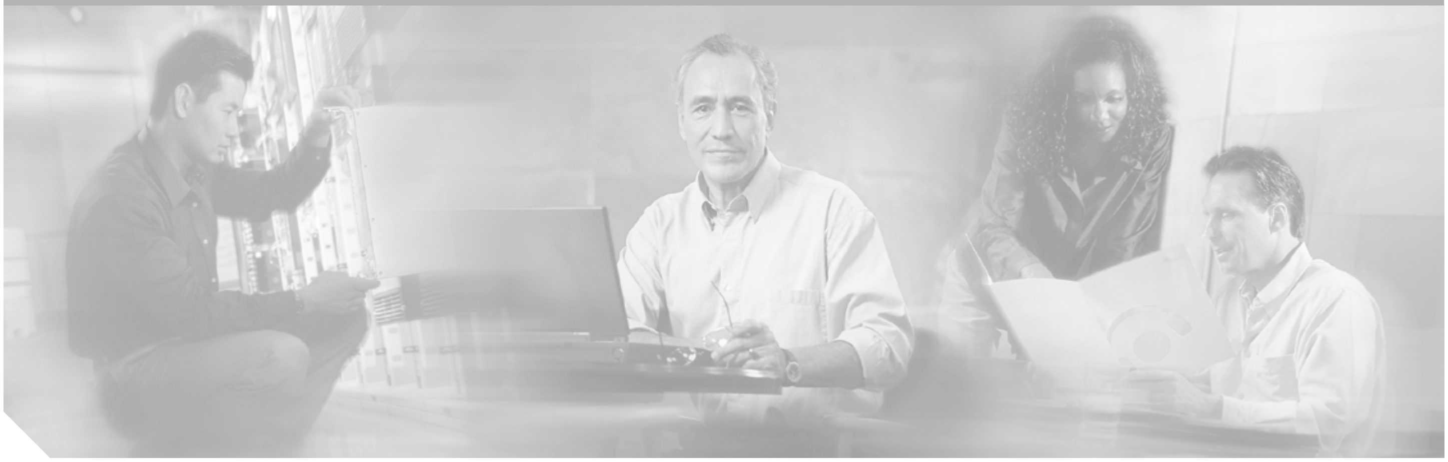


Deployment Guide: Configuring the Cisco Wireless Security Suite

Revision 3.0
April 2004

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-5820-01

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Cisco’s installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

Modifying the equipment without Cisco’s written authorization may result in the equipment no longer complying with FCC requirements for Class A or Class B digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Cisco equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

- Turn the television or radio antenna until the interference stops.

- Move the equipment to one side or the other of the television or radio.

- Move the equipment farther away from the television or radio.

- Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Cisco Systems, Inc. could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB’s public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

Deployment Guide: Configuring the Cisco Wireless Security Suite

CONTENTS

Summary

Numerous papers have been written on the topic of IEEE 802.11 security for wireless LANs (WLANs). The major vulnerabilities of 802.11 security can be summarized as follows:

- Weak device-only authentication: Client devices are authenticated, not users.
- Weak data encryption: Wired equivalent privacy (WEP) has been proven ineffective as a means to encrypt data.
- No message integrity: The integrity check value (ICV) has been proven ineffective as a means to ensure message integrity.

Cisco Systems recognizes that 802.11 security vulnerabilities can be a barrier to wireless LAN deployment. To address these vulnerabilities, Cisco has developed the Cisco Wireless Security Suite to provide robust enhancements to WEP encryption and centralized user-based authentication. This paper discusses the following Cisco Wireless Security Suite features and configurations:

- 802.1X authentication with Cisco LEAP
- Media access control (MAC) address authentication
- Temporal Key Integrity Protocol (TKIP) (per-packet key hashing and message integrity check [MIC]) encryption enhancements: Cisco TKIP and Wi-Fi Protected Access (WPA) TKIP

Although this paper focuses on deployment of the Cisco Wireless Security Suite and Cisco LEAP, the majority of the topics—including access point configuration, Remote Authentication Dial-In User Service (RADIUS) server setup, and encryption/key integrity mechanisms—are applicable to other Extensible Authentication Protocol (EAP) types such as EAP-Transport Layer Security (EAP-TLS) and Protected Extensible Authentication Protocol (PEAP).

Note Refer to the following URL if you need additional information on the Cisco Wireless Security Suite: http://www.cisco.com/go/aironet/security.

Prerequisites

The following software releases are the minimum requirements for each of the deployment configurations noted.

Cisco Aironet Access Point and Wireless Bridge Requirements

- Cisco Aironet 340 and 350 series access points and Cisco Aironet 350 series wireless bridges:
  - Access point firmware version 11.05a for Cisco LEAP
  - Access point firmware version 11.06a for MAC authentication
  - Access point firmware version 11.10T1 for TKIP MIC and per-packet keying
  - Wireless bridge firmware version 11.10T1 for Cisco LEAP
  - Access point or wireless bridge firmware version 11.21 for joint EAP/MAC authentication for public space deployments
- Cisco Aironet 350, 1100, and 1200 series access points:
  - Cisco IOS Software Release 12.2(4)JA for Cisco LEAP and Cisco TKIP
  - Cisco IOS Software Release 12.2(11)JA for WPA TKIP and Cisco Centralized Key Management (CCKM) for fast secure roaming support

Wireless LAN Client Adapter Requirements

- Cisco Aironet 340, 350, and CB20A wireless LAN client adapters with Windows platform:
  - Firmware version 4.25.23 for per-packet keying
  - Network Driver Interface Specification (NDIS) driver version 6.97 for Cisco LEAP
  - NDIS driver version 8.01.06 for MIC
  - Firmware version 5.20.17 for Cisco CCKM
  - Firmware version 5.30.17 for WPA TKIP
  - Cisco Aironet Client Utility (ACU) version 6.0 is recommended, but version 6.2 is required for WPA
- Cisco Aironet 340 and 350 series wireless LAN client adapters with Windows CE platform:
  - Windows CE driver version 1.5, but version 2.3 is recommended

Note At the time of this writing, software and encryption enhancements (TKIP) from Cisco are available for Windows 95, 98, 2000, Millennium (Me), XP, and NT; Windows CE 2.11 and 3.0; Macintosh 9.x and 10.x; and Linux kernel version 2.2 and 2.4 and the above-based clients. WPA TKIP support is available only for 350 and CB20A client adapters on computers running Windows 2000 or XP.

- Non-Cisco wireless LAN client adapters:
  - 802.1X-capable network interface cards (NICs)
  - Third-party supplicant:
    a. Funk Software Odyssey Client version 2.2
    b. Meetinghouse Data Communications AEGIS Client version 2.1
  - WPA-capable NIC card (drivers/firmware) required for WPA:

    http://www.wi-fialliance.com/OpenSection/certified_products.asp

Cisco Aironet Workgroup Bridge Requirements

- Cisco Aironet 340 and 350 series workgroup bridges:
  - Firmware version 8.65, but version 8.84 is recommended

Cisco Secure Access Control Server Requirements

- Cisco Secure Access Control Server (ACS):
  - Version 3.2 is recommended
  - Version 2.6 or 3.0 is required to process Cisco LEAP/MAC authentication requests
- If the Cisco Secure ACS is authenticating users with a Windows NT/2000 domain, it should be configured for external database support.
- If the Cisco Secure ACS is authenticating users with its own local user database, this database must be populated with the appropriate user IDs.

Instructions for Upgrading Components

- Instructions for upgrading Cisco Aironet access point firmware:

  http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo1200/accsspts/ap120scg/bkscgc10.htm
- Instructions for upgrading Cisco Aironet wireless LAN client adapter drivers and firmware:

  http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo_350/350cards/windows/incfg6/win5_ch3.htm
- Instructions for installing Cisco Secure ACS version 3.2:

  http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/acs32/win32sig.htm
- Instructions for configuring Cisco Secure ACS internal and external user databases (version 3.2):

  http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/acs32/user/d.htm
- Instructions for adding users to the local Cisco Secure ACS database (version 3.2):

  http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/acs32/user/u.htm
- Release Notes for Cisco Secure ACS Version 3.2:

  http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/acs32/rnwin321.htm

- Release Notes for Cisco Aironet 1200 series access points (Cisco IOS Software Release 12.2(4) and later and VxWorks revisions):

  http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo1200/accsspts/index.htm
- Release Notes for Cisco Aironet 1100 series access points (Cisco IOS Software Release 12.2(4) and later):

  http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo1100/accsspts/index.htm
- Documentation for Cisco Aironet 340, 350, and CB20A wireless LAN client adapters:

  http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo_350/350cards/index.htm
- Cisco Aironet wireless software (Cisco.com Software Center):

  http://www.cisco.com/public/sw-center/sw-wireless.shtml

Configuring Cisco LEAP

This section covers the basic configuration of Cisco LEAP on the Cisco Secure ACS, the access point, and various clients, including access point repeaters, non-root bridges, and workgroup bridges.

Adding the Access Point to the Cisco Secure ACS

Step 1 On the Cisco Secure ACS main menu, click **Network Configuration**.

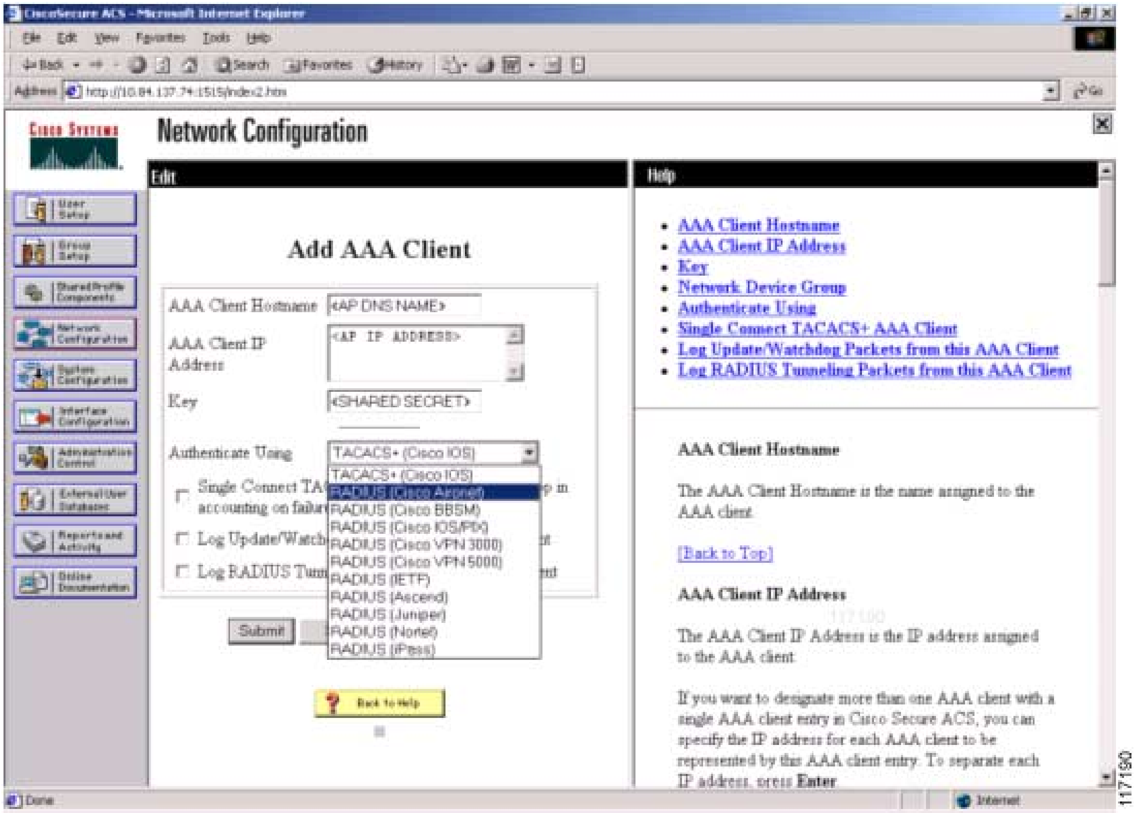
Step 2 Under AAA Clients, click **Add Entry**.

Step 3 Configure the domain name server (DNS) name of the access point, the IP address of the access point, the RADIUS shared secret, and the authentication method as shown in Figure 1.

Note Be sure to choose **RADIUS (Cisco Aironet)** from the Authenticate Using drop-down menu.

Step 4 Click **Submit + Restart** to finish.

Figure 1 Adding an Access Point to the Cisco Secure ACS



Network Configuration

Add AAA Client

AAA Client Hostname <AP DNS NAME>

AAA Client IP Address <AP IP ADDRESS>

Key <SHARED SECRET>

Authenticate Using TACACS+ (Cisco IOS)

□ Single Connect TA... accounting on failur...

□ Log Update/Watch...

□ Log RADIUS Tunn...

- AAA Client Hostname
- AAA Client IP Address
- Key
- Network Device Group
- Authenticate Using
- Single Connect TACACS+ AAA Client
- Log Update/Watchdog Packets from this AAA Client
- Log RADIUS Tunneling Packets from this AAA Client

AAA Client Hostname

The AAA Client Hostname is the name assigned to the AAA client.

[Back to Top]

AAA Client IP Address

The AAA Client IP Address is the IP address assigned to the AAA client.

If you want to designate more than one AAA client with a single AAA client entry in Cisco Secure ACS, you can specify the IP address for each AAA client to be represented by this AAA client entry. To separate each IP address, press **Enter**

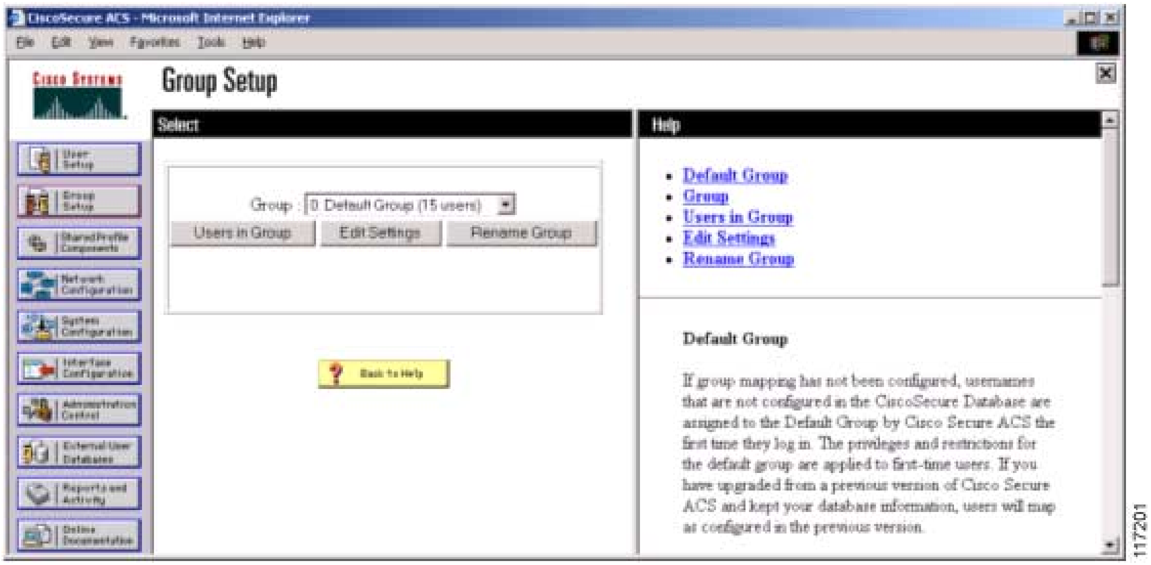
Configuring the Master Encryption Key/Session Timeout

The IEEE 802.1X standard specifies a reauthentication option. The Cisco LEAP algorithm uses this option to expire the current master encryption key for the user and issue a new master key. Although reauthentication is an option, it is disabled by default. This procedure enables the 802.1X WEP master encryption key timeout.

Step 1 On the Cisco Secure ACS main menu, click **Group Setup** (see Figure 2).

Step 2 Choose the group for which the master encryption key/session timeout is to be modified. In most cases, the default group is the one to modify. Click **Edit Settings**.

Figure 2 Cisco Secure ACS Group Setup



Group : 0 Default Group (15 users)

Default Group

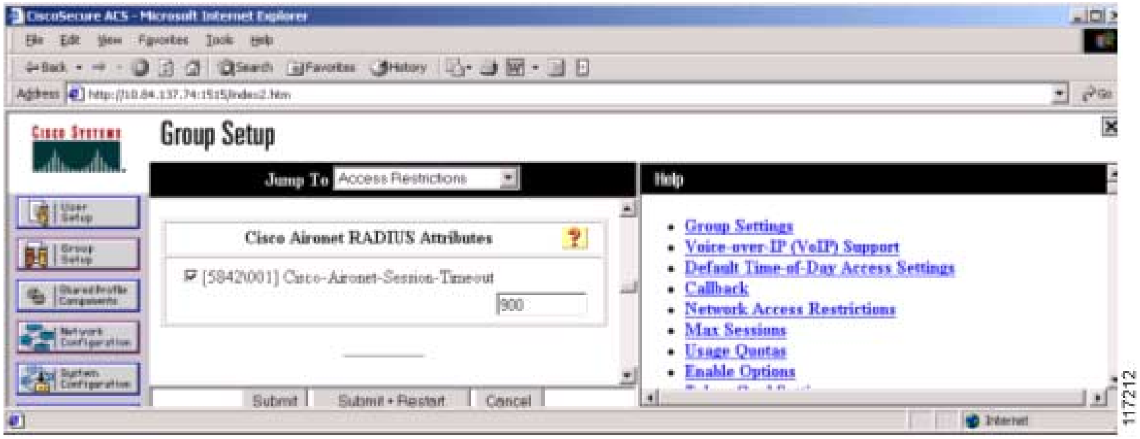
If group mapping has not been configured, usernames that are not configured in the CiscoSecure Database are assigned to the Default Group by Cisco Secure ACS the first time they log in. The privileges and restrictions for the default group are applied to first-time users. If you have upgraded from a previous version of Cisco Secure ACS and kept your database information, users will map as configured in the previous version.

Step 3 Use the Cisco Aironet RADIUS attribute value **[5842\001] Cisco-Aironet-Session-Timeout** to set the master encryption key timeout (see Figure 3). This timeout value is configured in seconds for per-user EAP keys, which should be set depending on the encryption modes used. Refer to the Cisco Wireless Security Suite documentation for guidelines on setting the session key timeout.

http://www.cisco.com/en/US/netsol/ns339/ns395/ns176/ns178/networking_solutions_white_paper09186a00800b469f.shtml

Note You may also set the Cisco Aironet RADIUS attribute for the Cisco Aironet session timeout if the Cisco Secure ACS is configured for per-user TACACS+/RADIUS attributes. This is configured under **Interface Configuration** > **Advanced Options**.

Figure 3 Cisco Aironet RADIUS Session Timeout (Group Setup)



Address: http://10.84.137.74:1515/index2.htm

Jump To: Access Restrictions

Cisco Aironet RADIUS Attributes

☑ [5842\001] Cisco-Aironet-Session-Timeout 900

Note The session timeout may be controlled with the IETF RADIUS Attributes or value **[027] Session Timeout**. This may be useful for non-Cisco access points that do not support Cisco RADIUS Vendor Specific Attributes (VSA). This setting affects all sessions (for example, virtual private network [VPN], dial, and so on) that are authenticated by the Cisco Secure ACS. Make sure that using this parameter will not negatively impact other authentication mechanisms.

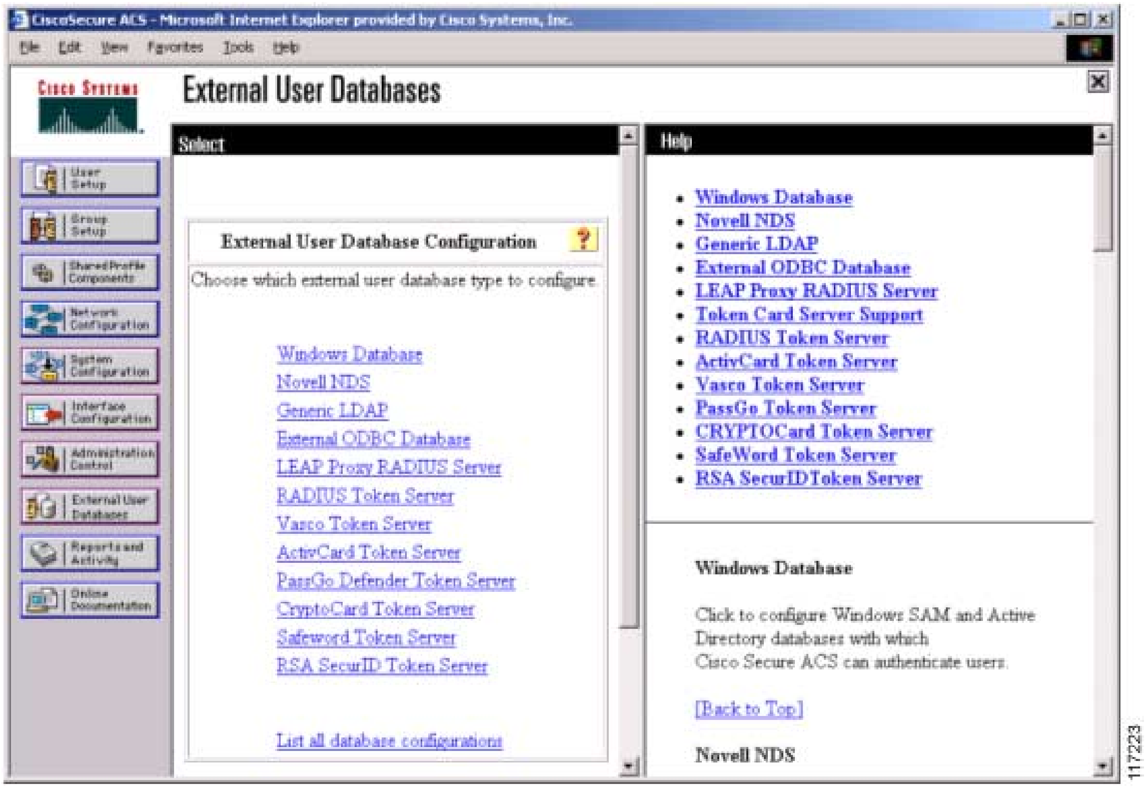
Step 4 Click **Submit + Restart** to finish.

Step 5 To use an external Microsoft database to authenticate users, add the external database to Cisco Secure ACS.

Step 6 Click **External User Databases** and **Database Configuration**.

Step 7 From the External User Database Configuration options list, choose **Windows Database** (see Figure 4).

Figure 4 External User Database Configuration



External User Databases

External User Database Configuration

Choose which external user database type to configure

Windows Database
Novell NDS
Generic LDAP
External ODBC Database
LEAP Proxy RADIUS Server
RADIUS Token Server
Vasco Token Server
ActivCard Token Server
PassGo Defender Token Server
CryptoCard Token Server
Safeword Token Server
RSA SecurID Token Server

List all database configurations

- Windows Database
- Novell NDS
- Generic LDAP
- External ODBC Database
- LEAP Proxy RADIUS Server
- Token Card Server Support
- RADIUS Token Server
- ActivCard Token Server
- Vasco Token Server
- PassGo Token Server
- CRYPTOCard Token Server
- SafeWord Token Server
- RSA SecurIDToken Server

Windows Database

Click to configure Windows SAM and Active Directory databases with which Cisco Secure ACS can authenticate users.

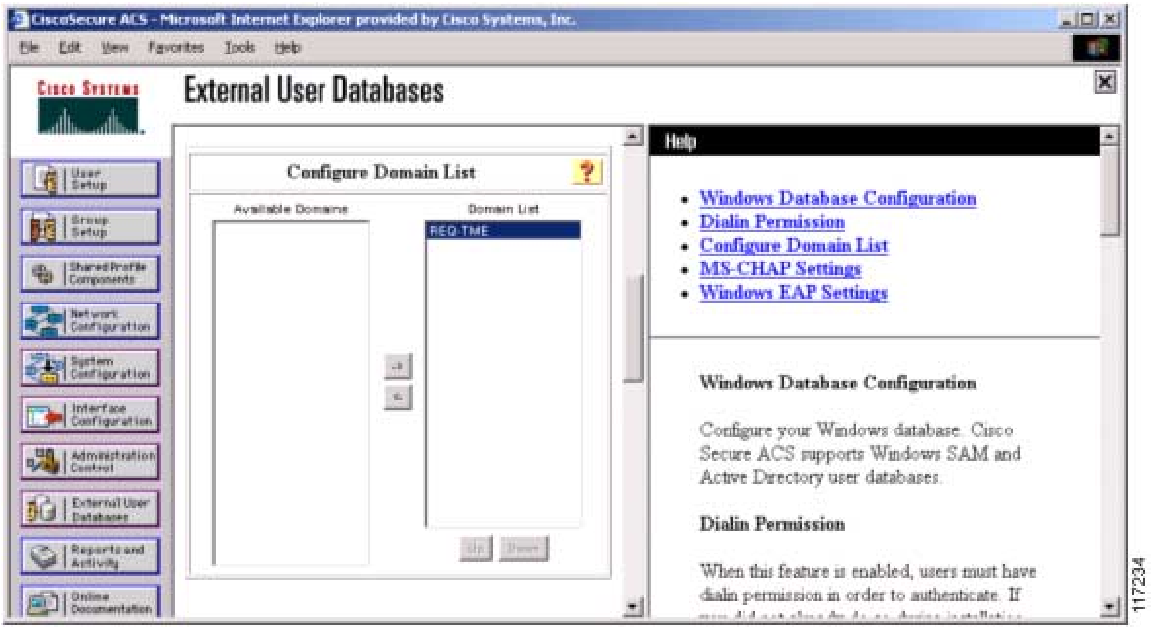
[Back to Top]

Novell NDS

Step 8 On the Edit Database page, click **Configure** to access the Windows User Database Configuration page.

Step 9 Scroll to the Configure Domain List section and choose the appropriate Microsoft domain to check for user authentication (see Figure 5).

Figure 5 Configure Domain for External Windows Database



External User Databases

Configure Domain List

- Windows Database Configuration
- Dialin Permission
- Configure Domain List
- MS-CHAP Settings
- Windows EAP Settings

Windows Database Configuration

Configure your Windows database. Cisco Secure ACS supports Windows SAM and Active Directory user databases.

Dialin Permission

When this feature is enabled, users must have dialin permission in order to authenticate. If

Step 10 Scroll to the bottom of the Windows User Database Configuration page and click **Submit**.

Step 11 An “unknown user policy” must be configured to permit Cisco LEAP authentication requests that are not reconciled on the local Aironet Client Utility (ACU) database to be checked with an external database. To authenticate Cisco LEAP users to the previously configured external Windows database, add the Windows database to the unknown user policy.

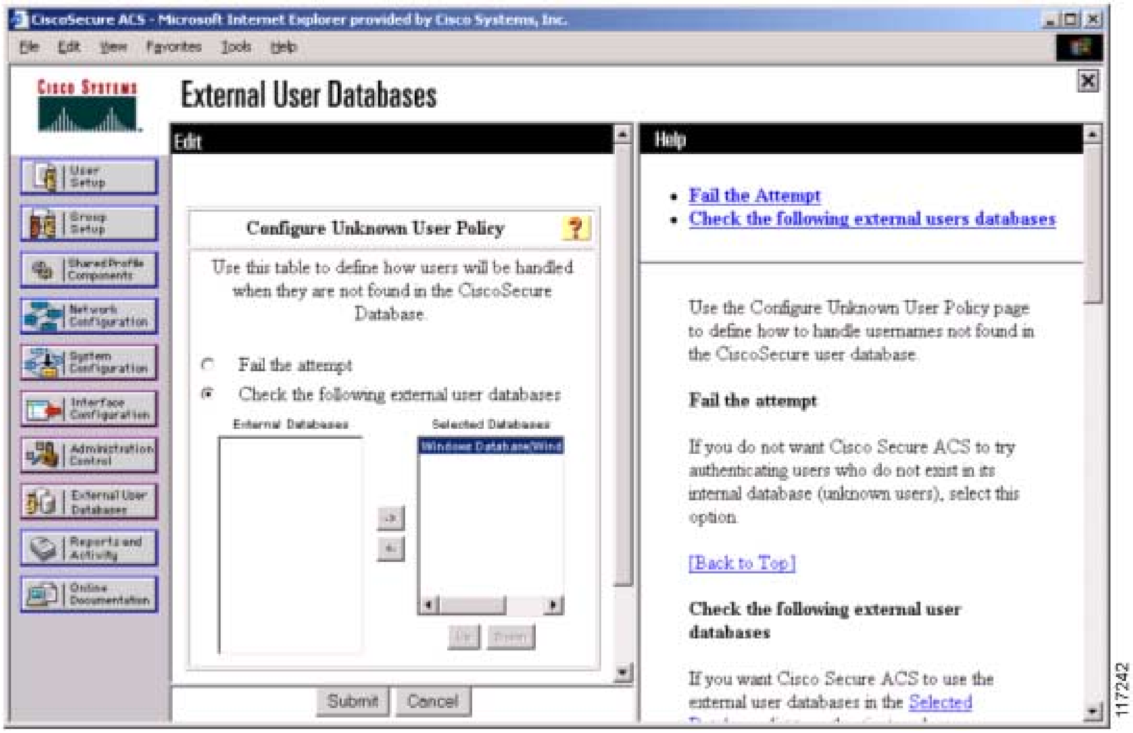
Step 12 Click **External User Databases** again and choose **Unknown User Policy**.

Step 13 On the Configure Unknown User Policy page, choose **Check the following external user databases**.

Step 14 From the External Databases list, add the Windows database to Selected Databases (see Figure 6).

Step 15 Scroll to the bottom of the Configure Unknown User Policy page and click **Submit**.

Figure 6 Configure Unknown User Policy for Windows Database



Configure Unknown User Policy

Use this table to define how users will be handled when they are not found in the CiscoSecure Database.

○ Fail the attempt

● Check the following external user databases

External Databases	Selected Databases
	Windows Database/Wind

- Fail the Attempt
- Check the following external users databases

Use the Configure Unknown User Policy page to define how to handle usernames not found in the CiscoSecure user database.

Fail the attempt

If you do not want Cisco Secure ACS to try authenticating users who do not exist in its internal database (unknown users), select this option.

[Back to Top]

Check the following external user databases

If you want Cisco Secure ACS to use the external user databases in the Selected

Configuring the Access Point for Local/Fallback RADIUS Server Functionality

Starting with Cisco IOS Software Release 12.2(11)JA, the 1100 and 1200 series access points have a feature that enables them to function as local or fallback RADIUS servers. This permits client devices to authenticate and receive dynamic encryption keys, even with failure of a WAN link between the access point and the centralized RADIUS server. The following steps describe how to configure local authentication and establish the local user database in the access point.

Note User Datagram Protocol (UDP) port 1812 is used for authentication messaging to the access point local authenticator (as opposed to the default of port 1645), and as many as 50 users are supported in the access point's local authentication database. The order in which the access point attempts to authenticate a user with the servers in the list matches the order in which the operator entered them in the configuration. For example, the secondary RADIUS server should be entered last, and the primary RADIUS server should be entered first. (From Server Manager, refer to the "Configuring Access Points Running Cisco IOS Software Release 12.2(4)JA or Later for Cisco LEAP" section on page 12.) The local/fallback server is automatically the last server attempted. The Dead RADIUS Server List should be enabled in order to permit reattempting primary server and failover to the local server.

Step 1 Configure the access point for Cisco LEAP authentication by following the steps outlined in the "Configuring Access Points Running Cisco IOS Software Release 12.2(4)JA or Later for Cisco LEAP" section on page 12 or the "Configuring Access Points Running VxWorks Software Release 12.03T or Earlier for Cisco LEAP" section on page 15. If the access point will be used without a centralized RADIUS server, configure the local authentication service first.

Step 2 Browse to the access point.

Step 3 Click **Security**.

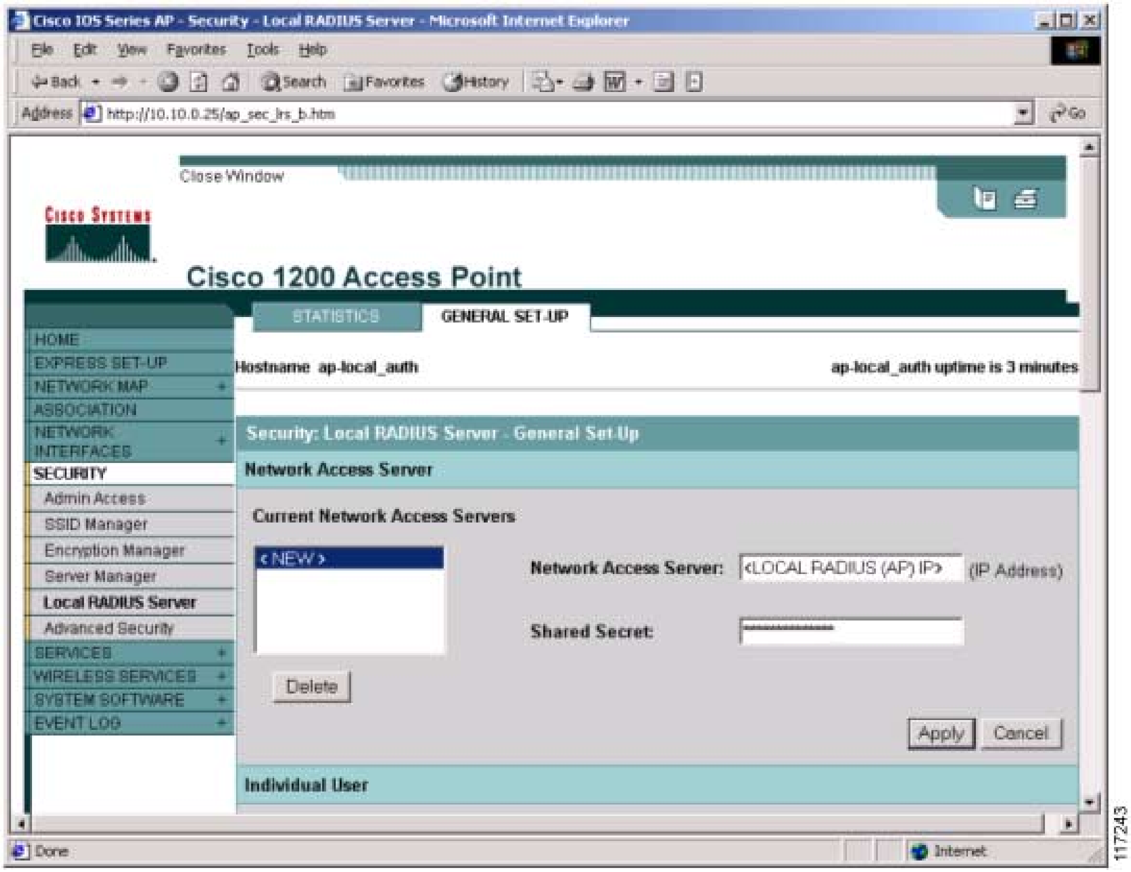
Step 4 From the Security submenu, click **Local RADIUS Server**.

Step 5 Click the **General Set-Up** tab (see Figure 7).

Step 6 Enter the access point's IP address in the Network Access Server field and the desired RADIUS shared secret in the Shared Secret field.

Step 7 Click **Apply** to activate the changes.

Figure 7 Local RADIUS Server Configuration - General Setup



Cisco IOS Series AP - Security - Local RADIUS Server - Microsoft Internet Explorer

Address http://10.10.0.25/ap_sec_lrs_b.htm

Cisco 1200 Access Point

Hostname ap-local_auth

ap-local_auth uptime is 3 minutes

Security: Local RADIUS Server - General Set-Up

Network Access Server

Current Network Access Servers

< NEW >

Network Access Server: <LOCAL RADIUS (AP) IP> (IP Address)

Shared Secret: ***********

Individual User

These CLI commands approximate the GUI steps above:

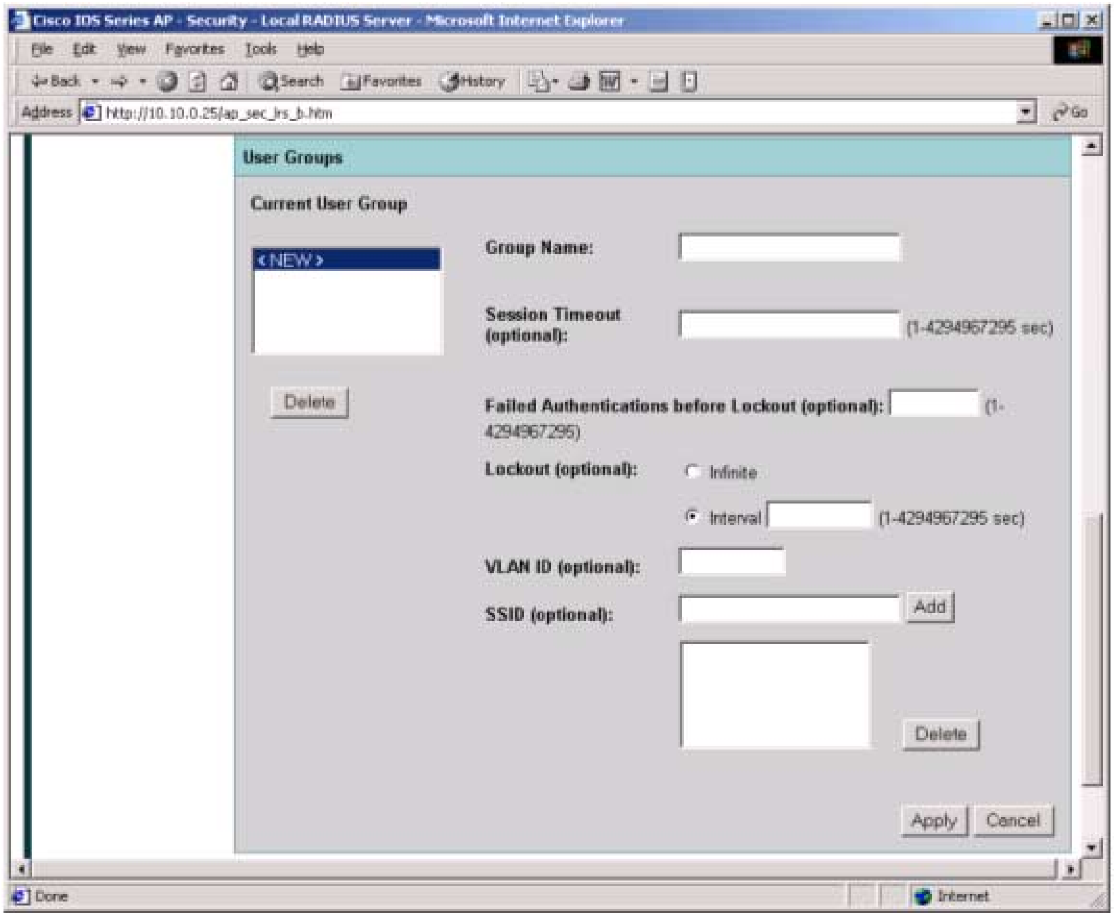
```
ap(config)# radius local
ap(config-rad-svr)# nas <ip address of NAS>
```

Step 8 RADIUS user groups may be configured to permit differentiation between groups for different access requirements. Add a new group in the Group Name field under the User Groups section of the General Set-Up page (see Figure 8).

Step 9 If necessary, configure the session timeout, failed authentication attempts, lockout timer, assigned virtual LAN (VLAN), and assigned service set identifier (SSID) RADIUS parameters for each user group.

Step 10 Click **Apply** to activate the changes and create the user group.

Figure 8 RADIUS User Group Configuration


Cisco IOS Series AP - Security - Local RADIUS Server - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address
Go
Done
Internet
117244

Address: http://10.10.0.25/ap_sec_lrs_b.htm

User Groups

Current User Group

<NEW>

Delete

Group Name:

Session Timeout (optional): (1-4294967295 sec)

Failed Authentications before Lockout (optional): (1-4294967295)

Lockout (optional): ○ Infinite

● Interval (1-4294967295 sec)

VLAN ID (optional):

SSID (optional): Add

Delete

Apply Cancel

These CLI commands approximate the GUI steps above:

```
ap(config-rad-svr)# group <groupname>

ap(config-rad-svr-group)# ssid <allowed SSID>

ap(config-rad-svr-group)# vlan <allowed vlan id>

ap(config-rad-svr-group)# reauthentication time <session timer>

ap(config-rad-svr-group)# block count <number attempts> time <lockout time>
```

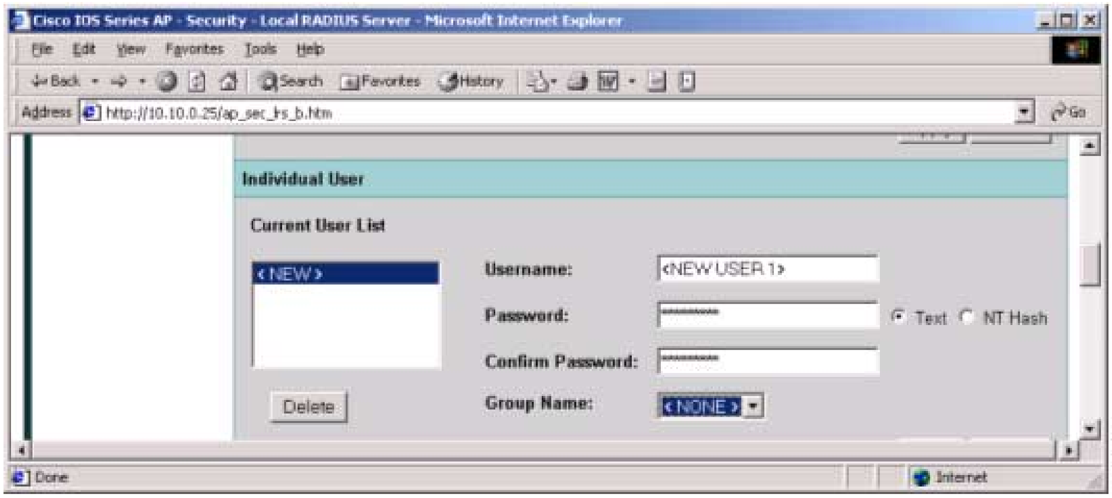
Step 11 Enter the user credentials for local authentication under the Individual User section of the Local RADIUS Server page (see Figure 9).

Step 12 Enter the Cisco LEAP username in the Username field. Spaces are not permitted.

Step 13 Enter the Cisco LEAP user password (up to 32 characters) in the Password field. You may enter the password in text (displayed as NT hash after entry) or directly as NT hash (see Figure 9).

Step 14 Click **Apply** to activate the changes and create a user in the local database.

Figure 9 Individual RADIUS User Configuration



Cisco IOS Series AP - Security - Local RADIUS Server - Microsoft Internet Explorer

Address http://10.10.0.25/ap_sec_ls_b.htm

Individual User

Current User List

< NEW >

Username: <NEW USER 1>

Password: ********** ● Text ○ NT Hash

Confirm Password: **********

Group Name: < NONE >

This CLI command approximates the GUI steps above:

```
ap(config-rad-svr)# user <username> password <pass> group <groupname>
```

Configuring Access Points Running Cisco IOS Software Release 12.2(4)JA or Later for Cisco LEAP

Step 1 Browse to the access point.

Step 2 Click **Security**.

Step 3 From the Security submenu, click **Server Manager**.

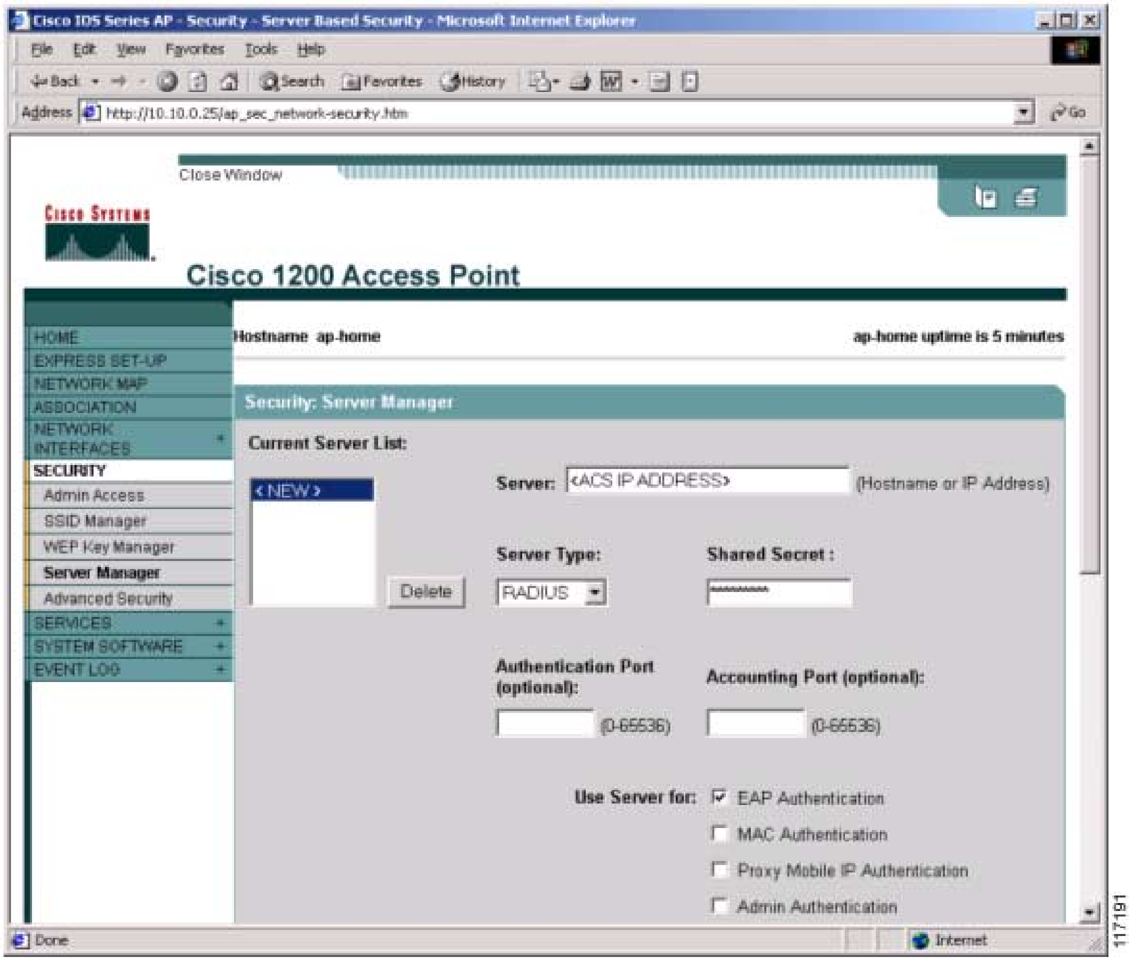
Step 4 Configure the IP address of the Cisco Secure ACS in the Server field.

Step 5 Choose **RADIUS** from the Server Type drop-down box and enter the shared secret in the Shared Secret field (see Figure 10).

Step 6 Check the **EAP Authentication** check box and specify an authentication port if you are not using the default value (1645).

Step 7 Click **Apply** to save the server configuration settings.

Figure 10 Server Manager Configuration for Cisco IOS Software Release 12.2(4)JA or Later



Cisco IOS Series AP - Security - Server Based Security - Microsoft Internet Explorer

Address http://10.10.0.25/ap_sec_network-security.htm

Cisco 1200 Access Point

Hostname ap-home

ap-home uptime is 5 minutes

Security: Server Manager

Current Server List:

Server: <ACS IP ADDRESS> (Hostname or IP Address)

Server Type: RADIUS

Shared Secret : *********

Authentication Port (optional): (0-65536)

Accounting Port (optional): (0-65536)

Use Server for:

☑ EAP Authentication

□ MAC Authentication

□ Proxy Mobile IP Authentication

□ Admin Authentication

These CLI commands approximate the GUI steps above:

```
ap(config)# radius-server host <ip address> auth-port 1645 acct-port 1646 key <shared secret>

ap(config)# radius-server retransmit <number retries>

ap(config)# radius-server timeout <seconds>

ap(config)# aaa group server radius <server groupname for EAP>

ap(config-sg-radius)# server <ip address> auth-port 1645 acct-port 1646

ap(config-sg-radius)# deadtime <minutes>

ap(config)# aaa authentication login <auth list for EAP> group <server groupname>
```

Step 8 In the Global Server Properties section of the Server Manager page, configure the non-default RADIUS Server Timeout (the default is 5 seconds), RADIUS Server Retransmit Retries (the default is three attempts), and Dead RADIUS Server List (the default is Disabled). The Dead RADIUS Server function controls the period of time that the access point stays on a secondary or backup before attempting to again authenticate users with the primary server.

> **Note** If the Dead RADIUS Server List is not enabled, all authentication attempts to the primary server must time out before the access point tries authentication with the backup server. Therefore, the Dead RADIUS Server List should be enabled for all deployments of backup RADIUS servers.

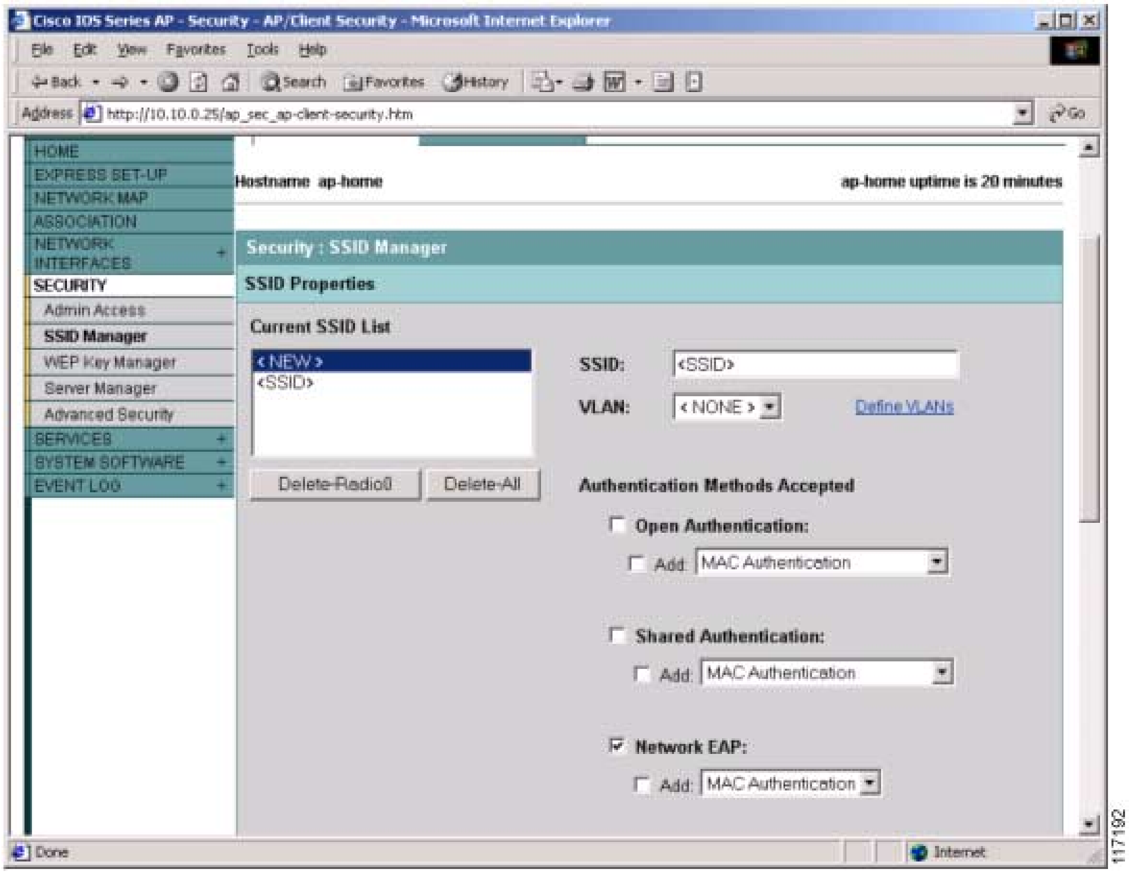
Step 9 Choose **SSID Manager** from the Security submenu.

Step 10 Choose **SSID** from the Current SSID List (see Figure 11) to configure Cisco LEAP for the active SSID.

Step 11 Check the **Network EAP** check box. If you are using non-Cisco client cards, specify **Open Authentication**, check the **Add** check box, and specify **EAP Authentication** in the drop-down box.

Step 12 Click **Apply** to activate changes to the appropriate radio interface (Radio0 for an internal radio, Radio1 for a modular radio).

Figure 11 SSID Manager Configuration for Cisco IOS Software Release 12.2(4)JA or Later



Address: http://10.10.0.25/ap_sec_ap-client-security.htm

Hostname ap-home   ap-home uptime is 20 minutes

Security : SSID Manager

SSID Properties

Current SSID List: < NEW >, <SSID>

SSID: <SSID>

VLAN: < NONE >

Authentication Methods Accepted

□ Open Authentication:
□ Add: MAC Authentication

□ Shared Authentication:
□ Add: MAC Authentication

☑ Network EAP:
□ Add: MAC Authentication

This CLI command approximates the GUI steps above:

```
ap(config-if-ssid)# authentication network-eap <auth list>
```

Step 13 Choose **WEP Key Manager** from the Security submenu.

Step 14 Choose **Optional** or **Mandatory** encryption from the WEP Encryption drop-down box under the Encryption Modes section. Choosing Optional encryption permits non-WEP clients to associate to the access point.

Step 15 Click **Apply** to activate changes for the appropriate radio interface.

Step 16 Choose **Advanced Security** from the Security submenu.

Step 17 Click the **Timers** tab.

Step 18 Under Global Client Properties, set the *client holdoff time*, the period of time that a client is disabled from reauthenticating after unsuccessful EAP retries. In addition, you can configure client EAP settings for (re)authentication and the EAP request interval. The EAP reauthentication interval setting enables the access point to force client reauthentication at a specified interval if not specified by the RADIUS server. The EAP client timeout controls the amount of time that the access point waits for an EAP response from the client before considering an EAP request failed.

These CLI commands approximate the GUI steps above:

```
ap(config-if)# encryption mode wep mandatory (or optional)

ap(config-if)# dot1x client-timeout (seconds that AP waits for client EAP response)

ap(config-if)# dot1x reauth-period (seconds, reauth interval)

ap(config)# dot11 holdoff-time (seconds, client lockout after unsuccessful EAP)
```

Configuring Access Points Running VxWorks Software Release 12.03T or Earlier for Cisco LEAP

Step 1 Browse to the access point or wireless bridge.

Step 2 From the Summary Status page, click **Setup**.

Step 3 From the Services menu, click **Security**.

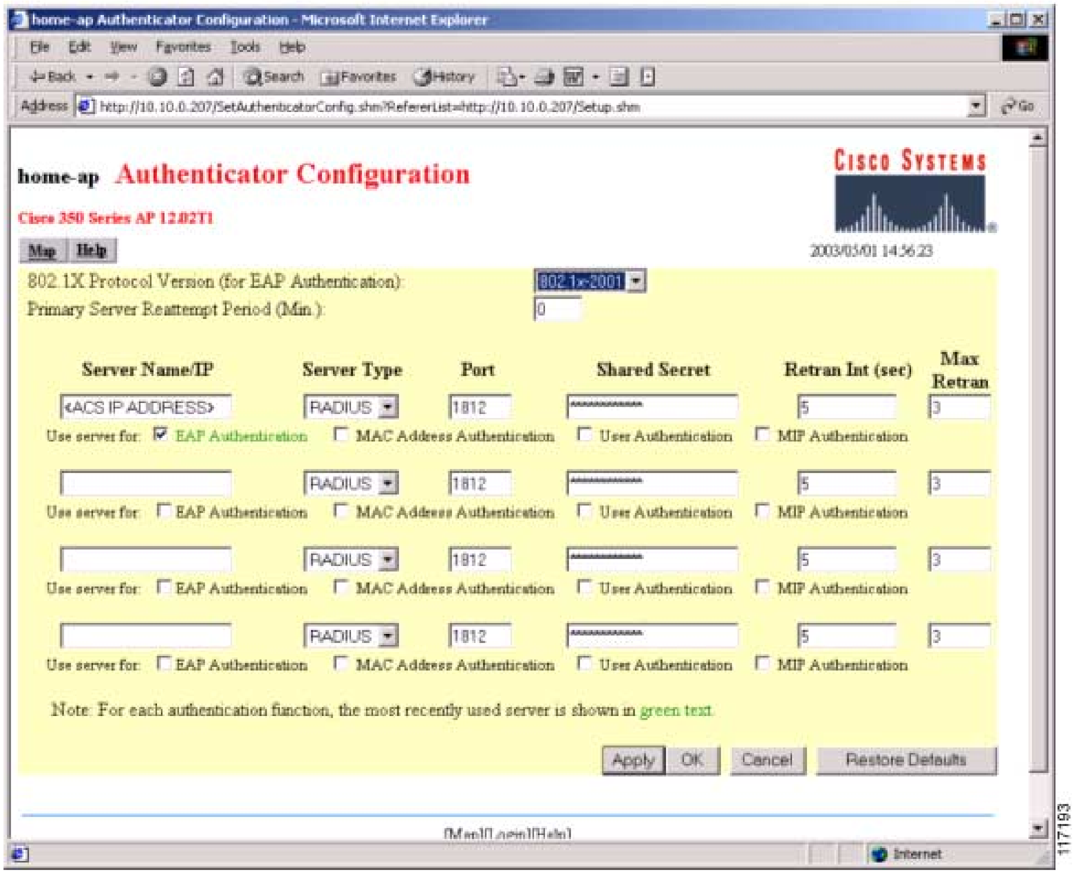
Step 4 Click **Authentication Server**.

Step 5 From the 802.1X Protocol Version drop-down box, select the version of 802.1X to run on this access point (see Figure 12). Note that IEEE 802.1X Draft 7 is no longer supported.

Note All clients using Cisco LEAP with these access points must be Draft 8 (4.25.x or earlier) to function with Draft 8 firmware on access points running VxWorks software (11.06 or earlier).

Figure 12 RADIUS Server Configuration for VxWorks Access Points

s


home-ap Authenticator Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address Go
CISCO SYSTEMS
Map Help
Apply OK Cancel Restore Defaults
[Map][Login][Help]
Internet
117193

Address: http://10.10.0.207/SetAuthenticatorConfig.shm?RefererList=http://10.10.0.207/Setup.shm

home-ap **Authenticator Configuration**

Cisco 350 Series AP 12.02T1

2003/03/01 14:56:23

802.1X Protocol Version (for EAP Authentication): 802.1x-2001

Primary Server Reattempt Period (Min.): 0

Server Name/IP	Server Type	Port	Shared Secret	Retran Int (sec)	Max Retran
<ACS IP ADDRESS>	RADIUS	1812	************	5	3
Use server for: ☑ EAP Authentication	☐ MAC Address Authentication		☐ User Authentication	☐ MIP Authentication	
	RADIUS	1812	************	5	3
Use server for: ☐ EAP Authentication	☐ MAC Address Authentication		☐ User Authentication	☐ MIP Authentication	
	RADIUS	1812	************	5	3
Use server for: ☐ EAP Authentication	☐ MAC Address Authentication		☐ User Authentication	☐ MIP Authentication	
	RADIUS	1812	************	5	3
Use server for: ☐ EAP Authentication	☐ MAC Address Authentication		☐ User Authentication	☐ MIP Authentication	

Note: For each authentication function, the most recently used server is shown in green text.

Step 6 Configure the IP address of the Cisco Secure ACS in the Server Name/IP field.

Step 7 Make sure that the Server Type drop-down box is set to **RADIUS**.

Step 8 Change the Port field to **1645**. This is the correct IP port number to use with the Cisco Secure ACS.

Step 9 Configure the Shared Secret field with the value configured on the Cisco Secure ACS.

Step 10 Check the **EAP Authentication** check box.

Step 11 Modify the Retran Int (retransmission interval) and Max Retran (maximum number of retransmissions) fields if desired. These are the interval and number of attempts for which authentication requests are sent by the access point to the Cisco Secure ACS. If the Cisco Secure ACS in use exceeds this value, the access point will attempt to communicate with the next configured Cisco Secure ACS in sequence. As shown in Figure 12, the access point supports up to four RADIUS servers or Cisco Secure ACSs.

Step 12 If necessary, set the Primary Server Reattempt Period to the interval upon which the access point will reattempt to authenticate using the primary (first listed AAA) server.

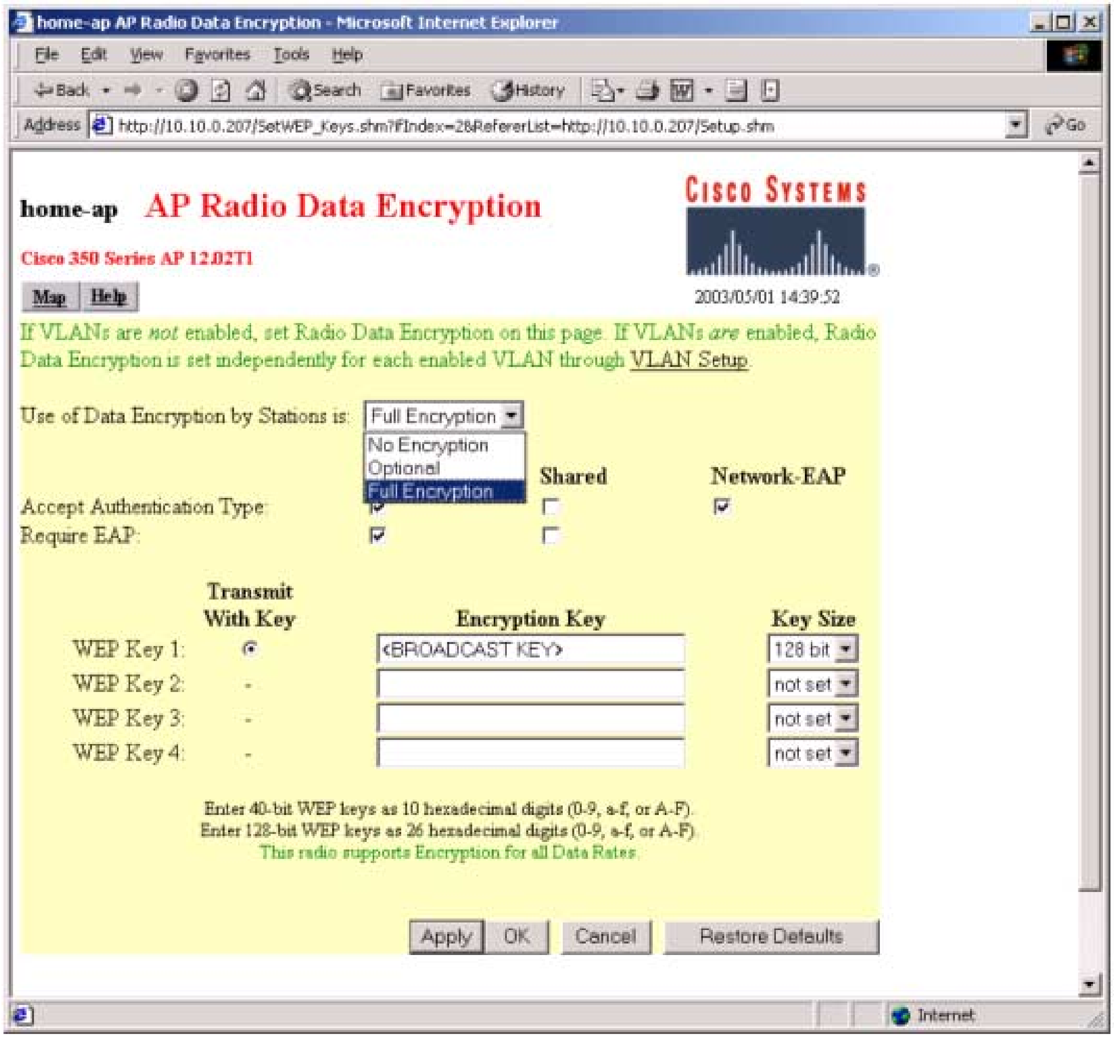
Step 13 Click **OK** when finished.

Step 14 The access point GUI returns to the Security Set-Up page.

Step 15 Click **Radio Data Encryption (WEP)**.

Step 16 Configure a WEP key by entering a 40- or 128-bit key value in the WEP Key 1 field (see Figure 13). This key is used as the broadcast WEP key if specified.

Figure 13 Encryption Configuration for VxWorks Access Points


home-ap AP Radio Data Encryption - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address
Go
Cisco Systems
Map Help
Apply OK Cancel Restore Defaults
Internet
117194

Address: http://10.10.0.207/SetWEP_Keys.shm?IFIndex=2&RefererList=http://10.10.0.207/Setup.shm

home-ap AP Radio Data Encryption

Cisco 350 Series AP 12.02T1

2003/05/01 14:39:52

If VLANs are *not* enabled, set Radio Data Encryption on this page. If VLANs *are* enabled, Radio Data Encryption is set independently for each enabled VLAN through VLAN Setup.

Use of Data Encryption by Stations is: Full Encryption (No Encryption / Optional / Full Encryption)

		Shared	Network-EAP
Accept Authentication Type:	☑	☐	☑
Require EAP:	☑	☐	

	Transmit With Key	Encryption Key	Key Size
WEP Key 1:	●	<BROADCAST KEY>	128 bit
WEP Key 2:	-		not set
WEP Key 3:	-		not set
WEP Key 4:	-		not set

Enter 40-bit WEP keys as 10 hexadecimal digits (0-9, a-f, or A-F).
Enter 128-bit WEP keys as 26 hexadecimal digits (0-9, a-f, or A-F).
This radio supports Encryption for all Data Rates.

Step 17 If only dynamic WEP client devices use this device, configure the access point for broadcast key rotation, which generates a dynamic broadcast key. See the "Configuring a Root Bridge or Access Point Running VxWorks for Cisco TKIP Enhancements" section on page 49.

Step 18 Choose the authentication types to use. Check the **Network-EAP**, **Open**, and **Require EAP** check boxes if applicable.

Step 19 Make sure that the Use of Data Encryption by Stations drop-down box is set to **Optional** or **Full Encryption**. Optional allows the simultaneous use of non-WEP and WEP clients on the same access point. Using non-WEP and WEP clients on the same access point may compromise the security of the access point because this configuration allows unencrypted client associations to the access point. Use Full Encryption if possible.

Step 20 Click **OK** to finish.

Configuring Cisco LEAP Clients

Configuring Windows Clients for Cisco LEAP

Step 1 Open Aironet Client Utility version 6.2.

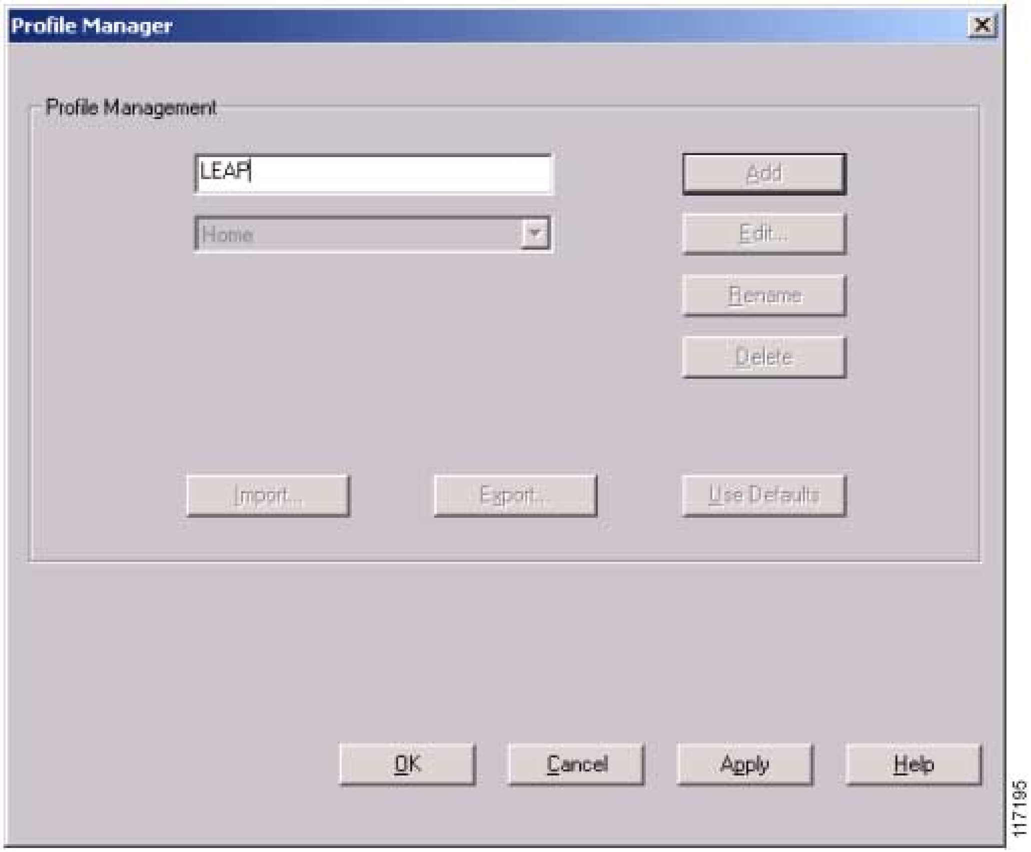
Note Refer to Appendix A: Verifying the Firmware and Driver Versions for client requirements.

Step 2 Choose **Profile Manager** from the Commands drop-down menu or click the **Profile Manager** icon.

Step 3 Click **Add** and enter a name for the profile (see Figure 14).

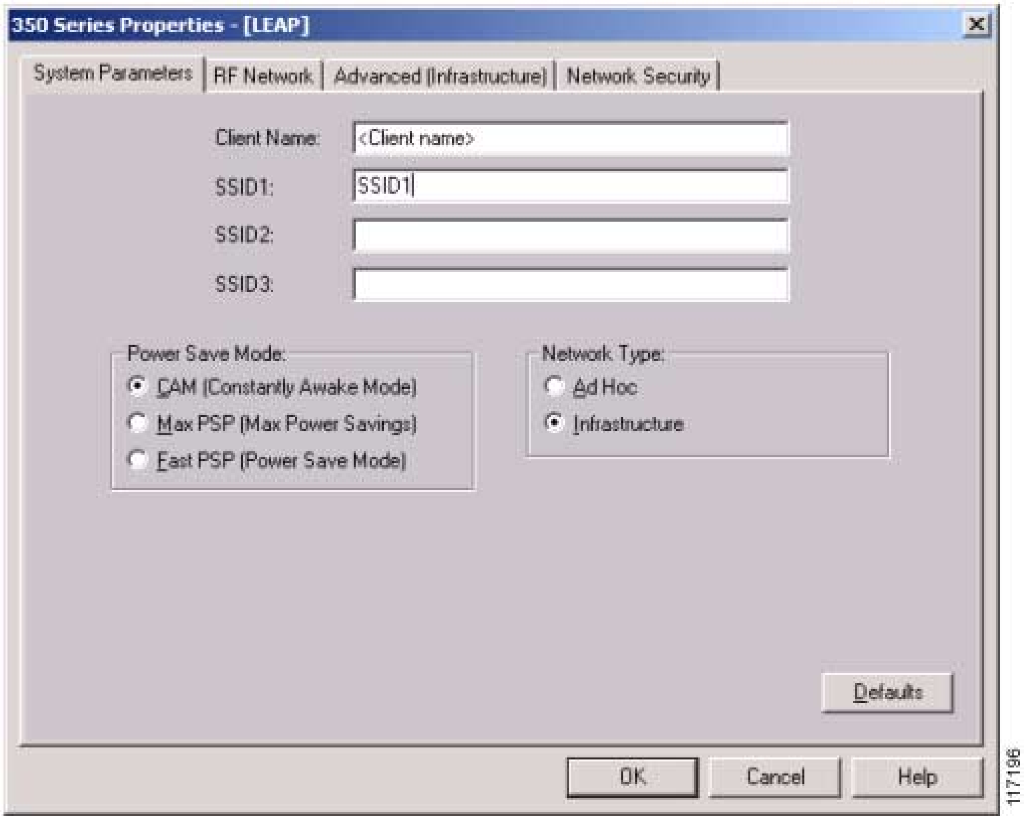
Step 4 Click **Apply**.

Figure 14 Profile Management for Aironet Client Utility Version 6.2



Step 5 On the Profile Properties screen, configure the client name, SSIDs, and power save mode and set the network type to **Infrastructure** (see Figure 15).

Figure 15 System Parameters for Aironet Client Utility Profile



350 Series Properties - [LEAP]

System Parameters | RF Network | Advanced (Infrastructure) | Network Security

Client Name: <Client name>

SSID1: SSID1

SSID2:

SSID3:

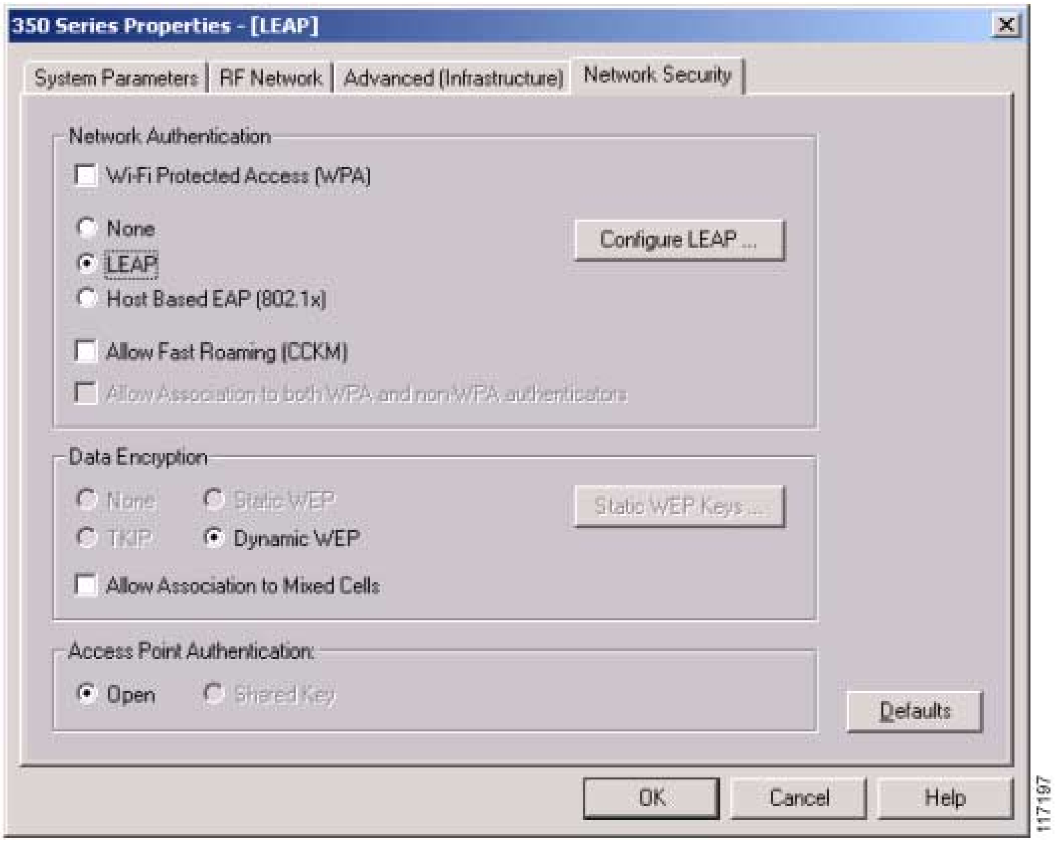
Power Save Mode:
● CAM (Constantly Awake Mode)
○ Max PSP (Max Power Savings)
○ Fast PSP (Power Save Mode)

Network Type:
○ Ad Hoc
● Infrastructure

Step 6 Configure the radio frequency (RF) Network and Advanced settings as necessary for the WLAN network and the device.

Step 7 Click the **Network Security** tab (see Figure 16).

Figure 16 Security Configuration for Aironet Client Utility Profile



350 Series Properties - [LEAP]

Network Authentication

□ Wi-Fi Protected Access (WPA)

○ None
● LEAP
○ Host Based EAP (802.1x)

□ Allow Fast Roaming (CCKM)
□ Allow Association to both WPA and non-WPA authenticators

Data Encryption

○ None ○ Static WEP
○ TKIP ● Dynamic WEP

□ Allow Association to Mixed Cells

Access Point Authentication:

● Open ○ Shared Key

Step 8 Choose **LEAP**.

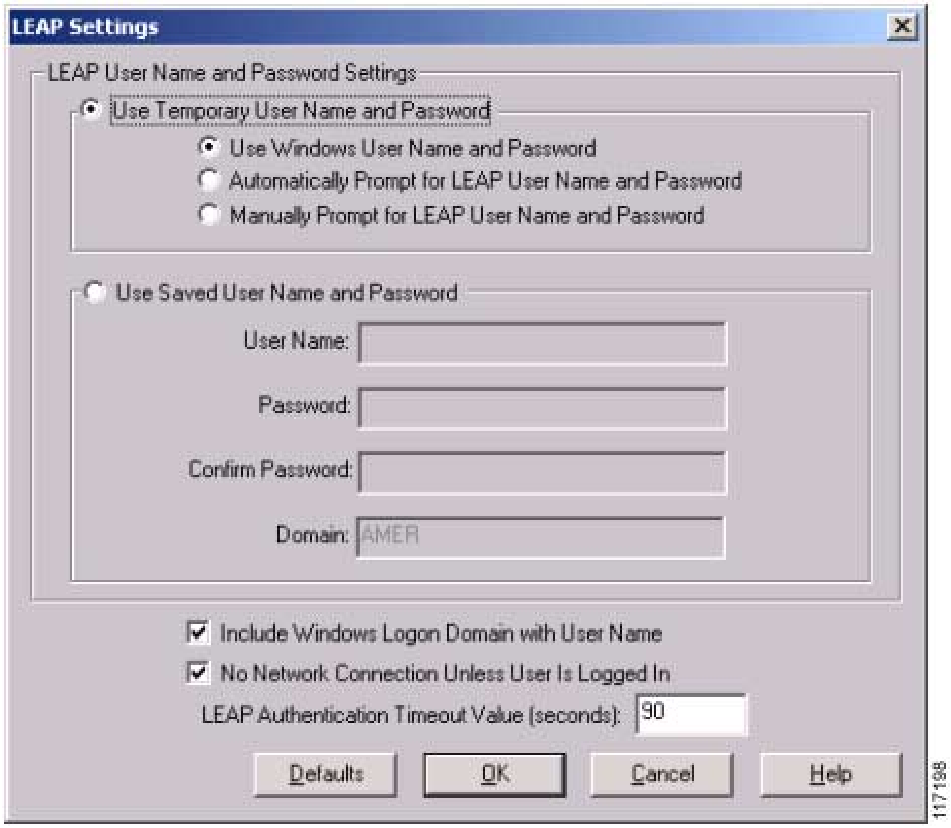
Note **Dynamic WEP** under Data Encryption is enabled by default when you choose LEAP.

Step 9 If applicable, check the **Wi-Fi Protected Access (WPA)** and **Allow Fast Roaming (CCKM)** check boxes.

Note Refer to the "Configuring Wi-Fi Protected Access (WPA) Security" section on page 54 and the "Configuring Cisco Centralized Key Management for Fast Secure Roaming" section on page 51.

Step 10 Click **Configure LEAP**. The LEAP Setting screen appears (see Figure 17).

Figure 17 LEAP Settings Screen



LEAP Settings

LEAP User Name and Password Settings

● Use Temporary User Name and Password

● Use Windows User Name and Password

○ Automatically Prompt for LEAP User Name and Password

○ Manually Prompt for LEAP User Name and Password

○ Use Saved User Name and Password

User Name:

Password:

Confirm Password:

Domain: AMER

☑ Include Windows Logon Domain with User Name

☑ No Network Connection Unless User Is Logged In

LEAP Authentication Timeout Value (seconds): 90

Step 11 Choose the desired user prompt mode for the Cisco LEAP authentication process (Windows credentials, automatic prompt, or manual prompt).

Note The Use Saved User Name and Password mode is not required for transparent reauthentication.

Step 12 Check the **Include Windows Logon Domain with User Name** check box if single sign-on to a Microsoft domain is desired.

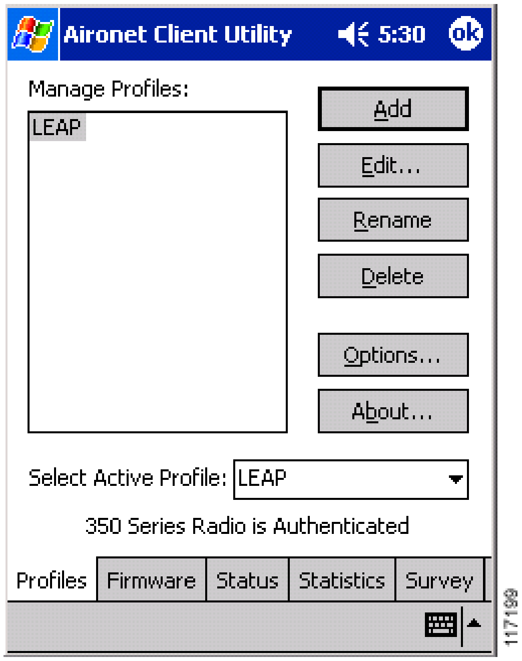
Step 13 Make sure that the **No Network Connection Unless User Is Logged In** check box is checked in order to automatically disassociate a client when a user logs off to prevent other users on a shared machine from using someone else’s credentials.

Step 14 Configure the LEAP Authentication Timeout Value to extend the time permitted to authenticate the user to a domain controller. (The default is 90 seconds; the minimum is 10 seconds.)

Configuring Windows CE Clients for Cisco LEAP

Step 1 Launch Aironet Client Utility version 2.3 on the Windows CE device (see Figure 18).

Figure 18 Windows CE Aironet Client Utility Version 2.3



Manage Profiles: LEAP

Select Active Profile: LEAP

350 Series Radio is Authenticated

Step 2 Click **Add** to add a profile.

Step 3 Tap **Edit** to access profile properties.

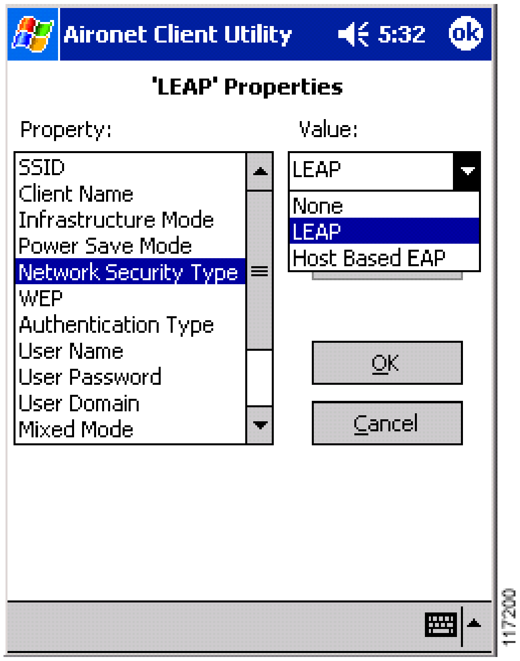
Step 4 Choose **Network Security Type** from the Property box.

Step 5 Choose **LEAP** from the Value drop-down box (see Figure 19).

Step 6 Tap **OK**.

Step 7 To enable your client adapter to automatically connect to a Cisco LEAP network upon card insertion or device resume, enter your username, password, and optional domain name in the User Name, User Password, and User Domain fields.

Figure 19 Profile Configuration for Windows CE Aironet Client Utility Version 2.3



Configuring a Repeater Access Point for Cisco LEAP

Configure an access point repeater for Cisco LEAP in the same manner as you would a root access point, as detailed in the "Configuring Access Points Running Cisco IOS Software Release 12.2(4)JA or Later for Cisco LEAP" section on page 12. Then perform the following additional steps.

Configuring Access Points Running Cisco IOS Software Release 12.2(4)JA or Later for Cisco LEAP

Step 1 Browse to the access point repeater.

Step 2 Click **Security**.

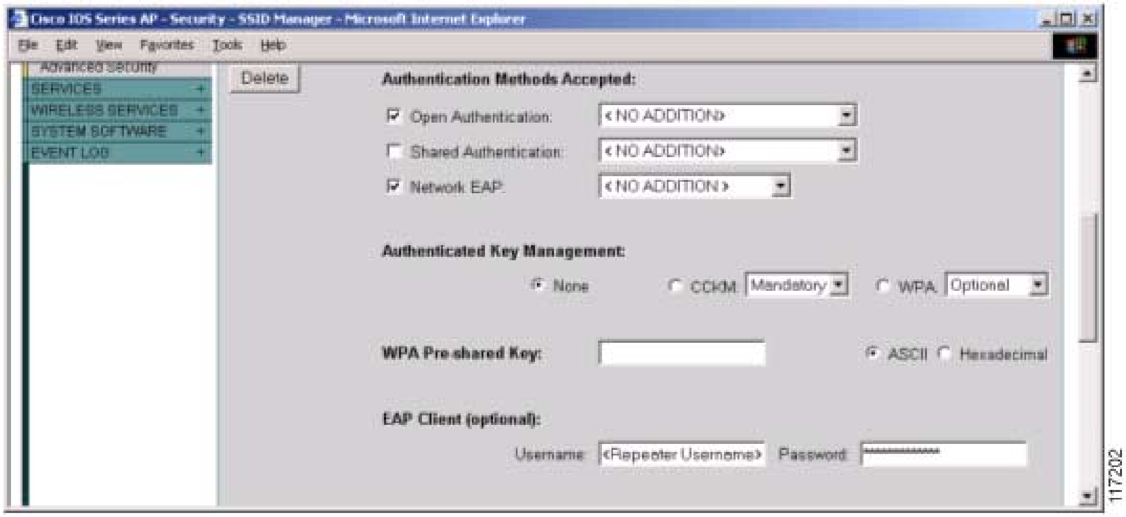
Step 3 From the Security submenu, click **SSID Manager** to access the authentication options.

Step 4 Make sure that the access point is configured for Network EAP authentication.

Step 5 Under EAP Client, configure the Username and Password to be used by the repeater in Cisco LEAP authentication to the root access point (see Figure 20).

Step 6 Click **Apply** to activate the changes.

Figure 20 IOS Repeater Access Point Configured as EAP Client


Cisco IOS Series AP - Security - SSID Manager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Advanced Security
SERVICES +
WIRELESS SERVICES +
SYSTEM SOFTWARE +
EVENT LOG +
Delete
117202

Authentication Methods Accepted:

☑ Open Authentication: < NO ADDITION>

□ Shared Authentication: < NO ADDITION>

☑ Network EAP: < NO ADDITION >

Authenticated Key Management:

● None ○ CCKM Mandatory ○ WPA Optional

WPA Pre-shared Key: ● ASCII ○ Hexadecimal

EAP Client (optional):

Username: <Repeater Username> Password: **************

This CLI command approximates the GUI steps above:

```
ap(config-if-ssid)# authentication client username <user> password <pass>
```

Configuring Access Points Running VxWorks Software Release 12.03T or Earlier for Cisco LEAP

Step 1 Browse to the access point or wireless bridge.

Step 2 Click **Setup**.

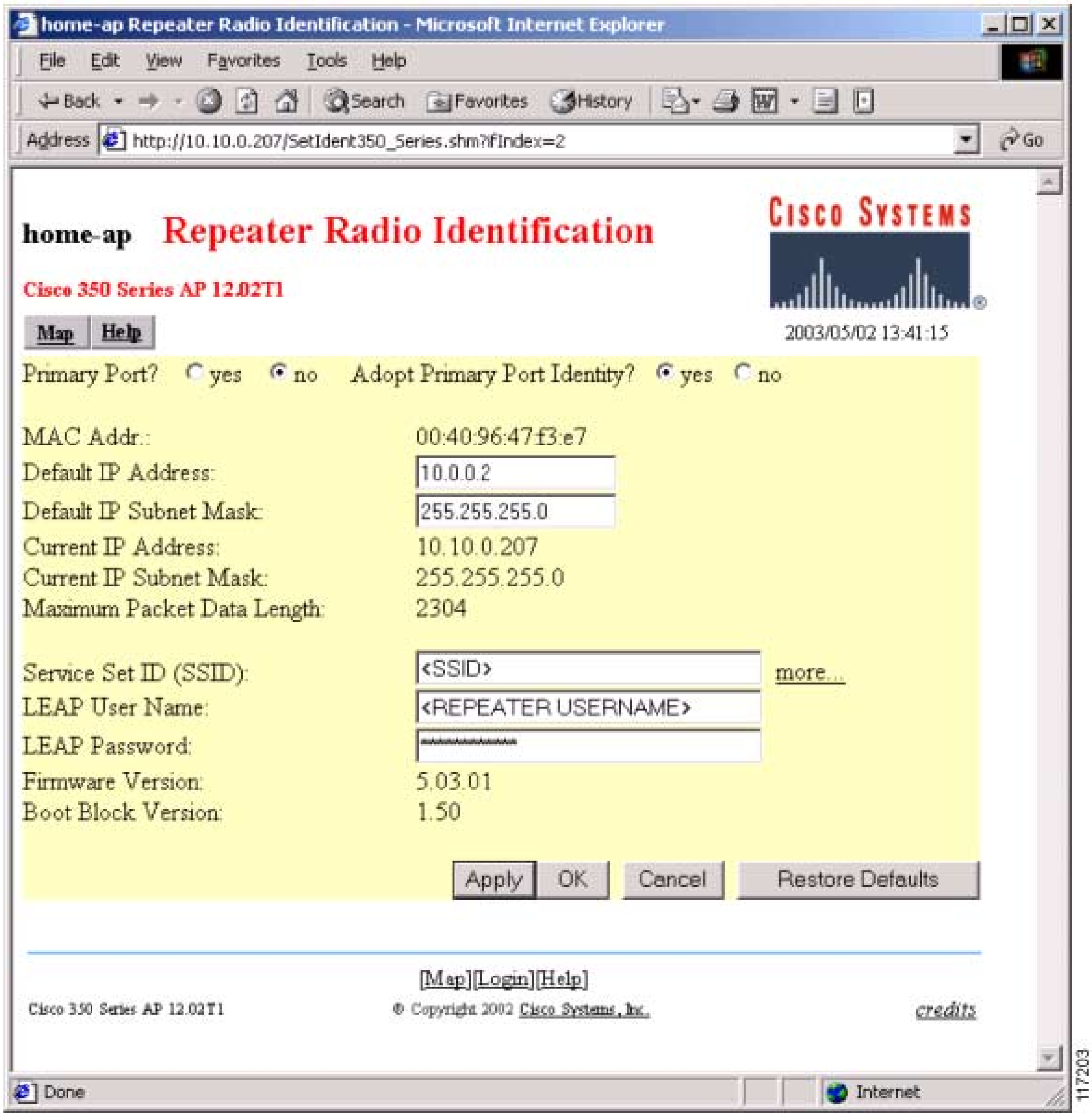
Step 3 Under Repeater Radio > Network Ports, choose **Identification**.

Step 4 Enter the correct Cisco LEAP username and password (see Figure 21).

Step 5 Click **OK**.

Note It is also possible to configure the repeater access point to serve as a network access server (NAS) or as an 802.1X EAP authenticator to clients or other repeaters. The repeater must be configured in the Cisco Secure ACS as a AAA client and must have the Cisco Secure ACS defined in its security configuration, as with a root access point.

Figure 21 VxWorks Repeater Access Point Configured as EAP Client



home-ap Repeater Radio Identification - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://10.10.0.207/SetIdent350_Series.shm?ifIndex=2
Go
Map Help
more...
Apply OK Cancel Restore Defaults
[Map][Login][Help]
credits
Done
Internet
117203

home-ap Repeater Radio Identification

Cisco 350 Series AP 12.02T1

2003/05/02 13:41:15

Primary Port? ○ yes ● no Adopt Primary Port Identity? ● yes ○ no

MAC Addr.:	00:40:96:47:f3:e7
Default IP Address:	10.0.0.2
Default IP Subnet Mask:	255.255.255.0
Current IP Address:	10.10.0.207
Current IP Subnet Mask:	255.255.255.0
Maximum Packet Data Length:	2304
Service Set ID (SSID):	<SSID>
LEAP User Name:	<REPEATER USERNAME>
LEAP Password:	************
Firmware Version:	5.03.01
Boot Block Version:	1.50

Cisco 350 Series AP 12.02T1 © Copyright 2002 Cisco Systems, Inc.

Configuring a Non-Root Cisco Aironet 350 Series Wireless Bridge for Cisco LEAP

Configure a non-root wireless bridge for Cisco LEAP in the same manner as you would a root bridge, as detailed in the "Configuring Access Points Running VxWorks Software Release 12.03T or Earlier for Cisco LEAP" section on page 15. Then perform the following additional steps.

Note Refer to the "Configuring Cisco LEAP" section on page 4 for additional guidance on Cisco LEAP configuration.

Step 1 Browse to the wireless bridge.

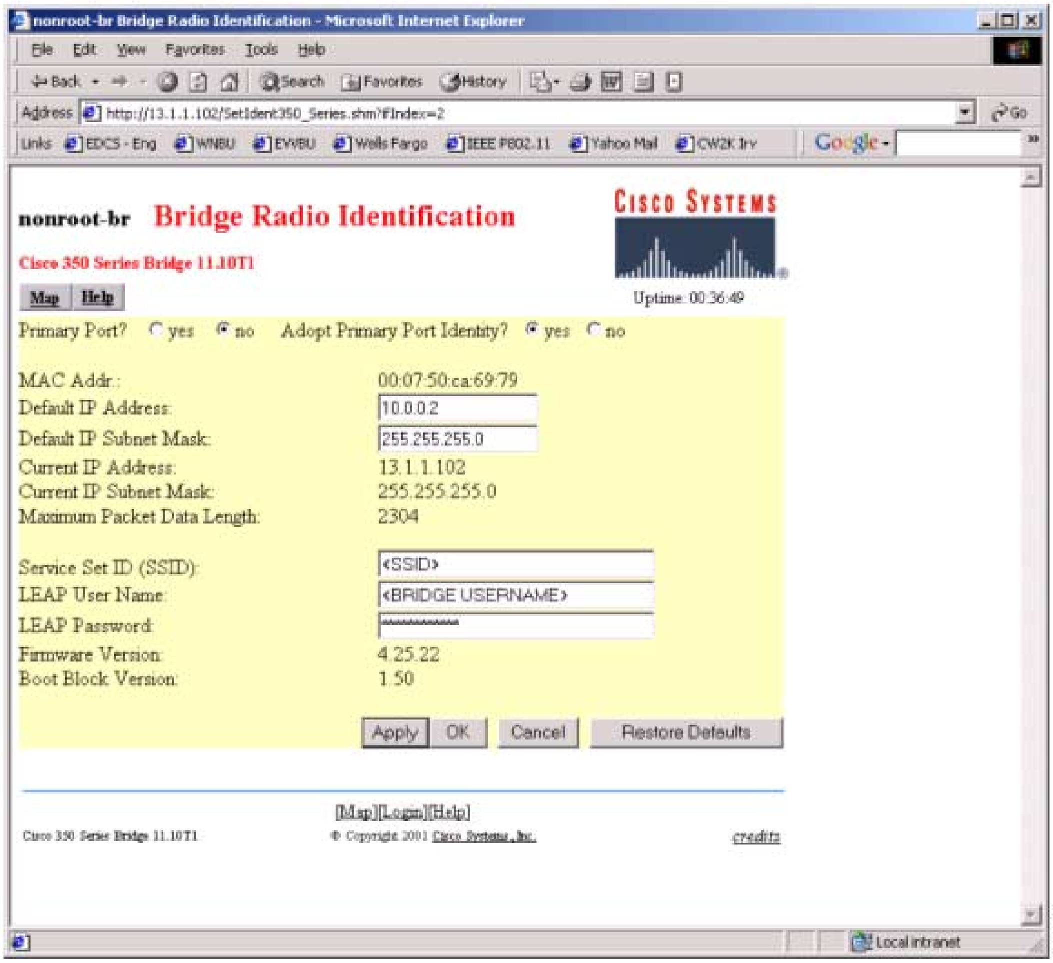
Step 2 Click **Setup**.

Step 3 Under Network Ports, under Bridge Radio, choose **Identification**.

Step 4 Configure the correct Cisco LEAP username and password (see Figure 22).

Step 5 Click **OK**.

Figure 22 VxWorks Non-Root Bridge Configured as EAP Client



nonroot-br Bridge Radio Identification - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://13.1.1.102/SetIdent350_Series.shm?IfIndex=2
Go
Links EDCS - Eng WNBU EWBU Wells Fargo IEEE P802.11 Yahoo Mail CW2K Irv
Google
Cisco Systems
Map Help
Apply OK Cancel Restore Defaults
Local intranet
117204

nonroot-br **Bridge Radio Identification**

Cisco 350 Series Bridge 11.10T1

Uptime: 00:36:49

Primary Port? ○ yes ● no Adopt Primary Port Identity? ● yes ○ no

MAC Addr.:	00:07:50:ca:69:79
Default IP Address:	10.0.0.2
Default IP Subnet Mask:	255.255.255.0
Current IP Address:	13.1.1.102
Current IP Subnet Mask:	255.255.255.0
Maximum Packet Data Length:	2304
Service Set ID (SSID):	<SSID>
LEAP User Name:	<BRIDGE USERNAME>
LEAP Password:	************
Firmware Version:	4.25.22
Boot Block Version:	1.50

[Map][Login][Help]

Cisco 350 Series Bridge 11.10T1 © Copyright 2001 Cisco Systems, Inc. credits

Configuring the Cisco Aironet 350 Series Workgroup Bridge for Cisco LEAP

Step 1 Browse to the workgroup bridge.

Step 2 Make sure that the SSID is correct.

Step 3 Click **Allow Config Changes**.

Step 4 In the Configuration box, click **Security**.

Step 5 In the Login User Name field, configure the username for Cisco LEAP authentication (see Figure 23).

Step 6 Click **Save**.

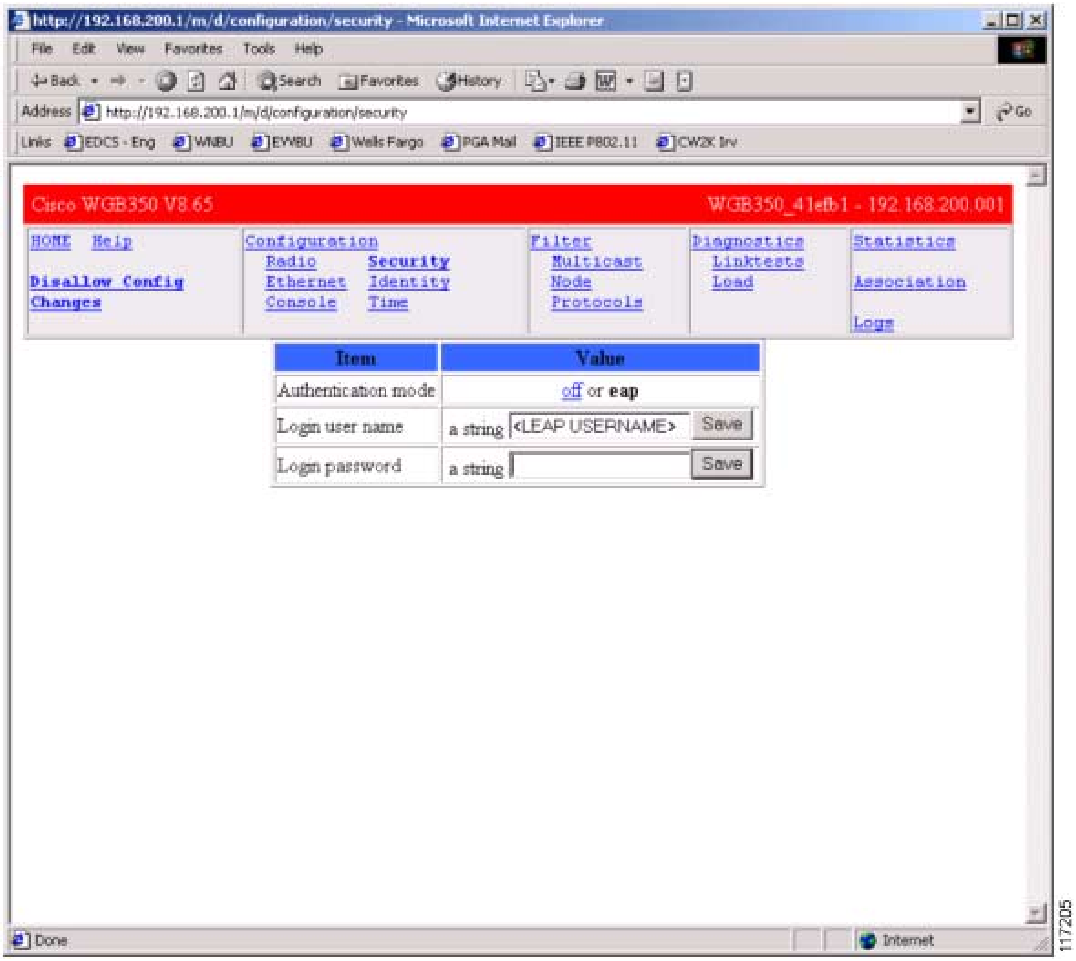
Step 7 In the Login Password field, configure the appropriate password.

Step 8 Click **Save**.

Step 9 For the Authentication Mode, click **EAP**.

Step 10 Verify association to the access point by clicking **Association** in the Statistics field.

Figure 23 Workgroup Bridge Security Configuration


http://192.168.200.1/m/d/configuration/security - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://192.168.200.1/m/d/configuration/security
Go
Links EDCS - Eng WNBU EWBU Wells Fargo PGA Mail IEEE P802.11 CW2K Irv
Cisco WGB350 V8.65
WGB350_41efb1 - 192.168.200.001
HOME Help
Disallow Config Changes
Configuration
Radio
Security
Ethernet
Identity
Console
Time
Filter
Multicast
Node
Protocols
Diagnostics
Linktests
Load
Statistics
Association
Logs
Done
Internet
117205

Item	Value
Authentication mode	off or **eap**
Login user name	a string <LEAP USERNAME> Save
Login password	a string Save

Configuring Non-Cisco Client Devices for Cisco LEAP

It is possible to configure other client devices for use with the Cisco Wireless Security Suite. The advent of the Cisco Compatible Extensions program for client devices and the availability of third-party supplicants have made it possible to share a common secure infrastructure with various vendors' devices. This section shows the basic configuration for Funk Software Odyssey and Meetinghouse Data Communications AEGIS supplicants.

If you are using the Funk or Meetinghouse supplicant for WPA authenticated key management, you must use a NIC card that has WPA-compliant firmware and drivers. Refer to the Wi-Fi Alliance website for details on WPA-certified NIC cards:

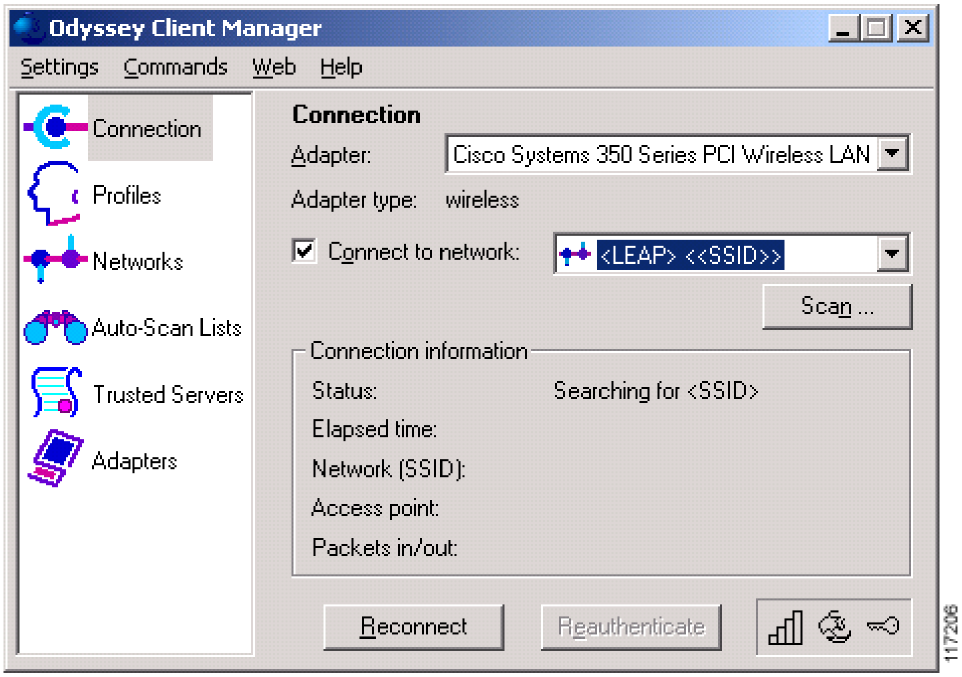
http://www.wifialliance.org

Configuring the Funk Software Supplicant for Cisco LEAP

This section describes how to configure the Funk Software Odyssey Client supplicant version 2.2 for Cisco LEAP authentication. If you are using non-Cisco client cards with Cisco Aironet access points running Cisco IOS Software Release 12.2(4)JA or later, the access point must be configured for Open authentication with EAP under SSID Manager.

Step 1 On the Connection screen (see Figure 24), choose the adapter to which the networks and profiles settings will be applied.

Figure 24 Funk Odyssey Connection Screen



Connection

Adapter: Cisco Systems 350 Series PCI Wireless LAN

Adapter type: wireless

☑ Connect to network: <LEAP> <<SSID>>

Connection information

Status: Searching for <SSID>

Elapsed time:

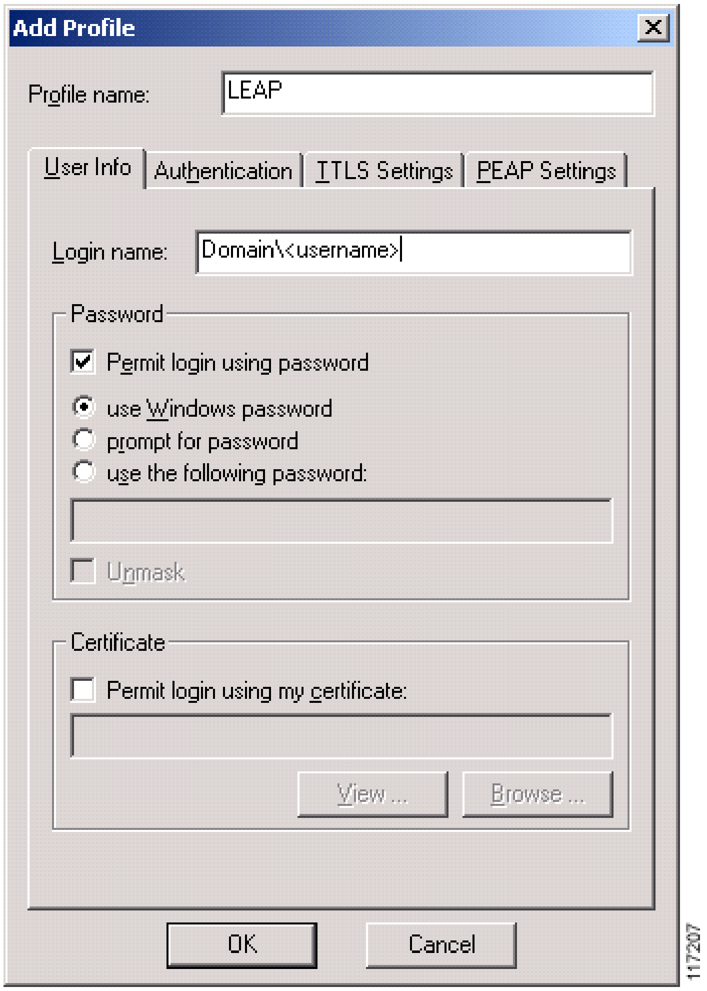
Network (SSID):

Access point:

Packets in/out:

Step 2 On the Add Profile screen, enter a profile name (see Figure 25). The first tab on the Add Profile screen is User Info. On this tab, enter your login name, including Microsoft domain if applicable. Specify the password entry method (Windows credentials or user-prompt mode).

Figure 25 Funk Odyssey Add Profile Screen - User Info Tab



Add Profile

Profile name: LEAP

Login name: Domain\<username>

Password

☑ Permit login using password

● use Windows password

○ prompt for password

○ use the following password:

□ Unmask

Certificate

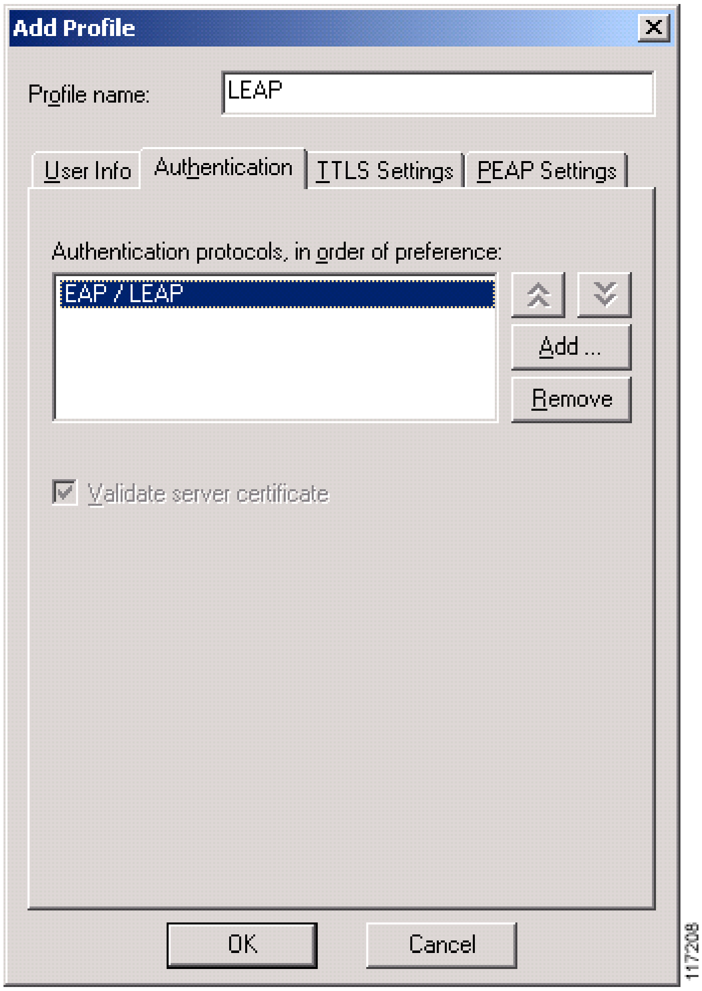
□ Permit login using my certificate:

Step 3 Click **OK** to save your user information.

Step 4 Click the Authentication tab, choose the authentication protocol to be used in the profile (see Figure 26), and click **OK**.

Note Click **Add** to access selections. For Cisco LEAP authentication, choose the **EAP/LEAP** option and click **OK** (see Figure 27).

Figure 26 Funk Odyssey Add Profile Screen - Authentication Tab



Add Profile

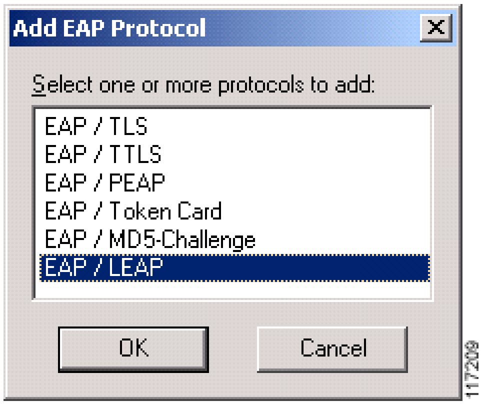
Profile name: LEAP

Authentication protocols, in order of preference:

EAP / LEAP

☑ Validate server certificate

Figure 27 Funk Odyssey Add EAP Protocol Screen



Add EAP Protocol

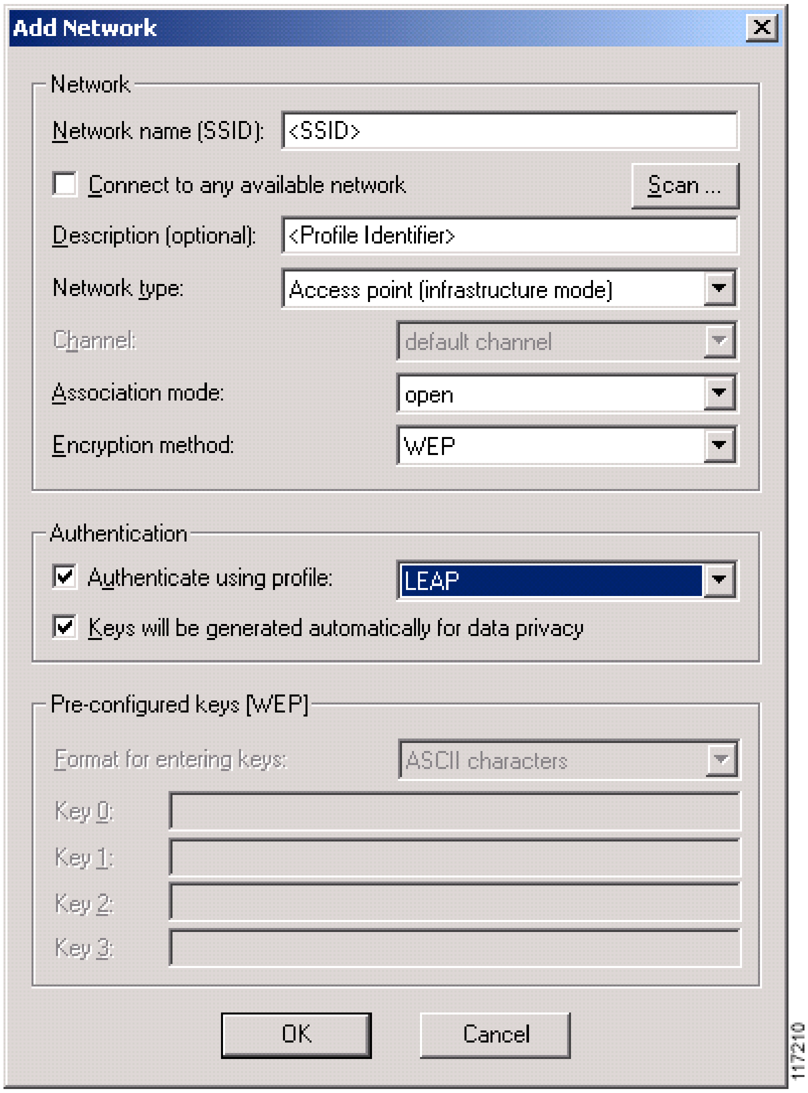
Select one or more protocols to add:

- EAP / TLS
- EAP / TTLS
- EAP / PEAP
- EAP / Token Card
- EAP / MD5-Challenge
- EAP / LEAP

Step 5 After you configure a profile for Cisco LEAP, you can configure a network to use the authentication profile. On the Add Network screen (see Figure 28), configure a network name, description, network type, association mode, encryption method, and authentication mechanism. The configuration shown in Figure 28 is for use with Cisco LEAP authentication and dynamic WEP encryption.

Note Set the Association Mode field to **WPA** and the Encryption Method field to **TKIP** if you are using WPA-authenticated key management.

Figure 28 Funk Odyssey Add Network Screen



Add Network

Network

Network name (SSID): <SSID>

□ Connect to any available network

Description (optional): <Profile Identifier>

Network type: Access point (infrastructure mode)

Channel: default channel

Association mode: open

Encryption method: WEP

Authentication

☑ Authenticate using profile: LEAP

☑ Keys will be generated automatically for data privacy

Pre-configured keys (WEP)

Format for entering keys: ASCII characters

Key 0:

Key 1:

Key 2:

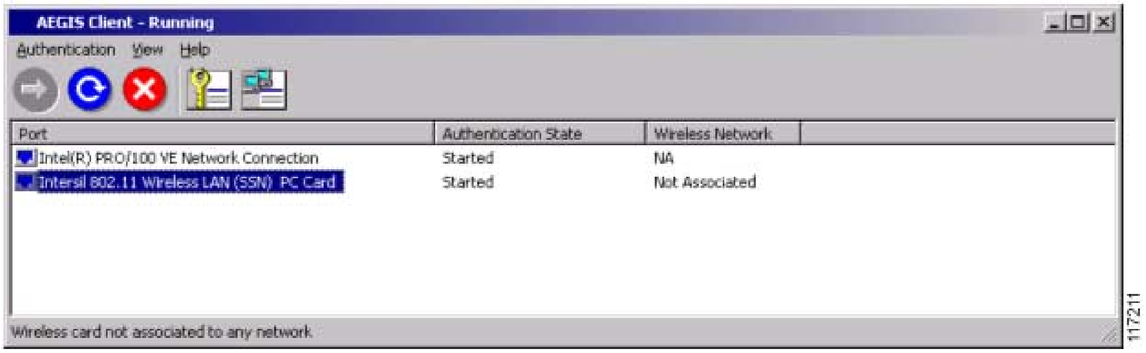
Key 3:

Configuring the Meetinghouse AEGIS Supplicant for Cisco LEAP

This section describes how to configure the Meetinghouse Data Communications AEGIS Client supplicant version 2.1 for Cisco LEAP authentication for client devices authenticating to Cisco Aironet access points running Cisco IOS Software Release 12.2(4) or later. The access point must be configured for Open authentication with EAP under SSID Manager for use with third-party supplicants.

Step 1 On the AEGIS Client main screen (see Figure 29), choose the adapter to configure for Cisco LEAP authentication. Right-click the adapter or click the **Network Profiles** icon to access the 802.11 network screen.

Figure 29 AEGIS Client Main Screen

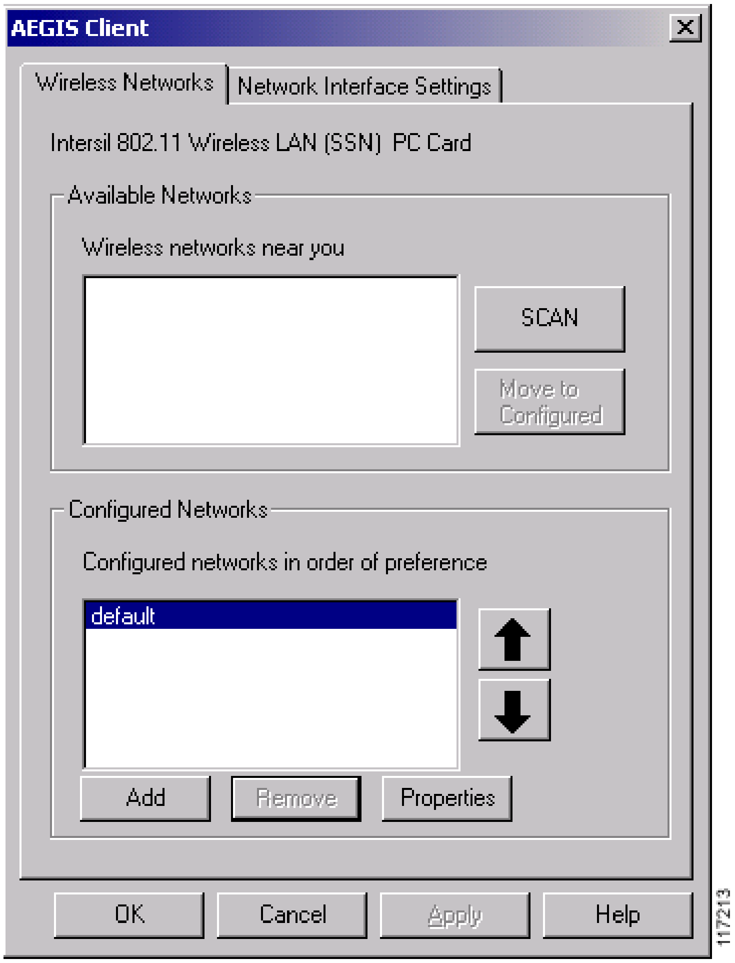


Port	Authentication State	Wireless Network
Intel(R) PRO/100 VE Network Connection	Started	NA
Intersil 802.11 Wireless LAN (SSN) PC Card	Started	Not Associated

Wireless card not associated to any network

Step 2 On the Wireless Networks screen (see Figure 30), choose the network to configure for Cisco LEAP from the Available Networks list or click **Add** to enter it manually.

Figure 30 AEGIS Client Wireless Networks Screen

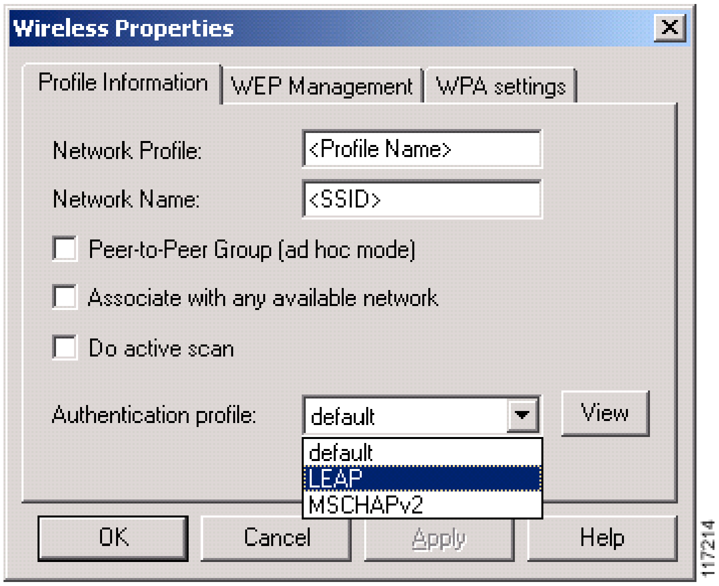


Intersil 802.11 Wireless LAN (SSN) PC Card

default

The Wireless Properties screen appears (see Figure 31).

Figure 31 AEGIS Client Wireless Properties Screen - Profile Information Tab



Network Profile: <Profile Name>

Network Name: <SSID>

□ Peer-to-Peer Group (ad hoc mode)

□ Associate with any available network

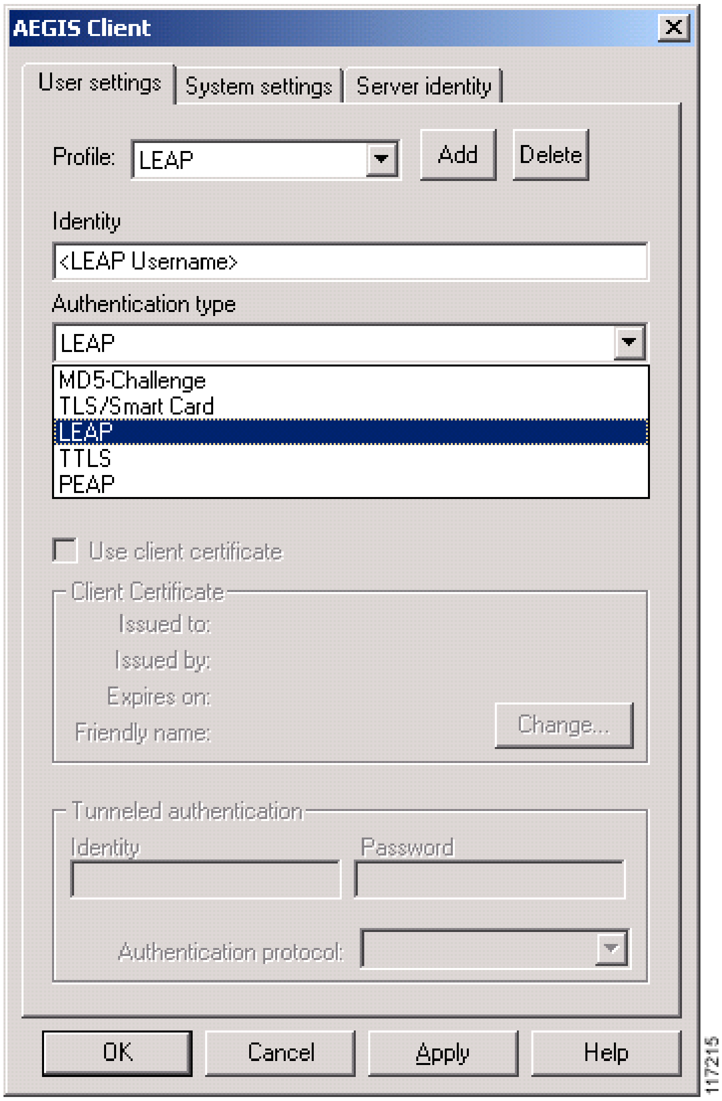
□ Do active scan

Authentication profile: default

Step 3 On the Wireless Properties screen, enter a name in the Network Profile field, enter the SSID for the Cisco LEAP network in the Network Name field, uncheck the **Associate with any available network** check box, and choose the authentication profile to be used with this network profile.

Step 4 Click **View** to access the AEGIS Client User Settings screen (see Figure 32) or access the screen from the **Authentication Profiles** icon on the AEGIS Client main screen.

Figure 32 AEGIS Client User Settings Screen



Profile: LEAP

Identity: <LEAP Username>

Authentication type: LEAP

□ Use client certificate

Step 5 Click **Add** to be prompted for an authentication profile name.

Step 6 Enter the user ID to be used for Cisco LEAP authentication in the Identity field.

Step 7 Choose **LEAP** from the Authentication Type drop-down box.

Step 8 Either check the **Use Windows logon credentials** check box or enter a password, as appropriate.

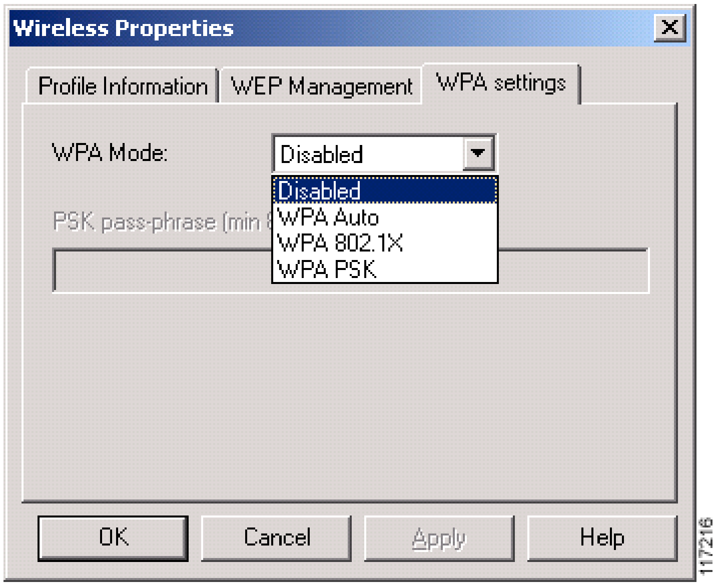
Step 9 Click **OK** to save the authentication profile.

Step 10 Return to the Wireless Properties screen and click the WEP Management tab to configure Provide Encryption Key Dynamically settings. Choose **Disabled** for WEP.

Step 11 Click the WPA Settings tab and choose **WPA 802.1X** for WPA Mode (see Figure 33).

Step 12 Click **OK** to save the changes.

Figure 33 AEGIS Client Wireless Properties Screen - WPA Settings Tab



Configuring MAC Authentication

MAC authentication is a way to centrally authenticate devices that do not support 802.1X. Because MAC authentication is an inherently weak form of authentication, the MAC addresses are transmitted unencrypted across the wireless medium. With MAC authentication, an eavesdropper can easily spoof a MAC address and gain entry to the network.

Note If the Cisco Secure ACS used for MAC authentication is also used for Cisco LEAP authentication, MAC addresses must be stored in clear text (Password Authentication Protocol [PAP] passwords) exclusively. A strong Challenge Handshake Authentication Protocol (CHAP)/MS-CHAP password—differing from the MAC address—is required as well. Failure to use a different, strong CHAP/MS-CHAP password for the Cisco Secure ACS enables unauthorized users to use a MAC address as a Cisco LEAP username and password to gain access to the network.

Adding the Access Point to the Cisco Secure ACS

The process for adding an access point that uses MAC authentication is identical to the process for adding an access point that uses Cisco LEAP authentication. Refer to the "Adding the Access Point to the Cisco Secure ACS" section on page 4 for instructions.

Adding a MAC Address to the Cisco Secure ACS

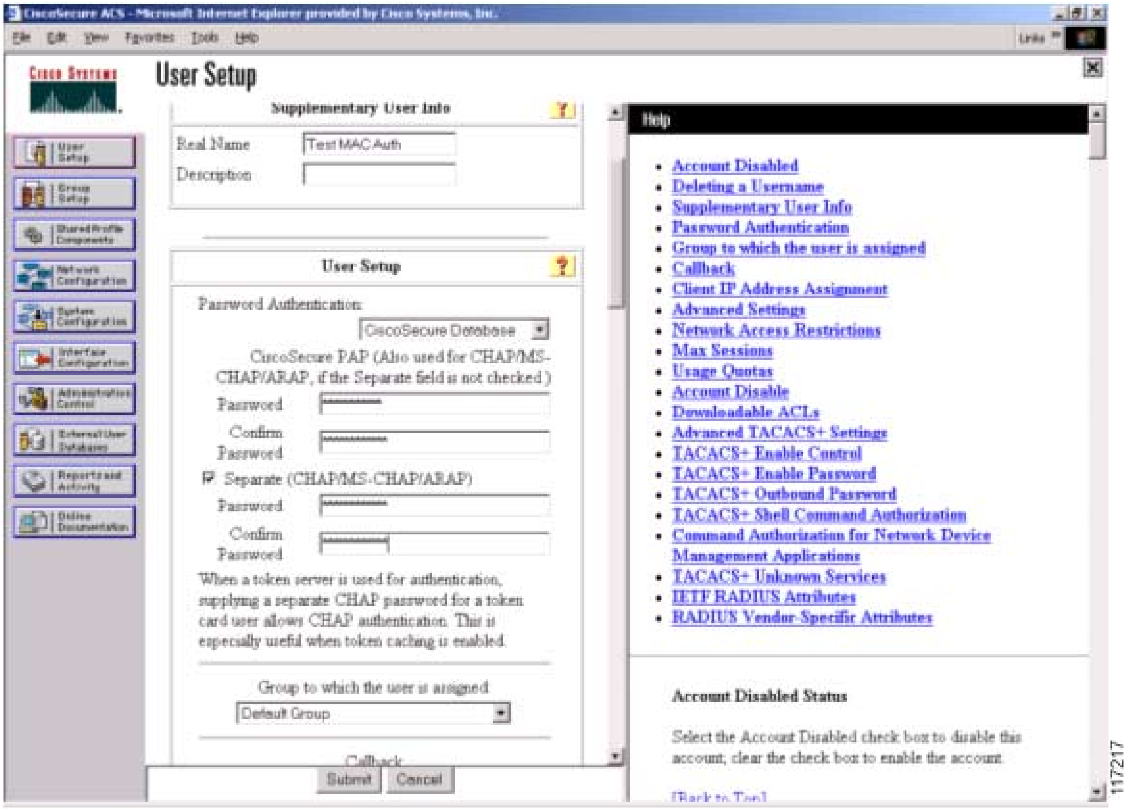
The Cisco Secure ACS can authenticate MAC addresses sent from an access point. A properly configured access point attempts to authenticate a MAC address using Secure-PAP authentication with the Cisco Secure ACS. The MAC addresses are entered into the Cisco Secure ACS as users, with the username and password being the MAC address.

Step 1 On the Cisco Secure ACS main menu, click **User Setup**.

Step 2 In the User field, enter the MAC address to add to the user database. Do not use dashes, periods, or any other delimiters.

Step 3 Enter the MAC address in the CiscoSecure PAP Password field (see Figure 34).

Figure 34 Cisco Secure ACS Version 3.2 User Setup for MAC Authentication



User Setup

Supplementary User Info

Real Name: Test MAC Auth

Description:

User Setup

Password Authentication: CiscoSecure Database

CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password: ************

Confirm Password: ************

☑ Separate (CHAP/MS-CHAP/ARAP)

Password: ************

Confirm Password: ************

When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.

Group to which the user is assigned: Default Group

Callback

- Account Disabled
- Deleting a Username
- Supplementary User Info
- Password Authentication
- Group to which the user is assigned
- Callback
- Client IP Address Assignment
- Advanced Settings
- Network Access Restrictions
- Max Sessions
- Usage Quotas
- Account Disable
- Downloadable ACLs
- Advanced TACACS+ Settings
- TACACS+ Enable Control
- TACACS+ Enable Password
- TACACS+ Outbound Password
- TACACS+ Shell Command Authorization
- Command Authorization for Network Device Management Applications
- TACACS+ Unknown Services
- IETF RADIUS Attributes
- RADIUS Vendor-Specific Attributes

Account Disabled Status

Select the Account Disabled check box to disable this account; clear the check box to enable the account.

[Back to Top]

Step 4 Check the **Separate (CHAP/MS-CHAP/ARAP)** check box.

Step 5 Enter a strong password for CHAP/MS-CHAP/ARAP. It should not match the MAC address.

Step 6 Click **Submit**.

Configuring MAC Authentication on the Root Bridge or Access Point

There are two modes for MAC authentication.

- **MAC authentication only**

  This mode allows for MAC address authentication as a way to augment open, shared key, or network-EAP authentication.

- **MAC authentication to coexist with EAP authentication**

  This mode allows for MAC address authentication or EAP to authenticate the device or user. The access point first attempts MAC authentication. If that fails, the access point attempts EAP authentication for open and shared-key clients. It is also possible to sequentially authenticate users—initially with MAC and subsequently with EAP.

Configuring MAC Authentication Only

Configuring Cisco Aironet Access Points Running Cisco IOS Software Release 12.2(4)JA or Later for MAC Authentication

Step 1 Browse to the access point.

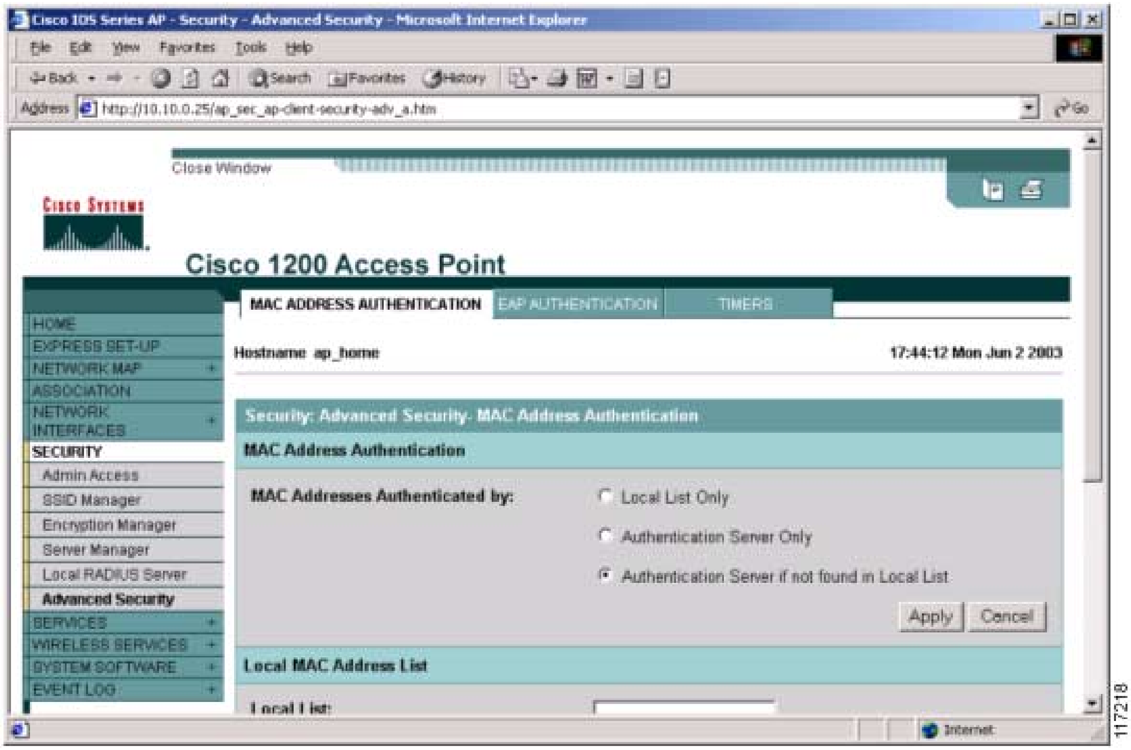
Step 2 Click **Security**.

Step 3 From the Security submenu, click **Advanced Security**.

Step 4 Set the MAC Addresses Authenticated By parameter to **Authentication Server Only** or **Authentication Server if not found in Local List** in order to permit RADIUS-based MAC authentication (see Figure 35).

Note In addition to centralized MAC authentication, it is possible to MAC-authenticate users against a locally configured database in the access point if either the **Local List Only** or **Authentication Server if not found in Local List** option is selected.

Figure 35 MAC Address Authentication Screen



Hostname ap_home 17:44:12 Mon Jun 2 2003

Security: Advanced Security- MAC Address Authentication

MAC Address Authentication

MAC Addresses Authenticated by:

○ Local List Only

○ Authentication Server Only

● Authentication Server if not found in Local List

Apply Cancel

Local MAC Address List

Local List:

Step 5 Click **Apply** to activate MAC authentication.

Step 6 From the Security submenu, click **Server Manager**.

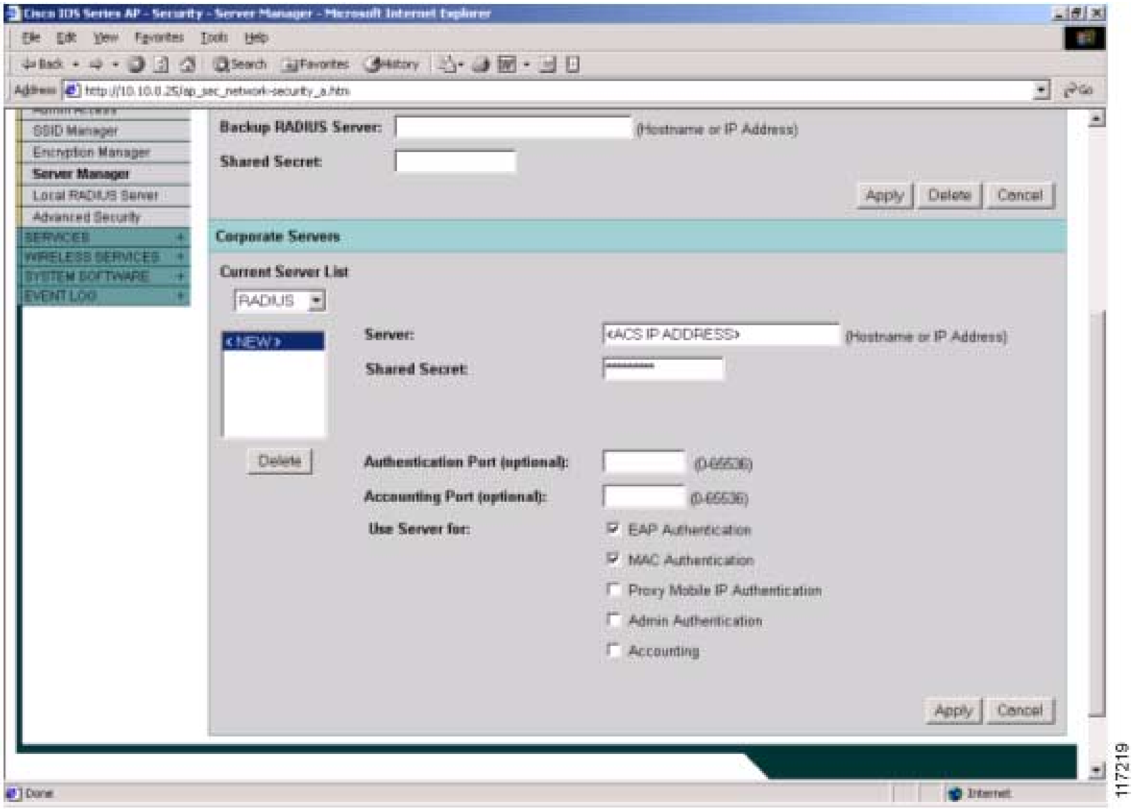
Step 7 Add the Cisco Secure ACS to be used for MAC authentication. Configure the server, shared secret, and authentication port. Then check the **Use Server for: MAC Authentication** check box (see Figure 36).

Note The same Cisco Secure ACS that is used for Cisco LEAP authentication may also be used for MAC authentication.

Step 8 If you want to use the local MAC database, enter the appropriate client MAC address in the New MAC Address field under the Local MAC Address List.

Step 9 Click **Apply** to activate the server configuration.

Figure 36 Configuring Server Manager for MAC Authentication



Backup RADIUS Server: (Hostname or IP Address)

Shared Secret:

Current Server List: RADIUS

<NEW>

Server: <ACS IP ADDRESS> (Hostname or IP Address)

Shared Secret: **********

Authentication Port (optional): (0-65536)

Accounting Port (optional): (0-65536)

Use Server for:
☑ EAP Authentication
☑ MAC Authentication
☐ Proxy Mobile IP Authentication
☐ Admin Authentication
☐ Accounting

These CLI commands approximate the GUI steps above:

```
ap(config)# radius-server host <ip address> auth-port 1645 acct-port 1646 key <shared secret>

ap(config)# radius-server retransmit <number retries>

ap(config)# radius-server timeout <seconds>

ap(config)# aaa group server radius <server groupname for MAC>

ap(config-sg-radius)# server <ip address> auth-port 1645 acct-port 1646

ap(config)# aaa authentication login <auth list for MAC> group <server groupname>

ap(config)# username <MAC> password <MAC address>
```

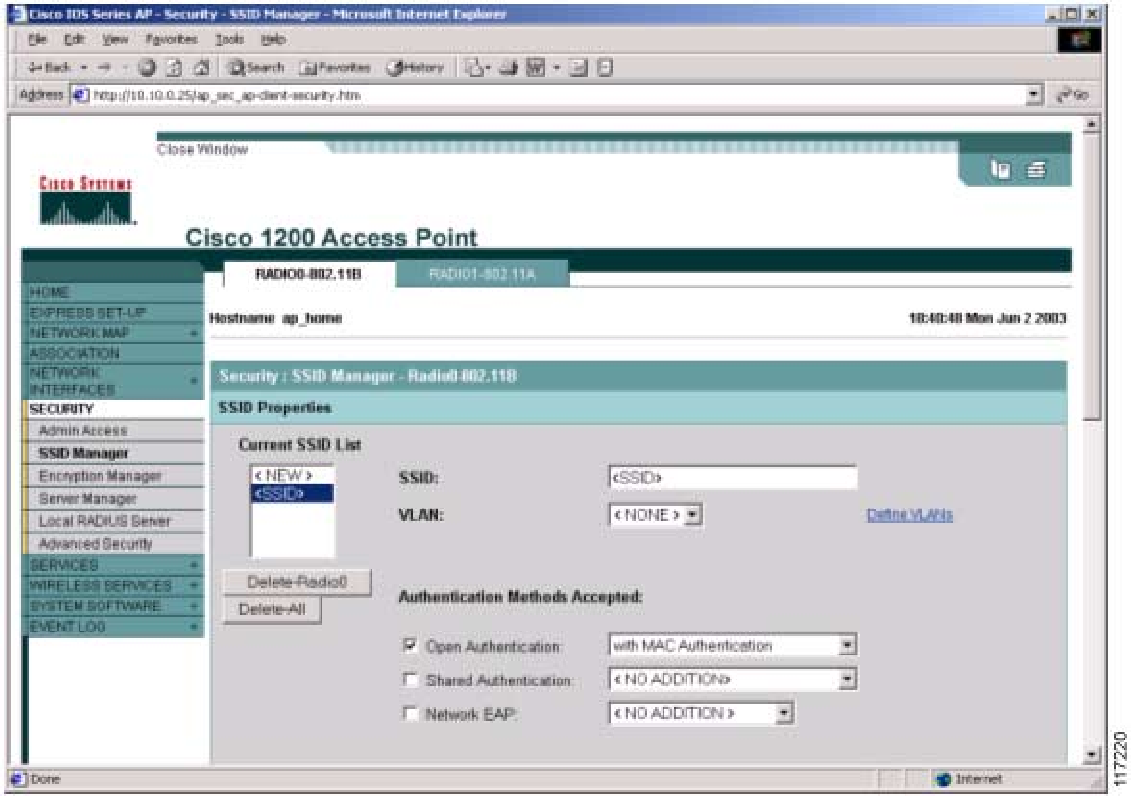
Step 10 From the Security submenu, click **SSID Manage**r.

Step 11 Choose an SSID from the Current SSID List or enter an SSID in the SSID field.

Step 12 Choose **With MAC Authentication** from the Open Authentication or Shared Authentication drop-down box, as applicable (see Figure 37).

Step 13 Click **Apply** to enable MAC authentication for the selected SSID.

Figure 37 Configuring SSID Manager for MAC Authentication



Hostname ap_home 18:40:48 Mon Jun 2 2003

Security : SSID Manager - Radio0-802.11B

SSID Properties

Current SSID List: < NEW >, <SSID>

SSID: <SSID>

VLAN: < NONE >

Authentication Methods Accepted:

☑ Open Authentication: with MAC Authentication

☐ Shared Authentication: < NO ADDITION>

☐ Network EAP: < NO ADDITION >

This CLI command approximates the GUI steps above:

```
ap(config-if-ssid)# authentication open mac-address <auth list for MAC>
```

Configuring Cisco Aironet Access Points Running VxWorks Software Release 12.03T or Earlier for MAC Authentication

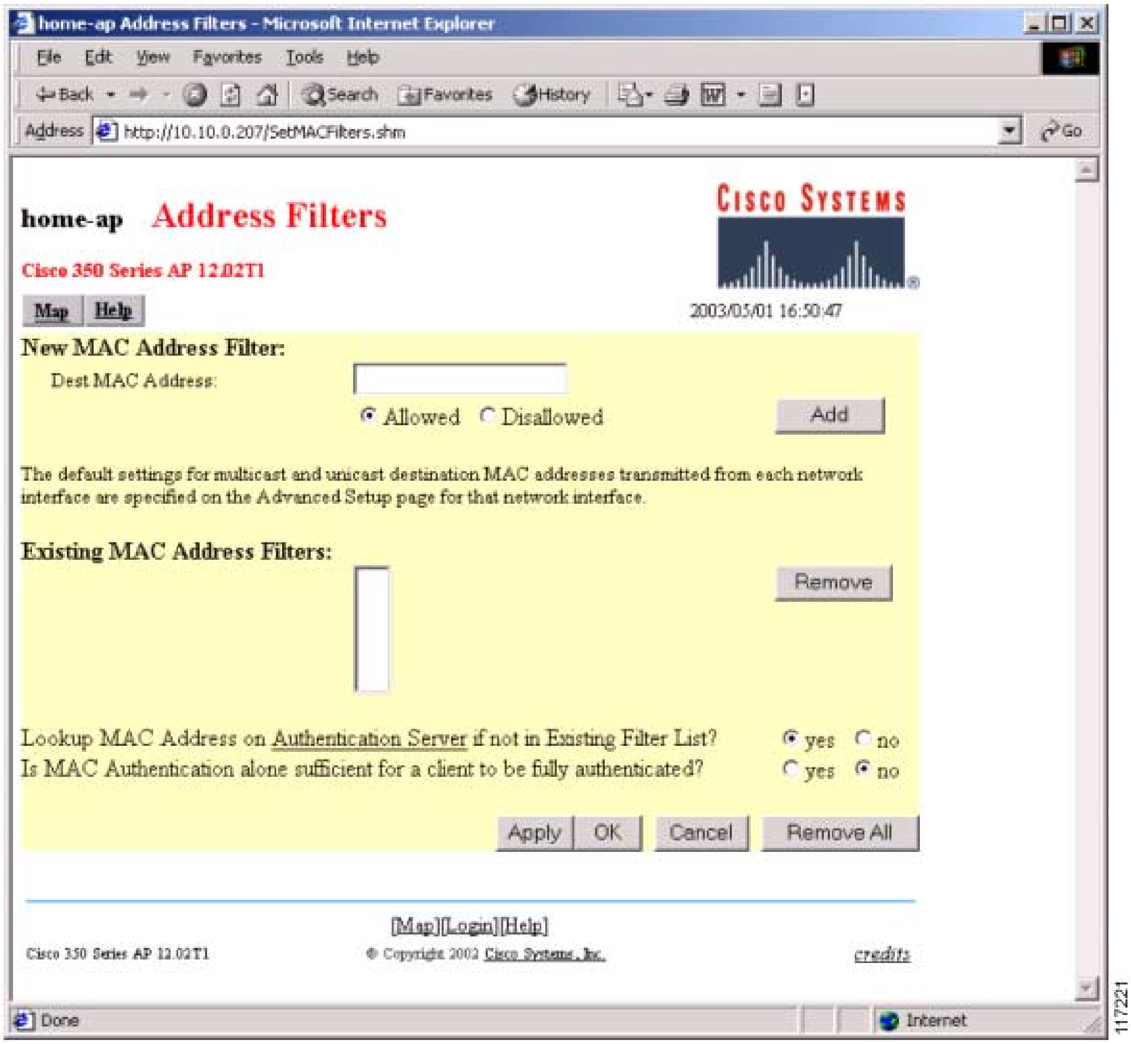
Step 1 Browse to the access point.

Step 2 On the Summary Status page, click **Setup**.

Step 3 In the Associations box, click **Address Filters**.

Step 4 Click the **Yes** radio button for the Lookup MAC Address on Authentication Server If Not in Existing Filter List? parameter (see Figure 38).

Figure 38 Address Filter Configuration for VxWorks



home-ap Address Filters - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address
Go
Cisco Systems
Map Help
Add
Remove
Apply OK Cancel Remove All
Done
Internet
117221

http://10.10.0.207/SetMACFilters.shm

home-ap Address Filters

Cisco 350 Series AP 12.02T1

2003/03/01 16:50:47

New MAC Address Filter:

Dest MAC Address:

● Allowed ○ Disallowed

The default settings for multicast and unicast destination MAC addresses transmitted from each network interface are specified on the Advanced Setup page for that network interface.

Existing MAC Address Filters:

Lookup MAC Address on Authentication Server if not in Existing Filter List? ● yes ○ no

Is MAC Authentication alone sufficient for a client to be fully authenticated? ○ yes ● no

[Map][Login][Help]

Cisco 350 Series AP 12.02T1

© Copyright 2002 Cisco Systems, Inc.

credits

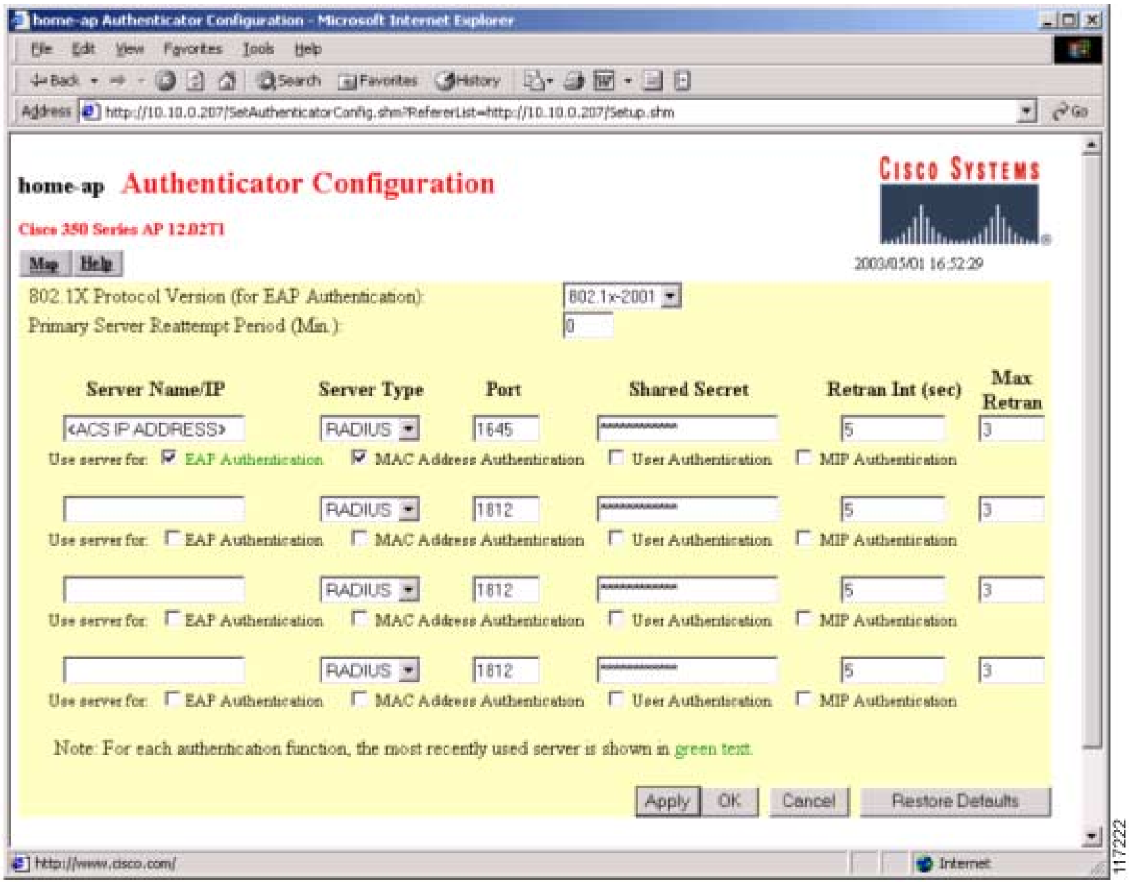
Step 5 Click the **No** radio button for the Is MAC Authentication Alone Sufficient for a Client to Be Fully Authenticated? parameter.

Step 6 Click the **Authentication Server** link.

Step 7 Add the Cisco Secure ACS for MAC authentication. Configure the server name/IP, server type, port, shared secret, and timeout (see Figure 39).

Note The same Cisco Secure ACS that is used for Cisco LEAP authentication may also be used for MAC authentication.

Figure 39 RADIUS Server Configuration for VxWorks


home-ap Authenticator Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address
Go
Map
Help
Apply
OK
Cancel
Restore Defaults
Internet
117222

http://10.10.0.207/SetAuthenticatorConfig.shm?RefererList=http://10.10.0.207/Setup.shm

home-ap **Authenticator Configuration**

Cisco 350 Series AP 12.02T1

CISCO SYSTEMS

2003/05/01 16:52:29

802.1X Protocol Version (for EAP Authentication): 802.1x-2001

Primary Server Reattempt Period (Min.): 0

Server Name/IP	Server Type	Port	Shared Secret	Retran Int (sec)	Max Retran
<ACS IP ADDRESS>	RADIUS	1645	**************	5	3
Use server for: ☑ EAP Authentication	☑ MAC Address Authentication		□ User Authentication	□ MIP Authentication	
	RADIUS	1812	**************	5	3
Use server for: □ EAP Authentication	□ MAC Address Authentication		□ User Authentication	□ MIP Authentication	
	RADIUS	1812	**************	5	3
Use server for: □ EAP Authentication	□ MAC Address Authentication		□ User Authentication	□ MIP Authentication	
	RADIUS	1812	**************	5	3
Use server for: □ EAP Authentication	□ MAC Address Authentication		□ User Authentication	□ MIP Authentication	

Note: For each authentication function, the most recently used server is shown in green text.

http://www.cisco.com/

Step 8 Check the **MAC Address Authentication** check box.

Step 9 Click **OK**. The Address Filters page reappears.

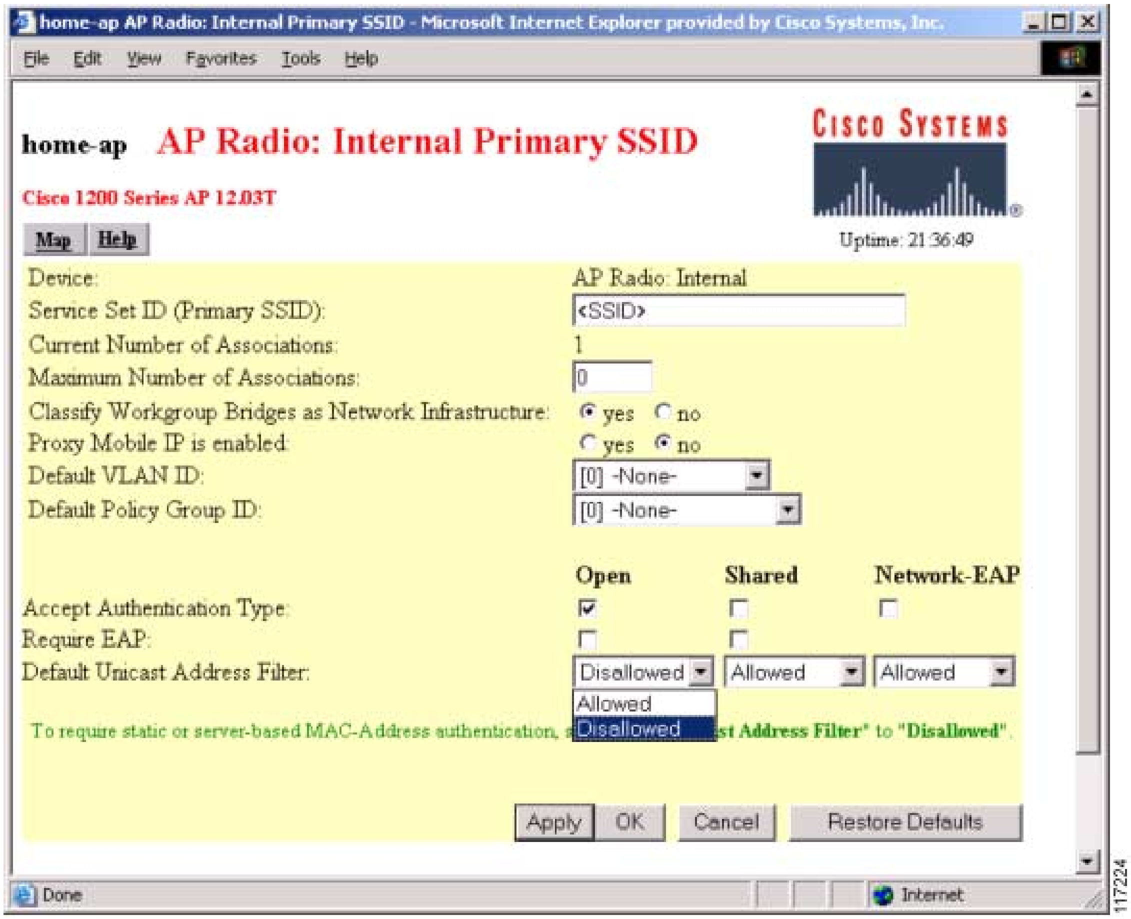
Step 10 Click **OK**.

Step 11 Browse to the Setup page.

Step 12 Choose **Service Sets** from the menu.

Step 13 Choose the SSID from the Existing SSIDs list. The SSID Configuration page appears (see Figure 40).

Figure 40 Enable MAC Authentication per Authentication Type for VxWorks


home-ap AP Radio: Internal Primary SSID - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Cisco Systems
Map Help
Apply OK Cancel Restore Defaults
Done
Internet
117224

home-ap **AP Radio: Internal Primary SSID**

Cisco 1200 Series AP 12.03T

Uptime: 21:36:49

Device:	AP Radio: Internal
Service Set ID (Primary SSID):	<SSID>
Current Number of Associations:	1
Maximum Number of Associations:	0
Classify Workgroup Bridges as Network Infrastructure:	● yes ○ no
Proxy Mobile IP is enabled:	○ yes ● no
Default VLAN ID:	[0] -None-
Default Policy Group ID:	[0] -None-

	Open	Shared	Network-EAP
Accept Authentication Type:	☑	□	□
Require EAP:	□	□	
Default Unicast Address Filter:	Disallowed Allowed Disallowed	Allowed	Allowed

To require static or server-based MAC-Address authentication, s st Address Filter" to "Disallowed".

Step 14 For non-EAP clients, enable MAC for the authentication type used by the clients. Either open authentication or shared-key authentication can be used. For each desired authentication type that is to use MAC authentication, choose **Disallowed** in the Default Unicast Address Filter drop-down box.

Step 15 Click **OK** to finish.

Configuring MAC Authentication to Coexist with EAP Authentication

This access point configuration permits the coexistence of MAC authentication and EAP authentication using a common SSID. This mode is useful for supporting both Cisco LEAP-capable devices and devices using static WEP or for sequentially authenticating MAC and Cisco LEAP WLAN clients.

Using MAC authentication and EAP authentication on the same SSID enables a static WEP key to be used to access the network. Therefore, this mode is less secure than a network that uses exclusively dynamic encryption (EAP authentication). Refer to the Cisco SAFE: Wireless LAN Security In-Depth White Paper for appropriate design guidelines.

Configuring Cisco Aironet Access Points Running Cisco IOS Software Release 12.2(4)JA or Later for MAC and EAP Coexistence

Step 1 Verify that MAC authentication is configured as detailed in the "Configuring Cisco Aironet Access Points Running Cisco IOS Software Release 12.2(4)JA or Later for MAC Authentication" section on page 38. Make sure that Server Manager is configured for the MAC authentication server and that the MAC Addresses Authenticated By parameter is set to **Authentication Server if not found in Local List** in Advanced Security.

Step 2 Browse to the access point.

Step 3 Click **Security**.

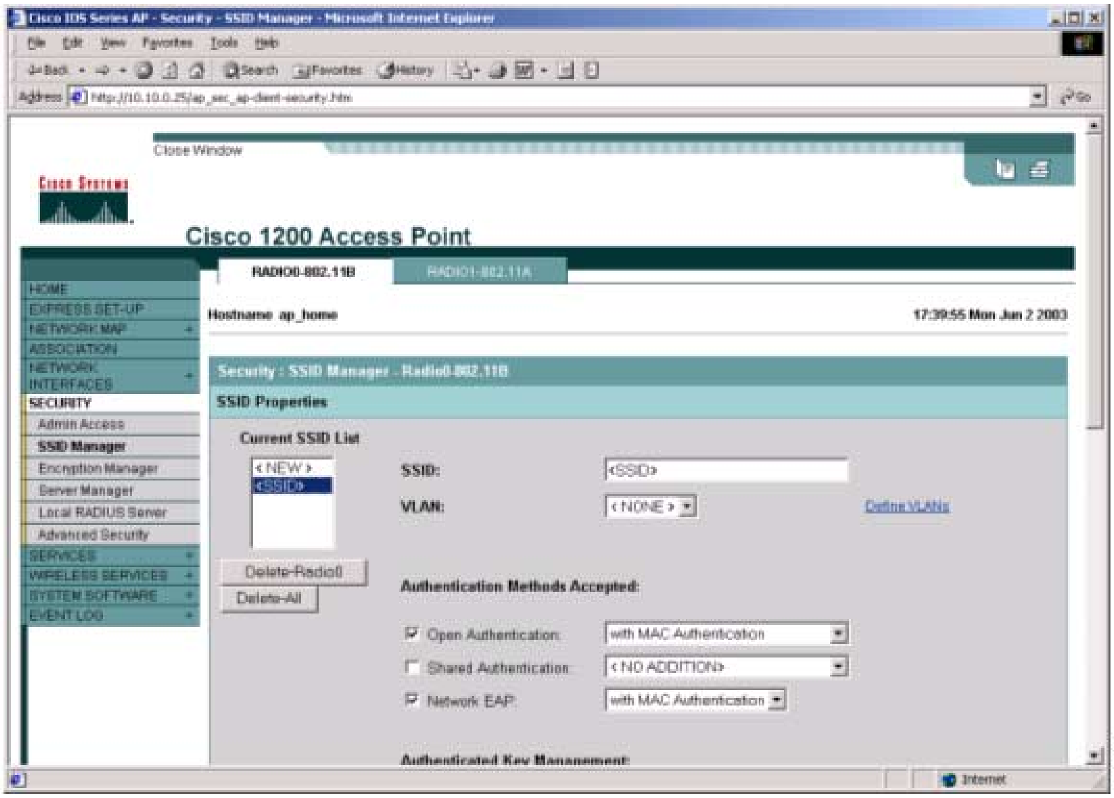
Step 4 From the Security submenu, click **SSID Manager**.

Step 5 Check the **Network EAP** check box under Authentication Methods Accepted and choose **With MAC Authentication** in the corresponding drop-down box (see Figure 41).

Step 6 If you want to also permit MAC authentication for non-EAP users through the same access point and SSID, check the **Open Authentication** check box under Authentication Methods Accepted and choose **With MAC Authentication** in the corresponding drop-down box.

Step 7 Click **Apply** to enable MAC (or MAC + EAP) authentication.

Figure 41 MAC + EAP Authentication for IOS



Cisco IOS Series AP - Security - SSID Manager - Microsoft Internet Explorer

Address: http://10.10.0.25/ap_sec_ap-client-security.htm

Cisco 1200 Access Point

Hostname ap_home

17:39:55 Mon Jun 2 2003

Security : SSID Manager - Radio0-802.11B

SSID Properties

Current SSID List: < NEW >, <SSID>

SSID: <SSID>

VLAN: < NONE >

Authentication Methods Accepted:

☑ Open Authentication: with MAC Authentication

☐ Shared Authentication: < NO ADDITION>

☑ Network EAP: with MAC Authentication

Authenticated Key Management

These CLI commands approximate the GUI steps above.

For use with MAC or EAP authentication (optional):

```
ap(config-if-ssid)# authentication open mac-address <auth list for MAC>
```

```
ap(config-if-ssid)# authentication network-eap <auth list for EAP>
```

For use with MAC and EAP authentication (sequential):

```
ap(config-if-ssid)# authentication network-eap <auth list for EAP> mac-address <auth list for MAC>
```

Configuring Cisco Aironet Access Points Running VxWorks Software Release 12.03T or Earlier for MAC and EAP Coexistence

Step 1 Verify that the Cisco Secure ACS is configured for both MAC authentication and EAP authentication as detailed in the "Configuring MAC Authentication" section on page 36 and the "Configuring Cisco LEAP" section on page 4.

Step 2 Browse to the access point or wireless bridge.

Step 3 Click **Setup**.

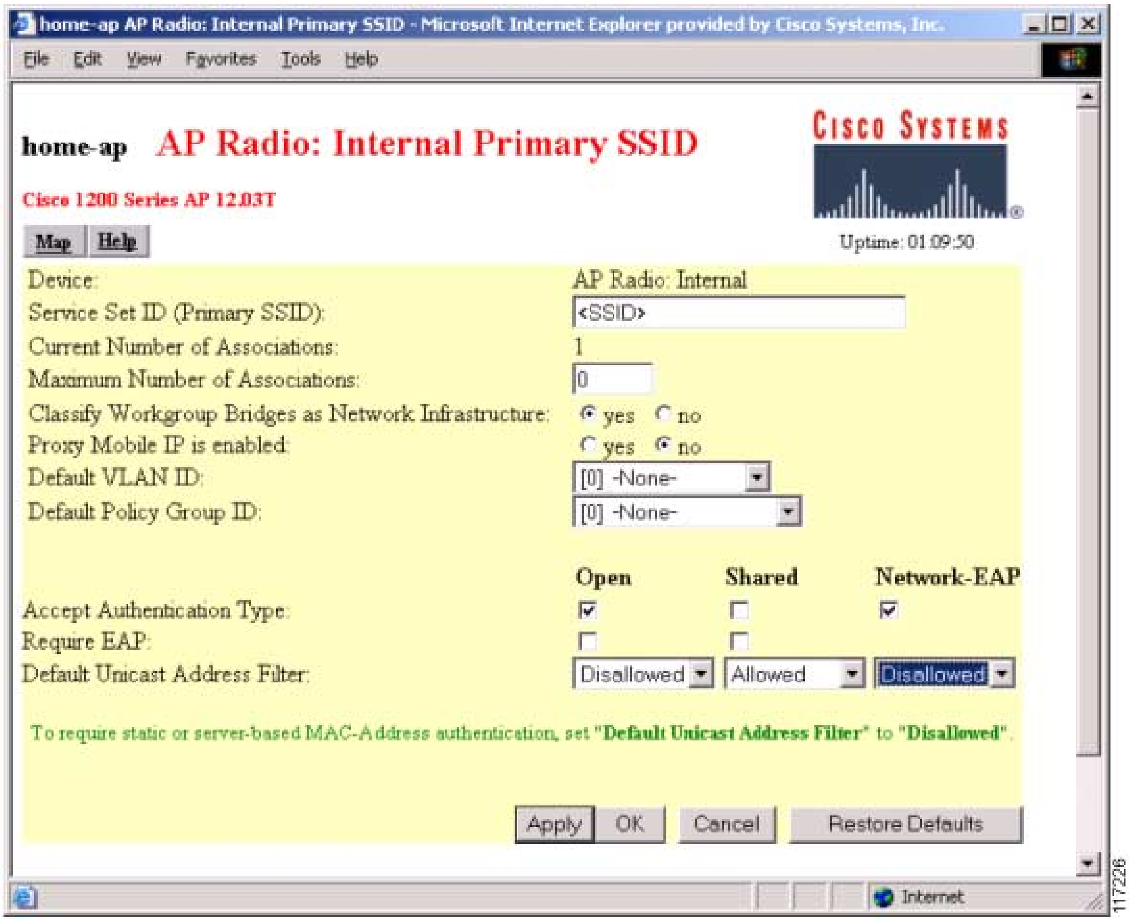
Step 4 In the Associations field, click **Address Filters**.

Step 5 Click the **No** radio button for the Is MAC Authentication Alone Sufficient for a Client to Be Fully Authenticated? parameter.

Step 6 Click **OK** to finish.

Step 7 For each authentication type configured on the SSID that is to use MAC authentication, make sure that the Default Unicast Address Filter parameter is set to **Disallowed**. The example shown in Figure 42 is configured for MAC authentication of both static WEP and Cisco LEAP users.

Figure 42 MAC + EAP Authentication for VxWorks



home-ap AP Radio: Internal Primary SSID - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Cisco Systems
Map
Help
Apply
OK
Cancel
Restore Defaults
Internet
117226

home-ap AP Radio: Internal Primary SSID

Cisco 1200 Series AP 12.03T

Uptime: 01:09:50

Device:	AP Radio: Internal
Service Set ID (Primary SSID):	<SSID>
Current Number of Associations:	1
Maximum Number of Associations:	0
Classify Workgroup Bridges as Network Infrastructure:	● yes ○ no
Proxy Mobile IP is enabled:	○ yes ● no
Default VLAN ID:	[0] -None-
Default Policy Group ID:	[0] -None-

	Open	Shared	Network-EAP
Accept Authentication Type:	☑	☐	☑
Require EAP:	☐	☐	
Default Unicast Address Filter:	Disallowed	Allowed	Disallowed

To require static or server-based MAC-Address authentication, set "**Default Unicast Address Filter**" to "**Disallowed**".

Configuring Cisco TKIP Enhancements

This section provides instructions for configuring the MIC, per-packet keying (encryption key hashing), and broadcast key rotation features for Cisco Aironet access points. Per-packet keying needs to be configured only on the access point. Cisco Aironet WLAN client adapters do not require explicit configuration.

TKIP is designed to improve the security of the standard WEP encryption mechanisms. Refer to the "Wireless LAN Client Adapter Requirements" section on page 2 for client firmware requirements to support MIC and per-packet keying. Learn more about TKIP encryption by reading the *Cisco Aironet Wireless LAN Security Overview*.

Configuring Cisco Aironet Access Points Running Cisco IOS Software Release 12.2(4)JA or Later for Cisco TKIP Enhancements

Step 1 Browse to the access point or wireless bridge.

Step 2 Click **Security**.

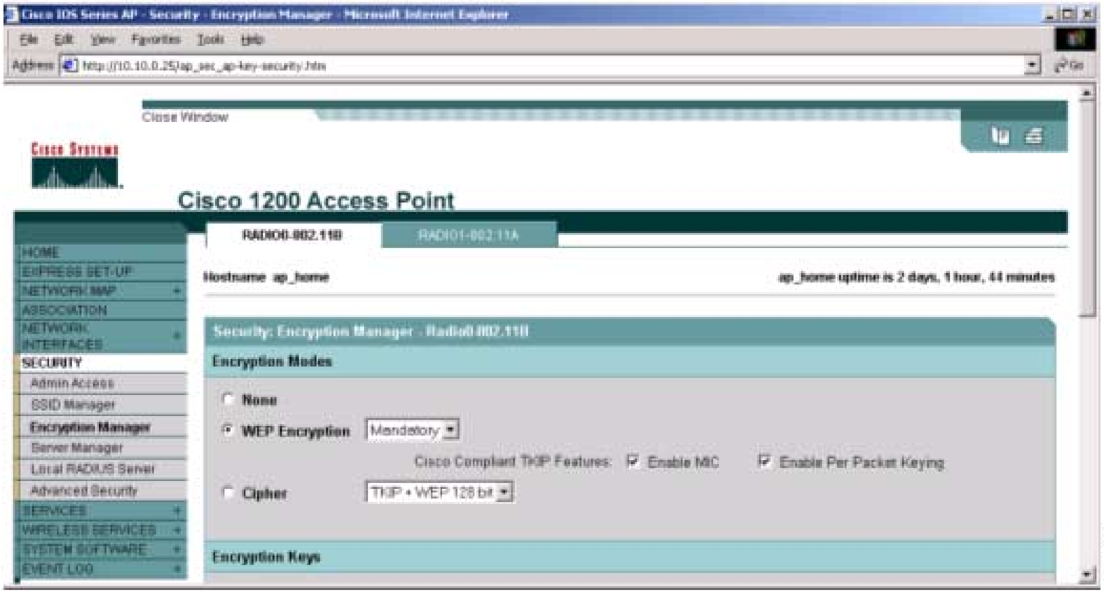
Step 3 From the Security submenu, click **Encryption Manager**.

Step 4 Under Encryption Modes, choose **WEP Encryption**. Then check or uncheck the **Enable MIC** (Cisco Message Integrity Protocol) and **Enable Per Packet Keying** (Cisco TKIP) check boxes (see Figure 43).

Note You can also select these Cisco and Cisco Compatible security options in the Cipher drop-down box by choosing **CKIP** for Cisco per-packet keying and/or **CMIC** for Cisco Message Integrity Protocol. The cipher setting should be enabled if these encryption settings will be used with Cisco Centralized Key Management (CCKM).

Step 5 Click **Apply-Radio0** (if so equipped) to enable the changes.

Figure 43 Configuring Cisco TKIP Enhancements for IOS



Cisco IOS Series AP - Security - Encryption Manager - Microsoft Internet Explorer

Address http://10.10.0.25/ap_sec_ap-key-security.htm

Cisco 1200 Access Point

Hostname ap_home

ap_home uptime is 2 days, 1 hour, 44 minutes

Security: Encryption Manager - Radio0-802.11B

Encryption Modes

○ None

● WEP Encryption Mandatory

Cisco Compliant TKIP Features: ☑ Enable MIC ☑ Enable Per Packet Keying

○ Cipher TKIP + WEP 128 bit

Encryption Keys

These CLI commands approximate the GUI steps above:

```
ap(config-if)# encryption mode wep mandatory key-hash

ap(config-if)# encryption mode wep mandatory mic
```

or

```
ap(config-if)# encryption mode ciphers ckip

ap(config-if)# encryption mode ciphers cmic

ap(config-if)# encryption mode ciphers ckip-cmic
```

Configuring a Root Bridge or Access Point Running VxWorks for Cisco TKIP Enhancements

Step 1 Browse to the access point or wireless bridge.

Step 2 Click **Setup**.

Step 3 In the Network Ports section for the radio, click **Advanced**.

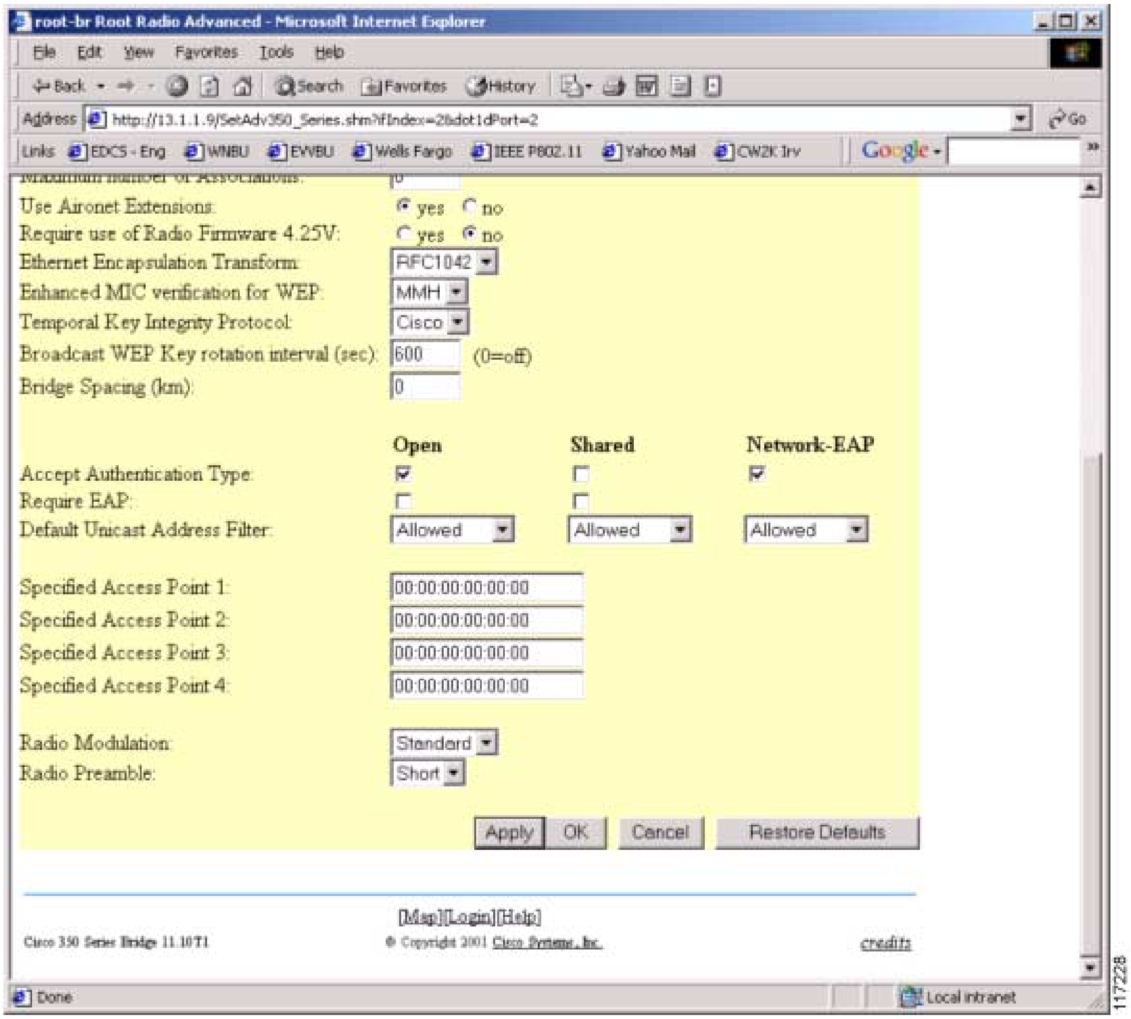
Step 4 To enable MIC, choose **MMH** in the Enhanced MIC Verification for WEP drop-down box (see Figure 44).

Step 5 To enable per-packet keying, choose **Cisco** in the Temporal Key Integrity Protocol drop-down box.

Step 6 To enable broadcast key rotation, enter the desired timeout for the WEP key used for 802.11 broadcast packets in the Broadcast WEP Key Rotation Interval field. Refer to documentation on the Cisco Wireless Security Suite at Cisco.com for theory and guidelines on broadcast WEP key rotation interval. See the following URL:

http://www.cisco.com/en/US/partner/netsol/ns339/ns395/ns176/ns178/networking_solutions_package.html

Figure 44 Configuring Cisco TKIP Enhancements for VxWorks


root-br Root Radio Advanced - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://13.1.1.9/SetAdv350_Series.shm?fIndex=2bdot1dPort=2
Go
Links EDCS - Eng WNBU EVVBU Wells Fargo IEEE P802.11 Yahoo Mail CW2K Irv
Google
Done
Local intranet
117228

Use Aironet Extensions: ● yes ○ no

Require use of Radio Firmware 4.25V: ○ yes ● no

Ethernet Encapsulation Transform: RFC1042

Enhanced MIC verification for WEP: MMH

Temporal Key Integrity Protocol: Cisco

Broadcast WEP Key rotation interval (sec): 600 (0=off)

Bridge Spacing (km): 0

	Open	Shared	Network-EAP
Accept Authentication Type:	☑	□	☑
Require EAP:	□	□	
Default Unicast Address Filter:	Allowed	Allowed	Allowed

Specified Access Point 1: 00:00:00:00:00:00

Specified Access Point 2: 00:00:00:00:00:00

Specified Access Point 3: 00:00:00:00:00:00

Specified Access Point 4: 00:00:00:00:00:00

Radio Modulation: Standard

Radio Preamble: Short

Apply OK Cancel Restore Defaults

[Map][Login][Help]

Cisco 350 Series Bridge 11.10T1 © Copyright 2001 Cisco Systems, Inc. credits

Configuring a Non-Root Wireless Bridge or Repeater for Cisco TKIP Enhancements

The configuration process for a non-root wireless bridge is the same as that for a root wireless bridge or access point as described in the preceding section.

Configuring Cisco Centralized Key Management for Fast Secure Roaming

This section provides instructions for configuring Cisco Centralized Key Management (CCKM) as it applies to the Cisco Wireless Security Suite. Fast secure roaming enables Cisco Aironet wireless LAN client adapters or Cisco Compatible client devices to roam between access points while maintaining an encrypted link without typical 802.11 and EAP keying delays. Voice, terminal emulation, and enterprise resource planning (ERP) applications are examples of applications that may benefit from the implementation of CCKM.

Cisco supports CCKM in Cisco Aironet access points running Cisco IOS Software Release 12.2(11)JA or later and in Cisco Aironet WLAN client adapters with firmware version 5.20.17 (or later) and PCM350 and CB20A driver version 8.4.9 (or later). CCKM functions only with the Cisco LEAP authentication protocol (as of 11/2003).

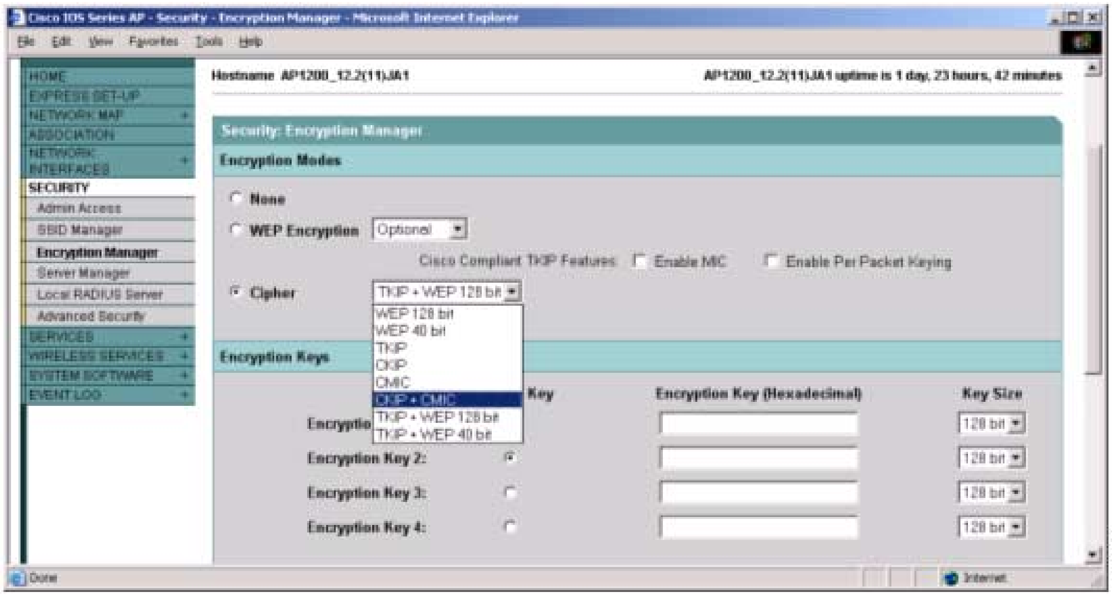
Step 1 Make sure that the access point and AAA server are configured for Cisco LEAP authentication.

Step 2 Click **Security**.

Step 3 From the Security submenu, click **Encryption Manager**

Step 4 Under Encryption Modes, choose **Cipher** and the **CKIP**, **CMIC**, **CKIP + CMIC**, **WEP 128 bit**, or **WEP40 bit** cipher (see Figure 45).

Figure 45 Encryption Manager - Cipher Settings for CCKM



Cisco IOS Series AP - Security - Encryption Manager - Microsoft Internet Explorer

Hostname AP1200_12.2(11)JA1

AP1200_12.2(11)JA1 uptime is 1 day, 23 hours, 42 minutes

Security: Encryption Manager

Encryption Modes

○ None

○ WEP Encryption Optional

Cisco Compliant TKIP Features: □ Enable MIC □ Enable Per Packet Keying

● Cipher TKIP + WEP 128 bit

Encryption Keys

	Transmit Key	Encryption Key (Hexadecimal)	Key Size
Encryption Key 1:			128 bit
Encryption Key 2:	●		128 bit
Encryption Key 3:	○		128 bit
Encryption Key 4:	○		128 bit

These CLI commands approximate the GUI steps above:

```
ap(config-if)# encryption mode ciphers ckip

ap(config-if)# encryption mode ciphers cmic

ap(config-if)# encryption mode ciphers ckip-cmic

ap(config-if)# encryption mode ciphers wep128

ap(config-if)# encryption mode ciphers wep40
```

Note Choose either wep128 or wep40 cipher.

Step 5 Click **SSID Manager** to modify an existing SSID to support CCKM or to add a new SSID to support CCKM.

Step 6 Enter or choose an SSID and VLAN (if configured).

Step 7 Under Authentication Methods Accepted, check the **Network EAP** check box.

Step 8 Under Authenticated Key Management, check the **CCKM** check box under Key Management and choose either **Mandatory** or **Optional** from the drop-down box. Optional key management enables the coexistence of CCKM and WEP clients, as used during the migration of clients to CCKM.

These CLI commands approximate the GUI steps above:

```
ap(config-if-ssid)# authentication network-eap eap  <auth-list for EAP>

ap(config-if-ssid)# authentication cckm optional

ap(config-if-ssid)# authentication cckm mandatory
```

Step 9 Configure Wireless Domain Services (WDS) and backup WDS(s) if required. Click **Wireless Services** > **WDS** from the left menu bar (see Figure 46).

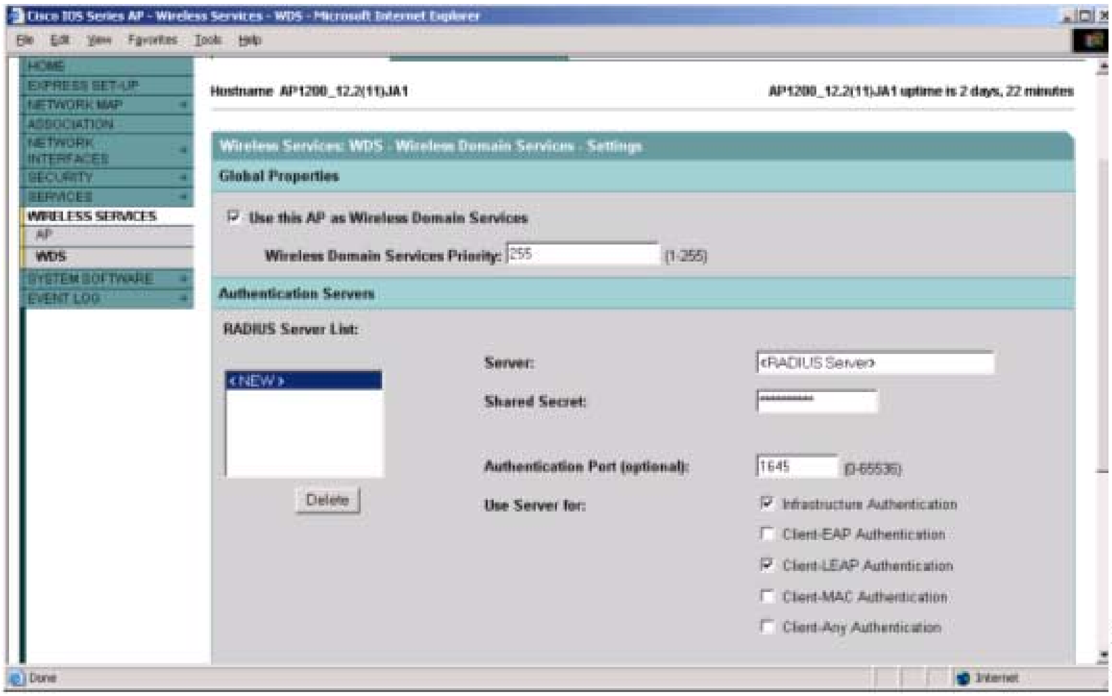
Step 10 Check the **Use This AP as Wireless Domain Services** check box and assign a Wireless Domain Services priority. (larger number = higher priority).

Step 11 Configure WDS for Cisco LEAP authentication, for authentication of both infrastructure devices (access points) and clients.

Step 12 WDS must be configured (at a minimum) with an authentication server for both infrastructure authentication and client authentication. For client authentication, all valid authentication types for clients that are authenticating through this WDS (or access points associated to the WDS) should be enabled.

Step 13 Click **Wireless Services** > **AP** from the left menu bar. Configure each access point for a username and password to be used to Cisco LEAP authenticate the access point with the Cisco Secure ACS. The Cisco Secure ACS must have an entry for each of these access points to be authenticated.

Figure 46 RADIUS Server Configuration - Wireless Domain Services (WDS)



Hostname AP1200_12.2(11)JA1

AP1200_12.2(11)JA1 uptime is 2 days, 22 minutes

Wireless Services: WDS - Wireless Domain Services - Settings

Global Properties

☑ Use this AP as Wireless Domain Services

Wireless Domain Services Priority: 255 (1-255)

Authentication Servers

RADIUS Server List: <NEW>

Server: <RADIUS Server>

Shared Secret: **********

Authentication Port (optional): 1645 (0-65536)

Use Server for:
☑ Infrastructure Authentication
☐ Client-EAP Authentication
☑ Client-LEAP Authentication
☐ Client-MAC Authentication
☐ Client-Any Authentication

These CLI commands approximate the GUI steps above:

```
ap(config)# aaa group server radius <EAP group for infrastructure>

ap(config-sg-radius)# server <ip address> auth-port 1645 acct-port 1646

ap(config)# aaa authentication login <EAP group for infrastructure> <server groupname>

ap(config)# aaa group server radius <EAP group for clients>

ap(config-sg-radius)# server <ip address> auth-port 1645 acct-port 1646

ap(config)# aaa authentication login <EAP group for clients> <server groupname>

ap(config)# wlccp authentication-server infrastructure <server group>

ap(config)# wlccp authentication-server client <server group>

ap(config)# wlccp ap username <user> password <pass>
```

Configuring Wi-Fi Protected Access (WPA) Security

This section provides instructions for configuring Cisco Aironet access points and Cisco Aironet WLAN client adapters to support the Wi-Fi Protected Access (WPA) security standard. WPA is a standards-based, interoperable security solution from the Wi-Fi Alliance industry consortium that is supported by the Cisco Wireless Security Suite. WPA supports 802.1X authenticated key management and TKIP encryption. It is derived from and will be compatible with the upcoming IEEE 802.11i WLAN security standard. The Wi-Fi Alliance verifies 802.11 equipment interoperability between multiple vendors.

WPA security requires three components:

- Software support in the access point
- Software support in the client devices (commonly referred to as a *WPA supplicant*)
- Wi-Fi certified client NIC card driver support for WPA key authentication and distribution

WPA key authentication may be used either in 802.1X mode or with a pre-shared key (PSK). WPA 802.1X mode permits the use of the WPA keying mechanism with any 802.1X EAP type, such as Cisco LEAP, PEAP, or EAP-TLS. The PSK mechanism is intended for use in small office/home office (SOHO) or other consumer environments that do not have an 802.1X-capable RADIUS server. This document focuses on the configuration of access points and clients to support Cisco LEAP with WPA.

Cisco supports WPA in Cisco Aironet access points running Cisco IOS Software Release 12.2(11)JA or later. Cisco also supports WPA in Cisco Aironet 350 and CB20A WLAN client adapters running firmware version 5.30.17 and driver version 8.4.9. WPA key authentication may coexist with static WEP and dynamic WEP encryption through WPA migration mode.

Step 1 Make sure that the access point and AAA server (Cisco Secure ACS) are configured for Cisco LEAP authentication.

Step 2 Click **Security**.

Step 3 From the Security submenu, click **Encryption Manager**.

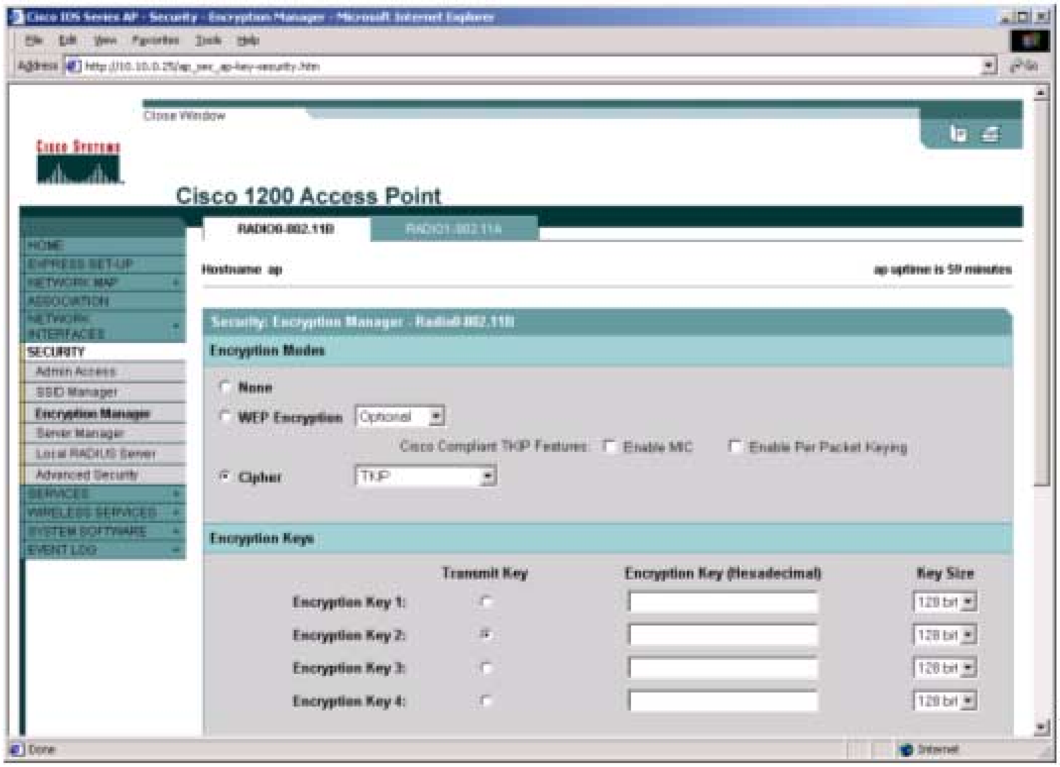
Step 4 Under Encryption Modes, choose **Cipher** and the **TKIP**, **TKIP + WEP128**, or **TKIP + WEP40** cipher (see Figure 47).

Note TKIP is not compatible with either the Cisco TKIP (CKIP) or Cisco MIC (CMIC) security enhancement option on a common SSID. If it is necessary to support CKIP/CMIC and TKIP clients, a multiple VLAN approach is required.

Step 5 Make sure that there are no static encryption keys defined for Encryption Key 1 or Encryption Key 4. These key positions are used in the WPA key authentication process.

Step 6 Click **Apply** to activate the changes.

Figure 47 Encryption Manager - Cipher Settings for WPA



Hostname ap

ap uptime is 59 minutes

Security: Encryption Manager - Radio0-802.11B

Encryption Modes

○ None

○ WEP Encryption Optional

Cisco Compliant TKIP Features: □ Enable MIC □ Enable Per Packet Keying

● Cipher TKIP

Encryption Keys

	Transmit Key	Encryption Key (Hexadecimal)	Key Size
Encryption Key 1:	○		128 bit
Encryption Key 2:	●		128 bit
Encryption Key 3:	○		128 bit
Encryption Key 4:	○		128 bit

These CLI commands approximate the GUI steps above:

```
ap(config-if)# encryption mode ciphers tkip
```

```
ap(config-if)# encryption mode ciphers tkip wep128
```

```
ap(config-if)# encryption mode ciphers tkip wep40
```

Step 7 Click **SSID Manager** to modify an existing SSID to support WPA or to add a new SSID to support WPA.

Step 8 Enter or choose an SSID and VLAN (if configured).

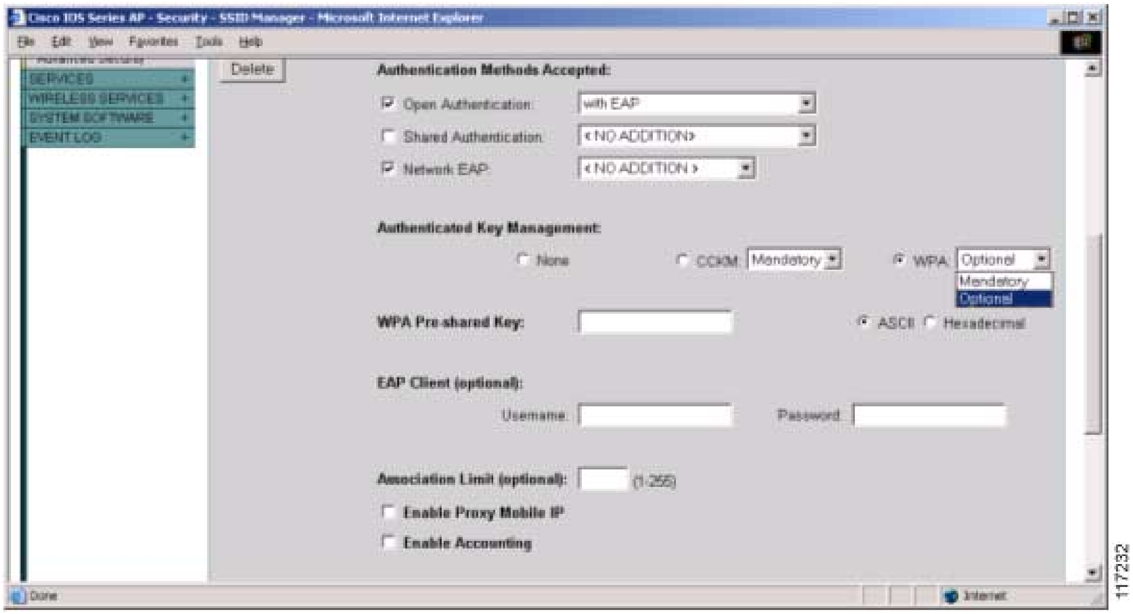
Step 9 Under Authentication Methods Accepted, check the **Open Authentication** and **Network EAP** check boxes (see Figure 48).

Step 10 Under Authenticated Key Management, choose **WPA** and either **Mandatory** or **Optional** in the drop-down box.

Note Optional key management enables WPA migration mode for coexistence of WPA and legacy WEP clients.

Step 11 Click **Apply** to activate the changes.

Figure 48 Authenticated Key Management Settings for SSID and WPA


Cisco IOS Series AP - Security - SSID Manager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
SERVICES +
WIRELESS SERVICES +
SYSTEM SOFTWARE +
EVENT LOG +
Delete
Done
Internet
117232

Authentication Methods Accepted:

☑ Open Authentication: with EAP

☐ Shared Authentication: < NO ADDITION>

☑ Network EAP: < NO ADDITION >

Authenticated Key Management:

○ None ○ CCKM: Mandatory ● WPA: Optional (Mandatory / Optional)

WPA Pre-shared Key: ● ASCII ○ Hexadecimal

EAP Client (optional):

Username: Password:

Association Limit (optional): (1-255)

☐ **Enable Proxy Mobile IP**

☐ **Enable Accounting**

These CLI commands approximate the GUI steps above:

```
ap(config-if-ssid)# authentication open eap <auth-list for EAP>

ap(config-if-ssid)# authentication network-eap eap  <auth-list for EAP>

ap(config-if-ssid)# authentication wpa optional

ap(config-if-ssid)# authentication wpa mandatory
```

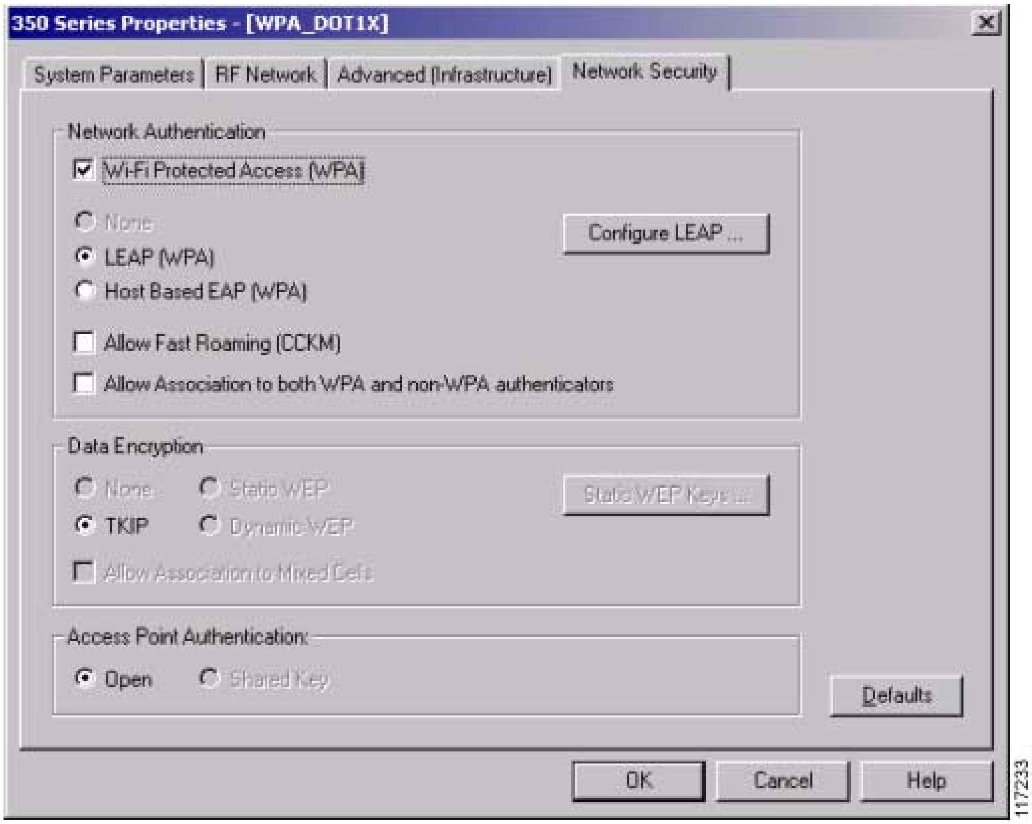
Step 12 To activate WPA on a client device, first make sure that the client is equipped with the appropriate drivers, firmware, and Aironet Client Utility version. (See the "Wireless LAN Client Adapter Requirements" section on page 2.)

Step 13 Make sure that the client is configured for Cisco LEAP (or another) authentication, the correct SSID is entered under System Parameters, and the Cisco LEAP authentication credentials under Configure LEAP are correct.

Step 14 On the Network Security tab, check the **Wi-Fi Protected Access (WPA)** check box under Network Authentication.

> **Note** This selection automatically forces the selection of **LEAP (WPA)** and **Data Encryption** > **TKIP** (see Figure 49).

Figure 49   Aironet Client Utility Version 6.2 WPA Configuration



Network Authentication

☑ Wi-Fi Protected Access (WPA)

○ None
● LEAP (WPA)
○ Host Based EAP (WPA)

□ Allow Fast Roaming (CCKM)
□ Allow Association to both WPA and non-WPA authenticators

Data Encryption

○ None ○ Static WEP
● TKIP ○ Dynamic WEP

□ Allow Association to Mixed Cells

Access Point Authentication:

● Open ○ Shared Key

Step 15 Click **OK** to activate the changes.

Step 16 After client authentication, the use of WPA and the TKIP cipher may be verified by using the Association table or the **show dot11 association <client MAC>** command.

Appendix A: Verifying the Firmware and Driver Versions

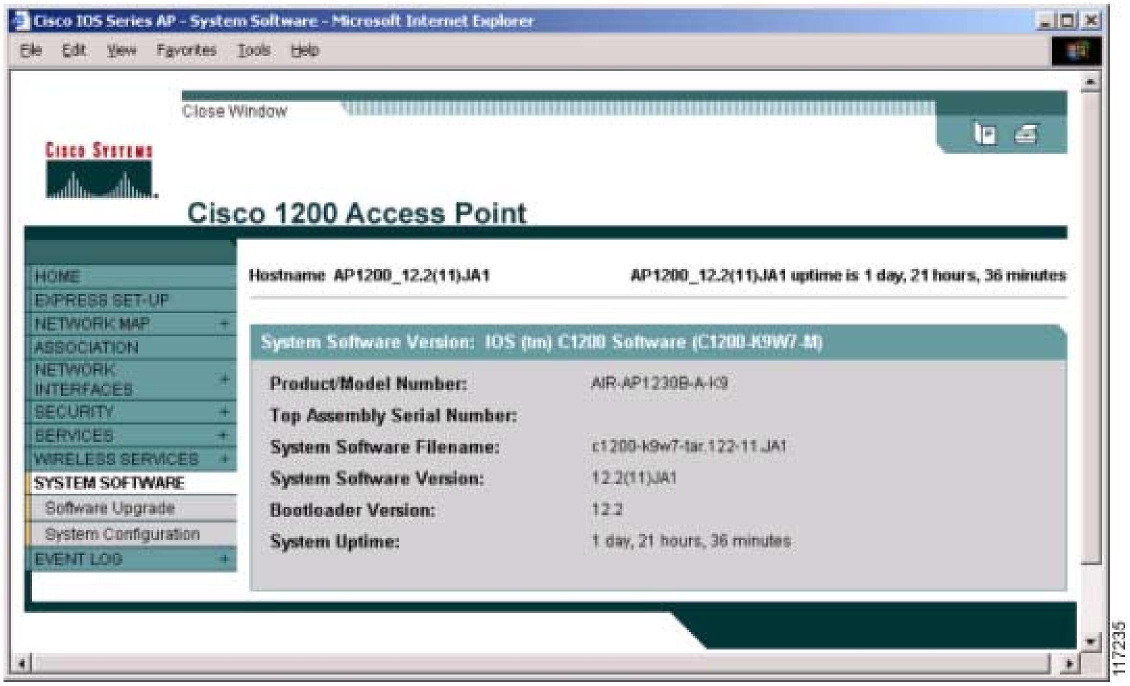
Verifying the Access Point Firmware Version

Step 1 Browse, Telnet, or console to the access point.

Step 2 Verify the access point’s Cisco IOS Software Release number by using the **System Software** option (see Figure 50).

Note You can also verify the Cisco IOS Software Release number from the access point’s command line by using the **show version** command, as in other Cisco IOS Software products.

Figure 50 Access Point Software Version Verification - Cisco IOS Software



Hostname AP1200_12.2(11)JA1

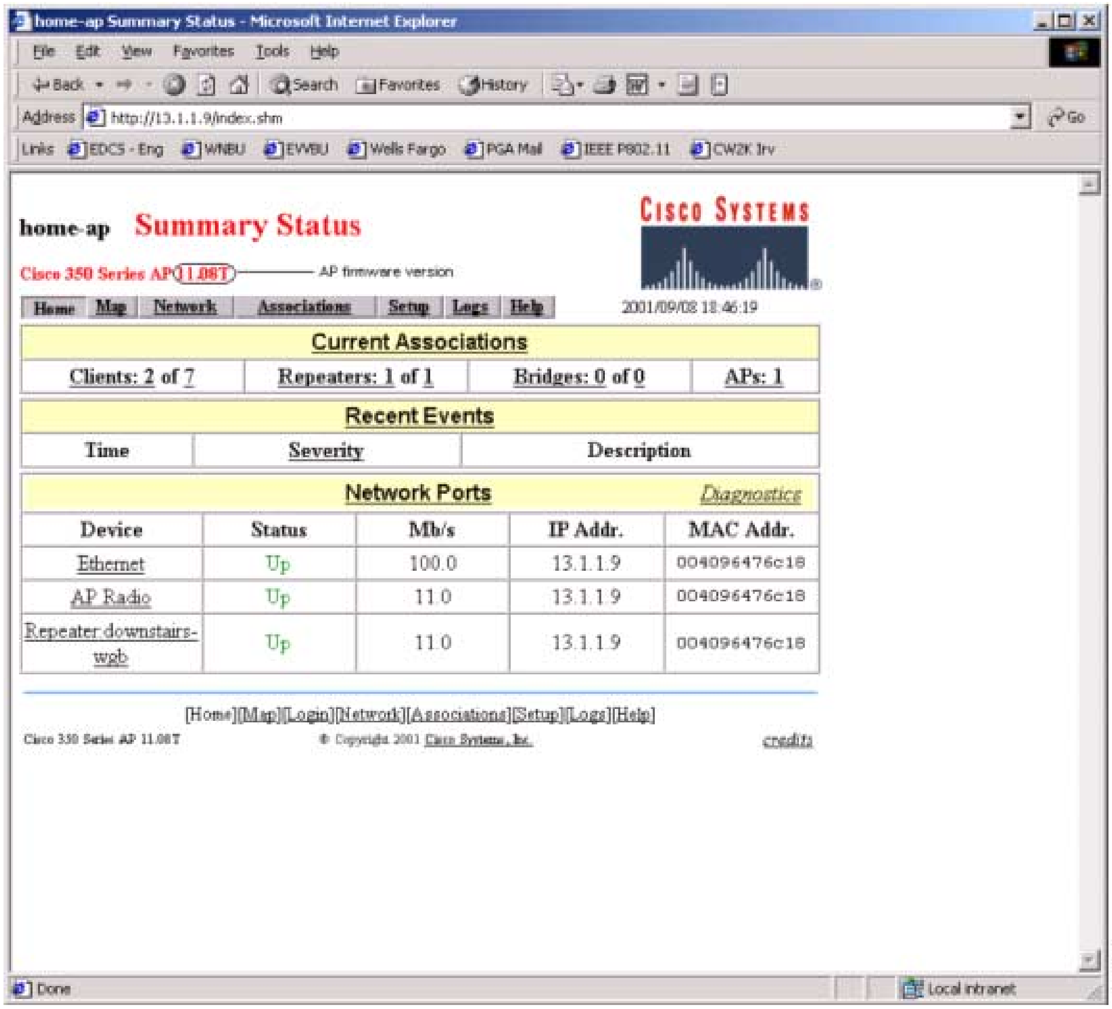
AP1200_12.2(11)JA1 uptime is 1 day, 21 hours, 36 minutes

System Software Version: IOS (tm) C1200 Software (C1200-K9W7-M)

Product/Model Number:	AIR-AP1230B-A-K9
Top Assembly Serial Number:	
System Software Filename:	c1200-k9w7-tar.122-11.JA1
System Software Version:	12.2(11)JA1
Bootloader Version:	12.2
System Uptime:	1 day, 21 hours, 36 minutes

Step 3 Refer to Figure 51 to see where to find the firmware version number for a VxWorks access point using HTTP.

Figure 51 Access Point Software Version Verification - VxWorks (HTTP)


home-ap Summary Status - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://13.1.1.9/index.shm
Go
Links EDCS - Eng WNBU EWBU Wells Fargo PGA Mail IEEE P802.11 CW2K Irv
Cisco Systems
Home Map Network Associations Setup Logs Help
Done
Local intranet
117236

home-ap Summary Status

Cisco 350 Series AP 11.08T — AP firmware version

2001/09/08 18:46:19

Current Associations			
Clients: 2 of 7	Repeaters: 1 of 1	Bridges: 0 of 0	APs: 1

Recent Events		
Time	Severity	Description

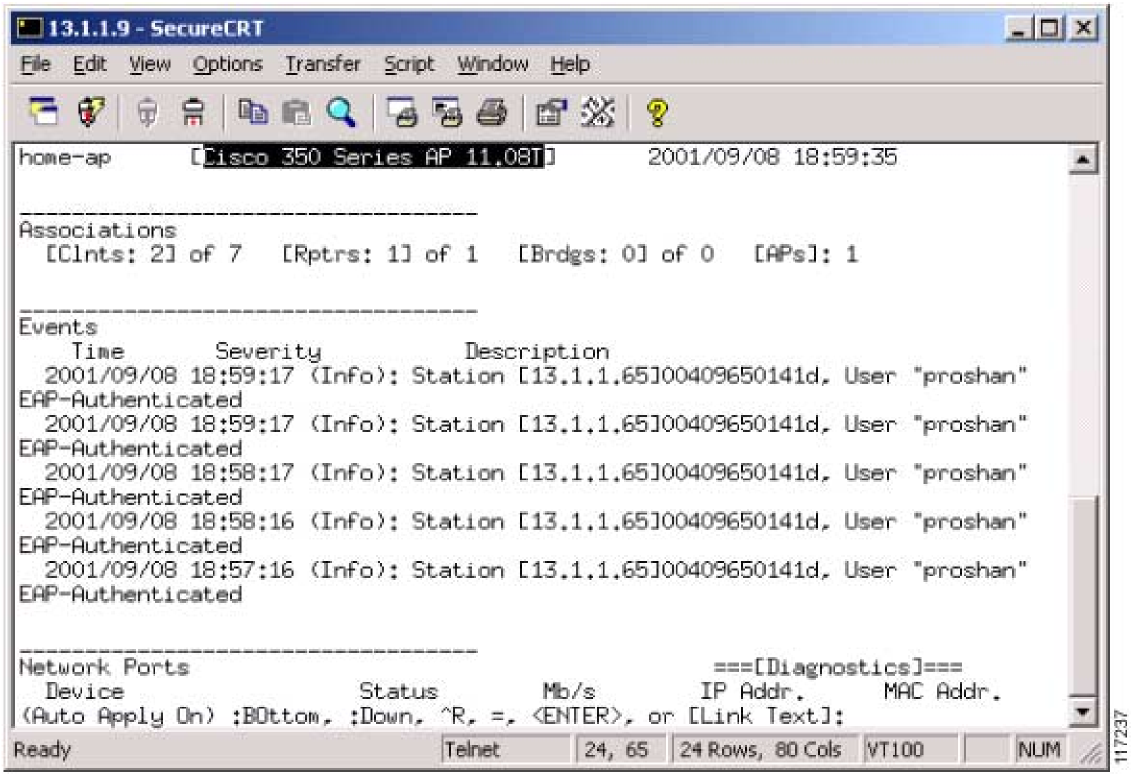
Network Ports				Diagnostics
Device	Status	Mb/s	IP Addr.	MAC Addr.
Ethernet	Up	100.0	13.1.1.9	004096476c18
AP Radio	Up	11.0	13.1.1.9	004096476c18
Repeater downstairs-wgb	Up	11.0	13.1.1.9	004096476c18

[Home][Map][Login][Network][Associations][Setup][Logs][Help]

Cisco 350 Series AP 11.08T © Copyright 2001 Cisco Systems, Inc. credits

Step 4 Refer to Figure 52 to see where to find the firmware version number for a VxWorks access point using Telnet or the console port.

Figure 52 Access Point Software Version Verification - VxWorks (Telnet/Console)



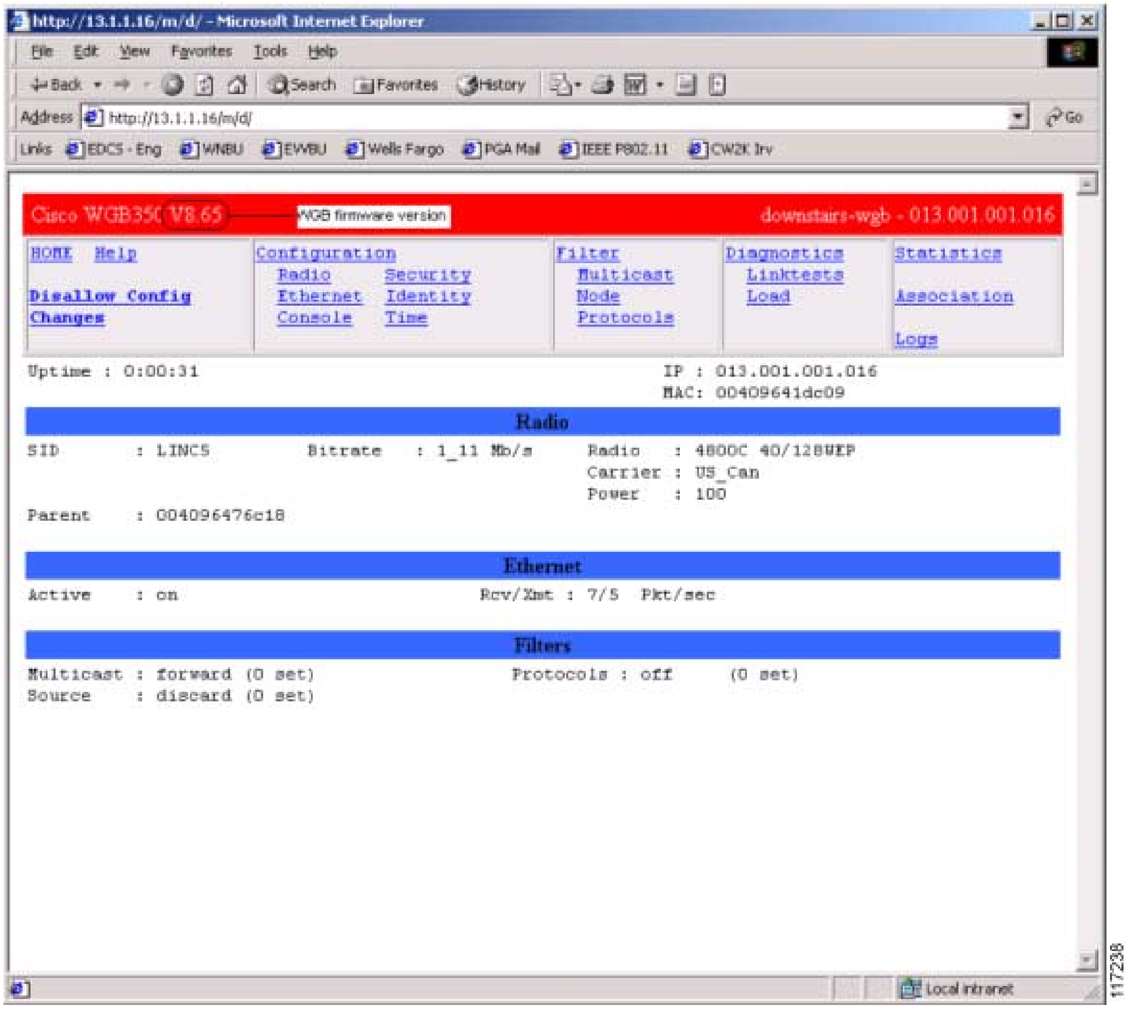
```
home-ap       [Cisco 350 Series AP 11.08T]       2001/09/08 18:59:35

-----------------------------------
Associations
  [Clnts: 2] of 7   [Rptrs: 1] of 1   [Brdgs: 0] of 0   [APs]: 1

-----------------------------------
Events
    Time       Severity          Description
  2001/09/08 18:59:17 (Info): Station [13.1.1.65]00409650141d, User "proshan"
EAP-Authenticated
  2001/09/08 18:59:17 (Info): Station [13.1.1.65]00409650141d, User "proshan"
EAP-Authenticated
  2001/09/08 18:58:17 (Info): Station [13.1.1.65]00409650141d, User "proshan"
EAP-Authenticated
  2001/09/08 18:58:16 (Info): Station [13.1.1.65]00409650141d, User "proshan"
EAP-Authenticated
  2001/09/08 18:57:16 (Info): Station [13.1.1.65]00409650141d, User "proshan"
EAP-Authenticated

-----------------------------------
Network Ports                                  ===[Diagnostics]===
  Device                  Status        Mb/s        IP Addr.      MAC Addr.
(Auto Apply On) :BOttom, :Down, ^R, =, <ENTER>, or [Link Text]:
```

Verifying the Workgroup Bridge Firmware Version

Step 1 Browse to the workgroup bridge.

Step 2 Refer to Figure 53 to see where to find the firmware version number for a workgroup bridge using HTTP.

Figure 53 Workgroup Bridge Software Version Verification


http://13.1.1.16/m/d/ - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://13.1.1.16/m/d/
Go
Links EDCS - Eng WNBU EWBU Wells Fargo PGA Mail IEEE P802.11 CW2K Irv
WGB firmware version
HOME Help
Disallow Config Changes
Configuration Radio Security Ethernet Identity Console Time
Filter Multicast Node Protocols
Diagnostics Linktests Load
Statistics Association Logs
Local intranet
117238

Cisco WGB350 V8.65 downstairs-wgb - 013.001.001.016

```
Uptime : 0:00:31                                     IP : 013.001.001.016
                                                     MAC: 00409641dc09
                                  Radio
SID       : LINCS        Bitrate    : 1_11 Mb/s      Radio   : 4800C 40/128WEP
                                                     Carrier : US_Can
                                                     Power   : 100
Parent    : 004096476c18

                                 Ethernet
Active    : on                                  Rcv/Xmt : 7/5   Pkt/sec

                                  Filters
Multicast : forward (0 set)                        Protocols : off     (0 set)
Source    : discard (0 set)
```

Verifying the Client Driver and Firmware Versions

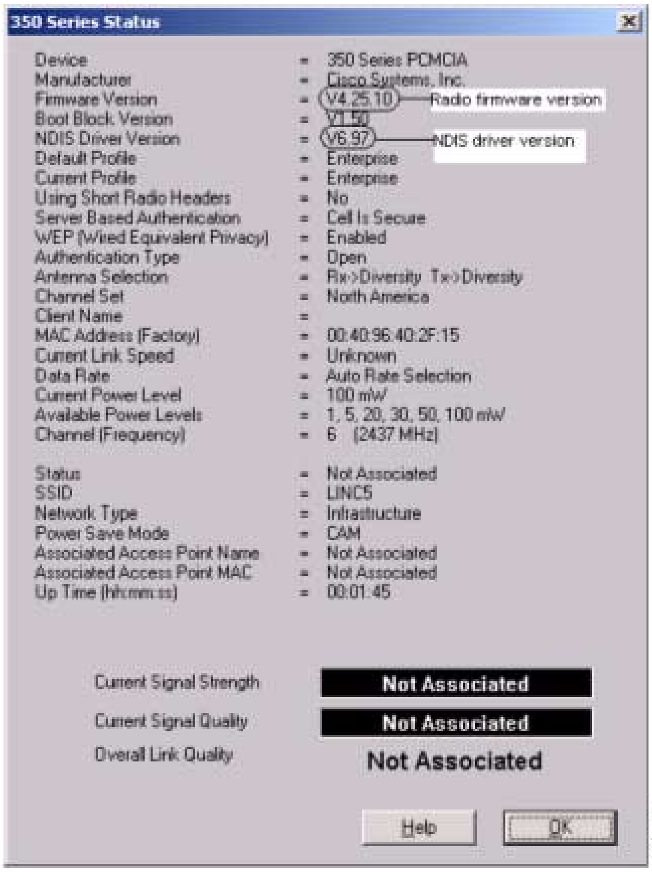
Windows Verification

Step 1 Open the Aironet Client Utility.

Step 2 Click the **Status** icon.

Step 3 Refer to Figure 54 to see where to find the client firmware and driver version numbers.

Figure 54 Verification of Client Firmware and Driver Versions - Windows



```
350 Series Status

Device                                =  350 Series PCMCIA
Manufacturer                          =  Cisco Systems, Inc.
Firmware Version                      =  V4.25.10
Boot Block Version                    =  V1.50
NDIS Driver Version                   =  V6.97
Default Profile                       =  Enterprise
Current Profile                       =  Enterprise
Using Short Radio Headers             =  No
Server Based Authentication           =  Cell Is Secure
WEP (Wired Equivalent Privacy)        =  Enabled
Authentication Type                   =  Open
Antenna Selection                     =  Rx>Diversity  Tx>Diversity
Channel Set                           =  North America
Client Name                           =
MAC Address (Factory)                 =  00:40:96:40:2F:15
Current Link Speed                    =  Unknown
Data Rate                             =  Auto Rate Selection
Current Power Level                   =  100 mW
Available Power Levels                =  1, 5, 20, 30, 50, 100 mW
Channel (Frequency)                   =  6   (2437 MHz)

Status                                =  Not Associated
SSID                                  =  LINC5
Network Type                          =  Infrastructure
Power Save Mode                       =  CAM
Associated Access Point Name          =  Not Associated
Associated Access Point MAC           =  Not Associated
Up Time (hh:mm:ss)                    =  00:01:45

        Current Signal Strength          Not Associated
        Current Signal Quality           Not Associated
        Overall Link Quality             Not Associated
```

Radio firmware version

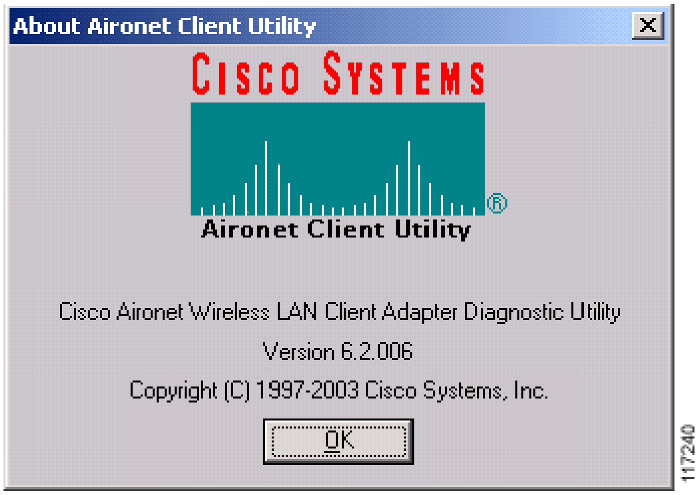
NDIS driver version

Step 4 Click **OK** to close the Status window.

Step 5 Click the **About** icon.

Step 6 Refer to Figure 55 to see where to find the Aironet Client Utility version number.

Figure 55 Verification of Aironet Client Utility Version - Windows



About Aironet Client Utility

Cisco Aironet Wireless LAN Client Adapter Diagnostic Utility

Version 6.2.006

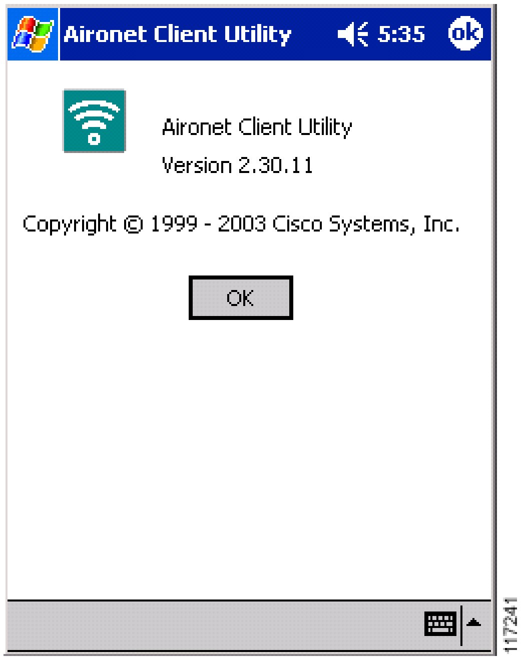
Copyright (C) 1997-2003 Cisco Systems, Inc.

Windows CE Verification

Step 1 Launch the Aironet Client Utility on your Windows CE device.

Step 2 Tap **About** to find the Aironet Client Utility version (see Figure 56).

Figure 56 Verification of Aironet Client Utility Version - Windows CE



Aironet Client Utility

Version 2.30.11

Copyright © 1999 - 2003 Cisco Systems, Inc.