Configuring Funk RADIUS to Authenticate Cisco Wireless Clients With LEAP

Document ID: 44900

Contents

Introduction

This document describes how to configure 340 and 350 Series access points and 350 Series bridges. It also describes how the Funk Software, Inc.   product, Steel−Belted Radius, works together with Light Extensible Authentication Protocol (LEAP) to authenticate a Cisco wireless client.

Note: The portions of this document that refer to non−Cisco products were written based on experience the author had with that non−Cisco product, not on formal training. They are intended for the convenience of Cisco customers, not as technical support. For authoritative technical support on non−Cisco products, contact the product technical support for the vendor.

Prerequisites

Requirements

The information presented in this document assumes that the Funk Software, Inc. product, Steel−Belted Radius, is successfully installed and working properly. It also assumes that you are gaining administrative access to the access point or to the bridge through the browser interface.

Components Used

The information in this document is based on the Cisco Aironet 340 and 350 Series access points and 350 Series bridges. The information in this document applies to all VxWorks firmware versions 12.01T and later.

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

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Configuration

Configuring the Access Point or Bridge

Complete these steps to configure the access point or bridge.

    1. From the Summary Status page, complete these steps:

        a. Click **Setup**.
        b. Click **Security**.
        c. Click **Radio Data Encryption (WEP)**.
        d. Enter a random WEP Key (26 hexadecimal characters) in the WEP Key 1 slot.
        e. Set the Key Size to **128 bit**.
        f. Click **Apply**.

        g. Click **OK**.
        h. Change the option **Use of Data Encryption by Stations is:** to **Full Encryption**.
        i. Check the **Open** and **Network EAP** boxes on the **Accept Authentication Type** line.

BR350-to-Radius   **Root Radio Data Encryption**   CISCO SYSTEMS

Cisco 350 Series Bridge 12.03T

Map   Help   2003/07/10 09:30:53

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 ▼

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

	Transmit With Key	Encryption Key	Key Size
WEP Key 1:	◉		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.

Apply   OK   Cancel   Restore Defaults

[Map][Login][Help]

Cisco 350 Series Bridge 12.03T   ® Copyright 2002 Cisco Systems, Inc.   credits

    j. Click **OK**.
2. From the Security Setup page, click **Authentication Server** and make these entries on the page:

    a. **Server Name/IP**: Enter the IP address or host name of the RADIUS server.
    b. **Shared Secret**: Enter the exact string as the one on the RADIUS server for this access point or bridge.
    c. On the **Use server for:** line for this RADIUS server, check the **EAP Authentication** check box.

BR350-to-Radius Authenticator Configuration

Cisco 350 Series Bridge 12.03T

CISCO SYSTEMS

Map Help   2003/07/10 09:45:11

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
172.30.1.124	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.

Apply   OK   Cancel   Restore Defaults

[Map][Login][Help]

Cisco 350 Series Bridge 12.03T   © Copyright 2002 Cisco Systems, Inc.   credits

3. When you have configured the parameters in Step 2, click **OK**.

With these settings, the access point or bridge is ready to authenticate LEAP clients against a RADIUS server.

Configuring the Funk Software, Inc. Product, Steel−Belted Radius

Complete the steps in the next procedure to configure the Funk Software, Inc. product, Steel−Belted Radius, to communicate with the access point or bridge. For more complete information on the server, refer to Funk Software .

Note: The portions of this document that refer to non−Cisco products were written based on experience the author had with that non−Cisco product, not on formal training. They are intended for the convenience of Cisco customers, not as technical support. For authoritative technical support on non−Cisco products, contact the product technical support for the vendor.

1. On the RAS Clients menu, click **Add** to create a new RAS Client.

Add New RAS Client

Client name:

☐ Any RAS client

OK   Cancel

2. Configure the parameters for client name, IP address and make/model.

   a. **Client Name**: Enter the name of the access point or bridge.
   b. **IP Address**: Enter the address of the access point or bridge that communicates with Steel−Belted Radius.

Note: The RADIUS server views the access point or bridge as a RADIUS client.

   c. **Make/model**: Select **Cisco Aironet Access Point**.
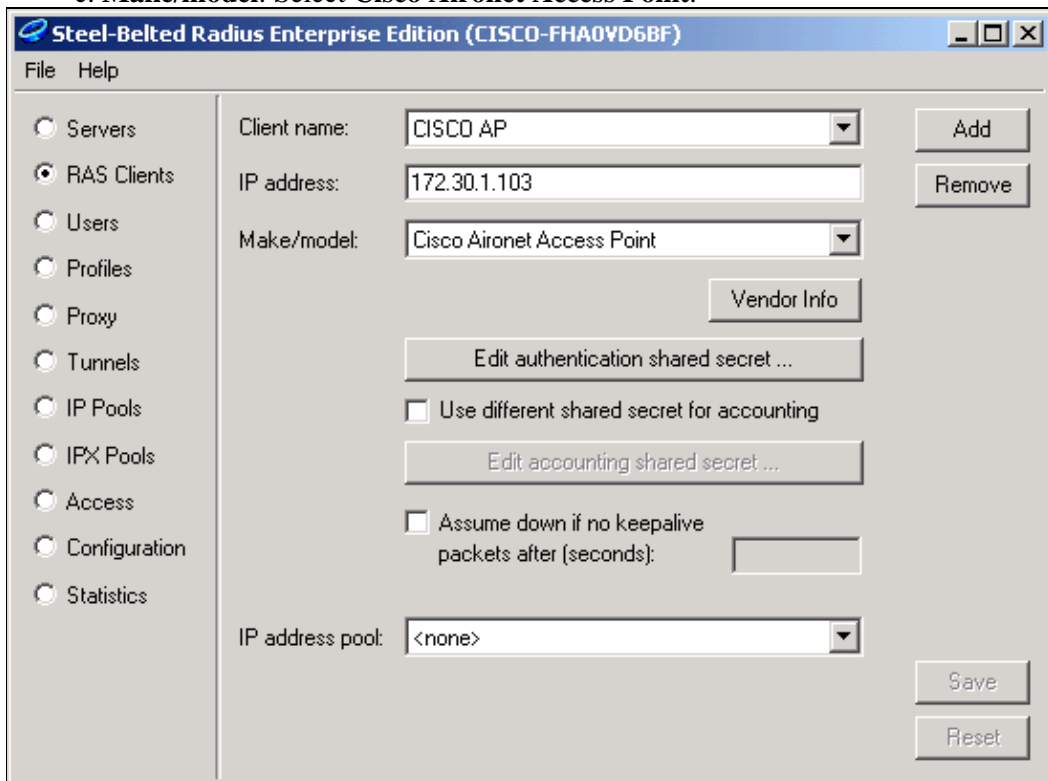
3. Click **Edit authentication shared secret**.
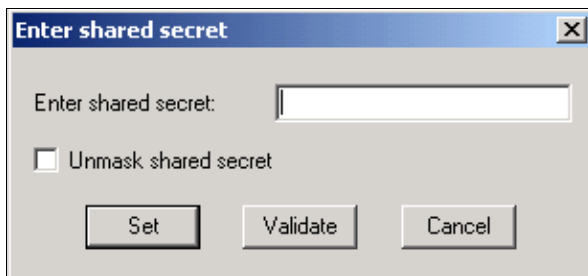
   a. Enter the exact string as the one on the access point or bridge for this server.

   b. Click **Set** to return to the previous dialog box.

   c. Click **Save**.

4. Look for the EAP.INI file that is located in the installation folder for Steel–Belted Radius (on a Windows–based PC, this file is normally located in **C:\Radius\Services**).

5. Verify that LEAP is an option for `EAP-Type`.

A sample file looks similar to this:

```
[Native-User]
EAP-Only = 0
First-Handle-Via-Auto-EAP = 0
EAP-Type = LEAP, TTLS
```

6. Save the modified EAP.INI file.

7. Stop and restart the RADIUS Service.

## Creating Users in Steel–Belted Radius

This section describes how to create a new native (local) user with the Funk Software, Inc. product, Steel–Belted Radius. If a Domain or Workgroup user needs to be added, contact Funk Software for

assistance. Native user entries require that the user s name and password be entered into the Steel–Belted Radius local database. For all other types of User entries, Steel–Belted Radius relies on another database to validate the credentials of a user.
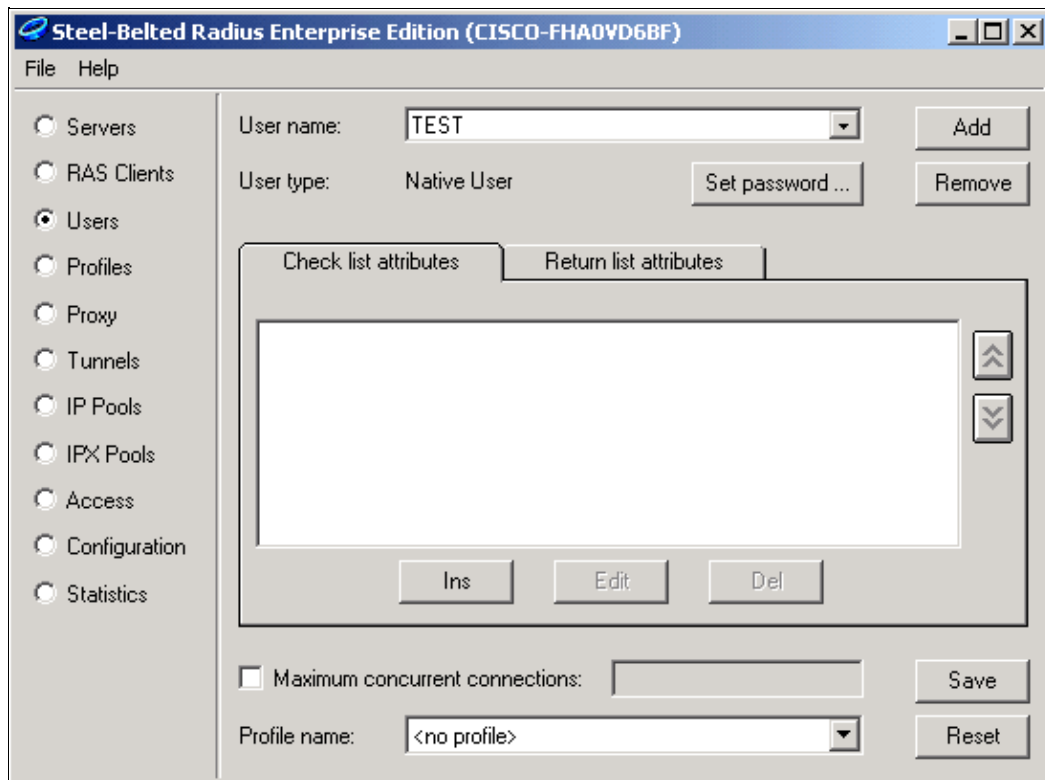
Complete these steps to configure a Native user in Steel–Belted Radius:

1. On the Users menu, click **Add** to create a new user.
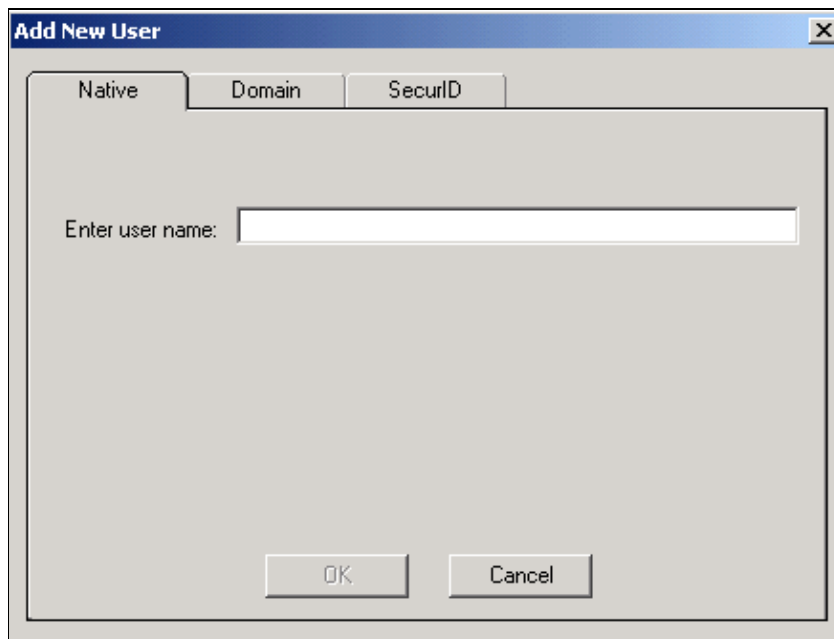
2. Click the **Native** tab, enter the user name into the field, and click **OK**.

   The Add New User dialog box closes.
3. In the Users dialog box, select the user and click **Set Password**.

4. Enter the password for the user and click **Set**.

5. In the Users dialog box, click **Save** and you have created the user.

Related Information

- **Security Setup**
- **Funk Software**
- **Wireless LAN (WLAN)**
- **Technical Support – Cisco Systems**

Updated: Apr 12, 2006   Document ID: 44900