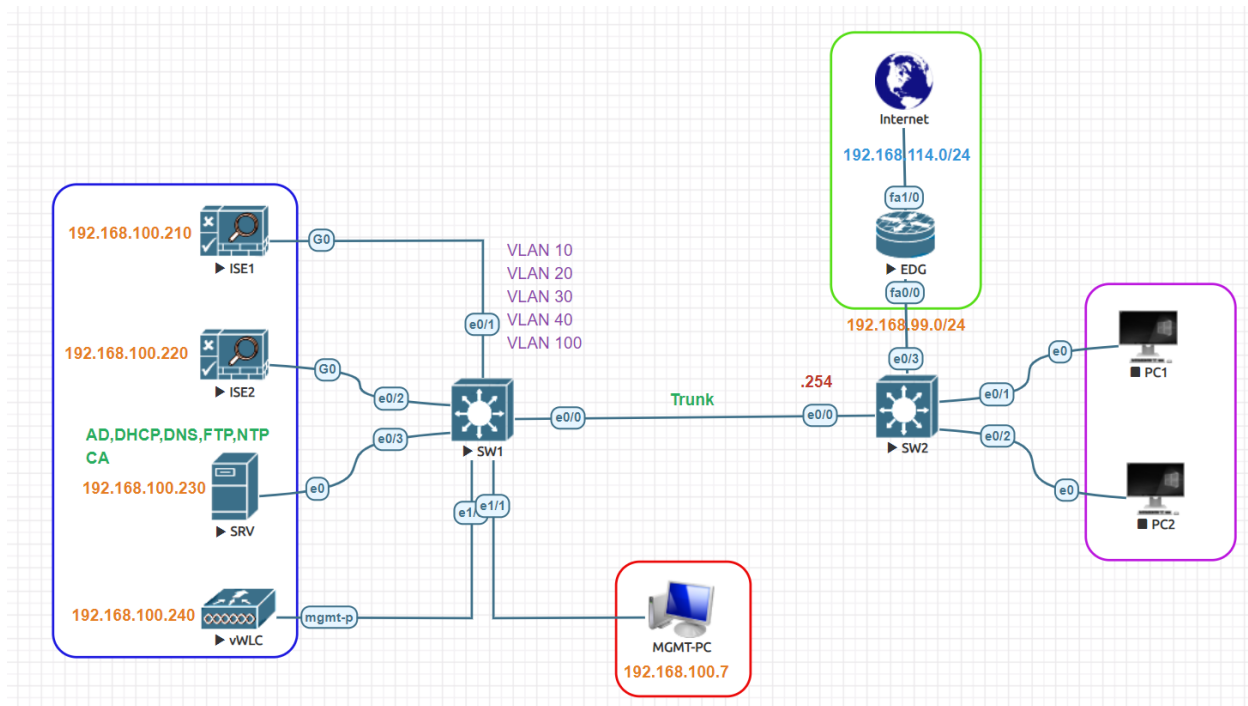


Hotspot Guest Access Lab:



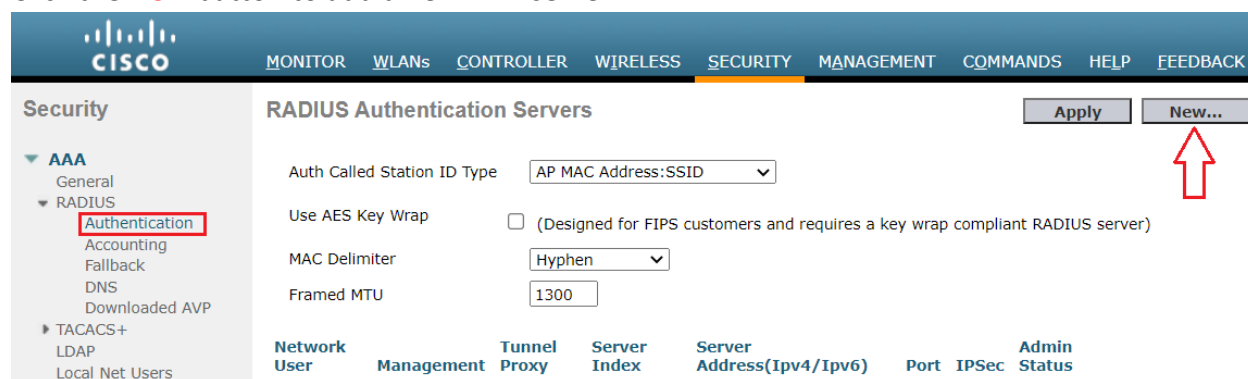
Cisco ISE Primary IP Address	192.168.100.210
Cisco ISE Secondary IP Address	192.168.100.220
AD, DHCP, DNS, FTP, NTP	192.168.100.230
CA Server IP Address	192.168.100.230
Domain Name	test.local
Test User/Group	Guest
Test VLAN	VLAN 40
VLAN Subnet	192.168.40.0/24
VLAN 20 Gateway	192.168.40.1
Authenticator 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:

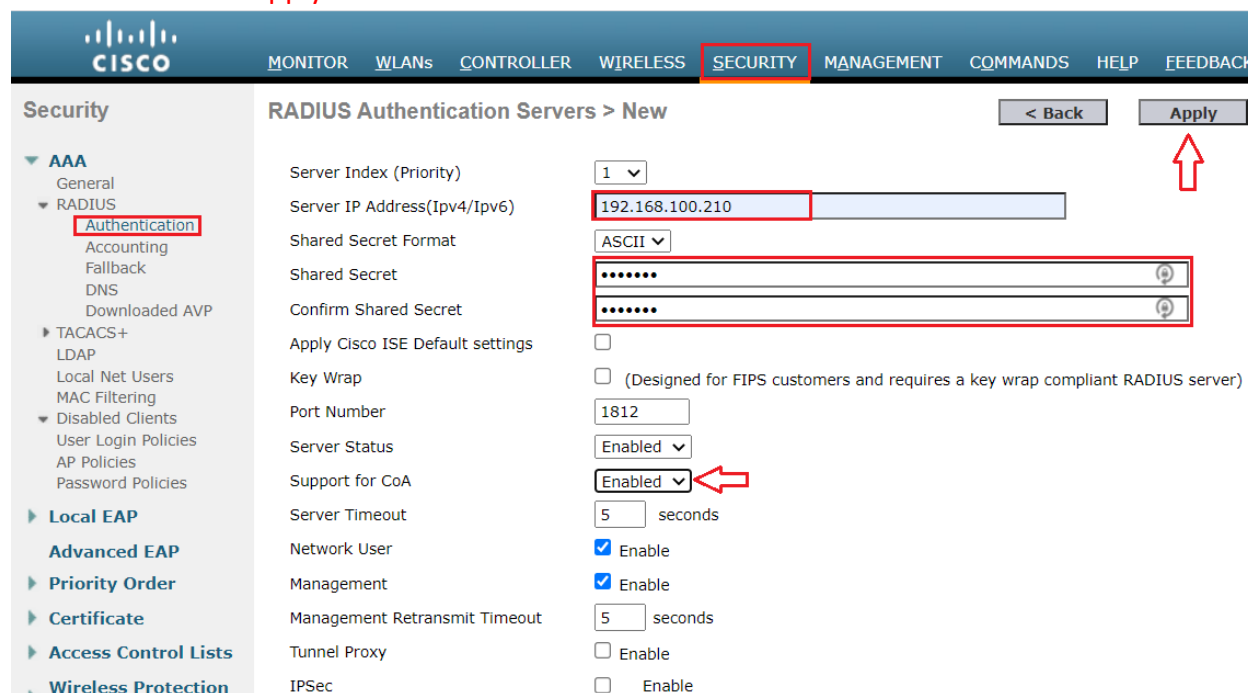
Log into the vWLC. Click the **security** tab at the top.



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**.

The screenshot shows the Cisco ISE interface with the 'SECURITY' tab selected. In the left sidebar, 'RADIUS' > 'Accounting' is selected. The main area is titled 'RADIUS Accounting Servers'. At the top right, there are 'Apply' and 'New...' buttons. A red arrow points to the 'New...' button.

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**

The screenshot shows the 'RADIUS Accounting Servers > New' configuration page. Fields for 'Server IP Address(Ipv4/Ipv6)' (192.168.100.210), 'Shared Secret', and 'Confirm Shared Secret' are highlighted with red boxes. The 'Apply' button at the top right is also highlighted with a red arrow.

RADIUS Authentication Servers

Auth Called Station ID Type:

Use AES Key Wrap: ☐ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

MAC Delimiter:

Framed MTU:

Network User	Management	Tunnel Proxy	Server Index	Server Address(Ipv4/Ipv6)	Port	IPSec	Admin Status
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1	*	192.168.100.210	1812	Disabled

RADIUS Accounting Servers

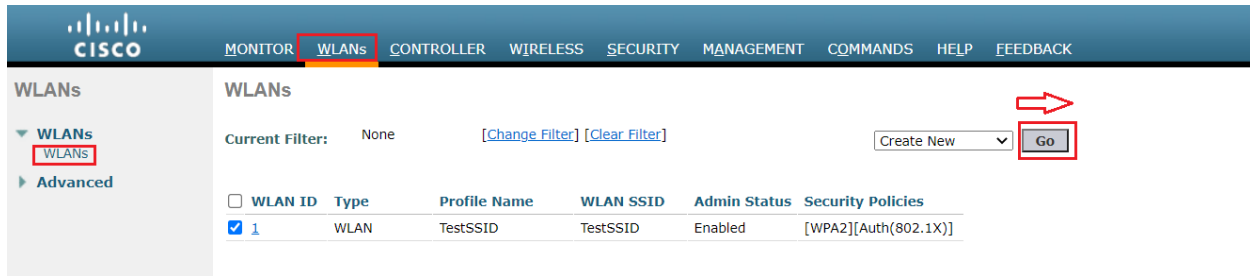
Acct Called Station ID Type:

MAC Delimiter:

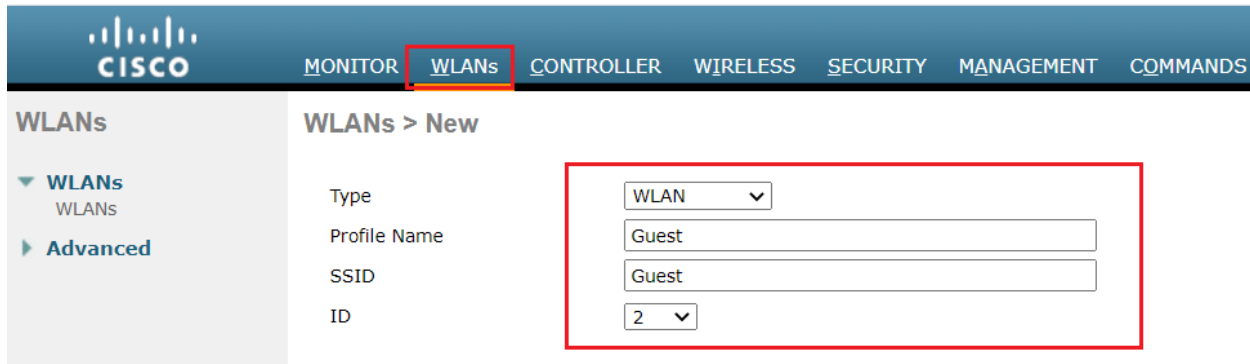
Network User	Tunnel Proxy	Server Index	Server Address(Ipv4/Ipv6)	Port	IPSec	Admin Status
<input checked="" type="checkbox"/>	<input type="checkbox"/>	1	*	192.168.100.210	1813	Disabled

Configuring Guest SSID:

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

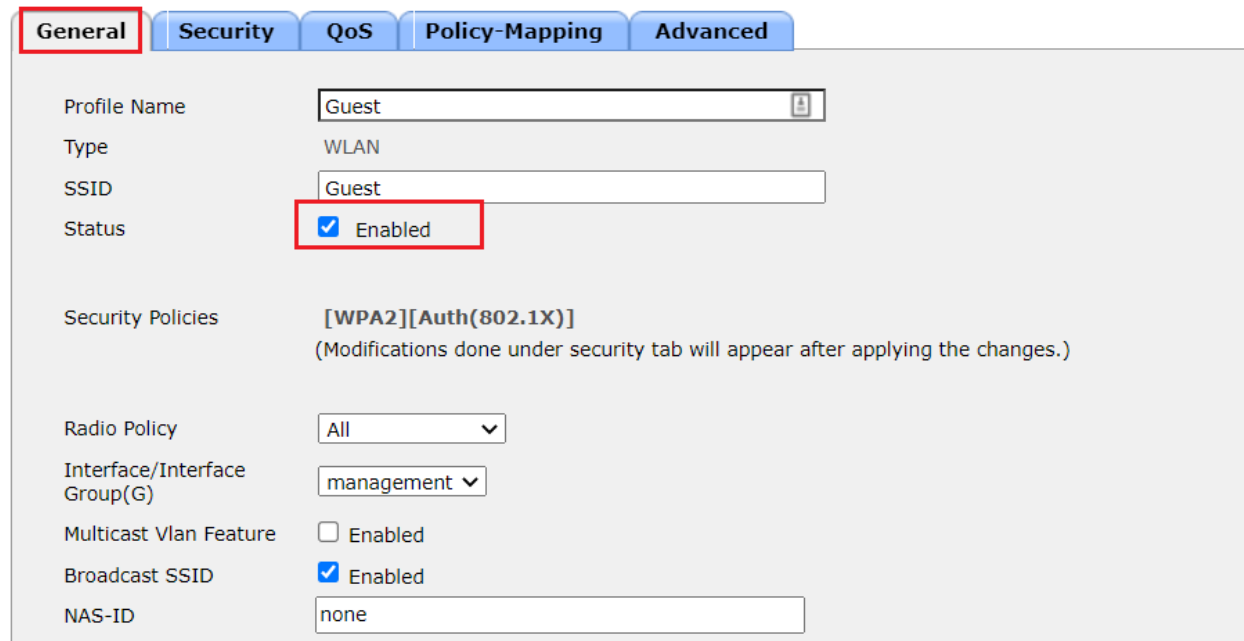


Choose **WLAN** for Type. Enter a **Profile Name** and a **WLAN SSID** of your choice, and click **Apply**.



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

WLANs > Edit 'Guest'




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

WLANs > Edit 'Guest'

General **Security** QoS Policy-Mapping Advanced

Layer 2 Layer 3 AAA Servers

Layer 2 Security ⁶ None

MAC Filtering⁹ ☒ 

Fast Transition

Fast Transition Adaptive

Over the DS ☒

Reassociation Timeout 20 Seconds

Lobby Admin Configuration

Lobby Admin Access ☐

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**.

WLANs > Edit 'Guest'

General **Security** QoS Policy-Mapping Advanced

Layer 2 Layer 3 **AAA Servers**


Select AAA servers below to override use of default servers on this WLAN

RADIUS Servers

RADIUS Server Overwrite interface ☐ Enabled

Apply Cisco ISE Default Settings ☒ Enabled

Authentication Servers		Accounting Servers	
<input checked="" type="checkbox"/> Enabled		<input checked="" type="checkbox"/> Enabled	
Server 1	IP:192.168.100.210, Port:1812	Server 1	IP:192.168.100.210, Port:1813
Server 2	None	Server 2	None
Server 3	None	Server 3	None
Server 4	None	Server 4	None
Server 5	None	Server 5	None
Server 6	None	Server 6	None



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 [48](#) ☐ Enabled

Override Interface ACL IPv4 IPv6

Layer2 Acl

URL ACL

P2P Blocking Action

Client Exclusion [3](#) ☒ Enabled 180
Timeout Value (secs)

Maximum Allowed Clients [8](#)

Static IP Tunneling [11](#) ☐ Enabled

Wi-Fi Direct Clients Policy

Maximum Allowed Clients Per AP Radio

DHCP

DHCP Server ☐ Override

DHCP Addr. Assignment ☒ Required

OEAP

Split Tunnel ☐ Enabled

Management Frame Protection (MFP)

MFP Client Protection [4](#)

DTIM Period (in beacon intervals)

802.11a/n (1 - 255)

802.11b/g/n (1 - 255)

NAC

NAC State

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**

On Channel Scanning Policy ☐ Enabled

Scan Defer Priority

Scan Defer Time(msecs)

FlexConnect

FlexConnect Local Switching [2](#) ☐ Enabled

FlexConnect Local Auth [12](#) ☐ Enabled

Learn Client IP Address [5](#) ☒ Enabled

Vlan based Central Switching [43](#) ☐ 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)

BSS Max Idle Service ☒

Directed Multicast Service ☒

Tunneling

Tunnel Profile

Finally, **Guest** SSID is configured.

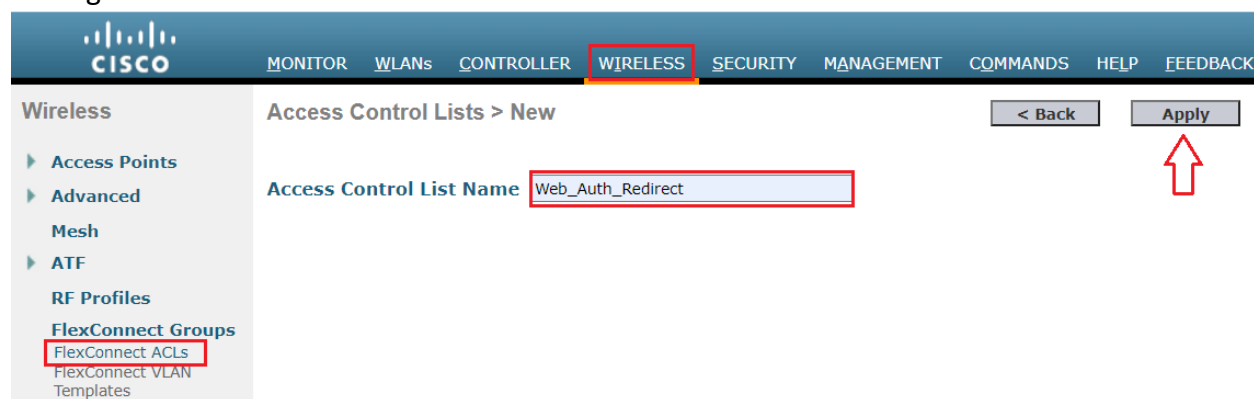
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK						
WLANs						
Current Filter: None [Change Filter] [Clear Filter] <input type="button" value="Create New"/> <input type="button" value="Go"/>						
<input type="checkbox"/> WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies	
<input type="checkbox"/> 1	WLAN	Employees	Employees	Enabled	[WPA2][Auth(802.1X)]	<input type="button" value="v"/>
<input type="checkbox"/> 2	WLAN	Guest	Guest	Enabled	MAC Filtering	<input type="button" value="v"/>

Configure ACLs:

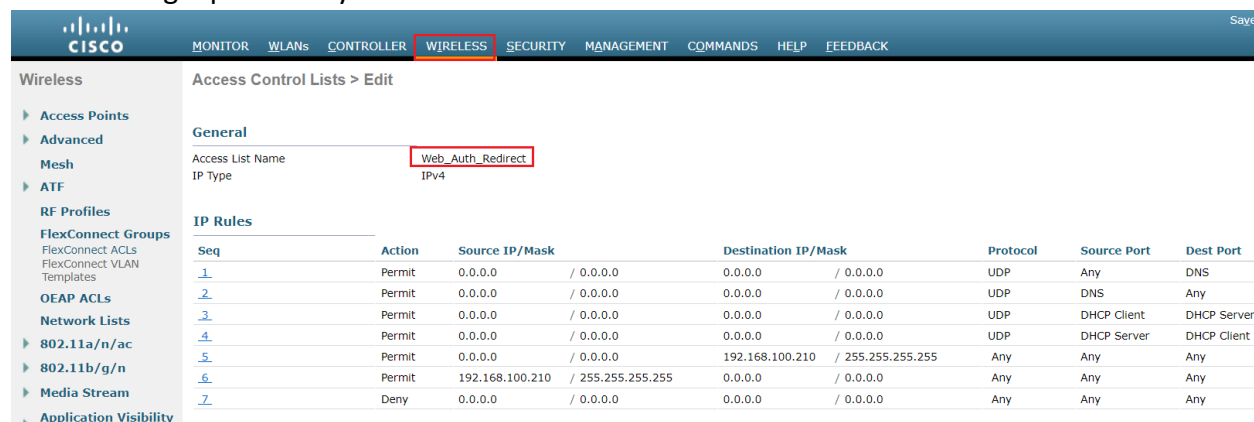
Next we have to create a few ACLs. One for Web Auth Redirect that will allow DNS and traffic to ISE and another ACL for restricting guest access. Go to **Wireless>FlexConnect ACLs** Click **New**.



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.



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.

Access Control Lists > New

Access Control List Name:

< Back Apply

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.

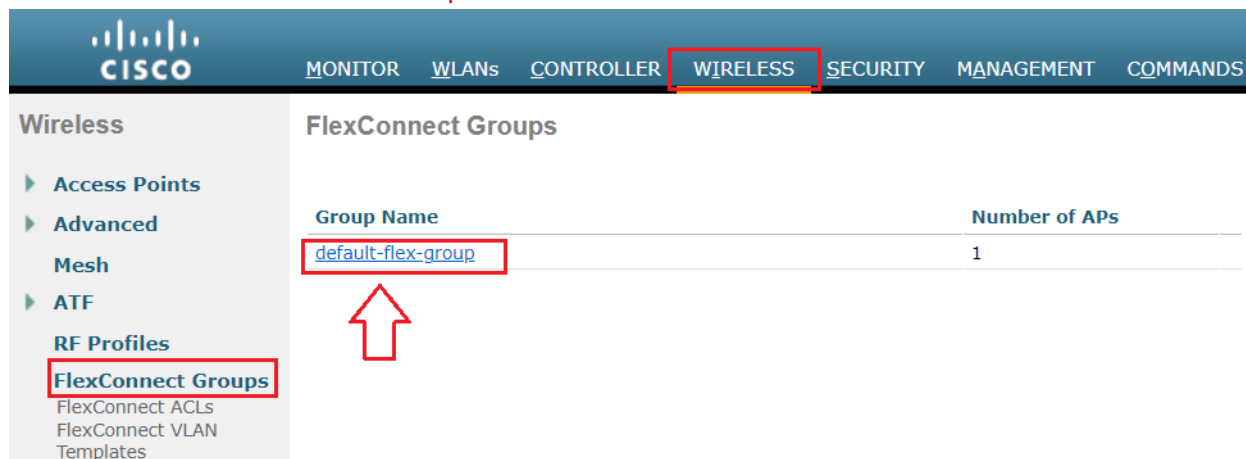
FlexConnect Access Control Lists

Acl Name

[Guest_ACL](#) ▼

[Web_Auth_Redirect](#) ▼

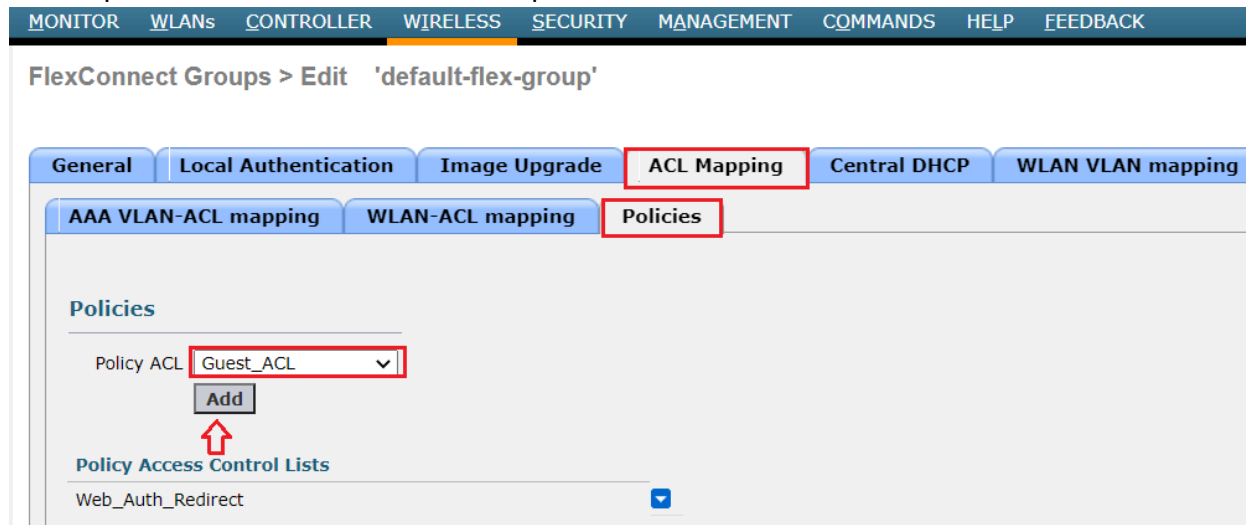
Go to **Wireless>FlexConnect Groups** click to edit.



The screenshot shows the Cisco Wireless configuration interface. The top navigation bar includes tabs for MONITOR, WLANs, CONTROLLER, WIRELESS (highlighted), SECURITY, MANAGEMENT, and COMMANDS. On the left, the 'Wireless' sidebar lists various configuration options, with 'FlexConnect Groups' highlighted. The main area, titled 'FlexConnect Groups', displays a table with two columns: 'Group Name' and 'Number of APs'. A single entry is shown: 'default-flex-group' with '1' AP. A red box highlights the 'default-flex-group' link, and a red arrow points to it.

Group Name	Number of APs
default-flex-group	1

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.



The screenshot shows the 'FlexConnect Groups > Edit 'default-flex-group'' configuration page. The 'ACL Mapping' tab is selected. Under the 'Policies' section, the 'Policy ACL' dropdown is set to 'Guest_ACL'. An 'Add' button is located below the dropdown. A red box highlights the 'Add' button, and a red arrow points to it. Below the 'Add' button, the 'Policy Access Control Lists' section shows 'Web_Auth_Redirect' with a checkmark icon.

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**

The screenshot shows the Cisco WLC GUI with the 'CONTROLLER' tab selected. In the 'General' configuration section, the 'Fast SSID change' option is highlighted with a red box and set to 'Enabled'. An 'Apply' button is highlighted with a red arrow.

Configuration Item	Value
Name	WLC
802.3x Flow Control Mode	Disabled
Broadcast Forwarding	Disabled
AP Multicast Mode	Unicast
AP IPv6 Multicast Mode	Unicast
AP Fallback	Enabled
CAPWAP Preferred Mode	ipv4
Fast SSID change	Enabled
Link Local Bridging	Disabled

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

The screenshot shows the Cisco WLC GUI with the 'CONTROLLER' tab selected. In the 'Advanced' configuration section, the 'DHCP' sub-tab is selected. The 'Enable DHCP Proxy' checkbox is highlighted with a red box and is unchecked. An 'Apply' button is highlighted with a red arrow.

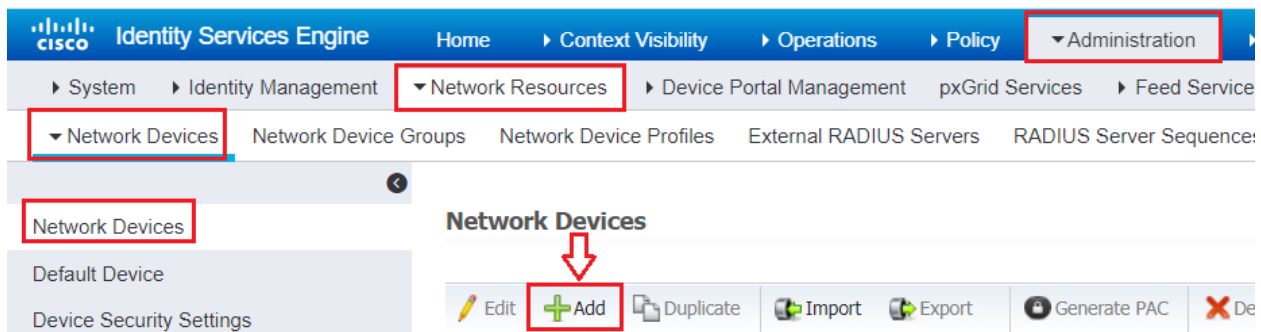
Configuration Item	Value
Enable DHCP Proxy	<input type="checkbox"/>
DHCP Option 82 Format	binary
DHCP Option 82 Remote Id field format	AP-MAC
DHCP Timeout (5 - 120 seconds)	120

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.

The screenshot shows the 'New Network Device' form in the Cisco ISE Administration console. The form fields are: Name (VWLC), Description (Virtual WLC), IP Address (192.168.100.240), Device Profile (Cisco), Model Name, Software Version, Network Device Group, Location (All Locations), IPSEC (Is IPSEC Device), and Device Type (All Device Types). The 'Add' button is highlighted with a red arrow. The left sidebar shows 'Network Devices' with options like 'Default Device' and 'Device Security Settings'. The top navigation bar shows 'Administration' and 'Network Resources'.

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**.

The screenshot shows the Cisco Identity Services Engine (ISE) navigation menu. The 'Work Centers' tab is selected. Under 'Guest Access', 'Policy Elements' is highlighted. Other categories like Network Access, TrustSec, Profiler, Device Administration, BYOD, and PassiveID are also visible.

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

The screenshot shows the 'Standard Authorization Profiles' page in Cisco ISE. The 'Add' button is highlighted. Below it, a table lists existing profiles:

<input type="checkbox"/>	Name	Profile
<input type="checkbox"/>	Authorization_Contractor	Cisco
<input type="checkbox"/>	Authorization_EasyConnect	Cisco
<input type="checkbox"/>	Authorization_Employees	Cisco
<input type="checkbox"/>	Authorization_Machine	Cisco

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**.

[Authorization Profiles](#) > [New Authorization Profile](#)

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Service Template ☐

Track Movement ☐

Passive Identity Tracking ☐

Common Tasks

VOICE Domain Permission

☒ Web Redirection (CWA, MDM, NSP, CPP) ACL Value

☒ Static IP/Host name/FQDN

☐ Suppress Profiler CoA for endpoints in Logical Profile

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

Advanced Attributes Settings

Select an item =

Attributes Details

Access Type = ACCESS_ACCEPT
cisco-av-pair = url-redirect-acl=Web_Auth_Redirect
cisco-av-pair = url-redirect=https://192.168.100.210:port/portal/gateway?sessionId=SessionIdValue&portal=f9b94c2f-a3fc-4154-acbb-d4c4fbed899d&action=cwa&type=drw

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**.

[Authorization Profiles](#) > [New Authorization Profile](#)

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Service Template ☐

Track Movement ☐

Passive Identity Tracking ☐

Common Tasks

☐ Interface Template

☐ Web Authentication (Local Web Auth)

☒ Airespace ACL Name

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

Advanced Attributes Settings

Select an item =

Attributes Details

Access Type = ACCESS_ACCEPT
Airespace-ACL-Name = Guest_ACL

Create Policy Set:

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

The screenshot shows the Cisco Identity Services Engine (ISE) navigation menu. The 'Work Centers' dropdown is highlighted. Under 'Guest Access', 'Policy Sets' is highlighted. Other categories like Network Access, TrustSec, Profiler, Device Administration, and PassiveID are also visible.

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

Policy Sets

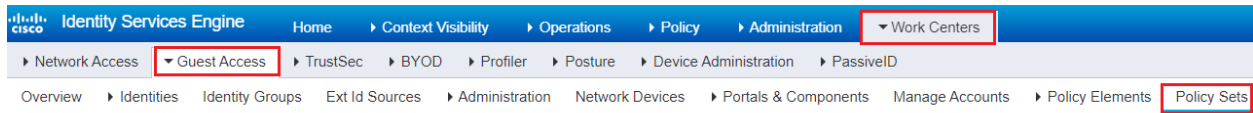
The screenshot shows the 'Policy Sets' table in the ISE GUI. A red box highlights the plus (+) icon in the upper-left corner of the table header. A red arrow points to the 'Search' input field below the table header.

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

The screenshot shows the 'Policy Sets' table in the ISE GUI. A new policy set named 'Guest-Hotspot' is added. The 'Conditions' column shows 'Wireless_MAB' and the 'Allowed Protocols / Server Sequence' column shows 'Default Network Access'. A red box highlights the new entry.

Authentication Policy:

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



Policy Sets

+	Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence
Search					
		Guest-Hotspot	Guest Hotspot	Wireless_MAB	Default Network Access x

Create new Authentication policy click by **plus** circle name rule.

▼ Authentication Policy (1)			
+	Status	Rule Name	Conditions
Search			


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**.

▼ Authentication Policy (1)				
+	Status	Rule Name	Conditions	Use
Search				
		Guest-Auth	OR Wired_MAB Wireless_MAB	<div>Internal Endpoints x </div> <div>▼ Options</div> <div>If Auth fail REJECT x </div> <div>If User not found CONTINUE x </div> <div>If Process fail DROP x </div>
		Default		<div>DenyAccess x </div> <div>► Options</div>

Authorization Policy:





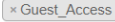

Next we'll create our new Authorization Policies for the Guest network. Expand Authorization Policy.

▼ Authorization Policy (14)









	Status	Rule Name	Conditions
			
<input type="text" value="Search"/>			

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





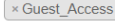




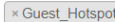




▼ Authorization Policy (1)

	Status	Rule Name	Conditions	Results
				Profiles
<input type="text" value="Search"/>				
		Guest-Access	AND  Wireless_MAB  IdentityGroup Name EQUALS Endpoint Identity Groups:GuestEndpoints	 

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.

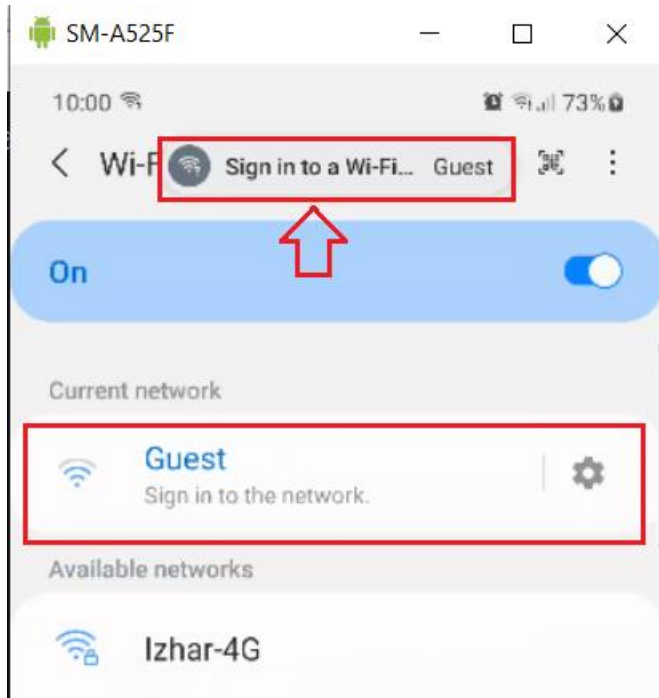
		Guest-Redirect	 Wireless_MAB	 
		Default		 

▼ Authorization Policy (1)

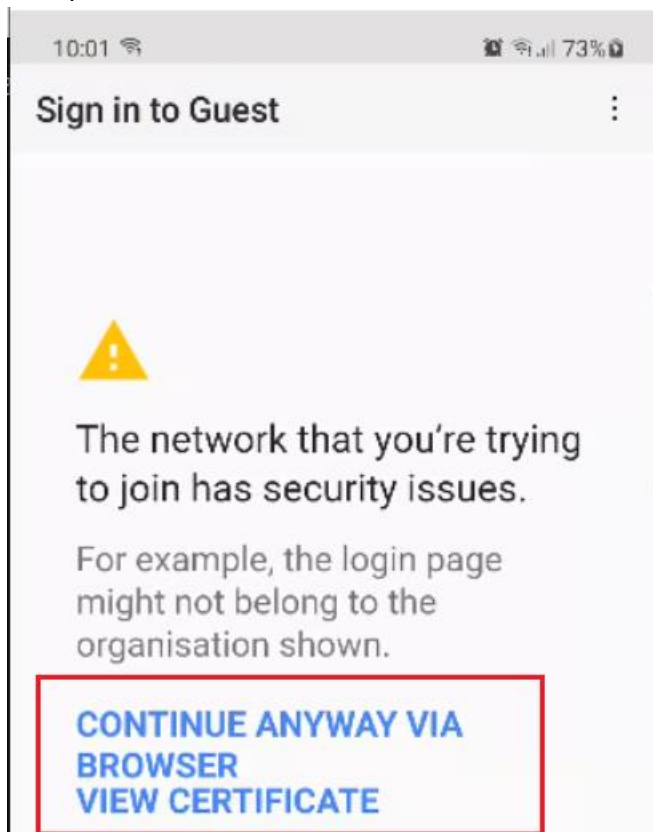
	Status	Rule Name	Conditions	Results
				Profiles
<input type="text" value="Search"/>				
		Guest-Access	AND  Wireless_MAB  IdentityGroup Name EQUALS Endpoint Identity Groups:GuestEndpoints	 
		Guest-Redirect	 Wireless_MAB	 
		Default		 

Testing and Verification:

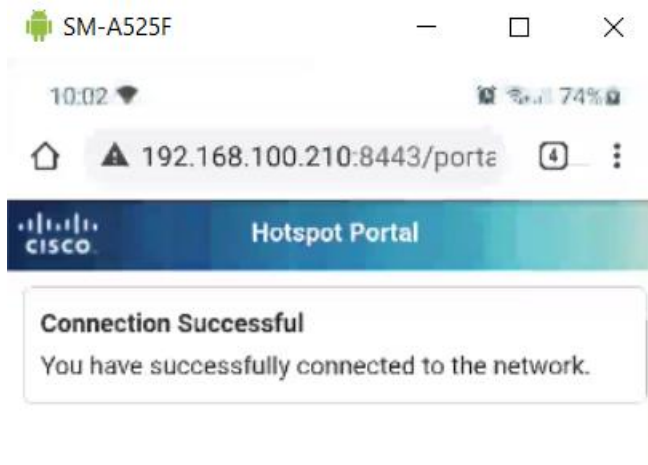
Connect to Guest Network in your mobile phone it will redirect to Guest Portal.



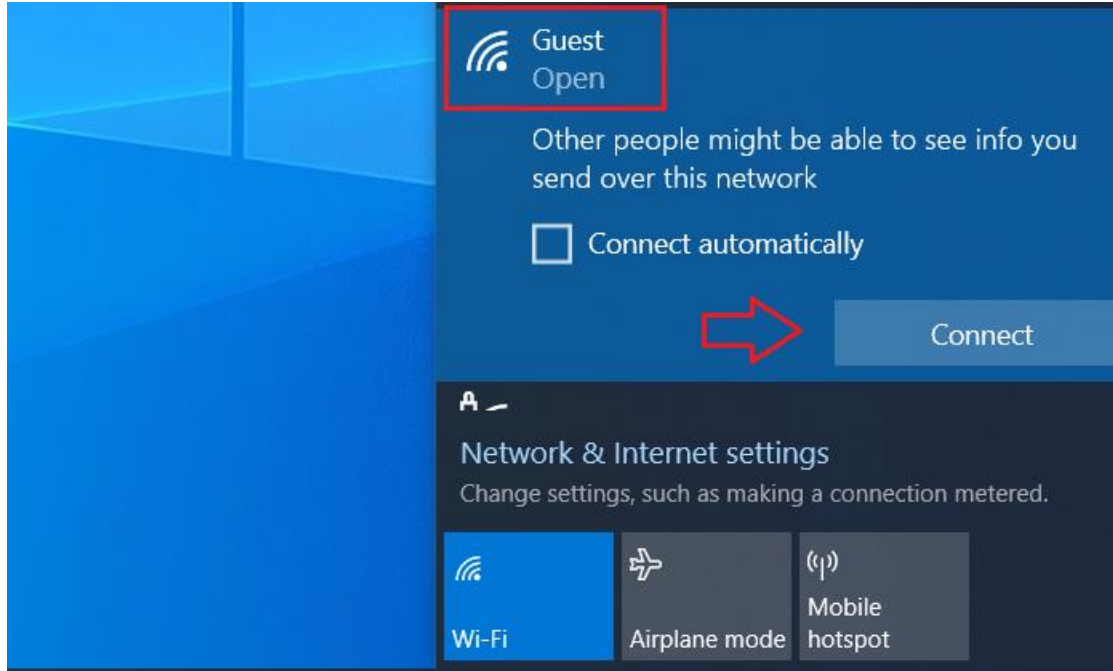
Accept the Certificate error to continue in real world we need to use public certificate.



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**.

🔒 <https://192.168.100.210:8443/portal/PortalSetup.action?portal=f9b94c2f-a3fc-4154-acbb-d4c4fbed899d&sessionId=f064a8c0000000124bc333c> ☆


You can access the Internet. [Open network login page](#)

 Hotspot Portal

Acceptable Use Policy

Please read the Acceptable Use Policy.


Please accept the policy: You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password. Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending unsolicited bulk e-mail, collection of other people's personal data without their knowledge and interference with other network users are all prohibited. Cisco Systems reserves the right to suspend the Service if Cisco Systems reasonably believes that your use of the Service is unreasonably excessive or you are using the Service for criminal or illegal activities. You do not have the right to resell this Service to a third party. Cisco Systems reserves the right to revise, amend or modify these Terms & Conditions, our other policies and agreements, and aspects of the Service itself. Notice of any revision, amendment, or modification will be posted on Cisco System's website and will be effective as to existing users 30 days after



Connection Successful message display now can use internet.

🔒 <https://192.168.100.210:8443/portal/AupSubmit.action?from=AUP>









You can access the Internet. [Open network login page](#)

 Hotspot Portal

Connection Successful

You have successfully connected to the network.

 Refresh
  Reset Repeat Counts
  Export To

Time	Status	Details	Repeat ...	Identity	Endpoint ID
x				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	Authentication	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