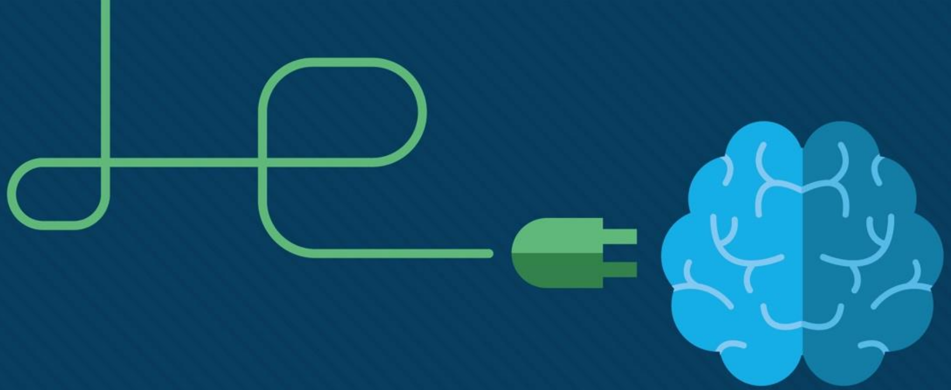


Chapter 20: Authenticating Wireless Clients

Instructor Materials

CCNP Enterprise: Core Networking

Chapter 20 Content

This chapter covers the following content:

- **Open Authentication -** This section covers authenticating wireless users using no credentials.

- **Authenticating with Pre-Shared Key -** This section covers authenticating clients with a static key that is shared prior to its use.

- **Authenticating with EAP -** This section covers authenticating clients with Extensible Authentication Protocol (EAP).

- **Authenticating with WebAuth -** This section covers authenticating clients through the use of a web page where credentials are entered.

Open Authentication

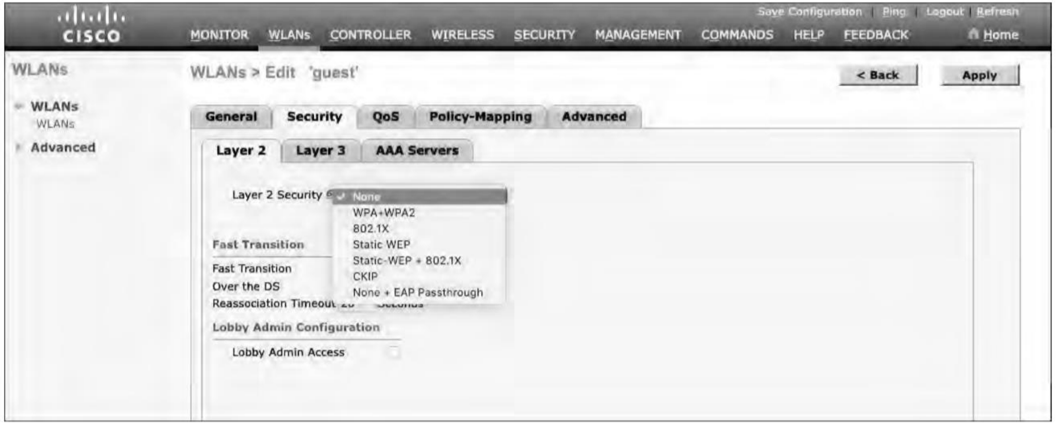
- To join and use a wireless network, wireless clients must first discover a basic service set (BSS) and then request permission to associate with it. At that point, clients should be authenticated by some means before they can become functioning members of a wireless LAN.
- The sections that follow explain four types of client authentication you will likely encounter on the CCNP and CCIE Enterprise ENCOR 350-401 exam and in common use.
- With each type, you will begin by creating a new WLAN on the wireless LAN controller, assigning a controller interface, and enabling the WLAN. Because wireless security is configured on a per-WLAN basis, all of the configuration tasks related to this chapter occur in the WLAN > Edit Security tab.

Open Authentication

- Recall 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.
- Open Authentication offers open access to a WLAN. The only requirement is that a client must use an 802.11 authentication request before it attempts to associate with an AP. No other credentials are needed.
- You have probably seen a WLAN with Open Authentication when you have visited a public location.
- If any client screening is used at all, it comes in the form of Web Authentication.

Creating a WLAN with Open Authentication

- Create a new WLAN and map it to the correct VLAN.
- Go to the General tab and enter the SSID string, apply the appropriate controller interface, and change the status to Enabled.
- Next, select the Security tab to configure the WLAN security and user authentication parameters. Select the Layer 2 tab and then use the Layer 2 Security drop-down menu to select None for Open Authentication, as shown in Figure 20-2.
- When you are finished configuring the WLAN, click the Apply button.



WLANs > Edit 'guest'

Layer 2 Security ✓ None

Fast Transition

Fast Transition

Over the DS

Reassociation Timeout 20 Seconds

Lobby Admin Configuration

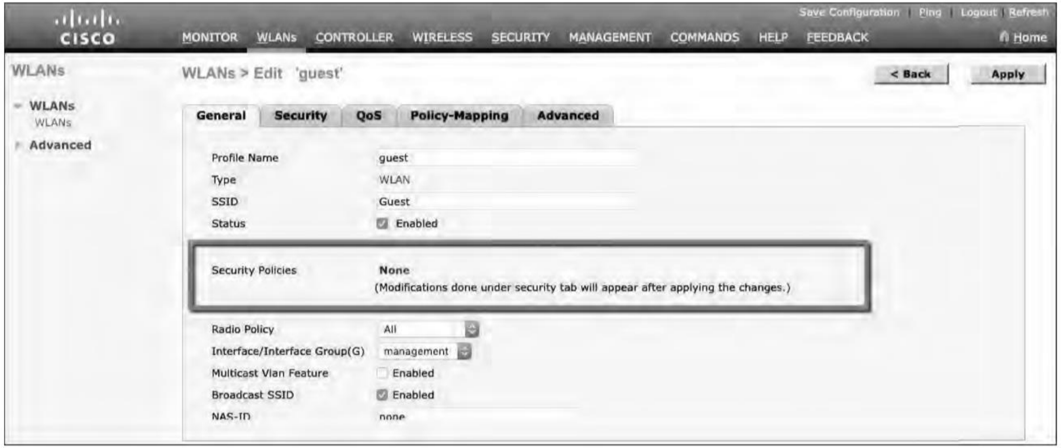
Lobby Admin Access □

Figure 20-2 *Configuring Open Authentication for a WLAN*

Creating a WLAN with Open Authentication (Cont.)

You can verify the WLAN and its security settings from the WLANs > Edit General tab, as shown in Figure 20-3 or from the list of WLANs, as shown in Figure 20-4.

In both figures, the Security Policies field is shown as None. You can also verify that the WLAN status is enabled and active.



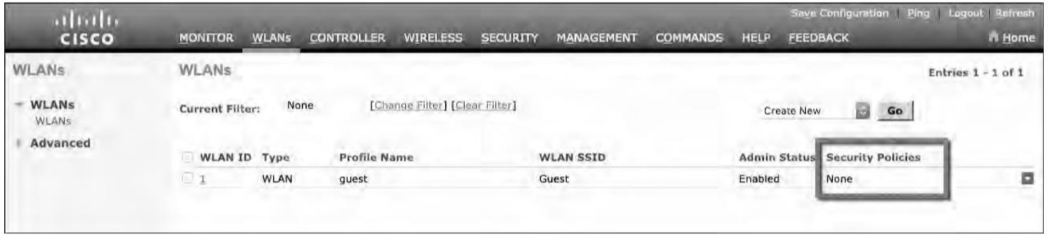
WLANs > Edit 'guest'

Profile Name: guest
Type: WLAN
SSID: Guest
Status: ☑ Enabled

Security Policies: None
(Modifications done under security tab will appear after applying the changes.)

Radio Policy: All
Interface/Interface Group(G): management
Multicast Vlan Feature: □ Enabled
Broadcast SSID: ☑ Enabled
NAS-ID: none

Figure 20-3 *Verifying Open Authentication in the WLAN Configuration*



WLANs

Entries 1 - 1 of 1

Current Filter: None [Change Filter] [Clear Filter]

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

Figure 20-4 *Verifying Open Authentication from List of WLANs*

Authenticating with Pre-Shared Key

- To secure wireless connections on a WLAN, you 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.
- All three WPA versions support two client authentication modes, Pre-Shared Key (PSK) or 802.1x, depending on the scale of the deployment.

Authenticating with Pre-Shared Key

Wi-Fi Protected Access PSK

To secure wireless connections on a WLAN, you can leverage one of the Wi-Fi Protected Access (WPA) versions: WPA (also known as WPA1), WPA2, or WPA3. The WPA versions also specify encryption and data integrity methods to protect data passing over the wireless connections.

All three WPA versions support two client authentication modes, Pre-Shared Key (PSK) or 802.1x, depending on the scale of the deployment. These are also known as personal mode and enterprise mode, respectively.

Personal mode:

- A key string must be shared or configured on every client and AP before the clients can connect to the wireless network.
- The pre-shared key is normally kept confidential so that unauthorized users have no knowledge of it.
- Clients and APs work through a four-way handshake procedure that uses the pre-shared key string to construct and exchange encryption key material that can be openly exchanged. When that process is successful, the AP can authenticate the client, and the two can secure data frames that are sent over the air.

Authenticating with Pre-Shared Key

Simultaneous Authentication of Equals (SAE)

With WPA-Personal and WPA2-Personal modes, a malicious user can eavesdrop and capture the four-way handshake between a client and an AP. A dictionary attack can be used to automate the guessing of the pre-shared key. If successful, the malicious user can then decrypt the wireless data or even join the network, posing as a legitimate user.

WPA3-Personal avoids such an attack by strengthening the key exchange between clients and APs through a method known as Simultaneous Authentication of Equals (SAE). Rather than a client authenticating against a server or AP, the client and AP can initiate the authentication process equally and even simultaneously.

Even if a password or key is compromised, WPA3-Personal offers forward secrecy, which prevents attackers from being able to use a key to unencrypt data that has already been transmitted over the air.

The personal mode of any WPA version is usually easy to deploy in a small environment.

Authenticating with Pre-Shared Key

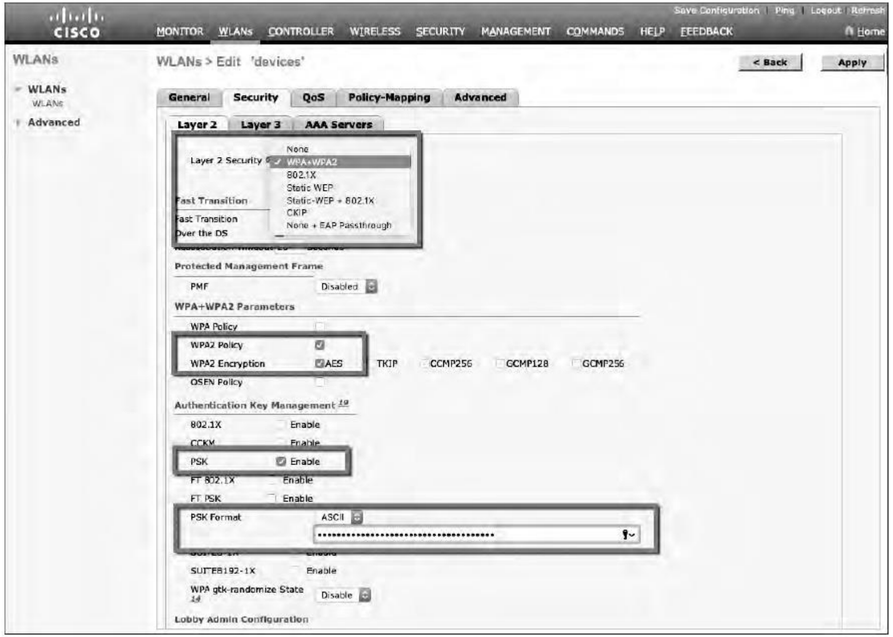
Configuring PSK

You can configure WPA2 or WPA3 personal mode and the pre-shared key with these steps:

Step 1. Navigate to WLANs, select Create New or select the WLAN ID of an existing WLAN to edit. Make sure the parameters on the General tab are set appropriately.

Step 2. Next, select the Security > Layer 2 tab. In the Layer 2 Security drop-down menu, select the appropriate WPA version for the WLAN. In Figure 20-5, WPA+WPA2 has been selected for the WLAN named devices.

Step 3. Under WPA+WPA2 Parameters, the WPA version has been narrowed to only WPA2 by unchecking the box next to WPA and checking both WPA2 Policy and WPA2 Encryption AES.



WLANs > Edit 'devices'

Layer 2 Security: WPA+WPA2

Fast Transition

Fast Transition Over the DS

Protected Management Frame

PMF: Disabled

WPA+WPA2 Parameters

WPA Policy □

WPA2 Policy ☑

WPA2 Encryption ☑ AES □ TKIP □ CCMP256 □ GCMP128 □ GCMP256

OSEN Policy □

Authentication Key Management 19

802.1X □ Enable

CCKM □ Enable

PSK ☑ Enable

FT 802.1X □ Enable

FT PSK □ Enable

PSK Format: ASCII

••

SUITEB192-1X □ Enable

WPA gtk-randomize State 14: Disable

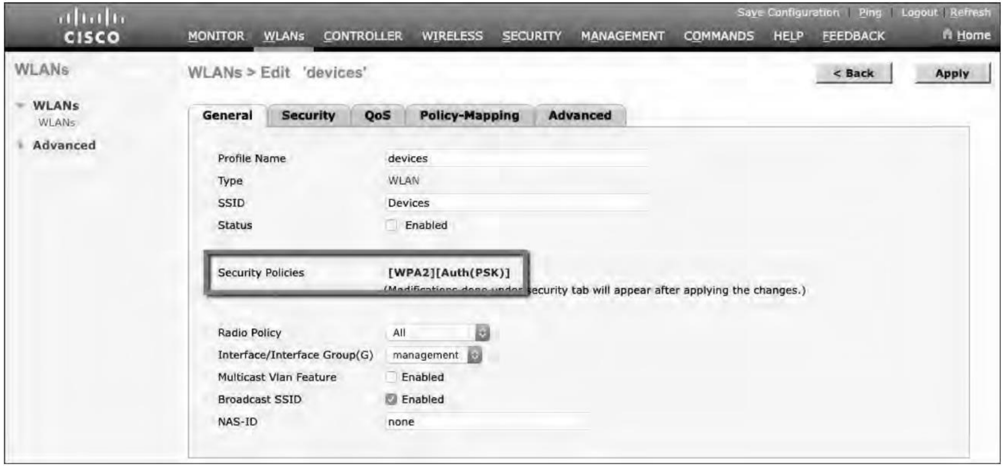
Lobby Admin Configuration

Figure 20-5 *Selecting the WPA2 Personal Security Suite for a WLAN*

Authenticating with Pre-Shared Key

Verifying PSK

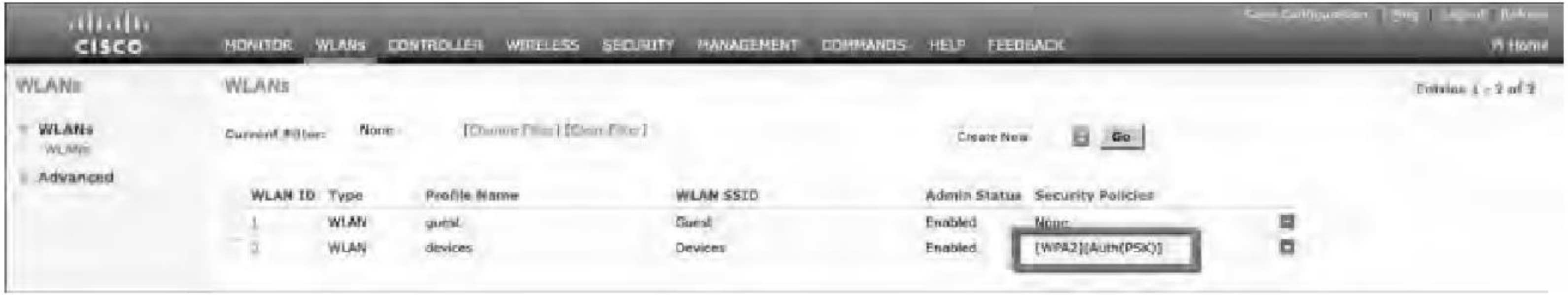
You can verify the WLAN and its security settings from the WLANs > Edit General tab, as shown in Figure 20-6 or from the list of WLANs, as shown in Figure 20-7. In both figures, the Security Policies field is shown as [WPA2][Auth(PSK)]. You can also verify that the WLAN status is enabled and active.



WLANs > Edit 'devices'

Profile Name	devices
Type	WLAN
SSID	Devices
Status	□ Enabled
Security Policies	[WPA2][Auth(PSK)] (Modifications done under security tab will appear after applying the changes.)
Radio Policy	All
Interface/Interface Group(G)	management
Multicast Vlan Feature	□ Enabled
Broadcast SSID	☑ Enabled
NAS-ID	none

Figure 20-6 *Verifying PSK Authentication in the WLAN Configuration*



WLANs

Entries 1 - 2 of 2

Current Filter: None

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)]

Figure 20-7 *Verifying PSK Authentication from the List of WLANs*

Authenticating with EAP

- Rather than build additional authentication methods into the 802.11 standard, Extensible Authentication Protocol (EAP) offers a more flexible and scalable authentication framework.
- 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.
- 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.

Authenticating with EAP
802.1x Client Authentication Roles

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.

Figure 20-8 shows the three-party 802.1x arrangement, which consists of the following entities:

- **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).

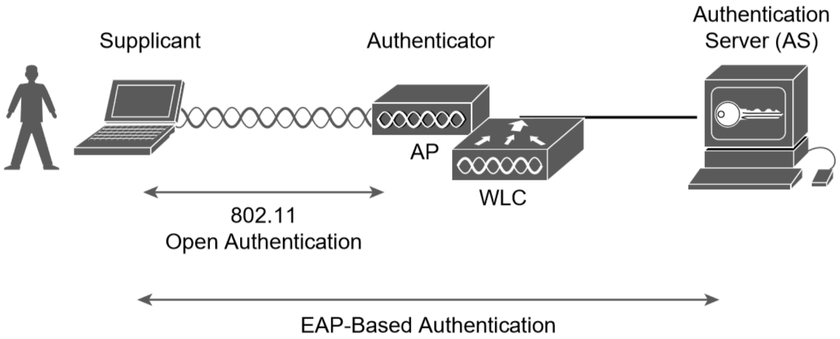


Figure 20-8 *802.1x Client Authentication Roles*

The controller becomes a middleman in the client authentication process, controlling user access with 802.1x and communicating with the authentication server using the EAP framework.

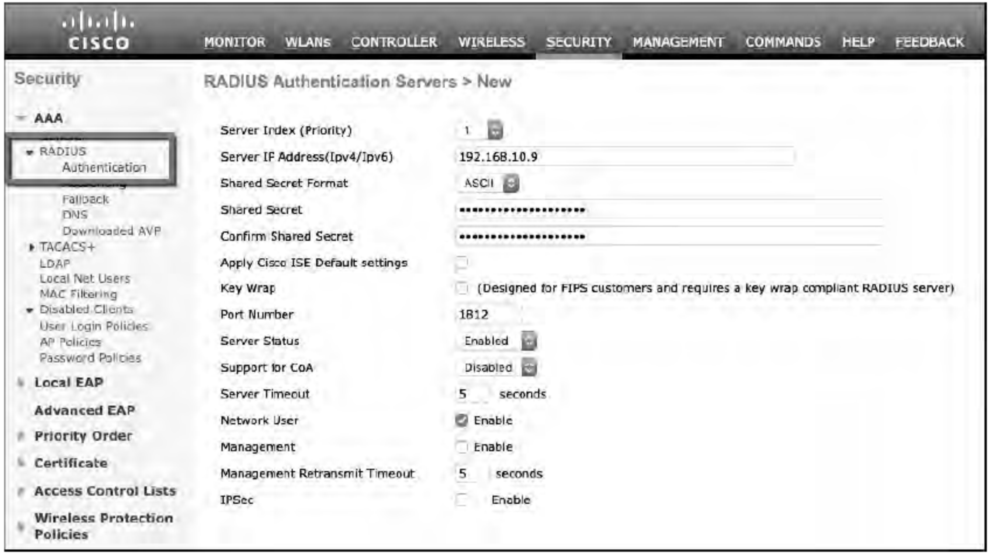
Authenticating with EAP

Configuring EAP-Based Authentication with External RADIUS Servers

Cisco WLCs can use either external RADIUS servers located somewhere on the wired network or a local EAP server located on the WLC.

You should begin by configuring one or more external RADIUS servers on the controller. Navigate to Security > AAA > RADIUS > Authentication.

- Click the New button to define a new server or select the Server Index number to edit an existing server definition.
- Enter the server's IP address and the shared secret key that the controller will use to communicate with the server.



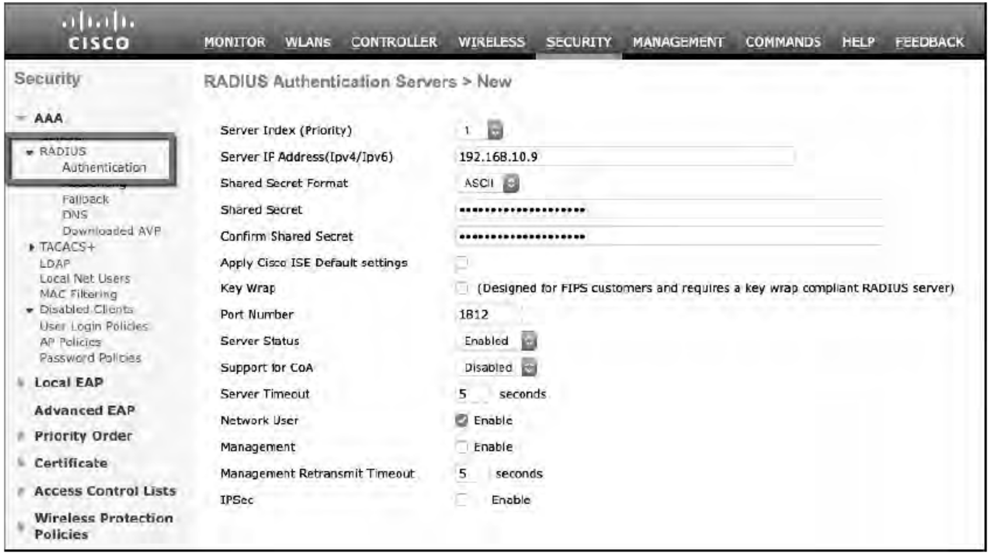
RADIUS Authentication Servers > New

Server Index (Priority)	1
Server IP Address(Ipv4/Ipv6)	192.168.10.9
Shared Secret Format	ASCII
Shared Secret	••••••••••••••••••••
Confirm Shared Secret	••••••••••••••••••••
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

Figure 20-9 *Defining a RADIUS Server for WPA2 Enterprise Authentication*

Configuring EAP-Based Authentication with External RADIUS Servers (Cont.)

- Make sure that the RADIUS port number is correct.
- The server status should be Enabled, as selected from the drop-down menu. You can disable a server to take it out of service if needed.
- To authenticate wireless clients, check the Enable box next to Network User. Click the Apply button to apply the new settings.



RADIUS Authentication Servers > New

Server Index (Priority)	1
Server IP Address(Ipv4/Ipv6)	192.168.10.9
Shared Secret Format	ASCII
Shared Secret	••••••••••••••••••••
Confirm Shared Secret	••••••••••••••••••••
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

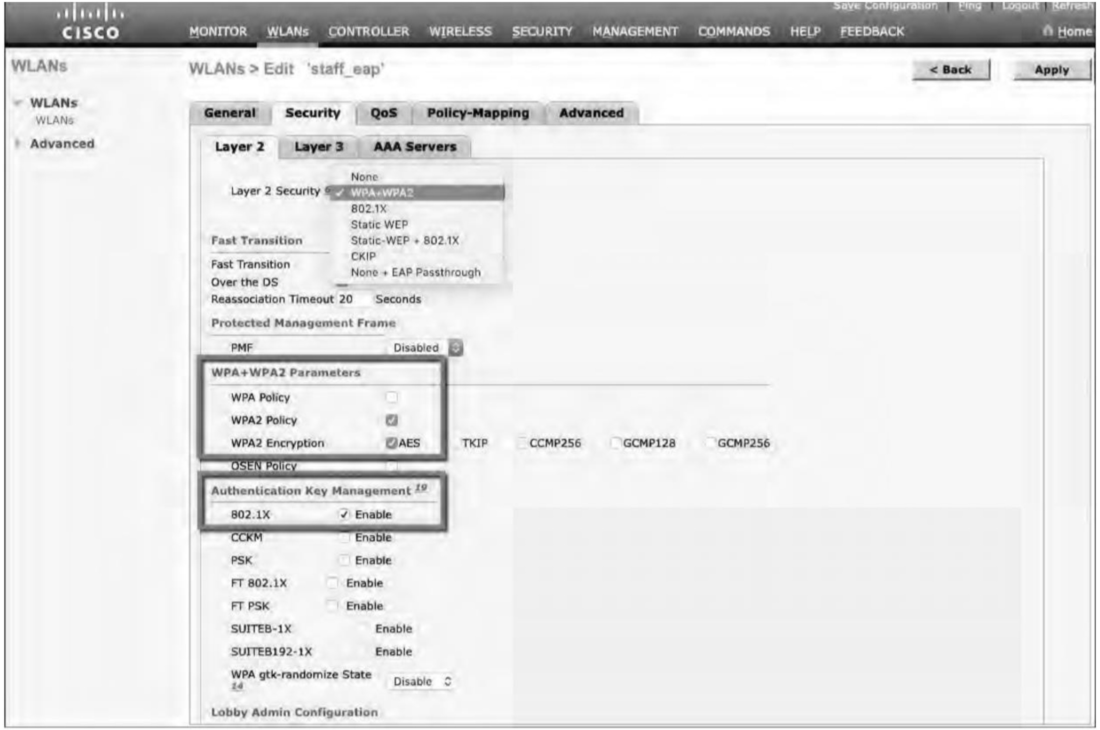
Figure 20-9 *Defining a RADIUS Server for WPA2 Enterprise Authentication*

Authenticating with EAP

Configuring EAP-Based Authentication with External RADIUS Servers (Cont.)

Next, you need to enable 802.1x authentication on the WLAN. Navigate to WLANs and select a new or existing WLAN to edit.

Figure 20-10 illustrates the settings that are needed on the WLAN named staff_eap.



WLANs > Edit 'staff_eap'

Layer 2 Security: ✓ WPA+WPA2

Fast Transition

Fast Transition Over the DS

Reassociation Timeout 20 Seconds

Protected Management Frame

PMF: Disabled

WPA+WPA2 Parameters

WPA Policy □

WPA2 Policy ☑

WPA2 Encryption ☑ AES □ TKIP □ CCMP256 □ GCMP128 □ GCMP256

OSEN Policy □

Authentication Key Management [19]

802.1X ☑ Enable

CCKM □ Enable

PSK □ Enable

FT 802.1X □ Enable

FT PSK □ Enable

SUITEB-1X Enable

SUITEB192-1X Enable

WPA gtk-randomize State [14]: Disable

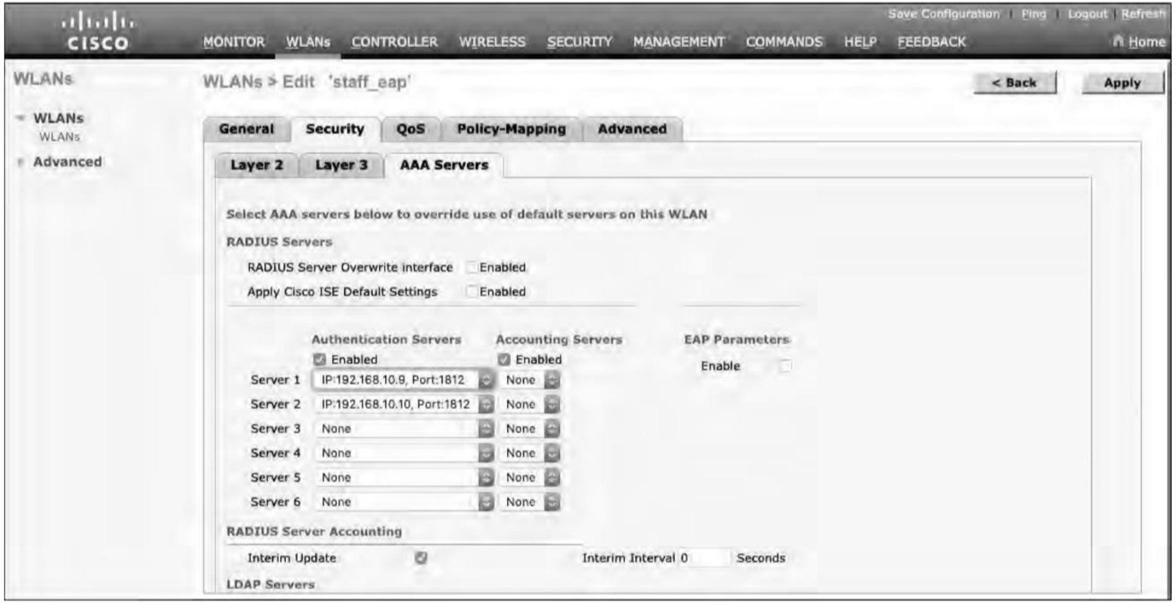
Lobby Admin Configuration

Figure 20-10 *Enabling WPA2 Enterprise Mode with 802.1x Authentication*

Configuring EAP-Based Authentication with External RADIUS Servers (Cont.)

By default, a controller uses the global list of RADIUS servers in the order you have defined under Security > AAA > RADIUS > Authentication.

You can override that list on the AAA Servers tab, where you can define which RADIUS servers will be used for 802.1x authentication.



WLANs > Edit 'staff_eap'

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	EAP Parameters
	☑ Enabled	☑ Enabled	Enable □
Server 1	IP:192.168.10.9, Port:1812	None	
Server 2	IP:192.168.10.10, Port:1812	None	
Server 3	None	None	
Server 4	None	None	
Server 5	None	None	
Server 6	None	None	

RADIUS Server Accounting

Interim Update ☑ Interim Interval 0 Seconds

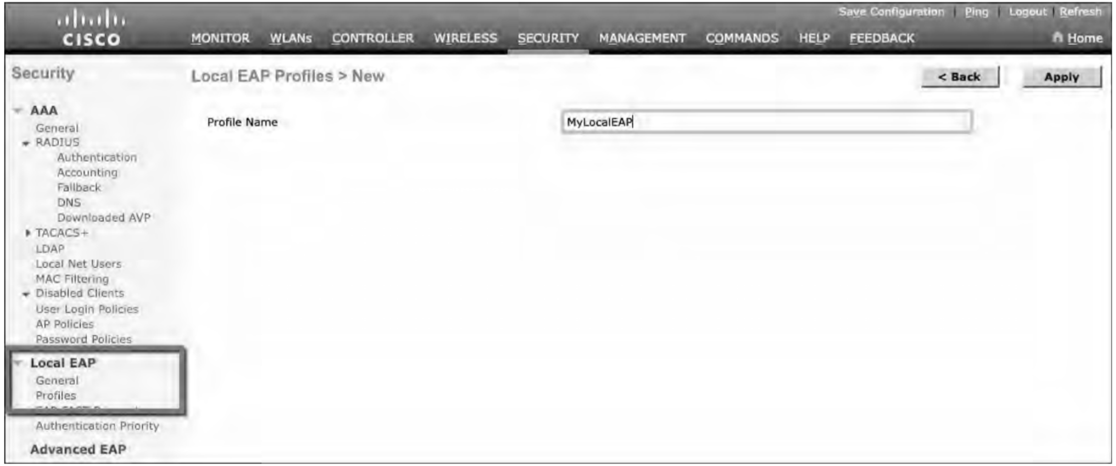
LDAP Servers

Figure 20-11 *Selecting RADIUS Servers to Authenticate Clients in the WLAN*

Authenticating with EAP

Configuring EAP-Based Authentication with Local EAP

- If your environment is small or you do not have a RADIUS server in production, you can use an authentication server that is built in to the WLC. This is called Local EAP, and it supports LEAP, EAP-FAST, PEAP, and EAP-TLS.
- Define and enable the local EAP service on the controller. Navigate to Security > Local EAP > Profiles and click the New button. Enter a name for the Local EAP profile, which will be used to define the authentication server methods.



Profile Name: MyLocalEAP

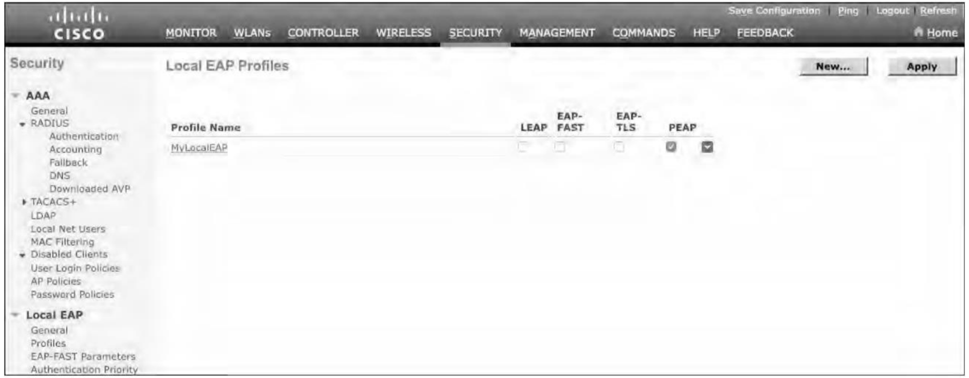
Figure 20-12 *Defining a Local EAP Profile on a Controller*

In Figure 20-12, a new profile called MyLocalEAP has been defined.

Authenticating with EAP

Configuring EAP-Based Authentication with Local EAP (Cont.)

Now you should see the new profile listed, along with the authentication methods it supports, as shown in Figure 20-13. From this list, you can check or uncheck the boxes to enable or disable each method.

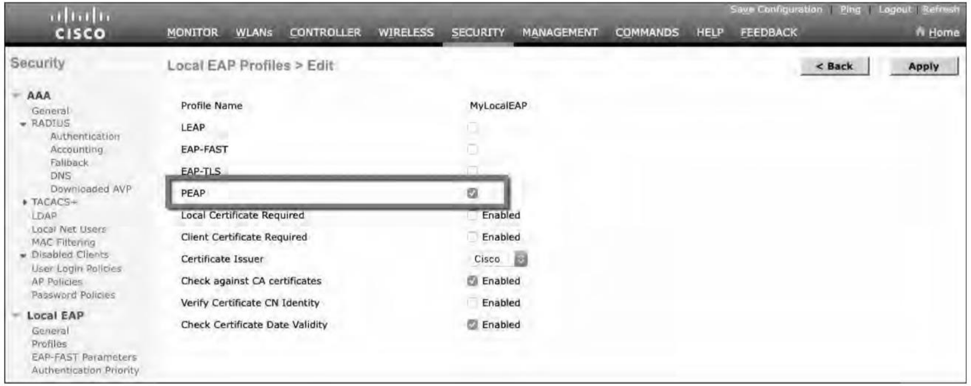


Local EAP Profiles

Profile Name	LEAP	EAP-FAST	EAP-TLS	PEAP	
MyLocalEAP	□	□	□	☑	▾

Figure 20-13 *Displaying Configured Local EAP Profiles*

Select the profile name to edit its parameters. In Figure 20-14, the profile named MyLocalEAP has been configured to use PEAP. Click the Apply button to activate your changes.



Local EAP Profiles > Edit

Profile Name	MyLocalEAP
LEAP	□
EAP-FAST	□
EAP-TLS	□
PEAP	☑
Local Certificate Required	□ Enabled
Client Certificate Required	□ Enabled
Certificate Issuer	Cisco ▾
Check against CA certificates	☑ Enabled
Verify Certificate CN Identity	□ Enabled
Check Certificate Date Validity	☑ Enabled

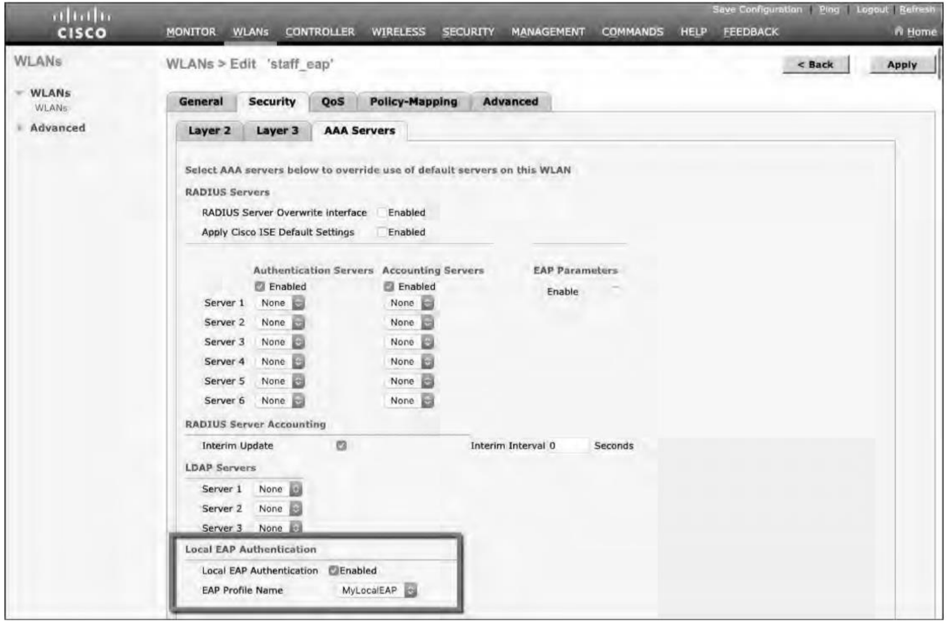
Figure 20-14 *Configuring a Local EAP Profile to Use PEAP*

Authenticating with EAP

Configure WLAN to Local EAP

Next, you need to configure the WLAN to use the Local EAP server rather than a regular external RADIUS server. Navigate to WLANs, select the WLAN ID, and then select the Security > Layer 2 tab and enable WPA2, AES, and 802.1x as before.

If you have defined any RADIUS servers in the global list under Security > AAA > RADIUS > Authentication or any specific RADIUS servers in the WLAN configuration, the controller will use those first. Local EAP will then be used as a backup method.



WLANs > Edit 'staff_eap'

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
	☑ Enabled	☑ Enabled
Server 1	None	None
Server 2	None	None
Server 3	None	None
Server 4	None	None
Server 5	None	None
Server 6	None	None

EAP Parameters

Enable

RADIUS Server Accounting

Interim Update ☑ Interim Interval 0 Seconds

LDAP Servers

Server 1	None
Server 2	None
Server 3	None

Local EAP Authentication

Local EAP Authentication ☑ Enabled

EAP Profile Name MyLocalEAP

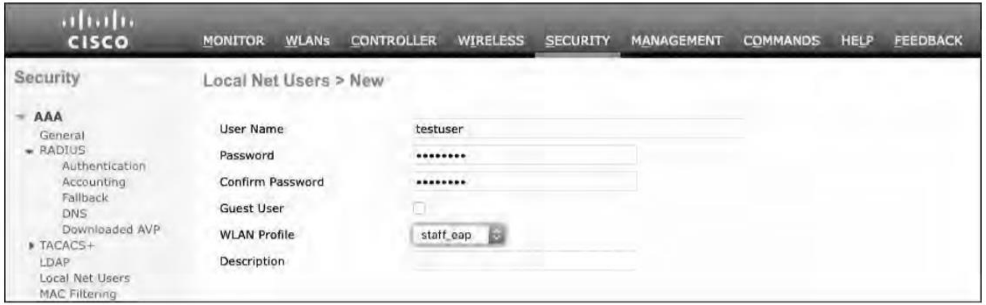
Figure 20-15 *Enabling Local EAP Authentication for a WLAN*

Authenticating with EAP

Verifying Configuration

Because the Local EAP server is local to the controller, you will have to maintain a local database of users or define one or more LDAP servers on the controller. You can create users by navigating to Security > AAA > Local Net Users. In Figure 20-16, a user named testuser has been defined and authorized for access to the staff_eap WLAN.

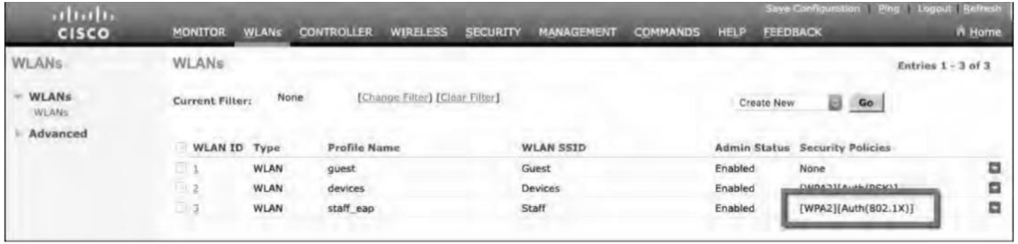
You can verify the WLAN and its security settings from the list of WLANs by selecting WLANs > WLAN, as shown in Figure 20-17.



Local Net Users > New

User Name	testuser
Password	•••••••••
Confirm Password	•••••••••
Guest User	□
WLAN Profile	staff_eap
Description	

Figure 20-16 *Creating a Local User for Local EAP Authentication*



WLANs

Entries 1 - 3 of 3

Current Filter: None [Change Filter] [Clear Filter]

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(802.1X)]

Figure 20-17 *Verifying EAP Authentication on a WLAN*

Authenticating with WebAuth

- You might have noticed that none of the authentication methods described so far involve direct interaction with the end user.
- Web Authentication (WebAuth) is different because it presents the end user with content to read and interact with before granting access to the network.
- WebAuth can be used as an additional layer in concert with Open Authentication, PSK-based authentication, and EAP-based authentication.

Local Web Authentication

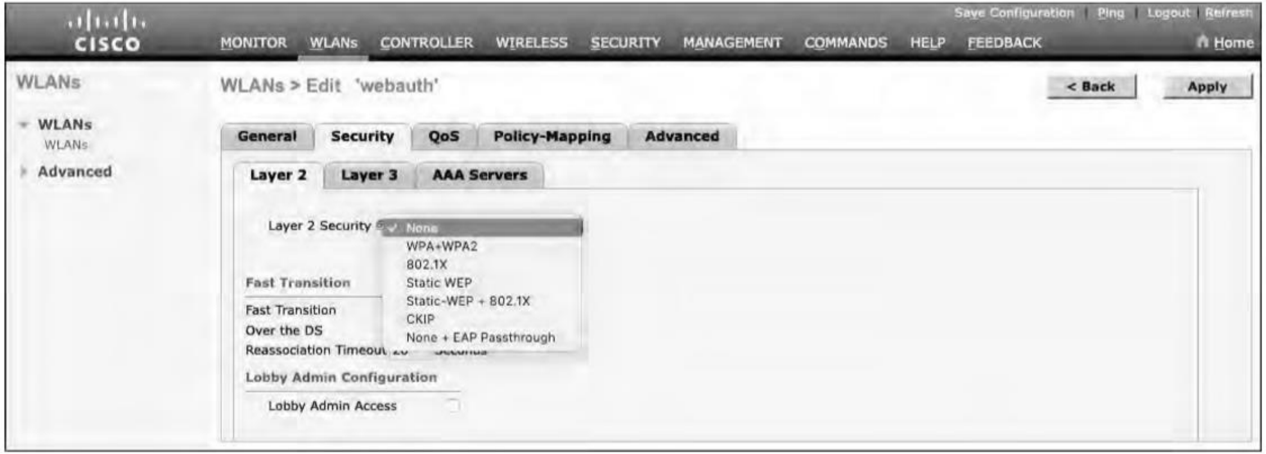
Web Authentication can be handled locally on the WLC for smaller environments through Local Web Authentication (LWA). You can configure LWA in the following modes:

- LWA with an internal database on the WLC
- LWA with an external database on a RADIUS or LDAP server
- LWA with an external redirect after authentication
- LWA with an external splash page redirect, using an internal database on the WLC
- LWA with passthrough, requiring user acknowledgment

When there are many controllers providing Web Authentication, it makes sense to use LWA with an external database on a RADIUS server, such as ISE, and keep the user database centralized. The next logical progression is to move the Web Authentication page onto the central server, too. This is called Central Web Authentication (CWA).

Configure WebAuth on WLAN

- First create the new WLAN and map it to the correct VLAN.
- Go to the General tab and enter the SSID string, apply the appropriate controller interface, and change the status to Enabled.
- On the Security tab, select the Layer 2 tab to choose a wireless security scheme to be used on the WLAN.



WLANs > Edit 'webauth'

Layer 2 Security ✓ None

Fast Transition

Over the DS

Reassociation Timeout 20 Seconds

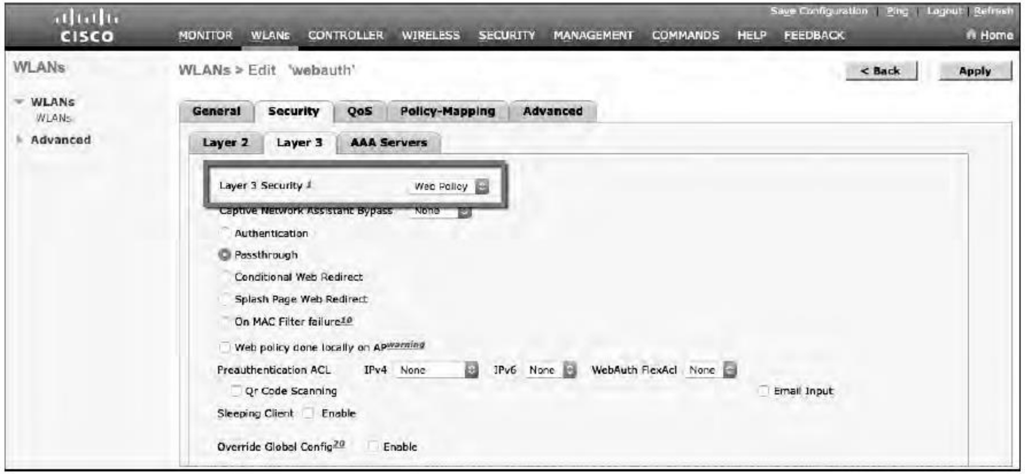
Lobby Admin Access □

Figure 20-18 *Configuring Open Authentication for WebAuth*

In Figure 20-18, the WLAN is named webauth, the SSID is Guest_webauth, and Open Authentication will be used because the None method has been selected.

Authenticating with WebAuth
Configure WebAuth on WLAN (Cont.)

- Next, select the Security > Layer 3 tab and choose the Layer 3 Security type Web Policy, as shown in Figure 20-19.
- When the Authentication radio button is selected (the default), Web Authentication will be performed locally on the WLC by prompting the user for credentials that will be checked against RADIUS, LDAP, or local EAP servers.
- In the figure, Passthrough has been selected, which will display web content such as an acceptable use policy to the user and prompt for acceptance.
- Through the other radio buttons, WebAuth can redirect the user to an external web server for content and interaction. Click the Apply button to apply the changes to the WLAN configuration.



WLANs > Edit 'webauth'

Layer 3 Security [1] Web Policy

Captive Network Assistant Bypass None

○ Authentication

● Passthrough

○ Conditional Web Redirect

○ Splash Page Web Redirect

○ On MAC Filter failure[10]

□ Web policy done locally on AP[warning]

Preauthentication ACL IPv4 None IPv6 None WebAuth FlexAcl None

□ Qr Code Scanning □ Email Input

Sleeping Client □ Enable

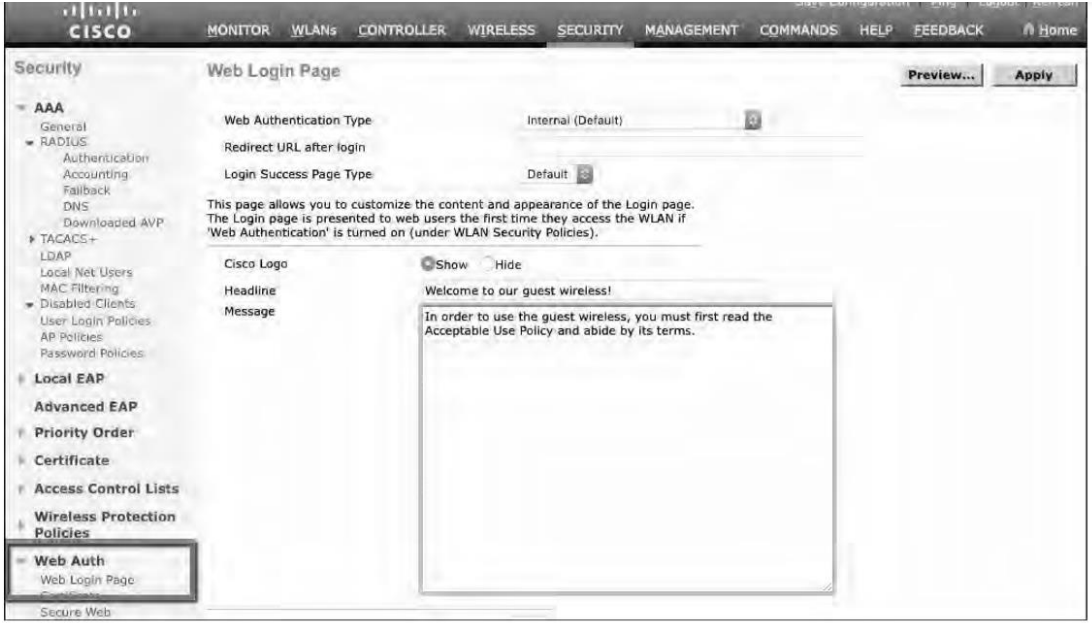
Override Global Config[20] □ Enable

Figure 20-19 *Configuring WebAuth with Passthrough Authentication*

Configure WebAuth on WLAN (Cont.)

You will need to configure the WLC’s local web server with content to display during a WebAuth session.

Navigate to Security > Web Auth > Web Login Page, as shown in Figure 20-20. By default, internal WebAuth is used. You can enter the web content that will be displayed to the user by defining a text string to be used as the headline, as well as a block of message text.



Web Login Page

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.

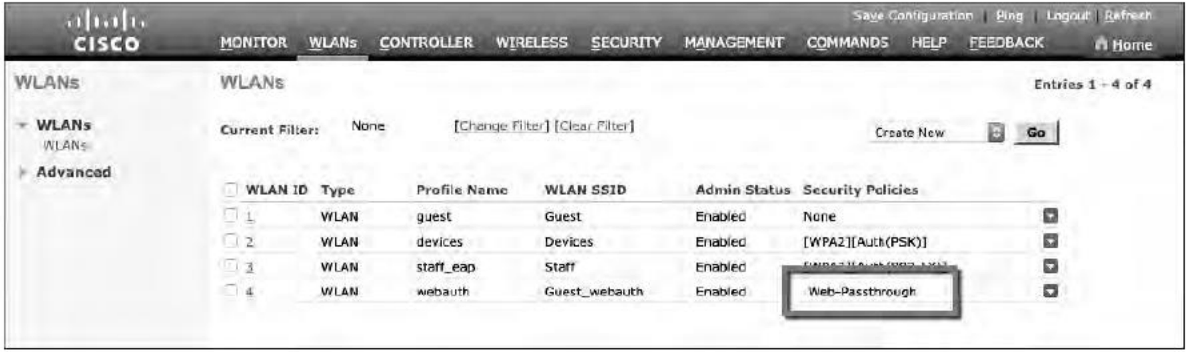
Figure 20-20 *Configuring the WebAuth Page Content*

Authenticating with WebAuth

Verifying WebAuth on a WLAN

You can verify the WebAuth security settings from the list of WLANs by selecting WLANs > WLAN.

In Figure 20-22, WLAN 4 with SSID Guest_webauth is shown to use the Web-Passthrough security policy. You can also verify that the WLAN status is enabled and active.



WLANs

Entries 1 - 4 of 4

Current Filter: None [Change Filter] [Clear Filter]

□ 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(802.1X)]
□ 4	WLAN	webauth	Guest_webauth	Enabled	Web-Passthrough

Figure 20-22 *Verifying WebAuth Authentication on a WLAN*

Prepare for the Exam

Prepare for the Exam

Key Topics for Chapter 20

Description
WPA personal mode for PSK
802.1x roles
WPA enterprise mode for EAP
WebAuth modes

Prepare for the Exam
Key Terms for Chapter 20

Term	
802.1x	RADIUS server
authentication server (AS)	supplicant
authenticator	Wi-Fi Protected Access (WPA)
Extensible Authentication Protocol (EAP)	WPA Version 2 (WPA2)
Open Authentication	WPA Version 3 (WPA3)
personal mode	