

APJ Workshop Lab Exercises – 2013Q4

by Aruba Networks

Table of Content

0. Initial Setup	2
Controller + AP	2
ClearPass	2
0.1. Install CPPM Patch - CLI	4
0.2. Add External Syslog Server.....	6
0.3. Join AD Domain.....	9
0.4. Add Authentication Sources.....	11
0.5. Create Self-Signed Certificate for unit credentials	14
0.6. Add Network Access Device	15
1.0. Basic ClearPass Configuration Workshop.....	16
1.1. Create CPPM ClearPass Admin Services using Service Templates.....	16
1.2. Create CPPM dot1X Services using Service Templates.....	18
1.3. Aruba Controller.....	24
2.0. Advance ClearPass Configuration Workshop.....	27
2.1. ClearPass – Guest -- Setup basic Guest WLAN Service to Aruba Controller	27
2.2. ClearPass – Onboard.....	43

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 want 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

The screenshot shows the 'Add License' page in the ClearPass Policy Manager web interface. At the top, a red banner reads: 'No license configured for the Policy Manager. Please add a license now.' Below this, the 'Select Application' dropdown is set to 'Policy Manager'. The 'Enter license key' field contains the evaluation license key: 'O6TK-Z7FFPL-VX5Y-3JZQUF-62ZYIH-RCNM-ZXEXPL-AVTDF4-MMSH-7TCMEQ'. Under the 'Terms and Conditions' section, the 'Aruba Networks, Inc. End-User Software License Agreement ("Agreement")' is displayed. It includes an 'IMPORTANT' notice and a checkbox labeled 'I agree to the above terms and conditions.', which is checked. An 'Add License' button is located at the bottom right of the form.

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 Manager > 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:

ClearPass 6.1 2013Q4 Partner Training Workshop Lab Exercises

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"

Edit Syslog Target

Host Address: 192.168.10.29

Description: External Syslog Server

Server Port: 514

Save Cancel

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

ClearPass 6.1 2013Q4 Partner Training Workshop Lab Exercises

Administration » External Servers » Syslog Export Filters » Add

Syslog Export Filters

General | Filter and Columns | Summary

Name:

Description:

Export Template:

Syslog Server: [Modify](#) [Add new Syslog target](#)

[Back to Syslog Filters](#) [Next >](#) [Save](#) [Cancel](#)

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

Administration » External Servers » Syslog Export Filters » Add

Syslog Export Filters

General | **Filter and Columns** | Summary

Syslog filter has not been saved

Option 1: For common use-cases, select Data Filter and Columns for export:

Data Filter: [Modify](#) [Add new Data filter](#)

Columns Selection:

Predefined Field Groups -

- Logged in users
- Failed Authentications
- RADIUS Accounting
- TACACS+ Administration

Available Columns -

Type:

[Common Alerts](#)
[Common Alerts - Present](#)
[Common Audit - Posture - Token](#)
[Common Auth - Type](#)
[Common Connection - Status](#)
[Common Enforcement - Profiles](#)
[Common Error - Code](#)

[Selected Columns -](#)

- 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:

As an example, click [here](#) to copy a sample SQL

[Back to Syslog Filters](#) [Next >](#) [Save](#) [Cancel](#)

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

ClearPass 6.1 2013Q4 Partner Training Workshop Lab Exercises

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:	<div>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</div>

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

The screenshot shows the ClearPass Policy Manager web interface. The left sidebar has a tree view with 'Administration' expanded, showing 'Server Manager' and 'Server Configuration'. The main content area is titled 'Server Configuration - pub.cppmv61 (192.168.10.201)'. It has tabs for 'System', 'Services Control', 'Service Parameters', 'System Monitoring', and 'Network'. The 'System' tab is active, showing fields for 'Hostname' (pub.cppmv61), 'Policy Manager Zone' (default), 'Enable Profile' (checked), and 'Enable Insight' (unchecked). Below these are 'Management Port' and 'Data/External Port' sections with IP Address, Subnet Mask, and Default Gateway fields. The 'DNS Settings' section has 'Primary' and 'Secondary' IP Address fields. The 'AD Domains' section shows a message 'Policy Manager is not part of any domain. Join to domain here.' and a 'Join AD Domain' button. At the bottom, there is a 'Back to Server Configuration' link and 'Save' and 'Cancel' buttons.

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

The screenshot shows the 'Join AD Domain' dialog box. It has a title bar with a close button. The main content area has a text prompt: 'Enter the FQDN of the controller and the short (NETBIOS) name for the domain:'. Below this are two input fields: 'Domain Controller' and 'NetBIOS Name'. There is a section titled 'In case of a controller name conflict' with three radio button options: 'Use specified Domain Controller' (selected), 'Use Domain Controller returned by DNS query', and 'Fail on conflict'. Below this is a checkbox labeled 'Use default domain admin user [Administrator]' which is checked. At the bottom, there are two input fields: 'Username' and 'Password'. At the very bottom right are 'Save' and 'Cancel' buttons.

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

ClearPass Policy Manager

Support | Help | Logout
admin (Super Administrator)

Configuration » Authentication » Sources

Authentication Sources

Filter: Name contains [] Go Clear Filter Show 100 records

#	Name	Type	Description
1.	[Admin User Repository]	Local SQL DB	Authenticate users against Policy Manager admin user database
2.	[Blacklist User Repository]	Local SQL DB	Blacklist database with users who have exceeded bandwidth or session related limits
3.	[Endpoints Repository]	Local SQL DB	Authenticate endpoints against Policy Manager local database
4.	[Guest Device Repository]	Local SQL DB	Authenticate guest devices against Policy Manager local database
5.	[Guest User Repository]	Local SQL DB	Authenticate guest users against Policy Manager local database
6.	[Insight Repository]	Local SQL DB	Insight database with session information for users and devices
7.	[Local User Repository]	Local SQL DB	Authenticate users against Policy Manager local user database
8.	[Onboard Devices Repository]	Local SQL DB	Authenticate Onboard devices against Policy Manager local database

Showing 1-8 of 8

Copy Export Delete

© Copyright 2013 Aruba Networks. All rights reserved. May 13, 2013 16:05:40 HKT ClearPass Policy Manager 6.1.0.50820 on CP-VA-500 platform

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

Configuration » Authentication » Sources » Add

Authentication Sources

General Primary Attributes Summary

Name: ad.arubademo.local

Description: APJ Workshop Active Directory

Type: Active Directory

Use for Authorization: ☒ Enable to use this authentication source to also fetch role mapping attributes

Authorization Sources:

Server Timeout: 300 seconds

Cache Timeout: 36000 seconds

Backup Servers Priority:

Remove View Details

Move Up Move Down

Add Backup Remove

Back to Authentication Sources

Next > Save Cancel

3. At Primary tab, enter as below:

ClearPass 6.1 2013Q4 Partner Training Workshop Lab Exercises

Configuration » Authentication » Sources » Add

Authentication Sources

General Primary Attributes Summary

Connection Details

Hostname:	192.168.10.30
Connection Security:	None
Port:	389 (For secure connection, use 636)
Verify Server Certificate:	<input checked="" type="checkbox"/> Enable to verify Server Certificate for secure connection
Bind DN:	adjoin@arubademo.local (e.g. administrator@example.com OR cn=administrator,cn=users,dc=example,dc=com)
Bind Password:	*****
NetBIOS Domain Name:	ARUBADEMO
Base DN:	dc=arubademo,dc=local Search Base Dn
Search Scope:	SubTree Search
LDAP Referrals:	<input type="checkbox"/> Follow referrals
Bind User:	<input checked="" type="checkbox"/> Allow bind using user password
User Certificate :	userCertificate

[Back to Authentication Sources](#) [Next >](#) [Save](#) [Cancel](#)

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")

LDAP Browser

Base DN: dc=arubademo,dc=local

- dc=arubademo,dc=local
 - CN=Builtin
 - CN=Computers
 - OU=Domain Controllers
 - CN=ForeignSecurityPrincipals
 - CN=Infrastructure
 - CN=LostAndFound
 - CN=Managed Service Accounts
 - CN=NTDS Quotas
 - CN=Program Data
 - CN=System
 - CN=Users

[Save](#) [Close](#)

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











ClearPass 6.1 2013Q4 Partner Training Workshop Lab Exercises

Configuration » Authentication » Sources » Add

Authentication Sources

General Primary **Attributes** Summary

Specify filter queries used to fetch authentication and authorization attributes

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	 

[Add More Filters](#)

[Back to Authentication Sources](#) [Next >](#) [Save](#) [Cancel](#)

0.5. Create Self-Signed Certificate for unit credentials

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

Home » Onboard » Certificate Management

Certificate Management

Upload a certificate signing request
 Generate a new certificate signing request
 Upload a code-signing certificate
 Upload a profile-signing certificate
 Upload a trusted certificate

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 list view to manage certificates.

Quick Help
 Columns

Certificate Authority:

Certificate Type:

Filter:

Common Name	Certificate Authority	Serial Number	Type	Valid From	Valid To	Device Type
ClearPass Onboard Local Certificate Authority	Local Certificate Authority	1	ca	2013-04-23 15:29:17+00	2023-04-24 15:59:17+00	None
ClearPass Onboard Local Certificate Authority (Signing)	Local Certificate Authority	2	ca	2013-04-23 15:29:17+00	2023-04-24 15:59:17+00	None

Refresh 1 Showing 1 - 2 of 2 10 rows per page

Back to Onboard

Back to main

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

Administration » Certificates » Server Certificate

Server Certificate

Create Self-Signed Certificate
 Create Certificate Signing Request
 Import Server Certificate
 Export Server Certificate

Select Server:

Server Certificate:	
Subject:	O=PolicyManager, CN=cppmv61.workshop
Issued by:	O=PolicyManager, CN=cppmv61.workshop
Issue Date:	May 14, 2013 11:07:04 HKT
Expiry Date:	May 14, 2014 11:07:04 HKT
Validity Status:	Valid

0.6. Add Network Access Device

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

Configuration » Network » Devices

Network Devices

[Add Device](#)
[Import Devices](#)
[Export Devices](#)

Filter: [Name] contains [] [Go](#) [Clear Filter](#) Show 10 records

#	Name	IP or Subnet Address	Description
1.	dl-office-lab	192.168.10.254	

Showing 1-1 of 1

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

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

Edit Device Details

[Device](#)
[SNMP Read Settings](#)
[SNMP Write Settings](#)
[CLI Settings](#)

Name: dl-office-lab
 IP or Subnet Address: 192.168.10.254 (e.g., 192.168.1.10 or 192.168.1.1/24)
 Description:
 RADIUS Shared Secret: Verify:
 TACACS+ Shared Secret: Verify:
 Vendor Name: Aruba
 Enable RADIUS CoA: ☒ RADIUS CoA Port: 3799

Attributes

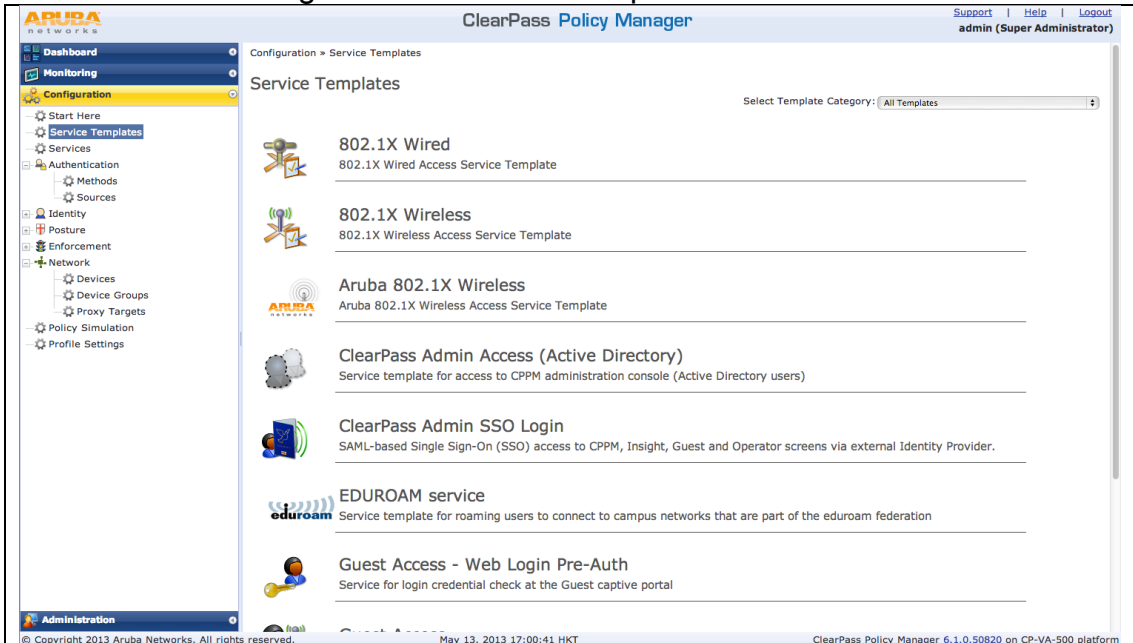
Attribute	Value
1. Click to add...	

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

1.0. Basic ClearPass Configuration 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

ClearPass 6.1 2013Q4 Partner Training Workshop Lab Exercises

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:

Authentication

Select AD*:

AD Name*:

Description:

Server*:

Identity*: (e.g., administrator@example.com OR cn=administrator,cn=users,dc=example,dc=com)

NETBIOS*:

Base DN*: (e.g., CN=Users,DC=example,DC=example,DC=com)

Password*:

Port*: (For secure connection, use port 636)

Role Mapping

Name*: Description:

Attribute Name*: Super Admin Condition*: (e.g., Enter AD group name for super admin users)

Attribute Name*: Read Only Admin Condition*: (e.g., Enter AD group name for read only users)

Attribute Name*: Help Desk Condition*: (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:

Strip Username Rules:

Roles:

Role Mapping Policy:

Enforcement:

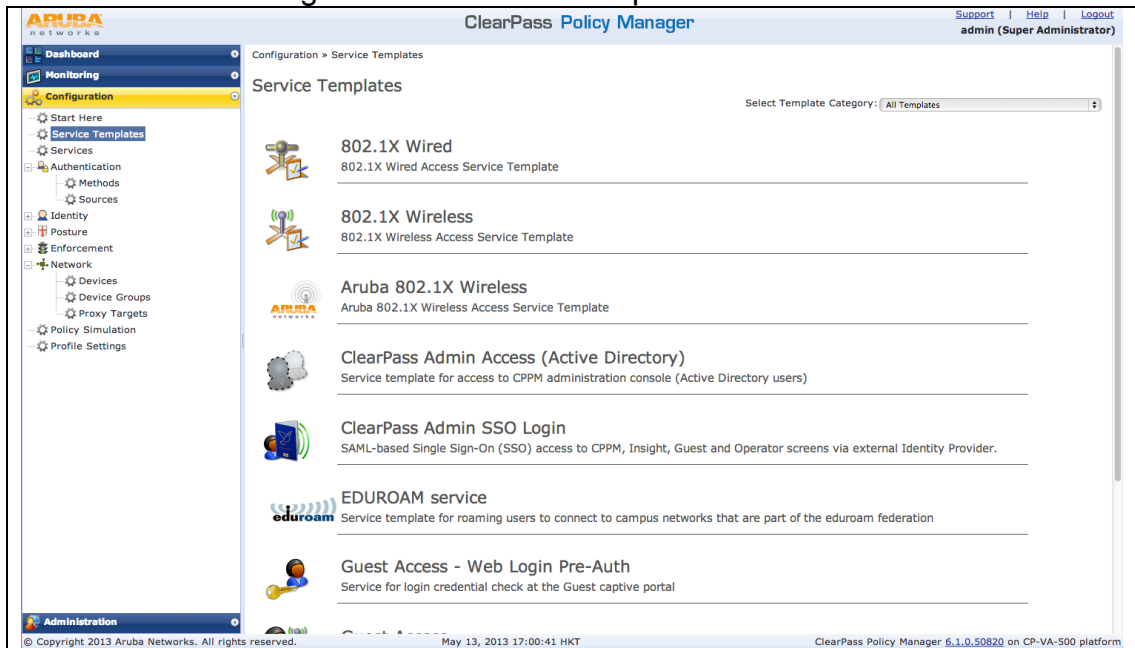
Use Cached Results:

Enforcement 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

ClearPass 6.1 2013Q4 Partner Training Workshop Lab Exercises

Service Templates - Aruba 802.1X Wireless

For wireless end-hosts connecting through an Aruba 802.11 wireless access device or controller, with authentication via IEEE 802.1X (Service rules customized for Aruba WLAN Mobility Controllers). This template configures an AD Authentication Source; joins this node to the AD Domain; creates Enforcement Policy for AD based attributes; and creates an Aruba Network Access Device.

Name Prefix:

Authentication

Select AD*:

AD Name*:

Description:

Server*:

Identity*: (e.g., administrator@example.com OR cn=administrator,cn=users,dc=example,dc=com)

NETBIOS*:

Base DN*: (e.g., CN=Users,DC=example,DC=example,DC=com)

Password*:

Port*: (For secure connection, use port 636)

Enforcement Details

Attribute Name	Attribute Value	Aruba Role
memberOf <input type="text" value="↓"/>	<input type="text" value="Student"/>	<input type="text" value="Student"/>
memberOf <input type="text" value="↓"/>	<input type="text" value="Employee"/>	<input type="text" value="Employee"/>
memberOf <input type="text" value="↓"/>	<input type="text" value="Executives"/>	<input type="text" value="Executives"/>
Default Role*	<input type="text" value="[Drop Access Profile]"/>	

Wireless Network Settings

Select wireless controller:

Wireless Controller Name:

Controller IP Address:

Vendor Name:

RADIUS Shared Secret:

Enable RADIUS CoA: ☒

RADIUS CoA Port:

4. Click "Add Service"

5. Corresponding Enforcement profiles will be generate:

5.	<input type="checkbox"/>	APJ Workshop Aruba 802.1X Wireless Default Profile	RADIUS
6.	<input type="checkbox"/>	APJ Workshop Aruba 802.1X Wireless Profile1	RADIUS
7.	<input type="checkbox"/>	APJ Workshop Aruba 802.1X Wireless Profile2	RADIUS
8.	<input type="checkbox"/>	APJ Workshop Aruba 802.1X Wireless Profile3	RADIUS

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

ClearPass 6.1 2013Q4 Partner Training Workshop Lab Exercises

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 employee
 - Staff_BYOD - for staff member BYOD
 - Student - for student
 - Student_BYOD - for student BYOD

Edit Role

Name:

Description:

Save Cancel

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

ClearPass 6.1 2013Q4 Partner Training Workshop Lab Exercises

Configuration » Identity » Role Mappings

Role Mappings

[Add Role Mapping](#)
[Import Role Mappings](#)
[Export Role Mappings](#)

Filter: Name contains [] Go Clear Filter Show 10 records

#	Name	Description	Default Role
1.	[Guest Roles]	The roles used by Guest.	[Employee]
2.	netadmin	Network Admin	[Other]

Showing 1-2 of 2

Copy Export Delete

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

Configuration » Identity » Role Mappings » Add

Role Mappings

Policy Mapping Rules Summary

Policy Name: APJ-WS-role-mapping

Description: APJ Workshop Role Map

Default Role: [Guest] View Details Modify Add new Role

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

Configuration » Identity » Role Mappings » Add

Role Mappings

Role mapping policy has not been saved

Policy Mapping Rules Summary

Rules Evaluation Algorithm: ☒ Select first match ☐ Select all matches

Role Mapping Rules:

Conditions	Role Name
1. (Authorization:ad.arubademo:Onboard Groups CONTAINS Student)	Student_BYOD
2. (Authorization:ad.arubademo:Onboard Groups CONTAINS Staff)	Staff_BYOD
3. (Authorization:ad.arubademo:Onboard Groups CONTAINS Executives)	Executives_BYOD
4. (Authorization:ad.arubademo:Groups CONTAINS Student)	Student
5. (Authorization:ad.arubademo:Groups CONTAINS Executives)	Executives
6. (Authorization:ad.arubademo:Groups CONTAINS Staff)	Staff
7. (Authorization:ad.arubademo:UserDN EXISTS)	Employee

Add Rule Move Up Move Down Edit Rule Remove Rule

Configuration » Identity » Role Mappings » Add

Role Mappings

Role mapping policy has not been saved

Policy Mapping Rules Summary

Policy:

Policy Name: APJ-WS-role-mapping

Description: APJ Workshop Role Map

Default Role: [Guest]

Mapping Rules:

Rules Evaluation Algorithm: First applicable

Conditions	Role Name
1. (Authorization:ad.arubademo:Onboard Groups CONTAINS Student)	Student_BYOD
2. (Authorization:ad.arubademo:Onboard Groups CONTAINS Staff)	Staff_BYOD
3. (Authorization:ad.arubademo:Onboard Groups CONTAINS Executives)	Executives_BYOD
4. (Authorization:ad.arubademo:Groups CONTAINS Student)	Student
5. (Authorization:ad.arubademo:Groups CONTAINS Executives)	Executives
6. (Authorization:ad.arubademo:Groups CONTAINS Staff)	Staff
7. (Authorization:ad.arubademo:UserDN EXISTS)	Employee

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

ClearPass 6.1 2013Q4 Partner Training Workshop Lab Exercises

Configuration » Services » Edit - APJ Workshop Aruba 802.1X Wireless

Services - APJ Workshop Aruba 802.1X Wireless

Summary	Service	Authentication	Authorization	Roles	Enforcement
Service:					
Name:	APJ Workshop Aruba 802.1X Wireless				
Description:	Aruba 802.1X Wireless Access Service				
Type:	Aruba 802.1X Wireless				
Status:	Enabled				
Monitor Mode:	Disabled				
More Options:	Authorization				
Service Rule					
Match ALL of the following conditions:					
Type	Name	Operator	Value		
1. Radius:IETF	NAS-Port-Type	EQUALS	Wireless-802.11 (19)		
2. Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Framed-User (2), Authenticate-Only (8)		
3. Radius:Aruba	Aruba-Essid-Name	EXISTS			
Authentication:					
Authentication Methods:	1. [EAP PEAP Without Fast Reconnect] 2. [EAP TLS] 3. [EAP TTLS] 4. [EAP FAST]				
Authentication Sources:	1. ad.arubademo 2. [Onboard Devices Repository] 3. [Local User Repository]				
Strip Username Rules:	-				
Authorization:					
Authorization Details:	1. ad.arubademo 2. [Onboard Devices Repository]				
Roles:					
Role Mapping Policy:	-				
Enforcement:					

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

Configuration » Services » Edit - APJ Workshop Aruba 802.1X Wireless

Services - APJ Workshop Aruba 802.1X Wireless

Summary	Service	Authentication	Authorization	Roles	Enforcement
Role Mapping Policy: APJ-WS-role-mapping Modify Add new Role Mapping Policy					
Role Mapping Policy Details					
Description:	APJ Workshop Role Map				
Default Role:	[Guest]				
Rules Evaluation Algorithm:	first-applicable				
Conditions	Role				
1. (Authorization:ad.arubademo:Onboard Groups CONTAINS Student)	Student_BYOD				
2. (Authorization:ad.arubademo:Onboard Groups CONTAINS Staff)	Staff_BYOD				
3. (Authorization:ad.arubademo:Onboard Groups CONTAINS Executives)	Executives_BYOD				
4. (Authorization:ad.arubademo:Groups CONTAINS Student)	Student				
5. (Authorization:ad.arubademo:Groups CONTAINS Executives)	Executives				
6. (Authorization:ad.arubademo:Groups CONTAINS Staff)	Staff				
7. (Authorization:ad.arubademo:UserDN EXISTS)	Employee				

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

Configuration » Services » Edit - APJ Workshop Aruba 802.1X Wireless

Services - APJ Workshop Aruba 802.1X Wireless

Summary	Service	Authentication	Authorization	Roles	Enforcement
Use Cached Results: <input type="checkbox"/> Use cached Roles and Posture attributes from previous sessions					
Enforcement Policy: APJ Workshop Aruba 802.1X Wireless Enforcement Modify Add new Enforcement Policy					
Enforcement Policy Details					
Description:					
Default Profile:	APJ Workshop Aruba 802.1X Wireless Default Profile				
Rules Evaluation Algorithm:	first-applicable				
Conditions	Enforcement Profiles				
1. (Authorization:ad.arubademo:memberOf CONTAINS Student)	APJ Workshop Aruba 802.1X Wireless Profile1				
2. (Authorization:ad.arubademo:memberOf CONTAINS Employee)	APJ Workshop Aruba 802.1X Wireless Profile2				
3. (Authorization:ad.arubademo:memberOf CONTAINS Executives)	APJ Workshop Aruba 802.1X Wireless Profile3				

14. Add Enforcement Profiles,

Enforcement Profile	Type	Name	Value
---------------------	------	------	-------

ClearPass 6.1 2013Q4 Partner Training Workshop Lab Exercises

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]"

Configuration » Enforcement » Policies » Edit - APJ Workshop Aruba 802.1X Wireless Enforcement Policy

Enforcement Policies - APJ Workshop Aruba 802.1X Wireless Enforcement Policy

Summary **Enforcement** **Rules**

Name: APJ Workshop Aruba 802.1X Wireless Enforcement Policy

Description:

Enforcement Type: RADIUS

Default Profile: [Drop Access Profile] [View Details](#) [Modify](#) [Add new Enforcement Profile](#)

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

Configuration » Enforcement » Policies » Edit - APJ Workshop Aruba 802.1X Wireless Enforcement Policy

Enforcement Policies - APJ Workshop Aruba 802.1X Wireless Enforcement Policy

Summary **Enforcement** **Rules**

Rules Evaluation Algorithm: ☒ Select first match ☐ Select all matches

Enforcement Policy Rules:

Conditions	Actions
1. (Tips:Role EQUALS Student_BYOD)	AP1_WS-BYOD Access Student
2. (Tips:Role EQUALS Staff_BYOD)	AP1_WS-BYOD Access Staff
3. (Tips:Role EQUALS Executives_BYOD)	AP1_WS-BYOD Access Exec
4. (Tips:Role EQUALS Staff) AND (Authentication:OuterMethod EQUALS EAP-TLS)	AP1_WS-BYOD Access Staff
5. (Tips:Role EQUALS Student) AND (Authentication:OuterMethod EQUALS EAP-TLS)	AP1_WS-BYOD Access Student
6. (Tips:Role EQUALS Executives) AND (Authentication:OuterMethod EQUALS EAP-TLS)	AP1_WS-BYOD Access Exec
7. (Tips:Role EQUALS Staff) AND (Tips:Role EQUALS [Machine Authenticated])	AP1_WS-Staff
8. (Tips:Role EQUALS Student) AND (Tips:Role EQUALS [Machine Authenticated])	AP1_WS-Student
9. (Tips:Role EQUALS Executives) AND (Tips:Role EQUALS [Machine Authenticated])	AP1_WS-Executive
10. (Tips:Role EQUALS [User Authenticated])	AP1_WS-Onboard Pre Provision

[Add Rule](#) [Move Up](#) [Move Down](#) [Edit Rule](#) [Remove Rule](#)

Rules Editor

Conditions

Match ALL of the following conditions:

Type	Name	Operator	Value
1. Tips	Role	EQUALS	[User Authenticated]
2. Click to add...			

Enforcement Profiles

Profile Names:

[RADIUS] APJ_WS-Onboard Pre Provision

Move Up
Move Down
Remove

--Select to Add--

Save Cancel

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" !
```

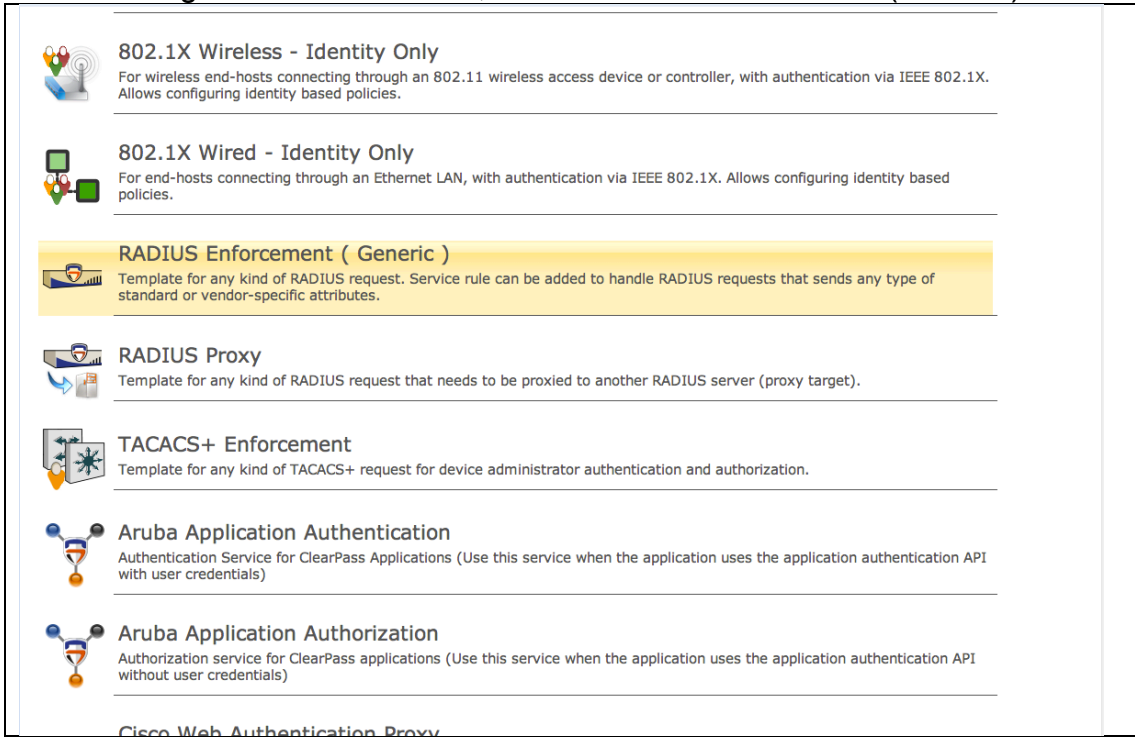
1.4. Testing Script

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 Configuration Workshop

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

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

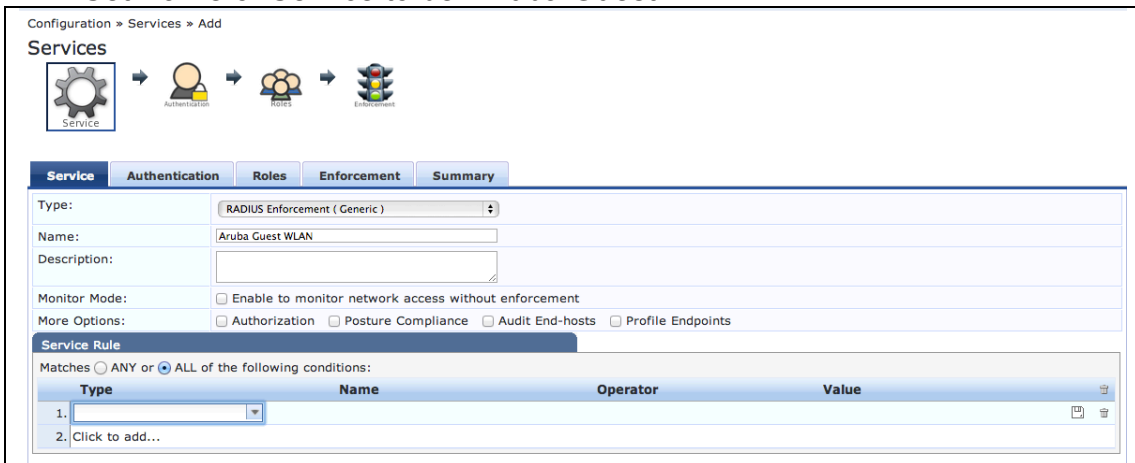


The screenshot shows the 'Services' page in ClearPass. It lists several service templates:

- 802.1X Wireless - Identity Only**: For wireless end-hosts connecting through an 802.11 wireless access device or controller, with authentication via IEEE 802.1X. Allows configuring identity based policies.
- 802.1X Wired - Identity Only**: For end-hosts connecting through an Ethernet LAN, with authentication via IEEE 802.1X. Allows configuring identity based policies.
- RADIUS Enforcement (Generic)**: Template for any kind of RADIUS request. Service rule can be added to handle RADIUS requests that sends any type of standard or vendor-specific attributes.
- RADIUS Proxy**: Template for any kind of RADIUS request that needs to be proxied to another RADIUS server (proxy target).
- TACACS+ Enforcement**: Template for any kind of TACACS+ request for device administrator authentication and authorization.
- Aruba Application Authentication**: Authentication Service for ClearPass Applications (Use this service when the application uses the application authentication API with user credentials)
- Aruba Application Authorization**: Authorization service for ClearPass applications (Use this service when the application uses the application authentication API without user credentials)

At the bottom, there is a link for **Cisco Web Authentication Proxy**.

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



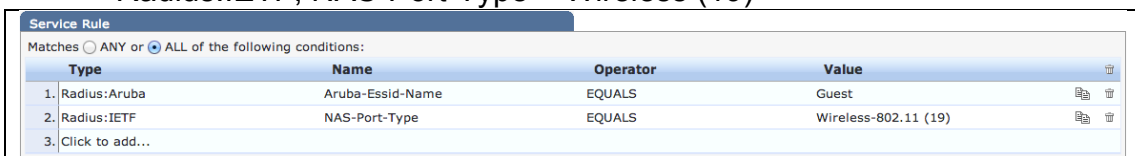
The screenshot shows the 'Configuration > Services > Add' page. The 'Service' tab is selected, and the service name is set to 'Aruba Guest WLAN'. The 'Type' is set to 'RADIUS Enforcement (Generic)'. The 'Description' field is empty. The 'Monitor Mode' is set to 'Enable to monitor network access without enforcement'. The 'More Options' section includes checkboxes for 'Authorization', 'Posture Compliance', 'Audit End-hosts', and 'Profile Endpoints'. The 'Service Rule' section shows a table with columns: Type, Name, Operator, and Value. The table contains two rows:

Type	Name	Operator	Value
1.	Radius:Aruba	EQUALS	Guest
2.	Radius:IETF	EQUALS	Wireless-802.11 (19)

The table also includes a 'Click to add...' option.

2.2. Set the following in Service Rules:

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



The screenshot shows the 'Service Rule' configuration page. It displays a table with columns: Type, Name, Operator, and Value. The table contains three rows:

Type	Name	Operator	Value
1.	Radius:Aruba	EQUALS	Guest
2.	Radius:IETF	EQUALS	Wireless-802.11 (19)
3.	Click to add...		

2.3. Set [PAP] as Authentication Method

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

The screenshot shows the 'Authentication' tab in the ClearPass configuration interface. It features two main sections: 'Authentication Methods' and 'Authentication Sources'. In the 'Authentication Methods' section, '[PAP]' is listed. In the 'Authentication Sources' section, '[Guest User Repository]' and '[Local SQL DB]' are listed. Below these sections, there is a 'Strip Username Rules' checkbox which is currently unchecked. The interface includes buttons for 'Move Up', 'Move Down', 'Remove', 'View Details', and 'Modify' for each item in the lists.

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)

The screenshot shows the 'Service Rule' configuration for the 'Guest PreAuth and OnBoard Authentication' service. The 'Type' is set to 'RADIUS Enforcement (Generic)'. The 'Name' is 'Guest PreAuth and OnBoard Authentication'. The 'Description' is empty. The 'Monitor Mode' checkbox is unchecked. The 'More Options' section includes checkboxes for 'Authorization', 'Posture Compliance', 'Audit End-hosts', and 'Profile Endpoints', all of which are unchecked. The 'Service Rule' section shows a table with the following conditions:

Type	Name	Operator	Value
1. Radius:IETF	NAS-IP-Address	EQUALS	127.0.0.1
2. Radius:IETF	NAS-Port-Type	EQUALS	Ethernet (15)
3. Radius:IETF	Service-Type	EQUALS	Authorize-Only (17)
4. Click to add...			

3.3. Set [PAP] as Authentication Method

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

The screenshot shows the 'Authentication' tab in the ClearPass configuration interface. The 'Authentication Methods' list now contains '[PAP]'. The 'Authentication Sources' list now contains '[Guest User Repository]' and 'ad.arubademo.local [Active Directory]'. The 'Strip Username Rules' checkbox remains unchecked. The interface includes buttons for 'Move Up', 'Move Down', 'Remove', 'View Details', and 'Modify' for each item in the lists.

3.5. Click “Save”

4. Configure ClearPass Guest

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

ClearPass 6.1 2013Q4 Partner Training Workshop Lab Exercises

Home » Configuration » Web Logins

Web Logins [Create a new web login page](#)

Many NAS devices support Web-based authentication for visitors.

By defining a web login page on the ClearPass Guest you are able to provide a customized graphical login page for visitors accessing the network through these NAS devices.

Use this list view to define new web login pages, and to make changes to existing web login pages.

Onboard device provisioning pages are now managed from the Web Login tab within provisioning settings

Name	Page Title	Page Name	Page Skin
There are no web login pages to display.			
0 web logins Reload Show all rows			

[Back to configuration](#)

[Back to main](#)

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

Home » Configuration » Web Logins

Web Login

Use this form to create a new RADIUS Web Login.

Web Login Editor	
* Name:	<input type="text" value="Guest Login"/> Enter a name for this web login page.
Page Name:	<input type="text" value="guest_login"/> Enter a page name for this web login. The web login will be accessible from "/guest/page_name.php".
Description:	<div></div> Comments or descriptive text about the web login.
* Vendor Settings:	<div>Aruba Networks</div> Select a predefined group of settings suitable for standard network configurations.
Address:	<input type="text" value="securelogin.arubanetworks.com"/> Enter the IP address or hostname of the vendor's product here.
Secure Login:	<div>Use vendor default</div> Select a security option to apply to the web login process.
Dynamic Address:	<input type="checkbox"/> The controller will send the IP to submit credentials In multi-controller deployments, it is often required to post credentials to different addresses made available as part of the original redirection. The address above will be used whenever the parameter is not available or fails the requirements below.
Login Form Options for specifying the behaviour and content of the login form.	
Authentication:	<div>Credentials — Require a username and password</div> Select the authentication requirement. Access Code requires a single code (username) to be entered. Anonymous allows a blank form requiring just the terms or a Log In button. A pre-existing account is required. Access Code and Anonymous require the account to have the Username Authentication field set.
Custom Form:	<input type="checkbox"/> Provide a custom login form If selected, you must supply your own HTML login form in the Header or Footer HTML areas.
Custom Labels:	<input type="checkbox"/> Override the default labels and error messages If selected, you will be able to alter labels and error messages for the current login form.
* Pre-Auth Check:	<div>RADIUS — check using a RADIUS request</div> Select how the username and password should be checked before proceeding to the NAS authentication.
Terms:	<input type="checkbox"/> Require a Terms and Conditions confirmation If checked, the user will be forced to accept a Terms and Conditions checkbox.

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

ClearPass 6.1 2013Q4 Partner Training Workshop Lab Exercises

* Login Delay: The time in seconds to delay while displaying the login message.

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

Post-Authentication
Actions to perform after a successful pre-authentication.

Policy Manager: ☐ Register the guest's MAC address with ClearPass Policy Manager
If selected and a ClearPass Policy Manager has been enabled, the username will be linked to the MAC.

* required field

[Back to RADIUS web logins](#)

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

Home » Configuration » Web Logins

Web Logins

Many NAS devices support Web-based authentication for visitors.

By defining a web login page on the ClearPass Guest you are able to provide a customized graphical login page for

Use this list view to define new web login pages, and to make changes to existing web login pages.

Onboard device provisioning pages are now managed from the Web Login tab within provisioning settings

Name	Page Title	Page Name	Page Skin
Guest Login	Login	guest-01_login	(Default)

Edit Duplicate Delete Test

1 web login Reload

4.5. Guest Login page, show on new Web Page

ClearPass Guest

Please login to the network using your ClearPass username and password.

Login

* Username:

* Password:

* required field

Contact a staff member if you are experiencing difficulty logging in.

5. Create New Guest User for Testing

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

5.2. Click “Add Guest User”

Configuration » Identity » Guest Users

Guest Users

[Add Guest User](#)
[Import Guest Users](#)
[Export Guest Users](#)

Filter: Username contains Show 10 records

#	<input type="checkbox"/>	Username ▲	Sponsor Name	Guest Type	Status	Expired	Source Application
1.	<input type="checkbox"/>	dickylcd@gmail.com	admin	USER	Enabled	Expired	Guest
2.	<input type="checkbox"/>	dickylcd@hotmail.com	admin	USER	Enabled	Expired	Guest

Showing 1-2 of 2

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

Add New Guest User

Guest Type	<input checked="" type="radio"/> USER <input type="radio"/> DEVICE
Username:	<input type="text" value="guest-01"/>
Password:	<input type="text" value="aruba123"/> <input type="button" value="Auto Generate"/>
Expiry Time:	<input type="text" value="2013-05-17 15:40:36"/> <input type="button" value="Calendar"/>
Enable Guest:	<input checked="" type="checkbox"/>

Attributes

Attribute	Value
1. Click to add...	

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

Configure WLAN/LANs

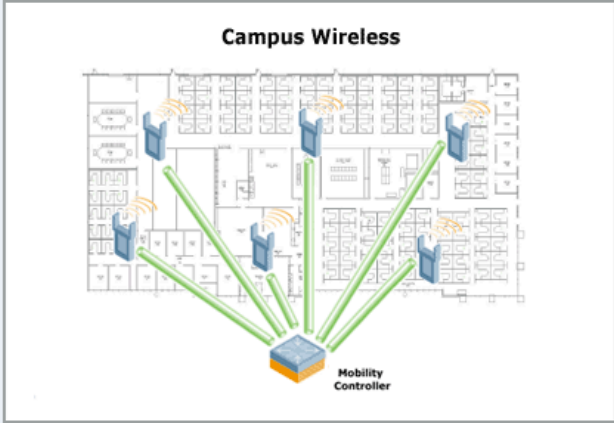
Welcome to the WLAN/LAN Configuration Wizard

Deployment scenario:

☒ Campus Only -- all of the access points will be physically connected to the local controller

☐ Remote Networking -- some of the access points will be deployed at remote locations

Campus Wireless



The diagram illustrates a campus wireless network. At the bottom center is a 'Mobility Controller' represented by a blue and orange cube. Above it, a floor plan of a building is shown. Several blue access point icons are placed on the floor plan. Green lines connect each access point to the Mobility Controller, indicating a central architecture where all APs are connected to a single controller.

Begin **Cancel**

6.1.2. Use "Default" AP-Group & Click "Next" button

Specify Group to Configure

An AP group is a set of APs that share Wireless LAN parameters. Initially there is a single group named Default. If you wish, you can create multiple groups. [More...](#)

Group **New**

Note: The setting you select in the Wireless LAN will apply to the Group you select here. If you wish to configure multiple groups you can make multiple passes through Wizards.

Next **Cancel**

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

Specify Wireless LAN (WLAN) for Group default

APs are organized into AP groups, and each AP group can advertise up to 8 WLANs. You can edit an existing WLAN or create a new WLAN. If you choose to edit an existing WLAN, note that WLANs can be assigned to multiple AP groups. Edit the shared WLAN if you wish to affect all AP groups, or edit a copy of the WLAN if you wish to affect only the selected AP group. [More...](#)

AP Groups	WLANs for default	WLAN Sharing
ALL AP GROUPS		
default		
dl-home		

You can:

- Select an existing WLAN in Group **default**
- Create a new WLAN by selecting Group **default** and clicking **New**
- Create a new WLAN by selecting an existing WLAN in any Group and clicking **Copy**
- Share a new WLAN that belongs to another Group by selecting the WLAN and...

Create new WLAN named:

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

Specify Forwarding Mode for Guest-01 in Group default

The Forwarding Mode provides a range of options for forwarding traffic back to the controller through the IPsec tunnel. [More...](#)

Forward Mode:

☒ Tunnel
☐ Decrypt-Tunnel
☐ Bridge

In Tunnel mode, the traffic is forwarded back to the controller through the IPsec tunnel.

BackNextCancel

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

- Radio Type: All
- VLAN: 20

Click "Next" button for continue.

Specify Radio Type and VLAN for Guest-01 in Group default

Specify the radio type on which this SSID is available, as well as the VLAN in which users connecting to this SSID are to be placed by default. Note: you can override the VLAN specified below by configuring per-role VLANs in Step 8. [More...](#)

Radio Type:

VLAN:

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

Specify whether WLAN is for Internal or Guest use for Guest-01 in Group default

Guest WLANs allow guests to access the Internet, while blocking access to the internal network. Guest WLANs are not encrypted, and at most require Web-based authentication. Internal WLANs typically employ encryption and stronger layer 2 authentication. [More...](#)

Is this WLAN intended for internal use or for use by guests?

☐ Internal

☒ Guest

Back

Next

Cancel

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."

Specify Authentication and Encryption for Guest-01 in Group default

The authentication and encryption options below are grouped by the level of security they guarantee. [More...](#)

More
Secure

- ☒ Captive portal with authentication via credentials(username and password) provided by user.
- ☐ Captive Portal with email registration.User's email is required but not verified
- ☐ Captive Portal with no authentication or registration
- ☐ Direct access to Internet (no Captive Portal)

Less
Secure

[Back](#) [Next](#) [Cancel](#)

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

Specify Captive Portal Options for Guest-01 in Group default

Captive portal provides web-based authentication. If captive portal is enabled, users who connect to this WLAN must authenticate by opening a web browser. They will be automatically redirected to the captive portal page and required to provide a username and password. Usernames and passwords can be stored either in a local database or on an external RADIUS server. [More...](#)

☒ Enable Captive Portal

Template: **Custom HTML**

Page Design: **Welcome Text** Policy Text

Background: **Default Image**

Logo: **Choose File** No file chosen

[Refresh >>](#)

[Preview current settings](#)

[Back](#) [Next](#) [Cancel](#)

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

Specify Authentication Server for Guest-01 in Group default

An enterprise environment typically uses an external RADIUS server for authentication. The controller also has an internal database that can be used for small scale or test deployments. [More...](#)

Ordered list of Authentication servers:

Up

Down

☐ Select from known servers

☒ Specify new server

Server type: ☒ RADIUS ☐ LDAP

Name:

IP address:

Auth port:

Acct port:

Shared key:

Retype key:

Ok

Cancel

Back

Next

Cancel

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 <table border="1"> <thead> <tr> <th>Source</th> <th>Dest</th> <th>Service</th> <th>Action</th> </tr> </thead> <tbody> <tr><td> </td><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td><td> </td></tr> </tbody> </table>	Source	Dest	Service	Action																					Policy Sharing <div> </div>
Source	Dest	Service	Action																								
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:

Authenticated role:

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](#).

WLAN Configuration is Complete

The configuration you have specified is summarized below. Configuration settings will be applied when you click the Finish button.

Mobility Controller Setup Summary Fri May 17 2013

1 Group

Group to Configure
Default

2 Wireless LANs

WLAN 1 (Created)

WLAN
APGroup: default
SSID: Guest-01
Forwarding Mode

[Back](#) [Finish](#) [Cancel](#)

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"

Servers | AAA Profiles | L2 Authentication | **L3 Authentication** | User Rules | Advanced

Captive Portal Authentication Profile

- default
 - Server Group default
 - + Guest-01-cp_prof
 - + NoAuthCPProfile
- + WISPr Authentication Profile
- + VPN Authentication Profile
- + Stateful NTLM Authentication Profile

Captive Portal Authentication Profile > default [Show Reference](#) [Save As](#) [Reset](#)

Default Role	guest	Default Guest Role	guest
Redirect Pause	1 sec	User Login	<input checked="" type="checkbox"/>
Guest Login	<input type="checkbox"/>	Logout popup window	<input type="checkbox"/>
Use HTTP for authentication	<input type="checkbox"/>	Logon wait minimum wait	5 sec
Logon wait maximum wait	10 sec	logon wait CPU utilization threshold	60 %
Show FQDN	<input type="checkbox"/>	Use CHAP (non-standard)	<input type="checkbox"/>
Login page	https://192.168.10.31/g	Welcome page	/auth/welcome.html
Show Welcome Page	<input type="checkbox"/>	Add switch IP address in the redirection URL	<input type="checkbox"/>
Allow only one active user session	<input type="checkbox"/>	White List	<div><input type="text"/> Delete Add</div>
Black List	<div><input type="text"/> Delete Add</div>	Show the acceptable use policy page	<input type="checkbox"/>

8. Modify Pre Authentication Role

8.1. At Configuration > Security > Access Control > Policies

8.2. Create new policy as below:

- Policy Name: allow-cppm

ClearPass 6.1 2013Q4 Partner Training Workshop Lab Exercises

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

Security > Firewall Policies > Add New Policy

User Roles | System Roles | Policies | Time Ranges | Guest Access

Policy Name: allow-cppm
Policy Type: Session

Rules

IP Version	Source	Destination	Service	Action	Log	Mirror	Queue	Time Range	Pause ARM Scanning	BlackList	Classify Media	TOS	802.1p Priority	Action
IPv4	user	host 192.168.10.31	svc-http	permit			low		No	No				Delete
IPv4	user	host 192.168.10.31	svc-https	permit			low		No	No				Delete

Commands

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

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

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

Security > Access Control > User Roles

User Roles | System Roles | Policies | Time Ranges | Guest Access

Name: Guest-01-guest-logout
logon-control/captiveportal/

Bandwidth Contract: Up:Not Enforced Down:Not Enforced

Actions: Show Reference, Edit, Delete

Firewall Policies

Name	Rule Count	Location	Action
allow-cppm	2		Edit, Delete
logon-control	5		Edit, Delete
captiveportal	6		Edit, Delete

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

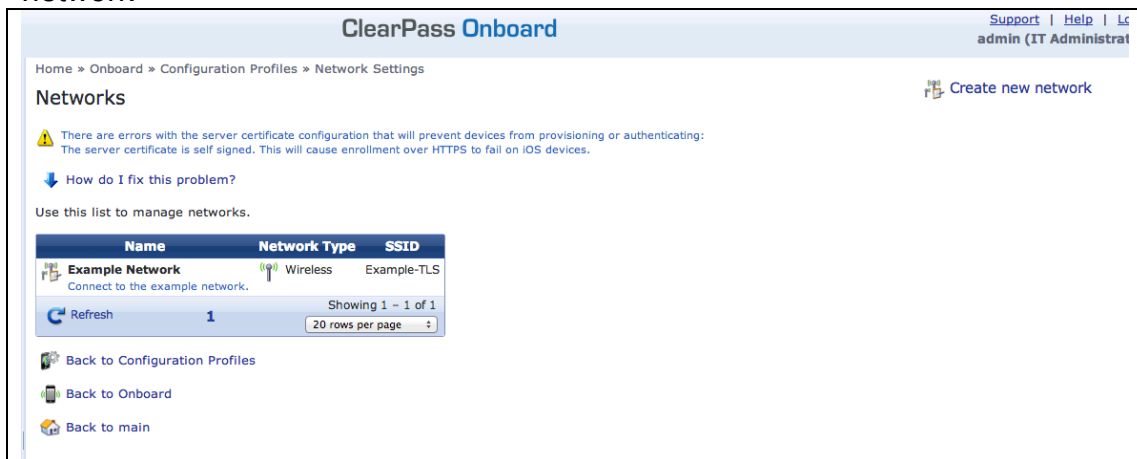
- It should login success and able to access to Internet
- It will show on ClearPass Access Checker.

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

Use this form to create the network settings that will be sent to a provisioned device.

Network Settings » Network Access	
Access#	Protocols
Authentication	Trust
Windows	Proxy
Network Access Options for basic network access.	
* Name:	<input type="text" value="SecureWLAN"/> Enter a name for the network.
Description:	<div></div> Enter a description for the network.
* Network Type:	<div>Wireless only</div> Select which types of network will be provisioned. Enterprise security (802.1X) will be selected if wired networks are to be supported.
* Security Type:	<div>Enterprise (802.1X)</div> Select the authentication method used for the network. Enterprise security (802.1X) will be selected if wired networks are to be supported.
Wireless Network Settings Options for wireless network access.	
* Security Version:	<div>WPA2 with AES (recommended)</div> Select the WPA encryption version for the wireless network. This setting is used for Windows, Android and Legacy OS X (10.5/6) devices only. iOS and OS X 10.7+ (Lion or later) devices auto-detect the WPA version.
* SSID:	<input type="text" value="securewlan"/> Enter the SSID of the wireless network to connect to.
Wireless:	<input type="checkbox"/> Hidden network Select this option if the wireless network is not open or broadcasting.
Auto Join:	<input checked="" type="checkbox"/> Automatically join network Select this option to automatically join the wireless network.
<div>Next</div> <div>Save Changes</div> <div>Cancel</div>	

* required field

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

ClearPass 6.1 2013Q4 Partner Training Workshop Lab Exercises

Use this form to create the network settings that will be sent to a provisioned device.

Network Settings » Enterprise Protocols

Access# Protocols Authentication Trust Windows Proxy

Enterprise Protocols
Options for 802.1X protocols supported on the network.

iOS & OS X EAP

iOS & OS X EAP: Accepted EAP Types
☒ TLS ☐ PEAP
☐ TTLS ☐ EAP-FAST
Select the authentication protocols to use when configuring an iOS or OS X 10.7+ (Lion or later) device.

Legacy OS X EAP

Legacy OS X EAP: PEAP with MSCHAPv2
The authentication protocol to use when configuring OS X 10.5/6 (Leopard/Snow Leopard) devices.

Android EAP

Android EAP: PEAP with MSCHAPv2
Select the authentication protocol to use when configuring an Android device.

Windows EAP

Windows EAP: PEAP with MSCHAPv2
The authentication protocol to use when configuring a Windows device.

Fast Reconnect: ☐ Enable Fast Reconnect

Quarantine: ☐ Enforce Network Access Protection
This setting is labeled 'Enable Quarantine checks' in older versions of Windows.

Cryptobinding: ☐ Enforce Cryptobinding

Previous Next Save Changes Cancel

* required field

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

Use this form to create the network settings that will be sent to a provisioned device.

Network Settings » Enterprise Authentication

Access# Protocols Authentication Trust Windows Proxy

Enterprise Authentication
Options for 802.1X authentication used on the network.

iOS & OS X Authentication

* iOS & OS X Credentials: Certificate
Select the type of credentials to provision for iOS and OS X 10.7+ (Lion or later) devices.

Windows Authentication

* Vista Credentials: Machine or User
Select the authentication mode to use for Windows Vista (or later) devices.

* XP Credentials: Machine or User
Select the authentication mode to use for Windows XP devices.

Previous Next Save Changes Cancel

* required field

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

Use this form to create the network settings that will be sent to a provisioned device.

Network Settings » Enterprise Trust	
Access#	Protocols
Authentication	Trust
Windows	Proxy
Enterprise Trust Certificate trust options for 802.1X protocols supported on the network.	
Configure Trust:	Automatically configure trust settings (recommended) Use automatic configuration if you are using Policy Manager for authentication. Otherwise, select manual configuration.
Trusted Server Names:	<input type="text"/> Enter the certificate names expected from the authentication server, one per line. Wildcards may be used to specify the name (e.g. wpa.*.example.com). If a server presents a certificate that isn't in this list, it won't be trusted.
<input type="button" value="Previous"/> <input type="button" value="Next"/> <input type="button" value="Save Changes"/> <input type="button" value="Cancel"/>	

* required field

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

Use this form to create the network settings that will be sent to a provisioned device.

Network Settings » Windows Network Settings	
Access#	Protocols
Authentication	Trust
Windows	Proxy
Windows Networking Settings These settings are only applicable to Windows devices.	
NAP Services:	<input type="checkbox"/> Enable NAP services See also 'Enforce Network Access Protection' on the Protocols tab.
Admin Username:	<input type="text"/> Enter if configuration of networking requires administrator credentials.
Admin Password:	<input type="text"/> Enter if configuration of networking requires administrator credentials.
IP Address:	<input checked="" type="checkbox"/> Assign IP address using DHCP
DNS:	<input checked="" type="checkbox"/> Assign DNS using DHCP
DNS Registration:	<input checked="" type="checkbox"/> Register IP address with DNS
Windows XP Networking	
Configure Using:	<input checked="" type="checkbox"/> Use Windows to configure wireless
Notification Icon:	<input checked="" type="checkbox"/> Show icon in notification
Notify Connectivity:	<input checked="" type="checkbox"/> Notify when connectivity is limited
<input type="button" value="Previous"/> <input type="button" value="Next"/> <input type="button" value="Save Changes"/> <input type="button" value="Cancel"/>	

* required field

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

ClearPass 6.1 2013Q4 Partner Training Workshop Lab Exercises

Use this form to make changes to the network settings that will be sent to a provisioned device.

Network Settings » Proxy


 Access  Protocols  Authentication  Trust  Windows  Proxy


Proxy Settings
Options for proxy settings on the network.

* Proxy Type:

Select your network's proxy server configuration type.

 Previous


 Save Changes


 Cancel


* required field

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


Home » Onboard » Provisioning Settings


Provisioning Settings  Create new 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 list to manage provisioning settings.

Name	CA	Profile
 Local Device Provisioning This is the default configuration set for device provisioning.	Local Certificate Authority	Default Profile

 Refresh 1 Showing 1 - 1 of 1 20 rows per page


 Back to Onboard

 Back to main

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

ClearPass 6.1 2013Q4 Partner Training Workshop Lab Exercises

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	
<div>General Web Login iOS iOS & OS X Legacy OS X Windows Android Onboard Client</div>	
* Name:	<input type="text" value="SecureWLAN Device Provisioning"/> <small>Enter a name for this configuration set.</small>
Description:	<div></div> <small>Enter a description for the configuration set.</small>
* Organization:	<input type="text" value="APJ ClearPass Workshop"/> <small>Enter an organization name for this configuration set. The organization name is displayed by the device during provisioning.</small>
Identity <small>These options control the generation of device credentials</small>	
* Certificate Authority:	<div>Local Certificate Authority</div> <small>Select the certificate authority that will be used to sign profiles and messages.</small>
* Key Type:	<div>2048-bit RSA — created by server</div> <small>Select the type of private key to use for TLS certificates.</small>
* Unique Device Credentials:	<input checked="" type="checkbox"/> Include the username in unique device credentials <small>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.</small>
Authorization <small>These options control how a device is authorized during provisioning.</small>	
* Configuration Profile:	<div>Default Profile</div> <small>Select the configuration profile that will be provisioned to devices.</small>
* Maximum Devices:	<div>1</div> <small>The maximum number of devices that a user may provision. Use 0 for unlimited.</small>
Supported Devices <small>These options control which devices may be provisioned.</small>	
* iOS & OS X Devices:	<input checked="" type="checkbox"/> Enable iOS and OS X 10.7+ (Lion or later) device provisioning <small>Provision iOS and OS X 10.7+ (Lion or later) devices via Apple's 'Over-the-Air' profile delivery process.</small>
* OS X 10.5/6 Devices:	<input checked="" type="checkbox"/> Enable OS X 10.5 (Leopard) and 10.6 (Snow Leopard) device provisioning <small>Downloads and executes an OS X application on a user's device to complete provisioning.</small>
* Windows Devices:	<input checked="" type="checkbox"/> Enable Windows XP, Vista and 7 (or later) device provisioning <small>Downloads and executes a Windows application on a user's device to complete provisioning.</small>
* Android Devices:	<input checked="" type="checkbox"/> Enable Android device provisioning <small>Downloads and executes an Android application on a user's device to complete provisioning.</small>
Unsupported Device:	<div><pre>{nwa_icontext type=error} {nwa_text id=10891}Your operating system is not supported. Please contact your network administrator.{/nwa_text}
<small>HTTP User-Agent: {Smarty.server.HTTP_USER_AGENT escape} </small> {/nwa_icontext}</pre></div> <div>Insert content item...</div> <small>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.</small>
<div>Next Save Changes Cancel</div>	

* 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	 Legacy OS X
 Windows	 Android
 Onboard Client	
Web Login Page Options for the weblogin landing page for Onboard.	
* Page Name:	<input type="text" value="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:	<input type="checkbox"/> Provide a custom login form If selected, you must supply your own HTML login form in the Header or Footer HTML areas.
Custom Labels:	<input type="checkbox"/> 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:	<input type="checkbox"/> 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:	<input type="text" value="(Default)"/> Choose the skin to use when this web login page is displayed.
Title:	<input type="text" value="Register Your Device"/> The title to display on the web login page.
Header HTML:	<div> <pre>{nwa_cookiecheck} {* Onboard instructions can be edited on a per device type basis under Onboard Provisioning Settings *} </pre> </div> <div> <input type="button" value="Insert content item..."/> <input type="button" value="Insert self-registration link..."/> </div> <p>HTML template code displayed before the login form.</p>

ClearPass 6.1 2013Q4 Partner Training Workshop Lab Exercises

Footer HTML:	<p><p> Contact a staff member if you are experiencing difficulty logging in. </p></p> <p>Insert content item... ▾ Insert self-registration link... ▾</p> <p>HTML template code displayed after the login form.</p>
Network Login Access Controls access to the login page.	
Allowed Access:	<input type="text"/> Enter the IP addresses and networks from which logins are permitted.
Denied Access:	<input type="text"/> 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.
<div> <input type="button" value="Previous"/> <input type="button" value="Next"/> <input type="button" value="Save Changes"/> <input type="button" value="Cancel"/> </div>	

* required field

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

Device Provisioning Settings	
<div> General# Web Login iOS iOS & OS X Legacy OS X Windows Android Onboard Client# </div>	
iOS & OS X Provisioning These options control Apple iOS (iPad, iPod, iPhone) and OS X (Lion or later) device provisioning.	
* Display Name:	<input type="text" value="Device Enrollment"/> Example: 'Device Enrollment'. This text is displayed as the title of the 'Install Profile' screen on the device.
* Profile Description:	<input type="text"/> 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:	<input type="checkbox"/> 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:	<input type="text" value="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.

ClearPass 6.1 2013Q4 Partner Training Workshop Lab Exercises

Instructions

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

Before Provisioning:

[illegible]

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.

ClearPass 6.1 2013Q4 Partner Training Workshop Lab Exercises

Manual Reconnect Interface:	<pre> {** * 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 %1 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. *} </pre> <p>Insert content item... ▾</p> <p>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.</p> <p>Enter the HTML code to display. Smarty template functions can be used here. Leave this field empty to use the default instructions.</p>
Connect Success:	<pre> {** * OPTIONAL. The contents of this section * will be shown AFTER a SUCCESSFUL * reconnect. *} </pre> <p>Insert content item... ▾</p> <p>The contents of this section will be shown after a successful reconnect.</p> <p>Enter the HTML code to display. Smarty template functions can be used here. Leave this field empty to use the default instructions.</p>
Connect Failure:	<pre> {** * 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 %1 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 %1 SSID to access the intranet.{/nwa_text} {/nwa_icontext} {else} </pre> <p>Insert content item... ▾</p> <p>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.</p> <p>Enter the HTML code to display. Smarty template functions can be used here. Leave this field empty to use the default instructions.</p>
After Connect:	<pre> {** * OPTIONAL. The contents of this section * will be shown AFTER a reconnect attempt, * regardless of success or failure. *} </pre> <p>Insert content item... ▾</p> <p>The contents of this section will be shown after a reconnect attempt, regardless of success or failure.</p> <p>Enter the HTML code to display. Smarty template functions can be used here. Leave this field empty to use the default instructions.</p>
* Advanced Settings:	<input checked="" type="checkbox"/> Show advanced reconnection settings
* Disconnect Delay:	<div>3 seconds</div> <p>When the web server receives a disconnect request, it will wait for this duration before issuing the disconnect request to the controller.</p> <p>This delay gives the client time to receive a valid HTTP response before begin disconnected from the network.</p>

ClearPass 6.1 2013Q4 Partner Training Workshop Lab Exercises

* Reconnect Delay:	<input type="text" value="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:	<input type="text" value="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.
<div> <input type="button" value="Previous"/> <input type="button" value="Next"/> <input type="button" value="Save Changes"/> <input type="button" value="Cancel"/> </div>	

* 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'}
```

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}
```








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.

* required field

ClearPass 6.1 2013Q4 Partner Training Workshop Lab Exercises

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:

```
{nwaicontext 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}
{/nwaicontext}
{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

ClearPass 6.1 2013Q4 Partner Training Workshop Lab Exercises

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

Device Provisioning Settings	
<div>General# Web Login iOS iOS & OS X Legacy OS X Windows Android Onboard Client#</div>	
Android Provisioning These options control Android device provisioning.	
Android Rootkit Detection:	<div>Provision all devices</div> <div>Control whether devices with a rootkit may be provisioned.</div>
Instructions These options control the text shown during provisioning for Android devices.	
Before Provisioning:	<div><pre>{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'}</pre></div> <div>Insert content item...</div> <div>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.</div>
Next Step:	<div><pre>{nwa_text id=10895}<p>After you have downloaded and installed the application, please click Next.</p>{/nwa_text} {assign var=link_text value=1732 NwaText:'Next'}</pre></div> <div>Insert content item...</div> <div>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.</div>

ClearPass 6.1 2013Q4 Partner Training Workshop Lab Exercises

Before Profile Install:	<div data-bbox="512 210 1157 488"><pre>{nwa_text id=10894}<p>To configure your device, you must now install the following network profile.</p>{/nwa_text} {assign var=link_text value=10901 NwaText:'Download the network profile and install it using QuickConnect.'} {assign var=link_command value=10900 NwaText:'Install Network Profile'}</pre></div> <div data-bbox="949 497 1145 519">Insert content item... ▾</div> <p>These instructions are shown to the user before they install the network profile on 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.</p>
After Provisioning:	<div data-bbox="512 607 1157 884"><pre>{nwa_text id=10892}<p>QuickConnect will now apply the network profile to your device.</p>{/nwa_text}</pre></div> <div data-bbox="949 893 1145 916">Insert content item... ▾</div> <p>These instructions are shown to the user after they have provisioned 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.</p>
<div data-bbox="497 1010 1094 1046">Previous Next Save Changes Cancel</div>	

* required field

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.

ClearPass 6.1 2013Q4 Partner Training Workshop Lab Exercises

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

Device Provisioning Settings	
<div> General# Web Login iOS & OS X Legacy OS X Windows Android Onboard Client# </div>	
Device Provisioning Options for Windows, Android and Legacy OS X (10.5/6) device provisioning. These settings are not used for iOS or OS X 10.7+ (Lion or later) devices.	
* Provisioning Address:	<input type="text" value="cpmv61.workshop (requires DNS resolution)"/> Select the hostname or IP address to use for device provisioning.
Provisioning Access:	To be provisioned, devices must be able to access cpmv61.workshop via HTTPS .
* Validate Certificate:	<input type="text" value="No, do not validate this web server's certificate"/> Specify whether the web server's certificate is to be validated during device provisioning. When testing with the default self-signed web server certificate, you may need to disable validation. This option applies to Windows, Android, and OS X 10.5/6 devices only.
Logo Image:	<div>  (Default) (188 x 53) </div> Select an image to use in the provisioning wizard. New images can be uploaded using the Content Manager.
* Wizard Title:	<input type="text" value="Onboard Wizard"/> Enter a title for the wizard used on Windows and Legacy OS X (10.5/6) devices.
Password Recovery URL:	<input type="text"/> Enter the URL displayed to users who have forgotten their password.
Helpdesk URL:	<input type="text"/> Enter the URL displayed to users who require helpdesk assistance.
<div> <input type="button" value="Previous"/> <input type="button" value="Save Changes"/> <input type="button" value="Cancel"/> </div>	

* required field

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

	802.1X Wireless For wireless end-hosts connecting through an 802.11 wireless access device or controller, with authentication via IEEE 802.1X. Allows configuring both identity and posture based policies.
	802.1X Wired For end-hosts connecting through an Ethernet LAN, with authentication via IEEE 802.1X. Allows configuring both identity and posture based policies.
	MAC Authentication MAC-based authentication bypass service, for end-hosts without an 802.1X supplicant or a posture agent (printers, other embedded devices, and computers owned by guests or contractors). Authentication is based on the MAC-address of the end-host being present in a white list or black list.
	Web-based Authentication Web-based authentication service for guests or agentless hosts, via the Policy Manager Portal. The user is redirected to the Policy Manager captive portal by the network device, or by a DNS server that is set up to redirect traffic on a subnet to a specific URL. The web page collects username and password, and also optionally collects health information.
	Web-based Health Check Only Web-based authentication service for guests or agentless hosts, via the Policy Manager Portal. Health-Check only.

3.1. At new service tab, enter below information:

Name: Secure Network Posture Assessment

More Options: check "Posture Compliance"

ClearPass 6.1 2013Q4 Partner Training Workshop Lab Exercises

The screenshot shows the 'Service' configuration page with the 'Posture' tab selected. The 'Type' is set to 'Web-based Health Check Only'. The 'Name' is 'Secure Network Posture Assessment'. The 'Description' field is empty. Under 'Monitor Mode', 'Enable to monitor network access without enforcement' is unchecked. Under 'More Options', 'Authorization' is unchecked and 'Posture Compliance' is checked. The 'Service Rule' section shows 'Matches' set to 'ALL of the following conditions:'. A table lists the conditions:

Type	Name	Operator	Value
1. Host	CheckType	MATCHES_ALL	Health
2. Click to add...			

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”

The screenshot shows the 'Policy' configuration page with the 'Policy' tab selected. The 'Policy Name' is 'Check Windows Posture'. The 'Description' field is empty. Under 'Posture Agent', 'OnGuard Agent (Persistent or Dissolvable)' is selected. Under 'Host Operating System', 'Windows' is selected. The 'Restrict by Roles' section is empty, with 'Remove' and 'Add' buttons visible.

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

The screenshot shows the 'Posture Plugins' configuration page. It displays a table of plugins with checkboxes and 'Configure' and 'View' buttons.

Plugin Name	Plugin Configuration
<input checked="" type="checkbox"/> ClearPass Windows Universal System Health Validator	Configure View
<input type="checkbox"/> Windows System Health Validator	Configure View
<input type="checkbox"/> Windows Security Health Validator	Configure View

- 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 6.1 2013Q4 Partner Training Workshop Lab Exercises

The image displays two screenshots of the ClearPass Windows Universal System Health Validator interface, showing the configuration for different Windows operating systems.

Top Screenshot: Windows XP Configuration

- Windows Server 2003**: ☒ Enable checks for Windows XP
- Windows XP**: ☒ A firewall application is on
 - Remediation checks: ☒ Auto Remediation, ☒ User Notification
 - Product-specific checks: ☐ (Uncheck to allow any product)
- Windows Vista**: ☐
- Windows 7**: ☐
- Windows Server 2008**: ☐
- Windows 8**: ☐
- Quarantine Message**:
- Buttons**: Reset, Save, Cancel

Left Panel (System Components):

- Services
- Processes
- Registry Keys
- AntiVirus
- AntiSpyware
- Firewall**
- Peer To Peer
- Patch Management
- Windows Hotfixes
- USB Devices
- Virtual Machines

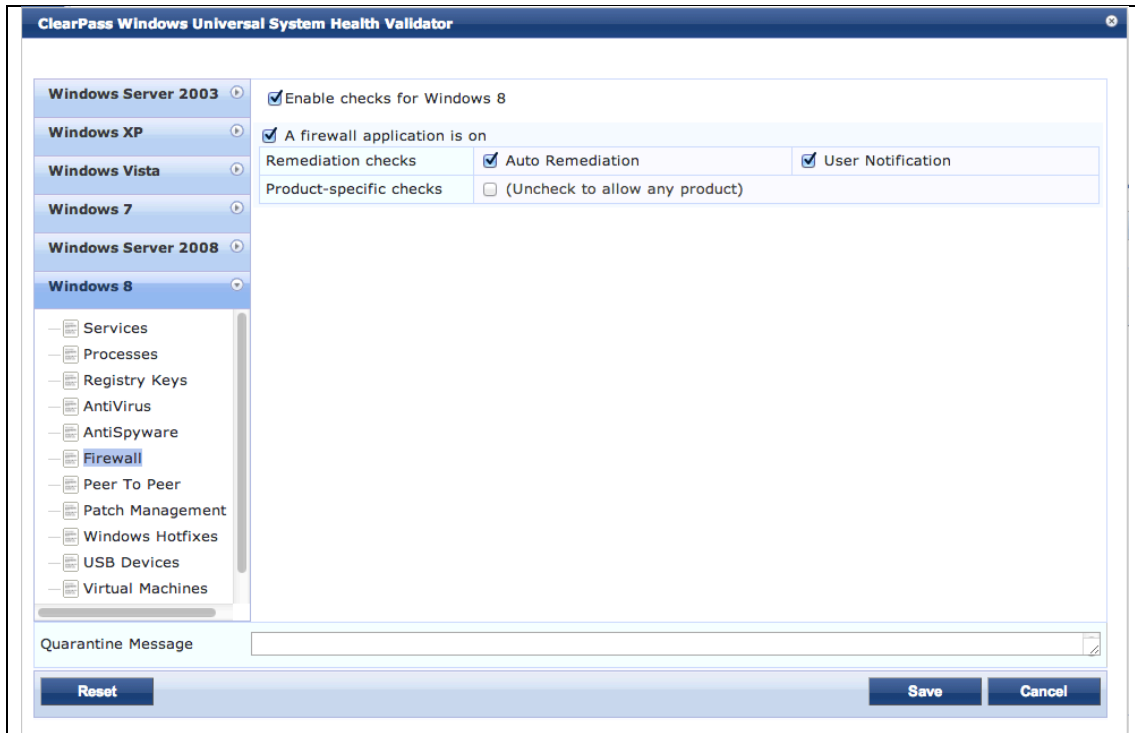
Bottom Screenshot: Windows 7 Configuration

- Windows Server 2003**: ☒ Enable checks for Windows 7
- Windows XP**: ☐ A firewall application is on
- Windows Vista**: ☐ A firewall application is on
 - Remediation checks: ☒ Auto Remediation, ☒ User Notification
 - Product-specific checks: ☐ (Uncheck to allow any product)
- Windows 7**: ☒ A firewall application is on
 - Remediation checks: ☒ Auto Remediation, ☒ User Notification
 - Product-specific checks: ☐ (Uncheck to allow any product)
- Windows Server 2008**: ☐
- Windows 8**: ☐
- Quarantine Message**:
- Buttons**: Reset, Save, Cancel

Left Panel (System Components):

- Services
- Processes
- Registry Keys
- AntiVirus
- AntiSpyware
- Firewall**
- Peer To Peer
- Patch Management
- Windows Hotfixes
- USB Devices
- Virtual Machines

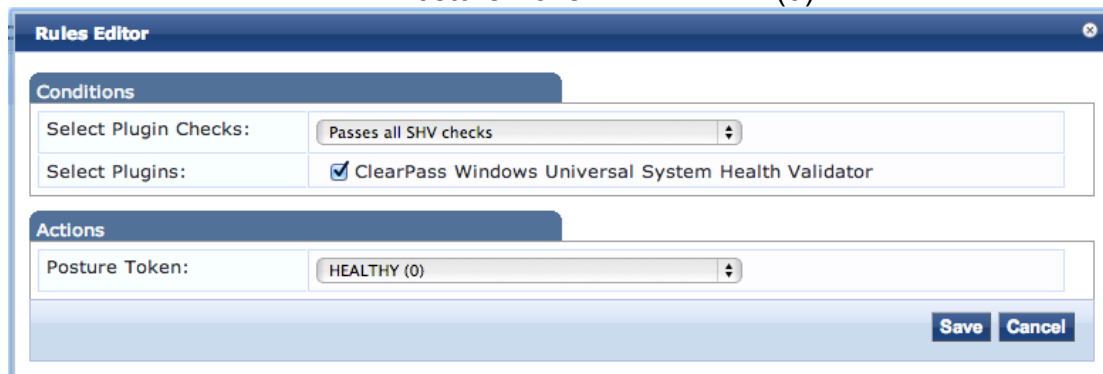
ClearPass 6.1 2013Q4 Partner Training Workshop Lab Exercises



- 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)

Rules Editor

Conditions

Select Plugin Checks: Fails one or more SHV checks

Select Plugins: ☒ ClearPass Windows Universal System Health Validator

Actions

Posture Token: QUARANTINE (20)

Save Cancel

- 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”

Policy Posture Plugins Rules Summary

Policy Name: Check Mac Posture

Description:

Posture Agent: ☐ NAP Agent ☒ OnGuard Agent (Persistent or Dissolvable)

Host Operating System: ☐ Windows ☐ Linux ☒ Mac OS X

Restrict by Roles:

Remove

Select or type role names

Add

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

Policy Posture Plugins Rules Summary

Select one/more plugins:

Plugin Name	Plugin Configuration
<input checked="" type="checkbox"/> ClearPass Mac OS X Universal System Health Validator	Configure View

- 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]

Enforcement	Rules	Summary
Name:	Bounce Client When Healthy	
Description:		
Enforcement Type:	<input type="radio"/> RADIUS <input type="radio"/> TACACS+ <input checked="" type="radio"/> WEBAUTH (SNMP/Agent/CLI/CoA) <input type="radio"/> Application	
Default Profile:	[RADIUS_CoA] [Aruba Terminate Session] View Details Modify	

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]

Enforcement	Rules	Summary
Rules Evaluation Algorithm: <input checked="" type="radio"/> Select first match <input type="radio"/> Select all matches		
Enforcement Policy Rules:		
Conditions		
Add Rule Move Up Move Down		

Rules Editor

Conditions				
Match ALL of the following conditions:				
Type	Name	Operator	Value	
1. Tips	Posture	EQUALS	HEALTHY (0)	
2. Click to add...				

Enforcement Profiles

Profile Names:	[RADIUS_CoA] [Aruba Terminate Session] Move Up Move Down Remove
	--Select to Add--

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

- 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 1 no logout-popup-
window login-page "https://cppm.arubademo.local/guest/device_provisioning.php" no
enable-welcome-page

switch ip in-redirect-url !

aaa authentication captive-portal "OnGuard-Redirect" redirect-pause 1 no logout-popup-
window login-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 quarantine access-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 --- >