



Configuring Authentication Types

This chapter describes how to configure authentication types on the access point/bridge. This chapter contains these sections:

- [Understanding Authentication Types, page 10-2](#)
- [Configuring Authentication Types, page 10-6](#)
- [Matching Authentication Types on Root and Non-Root Access Point/Bridges, page 10-12](#)

Understanding Authentication Types

This section describes the authentication types that you can configure on the access point/bridge. The authentication types are tied to the SSID that you configure on the access point/bridge.

Before access point/bridges can communicate, they must authenticate to each other using open or shared-key authentication. For maximum security, access point/bridges should also authenticate to your network using EAP authentication, an authentication type that relies on an authentication server on your network.

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

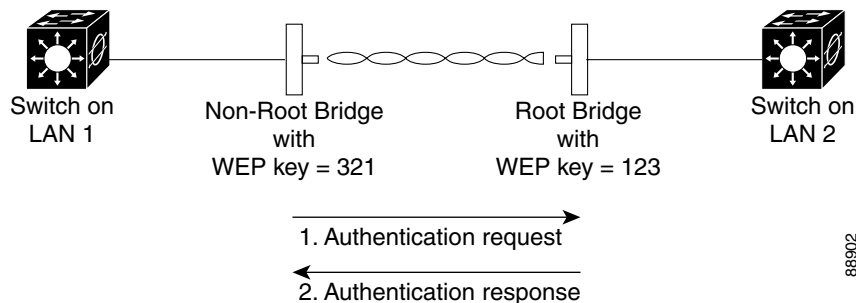
- [Open Authentication to the Access Point/Bridge, page 10-2](#)
- [Shared Key Authentication to the Access Point/Bridge, page 10-2](#)
- [EAP Authentication to the Network, page 10-3](#)

Open Authentication to the Access Point/Bridge

Open authentication allows any 1300 series access point/bridge to authenticate and then attempt to communicate with another 1300 series access point/bridge. Using open authentication, a non-root access point/bridge can authenticate to a root access point/bridge, but the non-root access point/bridge can communicate only if its WEP keys match the root access point/bridge's. An access point/bridge that is not using WEP does not attempt to authenticate with an access point/bridge that is using WEP. Open authentication does not rely on a RADIUS server on your network.

Figure 10-1 shows the authentication sequence between a non-root access point/bridge trying to authenticate and a root access point/bridge using open authentication. In this example, the device's WEP key does not match the access point/bridge's key, so it can authenticate but not pass data.

Figure 10-1 Sequence for Open Authentication



Shared Key Authentication to the Access Point/Bridge

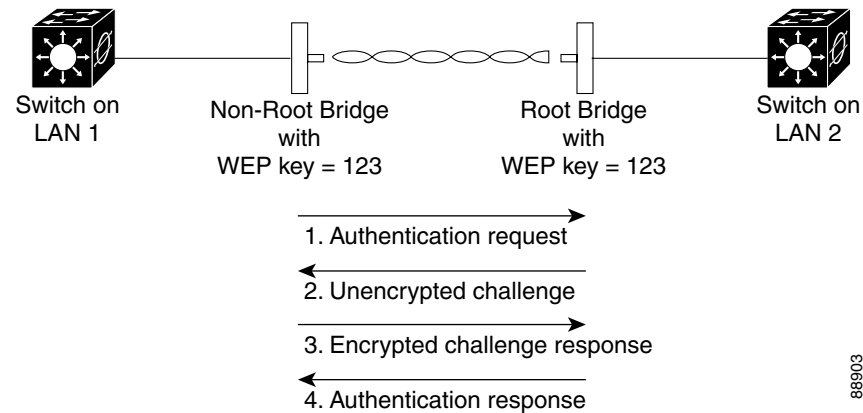
Cisco provides shared key authentication to comply with the IEEE 802.11b standard. However, because of shared key's security flaws, we recommend that you avoid using it.

During shared key authentication, the root access point/bridge sends an unencrypted challenge text string to other access point/bridges attempting to communicate with the root access point/bridge. The access point/bridge requesting authentication encrypts the challenge text and sends it back to the root

access point/bridge. If the challenge text is encrypted correctly, the root access point/bridge allows the requesting device to authenticate. Both the unencrypted challenge and the encrypted challenge can be monitored, however, which leaves the root access point/bridge 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 10-2 shows the authentication sequence between a device trying to authenticate and an access point/bridge using shared key authentication. In this example the device's WEP key matches the access point/bridge's key, so it can authenticate and communicate.

Figure 10-2 Sequence for Shared Key Authentication

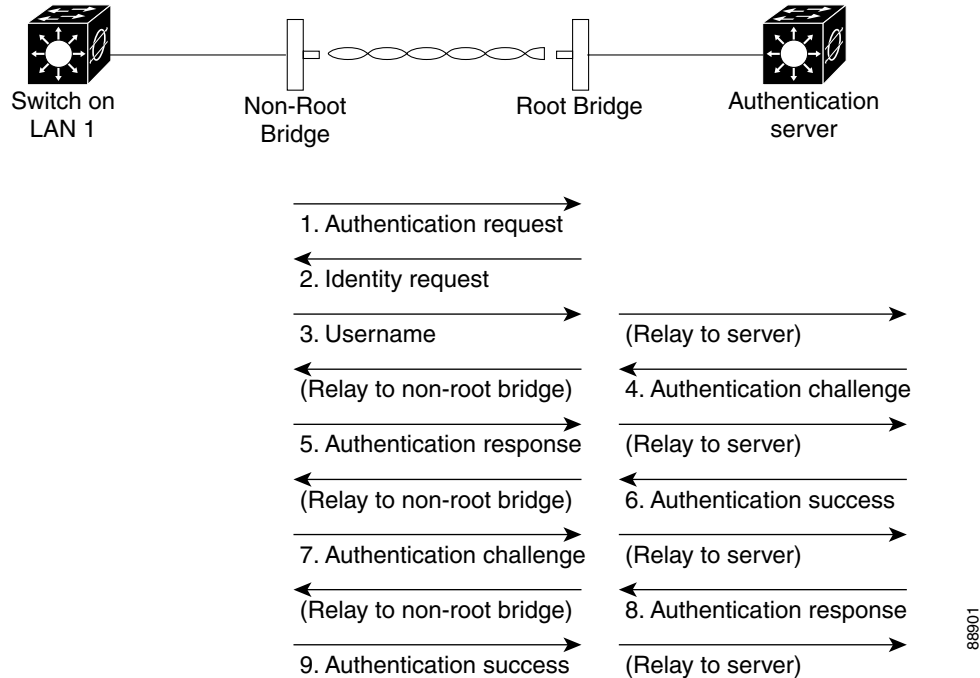


EAP Authentication to the Network

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 root access point/bridge helps another access point/bridge and the RADIUS server to perform mutual authentication and derive a dynamic unicast WEP key. The RADIUS server sends the WEP key to the root access point/bridge, which uses it for all unicast data signals that it sends to or receives from the non-root access point/bridge. The root access point/bridge also encrypts its broadcast WEP key (entered in the access point/bridge's WEP key slot 1) with the non-root access point/bridge's unicast key and sends it to the non-root access point/bridge.

When you enable EAP on your access point/bridges, authentication to the network occurs in the sequence shown in [Figure 10-3](#):

Figure 10-3 Sequence for EAP Authentication



In Steps 1 through 9 in [Figure 10-3](#), a non-root access point/bridge and a RADIUS server on the wired LAN use 802.1x and EAP to perform a mutual authentication through the root access point/bridge. The RADIUS server sends an authentication challenge to the non-root access point/bridge. The non-root access point/bridge uses a one-way encryption of the user-supplied password 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 non-root access point/bridge. When the RADIUS server authenticates the non-root access point/bridge, the process repeats in reverse, and the non-root access point/bridge authenticates the RADIUS server.

When mutual authentication is complete, the RADIUS server and the non-root access point/bridge determine a WEP key that is unique to the non-root access point/bridge and provides the non-root access point/bridge with the appropriate level of network access, thereby approximating the level of security in a wired switched segment to an individual desktop. The non-root access point/bridge 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, called a *session key*, over the wired LAN to the root access point/bridge. The root access point/bridge encrypts its broadcast key with the session key and sends the encrypted broadcast key to the non-root access point/bridge, which uses the session key to decrypt it. The non-root access point/bridge and the root access point/bridge activate WEP and use the session and broadcast WEP keys for all communications during the remainder of the session.

There is more than one type of EAP authentication, but the access point/bridge 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 10-6](#) for instructions on setting up EAP on the access point/bridge.

**Note**

If you use EAP authentication, you can select open or shared key authentication, but you don't have to. EAP authentication controls authentication both to your access point/bridge and to your network.

Using CCKM for Authenticated Access Point/Bridges

Using Cisco Centralized Key Management (CCKM), authenticated non-root access point/bridges can roam from one root access point/bridge to another without any perceptible delay during reassociation. An access point or switch on your network provides Wireless Domain Services (WDS) and creates a cache of security credentials for CCKM-enabled access point/bridges on the subnet. The WDS device's cache of credentials dramatically reduces the time required for reassociation when a CCKM-enabled non-root access point/bridge roams to a new root access point/bridge. When a non-root access point/bridge roams, the WDS device forwards the access point/bridge's security credentials to the new root access point/bridge, and the reassociation process is reduced to a two-packet exchange between the roaming access point/bridge and the new root access point/bridge. Roaming access point/bridges 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 10-6 for instructions on enabling CCKM on your access point/bridge. See Chapter 10 in the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points* for detailed instructions on setting up a WDS access point on your wireless LAN.

Using WPA Key Management

Wi-Fi Protected Access (WPA) is a standards-based, interoperable security enhancement that strongly increases the level of data protection and access control for existing and future wireless LAN systems. It is derived from and will be forward-compatible with the upcoming IEEE 802.11i standard. WPA leverages TKIP (Temporal Key Integrity Protocol) for data protection and 802.1X for authenticated key management.

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

**Note**

Unicast and multicast cipher suites advertised in the 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 root access point/bridge and the non-root access point/bridge to switch back to the new cipher suite. Currently, the WPA and CCKM protocols do not allow the cipher suite to be changed after the initial 802.11 cipher negotiation phase. In this scenario, the non-root access point/bridge is disassociated from the wireless LAN.

See the [“Assigning Authentication Types to an SSID”](#) section on page 10-6 for instructions on configuring WPA key management on your access point/bridge.

Configuring Authentication Types

This section describes how to configure authentication types. You attach configuration types to the access point/bridge's SSID. See [Chapter 7, “Configuring SSIDs,”](#) for details on setting up the access point/bridge SSID. This section contains these topics:

- [Default Authentication Settings, page 10-6](#)
- [Assigning Authentication Types to an SSID, page 10-6](#)
- [Configuring Authentication Holdoffs, Timeouts, and Intervals, page 10-10](#)

Default Authentication Settings

The default SSID on the access point/bridge is *autoinstall*. [Table 10-1](#) shows the default authentication settings for the default SSID:

Table 10-1 Default Authentication Configuration

Feature	Default Setting
SSID	autoinstall
Guest Mode SSID	autoinstall (The access point/bridge broadcasts this SSID in its beacon and allows access point/bridges with no SSID to associate.)
Authentication types assigned to tsunami	open

Assigning Authentication Types to an SSID

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

	Command	Purpose
Step 1	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>interface dot11radio 0</code>	Enter interface configuration mode for the radio interface.
Step 3	<code>ssid ssid-string</code>	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. Note Do not include spaces in SSIDs.

	Command	Purpose
Step 4	authentication open [eap list-name]	<p>(Optional) Set the authentication type to open for this SSID. Open authentication allows any access point/bridge to authenticate and then attempt to communicate with the access point/bridge.</p> <ul style="list-style-type: none"> (Optional) Set the SSID's authentication type to open with EAP authentication. The access point/bridge forces all other access point/bridges to perform EAP authentication before they are allowed to join the network. For <i>list-name</i>, specify the authentication method list. <p>Note A access point/bridge configured for EAP authentication forces all access point/bridges that associate to perform EAP authentication. Access points and bridges that do not use EAP cannot communicate with the access point/bridge.</p>
Step 5	authentication shared [eap list-name]	<p>(Optional) Set the authentication type for the SSID to shared key.</p> <p>Note Because of shared key's security flaws, Cisco recommends that you avoid using it.</p> <ul style="list-style-type: none"> (Optional) Set the SSID's authentication type to shared key with EAP authentication. For <i>list-name</i>, specify the authentication method list.
Step 6	authentication network-eap <i>list-name</i>	<p>(Optional) Set the authentication type for the SSID to use LEAP for authentication and key distribution. Cisco access point/bridges only support LEAP, while other wireless clients may support other EAP methods such as EAP, PEAP, or TLS.</p>

	Command	Purpose
Step 7	authentication key-management {[wpa] [cckm]} [optional]	<p>(Optional) Set the authentication type for the SSID to WPA, CCKM, or both. If you use the optional keyword, non-root access point/bridges not configured for WPA or CCKM can use this SSID. If you do not use the optional keyword, only WPA or CCKM access point/bridges are allowed to use the SSID.</p> <p>To enable CCKM for an SSID, you must also enable Network-EAP authentication. To enable WPA for an SSID, you must also enable Open authentication or Network-EAP or both.</p> <p>Note Only 802.11b and 802.11g radios support WPA and CCKM simultaneously.</p> <p>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. To enable both CCKM and WPA, you must set the encryption mode to a cipher suite that includes TKIP. See the “Configuring Cipher Suites and WEP” section on page 9-3 for instructions on configuring the VLAN encryption mode.</p> <p>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” section on page 10-9 for instructions on configuring a pre-shared key.</p> <p>Note To support CCKM, your root access point/bridge must interact with the WDS device on your network. See the “Configuring the Root Access Point/Bridge to Interact with the WDS Device” section on page 10-9 for instructions on configuring your root access point/bridge to interact with your WDS device.</p>
Step 8	end	Return to privileged EXEC mode.
Step 9	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 access point/bridgeman to open with EAP authentication. Access points and bridges using the access point/bridge an SSID attempt EAP authentication using a server named *adam*.

```
bridge# configure terminal
bridge(config)# configure interface dot11radio 0
bridge(config-if)# ssid bridgeman
bridge(config-ssid)# authentication open eap adam
bridge(config-ssid)# end
```

The configuration on non-root access point/bridges associated to this access point/bridge would also contain these commands:

```
bridge(config)# configure interface dot11radio 0
bridge(config-if)# ssid bridgeman
bridge(config-ssid)# authentication client username bridge7 password catch22
```

```
bridge(config-ssid)# authentication open eap adam
```

This example sets the authentication type for the SSID access point/bridget to network-EAP with a static WEP key. EAP-enabled access point/bridges using the access point/bridget SSID attempt EAP authentication using a server named *eve*, and access point/bridges using static WEP rely on the static WEP key.

```
bridge# configure terminal
bridge(config)# configure interface dot11radio 0
bridge(config-if)# encryption key 2 size 128 12345678901234567890123456
bridge(config-if)# ssid bridget
bridge(config-ssid)# authentication network-eap eve
bridge(config-ssid)# end
```

The configuration on non-root access point/bridges associated to this access point/bridge would also contain these commands:

```
bridge(config)# configure interface dot11radio 0
bridge(config-if)# ssid bridget
bridge(config-ssid)# authentication client username bridge11 password 99bottles
```

Configuring the Root Access Point/Bridge to Interact with the WDS Device

To support non-root access point/bridges using CCKM, your root access point/bridge must interact with the WDS device on your network, and your authentication server must be configured with a username and password for the root access point/bridge. For detailed instructions on configuring WDS and CCKM on your wireless LAN, see Chapter 11 in the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*.

On your root access point/bridge, enter this command in global configuration mode:

```
bridge(config)# wlccp ap username username password password
```

You must configure the same username and password pair when you set up the root access point/bridge as a client on your authentication server.

Configuring Additional WPA Settings

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

Setting a Pre-Shared Key

To support WPA on a wireless LAN where 802.1x-based authentication is not available, you must configure a pre-shared key on the access point/bridge. 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/bridge 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 root access point/bridge distributes a group key to the authenticated non-root access point/bridge. You can use these optional settings to configure the root access point/bridge to change and distribute the group key based on association and disassociation of non-root access point/bridges:

- Membership termination—the root access point/bridge generates and distributes a new group key when any authenticated non-root access point/bridge disassociates from the root access point/bridge. This feature keeps the group key private for associated access point/bridges.
- Capability change—the root access point/bridge generates and distributes a dynamic group key when the last non-key management (static WEP) non-root access point/bridge disassociates, and it distributes the statically configured WEP key when the first non-key management (static WEP) non-root access point/bridge authenticates. In WPA migration mode, this feature significantly improves the security of key-management capable clients when there are no static-WEP access point/bridges associated to the root access point/bridge.

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	interface dot11radio 0	Enter interface configuration mode for the radio interface.
Step 3	ssid <i>ssid-string</i>	Enter SSID configuration mode for the SSID.
Step 4	wpa-psk { hex ascii } [0 7] <i>encryption-key</i>	Enter a pre-shared key for access point/bridges using WPA that also use static WEP keys. Enter the key using either hexadecimal or ASCII characters. 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/bridge expands the key for you. You can enter a maximum of 63 ASCII characters.
Step 5	end	Return to privileged EXEC mode.
Step 6	copy running-config startup-config	(Optional) Save your entries in the configuration file.

This example shows how to configure a pre-shared key for non-root access point/bridges using WPA and static WEP, with group key update options:

```
bridge# configure terminal
bridge(config)# configure interface dot11radio 0
bridge(config-if)# ssid batman
bridge(config-ssid)# wpa-psk ascii batmobile65
bridge(config-ssid)# end
```

Configuring Authentication Holdoffs, Timeouts, and Intervals

Beginning in privileged EXEC mode, follow these steps to configure holdoff times, reauthentication periods, and authentication timeouts for non-root access point/bridges authenticating through your root access point/bridge:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	dot11 holdoff-time <i>seconds</i>	Enter the number of seconds a root access point/bridge must wait before it disassociates and idle client. Enter a value from 1 to 65555 seconds.

	Command	Purpose
Step 3	interface dot11radio 0	Enter interface configuration mode for the radio interface.
Step 4	dot1x client-timeout <i>seconds</i>	Enter the number of seconds the bridge should wait for a reply from a non-root access point/bridge attempting to authenticate before the authentication fails. Enter a value from 1 to 65555 seconds.
Step 5	dot1x reauth-period <i>seconds</i> [<i>server</i>]	Enter the interval in seconds that the access point/bridge waits before forcing an authenticated non-root access point/bridge to reauthenticate. <ul style="list-style-type: none"> (Optional) Enter the server keyword to configure the access point/bridge 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 non-root access point/bridge before termination of the session or prompt. The server sends this attribute to the root access point/bridge when a non-root access point/bridge performs EAP authentication.
Step 6	end	Return to privileged EXEC mode.
Step 7	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.

Setting Up a Non-Root Access Point/Bridge as a LEAP Client

You can set up a non-root access point/bridge to authenticate to your network like other wireless client devices. After you provide a network username and password for the non-root access point/bridge, it authenticates to your network using LEAP, Cisco's wireless authentication method, and receives and uses dynamic WEP keys.

Setting up a non-root access point/bridge as a LEAP client requires three major steps:

1. Create an authentication username and password for the non-root access point/bridge on your authentication server.
2. Configure LEAP authentication on the root access point/bridge to which the non-root access point/bridge associates.
3. Configure the non-root access point/bridge to act as a LEAP client.

Beginning in Privileged Exec mode, follow these instructions to set up the non-root access point/bridge as a LEAP client:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio 0	Enter interface configuration mode for the radio interface.
Step 3	ssid <i>ssid-string</i>	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.

	Command	Purpose
Step 4	authentication client username <i>username</i> password <i>password</i>	Configure the username and password that the non-root bridge uses when it performs LEAP authentication. This username and password must match the username and password that you set up for the non-root access point/bridge on the authentication server.
Step 5	end	Return to privileged EXEC mode.
Step 6	copy running-config startup-config	(Optional) Save your entries in the configuration file.

This example sets a LEAP username and password for the SSID bridgeman:

```
bridge# configure terminal
bridge(config)# configure interface dot11radio 0
bridge(config-if)# ssid bridgeman
bridge(config-ssid)# authentication client username buggy password run4yerlife
bridge(config-ssid)# end
```

Matching Authentication Types on Root and Non-Root Access Point/Bridges

To use the authentication types described in this section, the root access point/bridge authentication settings must match the settings on the non-root access point/bridges that associate to the root access point/bridge.

Table 10-2 lists the settings required for each authentication type on the root and non-root access point/bridges.

Table 10-2 Client and Access Point/Bridge Security Settings

Security Feature	Non-Root Access Point/Bridge Setting	Root Access Point/Bridge Setting
Static WEP with open authentication	Set up and enable WEP	Set up and enable WEP and enable Open Authentication
Static WEP with shared key authentication	Set up and enable WEP and enable Shared Key Authentication	Set up and enable WEP and enable Shared Key Authentication
LEAP authentication	Configure a LEAP username and password	Set up and enable WEP and enable network-EAP authentication
CCKM key management	Set up and enable WEP and enable CCKM authentication	Set up and enable WEP and enable CCKM authentication, configure the root access point/bridge to interact with your WDS device, and add the root access point/bridge to your authentication server as a client device
WPA key management	Set up and enable WEP and enable WPA authentication	Set up and enable WEP and enable WPA authentication

