Cisco-SW redirect Web Authen and use MAC Caching

Switch	Ports	Model	SW Version	SW Image
* 1	28	WS-C2960S-24TS-L	15.0(2)SE8	C2960S-UNIVERSALK9-M

CISCO-SW CLI

```
 radius-server host 192.100.10.62 key 123456
 aaa new-model
 aaa authorization network default group radius
 aaa accounting update periodic 1


 aaa server radius dynamic-author
 client 192.100.10.62 server-key 123456
 port 3799
 auth-type all
 exit

 ip device tracking
 ip http server
 radius-server vsa send authentication


 ip access-list extended redir-acl
  deny udp host 0.0.0.0 host 255.255.255.255 eq bootps
  deny tcp any host 192.100.10.62
  permit tcp any any

interface gi1/0/1
 switchport access vlan 1
 switchport mode access
 mab
 authentication port-control auto
```

Clearpass Setup

1)

2 Services

1. MAC Authentication
2. Web Login – Web Auth

MAC Authentication Service

→ RADIUS Accept with URL-Redirect Attribute
(http://(Clearpass-IP)/guest/(page-name).php)

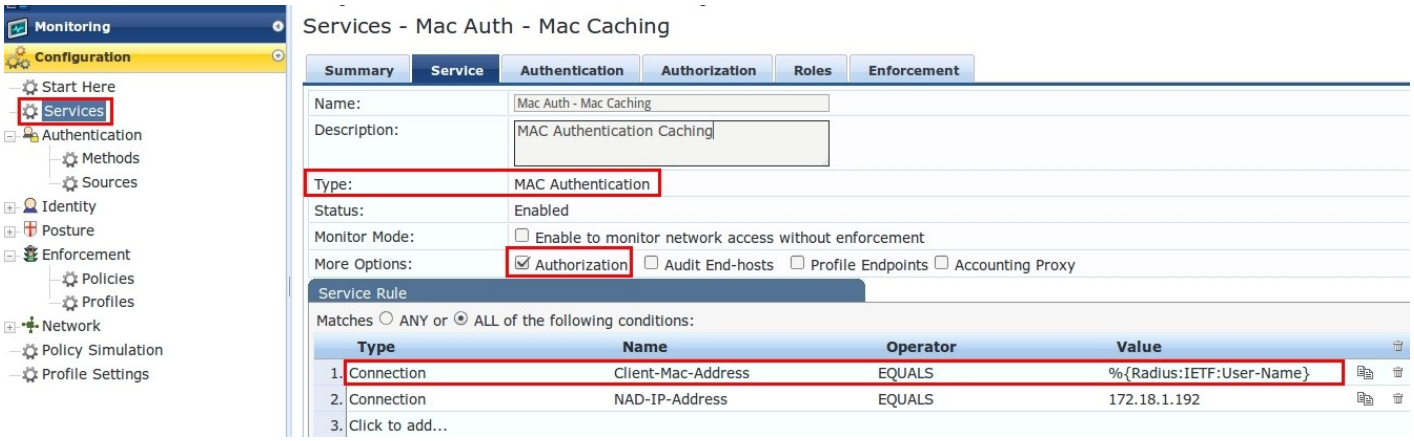
Web Login – Web Auth Service

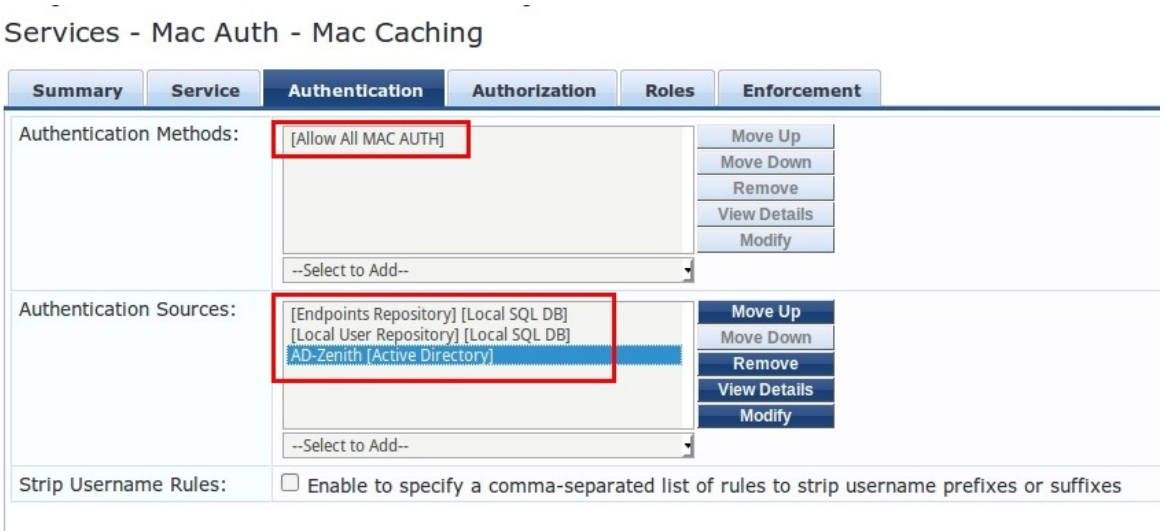
→ RADIUS CoA Terminate Session

MAC Authentication Service

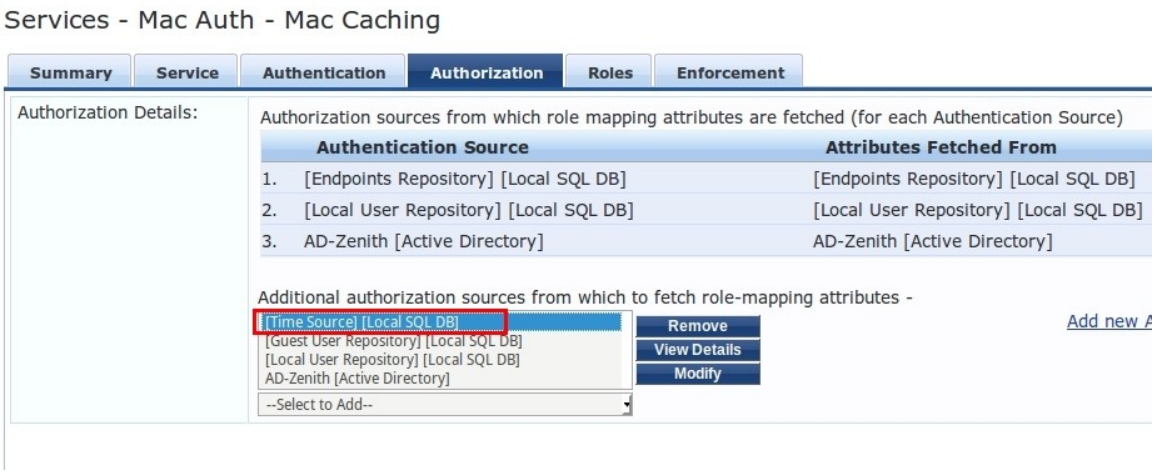
→ RADIUS Accept. Full Access.

Create Service for MAC Authen

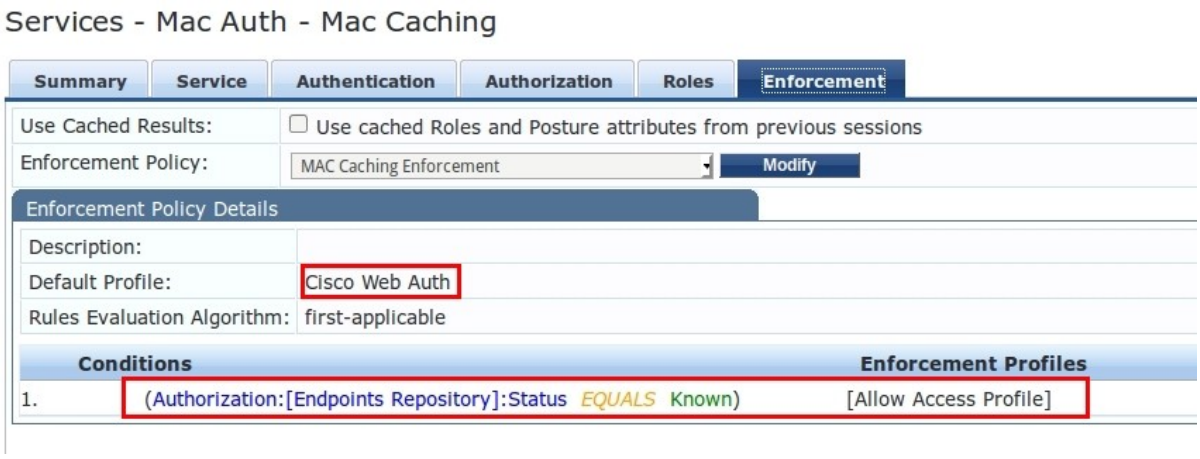




- need [Allow All MAC Auth]
- Endpoints Repository needs for check MAC Caching [Endpoint know or unknow]



- Time Source needs for check expire of endpoint (MAC Caching)



- Endpoint status = Known means this endpoint (MAC) already success to login with Web Authen
- Cisco Web Auth for whole client not yet login with Web Authen , see figure as below

Enforcement Profiles - Cisco Web Auth

Summary | Profile | Attributes

Profile:

Name:	Cisco Web Auth
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Radius:Cisco	Cisco-AVPair	=	url-redirect-acl=redir-acl
2.	Radius:Cisco	Cisco-AVPair	=	url-redirect=http://192.100.10.62/guest/login.php?mac=%{Connection:Client-Mac-Address-Colon}

url-redirect-acl=redir-acl (follow ACL of SW)
url-redirect=http://192.100.10.62/guest/login.php?mac=%{Connection:Client-Mac-Address-Colon}

2) Create Service for Web Authen to Enforce Endpoint to known

Services - Web Auth - User login

Summary | Service | Authentication | Roles | Enforcement

Name:	Web Auth - User login
Description:	
Type:	Web-based Authentication
Status:	Enabled
Monitor Mode:	Enable to monitor network access without enforcement
More Options:	Authorization Posture Compliance

Service Rule

Matches ANY or ALL of the following conditions:

	Type	Name	Operator	Value
1.	Click to add...			

- Select Type = Web-based Authentication
Because this service for client login Captive-portal direct with Clearpass (not login with SW)

Services - Web Auth - User login

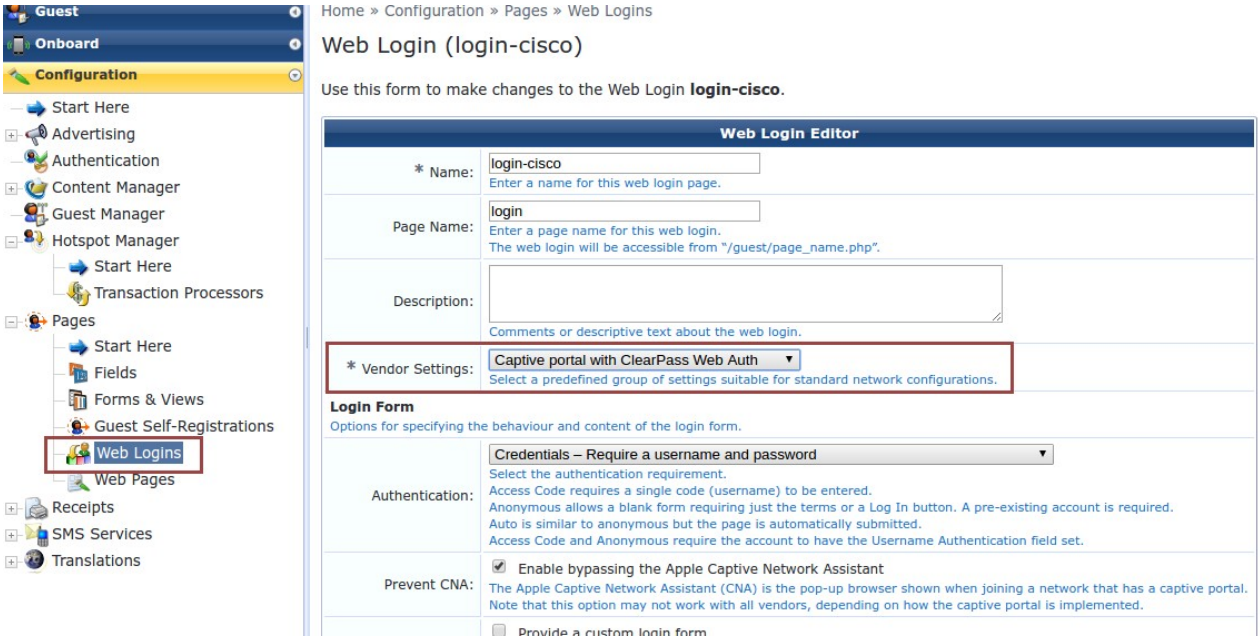
Summary | Service | Authentication | Roles | Enforcement

Authentication Sources:	AD-Zenith [Active Directory] [Guest User Repository] [Local SQL DB] [Local User Repository] [Local SQL DB] --Select to Add--
Strip Username Rules:	Enable to specify a comma-separated list of rules to strip use

Move Up | Move Down | Remove | View Details | Modify

- [Update Endpoint Known] = Enforce CPPM keep MAC to Endpoint Known
- [Cisco – Terminate session] = terminate client to re-authen with MAC again

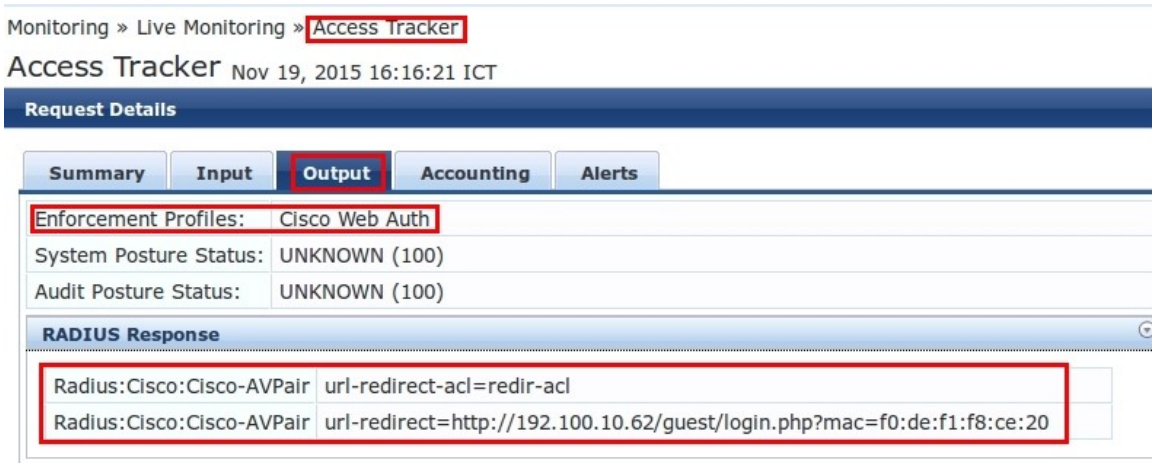
You must create Web_login page to appropriate with your url-redirect
and Select Vendor Setting = “Captive portal with Clearpass Web Auth”



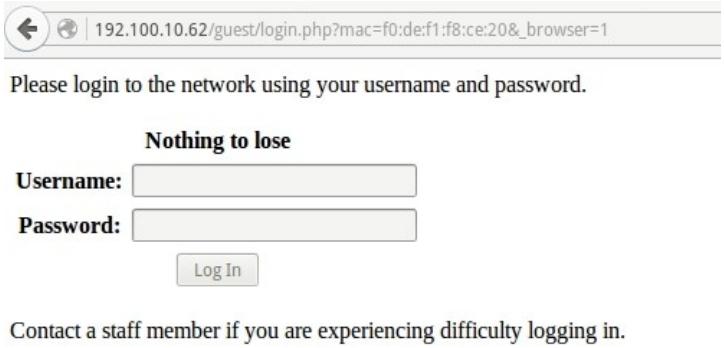
3) How to Track

Switch#show authentication session

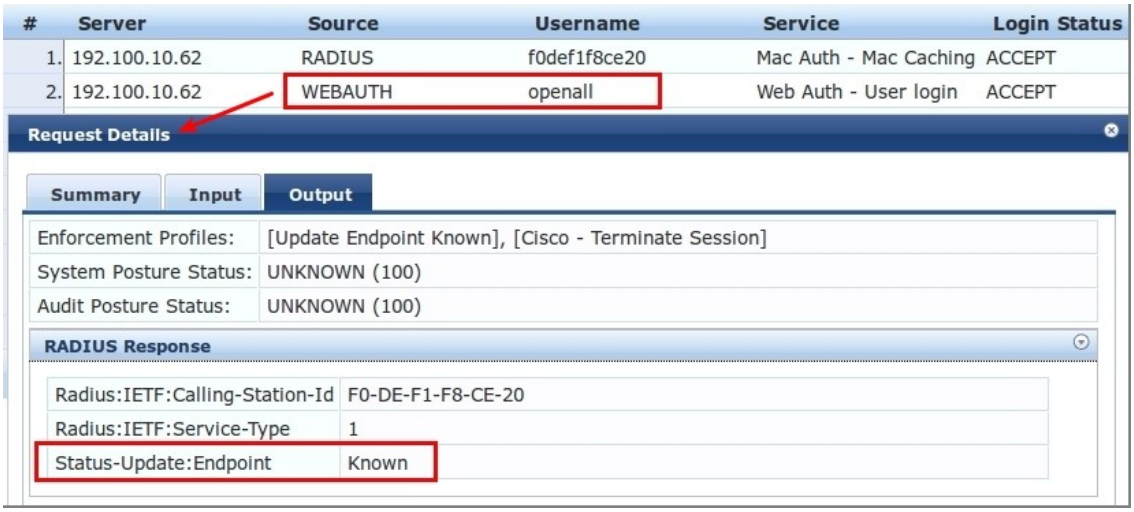
Interface MAC Address Method Domain Status Session ID
Gi1/0/1 f0de.f1f8.ce20 mab DATA Authz Success
AC1201C0000000200082E3C2

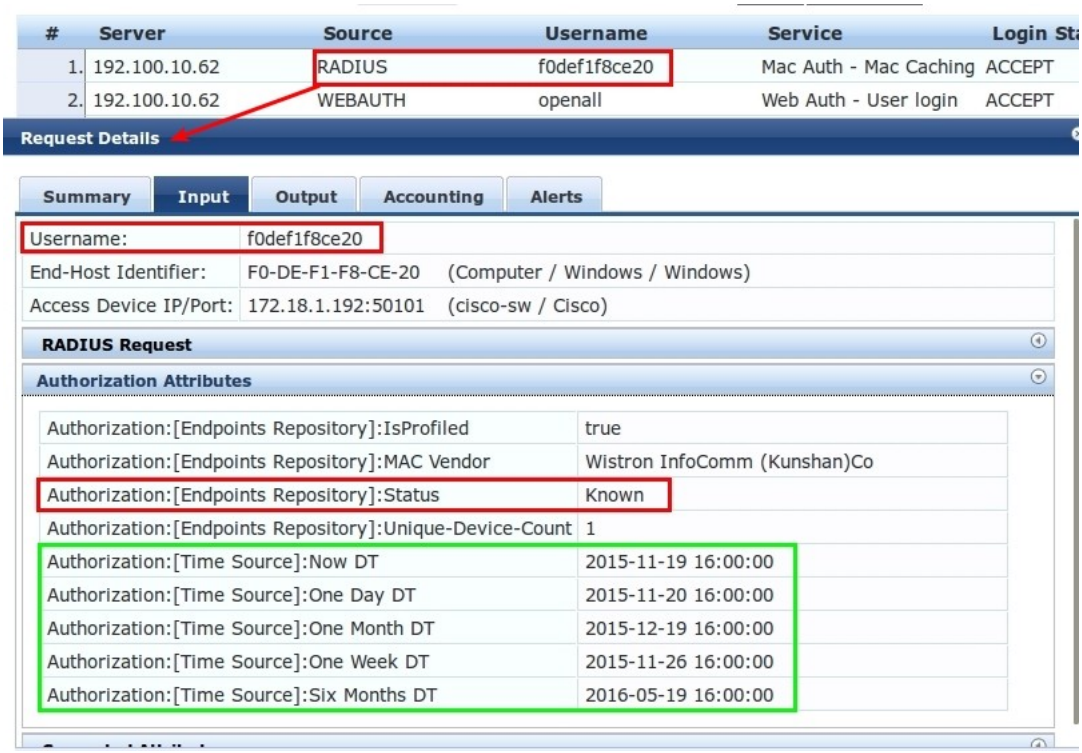


- Client should be redirect to Captive portal from CPPM



- After user post credential for this Captive portal
  If you see like exam below , it work ...





- Option : Time Source need for limit expire for MAC Caching