

Configurar el modo RADIUS para autenticar a los clientes de la tecnología inalámbrica de Cisco con el SALTO

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Configuración](#)

[Configurar el Punto de acceso o el Bridge](#)

[Configurar el producto de Funk Software, Inc., radio de Acero Ceñido](#)

[Crear a los usuarios en el radio de Acero Ceñido](#)

[Información Relacionada](#)

[Introducción](#)

Este documento describe cómo configurar los Puntos de acceso de las 340 y 350 Series y los Bridges de las 350 Series. También describe cómo el producto de [Funk Software, Inc.](#), radio de Acero Ceñido, los trabajos así como el protocolo light extensible authentication (SALTO) para autenticar a un cliente de la tecnología inalámbrica de Cisco.

Nota: Las porciones de este documento que refieren a los Productos del no Cisco fueron escritas basadas encendido experimentan al autor tenían con ese producto del no Cisco, no en la capacitación formal. Se piensan para ayudar los clientes de Cisco, no como Soporte técnico. Para el Soporte técnico autoritario en los Productos del no Cisco, entre en contacto el Soporte técnico del producto para el vendedor.

[prerrequisitos](#)

[Requisitos](#)

La Información presentada en este documento asume que el producto de Funk Software, Inc., radio de Acero Ceñido, es instalado con éxito y de trabajo correctamente. También asume que usted está teniendo el acceso administrativo al Punto de acceso o al Bridge a través de la interfaz del buscador.

[Componentes Utilizados](#)

La información en este documento se basa en los Puntos de acceso del Series Cisco Aironet 340 y 350 y los Bridges de las 350 Series. La información en este documento se aplica a todas las versiones de firmware 12.01T de VxWorks y posterior.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

[Convenciones](#)

Para obtener más información sobre las convenciones del documento, consulte las [Convenciones de Consejos Técnicos de Cisco](#).

[Configuración](#)

[Configurar el Punto de acceso o el Bridge](#)

Complete estos pasos para configurar el Punto de acceso o el Bridge.

1. De la página del estado resumido, complete estos pasos:Haga clic en Setup (Configuración).Haga clic la **Seguridad**.Haga clic en Radio Data Encryption (WEP) (Cifrado de datos de Radio (WEP)).Ingrese una clave WEP al azar (26 caracteres hexadecimales) en el slot de la clave WEP 1.Fije el tamaño de clave al **bit 128**.Haga clic en Apply (Aplicar).

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](#)

Haga clic en OK. Cambie la opción **Use of Data Encryption** por las estaciones está: a la **encripción completa**. Marque los cuadros abiertos y de la red EAP en la línea del tipo de autenticación del validar.



[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.

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

Haga clic en OK.

- De la página de la configuración de seguridad, el **servidor de autenticación** del teclado y hace estas entradas en la página:**Servidor Name/IP:** Ingrese el IP Address o el nombre del host del servidor de RADIUS.**Secreto compartido:** Ingrese la cadena exacta como la que está en el servidor de RADIUS para este Punto de acceso o Bridge.En el **servidor del uso para:** alinee para este servidor de RADIUS, marque la casilla de verificación de la **autenticación EAP**.

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. Cuando usted ha configurado los parámetros en el paso 2, haga clic la **AUTORIZACIÓN**. Con estas configuraciones, el Punto de acceso o el Bridge está listo para autenticar a los clientes del SALTO contra un servidor de RADIUS.

[Configurar el producto de Funk Software, Inc., radio de Acero Ceñido](#)

Complete los pasos en el procedimiento siguiente para configurar el producto de Funk Software, Inc., radio de Acero Ceñido, para comunicar con el Punto de acceso o el Bridge. Para información más completa sobre el servidor, refiera al [software Funk](#) .

Nota: Las porciones de este documento que refieren a los Productos del no Cisco fueron escritas basadas encendido experimentan al autor tenían con ese producto del no Cisco, no en la capacitación formal. Se piensan para ayudar los clientes de Cisco, no como Soporte técnico. Para el Soporte técnico autoritario en los Productos del no Cisco, entre en contacto el Soporte técnico del producto para el vendedor.

1. En el menú RAS Client, el tecleo **agrega** para crear a un nuevo cliente

RAS.

Add New RAS Client [X]

Client name:

Any RAS client

OK Cancel

- Configure los parámetros para el Nombre del cliente, dirección IP y hágalos/modelo. **Nombre del cliente:** Ingrese el nombre del Punto de acceso o del Bridge. **Dirección IP:** Ingrese el direccionamiento del Punto de acceso o del Bridge que comunica con el radio de Acero Ceñido. **Nota:** El servidor de RADIUS ve el Punto de acceso o el Bridge como cliente RADIUS. **Haga/modelo:** Seleccione el **Punto de acceso del Cisco Aironet**.

- El teclado edita el secreto compartido de

autenticación. Ingrese la cadena exacta como la que está en el Punto de acceso o el Bridge para este servidor. Haga clic el conjunto para volver al cuadro de diálogo anterior. Haga clic en Save (Guardar).

- Busque el archivo EAP.INI que está situado en la carpeta de instalación para el radio de Acero Ceñido (en un PC basado en Windows, este archivo está situado normalmente en **C:\Radius\Services**).
- Verifique que el SALTO sea una opción para el EAP-tipo. Un archivo de ejemplo parece similar a esto:

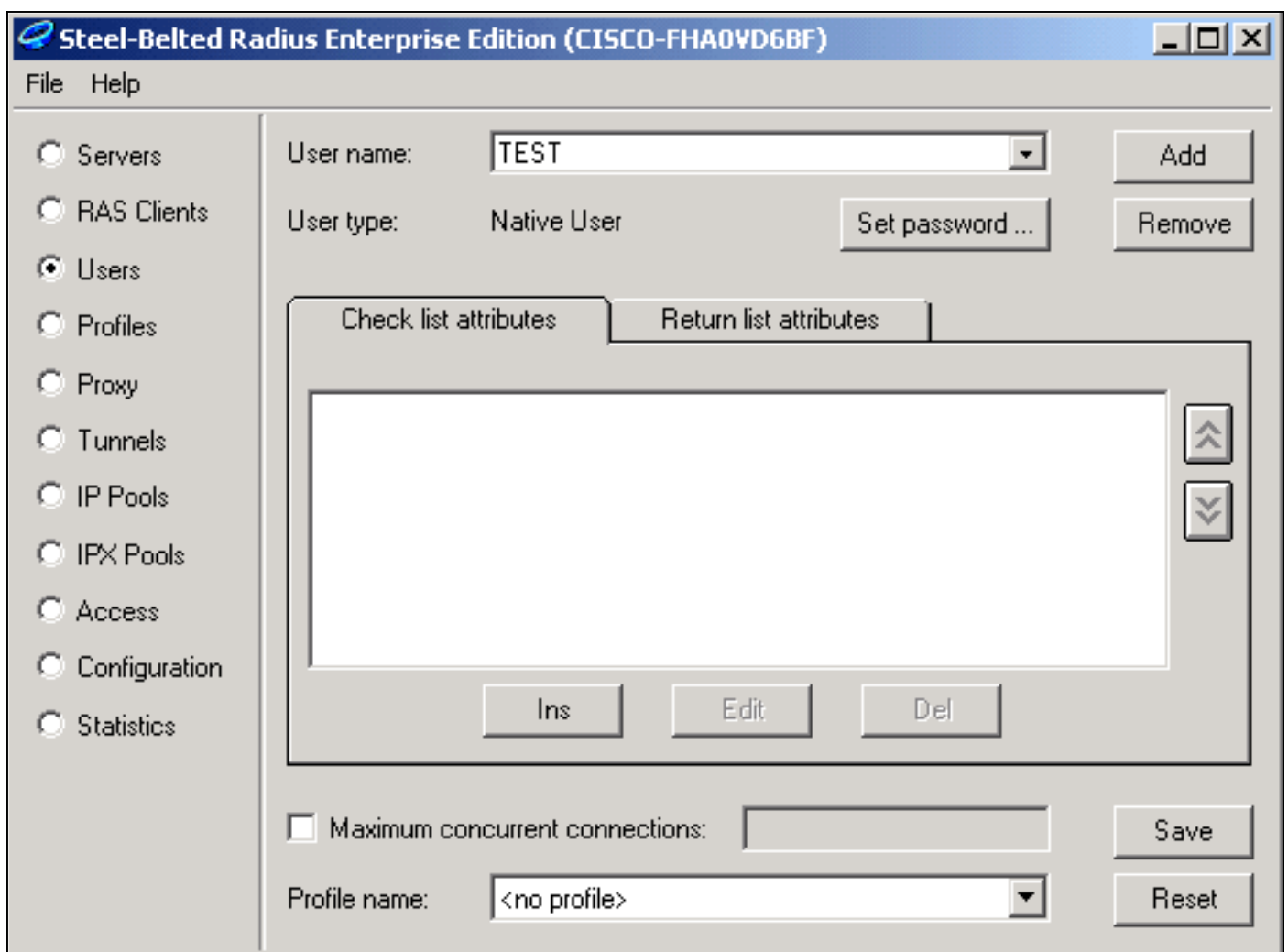

```
[Native-User]
EAP-Only = 0
First-Handle-Via-Auto-EAP = 0
```

EAP-Type = LEAP, TTLS

6. Salve el archivo modificado EAP.INI.
7. Pare y recomience el servicio RADIUS.

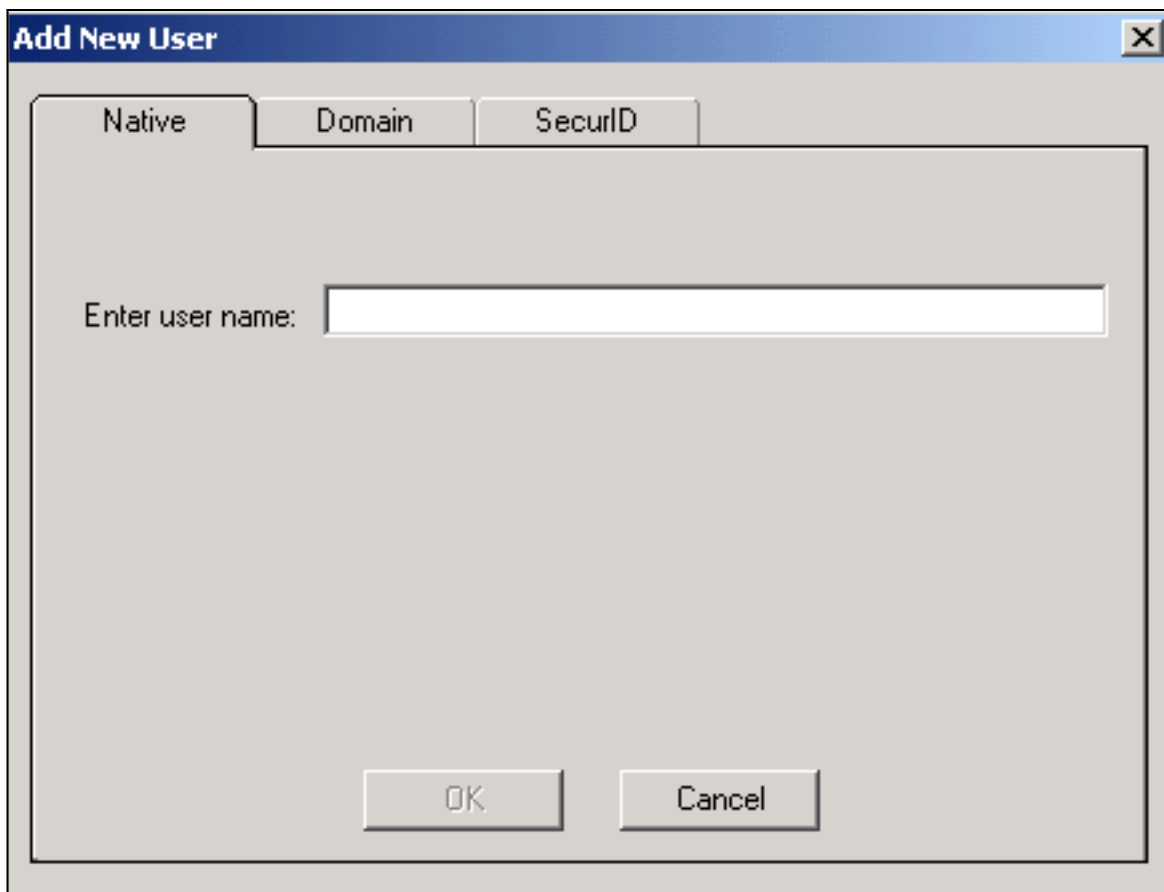
Crear a los usuarios en el radio de Acero Ceñido

Esta sección describe cómo crear a un nuevo usuario (local) nativo con el producto de Funk Software, Inc., radio de Acero Ceñido. Si un dominio o un usuario del Grupo de trabajo necesita ser agregado, entre en contacto el [software Funk](#) para la ayuda. [Las entradas de Usuario nativo requieren que el nombre y la contraseña de usuario estén ingresados en la base de datos local del radio de Acero Ceñido. Para el resto de los tipos de entradas de usuario, el radio de Acero Ceñido confía en otra base de datos para validar las credenciales de un usuario.](#)



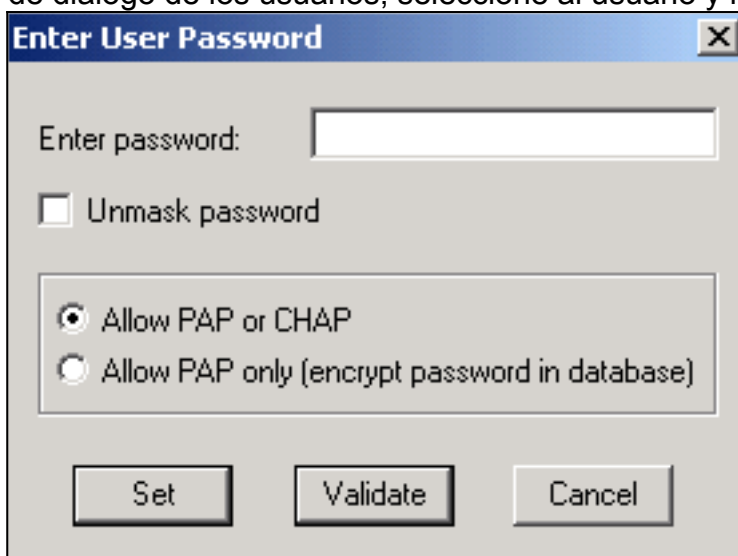
Complete estos pasos para configurar a un Usuario nativo en el radio de Acero Ceñido:

1. En el menú Users (Usuarios), el tecleo **agrega** para crear a un usuario



nuevo.

2. Haga clic la lengüeta **nativa**, ingrese el Nombre de usuario en el campo, y haga clic la **AUTORIZACIÓN**. El cuadro de diálogo del usuario nuevo del agregar se cierra.
3. En el cuadro de diálogo de los usuarios, seleccione al usuario y haga clic la **contraseña**



determinada.

4. Ingrese la contraseña para el usuario y haga clic el **conjunto**.
5. En el cuadro de diálogo de los usuarios, la **salvaguardia** y usted del tecleo han creado al usuario.

[Información Relacionada](#)

- [Configuración de seguridad](#)
- [Software Funk](#)
- [Wireless LAN \(red inalámbrica \(WLAN\)\)](#)
- [Soporte Técnico - Cisco Systems](#)