

Konfigurieren des Captive Portals auf dem Wireless Access Point mithilfe des Setup-Assistenten

Ziel

Captive Portal ist eine Funktion in Ihrem Wireless Access Point, mit der Sie ein Gastnetzwerk einrichten können, in dem Wireless-Benutzer zuerst authentifiziert werden müssen, bevor sie auf das Internet zugreifen können. Sie ermöglicht den Wireless-Zugriff für Ihre Besucher und gewährleistet gleichzeitig die Sicherheit Ihres internen Netzwerks.

In diesem Artikel erfahren Sie, wie Sie das Captive Portal mit dem Setup-Assistenten auf Ihrem Wireless Access Point konfigurieren.

Anwendbare Geräte

- WAP131
- WAP150
- WAP321
- WAP361

Softwareversion

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

Captive Portal konfigurieren

Konfigurieren des Captive Portals mithilfe des Setup-Assistenten

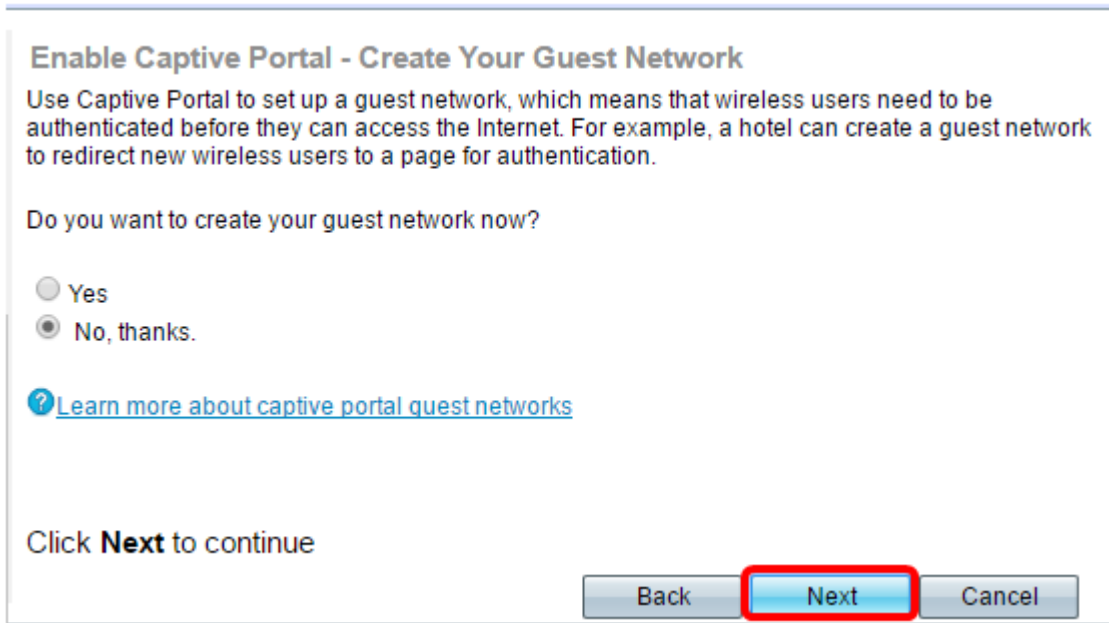
Hinweis: Die folgenden Bilder stammen aus dem WAP150. Diese Bilder können je nach dem genauen Modell Ihres Access Points variieren.

Schritt 1: Melden Sie sich beim webbasierten Dienstprogramm des Access Points an, und wählen Sie im Navigationsbereich die Option **Setup Wizard (Installationsassistent ausführen)** aus.



Schritt 2: Klicken Sie weiter auf **Weiter**, bis der Bildschirm "Captive Portal - Create Your

Guest Network" (Captive Portal aktivieren - Gastnetzwerk erstellen) angezeigt wird.



Enable Captive Portal - Create Your Guest Network

Use Captive Portal to set up a guest network, which means that wireless users need to be authenticated before they can access the Internet. For example, a hotel can create a guest network to redirect new wireless users to a page for authentication.

Do you want to create your guest network now?

Yes

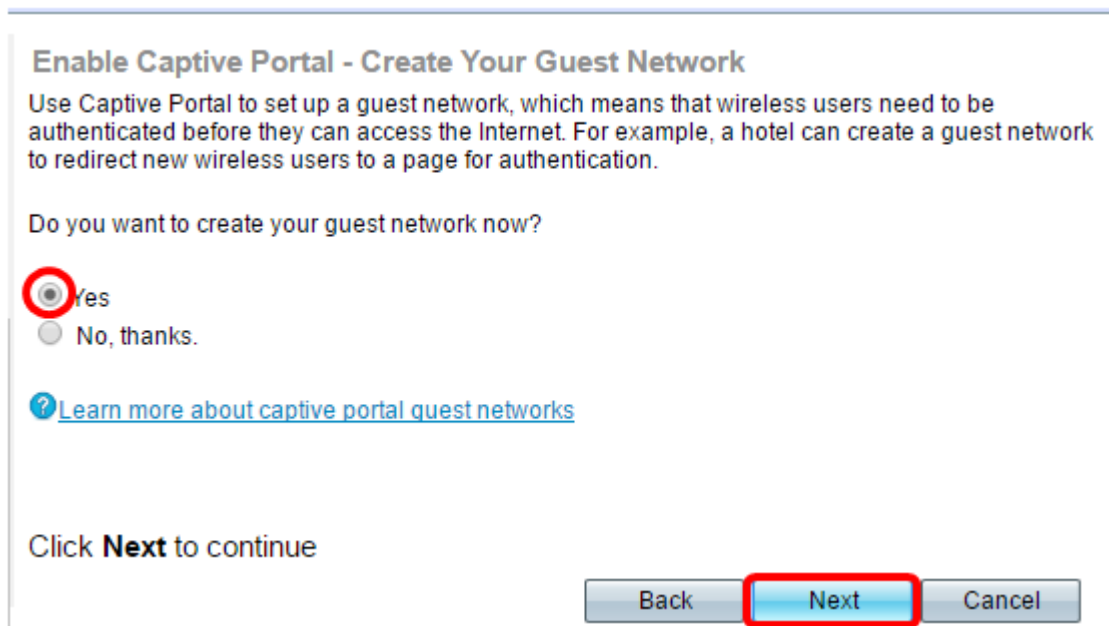
No, thanks.

[? Learn more about captive portal quest networks](#)

Click **Next** to continue

Back Next Cancel

Schritt 3: Klicken Sie auf das Optionsfeld **Ja**, um das Gastnetzwerk zu erstellen, und klicken Sie dann auf **Weiter**.



Enable Captive Portal - Create Your Guest Network

Use Captive Portal to set up a guest network, which means that wireless users need to be authenticated before they can access the Internet. For example, a hotel can create a guest network to redirect new wireless users to a page for authentication.

Do you want to create your guest network now?

Yes

No, thanks.

[? Learn more about captive portal quest networks](#)

Click **Next** to continue

Back Next Cancel

Schritt 4: Klicken Sie auf das Optionsfeld für das Funkband, in dem Sie das Gastnetzwerk erstellen möchten.

Enable Captive Portal - Name Your Guest Network

Your guest network needs a new name, known as an SSID. The name identifies your guest network so that wireless users can find it.

Enter a name for your guest network:

Radio: Radio 1 (2.4 GHz)
 Radio 2 (5 GHz)

Guest Network name:
For example: MyGuestNetwork

Hinweis: In diesem Beispiel wird Radio 1 (2,4 GHz) ausgewählt.

Schritt 5: Erstellen Sie einen Namen für das Gastnetzwerk im *Feld Guest Network* (*Gastnetzwerk*), und klicken Sie dann auf **Weiter**.

Enable Captive Portal - Name Your Guest Network

Your guest network needs a new name, known as an SSID. The name identifies your guest network so that wireless users can find it.

Enter a name for your guest network:

Radio: Radio 1 (2.4 GHz)
 Radio 2 (5 GHz)

Guest Network name:
For example: MyGuestNetwork

[? Learn more about network names](#)

Click **Next** to continue

Hinweis: In diesem Beispiel wird ForTheGuests als Gastnetzwerkname verwendet.

Schritt 6: Klicken Sie auf ein Optionsfeld, um einen Sicherheitstyp auszuwählen, den Sie im Gastnetzwerk verwenden möchten. Folgende Optionen stehen zur Verfügung:

- **Best Security (WPA2 Personal - AES):** Bietet die beste Sicherheit und wird empfohlen, wenn Ihre Wireless-Geräte diese Option unterstützen. WPA2 Personal verwendet Advanced Encryption Standard (AES) und einen Pre-Shared Key (PSK) zwischen den Clients und dem Access Point. Für jede Sitzung wird ein neuer Verschlüsselungsschlüssel verwendet, was die Kompromittierung erschwert.
- **Starke Sicherheit (WPA/WPA2 Personal - TKIP/AES)** - Bietet Sicherheit, wenn es ältere Wireless-Geräte gibt, die WPA2 nicht unterstützen. WPA Personal verwendet AES und Temporal Key Integrity Protocol (TKIP). Er verwendet den IEEE 802.11i Wi-Fi-Standard.
- **Keine Sicherheit (Nicht empfohlen)** - Das Wireless-Netzwerk benötigt kein Kennwort und kann von jedem Benutzer aufgerufen werden. Bei Auswahl dieser Option wird ein Popup-Fenster

mit der Frage angezeigt, ob Sie die Sicherheit deaktivieren möchten. klicken Sie auf **Ja**, um fortzufahren. Wenn diese Option ausgewählt ist, fahren Sie mit

Enable Captive Portal - Secure Your Guest Network
Select your network security strength.

Best Security (WPA2 Personal - AES)
Recommended for new wireless computers and devices that support this option.
Older wireless devices might not support this option.

Better Security (WPA/WPA2 Personal - TKIP/AES)
Recommended for older wireless computers and devices that might not support WPA2.

No Security (Not recommended)

Hinweis: In diesem Beispiel wird "Better Security" (WPA/WPA2 Personal - TKIP/AES) ausgewählt.

Schritt 7: Erstellen Sie im Feld ein Kennwort für das Gastnetzwerk. Die farbige Leiste rechts neben diesem Feld zeigt die Komplexität des eingegebenen Kennworts.

Enter a security key with 8-63 characters.

***** Session Key Refresh Rate

Show Key as Clear Text

[? Learn more about your network security options](#)

Schritt 8: (Optional) Um das Kennwort während der Eingabe anzuzeigen, aktivieren Sie das Kontrollkästchen **Schlüssel als Klartext anzeigen**, und klicken Sie dann auf **Weiter**.

Enter a security key with 8-63 characters.

Guests123 Weak

Show Key as Clear Text

[? Learn more about your network security options](#)

Click **Next** to continue

Back **Next** Cancel

Schritt 9: Geben Sie im Feld Enable Captive Portal - Assign The VLAN ID area (Captive Portal aktivieren - VLAN-ID zuweisen) die VLAN-ID für das Gastnetzwerk ein, und klicken Sie dann auf **Next (Weiter)**. Der Bereich der VLAN-ID liegt zwischen 1 und 4094.

Hinweis: Für WAP131 und WAP361 müssen Sie in der Dropdown-Liste die VLAN-ID auswählen.

Enable Captive Portal - Assign The VLAN ID

We strongly recommend that you assign different VLAN ID for your guest network than the management VLAN ID. By doing that, your guest will have no access to your private network.

Enter a VLAN ID for your guest network:

VLAN ID: (Range: 1 - 4094)

[? Learn more about vlan ids](#)

Click **Next** to continue

Hinweis: In diesem Beispiel wird die VLAN-ID 2 verwendet.

Schritt 10: (Optional) Aktivieren Sie im Bildschirm Enable Captive Portal - Enable Redirect URL das Kontrollkästchen **Enable Redirect URL** (Umleitung aktivieren), wenn Sie eine bestimmte Webseite haben, die angezeigt werden soll, nachdem die Benutzer die Nutzungsbedingungen von der Willkommenseite akzeptiert haben.

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 :

Schritt 11: Geben Sie die URL in das Feld *Umleitungs-URL* ein, und klicken Sie dann auf **Weiter**.

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 :

[? Learn more about redirect urls](#)

Click **Next** to continue

Schritt 12: Überprüfen Sie Ihre konfigurierten Einstellungen im Bildschirm "Summary - Confirm Your Settings" (Zusammenfassung - Einstellungen bestätigen). Wenn Sie eine Einstellung ändern möchten, klicken Sie auf die **Zurück**-Schaltfläche, bis die gewünschte Seite angezeigt wird. Andernfalls klicken Sie auf **Senden**, um die Einstellungen auf dem WAP zu aktivieren.

Summary - Confirm Your Settings

Security Key:	
VLAN ID:	1

Radio 2 (5 GHz)

Network Name (SSID):	ciscosb
Network Security Type:	plain-text
Security Key:	
VLAN ID:	1

Captive Portal (Guest Network) Summary

Guest Network Radio:	Radio 1
Network Name (SSID):	ForTheGuests
Network Security Type:	WPA/WPA2 Personal - TKIP/AES
Security Key:	Guests123
Verification:	Guest
Redirect URL:	http://MyWebsite.com

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

Back **Submit** Cancel

Einstellungen des Captive Portals überprüfen

Schritt 13: Melden Sie sich beim webbasierten Dienstprogramm an, und wählen Sie **Captive Portal > Instance Configuration** aus.

- ▶ Quality of Service
- ▶ ACL
- ▶ SNMP
- ▼ **Captive Portal**
 - Global Configuration
 - Local User
 - Instance Configuration**
 - Web Portal Customization
 - Authenticated Clients

Schritt 14: Überprüfen Sie auf der Seite "Instance Configuration" (Instanzkonfiguration) die Einstellungen, die Sie im Setup-Assistenten konfiguriert haben, und stellen Sie sicher, dass sie dem richtigen Virtual Access Point (VAP) oder Netzwerk zugeordnet sind. Der Name des Gastnetzwerks sollte ebenfalls angezeigt werden.

Administrative Mode:	<input checked="" type="checkbox"/> Enable
Protocol:	HTTP ▾
Verification:	Guest ▾
Redirect:	<input checked="" type="checkbox"/> Enable
Redirect URL:	<input type="text" value="http://MyWebsite.com"/> (Range: 0 - 256 Characters)
Away Timeout:	<input type="text" value="60"/> (Range: 0 - 1440 Min, Default: 60)
Session Timeout:	<input type="text" value="0"/> (Range: 0 - 1440 Min, Default: 0)
Maximum Bandwidth Upstream:	<input type="text" value="0"/> (Range: 0 - 300 Mbps, Default: 0)
Maximum Bandwidth Downstream:	<input type="text" value="0"/> (Range: 0 - 300 Mbps, Default: 0)
Associate VAP (2.4 GHz):	VAP 1 (ForTheGuests) ▾
Associate VAP (5 GHz):	▾

Schritt 15: Klicken Sie .

Sie sollten jetzt das Captive Portal auf Ihrem Cisco Wireless Access Point erfolgreich konfiguriert haben.

Sehen Sie sich ein Video zu diesem Artikel an..

[Klicken Sie hier, um weitere Tech Talks von Cisco anzuzeigen.](#)