Configure Captive Portal on your Wireless Access Point Using the Setup Wizard

Objective

Captive Portal is a feature on your Wireless Access Point that allows you to set up a guest network where wireless users need to be authenticated first before they can have access to the Internet. It provides wireless access to your visitors while maintaining the security of your internal network.

The objective of this article is to show you how to configure Captive Portal on your Wireless Access Point using the Setup Wizard.

Applicable Devices

- WAP131
- WAP150
- WAP321
- WAP361

Software Version

- 1.0.2.8 — WAP131
- 1.0.1.7 — WAP150, WAP361
- 1.0.6.5 — WAP321

Configure Captive Portal

Configure Captive Portal Using the Setup Wizard

Note: The images below are taken from WAP150. These images may vary depending on the exact model of your Access Point.

Step 1. Log in to your access point web-based utility and choose Run Setup Wizard from the navigation pane.

Step 2. Keep clicking Next until you get to the Enable Captive Portal – Create Your Guest Network screen.
Step 3. Click the Yes radio button to create the guest network then click Next.

Step 4. Click the radio button for the Radio band where you want to create the guest network.

**Note:** In this example, Radio 1 (2.4 GHz) is chosen.
Step 5. Create a name for the guest network in the *Guest Network name* field then click **Next**.

![Image](image.png)

**Note:** In this example, ForTheGuests is used as the guest network name.

Step 6. Click a radio button to choose a type of security you want to use on the guest network. The options are:

- **Best Security (WPA2 Personal - AES)** — Provides the best security and is recommended if your wireless devices support this option. WPA2 Personal uses Advanced Encryption Standard (AES) and a Pre-Shared Key (PSK) between the clients and the access point. It uses a new encryption key for each session, which makes it difficult to compromise.
- **Better Security (WPA/WPA2 Personal - TKIP/AES)** — Provides security when there are older wireless devices that do not support WPA2. WPA Personal uses AES and Temporal Key Integrity Protocol (TKIP). It uses IEEE 802.11i Wi-Fi Standard.
- **No Security (Not recommended)** — The wireless network does not require a password and can be accessed by anyone. If chosen, a pop-up window will appear asking if you want to disable security; click **Yes** to continue. If this option is chosen, skip to

![Image](image.png)

**Note:** In this example, Better Security (WPA/WPA2 Personal - TKIP/AES) is chosen.

Step 7. Create a password for the guest network in the field provided. The colored bar to the
right of this field shows the complexity of the entered password.

Step 8. (Optional) To see the password as you type, check the **Show Key as Clear Text** check box then click **Next**.

Note: For WAP131 and WAP361, you need to choose the VLAN ID from the drop-down list.

**Note:** In this example, VLAN ID 2 is used.

Step 9. In the **Enable Captive Portal – Assign The VLAN ID** area, enter the VLAN ID for the guest network then click **Next**. The VLAN ID range is from 1-4094.

**Note:** For WAP131 and WAP361, you need to choose the VLAN ID from the drop-down list.

**Note:** In this example, VLAN ID 2 is used.

Step 10. (Optional) In the **Enable Captive Portal – Enable Redirect URL** screen, check the **Enable Redirect URL** check box if you have a specific web page you want to show after users accept the terms of service from the welcome page.
Step 11. Enter the URL in the *Redirect URL* field then click **Next**.

**Enable Captive Portal - Enable Redirect URL**

If you enable a redirect URL, when new wireless users have completed the authentication process, they can be redirected to an alternate startup page.

- **Enable Redirect URL**
- **Redirect URL**: [http://MyWebsite.com](http://MyWebsite.com)

*Learn more about redirect urls*

Click **Next** to continue

---

Step 12. Check your configured settings in the Summary – Confirm Your Settings screen. If you would like to change a setting, click the **Back** button until the desired page is reached. Otherwise, click **Submit** to enable your settings on the WAP.

**Summary - Confirm Your Settings**

<table>
<thead>
<tr>
<th>Security Key:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>VLAN ID</strong>:</td>
<td>1</td>
</tr>
<tr>
<td><strong>Radio 2 (5 GHz)</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Network Name (SSID)</strong>:</td>
<td>ciscob</td>
</tr>
<tr>
<td><strong>Network Security Type</strong>:</td>
<td>plain-text</td>
</tr>
<tr>
<td><strong>Security Key</strong>:</td>
<td></td>
</tr>
<tr>
<td><strong>VLAN ID</strong>:</td>
<td>1</td>
</tr>
</tbody>
</table>

**Captive Portal (Guest Network) Summary**

<table>
<thead>
<tr>
<th>Guest Network Radio:</th>
<th>Radio 1</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Network Name (SSID)</strong>:</td>
<td>ForTheGuests</td>
</tr>
<tr>
<td><strong>Network Security Type</strong>:</td>
<td>WPA/WPA2 Personal - TKIP/AES</td>
</tr>
<tr>
<td><strong>Security Key</strong>:</td>
<td>Guests123</td>
</tr>
<tr>
<td><strong>Verification</strong>:</td>
<td>Guest</td>
</tr>
<tr>
<td><strong>Redirect URL</strong>:</td>
<td><a href="http://MyWebsite.com">http://MyWebsite.com</a></td>
</tr>
</tbody>
</table>

Click **Submit** to enable settings on your Cisco Wireless Access Point

---

**Verify Captive Portal Settings**

Step 13. Log in to the web-based utility and choose **Captive Portal > Instance Configuration**.
Step 14. In the Instance Configuration page, verify the settings you have configured in the Setup Wizard and make sure it is associated to the correct Virtual Access Point (VAP) or network. The guest network name should also show.

![Captive Portal Configuration Page]

Step 15. Click

You should now have successfully configured Captive Portal on your Cisco Wireless Access Point.

View a video related to this article...

Click here to view other Tech Talks from Cisco