Contents

1 Overview 2

2 Requirements 3

2.1 Java 3

2.2 PHP / MySQL / Apache 3

3 CoovaRADIUS Personal Edition 3

3.1 Installation 4

3.2 Basic Setup 4

4 Drupal Captive Portal 5

4.1 Required Modules 5

4.2 Installation 6

4.3 Configuration 6

4.4 Modules Settings 6

4.5 Other settings 10

5 CoovaChilli Configuration 10

5.1 Basic Settings 10

5.2 CoovaAP Example 11

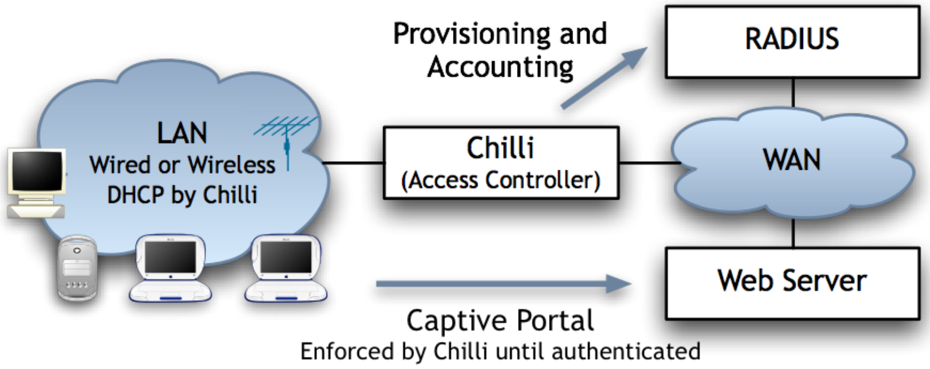
5.3 Open-mesh.com Example 13

6 Getting On-line 15

7 Online Resources 17

1 Overview

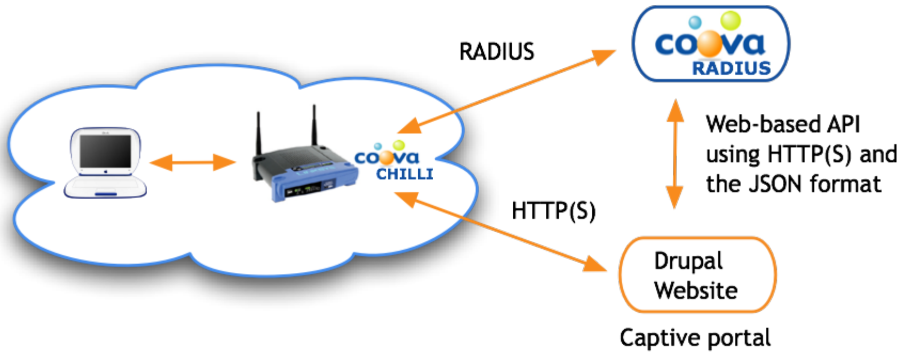
This guide explains how to setup a basic Hotspot using the freeware CoovaRADIUS Personal Edition and the Drupal content management system together with CoovaChilli.



CoovaChilli is access controller software which typically resides in the WiFi router. It can be installed easily on any Linux-based router, including OpenWrt routers, and also comes standard in CoovaAP (see section 5.2) and Open-mesh.com (see section 5.3) nodes.

In the guide, we are building up a Drupal website whereby logged-in Drupal users automatically get Internet access. We will also be configuring an option to allow anonymous users access where we limit the bandwidth to 10KBps and only give the user one minute of Internet access time before having to revisit the captive portal.

In order to achieve this, we utilize the Drupal Hotspot module to handle the interaction with CoovaChilli. The CoovaEWT and CoovaRADIUS modules provide additional integration for provisioning access through the CoovaRADIUS Server, as shown below.



The reader is assumed to be familiar with basic system administration and has installed Drupal before. Command line instructions provided here are for Ubuntu Linux, but the basic concepts and procedure would be the same on other platforms, including Mac and Windows.

Of course, there are many other possible configurations! The Drupal modules mentioned in the guide are in active development and more features will become available. However, also be warned that not all options in the modules work and there are still a few bugs in certain configurations. Contributions, bug reports, and suggestions are all welcome!

2 Requirements

CoovaRADIUS Personal Edition requires only Java 6. The Drupal website requires more; mainly PHP, a database, and a web server. You can either install your own Drupal website or find one of the many companies offering PHP website and database hosting services.

2.1 Java

Download and install Java JRE or JDK version 6 from http://java.sun.com/. On Ubuntu, do the following:

```
sudo apt-get install sun-java6-bin
```

Once installed, ensure that java program is in your path. If you installed using the above command, then the following is required:

```
export JAVA_HOME=/usr/lib/jvm/java-6-sun
export PATH=$JAVA_HOME/bin:$PATH
```

2.2 PHP / MySQL / Apache

We assume the reader is able to install a typical Drupal environment or has access to one. Drupal requires PHP, a database, and a web server. For the database we used MySQL and Apache for the web server, but it doesn't necessarily matter.

The Drupal modules do require the JSON and CURL extensions built into PHP, which is typical in most installations. On Ubuntu, do the following to get the required software:

```
sudo apt-get install mysql-server
sudo apt-get install apache2 libapache2-mod-php5
sudo apt-get install php5-curl php5-mysql
```

3 CoovaRADIUS Personal Edition

The CoovaRADIUS Personal Edition is available for non-commercial use as freeware. For a database this edition uses an embedded HSQLDB. To use with another database, for additional features, or for a commercial license, contact consulting@coova.com.

3.1 Installation

Download and start CoovaRADIUS Personal Edition by doing the following:

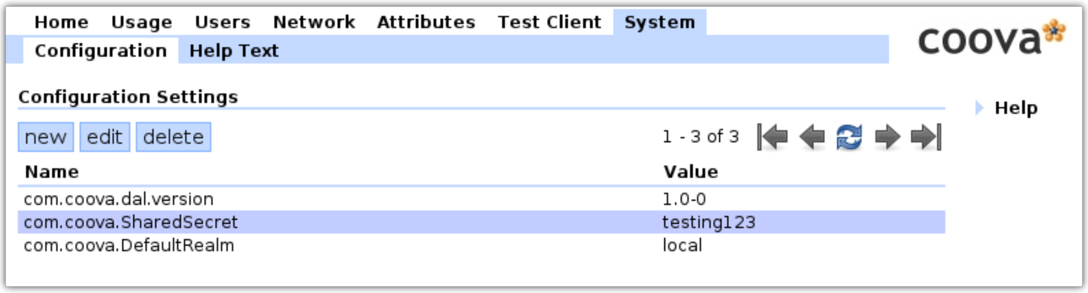
```
wget http://ap.coova.org/coova-radius-personal.zip
unzip coova-radius-personal.zip
cd coova-jradius
sh start.sh
```

Access the web administration interface using the URL:

```
http://localhost:1900/ewt/com.coova.ewt.Home/Coova.html
```

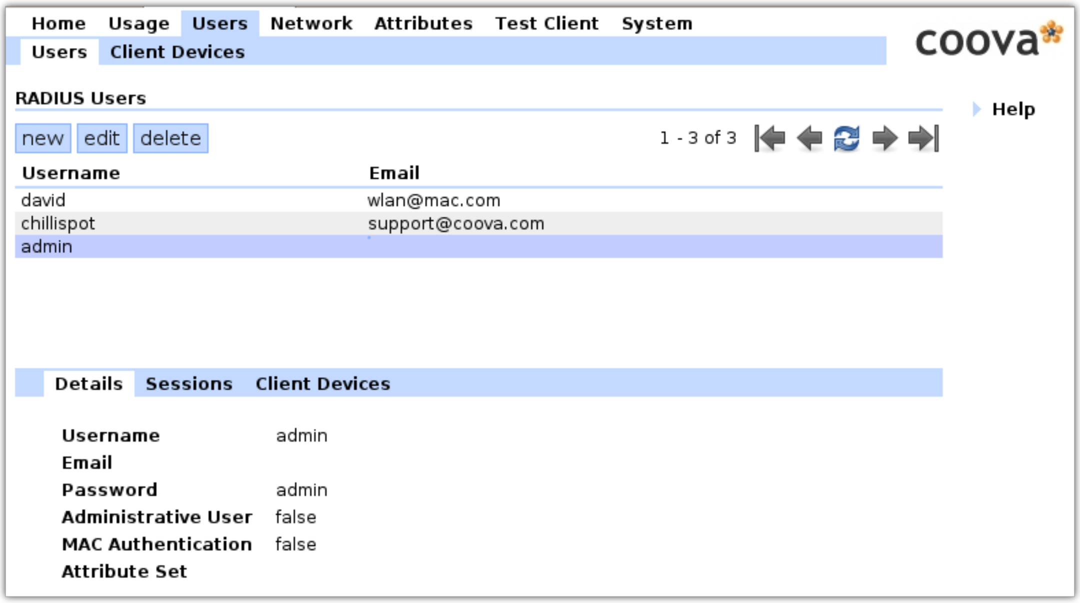
3.2 Basic Setup

In the System Configuration tab, edit the configuration item with name `com.coova.SharedSecret`, setting the value to be the RADIUS shared secret you plan on using. The default is `testing123`.



Name	Value
com.coova.dal.version	1.0-0
com.coova.SharedSecret	testing123
com.coova.DefaultRealm	local

Under the Users tab, you might change the `admin` user password, which defaults to `admin`. This user is the only user able to access the administration interface. It is also used as the EWT API User configured later on.



RADIUS Users

Username	Email
david	wlan@mac.com
chillispot	support@coova.com
admin	

Username	admin
Email	
Password	admin
Administrative User	false
MAC Authentication	false
Attribute Set	

Also see the CoovaRADIUS Personal Edition documentation for more information on the features available in this CoovaRADIUS platform and administrative interface.

4 Drupal Captive Portal

Here we will show how to setup Drupal with the Hotspot and CoovaEWT modules to integrate with CoovaRADIUS. Though, the Drupal Hotspot module is made to be generic and can be used as-is to provide a simple login form to authenticate your users against an existing RADIUS server.

4.1 Required Modules

The required Drupal modules:

Hotspot

The Hotspot module provides the integration glue between CoovaChilli and Drupal, making your Drupal website able to operate as a captive portal hotspot login page. It also serves as an example for any PHP website.

Included with the Hotspot module, but activated separately, is the CoovaRADIUS module. This module extends the Hotspot module and interfaces with the CoovaRADIUS Java Server through the use of the CoovaEWT module.

CoovaEWT

The CoovaEWT module is needed to integrate the Hotspot and CoovaRADIUS Drupal modules with CoovaRADIUS Java Server to provide advanced access provisioning options. Additionally, the CoovaEWT module provides the ability to integrate graphical users interfaces and data from CoovaRADIUS Server into Drupal pages.

4.2 Installation

Download and install Drupal 6.6. If you are already using Drupal 6, you should be able to just add the required modules to your existing installation. Otherwise, here are some simple instructions for installing Drupal.

To make things easier, we have packaged up the standard Drupal 6.6 distribution with the required modules.

To install:

```
cd /var/www/
wget http://ap.coova.org/drupal-6.6-with-coova-hotspot.tgz
tar xzvf drupal-6.6-with-coova-hotspot.tgz
```

Create your Drupal database:

```
mysqladmin create drupal
```

Finish up the installation for Drupal using your browser. In our case, this URL is:

```
http://localhost/drupal-6.6/
```

Follow the installation instructions to get your Drupal site up and running.

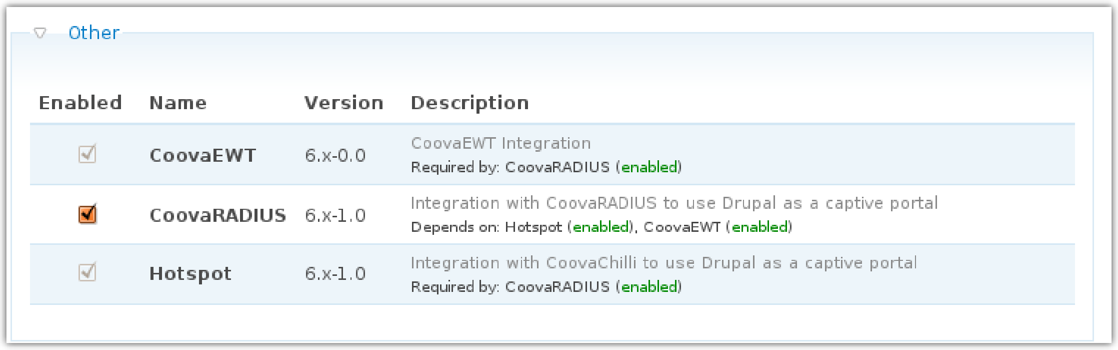
For additional help installing Drupal, see the videocast at Drupal.org.

4.3 Configuration

Here we give instructions on how to setup Drupal and the modules. When referring to Drupal pages, we provide the Drupal path to make it easier to know exactly what page we are discussing. To access the page in your Drupal site, simply change the URL in your browser.

4.4 Modules Settings

Drupal Page: `admin/build/modules`



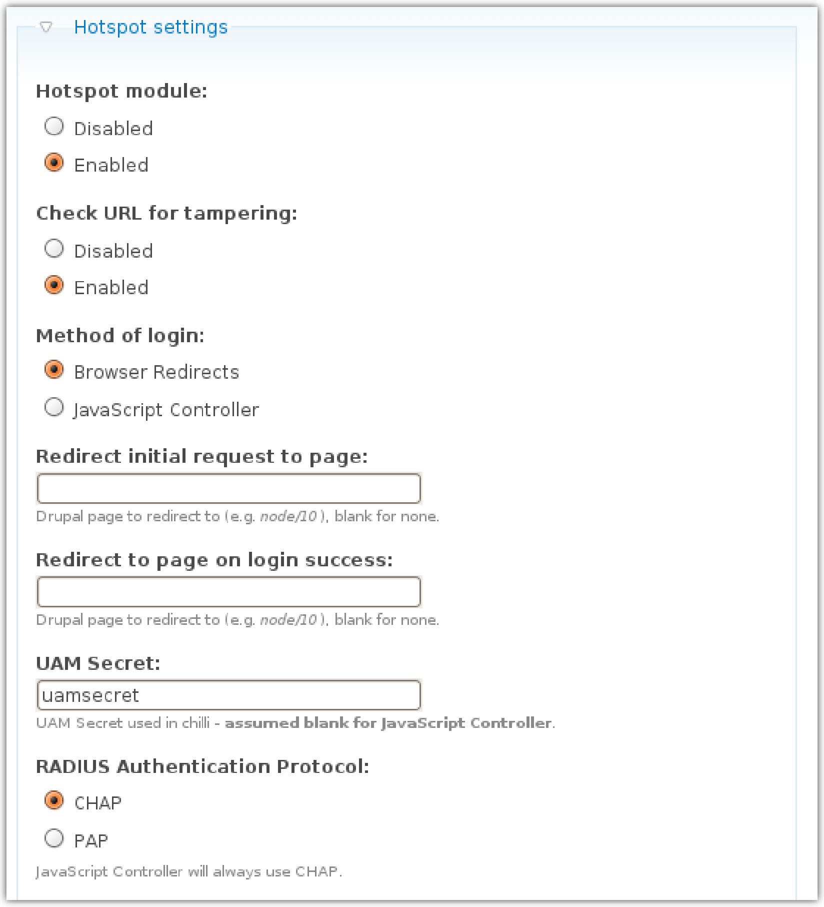
▽ Other

Enabled	Name	Version	Description
☑	CoovaEWT	6.x-0.0	CoovaEWT Integration Required by: CoovaRADIUS (enabled)
☑	CoovaRADIUS	6.x-1.0	Integration with CoovaRADIUS to use Drupal as a captive portal Depends on: Hotspot (enabled), CoovaEWT (enabled)
☑	Hotspot	6.x-1.0	Integration with CoovaChilli to use Drupal as a captive portal Required by: CoovaRADIUS (enabled)

Enable the CoovaEWT, CoovaRADIUS, and Hotspot modules.

Hotspot Module Settings

Drupal Page: `admin/settings/hotspot`



▽ Hotspot settings

Hotspot module:
○ Disabled
● Enabled

Check URL for tampering:
○ Disabled
● Enabled

Method of login:
● Browser Redirects
○ JavaScript Controller

Redirect initial request to page:

Drupal page to redirect to (e.g. *node/10*), blank for none.

Redirect to page on login success:

Drupal page to redirect to (e.g. *node/10*), blank for none.

UAM Secret:
uamsecret
UAM Secret used in chilli - **assumed blank for JavaScript Controller**.

RADIUS Authentication Protocol:
● CHAP
○ PAP
JavaScript Controller will always use CHAP.

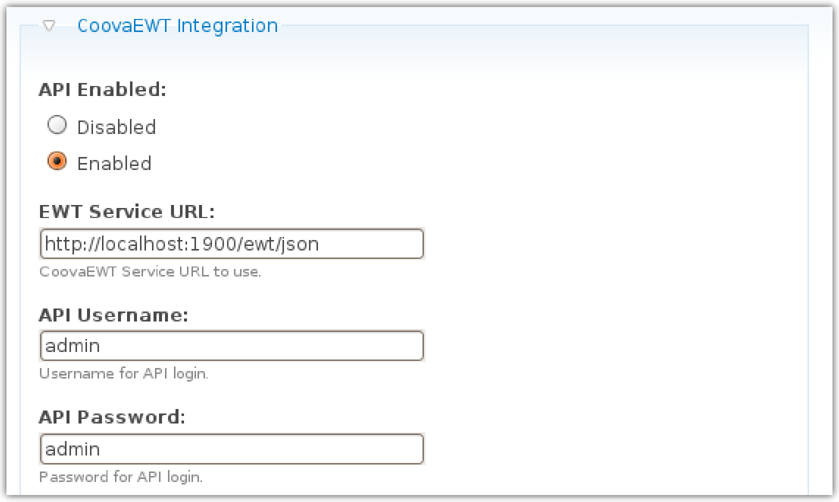
Enable the Hotspot module and set the following values:

- **Hotspot module** set to `Enabled`
- **Check URL for tampering** if set to `Enabled`, the module will ensure the URL carrying information from CoovaChilli has not been tampered with.
- **Method of login** set to `Browser Redirects`, at the moment this is the more robust method.
- **UAM Secret** in this case is set to `uamsecret`, but you should create your own UAM secret. It can be anything, it just needs to match what you configure in CoovaChilli.
- **RADIUS authentication protocol** is set to `CHAP`.

There are additional settings possible too. For instance, you may want to remove the login form from the landing page altogether if you only plan on authenticating your Drupal users. To do so, simply disable the login form under the "Access Provisioning" section of the same page.

CoovaEWT Module Settings

Drupal Page: `admin/settings/ewt`



▽ CoovaEWT Integration

API Enabled:

○ Disabled

● Enabled

EWT Service URL:

http://localhost:1900/ewt/json

CoovaEWT Service URL to use.

API Username:

admin

Username for API login.

API Password:

admin

Password for API login.

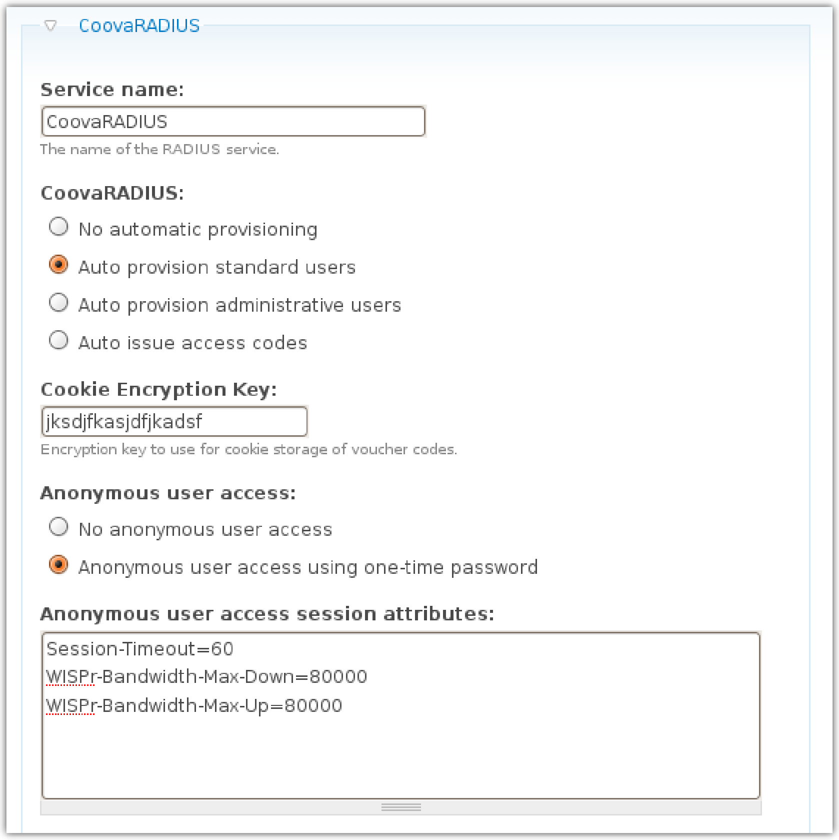
Set the following values, which may be different for you depending on how you configured CoovaRADIUS.

- **API Enabled** set to `Enabled`
- **EWT Service URL** set to `http://localhost:1900/ewt/json` - which is the EWT API URL in CoovaRADIUS running on the same server.
- **API Username** set to `admin`
- **API Password** set to `admin`, or to another value if you changed the password in CoovaRADIUS.

The **Enable CoovaEWT GUI and Ajax Proxy** option (not shown) is not needed and should be left on `Disabled`.

CoovaRADIUS Module Settings

Drupal Page: `admin/settings/coova_radius`



CoovaRADIUS

Service name:

CoovaRADIUS

The name of the RADIUS service.

CoovaRADIUS:

○ No automatic provisioning

● Auto provision standard users

○ Auto provision administrative users

○ Auto issue access codes

Cookie Encryption Key:

jksdjfkasjdfjkadsf

Encryption key to use for cookie storage of voucher codes.

Anonymous user access:

○ No anonymous user access

● Anonymous user access using one-time password

Anonymous user access session attributes:

```
Session-Timeout=60
WISPr-Bandwidth-Max-Down=80000
WISPr-Bandwidth-Max-Up=80000
```

In this example, we have set **Auto provision standard users** to have logged in Drupal users automatically logged into the Internet.

Also set a **Cookie Encryption Key** to any random string. It's used to protect information the module might store in a Cookie stored in the user's browser.

We also enabled **Anonymous user access** to have a link displayed for anonymous users to gain access for free. You can also provide RADIUS attributes for these free sessions. Here, using the following attributes, we will limit the up/down speed to 10KBps and have the user return to the portal every 60 seconds.

```
Session-Timeout=60
```

```
WISPr-Bandwidth-Max-Down=80000
WISPr-Bandwidth-Max-Up=80000
```

Under `CoovaRADIUS Advanced` menu, only a couple options are valid for use with CoovaRADIUS Personal. You can, however, Enable MAC authentication for auto-created users.

4.5 Other settings

Blocks

Drupal Page: `admin/build/block`

Here, you can add the **Hotspot Status block** to your preferred page region to give users a status of their Internet session.

Other settings

Drupal Page: `admin/user/settings`

The default in Drupal is to send an e-mail to newly registered users with their automatically generated password. Therefore, the user must have access to their e-mail to complete their Drupal login. This will prevent people from signing up at your hotspot - unable to check their e-mail until later. To change this, uncheck the option **Require e-mail verification when a visitor creates an account**.

5 CoovaChilli Configuration

CoovaChilli can run on many types of routers and systems. We will give some basic instructions on how to configure CoovaChilli, but how you configure it may greatly depend on your specific situation. For instance, if running Open-mesh routers, you can configure the relevant settings in the Open-mesh Dashboard. For more information on configuring CoovaChilli, refer to the CoovaChilli Documentation on-line.

5.1 Basic Settings

Ultimately, you need CoovaChilli configured with the following settings. We only show the relevant as there are many ways to setup CoovaChilli, which is outside the scope of this document.

```
radiusserver1   192.168.10.109
radiusserver2   192.168.10.109
radiussecret    testing123
radiusauthport  1812
```

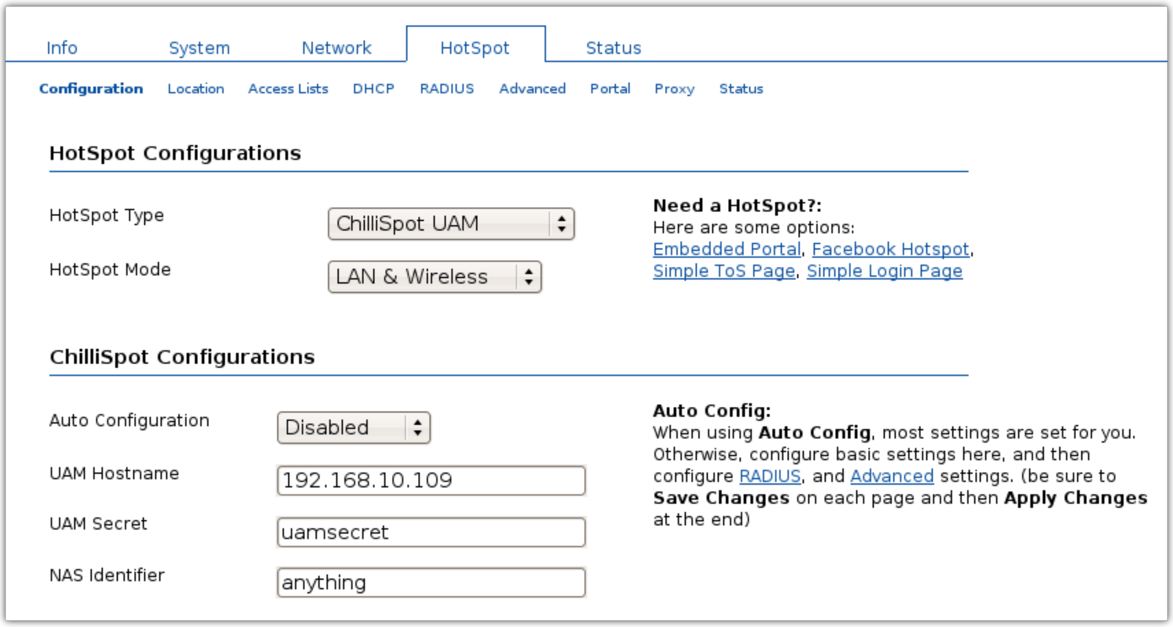
```
radiusacctport  1813
uamserver       http://192.168.10.109/drupal-6.6/?q=hotspot
uamsecret       uamsecret
```

Your settings will vary, to explain:

- **radiusserver1** is set to the IP address of the computer running CoovaRADIUS. In our case, we are setup on `192.168.10.109`, your address will be different.
- **radiusserver2** same as above for now.
- **radiussecret** is the RADIUS shared secret configured in CoovaRADIUS, we're using the default `texting123` for now.
- **radiusauthport** and **radiusacctport** must be 1812 and 1813 respectively.
- **uamserver** is the full URL to your Drupal installation, referencing the hotspot module page.
- **uamsecret** is the same UAM Secret configured in the Drupal Hotspot module.

5.2 CoovaAP Example

Select the `ChlliSpot UAM` option for **Hotspot Type**, as shown:



HotSpot Configurations

HotSpot Type: ChilliSpot UAM

HotSpot Mode: LAN & Wireless

Need a HotSpot?:
Here are some options:
Embedded Portal, Facebook Hotspot, Simple ToS Page, Simple Login Page

ChilliSpot Configurations

Auto Configuration: Disabled

UAM Hostname: 192.168.10.109

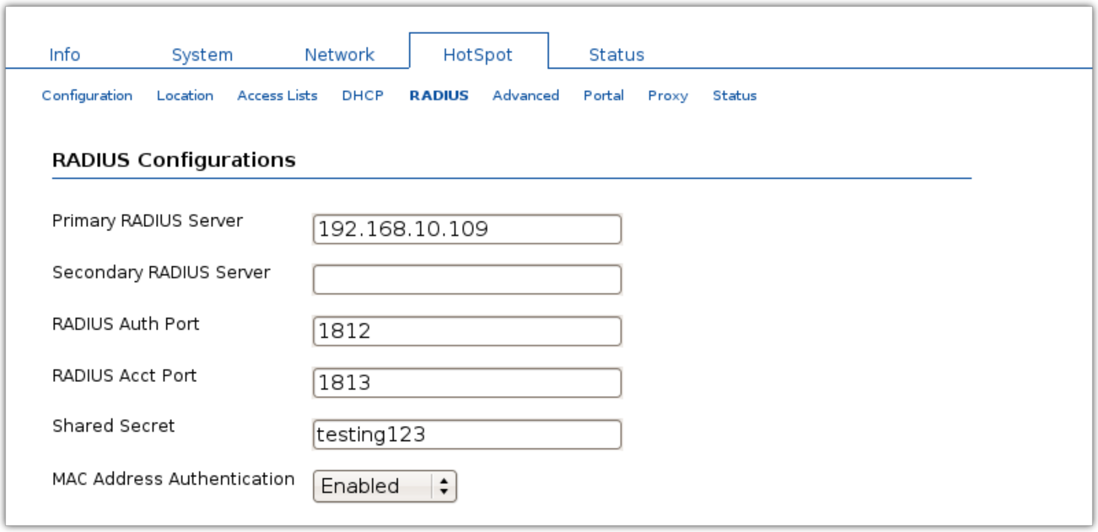
UAM Secret: uamsecret

NAS Identifier: anything

Auto Config:
When using **Auto Config**, most settings are set for you. Otherwise, configure basic settings here, and then configure RADIUS, and Advanced settings. (be sure to **Save Changes** on each page and then **Apply Changes** at the end)

Set the **UAM Server** to be your Drupal website's IP address or hostname. On this page also set the **UAM Secret** you have configured in the Drupal hotspot module. We used `uamsecret`.

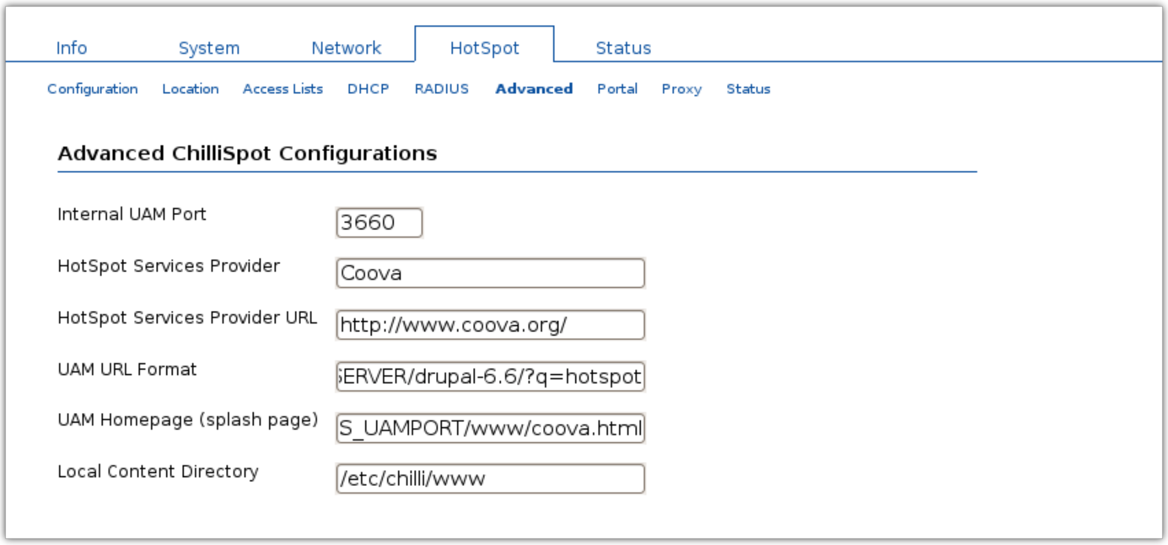
Under the **RADIUS** tab, set the **Primary RADIUS Server** to be the IP address of the machine running CoovaRADIUS, using the default ports of 1812 and 1813. In our example, we kept the default RADIUS shared secret `testing123`, as shown.



RADIUS Configurations

Primary RADIUS Server	192.168.10.109
Secondary RADIUS Server	
RADIUS Auth Port	1812
RADIUS Acct Port	1813
Shared Secret	testing123
MAC Address Authentication	Enabled

Finally, under the **Advanced** tab we need to set the **UAM URL Format** to be that of the Drupal website. Note that this field allows for a variable (the previously configured **UAM Server**). Not completely shown in the screen-shot, the value we used here was `http://$HS_UAMSERVER/drupal-6.6/?q=hotspot`. Keep the default values for everything else.

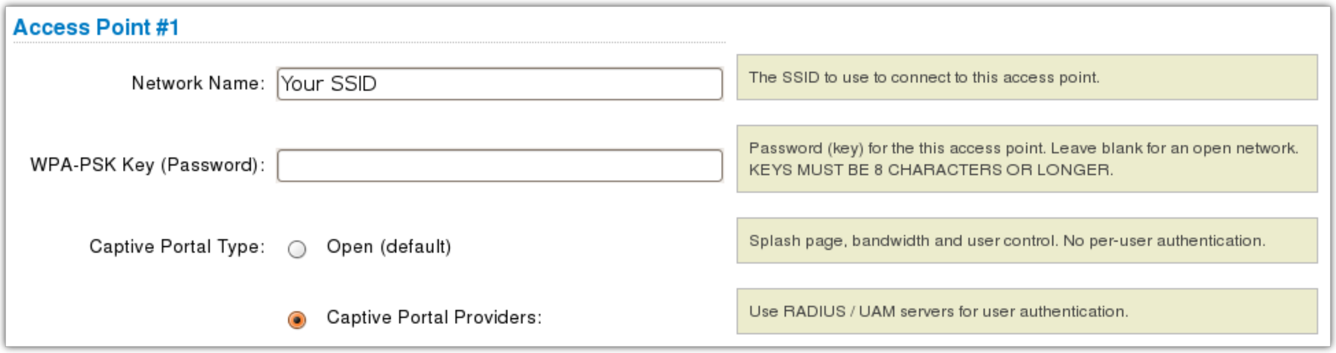


Advanced ChilliSpot Configurations

Internal UAM Port	3660
HotSpot Services Provider	Coova
HotSpot Services Provider URL	http://www.coova.org/
UAM URL Format	;ERVER/drupal-6.6/?q=hotspot
UAM Homepage (splash page)	S_UAMPORT/www/coova.html
Local Content Directory	/etc/chilli/www

5.3 Open-mesh.com Example

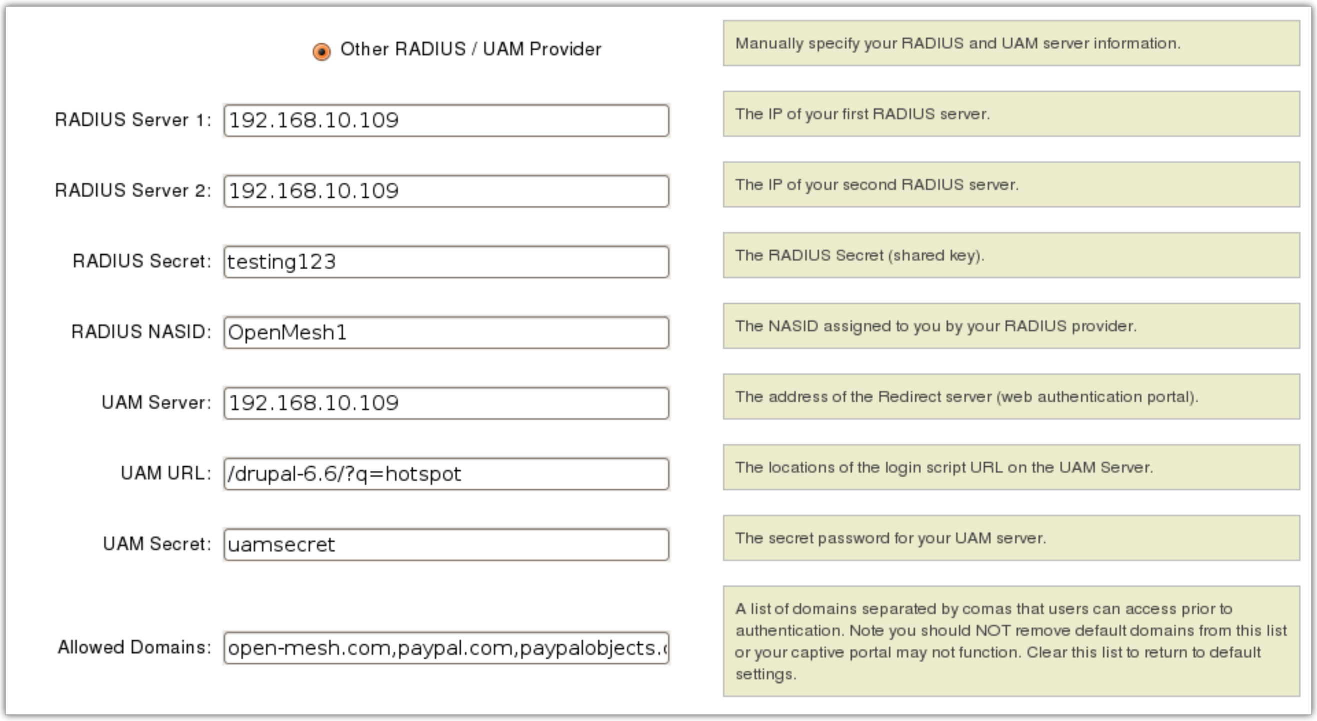
To test things out on your open-mesh.com network, configure your **Access Point #1** in the Open-mesh Dashboard to use a Captive Portal Provider, as shown below.



Access Point #1

Network Name:	Your SSID	The SSID to use to connect to this access point.
WPA-PSK Key (Password):		Password (key) for the this access point. Leave blank for an open network. KEYS MUST BE 8 CHARACTERS OR LONGER.
Captive Portal Type:	○ Open (default)	Splash page, bandwidth and user control. No per-user authentication.
	● Captive Portal Providers:	Use RADIUS / UAM servers for user authentication.

Open-mesh.com supports a number of back-end service, including CoovaAAA, but in this case, we want to select **Other RADIUS / UAM Provider**.



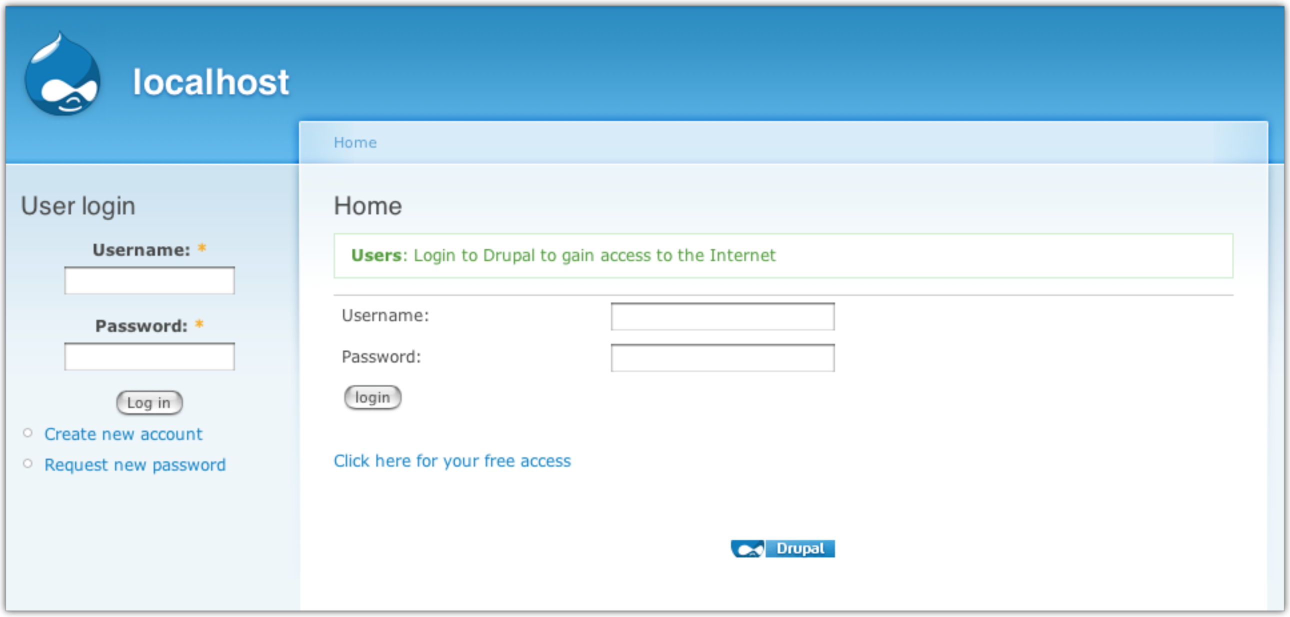
	● Other RADIUS / UAM Provider	Manually specify your RADIUS and UAM server information.
RADIUS Server 1:	192.168.10.109	The IP of your first RADIUS server.
RADIUS Server 2:	192.168.10.109	The IP of your second RADIUS server.
RADIUS Secret:	testing123	The RADIUS Secret (shared key).
RADIUS NASID:	OpenMesh1	The NASID assigned to you by your RADIUS provider.
UAM Server:	192.168.10.109	The address of the Redirect server (web authentication portal).
UAM URL:	/drupal-6.6/?q=hotspot	The locations of the login script URL on the UAM Server.
UAM Secret:	uamsecret	The secret password for your UAM server.
Allowed Domains:	open-mesh.com,paypal.com,paypalobjects.c	A list of domains separated by comas that users can access prior to authentication. Note you should NOT remove default domains from this list or your captive portal may not function. Clear this list to return to default settings.

Explanation of the settings is as follows:

- **RADIUS Server 1** is set to the IP address of the computer running CoovaRADIUS. In our case, we are setup on `192.168.10.109`, your address will be different.
- **RADIUS Server 2** same as above for now.
- **RADIUS Secret** is the RADIUS shared secret configured in CoovaRADIUS, we're using the default `texting123` for now.
- **RADIUS NASID** is not important in this case.
- **UAM Server** is the IP address or hostname of your Drupal server.
- **UAM URL** is the URL path, on the UAM Server, for your Drupal installation's hotspot module page. In our case, we installed Drupal into the base path `/drupal-6.6/`. The `?q=hotspot` query string is added such that the Hotspot module handles the request.
- **UAM Secret** is the same UAM Secret configured in the Drupal Hotspot module.
- **Allowed Domains** defines your walled garden domains. Configure this to allow users access to certain websites before logging in.

6 Getting On-line

With everything up and running, visitors to your hotspot should see the Drupal landing page, as down below.



localhost

Home

User login

Username: *

Password: *

Log in

- Create new account
- Request new password

Home

Users: Login to Drupal to gain access to the Internet

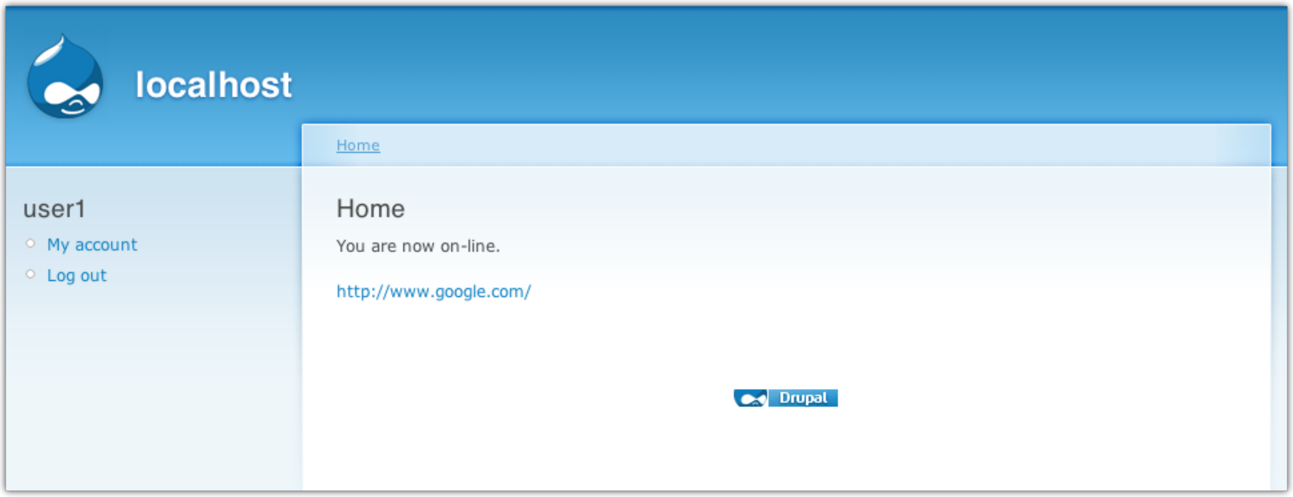
Username:

Password:

login

Click here for your free access

We have it configured to show the Hotspot login form (the login form in the middle of the page), but this can also be removed if you are only allowing logged-in Drupal users on-line. Users configured in RADIUS, but not necessarily Drupal users, can still login using this form. Anonymous users, per our setup, get a link that allows them to get on-line with a reduced bandwidth.

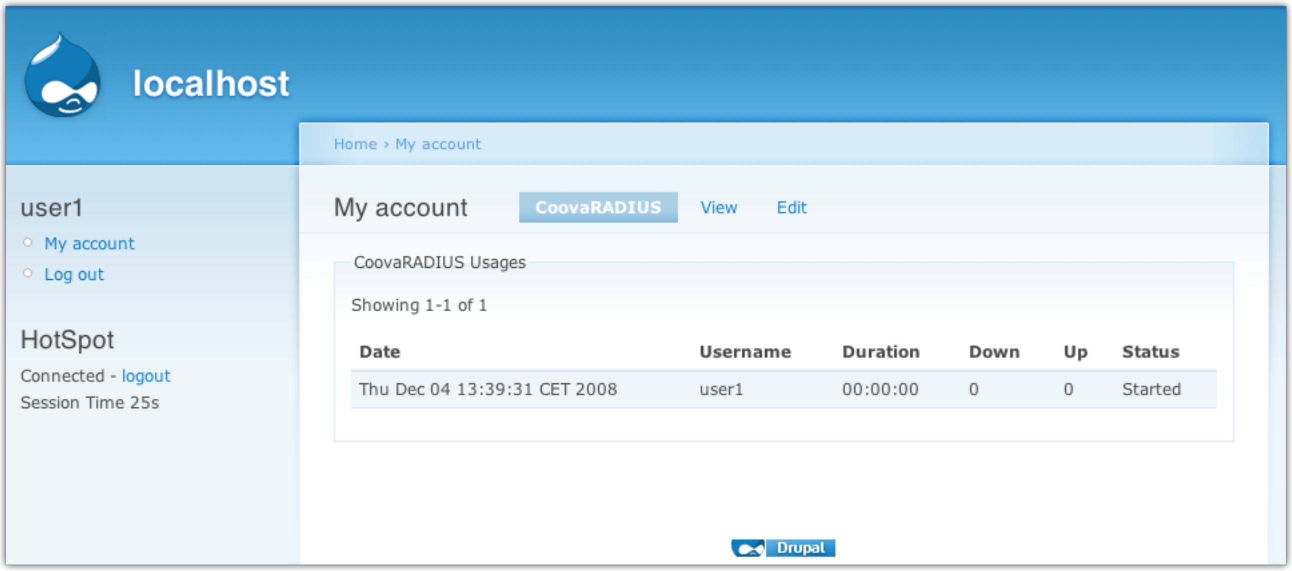


Home

You are now on-line.

http://www.google.com/

When users login to Drupal and try to access the Internet, they instantly get on-line, as shown above. By clicking on their "My Account" link, users are able to see their Hotspot usage, as shown below.



HotSpot

Connected - logout

Session Time 25s

My account

CoovaRADIUS Usages

Showing 1-1 of 1

Date	Username	Duration	Down	Up	Status
Thu Dec 04 13:39:31 CET 2008	user1	00:00:00	0	0	Started

This example showed just one possible use of the Drupal Hotspot module. Just like with Drupal itself, the possibilities are endless.

7 Online Resources

- CoovaChilli Website - The official website of the CoovaChilli project.
- CoovaAP Website - The official website of the CoovaAP firmware project.
- ROBIN Firmware - The official website of the ROBIN firmware project.
- CoovaSX Website - Login "smart-client" for your cell phone.
- CoovaFX Website - Login "smart-client" for your firefox browser.
- JRadius Website - The official website of the JRadius project.
- Using JRadius with FreeRADIUS - Information on how to compile and configure FreeRADIUS for use with JRadius.
- Running JRadius Server - Information on running the JRadius server, a Java server that runs independently of FreeRADIUS.
- Building JRadius Dictionary - Follow these instructions to create a new JRadius RADIUS attributes dictionary.
- RADIUS Simulator - The graphical JRadiusSimulator application to construct RADIUS packets by hand for testing purposes.
- JRadius JavaDoc - Download or view the JRadius javadoc on-line.