

# 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 services 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 3<sup>rd</sup> party AAA RADIUS hotspot services<sup>1</sup>
  - 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 3<sup>rd</sup> party services

---

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

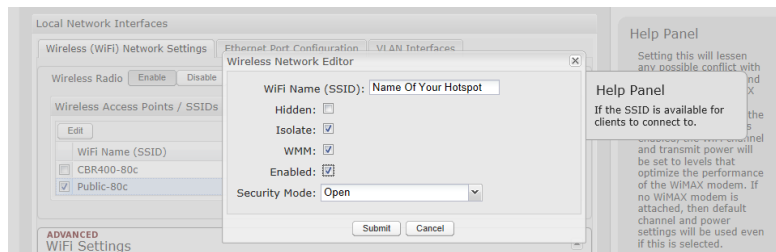
## Generic Setup Steps For Any Hotspot:

Setup and configure the SSID and LAN for Hotspot mode

### Go to Network Settings → WiFi / Local Networks

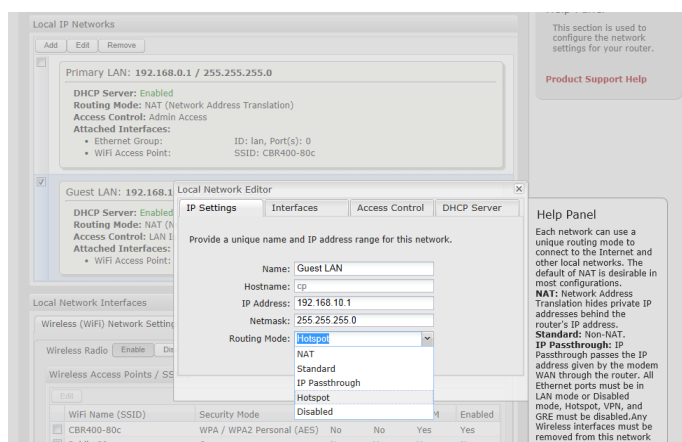


Find **Local Network Interfaces** and select the **WiFi Name (SSID)** you want to make the hotspot (Public-xxx suggested) and click **Edit**. Change the WiFi Name (SSID) to something you choose and select **Enabled**. Click **Submit**.



### 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**. Click **Submit**.

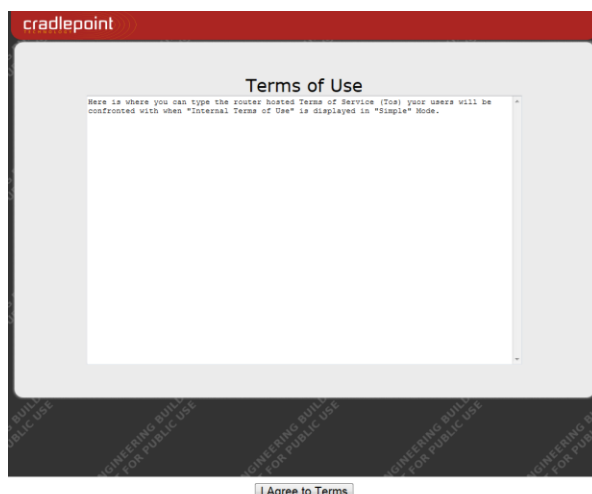
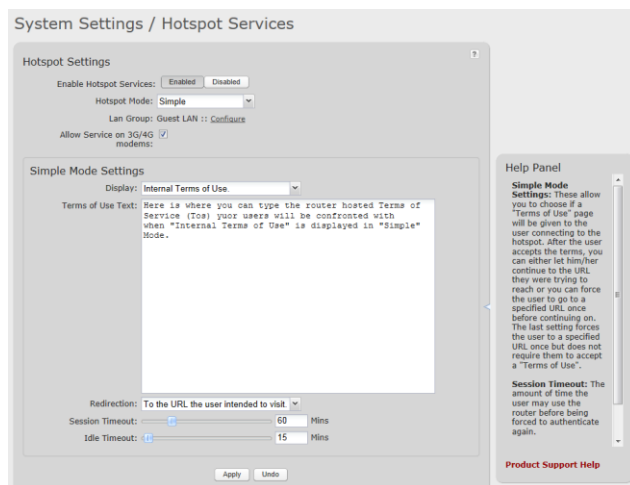


## Go to System Settings → Hotspot Services

### 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.

### Simple Hotspot Setup (Internal Terms of Use)



### Simple Hotspot Internal Terms of Use When Attempting to Connect

## Simple Hotspot Setup (External Terms of Use)

### System Settings / Hotspot Services

#### Hotspot Settings

Enable Hotspot Services:  Enabled  Disabled

Hotspot Mode: Simple

Lan: Guest LAN

Allow Service on 3G/4G modems:

---

#### Simple Mode Settings

Display: External Terms of Use.

Terms of Use URL: www.cradlepoint.com

Redirection: To the URL the user intended to visit.

Session Timeout: 60 Mins

Idle Timeout: 15 Mins

---

<input type="checkbox"/>	Host / Domain Name

#### Help Panel

**Simple Mode Settings:** These allow you to choose if a "Terms of Use" page will be given to the user connecting to the hotspot. After the user accepts the terms, you can either let him/her continue to the URL they were trying to reach or you can force the user to go to a specified URL once before continuing on. The last setting forces the user to a specified URL once but does not require them to accept a "Terms of Use".

**Session Timeout:** The amount of time the user may use the router before being forced to authenticate again.

**Idle Timeout:** If the user is idle for this amount of time, make them re-authenticate.

[Product Support Help](#)

Copyright © CradlePoint Technology, Inc. 2011 All rights reserved. Licenses wipipe.

## Simple Hotspot External Terms of Use When Attempting to Connect

The screenshot shows the CradlePoint website with a prominent banner for a new product: "Create Secure Instant WiFi Networks." Below the banner, there are several news articles and product highlights, including "Easily Create Instant, Secure Networks," "CradlePoint Advances Support for Verizon Wireless 4G LTE Network," and "CradlePoint releases router specifically designed to provide full 4G LTE and WiMAX performance." At the bottom of the page, there is a button that says "I Agree to Terms".

**Mode 2: Radius Authentication Captive Portal:**

The captive portal Radius mode allows the admin/owner to configure a third-party RADIUS server<sup>2</sup> 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](http://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.

---

<sup>2</sup> CradlePoint does not offer the 3<sup>rd</sup> 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](http://www.hotspotsystem.com/en/hotspot/install_guide_cradlepoint_3g_mobile.html)

When using [www.hotspotsystem.com](http://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

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: Redirect to the UAM Server

Session Timeout: 60 Mins

Idle Timeout: 15 Mins

**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).

Find Allowed Hosts Prior to Authentication. Click add.

Add the following values:

hotspotsystem.com, worldpay.com, rbsworldpay.com, paypal.com, paypalobjects.com, paypal.112.207.net, adyen.com

You will have to enter them one by one.

### Hotspotsystem Example:

The screenshot displays the 'System Settings / Hotspot Services' configuration interface. It is divided into several sections:

- Hotspot Settings:** Includes 'Hotspot Mode' set to 'RADIUS/UAM', 'Local IP Network' as 'Guest LAN', 'Allow Service on 3G/4G modems' checked, 'Redirect HTTPS Requests' checked, and 'Hotspot/UAM Authentication Port' set to 3990.
- RADIUS Settings:** Includes 'Server Address 1' (radius.hotspotsystem.com), 'Server Address 2' (radius2.hotspotsystem.co), 'Authentication Port' (1812), 'Accounting Port' (1813), 'Shared Secret' and 'Confirm Secret' (masked), 'Redirection' options (selected: 'Redirect to the UAM Server'), 'Session Timeout' (60 Mins), and 'Idle Timeout' (15 Mins).
- UAM Settings:** Includes 'Login URL' (https://customer.hotspotsystem.com/customer/hotspotlogin.php?m...), 'Shared Secret' and 'Confirm Secret' (masked), and 'NAS/Gateway ID' (operatorusername\_locati...).
- Allowed Hosts Prior to Authentication:** A table with columns for 'Host Name' and 'Allowed Hosts Prior to Authentication'. It contains two entries: 'hotspotsystem.com' and 'worldpay.com'.

Buttons for 'Apply' and 'Undo' are located below the UAM Settings section.

**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.
- 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.