



Configuring Fast Reassociation

This chapter describes how to configure the access point for fast reassociation of roaming client devices. This chapter contains these sections:

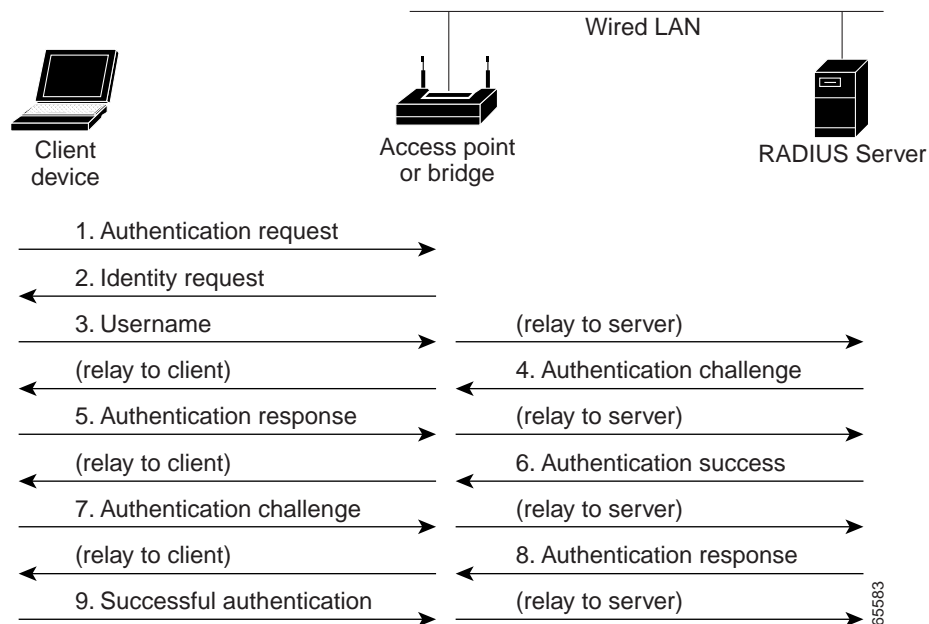
- [Understanding Fast Reassociation, page 11-2](#)
- [Configuring Fast Reassociation, page 11-4](#)

Understanding Fast Reassociation

Access points in many wireless LANs serve mobile client devices that roam from access point to access point throughout the installation. Some applications running on client devices require fast reassociation when they roam to a different access point. Voice applications, for example, require seamless roaming to prevent delays and gaps in conversation.

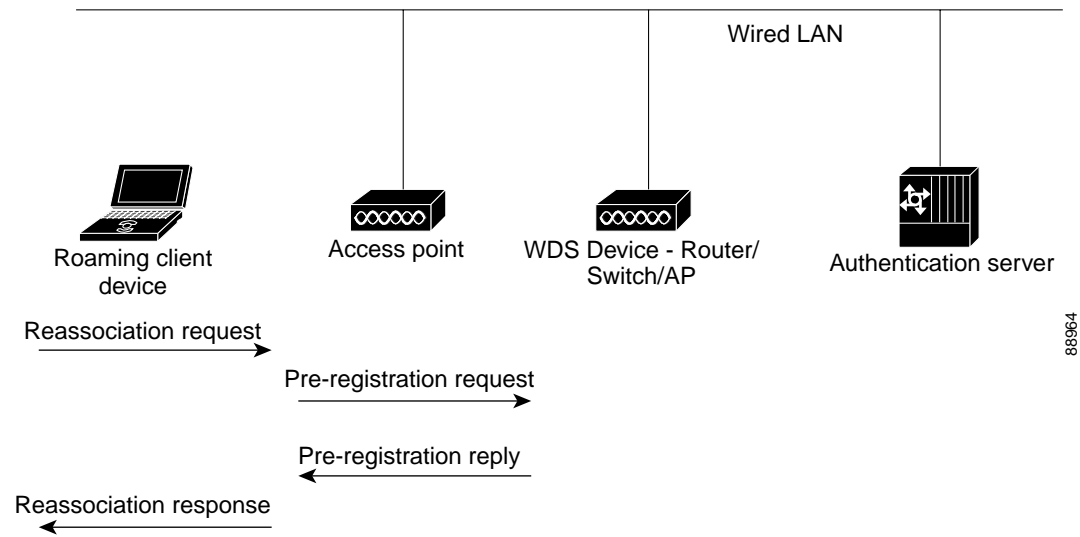
During normal operation, LEAP-enabled client devices mutually authenticate with a new access point by performing a complete LEAP authentication, including communication with the main RADIUS server, as in [Figure 11-1](#).

Figure 11-1 Client Authentication Using a RADIUS Server



When you configure your wireless LAN for fast reassociation, however, LEAP-enabled client devices roam from one access point to another without involving the main server. Using Cisco Centralized Key Management (CCKM), an access point configured to provide Wireless Domain Services (WDS) takes the place of the RADIUS server and authenticates the client so quickly that there is no perceptible delay in voice or other time-sensitive applications. [Figure 11-2](#) shows client authentication using CCKM.

Figure 11-2 Client Reassociation Using CCKM and a WDS Access Point



The WDS access point maintains a cache of credentials for CCKM-capable client devices on your wireless LAN. When a CCKM-capable client roams from one access point to another, the client sends a reassociation request to the new access point, and the new access point relays the request to the WDS access point. The WDS access point forwards the client's credentials to the new access point, and the new access point sends the reassociation response to the client. Only two packets pass between the client and the new access point, greatly shortening the reassociation time. The client also uses the reassociation response to generate the unicast key.

The WDS access point performs several tasks on your wireless LAN:

- Authenticates all access points in the subnet and establishes a secure communication channel with each of them.
- Registers all client devices in the subnet, establishes session keys for them, and caches their security credentials. When a client roams to another access point, the WDS access point forwards the client's security credentials to the new access point.
- Advertises its WDS capability and participates in electing the best WDS access point for your wireless LAN. When you configure your wireless LAN for fast reassociation, you set up one access point as the main WDS access point candidate and one or more additional access points as backup WDS access point candidates.

The access points on your wireless LAN interact with the WDS access point in these activities:

- Discover and track the current WDS access point and relay WDS advertisements to the wireless LAN.
- Authenticate with the WDS access point and establish a secure communication channel to the WDS access point.
- Register associated client devices with the WDS access point.

Configuring Fast Reassociation

This section describes how to set up your wireless LAN to use fast reassociation for roaming client devices. This section includes these sections:

- [Requirements for Fast Reassociation, page 11-4](#)
- [Guidelines for Fast Reassociation, page 11-4](#)
- [Configuration Overview, page 11-4](#)
- [Configuring Access Points as Potential WDS Access Points, page 11-5](#)
- [Configuring Access Points to use the WDS Access Point, page 11-9](#)
- [Configuring the Authentication Server to Support Fast Reassociation, page 11-10](#)
- [Viewing WDS Information, page 11-16](#)
- [Using Debug Messages, page 11-17](#)

Requirements for Fast Reassociation

To set up fast reassociation, you must have these items on your wireless LAN:

- At least one access point that you can configure as the WDS access point
- Cisco Aironet client devices running Cisco client firmware version 5.20.17 or later

Guidelines for Fast Reassociation

Follow these guidelines when configuring fast reassociation:

- Configure an access point that does not serve a large number of client devices as the WDS access point. If client devices associate to the WDS access point when it starts up, the clients might wait up to 10 minutes to be authenticated.
- Repeater access points do not support WDS. Do not configure a repeater access point as a WDS candidate, and do not configure a WDS access point to return (fall back) to repeater mode in case of Ethernet failure.
- You cannot configure a 350 series access point as a WDS access point. However, you can configure 350 series access points to use the WDS access point.

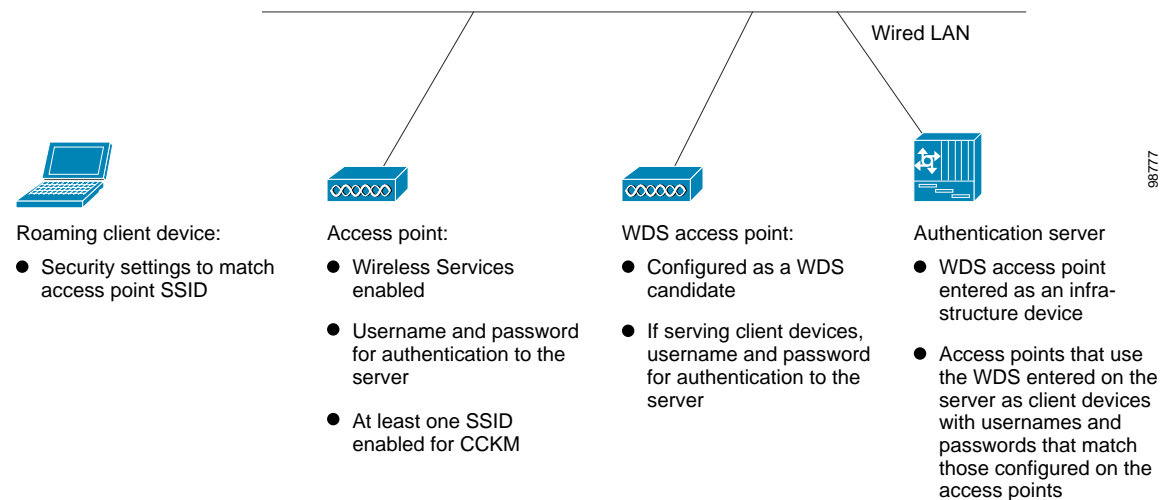
Configuration Overview

You must complete three major steps to set up fast reassociation:

1. Configure access points on your wireless LAN as potential WDS access points.
2. Configure the rest of your access points to use the WDS access point.
3. Enable access points on the subnet to allow CCKM authenticated key management for at least one SSID. See the [“Configuring Authentication Types” section on page 10-9](#) for complete instructions on enabling CCKM.
4. Configure the authentication server on your network to authenticate the WDS access point and the access points that use the WDS access point.

Figure 11-3 shows the required configuration for each device that participates in fast reassociation.

Figure 11-3 Configurations on Devices Participating in CCKM



98777

Configuring Access Points as Potential WDS Access Points



Note

For the main WDS candidate, configure an access point that does not serve a large number of client devices. If client devices associate to the WDS access point when it starts up, the clients might wait up to 10 minutes to be authenticated.



Note

Repeater access points do not support WDS. Do not configure a repeater access point as a WDS candidate, and do not configure a WDS access point to fall back to repeater mode in case of Ethernet failure.



Note

When WDS is enabled, the WDS access point performs and tracks all LEAP authentications. Therefore, you must configure EAP security settings on the WDS access point. See [Chapter 10, “Configuring Authentication Types,”](#) for instructions on configuring EAP on the access point.



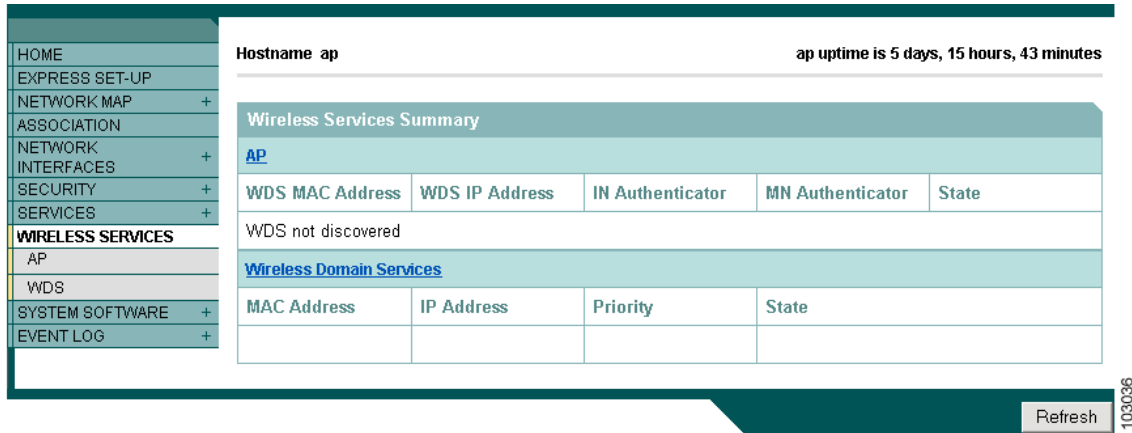
Note

You cannot configure a 350 series access point as a WDS access point. However, you can configure 350 series access points to use the WDS access point.

On the access point that you want to configure as your primary WDS access point, follow these steps to configure the access point as the main WDS candidate:

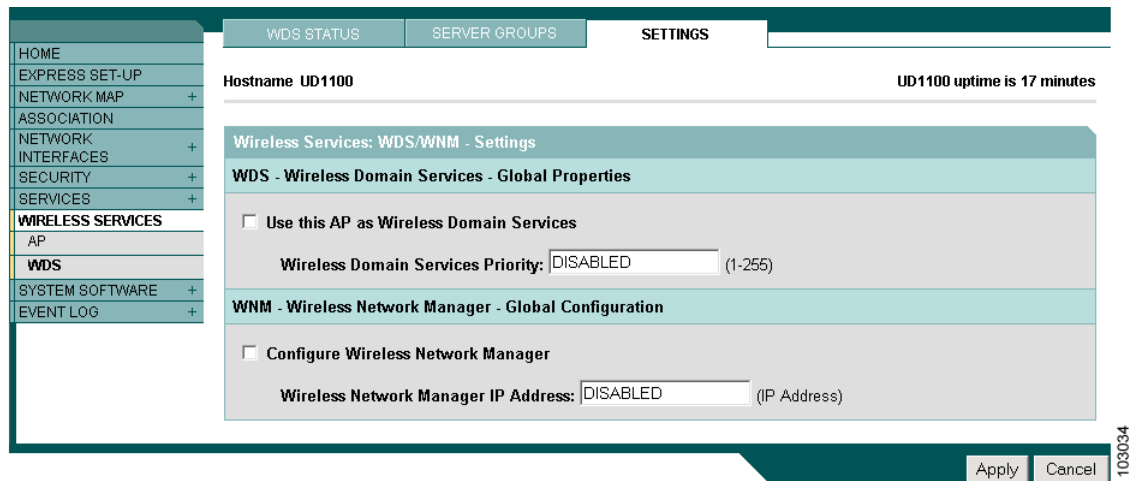
- Step 1 Browse to the Wireless Services Summary page. Figure 11-4 shows the Wireless Services Summary page.

Figure 11-4 Wireless Services Summary Page



- Step 2 Click **WDS** to browse to the WDS/WNM Summary page.
- Step 3 On the WDS/WNM Summary page, click **Settings** to browse to the WDS/WNM Settings page. Figure 11-5 shows the WDS/WNM Settings page.

Figure 11-5 WDS/WNM Settings Page



- Step 4 Check the *Use this AP as Wireless Domain Services* check box.
- Step 5 In the Wireless Domain Services Priority field, enter a priority number from 1 to 255 to set the priority of this WDS candidate. The WDS access point candidate with the highest priority number becomes the acting WDS access point.

- Step 6** (Optional) If you use a Wireless LAN Solutions Engine (WLSE) on your network, check the *Configure Wireless Network Manager* check box and enter the IP address of the WLSE device in the *Wireless Network Manager IP Address* field. The WDS access point collects radio measurement information from access points and client devices and sends the aggregated data to the WLSE device.
- Step 7** Click **Apply**.
- Step 8** Click **Server Groups** to browse to the WDS Server Groups page. [Figure 11-6](#) shows the WDS Server Groups page.

Figure 11-6 WDS Server Groups Page

The screenshot displays the 'WDS Server Groups' configuration page. On the left is a navigation sidebar with options like HOME, EXPRESS SET-UP, NETWORK MAP, ASSOCIATION, NETWORK INTERFACES, SECURITY, SERVICES, WIRELESS SERVICES, AP, WDS, SYSTEM SOFTWARE, and EVENT LOG. The top navigation bar has tabs for SETTINGS, SERVER GROUPS, and WDS STATUS. The main content area is titled 'Wireless Services: WDS - Server Groups' and shows the configuration for a server group named 'cckm_roamers'. It includes a 'Server Group List' with a 'Delete' button, 'Group Server Priorities' (Priority 1: 10.91.6.159, Priority 2: <NONE>, Priority 3: <NONE>), 'Use Group For' (Client Authentication selected), 'Authentication Settings' (Any Authentication selected), and 'SSID Settings' (Restrict SSIDs selected with a list containing 'fred' and 'ginger'). At the bottom right are 'Apply' and 'Cancel' buttons.

- Step 9** Create a group of servers to be used for 802.1x authentication for the infrastructure devices (access points) that use the WDS access point. Enter a group name in the Server Group Name field.
- Step 10** Select the primary server from the Priority 1 drop-down menu. (If a server that you need to add to the group does not appear in the Priority drop-down menus, click **Define Servers** to browse to the Server Manager page. Configure the server there, and then return to the WDS Server Groups page.)
- Step 11** (Optional) Select backup servers from the Priority 2 and 3 drop-down menus.
- Step 12** Click **Apply**.

- Step 13** Configure the list of servers to be used for 802.1x authentication for CCKM-enabled client devices. You can specify a separate list for clients using a certain type of authentication, such as EAP, LEAP, or MAC-based, or specify a list for client devices using any type of authentication. Enter a group name for the server or servers in the Server Group Name field.
- Step 14** Select the primary server from the Priority 1 drop-down menu. (If a server that you need to add to the group does not appear in the Priority drop-down menus, click **Define Servers** to browse to the Server Manager page. Configure the server there, and then return to the WDS Server Groups page.)
- Step 15** (Optional) Select backup servers from the Priority 2 and 3 drop-down menus.
- Step 16** (Optional) Select **Restrict SSIDs** to limit use of the server group to client devices using specific SSIDs. Enter an SSID in the SSID field and click **Add**. To remove an SSID, highlight it in the SSID list and click **Remove**.
- Step 17** Click **Apply**.
- Step 18** Configure the WDS access point for EAP authentication. See [Chapter 10, “Configuring Authentication Types,”](#) for instructions on configuring EAP authentication.

**Note**

If your WDS access point serves client devices, follow the instructions in the [“Configuring Access Points to use the WDS Access Point”](#) section on page 11-9 to configure the WDS access point to use the WDS.

CLI Configuration Example

This example shows the CLI commands that are equivalent to the steps listed in the [“Configuring Access Points as Potential WDS Access Points”](#) section on page 11-5:

```
AP# configure terminal
AP(config)# aaa new-model
AP(config)# wlccp wds priority 200 interface bv11
AP(config)# wlccp authentication-server infrastructure cckm_infra
AP(config)# wlccp authentication-server client any cckm_roamers
AP(config-wlccp-auth)# ssid fred
AP(config-wlccp-auth)# ssid ginger
AP(config)# end
```

In this example, infrastructure devices are authenticated using server group *cckm_infra*; CCKM-enabled client devices using SSIDs *fred* or *ginger* are authenticated using server group *cckm_roamers*.

For complete descriptions of the commands used in this example, consult the *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*.

Configuring Access Points to use the WDS Access Point

Follow these steps to configure an access point to authenticate through the WDS access point and participate in CCKM:

- Step 1** Browse to the Wireless Services Summary page.
- Step 2** Click **AP** to browse to the Wireless Services AP page. [Figure 11-7](#) shows the Wireless Services AP page.

Figure 11-7 Wireless Services AP Page

The screenshot displays the configuration interface for an access point. On the left is a navigation menu with options like HOME, EXPRESS SET-UP, NETWORK MAP, ASSOCIATION, NETWORK INTERFACES, SECURITY, SERVICES, WIRELESS SERVICES, AP (selected), WDS, SYSTEM SOFTWARE, and EVENT LOG. The main area shows the 'Wireless Services: AP' configuration. At the top, it indicates 'Hostname ap' and 'ap uptime is 6 days, 12 hours, 4 minutes'. The 'Wireless Services' section has a radio button for 'Enabled' selected. Below are three input fields: 'Username' containing 'APWestWing', 'Password' with masked characters, and 'Confirm Password' also with masked characters. At the bottom right, there are 'Apply' and 'Cancel' buttons. A vertical ID '103035' is visible on the right edge.

- Step 3** Click **Enabled** for Wireless Services.
- Step 4** In the Username field, enter a username for the access point. This username must match the username that you create for the access point on your authentication server.
- Step 5** In the Password field, enter a password for the access point, and enter the password again in the Confirm Password field. This password must match the password that you create for the access point on your authentication server.
- Step 6** Click **Apply**.

The access points that you configure to interact with the WDS automatically perform these steps:

- Discover and track the current WDS access point and relay WDS advertisements to the wireless LAN.
- Authenticate with the WDS access point and establish a secure communication channel to the WDS access point.
- Register associated client devices with the WDS access point.

CLI Configuration Example

This example shows the CLI commands that are equivalent to the steps listed in the “[Configuring Access Points to use the WDS Access Point](#)” section on page 11-9:

```
AP# configure terminal
AP(config)# wlccp ap username APWestWing password 7 wes7win8
AP(config)# end
```

In this example, the access point is enabled to interact with the WDS access point, and it authenticates to your authentication server using *APWestWing* as its username and *wes7win8* as its password. You must configure the same username and password pair when you set up the access point as a client on your authentication server.

For complete descriptions of the commands used in this example, consult the *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*.

Configuring the Authentication Server to Support Fast Reassociation

The WDS access point and all access points participating in CCKM must authenticate to your authentication server. On your server, you must configure usernames and passwords for the access points and a username and password for the WDS access point.

If your server runs Cisco ACS, follow these steps to configure the access points on your server:

-
- Step 1** Log into Cisco Secure ACS and click **Network Configuration** to browse to the Network Configuration page. You must use the Network Configuration page to create an entry for the WDS access point. [Figure 11-8](#) shows the Network Configuration page.

Figure 11-8 Network Configuration Page

The screenshot shows the Cisco Network Configuration page. On the left is a navigation menu with the following items: User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration, Interface Configuration, Administration Control, External User Databases, Reports and Activity, and Online Documentation. The main content area is titled "Network Configuration" and contains two tables. The first table is "AAA Clients" and the second is "AAA Servers". Both tables have "Add Entry" and "Search" buttons below them.

AAA Client Hostname	AAA Client IP Address	Authenticate Using
DD_3600	10.10.0.2	TACACS+ (Cisco IOS)
DD_TME_1200_1	10.10.0.24	RADIUS (Cisco Aironet)
DD_TME_1200_2	10.10.0.25	RADIUS (Cisco Aironet)

AAA Server Name	AAA Server IP Address	AAA Server Type
proliant	10.91.104.76	CiscoSecure ACS

Step 2 Click **Add Entry** under the AAA Clients table. The Add AAA Client page appears. [Figure 11-9](#) shows the Add AAA Client page.

Figure 11-9 Add AAA Client Page

Network Configuration

Add AAA Client

AAA Client Hostname: APSouthside

AAA Client IP Address: 10.91.104.99

Key: password

Authenticate Using: RADIUS (Cisco Aironet)

Single Connect TACACS+ AAA Client (Record stop in accounting on failure).

Log Update/Watchdog Packets from this AAA Client

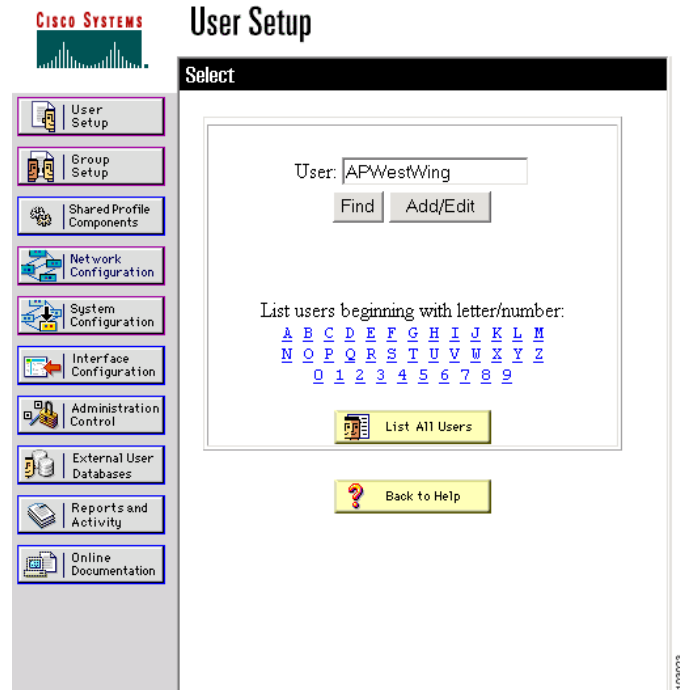
Log RADIUS Tunneling Packets from this AAA Client

Replace RADIUS Port info with Username from this AAA Client

Submit Submit + Restart Cancel

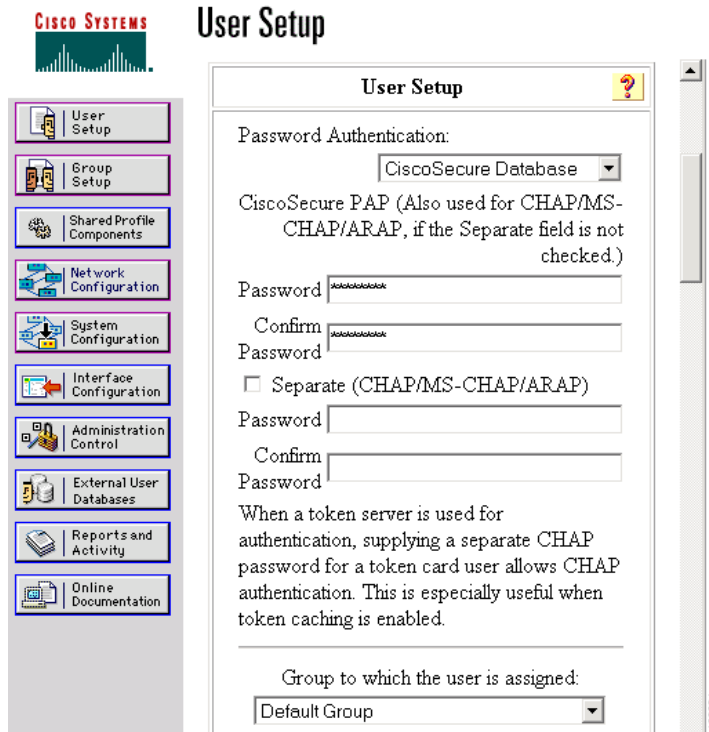
- Step 3** In the AAA Client Hostname field, enter the name of the WDS access point.
- Step 4** In the AAA Client IP Address field, enter the IP address of the WDS access point.
- Step 5** In the Key field, enter exactly the same password that is configured on the WDS access point.
- Step 6** From the Authenticate Using drop-down menu, select **RADIUS (Cisco Aironet)**.
- Step 7** Click **Submit**.
- Step 8** Repeat [Step 2](#) through [Step 7](#) for each WDS access point candidate.
- Step 9** Click **User Setup** to browse to the User Setup page. You must use the User Setup page to create entries for the access points that use the WDS access point. [Figure 11-10](#) shows the User Setup page.

Figure 11-10 User Setup Page



- Step 10 Enter the name of the access point in the User field.
- Step 11 Click **Add/Edit**.
- Step 12 Scroll down to the User Setup box. [Figure 11-11](#) shows the User Setup box.

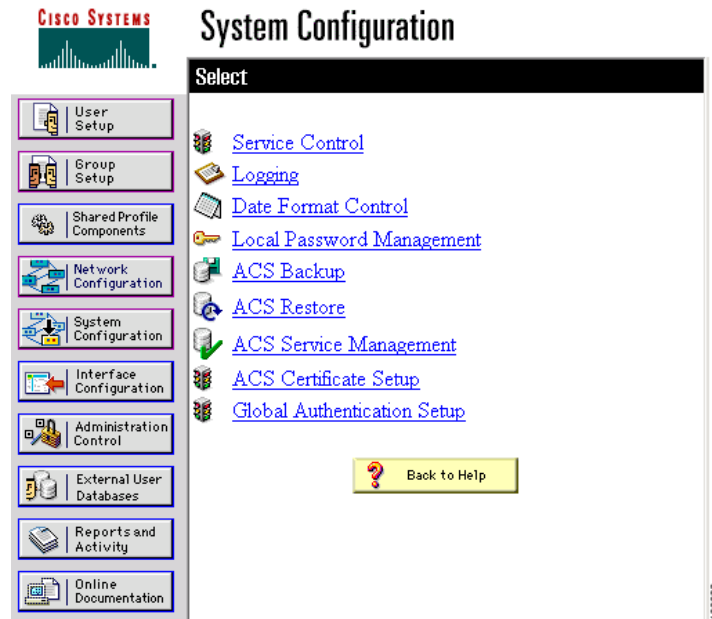
Figure 11-11 ACS User Setup Box



- Step 13 Select **CiscoSecure Database** from the Password Authentication drop-down menu.
- Step 14 In the Password and Confirm Password fields, enter exactly the same password that you entered on the access point on the Wireless Services AP page.
- Step 15 Click **Submit**.
- Step 16 Repeat [Step 10](#) through [Step 15](#) for each access point that uses the WDS access point.

- Step 17 Browse to the System Configuration page, click **Service Control**, and restart ACS to apply your entries. [Figure 11-12](#) shows the System Configuration page.

Figure 11-12 ACS System Configuration Page



Viewing WDS Information

On the web-browser interface, browse to the Wireless Services Summary page to view a summary of WDS status.

On the CLI in privileged exec mode, use these commands to view information about the current WDS access point and other access points participating in CCKM:

Command	Description
show wlccp ap	Use this command on access points participating in CCKM to display the WDS access point's MAC address, the WDS access point's IP address, the access point's state (authenticating, authenticated, or registered), the IP address of the infrastructure authenticator, and the IP address of the client device (MN) authenticator.
show wlccp wds { ap mn } [detail] [mac-addr mac-address]	<p>On the WDS access point only, use this command to display cached information about access points and client devices.</p> <ul style="list-style-type: none"> • ap—Use this option to display access points participating in CCKM. The command displays each access point's MAC address, IP address, state (authenticating, authenticated, or registered), and lifetime (seconds remaining before the access point must reauthenticate). Use the mac-addr option to display information about a specific access point. • mn—Use this option to display cached information about client devices, also called mobile nodes. The command displays each client's MAC address, IP address, the access point to which the client is associated (cur-AP), and state (authenticating, authenticated, or registered). Use the detail option to display the client's lifetime (seconds remaining before the client must reauthenticate), SSID, and VLAN ID. Use the mac-addr option to display information about a specific client device. <p>If you only enter show wlccp wds, the command displays the access point's IP address, MAC address, priority, and interface state (administratively standalone, active, backup, or candidate). If the state is backup, the command also displays the current WDS access point's IP address, MAC address, and priority.</p>

Using Debug Messages

In privileged exec mode, use these debug commands to control the display of debug messages for devices interacting with the WDS access point:

Command	Description
debug wlccp ap { mn wds-discovery state }	Use this command to turn on display of debug messages related to client devices (mn), the WDS discovery process, and access point authentication to the WDS access point (state).
debug wlccp leap-client	Use this command to turn on display of debugging messages related to LEAP-enabled client devices.
debug wlccp packet	Use this command to turn on display of packets to and from the WDS access point.
debug wlccp wds [state statistics]	Use this command and the state option to turn on display of WDS debug and state messages. Use the statistics option to turn on display of failure statistics.

