

# Wireless Domain Services AP as an AAA Server Configuration Example

Document ID: 68098

---

## Introduction

### Prerequisites

Requirements

Components Used

Conventions

### Background Information

### Configure

Configure the WDS AP

Configure the Infrastructure AP

Configure Client Authentication Method

### Verify

### Troubleshoot

### Related Information

---

## Introduction

This document provides a sample configuration for configuring an Access Point (AP) to:

- Provide Wireless Domain Services (WDS).
- Perform the role of an Authentication, Authorization, and Accounting (AAA) server.

You can use this kind of setup when you do not have an external RADIUS server to authenticate infrastructure APs and client devices that participate in WDS.

## Prerequisites

### Requirements

Ensure that you meet these requirements before you attempt this configuration:

- Basic knowledge of WDS
- Knowledge of current Extensible Authentication Protocol (EAP) security methods

### Components Used

The information in this document is based on these software and hardware versions:

- Cisco Aironet 1200 series APs that run Cisco IOS® Software Release 12.3(7)JA1

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

## Background Information

WDS is a part of the Cisco Structured Wireless–Aware Network (SWAN). WDS is a collection of Cisco IOS Software features that enhance Wireless LAN (WLAN) client mobility and simplify WLAN deployment and management.

WDS is the base for many features such as Fast Secure Roaming, Layer 3 mobility, and radio management.

Refer to Configuring WDS, Fast Secure Roaming, Radio Management, and Wireless Intrusion Detection Services for more information on these features.

One of the main purposes of WDS is to cache the user credentials at the first authentication of the client by the authentication server. On subsequent tries, WDS authenticates the client on the basis of the cached information. In order to accomplish this:

- One of the APs must be configured as a WDS AP.
- Other APs must be configured as infrastructure APs that communicate to the WDS AP.
- WDS AP must establish a relationship with the authentication server by authenticating to it with a WDS username and password.

This authentication server validates the credentials of the infrastructure APs and the clients when these devices authenticate for the first time. The authentication server can either be an external RADIUS server or the local RADIUS server on the WDS AP.

The WDS and the infrastructure APs communicate over a multicast protocol called the Wireless LAN Context Control Protocol (WLCCP). These multicast messages cannot be routed. Therefore, a WDS and associated infrastructure APs must be in the same IP subnetwork and on the same LAN segment.

This document explains how to use the local RADIUS server feature on the WDS AP to perform the validation of credentials.

## Configure

### Configure the WDS AP

In this section, you are presented with the information to configure the features described in this document.

In order to configure the AP to serve as a WDS AP with AAA server functionality, you must first enable the local RADIUS server feature on the AP.

Complete these steps:

1. Log in to the AP through the GUI.

The Summary Status Page appears.

The screenshot shows the configuration page for a Cisco Aironet 1200 Series Access Point. The page title is "Cisco Aironet 1200 Series Access Point". The hostname is "WDS" and the WDS uptime is 14 minutes. The left sidebar contains a menu with options: HOME, EXPRESS SET-UP, EXPRESS SECURITY, NETWORK MAP, ASSOCIATION, NETWORK INTERFACES, SECURITY, SERVICES, WIRELESS SERVICES, SYSTEM SOFTWARE, and EVENT LOG. The main content area displays the "Home: Summary Status" section, which includes the following information:

- Association:** Clients: 0, Repeaters: 0
- Network Identity:** IP Address: 10.0.0.1, MAC Address: 000e.d77c.343e
- Network Interfaces:**

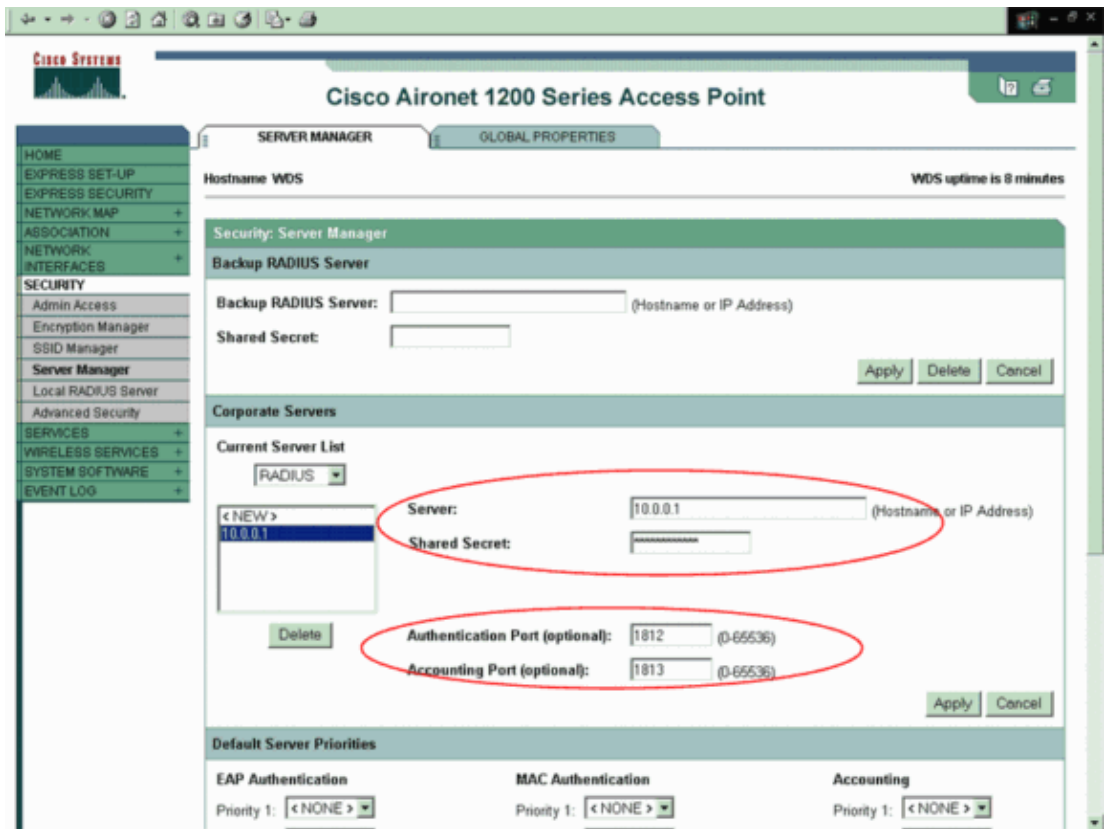
Interface	MAC Address	Transmission Rate
FastEthernet	000e.d77c.343e	100Mbps
Radio0-802.11B	000d.eded.708a	11.0Mbps
Radio1-802.11A	000e.8405.0d4d	54.0Mbps
- Event Log:**

Time	Severity	Description
Mar 1 00:07:11.854	Notification	Configured from console by console
Mar 1 00:00:37.008	Information	Interface BV1 assigned DHCP address 172.16.1.3, mask 255.255.255.0, hostname ap
Mar 1 00:00:28.874	Notification	Line protocol on interface BV1, changed state to up
Mar 1 00:00:27.927	Notification	SNMP agent on host ap is undergoing a cold start
Mar 1 00:00:27.927	Notification	System restarted --
Mar 1 00:00:26.779	Notification	Line protocol on interface Dot11Radio0, changed state to down
Mar 1 00:00:26.775	Notification	Line protocol on interface Dot11Radio1, changed state to down

2. Select **Security > Server Manager** from the left side menu on the AP.
3. Enter the IP address and the shared secret of the AP that acts as the RADIUS server under Corporate Servers.

In this case enter the IP address of the WDS AP since the WDS AP is going to act as the RADIUS server. The example uses the IP address 10.0.0.1. Since this is a local RADIUS server you must use 1812 and 1813 as the Authentication and Accounting ports as this example shows.

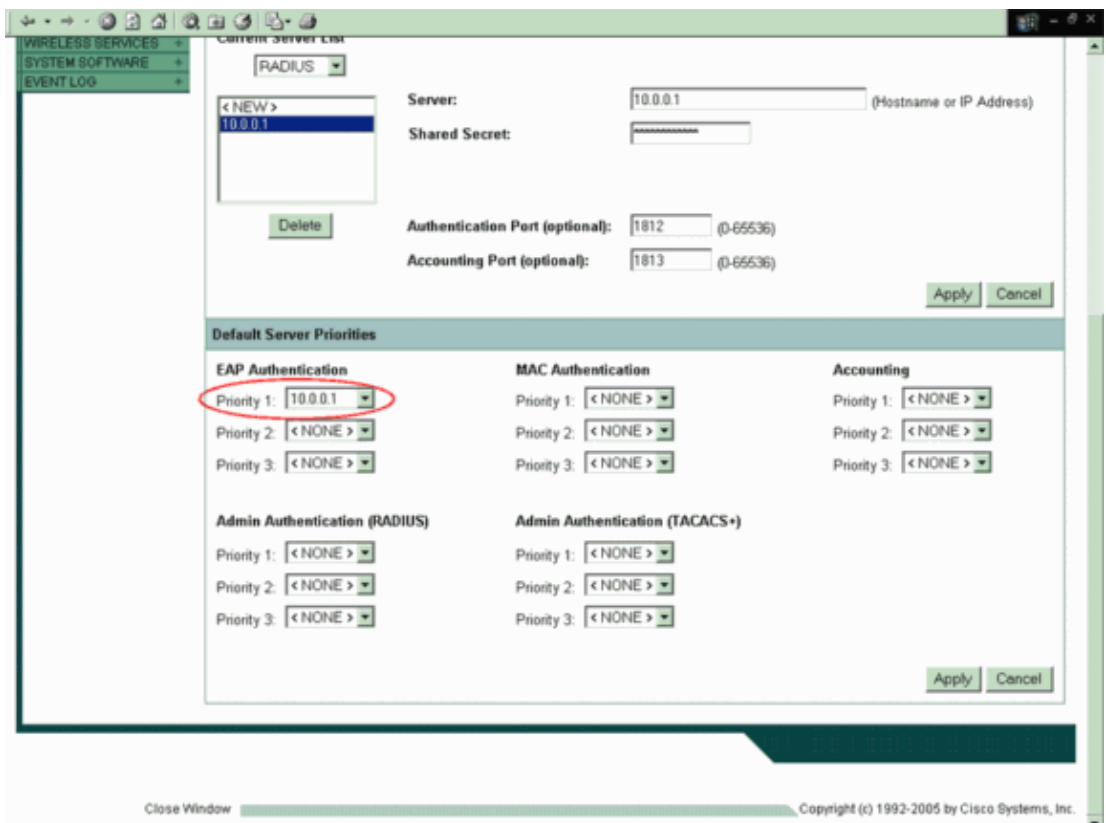
4. Click **Apply**.



5. Select the WDS APs IP address as **Priority 1** under Default Server Priorities for EAP Authentication.

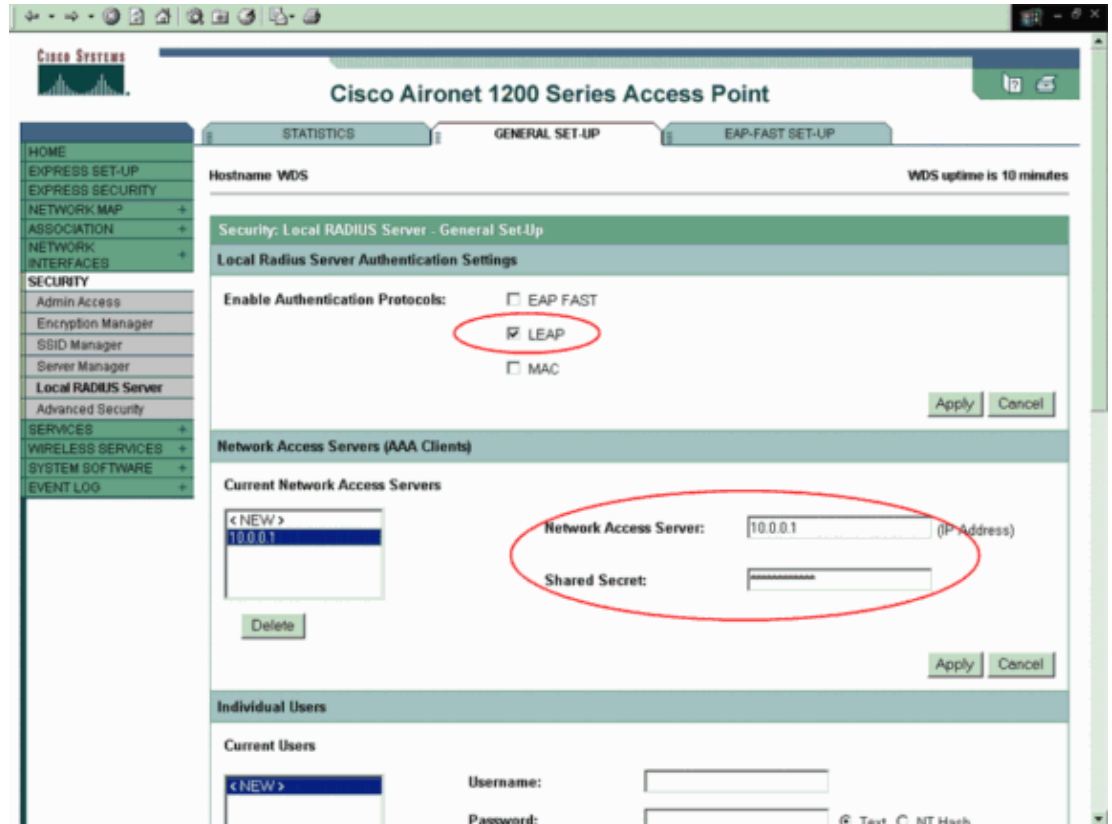
Click **Apply**.

This allows the local RADIUS server to be the first choice for authenticating infrastructure APs and clients.



6. Select **Security > Local Radius server** from the left side menu .

- a. Click **General Set-up** in order to configure local RADIUS server parameters.
- b. Select **LEAP** under Local Radius Server Authentication Settings and click **Apply**.
- c. Enter the IP address of the WDS AP and a shared secret password under Network Access Servers. This example uses the shared secret password as **test123**.
- d. Click **Apply**.



7. Enter the username and password of all infrastructure APs and clients that communicate with the WDS AP under Individual Users.

Click **Apply**.

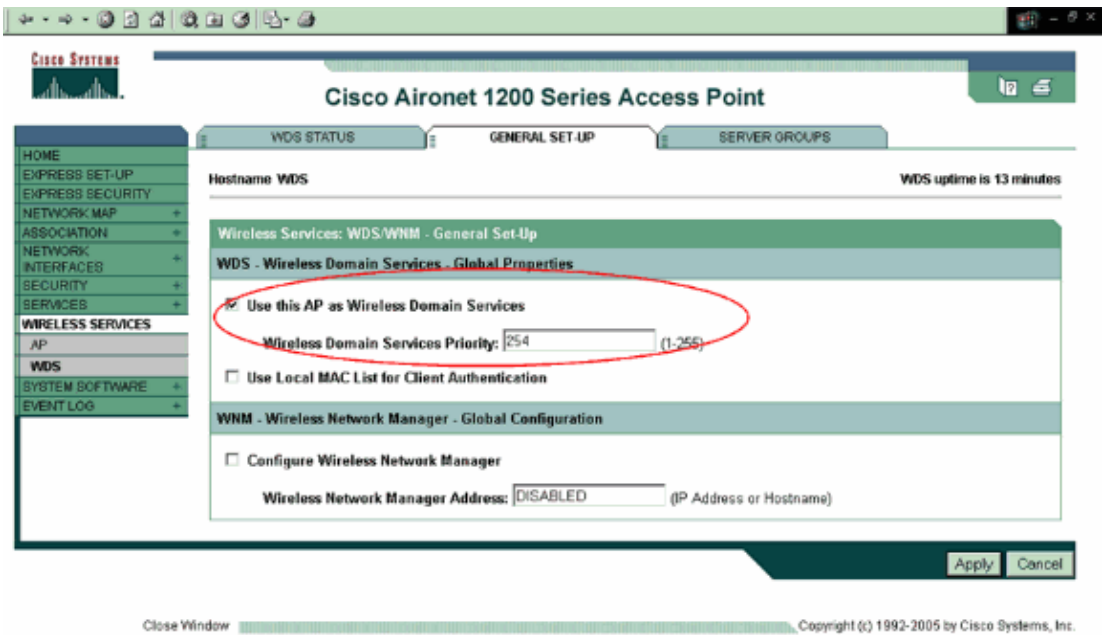
This example includes the username and password of the infrastructure AP that you configure to register with the WDS AP. This example uses the username as **infrastructureAP1** and the password as **Cisco**. The same username and password needs to be configured on the infrastructure access point.

The screenshot displays the 'Individual Users' configuration window. It is divided into two main sections: 'Current Users' and 'User Groups'.  
In the 'Current Users' section, a list on the left contains '<NEW >' and 'infrastructureAPI'. The 'infrastructureAPI' user is selected. To the right, the configuration fields are: 'Username' (infrastructureAPI), 'Password' (masked), 'Confirm Password' (empty), 'Group Name' (<NONE >), and 'MAC Authentication Only' (unchecked). A red oval highlights the 'Username' and 'Password' fields.  
In the 'User Groups' section, a list on the left contains '<NEW >'. The configuration fields for a new group are: 'Group Name' (empty), 'Session Timeout (optional)' (empty, range 1-4294967295 sec), 'Failed Authentications before Lockout (optional)' (empty, range 1-4294967295), 'Lockout (optional)' (Interval selected, empty, range 1-4294967295 sec), 'VLAN ID (optional)' (empty), and 'SSID (optional)' (empty).  
Buttons for 'Delete', 'Apply', and 'Cancel' are present at the bottom of each section.

After you configure the local RADIUS server feature on the AP, you need to enable WDS functionality on the AP.

Complete these steps:

1. Select **Wireless Services > WDS** from the left side menu on the AP.
2. Click **General Set-up**.



3. Check **Use this AP as Wireless Domain Services** on the General Set-up page.

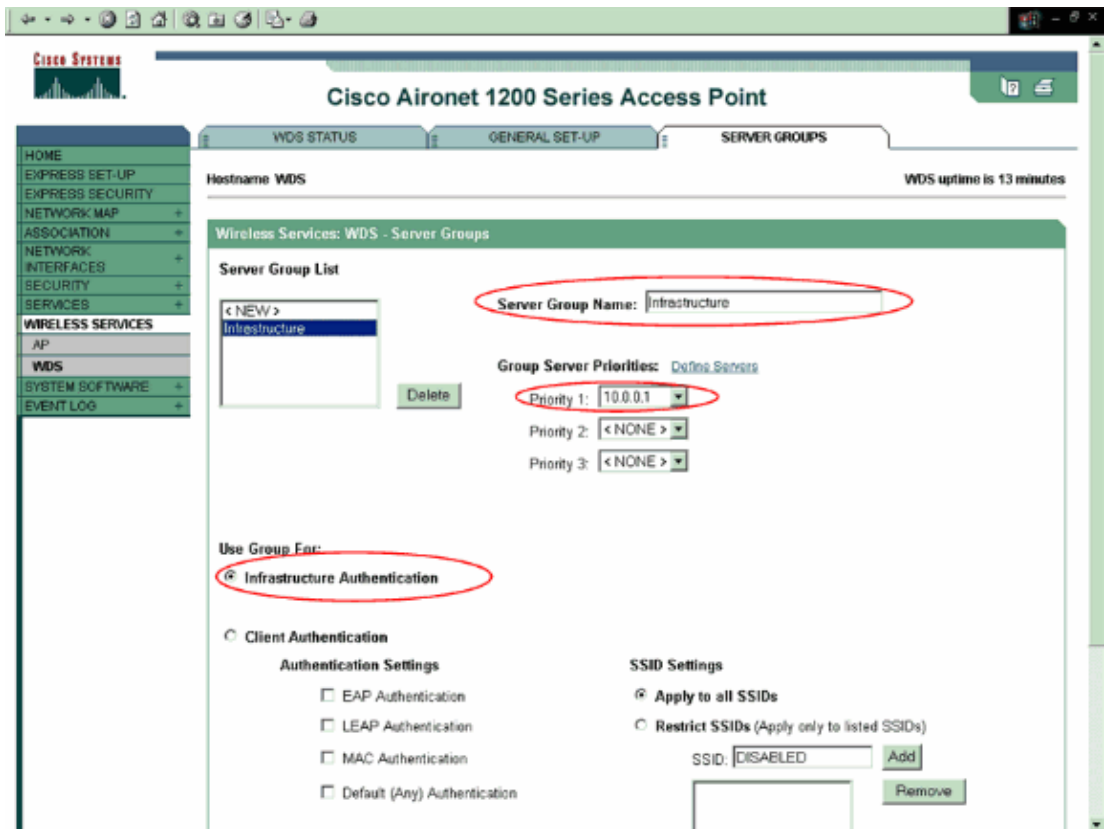
Enter **254** in the Wireless Domain Services Priority field. Click **Apply**.

4. Enable infrastructure authentication.

- a. Click **Server Groups** on the WDS page.
- b. Enter a name in the Server Group Name field to authenticate the infrastructure APs. This example uses the Server Group Name as **Infrastructure**.
- c. Select the IP address of the local RADIUS server from the Group Server Priorities drop-down list.

The WDS AP uses this server to authenticate the infrastructure APs.

- d. Select **Infrastructure Authentication** under Use Group For.
- e. Click **Apply**.



The WDS AP now acts as an AAA server. Configure one of the infrastructure APs to register itself with the WDS AP.

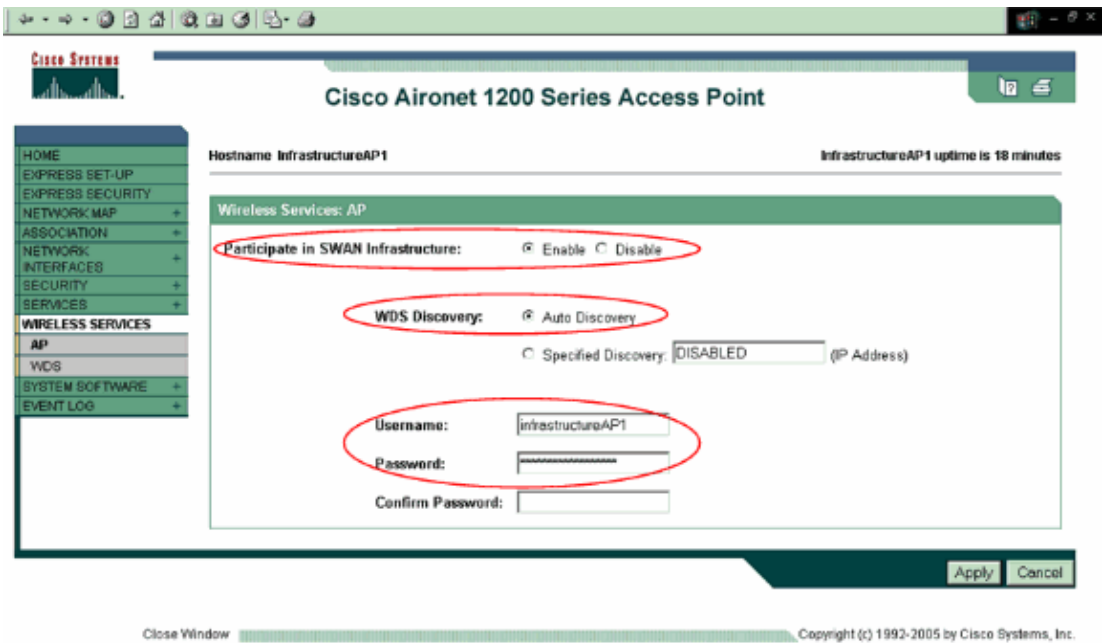
**Note:** Use the Command Lookup Tool (registered customers only) to find more information on the commands used in this document.

## Configure the Infrastructure AP

This section explains the configuration required on the infrastructure AP to register itself with the WDS AP. The clients associate to infrastructure APs. The infrastructure APs request the WDS AP to perform authentication for them.

Complete these steps to add an infrastructure AP that uses the services of the WDS:

1. Select **Wireless Services > AP** from the left side menu.
2. Select **Enable** under Participate in SWAN Infrastructure.
3. Select **Auto Discovery** under WDS Discovery .

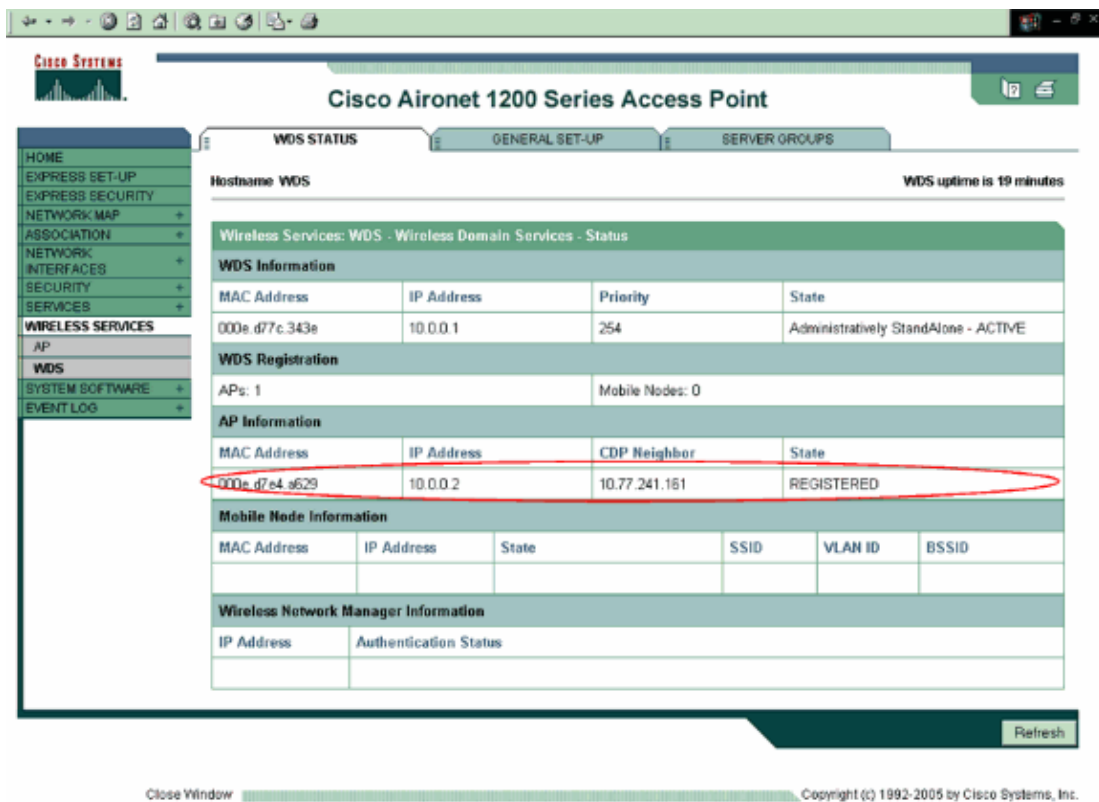


4. Enter the WDS username and password in the appropriate fields.

Click **Apply**.

The username and password must exist on the local RADIUS server. You must define a WDS username and password on the authentication server for all devices that are to be members of the WDS.

The infrastructure AP appears in the AP Information area with State as REGISTERED once you configure the WDS AP and the infrastructure AP on the WDS AP, WDS Status tab. This is under the Wireless Services > WDS menu item.



Incorrect authentication settings either on the WDS AP or the infrastructure AP can cause the AP to not appear as ACTIVE and/or REGISTERED. Check the Authentication server statistics for any errors or failed authentication attempts. Select **Security > Local Radius Server > Statistics** for Authentication server statistics.

You can also use the command **show wlcgp wds ap** from the CLI on the WDS AP to verify the configuration. On successful registration with the WDS AP, the output after a successful registration with the WDS AP looks like this example:

```
WDS#show wlcgp wds ap
MAC-ADDR      IP-ADDR      STATE      LIFETIME      CDP-NEIGHBOR
000e.d7e4.a629 10.0.0.2     REGISTERED  97             10.77.241.161
```

## Configure Client Authentication Method

Add a client authentication method to the WDS.

Complete these steps:

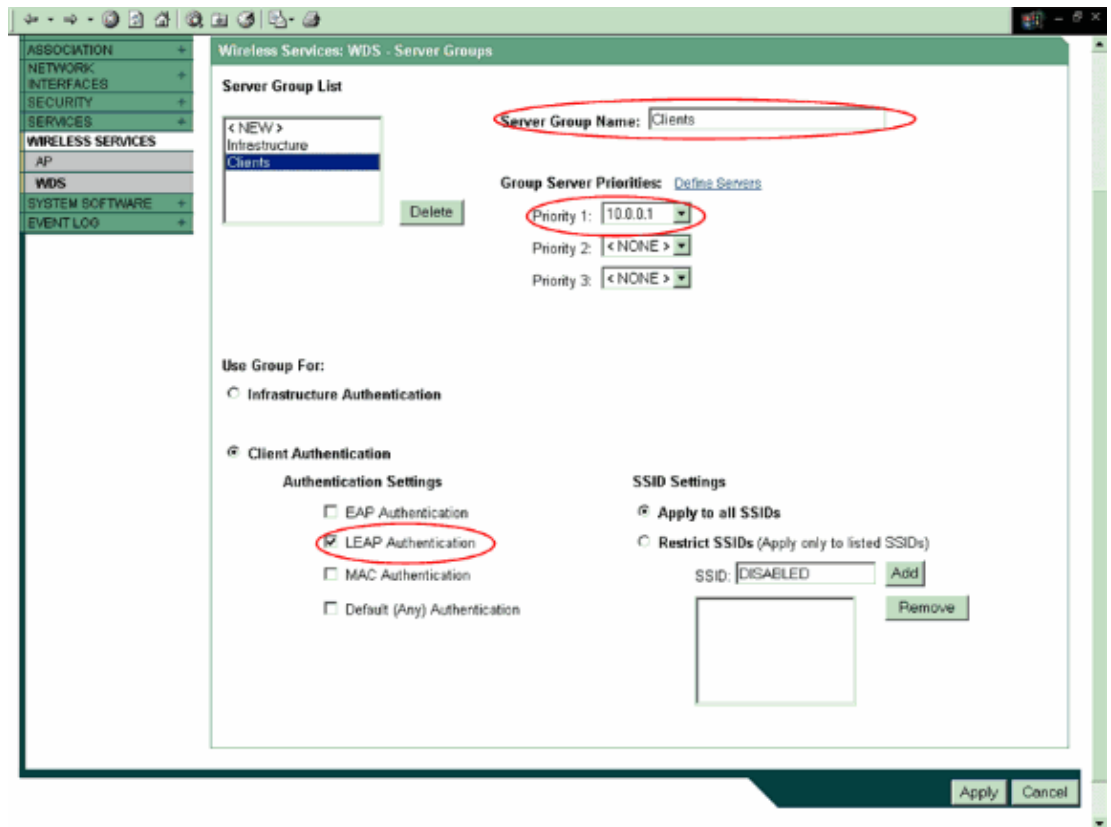
1. Select **Wireless Services > WDS > Server Groups** on the WDS AP.
  - a. Define a server group that authenticates clients (a client group).

This should be different from the previously configured server group for infrastructure authentication. This example uses the Server Group Name as **Clients**.

- b. Set Priority 1 to the local RADIUS server.
- c. Select the type of authentication (LEAP, EAP, MAC, and so forth) to use for client authentication.

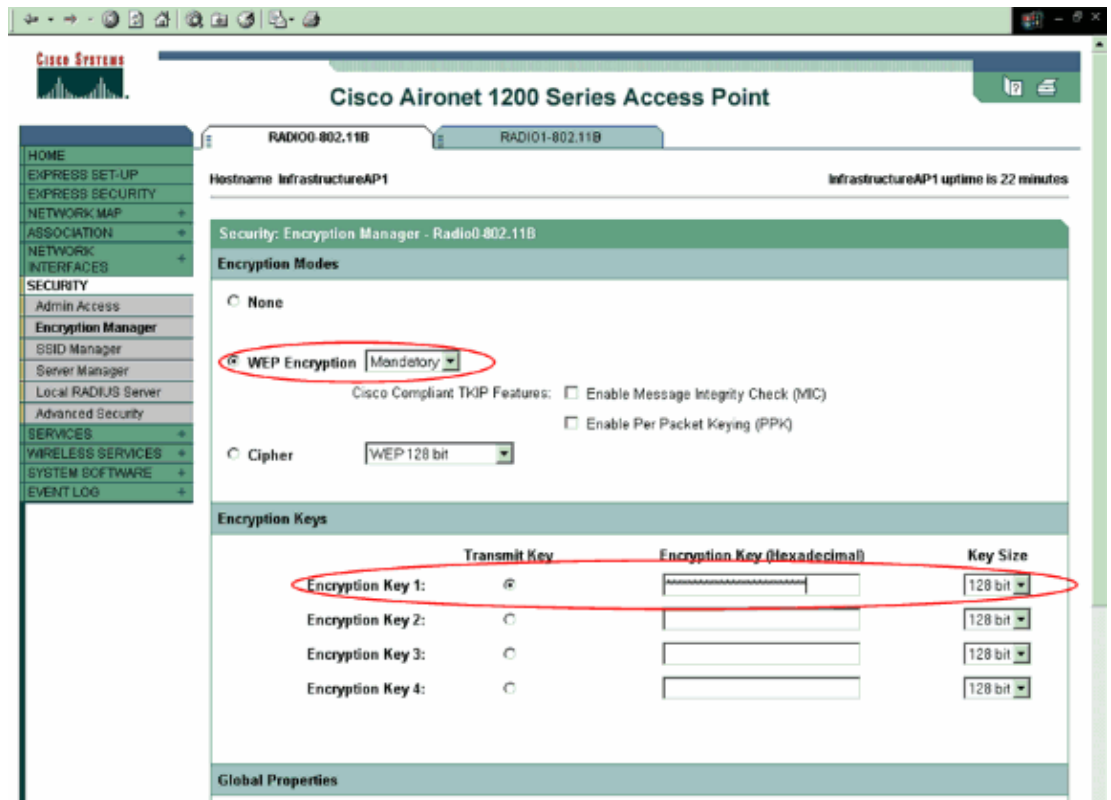
This example uses LEAP authentication.

d. Apply the settings to the relevant SSIDs.



2. Complete these steps on the infrastructure AP:

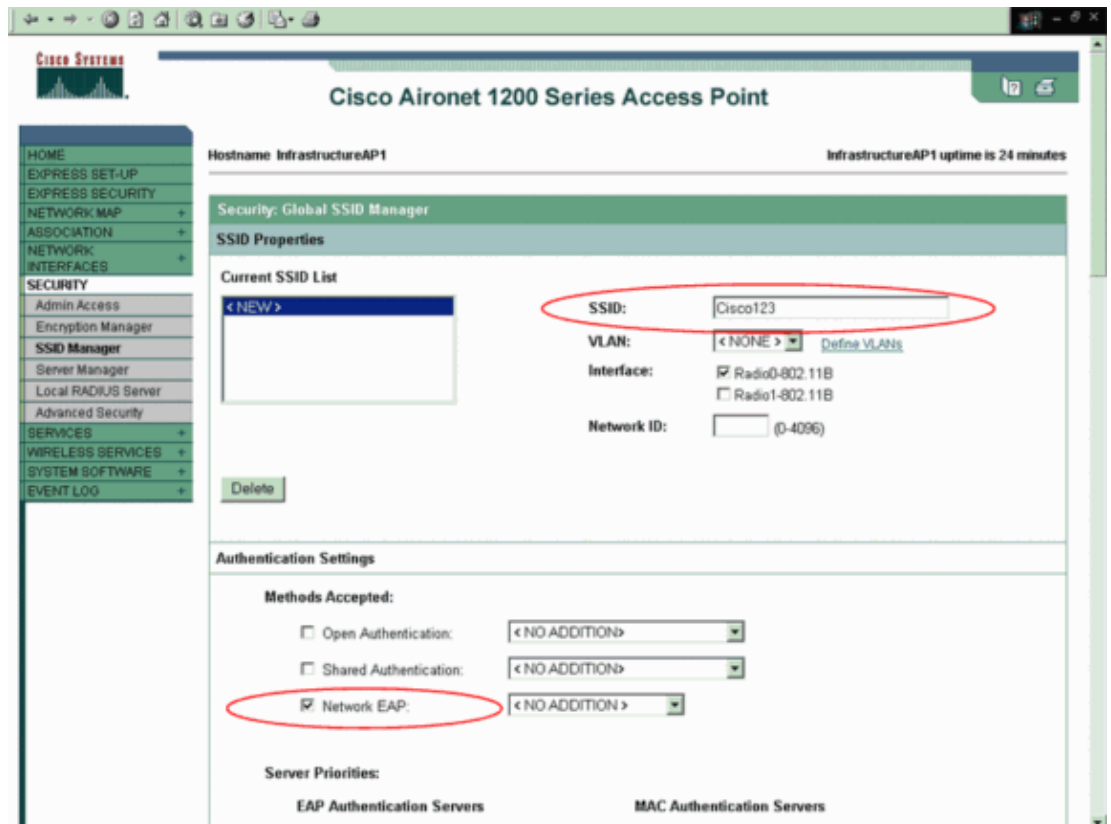
- a. Select **Security > Encryption Manager** and click **WEP Encryption** and choose **Mandatory** from the drop-down menu. Under Encryption Keys, enter the 128-bit WEP encryption key. This example uses the encryption key as **1234567890abcdef1234567890**.



b. Select **Security > SSID Manager** and create a new SSID.

This example uses the SSID as **Cisco123**. Next, choose the authentication method.

c. Select **Network EAP** on the infrastructure AP.



Test that the clients authenticate successfully and associate with the infrastructure APs. The client passes on

its credentials to the infrastructure AP when it comes up for the first time. The infrastructure AP then forwards the same to the WDS AP, which validates the credentials.

**Note:** This document does not explain how to configure the client adapter. Refer to Cisco Aironet Wireless LAN Client Adapters for information on how to configure the client adapter.

## Verify

Use this section to confirm that your configuration works properly.

- **show wlccp wds mn** – Use this command from the CLI on the WDS AP to verify successful client authentication and association with the WDS AP.

```
WDS#show wlccp wds mn
  MAC-ADDR      IP-ADDR      Curr-AP      STATE
0040.96a5.b5d4  10.0.0.15    000e.d7e4.a629 REGISTERED
```

The following debug commands are also helpful.

- **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 packet** – Use this command to turn on display of packets to and from the WDS access point.
- **debug radius local-server** – Activates display of error messages related to failed client authentications to the local authenticator

## Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

---

## Related Information

- [Wireless Domain Services Configuration](#)
  - [Cisco Aironet Client Adapters](#)
  - [Wireless Domain Services FAQ](#)
  - [WLAN Configuration Examples and TechNotes](#)
  - [Cisco Aironet 1200 Series Configuration Examples and TechNotes](#)
  - [Technical Support & Documentation – Cisco Systems](#)
- 

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

---

Updated: Jan 18, 2007

Document ID: 68098

---