

Konfigurieren der Authentifizierung von Drittanbietern auf WAP571 oder WAP571E

Ziel

Dieser Artikel führt Sie durch die Konfiguration der Authentifizierung von Drittanbietern für einen WAP571- oder WAP71E-Access Point.

Einführung

Netzwerkbenutzer stellen häufig eine Verbindung zu einem Wireless Access Point (WAP) her, um im Vergleich zum Carrier-Service ihres Mobilgeräts schnellere Internetgeschwindigkeiten zu erhalten. Ein reibungsloser Login-Prozess und eine einfache Navigation sorgen für ein positives Benutzererlebnis. Sie können Ihren WAP571 oder WAP571E so konfigurieren, dass einige einfache Optionen für die Benutzeranmeldung verfügbar sind, ohne dass die Sicherheit Ihres Netzwerks beeinträchtigt wird.

Die Authentifizierung von Drittanbietern über Google oder Facebook ist eine Funktion, die mit diesem neuesten Update verfügbar ist. Bei Verwendung des Drittanbieterkontos des Benutzers fungiert es als "Pass", der dem Benutzer Zugriff auf Ihr Wireless-Netzwerk gewährt. Egal, ob Sie ein Café oder ein Immobilienbüro betreiben, es wird den Besuchern einen einfachen Zugang zu Ihrem Netzwerk ermöglichen und ihnen ein tolles Besuchererlebnis bieten.

Anwendbare Geräte

WAP571

WAP571E

Softwareversion

1,1/03

Anforderungen

Internetzugang, damit Sie eine Verbindung zu den Authentifizierungsservern von Google und/oder Facebook herstellen können.

Benutzer müssen über ein vorhandenes Konto bei Google und/oder Facebook verfügen.

Drittanbieterauthentifizierung konfigurieren

Schritt 1: Melden Sie sich beim Webkonfigurations-Dienstprogramm des WAP an, indem Sie den Benutzernamen und das Kennwort eingeben. Der Standardbenutzername und das Standardkennwort sind *cisco/cisco*. Wenn Sie einen neuen Benutzernamen oder ein neues Kennwort konfiguriert haben, geben Sie diese stattdessen ein. Klicken Sie auf **Anmelden**.

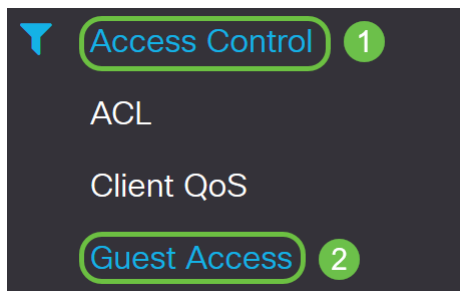


Wireless Access Point

The login form consists of three main elements: a username field containing "cisco" (marked with a green circle 1), a password field with ten black dots (marked with a green circle 2), and a blue "Login" button (marked with a green circle 3). Below the password field is a language dropdown menu currently set to "English".

Hinweis: In diesem Artikel wird der WAP571E verwendet, um die Konfiguration der Gastauthentifizierung von Drittanbietern zu veranschaulichen. Die Menüoptionen können je nach Gerät leicht variieren.

Schritt 2: Wählen Sie **Zugriffskontrolle > Gastzugriff** aus.



Schritt 3: In der *Gastzugriffs-Instanztabelle* können Sie entweder eine neue *Gastzugriffsinstanz* hinzufügen oder eine vorhandene bearbeiten.

In diesem Beispiel wird eine neue *Gastzugriffsinstanz* durch Klicken auf das **Pluszeichen** hinzugefügt.

Guest Access Apply Cancel

Guest Access Instance Table

+ ✎ 🗑

<input type="checkbox"/>	Enable	Guest Access Instance	Protocol	Authenticati...	Guest Group	Redirect URL	Session Timeout (min.)	Web Portal Locale
--------------------------	--------	-----------------------	----------	-----------------	-------------	--------------	------------------------	-------------------

Schritt 4: Benennen Sie die *Gastzugriffsinstanz*. In diesem Beispiel wurde sie als **Facebook** bezeichnet.

Guest Access Instance Table

+ ✎ 🗑

<input type="checkbox"/>	Enable	Guest Access Instance	Protocol	Authentication Method	Guest Group
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Facebook	HTTP : 80	No Authentica	Default

Schritt 5: Wählen Sie im Dropdown-Menü das *Protokoll*, das während des Überprüfungsprozesses verwendet werden soll.

HTTP - Keine Verschlüsselung bei der Überprüfung.

HTTPS - Verwendet SSL (Secure Sockets Layer), für das ein Zertifikat zur Verschlüsselung erforderlich ist. Das Zertifikat wird dem Benutzer zum Zeitpunkt der Verbindung angezeigt.

Hinweis: Es ist sehr wichtig, dass ein Client die Captive Portal-Seite so konfiguriert, dass sie HTTPS und nicht HTTP verwendet, da erstere sicherer ist. Wenn ein Client HTTP auswählt, kann er Benutzernamen und Kennwörter versehentlich verfügbar machen, indem er sie in unverschlüsseltem Klartext überträgt. Es empfiehlt sich, eine HTTPS-Seite für das Captive Portal zu verwenden.

Guest Access Instance Table

+ ✎ 🗑

<input type="checkbox"/>	Enable	Guest Access Instance	Protocol	Authenticati...	Guest Group
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Facebook	HTT : 80	No Authe	Default

Schritt 6: Wählen Sie die *Authentifizierungsmethode* als **3 Anmeldeinformationen von**

Drittanbietern aus.

Guest Access Instance Table

+ ✎ 🗑

<input type="checkbox"/>	Enable	Guest Access Instance	Protocol	Authenticati... Method	Guest Group
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Facebook	HTT : 443	3rd Party ... Local Database Radius Authentication No Authentication 3rd Party Credentials Active Directory Service External Captive Portal	Default

Guest Group Table


+ ✎ 🗑

Hinweis: Das WAP-Gerät verwendet die Anmeldeinformationen des Social-Media-Kontos, um die Benutzer zu authentifizieren.

Schritt 7: Klicken Sie in der Spalte *Authentifizierungsmethode* neben Anmeldeinformationen von Drittanbietern auf das **blaue** Augensymbol.

Guest Access Instance Table

+ ✎ 🗑

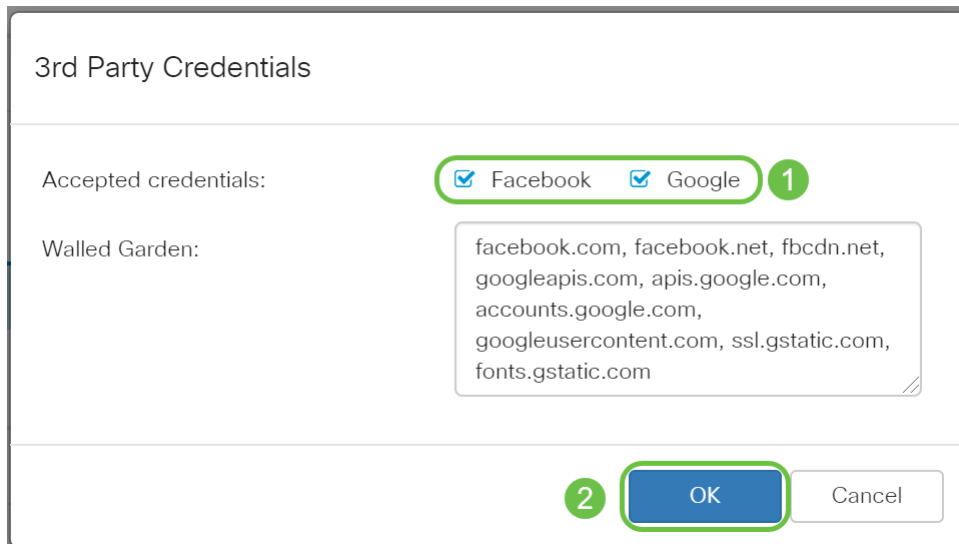
<input type="checkbox"/>	Enable	Guest Access Instance	Protocol	Authentication Method	Guest Group
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Facebook	HTTPS : 443	3rd Party Cre 	Default

Schritt 8: Konfigurieren Sie die folgende Authentifizierungseinstellung für *Anmeldeinformationen von Drittanbietern*.

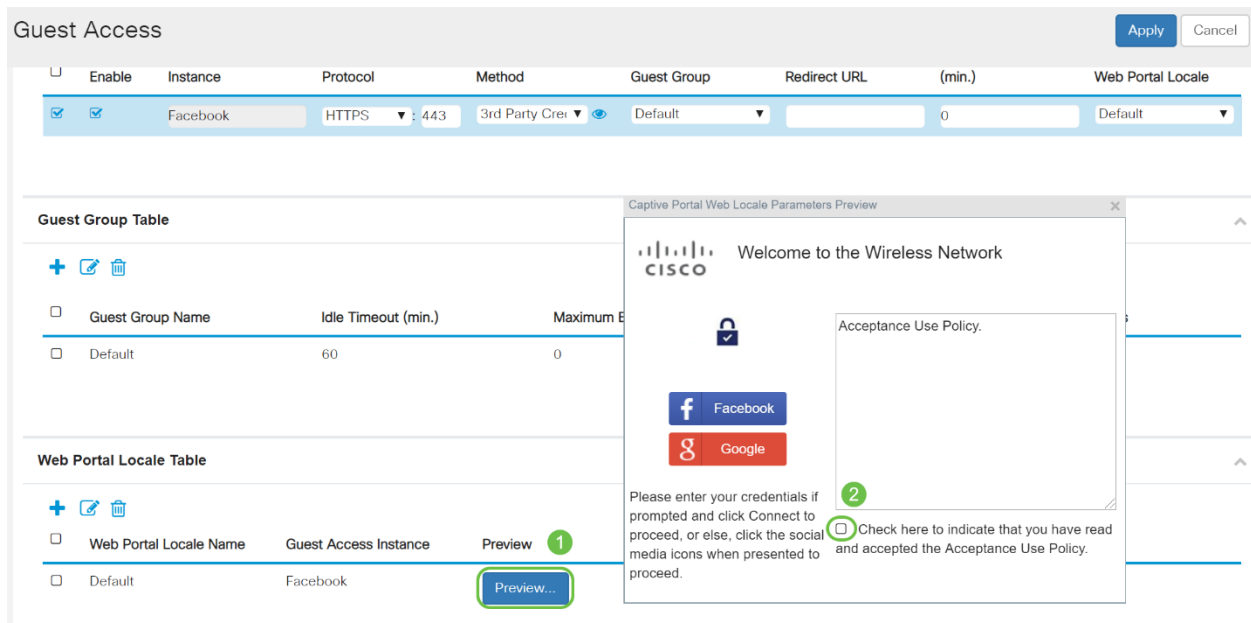
Angenommene Anmeldeinformationen: Wählen Sie Facebook, Google oder beides aus.

Walled Garden: Die entsprechende Standardkonfiguration wird automatisch festgelegt, während die Option Angenommene Anmeldeinformationen ausgewählt wird.

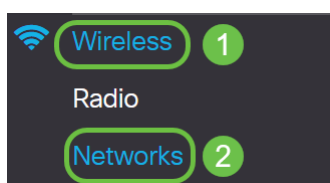
In diesem Beispiel sind sowohl **Facebook** als auch **Google** ausgewählt. Klicken Sie auf **OK**.



Schritt 9: (Optional) Um eine Vorschau der Captive Portal-Seite anzuzeigen, klicken Sie unter *Web Portal Locale Table* auf die Schaltfläche **Preview**. In einem neuen Fenster wird die Vorschauseite angezeigt, auf der die Benutzer aufgefordert werden, ihre Facebook- oder Google-Anmeldeinformationen einzugeben. Die Benutzer müssen außerdem das Kontrollkästchen "Acceptance Use Policy" (Richtlinie zur Akzeptanznutzung) aktivieren.



Schritt 10: Gehen Sie zum Menü, und wählen Sie **Wireless > Networks (Wireless > Netzwerke)** aus.



Schritt 11: Wählen Sie das Netzwerk aus, und geben Sie an, dass **Facebook** als *Gastzugriffsinstanz* für die Authentifizierung ausgewählt wird. In diesem Beispiel ist das Netzwerk **WAP571-Guest**.

Virtual Access Points (SSIDs)

No.	Enable	VLAN ID	SSID Name	SSID Broadcast	WMF	Security	Client Filter	Channel Isolation	Band Steer	Scheduler	Guest Access Instance
0	<input checked="" type="checkbox"/>	1	WAP571-5G	<input checked="" type="checkbox"/>	<input type="checkbox"/>	WPA Personal	Disabled	<input type="checkbox"/>	<input type="checkbox"/>	None	None
1	<input checked="" type="checkbox"/>	1	WAP571-Gues	<input checked="" type="checkbox"/>	<input type="checkbox"/>	None	Disabled	<input type="checkbox"/>	<input type="checkbox"/>	None	Facebook

Schritt 12: Klicken Sie auf **Übernehmen**.

Networks Apply Cancel

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

Virtual Access Points (SSIDs)

No.	Enable	VLAN ID	SSID Name	SSID Broadcast	WMF	Security	Client Filter	Channel Isolation	Band Steer	Scheduler	Guest Access Instance
0	<input checked="" type="checkbox"/>	1	WAP571-5G	<input checked="" type="checkbox"/>	<input type="checkbox"/>	WPA Personal	Disabled	<input type="checkbox"/>	<input type="checkbox"/>	None	None
1	<input checked="" type="checkbox"/>	1	WAP571-Gues	<input checked="" type="checkbox"/>	<input type="checkbox"/>	None	Disabled	<input type="checkbox"/>	<input type="checkbox"/>	None	Facebook

Schlussfolgerung

Sie haben die Authentifizierung von Drittanbietern über Google, Facebook oder beide auf einem WAP571 oder WAP571E erfolgreich konfiguriert.