

Configurazione di Funk RADIUS per autenticare i client wireless Cisco con LEAP

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Configurazione](#)

[Configurazione del punto di accesso o del bridge](#)

[Configurazione del prodotto Funk Software, Inc., Steel-Belted Radius](#)

[Creazione di utenti nel raggio con cinghie d'acciaio](#)

[Informazioni correlate](#)

[Introduzione](#)

In questo documento viene descritto come configurare gli access point serie 340 e 350 e i bridge serie 350. Descrive anche come il prodotto [Funk Software, Inc.](#), Steel-Belted Radius, funziona insieme al Light Extensible Authentication Protocol (LEAP) per autenticare un client wireless Cisco.

Nota: le parti di questo documento che fanno riferimento a prodotti non Cisco sono state scritte in base all'esperienza dell'autore con quel prodotto non Cisco, non sulla formazione formale. Sono concepiti per offrire vantaggi ai clienti Cisco e non come supporto tecnico. Per il supporto tecnico autorevole su prodotti non Cisco, contattare il supporto tecnico del prodotto per il fornitore.

[Prerequisiti](#)

[Requisiti](#)

Le informazioni presentate in questo documento presuppongono che il prodotto Funk Software, Inc., Steel-Belted Radius, sia stato installato e funzioni correttamente. Presuppone inoltre che si stia ottenendo l'accesso amministrativo al punto di accesso o al bridge tramite l'interfaccia del browser.

[Componenti usati](#)

Per la stesura del documento, sono stati usati Cisco Aironet serie 340 e 350 Access Point e bridge serie 350. Le informazioni di questo documento si applicano a tutti i firmware VxWorks versione 12.01T e successive.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

[Convenzioni](#)

Per ulteriori informazioni sulle convenzioni usate, consultare il documento [Cisco sulle convenzioni nei suggerimenti tecnici](#).

[Configurazione](#)

[Configurazione del punto di accesso o del bridge](#)

Completare la procedura seguente per configurare il punto di accesso o il bridge.

1. Nella pagina Stato riepilogo effettuare le operazioni riportate di seguito. Fare clic su **Imposta**. Fare clic su **Protezione**. Fare clic su **Crittografia dati radio (WEP)**. Immettere una chiave WEP casuale (26 caratteri esadecimale) nello slot Chiave WEP 1. Impostare la dimensione della chiave su **128 bit**. Fare clic su **Apply** (Applica).



[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

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

	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](#)

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

Fare clic su **OK**. Modificare l'opzione **Use of Data Encryption by Stations** come indicato di seguito: alla **crittografia completa**. Selezionare le caselle **Open** (Apri) e **Network EAP** (Rete) nella riga **Accetta tipo di autenticazione**.



[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.

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

Fare clic su **OK**.

- Dalla pagina Impostazione protezione, fare clic su **Authentication Server** (Server di autenticazione) e nella pagina inserire le seguenti voci:
Nome server/IP: Immettere l'indirizzo IP o il nome host del server RADIUS.
Segreto condiviso: Immettere la stringa esatta del server RADIUS per il punto di accesso o il bridge.
Sul server Usa per: per questo server RADIUS, selezionare la casella di controllo **Autenticazione 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](#)

- Una volta configurati i parametri al punto 2, fare clic su **OK**. Con queste impostazioni, il punto di accesso o il bridge è pronto per autenticare i client LEAP su un server RADIUS.

Configurazione del prodotto Funk Software, Inc., Steel-Belted Radius

Completare la procedura seguente per configurare il prodotto Funk Software, Inc., Steel-Belted Radius, per comunicare con il punto di accesso o il ponte. Per informazioni più complete sul server, consultare il documento [Funk Software](#).

Nota: le parti di questo documento che fanno riferimento a prodotti non Cisco sono state scritte in base all'esperienza dell'autore con quel prodotto non Cisco, non sulla formazione formale. Sono concepiti per offrire vantaggi ai clienti Cisco e non come supporto tecnico. Per il supporto tecnico autorevole su prodotti non Cisco, contattare il supporto tecnico del prodotto per il fornitore.

- Scegliere **Aggiungi** dal menu Client RAS per creare un nuovo client

Add New RAS Client

Client name:

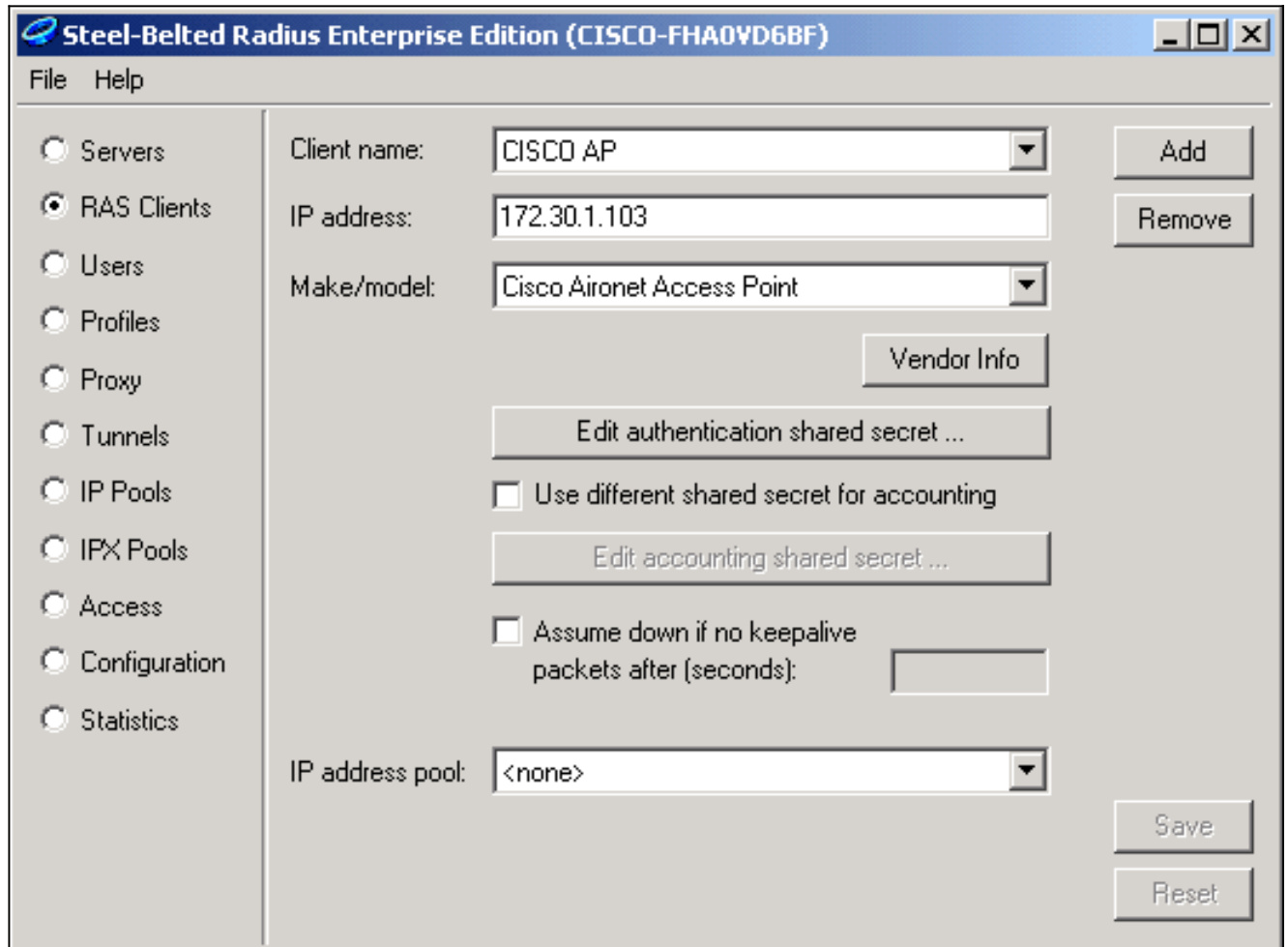
Any RAS client

OK Cancel

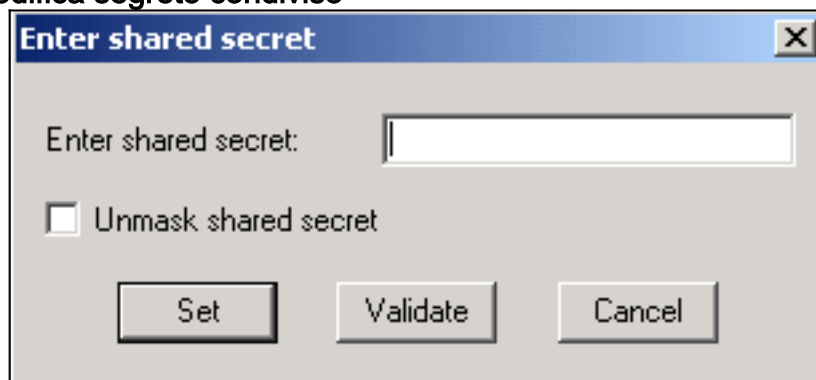
RAS.

- Configurare i parametri per nome client, indirizzo IP e marca/modello. **Nome client:** Immettere il nome del punto di accesso o del bridge. **Indirizzo IP:** Immettere l'indirizzo del punto di

accesso o del ponte che comunica con il raggio cinturato in acciaio.**Nota:** Il server RADIUS visualizza il punto di accesso o il bridge come client RADIUS.**Marca/modello:** Selezionare **Cisco Aironet Access Point**.



3. Fare clic su **Modifica segreto condiviso**



autenticazione. Immettere la stringa esatta corrispondente a quella del punto di accesso o del bridge per il server. Fare clic su **Imposta** per tornare alla finestra di dialogo precedente. Fare clic su **Salva**.

4. Cercare il file EAP.INI che si trova nella cartella di installazione di Steel-Belted Radius (su un PC basato su Windows, questo file si trova normalmente in **C:\Radius\Services**).

5. Verificare che LEAP sia un'opzione per `EAP-Type`. Un file di esempio è simile al seguente:

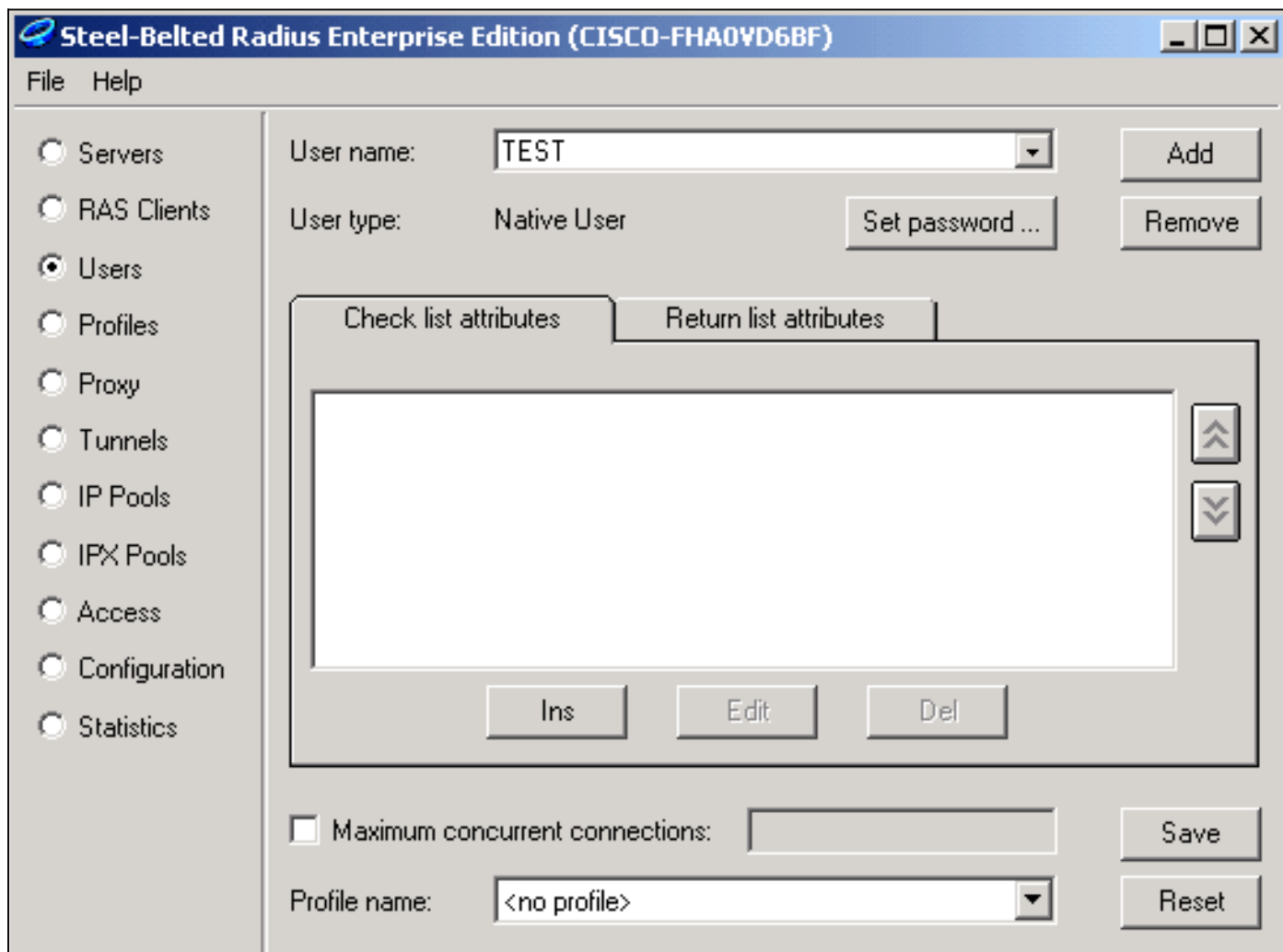
```
[Native-User]
EAP-Only = 0
First-Handle-Via-Auto-EAP = 0
EAP-Type = LEAP, TTLS
```

6. Salvare il file EAP.INI modificato.

7. Arrestare e riavviare il servizio RADIUS.

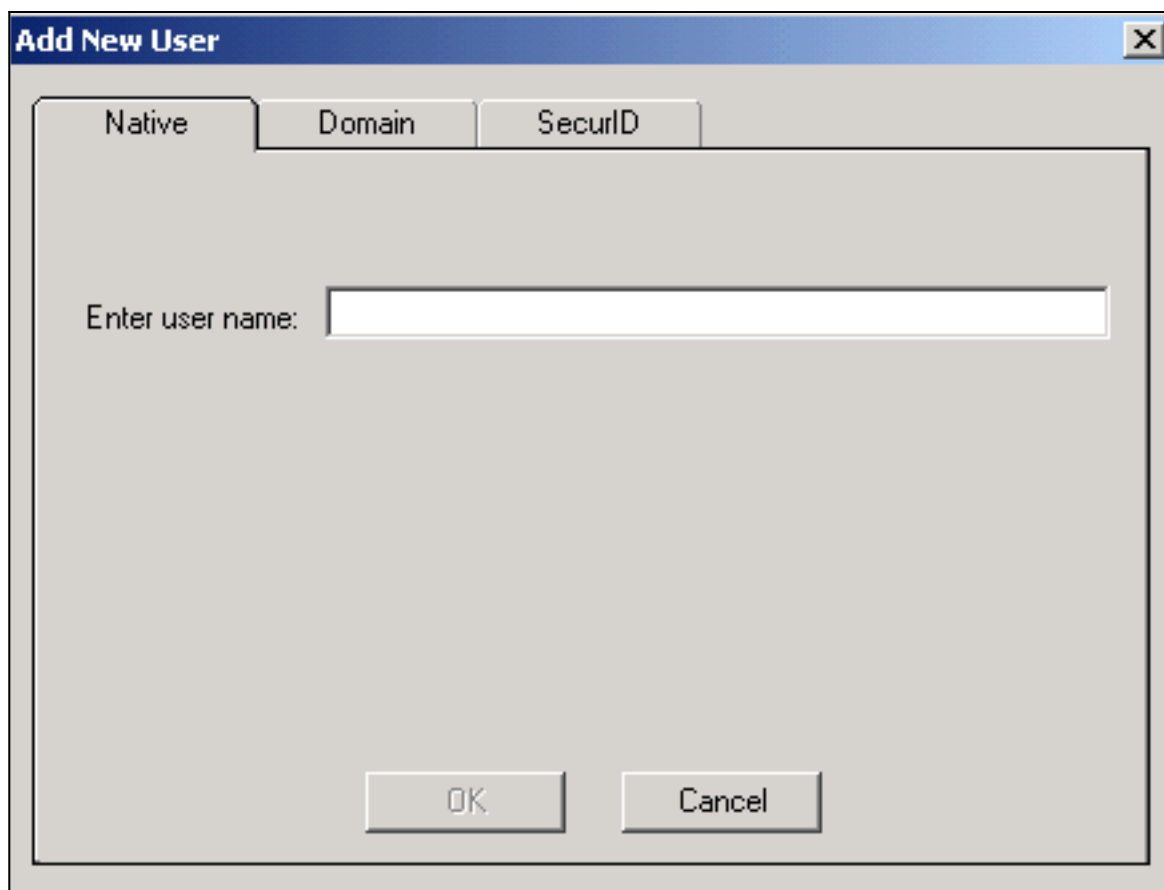
[Creazione di utenti nel raggio con cinghie d'acciaio](#)

Questa sezione descrive come creare un nuovo utente nativo (locale) con il prodotto Funk Software, Inc., Steel-Belted Radius. Se è necessario aggiungere un utente di dominio o di gruppo di lavoro, contattare [Funk Software](#) per assistenza. Le voci utente native richiedono l'immissione del nome utente e della password nel database locale Steel-Belted Radius. Per tutti gli altri tipi di voci utente, Steel-Belted Radius si basa su un altro database per convalidare le credenziali di un utente.



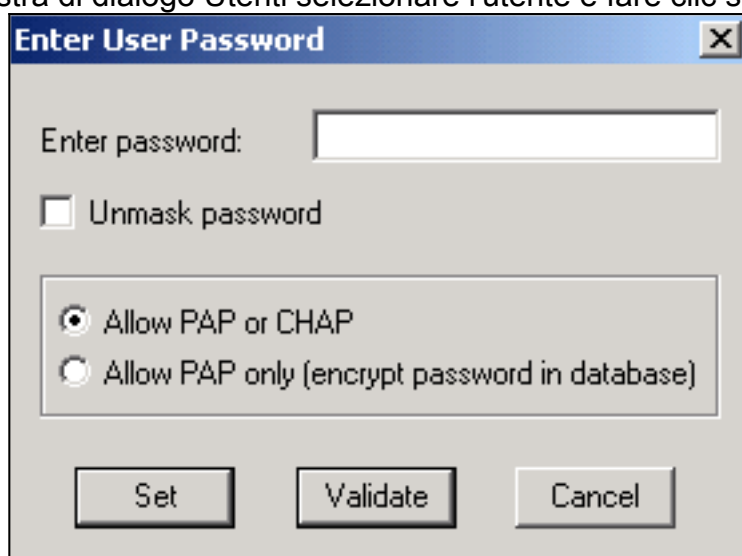
Completare la procedura seguente per configurare un utente nativo in Steel-Belted Radius:

1. Scegliere **Aggiungi** dal menu Utenti per creare un nuovo



utente.

2. Fare clic sulla scheda **Native**, immettere il nome utente nel campo e fare clic su **OK**. La finestra di dialogo Aggiungi nuovo utente si chiude.
3. Nella finestra di dialogo Utenti selezionare l'utente e fare clic su **Imposta**



password.

4. Immettere la password per l'utente e fare clic su **Imposta**.
5. Nella finestra di dialogo Utenti fare clic su **Salva** per creare l'utente.

[Informazioni correlate](#)

- [Configurazione della protezione](#)
- [Software Funk](#)
- [WLAN \(Wireless LAN\)](#)
- [Supporto tecnico – Cisco Systems](#)