Configuring Authentication Types

This chapter describes how to configure authentication types on the access point.

Understanding Authentication Types

This section describes in detail the authentication types that you can configure on the access point. The authentication types are tied to the SSIDs that you configure for the access point. The SSID is then tied to a VLAN or a radio interface with a possible configured encryption mechanism. Hence, make sure that the authentication scheme you configure for the SSID is compatible with the encryption method configured for the associated VLAN or radio interface.

See Chapter 10, "Understanding Authentication and Encryption Mechanisms," section for more details. If you want to serve different types of client devices with the same access point, you can configure multiple SSIDs. See Chapter 7, "Configuring Multiple SSIDs." for complete instructions on configuring multiple SSIDs.

Before a wireless client device can communicate on your network through the access point, it must authenticate to the access point using open or shared-key authentication. For maximum security, client devices should also authenticate to your network using MAC-address or EAP authentication, both of which rely on an authentication server on your network.

The authentication server can be configured on the AP or on an external server. You can set the client authentication process to be as follows:

1. The client can authenticate to the access point (using open or shared key).
2. During the association phase, optionally the client can be authenticated using it's MAC address
3. After association to the AP, optionally the client can be authenticated against a RADIUS server,
4. Individual client key generation and management can be done using EAP/802.1x. EAP/802.1x mechanism.

Note By default, the access point sends re-authentication requests to the authentication server with the service-type attribute set to authenticate-only. However, some Microsoft IAS servers do not support the authenticate-only service-type attribute. Depending on the user requirements, set the service-type attribute to: **dot11 aaa authentication attributes service-type login-user** or **dot11 aaa authentication attributes service-type framed-user**. By default the service type "login" is sent in the access request.

The access point uses several authentication mechanisms or types and can use more than one at the same time. These sections explain each authentication type:

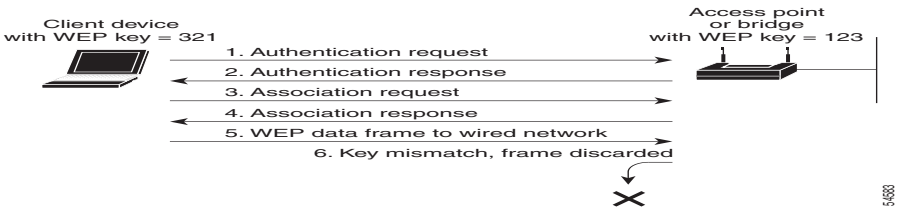
Open Authentication to the Access Point

Open authentication allows any device to authenticate and then attempt to communicate with the access point. Using open authentication, any wireless device can authenticate with the access point, Open authentication does not rely on a RADIUS server on your network.

In a scenario where you use Open authentication and WEP encryption, authentication will be successful even if the client and the AP WEP are mismatched. The client will not be able to send data (including DHCP requests) after Open authentication completes. However, with Open authentication and no encryption, the wireless client can transmit data as soon as the association phase is complete.

Figure 11-1 shows the authentication sequence between a device trying to authenticate and an access point using open authentication. In this example, the device's WEP key does not match the access point's key, so it can authenticate but not pass data.

Figure 11-1 Sequence for Open Authentication



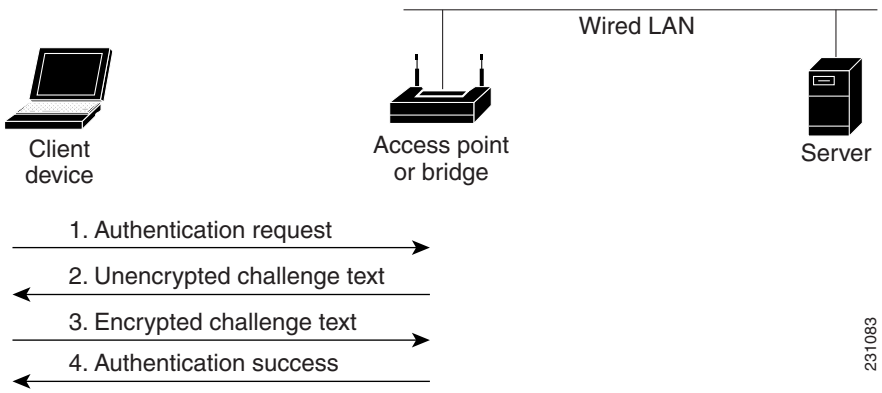
WEP Shared Key Authentication to the Access Point

Cisco provides shared key authentication to comply with WEP authentication described in the 802.11 standard. However, because of a shared key's security flaws WEP has been deprecated. The IEEE and Cisco recommend that you avoid using it.

During shared key authentication, the access point sends an unencrypted challenge text string to any device attempting to communicate with the access point. The device requesting authentication encrypts the challenge text and sends it back to the access point. If the challenge text is encrypted correctly, the access point allows the requesting device to authenticate. Both the unencrypted challenge and the encrypted challenge can be monitored, however, which leaves the access point open to attack from an intruder who calculates the WEP key by comparing the unencrypted and encrypted text strings. Because of this weakness, shared key authentication can be less secure than open authentication. Like open authentication, shared key authentication does not rely on a RADIUS server on your network.

Figure 11-2 shows the authentication sequence between a device trying to authenticate and an access point using shared key authentication. In this example the device's WEP key matches the access point's key, so it can authenticate and communicate.

Figure 11-2 Sequence for Shared Key Authentication



EAP Authentication to the Network

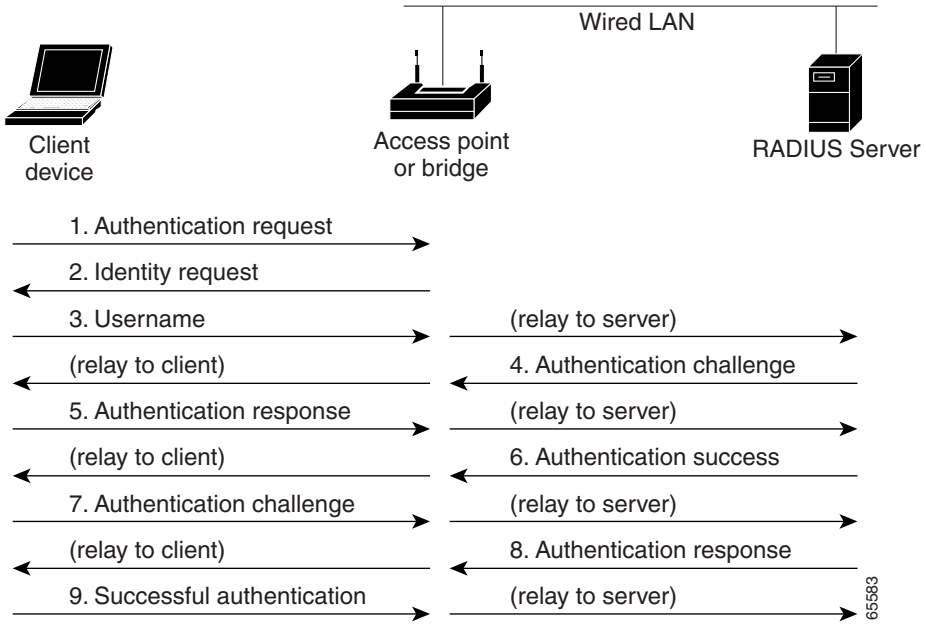
This authentication type provides the highest level of security for your wireless network. By using the Extensible Authentication Protocol (EAP) to interact with an EAP-compatible RADIUS server, the access point helps a wireless client device and the RADIUS server to perform mutual authentication and derive a dynamic unicast key. The RADIUS server sends the key to the access point, which uses it for all unicast data signals that it sends to or receives from the client. The access point also encrypts its broadcast key with the client's unicast key and sends it to the client.

Depending on the underlying security framework (802.1X with dynamic WEP, WPA or WPA 2), the key is used:

- In the case of WEP – directly by the Access Point for all unicast data signals that it sends to or receives from the client,
- In the case of WPAv1/v2 – the key is used to derive unicast keys that are used for all unicast data signals that it sends to or receives from the client.

When you enable EAP on your access points and client devices, authentication to the network occurs in the sequence shown in Figure 11-3:

Figure 11-3 Sequence for EAP Authentication



In Steps 1 through 9 in Figure 11-3, a wireless client device and a RADIUS server on the wired LAN use 802.1x and EAP to perform a mutual authentication through the access point. The RADIUS server sends an authentication challenge to the client. The client uses a one-way encryption of the user-supplied or machine-supplied credentials to generate a response to the challenge and sends that response to the RADIUS server. Using information from its user database, the RADIUS server creates its own response and compares that to the response from the client. When the RADIUS server authenticates the client, the process repeats in reverse, and the client authenticates the RADIUS server.

When mutual authentication is complete, the RADIUS server and the client determine a a WEP key or a Pairwise Master Key (WPAv1/v2) that is unique to the client and provides the client with the appropriate level of network access, thereby approximating the level of security in a wired switched segment to an individual desktop. The client loads this key and prepares to use it for the logon session.

During the logon session, the RADIUS server encrypts and sends the WEP key, or the WPAv1/v2 Pairwise Master Key, over the wired LAN to the access point. The AP uses this key to encrypt its broadcast key, and sends the encrypted broadcast key to the client, which uses its identical unicast key to decrypt it. The client and access point activate encryption and use the unicast and broadcast keys for all communications during the remainder of the session.

There is more than one type of EAP authentication, but the access point behaves the same way for each type: it relays authentication messages from the wireless client device to the RADIUS server and from the RADIUS server to the wireless client device. See the "Assigning Authentication Types to an SSID" section on page 11-9 for instructions on setting up EAP on the access point.

Note If you use EAP authentication, you can select open or shared key authentication, but you do not have to. EAP authentication controls authentication both to your access point and to your network.

MAC Address Authentication to the Network

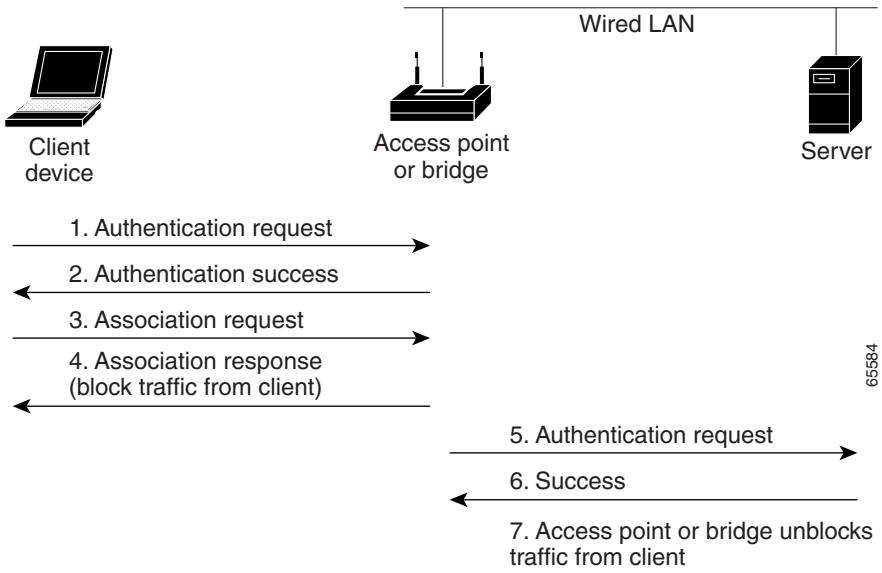
The access point relays the wireless client device's MAC address to a RADIUS server on your network, and the server checks the address against a list of allowed MAC addresses. Intruders can create counterfeit MAC addresses, so MAC-based authentication is less secure than EAP authentication. However, MAC-based authentication provides an alternate authentication method for client devices that do not have EAP capability. See the "Assigning Authentication Types to an SSID" section on page 11-9 for instructions on enabling MAC-based authentication.

Tip If you do not have a RADIUS server on your network, you can create a list of allowed MAC addresses on the access point's Advanced Security: MAC Address Authentication page. Devices with MAC addresses not on the list are not allowed to authenticate.

Tip If MAC-authenticated clients on your wireless LAN roam frequently, you can enable a MAC authentication cache on your access points. MAC authentication caching reduces overhead because the access point authenticates devices in its MAC-address cache without sending the request to your authentication server. See the "Configuring MAC Authentication Caching" section on page 11-15 for instructions on enabling this feature.

Figure 11-4 shows the authentication sequence for MAC-based authentication.

Figure 11-4 Sequence for MAC-Based Authentication



Combining MAC-Based, EAP, and Open Authentication

You can set up the access point to authenticate client devices using a combination of MAC-based and EAP authentication. When you enable this feature, client devices that associate to the access point using 802.11 open authentication first attempt MAC authentication; if MAC authentication succeeds, the client device joins the network. If MAC authentication fails, EAP authentication takes place. See the "Assigning Authentication Types to an SSID" section on page 11-9 for instructions on setting up this combination of authentications.

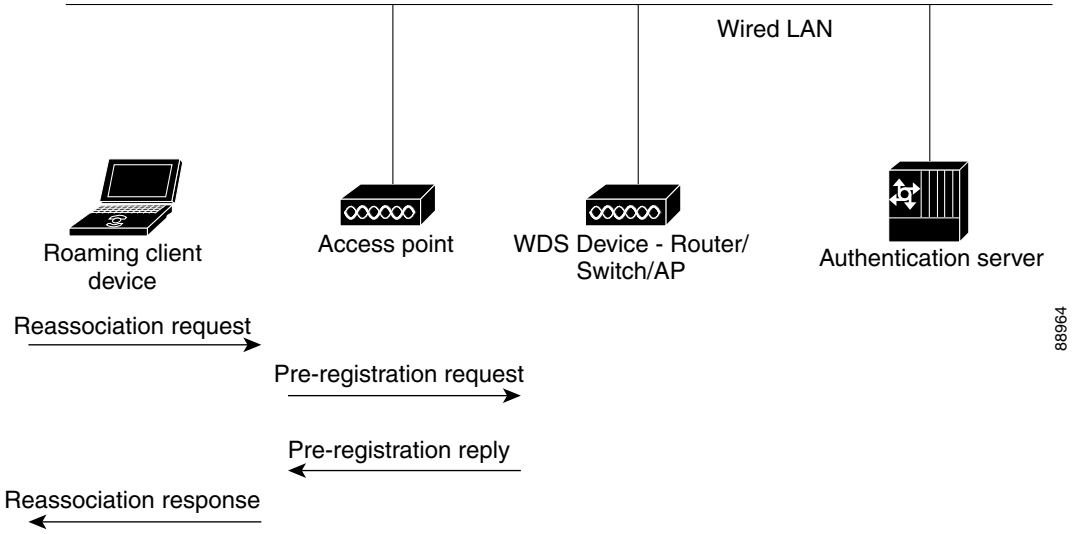
Using CCKM for Authenticated Clients

Using Cisco Centralized Key Management (CCKM), authenticated client devices can roam from one access point to another without any perceptible delay during reassociation. An access point on your network provides Wireless Domain Services (WDS) and creates a cache of security credentials for CCKM-enabled client devices on the subnet. The WDS access point's cache of credentials dramatically reduces the time required for reassociation when a CCKM-enabled client device roams to a new access point. When a client device roams, the WDS access point forwards the client's security credentials to the new access point, and the reassociation process is reduced to a two-packet exchange between the roaming client and the new access point. Roaming clients reassociate so quickly that there is no perceptible delay in voice or other time-sensitive applications. See the "Assigning Authentication Types to an SSID" section on page 11-9 for instructions on enabling CCKM on your access point. See the "Configuring Access Points as Potential WDS Devices" section on page 12-7 for detailed instructions on setting up a WDS access point on your wireless LAN.

Note The RADIUS-assigned VLAN feature is not supported for client devices that associate using SSIDs with CCKM enabled.

Figure 11-5 shows the reassociation process using CCKM.

Figure 11-5 Client Reassociation Using CCKM



Using WPA Key Management

WPAv1 is a Wi-Fi Alliance certification based on an early draft of the 802.11i amendment. WPAv1 leverages TKIP (Temporal Key Integrity Protocol) for data protection. WPAv2 is a Wi-Fi Alliance certification based on the final 802.11i amendment published in the year 2004. WPAv2 leverages AES (Advanced Encryption Standard) with the Counter-Mode Cipher Block Chaining (CBC) Message Authentication Code (MAC) Protocol. Both WPAv1 and WPAv2 allow authentication using pre-shared key (PSK) for home-type of deployment, and 802.1X for authenticated key management for enterprise-type of deployments.

Note WPA recommends the use of TKIP, and allows the use of AES. WPA2 recommends the use of AES-CCMP, and allows the use of TKIP for backward compatibility. Cisco and the Wi-Fi Alliance recommend that you do not use WPAv1 with AES, or WPAv2 with TKIP. The strongest level of security is achieved with WPAv2 and AES-CCMP. WPAv1 and TKIP can be used in networks where clients do not support WPAv2 with AES-CCMP.

Using WPA (WPAv1 or WPAv2) key management, clients and the authentication server authenticate to each other using an EAP authentication method, and the client and server generate a pairwise master key (PMK). Using WPA, the server generates the PMK dynamically and passes it to the access point. Using WPA-PSK, however, you configure a pre-shared key on both the client and the access point, and that pre-shared key is used as the PMK.

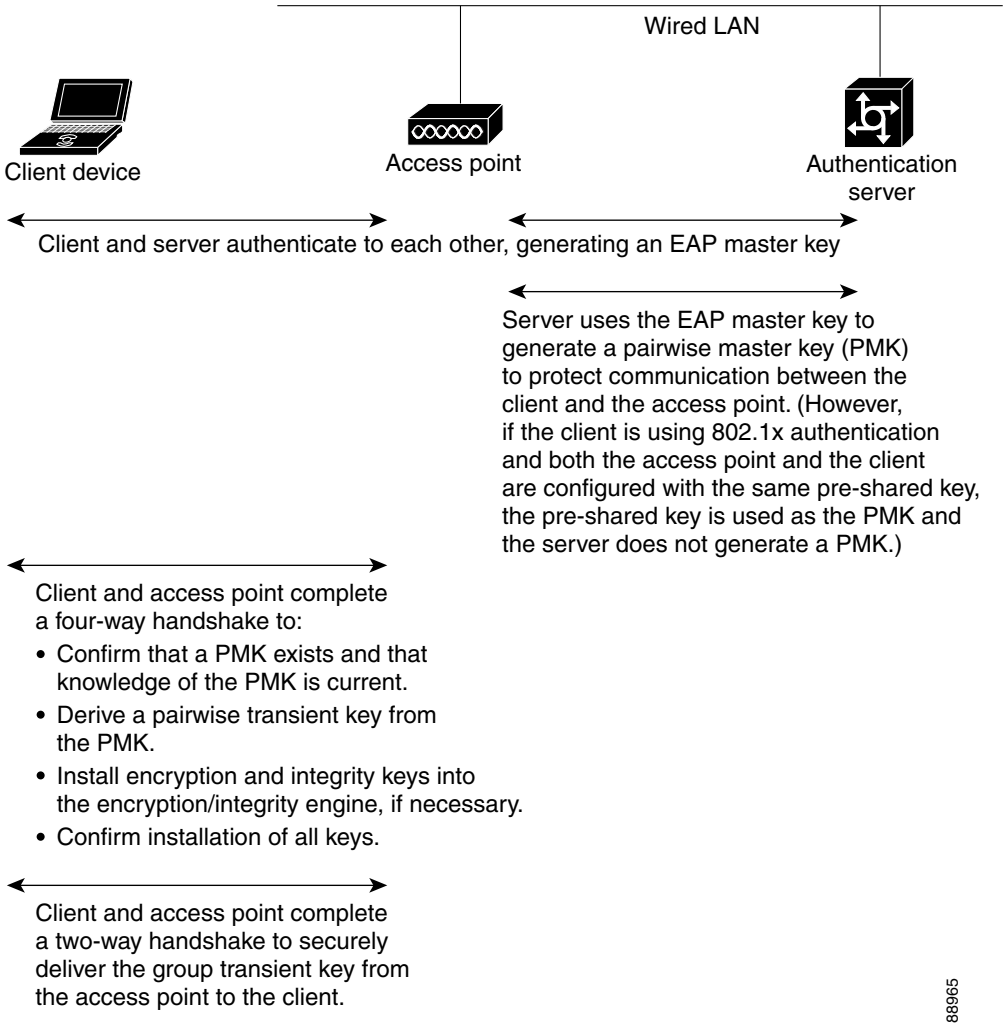
WPA key management supports two mutually exclusive management types: WPA and WPA-pre-shared key (WPA-PSK). Using WPA key management, clients and the authentication server authenticate to each other using an EAP authentication method, and the client and server generate a pairwise master key (PMK). Using WPA, the server generates the PMK dynamically and passes it to the access point. Using WPA-PSK, however, you configure a pre-shared key on both the client and the access point, and that pre-shared key is used as the PMK.

Note Unicast and multicast cipher suites advertised in WPA information element (and negotiated during 802.11 association) may potentially mismatch with the cipher suite supported in an explicitly assigned VLAN. If the RADIUS server assigns a new vlan ID which uses a different cipher suite from the previously negotiated cipher suite, there is no way for the access point and client to switch back to the new cipher suite. Currently, the WPA and CCKM protocols does not allow the cipher suite to be changed after the initial 802.11 cipher negotiation phase. In this scenario, the client device is disassociated from the wireless LAN.

See the "Assigning Authentication Types to an SSID" section on page 11-9 for instructions on configuring WPA key management on your access point.

Figure 11-6 shows the WPA key management process.

Figure 11-6 WPA Key Management Process



Configuring Authentication Types

This section describes how to configure authentication types. You attach configuration types to the access point's SSIDs. See the "Configuring Multiple SSIDs" section on page 7-3 for details on setting up multiple SSIDs. This section contains these topics:

Assigning Authentication Types to an SSID

The SSID you configure will be mapped to a VLAN or a radio interface. Hence, make sure that the authentication type you define for the SSID is compatible with the encryption type defined for the associated VLAN or radio interface. See Chapter 10, "Understanding Authentication and Encryption Mechanisms," for more details.

Beginning in privileged EXEC mode, follow these steps to configure authentication types for SSIDs:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**dot11 ssid** *ssid-string*	Create an SSID and enter SSID configuration mode for the new SSID. The SSID can consist of up to 32 alphanumeric characters. SSIDs are case sensitive. Some clients do not support special characters in the SSID string. Cisco recommends avoiding the following characters in the SSID string: !#;+\/"

	Command	Purpose
Step 3	**authentication open** [**mac-address** *list-name* [**alternate**]] [[**optional**] **eap** *list-name*]	(Optional) Set the authentication type to open for this SSID. Open authentication allows any device to authenticate and then attempt to communicate with the access point. • (Optional) Set the SSID's authentication type to open with MAC address authentication. The access point forces all client devices to perform MAC-address authentication before they are allowed to join the network. For *list-name*, specify the authentication method list. • Use the **alternate** keyword to allow client devices to join the network using either MAC or EAP authentication; clients that successfully complete either authentication are allowed to join the network. • (Optional) Set the SSID's authentication type to open with EAP authentication. The access point forces all client devices to perform EAP authentication before they are allowed to join the network. For *list-name*, specify the authentication method list. Use the **optional** keyword to allow client devices using either open or EAP authentication to associate and become authenticated. This setting is used mainly by service providers that require special client accessibility. **Note** An access point configured for EAP authentication forces all client devices that associate to perform EAP authentication. Client devices that do not use EAP cannot use the access point.
Step 4	**authentication shared** [**mac-address** *list-name*] [**eap** *list-name*]	(Optional) Set the authentication type for the SSID to shared key. **Note** Because of WEP shared key's security flaws, We recommend that you avoid using it. • (Optional) Set the SSID's authentication type to shared key with MAC address authentication. For list-name, specify the authentication method list. • (Optional) Set the SSID's authentication type to shared key with EAP authentication. For list-name, specify the authentication method list. This mode is designed for networks with phased migration to EAP. Clients supporting EAP will use individual client authentication and individual client key management, while clients supporting only static WEP will be allowed to associate using static WEP.

	Command	Purpose
Step 5	**authentication network-eap** *list-name* [**mac-address** *list-name*]	(Optional) set the authentication type for the SSID to Network-EAP. Using the Extensible Authentication Protocol (EAP) to interact with an EAP-compatible RADIUS server supporting Cisco LEAP, the access point helps a wireless client device and the RADIUS server to perform mutual authentication and derive a dynamic unicast key. • (Optional) Set the SSID's authentication type to Network-EAP with MAC address authentication. All client devices that associate to the access point are required to perform MAC-address authentication. For list-name, specify the authentication method list.

	Command	Purpose
Step 6	**authentication key-management** { [**wpa [version** *versionnumber*]] | [**cckm**] } [**optional**]	(Optional) Set the authentication type for the SSID to WPA, CCKM, or both. If you use the **optional** keyword, client devices other than WPA (WPAv1 or WPAv2) and CCKM clients can use this SSID. If you do not use the **optional** keyword, only WPA (WPAv1 or WPAv2) or CCKM client devices are allowed to use the SSID. To enable CCKM for an SSID, you must also enable a form of EAP authentication (Open with EAP and/or Network EAP). When CCKM and EAP are enabled for an SSID, client devices using LEAP, EAP-FAST, PEAP/GTC, MSPEAP, EAP-TLS, and EAP-FAST authenticate using the SSID, and can benefit from fast roaming using CCKM. To enable WPA key management for an SSID (with WPAv1 or WPAv2), you must also enable Open authentication with EAP or Network-EAP or both (with or without additional MAC authentication). In that case, individual client authentication will occur using EAP, and individual client Pairwise Master Key will be defined. Alternatively, you can enable Open and define a WPA pre-shared key. In that case, the pre-shared key will be used as the Pairwise Master Key (PMK) by the AP and the wireless client. **Note** When you enable both WPA and CCKM for an SSID from the CLI, you must enter WPA first and CCKM second (but from the WebUI, simply check both options). Any WPA client can attempt to authenticate, but only CCKM voice clients can attempt to authenticate. **Note** Before you can enable CCKM or WPA, you must set the encryption mode for the SSID's VLAN to one of the cipher suite options. See the Chapter 10, "Configuring Encryption Modes," for instructions on configuring the VLAN encryption mode. **Note** If you enable WPA for an SSID without a pre-shared key, the key management type is WPA. If you enable WPA with a pre-shared key, the key management type is WPA-PSK. See the Configuring Additional WPA Settings for instructions on configuring a pre-shared key. See Chapter 12, "Configuring Other Services," for detailed instructions on setting up your wireless LAN to use CCKM and a subnet context manager. (Optional) When using WPA, you can specify which WPA version you want to support – WPAv1 or WPAv2.
Step 7	**end**	Return to privileged EXEC mode.
Step 8	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Use the **no** form of the SSID commands to disable the SSID or to disable SSID features.

This example sets the authentication type for the SSID *batman* to Network-EAP with CCKM authenticated key management. Client devices using the batman SSID authenticate using the adam server list. After they are authenticated, CCKM-enabled clients can perform fast reassociations using CCKM.

```
ap1200# configure terminal
ap1200(config-if)# ssid batman
ap1200(config-ssid)# authentication network-eap adam
ap1200(config-ssid)# authentication key-management cckm optional
ap1200(config)# interface dot11radio 0
ap1200(config-if)# ssid batman
ap1200(config-ssid)# end
```

Configuring WPA Migration Mode for Legacy WEP SSIDs

WPA migration is a specific mode intended for SSIDs needing to support legacy WEP client types while still allowing for more secure authentication and encryption. This specific mode allows for the following client device types:

- WPA clients capable of TKIP and authenticated key management
- 802.1X-2001 clients (such as legacy LEAP clients and clients using TLS) capable of authenticated key management but not TKIP
- Static-WEP clients not capable of TKIP or authenticated key management

If all three client types associate using the same SSID, the multicast cipher suite for the SSID must be WEP. If only the first two types of clients use the same SSID the multicast key can be dynamic, but if the static-WEP clients use the SSID, the key must be static. The access point can switch automatically between a static and a dynamic group key to accommodate associated client devices. To support all three types of clients on the same SSID, you must configure the static key in key slots 2 or 3.

To set up an SSID for WPA migration mode, configure these settings:

- WPA optional
- A cipher suite containing TKIP and 40-bit or 128-bit WEP
- A static WEP key in key slot 2 or 3

This example sets the SSID migrate for WPA migration mode:

```
ap1200# configure terminal
ap1200(config-if)# ssid migrate
ap1200(config-if)# encryption mode cipher tkip wep128
ap1200(config-if)# encryption key 3 size 128 12345678901234567890123456 transmit-key
ap1200(config-ssid)# authentication open
ap1200(config-ssid)# authentication network-eap adam
ap1200(config-ssid)# authentication key-management wpa optional
ap1200(config-ssid)# wpa-psk ascii batmobile65
ap1200(config)# interface dot11radio 0
ap1200(config-if)# ssid migrate
ap1200(config-ssid)# end
```

Configuring Additional WPA Settings

Use two optional settings to configure a pre-shared key on the access point and adjust the frequency of group key updates.

Setting a pre-shared Key

To support WPA (WPAv1 or WPAv2) on a wireless LAN where 8021X/EAP-based authentication is not available, you must configure a pre-shared key on the access point. You can enter the pre-shared key as ASCII or hexadecimal characters. If you enter the key as ASCII characters, you enter between 8 and 63 characters, and the access point expands the key using the process described in the *Password-based Cryptography Standard* (RFC2898). If you enter the key as hexadecimal characters, you must enter 64 hexadecimal characters.

Configuring Group Key Updates

In the last step in the WPA process, the access point distributes a group key to the authenticated client device. You can use these optional settings to configure the access point to change and distribute the group key based on client association and disassociation:

- Membership termination—the access point generates and distributes a new group key when any authenticated device disassociates from the access point. This feature keeps the group key private for associated devices, but it might generate some overhead traffic if clients on your network roam frequently among access points.
- Capability change—the access point generates and distributes a dynamic group key when there is a change in the cell clients capability. For example, in a cell allowing AES, TKIP and WEP and currently containing only AES clients, the broadcast key uses AES. The access point generates a new broadcast key using TKIP when the first TKIP client joins the cell, and generates a new broadcast key when the first WEP client joins the cell. Symmetrically, the access point generates a new broadcast key when the last WEP client leaves the cell. If at that time all clients support AES, the new broadcast key will use AES. If some clients use TKIP and others use AES (AES clients also support TKIP), the new broadcast key will use TKIP. When the last TKIP client leaves the cell, with only AES clients left in the cell, the access point generates a new broadcast key using AES.

Beginning in privileged EXEC mode, follow these steps to configure a WPA pre-shared key and group key update options:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ssid** *ssid-string*	Enter SSID configuration mode for the SSID.
Step 3	**wpa-psk** { **hex** | **ascii** } [**0** | **7**] *encryption-key*	Enter a pre-shared key for client devices using WPA that also use static WEP keys. Enter a pre-shared key for client devices using WPAv1 or WPAv2 with PSK authentication. If you use hexadecimal, you must enter 64 hexadecimal characters to complete the 256-bit key. If you use ASCII, you must enter a minimum of 8 letters, numbers, or symbols, and the access point expands the key for you. You can enter a maximum of 63 ASCII characters.

	Command	Purpose
Step 4	**interface dot11radio** { **0** | **1** }	Enter interface configuration mode for the radio interface. The 2.4-GHz radio and the 2.4-GHz 802.11n radio is 0. The 5-GHz radio and the 5-GHz 802.11n radio is 1.
Step 5	**ssid** *ssid-string*	Enter the ssid defined in Step 2 to assign the ssid to the selected radio interface.
Step 6	**exit**	Return to privileged EXEC mode.
Step 7	**broadcast-key** [**vlan** *vlan-id*] { **change** *seconds* } [**membership-termination**] [**capability-change**]	Use the **broadcast key rotation** command to configure additional updates of the WPA group key.
Step 8	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

This example shows how to configure a pre-shared key for clients using WPA and static WEP, with group key update options:

```
ap# configure terminal
ap(config-if)# ssid batman
ap(config-ssid)# wpa-psk ascii batmobile65
ap(config)# interface dot11radio 0
ap(config-ssid)# ssid batman
ap(config-if)# exit
ap(config)# broadcast-key vlan 87 membership-termination capability-change
```

Configuring MAC Authentication Caching

If MAC-authenticated clients on your wireless LAN roam frequently, you can enable a MAC authentication cache on your access points. MAC authentication caching reduces overhead because the access point authenticates devices in its MAC-address cache without sending the request to your authentication server. When a client device completes MAC authentication to your authentication server, the access point adds the client's MAC address to the cache.

Beginning in privileged EXEC mode, follow these steps to enable MAC authentication caching:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**dot11 aaa authentication mac-authen filter-cache** [**timeout** *seconds*]	Enable MAC authentication caching on the access point. Use the **timeout** option to configure a timeout value for MAC addresses in the cache. Enter a value from 30 to 65555 seconds. The default value is 1800 (30 minutes). When you enter a timeout value, MAC-authentication caching is enabled automatically.
Step 3	**exit**	Return to privileged EXEC mode.
Step 4	**show dot11 aaa authentication mac-authen filter-cache** [*address*]	Show entries in the MAC-authentication cache. Include client MAC addresses to show entries for specific clients.
Step 5	**clear dot11 aaa authentication mac-authen filter-cache** [*address*]	Clear all entries in the cache. Include client MAC addresses to clear specific clients from the cache.

	Command	Purpose
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

This example shows how to enable MAC authentication caching with a one-hour timeout:

```
ap# configure terminal
ap(config)# dot11 aaa authentication mac-authen filter-cache timeout 3600
ap(config)# end
```

Use the **no** form of the **dot11 aaa authentication mac-authen filter-cache** command to disable MAC authentication caching. For example:

```
no dot11 aaa authentication mac-authen filter-cache
```

or

```
no wlccp wds aaa authentication mac-authen filter-cache
```

Configuring Authentication Holdoffs, Timeouts, and Intervals

Beginning in privileged EXEC mode, follow these steps to configure holdoff times, reauthentication periods, and authentication timeouts for client devices authenticating through your access point:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**dot11 holdoff-time** *seconds*	Enter the number of seconds a client device must wait before it can reattempt to authenticate following a failed authentication. The holdoff time is invoked when a client fails three login attempts or fails to respond to three authentication requests from the access point. Enter a value from 1 to 65555 seconds.
Step 3	**dot1x timeout supp-response** *seconds* [local]	Enter the number of seconds the access point should wait for a client to reply to an EAP/dot1x message before the authentication fails. Enter a value from 1 to 120 seconds. The RADIUS server can be configured to send a different timeout value which overrides the one that is configured. Enter the **local** keyword to configure the access point to ignore the RADIUS server value and use the configured value. The optional **no** keyword resets the timeout to its default state, 30 seconds.
Step 4	**interface dot11radio** { **0** | **1** }	Enter interface configuration mode for the radio interface. The 2.4-GHz radio and the 2.4-GHz 802.11n radio is 0. The 5-GHz radio and the 5-GHz 802.11n radio is 1.

	Command	Purpose
Step 5	**dot1x reauth-period** { *seconds* | **server** }	Enter the interval in seconds that the access point waits before forcing an authenticated client to reauthenticate. Enter the **server** keyword to configure the access point to use the reauthentication period specified by the authentication server. If you use this option, configure your authentication server with RADIUS attribute 27, Session-Timeout. This attribute sets the maximum number of seconds of service to be provided to the client before termination of the session or prompt. The server sends this attribute to the access point when a client device performs EAP authentication. **Note** If you configure both MAC address authentication and EAP authentication for an SSID, the server sends the Session-Timeout attribute for both MAC and EAP authentications for a client device. The access point uses the Session-Timeout attribute for the last authentication that the client performs. For example, if a client performs MAC address authentication and then performs EAP authentication, the access point uses the server's Session-Timeout value for the EAP authentication. To avoid confusion on which Session-Timeout attribute is used, configure the same Session-Timeout value on your authentication server for both MAC and EAP authentication.
Step 6	**countermeasure tkip hold-time** *seconds*	Configure a TKIP MIC failure holdtime. You can specify a hold-time in the range 0 to 65535 seconds. The default is 60 seconds. If the access point detects two MIC failures within, for example 60 seconds, it blocks all the TKIP clients on that interface for the holdtime period.
Step 7	**end**	Return to privileged EXEC mode.
Step 8	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Use the **no** form of these commands to reset the values to default settings.

Creating and Applying EAP Method Profiles for the 802.1X Supplicant

This section describes the optional configuration of an EAP method list for the 802.1X supplicant. Configuring EAP method profiles enables the supplicant not to acknowledge some EAP methods, even though they are available on the supplicant. For example, if a RADIUS server supports EAP-FAST and LEAP, under certain configurations, the server might initially employ LEAP instead of a more secure method. If no preferred EAP method list is defined, the supplicant supports LEAP, but it may be advantageous to force the supplicant to force a more secure method such as EAP-FAST.

See Creating a Credentials Profile, page 4-25 for additional information about the 802.1X supplicant.

Creating an EAP Method Profile

Beginning in privileged exec mode, follow these steps to define a new EAP profile:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**eap profile** *profile name*	Enter a name for the profile
Step 3	**description**	(Optional)—Enter a description for the EAP profile
Step 4	**method** {**fast** | **gtc** | **leap** | **md5** | **mschapv2** | **peap** | **tls**}	Enter an allowed EAP method or methods. **Note** Although they appear as sub-parameters, EAP-GTC, EAP-MD5, and EAP-MSCHAPV2 are intended as inner methods for tunneled EAP authentication and should not be used as the primary authentication method.
Step 5	**end**	Return to the privileged EXEC mode.
Step 6	**copy running config startup-config**	(Optional) Save your entries in the configuration file.

Use the **no** command to negate a command or set its defaults.

Use the **show eap registrations method** command to view the currently available (registered) EAP methods.

```
ap#show eap registrations method
Registered EAP Methods:
  Method  Type            Name
    4     Auth and Peer   MD5
    6     Auth and Peer   GTC
    13    Auth and Peer   TLS
    17    Auth and Peer   LEAP
    25    Auth and Peer   PEAP
    26    Auth and Peer   MSCHAPV2
    43    Auth and Peer   FAST
```

Use the **show eap sessions** command to view existing EAP sessions.

Applying an EAP Profile to the Fast Ethernet Interface

This operation normally applies to access points that need to be authenticated against a RADIUS server, when they are connected to a switch port that is configured to perform 802.1x authentication of connected devices. The AP will act as a 802.1x client, and will need to provide credentials to be authenticated.

Beginning in privileged exec mode, follow these steps to apply an EAP profile to the Fast Ethernet interface:

	Command	Purpose
Step 1	**configure terminal**	Enter the global configuration mode.
Step 2	**interface gigabitethernet 0**	Enter the interface configuration mode for the access point's Fast Ethernet port. You can also use **interface g0** to enter the fast Ethernet configuration mode.
Step 3	**dot1x eap profile** *profile*	Enter the profile preconfigured profile name.
Step 4	**end**	Exit the interface configuration mode.

Applying an EAP Profile to an Uplink SSID

This operation typically applies to repeater access points, non-root bridges and workgroup bridges needing to authenticate over their radio link to a root-AP or root bridge. Beginning in the privileged exec mode, follow these steps to apply an EAP profile to the uplink SSID.

	Command	Purpose
Step 1	**configure terminal**	Enter the global configuration mode.
Step 2	**interface dot11radio** {**0** | **1**}	Enter interface configuration mode for the radio interface. The 2.4-GHz radio and the 2.4-GHz 802.11n radio is 0. The 5-GHz radio and the 5-GHz 802.11n radio is 1.
Step 3	**ssid** *ssid*	Assign the uplink SSID to the radio interface.
Step 4	**dot1x** {**credentials** | **default** | **eap**}	You can specify one of the following: • credentials—Credentials profile configuration • default—Configure Dot1x with default values for this SSID • eap—Configure EAP specific parameters
Step 5	**dot1x eap profile** *profilename*	Enter the profile preconfigured profile name.
Step 6	**end**	Return to the privileged EXEC mode.
Step 7	**copy running config startup-config**	(Optional) Save your entries in the configuration file.

Matching Access Point and Client Device Authentication Types

To use the authentication types described in this section, the access point authentication settings must match the authentication settings on the client adapters that associate to the access point. Refer to Configuring Encryption Modes, page 10-7 for instructions on configuring cipher suites and WEP on the access point.

Table 11-1 lists the client and access point settings required for each authentication type.

Note Some non-Cisco Aironet client adapters do not perform 802.1X authentication to the access point unless you configure **Open authentication with EAP**. To allow both Cisco Aironet clients using LEAP and non-Cisco Aironet clients using LEAP to associate using the same SSID, you might need to configure the SSID for both **Network EAP** authentication and **Open authentication with EAP**.

Table 11-1 Client and Access Point Security Settings

Security Feature	Client Setting	Access Point Setting
Static WEP with open authentication	Create a WEP key and enable Use Static WEP Keys and Open Authentication	Set up and enable WEP and enable Open Authentication for the SSID
Static WEP with shared key authentication	Create a WEP key and enable Use Static WEP Keys and Shared Key Authentication	Set up and enable WEP and enable Shared Key Authentication for the SSID
LEAP authentication	Enable LEAP	Set up and enable WEP and enable Network-EAP for the SSID[1]
EAP-FAST authentication	Enable EAP-FAST and enable automatic provisioning or import a PAC file	Set up and enable WEP and enable Network-EAP for the SSID[1] If radio clients are configured to authenticate using EAP-FAST, open authentication with EAP should also be configured. If you do not configure open authentication with EAP, the following GUI warning message appears: WARNING: Network EAP is used for LEAP authentication only. If radio clients are configured to authenticate using EAP-FAST, Open Authentication with EAP should also be configured. If you are using the CLI, this warning message appears: SSID CONFIG WARNING: [SSID]: If radio clients are using EAP-FAST, AUTH OPEN with EAP should also be configured.
EAP-FAST authentication with WPA	Enable EAP-FAST and Wi-Fi Protected Access (WPA) and enable automatic provisioning or import a PAC file. To allow the client to associate to both WPA and non-WPA access points, enable Allow Association to both WPA and non-WPA authenticators.	Select a cipher suite that includes TKIP, set up and enable WEP, and enable Network-EAP and WPA for the SSID. **Note** To allow both WPA and non-WPA clients to use the SSID, enable optional WPA.

Table 11-1 Client and Access Point Security Settings (continued)

Security Feature	Client Setting	Access Point Setting
802.1X authentication and CCKM	Enable LEAP	Select a cipher suite and enable Open with EAP and/or Network EAP, and CCKM for the SSID. **Note** To allow both 802.1X clients and non-802.1X clients to use the SSID, enable optional CCKM.
802.1X authentication and WPA	Enable any 802.1X authentication method	Select a cipher suite and enable Open with EAP and WPA for the SSID (you can also enable Network-EAP authentication in addition to or instead of Open with EAP) **Note** To allow both WPA clients and non-WPA clients to use the SSID, enable optional WPA.
802.1X authentication and WPA-PSK	Enable any 802.1X authentication method	Select a cipher suite and enable Open authentication with Optional EAP and WPA for the SSID (you can also enable Network-EAP authentication in addition to or instead of Open authentication with Optional EAP). Enter a WPA pre-shared key. Clients using 802.1x/EAP will generate individual WPA PMKs. Clients using WPA-PSK will use the PSK as a PMK. **Note** To allow both WPA clients and non-WPA clients to use the SSID, enable optional WPA.
EAP-TLS authentication with dynamic WEP encryption		
If using Windows to configure card	Select Enable network access control using IEEE 802.1X and Smart Card or other Certificate as the EAP Type	Set up and enable WEP and enable EAP and Open with EAP for the SSID
EAP-MD5 authentication with dynamic WEP encryption		
If using Windows XP to configure card	Select Enable network access control using IEEE 802.1X and MD5-Challenge as the EAP Type	Set up and enable WEP and enable EAP and Open Authentication for the SSID

Table 11-1 Client and Access Point Security Settings (continued)

Security Feature	Client Setting	Access Point Setting
PEAP authentication with dynamic WEP encryption		
If using Windows to configure card	Select Enable network access control using IEEE 802.1X and PEAP as the EAP Type	Set up and enable WEP and enable Require EAP and Open with EAP for the SSID
EAP-SIM authentication with dynamic WEP encryption		
If using Windows to configure card	Select Enable network access control using IEEE 802.1X and SIM Authentication as the EAP Type	Set up and enable WEP with full encryption and enable Require EAP and Open with EAP for the SSID

1. Some non-Cisco Aironet client adapters do not perform 802.1X authentication to the access point unless you configure **Open authentication with EAP**. To allow both Cisco Aironet clients using LEAP and non-Cisco Aironet clients using LEAP to associate using the same SSID, you might need to configure the SSID for both **Network EAP** authentication and **Open authentication with EAP**.

Guest Access Management

Guest Access allows a guest to gain access to the Internet, and the guest's own enterprise without compromising the security of the host enterprise.

Guest access is allowed through these methods:

- Web Authentication (secured)
- Web Pass-through

Web Authentication (secured)

Web authentication is a Layer 3 security feature that enables the Autonomous AP to block IP traffic (except DHCP & DNS-related packets) until the guest provides a valid username and password.

In web authentication, a separate username and password must be defined for each guest. Using the username and password, the guest is authenticated either by the local radius server or an external RADIUS server.

Perform these steps to enable web authentication:

Step 1 Browse to the Security page on the access point GUI.

Step 2 Select SSID Manager.

Step 3 Check the **Web Authentication** check box.

Beginning in privileged EXEC mode, use these commands to enable web authentication:

- The network security type is set to none by default, because the authentication will occur at Layer 3 through the web interface, and therefore does not need to occur at Layer 2. However, you can combine Layer 3 security with any Layer 2 security. Web authentication is supported only with Open authentication. No encryption is allowed.
  - ap(config)# **dot11 ssid guestssid**
  - ap(config-ssid)# **web-auth**

  - ap(config-ssid)# **authentication open**
  - ap(config-ssid)# **exit**
- To enable web authentication:
  - ap(config)# **ip admission name Web_auth proxy http**
  - ap(config)# **interface dot11Radio 0**
  - ap(config-if)# **ip admission Web_auth**

Web Pass-through

Web Pass-through is similar to Web Authentication. However, the guest is not required to provide authentication details.

In Web Pass-through, guests are redirected to the usage policy page when they use the Internet for the first time. When the policy is accepted, access is granted. The access point redirects the guest to the policy page.

Perform these steps to enable web authentication:

Step 1 Browse to the Security page on the access point GUI.

Step 2 Select SSID Manager.

Step 3 Check the **Web Pass** check box.

Beginning in privileged EXEC mode, use these commands to enable Web Pass-through:

- ap(config)# **ip admission name Web_passthrough consent**
- ap(config)# **interface dot11Radio 0**
- ap(config-if)# **ip admission Web_passthrough**

Note Web Authentication or Web Pass-through works in an interface only when there is no VLAN. The IP admission Web_auth or IP admission Web_passthrough must be configured in the VLAN when the SSID is mapped to the VLAN.

Guest Account Creation

Perform these steps to create new guest accounts:

Step 1 Browse to **Management > Guest Management Services** page on the access point in the GUI.

Step 2 Select **New** to create a new guest account.

The Webauth page is displayed.

Step 3 Enter these values:

- Username
- Password
- Confirm Password
- Lifetime

Step 4 To let the system automatically generate a random string as a password, check the **Generate Password** check box. Alternatively, you can manually enter the password value.

Step 5 Click **Apply.**

Perform these steps to delete an existing user:

Step 1 Browse to the Guest Management Services page on the access point GUI.

Step 2 Select the username to be deleted.

Step 3 Click **Delete**.

A confirmation message appears.

Step 4 Click **Ok** to delete the user or **Cancel** to cancel the changes.

Beginning in privileged EXEC mode, use these commands to create guest accounts using CLI commands:

- ap(config)# **dot11 guest**
- ap(config-guest-mode)# **username Gues-1 lifetime 40 password t_ksdgon**
- ap(config-guest-mode)# **username Gues-2 lifetime 35 password gp2**
- ap(config)# **exit**

Guest access is allowed for a maximum of twenty-four days (35791 minutes) and a minimum of five minutes.

Beginning in privileged EXEC mode, use this command to delete a guest user:

ap# **clear dot11 guest-user Gues-1**

Beginning in privileged EXEC mode, use this command to display guest users:

ap# **show dot11 guest-users**

Customized Guest Access Pages

The Webauth Login guest access pages can be customized to display a custom logo or other images. You can customize the Login page, Success page, Failure page, or the Expired page. To customize a page, follow these steps:

Step 1 Save the image to be displayed in the customized page, on a web server and set the web server's IP address as allowed in the ACL in/out lists.

Step 2 Get the default HTML code of the page to be customized.

Step 3 Edit the source code of the page to insert the images, by specifying the full path of the image files on the web-server. For example: <Body background="http://40.40.5.10/image.jpg" width="600" height="600">, where the image.jpg file resides on the web server with IP address 40.40.5.10.

Note When editing the HTML code of the default page, do not make any changes to the code for the submit function and for the fields of Username and Password.

Step 4 Save the customized pages to the web server.

Step 5 In the access point GUI, browse to the **Management > Guest Management Services** page.

Step 6 Select **Webauth Login.**

Step 7 Browse and upload these pages from the web server:

- Login Page
- Success Page
- Failure Page
- Expired page

Note It is mandatory to load the Login page, Success page, Failure page, and Expired page when you customize the guess access login.

Step 8 Select the file transfer method: FTP or TFTP.

Step 9 Enter the **Username**.

Step 10 Enter the **Password**.

Step 11 Enter the **Allowed-In ACL Name** and the **Allowed-Out ACL Name**.

Step 12 Click **Close Window** to save your changes.

Alternatively, you can use the following CLI commands to configure a customized guest access page. Copy all edited files to the flash memory. Then, beginning in privileged EXEC mode, use these commands to load all the edited files from flash:

- ap(config)# **ip auth-proxy proxy http login page file flash:web_login.html**
- ap(config)# **ip auth-proxy proxy http success page file flash:web_success.html**
- ap(config)# **ip auth-proxy proxy http failure page file flash:web_fail.html**
- ap(config)# **ip auth-proxy proxy http login expired page file flash:web_logout.html**

To configure the IP address of the web server (IP address here is 40.40.5.10) in the ACL, the following commands are also required. Beginning in privileged EXEC mode, use these ACL commands:

- ap(config)# **dot11 webauth allowed incoming webauth_acl_in outgoing webaut_acl_out**
- ap(config)# **ip access-list extended webauth_acl_in**
- ap(config-ext-nacl)# **permit tcp any host 40.40.5.10 eq www**
- ap(config-ext-nacl)# **permit tcp any host 40.40.5.10 eq 443**
- ap(config-ext-nacl)# **permit tcp any host 40.40.5.10 eq 443**
- ap(config-ext-nacl)# **exit**
- ap(config)# **ip access-list extended webauth_acl_out**
- ap(config-ext-nacl)# **permit tcp any host 40.40.5.10 eq www**
- ap(config-ext-nacl)# **permit tcp any host 40.40.5.10 eq 443**
- ap(config-ext-nacl)# **exit**

Note In the previous commands acl-in and acl-out are the names of the Access-list. These ACLs allow you to download the image file from the machine, where it is stored and use it for the customization of web page.

The default page displays only the username, password, OK page.

Guest access does not support these:

- IPv6
- SNMP
- Roaming