

Настройка Funk RADIUS на проверку подлинности клиентов беспроводной связи Cisco с помощью LEAP

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Условные обозначения](#)

[!--- конфигурацию](#)

[Настройка точка доступа или мост](#)

[Настройка продукт Funk Software, Inc., радиус Steel-Belted](#)

[Создание пользователей в радиусе Steel-Belted](#)

[Дополнительные сведения](#)

Введение

Этот документ описывает, как настроить точки доступа серии 340 и 350 и мосты серии 350. Это также описывает, как продукт [Funk Software, Inc.](#), Радиус Steel-Belted, сотрудничает со Световым расширяемым протоколом аутентификации (LEAP) для аутентификации клиента беспроводной связи Cisco.

Примечание: Части этого документа, которые обращаются к продуктам не-Cisco, были записаны на основе опыта, который автор имел с тем продуктом не-Cisco, не на формальном обучении. Они предназначены для удобства Клиентов Cisco, не как техническая поддержка. Для авторитетной технической поддержки на продуктах не-Cisco свяжитесь с технической поддержкой продукта для поставщика.

Предварительные условия

Требования

Информация, содержащаяся в данном документе предполагает, что продукт Funk Software, Inc., Радиус Steel-Belted, успешно установлен и работающий должным образом. Это также предполагает получение административного доступа к точке доступа или в мост через интерфейс обозревателя.

Используемые компоненты

Сведения в этом документе основываются на Cisco Aironet 340 и точках доступа серии 350 и мостах серии 350. Сведения в этом документе применяются ко всем версиям микропрограммы VxWorks 12.01T и позже.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

[Дополнительные сведения об условных обозначениях см. в документе Технические рекомендации Cisco. Условные обозначения.](#)

!--- конфигурацию

Настройка точка доступа или мост

Выполните эти шаги для настройки точки доступа или моста.

1. От страницы Summary Status выполните эти шаги:**Нажмите кнопку Setup (Настройка).Нажмите Security.Выберите Radio Data Encryption (WEP) (Шифрование данных в беспроводной сети – WEP).Введите случайный КЛЮЧ WEP (26 шестнадцатеричных символов) в слоте WEP Key 1.Установите Размер ключа в 128 битов.Щелкните "Применить".**



[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](#)

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

Нажмите кнопку ОК.Измените опция Use of Data Encryption by Stations: к Полному шифрованию.Установите Открытые и Сетевые флажки EAP на Принять линии Типа проверки подлинности.



[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.

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

Нажмите кнопку ОК.

- От страницы Security Setup нажмите **Authentication Server** и сделайте эти записи на странице:
 - IP Имени сервера:** Введите IP-адрес или имя хоста сервера RADIUS.
 - Общий secret:** Введите точную строку как ту на сервере RADIUS для этой точки доступа или моста. На сервере **Использования для:** линия для этого сервера RADIUS, проверьте флажок **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

- При настройке параметров в Шаге 2 нажмите **OK**. С этими параметрами настройки, точкой доступа или мостом готово аутентифицировать клиентов LEAP против сервера RADIUS.

[Настройка продукт Funk Software, Inc., радиус Steel-Belted](#)

Выполните шаги в следующей процедуре для настройки продукта Funk Software, Inc., Радиуса Steel-Belted, для передачи с точкой доступа или мостом. Для большего количества полной информации на сервере обратитесь к [Компании Funk Software](#).

Примечание: Части этого документа, которые обращаются к продуктам не-Cisco, были записаны на основе опыта, который автор имел с тем продуктом не-Cisco, не на формальном обучении. Они предназначены для удобства Клиентов Cisco, не как техническая поддержка. Для авторитетной технической поддержки на продуктах не-Cisco свяжитесь с технической поддержкой продукта для поставщика.

- На Меню клиентов RAS нажмите **Add** для создания нового Клиента

Add New RAS Client

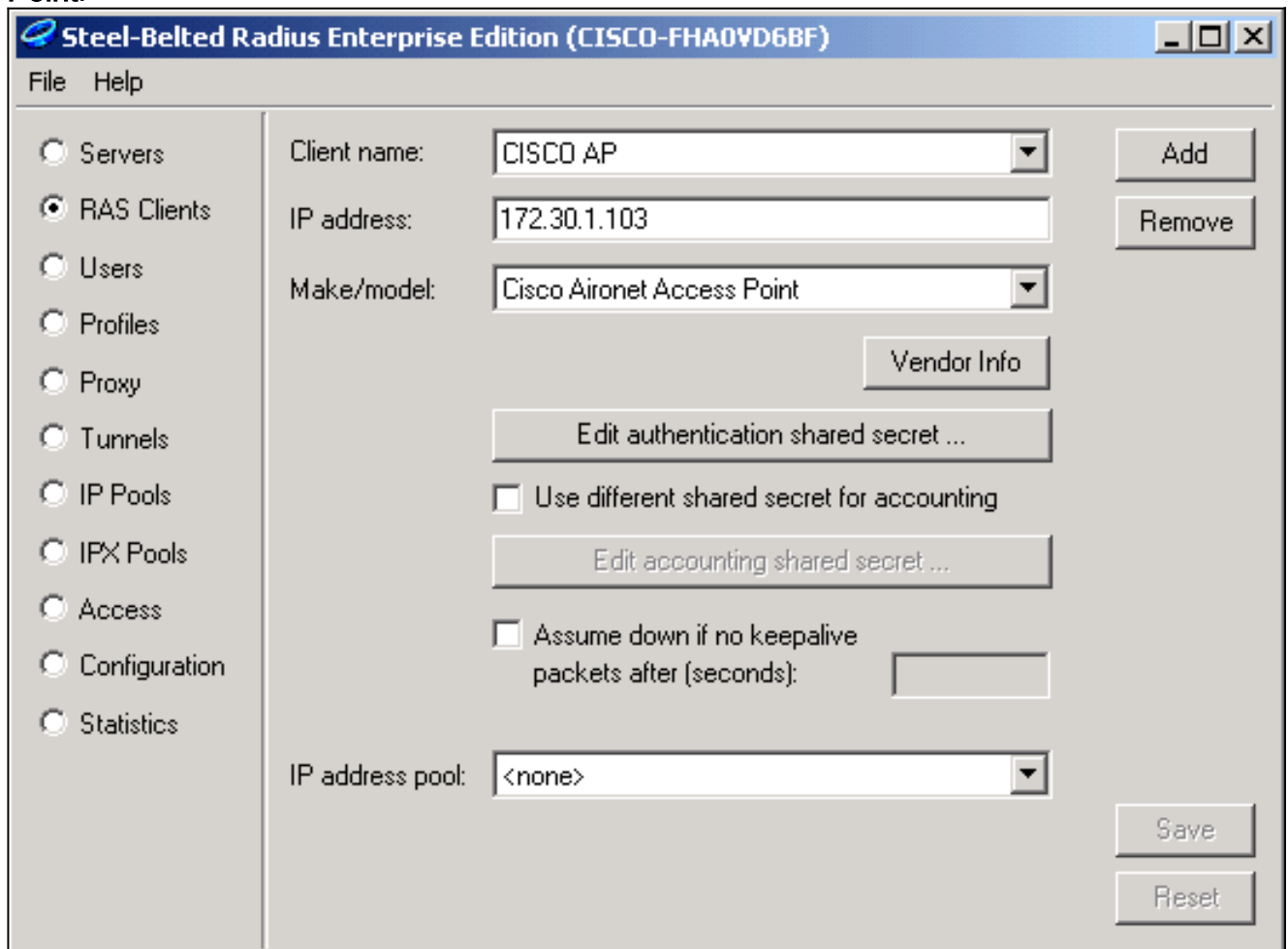
Client name:

Any RAS client

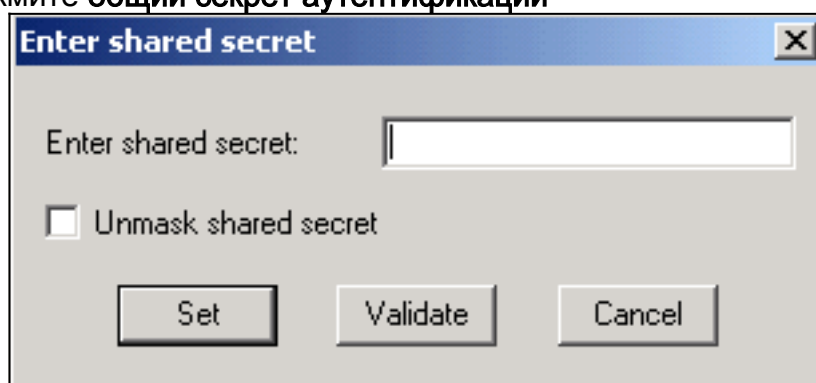
OK Cancel

RAS.

2. Настройте параметры для имени клиента, IP-адреса и сделайте/моделируйте. **Имя клиента:** Введите имя точки доступа или моста. **IP-адрес:** Введите адрес точки доступа или моста, который связывается с Радиусом Steel-Belted. **Примечание:** Сервер RADIUS просматривает точку доступа или мост как Клиент RADIUS. **Марка / модель:** Выберите **Cisco Aironet Access Point**.



3. Нажмите **общий секрет аутентификации**



Edit. Введите точную строку как ту на точке доступа или мосту для этого сервера. Нажмите **Set** для возврата к предыдущему диалоговому окну. Нажмите **Save**.

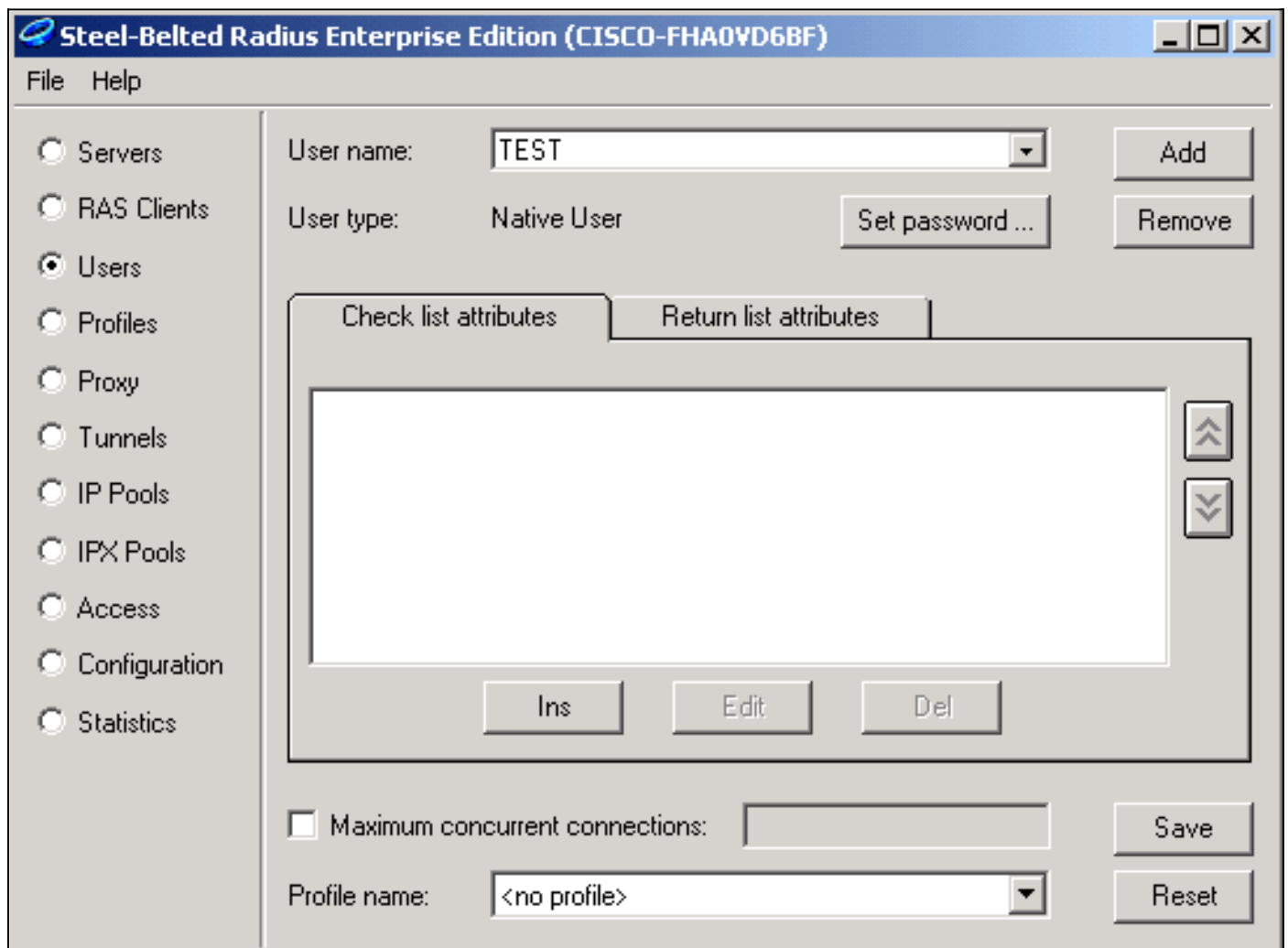
4. Ищите файл EAP.INI, который расположен в каталоге установки для Радиуса Steel-Belted (на ПК под управлением Windows, этот файл обычно располагается в **C:\Radius\Services**).
5. Проверьте, что LEAP является опцией для EAP-Type. Файл примера выглядит подобным **этому:**
- ```
[Native-User]
EAP-Only = 0
First-Handle-Via-Auto-EAP = 0
```

EAP-Type = LEAP, TTLS

6. Сохраните модифицированный файл EAP.INI.
7. Остановите и перезапустите Сервис RADIUS.

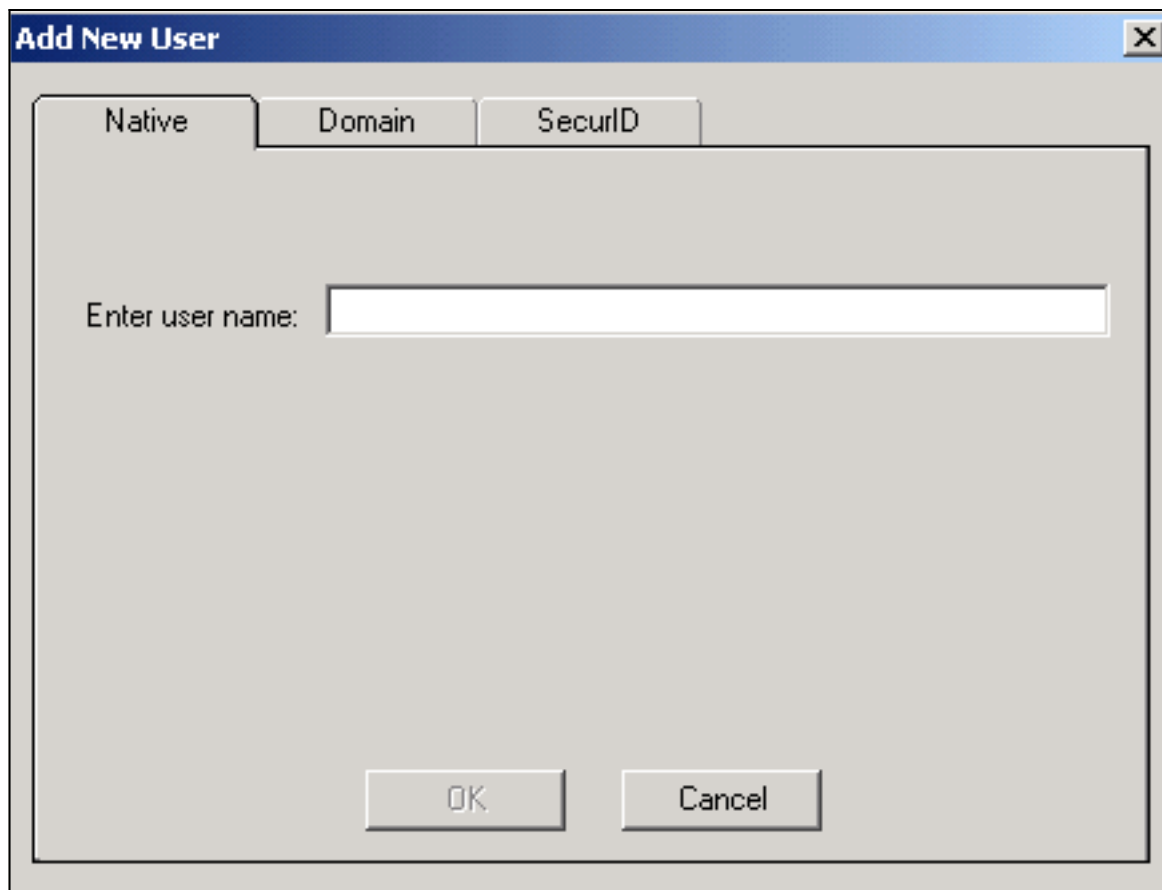
## Создание пользователей в радиусе Steel-Belted

В этом разделе описывается создать нового собственного (локального) пользователя с продуктом Funk Software, Inc., Радиусом Steel-Belted. Если Домен или Пользователь рабочей группы должны быть добавлены, свяжитесь [с Компанией Funk Software](#) для помощи. Записи собственного пользователя требуют, чтобы имя и пароль пользователя было введено в локальную базу данных Радиуса Steel-Belted. Для всех других типов Вводов пользователя Радиус Steel-Belted полагается на другую базу данных для проверки учетных данных пользователя.



Выполните эти шаги для настройки Собственного пользователя в Радиусе Steel-Belted:

1. На Меню Users **нажмите Add** для создания нового пользователя.



2. Нажмите вкладку **Native**, введите имя пользователя в поле и нажмите **OK**. Добавление Новых завершений диалогового окна User.
3. В диалоговом окне Users выберите пользователя и нажмите **Set**



Password.

4. Введите пароль для пользователя и нажмите **Set**.
5. В диалоговом окне Users нажмите **Save**, и вы создали пользователя.

## [Дополнительные сведения](#)

- [Настройка безопасности](#)
- [Компания Funk Software](#)
- [Wireless, LAN \(WLAN\)](#)
- [Техническая поддержка - Cisco Systems](#)