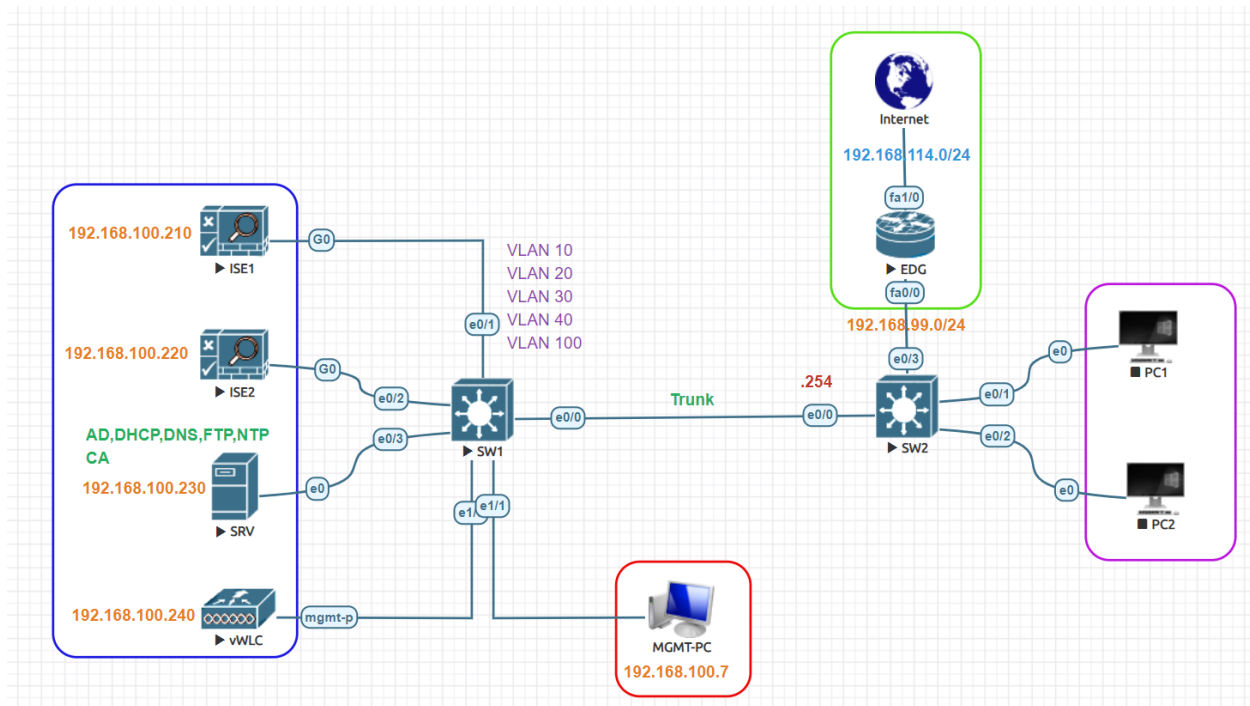


Central Web Authentication (CWA) Lab:



Cisco ISE Primary IP Address	192.168.100.210
Cisco ISE Secondary IP Address	192.168.100.220
AD,DHCP,DNS,FTP,NTP CA	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	Guest Portal

Configure RADIUS on WLC:

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

The screenshot shows the Cisco vWLC interface with the **WIRELESS** tab selected in the top navigation bar. The left sidebar shows the **Wireless** section with **Access Points** expanded, listing **All APs**, **Radios**, and specific radio models. The main content area displays **All APs** with a **Current Filter** of *None* and a **Number of APs** of 1. A red box highlights the **WIRELESS** tab in the top navigation bar.

Click the **New** button to add a new AAA server.

The screenshot shows the Cisco vWLC interface with the **SECURITY** tab selected. The left sidebar shows the **Security** section with **AAA** expanded, and **RADIUS** expanded, with **Authentication** highlighted. The main content area displays **RADIUS Authentication Servers** with a **New...** button highlighted by a red arrow. The configuration fields include **Auth Called Station ID Type** (AP MAC Address:SSID), **Use AES Key Wrap** (unchecked), **MAC Delimiter** (Hyphen), and **Framed MTU** (1300). A table at the bottom lists columns for **Network User**, **Management**, **Tunnel Proxy**, **Server Index**, **Server Address(Ipv4/Ipv6)**, **Port**, **IPSec**, and **Admin Status**.

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**.

The screenshot shows the Cisco vWLC interface with the **SECURITY** tab selected. The left sidebar shows the **Security** section with **AAA** expanded, and **RADIUS** expanded, with **Authentication** highlighted. The main content area displays **RADIUS Authentication Servers > New** with a **Apply** button highlighted by a red arrow. The configuration fields include **Server Index (Priority)** (1), **Server IP Address(Ipv4/Ipv6)** (192.168.100.210), **Shared Secret Format** (ASCII), **Shared Secret** (masked), **Confirm Shared Secret** (masked), **Apply Cisco ISE Default settings** (unchecked), **Key Wrap** (unchecked), **Port Number** (1812), **Server Status** (Enabled), **Support for CoA** (Enabled, highlighted by a red arrow), **Server Timeout** (5 seconds), **Network User** (checked), **Management** (checked), **Management Retransmit Timeout** (5 seconds), **Tunnel Proxy** (unchecked), and **IPSec** (unchecked).

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' and contains an 'Apply' button and a 'New...' button. 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 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

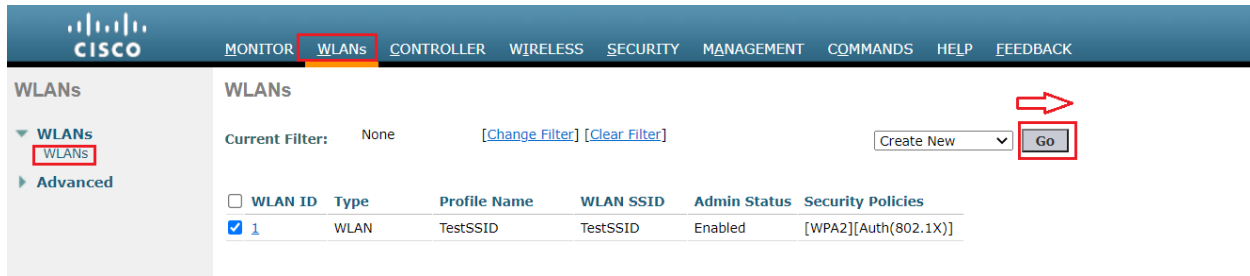
Acct Called Station ID Type:

MAC Delimiter:

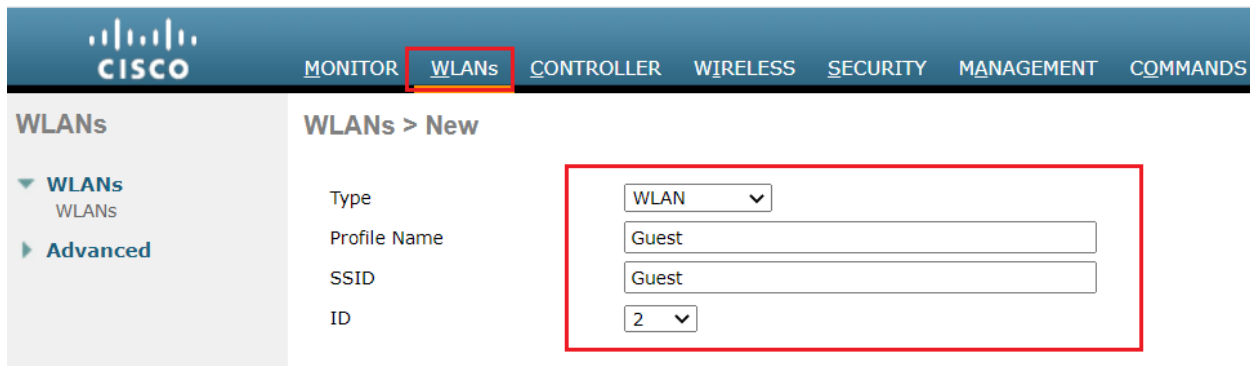
Network User	Tunnel Proxy	Server Index	Server Address(Ipv4/Ipv6)	Port	IPSec	Admin Status
<input checked="" type="checkbox"/>	<input type="checkbox"/>	1	*	192.168.100.210	1813	Disabled

Configuring Guest SSID:

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

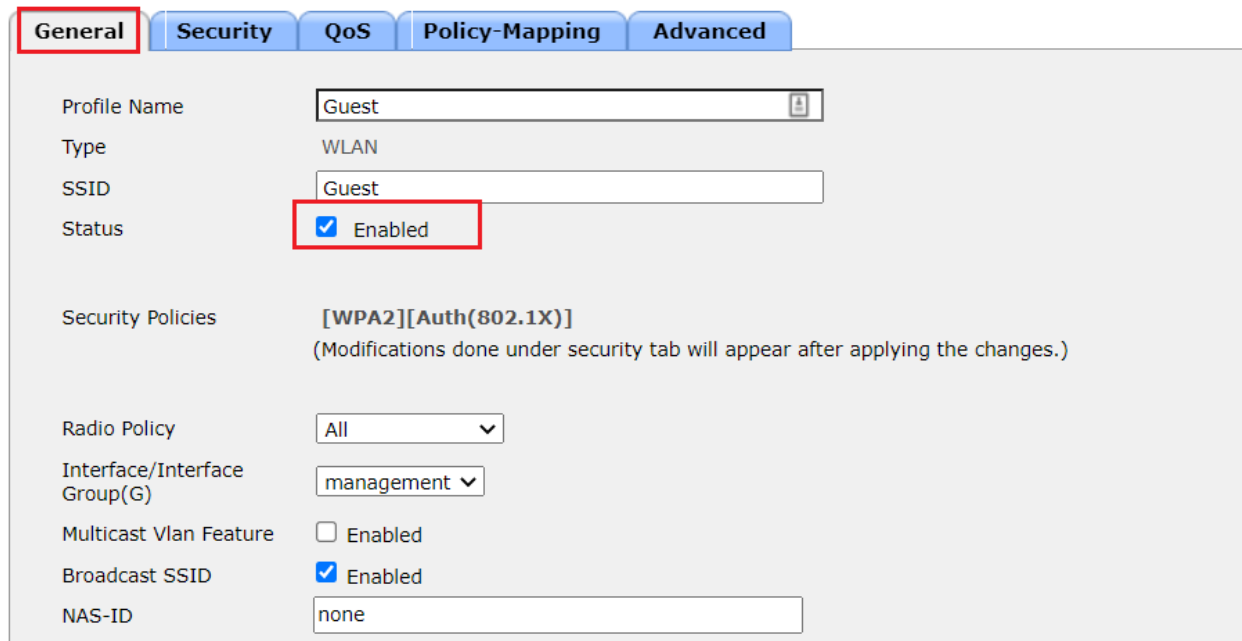


Choose **WLAN** for Type. Enter a **Profile Name** and a **WLAN SSID** of your choice, and click **Apply**.



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 Over the DS ☒ Adaptive

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.

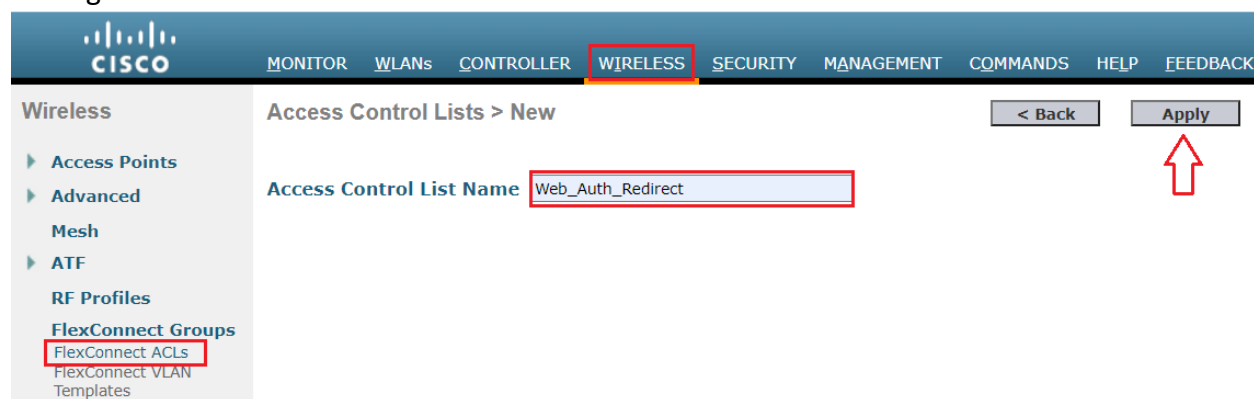
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK						
WLANs						
Current Filter: None [Change Filter] [Clear Filter] <input type="button" value="Create New"/> <input type="button" value="Go"/>						
<input type="checkbox"/> WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	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:

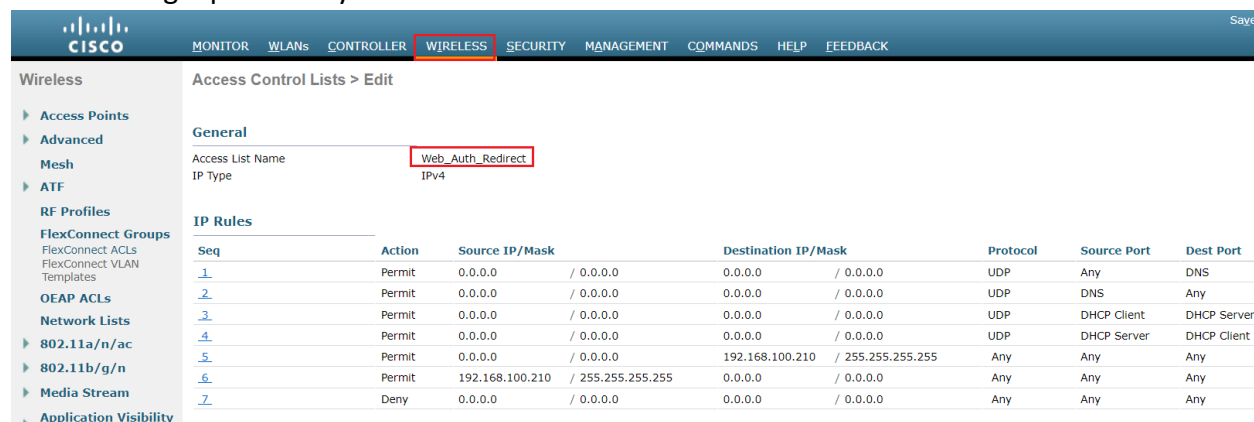
Next we have to create a few ACLs. One for Web Auth Redirect that will allow DNS and traffic to ISE and another ACL for restricting guest access. Go to **Wireless>FlexConnect ACLs** Click **New**.



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.



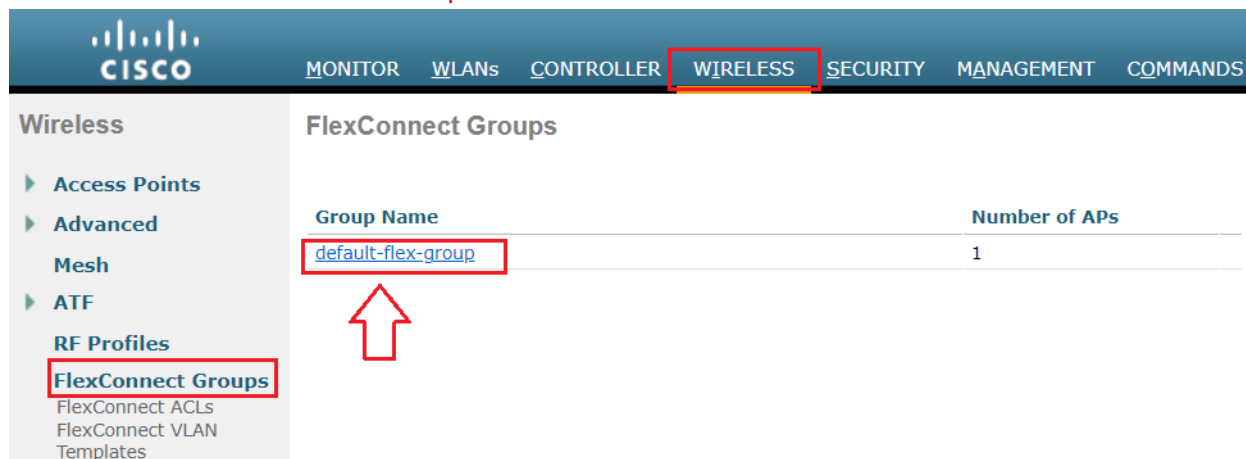
Create a new ACL if you'd like to place any restrictions on your guest network such as blocking access to any of your private IP or internal Network space.

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.

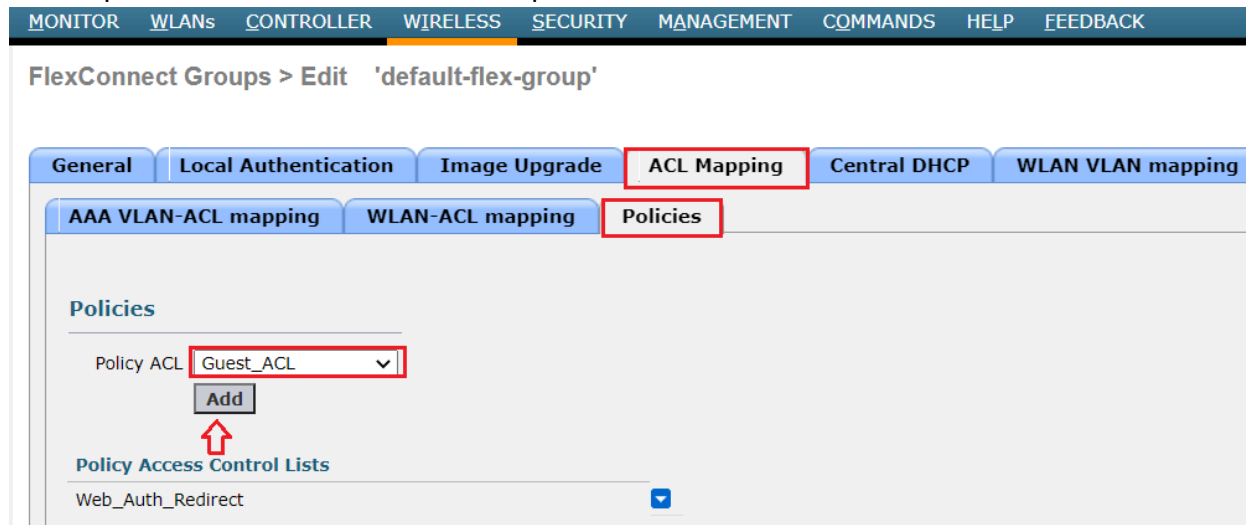


The screenshot shows the Cisco Wireless configuration interface. The top navigation bar includes tabs for MONITOR, WLANs, CONTROLLER, WIRELESS (highlighted), SECURITY, MANAGEMENT, and COMMANDS. On the left, the 'Wireless' sidebar lists various configuration options, with 'FlexConnect Groups' highlighted. The main area displays a table of FlexConnect Groups:

Group Name	Number of APs
default-flex-group	1

A red arrow points to the 'default-flex-group' link in the table.

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 visible below the dropdown. A red arrow points to the 'Add' button. Below the 'Add' button, the 'Policy Access Control Lists' section shows 'Web_Auth_Redirect' selected with a checkmark.

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. The 'General' configuration page is displayed. 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. The 'Advanced' configuration page is displayed, and the 'DHCP' sub-tab is selected. The 'Enable DHCP Proxy' checkbox is unchecked and highlighted with a red box. An 'Apply' button is highlighted with a red arrow.

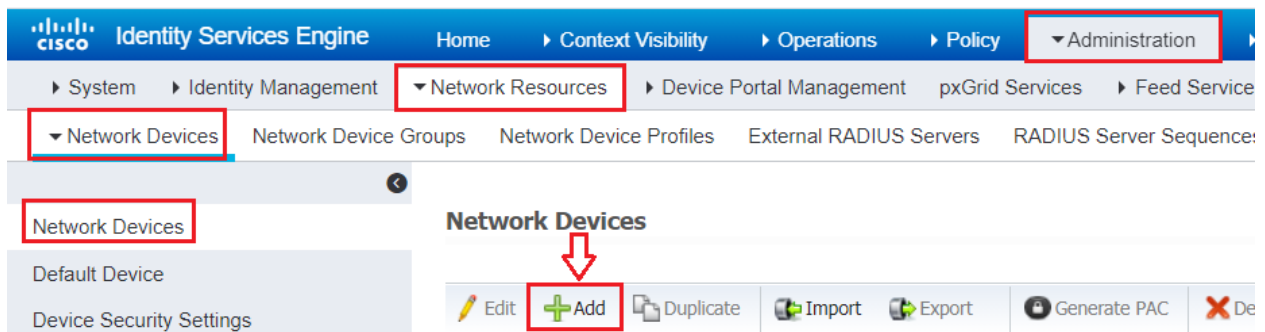
Configuration Item	Value
Enable DHCP Proxy	<input type="checkbox"/>
DHCP Option 82 Format	binary
DHCP Option 82 Remote Id field format	AP-MAC
DHCP Timeout (5 - 120 seconds)	120

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 (vWLC).



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: [Empty]
- Software Version: [Empty]
- * Network Device Group: [Empty]
- Location: All Locations
- Is IPSEC Device: Is IPSEC Device
- Device Type: All Device Types

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) interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The 'Work Centers' dropdown is expanded, showing several categories: Network Access, TrustSec, Profiler, Device Administration, BYOD, and PassiveID. Each category has a list of sub-items. The 'Guest Access' category is highlighted, and within it, 'Policy Elements' is selected. Other categories like Network Access, TrustSec, Profiler, Device Administration, BYOD, and PassiveID are also visible with their respective sub-items.

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 page title is 'Standard Authorization Profiles' and it includes a subtitle: 'For Policy Export go to Administration > System > Backup & Restore > Policy Export Page'. On the left sidebar, the 'Results' section is expanded, and 'Authorization Profiles' is selected. The main content area shows a table of existing authorization profiles. The 'Add' button is highlighted. The table has columns for 'Name' and 'Profile'. The existing profiles are: Authorization_Contractor, Authorization_EasyConnect, Authorization_Employees, and Authorization_Machine, all associated with the 'Cisco' profile.

Name	Profile
Authorization_Contractor	Cisco
Authorization_EasyConnect	Cisco
Authorization_Employees	Cisco
Authorization_Machine	Cisco

Scroll down to the **Common Tasks** and check Web Redirection. Select **Centralized Web Auth** from the drop down. Enter **Web_Auth_Redirect** as the ACL and the value will be the **Self-Registered Guest Portal**.

[Authorization Profiles](#) > [Guest_Hotspot](#)

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Service Template ☐

Track Movement ☐

Passive Identity Tracking ☐

Common Tasks

ACL Value

☒ Display Certificates Renewal Message

☒ Static IP/Host name/FQDN

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 expanded, showing the following categories and their sub-items:

- Network Access**
 - Overview
 - Identities
 - Id Groups
 - Ext Id Sources
 - Network Resources
 - Policy Elements
 - Policy Sets
 - Troubleshoot
 - Reports
 - Settings
 - Dictionaries
- Guest Access** (highlighted with a red box)
 - Overview
 - Identities
 - Identity Groups
 - Ext Id Sources
 - Administration
 - Network Devices
 - Portals & Components
 - Manage Accounts
 - Policy Elements
 - Policy Sets** (highlighted with a red box)
 - Reports
- TrustSec**
 - Overview
 - Components
 - TrustSec Policy
 - Policy Sets
 - SXP
 - Troubleshoot
 - Reports
 - Settings
- BYOD**
 - Overview
 - Identities
 - Identity Groups
 - Network Devices
 - Ext Id Sources
 - Client Provisioning
 - Portals & Components
 - Policy Elements
 - Policy Sets
 - Reports
 - Custom Portal Files
 - Settings
- Profiler**
 - Overview
 - Ext Id Sources
 - Network Devices
 - Endpoint Classification
 - Node Config
 - Feeds
 - Manual Scans
 - Policy Elements
 - Profiling Policies
 - Policy Sets
 - Troubleshoot
 - Reports
 - Settings
 - Dictionaries
- Posture**
 - Overview
 - Network Devices
 - Client Provisioning
 - Policy Elements
 - Posture Policy
 - Policy Sets
 - Troubleshoot
 - Reports
- Device Administration**
 - Overview
 - Identities
 - User Identity Groups
 - Ext Id Sources
 - Network Resources
 - Policy Elements
 - Device Admin Policy Sets
 - Reports
 - Settings
- PassiveID**
 - Overview
 - Providers
 - Subscribers
 - Certificates
 - Troubleshoot
 - Reports

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

Policy Sets

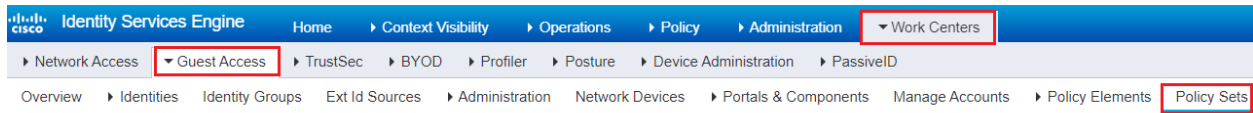
The screenshot shows the 'Policy Sets' table in the ISE GUI. The table has the following columns: Status, Policy Set Name, Description, and Conditions. A red box highlights the plus (+) icon in the upper-left corner of the table, and a red arrow points to the 'Search' input field below it.

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. The table has the following columns: Status, Policy Set Name, Description, Conditions, and Allowed Protocols / Server Sequence. A new policy set 'Guest-Hotspot' is added with a green checkmark icon. The 'Conditions' column shows 'Wireless_MAB' and the 'Allowed Protocols / Server Sequence' column shows 'Default Network Access'.

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"/>			

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





▼ Authorization Policy (3)

	Status	Rule Name	Conditions	Results	Profiles
					
<input type="text" value="Search"/>					
	Guest-Access	AND	<div>Wireless_MAB</div> <div>Guest_Flow</div>	<div>× Guest_Access</div>	

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

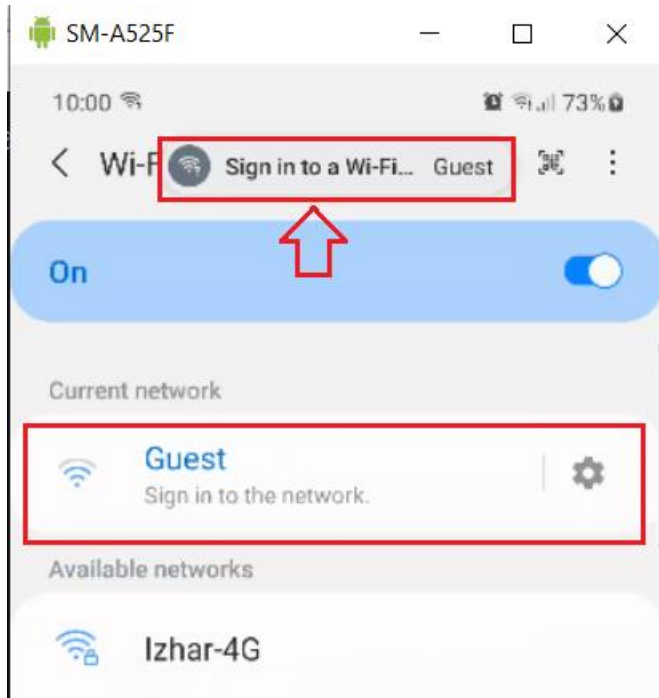
	Guest-Redirect	<div>Wireless_MAB</div>	<div>× Guest_Hotspot</div>
	Default		<div>× DenyAccess</div>

▼ Authorization Policy (3)

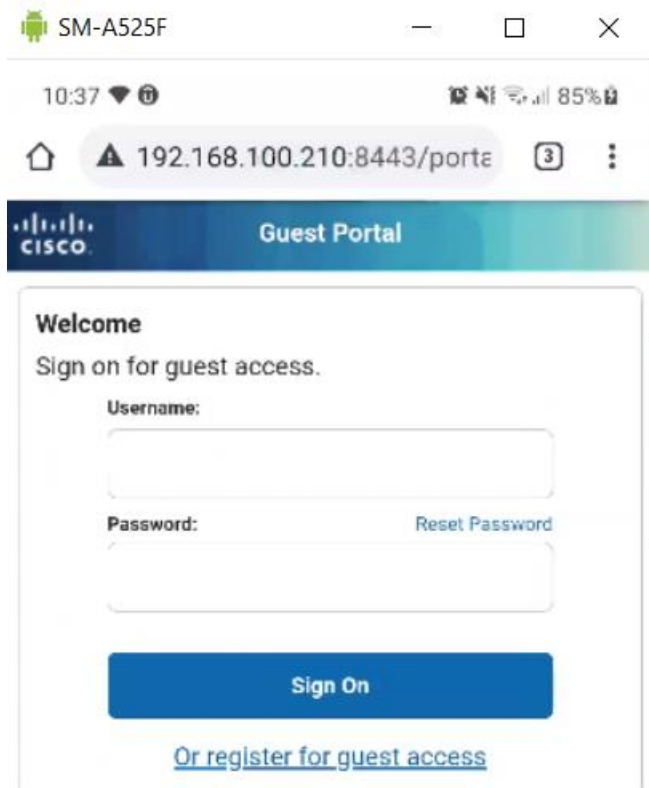
	Status	Rule Name	Conditions	Results	Profiles
					
<input type="text" value="Search"/>					
	Guest-Access	AND	<div>Wireless_MAB</div> <div>Guest_Flow</div>	<div>× Guest_Access</div>	
	Guest-Redirect	<div>Wireless_MAB</div>	<div>× Guest_Hotspot</div>		
	Default		<div>× DenyAccess</div>		

Testing and Verification:

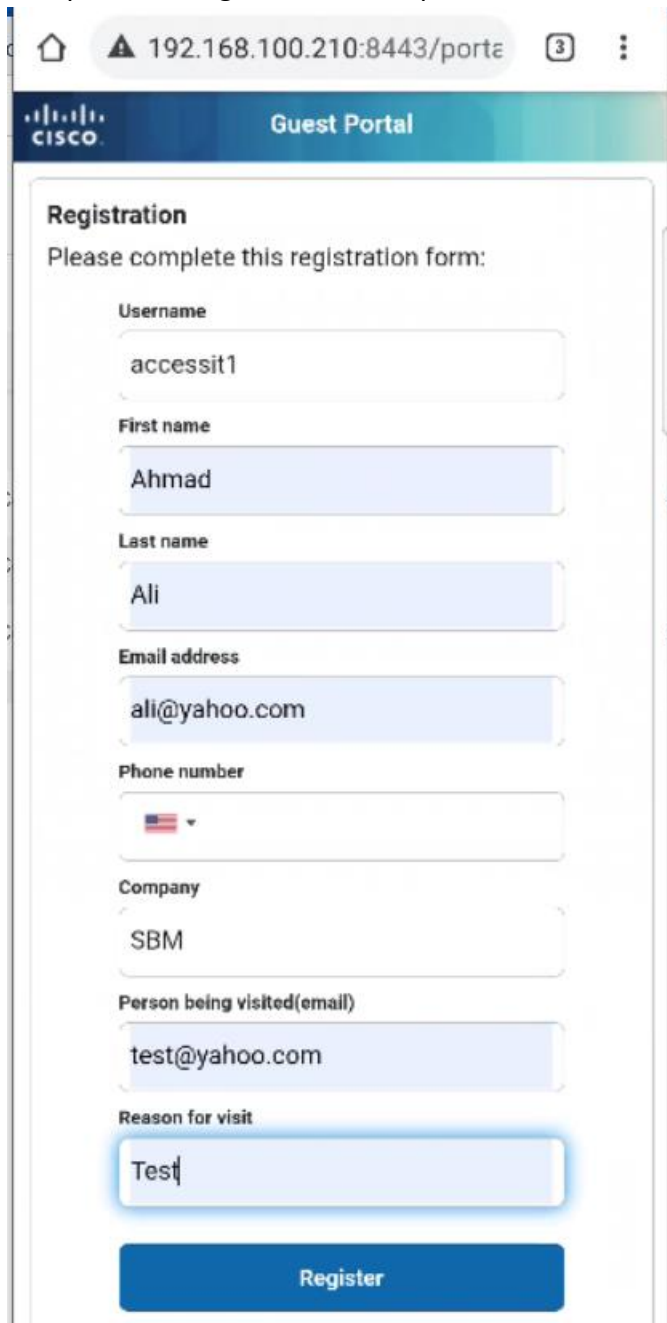
Connect to Guest Network in your mobile phone it will redirect to Self-Registered Guest Portal.



Click on [or register for guest access](#)



Complete the registration form provide the information and click **Register**.



The image shows a web browser window displaying a Cisco Guest Portal registration form. The browser's address bar shows the URL 192.168.100.210:8443/portal. The page has a blue header with the Cisco logo and the text "Guest Portal". The main content area is titled "Registration" and contains the instruction "Please complete this registration form:". Below this, there are several input fields, each with a label above it: "Username" (containing "accessit1"), "First name" (containing "Ahmad"), "Last name" (containing "Ali"), "Email address" (containing "ali@yahoo.com"), "Phone number" (with a dropdown menu showing a US flag), "Company" (containing "SBM"), "Person being visited(email)" (containing "test@yahoo.com"), and "Reason for visit" (containing "Test"). At the bottom of the form is a blue button labeled "Register".

Registration

Please complete this registration form:

Username
accessit1

First name
Ahmad

Last name
Ali

Email address
ali@yahoo.com

Phone number
US

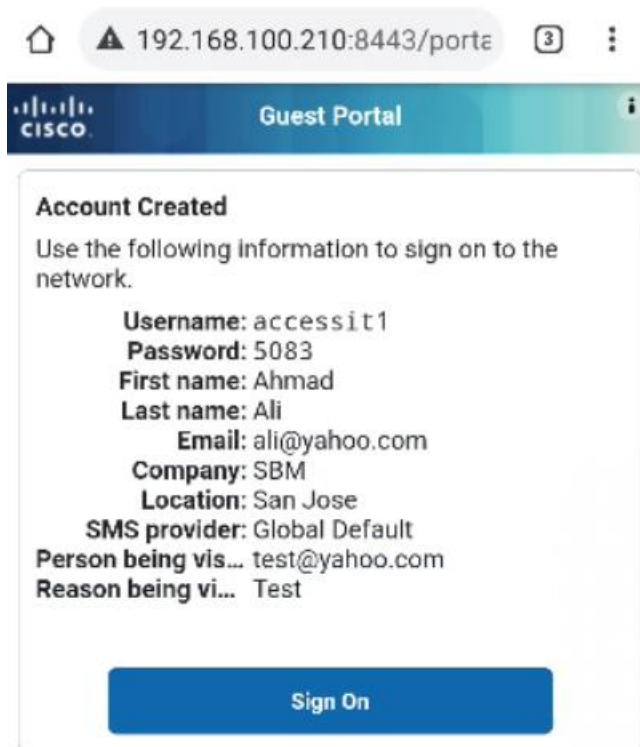
Company
SBM

Person being visited(email)
test@yahoo.com

Reason for visit
Test

Register

Guest Portal Account is created and will show Username and Password.

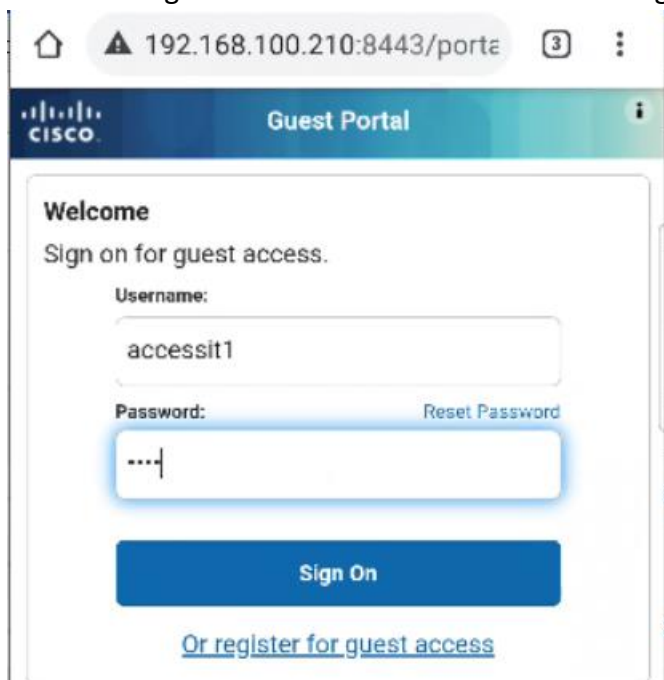


The screenshot shows the Cisco Guest Portal interface. At the top, the browser address bar displays '192.168.100.210:8443/porta'. The page header includes the Cisco logo and 'Guest Portal'. The main content area is titled 'Account Created' and instructs the user to use the provided information to sign on. The account details are as follows:

- Username: accessit1
- Password: 5083
- First name: Ahmad
- Last name: Ali
- Email: ali@yahoo.com
- Company: SBM
- Location: San Jose
- SMS provider: Global Default
- Person being vis... test@yahoo.com
- Reason being vi... Test

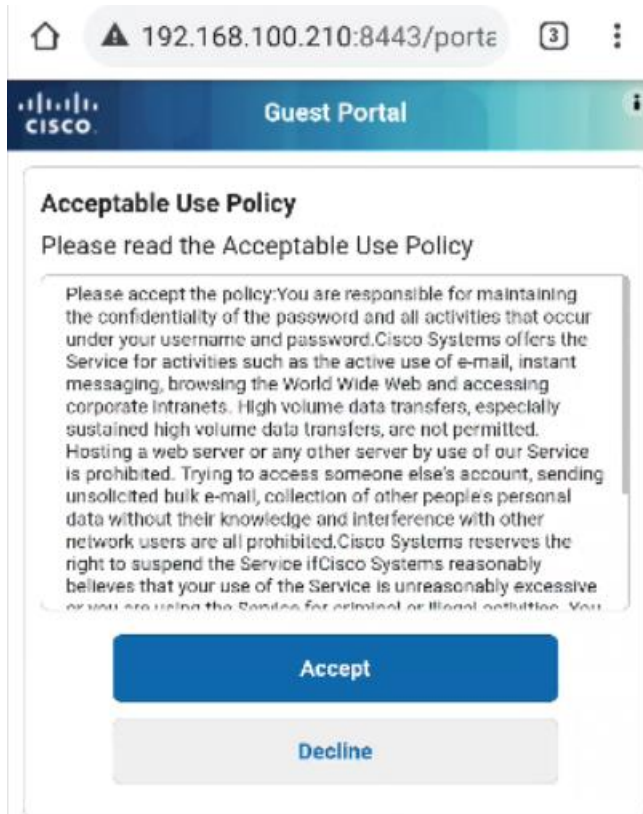
A blue 'Sign On' button is located at the bottom of the account details box.

Provide the given Username and Password click Sign On to login.



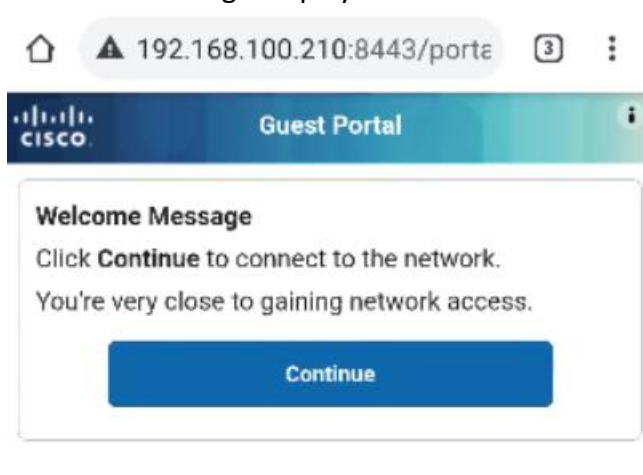
The screenshot shows the Cisco Guest Portal 'Welcome' screen. The browser address bar remains the same. The page header is consistent. The main content area is titled 'Welcome' and says 'Sign on for guest access.' Below this, there are input fields for 'Username' and 'Password'. The 'Username' field contains 'accessit1'. The 'Password' field contains '5083' (masked with dots). A 'Reset Password' link is visible next to the password field. A blue 'Sign On' button is at the bottom of the login section. Below the button is a link that says 'Or register for guest access'.

Accept the Acceptable Use Policy to proceed.



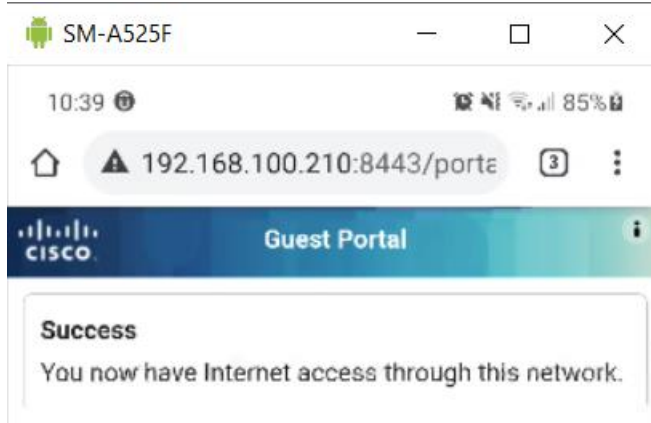
The screenshot shows a web browser window with the address bar displaying '192.168.100.210:8443/portal'. The page header features the Cisco logo and the text 'Guest Portal'. The main content area is titled 'Acceptable Use Policy' and includes a sub-header 'Please read the Acceptable Use Policy'. Below this, a text box contains the policy details: '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'. At the bottom of the policy text box, there are two buttons: a blue 'Accept' button and a grey 'Decline' button.

Welcome Message Display click **Continue**.



The screenshot shows the same web browser window as the previous one, but the page content has changed. The header remains the same. The main content area is titled 'Welcome Message' and includes the text: 'Click **Continue** to connect to the network. You're very close to gaining network access.' Below this text is a single blue button labeled 'Continue'.

Success Message Display now can browse the Internet.



Export To ▼

Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authenticat...
▼			Identity	Endpoint ID	Endpoint Profi	Authentication
!		0	accessit1	26:CF:51:98:98:31	Linux-Works...	Guest-Hotspot
✓			accessit1	26:CF:51:98:98:31	Android	Guest-Hotspot
✓				26:CF:51:98:98:31		
✓			accessit1	26:CF:51:98:98:31		

CISCO

MONITOR

WLANs

CONTROLLER

WIRELESS

SECURITY

MANAGEMENT

COMMANDS

HELP

Monitor

Summary

Access Points

Cisco CleanAir

Statistics

CDP

Rogues

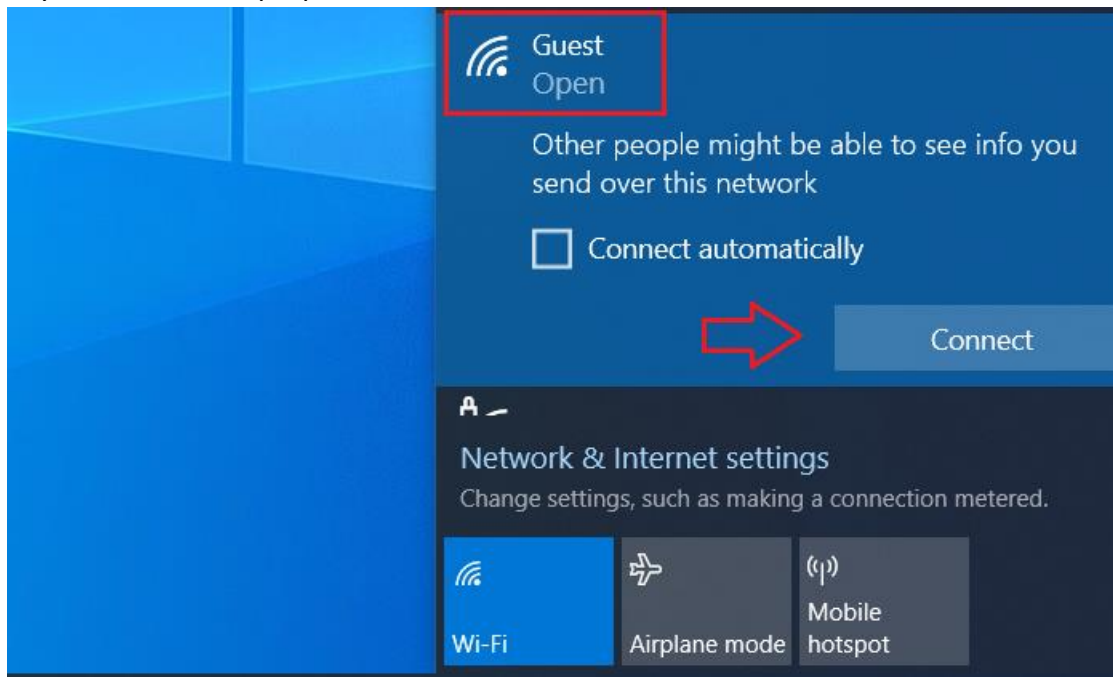
Clients

Clients

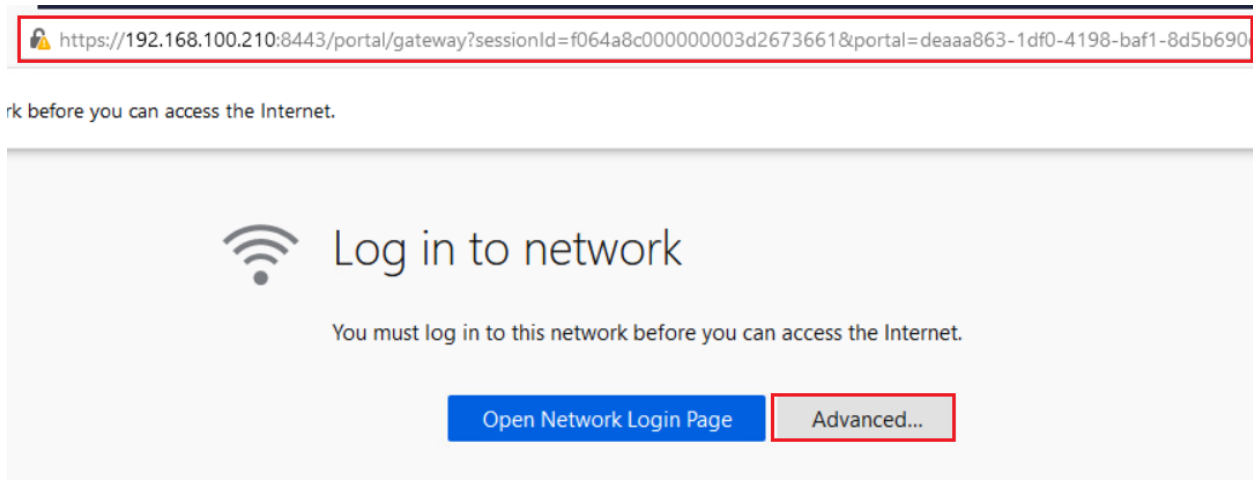
Current Filter None [Change Filter] [Clear Filter]

Client MAC Addr	IP Address(Ipv4/Ipv6)	AP Name	WLAN Profile	WLAN SSID	User Name
26:cf:51:98:98:31	192.168.100.22	AP	Guest	Guest	accessit1
28:ee:52:1d:13:7b	192.168.100.24	AP	Guest	Guest	accessa

In your windows Laptop connect to Guest SSID.



Click on Advanced button.





Log in to network

You must log in to this network before you can access the Internet.

[Open Network Login Page](#)

[Advanced...](#)

Someone could be trying to impersonate the site and you should not continue.

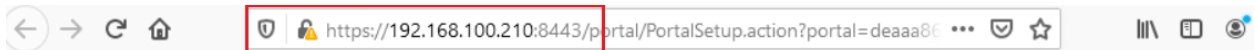
Web sites prove their identity via certificates. Firefox does not trust 192.168.100.210:8443 because its certificate issuer is unknown, the certificate is self-signed, or the server is not sending the correct intermediate certificates.

Error code: [SEC_ERROR_UNKNOWN_ISSUER](#)

[View Certificate](#)

[Go Back \(Recommended\)](#)

[Accept the Risk and Continue](#)



You must log in to this network before you can access the Internet.

[Open Network Login Page](#)



Guest Portal

Welcome

Sign on for guest access.

Username:

Password:

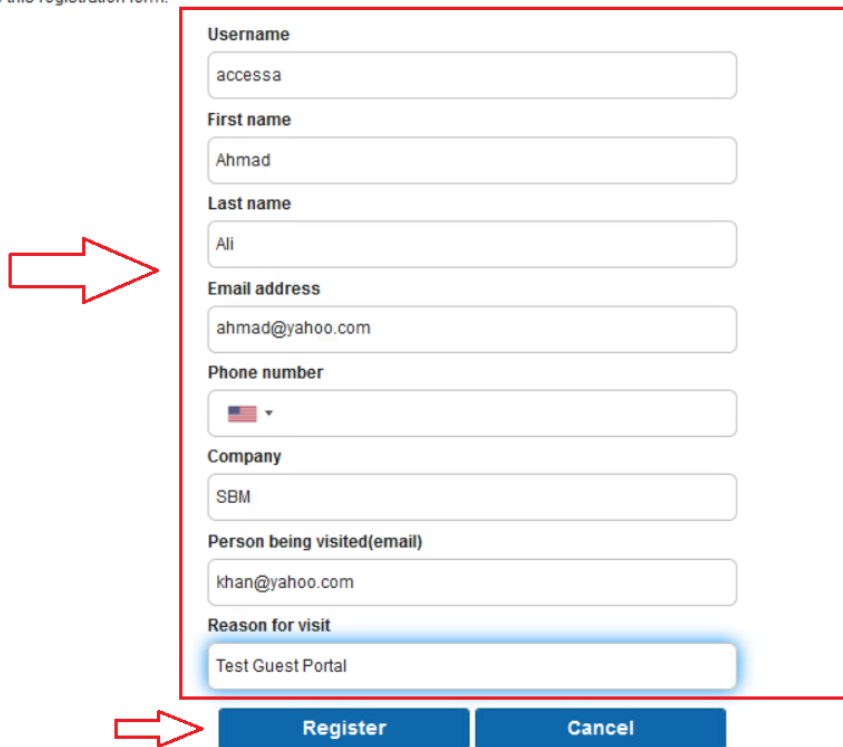
[Reset Password](#)

[Sign On](#)

[Or register for guest access](#)

Registration

Please complete this registration form:



Username
accessa

First name
Ahmad

Last name
Ali

Email address
ahmad@yahoo.com

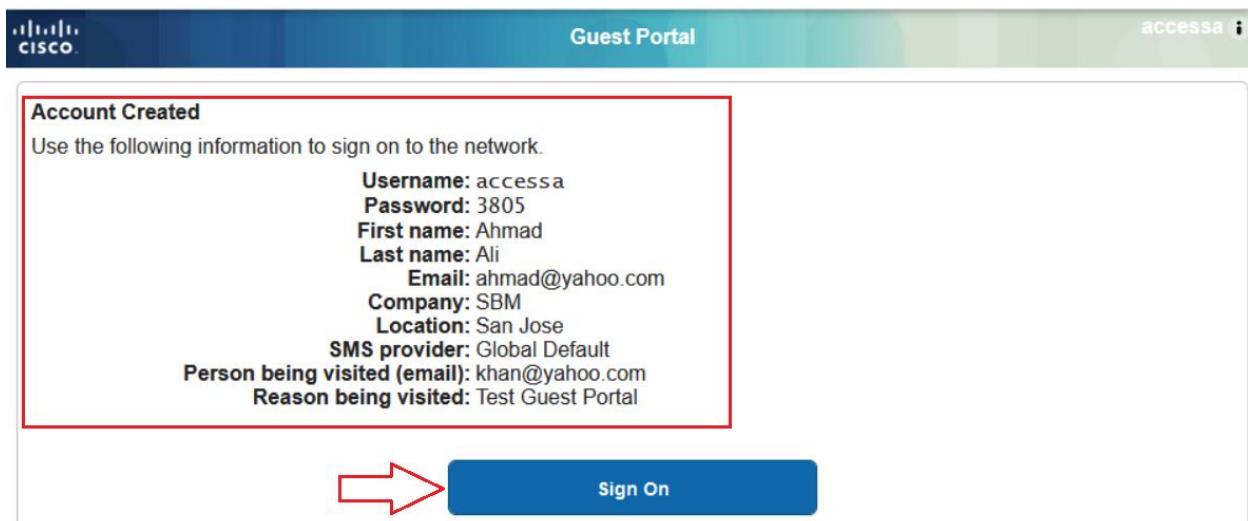
Phone number
[Country Code] [Phone Number]

Company
SBM

Person being visited(email)
khan@yahoo.com

Reason for visit
Test Guest Portal

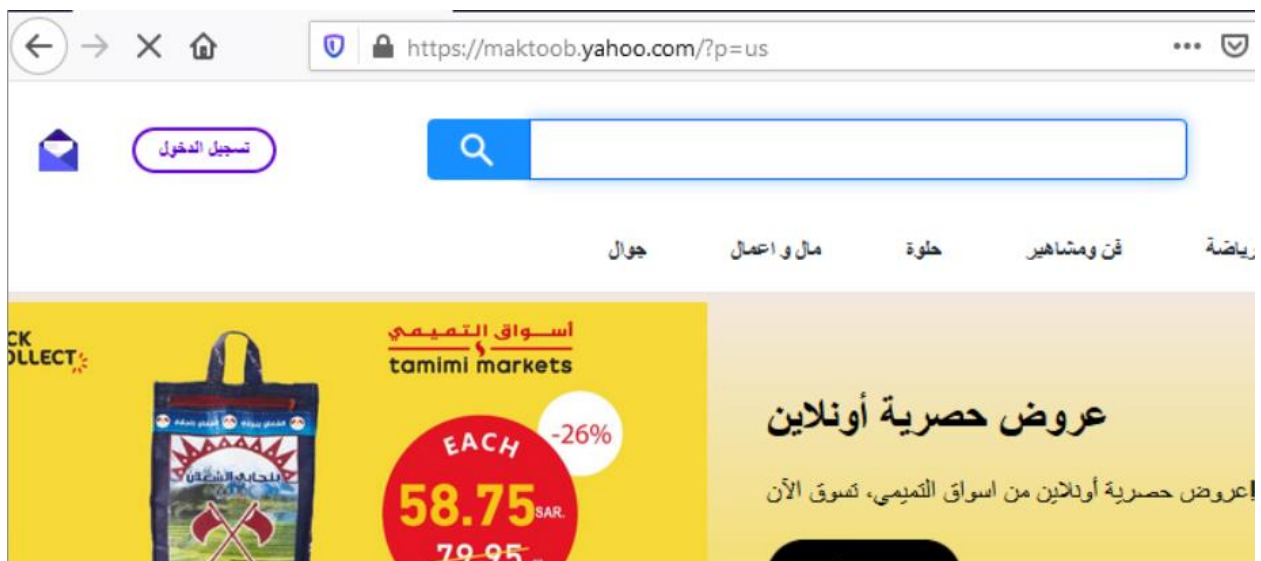
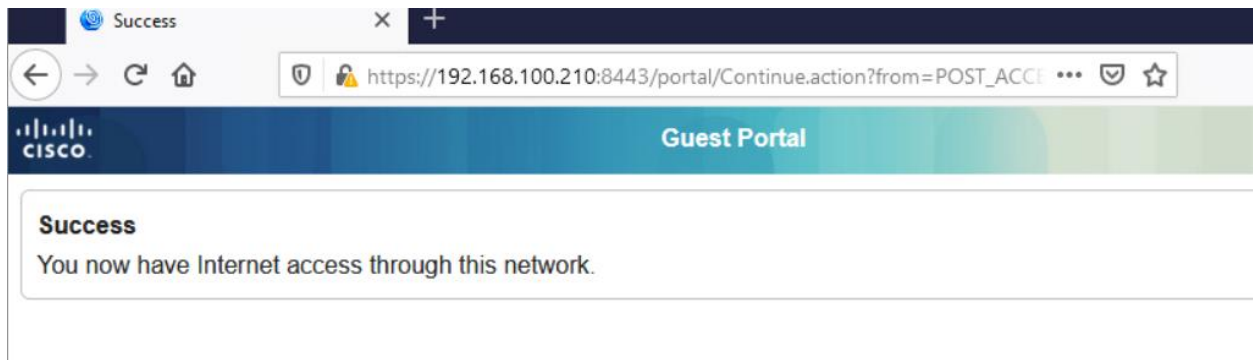
Register **Cancel**



Account Created
Use the following information to sign on to the network.

Username: accessa
Password: 3805
First name: Ahmad
Last name: Ali
Email: ahmad@yahoo.com
Company: SBM
Location: San Jose
SMS provider: Global Default
Person being visited (email): khan@yahoo.com
Reason being visited: Test Guest Portal

Sign On



Refresh Reset Repeat Counts Export To

	Time	Status	Details	Repeat ...	Identity	Endpoint ID
x					Identity	Endpoint ID
	Sep 06, 2021 07:20:52.437 PM			0	accessa	28:EE:52:1D:13:7B
	Sep 06, 2021 07:20:52.412 PM				accessa	28:EE:52:1D:13:7B
	Sep 06, 2021 07:20:52.380 PM					28:EE:52:1D:13:7B
	Sep 06, 2021 07:20:22.624 PM				accessa	28:EE:52:1D:13:7B