



Networkforyou

Subscribe to our
You Tube Channel



Networkforyou



**Welcome
To
Network for you
Wireless security features**



Email us:
networkforyou4@gmail.com

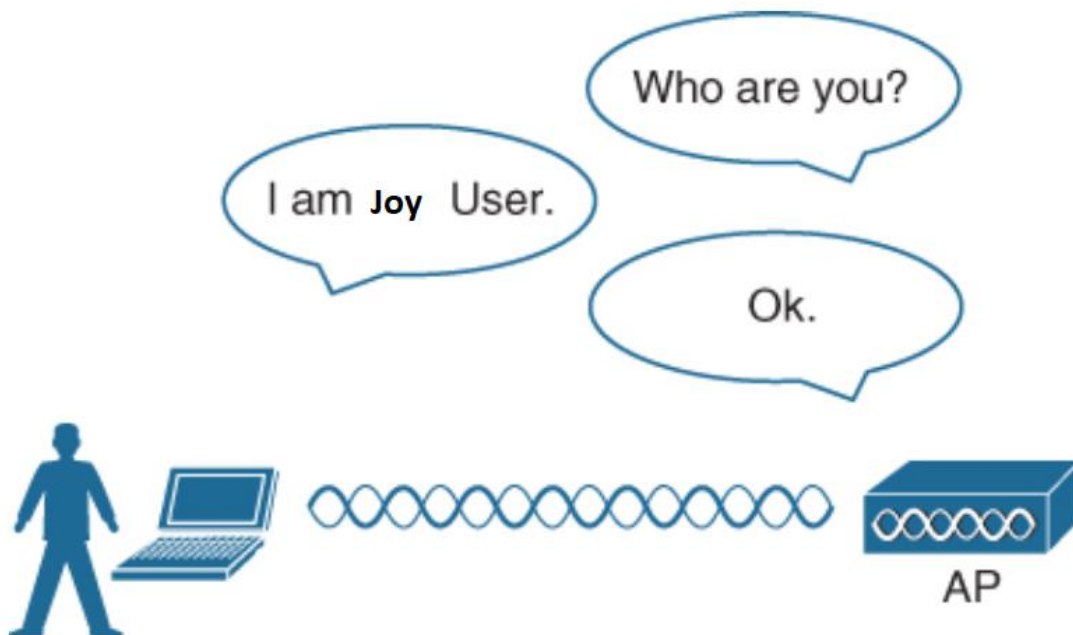
1 of 12

WhatsApp Us : +918143809578



Wireless security features:

- To join and use a wireless network, wireless clients must first discover a basic service set (BSS) and then request permission to associate with it.
- At that point, clients should be authenticated by some means before they can become functioning members of a wireless LAN.
- Suppose that your wireless network connects to corporate resources where confidential information can be accessed.
- In that case, only devices known to be trusted and expected should be given access.
- Guest users, if they are permitted at all, should be allowed to join a different guest WLAN where they can access non confidential or public resources.
- Rogue clients, which are not expected or welcomed, should not be permitted to associate at all. After all, they are not affiliated with the corporate network and are likely to be unknown devices that happen to be within range of your network.
- To control access, wireless networks can authenticate the client devices before they are allowed to associate. Potential clients must identify themselves by presenting some form of credentials to the APs. Shows the basic client authentication process diagram.



- Wireless authentication can take many forms.
- Some methods require only a static text string that is common across all trusted clients and APs.

Email us:
networkforyou4@gmail.com

2 of 12

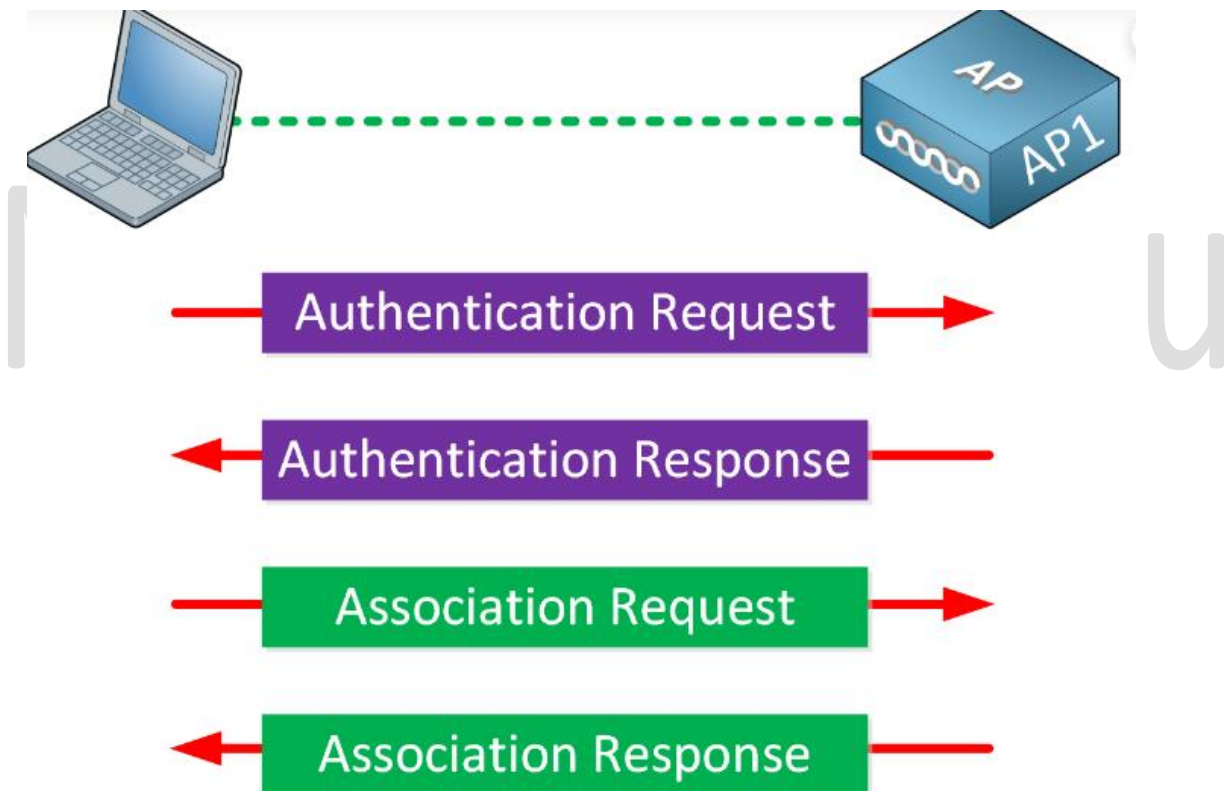
WhatsApp Us : +918143809578



- The text string is stored on the client device and presented directly to the AP when needed
- What might happen if the device is stolen or lost? Most likely, any user who possesses the device would still be able to authenticate to the network.
- Other more stringent authentication methods require interaction with a corporate user database. In those cases, the end user must enter a valid username and password.

OPEN AUTHENTICATION

- As we know that a wireless client device must send **802.11 authentication request and association request frames to an AP** when it asks to join a wireless network.
- The original 802.11 standard offered only two choices to authenticate a client: **Open Authentication and WEP.**



- Using open authentication doesn't automatically mean that there is no authentication at all. You can still authenticate wireless users on another level. If you have ever used a public wireless network at an airport, hotel, or fast food restaurant.

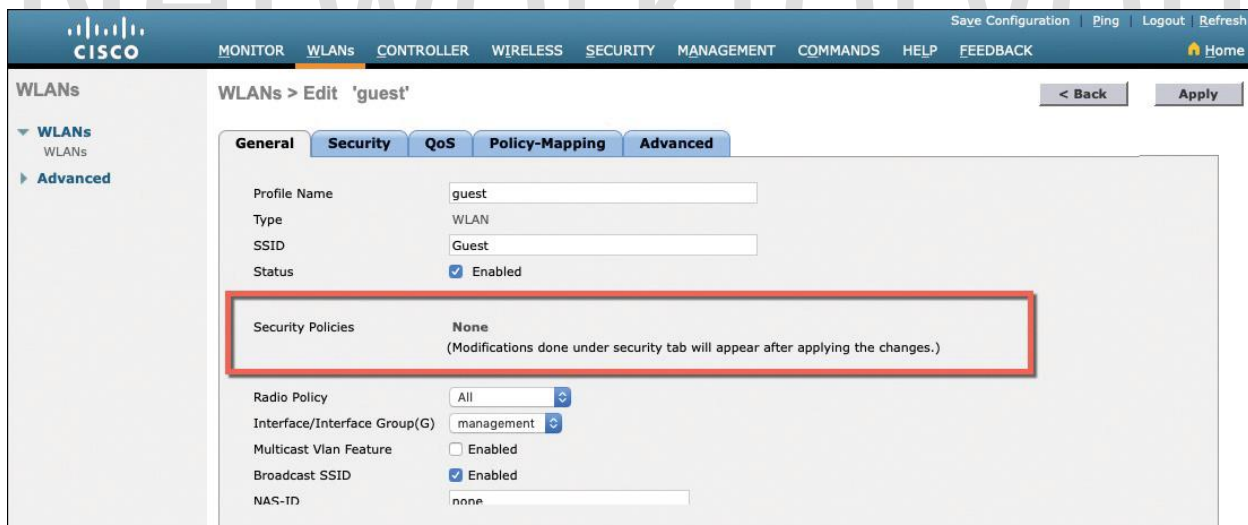
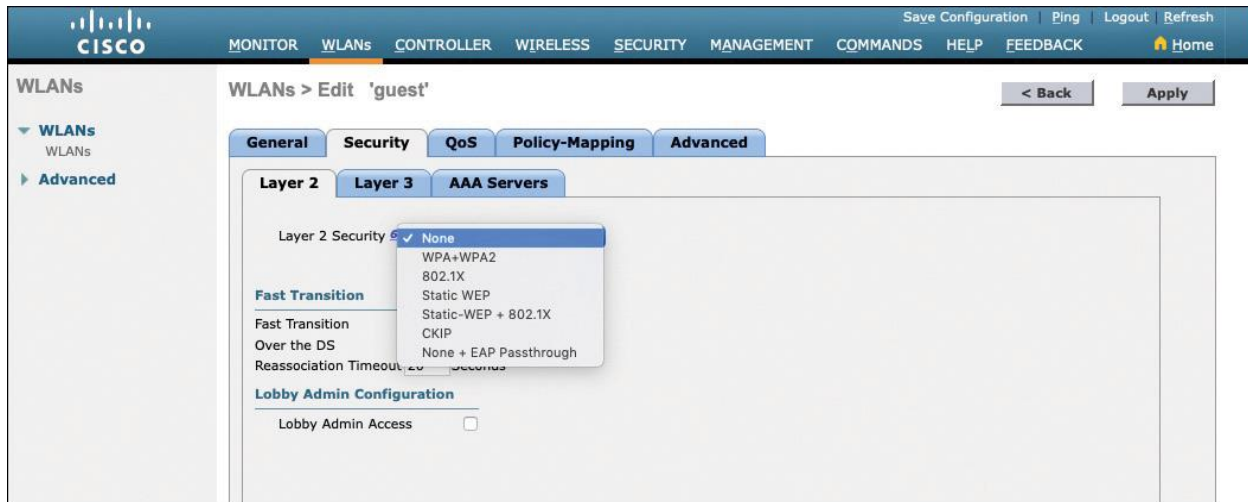
Email us:
networkforyou4@gmail.com

3 of 12

WhatsApp Us : +918143809578



- You can connect to the network without any issues, but as soon as you open your web browser, you see a web page where you have to enter your credentials.
- Until you enter your credentials, all traffic is blocked. On the wireless level, there is no authentication, but there is on the upper layers.



Email us:
networkforyou4@gmail.com

4 of 12

WhatsApp Us : +918143809578



WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
1	WLAN	guest	Guest	Enabled	None

AUTHENTICATING WITH PRE-SHARED KEY:

- To secure wireless connections on a WLAN, we can leverage one of the Wi-Fi Protected Access (WPA) versions—WPA (also known as WPA1), WPA2, or WPA3.
- Each version is certified by the Wi-Fi Alliance so that wireless clients and APs using the same version are known to be compatible.
- The WPA versions also specify encryption and data integrity methods to protect data passing over the wireless connections.

Layer 2 Security: **WPA+WPA2**

WPA2 Policy:

WPA2 Encryption: AES

PSK: Enable

PSK Format: ASCII

Email us:
networkforyou4@gmail.com

5 of 12

WhatsApp Us : +918143809578



The screenshot shows the Cisco WLAN configuration interface for a profile named 'devices'. The 'Security' tab is selected, and the 'Security Policies' field is highlighted with a red box, showing the value '[WPA2][Auth(PSK)]'. Below this, there is a note: '(Modifications done under security tab will appear after applying the changes.)'. Other fields include Profile Name (devices), Type (WLAN), SSID (Devices), Status (Enabled), Radio Policy (All), Interface/Interface Group(G) (management), Multicast Vlan Feature (Enabled), Broadcast SSID (Enabled), and NAS-ID (none).

The screenshot shows the Cisco WLAN configuration interface displaying a list of WLANs. The table has columns for WLAN ID, Type, Profile Name, WLAN SSID, Admin Status, and Security Policies. The second entry is highlighted with a red box, showing Profile Name 'devices', WLAN SSID 'Devices', Admin Status 'Enabled', and Security Policies '[WPA2][Auth(PSK)]'.

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
1	WLAN	guest	Guest	Enabled	None
2	WLAN	devices	Devices	Enabled	[WPA2][Auth(PSK)]

AUTHENTICATING WITH EAP (Extensible Authentication Protocol):

- Client authentication generally involves some sort of challenge, a response, and then a decision to grant access. Behind the scenes, it can also involve an exchange of session or encryption keys, in addition to other parameters needed for client access.
- Each authentication method might have unique requirements as a unique way to pass information between the client and the AP.
- Rather than build additional authentication methods into the 802.11 standard, Extensible Authentication Protocol (EAP) offers a more flexible and scalable authentication framework.
- As its name implies, EAP is extensible and does not consist of any one authentication method. Instead, EAP defines a set of common functions that actual authentication methods can use to authenticate users.
- **EAP has another interesting quality: It can integrate with the IEEE 802.1x port-based access control standard.**

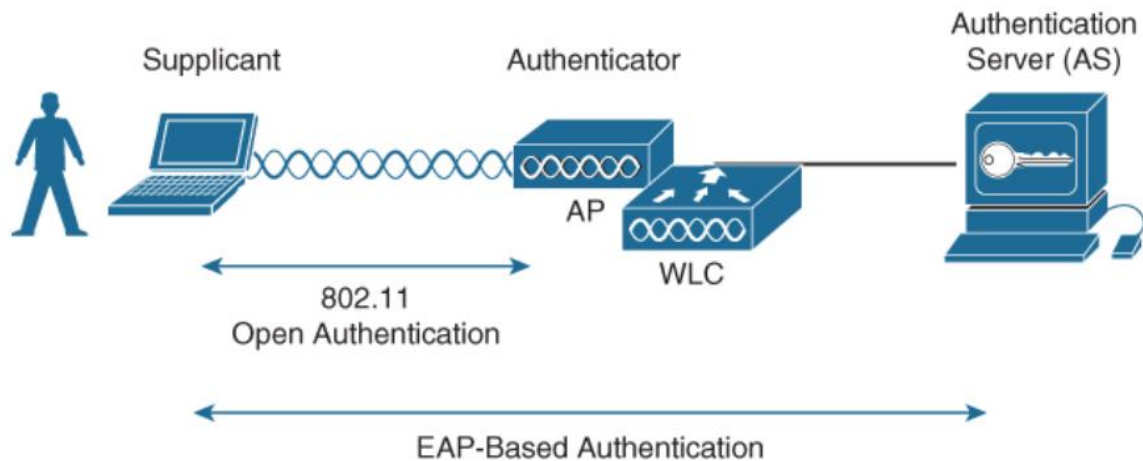
Email us:
networkforyou4@gmail.com

6 of 12

WhatsApp Us : +918143809578



- When 802.1x is enabled, it limits access to a network medium until a client authenticates. This means that a wireless client might be able to associate with an AP but will not be able to pass data to any other part of the network until it successfully authenticates.
- With Open Authentication and PSK authentication, wireless clients are authenticated locally at the AP without further intervention.
- The scenario changes with 802.1x; the client uses Open Authentication to associate with the AP, and then the actual client authentication process occurs at a dedicated authentication server.



Supplicant: The client device that is requesting access.

Authenticator: The network device that provides access to the network (usually a wireless LAN controller [WLC])

Authentication server (AS): The device that takes user or client credentials and permits or denies network access based on a user database and policies (usually a RADIUS server)

Email us:
networkforyou4@gmail.com

7 of 12

WhatsApp Us : +918143809578

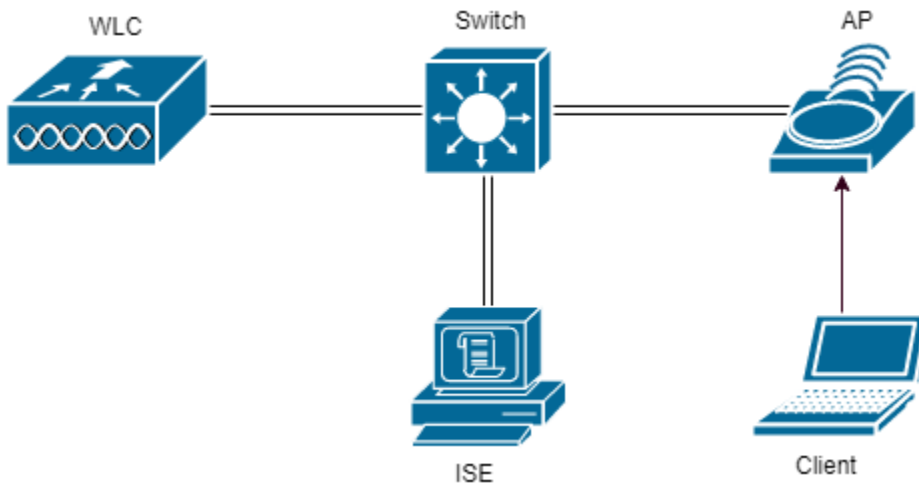


The screenshot shows the Cisco ISE Security configuration page for RADIUS Authentication Servers. The left sidebar shows the navigation menu with 'RADIUS Authentication' highlighted. The main content area is titled 'RADIUS Authentication Servers > New' and contains the following configuration fields:

- Server Index (Priority): 1
- Server IP Address(Ipv4/Ipv6): 192.168.10.9
- Shared Secret Format: ASCII
- Shared Secret: [Redacted]
- Confirm Shared Secret: [Redacted]
- Apply Cisco ISE Default settings:
- Key Wrap: (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
- Port Number: 1812
- Server Status: Enabled
- Support for CoA: Disabled
- Server Timeout: 5 seconds
- Network User: Enable
- Management: Enable
- Management Retransmit Timeout: 5 seconds
- IPSec: Enable

NetworkforYou

Web Authentication:



Email us:
networkforyou4@gmail.com

WhatsApp Us : +918143809578



Login

Welcome to the Cisco wireless network

Cisco is pleased to provide the Wireless LAN infrastructure for your network. Please login and put your unified wireless solution to work.

User Name

Password

Submit

- Enable authentication and authorization via HTTP or HTTPs portal.
- Automatic HTTP or HTTPs redirection to the authentication portal.
- Deployed for visitors, guests and optionally as 802.1X fallback.
- Web Authentication supports by both wired and wireless access.
- User is redirected to the Cisco ISE web service for authentication.
- Cisco ISE sends CoA request to Network Access Device after authentication.
- CWA is for interactive users who have web browser, manually enter details.
- Multiple devices will require configuration to enable Central Web Authentication.
- Such as a redirection ACL, & ISE need authentication & Authorization rules set up.
- Central Web Authentication is the process in which web-based authentication.
- When Client failed to authenticate via Dot1x or MAB, Client is redirected to Web Portal.
- Authorization profile configured on Authentication server will authorize this guest login.
- Central Web Authentication are, it configures along with dot1x and MAB authentication.
- Switch must run HTTP & HTTPS service & have redirect ACL to support Central WebAuth.
- Central Web mostly often used for centralized guest authentication & authorization.
- User is authenticated in the web portal hosted on Cisco Identity Service Engine.
- Web Authentication (WebAuth) is different because it presents the end user with content to read and interact with before granting access to the network.
- For example, it can present an acceptable use policy (AUP) that the user must accept before accessing the network.
- It can also prompt for user credentials, display information about the enterprise, and so on.
- Naturally, the user must open a web browser to see the WebAuth content.

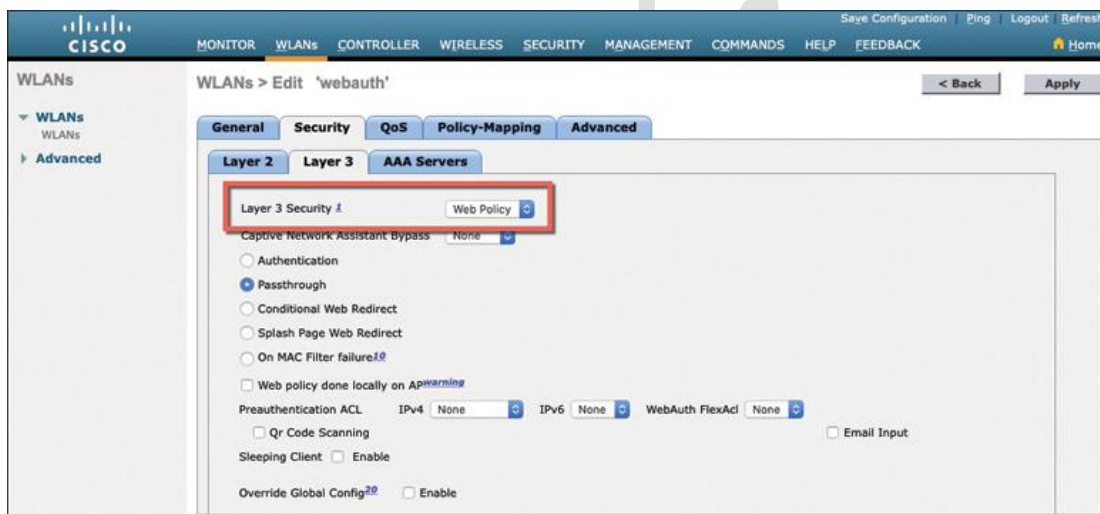
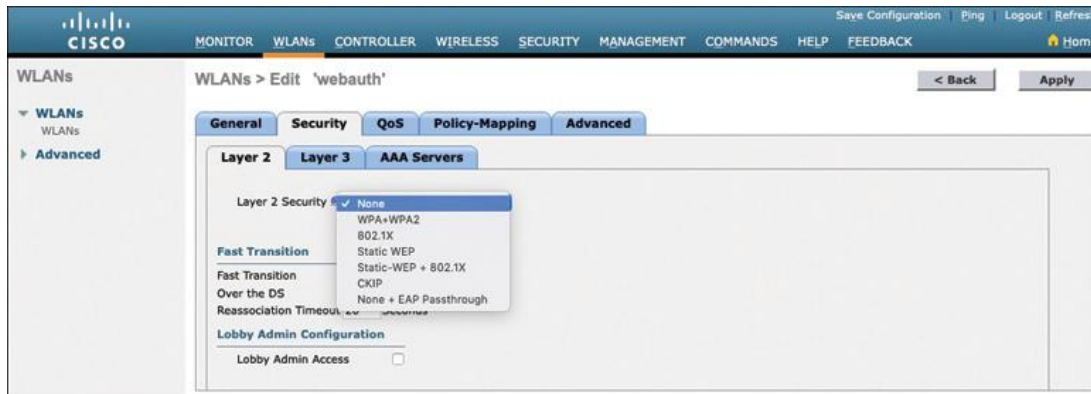
Email us:
networkforyou4@gmail.com

9 of 12

WhatsApp Us : +918143809578



- WebAuth can be used as an additional layer in concert with Open Authentication, PSK-based authentication, and EAP-based authentication.
- Web Authentication can be handled locally on the WLC for smaller environments through Local Web Authentication (LWA) or we can use CISCO ISE.



Email us:
networkforyou4@gmail.com

WhatsApp Us : +918143809578

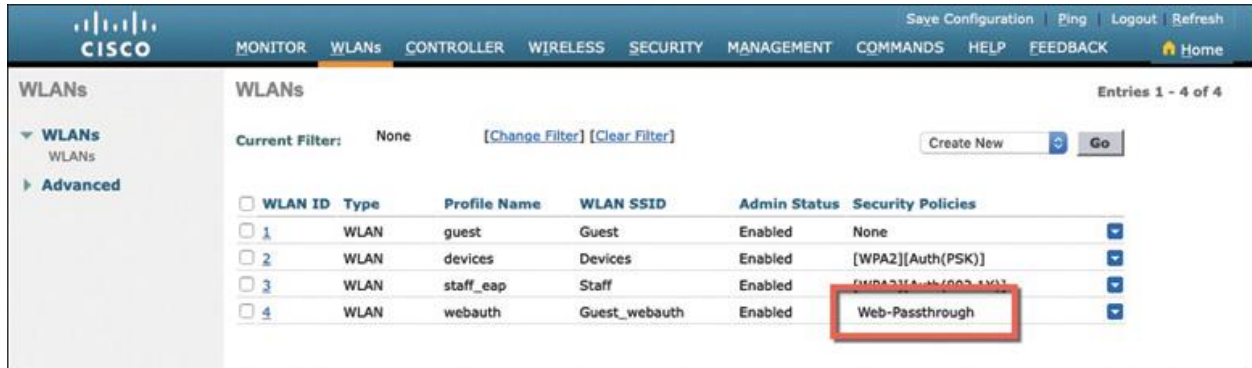


The screenshot shows the Cisco Web Management Interface for the Security section. The left sidebar lists various configuration options, with 'Web Auth' and 'Web Login Page' highlighted in a red box. The main content area is titled 'Web Login Page' and includes configuration fields for 'Web Authentication Type' (set to 'Internal (Default)'), 'Redirect URL after login', and 'Login Success Page Type' (set to 'Default'). Below these fields is a text box containing the message: 'In order to use the guest wireless, you must first read the Acceptable Use Policy and abide by its terms.' The interface also includes 'Preview...' and 'Apply' buttons.

The screenshot shows the Cisco Connect Web Login Page. The header features the Cisco logo and the word 'Connect'. The main content area displays the message: 'Welcome to our guest wireless!' followed by 'In order to use the guest wireless, you must first read the Acceptable Use Policy and abide by its terms.' Below the message is an 'Accept' button.

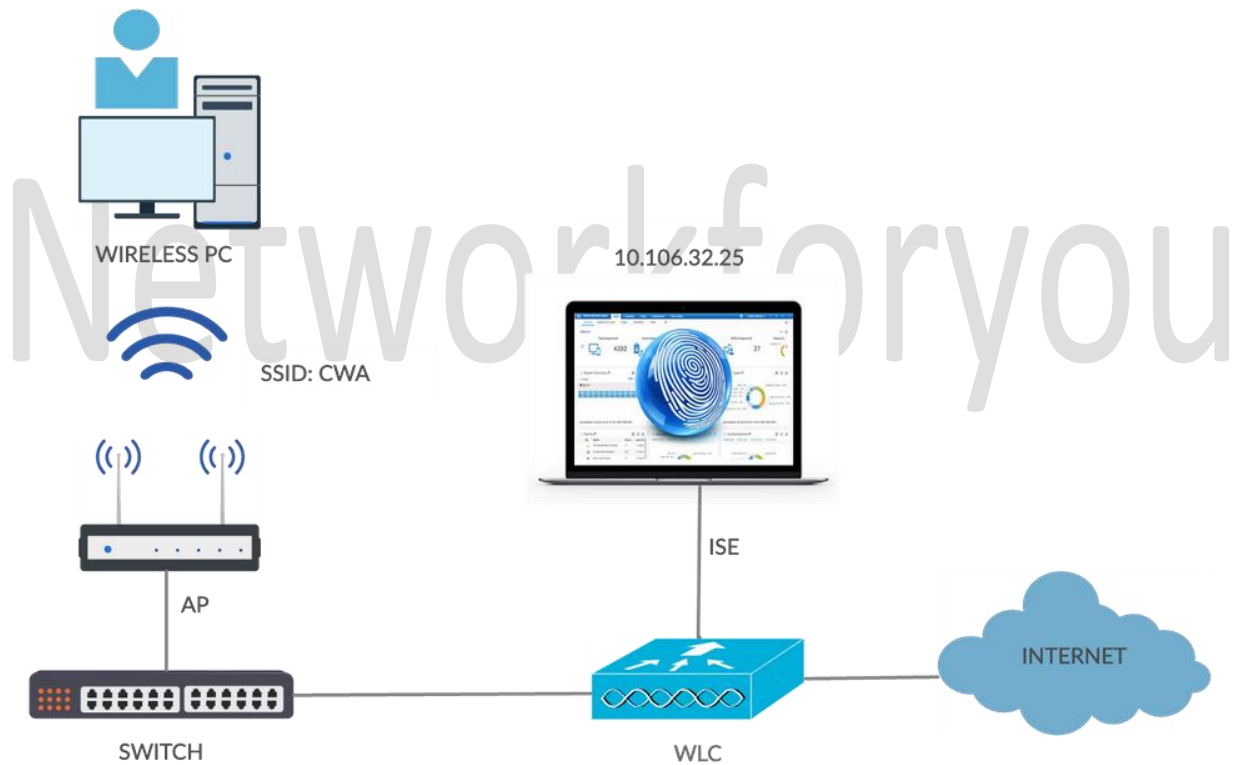
Email us:
networkforyou4@gmail.com

WhatsApp Us : +918143809578



The screenshot shows the Cisco WLAN configuration interface. The 'WLANs' tab is selected, and a table lists four WLANs. The 'Security Policies' column for the fourth WLAN, 'webauth', is highlighted with a red box and contains the text 'Web-Passthrough'.

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
1	WLAN	guest	Guest	Enabled	None
2	WLAN	devices	Devices	Enabled	[WPA2][Auth(PSK)]
3	WLAN	staff_eap	Staff	Enabled	[WPA2][Auth(PSK)]
4	WLAN	webauth	Guest_webauth	Enabled	Web-Passthrough



Email us:
networkforyou4@gmail.com

WhatsApp Us : +918143809578