Configure domain ........................................................................................................ 24
Configure WLAN ESS ............................................................................................... 24
Configure Service template ...................................................................................... 24
Assign Service template to AP .................................................................................. 24
Save your work ........................................................................................................... 24
Reset the AP ............................................................................................................... 24
Configure ClearPass .................................................................................................... 24
  Log in ......................................................................................................................... 24
  Add controller as device on ClearPass ................................................................. 25
Create a new user (MAC Address) on ClearPass internal DB ................................. 27
Create a new Enforcement Profile ......................................................................... 28
Create a new Enforcement Policy ............................................................................ 29
Create a new Service ................................................................................................. 31
Verify expected behavior ......................................................................................... 33
Conclusion .................................................................................................................. 33

Guest Access with MAC Caching .............................................................................. 33
Configure ClearPass .................................................................................................... 34
  Log In to Guest Manager ......................................................................................... 34
  Create Guest User Account ..................................................................................... 34
  Create Guest Web Login Page .................................................................................. 35
Log In to Policy Manager .......................................................................................... 37
Run Guest Authentication with MAC Caching Service Template ............................. 38
Edit MAC Authentication Service .......................................................................... 41
Disable Unneeded Service ......................................................................................... 41
Run Web-based Authentication Service Template .................................................... 42
Modify Web Authentication Service ......................................................................... 47
Configure WLC ............................................................................................................ 48
  Configure RADIUS scheme ...................................................................................... 48
  Configure domain ................................................................................................... 48
  Define ClearPass as the portal server ..................................................................... 48
  Configure Services VLAN 50 .................................................................................. 48
  Configure URL for the captive portal page on ClearPass ....................................... 49
  Configure VLAN 50 DHCP server and IP pool ....................................................... 49
  Enable Port security .................................................................................................. 49
  Enable controller as DNS server ............................................................................ 49
  Configure a DNS server for the controller to communicate with ......................... 49
  Allow for return traffic to reach its destination ...................................................... 49
  Allow traffic to and from ClearPass server ............................................................. 49
  Allow DNS traffic to DNS server ........................................................................... 49
  Create NAT ACL ...................................................................................................... 49
  Translate guest IP address ....................................................................................... 49
  Do not translate any other source IP address .......................................................... 49
  Configure WLAN ESS ............................................................................................ 49
  Configure Service template ..................................................................................... 50
  Assign service template to AP and radio .................................................................. 50
Verify expected behavior ......................................................................................... 50
FIGURES

Figure 1. Network overview ................................................................. 7
Figure 2. ClearPass Login .................................................................. 14
Figure 3. Add Network Device ............................................................. 15
Figure 4. Add Network Device Details ................................................ 16
Figure 5. Create a new Local User ....................................................... 16
Figure 6. Add Local User .................................................................. 17
Figure 7. Local User Details ............................................................... 17
Figure 8. Configuration Templates ...................................................... 18
Figure 9. Start 802.1X Wireless Template .......................................... 18
Figure 10. 802.1X Service Template - General .................................... 19
Figure 11. 802.1X Service Template - General .................................... 19
Figure 12. 802.1X Service Template - Authentication ......................... 19
Figure 13. 802.1X Service Template - Authentication ......................... 20
Figure 14. 802.1X Service Template – Wireless Network Settings ......... 20
Figure 15. 802.1X Service Template – Enforcement Details ................. 20
Figure 16. 802.1X Service Template – Add Service ............................. 21
Figure 17. 802.1X Service Template – Elements Added ....................... 21
Figure 18. View Policies/Profiles ....................................................... 21
Figure 19. Edit Enforcement Policy .................................................... 22
Figure 20. Edit Enforcement Policy .................................................... 22
Figure 21. Edit Enforcement Policy .................................................... 23
Figure 22. ClearPass Login ............................................................... 25
Figure 23. Add Network Device ........................................................ 26
Figure 24. Add Network Device Details ............................................. 27
Figure 25. Local Users .................................................................... 27
Figure 26. Add Local User ............................................................... 28
Figure 27. Local User Details ............................................................ 28
Figure 28. Add Enforcement Profile .................................................. 29
Figure 29. Enforcement Profile Details .............................................. 29
Figure 30. Add Enforcement Policy .................................................... 30
Figure 31. Enforcement Policy Details .............................................. 30
Figure 32. Enforcement Policy Rules ................................................ 31
Figure 33. Add Service ................................................................... 31
Figure 34. Select Service Type .......................................................... 32
Figure 35. Add Authentication Info .................................................... 32
Figure 36. Select Enforcement Policy ............................................... 33
Figure 37. Create Guest Account ...................................................... 34
Figure 38. Guest Account Details ...................................................... 35
Figure 39. Create Guest Web Login Page .......................................... 35
Figure 40. Create Guest Web Login Page .......................................... 36
Figure 41. Guest Web Login Page Details ........................................ 36
Figure 42. Adjust Pre-Auth Check ..................................................... 37
Figure 43. Adjust Login Delay .......................................................... 37
Figure 44. Policy Manager Dashboard .............................................. 38
Figure 45. Guest Authentication Template ....................................... 38
Figure 46. Guest Authentication Template - General ......................... 39
Figure 47. Guest Authentication Template – Wireless Network Settings .... 39
Figure 48. Guest Authentication Template – MAC Caching Settings ...... 39
Figure 49. Guest Authentication Template – Posture Settings .............. 40
Figure 50. Guest Authentication Template – Access Restrictions ......... 40
Figure 51. Guest Authentication Template Services ............................ 40
Figure 52. MAC Authentication Service ............................................ 41
Figure 53. Enable [Allow All MAC AUTH] ......................................... 41
Figure 54. Disable Service ............................................................... 42
Figure 55. Full Template List ............................................................ 42
Figure 56. Web-based Authentication Template ................................... 43
Figure 57. Web-based Authentication Template - Service .................................................. 43
Figure 58. Web-based Authentication Template - Authentication ..................................... 44
Figure 59. Web-based Authentication Template - Enforcement ....................................... 44
Figure 60. Create Enforcement Policy ........................................................................... 45
Figure 61. Enforcement Policy Details ........................................................................... 45
Figure 62. Web-based Authentication Template - Summary ............................................. 46
Figure 63. Web-based Authentication Template – Enforcement Policy .............................. 46
Figure 64. Web-based Authentication Template - Summary ............................................. 47
Figure 65. Add Authorization ......................................................................................... 47
Figure 66. Add Time Source ......................................................................................... 48
TABLES

Table 1. VLANS........................................................................................................................................8
Table 2. Console Parameters................................................................................................................8
INTRODUCTION
This document describes three different methods of setting a ClearPass instance as the AAA for a UWW controller:

• 802.1x Authentication
• MAC Authentication
• Guest Authentication

While it is assumed that the reader is familiar with HP WLC, the steps depicted below are for a system that is in default factory state. The steps that are specific for setting up the ClearPass configuration are called out later in the document, and if the reader is already familiar with HP WLC’s configuration, the reader may skip ahead to the ClearPass-specific sections.

In this document we will create all 3 scenarios starting with 802.1x authentication and adding to the configuration MAC Authentication and finally Guest/Onboarding authentication.

BACKGROUND INFORMATION
Requirements
• UWW controller and compatible APs
• Controller firmware greater than P37
• External DHCP server
  ○ IP Helper on all relevant VLANs
  ○ Appropriate routes on DHCP server
• ClearPass instance

Network diagram
In this example, the minimum number of devices will be utilized. Note that the WLC and the LAN Switch (LSW) are modules of the HP 830 UWW controller.
**VLANs**

VLAN 1  This is the management and data VLAN. All infrastructure devices have an IP address in this scope. Since the controller and the AP are both on this domain, APs are adopted via L2. To minimize complexity we have elected to use a single VLAN rather than split management/core and traffic into different VLANs.

VLAN 50  This is the Guest/Onboarding VLAN in which un-authenticated devices will be adopted to until they are authenticated and assigned to their appropriate VLAN. The use of VLAN 50 is not needed until Guest authentication scenario is described.

Table 1. VLANS

**SWITCH CONFIGURATION**

**Initial setup**

This document describes configuration of the WLC/LSW from factory default stage where the first step will be to configure a serial connection and setup the management interface.

**Serial connection**

To log-in through the console port, make sure the console terminal has a terminal emulation program. In addition, the port settings of the terminal emulation program must be the same as the default settings of the console port as described in the following table.

<table>
<thead>
<tr>
<th>Bits per second</th>
<th>9600 bps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flow control</td>
<td>None</td>
</tr>
<tr>
<td>Parity</td>
<td>None</td>
</tr>
<tr>
<td>Stop bits</td>
<td>1</td>
</tr>
<tr>
<td>Data bits</td>
<td>8</td>
</tr>
<tr>
<td>Bits per second</td>
<td>9600 bps</td>
</tr>
</tbody>
</table>

Table 2. Console Parameters

**Select country code**

When you first connect, you will be prompted for country/region code. Note that not all APs are compatible with all country/region codes. Care must be taken that all APs connected are compatible with selected country/region. For more information, see section: “Specifying a country/region code” Under WLAN Configuration Guide manual.

Please set your country/region code.
Input? to get the country code list, or input q to log out.
US
Change to LSW CLI
Note that the initial serial connection is to the WLC (Wireless LAN Controller) CLI, not the LSW (LAN Switch) CLI. To access LSW CLI, from User View, connect to slot 0 (zero). (To get to User View, press Ctrl + Z from any context.) To get back from LSW CLI to WLC CLI, press Ctrl + K.

<HP> oap connect slot 0

Disable logging to terminal (optional)
This step is to avoid the multiple debug messages that are sent to serial console. In actuality, there are not a lot of debug messages being displayed. Hence the user may choose to not disable this feature.

<HP> undo terminal monitor

Configure system name (optional)
While this step is optional, it is a good practice to give each device an individual name. In this example, the last three characters are LSW to differentiate it from the WLC. (830_LSW vs. 830_WLC)

<HP> system-view
[HP] sysname 830_LSW

Configure management traffic route to WLC
[830_LSW] oap management-ip 10.0.0.14 slot 1

Configure VLAN 1 IP address
[830_LSW] interface Vlan-interface 1
[830_LSW-Vlan-interface1] ip address 10.0.0.13 255.255.255.0

Configure default gateway
[830_LSW] ip route-static 0.0.0.0 0.0.0.0 10.0.0.254

Enable Telnet and SSH server
[ClearPass_830_WLC] telnet server enable
[ClearPass_830_WLC] ssh server enable

Assign admin user password and enable telnet, SSH and weblogin
[ClearPass_830_WLC] local-user admin
[ClearPass_830_WLC] password simple <Admin Password>
[ClearPass_830_WLC] authorization-attribute level 3
[ClearPass_830_WLC] service-type ssh telnet
[ClearPass_830_WLC] service-type web
[ClearPass_830_WLC] user-interface con 0
[ClearPass_830_WLC] user-interface vty 0 4
[ClearPass_830_WLC] authentication-mode scheme
[ClearPass_830_WLC] user privilege level 3

Save your work
[830_LSW] save
It is now time to return to WLC and configure it. From User View press:

Ctrl+K.

If you are not already in User View, press Ctrl+Z. User View is denoted by angle brackets around the LSW name. i.e., `<830_LSW>

**WLC CONFIGURATION—INITIAL SETUP**

**Disable logging to terminal (optional)**
This step is to avoid the multiple debug messages that are sent to serial console. In actuality, there are not a log of debug messages being displayed. Hence the user may choose to not disable this feature.

::<HP> undo terminal monitor

**Configure system name (optional)**
While this step is optional, it is a good practice to give each device an individual name. In this example, the last three characters are WLC to differentiate it from the LSW. (Bonjour LSW vs. Bonjour WLC)

::<HP> system-view
[HP] sysname ClearPass_830_WLC

**Configure management traffic route to switch**
[ClearPass_830_WLC] oap management-ip 10.10.0.13 slot 0

**Configure management VLAN 1**
VLAN 1 is our management VLAN. It is used to communicate with all devices, including APs.

[ClearPass_830_WLC] vlan 1
[ClearPass_830_WLC-vlan1] description Management VLAN
[ClearPass_830_WLC-vlan1] quit
[ClearPass_830_WLC] interface Vlan-interface 1
[ClearPass_830_WLC-Vlan-interface1] ip address 10.0.0.14 255.255.255.0
[ClearPass_830_WLC-Vlan-interface1] quit

**Configure default gateway**
[ClearPass_830_WLC] ip route-static 0.0.0.0 0.0.0.0 10.0.0.254 permanent

**Enable Telnet and SSH server**
[ClearPass_830_WLC] telnet server enable
[ClearPass_830_WLC] ssh server enable

**Assign admin user password and enable telnet, SSH and weblogin**
[ClearPass_830_WLC] local-user admin
[ClearPass_830_WLC] password simple <Admin Password>
[ClearPass_830_WLC] authorization-attribute level 3
[ClearPass_830_WLC] service-type ssh telnet
[ClearPass_830_WLC] service-type web
[ClearPass_830_WLC] user-interface con 0
[ClearPass_830_WLC] user-interface vty 0 4
[ClearPass_830_WLC] authentication-mode scheme
[ClearPass_830_WLC] user privilege level 3
WLC CONFIGURATION—AP

Note that an AP Template will not be used to adopt the AP. A different approach will be used here since only one AP will be adopted. In this document, the AP will be adopted by auto-AP method.

Enable auto-AP discovery & Configuration

[ClearPass_830_WLC] wlan auto-ap enable

Verify adopted AP(s)

Validate AP adoption and connectivity to the WLC.

[ClearPass_830_WLC] display wlan ap all

Do you see the APs adopted? If not, wait a few more minutes and repeat command. Eventually, you should see your AP in the list. If you do not, verify that the AP has an IP address and that it can reach the WLC. Take note of the “AP Name” as you will need it a few steps later.

Disable auto-AP discovery (optional)

After AP has been adopted, disable auto-AP. If you do not perform this step and other APs come online, they may be adopted by this WLC. For security reasons, it is recommended that auto-AP be disabled.

[ClearPass_830_WLC] undo wlan auto-ap enable

Rename AP and make persistent

In order to modify AP settings, the AP must be made persistent.

[ClearPass_830_WLC] wlan auto-persistent enable

Save your work

[ClearPass_830_WLC] save

Check network connectivity to all network elements.

At this point, you should be able to reach both the LSW and WLC with a browser. If you don't have connectivity, stop and verify all steps above. Start by pinging the LSW IP address from the WLC side.

ping 10.0.0.13

Try pinging DGW IP address from the WLC side.

ping 10.0.0.254

Try pinging ClearPass IP address from the WLC side.

ping 10.0.0.22

802.1X AUTHENTICATION

WLC configuration

The basic 802.1x authentications calls for an AAA server which is connected to a user/password DB. In our case the AAA server is ClearPass and the DB will be a ClearPass internal DB that will hold the users repository. We start by configuring the
WLC to use ClearPass as the AAA server and associate a SSID to the AAA for authentication.

Enable Port security

```
[ClearPass_830_WLC] port-security enable
```

Define authentication method

```
[ClearPass_830_WLC] dot1x authentication-method eap
```

Configure RADIUS scheme

Here we create a RADIUS scheme named cppm01 where we declare the ClearPass server as the primary authentication and accounting server (IP 10.0.0.22).

```
[ClearPass_830_WLC] radius scheme cppm01
[ClearPass_830_WLC-radius-cppm01] primary authentication 10.0.0.22 key simple <authentication key>
[ClearPass_830_WLC-radius-cppm01] primary accounting 10.0.0.22 key simple <Authentication key>
[ClearPass_830_WLC-radius-cppm01] user-name-format without-domain
[ClearPass_830_WLC-radius-cppm01] quit
```

Configure domain

Here we create a domain (Named cppm) which is binding the RADIUS scheme (cppm01) which we created earlier.

```
[ClearPass_830_WLC] domain cppm
[ClearPass_830_WLC-isp-cppm] authentication default radius-scheme cppm01
[ClearPass_830_WLC-isp-cppm] authorization default radius-scheme cppm01
[ClearPass_830_WLC-isp-cppm] access-limit disable
[ClearPass_830_WLC-isp-cppm] state active
[ClearPass_830_WLC-isp-cppm] idle-cut disable
[ClearPass_830_WLC-isp-cppm] self-service-url disable
[ClearPass_830_WLC-isp-cppm] quit
```

Configure WLAN ESS

```
[ClearPass_830_WLC] interface WLAN-ESS 1
[ClearPass_830_WLC-WLAN-ESS1] description hpn-dot1x
[ClearPass_830_WLC-WLAN-ESS1] port link-type hybrid
[ClearPass_830_WLC-WLAN-ESS1] port hybrid vlan 1 untagged
[ClearPass_830_WLC-WLAN-ESS1] mac-vlan enable
[ClearPass_830_WLC-WLAN-ESS1] qos trust dscp
[ClearPass_830_WLC-WLAN-ESS1] port-security port-mode userlogin-secure-ext
[ClearPass_830_WLC-WLAN-ESS1] port-security tx-key-type 11key
[ClearPass_830_WLC-WLAN-ESS1] undo dot1x handshake
[ClearPass_830_WLC-WLAN-ESS1] dot1x mandatory-domain cppm
[ClearPass_830_WLC-WLAN-ESS1] undo dot1x multicast-trigger
[ClearPass_830_WLC-WLAN-ESS1] quit
[ClearPass_830_WLC-WLAN-ESS1] wlan service-template 1 crypto
[ClearPass_830_WLC-WLAN-ESS1] wlan service-template 1 description hpn-dot1x
[ClearPass_830_WLC-WLAN-ESS1] ssid hpn-dot1x
[ClearPass_830_WLC-WLAN-ESS1] ip verify source
[ClearPass_830_WLC-WLAN-ESS1] bind WLAN-ESS 1
cipher-suite ccmp
[ClearPass_830_WLC-WLAN-ESS1] security-ie rsn
[ClearPass_830_WLC-WLAN-ESS1] multicast optimization enable
[ClearPass_830_WLC-WLAN-ESS1] service-template enable
[ClearPass_830_WLC-WLAN-ESS1] quit
[ClearPass_830_WLC-WLAN-ESS1] quit
[ClearPass_830_WLC] interface WLAN-ESS 1
[ClearPass_830_WLC-WLAN-ESS1] description hpn-dot1x
[ClearPass_830_WLC-WLAN-ESS1] port link-type hybrid
```
Configure ClearPass

This document is written under the assumption the reader has already installed, commissioned and licensed an Aruba ClearPass server.

Log in

Open a browser and enter https://<IP>/tips using the IP address of the Aruba ClearPass server. Enter credentials for the admin user.
Add controller as device on ClearPass

Go to Configuration > Network > Devices tab and click on "Add" to create a new device.
Enter the Controller information making sure the RADIUS shared key matches the shared key configured on the RADIUS scheme cppm01 on the controller. By doing so we are indicating that the controller which has ClearPass as its Authenticating and Accounting entity be recognized as a device which is authorized to interact with ClearPass for RADIUS messages.
Click on Save and close the screen. The controller should show on the ClearPass server as a network device.

Create a new user on ClearPass internal DB.
Under Identity select Local Users.

Figure 5. Create a new Local User
Click on Add, to create a new local user.

![Add Local User](image)

Figure 6. Add Local User

Enter User ID, Name, Password and enable the user, assign a “Role” as [Employee]. We will use bob and password as the user and password information.

![Edit Local User](image)

Figure 7. Local User Details
Create a new Service.

After creating a local user and configuring the controller as an authorized device on ClearPass we are now reaching the stage where we configure the actual service which in turn defines how and what type of service will be assigned to the user.

As in many cases with ClearPass, there are multiple ways to go about creating a service. You can create each element that comprise the service manually and bind them all to a service at the end, or you can use a template (wizard) to help you create the elements and manipulate their values later.

In this document we will use the wizard.

Under Configuration click “Start Here”

**Figure 8. Configuration Templates**

Select 802.1X Wireless

**Figure 9. Start 802.1X Wireless Template**

Enter a Prefix that will represent the type of service we are creating
Click on “Next”.

From the authentication source select [Local User Repository] for the system to use the internal DB where we have previously created users.

Click on “Next”
Figure 13. 802.1X Service Template - Authentication
Select the UWW controller that was previously configured

Figure 14. 802.1X Service Template – Wireless Network Settings
Skip Posture Setting Tab and select Enforcement Details. Assign the VLAN ID in which traffic would be assigned to in case Authentication is successful and assign the Default VLAN in which traffic will be assigned in case the default service will be used (Authentication failed and some level of access is still granted). In our case we are using the same VLAN as it is just for demo purposes.

Figure 15. 802.1X Service Template – Enforcement Details
Click on “Add Service”.
Next what we will see is that 2 enforcement profiles, 1 enforcement policy, and 1 service were added.

To view each of the created profiles, policies and service we will select Policies, Profiles or Services from the left side menu.

After the creation of the policy we need to edit it in-order to align the manner in which it operates with our needs. The profiles describe the actions that will take place and we can have multiple profiles that detail different actions (a profile for each day of the week, a profile for authentication failure and so on). The profiles are then bound to a policy.
The wizard we used above creates by default 2 profiles (default profile and a regular profile) these profile are identical by default and can be edited.

We will look at how they are bound to the Policy and manipulate the rules assigned to them.

Select Policies from the left panel and choose the policy created earlier.

Figure 19. Edit Enforcement Policy

We can leave the Summary and Enforcement tabs as is and open the Rules Tab. Here we will create a rule that will be applied for all days of the week. The Type will be date, Name: Day-of-Week, operator will be BELONGS_TO and under values we will select the entire week.

Figure 20. Edit Enforcement Policy

Save the rule and the Policy
Figure 21: Edit Enforcement Policy

At this point the policy is ready and you can connect to the SSID using the credentials created for the above user.

**Verify expected behavior**

We are now ready to verify if it is possible to authenticate a user that was created on the internal Clear Pass DB via the hpn-dot1x SSID. At this point, the AP should be beaconing hpn-dot1x SSIDs. Verify this is the case before proceeding. If SSID is not being broadcasted, verify steps above. If hpn-dot1x SSID is seen try to connect to it using the credentials of the user created above: “bob, password”. And check that you are able to connect.

**Conclusion**

WLC is now configured to use ClearPass as the AAA server and ClearPass is configured to identify the WLC as a legitimate entity; ClearPass is also configured to hold the DB of users and passwords and direct the WLC on which VLAN the users should be assigned after authentication.

**MAC AUTHENTICATION**

**WLC configuration**

The use of MAC authentication is mostly used when there are “dumb” devices on the network that can not authenticated using more advanced technologies – such as 802.1X (i.e., Scanner, printers and other legacy devices).

There are no changes in the LWS configuration compared to the configuration described above therefore we will detail only the configuration of the WLC. This scenario will demonstrate how the functionality and authentication sources might be different than the local DB on ClearPass.

Enable Port security

```
[ClearPass_830_WLC] port-security enable
```

Configure RADIUS scheme

Here we create a radius scheme named cppm01 were we declare the ClearPass server as the primary authentication and accounting server (IP 10.0.0.22).

```
[ClearPass_830_WLC] radius scheme cppm01
[ClearPass_830_WLC-radius-cppm01] primary authentication 10.0.0.22 key simple <authentication key>
[ClearPass_830_WLC-radius-cppm01] primary accounting 10.0.0.22 key simple <Authentication key>
[ClearPass_830_WLC-radius-cppm01] user-name-format without-domain
[ClearPass_830_WLC-radius-cppm01] quit
```
Configure domain

Here we create a domain (Named cppm) which is binding the radius scheme (cppm01) which we created earlier.

```
[ClearPass_830_WLC] domain cppm
[ClearPass_830_WLC-isp-cppm] authentication default radius-scheme cppm01
[ClearPass_830_WLC-isp-cppm] authorization default radius-scheme cppm01
[ClearPass_830_WLC-isp-cppm] accounting default radius-scheme cppm01
[ClearPass_830_WLC-isp-cppm] access-limit disable
[ClearPass_830_WLC-isp-cppm] state active
[ClearPass_830_WLC-isp-cppm] idle-cut disable
[ClearPass_830_WLC-isp-cppm] self-service-url disable
[ClearPass_830_WLC-isp-cppm] quit
```

Configure WLAN ESS

```
[ClearPass_830_WLC] interface WLAN-ESS 2
[ClearPass_830_WLC-WLAN-ESS2] port link-type hybrid
[ClearPass_830_WLC-WLAN-ESS2] port hybrid vlan 1 untagged
[ClearPass_830_WLC-WLAN-ESS2] mac-vlan enable
[ClearPass_830_WLC-WLAN-ESS2] mac-authentication domain cppm
[ClearPass_830_WLC-WLAN-ESS2] quit
```

Configure Service template

```
[ClearPass_830_WLC] wlan service-template 2 clear
[ClearPass_830_WLC-wlan-st-1] description ClearPass MAC Auth
[ClearPass_830_WLC-wlan-st-1] ssid hpnMACAuth
[ClearPass_830_WLC-wlan-st-1] ip verify source
[ClearPass_830_WLC-wlan-st-1] bind WLAN-ESS 2
[ClearPass_830_WLC-wlan-st-1] service-template enable
[ClearPass_830_WLC-wlan-st-1] quit
```

Assign Service template to AP

```
[ClearPass_830_WLC] wlan ap <AP Name>
[ClearPass_830_WLC-wlan-ap-7848-5942-bdc0] radio 1
[ClearPass_830_WLC-wlan-ap-7848-5942-bdc0] service-template 2
[ClearPass_830_WLC-wlan-ap-7848-5942-bdc0] radio enable
[ClearPass_830_WLC-wlan-ap-7848-5942-bdc0] radio 2
[ClearPass_830_WLC-wlan-ap-7848-5942-bdc0] service-template 2
[ClearPass_830_WLC-wlan-ap-7848-5942-bdc0] radio enable
[ClearPass_830_WLC-wlan-ap-7848-5942-bdc0] quit
```

Save your work

```
[ClearPass_830_WLC] save
```

Reset the AP

Reset the AP so that all changes get applied.

**Configure ClearPass**

This document is written under the assumption the reader has already installed, commissioned and licensed an Aruba ClearPass server.

Log in

Open a browser and enter `https://<IP>/tips` using the IP address of the Aruba ClearPass server. Enter credentials for the admin user.
Add controller as device on ClearPass

Go to Configuration > Network > Devices tab and click on “Add” to create a new device.
Enter the Controller information making sure the RADIUS shared key matches the shared key configured on the RADIUS scheme cppm01 on the controller. By doing so we are indicating that the controller which has ClearPass as its Authenticating and Accounting entity be recognized as a device which is authorized to interact with ClearPass for RADIUS messages.
Figure 24. Add Network Device Details

Click on Save and close the screen. The controller should show on the ClearPass server as a network device.

Create a new user (MAC Address) on ClearPass internal DB.

Under Identity select Local Users.

Figure 25. Local Users
Click on “Add”, to create a new local user.

Figure 26. Add Local User

Enter device MAC address all in lower-case and no spaces on the following fields: User ID, Name and Password. **Enable** the user, assign a “Role” as “other”.

Figure 27. Local User Details

Create a new Enforcement Profile

This time we are creating each profile element manually rather than with the wizard. The Profile will describe the “Action”, in our case “Accept”, – accepting the device into the network. From the profiles option on the left menu click on add and select template to be VLAN Enforcement. The idea here is to assign the printer once authenticated to the printers VLAN. Add a name and description. And select “Accept” as the action.
Figure 28. Add Enforcement Profile
On the Attributes tab the fifth line “Tunnel-Private-Group-Id set the value to match the Printers VLAN on your network (in our case its going to be VLAN 1

Figure 29. Enforcement Profile Details
Save the Profile.
Create a new Enforcement Policy
On the left side menu select Policies and click on Add to create a new policy.
Figure 30. Add Enforcement Policy

The Policy is where we match Conditions to actions (Profiles). Here we will create a condition that matches the days of the week – basically, this condition will always be matched as no matter at what time a device will try to connect it will always be one of the days in the week... the default profile (which will take control if the described condition will not be matched) will be to deny access. Assign a name, description and select Deny Access Profile under the default profile.

Figure 31. Enforcement Policy Details

Under the Rules Tab, we will create the condition we described above. Set Type to be Date, Name- Day-of-Week, Operator-BELONGS_TO and under value select ALL days of the week. For Profile name select the profile created in the previous step.
Figure 32. Enforcement Policy Rules

Save the rule and Policy.

Create a new Service

Next will be creating the services that will incorporate the profile and policy. From the left panel select Services, and click on Add.

Figure 33. Add Service

From the service type select MAC Authentication.
Figure 34. Select Service Type

On the Authentication Tab set the Authentication Method to [MAC AUTH], change the Authentication Sources [Local User Repository] [Local SQL DB].

Figure 35. Add Authentication Info

Under the Enforcement Tab /enforcement Policy select the Policy created above.
Save the Service and exit.

At this point ClearPass is configured to authenticate a new device coming from the specific SSID based on the internal DB of MAC addresses preconfigured in its repository.

**Verify expected behavior**

We are now ready to verify if it is possible to authenticate a user that was created on the internal ClearPass DB via the hpnMACAuth SSID. At this point, the AP should be beaocing hpnMACAuth SSIDs. Verify this is the case before proceeding. If SSID is not being broadcasted, verify steps above. If hpnMACAuth SSID is seen, try to connect to it using the device with the MAC address entered into the local DB. Check that you are able to connect.

**Conclusion**

WLC is now configured to use ClearPass as the AAA server and ClearPass is configured to identify the WLC as a legitimate entity. ClearPass is also configured to hold the DB MAC addresses and direct the WLC on which VLAN the Printer should be assigned after authentication.

**GUEST ACCESS WITH MAC CACHING**

Guest access is for those people who are not a regular part of the organization but need some level of network access. Since these people are not regular users and are not stored as users in the company DB, a guest user account should be created for them. Once authenticated these individuals will, in most cases, be granted only limited access such as the ability to access the internet.

When a Guest connects to the guest SSID for the first time, they are placed in a segregated VLAN (50 in the example below), which is blocked by a captive portal page. This segregated VLAN exists only on the controller and does not exist anywhere else on the network nor is there a way to reach it from any other segment of the network.

The Guest will authenticate via the captive portal page. Upon successful authentication, their MAC address will be cached in the local repository on ClearPass and a “session termination” Change of Authorization (CoA) will be initiated which will disconnect the Guest user’s device. The user’s device will automatically try to reconnect and authenticate. This time ClearPass will recognize the MAC address is already stored in the local repository and grant access – only this time it will not be assigned to VLAN 50 but to the authenticated VLAN.

In this scenario will will start with the configuration of ClearPass as we will need the URL of the captive portal to be
configured on the controller.

**Configure ClearPass**

This document is written under the assumption the reader has already installed, commissioned and licensed an Aruba ClearPass server.

Before configuring ClearPass, it’s important to understand the Guest workflow when working with Unified. It looks like this:

1. Guest user connects to Guest SSID
2. Guest user’s device attempts to MAC-auth
3. If MAC address has been cached due to a previously successful web-based authentication by the user, the device will be authenticated and assigned to the authenticated VLAN
4. If the MAC address is unknown or the cache has expired, the Guest will be assigned to the Captive Portal VLAN
5. Guest user opens a browser and is redirected to the captive portal page hosted on ClearPass
6. Guest user enters their guest username/password
7. If the authentication is successful, the device information is cached and the user’s session is terminated forcing a new authentication (step 2)
8. If the authentication is unsuccessful, the user’s session is terminated forcing a new authentication (step 2)

**Log In to Guest Manager**

Open a browser and enter the IP address of the Aruba ClearPass server and add /guest (https://<IP>/guest). Enter credentials for the admin user.

**Create Guest User Account**

We will start by creating a Guest user, select Create Account from the left side menu

![Create Guest Account](image)

**Figure 37. Create Guest Account**

Fill in the required information, making sure you check the box for accepting terms and conditions and click on Create. Make note of the Password – you will need it later.
Create Guest Web Login Page

Next we need to create the Guest web login page for the captive portal. Under Configuration select Web Logins.

Click on Create a new web login page
Figure 40. Create Guest Web Login Page

Enter a Name and a Page Name. Make note of the URL that is shown (written in blue in the Page name section). We will use that URL later when we configure the captive portal on the controller. You must also change the Login Method to Server Initiated as the default option is not supported by the controller.

Figure 41. Guest Web Login Page Details

Change the Pre-Auth Check to None.
Figure 42. Adjust Pre-Auth Check

Change the Login Delay from its default of 60 to 15 seconds. We might adjust this value to an even smaller number later on, but for testing set it to 15 seconds. We need to allow enough time for the CoA to be sent, processed by the controller, and for the client to get a new IP address.

Figure 43. Adjust Login Delay

Save and exit.

Log In to Policy Manager

Now we will go back to the Policy Manager module to complete the ClearPass configuration (open a new Tab and enter https://<IP>/tips).
Run Guest Authentication with MAC Caching Service Template

We will be creating multiple services and enforcement policies/profiles. We will use the Service Templates for the majority of the work, but will need to make some adjustments to the elements created by the templates. The first step is to use the Guest Authentication with MAC Caching template to create our initial set of configuration. Go to Configuration > Start Here and click Guest Authentication with MAC Caching.

Assign a Name Prefix to the template and click on Next
Figure 46. Guest Authentication Template - General
Populate the mandatory fields and click Next

Figure 47. Guest Authentication Template – Wireless Network Settings
Select a Caching time for each role and click on Next. These can be left at their default values if you choose.

Figure 48. Guest Authentication Template – MAC Caching Settings
Since we are not using any of the parameters for Posture settings leave it as it is.
Figure 49. Guest Authentication Template – Posture Settings

For Access Restrictions select Enforcement Type to be VLAN Enforcement - as we would like to segregate Guest users to an isolated VLAN until they authenticate (in our case it would be VLAN 50) and click on Add Service.

Figure 50. Guest Authentication Template – Access Restrictions

This will result in adding the following:

- 8 Enforcement profiles
- 2 Enforcement Policies
- 2 Role mapping Policies
- 2 Services

Figure 51. Guest Authentication Template Services
Edit MAC Authentication Service

You need to edit the MAC Authentication RADIUS service to allow all MAC authentications. By default, only MAC addresses that are recognized will be authenticated. However, in order to handle unknown devices (ones that haven't been seen before) and to put them in the captive portal VLAN, you must permit those devices to successfully MAC authenticate. To make this change, navigate to Configuration > Services and click on the MAC Authentication service you just created via the service template.

![Figure 52. MAC Authentication Service](image)

Click on the Authentication tab. Note that only [MAC AUTH] is enabled as an Authentication Method. Select [Allow All MAC AUTH] from the pull-down menu. Then click on [MAC AUTH] and click Remove to remove the prior authentication method. When you’re done it should look like this. Click Save when done.

![Figure 53. Enable [Allow All MAC AUTH]](image)

Disable Unneeded Service

Next we need to disable the User Authentication with MAC Caching service that was created by the template. The reason for disabling this service is that we’re going to rely on a different authentication method for Guest users. Remember from the Web Login page, we set the Login Method to Server Initiated. This means that the server (ClearPass) will be initiating the CoA, instead of having the user post a web form to the controller which would then do a RADIUS auth to ClearPass. Because of this change in workflow, we need to disable the RADIUS service and will instead create a Web Auth service that the Guest user will use to authenticate. The creation of the replacement service is described starting in the next step. Click on the green dot next to the service to disable it.
Figure 54. Disable Service

Run Web-based Authentication Service Template
Go to Configuration > Start Here, then click the link to open the full wizard list.

Figure 55. Full Template List
From the full list of templates select Web-based Authentication.
Start by assigning a Name to the Service

For the Authentication source select [Guest User Repository] to allow the system to find and authenticate with the Guest user we created initially.
Since we are not dealing with Roles in this scenario we can skip that tab and head to Enforcement. By default, there will be some existing Enforcement Policy shown – you can ignore this one. We will be creating a new Enforcement Policy using Enforcement Profiles created by the previous template. Click Add New Enforcement Policy.

Enter a Name and select [HP – Terminate Session] as the Default Profile. Click Next.
Figure 60. Create Enforcement Policy
Click Add Rule. In the Rules Editor, create a Rule for every day of the week using the following Enforcement Profiles:

- MAC Caching Bandwidth Limit
- MAC Caching Session Limit
- MAC Caching Do Expire
- MAC Caching Expire Post Login
- Guest MAC Caching
- [Update Endpoint Known]
- [HP - Terminate Session]

Figure 61. Enforcement Policy Details
Click Save, then Next.
Click Save again to save the Policy. When back in the Template, select the Policy you just created.

Click Save to exit the Template.
Modify Web Authentication Service

We need to make one final adjustment to the Service we just created. Go to Configuration > Services and click on the service we just created (UWW Guest Web Authentication). We need to add [Time Source] as an Authorization source so that the Guest user’s device can be updated with the appropriate expiration time. Within the service, click the Service tab and then click Authorization to expose the Authorization tab.

Next click on the Authorization tab and select [Time Source] from the Additional Authorizations Sources pull-down menu. Click Save and the service is ready for use.
This concludes the configuration portion on ClearPass and we will now move to configuring the controller.

**Configure WLC**

Configure RADIUS scheme

Here we create a radius scheme named cppm01 where we declare the ClearPass server as the primary authentication and accounting server (IP 10.0.0.22).

```plaintext
<ClearPass_830_WLC> system-view
[ClearPass_830_WLC] radius scheme cppm01
[ClearPass_830_WLC-radius-cppm01] primary authentication 10.0.0.22 key simple <authentication key>
[ClearPass_830_WLC-radius-cppm01] primary accounting 10.0.0.22 key simple <Authentication key>
[ClearPass_830_WLC-radius-cppm01] user-name-format without-domain
[ClearPass_830_WLC-radius-cppm01] quit
```

Configure domain

Here we create a domain (Named cppm) which is binding the radius scheme (cppm01) which we created earlier.

```plaintext
[ClearPass_830_WLC] domain cppm
[ClearPass_830_WLC-isp-cppm] authentication default radius-scheme cppm01
[ClearPass_830_WLC-isp-cppm] authorization default radius-scheme cppm01
[ClearPass_830_WLC-isp-cppm] accounting default radius-scheme cppm01
[ClearPass_830_WLC-isp-cppm] access-limit disable
[ClearPass_830_WLC-isp-cppm] idle-cut disable
[ClearPass_830_WLC-isp-cppm] self-service-url disable
[ClearPass_830_WLC-isp-cppm] quit
```

Define ClearPass as the portal server

```plaintext
[ClearPass_830_WLC] portal server CPPM01 ip 10.0.0.22 server-type noc
```

Configure Services VLAN 50

VLAN 50 is used for unauthenticated users in conjunction with the Guest scenario. This VLAN does **not** need to be configured on any other part of the network and is used solely on the WLC side.

```plaintext
[ClearPass_830_WLC] vlan 50
```
Configure VLAN 50 DHCP server and IP pool
Since VLAN 50 is only used internally on the WLC we need to configure the DHCP server that will allocate IP addresses to the connecting clients.

```bash
[ClearPass_830_WLC] dhcp enable
[ClearPass_830_WLC] dhcp server ip-pool vlan_50
[ClearPass_830_WLC-dhcp-pool-vlan_50] network 192.168.50.0 mask 255.255.255.0
[ClearPass_830_WLC-dhcp-pool-vlan_50] network ip range 192.168.50.100 192.168.50.150
[ClearPass_830_WLC-dhcp-pool-vlan_50] gateway-list 192.168.50.1
[ClearPass_830_WLC-dhcp-pool-vlan_50] dns-list 192.168.50.1
[ClearPass_830_WLC-dhcp-pool-vlan_50] quit
[ClearPass_830_WLC-Vlan-Vlan-interface50] ip address 192.168.50.1 255.255.255.0
[ClearPass_830_WLC-Vlan-Vlan-interface50] quit

[ClearPass_830_WLC-Vlan-Vlan-interface50] description Guest VLAN
[ClearPass_830_WLC-Vlan-Vlan-interface50] portal server CPPM01 method layer3
[ClearPass_830_WLC-Vlan-Vlan-interface50] portal domain cppm

Configure URL for the captive portal page on ClearPass
https://10.0.0.22/guest/uww_guest.php?nasid=%n&nasip=%a&loginport=%p&ipaddress=%c&mac=%m&original_url=%o

Configure VLAN 50 DHCP server and IP pool
Since VLAN 50 is only used internally on the WLC we need to configure the DHCP server that will allocate IP addresses to the connecting clients.

Enable Port security
[ClearPass_830_WLC] port-security enable

Enable controller as DNS server
[ClearPass_830_WLC] dns proxy enable

Configure a DNS server for the controller to communicate with
[ClearPass_830_WLC] dns server 15.234.147.195

Allow for return traffic to reach its destination
By default, when the captive portal is enabled, all traffic is blocked. Need to create some portal free rules to allow the traffic.

[ClearPass_830_WLC] portal free-rule 1 source interface Bridge-Aggregation1 destination any
[ClearPass_830_WLC] portal free-rule 2 source ip any destination ip 10.0.0.22 mask 255.255.255.255
[ClearPass_830_WLC] portal free-rule 3 source ip any destination ip 15.234.147.195 mask 255.255.255.255 udp 53

Create NAT ACL
[ClearPass_830_WLC] acl number 2001 name NAT_Source_Vlan_50

Translate guest IP address
[ClearPass_830_WLC-acl-basic-2001-NAT_Source_Vlan_50] rule 0 permit source 192.168.50.0 0.0.0.255

Do not translate any other source IP address
[ClearPass_830_WLC-acl-basic-2001-NAT_Source_Vlan_50] rule 5 deny
[ClearPass_830_WLC-acl-basic-2001-NAT_Source_Vlan_50] quit

Configure WLAN ESS
[ClearPass_830_WLC] interface WLAN-ESS3
[ClearPass_830_WLC-WLAN-ESS3] description Guest with MAC Caching
Configure Service template
[ClearPass_830_WLC-wlan-service-template 3 clear
[ClearPass_830_WLC-wlan-st-3] description Guest with MAC Caching
[ClearPass_830_WLC-wlan-st-3] ssid hpnGuestMac
[ClearPass_830_WLC-wlan-st-3] bind WLAN-ESS 3
[ClearPass_830_WLC-wlan-st-3] service-template enable
[ClearPass_830_WLC] quit

Assign service template to AP and radio
[ClearPass_830_WLC-wlan-ap 7848-5942-bdc0 model 425-AM id 3
[ClearPass_830_WLC-wlan-ap-7848-5942-bdc0] serial-id CN46G660M8
[ClearPass_830_WLC-wlan-ap-7848-5942-bdc0] radio 1
[ClearPass_830_WLC-wlan-ap-7848-5942-bdc0-radio-1] service-template 3
[ClearPass_830_WLC-wlan-ap-7848-5942-bdc0-radio-1] radio enable
[ClearPass_830_WLC-wlan-ap-7848-5942-bdc0-radio-1] radio 2
[ClearPass_830_WLC-wlan-ap-7848-5942-bdc0-radio-2] radio enable
[ClearPass_830_WLC-wlan-ap-7848-5942-bdc0-radio-2] quit

Verify expected behavior
We are now ready to verify if it is possible to authenticate a guest.
• Connect a client to hpnGuestMac SSID
• And open a browser
• You should now be directed to the captive portal
• Check your IP address and validate it belongs to VLAN 50 (192.168.x.x)
• Try pinging any public URL (www.google.com) verify it is not possible.
• Authenticate using the credentials allocated for the guest user
• Check your IP address and validate it is part of VLAN 1
• Try browsing to a public URL. You should now be able to access the Internet.