

配置Funk RADIUS认证有LEAP的Cisco无线客户端

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[配置](#)

[配置接入点或网桥](#)

[配置Funk软件， Inc. Product， 钢围绕的Radius](#)

[创建钢围绕的Radius的用户](#)

[相关信息](#)

简介

本文描述如何配置340和350系列接入点和350系列网桥。它如何与小型可扩展认证协议(LEAP)一起也描述[Funk软件](#)，公司产品，钢围绕的Radius，工作验证Cisco无线客户端。

注意： 参考非Cisco的产品本文的部分写入基于体验作者有与该非思科产品，不在正式培训。他们打算为Cisco用户方便起见，不作为技术支持。对于在非Cisco的产品的授权技术支持，请与供应商的产品支持联系。

先决条件

要求

本文提供的信息假设， Funk软件，公司产品，钢围绕的Radius，顺利地安装和工作正常。它也假设，您通过浏览器接口获得管理访问对接入点或对网桥。

使用的组件

本文档中的信息根据Cisco Aironet 340及350系列接入点和350系列网桥。本文档中的信息运用对所有VxWorks固件版本12.01T和以后。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

配置

配置接入点或网桥

完成这些步骤配置接入点或网桥。

1. 从Summary Status页，请完成这些步骤：单击**设置**。单击 **Security**。单击 **Radio Data Encryption (WEP)**。输入一把随机的WEP密钥(26十六进制字符)在WEP密钥1 slot。设置密钥大小为**128位**。单击 **Apply**。

BR350-CLEAR Root Radio Data Encryption **CISCO SYSTEMS**

Cisco 350 Series Bridge 12.03T

Map Help Uptime: 01:45:05

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: Not Available
Must set an Encryption Key or enable Broadcast Key Rotation first

Accept Authentication Type: Open Shared Network-EAP
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

单击 **Ok**。由站点更改选项**Use of Data Encryption**是：对完全加密。检查在**Accept Authentication Type**线路的开放和网络**EAP**方框。



[Map](#) [Help](#)

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:

	Open	Shared	Network-EAP
Accept Authentication Type:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Require EAP:	<input type="checkbox"/>	<input type="checkbox"/>	

	Transmit With Key	Encryption Key	Key Size
WEP Key 1:	<input checked="" type="radio"/>	<input type="text"/>	<input type="text" value="128 bit"/>
WEP Key 2:	<input type="radio"/>	<input type="text"/>	<input type="text" value="not set"/>
WEP Key 3:	<input type="radio"/>	<input type="text"/>	<input type="text" value="not set"/>
WEP Key 4:	<input type="radio"/>	<input type="text"/>	<input type="text" value="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.

[\[Map\]](#)[\[Login\]](#)[\[Help\]](#)

单击 Ok。

- 从Security Setup页，请点击**认证服务器**并且做这些条目在页：**服务器名/IP**：输入RADIUS服务器的IP地址或主机名。共享密钥:输入确切的字符串作为那个在此接入点或网桥的RADIUS服务器。在**使用服务器上**为：此RADIUS服务器的线路，检查**EAP Authentication**复选框。

BR350-to-Radius Authenticator Configuration CISCO SYSTEMS

Cisco 350 Series Bridge 12.03T 2003/07/10 09:45:11

Map Help

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: <input checked="" type="checkbox"/> EAP Authentication <input type="checkbox"/> MAC Address Authentication <input type="checkbox"/> User Authentication <input type="checkbox"/> MIP Authentication					
	RADIUS	1812	*****	5	3
Use server for: <input checked="" type="checkbox"/> EAP Authentication <input type="checkbox"/> MAC Address Authentication <input type="checkbox"/> User Authentication <input type="checkbox"/> MIP Authentication					
	RADIUS	1812	*****	5	3
Use server for: <input checked="" type="checkbox"/> EAP Authentication <input type="checkbox"/> MAC Address Authentication <input type="checkbox"/> User Authentication <input type="checkbox"/> MIP Authentication					
	RADIUS	1812	*****	5	3
Use server for: <input checked="" type="checkbox"/> EAP Authentication <input type="checkbox"/> MAC Address Authentication <input type="checkbox"/> User Authentication <input type="checkbox"/> 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

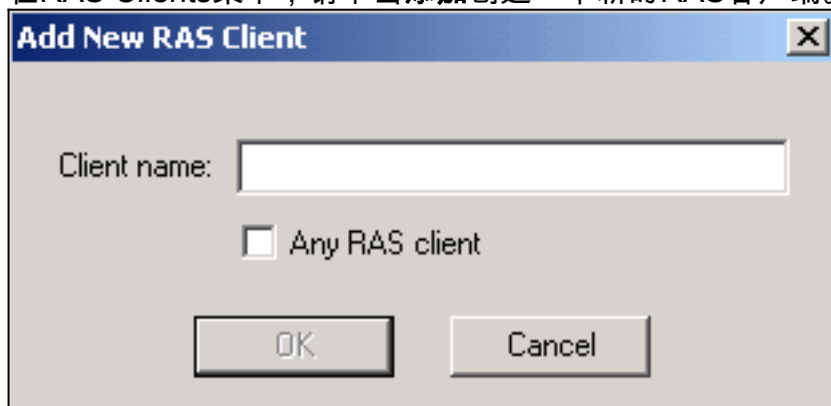
3. 当您配置在步骤2时的参数，请点击OK键。使用这些设置，接入点或网桥准备利用RADIUS服务器验证LEAP客户端。

配置Funk软件， Inc. Product， 钢围绕的Radius

完成在下一个步骤的步骤配置Funk软件，公司产品，钢围绕的Radius，用接入点或网桥通信。关于服务器的更全面的信息，参考[Funk软件](#)。

注意： 参考非Cisco的产品本文的部分写入基于体验作者有与该非思科产品，不在正式培训。他们打算为Cisco用户方便起见，不作为技术支持。对于在非Cisco的产品的授权技术支持，请与供应商的产品支持联系。

1. 在RAS Clients菜单，请单击**添加**创建一个新的RAS客户端。



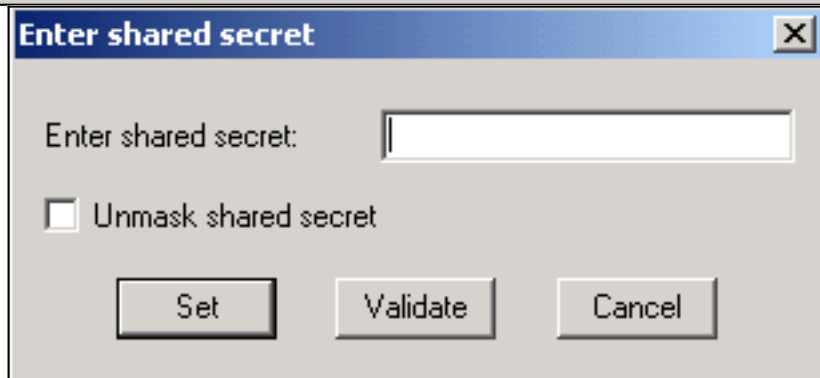
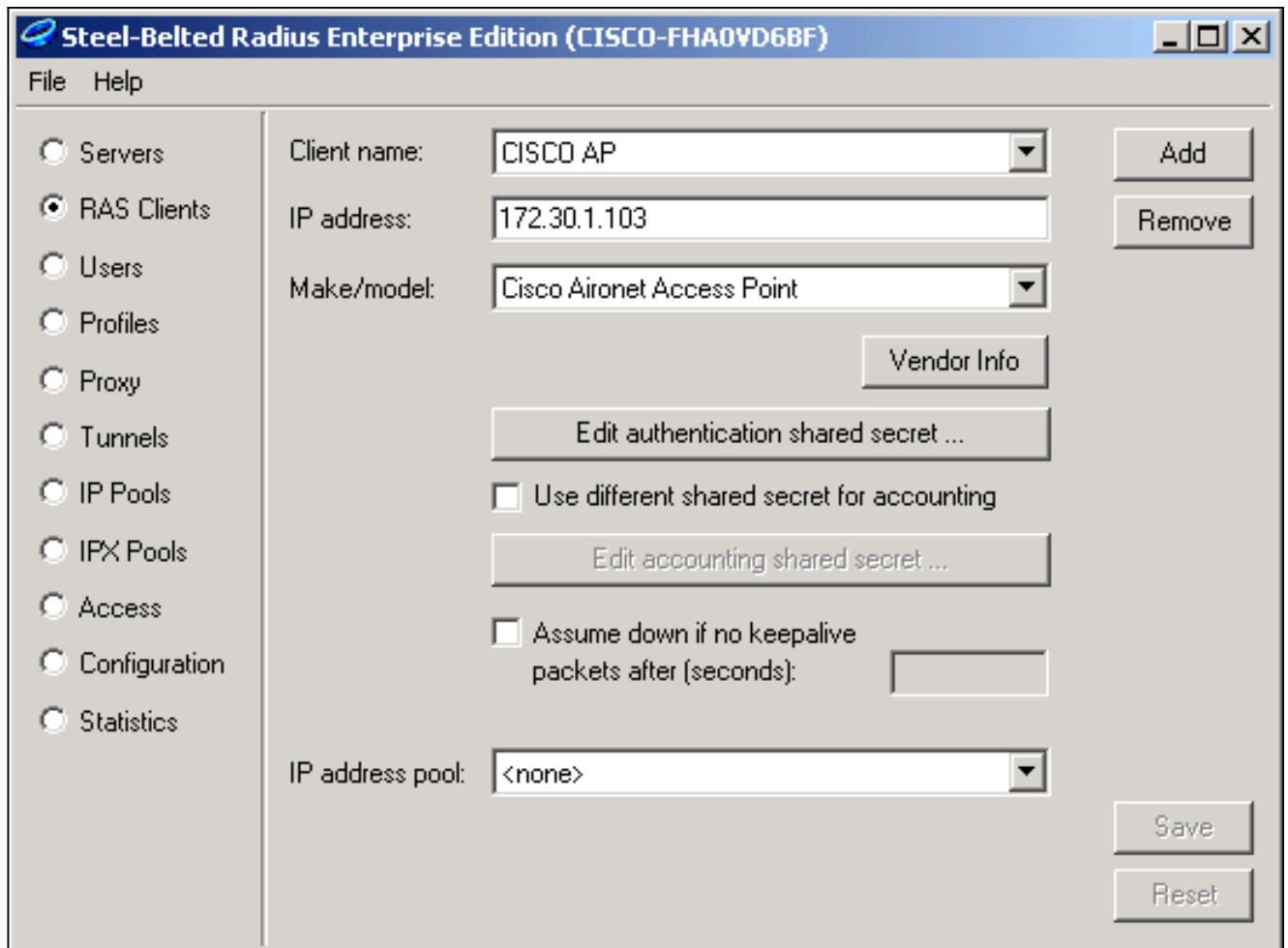
Add New RAS Client

Client name:

Any RAS client

OK Cancel

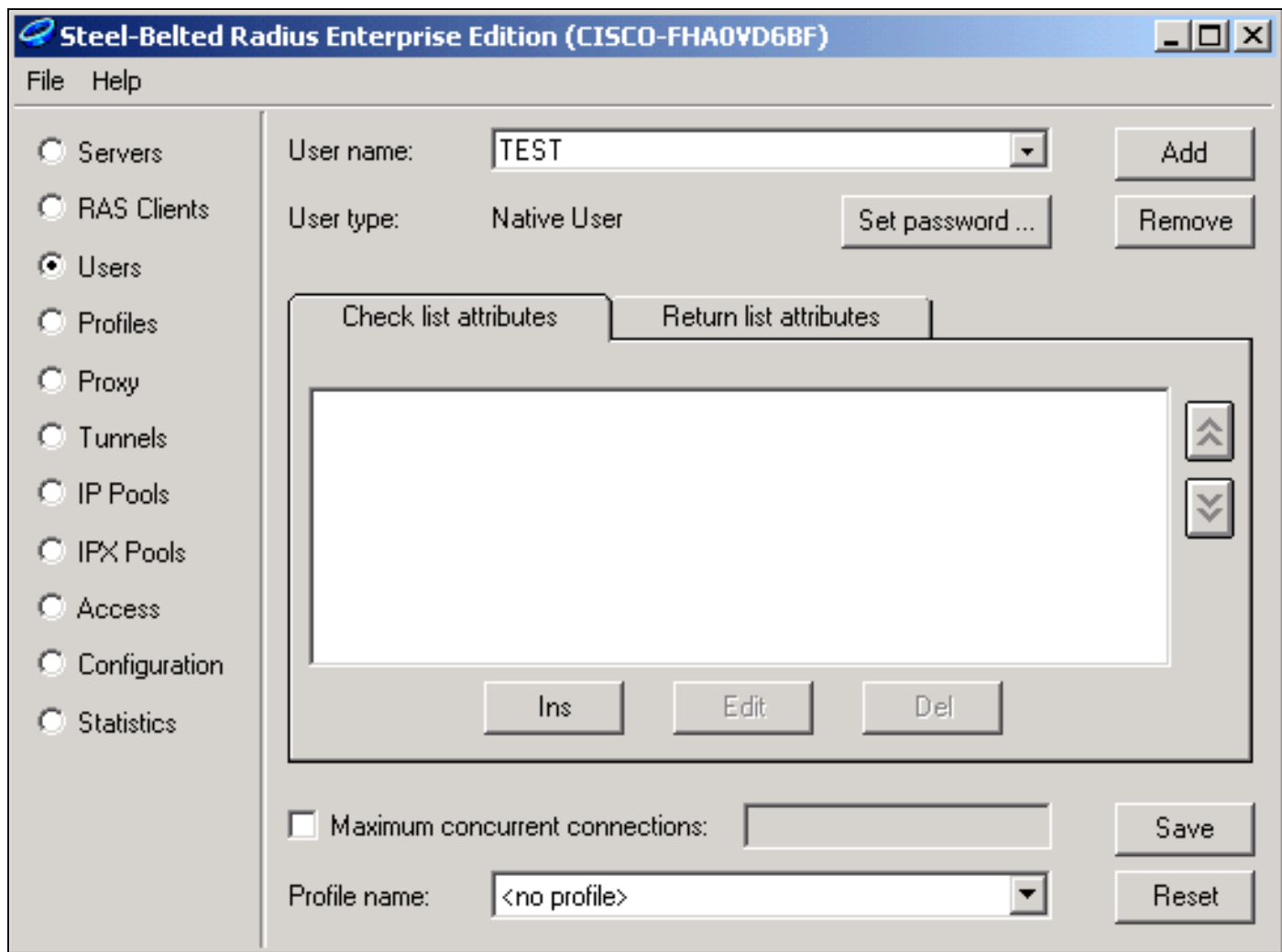
2. 配置客户端名称的参数，IP地址并且做/型号。**客户端名称**：输入接入点或网桥的名称。IP地址：输入与钢围绕的Radius联络接入点或网桥的地址。**注意**：RADIUS服务器观看接入点或网桥作为RADIUS客户端。**做/型号**：选择Cisco Aironet接入点。



3. 单击**编辑验证共享的机密**。输入确
切的字符串作为那个在接入点或网桥此服务器的。点击**集**返回到上一个对话框。单击 **Save**。
4. 寻找在钢围绕的Radius的安装文件夹查找的EAP.INI文件(在基于Windows个人计算机，此文件在C:\Radius\Services通常查找)。
5. 验证LEAP是EAP一个选项。示例文件看起来类似于此：`[Native-User]`
`EAP-Only = 0`
`First-Handle-Via-Auto-EAP = 0`
`EAP-Type = LEAP, TTLS`
6. 保存已修改EAP.INI文件。
7. 终止并且重新启动RADIUS服务。

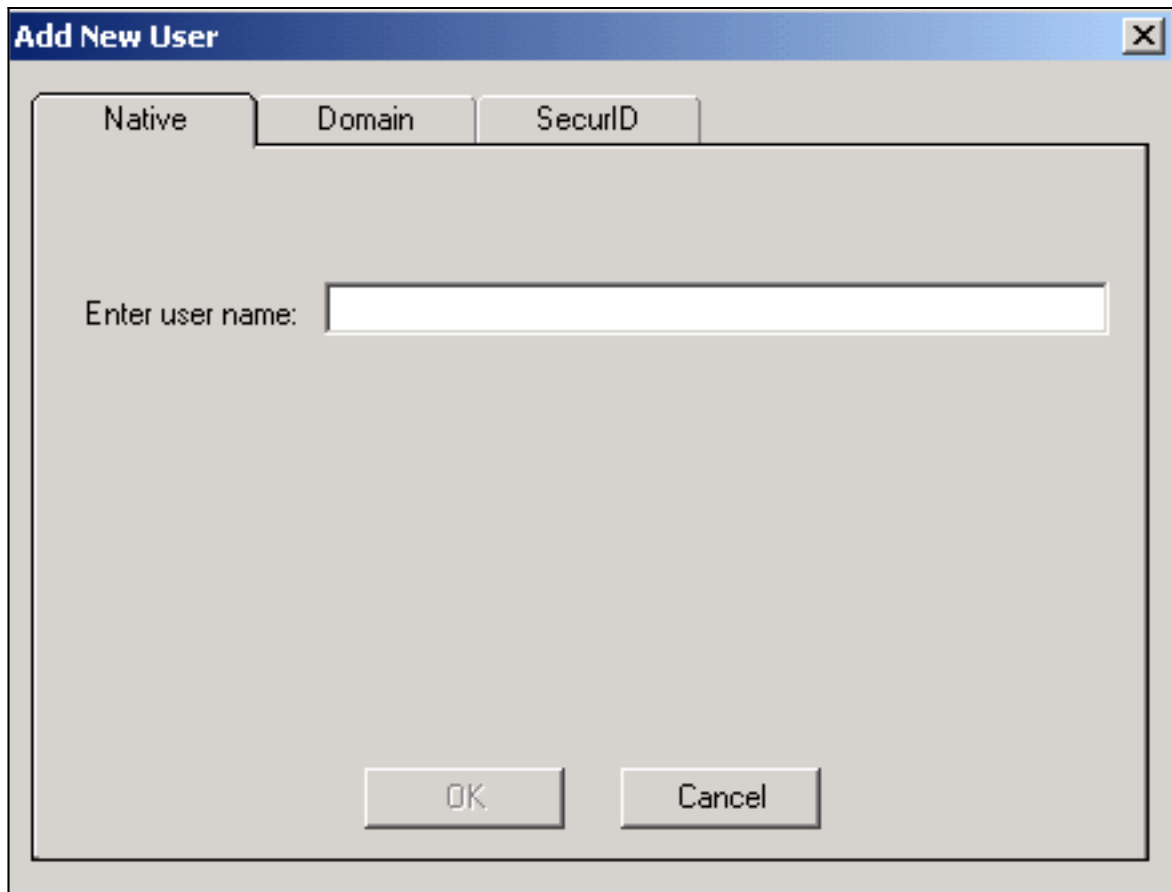
创建钢围绕的Radius的用户

此部分描述如何创建有Funk软件的一个新的本地(本地)用户，公司产品，钢围绕的Radius。如果域或工作组用户需要被添加，请与 协助的[Funk软件联系](#)。[本地用户输入要求用户名和密码输入到钢围绕的Radius本地数据库。对于用户输入的其他类型，钢围绕的Radius依靠另一个数据库验证用户的凭证。](#)



完成这些步骤配置钢围绕的Radius的一个本地用户：

1. 在Users菜单，请单击**添加**创建新用户。



2. 点击**Native**选项，输入用户名到字段，并且点击OK键。添加新用户对话框关闭。
3. 在用户对话框中，请选择用户并且点击**Set password**。



4. 输入用户的密码并且点击**集**。
5. 在用户对话框中，请点击“**Save**”，并且您创建用户。

[相关信息](#)

- [安全设置](#)
- [Funk软件](#)
- [无线局域网\(WLAN\)](#)
- [技术支持 - Cisco Systems](#)