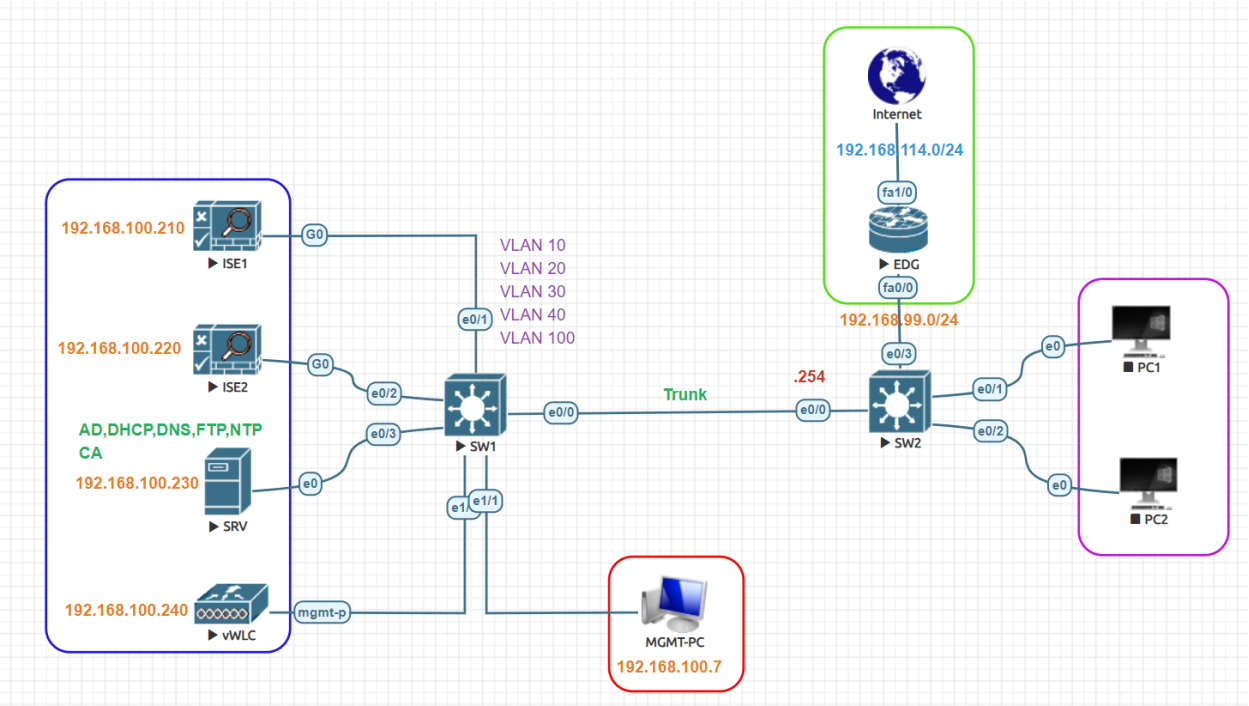
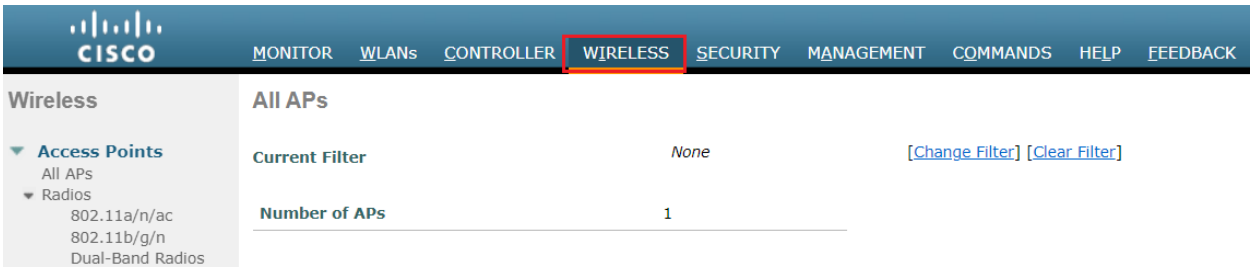
Hotspot Guest Access Lab:



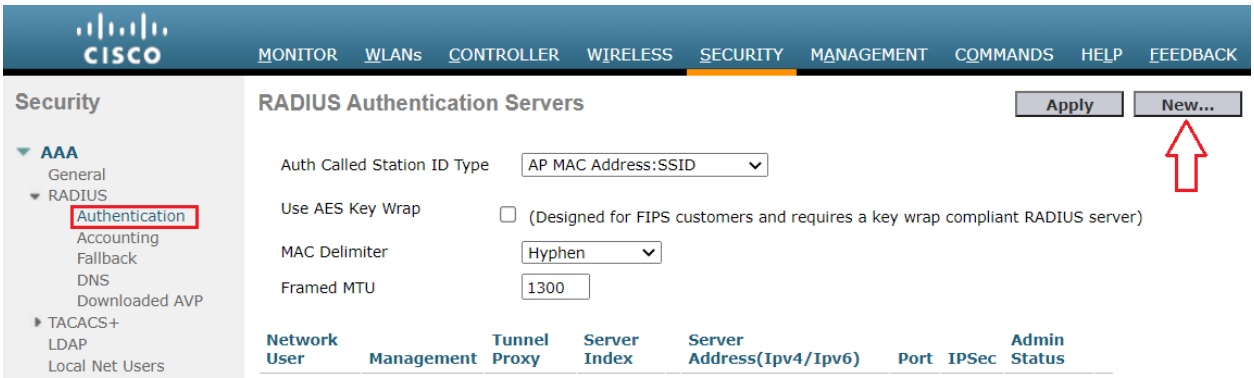
Cisco ISE Primary IP Address	192.168.100.210
Cisco ISE Secondary IP Address	192.168.100.220
AD and DNS IP Address	192.168.100.230
CA Server IP Address	192.168.100.230
Domain Name	test.local
Test User/Group	Guest
Test VLAN	VLAN 40
VLAN Subnet	192.168.40.0/24
VLAN 20 Gateway	192.168.40.1
Authenticator Device	vWLC
Default Route IP	192.168.100.254
Wireless LAN Controller IP	192.168.100.240
Computer	Window 10
Mobile Phone	Samsung Android
Wireless SSID	Guest
ACL Names	Web_Auth_Redirect and Guest_ACL
Guest Portal Name	Hotspot Guest Portal

Configure RADIUS on WLC:

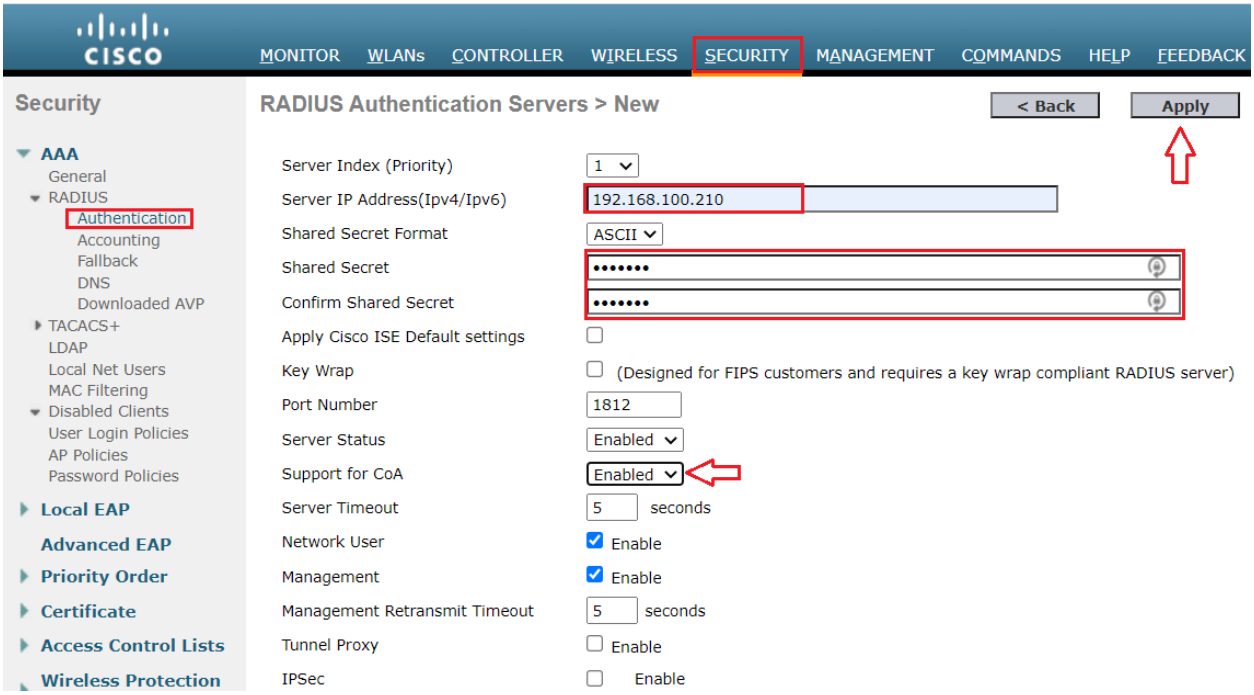
Log into the vWLC. Click the security tab at the top.



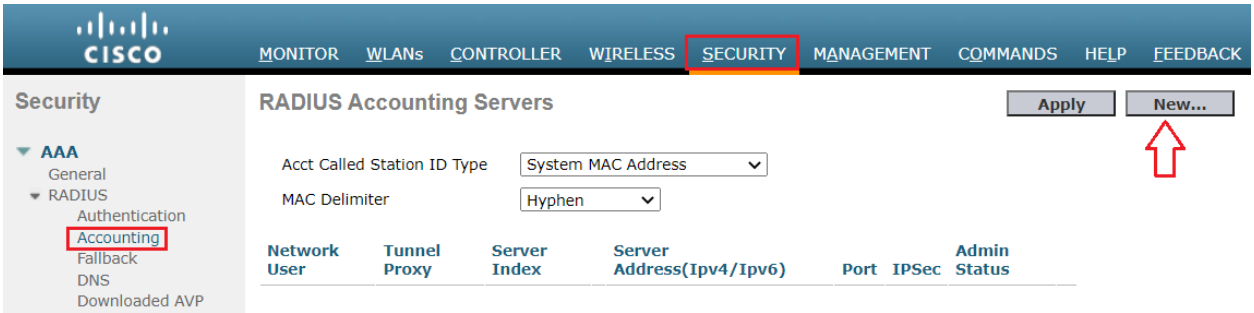
Click the New button to add a new AAA server.



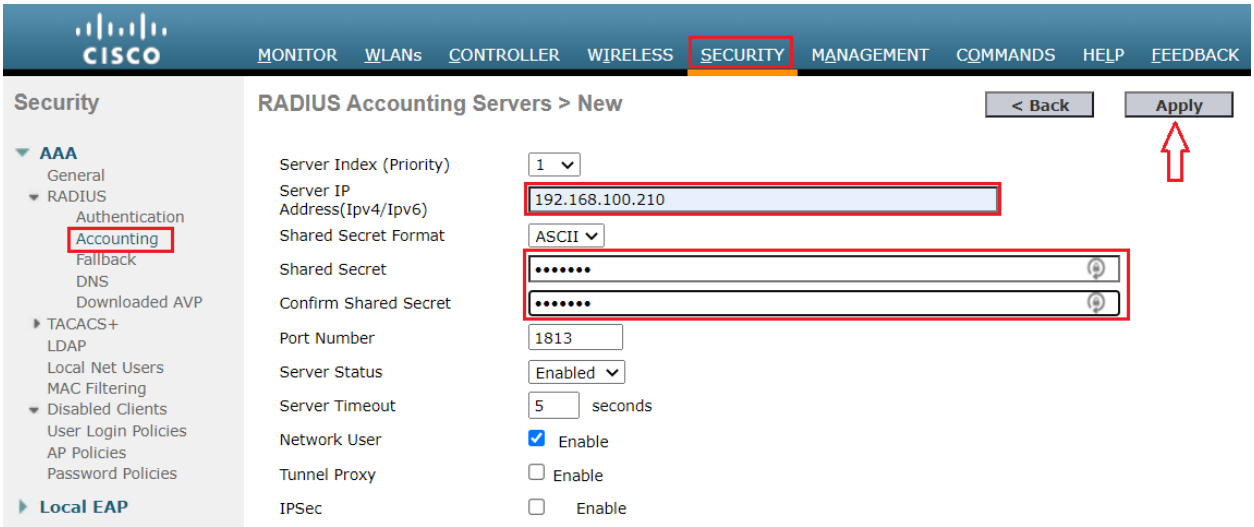
Enter IP address of the ISE server, port number is 1812, and that Support for COA is checked. Change of Authorization is a feature that allows a RADIUS server to adjust an active client session. Create a Shared Secret and make note of it as ISE will need to be configured with the same secret. Click Apply.



Configure RADIUS Accounting Go to Security -> RADIUS -> Accounting. The RADIUS Accounting servers page appears. To add a new RADIUS Server, click New.

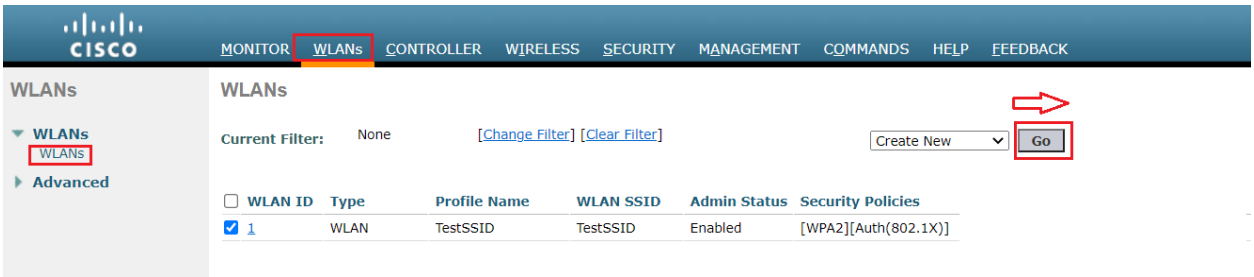


In the RADIUS Accounting Servers > New page, enter the parameters specific to the RADIUS server. In Server IP Address (Ipv4/Ipv6) type Cisco ISE IP 192.168.100.210

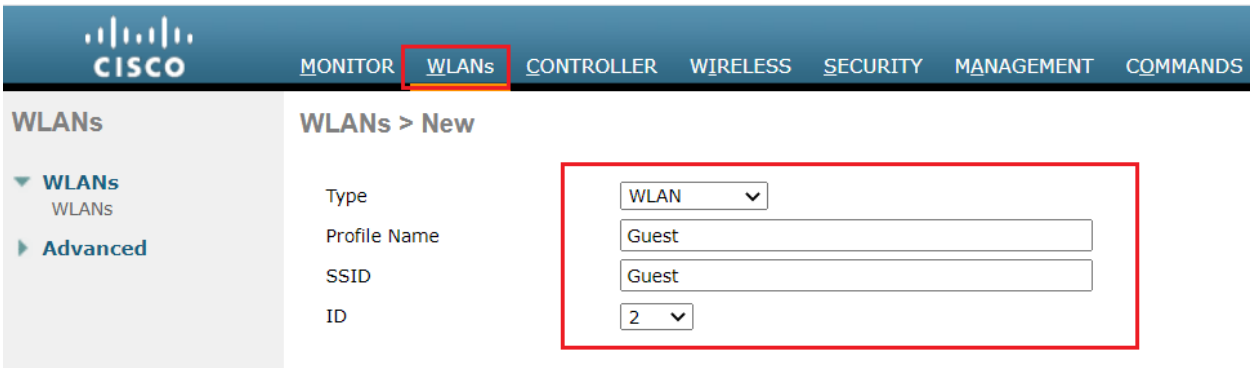


Configuring Guest SSID:

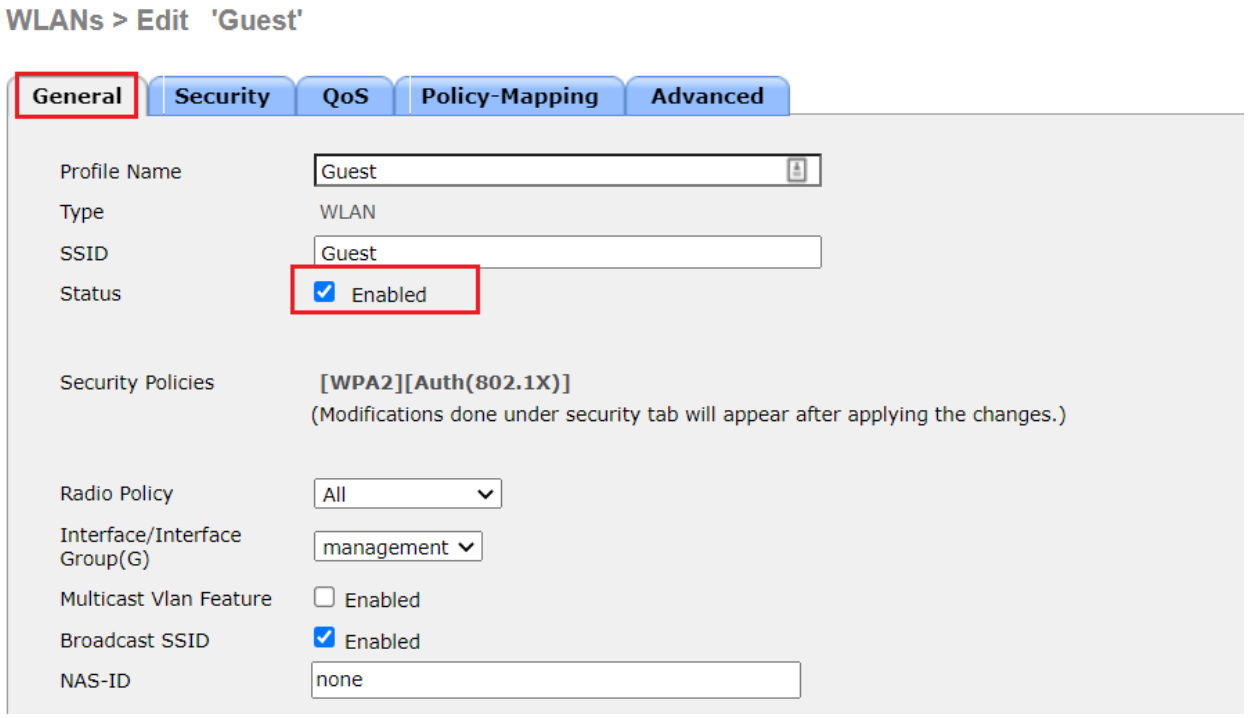
Log into WLC and click the WLANs tab. Choose Create New from drop down box and click Go.



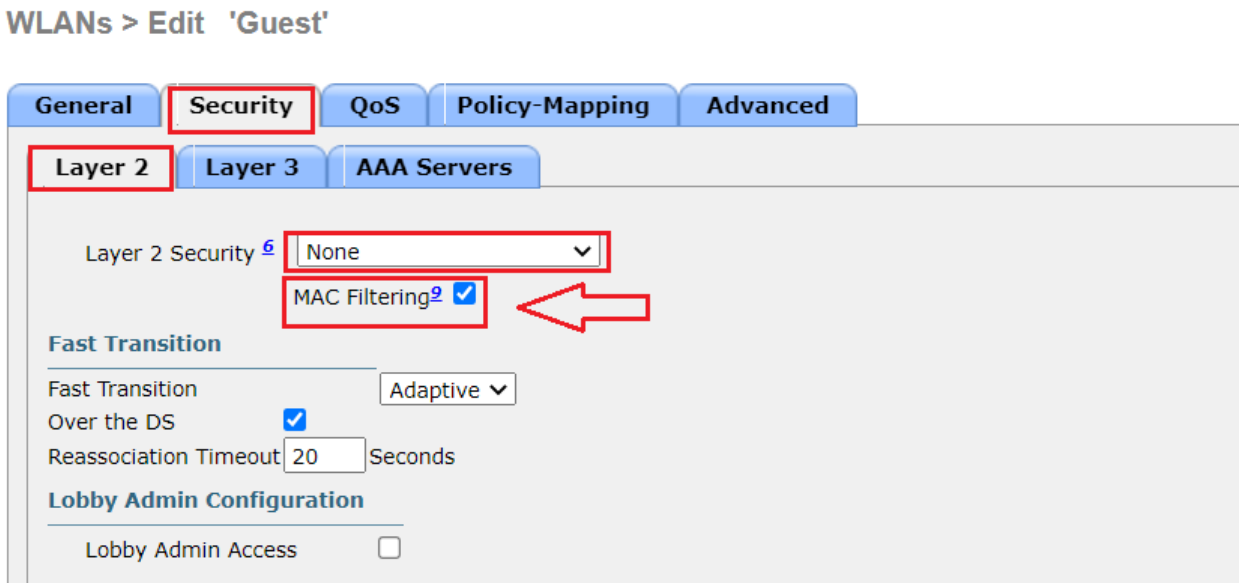
Choose WLAN for Type. Enter a Profile Name and a WLAN SSID of your choice, and click Apply.



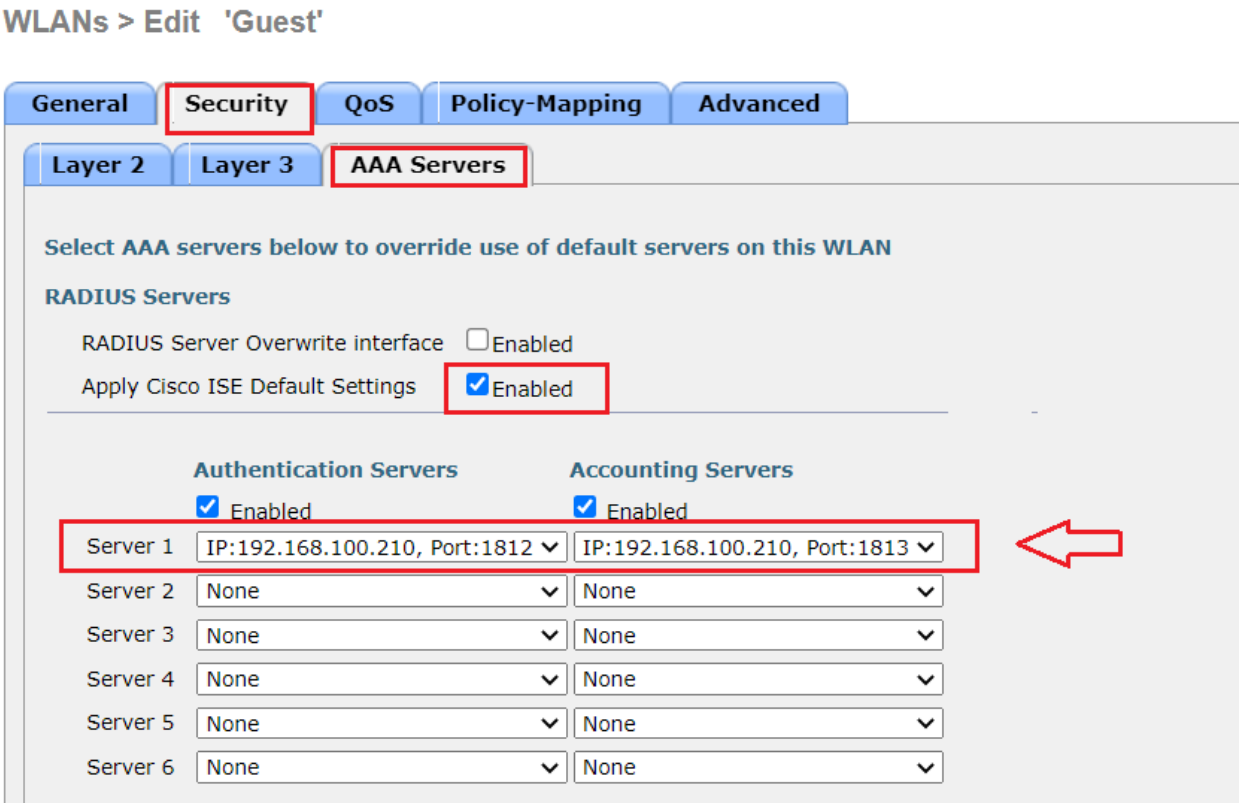
Select Status Enabled, and the correct interface for your guest traffic.



Next click the Security Tab. Change Layer 2 Security to None, and check MAC Filtering.



Click AAA Servers, and change the Authentication and Authorization servers to the ISE server via the drop down boxes and enabled Apply Cisco ISE Default Settings.



Click Advanced Tab. Check Allow AAA Override. Under NAC change the drop down to ISE NAC.

General | Security | QoS | Policy-Mapping | Advanced

Allow AAA Override: Enabled
Coverage Hole Detection: Enabled
Enable Session Timeout: 1800 Session Timeout (secs)
Aironet IE: Enabled
Diagnostic Channel 18: Enabled
Override Interface ACL: IPv4 None, IPv6 None
Layer2 Acl: None
URL ACL: None
P2P Blocking Action: Disabled
Client Exclusion 3: Enabled 180 Timeout Value (secs)
Maximum Allowed Clients 8: 0
Static IP Tunneling 11: Enabled
Wi-Fi Direct Clients Policy: Disabled
Maximum Allowed Clients Per AP Radio: 200

DHCP
DHCP Server: Override
DHCP Addr. Assignment: Required
OEAP
Split Tunnel: Enabled
Management Frame Protection (MFP)
MFP Client Protection 4: Optional
DTIM Period (in beacon intervals)
802.11a/n (1 - 255): 1
802.11b/g/n (1 - 255): 1
NAC
NAC State: ISE NAC
Load Balancing and Band Select

Uncheck Flex Connect Local Switching if enabled. Check DHCP/HTTP profiling under Radius Client Profiling and Click Apply to save settings.

General | Security | QoS | Policy-Mapping | Advanced

Scan Defer Priority: 0 1 2 3 4 5 6 7
Scan Defer Time(msecs): 100
FlexConnect
FlexConnect Local Switching 2: Enabled
FlexConnect Local Auth 12: Enabled
Learn Client IP Address 5: Enabled
Vlan based Central Switching 13: Enabled
Central DHCP Processing: Enabled
Override DNS: Enabled
NAT-PAT: Enabled
Central Assoc: Enabled
11k
Neighbor List: Enabled

Radius Client Profiling
DHCP Profiling
HTTP Profiling
Local Client Profiling
DHCP Profiling
HTTP Profiling
Universal AP Admin Support
Universal AP Admin
11v BSS Transition Support
BSS Transition
Optimized Roaming Disassociation Timer(0 to 40 TBTT): 40
BSS Max Idle Service
Directed Multicast Service
Tunneling
Tunnel Profile: None

Finally, Guest SSID is configured.

MONITOR | WLANs | CONTROLLER | WIRELESS | SECURITY | MANAGEMENT | COMMANDS | HELP | FEEDBACK

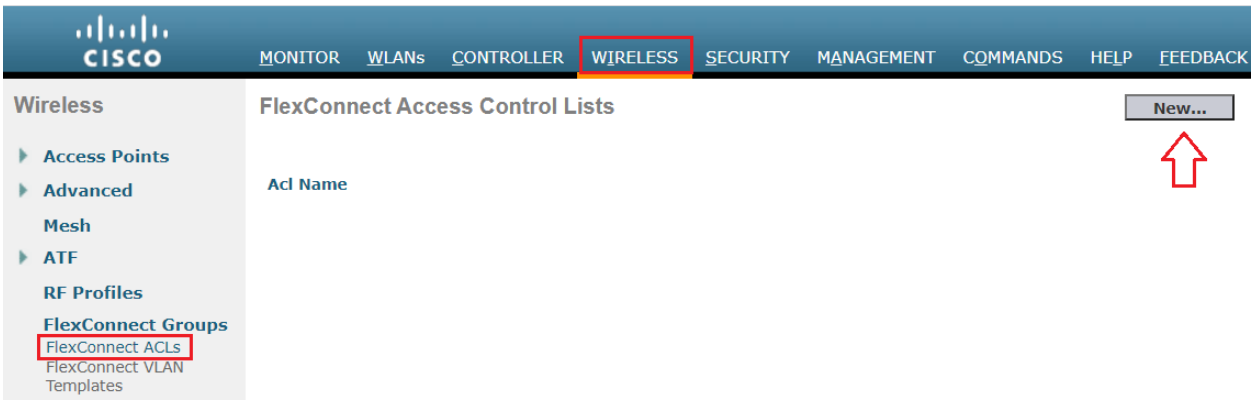
WLANs

Current Filter: None [Change Filter] [Clear Filter] Create New Go

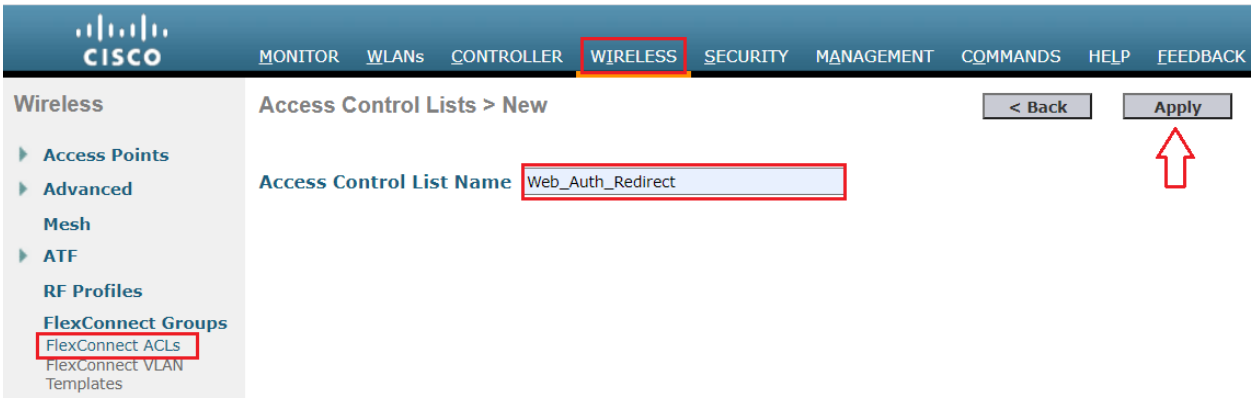
WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
1	WLAN	Employees	Employees	Enabled	[WPA2][Auth(802.1X)]
2	WLAN	Guest	Guest	Enabled	MAC Filtering

Configure ACLs:

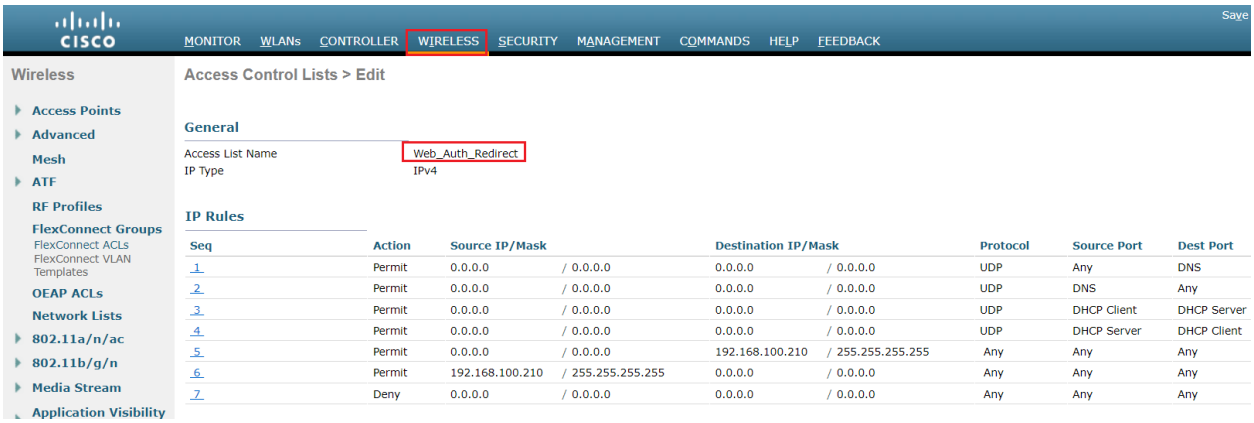
Next we have to create a few ACLs. One for Web Auth Redirect that will allow DNS and traffic to ISE and another ACL for restricting guest access. Go to Wireless>FlexConnect ACLs Click New.



For the ACL name type Web_Auth_Redirect. Click Apply, then click the ACL name to start editing the access control list rules.

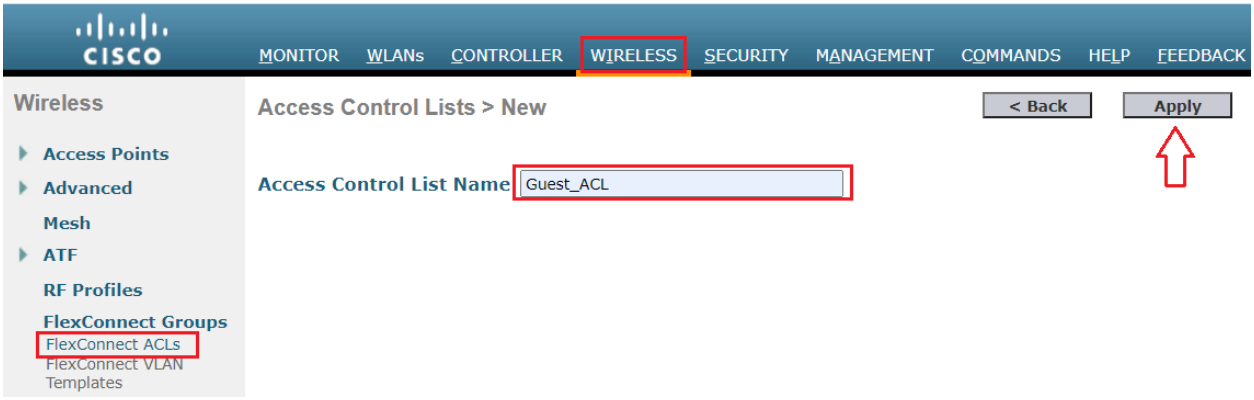


Click Add New Rule. Create a rule allowing destination DNS (udp/53) from any to any. Create a rule allowing source DNS from any to any. Create a rule allowing tcp from ISE to any. Create a rule allowing tcp from any to ISE.



Seq	Action	Source IP/Mask		Destination IP/Mask		Protocol	Source Port	Dest Port
1	Permit	0.0.0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	UDP	Any	DNS
2	Permit	0.0.0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	UDP	DNS	Any
3	Permit	0.0.0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	UDP	DHCP Client	DHCP Server
4	Permit	0.0.0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	UDP	DHCP Server	DHCP Client
5	Permit	0.0.0.0	/ 0.0.0.0	192.168.100.210	/ 255.255.255.255	Any	Any	Any
6	Permit	192.168.100.210	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	Any	Any	Any
7	Deny	0.0.0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any

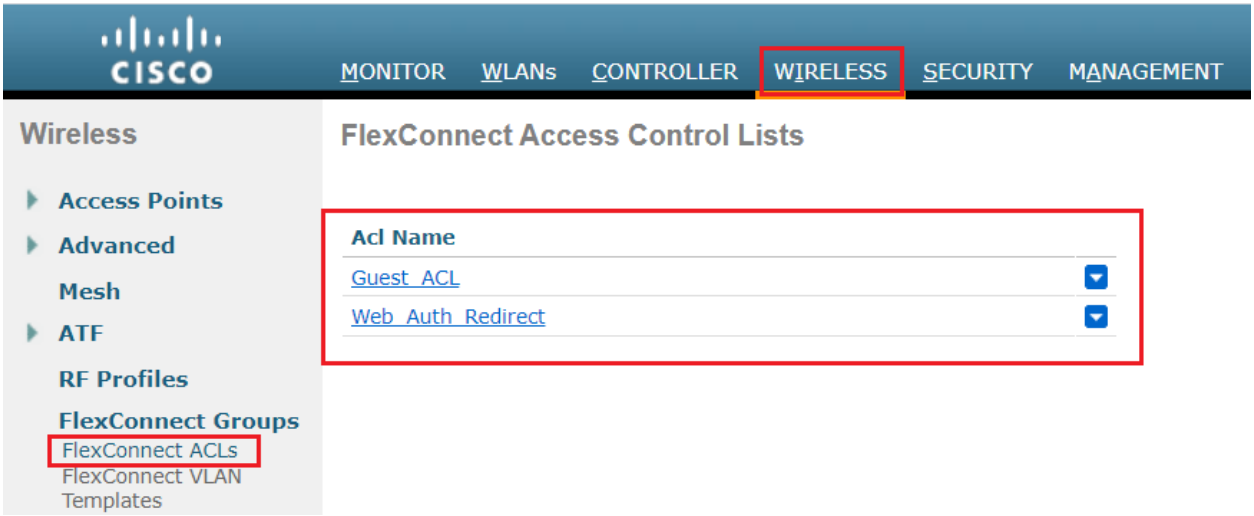
Create a new ACL if you'd like to place any restrictions on your guest network such as blocking access to any of your private IP or internal Network space.



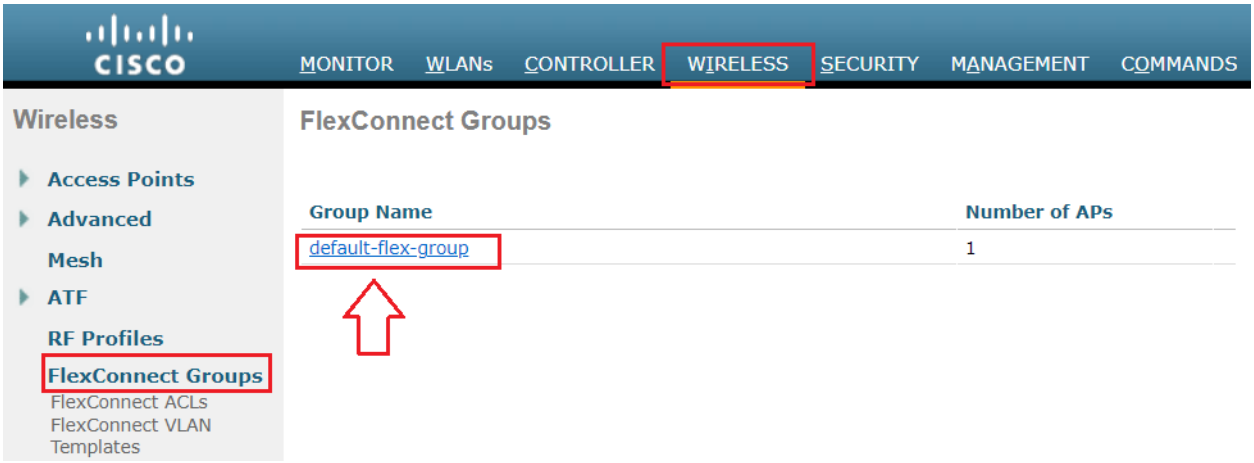
Guest_ACL
IPv4

Action	Source IP/Mask		Destination IP/Mask		Protocol	Source Port	Dest Port
Permit	0.0.0.0	/ 0.0.0.0	192.168.100.230	/ 255.255.255.255	UDP	Any	DNS
Permit	192.168.100.230	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	UDP	DNS	Any
Permit	192.168.100.210	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	TCP	Any	8443
Permit	0.0.0.0	/ 0.0.0.0	192.168.100.210	/ 255.255.255.255	TCP	8443	Any
Permit	0.0.0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any

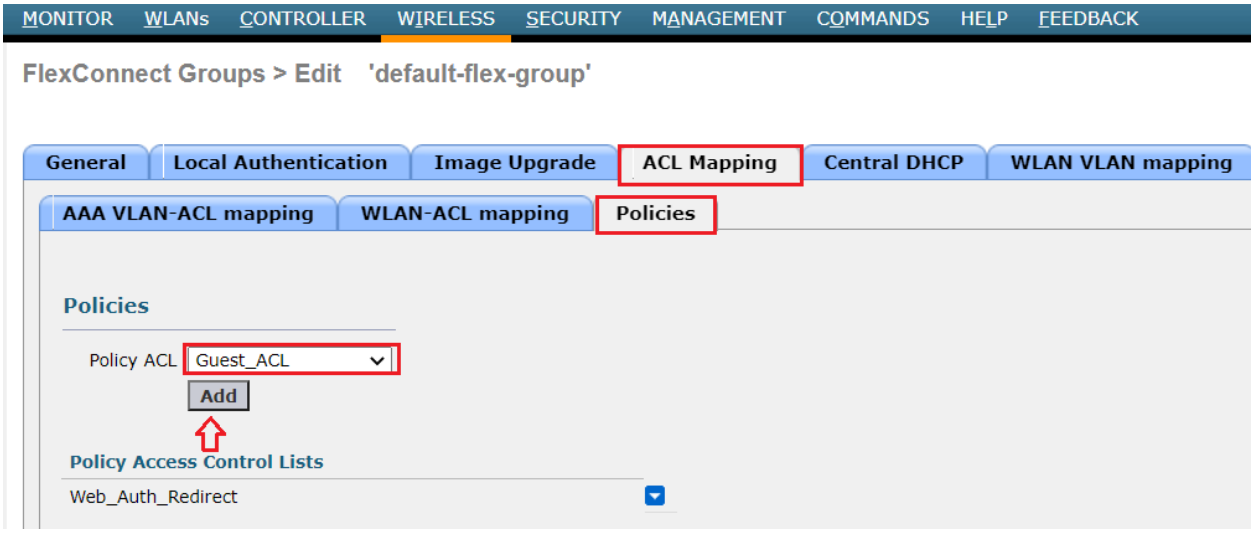
Finally, we ACLs are configured Guest_ACL and Web_Auth_Redirect ACL.



Go to Wireless>FlexConnect Groups click to edit.



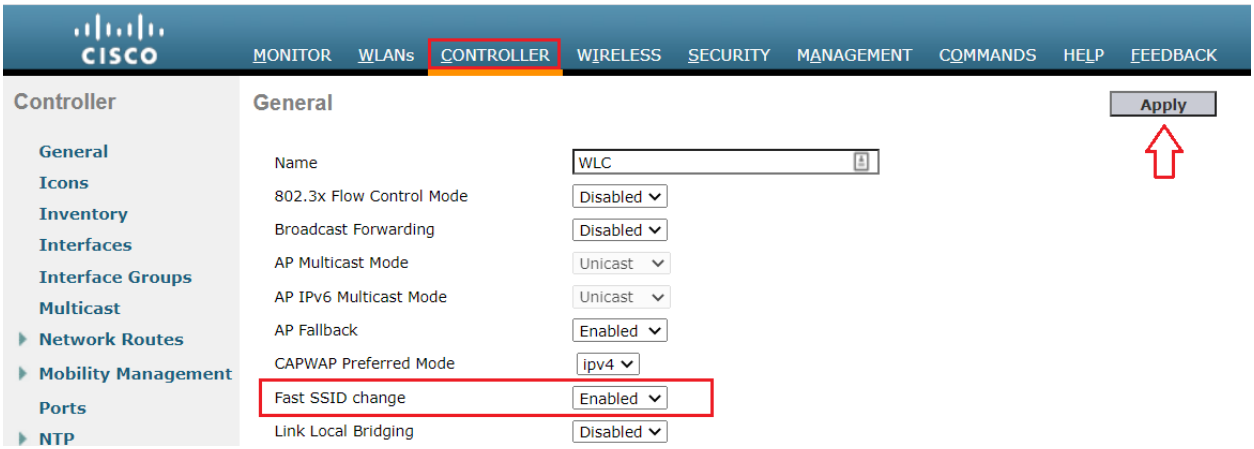
Go to ACL Mapping>Policies in Policy ACL from drop down choose Web_Auth_Redirect ACL click Add to push the ACL to WLC and Access points.



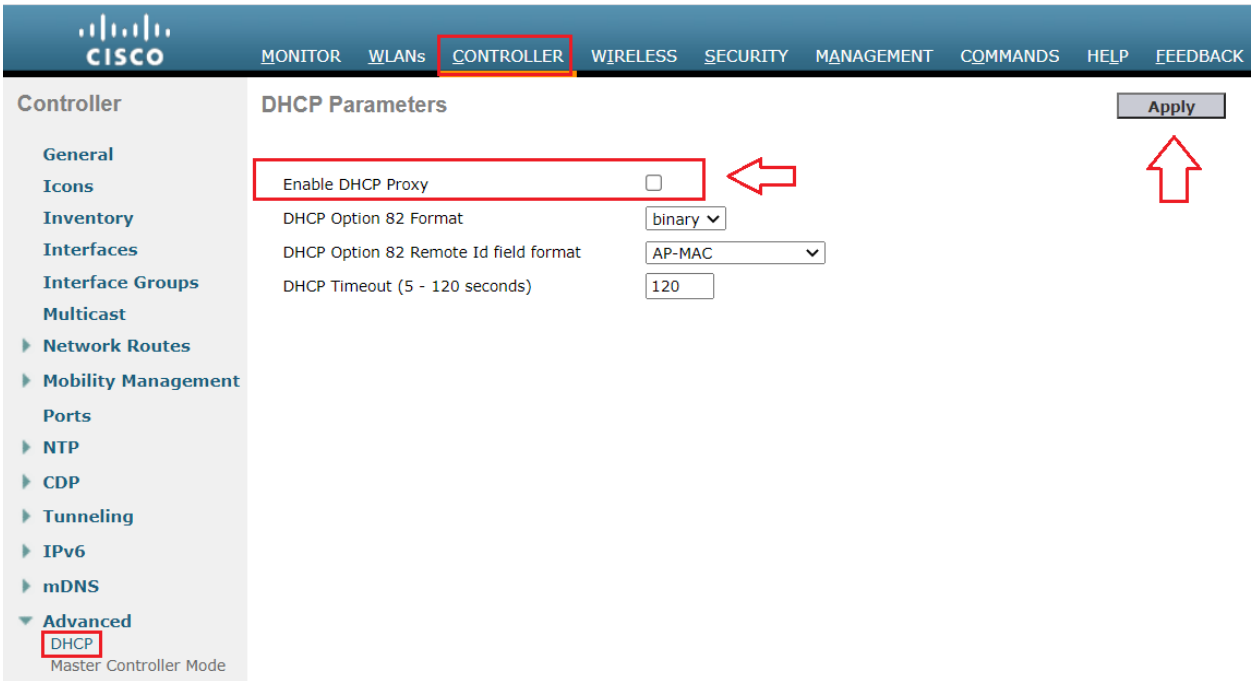
Let's verify the ACLs has been pushed to Access Point (AP).

```
AP#show access-lists
Extended IP access list Web_Auth_Redirect
    1 permit udp any range 0 65535 any eq domain
    2 permit udp any eq domain any range 0 65535
    3 permit udp any eq bootpc any eq bootps
    4 permit udp any eq bootps any eq bootpc
    5 permit ip any host 192.168.100.210
    6 permit ip host 192.168.100.210 any
    7 deny ip any any
AP#
```

Enabling Enable fast-SSID-change feature allows wireless clients to transition from Open SSID to Secured SSID without delay. Access the WLC GUI and navigate to Controller > General Enable Fast SSID Change. Click Apply and Save Configuration



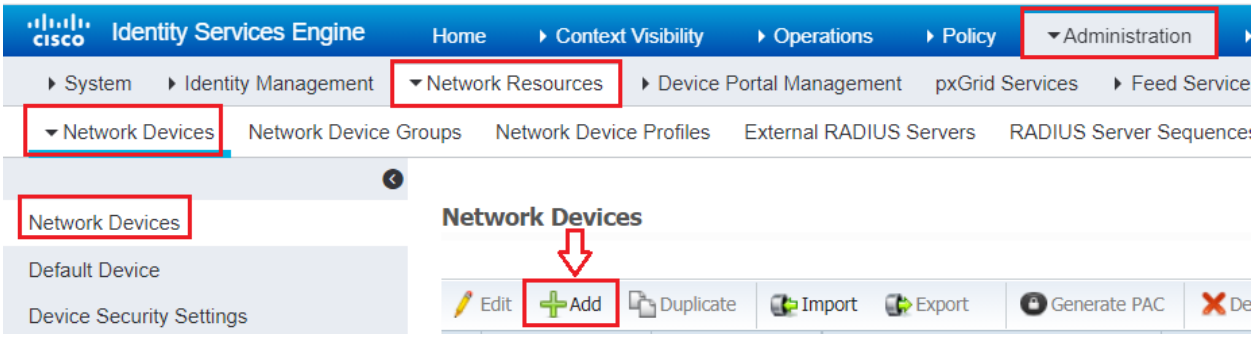
Next navigate to Controller>Advanced>DHCP in DHCP Parameters unchecked Enable DHCP Proxy and click Apply button to save setting.



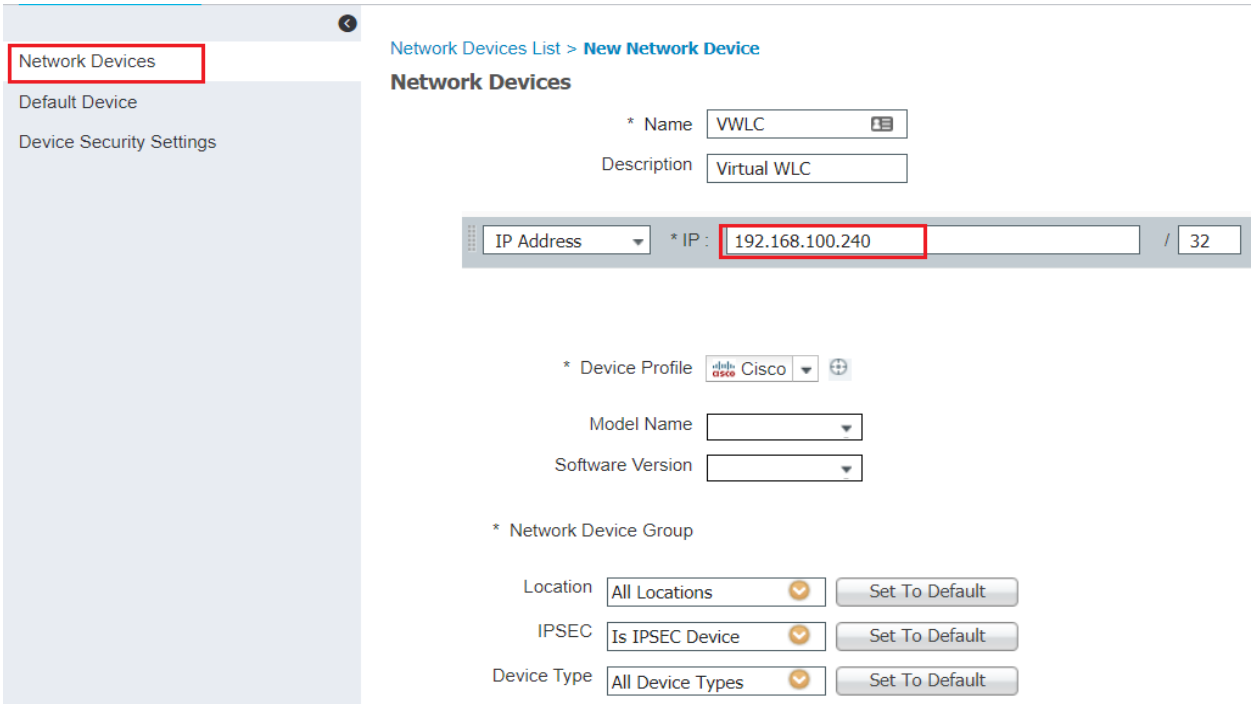
Add WLC Network Device:

Next we will log into ISE and configure the WLC as a network device. Go to Administration > Network Resources > Network Devices to add the Device (WLC).

Click on Add button to add Network Device like Cisco Wireless LAN Controller.

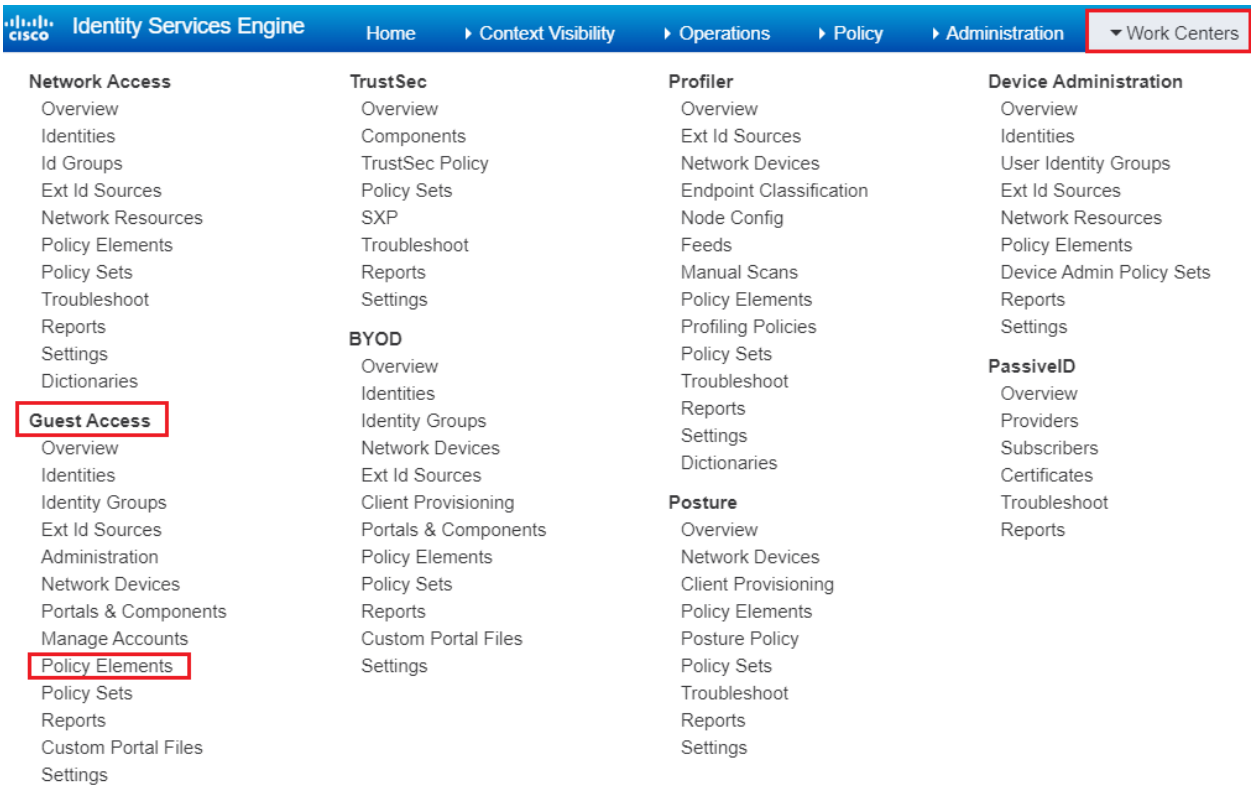


Configure **Name** of device, **IP address** configured. Scroll down to set Authentication settings.

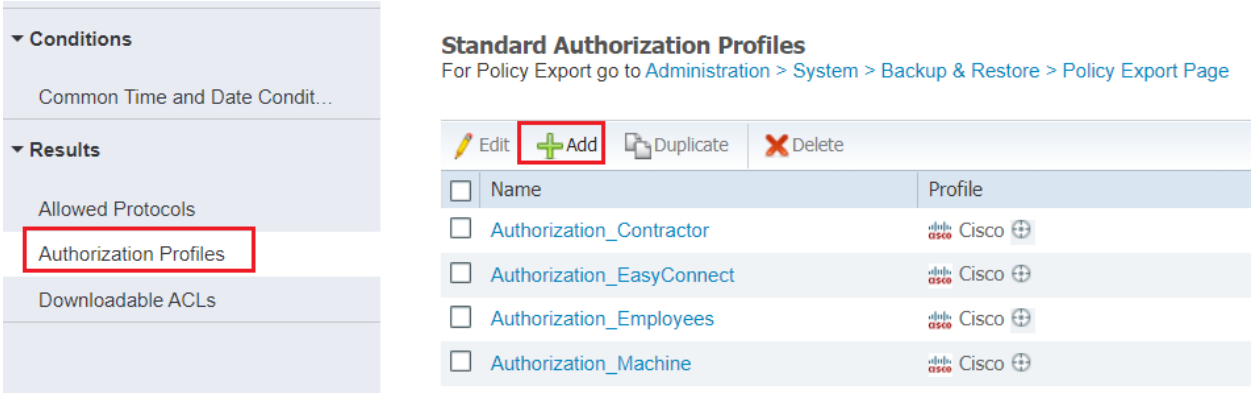


Configure ISE Policies:

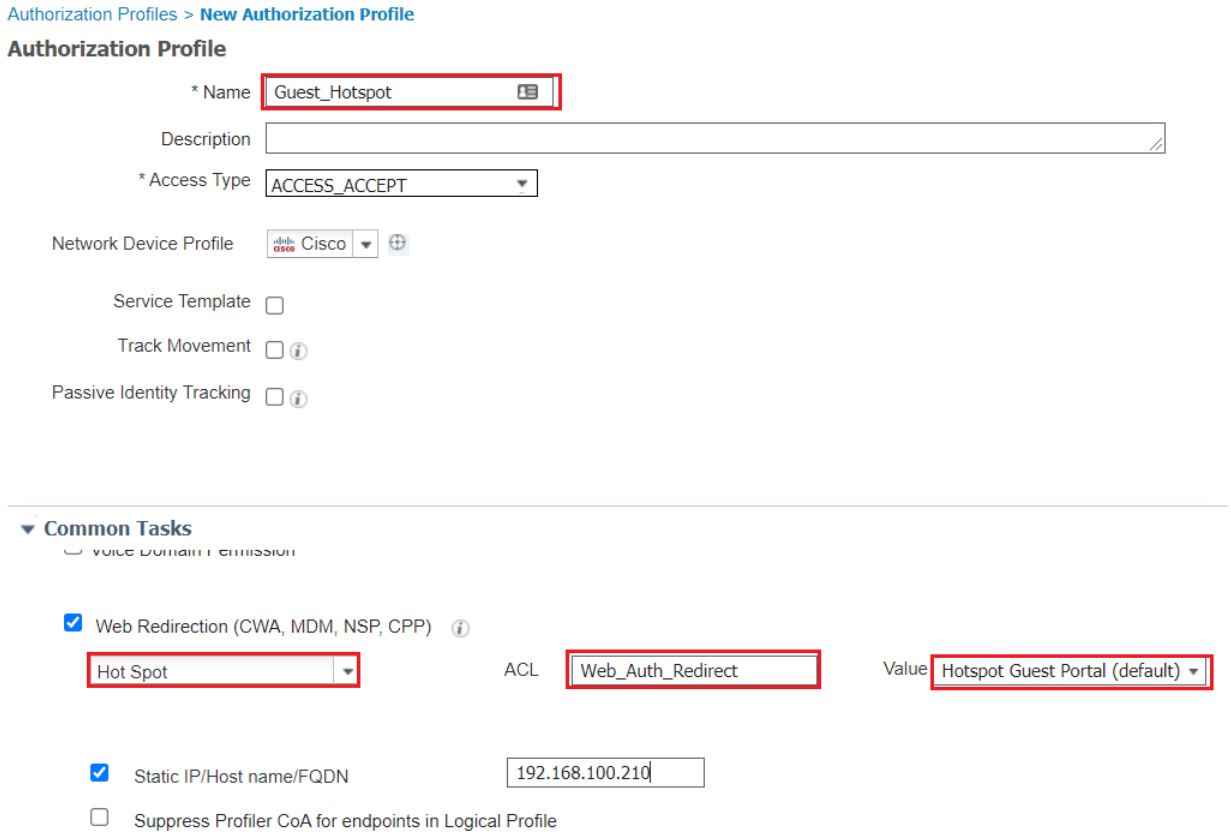
Our policy goals are redirect users who connect to the Guest network to a web portal. Once AUP has been accepted they will get new policy applied to them restricting their access to internet only via ACL we created earlier. Go to Work Centers>Guest Access>Policy Elements.



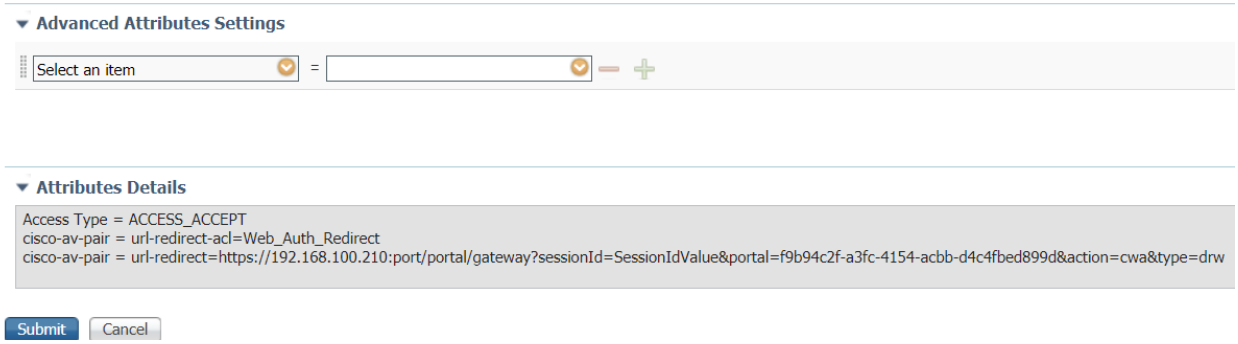
Click Results and go to Authorization Profiles. Click Add to create a new profile. Give the policy a descriptive name and description.



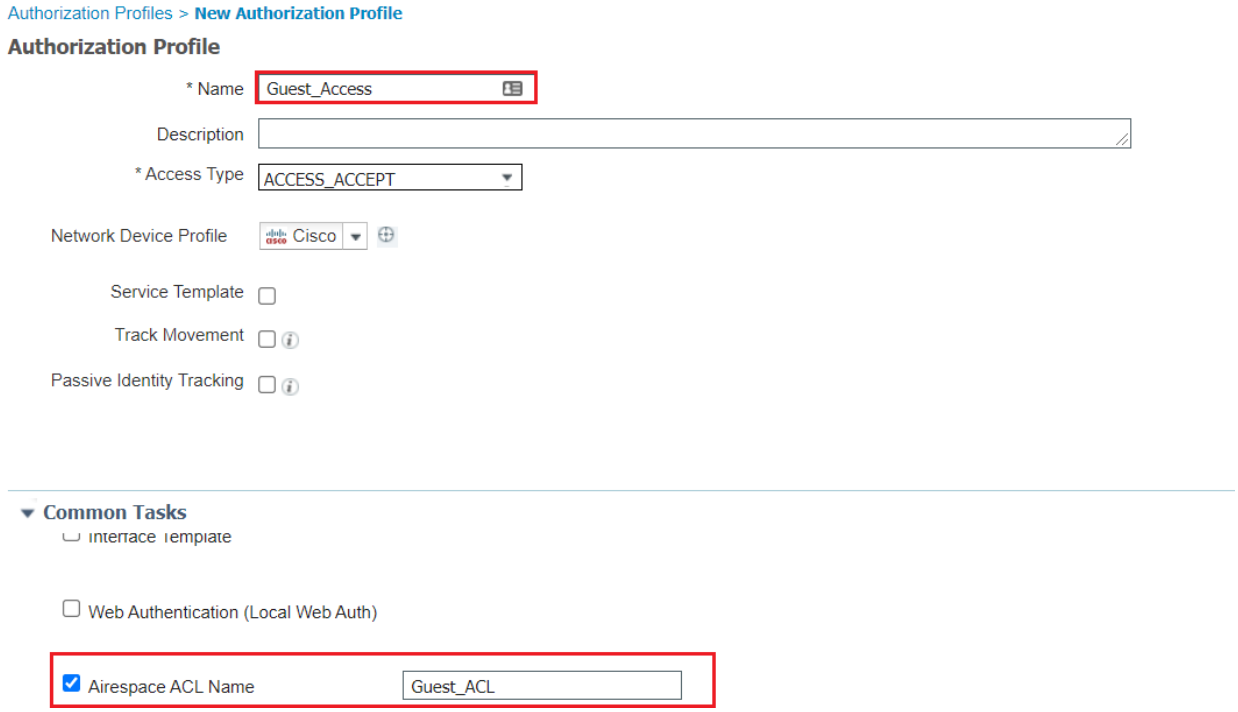
Scroll down to the Common Tasks and check Web Redirection. Select Hotspot from the drop down. Enter Web_Auth_Redirect as the ACL and the value will be the Hotspot guest portal.



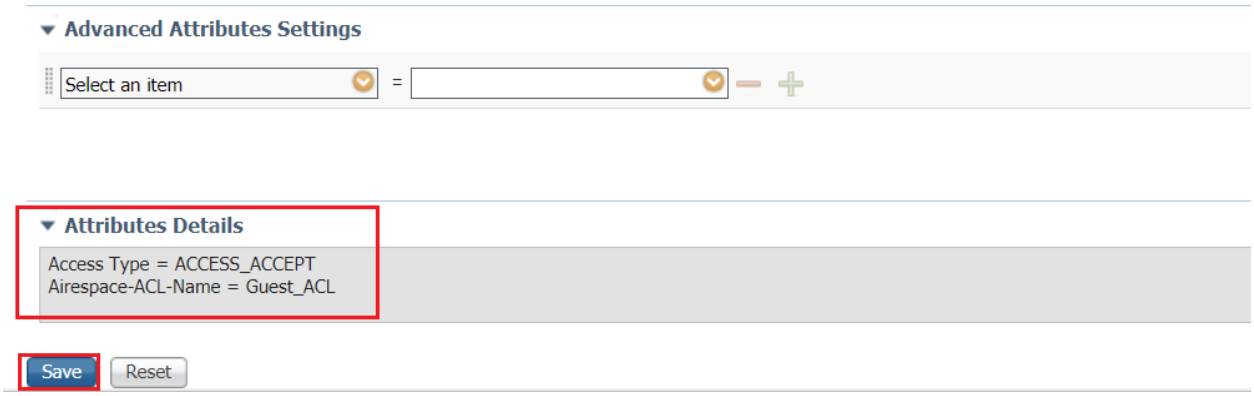
Check all the setting and finally click Submit to save the setting.



Click Add again, enter a new name and description. This policy will apply the guest restriction ACL we created on the WLC. Scroll down into the Common Tasks and find Airespace ACL, enter the name Guest_ACL Click Submit.

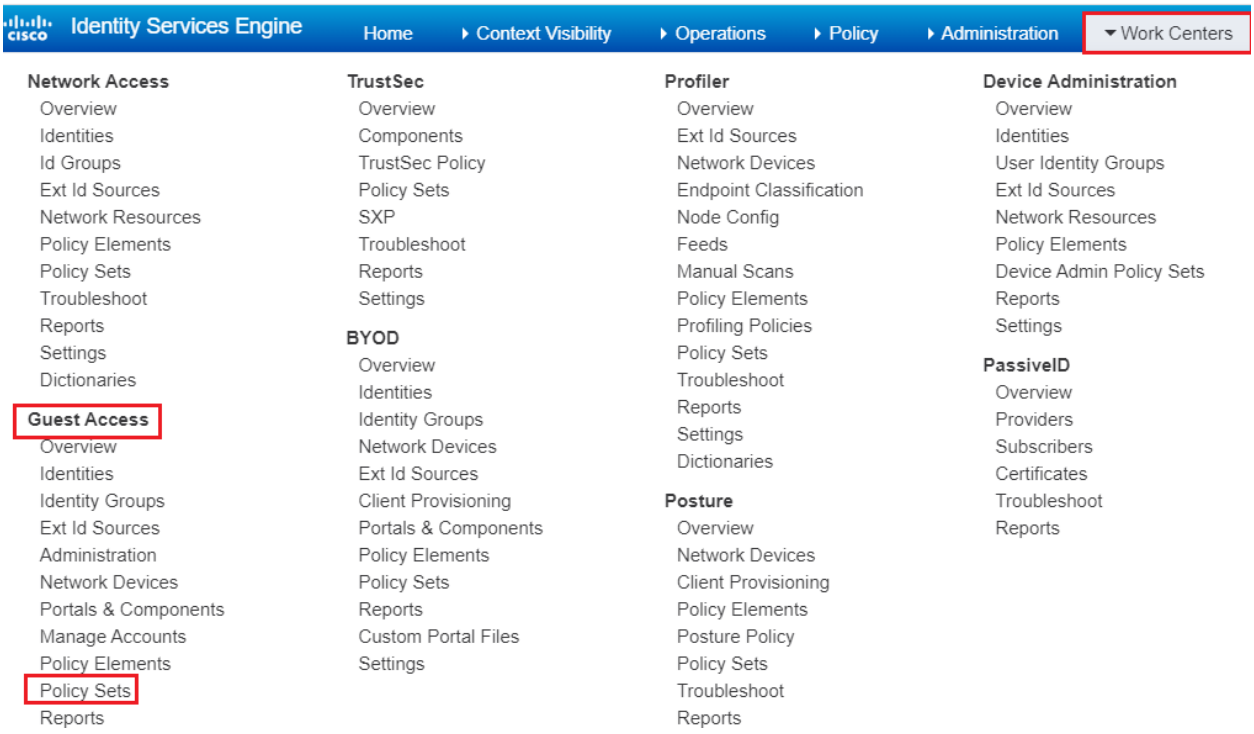


Check all the setting and finally click Submit to save the setting.

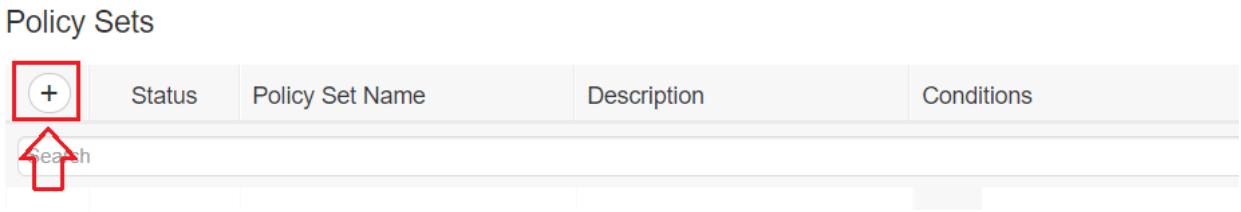


Create Policy Set:

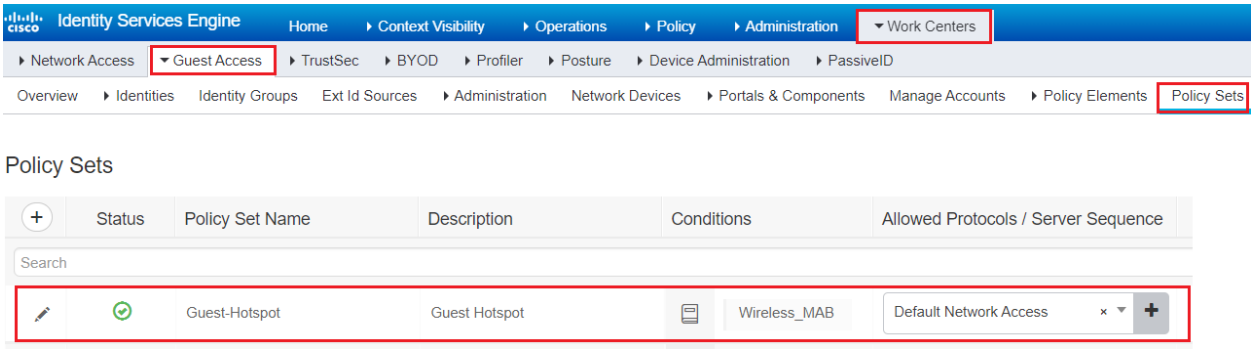
Now, go to Work Centers>Guest Access>Policy Sets.



In order to create a Policy Set from ISE GUI, click on plus (+) icon on the upper-left corner.

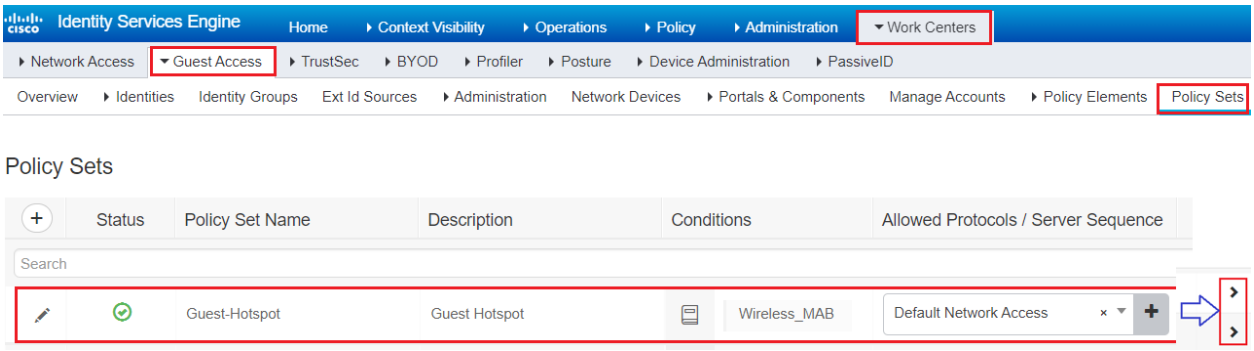


Enter a new policy Set name and description. Choose the Conditions Wireless_MAB and set allow Protocols Default Network Access.

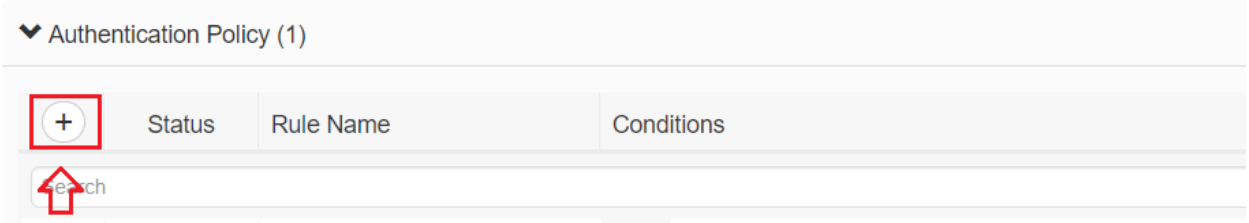


Authentication Policy:

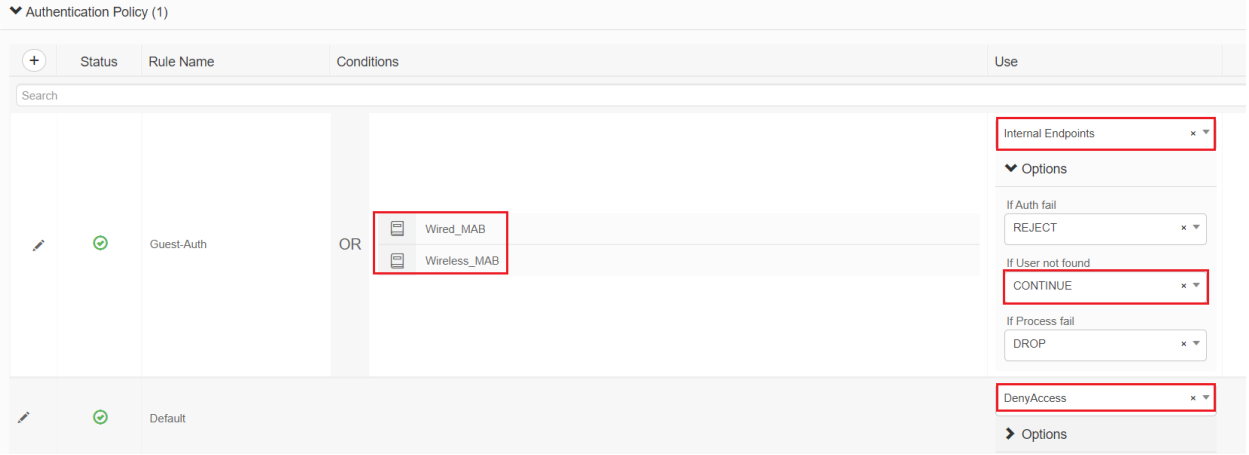
Expand the policy set by clicking the arrow on the right. Expand the Authentication Policy be clicking the arrow.



Create new Authentication policy click by plus circle name rule.

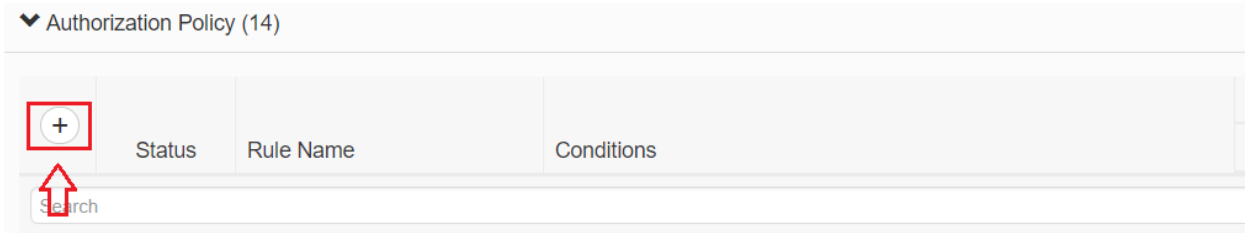


Set the condition Wireless_MAB and Database Internal Endpoints. Be sure the option for "If User not found" is set to Continue. Set the default rule to DenyAccess.

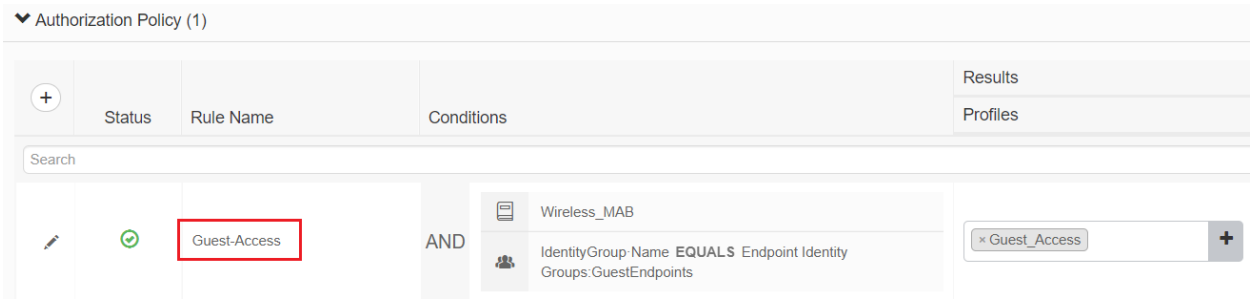


Authorization Policy:

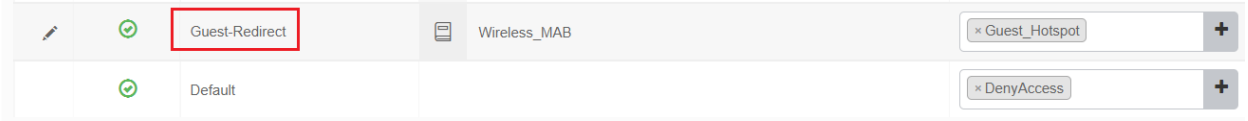
Next we'll create our new Authorization Polices for the Guest network. Expand Authorization Policy.

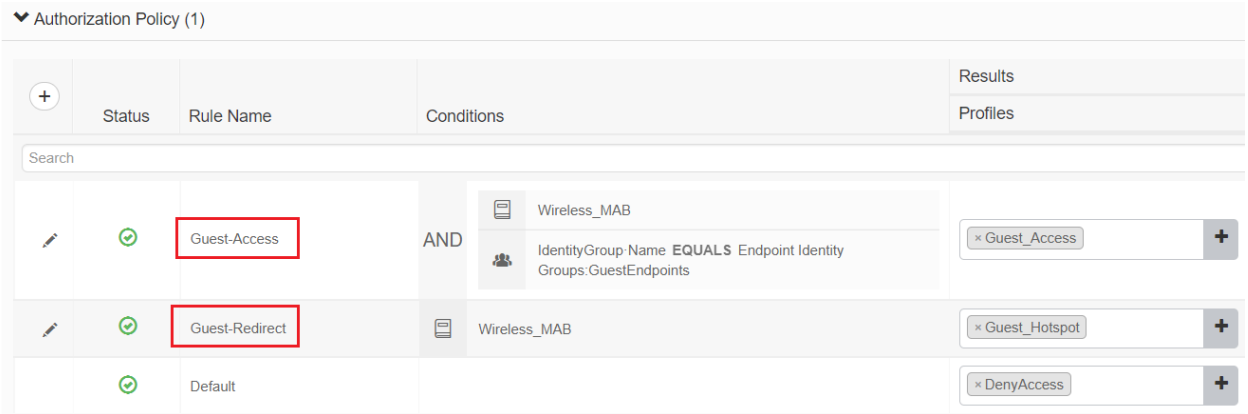


Enter a name for the policy. Select Wireless_MAB as the condition, and Guest_Hotspot as the Profile.



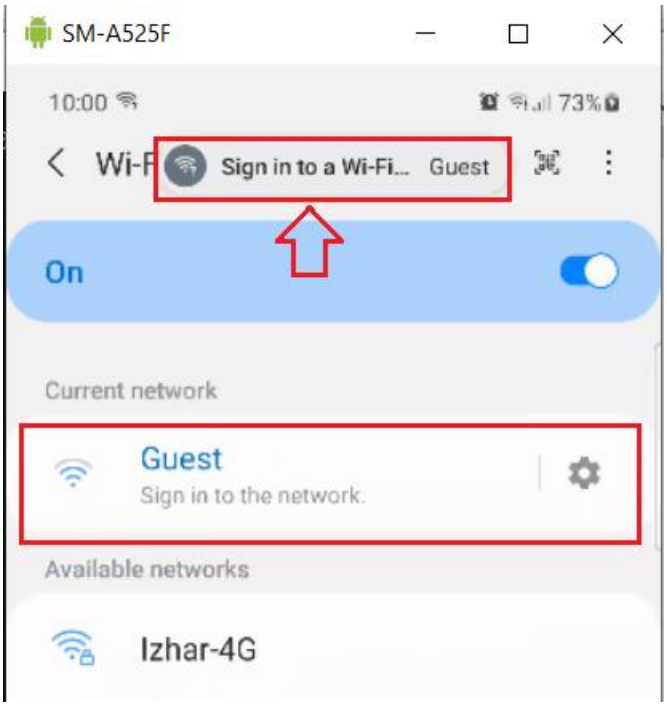
Add a new profile above the one we just created. This will be for applying the Guest ACL for the user once going through the portal. Conditions will be Wireless_MAB, IdentityGroup = GuestEndpoints, and Guest_Flow. Result will be the Guest_Access policy we created which applies the ACL we created on the WLC.



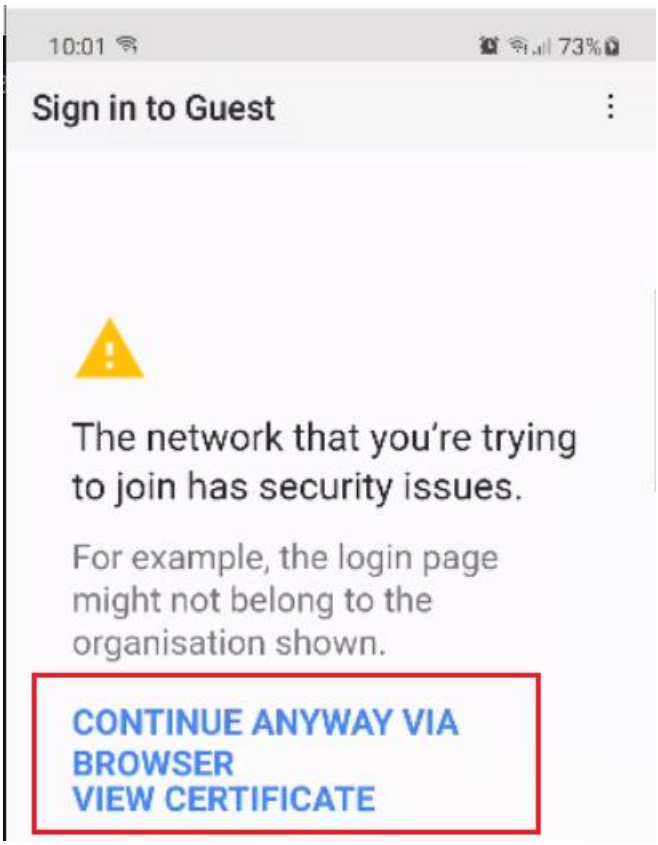


Testing and Verification:

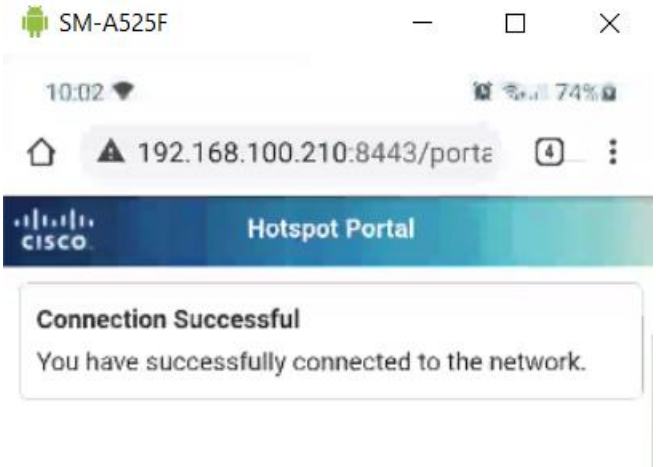
Connect to Guest Network in your mobile phone it will redirect to Guest Portal.



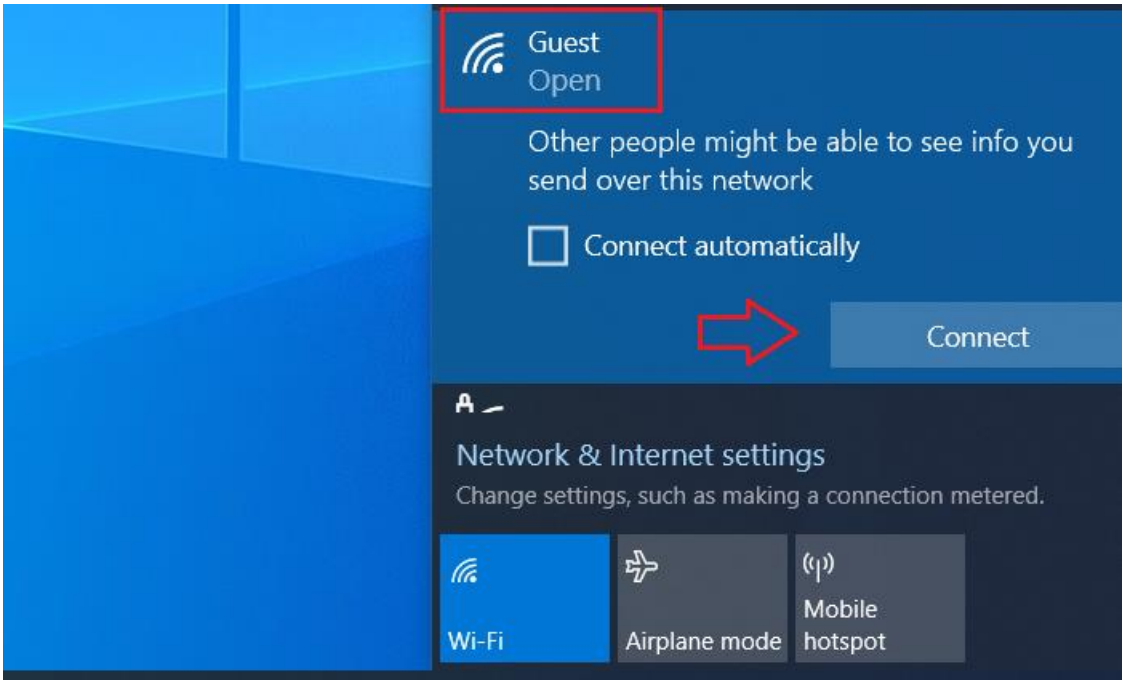
Accept the Certificate error to continue in real world we need to use public certificate.



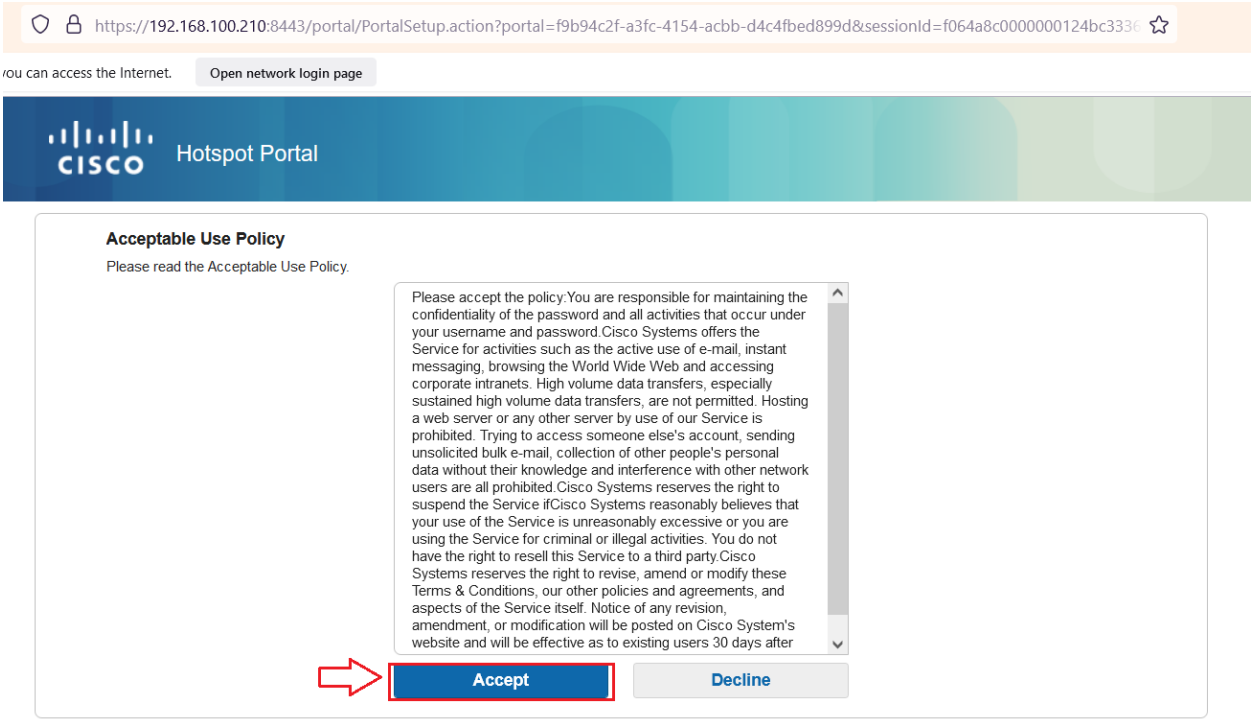
It shows Connection Successful message now can browse the internet.



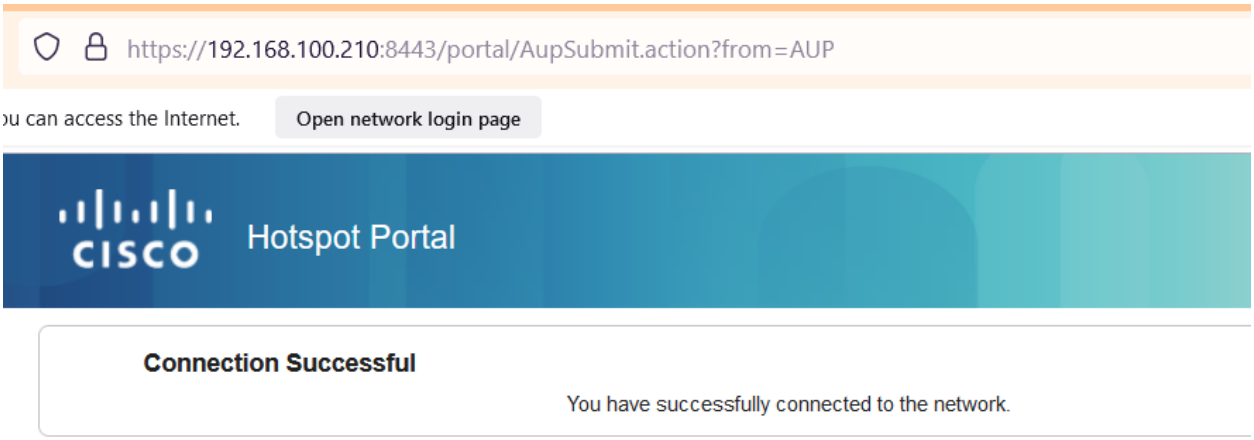
In your windows Laptop connect to Guest SSID.



Accept Hotspot Portal Acceptable User Policy by clicking Accept.



Connection Successful message display now can use internet.



Identity Services Engine | Home | Context Visibility | Operations | Policy | Administration | Work Centers

RADIUS | Threat-Centric NAC Live Logs | TACACS | Troubleshoot | Adaptive Network Control | Reports

Live Logs | Live Sessions

Refresh | Reset Repeat Counts | Export To

Time	Status	Details	Repeat ...	Identity	Endpoint ID
				Identity	Endpoint ID
Sep 04, 2021 07:05:25.491 PM			0	AC:67:5D:4B:82:41	AC:67:5D:4B:82:41
Sep 04, 2021 07:05:25.468 PM				AC:67:5D:4B:82:41	AC:67:5D:4B:82:41
Sep 04, 2021 07:05:25.425 PM					AC:67:5D:4B:82:41
Sep 04, 2021 07:04:44.837 PM				AC:67:5D:4B:82:41	AC:67:5D:4B:82:41

Endpoint P...	Authenticat...	Authorizati...	Authorizati...	IP Address	Network Device
Endpoint Profi	Authenticatior	Authorization	Authorization	IP Address	Network Device
Windows10-...	Guest-Hotspot	Guest-Hotsp...	Guest_Access	192.168.100.6	
Windows10-...	Guest-Hotspot	Guest-Hotsp...	Guest_Access		VWLC
					VWLC
Windows10-...	Guest-Hotsp...	Guest-Hotsp...	Guest_Hotspot		VWLC
Android	Guest-Hotsp...	Guest-Hotsp...	Guest_Hotspot	192.168.100.22	
Linux-Works...	Guest-Hotsp...	Guest-Hotsp...	Guest_Hotspot		VWLC
Windows10-...	Guest-Hotsp...	Guest-Hotsp...	Guest_Hotspot		VWLC
Android	Guest-Hotspot	Guest-Hotsp...	Guest_Access		VWLC

Overview

Event	5200 Authentication succeeded
Username	26:CF:51:98:98:31
Endpoint Id	26:CF:51:98:98:31
Endpoint Profile	Linux-Workstation
Authentication Policy	Guest-Hotspot >> Guest-Auth
Authorization Policy	Guest-Hotspot >> Guest-Redirect
Authorization Result	Guest_Hotspot