

Configuration de Funk RADIUS pour authentifier les clients Cisco sans fil avec LEAP

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Conventions](#)

[Configuration](#)

[Configuration du point d'accès ou du pont](#)

[Configuration du produit Funk Software, Inc., Steel-Belted Radius](#)

[Création d'utilisateurs dans un rayon en acier](#)

[Informations connexes](#)

[Introduction](#)

Ce document décrit comment configurer les points d'accès des gammes 340 et 350 et les ponts des gammes 350. Il décrit également comment le produit [Funk Software, Inc.](#), Steel-Belted Radius, fonctionne avec le Light Extensible Authentication Protocol (LEAP) pour authentifier un client sans fil Cisco.

Remarque : Les parties de ce document qui font référence à des produits non Cisco ont été écrites en fonction de l'expérience que l'auteur a acquise avec ce produit non Cisco et non en fonction d'une formation formelle. Elles sont destinées à la commodité des clients Cisco et non à l'assistance technique. Pour obtenir une assistance technique faisant autorité sur les produits non Cisco, contactez l'assistance technique du fournisseur.

[Conditions préalables](#)

[Conditions requises](#)

Les informations présentées dans ce document supposent que le produit Funk Software, Inc., Steel-Belted Radius, est installé et fonctionne correctement. Il suppose également que vous obtenez un accès administratif au point d'accès ou au pont via l'interface du navigateur.

[Components Used](#)

Les informations de ce document sont basées sur les points d'accès Cisco Aironet 340 et 350 et les ponts de la gamme 350. Les informations de ce document s'appliquent à toutes les versions de microprogramme VxWorks 12.01T et ultérieures.

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](#)

[Configuration du point d'accès ou du pont](#)

Exécutez ces étapes pour configurer le point d'accès ou le pont.

1. À partir de la page Résumé de l'état, procédez comme suit : Cliquez sur **Setup**. Cliquez sur **Sécurité**. Cliquez sur **Radio Data Encryption (WEP)**. Saisissez une clé WEP aléatoire (26 caractères hexadécimaux) dans le logement WEP Key 1. Définissez la taille de la clé sur **128 bits**. Cliquez sur **Apply**.

BR350-CLEAR Root Radio Data Encryption

CISCO SYSTEMS



Cisco 350 Series Bridge 12.03T

Uptime: 01:45:05

[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: 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](#)

Click OK. Modifier l'option **Utiliser le chiffrement des données par stations est** : au **chiffrement complet**. Cochez les cases **Open** et **Network EAP** sur la ligne **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.

2. Dans la page Security Setup, cliquez sur **Authentication Server** et saisissez les entrées suivantes sur la page :
Nom/adresse IP du serveur : Saisissez l'adresse IP ou le nom d'hôte du serveur RADIUS.
Secret partagé : Entrez la chaîne exacte sur le serveur RADIUS pour ce point d'accès ou ce pont.
Sur le serveur Utiliser pour : pour ce serveur RADIUS, cochez la case **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

- Lorsque vous avez configuré les paramètres à l'étape 2, cliquez sur **OK**. Avec ces paramètres, le point d'accès ou le pont est prêt à authentifier les clients LEAP sur un serveur RADIUS.

[Configuration du produit Funk Software, Inc., Steel-Belted Radius](#)

Suivez les étapes de la procédure suivante pour configurer le produit Funk Software, Inc., Steel-Belted Radius, pour communiquer avec le point d'accès ou le pont. Pour plus d'informations sur le serveur, reportez-vous à [Funk Software](#).

Remarque : Les parties de ce document qui font référence à des produits non Cisco ont été écrites en fonction de l'expérience que l'auteur a acquise avec ce produit non Cisco et non en fonction d'une formation formelle. Elles sont destinées à la commodité des clients Cisco et non à l'assistance technique. Pour obtenir une assistance technique faisant autorité sur les produits non Cisco, contactez l'assistance technique du fournisseur.

- Dans le menu Clients RAS, cliquez sur **Ajouter** pour créer un client

RAS.

Add New RAS Client X

Client name:

Any RAS client

OK Cancel

2. Configurez les paramètres pour le nom du client, l'adresse IP et make/model. **Nom du client** : Saisissez le nom du point d'accès ou du pont. **Adresse IP**: Saisissez l'adresse du point d'accès ou du pont qui communique avec le rayon en acier. **Remarque** : le serveur RADIUS voit le point d'accès ou le pont comme un client RADIUS. **Marque/modèle** : Sélectionnez **Point d'accès Cisco Aironet**.

3. Cliquez sur **Modifier le secret partagé**

d'authentification. Entrez la chaîne exacte comme celle du point d'accès ou du pont pour ce serveur. Cliquez sur **Définir** pour revenir à la boîte de dialogue précédente. Cliquez **Save**.

4. Recherchez le fichier EAP.INI qui se trouve dans le dossier d'installation de Steel-Belted Radius (sur un PC Windows, ce fichier se trouve normalement dans **C:\Radius\Services**).
5. Vérifiez que LEAP est une option pour `EAP-Type`. Un exemple de fichier ressemble à ceci :

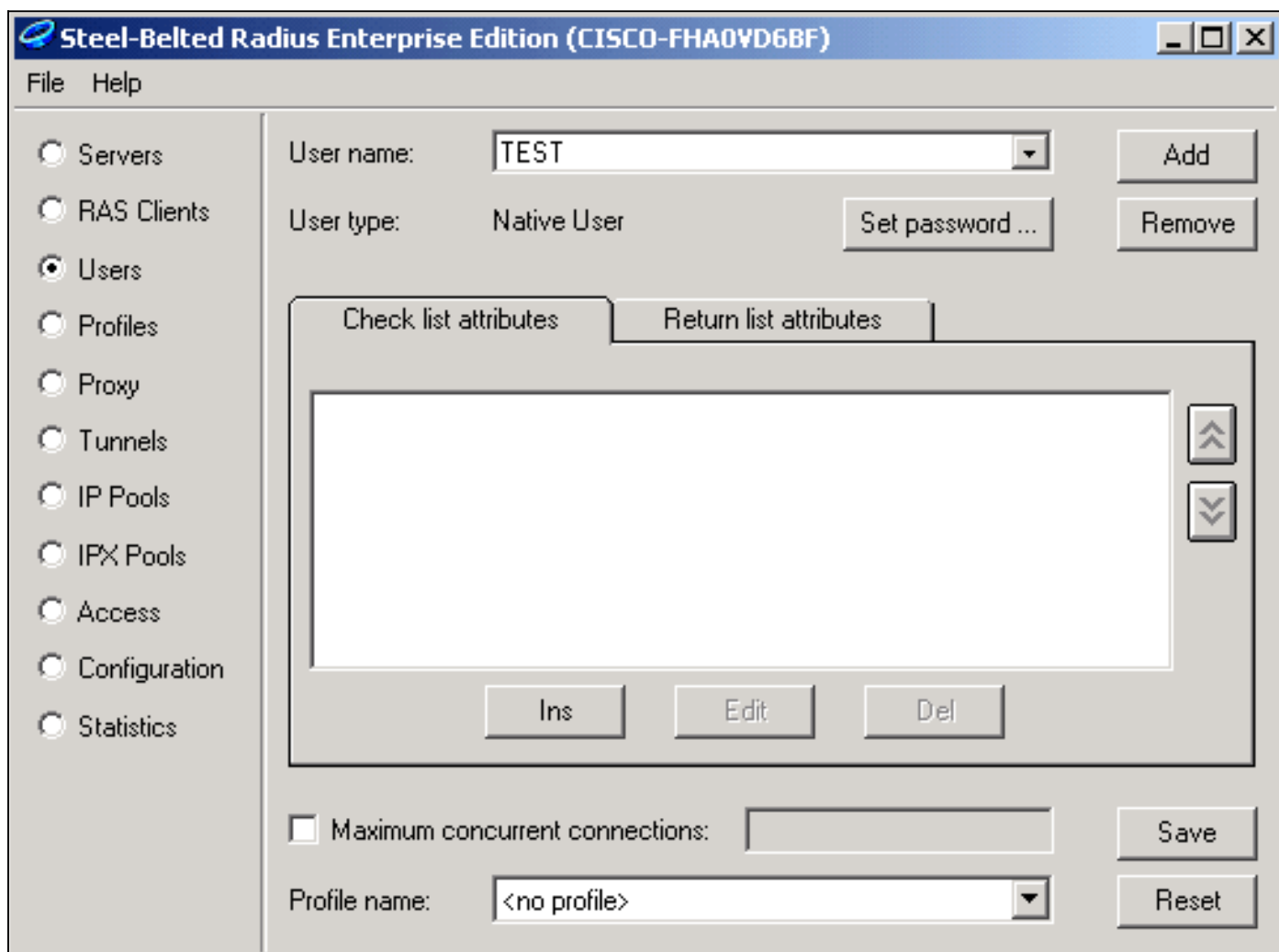
```
[Native-User]
EAP-Only = 0
First-Handle-Via-Auto-EAP = 0
EAP-Type = LEAP, TTLS
```

6. Enregistrez le fichier EAP.INI modifié.

7. Arrêtez et redémarrez le service RADIUS.

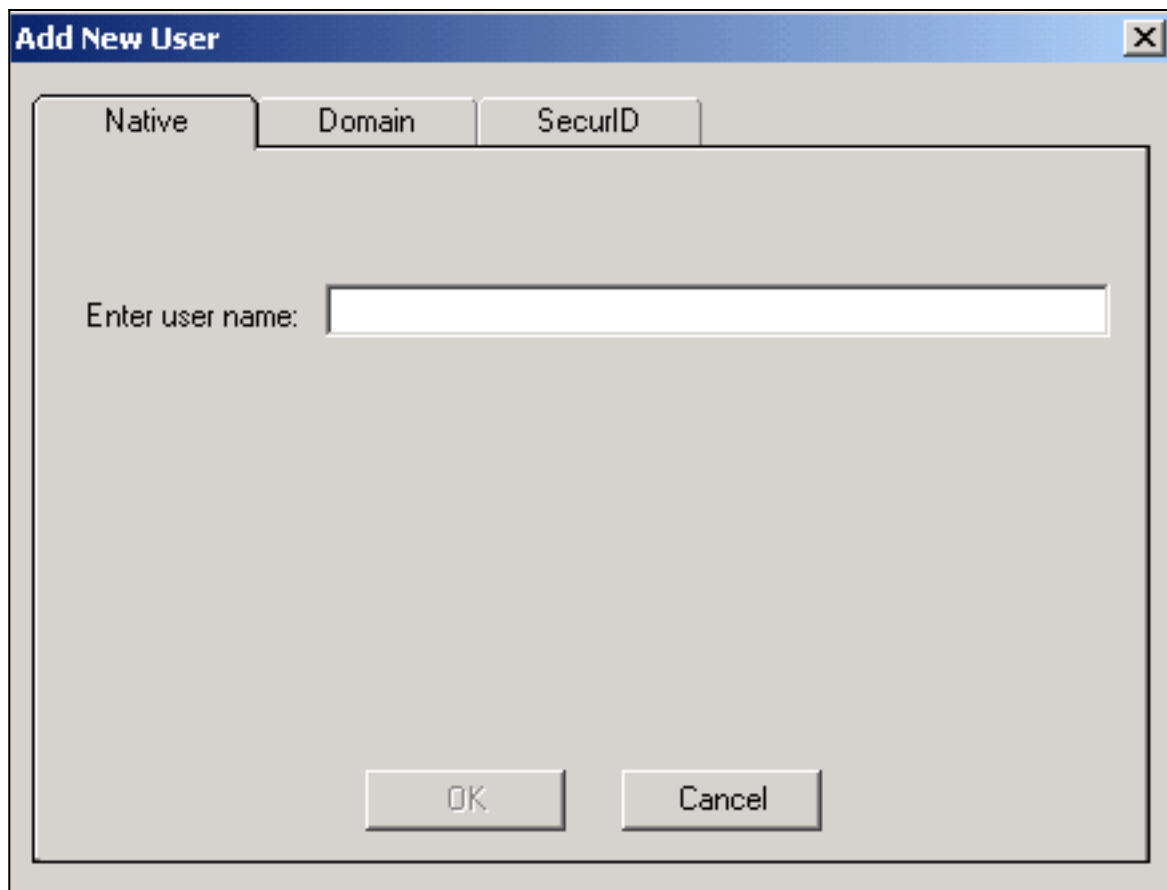
Création d'utilisateurs dans un rayon en acier

Cette section décrit comment créer un nouvel utilisateur natif (local) avec le produit Funk Software, Inc., Steel-Belted Radius. Si un utilisateur de domaine ou de groupe de travail doit être ajouté, contactez [Funk Software](#) pour obtenir de l'aide. Les entrées d'utilisateur natif exigent que le nom et le mot de passe de l'utilisateur soient entrés dans la base de données locale de Radius en acier. Pour tous les autres types d'entrées utilisateur, Steel-Belted Radius s'appuie sur une autre base de données pour valider les informations d'identification d'un utilisateur.



Complétez ces étapes pour configurer un utilisateur natif dans Radius en acier :

1. Dans le menu Utilisateurs, cliquez sur **Ajouter** pour créer un nouvel



utilisateur.

2. Cliquez sur l'onglet **Native**, saisissez le nom d'utilisateur dans le champ, puis cliquez sur **OK**. La boîte de dialogue Ajouter un nouvel utilisateur se ferme.
3. Dans la boîte de dialogue Utilisateurs, sélectionnez l'utilisateur et cliquez sur **Définir le mot**



de passe.

4. Entrez le mot de passe de l'utilisateur et cliquez sur **Définir**.
5. Dans la boîte de dialogue Utilisateurs, cliquez sur **Enregistrer** et vous avez créé l'utilisateur.

[Informations connexes](#)

- [Configuration de la sécurité](#)
- [Logiciel Funk](#)
- [LAN sans fil \(WLAN\)](#)
- [Support technique - Cisco Systems](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.