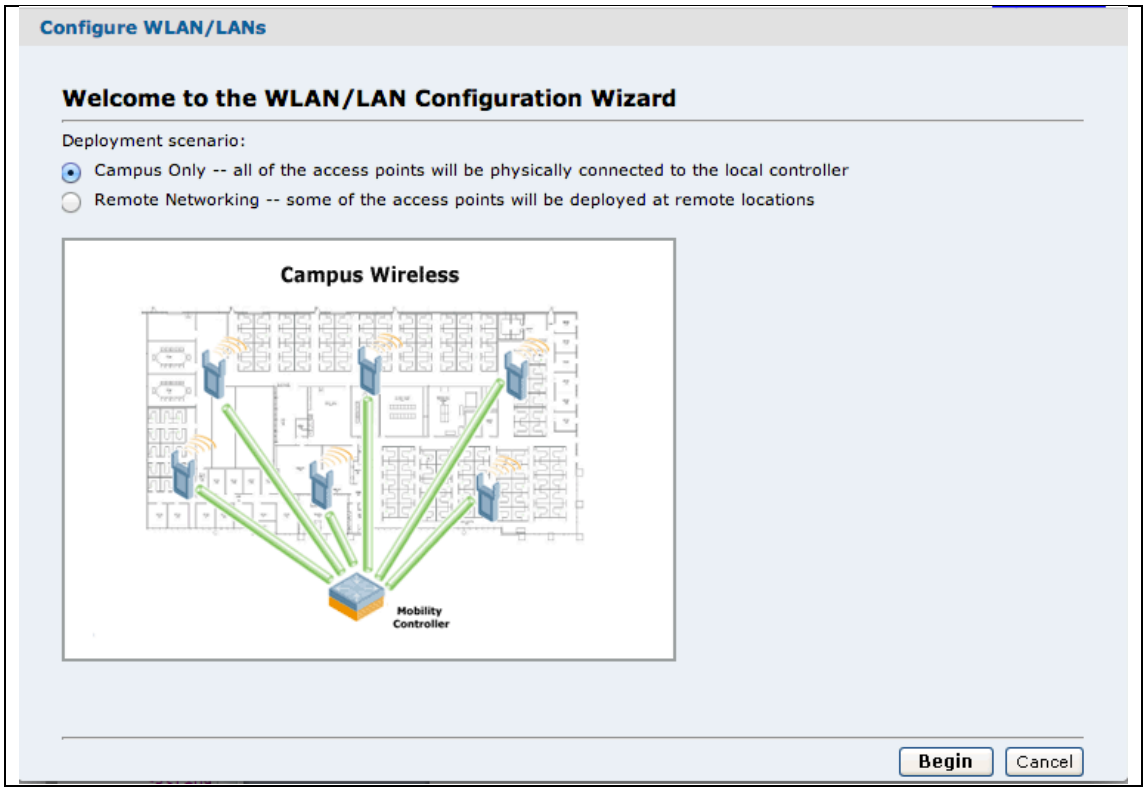


5.3. Create guest user, and then click “Add” button

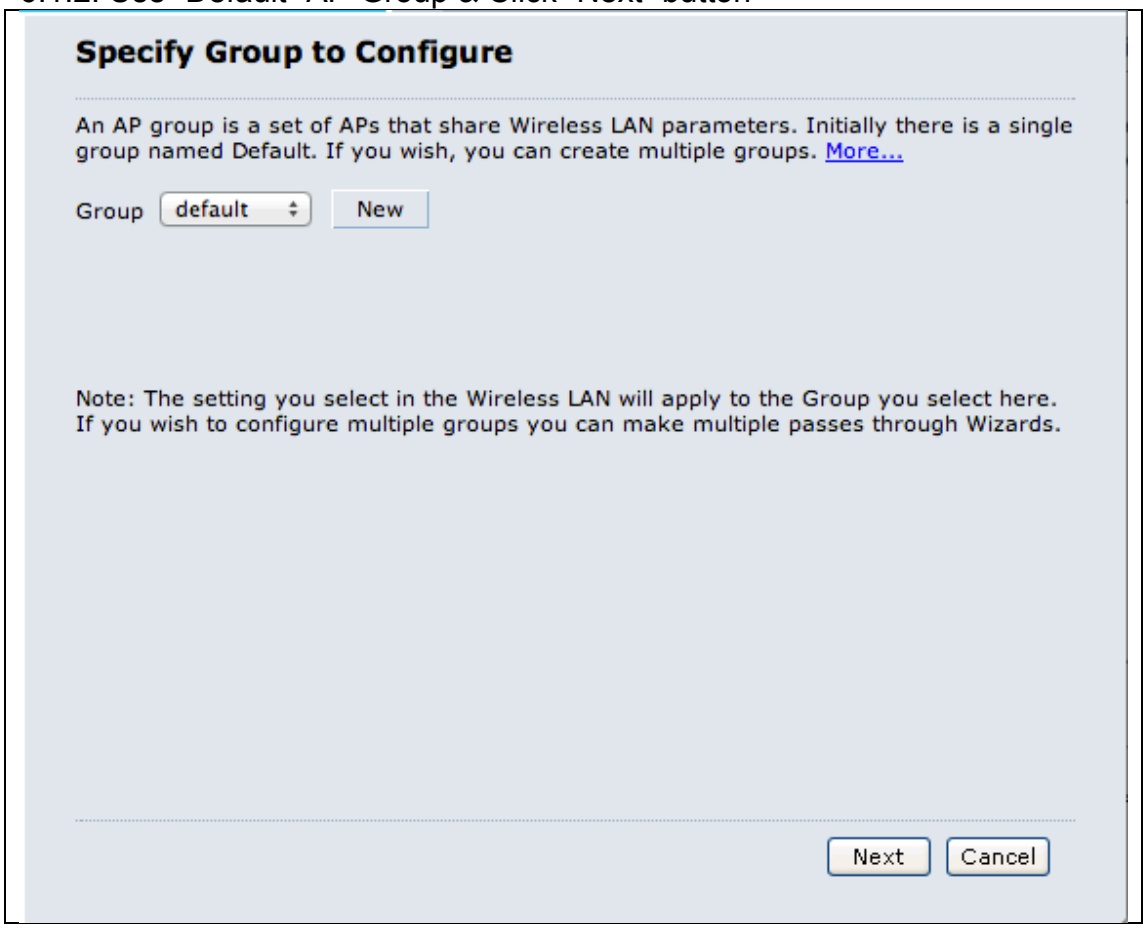
6. Configure WLAN on Controller

6.1. At Controller WebUI, go to Configuration > WLAN/LAN Wizard

6.1.1. Configure WLAN/LANs, Click “Campus” & “Begin” button



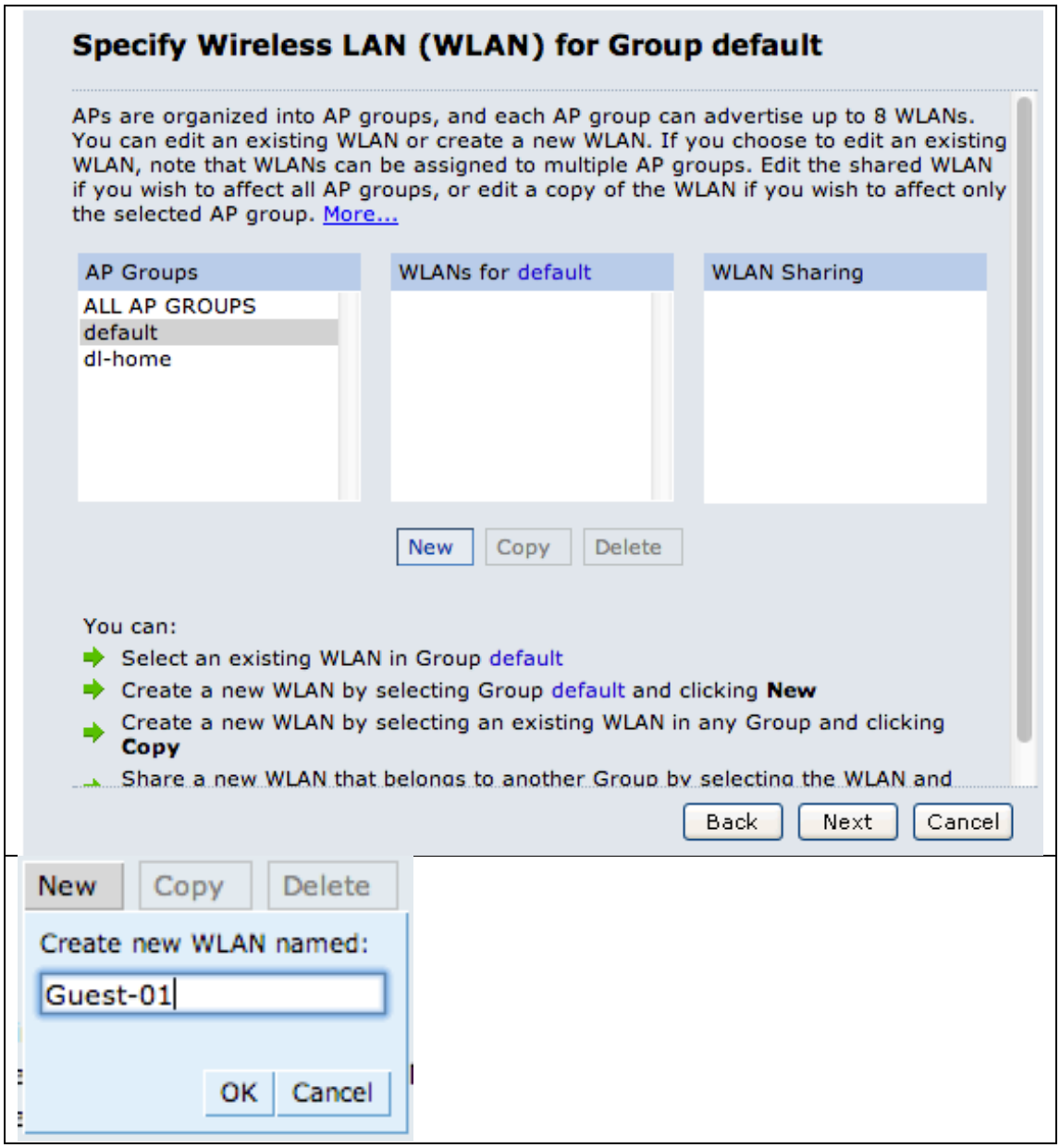
6.1.2. Use “Default” AP-Group & Click “Next” button



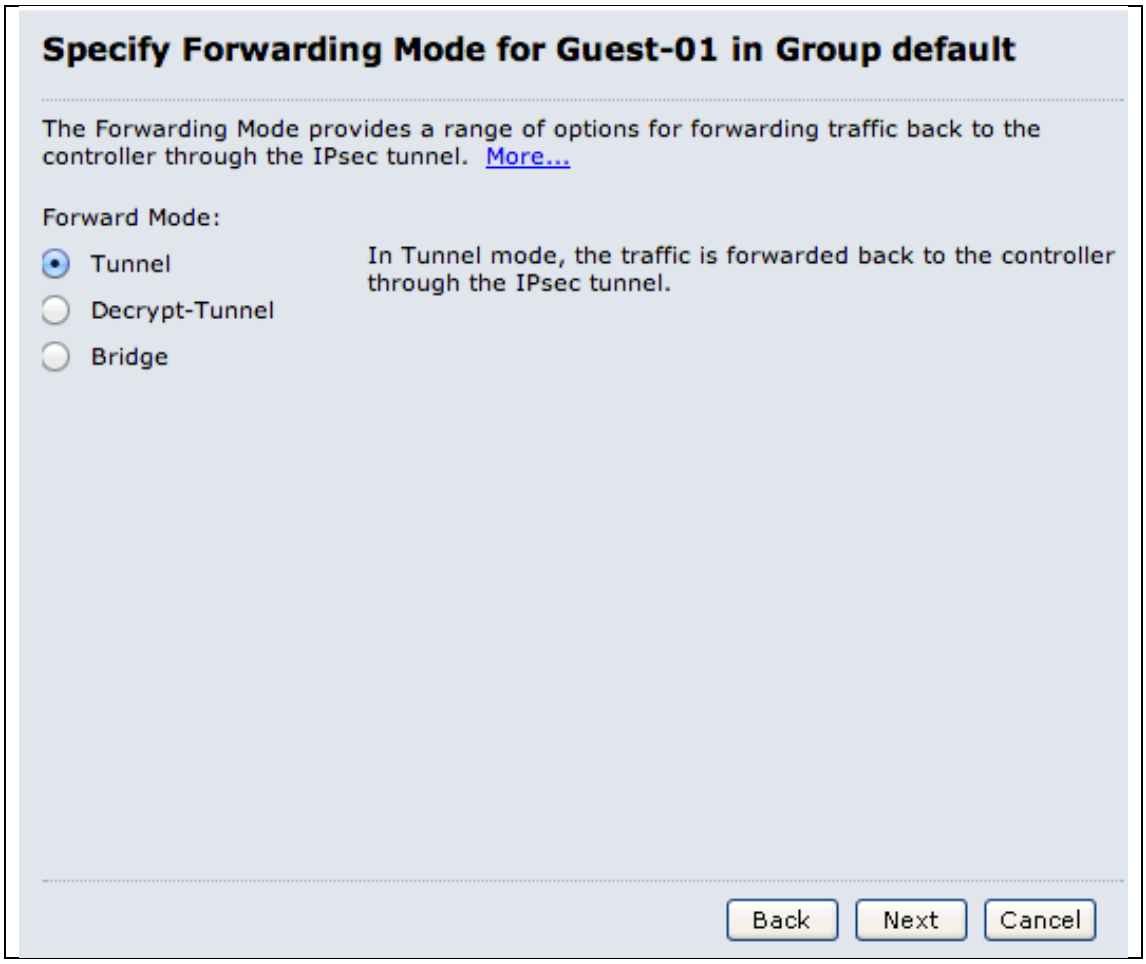
6.1.3. At “Ready to Configure Wireless LANs for Group default”, click

"Continue".

6.1.4. At Specify Wireless LAN (WLAN) for Group default, Click "New" button enter "Guest-X" & click "Next" button for continue



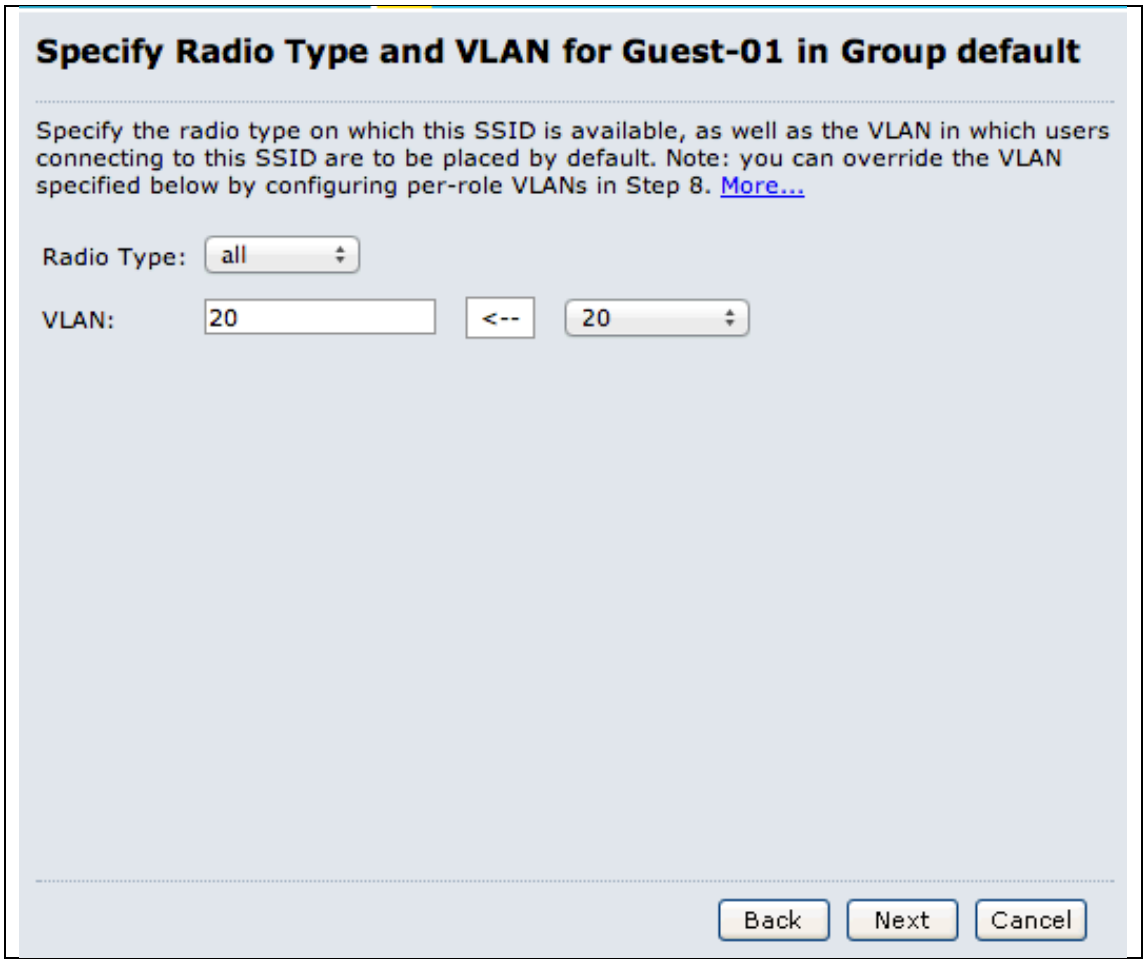
6.1.5. Specify Forwarding Mode for Guest-X in Group default, select "Tunnel" forward mode & click "Next" button for continue



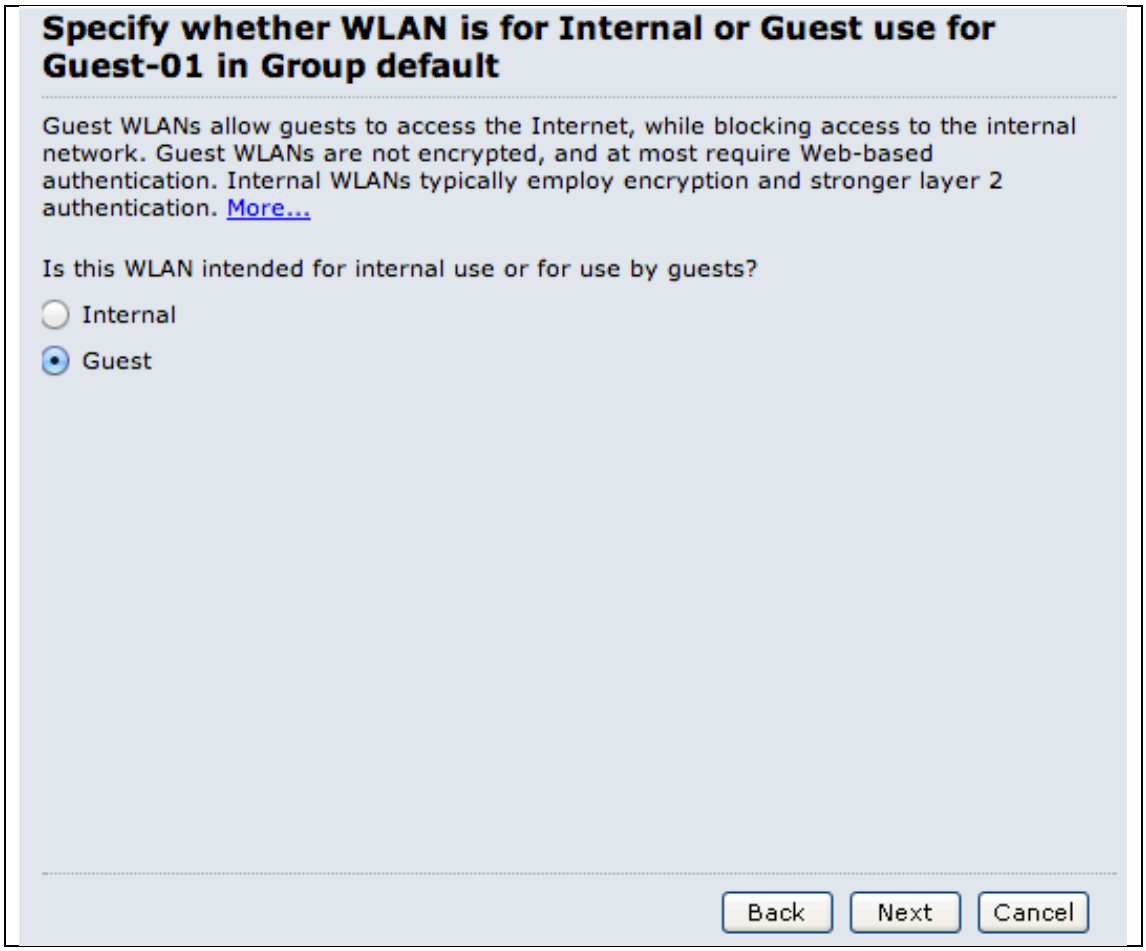
6.1.6. Specify Radio Type and VLAN for Guest-X in Group default:

- Radio Type: All
- VLAN: 20

Click “Next” button for continue.



6.1.7. Specify whether WLAN is for Internal or Guest use for Guest-X in Group default, Select “Guest” & click “Next” button for continue

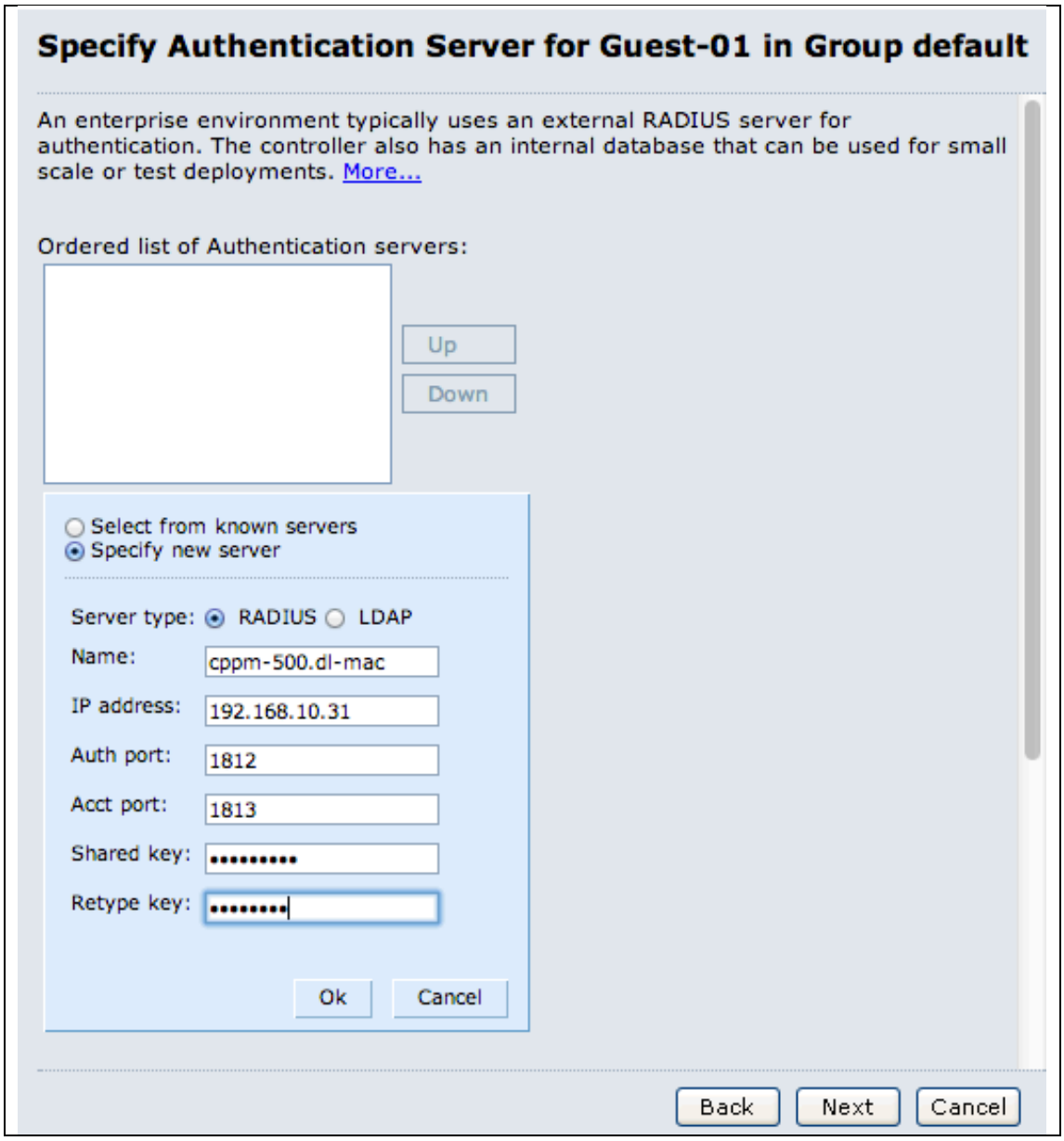


6.1.8. Specify Authentication and Encryption for Guest-X in Group default, select “Captive portal with authentication via credentials (username and password) provided by user.”

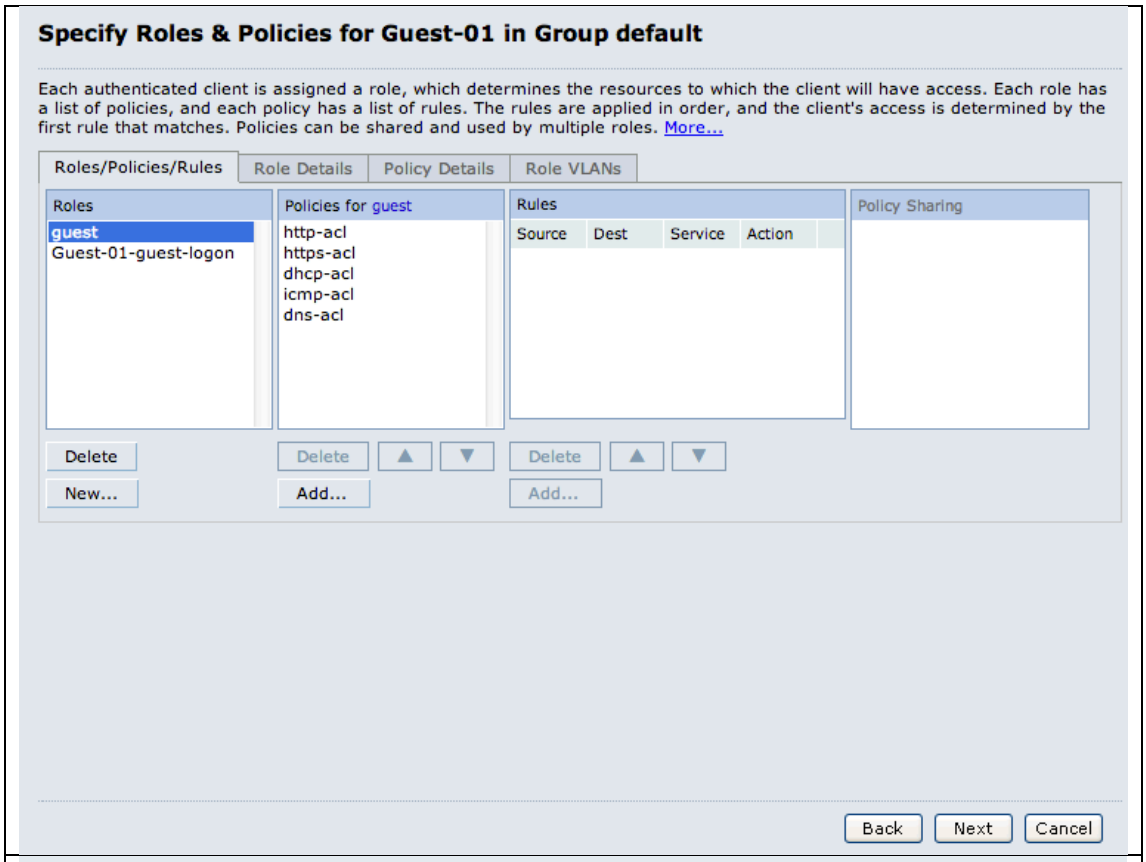
6.1.9. Keep default configure at Specify Captive Portal Options for Guest-X in Group default, click “Next” button for continue

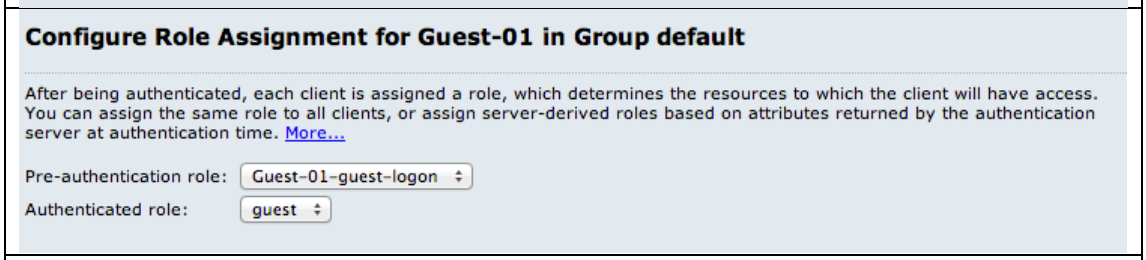
6.1.10. Specify Authentication Server for Guest-X in Group default, click "New" button to add new Authentication servers and enter following:

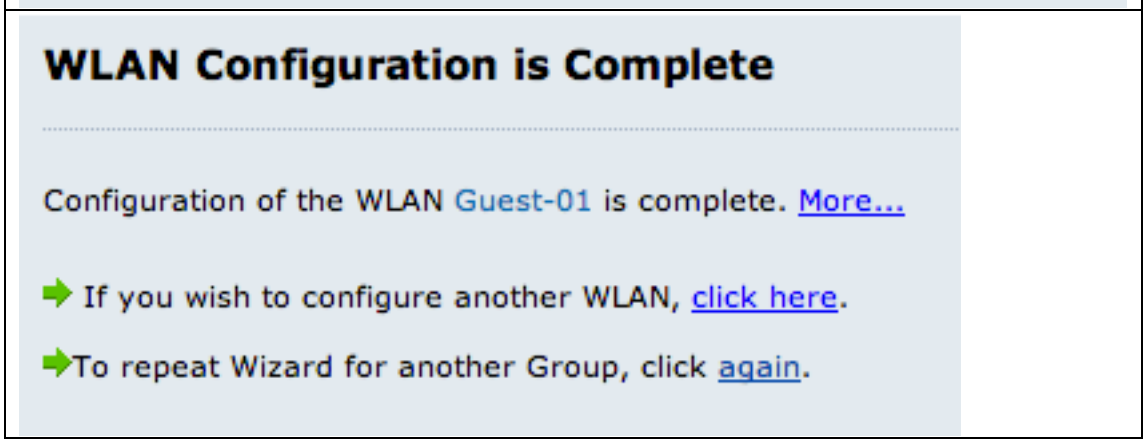
- Select "Specify new server"
- Server type: RADIUS
- Name: cppm-500.X
- IP Address: 192.168.10.XX
- Auth port: 1812 (default value)
- Acct port: 1813 (default value)
- Shared key & Retype key: aruba123

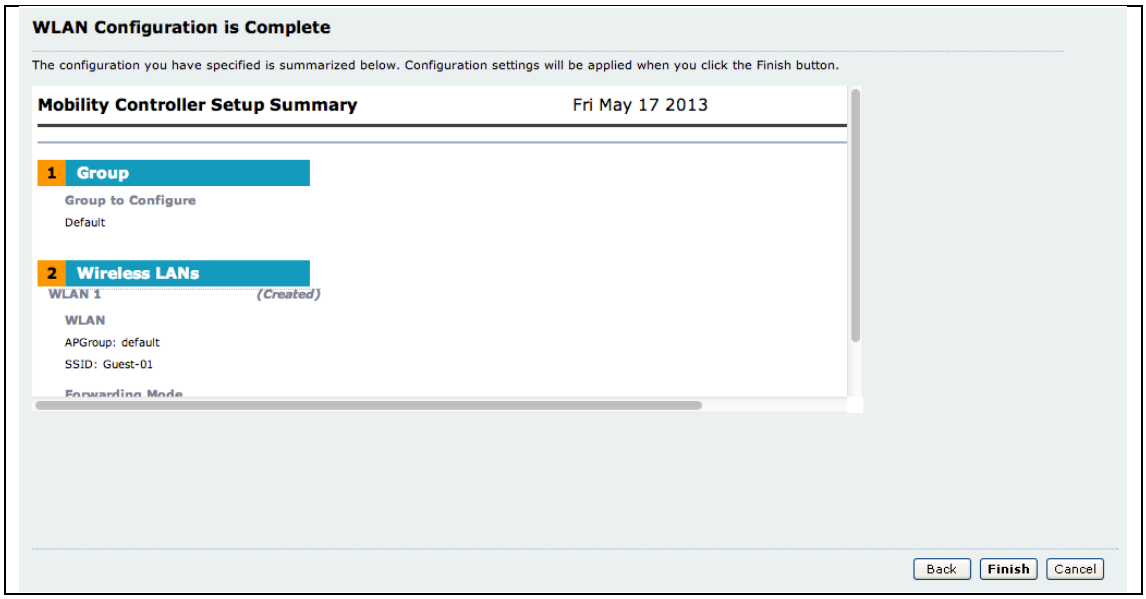


6.1.11. Select “Guest” roles and keep default value and click “Finish” button to complete configuration


Specify Roles & Policies for Guest-01 in Group default
Each authenticated client is assigned a role, which determines the resources to which the client will have access. Each role has a list of policies, and each policy has a list of rules. The rules are applied in order, and the client's access is determined by the first rule that matches. Policies can be shared and used by multiple roles. More...
Roles/Policies/Rules
Role Details
Policy Details
Role VLANs
Roles
guest
Guest-01-guest-logon
Policies for guest
http-acl
https-acl
dhcp-acl
icmp-acl
dns-acl
Rules
Source
Dest
Service
Action
Policy Sharing
Delete
New...
Delete
Add...
Delete
Add...
Back
Next
Cancel

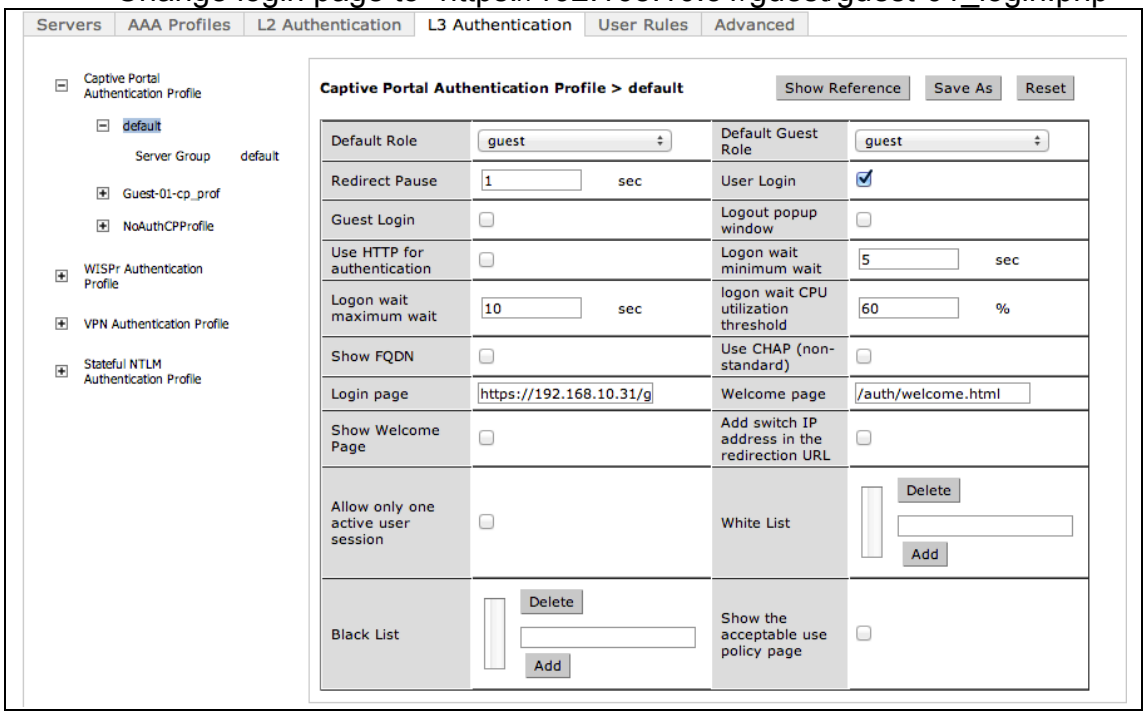

Configure Role Assignment for Guest-01 in Group default
After being authenticated, each client is assigned a role, which determines the resources to which the client will have access. You can assign the same role to all clients, or assign server-derived roles based on attributes returned by the authentication server at authentication time. More...
Pre-authentication role:
Guest-01-guest-logon
Authenticated role:
guest


WLAN Configuration is Complete
Configuration of the WLAN Guest-01 is complete. More...
If you wish to configure another WLAN, click here.
To repeat Wizard for another Group, click again.



7. Modify Captive Portal Profile
7.1. At Configuration > Security > Authentication > L3 Authentication
7.2. Select the Captive Portal Profile the wizard created, and change as followings:

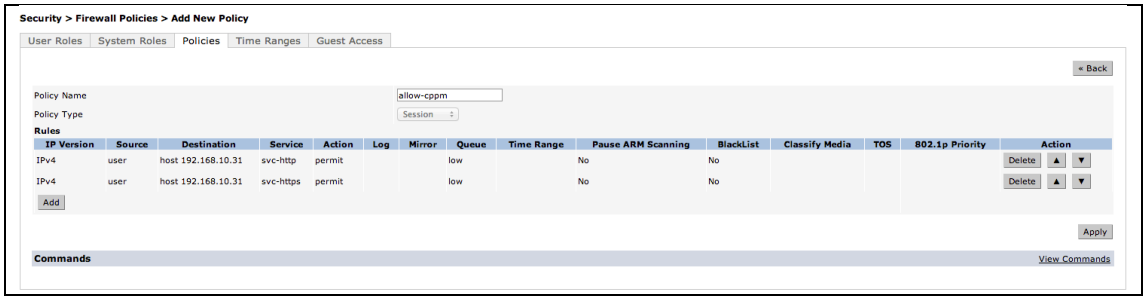
- Disable welcome page
- Change redirect pause to 1
- No Logout Pop-Up Windows
- Change login page to “https://192.168.10.31/guest/guest-01_login.php”



8. Modify Pre Authentication Role
8.1. At Configuration > Security > Access Control > Polices
8.2. Create new policy as below:

- Policy Name: allow-cppm

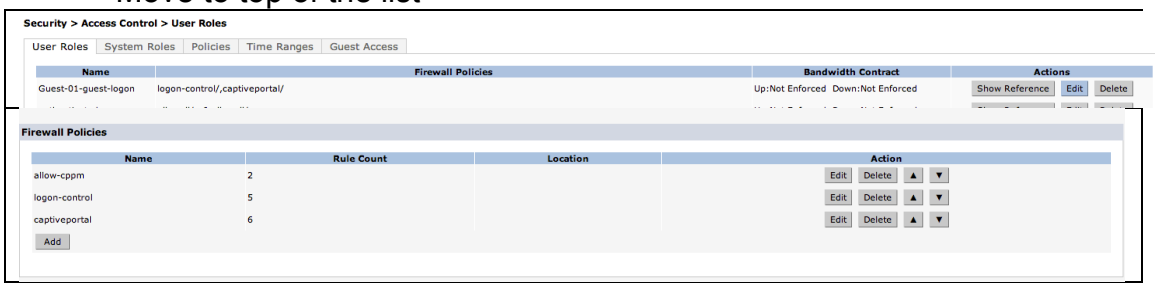
- Source: User
- Destination: CPPM IP Address
- Service: HTTP and HTTPS
- Action: Permit



8.3. At Configuration > Security > Access Control > User Roles

8.3.1. Modify “Guest-X-guest-logon” role which created at Wizard:

- Add “allow-cppm” policy to Role
- Move to top of the list



9. Testing

9.1. Connect client to new created SSID “Guest-X”

9.2. Open Web Browser, and it will redirected to Captive Portal

9.3. Enter credential created before

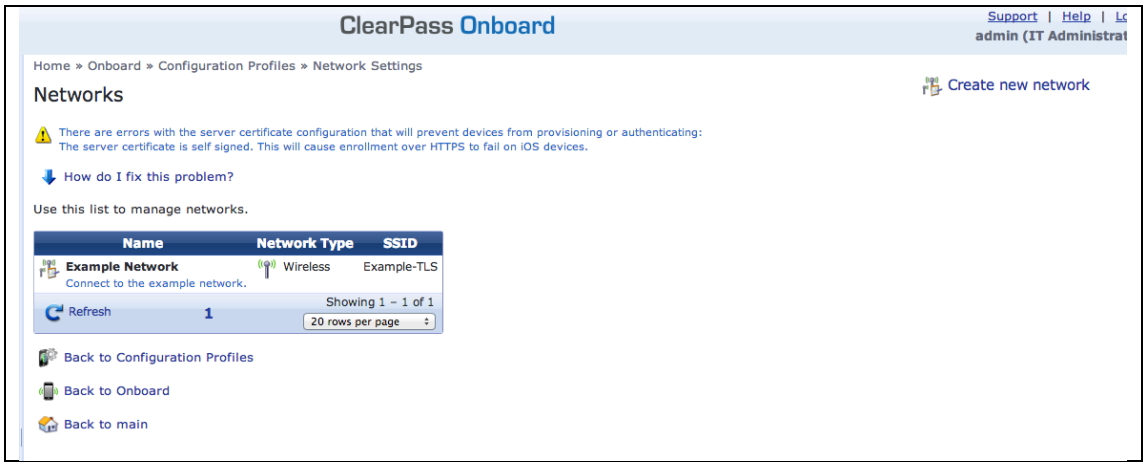
- It should login success and able to access to Internet
- It will show on ClearPass Access Checker.

2.2. ClearPass – Onboard

So with CP6.1, CPG has changed but it still has the same look and feel of CPG 3.9.x

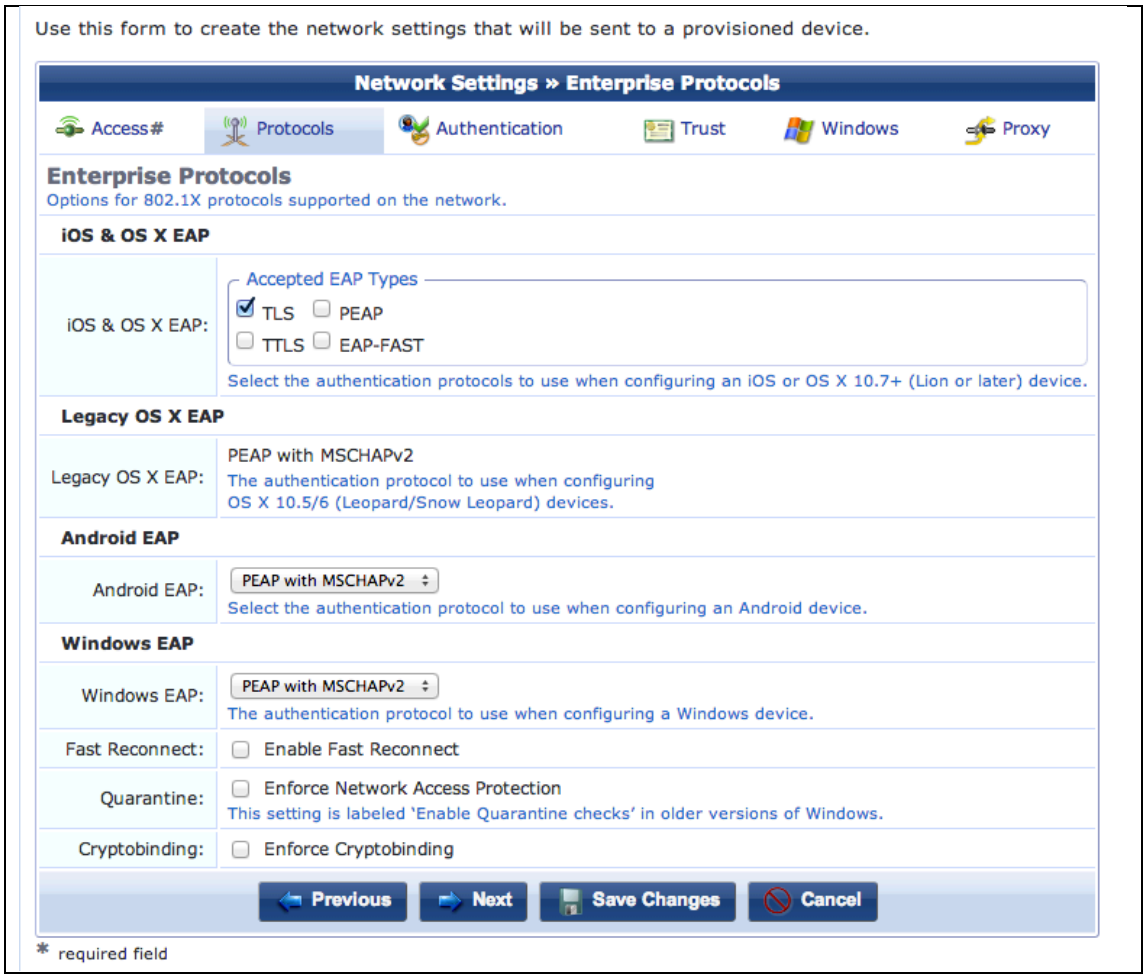
You already know how to use the quick link to get to it. You can also connect to it directly it using your browser. The IP address is the same as CPPM but with /guest. In fact all the CPG URLs has been prepended with /guest (al the web logins, self-registration, etc.)

1. Onboard Network Settings, at ClearPass Guest > Onboard > Configuration profiles > Network Settings, click “Create new network” for create new network

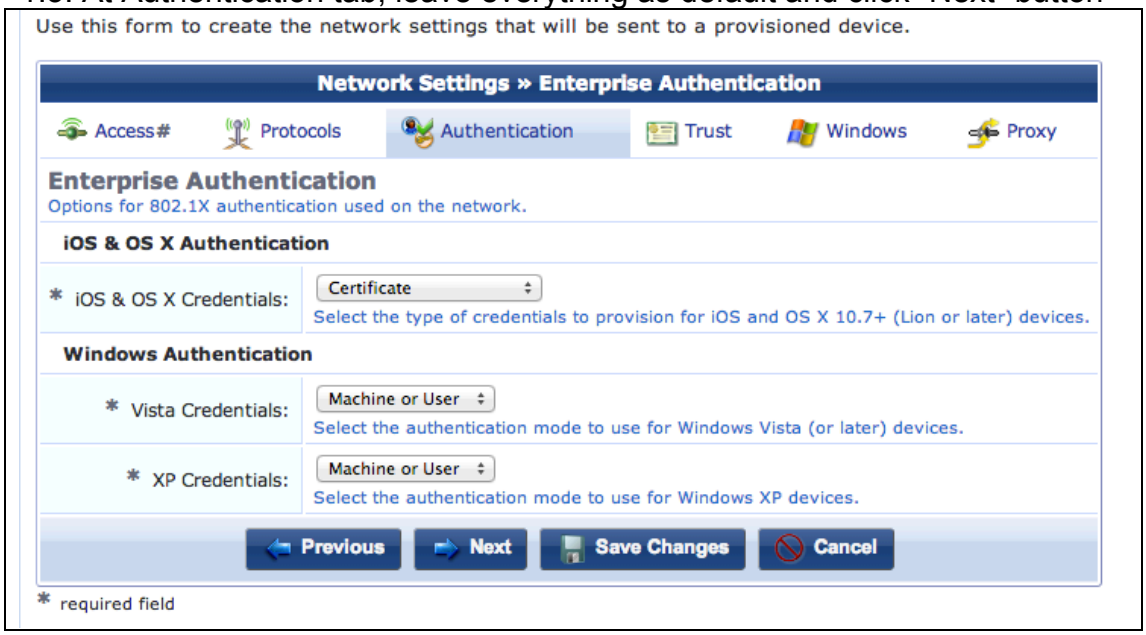


1.1. Enter Network Access name “SecureWLAN” and SSID “securewlan”, click “Next” button

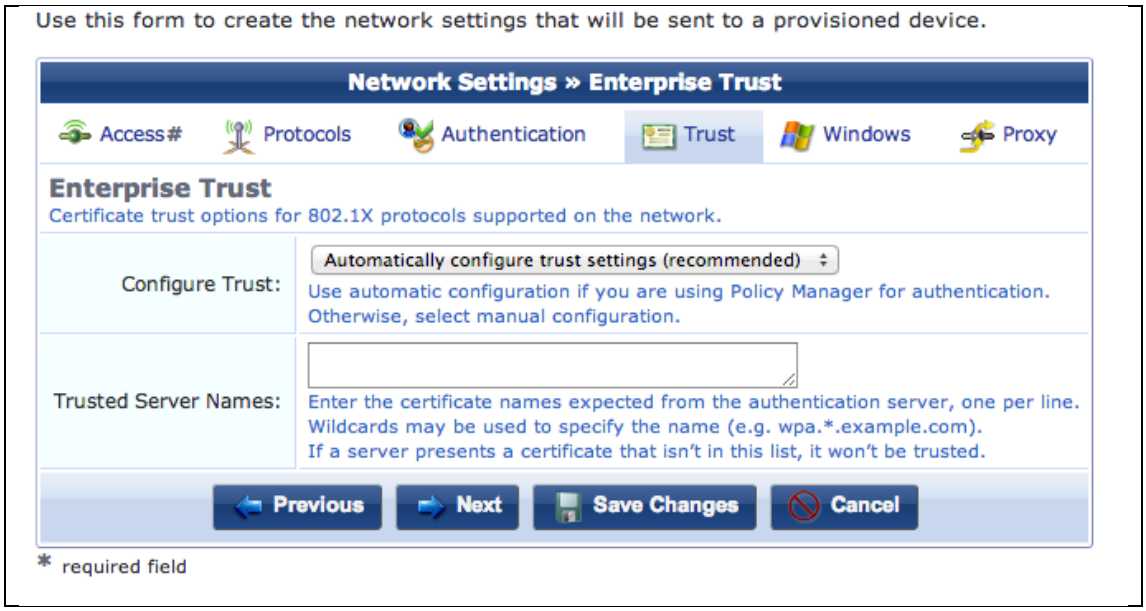
1.2. At protocols tab, leave everything as default and click “Next” button



1.3. At Authentication tab, leave everything as default and click “Next” button

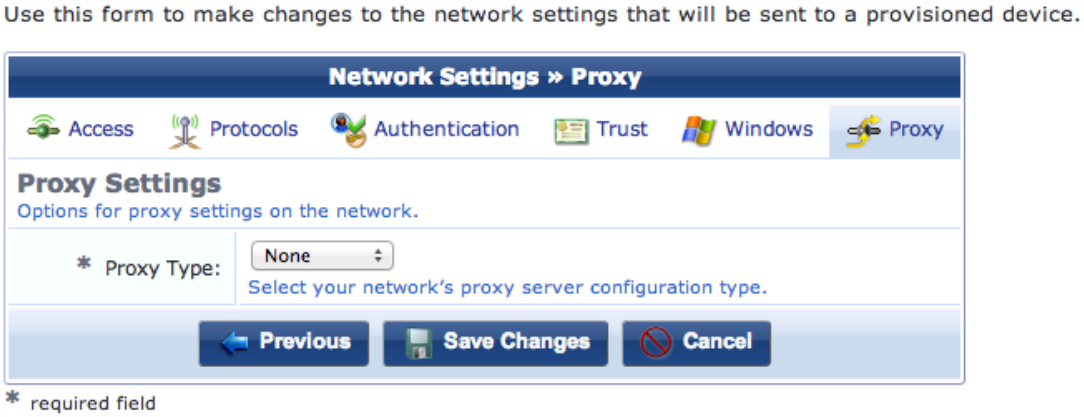


1.4. At Trust tab, leave everything as default and click “Next” button

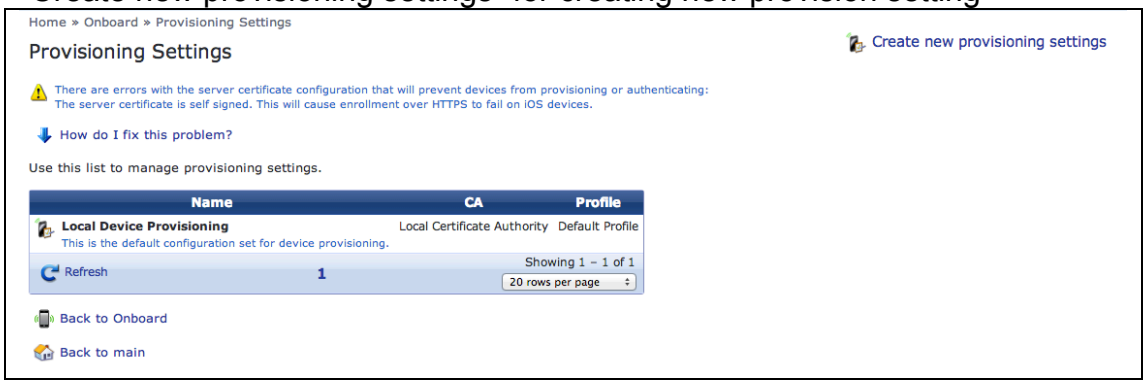


1.5. At Windows tab, leave everything as default and click “Next” button

1.6. At Proxy tab, leave everything as default and click “Save Changes” button



2. Onboard Provisioning Settings, at Onboard > Provisioning Settings, click "Create new provisioning settings" for creating new provision setting



2.1. At General tab, enter below information:
Name: SecureWLAN Device Provisioning
Organization: APJ ClearPass Workshop
Certificate Authority: Local Certificate Authority
Key Type: 2048-bit RSA – created by server
Maximum Devices: 1
Click "Next" to continue

Provisioning Settings

There are errors with the server certificate configuration that will prevent devices from provisioning or authenticating:
The server certificate is self signed. This will cause enrollment over HTTPS to fail on iOS devices.

How do I fix this problem?

Use this form to make changes to the basic configuration options for device provisioning.

Device Provisioning Settings

General | Web Login | iOS & OS X | Legacy OS X | Windows | Android | Onboard Client

* Name:	SecureWLAN Device Provisioning Enter a name for this configuration set.
Description:	Enter a description for the configuration set.
* Organization:	APJ ClearPass Workshop Enter an organization name for this configuration set. The organization name is displayed by the device during provisioning.

Identity
These options control the generation of device credentials

* Certificate Authority:	Local Certificate Authority Select the certificate authority that will be used to sign profiles and messages.
* Key Type:	2048-bit RSA — created by server Select the type of private key to use for TLS certificates.
* Unique Device Credentials:	☑ Include the username in unique device credentials When checked, the username is prefixed to the device's PEAP credentials. This unique set of credentials is used to identify the user and device on the network.

Authorization
These options control how a device is authorized during provisioning.

* Configuration Profile:	Default Profile Select the configuration profile that will be provisioned to devices.
* Maximum Devices:	1 The maximum number of devices that a user may provision. Use 0 for unlimited.

Supported Devices
These options control which devices may be provisioned.

* iOS & OS X Devices:	☑ Enable iOS and OS X 10.7+ (Lion or later) device provisioning Provision iOS and OS X 10.7+ (Lion or later) devices via Apple's 'Over-the-Air' profile delivery process.
* OS X 10.5/6 Devices:	☑ Enable OS X 10.5 (Leopard) and 10.6 (Snow Leopard) device provisioning Downloads and executes an OS X application on a user's device to complete provisioning.
* Windows Devices:	☑ Enable Windows XP, Vista and 7 (or later) device provisioning Downloads and executes a Windows application on a user's device to complete provisioning.
* Android Devices:	☑ Enable Android device provisioning Downloads and executes an Android application on a user's device to complete provisioning.
Unsupported Device:	{nwa_icontext type=error} {nwa_text id=10891}Your operating system is not supported. Please contact your network administrator.{/nwa_text} {/nwa_icontext} Insert content item... These instructions are shown to the user if they attempt to provision an unsupported device. Enter the HTML code to display. Smarty template functions can be used here. Leave this field empty to use the default instructions.

Next | Save Changes | Cancel

* required field

2.2. At Web Login / iOS & OS X tab / Legacy OS X / Windows / Android tabs,

use default value and click “Next” button for continue

Use this form to make changes to the basic configuration options for device provisioning.

Device Provisioning Settings

General# | Web Login | iOS & OS X | Legacy OS X | Windows | Android | Onboard Client

Web Login Page

Options for the weblogin landing page for Onboard.

* Page Name:	device_provisioning2 Enter a page name for this web login. The web login will be accessible from "/guest/page_name.php".

Login Form

Options for specifying the behaviour and content of the login form.

Custom Form:	☐ Provide a custom login form If selected, you must supply your own HTML login form in the Header or Footer HTML areas.
Custom Labels:	☐ Override the default labels and error messages If selected, you will be able to alter labels and error messages for the current login form.
Terms:	☐ Require a Terms and Conditions confirmation If checked, the user will be forced to accept a Terms and Conditions checkbox.

Login Page

Options for controlling the look and feel of the login page.

* Skin:	(Default) Choose the skin to use when this web login page is displayed.
Title:	Register Your Device The title to display on the web login page.
Header HTML:	{nwa_cookiecheck} {* Onboard instructions can be edited on a per device type basis under Onboard Provisioning Settings *} Insert content item... | Insert self-registration link... HTML template code displayed before the login form.

Footer HTML:

```
<p>
Contact a staff member if you are experiencing
difficulty logging in.
</p>
```

Insert content item... | Insert self-registration link...

HTML template code displayed after the login form.

Network Login Access

Controls access to the login page.

Allowed Access:

Enter the IP addresses and networks from which logins are permitted.

Denied Access:

Enter the IP addresses and networks that are denied login access.

* Deny Behavior: Send HTTP 404 Not Found status

Select the response of the system to a request that is not permitted.

Previous | Next | Save Changes | Cancel

* required field

Use this form to make changes to the basic configuration options for device provisioning.

Device Provisioning Settings

General# | Web Login | iOS & OS X | Legacy OS X | Windows | Android | Onboard Client#

iOS & OS X Provisioning

These options control Apple iOS (iPad, iPod, iPhone) and OS X (Lion or later) device provisioning.

* Display Name: Device Enrollment

Example: 'Device Enrollment'.
This text is displayed as the title of the 'Install Profile' screen on the device.

* Profile Description:

```
This configuration profile has network and security settings for your device to allow
you to connect to the intranet and access local applications.
```

Enter the description to display on the 'Install Profile' screen of the device.
This should provide help text for the user and instruct them to install the profile.

* Profile Security: Always allow removal

Select when the configuration profile may be removed.

Profile Type: User

Select the type of profile to create when provisioning OS X 10.7+ (Lion or later) devices.

Edit ID: ☐ Change the profile ID

The current profile ID is **'com.example.device.provisioning.a9e483e9-48d5-4a1e-9931-489fafa74446'**

Profile Signing

These options control the way profiles are signed for iOS and OS X devices.

* Certificate Source: Generate using the Onboard CA

Choose how to obtain the certificate used to sign iOS and OS X 10.7+ profiles.

* Common Name: Device Enrollment (Profile Signing)

Enter the common name to use for the certificate used to sign iOS and OS X 10.7+ profiles.
This will appear as the "Signed" field on the install profile dialog.

Instructions

These options control the text shown during provisioning for iOS and OS X devices.

Before Provisioning:

```
<p>
Please configure security and network settings on your device to allow
secure<br>access to the internal network. Please follow the instructions listed
below:<br><br>
{if $client_require_root}
<strong>{counter}.</strong>    {nwa_iconlink
icon="images/icon-certificate22.png" text="Install root certificate (click here)"}
{nwa_mdps_config name=root_cert}{/nwa_iconlink}{nwa_mdps_config
name=root_cert_warning}<br>
{/if}
<strong>{counter}.</strong>    Login below using your
{nwa_mdps_config name=organization_name} credentials<br>
<strong>{counter}.</strong>    Install the certificate
when prompted<br>
<strong>{counter}.</strong>    Go to your Wi-Fi
```

Insert content item...

These instructions are shown to the user before they provision an iOS or OS X 10.7+ (Lion or later) device.
Enter the HTML code to display. Smarty template functions can be used here.
Leave this field empty to use the default instructions.

After Provisioning:

```
{**
 * OPTIONAL. The contents of this section will
 * be shown AFTER the device has been provisioned,
 * but BEFORE any reconnection attempt has been
 * made (either automatic or manual).
 *}
```

Insert content item...

These instructions are shown to the user after they have provisioned an iOS or OS X 10.7+ (Lion or later) device.
Enter the HTML code to display. Smarty template functions can be used here.
Leave this field empty to use the default instructions.

iOS-4 Same SSID:

```
{nwa_icontext type=error}
{nwa_text id=11018}Provisioning using this SSID is not supported for your iOS 4
device.{/nwa_text}
{/nwa_icontext}
{nwa_text id=11017 1=$extra_fields.essid}
<p>
 Due to a software issue with iOS 4, you cannot provision your iOS device
 using the <b>%1</b> SSID, to which you are currently connected.
</p>
{/nwa_text}
{nwa_icontext type=arrow}
{nwa_text id=11016}Please connect and login using a different SSID.{/nwa_text}
{/nwa_icontext}
```

Insert content item...

Due to a software issue with iOS 4, 'same SSID' provisioning is not supported.
These instructions are shown to the user of an iOS 4 device if they attempt to provision their device while connected to an SSID that will be provisioned.

Enter the HTML code to display. Smarty template functions can be used here.
Leave this field empty to use the default instructions.

Reconnect

These options control the reconnect behaviour for iOS and OS X devices.
Reconnect is only supported by iOS 5+ and OS X 10.7+ (Lion or later) devices.

*** Allow Automatic Reconnect:**

☑ Allow the device to be automatically reconnected to the provisioned network

Automatic reconnect is only possible if there is a single network configured with 'Automatically join network', and the controller provides both the 'mac' and 'switchip' parameters to the captive portal.
Reconnect is only supported by iOS 5+ and OS X 10.7+ (Lion or later) devices.

*** Allow Manual Reconnect:**

☑ Allow the device to be manually reconnected to the provisioned network

Manual reconnect is only applicable if automatic reconnect is not allowed or not applicable.
Reconnect is only supported by iOS 5+ and OS X 10.7+ (Lion or later) devices.

Manual Reconnect Interface:

```
{**
 * The contents of this section can be
 * used to provide the user with a manual
 * reconnect user interface.
 *}
{nwa_icontext icon="images/icon-radius-session-active22.png"}
 {nwa_text id=11015 1=$ssids.0}You should now connect to the <b>%1</b>
network using the installed settings.{/nwa_text}
{/nwa_icontext}
<div>
{**
 * The network name passed to the
 * 'ConnectNetwork' function is used
 * for display only.  It does NOT
 * 'control' which network a device
 * will connect to.
 *}
 <a href="#Connect"
   style="margin-left: 26px;"
   onclick="return ConnectNetwork('{$ssids.0|NwaQuoteJsBody}');">
```

Insert content item...

The contents of this section will be shown if a manual reconnect is allowed and applicable. Reconnect is only supported by iOS 5+ and OS X 10.7+ (Lion or later) devices.

Enter the HTML code to display. Smarty template functions can be used here. Leave this field empty to use the default instructions.

Connect Success:

```
{**
 * OPTIONAL. The contents of this section
 * will be shown AFTER a SUCCESSFUL
 * reconnect.
 *}
```

Insert content item...

The contents of this section will be shown after a successful reconnect.

Enter the HTML code to display. Smarty template functions can be used here. Leave this field empty to use the default instructions.

Connect Failure:

```
{**
 * OPTIONAL. The contents of this section
 * will be shown AFTER a FAILED reconnect.
 *}
{if $auto_connect}
 {nwa_icontext icon="images/icon-radius-session-active22.png"}
  {nwa_text id=11770 1=$auto_connect_network}You should now change your
network settings. Select the <b>%1</b> network to access the intranet.
{/nwa_text}
 {/nwa_icontext}
{elseif empty($ssids)}
 {nwa_icontext icon="images/icon-radius-session-active22.png"}
  {nwa_text id=11014}You should now change your network settings.{/nwa_text}
 {/nwa_icontext}
{elseif count($ssids) == 1}
 {nwa_icontext icon="images/icon-radius-session-active22.png"}
  {nwa_text id=9920 1=$ssids.0}You should now change your network settings.
Select the <b>%1</b> SSID to access the intranet.{/nwa_text}
 {/nwa_icontext}
{else}
```

Insert content item...

The contents of this section will be shown after a failed reconnect or if the device does not support reconnection, such as for iOS 4 (and earlier) devices.

Enter the HTML code to display. Smarty template functions can be used here. Leave this field empty to use the default instructions.

After Connect:

```
{**
 * OPTIONAL. The contents of this section
 * will be shown AFTER a reconnect attempt,
 * regardless of success or failure.
 *}
```

Insert content item...

The contents of this section will be shown after a reconnect attempt, regardless of success or failure.

Enter the HTML code to display. Smarty template functions can be used here. Leave this field empty to use the default instructions.

*** Advanced Settings:** ☑ Show advanced reconnection settings

*** Disconnect Delay:** 3 seconds

When the web server receives a disconnect request, it will wait for this duration before issuing the disconnect request to the controller.

This delay gives the client time to receive a valid HTTP response before begin disconnected from the network.

* Reconnect Delay:	10 seconds After the client sends a disconnect request to the web server, it will wait for this duration before attempting to send a reconnect request. This timer needs to give the web server and the controller enough time to negotiate a disconnect for the device.
* Reconnect Timeout:	15 seconds After the client has sent a reconnect request to the web server, it will wait for this duration to receive a valid response. This timer needs to allow enough time for the client to be reconnected to the network (using the newly installed settings) and for the web server to then acknowledge the HTTP request.

Previous | Next | Save Changes | Cancel

* required field

Use this form to make changes to the basic configuration options for device provisioning.

Device Provisioning Settings

General# | Web Login | iOS & OS X | Legacy OS X | Windows | Android | Onboard Client#

Instructions

These options control the text shown during provisioning for OS X 10.5/6 (Leopard/Snow Leopard) devices.

Before Provisioning:

```
{nwa_text id=10893}<p>To apply the network profile, you need to download and
start the QuickConnect application.</p>{/nwa_text}
{assign var=link_text value=10899|NwaText:'Download and start the QuickConnect
network configuration application.'}
{assign var=link_command value=10898|NwaText:'Start QuickConnect'}
```

Insert content item...

These instructions are shown to the user before they provision an OS X 10.5/6 (Leopard/Snow Leopard) device.
Enter the HTML code to display. Smarty template functions can be used here.
Leave this field empty to use the default instructions.

After Provisioning:

```
{nwa_text id=10892}<p>QuickConnect will now apply the network profile to your
device.</p>{/nwa_text}
```

Insert content item...

These instructions are shown to the user after they have provisioned an OS X 10.5/6 (Leopard/Snow Leopard) device.
Enter the HTML code to display. Smarty template functions can be used here.
Leave this field empty to use the default instructions.

Previous | Next | Save Changes | Cancel

* required field

Use this form to make changes to the basic configuration options for device provisioning.

Device Provisioning Settings

General# | Web Login | iOS & OS X | Legacy OS X | Windows | Android | Onboard Client#

Windows Provisioning

These options control Windows device provisioning.

* Code-Signing Certificate: None — Do not sign the application

Select a certificate for signing the Windows provisioning application.

Instructions

These options control the text shown during provisioning for Windows devices.

Before Provisioning:

```
{nwa_icontext type=info}
{nwa_text id=10897}In order to connect to this network, your device must be
configured for enhanced security.  Aruba Networks' QuickConnect application will
guide you through the configuration process.{/nwa_text}
{/nwa_icontext}
{nwa_text id=10893}<p>To apply the network profile, you need to download and
start the QuickConnect application.</p>{/nwa_text}
{assign var=link_text value=10899|NwaText:'Download and start the QuickConnect
network configuration application.'}
{assign var=link_command value=10898|NwaText:'Start QuickConnect'}
```

Insert content item...

These instructions are shown to the user before they provision a Windows device.
Enter the HTML code to display. Smarty template functions can be used here.
Leave this field empty to use the default instructions.

After Provisioning:

```
{nwa_text id=10892}<p>QuickConnect will now apply the network profile to your
device.</p>{/nwa_text}
```

Insert content item...

These instructions are shown to the user after they have provisioned a Windows device.
Enter the HTML code to display. Smarty template functions can be used here.
Leave this field empty to use the default instructions.

Previous | Next | Save Changes | Cancel

* required field

Use this form to make changes to the basic configuration options for device provisioning.

Device Provisioning Settings

General# | Web Login | iOS & OS X | Legacy OS X | Windows | Android | Onboard Client#

Android Provisioning

These options control Android device provisioning.

Android Rootkit Detection: Provision all devices

Control whether devices with a rootkit may be provisioned.

Instructions

These options control the text shown during provisioning for Android devices.

Before Provisioning:

```
{nwa_icontext type=info}
{nwa_text id=10897}In order to connect to this network, your device must be
configured for enhanced security.  Aruba Networks' QuickConnect application will
guide you through the configuration process.{/nwa_text}
{/nwa_icontext}
{nwa_text id=10896}<p>To apply the network profile, you first need to download
and install the QuickConnect application from the Android marketplace.</p>
{/nwa_text}
{assign var=link_text value=10903|NwaText:'Download and install the QuickConnect
network configuration application.'}
{assign var=link_command value=10902|NwaText:'Install QuickConnect'}
```

Insert content item...

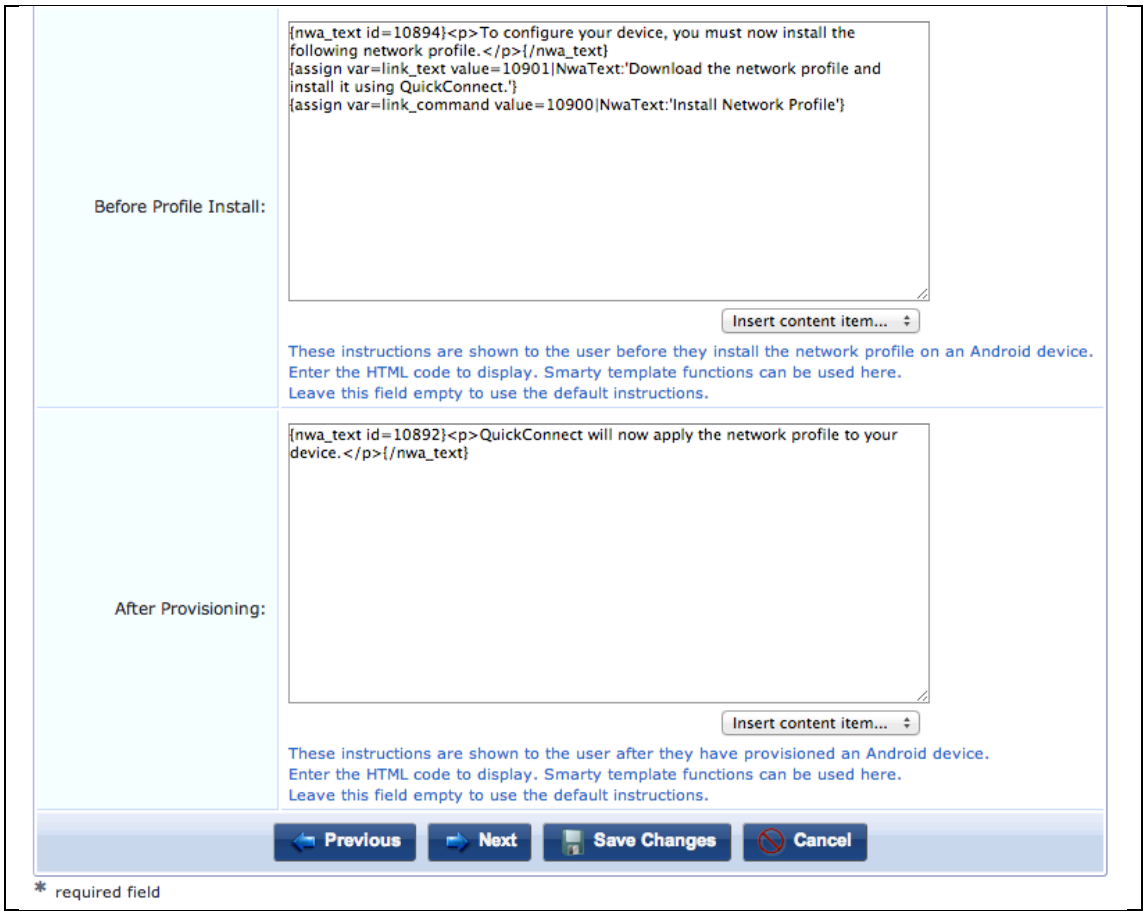
These instructions are shown to the user before they provision an Android device.
Enter the HTML code to display. Smarty template functions can be used here.
Leave this field empty to use the default instructions.

Next Step:

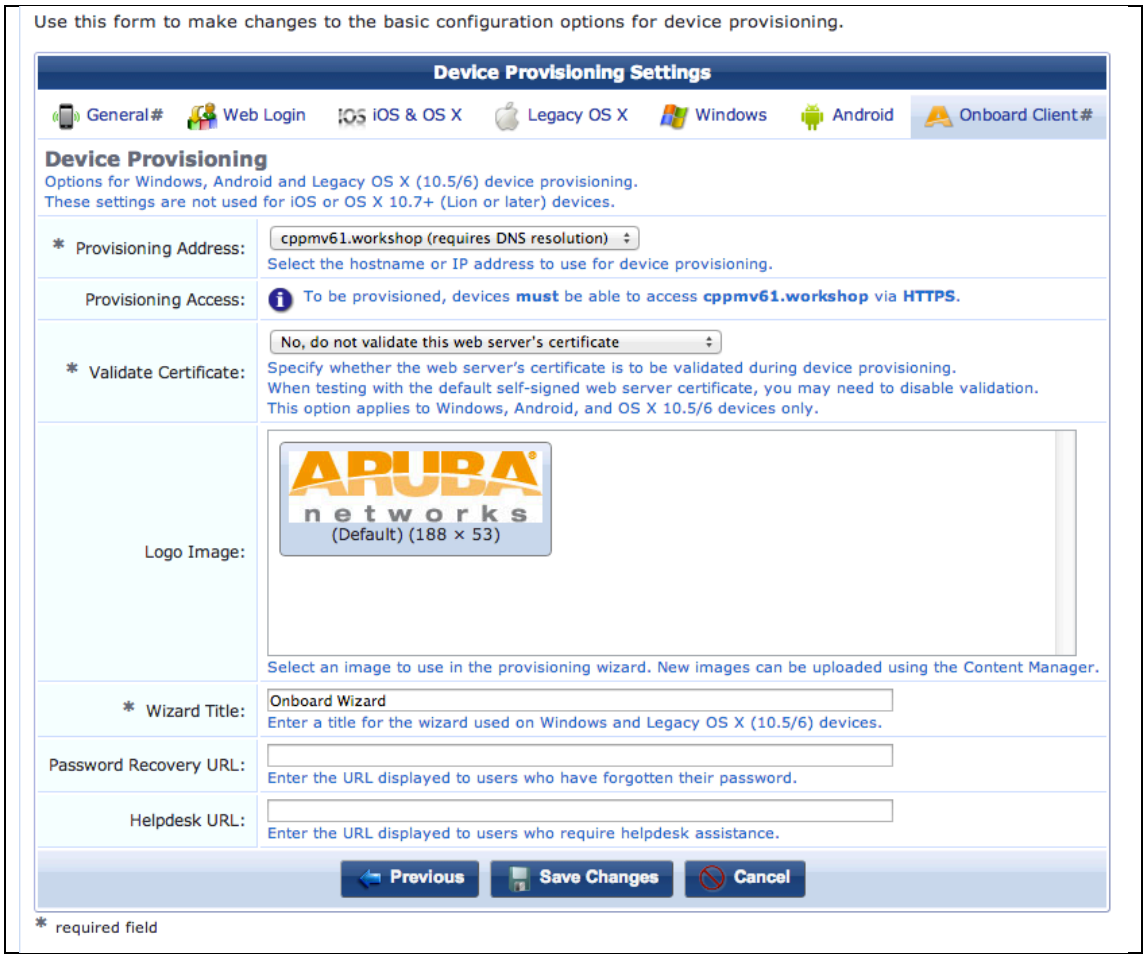
```
{nwa_text id=10895}<p>After you have downloaded and installed the application,
please click <b>Next</b>.</p>{/nwa_text}
{assign var=link_text value=1732|NwaText:'Next'}
```

Insert content item...

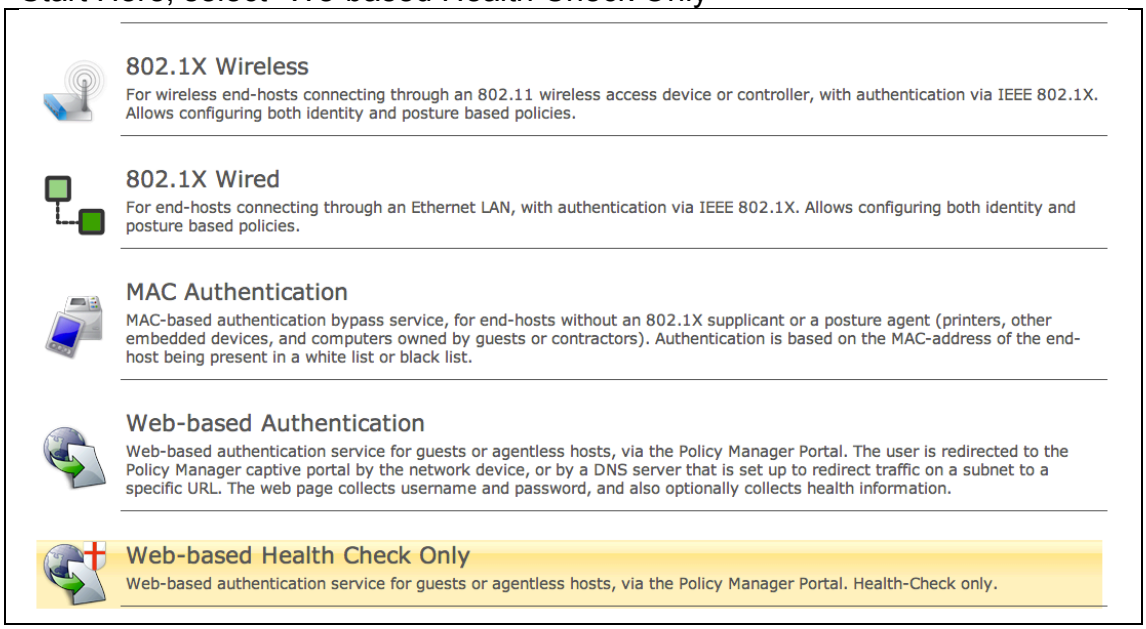
These instructions are shown to the user after they download the application to an Android device.
Enter the HTML code to display. Smarty template functions can be used here.
Leave this field empty to use the default instructions.



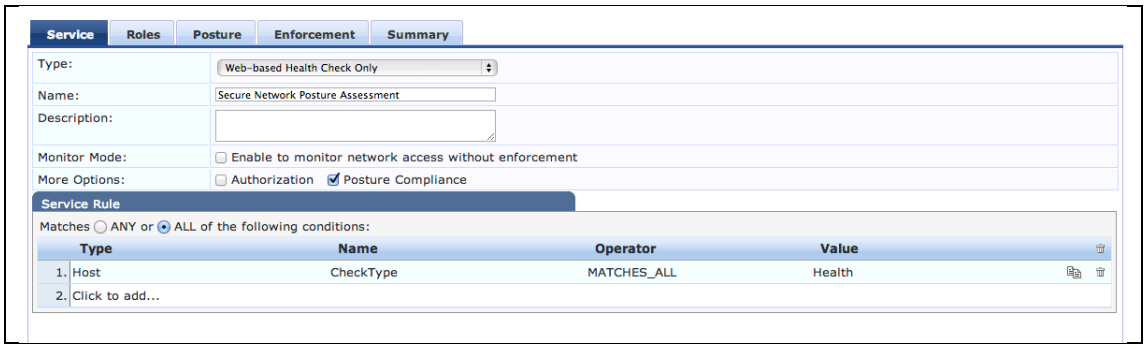
2.3. At Onboard Client# tab, Validate Certificate select “No, do not validate this web server’s certificate” and click “Save Changes” button for save all changes.



3. Create Posture Service, at ClearPass Policy Manager > Configuration > Start Here, select “We-based Health Check Only”

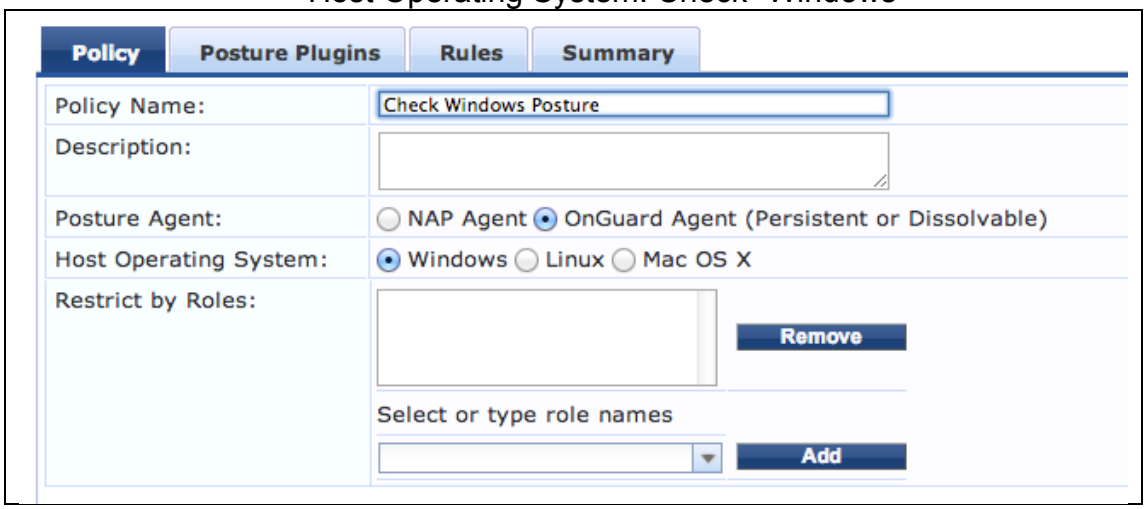


3.1. At new service tab, enter below information:
Name: Secure Network Posture Assessment
More Options: check “Posture Compliance”

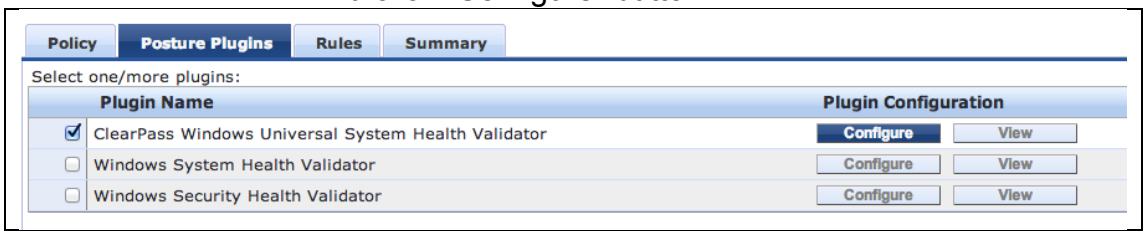


3.2. At Posture tab, enter below information:
Click Add new posture policy, add new Posture Policy for Mac & Windows

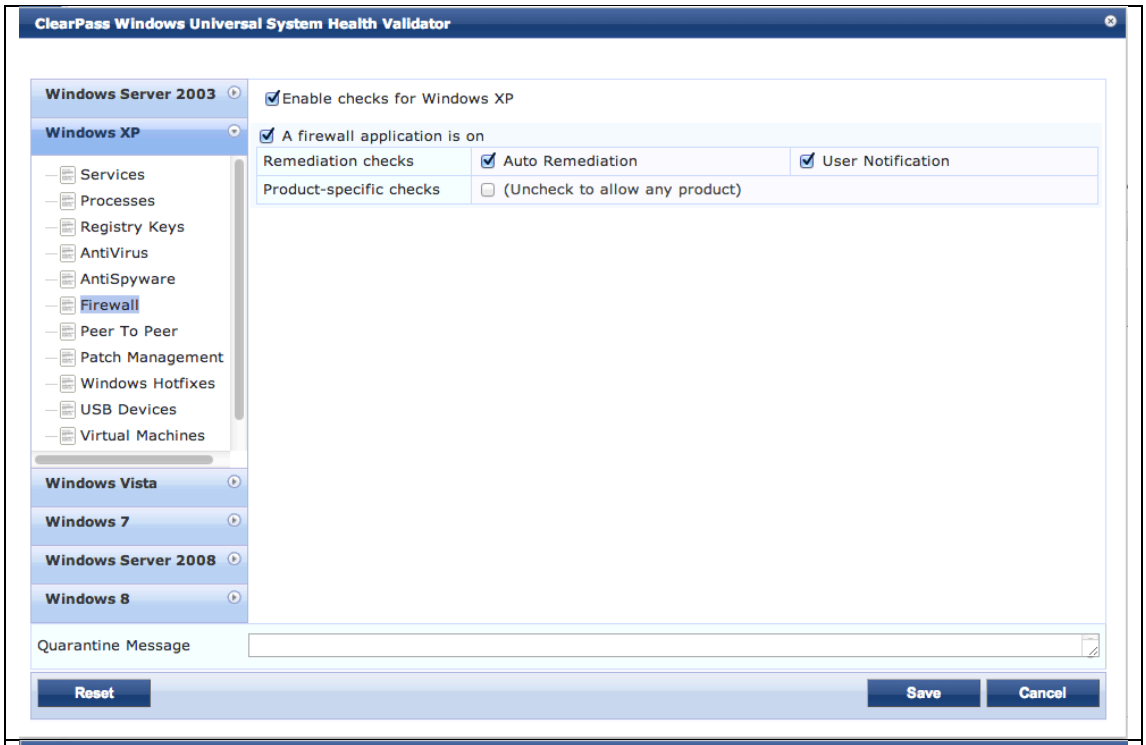
- Windows Policy
  - At Policy Tab:
    - Name: Check Windows Posture
    - Posture Agent: Check “OnGuard Agent”
    - Host Operating System: Check “Windows”

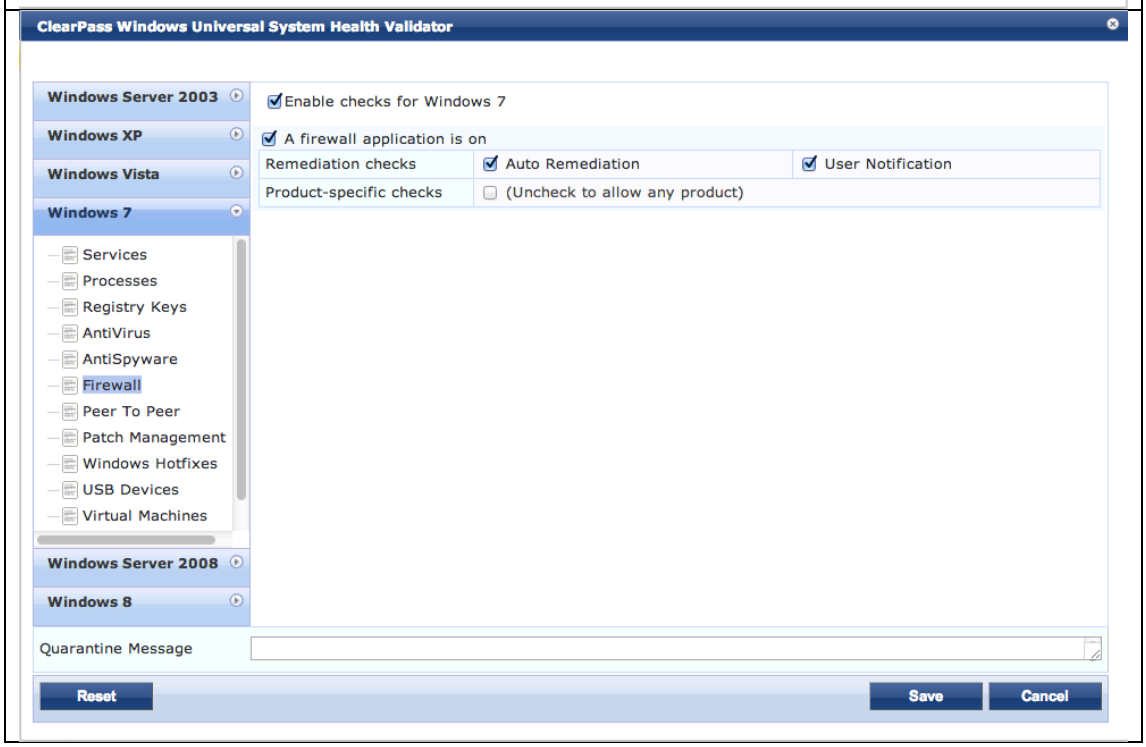


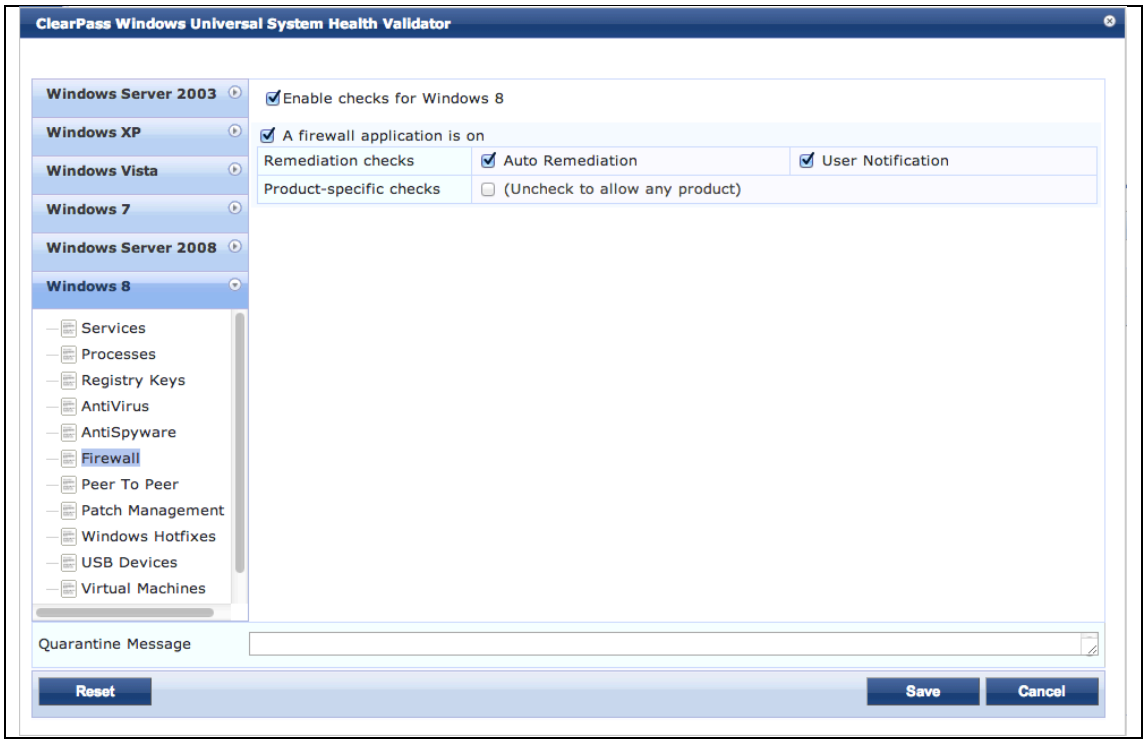
  - At Posture Plugins tab, at plugin table:
    - Check “ClearPass Windows Universal System Health Validator”
    - And click “Configure” button



    - Under Windows XP, Windows 7 & Windows 8 do followings
      - Check “Enable checks for Windows XP”
      - Select “Firewall” under Windows XP list
      - Check “A firewall application is on”
        - Product-specific checks: uncheck “Uncheck to allow any product”

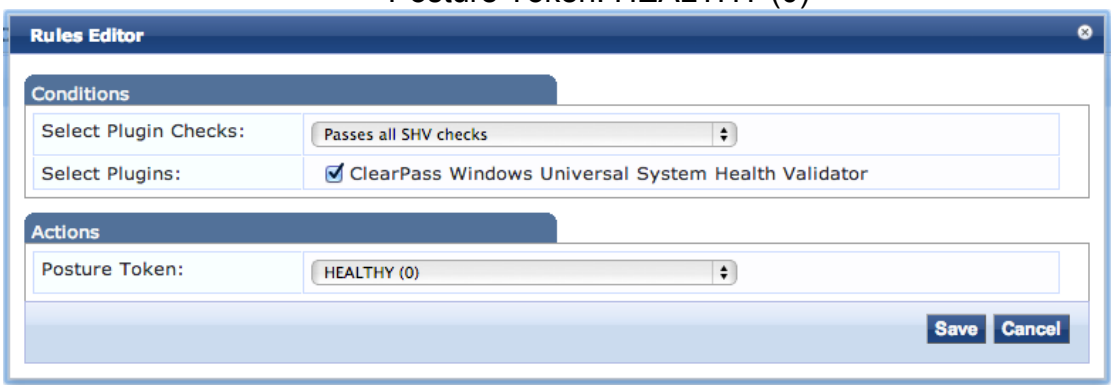

ClearPass Windows Universal System Health Validator
Windows Server 2003
Windows XP
Services
Processes
Registry Keys
AntiVirus
AntiSpyware
Firewall
Peer To Peer
Patch Management
Windows Hotfixes
USB Devices
Virtual Machines
Windows Vista
Windows 7
Windows Server 2008
Windows 8
Enable checks for Windows XP
A firewall application is on
Remediation checks
Auto Remediation
User Notification
Product-specific checks
(Uncheck to allow any product)
Quarantine Message
Reset
Save
Cancel


ClearPass Windows Universal System Health Validator
Windows Server 2003
Windows XP
Windows Vista
Windows 7
Services
Processes
Registry Keys
AntiVirus
AntiSpyware
Firewall
Peer To Peer
Patch Management
Windows Hotfixes
USB Devices
Virtual Machines
Windows Server 2008
Windows 8
Enable checks for Windows 7
A firewall application is on
Remediation checks
Auto Remediation
User Notification
Product-specific checks
(Uncheck to allow any product)
Quarantine Message
Reset
Save
Cancel



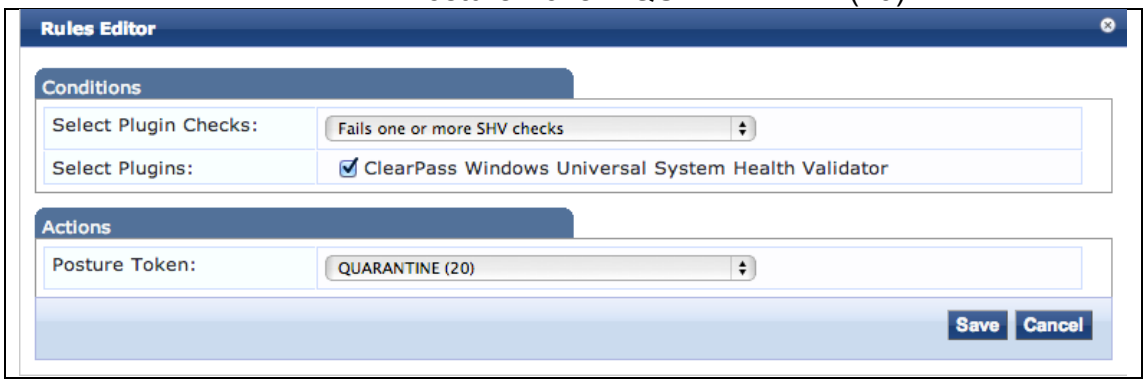
- At Rules tab, Click “Add Rule” button for add two new rules as below:

- Rule 1:
  - Select Plugin Checks: Passes all SHV checks
  - Select Plugins: Check “ClearPass Windows Universal System Health Validator”
  - Posture Token: HEALTHY (0)



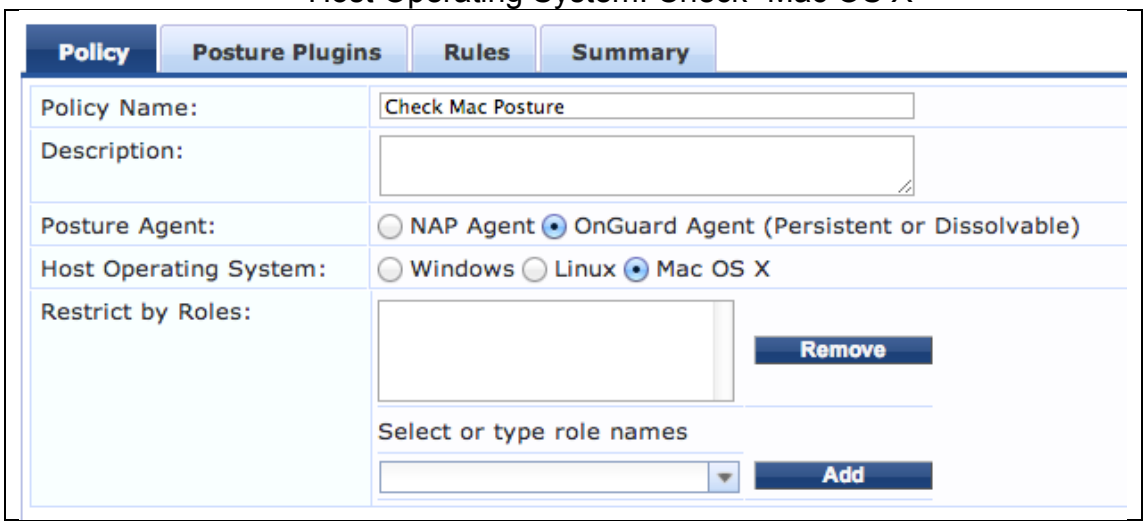
- Rule 2:
  - Select Plugin Checks: Fails one or more SHV

checks
- Select Plugins: Check “ClearPass Windows Universal System Health Validator”
- Posture Token: QUARANTINE (20)

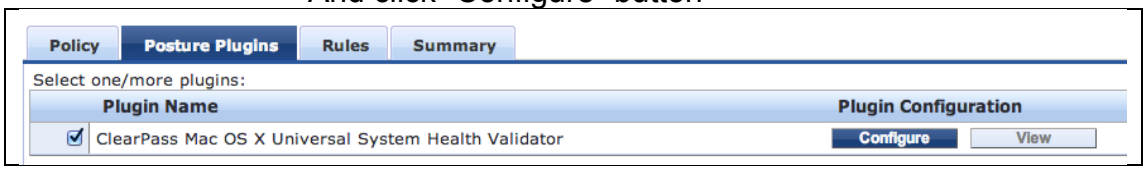


- Click “Save” button for save the policy and go back to “services”

- Mac Policy
  - At Policy Tab:
    - Name: Check Mac Posture
    - Posture Agent: Check “OnGuard Agent”
    - Host Operating System: Check “Mac OS X”

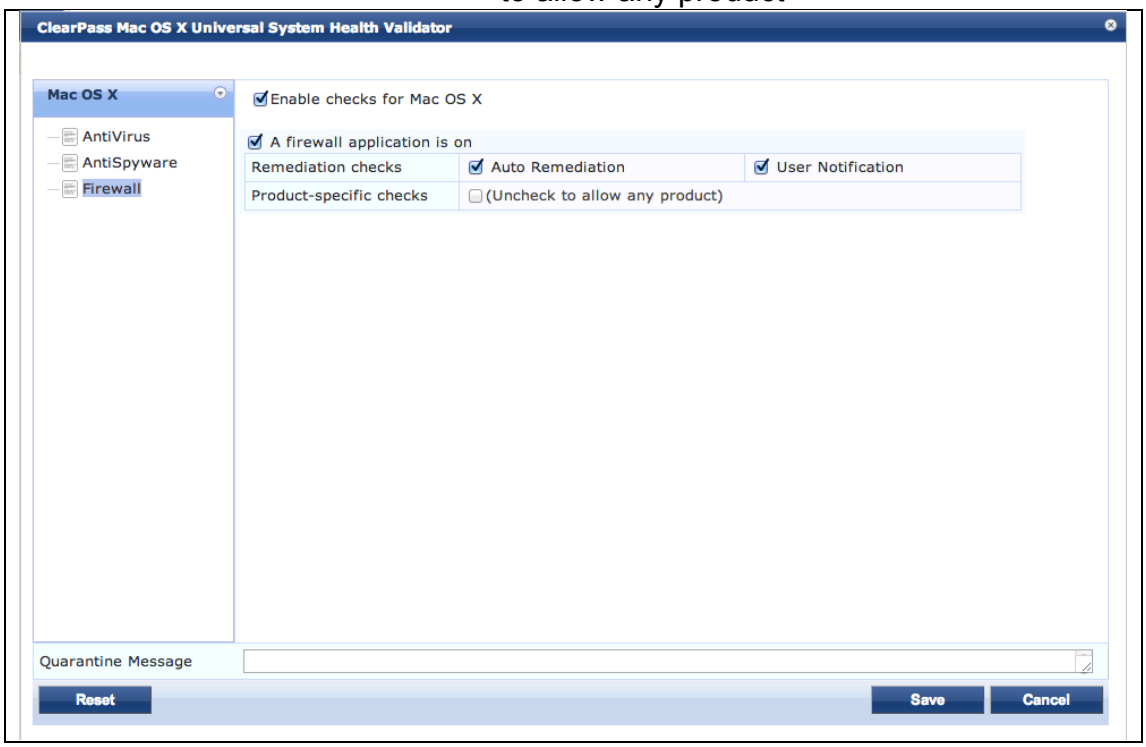


  - At Posture Plugins tab, at plugin table:
    - Check “ClearPass Mac OS X Universal System Health Validator”
    - And click “Configure” button



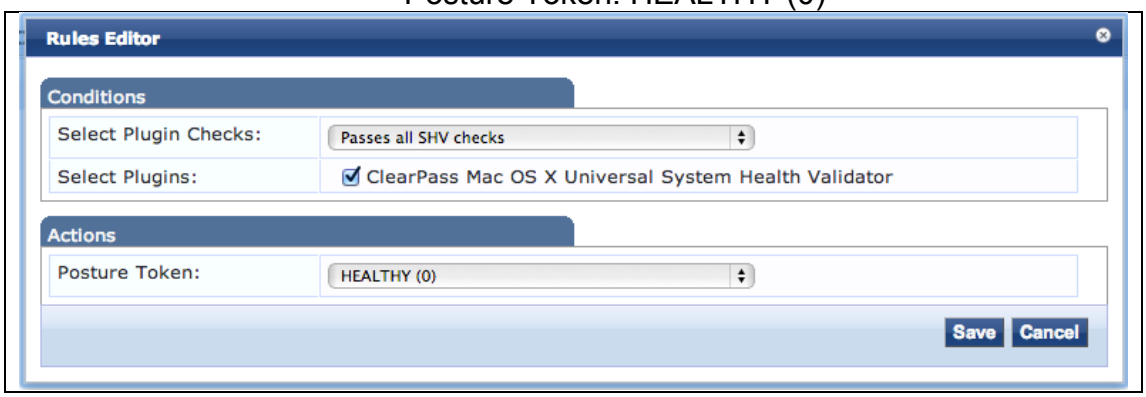
    - Under Mac OS X do followings
      - Check “Enable checks for Mac OS X”
      - Select “Firewall” under Mac OS X list
      - Check “A firewall application is on”

- Product-specific checks: uncheck “Uncheck to allow any product”

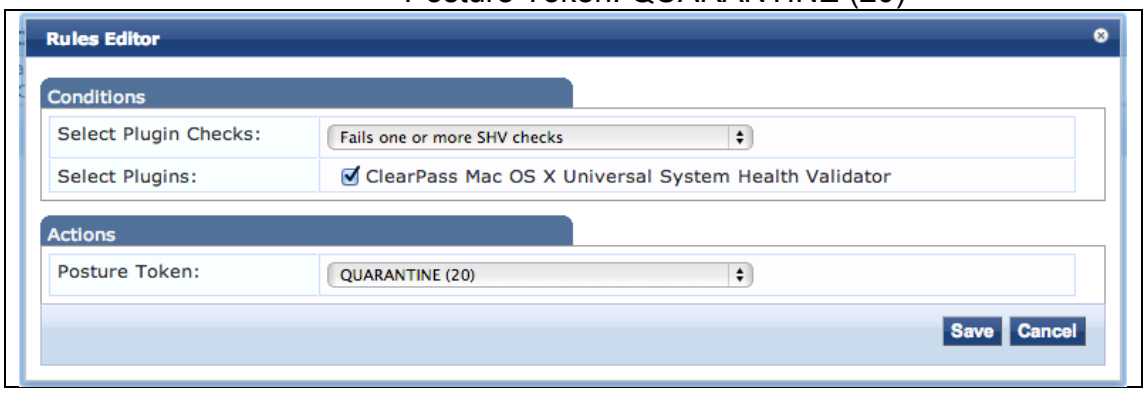


- At Rules tab, Click “Add Rule” button for add two new rules as below:

- Rule 1:
  - Select Plugin Checks: Passes all SHV checks
  - Select Plugins: Check “ClearPass Mac OS X Universal System Health Validator”
  - Posture Token: HEALTHY (0)

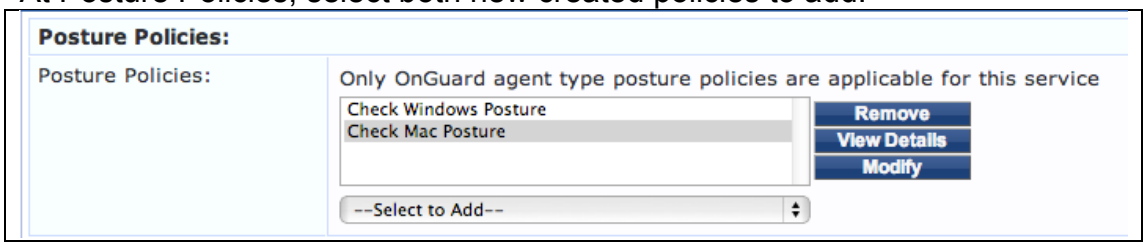


- Rule 2:
  - Select Plugin Checks: Fails one or more SHV checks
  - Select Plugins: Check “ClearPass Mac OS X Universal System Health Validator”
  - Posture Token: QUARANTINE (20)



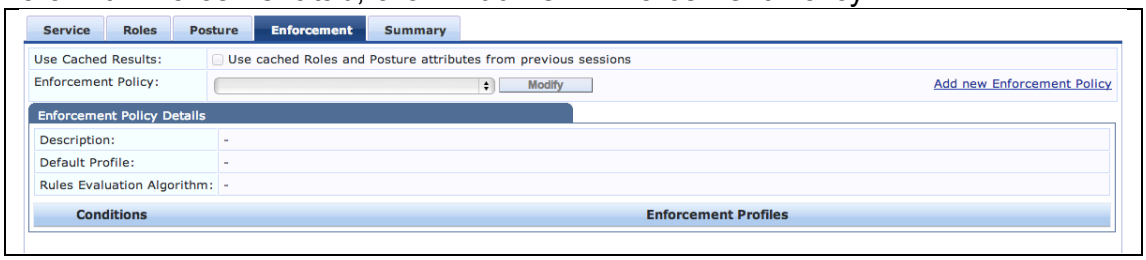
- Click “Save” button for save the policy and go back to “services”

At Posture Policies, select both new created policies to add:



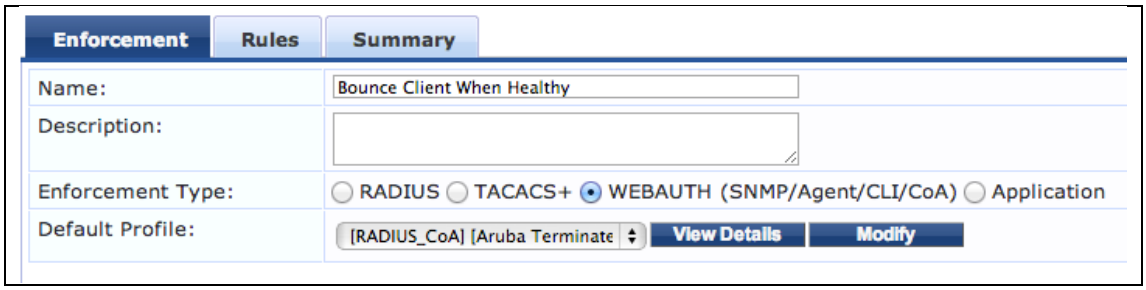
Default Posture Token: UNKNOWN (100) – default value
Remediate End-Hosts: Check “Enable auto-remediation of non-compliant end-hosts”

3.3. At Enforcement tab, click “Add new Enforcement Policy”



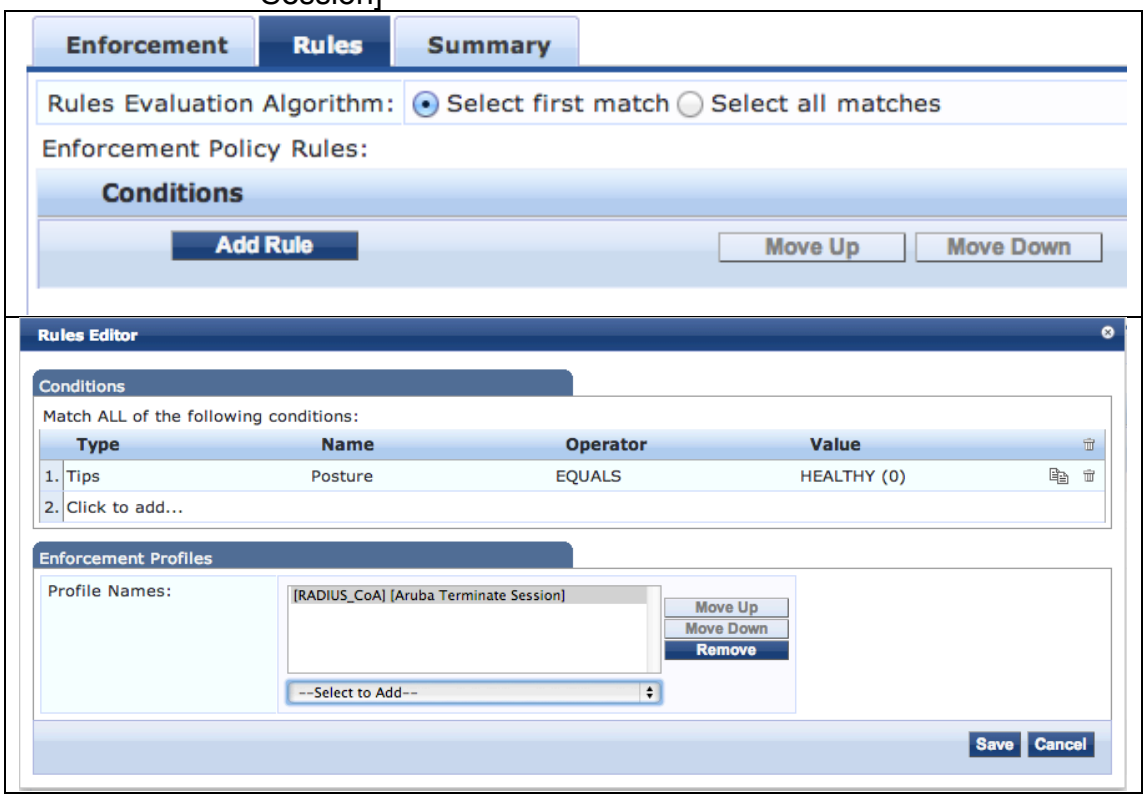
3.3.1. At Enforcement Policies > Enforcement tab, enter below information:

- Name: Bounce Client When Healthy
- Default Profile: [RADIUS_CoA] [Aruba Terminate Session]



3.3.2. At Enforcement Policies > Rules tab, enter below information:

- Rules Evaluation Algorithm: Select first match
- Click “Add Rule” button to add new rule:
  - Type: Tips
  - Name: Posture
  - Operator: EQUALS
  - Value: HEALTHY (0)
  - Enforcement Profile: [RADIUS_CoA] [Aruba Terminate Session]



- Click “Save” button for save the policy and go back to “services”
- At Service click “Next” and “Save” button for save the new created service.

4. Create Roles on Aruba Controller

Controller Configuration:

```
netdestination cppm host 192.168.146.11
```

```
!ip access-list session allow-cppm

user alias cppm svc-https permit

user alias cppm svc-http permit !

aaa authentication captive-portal "OnBoard-Redirect"redirect-pause 1no logout-popup-
windowlogin-page "https://cppm.arubademo.local/guest/device_provisioning.php" no
enable-welcome-page

switchip-in-redirection-url !

aaa authentication captive-portal "OnGuard-Redirect" redirect-pause 1no logout-popup-
windowlogin-page "https://cppm.arubademo.local/agent/portal/" no enable-welcome-page

!user-role onguard-redirect

captive-portal "OnGuard-Redirect" access-list session allow-cppm access-list session
logon-control access-list session captiveportal

!user-role onboard-redirect

captive-portal "OnBoard-Redirect" access-list session allow-cppm access-list session
logon-control access-list session captiveportal

!user-role non-employee-restricted

access-list session allowall !

user-role quarantineaccess-list session logon-control

!user-role exec-byod-restricted

access-list session allowall !

aaa rfc-3576-server "192.168.10.XX" key aruba123

!aaa profile "DemoSecure-aaa_prof"

authentication-dot1x "dot1x_prof-tad05" dot1x-default-role "authenticated" dot1x-
server-group "DemoSecure_srvgrp-hey19" radius-accounting "DemoSecure_srvgrp-hey19"
radius-interim-accounting

rfc-3576-server "192.168.10.XX"
```

5. Copy and Modify existing “APJ Workshop” service:

5.1. Select “copy_APJ Workshop” service, at service tab:

- Enable “Authorization” and “Profiler”

5.2. At Authentication tab:

- Remove EAP-TTLS, EAP-TLS, and EAP-FAST from authentication methods
- Add “[EAP TLS] with OCSP Check” to authentication methods
- Add [Onboard Device Repository] to authentication sources

5.3. At Authorization tab:

- Add [Endpoint Device Repository] to additional authorization sources

5.4. At Roles tab:

- Add a new Role Mapping Policy called “Secure WLAN Roles”
- Add new roles named:
    - Onboarded Device
    - Vendor

    - Executive
    - iOS Device
    - Contractor
    - Computer
    - Unknown
- Set default role to “Unknown”
- Create the following role mapping rules and set as “Evaluate All”:
- Authorization:ad.arubademo.local memberOf CONTAINS Executive OR Authorization:ad.arubademo.local for PEAP OnBoarded Devices CONTAINS Executive SET ROLE Executive
- Authorization:ad.arubademo.local memberOf CONTAINS Contractor OR Authorization:ad.arubademo.local for PEAP OnBoarded Devices CONTAINS Contractor SET ROLE Contractor
- Authorization:ad.arubademo.local memberOf CONTAINS Vendor OR Authorization:ad.arubademo.local for PEAP OnBoarded Devices CONTAINS Vendor SET ROLE Vendor
- Authorization:[Endpoints Repository Category EQUALS Computer SET ROLE Computer
- Authorization:[Endpoints Repository] Category EQUALS SmartDevice AND Authorization:[Endpoints Repository] OS Family EQUALS Apple SET ROLE iOS Device
- Certificate Issuer-CN EQUALS ClearPass Onboard Local Certificate Authority OR Authorization:[Onboard Devices Repository] Owner EXISTS SET Role Onboarded Device

5.5. At Enforcement tab:

- Enable “Use Cached Roles and Posture...”
- Create a new enforcement profile named “Secure WLAN Enforcement”
- Set default enforcement to [Deny Access Profile]
- Create the following new enforcement profiles based on the Aruba Radius Enforcement template:
    - Name = “Redirect to OnBoard - Aruba Controller”, Accept, Aruba-User-Role = onboard-redirect
    - Name = “"Redirect to OnGuard - Aruba Controller", Accept, Aruba-User-Role = onguard-redirect
    - Name = "Non-Employee Restricted", Accept, Aruba-User-Role = non-employee-restricted
    - Name = "Quarantine Role", Accept, Aruba-User-Role = quarantine
    - Name = "executive-byod-restricted", Accept, Aruba-User-Role = exec-byod-restricted
- Create the following enforcement rules set as “first applicable” in this order:
    - Tips Posture NOT_EQUALS Healthy AND Tips Role EQUALS Computer AND Tips Role MATCHES_ANY Contractor | Vendor Set Policy "Redirect to OnGuard - Aruba Controller”
    - Tips Posture NOT_EQUALS Healthy AND Tips Role EQUALS Computer AND Tips Role MATCHES_ALL [User Authenticated]

| [Machine Authenticated] Set Policy "Redirect to OnGuard - Aruba Controller”
    - Tips Posture NOT_EQUALS Healthy AND Tips Role EQUALS Computer AND Tips Role EQUALS [Machine Authenticated] Set Policy "Redirect to OnGuard - Aruba Controller”
    - Tips Role EQUALS Computer AND Tips Role MATCHES_ANY Contractor | Vendor AND Tips Posture EQUALS Healthy AND Tips Role EQUALS Onboarded Device Set Policy “Non-Employee Restricted”
    - Tips Role MATCHES_ALL [User Authenticated] | [Machine Authenticated] AND Tips Posture EQUALS Healthy Set Policy [Allow Access Profile]
    - Tips Role EQUALS [Machine Authenticated] AND Tips Posture EQUALS Healthy Set Policy [Allow Access Profile]
    - Tips Role EQUALS Executive AND Tips Role EQUALS iOS Device AND Tips Role EQUALS Onboarded Device Set Policy “executive-byod-restricted”
    - Tips Role EQUALS Computer AND Tips Role MATCHES_ANY Contractor | Vendor AND Tips Posture EQUALS Healthy Set Policy “Redirect to OnBoard – Aruba Controller”
    - Tips Role EQUALS Executive AND Tips Role EQUALS iOS Device Set Policy “Redirect to OnBoard – Aruba Controller”
    - Tips Role EQUALS [User Authenticated] and Authorizations:[Endpoints Repository] Category EXISTS Set Policy [Deny Access Profile] Tips Role [User Authenticated] Set Policy “Quarantine Role”
- At Profile tab:
    - Select “Any Category/ OS Family / Name” under Endpoint Classification
    - Select [Aruba Terminate Session] as the Radius CoA Action

5.6. Save Service.

6. Testing:

6.1. Connect a client with a iOS Device (or any device other than computer) to DemoSecure that DOES NOT exist in the endpoint database with sales1 credentials

- Client should connect, get placed in “quarantine” role initially, then a CoA should take place, and client will reauth and fail authentication as this client is not allowed to use a SmartDevice on the network.
- Show in Access Tracker

6.2. Connect a client with a iOS Device to DemoSecure with the executive1 credentials

- Client should connect and get placed into the Redirect to OnBoard role.
- Open browser and walk through Onboarding of the client
- Client should automatically reconnect with new credentials and get placed in the exec-byod-restricted role
- Show in Access Tracker

6.3. Connect a client with a non-domain Computer to DemoSecure with the

executive1 credentials

- Client should get rejected
- Show in Access Tracker

6.4. Connect a client with a domain Computer and persistent agent installed and running to DemoSecure with the executive1 credentials

- With client logged off of computer, client should be in the authenticated role Maybe in the Redirect to OnGuard role temporarily until OnGuard runs
- Log onto Windows with executive1 credentials, client should remain in the authenticated role
- Show in Access Tracker

6.5. Connect a client on a non-domain Computer without persistent agent installed to DemoSecure with contractor1 credentials

- Client should get placed in the Redirect to OnGuard Role
- Open browser and allow OnGuard to run
- Client should reauth and get placed in Redirect to OnBoard role
- Open browser and go through OnBoard process
    - If windows, client should automatically reconnect
    - If Mac, may need to manually disconnect and reconnect
- Client should be in the non-employee-restricted role
- Show in Access Tracker

< --- End of Workshop --- >