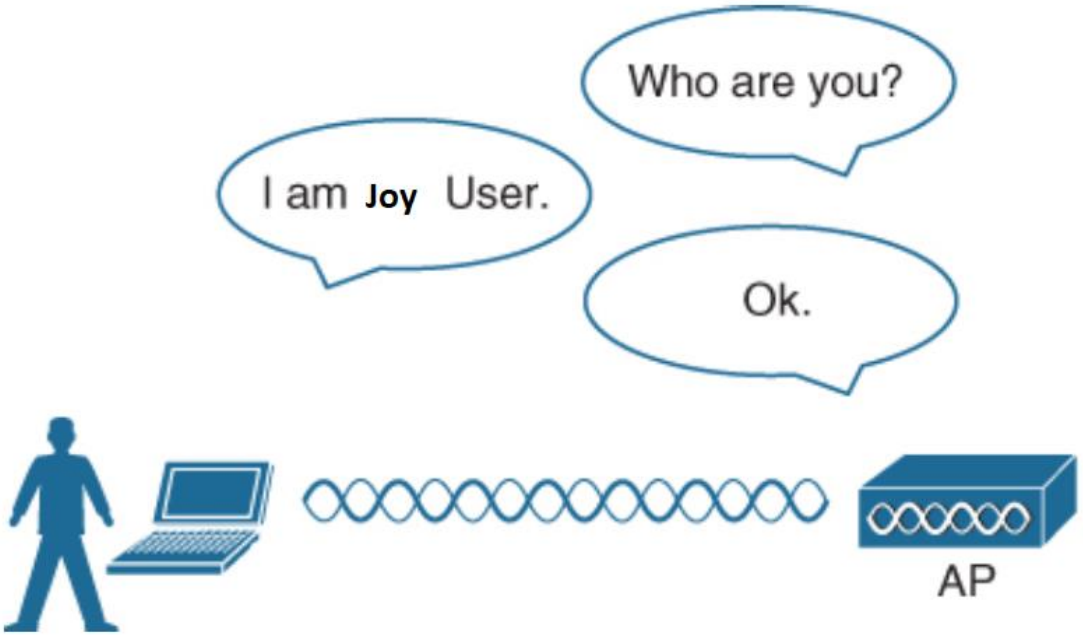

Networkforyou
Welcome
To
Network for you
Wireless security features
Networkforyou

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.

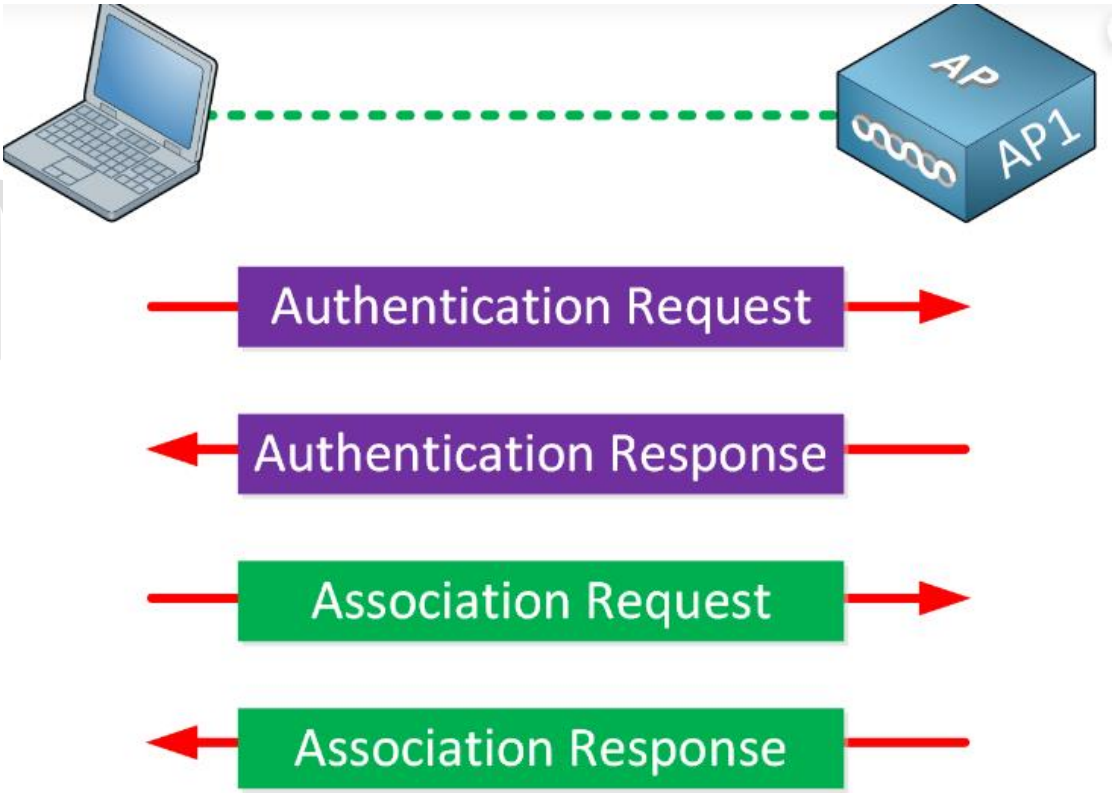


- Wireless authentication can take many forms.
- Some methods require only a static text string that is common across all trusted clients and APs.

- 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.

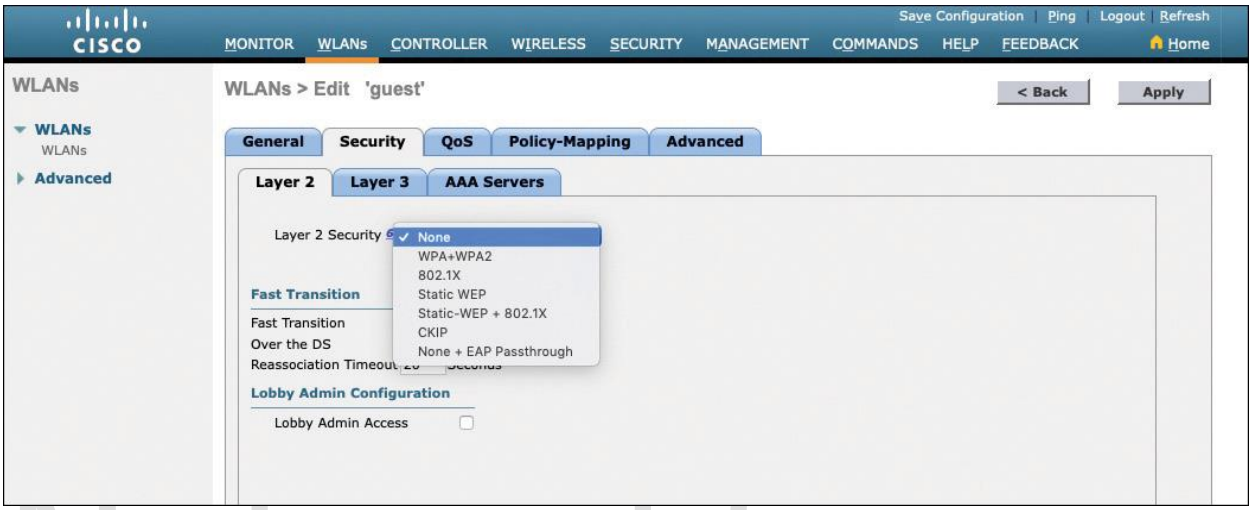
OPEN AUTHENTICATION

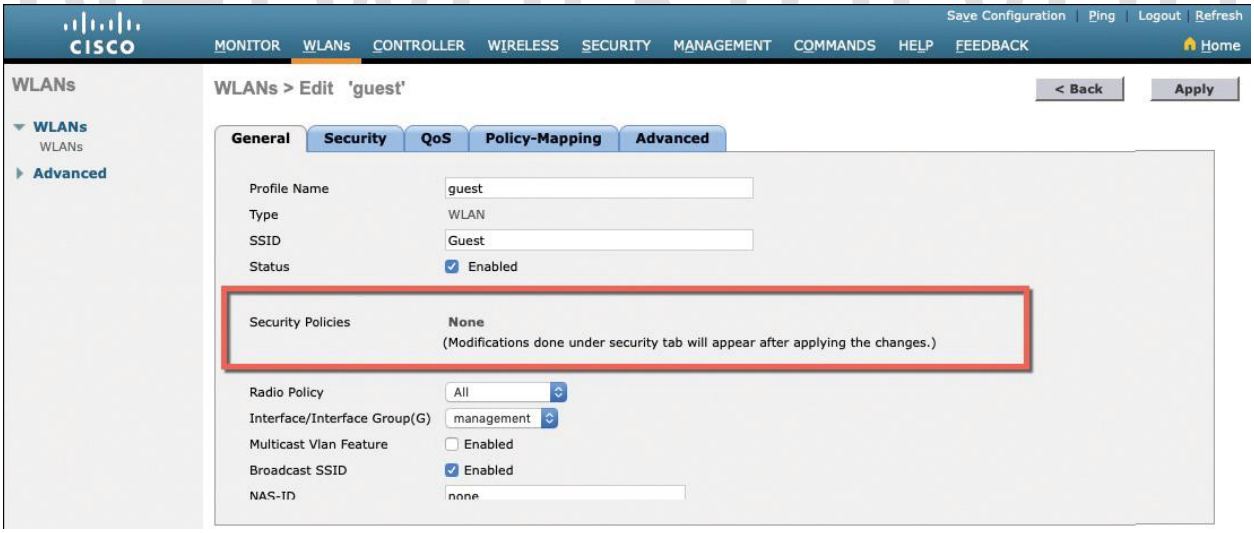
- As we know that a wireless client device must send **802.11 authentication request and association request frames to an AP** when it asks to join a wireless network.
- The original 802.11 standard offered only two choices to authenticate a client: **Open Authentication and WEP.**



- 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.

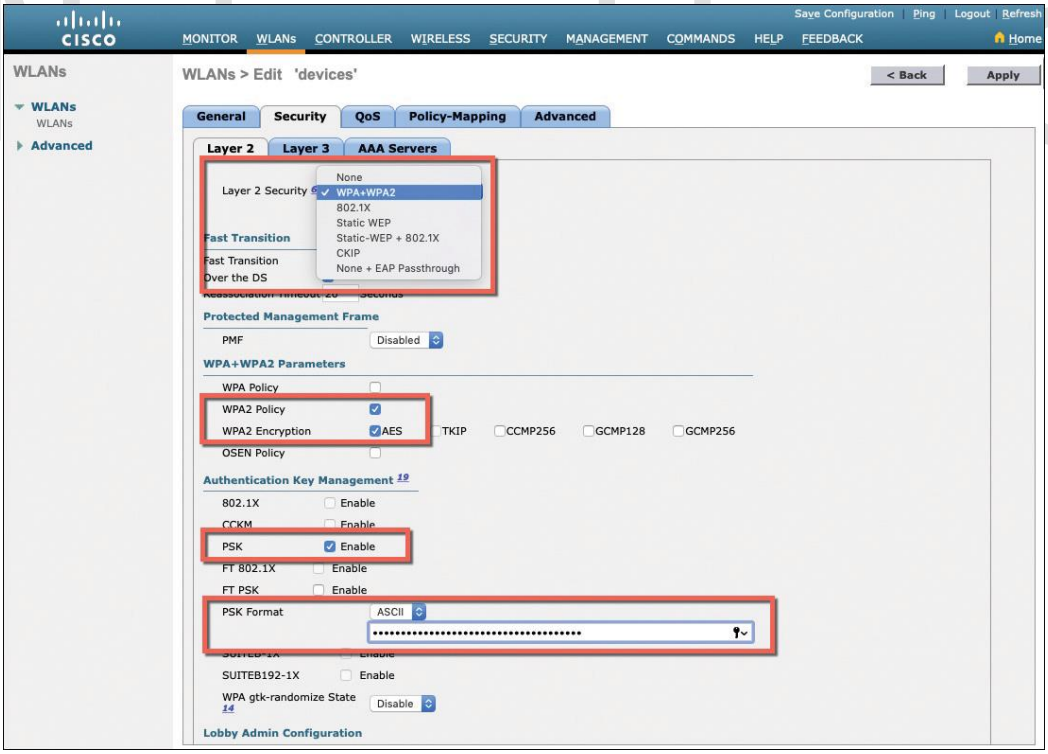
- You can connect to the network without any issues, but as soon as you open your web browser, you see a web page where you have to enter your credentials.
- Until you enter your credentials, all traffic is blocked. On the wireless level, there is no authentication, but there is on the upper layers.

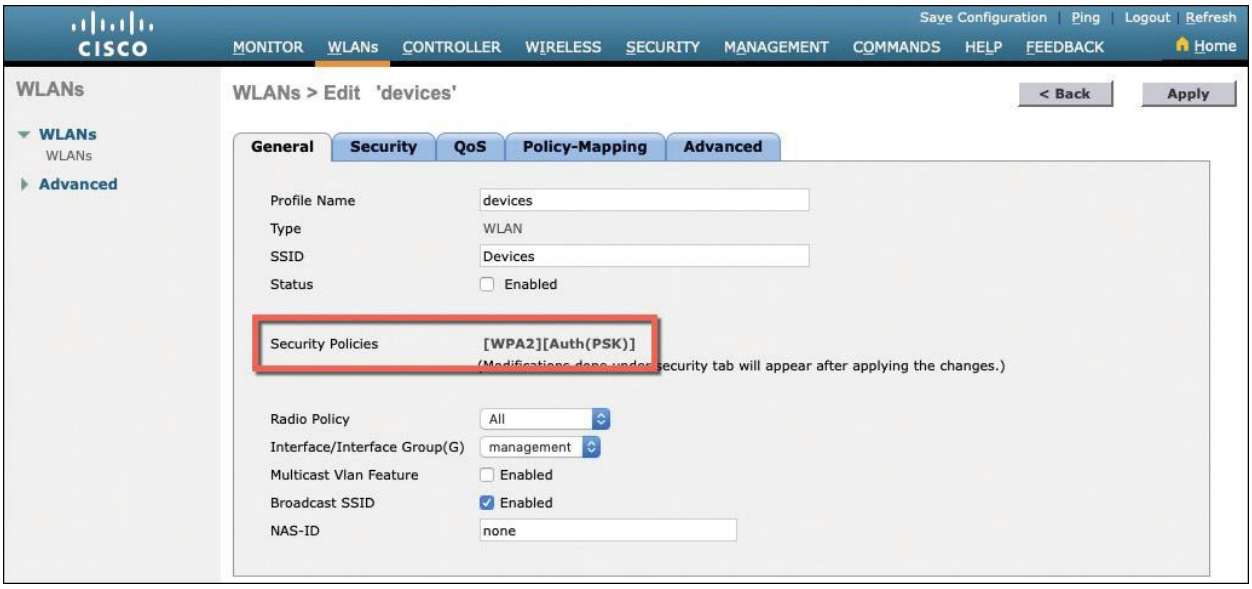




AUTHENTICATING WITH PRE-SHARED KEY:

- 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.

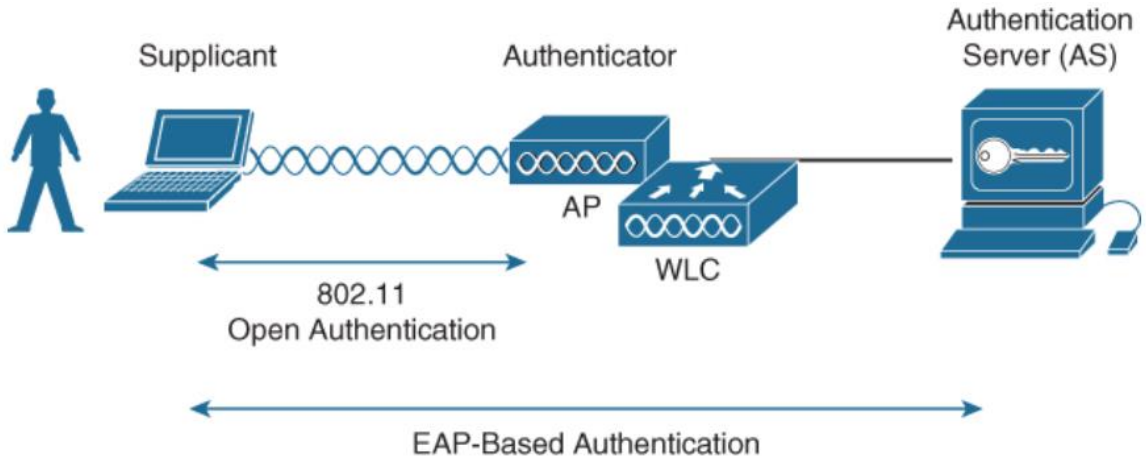




AUTHENTICATING WITH EAP (Extensible Authentication Protocol):

- 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**.

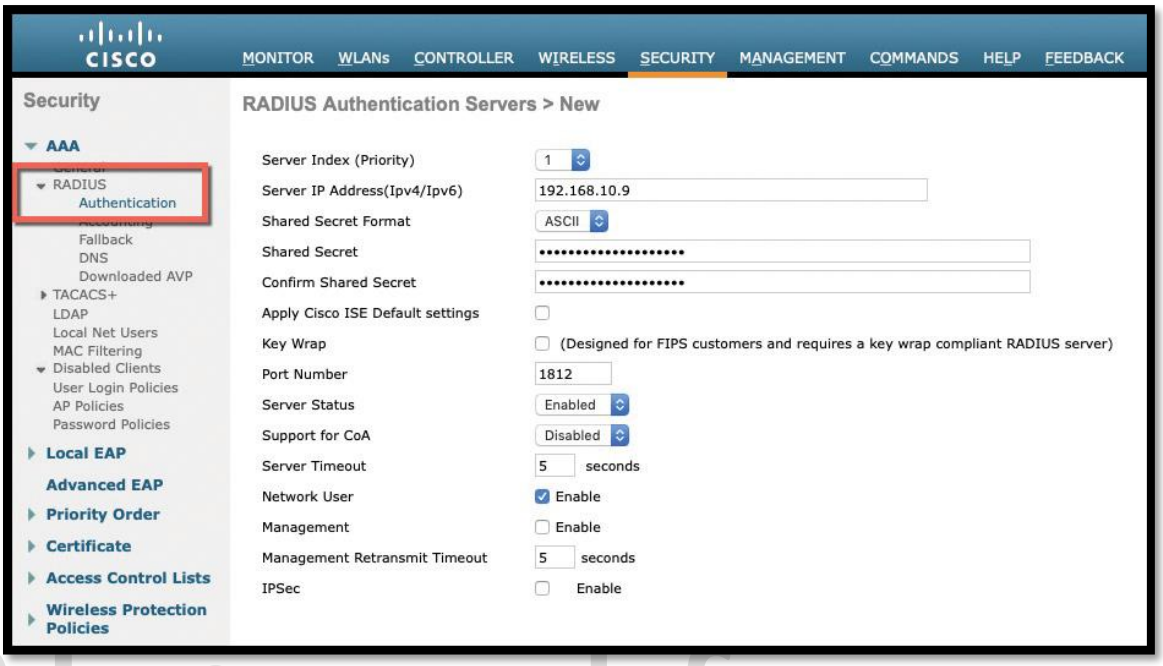
- When 802.1x is enabled, it limits access to a network medium until a client authenticates. This means that a wireless client might be able to associate with an AP but will not be able to pass data to any other part of the network until it successfully authenticates.
- With Open Authentication and PSK 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.



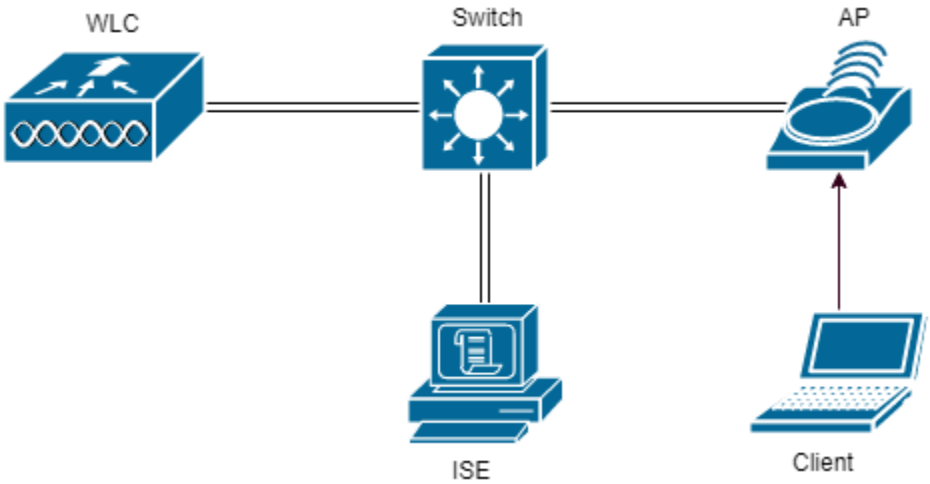
Supplicant: The client device that is requesting access.

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)

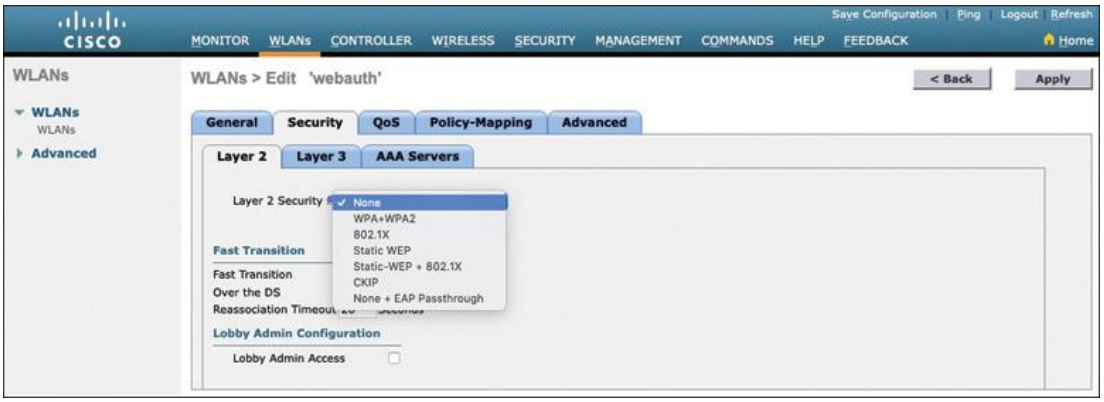


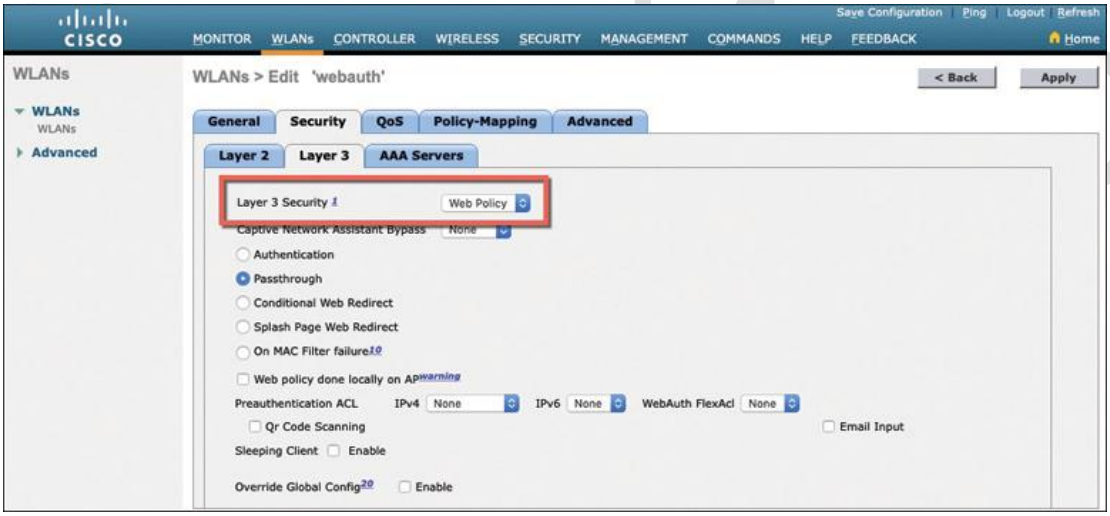
Web Authentication:

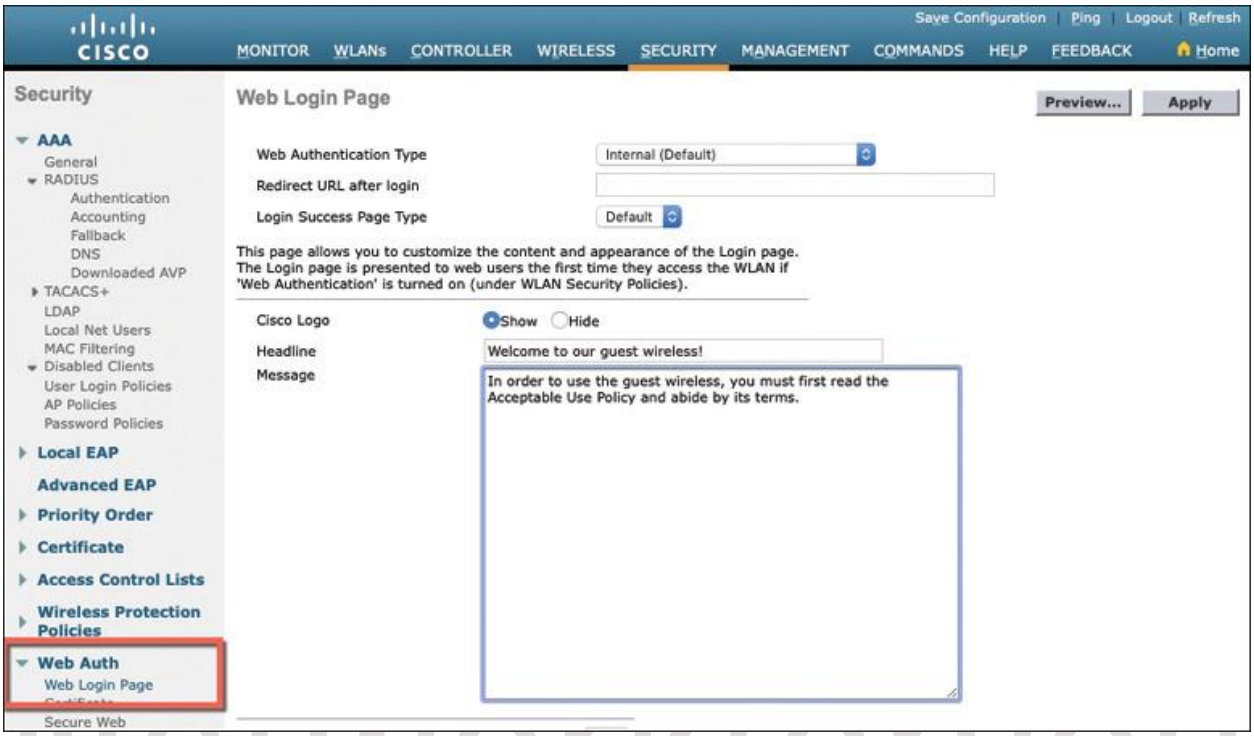


- Enable authentication and authorization via HTTP or HTTPs portal.
- Automatic HTTP or HTTPs redirection to the authentication portal.
- Deployed for visitors, guests and optionally as 802.1X fallback.
- Web Authentication supports by both wired and wireless access.
- User is redirected to the Cisco 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 Identify 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.

- 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.






Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK Home
Security
AAA
General
RADIUS
Authentication
Accounting
Fallback
DNS
Downloaded AVP
TACACS+
LDAP
Local Net Users
MAC Filtering
Disabled Clients
User Login Policies
AP Policies
Password Policies
Local EAP
Advanced EAP
Priority Order
Certificate
Access Control Lists
Wireless Protection Policies
Web Auth
Web Login Page
Secure Web
Web Login Page
Preview...
Apply
Web Authentication Type
Internal (Default)
Redirect URL after login
Login Success Page Type
Default
This page allows you to customize the content and appearance of the Login page.
The Login page is presented to web users the first time they access the WLAN if
'Web Authentication' is turned on (under WLAN Security Policies).
Cisco Logo
Show
Hide
Headline
Welcome to our guest wireless!
Message
In order to use the guest wireless, you must first read the
Acceptable Use Policy and abide by its terms.


Connect
Welcome to our guest wireless!
In order to use the guest wireless, you must first read the Acceptable Use Policy and abide by its terms.
Accept