MikroTik RB941 2nd Haplite Router Configuration Guide

For External Captive Portal Authentication System

PART 1: ACCESSING YOUR ROUTER

1. **Connect to your router**:
2. Connect your computer to the router using an Ethernet cable
3. Plug the cable into any LAN port (usually ports 2-4)
4. **Access the router administration**:
5. Open a web browser (Chrome, Firefox, etc.)
6. Type `192.168.88.1` in the address bar (default IP)
7. Press Enter
8. **Login to your router**:
9. Username: admin (default)
10. Password: (blank by default or your custom password)
11. Click the blue "Login" button

PART 2: ENABLE API ACCESS

1. **Navigate to IP Services**:
2. In the left menu, click on "IP"
3. From the dropdown, click on "Services"

4. **Enable the API service**:

5. In the services list, look for "api" (usually enabled by default)
6. If it's not enabled, double-click on "api" to open its settings
7. Make sure "Enabled" is checked
8. Set "Available From" to either your specific server IP or 0.0.0.0/0 (all addresses, less secure)

9. Click "OK" to save

10. **Create a dedicated API user (recommended)**:

11. In the left menu, click on "System"
12. Click on "Users"
13. Click the blue "+" button to add a new user
14. Enter a username (e.g., "apiuser")
15. Enter a strong password
16. Set Group to "full" (or create a custom group with more limited permissions)
17. Click "OK" to save

PART 3: CONFIGURE HOTSPOT

1. **Setup the Hotspot Interface**:
2. In the left menu, click on "IP"
3. Click on "Hotspot"
4. Click on the blue "Hotspot Setup" button
5. Select your public interface (usually "ether1" or "wlan1")

6. Click "Next"

7. **Configure Local Address**:

8. Keep the default local address (usually 192.168.88.1) or change if needed

9. Click "Next"

10. **Set Address Pool**:

11. Keep the default address pool (usually 192.168.88.10-192.168.88.254) or change if needed

12. Click "Next"

13. **Select Certificate**:

14. Select "none" for certificate (we'll use our external authentication)

15. Click "Next"

16. **SMTP Server**:

17. Leave blank, click "Next"

18. **DNS Servers**:

19. Keep default values (usually 192.168.88.1 or your custom DNS)

20. Click "Next"

21. **DNS Name**:

22. Type a domain name for local identification (e.g., "hotel.hotspot")

23. Click "Next"

24. **Complete Setup**:

25. Review the setup and click "Next"
26. Click "OK" on the final confirmation

PART 4: CONFIGURE EXTERNAL LOGIN PAGE

1. **Modify Hotspot Settings**:
2. In the left menu, click on "IP"
3. Click on "Hotspot"

4. Click on the "Server Profiles" tab
5. Double-click on the default profile ("hsprof1")
6. **Change Login Page**:
7. Find "Login By" dropdown and select "HTTP PAP"
8. Find "Login Page" field
9. Replace with the URL of your deployed application (e.g., https://your-app-name.replit.app)
10. Click "OK" to save

PART 5: CONFIGURE FIREWALL FOR API ACCESS

1. **Add a Firewall Rule**:
2. In the left menu, click on "IP"
3. Click on "Firewall"
4. Click on the "Filter Rules" tab
5. Click the blue "+" button to add a new rule
6. **Configure the Rule**:
7. In the "General" tab:
    - Set "Chain" to "input"
    - Set "Protocol" to "tcp"
    - Set "Dst. Port" to "8728" (API port)
8. In the "Action" tab:
    - Set "Action" to "accept"
9. Click "OK" to save

PART 6: UPDATE APPLICATION SETTINGS

1. **Note your router's public IP**:
2. If your router has a static public IP, note it down

3. If you're using a dynamic IP, consider using a Dynamic DNS service
4. **Update the application environment variables**:
5. MIKROTIK_HOST: Your router's public IP or domain
6. MIKROTIK_USERNAME: The admin or API user you created
7. MIKROTIK_PASSWORD: The password for that user
8. **Testing the connection**:
9. Make sure your application server can reach your router's API port (8728)
10. Verify that the router allows incoming connections from your server's IP

PART 7: CREATE BLOCK LIST FOR DISCONNECTED USERS

1. **Create Address List**:
2. In the left menu, click on "IP"
3. Click on "Firewall"
4. Click on the "Address Lists" tab
5. Click the blue "+" button to add a new address list
6. **Configure Address List**:
7. Set "List Name" to "blocked-hotspot-users"
8. Click "OK" to save
9. **Create Blocking Rule**:
10. In the "Filter Rules" tab, click the blue "+" button
11. In the "General" tab:
    - Set "Chain" to "forward"
    - Set "Src. Address List" to "blocked-hotspot-users"

12. In the "Action" tab:
    - Set "Action" to "drop"
13. In the "Advanced" tab:
    - Set "Comment" to "Block disconnected hotspot users"
14. Click "OK" to save
15. Use the up arrows to move this rule above the hotspot rules

Troubleshooting

If you encounter issues with the connection between your application and the MikroTik router:

1. **Check API accessibility**:
2. Verify the API service is enabled and running
3. Ensure the firewall allows connections to port 8728 from your server's IP
4. Try accessing the API from the same network to isolate network issues
5. **Verify credentials**:
6. Double-check username and password
7. Ensure the user has sufficient permissions
8. **Network connectivity**:
9. If your router is behind NAT, ensure port forwarding is set up for the API port
10. Check if any firewall between the server and router might be blocking connections

Support

For additional help or questions: - MikroTik documentation: https://help.mikrotik.com/docs/ - RouterOS API documentation: https://wiki.mikrotik.com/wiki/Manual:API

Generated for WiFi Captive Portal Authentication System - workspace