



ISPBrain / RouterOS Quick Start Guide

This guide will help you to quickly deploy an ISPBrain regulated authentication router using an ISPBrain Server and a device running RouterOS. Your ISPBrain must be connected to a network that is accessible by the RouterOS device, such as the internet or a local area network. You will need administrative access to the ISPBrain web portal as well as all proper IP address information associated with both devices.

Required Open Ports

The RouterOS device must be able to contact the ISPBrain on TCP ports 22 (or other SSH), 80, 161, 443, 1812 and 1813. It is recommended that ICMP packets are allowed between the devices for management and troubleshooting purposes.

Required Configuration Options

The RouterOS device must be configured to allow ssh access from the ISPBrain on a specified port.

Deploying the Authentication Router – Make Device Entries in the ISPBrain

Ensure that the ISPBrain and the RouterOS device are both connected and on network before beginning the configuration tasks below.

Adding the Authentication Router into the ISPBrain Device Database

1. Login to the ISPBrain as an administrator
2. Click Manage Devices
3. Click Add New Device
4. Fill out the device settings for the RouterOS device that will be used as an authentication router. Make note of the required settings listed below:
 - a. Device Type must be set to “Authentication Router”
 - b. IP Address must be the IP address that the RouterOS device can be reached at from the ISPBrain
 - c. Login Name and Login Password must be an administrator password on the RouterOS device
 - d. Login Port # must be the port number that is currently running SSH on the RouterOS device
 - e. (optional) SNMP strings must be set to those in use currently on the RouterOS device
5. Click the “Add Device” button

Configuring the ISPBrain Authentication Router Settings

1. In the ISPBrain administration portal, click on “Manage Authentication Routers” under the “Manage Device” navigation section.
2. Find the Authentication Router that was added in the previous steps and click on the corresponding edit icon

3. Please make note of the critical settings that must be properly set in order for the authentication router to function properly:
 - a. Calling IP must be the IP address which the ISPBrain sees as the RouterOS device connects to it
 - b. RADIUS Secret must match the radius secret programmed into the RouterOS device
 - c. Login URL is used in Hotspot deployments and must be the path that a client connected to the RouterOS device would use to access the login form onboard the RouterOS device. For instance, if the RouterOS device is running a destination nat to the clients, the Login URL would typically be http://[client-gateway-ip]/login. The ISPBrain will put this form into an iframe on the captive portal page.
 - d. Available Services – the services that should be made available to registering users at the hotspot location should all be selected
 - e. Base Service Level – (optional) this is the service level that will be offered free to registrants at this location.
 - f. Upload Files – If the RouterOS device will act as a hotspot location, this box should be checked to ensure that proper login form files are uploaded to the RouterOS device.
4. Click the “Edit Device” button

Configuring the RouterOS Device

1. Connect to the RouterOS device via ssh or Winbox.
2. Configure the RouterOS device so that clients connected to the client interface can freely gain access to the internet – usually done with a DHCP server
3. Add a new Radius Server with the following attributes:
 - a. Enable ppp, hotspot, and login services
 - b. Set the address to the reachable IP address of the ISPBrain
 - c. Set the secret to the RADIUS Secret that was configured for the Authentication Router in the ISPBrain administration
 - d. Leave all other settings as default

Configuring for PPPoE Authentication

1. Add a new PPPoE server with the following settings
 - a. Interface – choose the interface on which the clients will be initiating PPPoE sessions – note that all clients must have broadcast access to this interface.

Configuring a Hotspot Server

Configure the following settings in the Hotspot section (or run the hotspot setup wizard from Winbox)

- e. Server Tab
 - i. Add a new Hotspot Server on the Interface that clients will be connecting – note that clients must have broadcast access to this interface

- ii. Address Pool – select the DHCP address pool that is dedicated for use by the Hotspot Server
 - iii. Make note of the selected Profile being used on this hotspot server
 - iv. Idle Timeout – for mobile locations this may be set lower (i.e. 1 minute). For end user / fixed subscriber locations, this may be set to 1 day or more
- f. **Hotspot Server Profile Required Settings:**
- i. General Tab
 - 1. Hotspot Address: must be checked and set to the local IP address of the hotspot server (or client gateway when client connects)
 - 2. HTML Directory: typically set to “login” – this corresponds to the LoginURL that was set up in the ISPBrain Authentication Router settings – these directory names must match
 - ii. Login Tab
 - 1. Check Login By
 - a. HTTP CHAP
 - b. HTTP PAP
 - c. Cookie (optional if you want the hotspot to remember client logins)
 - iii. Radius Tab
 - 1. Check “Use RADIUS”
 - 2. Interim Update – set to around 30 seconds or 1 minute – may be longer if you need to increase the capacity of the system and reduce the load on the radius server
- g. **Walled Garden Tab**
- i. Dst. Host - Add an entry and set to the IP address of the ISPBrain Server (you may also wish to add one with the hostname of the ISPBrain Server)
 - ii. Dst. Port - For these entries, set to 80
 - iii. Server - Select the hotspot server that you created above

Troubleshooting Guide

- **ISSUE:** When client connects to the network, the browser rapidly refreshes in a loop.

RESOLUTION: This is normally caused by the “rlogin.html” file on the RouterOS device having an improper redirect URL. This can happen either because the ISPBrain did not upload files when the authentication router was added to the ISPBrain database or the files on the ISPBrain are not configured properly.

Specifically, in the rlogin.html file on the RouterOS device, the meta http-equiv="refresh" url should be set to that of your ISPBrain. You should also change the URL in the link that shows up in the HTML body of this page.

This rlogin.html file may need to be updated in your ISPBrain configuration to correspond with the URL of your ISPBrain system. Please contact ISPBrain support for assistance in updating this file on your ISPBrain.

- **ISSUE:** When client connects to the network, the ISPBrain welcome page is displayed with a message that states that the area is not covered by ISPBrain service.

RESOLUTION: This is normally caused by having an incorrect setting in the "Calling IP" field in the ISPBrain Authentication Router settings. Ensure that the IP address in this field is the IP that is seen by the ISPBrain when a client connects to the network. This is normally the src-nat address or the address that the NAT masquerades to.

- **ISSUE:** When a client attempts to login, a message appears stating that the username or password is invalid, even though the username and password exists in the ISPBrain subscriber database.

RESOLUTION: In order for a subscriber to logon to gain internet access, the username / password must be valid and the subscriber must have service provisioned to their account. In the ISPBrain administrative portal, click "Manage Current Service" under the subscriber in question and ensure that service has been applied to the account.

- **ISSUE:** When a client attempts to login via hotspot, a message appears stating that the "RAIDUS Server is Not Responding".

RESOLUTION: This message can be caused by improper RADIUS settings on the RouterOS device. Check the RADIUS section of RouterOS and ensure that a RADIUS server has been added and has proper IP configuration settings. Also check the Hotspot Profile and ensure that the "Use Radius" box is checked on the RADIUS tab.

If the problem persists, please contact ISPBrain Technical Support.