Captive Portal

Functional Overview

The Captive Portal solution provided by CradlePoint routers allows businesses the ability to provide their customers with a public WiFi hotspot with access controls. The controls can be as simple as requiring acceptance of a Terms of Service (ToS) agreement. Advanced features can control and monitor usage, require login, direct users to specific web pages, provide revenue through service fees or paid advertising and more.

Overview

- Two Modes: Simple (router only) and RADIUS authentication (hosted server).
- Captive portal allows the admin/owner of the router to capture all associating clients attempting to access the web in a limited service "walled garden".
- Only specified web access is allowed until the client accepts either Terms of Service (ToS) or meets other authentication requirements.
- After the authentication requirements are met, the client can then surf normally outside the walled garden.
- This feature is found at System Settings->Hotspot Services
- Available with the following CradlePoint Routers: MBR1400, CBR400, COR IBR600

Key Features

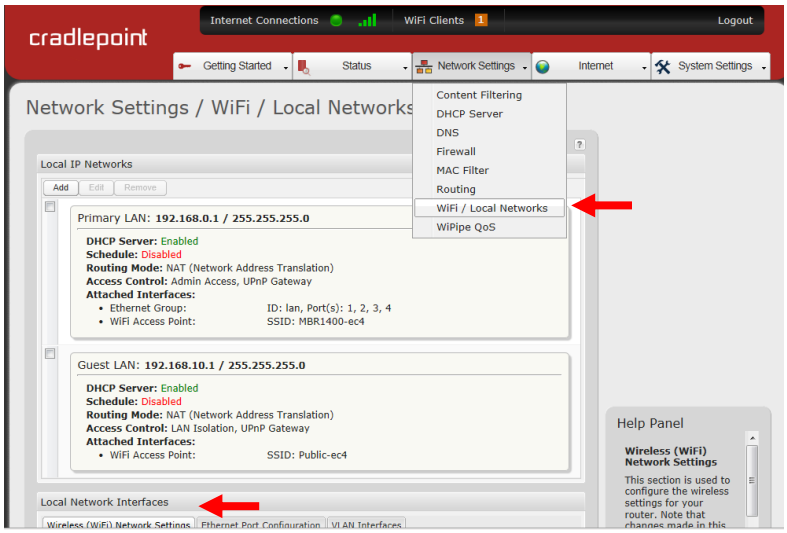
- Require ToS acceptance to use WiFi hotspot if desired
- URL redirect to administer-defined URL on authentication if desired
- Disable WiFi hotspot service when on 3G/4G failover service if desired
- The ability to utilize 3rd party AAA RADIUS hotspot services[1]
    - Customizable splash pages
    - User login credential checking
    - Hotspot billing services (credit cards, vouchers, SMS authentication, etc)
    - Revenue sharing
    - Advertising revenue
    - Transaction reports
    - User search and usage information
    - Custom reporting
    - And much more offered by 3rd party services

[1] CradlePoint does not offer the 3rd Party AAA RADUS authentication service and additional fees may apply, though free services are available.

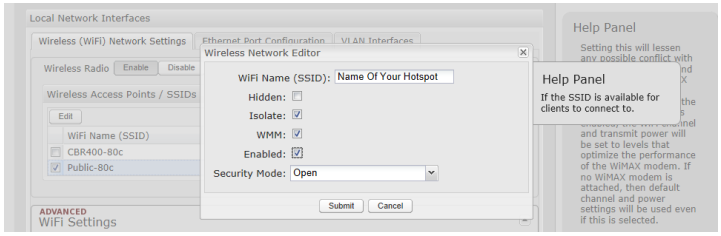
Generic Setup Steps for Any Hotspot:

Setup and configure the SSID and LAN for Hotspot mode

Go to Network Settings → WiFi / Local Networks

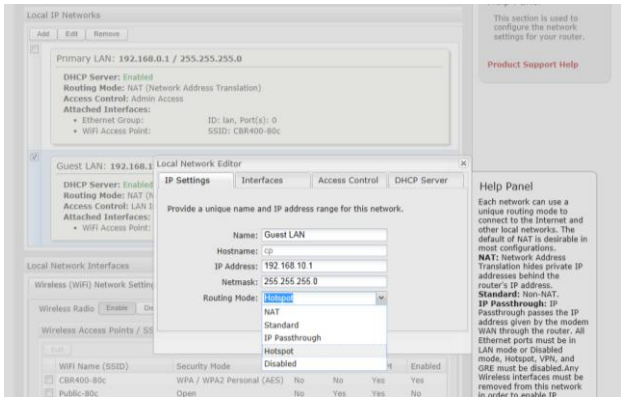


Find **Local Network Interfaces** and select the **WiFi Name (SSID)** you want to make the hotspot (Public-xxx suggested) and click **Edit**. Change the WiFi Name (SSID) to something you choose and select **Enabled**. Click **Submit**.



Configure LAN for Hotspot Routing Mode

Find **Local IP Networks** and select the **LAN** you want to use for the hotspot (Guest LAN suggested) and click **Edit**. Change the Routing Mode to **Hotspot**. On the **Interface** tab ensure **Enable** is selected. Click **Submit**.



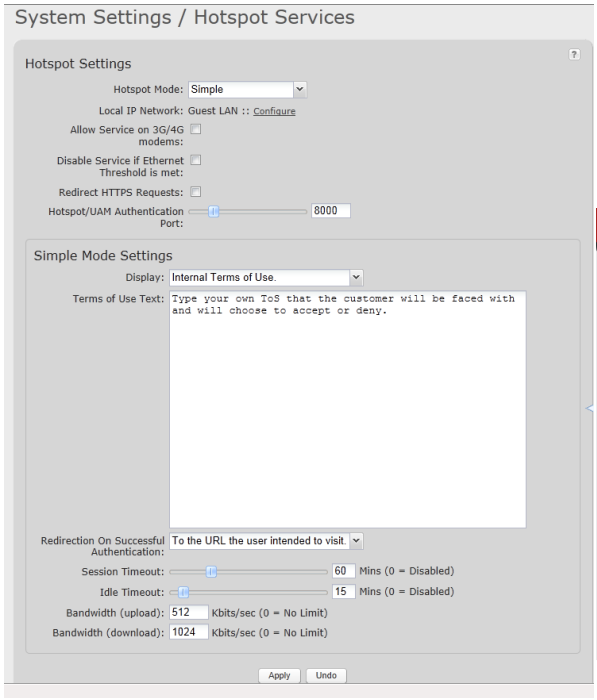
Go to System Settings → Hotspot Services

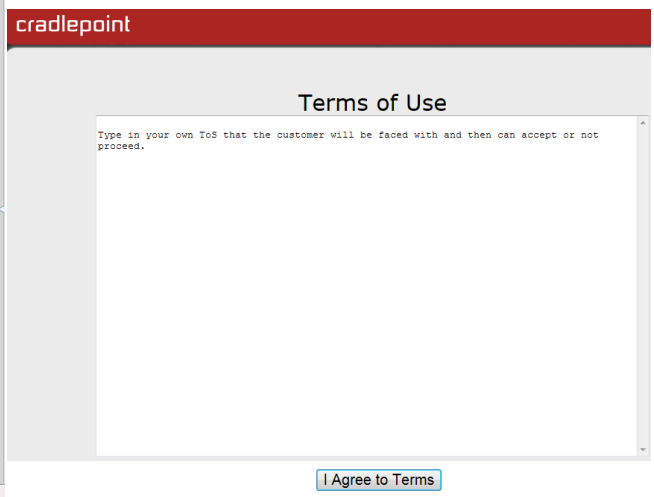
Mode 1: Simple Captive Portal Mode – Terms of Service (ToS):

Simple mode redirects any associated clients attempting to surf the web to a CradlePoint branded *Terms of Service* page. From here, the client either accepts the owner/admin defined terms of service – allowing them to surf normally outside the walled garden - or the client does not accept and remains 'captive' in the walled garden with internet access denied except for owner specified URL locations.

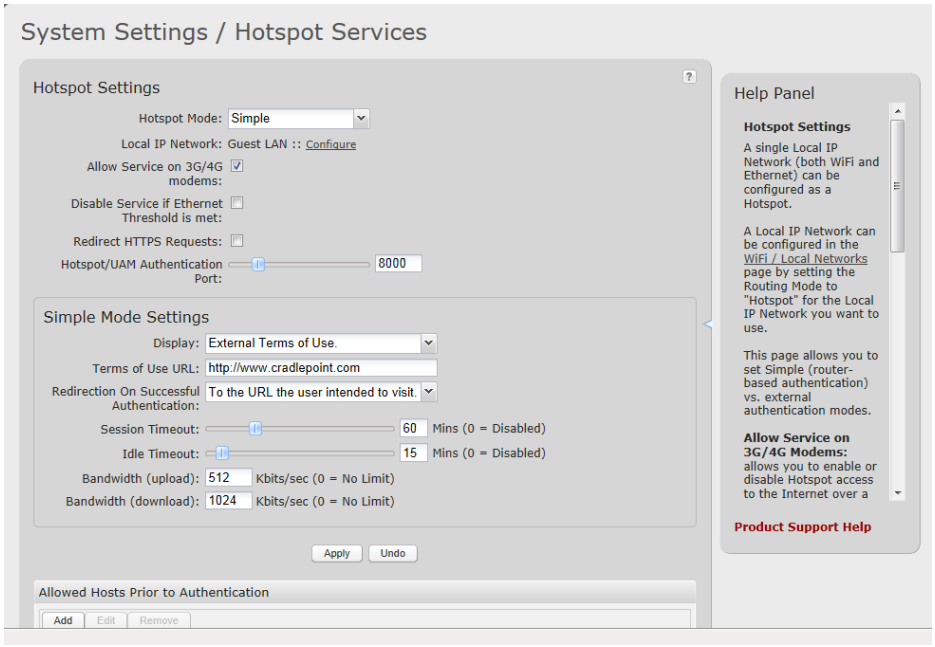
There are also a number of settings you may wish to configure including allowing captive portal on 3G/4G modems, disabling service if thresholds are met, session timeouts and bandwidth limiting. See the help bar for more detailed explanations.

Simple Hotspot Setup (Internal Terms of Use)



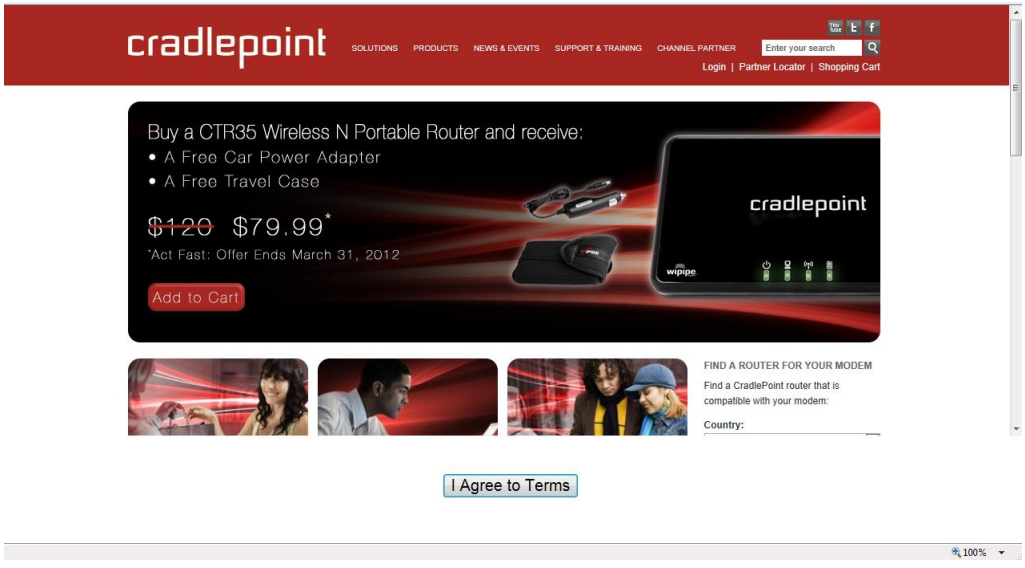


Simple Hotspot Setup (External Terms of Use)



Simple Hotspot External Terms of Use When Attempting to Connect

(Note: you would direct them to an external webpage that you created with ToS listed on the page, we use our homepage as an example external page but it doesn't actually have any terms to accept.)



Mode 2: Radius Authentication Captive Portal:

The captive portal Radius mode allows the admin/owner to configure a third-party RADIUS server[2] with customizable splash pages and provides a standard UAM (Universal Access Method) form and can account for all clients associating. Clients in this case would be required to authenticate before accessing the web. The client(s) will be more or less unaware of the existence of the RADIUS server beyond entering credentials (rather than a simple acceptance of Terms of Service) to gain access to the Internet.

The radius mode allows for use of either an 'in-house' RADIUS hosted server, set up, and configured by the admin/owner or a 'hosted' RADIUS server set up and configured by a third party but customized by the admin/owner for use with the CradlePoint captive portal feature.

Example: Hosted RADIUS server solutions include www.hotspotsystem.com.

NOTE: The captive portal feature does not remember clients. Each time a client's session is terminated for any reason re-authentication will be required before the client can surf again.

[2] CradlePoint does not offer the 3rd Party AAA RADUS authentication service and additional fees may apply, though free services are available.

Hotspotsystem Example:

HOTSPOTSYSTEM has an example setup on their website optimized for use with CradlePoint routers:
http://www.hotspotsystem.com/en/hotspot/install_guide_cradlepoint_3g_mobile.html

When using www.hotspotsystem.com here are the recommended settings

Hotspot Mode: RADIUS/UAM

LAN: Guest LAN (though you can choose a different LAN)

Allow Service on 3G/4G modems: YES (if desired)

Disable Service if Ethernet Threshold is met: (if desired)

Redirect HTTPS Requests: YES

Hotspot/UAM Authentication Port: 3990

RADIUS Settings

Server Address: radius.hotspotsystem.com

Server Address: radius2.hotspotsystem.com

Authentication Port: 1812

Accounting Port: 1813

Shared Secret: hotsys123

Confirm Secret: hotsys123

Redirection on Successful Authentication: To the UAM Server

Session Timeout: 60 Mins

Idle Timeout: 15 Mins

Bandwidth (upload): 512 (note: the radius service may provide thresholds as well in which case this number may be ignored)

Bandwidth (download): 1024 (note: the radius service may provide thresholds as well in which case this number may be ignored)

UAM Settings:

https://customer.hotspotsystem.com/customer/hotspotlogin.php?mode=comb

Shared Secret: hotsys123

Confirm Secret: hotsys123

NAS/GatewayID: operatorusername_locationID. You must register with hotspotsystems and they will provide this ID. (It is a combination of your login username and Location ID).

operatorusername_locationID (example: if your operator username is "cafehotspot" and this is your first location, enter "cafehotspot_1")

Find Allowed Hosts Prior to Authentication. Click add.

Add the following values:

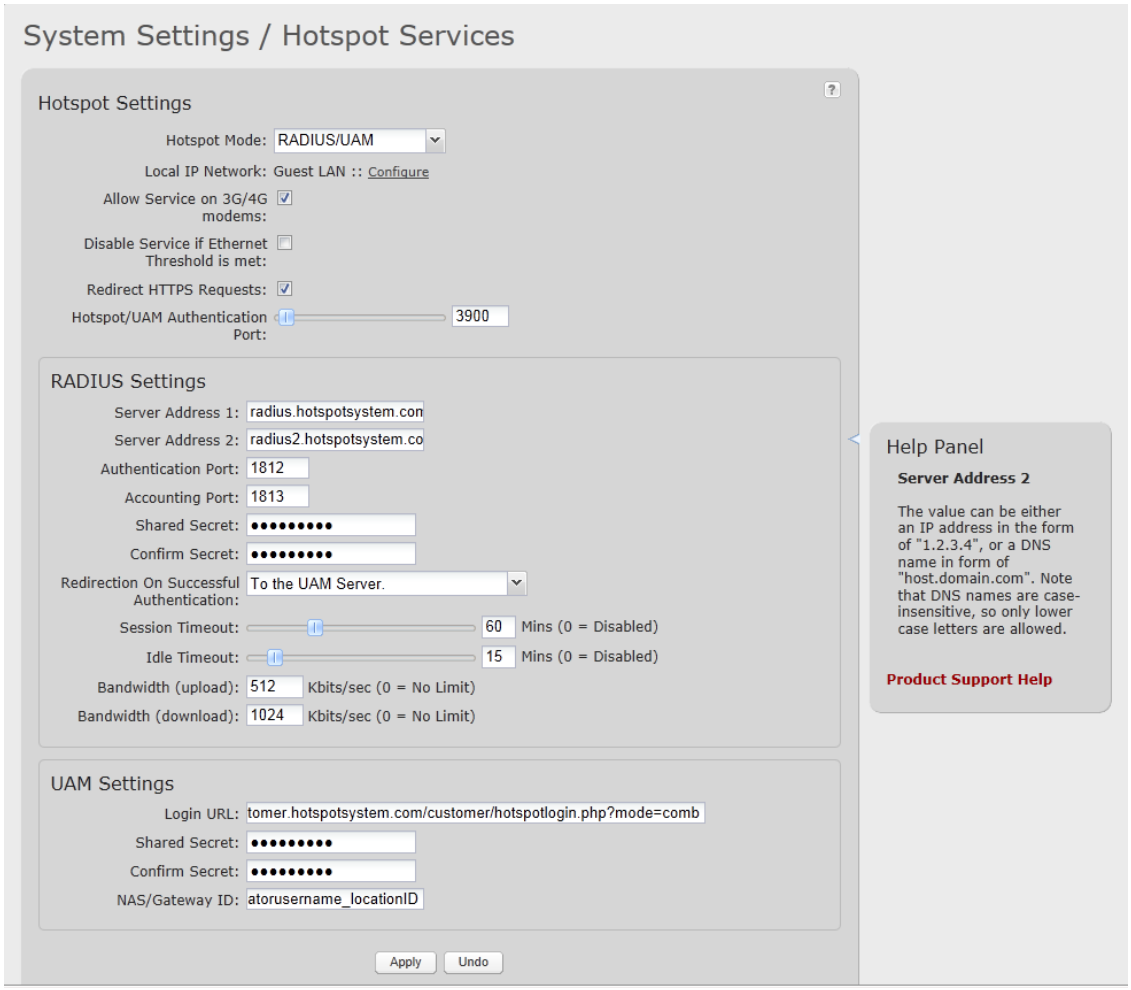
- Add the following values:

*.hotspotsystem.com
*.worldpay.com
*.paypal.com
*.paypalobjects.com
paypal.112.2O7.net
*.paypal-metrics.com
altfarm.mediaplex.com
*.adyen.com
194.149.46.0
198.241.128.0
66.211.128.0
216.113.128.0
70.42.128.0
128.242.125.0
216.52.17.0
62.249.232.74
155.136.68.77
66.4.128.0
66.211.128.0
66.235.128.0
88.221.136.146
195.228.254.149
195.228.254.152
203.211.140.157
203.211.150.204
82.199.90.136
82.199.90.160
91.212.42.0

For Hotspot FREE SOCIAL locations: you must add 'www.apple.com' too!

You will have to enter them one by one.

Hotspotsystem Example:



Additional Captive Portal Behaviors:

- Captive Portal is available on any SSID. We recommend using the Guest SSID which is on the Guest LAN because it has no administrative access. Other SSIDs and LANs can be configured to restrict administrative access.
- Non-ToS redirect. The admin can allow all associated clients to surf without a ToS/Auth but first the clients are redirected to an admin-specified URL.
- Users on the guest SSID with captive portal and LAN isolation enabled have no visibility to the LAN/WLAN machines including the router configuration pages
- Admin can specify a timeout/time limit for clients using the guest SSID with Captive Portal. There are 2 timeouts, a session timeout and an idle timeout.
- Admin can either redirect the client to their original request after they have authenticated or to a specified web page.
- Admin may add, change, or remove available services/URLs within the Walled Garden.
- User on the Guest SSID with captive portal enabled will be using the router's DNS.
- No sub-link bypass of the Captive Portal's walled garden restrictions.