

Configurando o Funk RADIUS para Autenticar Cisco Wireless Clients com LEAP

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Conventions](#)

[Configuração](#)

[Configurando o ponto de acesso ou a ponte](#)

[Configurando o produto Funk Software, Inc., Steel-Belted Radius](#)

[Criando usuários no Raio de Cinto de Aço](#)

[Informações Relacionadas](#)

[Introduction](#)

Este documento descreve como configurar access points 340 e 350 Series e 350 Series Bridges. Ele também descreve como o [Funk Software, Inc.](#), produto Steel-Belted Radius, trabalha junto com o Light Extensible Authentication Protocol (LEAP) para autenticar um cliente sem fio da Cisco.

Observação: as partes deste documento que se referem a produtos que não são da Cisco foram escritas com base na experiência que o autor teve com esse produto que não é da Cisco, e não em treinamento formal. Eles se destinam à conveniência dos clientes da Cisco, não como suporte técnico. Para obter suporte técnico oficial sobre produtos que não são da Cisco, entre em contato com o suporte técnico do produto para o fornecedor.

[Prerequisites](#)

[Requirements](#)

As informações apresentadas neste documento pressupõem que o produto Funk Software, Inc., Steel-Belted Radius, foi instalado e está funcionando corretamente. Ele também pressupõe que você esteja obtendo acesso administrativo ao ponto de acesso ou à ponte por meio da interface do navegador.

[Componentes Utilizados](#)

As informações neste documento são baseadas nos access points Cisco Aironet 340 e 350 Series e nas bridges 350 Series. As informações neste documento se aplicam a todas as versões

de firmware 12.01T e posteriores do VxWorks.

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](#).

Configuração

Configurando o ponto de acesso ou a ponte

Conclua estes passos para configurar o ponto de acesso ou ponte.

1. Na página Status do resumo, faça o seguinte:Clique em Setup.Clique em **Segurança**.Clique em Radio Data Encryption (WEP).Insira uma chave WEP aleatória (26 caracteres hexadecimais) no slot WEP Key 1.Defina o tamanho da chave como **128 bits**.Clique em 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](#)

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

Click **OK**. Altere a opção **Usar a criptografia de dados por estações é: para Criptografia completa**. Marque as caixas **Open** e **Network EAP** na linha **Accept Authentication Type**.



[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.

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

Click **OK**.

- Na página Security Setup (Configuração de segurança), clique em **Authentication Server (Servidor de autenticação)** e faça as seguintes entradas na página:
 - Nome do servidor/IP:** Insira o endereço IP ou o nome do host do servidor RADIUS.
 - shared secret:** Digite a string exata como a do servidor RADIUS para este ponto de acesso ou ponte.
 - No servidor Use para:** para este servidor RADIUS, marque a caixa de seleção **EAP Authentication**.

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](#)

- Quando tiver configurado os parâmetros na Etapa 2, clique em **OK**. Com essas configurações, o ponto de acesso ou ponte está pronto para autenticar clientes LEAP em um servidor RADIUS.

[Configurando o produto Funk Software, Inc., Steel-Belted Radius](#)

Conclua as etapas do próximo procedimento para configurar o produto Funk Software, Inc., Steel-Belted Radius, para se comunicar com o ponto de acesso ou ponte. Para obter informações mais completas sobre o servidor, consulte [Funk Software](#).

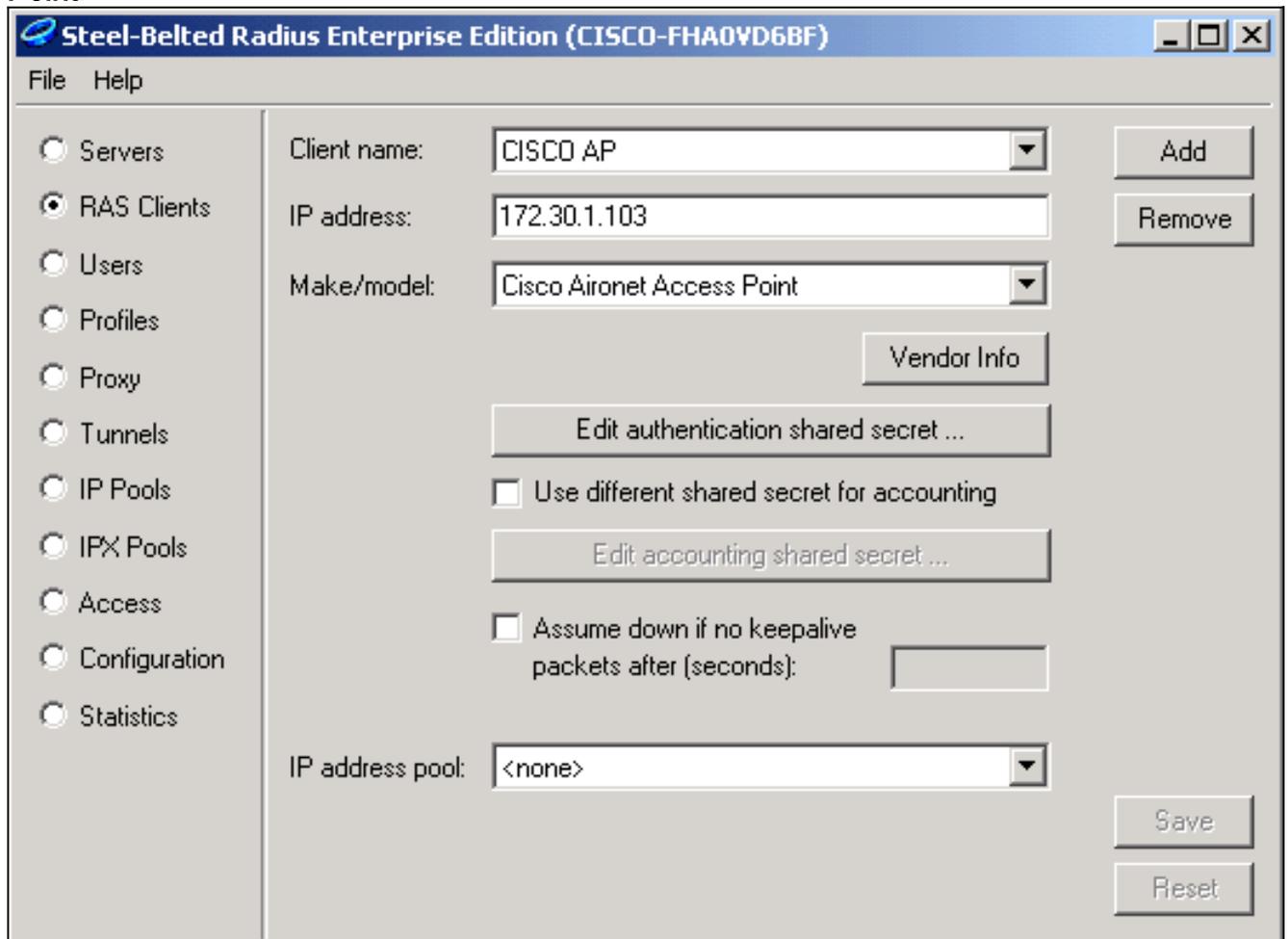
Observação: as partes deste documento que se referem a produtos que não são da Cisco foram escritas com base na experiência que o autor teve com esse produto que não é da Cisco, e não em treinamento formal. Eles se destinam à conveniência dos clientes da Cisco, não como suporte técnico. Para obter suporte técnico oficial sobre produtos que não são da Cisco, entre em contato com o suporte técnico do produto para o fornecedor.

- No menu Clientes RAS, clique em **Adicionar** para criar um novo Cliente

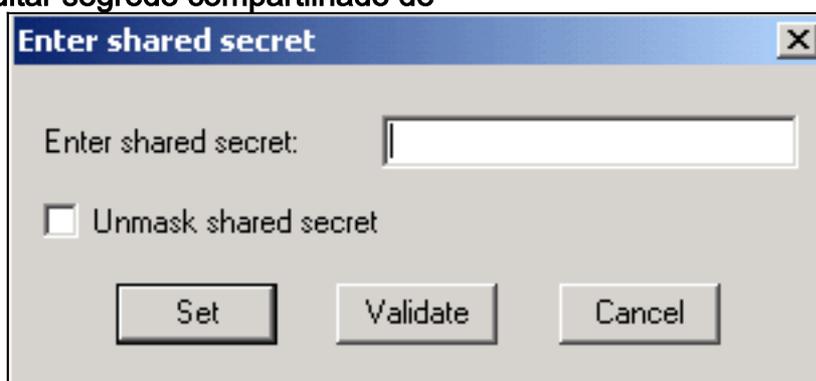
RAS.



2. Configure os parâmetros para o nome do cliente, endereço IP e make/model. **Nome do cliente:** Digite o nome do ponto de acesso ou ponte. **Endereço IP:** Digite o endereço do ponto de acesso ou ponte que se comunica com o Raio de aço. **Observação:** o servidor RADIUS visualiza o ponto de acesso ou ponte como um cliente RADIUS. **Marca/modelo:** Selecione **Cisco Aironet Access Point**.



3. Clique em **Editar segredo compartilhado de**



autenticação. Digite a string exata como a do ponto de acesso ou ponte para este servidor. Clique em **Definir** para retornar à caixa de diálogo anterior. Click **Save**.

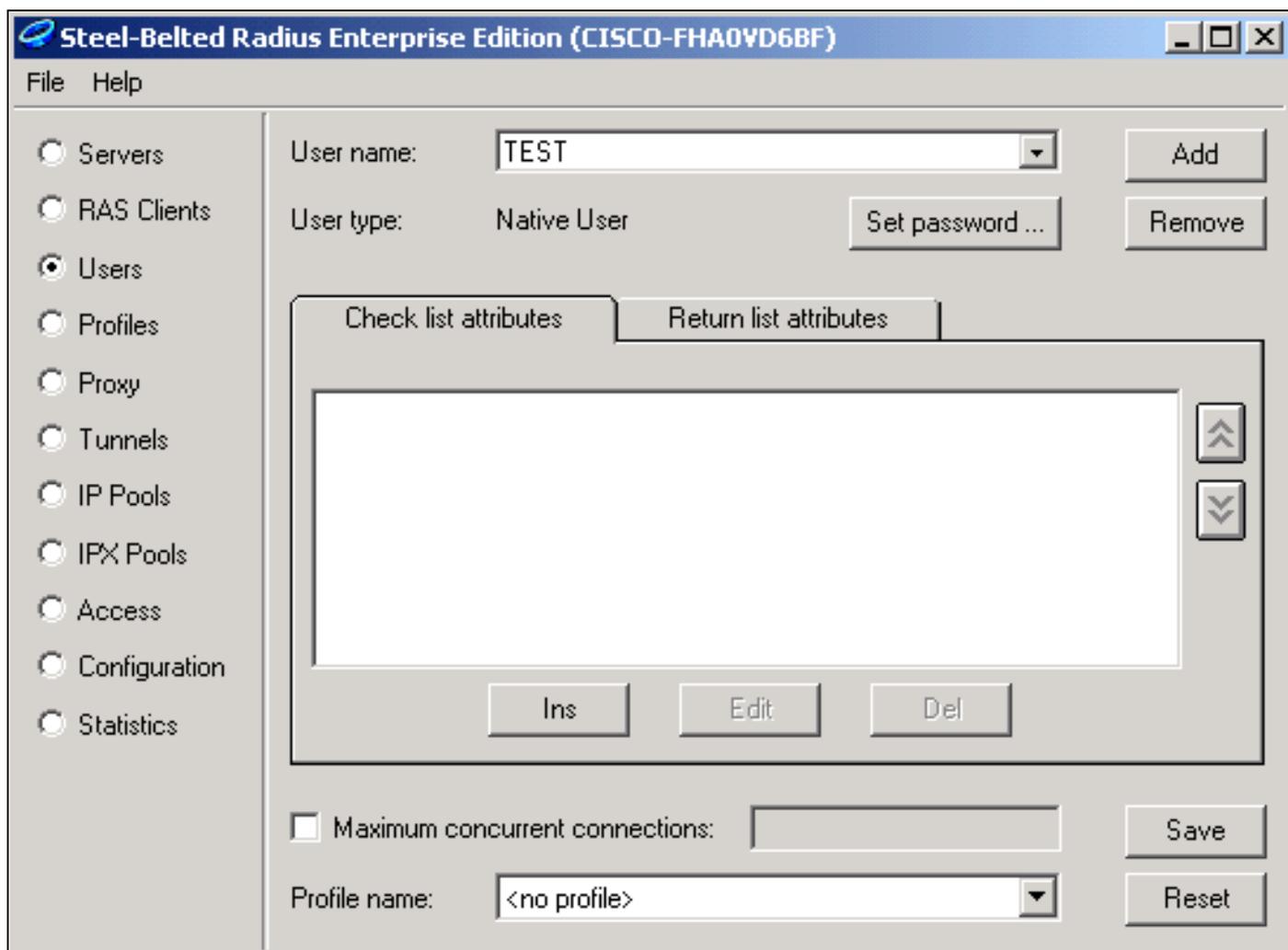
4. Procure o arquivo EAP.INI localizado na pasta de instalação do Steel-Belted Radius (em um PC baseado em Windows, esse arquivo normalmente está localizado em **C:\Radius\Services**).
5. Verifique se LEAP é uma opção para `EAP-Type`. Um arquivo de exemplo é semelhante a este:

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

6. Salve o arquivo EAP.INI modificado.
7. Pare e reinicie o serviço RADIUS.

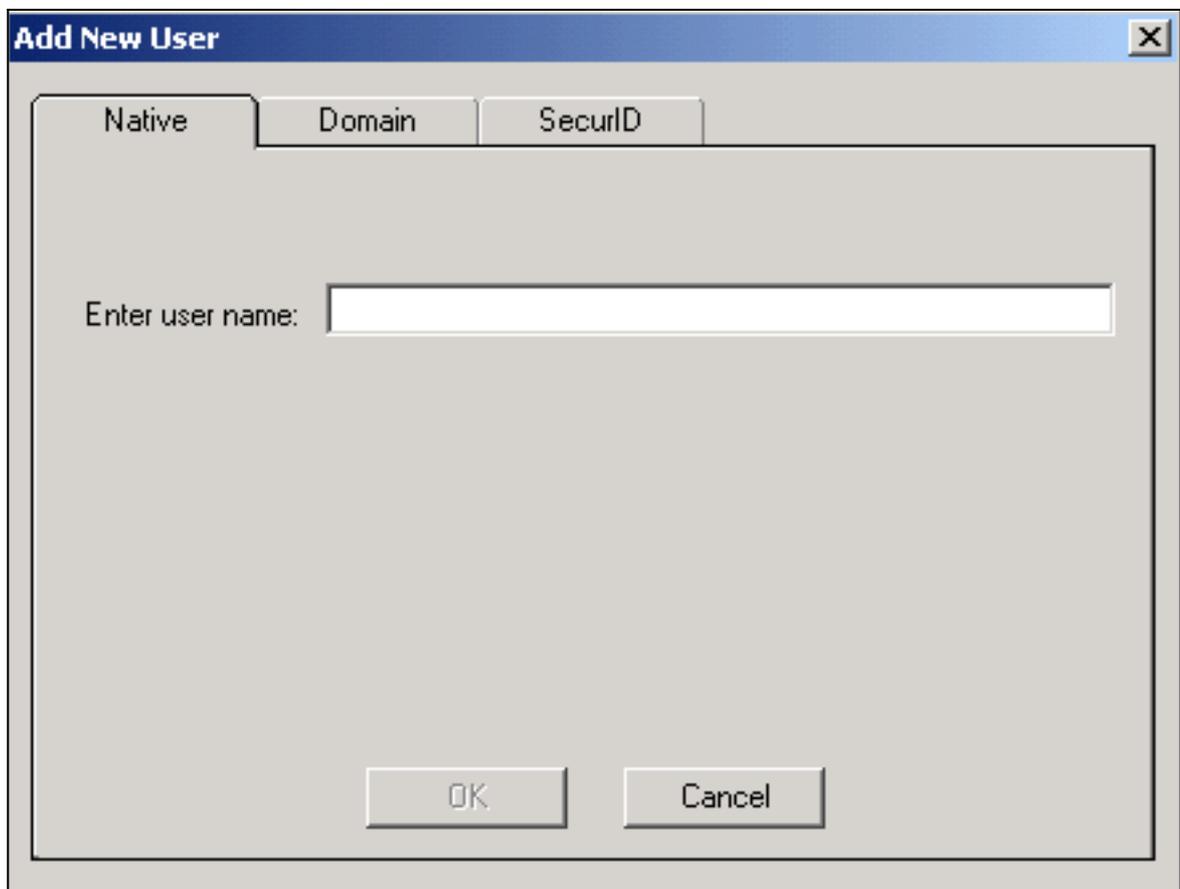
Criando usuários no Raio de Cinto de Aço

Esta seção descreve como criar um novo usuário nativo (local) com o produto Funk Software, Inc., Steel-Belted Radius. Se um usuário de Domínio ou Grupo de Trabalho precisar ser adicionado, entre em contato com o [Funk Software](#) para obter assistência. As entradas de usuário nativo exigem que o nome e a senha do usuário sejam inseridos no banco de dados local do Steel-Belted Radius. Para todos os outros tipos de entradas de usuário, o Steel-Belted Radius depende de outro banco de dados para validar as credenciais de um usuário.



Conclua estes passos para configurar um usuário nativo em Raio de aço:

1. No menu Usuários, clique em **Adicionar** para criar um novo



usuário.

2. Clique na guia **Nativo**, insira o nome de usuário no campo e clique em **OK**. A caixa de diálogo Adicionar novo usuário é fechada.
3. Na caixa de diálogo Usuários, selecione o usuário e clique em **Definir**



senha.

4. Digite a senha para o usuário e clique em **Definir**.
5. Na caixa de diálogo Usuários, clique em **Salvar** e você criou o usuário.

[Informações Relacionadas](#)

- [Configuração de segurança](#)
- [Software Funk](#)
- [LAN sem fio \(WLAN\)](#)
- [Suporte Técnico - Cisco Systems](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.