

Features: How to set up my wireless hotspot to work together with CafeSuite?

The new CafeSuite RADIUS module makes it possible to authorize laptop users through CafeSuite. The requirement is to have a wifi router with RADIUS-authenticated captive portal feature, for example [Open-Mesh](#) or routers flashed with DD-WRT firmware. It's a bit tricky to set up, but perhaps we will have pre-configured routers in offer soon.

You will need:

- the latest CafeSuite (available on [Downloads](#) page)
- router wifi with DD-WRT firmware or similar that has a hotspot/captive portal feature (e.g. OpenMesh, CoovaAP)
- optionally https server where logon page will be hosted (or alternatively you could use our server)

Steps:

- upgrade CafeSuite to the latest version
- during installation leave Install CafeSuite Radius Service for wifi hotspot checkbox enabled
- execute CafeStation and enter main program settings (menu Program/Options)
- activate option Enable RADIUS server on Advanced/Radius page, leave default port numbers, enter any password as Secret and remember it
- activate option Enable built-in web server on Advanced/Web services page, type some username and password for security
- enter your router's hotspot settings (Services/Hotspot/Chillispot for DD-WRT or Dashboard/Edit network/SSID #1 for OpenMesh)

Settings for Chillispot:

[*] Chillispot: Enable

[*] Separate Wifi from the LAN Bridge: Enable

[*] Primary Radius Server IP/DNS: IP number of PC with CafeSuite Radius Module

[*] Backup Radius Server IP/DNS:

[*] Shared Key: earlier typed password at Secret field on Advanced/Radius page

[*] DNS IP: IP number of a DNS server in LAN Remote Network: 192.168.182.0/24 (IP number and network mask of wifi network)

[*] Redirect URL: <https://cafegate.com/hotspot/timecode.php> (if users should log in with timecode only) or <https://cafegate.com/hotspot/> (if username/password logon is required)

[*] DHCP Interface: eth1

[*] Radius NAS ID: anything, e.g. CAFE1

[*] UAM Secret: test

[*] UAM Any DNS: 0

[*] UAM Allowed: websites that can be accessed without logging in separated by comma

[*] MACauth: disabled

More information about settings: <http://www.dd-wrt.com/wiki/index.php/Chillispot>

Settings for Open-Mesh routers:

[*] Captive Portal Options: Other RADIUS Provider

Features: How to set up my wireless hotspot to work together with CafeSuite?

- [*] RADIUS Server: IP number of PC with CafeSuite Radius Module
- [*] RADIUS Secret: earlier typed password at Secret field on Advanced/Radius page
- [*] RADIUS NASID: anything, e.g. CAFE1
- [*] UAM Server: <https://cafegate.com/hotspot/timecode.php> (if users should log in with timecode only) or <https://cafegate.com/hotspot/> (if username/password logon is required)
- [*] UAM URL:
- [*] UAM Secret: test
- [*] Allowed Domains: websites that can be accessed without logging in separated by comma
- [*] ChilliSpot Compatible: enabled

Logon script can also be hosted on your own www server - the php and cgi code is available in CafeSuite/Radius folder. Then instead of <https://cafegate.com/hotspot/> you need to enter URL to your own logon page and set identical UAM secret as in page script.

After connecting laptop with your public WIFI network and opening browser, user should get redirected to logon page. After correct logon, in CafeStation a new session will be started on a new workstation assigned to wifi group. After user logs off, the workstation will automatically be removed.

Unique solution ID: #1188

Author: Przemek Miszczuk

Last update: 2014-05-20 14:06