Captive Portal auf einem WAP571 oder WAP571E konfigurieren

Ziel

Über ein Captive Portal (CP) können Sie den Zugriff auf Ihr Wireless-Netzwerk beschränken, bis die Wireless-Benutzer verifiziert wurden. Wenn ein Benutzer einen Webbrowser öffnet, wird er auf eine Anmeldeseite umgeleitet, auf der er seinen Benutzernamen und sein Kennwort eingeben muss. Es können zwei Arten von Benutzern autorisiert werden, auf Ihr Netzwerk zuzugreifen. authentifizierte Benutzer und Gäste. Authentifizierte Benutzer müssen einen Benutzernamen und ein Kennwort bereitstellen, die entweder einer lokalen Datenbank oder der Datenbank eines RADIUS-Servers entsprechen. Sie müssen keinen Benutzernamen oder kein Kennwort eingeben.

In diesem Artikel wird erläutert, wie Sie das Captive Portal auf Ihrem Wireless Access Point (WAP) konfigurieren.

Anwendbare Geräte

- WAP500-Serie - WAP571, WAP571E

Softwareversion

- 1.0.0.15 - WAP571, WAP571E

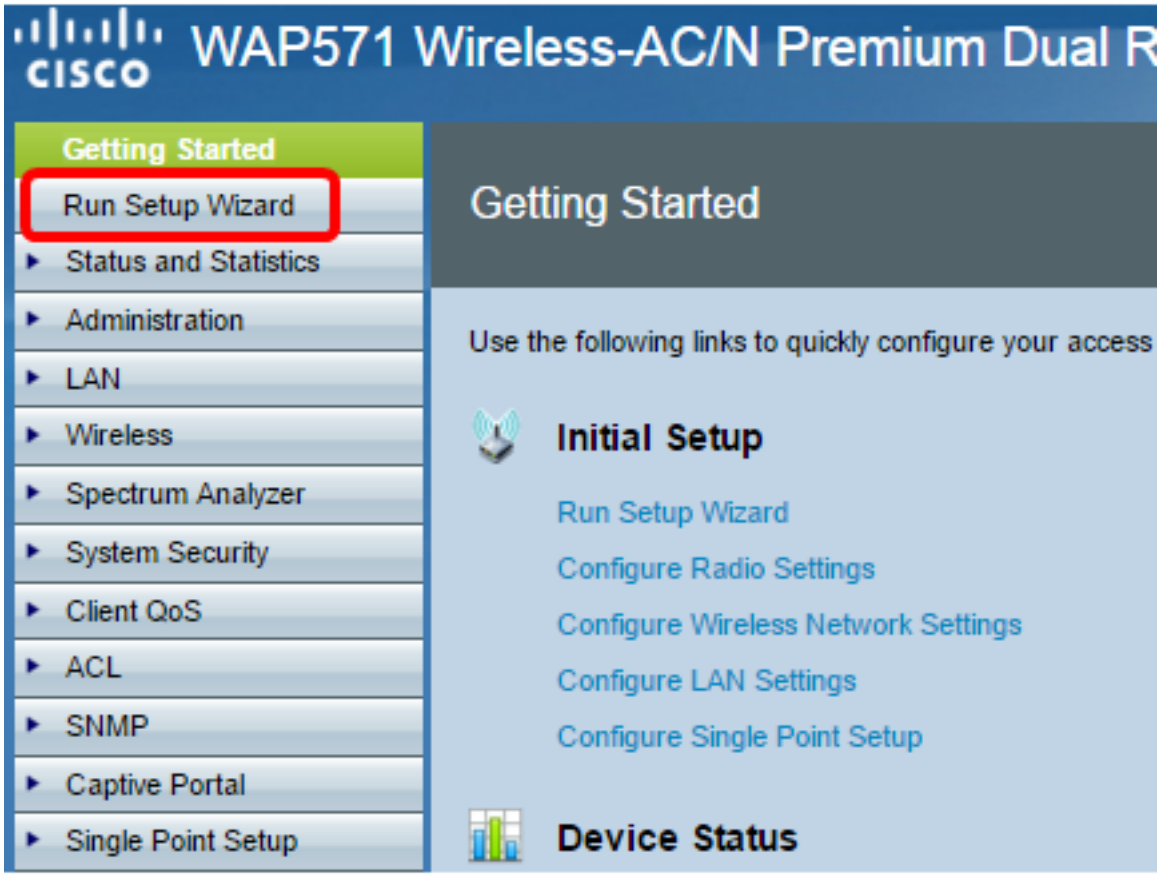
Captive Portal konfigurieren

Die Grundeinstellungen des Captive Portals können über den Setup-Assistenten eingerichtet werden, während die erweiterten Einstellungen über das webbasierte Dienstprogramm konfiguriert werden können. Für eine schnelle und einfache Einrichtung können Sie die Funktion mithilfe des Setup-Assistenten aktivieren. Siehe die Schritte unten:

Hinweis: Die folgenden Bilder werden aus WAP571 erfasst.

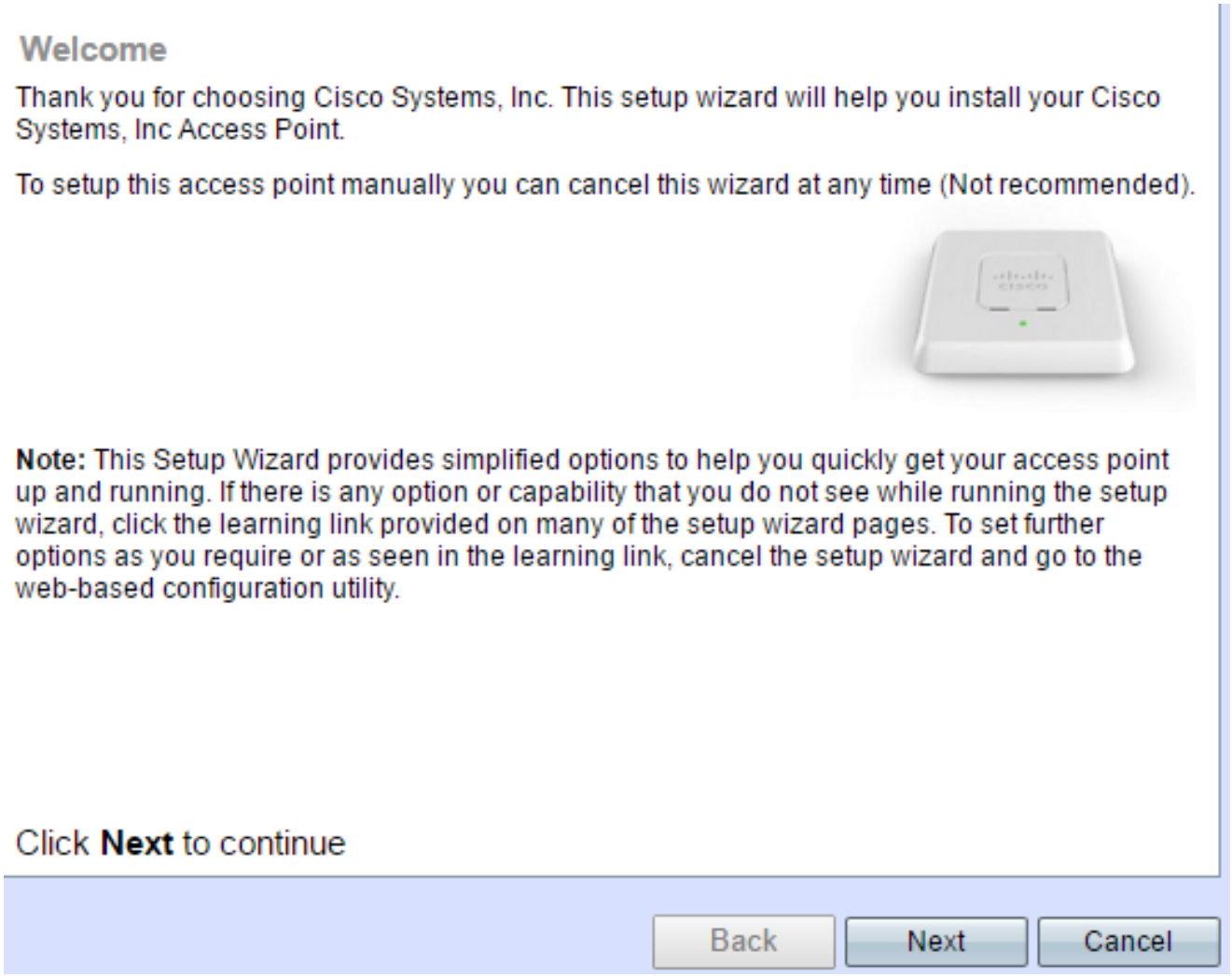
Verwenden des Installationsassistenten

Schritt 1: Melden Sie sich beim webbasierten Dienstprogramm an, und klicken Sie dann auf **Setup Wizard (Installationsassistent ausführen)**.

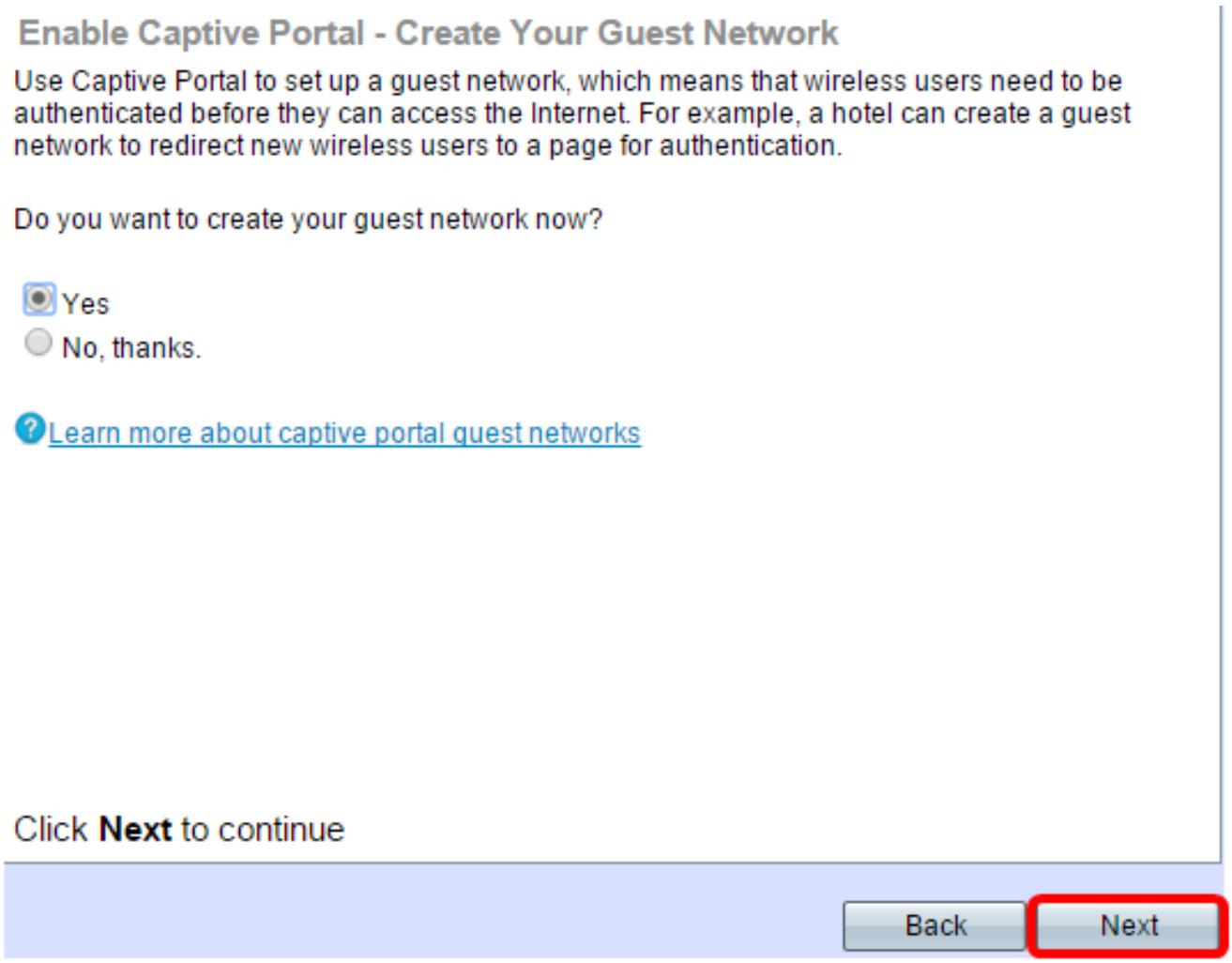


Hinweis: Wenn Sie den WAP zum ersten Mal einrichten, wird automatisch der Setup-Assistent geöffnet.

Schritt 2: Befolgen Sie die Anweisungen im Bildschirm des Installationsassistenten. Eine schrittweise Konfiguration Ihres WAP mithilfe des Setup-Assistenten finden Sie hier.

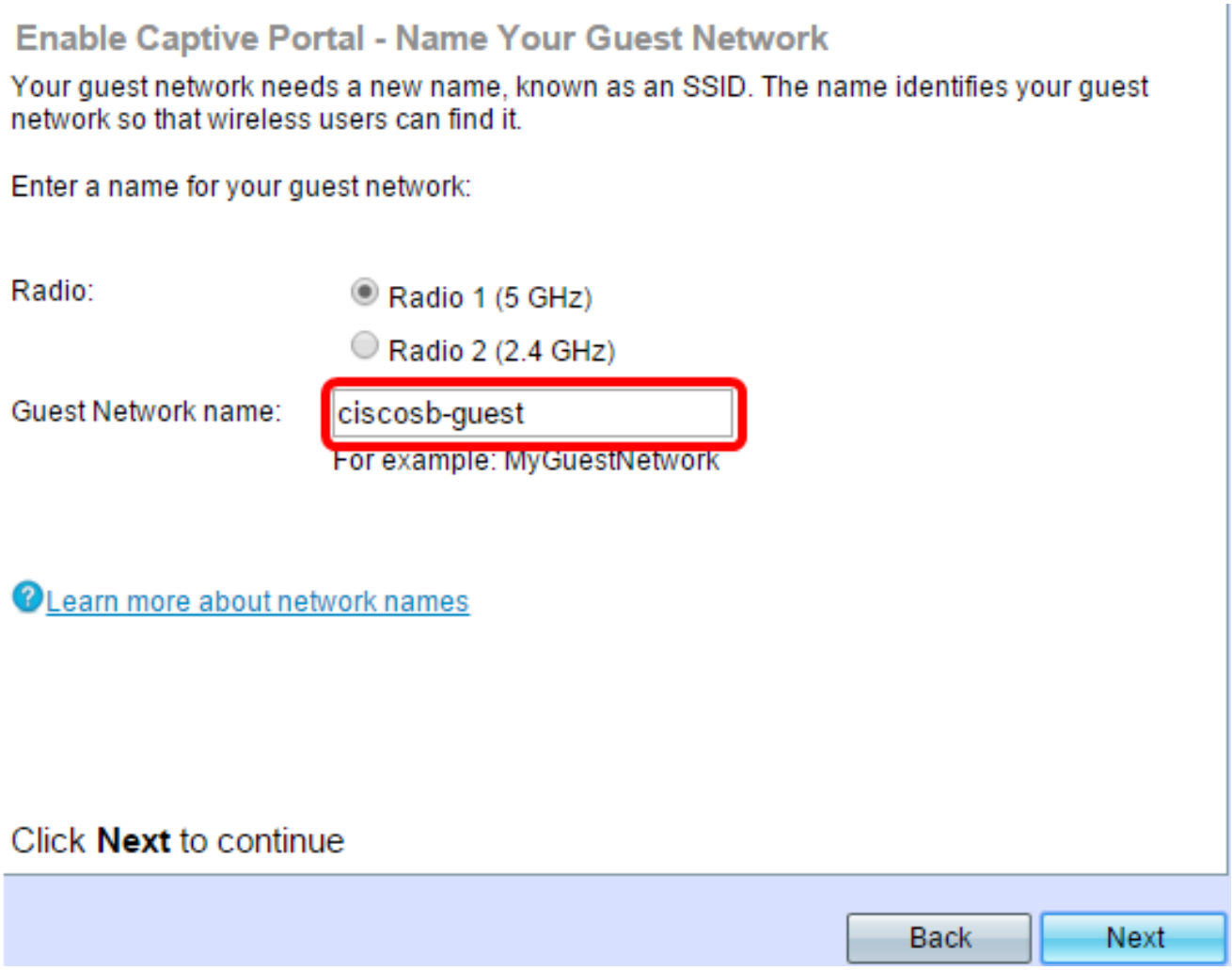


Schritt 3: Wenn der Bildschirm Enable Captive Portal - Create Your Guest Network (Captive Portal aktivieren - Gastnetzwerk erstellen) angezeigt wird, wählen Sie **Yes (Ja) aus,** und klicken Sie dann auf **Next (Weiter)**.



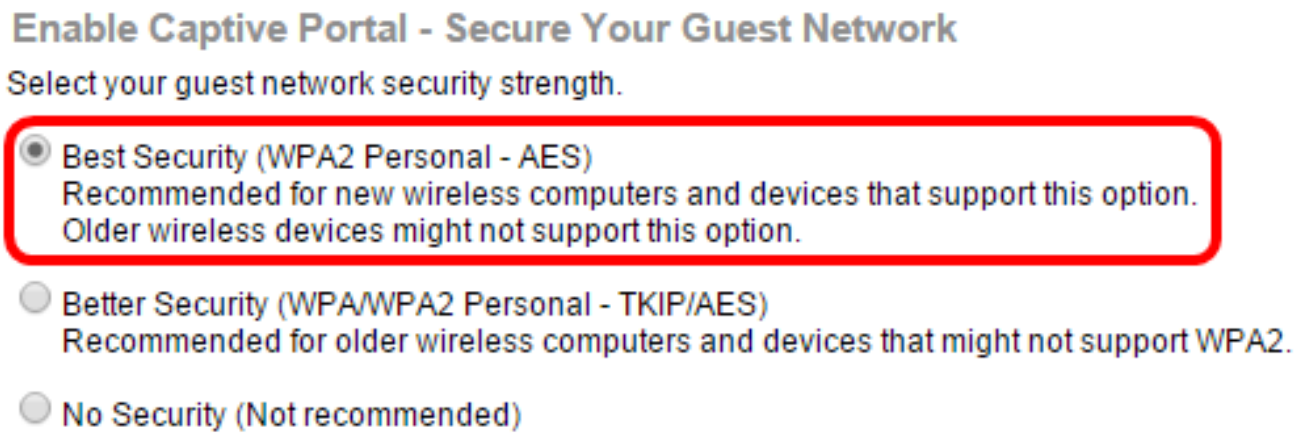
Schritt 4: Geben Sie den Namen des Gastnetzwerks ein, und klicken Sie auf **Weiter**.

Hinweis: Der Standard-Gastnetzwerkname lautet ciscosb-guest.

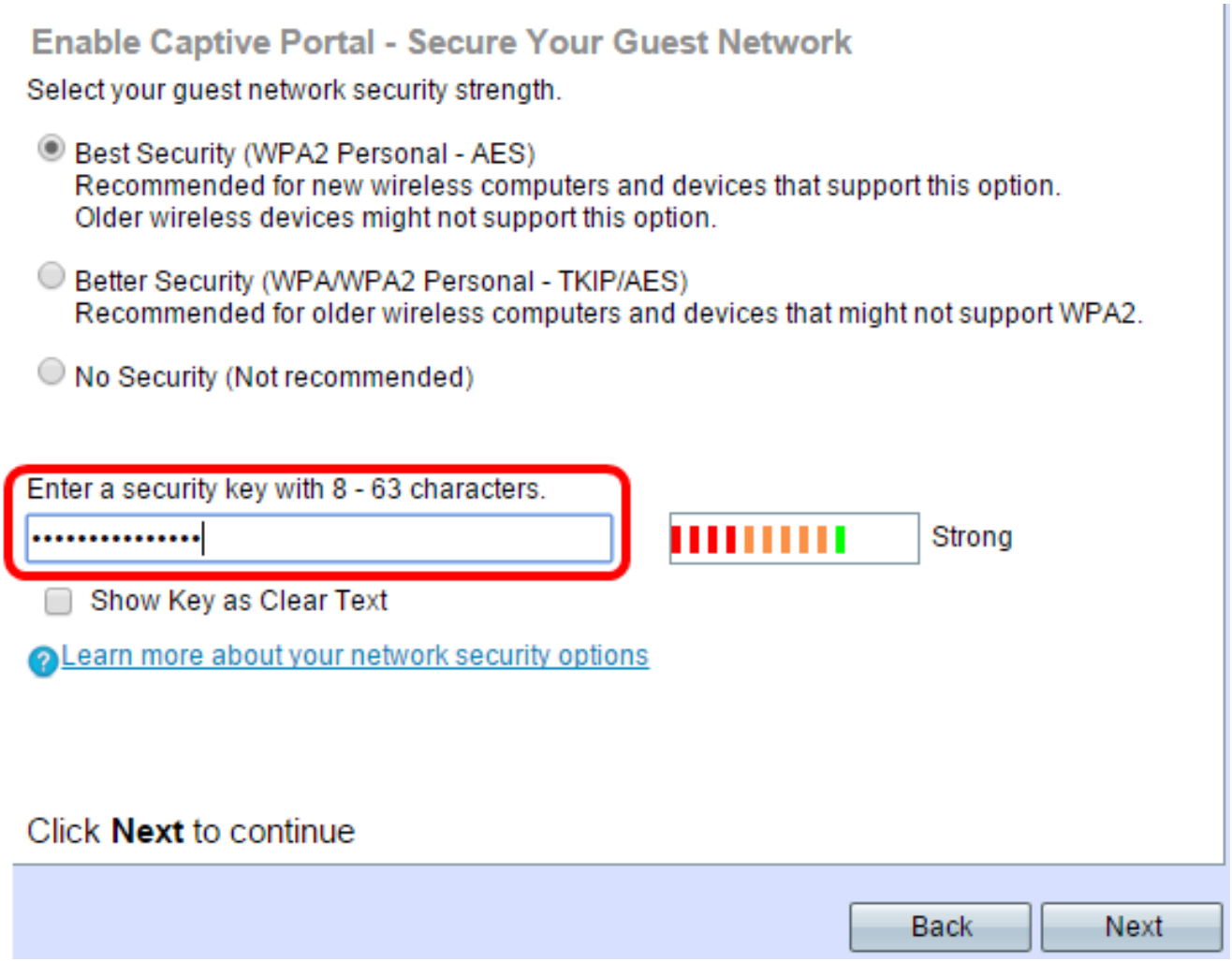


Schritt 5: Wählen Sie einen Sicherheitstyp für Ihr Wireless-Gastnetzwerk aus.

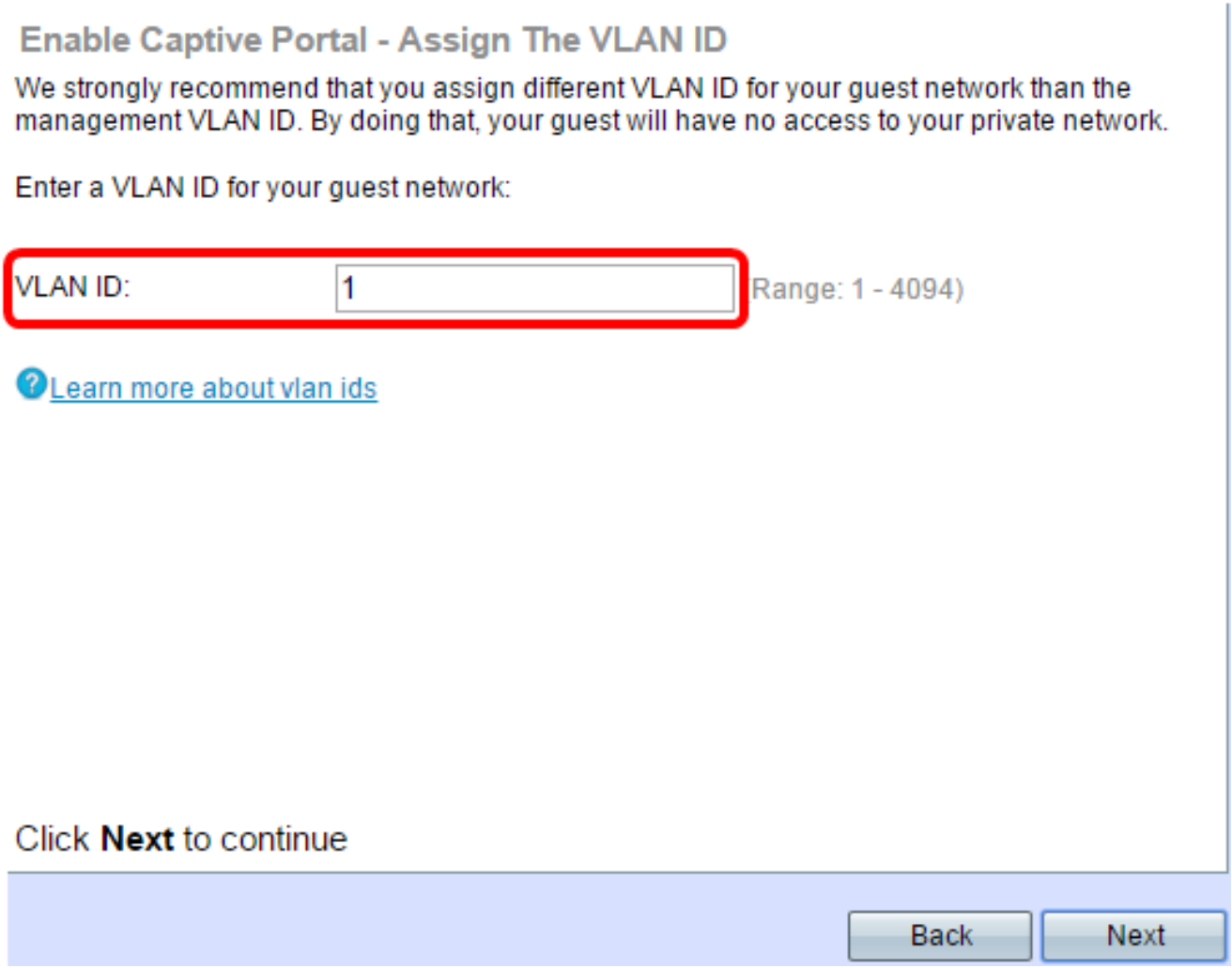
Hinweis: Als Beispiel unten wird die beste Sicherheit (WPA2 Personal - AES) ausgewählt.



Schritt 6: Geben Sie Ihren Sicherheitsschlüssel ein und klicken Sie auf **Weiter**.

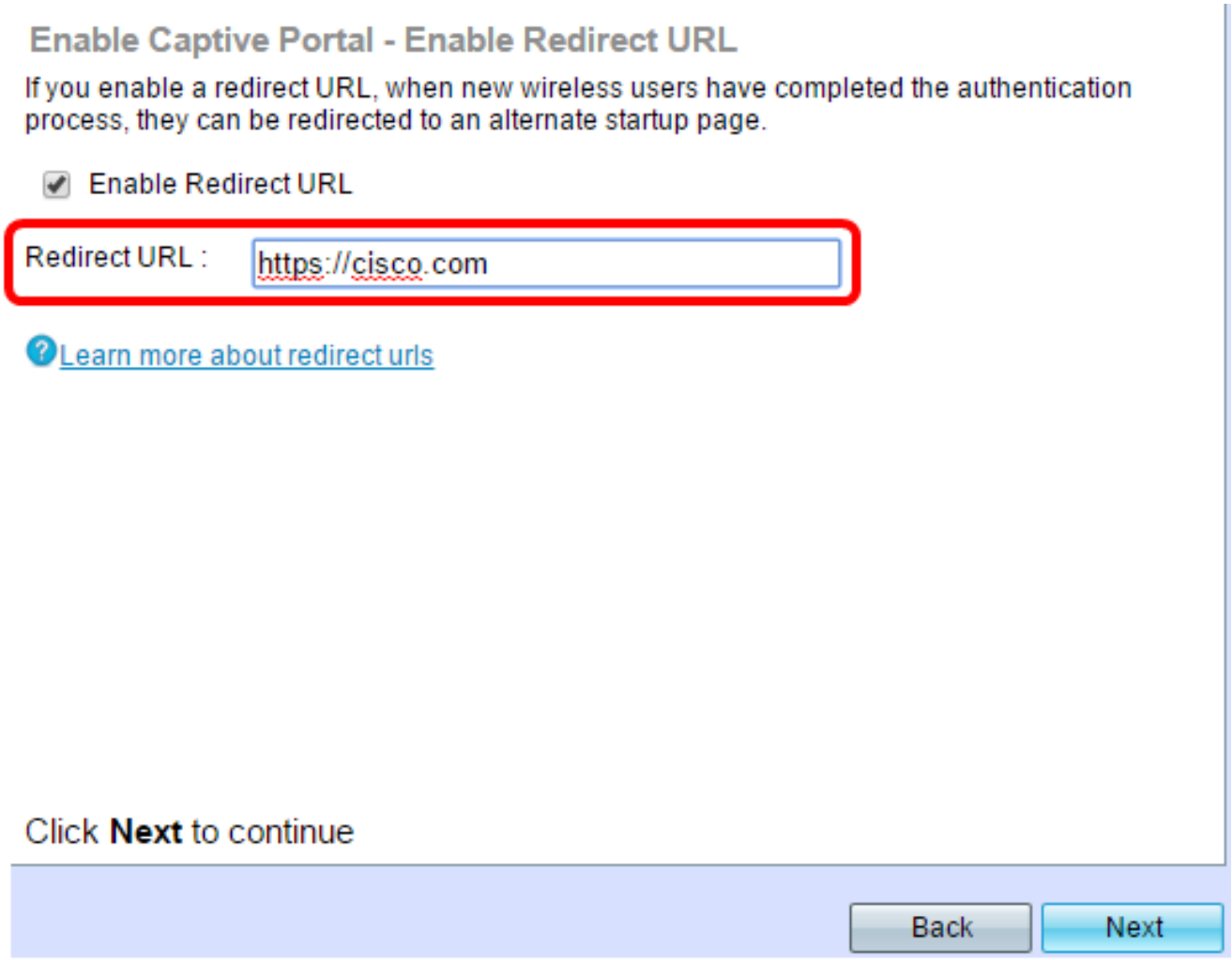


Schritt 7: Geben Sie eine VLAN-ID für Ihr Gastnetzwerk ein, und klicken Sie auf **Weiter**.

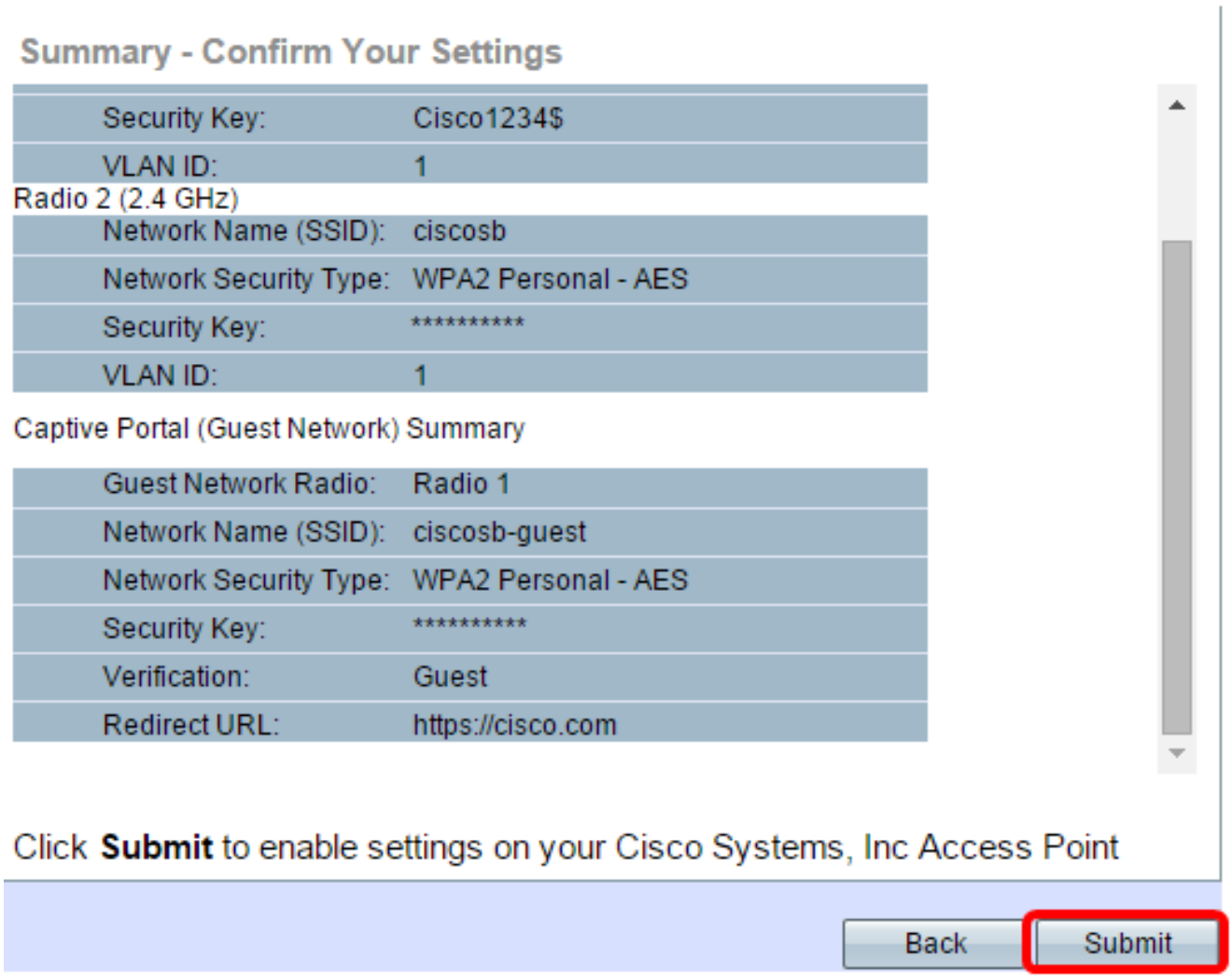


Schritt 8: (Optional) Wenn Sie eine bestimmte Webseite haben, die angezeigt werden soll, nachdem die Benutzer die Nutzungsbedingungen von der Willkommensseite akzeptiert haben, aktivieren Sie das Kontrollkästchen **Enable Redirect URL (Umleiten-URL aktivieren)**. Geben Sie die URL ein, und klicken Sie dann auf **Weiter**.

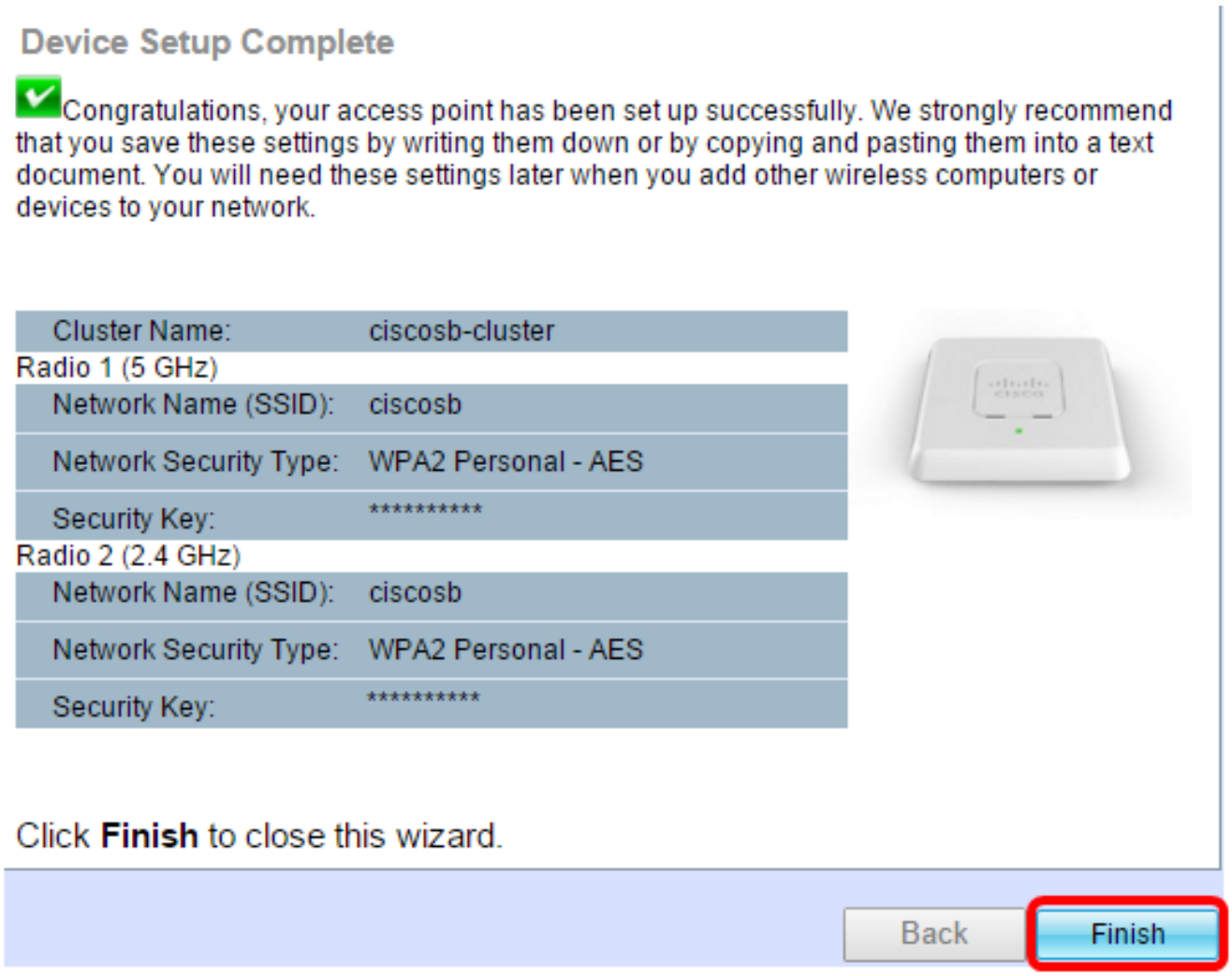
Hinweis: Die URL kann Ihre Firmenwebsite sein.



Schritt 9: Überprüfen und bestätigen Sie Ihre Einstellungen, und klicken Sie dann auf **Senden**.



Schritt 10: Wenn der Bildschirm Geräte-Setup abgeschlossen angezeigt wird, klicken Sie auf **Fertig stellen**, um den Setup-Assistenten zu schließen.



Sie sollten jetzt die Grundeinstellungen der Captive Portal-Funktion Ihres WAP konfiguriert haben.

Verwenden des webbasierten Dienstprogramms

Um die erweiterten Einstellungen des Captive Portals auf dem WAP zu konfigurieren, müssen Sie mehrere Schritte ausführen:

Global Enable the Captive Portal (Captive Portal global aktivieren) - Dadurch können Captive Portale wirksam werden.

Captive Portal Instance erstellen - Eine Captive Portal-Instanz ist ein Satz von Parametern, die steuern, wie sich ein Benutzer bei einem virtuellen Access Point (VAP) anmeldet.

Ordnen Sie eine Captive Portal-Instanz einem VAP zu. Benutzer, die versuchen, auf den VAP zuzugreifen, müssen die für die Instanz konfigurierten Parameter befolgen.

Anpassen des Webportals - Das Webportal ist die Webseite, auf der Benutzer umgeleitet werden, wenn sie versuchen, sich beim VAP anzumelden.

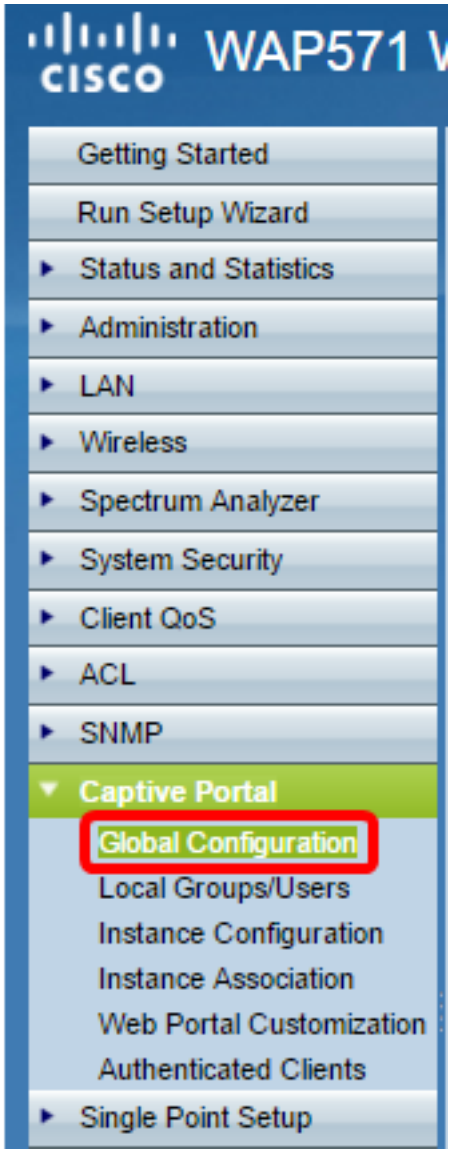
Create Local Group (Lokale Gruppe erstellen) - Die lokale Gruppe kann einer Instanz

zugewiesen werden, die Benutzer akzeptiert, die dieser Gruppe angehören.

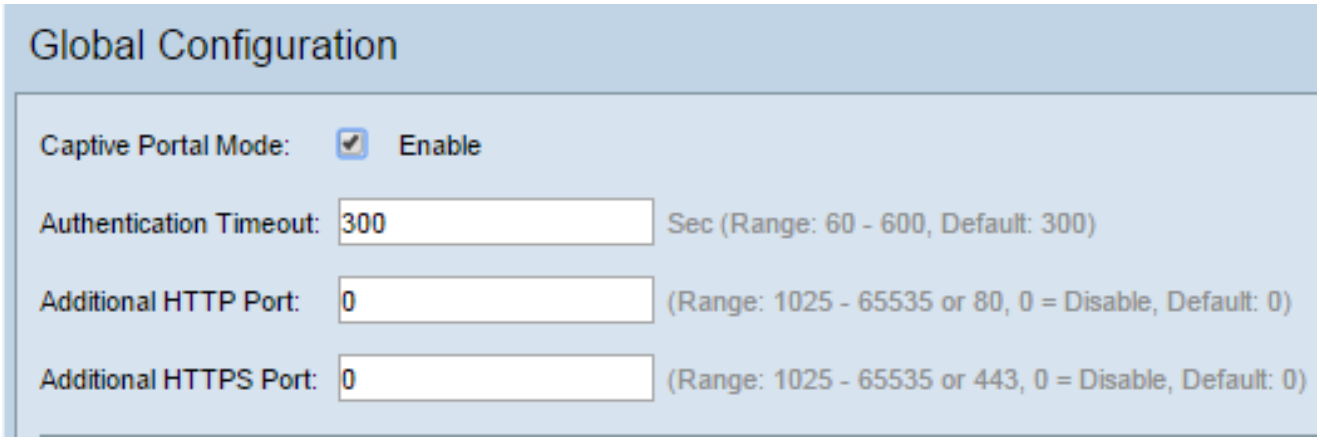
Lokalen Benutzer erstellen: Lokale Benutzer werden einer lokalen Gruppe hinzugefügt und können auf das Captive Portal zugreifen, für das die Gruppe konfiguriert ist.

Global aktivieren Sie das Captive Portal

Schritt 1: Wählen Sie im webbasierten Dienstprogramm **Captive Portal > Global Configuration aus**.



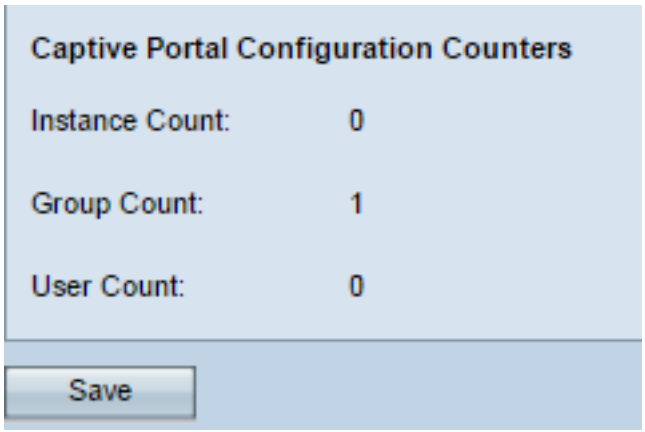
Schritt 2: (Optional) Geben Sie die Anzahl der Sekunden ein, die der Benutzer Authentifizierungsinformationen eingeben muss, bevor der WAP die Authentifizierungssitzung im Feld *Authentifizierungs-Timeout* schließt.



Schritt 3: (Optional) Wenn die HTTP-Informationen zwischen dem WAP und dem Client neben der Standardeinstellung einen anderen Port verwenden sollen, geben Sie die HTTP-Portnummer ein, die Sie im Feld *Zusätzlicher HTTP-Port* hinzufügen möchten. HTTP und andere Internetprotokolle verwenden Ports, um sicherzustellen, dass Geräte wissen, wo ein bestimmtes Protokoll zu finden ist. Sie können zwischen 80, 1025 und 65535 wählen oder 0 eingeben, um die Funktion zu deaktivieren. Der HTTP-Port und der HTTPS-Port dürfen nicht identisch sein.

Schritt 4: (Optional) Wenn für die HTTP-Informationen zwischen dem WAP und dem Client neben der Standardeinstellung ein anderer Port verwendet werden soll, geben Sie die HTTPS-Portnummer ein, die Sie im Feld *Zusätzlicher HTTPS-Port* hinzufügen möchten. Die Optionen sind 443, zwischen 1025 und 65535, oder geben Sie 0 ein, um zu deaktivieren. Der HTTP-Port und der HTTPS-Port dürfen nicht identisch sein.

Die folgenden Informationen werden im Bereich "Captive Portal Configuration Counters" angezeigt und können nicht konfiguriert werden.



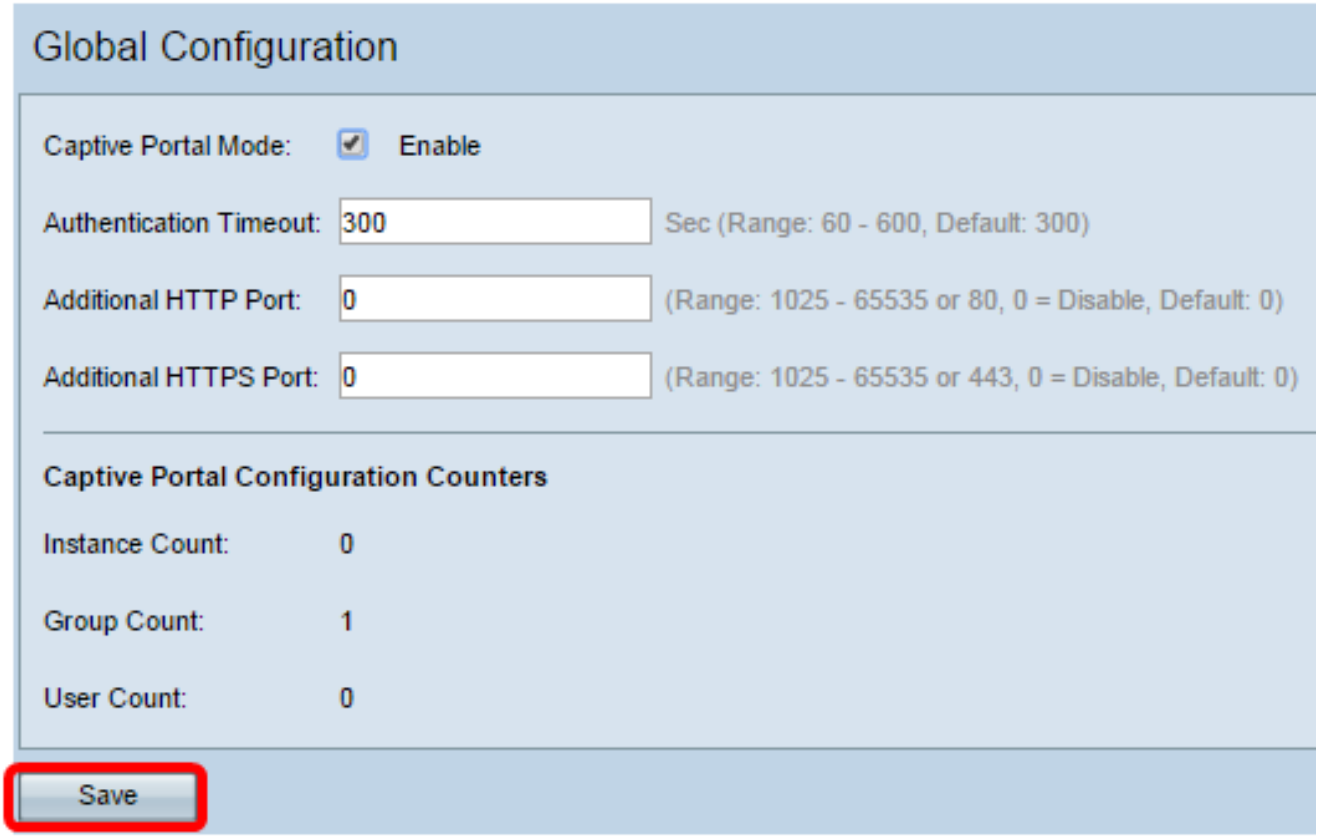
Instanzanzahl - Die Anzahl der auf dem WAP-Gerät konfigurierten CP-Instanzen. Auf dem WAP können maximal zwei CP konfiguriert werden.

Gruppenanzahl - Die Anzahl der auf dem WAP-Gerät konfigurierten CP-Gruppen. Es können bis zu zwei Gruppen konfiguriert werden. Die Standardgruppe kann nicht gelöscht werden.

Benutzeranzahl - Die Anzahl der auf dem WAP-Gerät konfigurierten CP-Benutzer. Auf dem WAP können maximal 128 Benutzer konfiguriert werden.

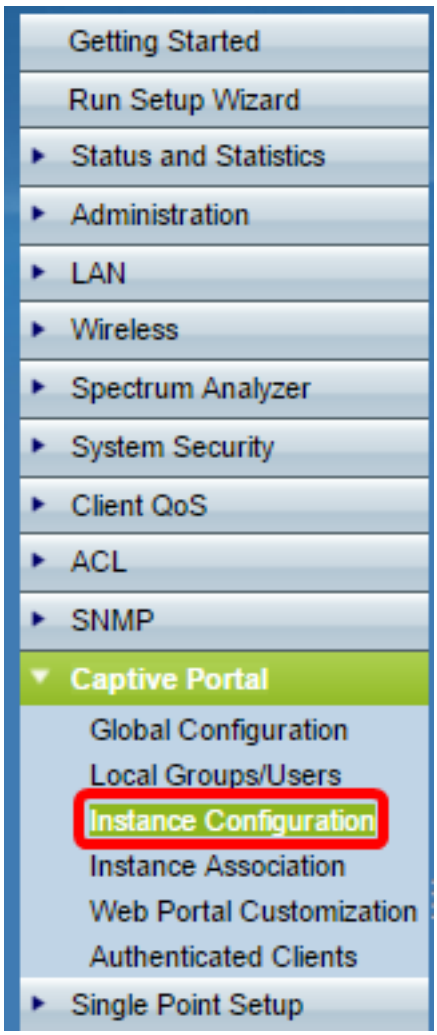
Schritt 5: Klicken Sie auf **Speichern**.

Hinweis: Die Änderungen werden in der Startkonfiguration gespeichert.



Instanzkonfiguration

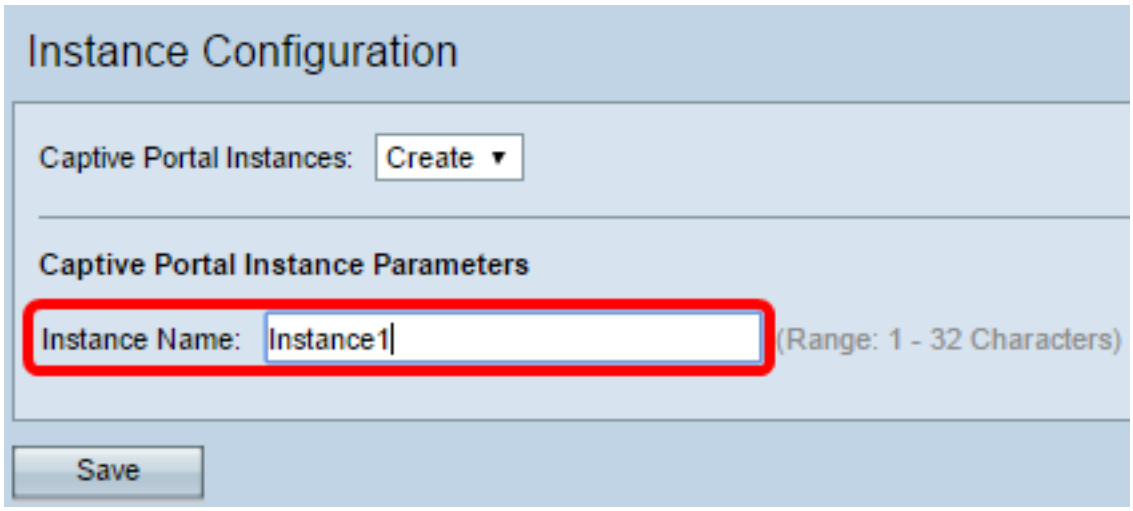
Schritt 6: Wählen Sie im webbasierten Dienstprogramm **Captive Portal > Instance Configuration aus**.



Schritt 7: In der Dropdown-Liste "Captive Portal Instances" (Captive Portal-Instanzen) sollten Sie die Instanz wiz-cp-inst1 bemerken. Sie können diesen Namen auswählen oder einen neuen Namen für die Instanzkonfiguration erstellen.

Schritt 8: (Optional) Geben Sie im Feld *Instanzname* einen Namen für die Konfiguration ein, und klicken Sie dann auf **Speichern**.

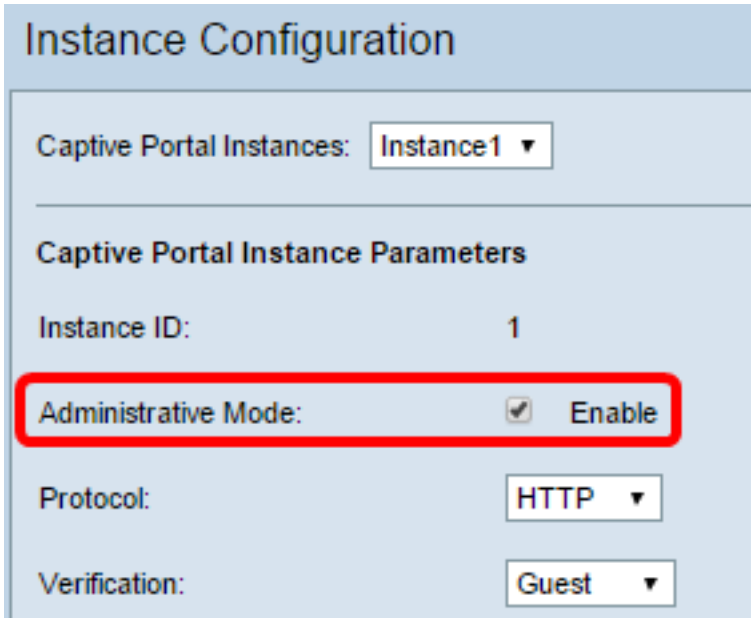
Hinweis: In diesem Beispiel wird eine neue Instanz erstellt.



Hinweis: Sie können maximal zwei Konfigurationen erstellen. Wenn Sie bereits zwei Instanzen erstellt haben, müssen Sie eine Instanz zum Bearbeiten auswählen.

Schritt 9: Im Fenster Instanzkonfiguration werden zusätzliche Informationen angezeigt. Die Instanz-ID ist ein nicht konfigurierbares Feld, das die Instanz-ID der aktuellen Instanz anzeigt.

Schritt 10: Aktivieren Sie das **Kontrollkästchen Aktivieren** im Verwaltungsmodus, um die CP-Instanz zu aktivieren.



Schritt 11: Wählen Sie aus der Dropdown-Liste Protocol (Protokoll) das Protokoll aus, das Sie für den Authentifizierungsprozess verwenden möchten.

HTTP: Verschlüsselt keine Informationen, die im Authentifizierungsprozess verwendet werden.

HTTPS: Stellt Verschlüsselung für Informationen bereit, die im Authentifizierungsprozess verwendet werden.

Hinweis: In diesem Beispiel wird HTTP verwendet.

Schritt 12: Wählen Sie aus der Dropdown-Liste Überprüfung eine Authentifizierungsmethode für CP aus.

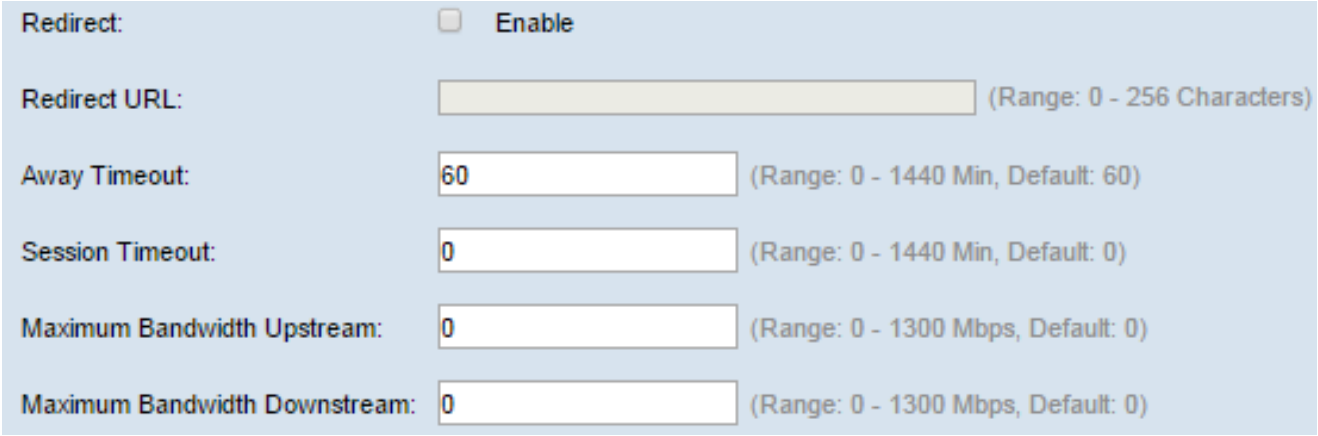
Guest (Gast): Der Benutzer muss keine Authentifizierung bereitstellen.

Local (Lokal): Der WAP überprüft die vom Benutzer bereitgestellten Authentifizierungsinformationen mit einer lokalen Datenbank, die auf dem WAP gespeichert ist.

RADIUS (RADIUS): Der WAP überprüft die vom Benutzer bereitgestellten Authentifizierungsinformationen mit der Datenbank eines Remote-RADIUS-Servers.

Zeitgeber: Wenn Sie Lokal oder Gast auswählen, fahren Sie mit Schritt 28 fort.

Schritt 13: (Optional) Wenn Sie Benutzer, die für eine konfigurierte URL verifiziert sind, umleiten möchten, aktivieren Sie das Kontrollkästchen **Enable** Redirect (Umleitung aktivieren). Wenn diese Option deaktiviert ist, wird für verifizierte Benutzer eine länderspezifische Willkommensseite angezeigt.



Schritt 14: (Optional) Geben Sie die URL ein, zu der Sie die verifizierten Benutzer umleiten möchten.

Hinweis: Dieser Schritt ist nur anwendbar, wenn Sie Redirect in Schritt 13 aktiviert haben.

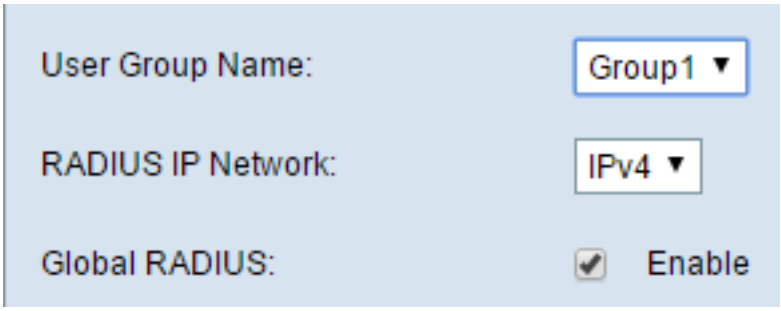
Schritt 15: Geben Sie im Feld *Away Timeout* (Abwesenheitszeit in Minuten) ein, wie viel Zeit ein Benutzer vom WAP trennen und in der Liste der WAP-authentifizierten Clients verbleiben kann. Wenn der Benutzer nicht länger mit dem WAP verbunden ist als mit dem Abwesenheitszeitwert, muss er erneut autorisiert werden, bevor er den WAP verwenden kann.

Schritt 16: Geben Sie im Feld *Session Timeout* (Sitzungszeitüberschreitung) die Zeitdauer (in Minuten) ein, die der WAP wartet, bevor er die Sitzung beendet. Ein Wert von 0 bedeutet, dass die Zeitüberschreitung nicht erzwungen wird.

Schritt 17: Geben Sie *im* Feld *Maximale Bandbreite für Upstream* die maximale Upload-Geschwindigkeit (in Mbit/s) ein, die ein Client über das Captive Portal senden kann.

Schritt 18: Geben Sie im Feld *Maximum Bandwidth Downstream* (Maximale Downstream-Bandbreite) die maximale Download-Geschwindigkeit (in Mbit/s) ein, die ein Client über das Captive Portal empfangen kann.

Schritt 19: Wählen Sie aus der Dropdown-Liste User Group Name (Benutzername) die Gruppe aus, die Sie der CP-Instanz zuweisen möchten. Jeder Benutzer, der Mitglied der Gruppe ist, die Sie auswählen, darf auf den WAP zugreifen.



Hinweis: Der Überprüfungsmodus in Schritt 12 muss entweder Local (Lokal) oder RADIUS (RADIUS) sein, um eine Gruppe zuzuweisen.

Schritt 20: Wählen Sie aus der Dropdown-Liste RADIUS IP Network (RADIUS-IP-Netzwerk) den Typ des Internetprotokolls aus, der vom RADIUS-Client verwendet wird.

IPv4 - Die Adresse des RADIUS-Clients hat das Format xxx.xxx.xxx.xxx (192.0.2.10).

IPv6 - Die Adresse des RADIUS-Clients hat das Format xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx (2001:DB8::CAD5:7D91).

Schritt 21: (Optional) Aktivieren Sie das Kontrollkästchen **Enable** Global RADIUS (Globalen RADIUS aktivieren), wenn Sie die globale RADIUS-Serverliste für die Authentifizierung verwenden möchten. Wenn Sie einen separaten Satz von RADIUS-Servern verwenden möchten, lassen Sie das Kontrollkästchen deaktiviert, und konfigurieren Sie die RADIUS-Server auf dieser Seite.

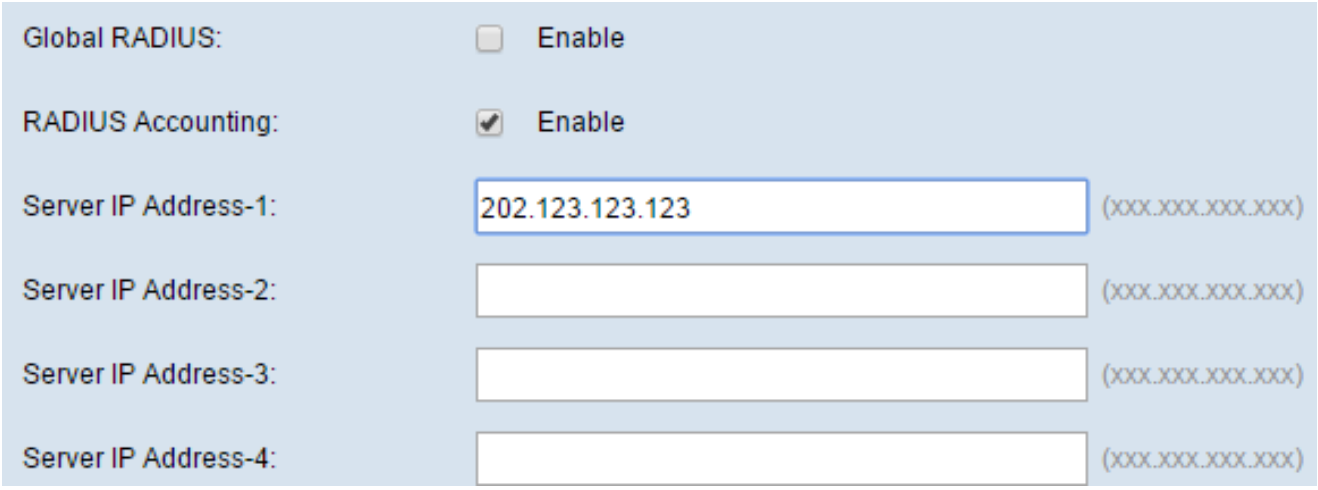
Zeitgeber: Fahren Sie mit Schritt 28 fort, wenn Sie Global RADIUS aktivieren.

Hinweis: In diesem Beispiel ist Global RADIUS nicht aktiviert.

Schritt 22: (Optional) Aktivieren Sie das Kontrollkästchen **Enable** RADIUS Accounting (RADIUS-Accounting **aktivieren**), wenn Sie die Zeit und die Datennutzung der Clients im WAP-Netzwerk nachverfolgen und messen möchten.

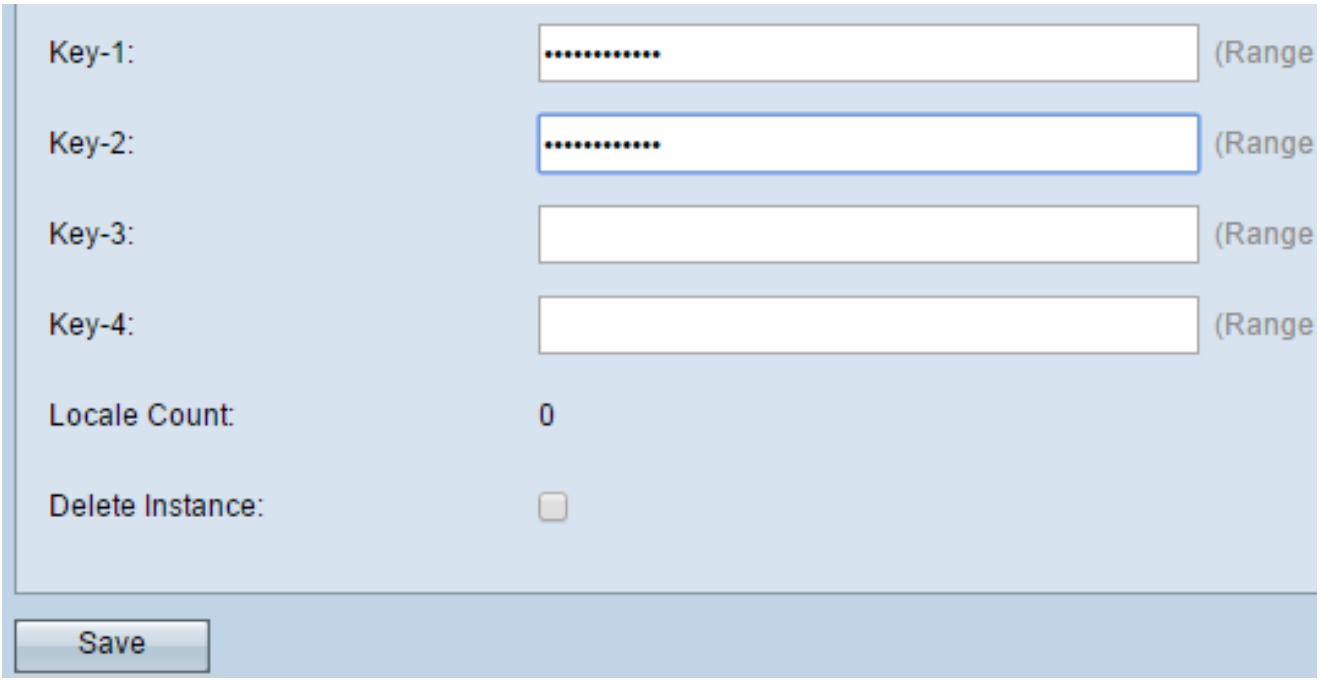
Hinweis: Wenn das Kontrollkästchen Global RADIUS in Schritt 21 aktiviert wurde, müssen Sie keine zusätzlichen RADIUS-Server konfigurieren.

Schritt 23: Geben Sie im Feld *Server IP Address-1 (Server-IP-Adresse-1*) die IP-Adresse des RADIUS-Servers ein, den Sie als Primärserver verwenden möchten. Die IP-Adresse sollte dem jeweiligen Adressformat von IPv4 oder IPv6 entsprechen.



Schritt 24: (Optional) Sie können bis zu drei Backup-RADIUS-Server konfigurieren, die nacheinander überprüft werden, bis eine Übereinstimmung gefunden ist. Wenn keine Übereinstimmung gefunden wird, wird dem Benutzer der Zugriff verweigert. Geben Sie in die Felder Server IP Address (Server-IP-Adresse) (2 bis 4) die IP-Adresse der Backup-RADIUS-Server ein, die verwendet werden soll, wenn die Authentifizierung mit dem primären Server fehlschlägt.

Schritt 25: Geben Sie im Feld *Key-1* den gemeinsamen geheimen Schlüssel ein, den das WAP-Gerät für die Authentifizierung beim primären RADIUS-Server verwendet. Dabei muss es sich um denselben Schlüssel handeln, der auf dem RADIUS-Server konfiguriert wurde.



Schritt 26: Geben Sie in den übrigen Schlüsselfeldern (2-4) den gemeinsamen geheimen Schlüssel ein, den das WAP-Gerät zur Authentifizierung der entsprechenden Backup-RADIUS-Server verwendet.

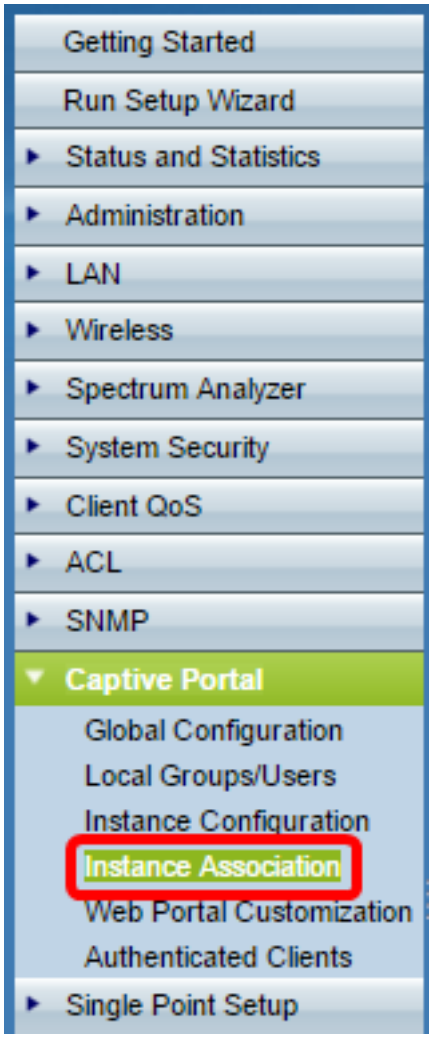
Hinweis: Locale Count ist ein nicht konfigurierbares Feld, das die Anzahl der Gebietsschemas anzeigt, die dieser Instanz zugeordnet sind.

Schritt 27: (Optional) Um die aktuelle Instanz zu löschen, aktivieren Sie das Kontrollkästchen **Instanz löschen**.

Schritt 28: Klicken Sie auf **Speichern**.

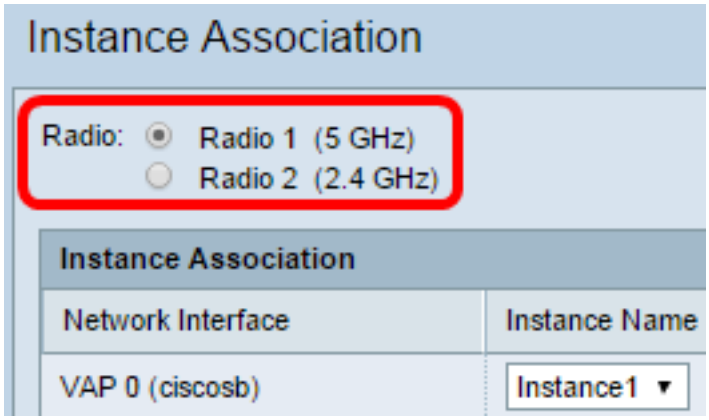
Zuordnen der Instanz zu VAP

Schritt 29: Wählen Sie im webbasierten Dienstprogramm **Captive Portal > Instance Association aus**.



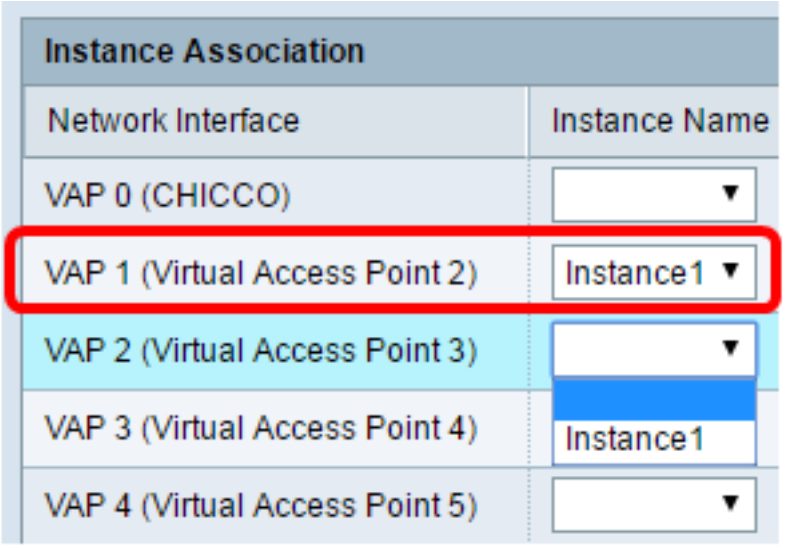
Schritt 30: Klicken Sie auf das Optionsfeld des Radios, dem Sie eine Instanz im Bereich Radio (Funkübertragung) zuordnen möchten.

Hinweis: In diesem Beispiel wird Radio 1 (5 GHz) ausgewählt.

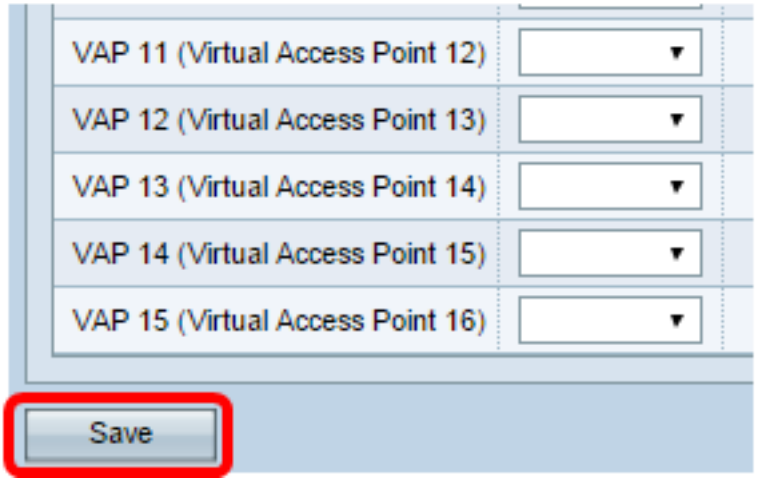


Schritt 31: Wählen Sie eine Instanzkonfiguration aus der Dropdown-Liste Instanzname aus, um eine Verknüpfung mit dem angegebenen VAP herzustellen.

Hinweis: In diesem Beispiel wird die in Schritt 8 erstellte Instanz1 für VAP 1 (Virtual Access Point 2) verwendet.



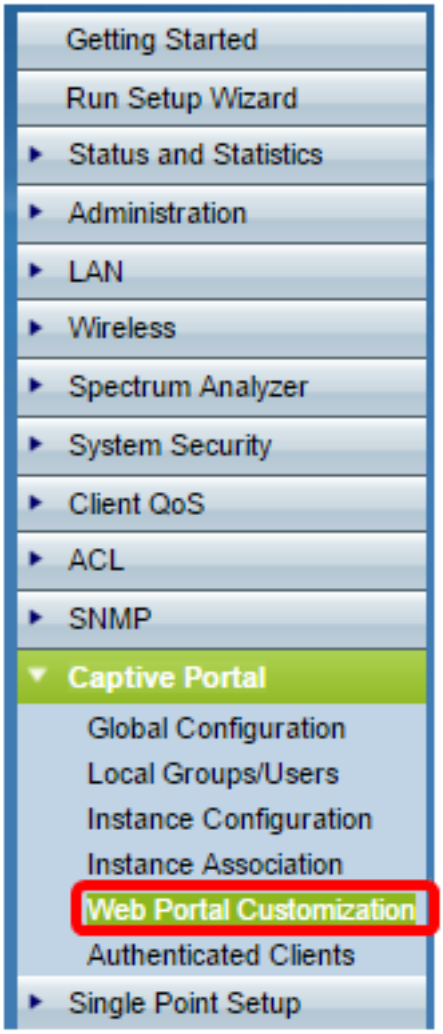
Schritt 32: Klicken Sie auf **Speichern**.



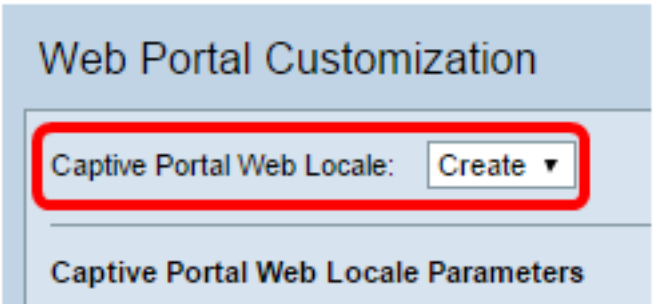
Webportal anpassen

Ein Gebietsschema (Authentifizierungs-Webseite) ist die Webseite, die der WAP-Benutzer sieht, wenn er versucht, auf das Internet zuzugreifen. Auf der Seite zur Anpassung des Webportals können Sie ein Gebietsschema anpassen und einer Captive Portal-Instanz zuweisen.

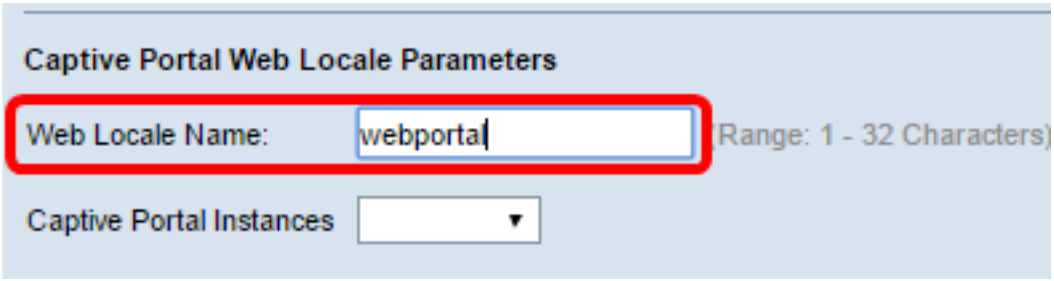
Schritt 33: Wählen Sie im webbasierten Dienstprogramm **Captive Portal > Web Portal Customization aus**.



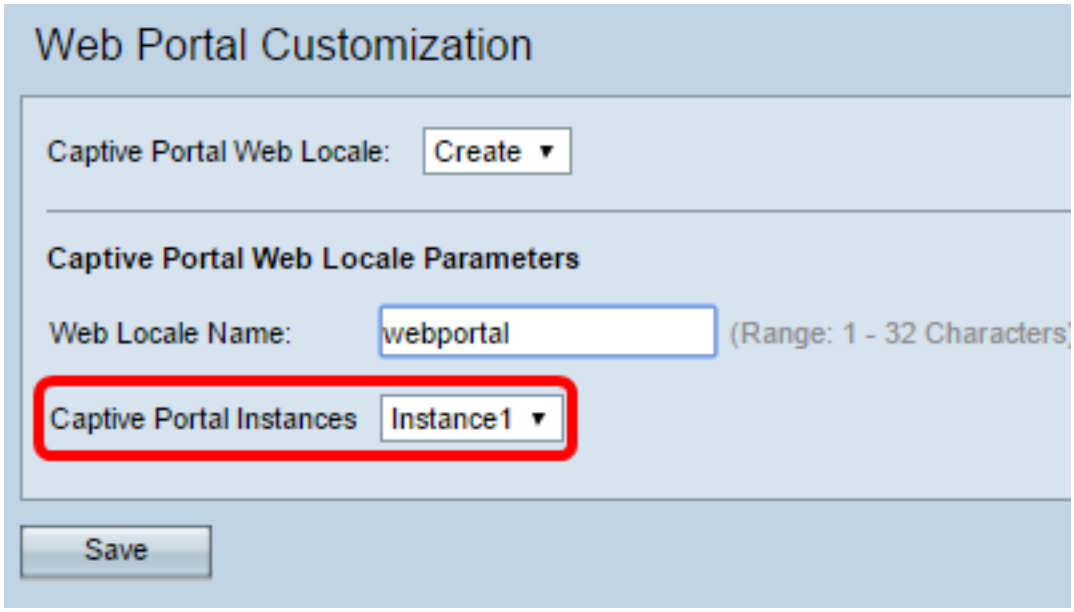
Schritt 34: Wählen Sie **Create** (Erstellen) aus der Dropdown-Liste Captive Portal Web Locale aus, um ein neues Gebietsschema zu erstellen.



Schritt 35: Geben Sie den Namen des Gebietsschemas in das Feld *Web Locale Name* ein.

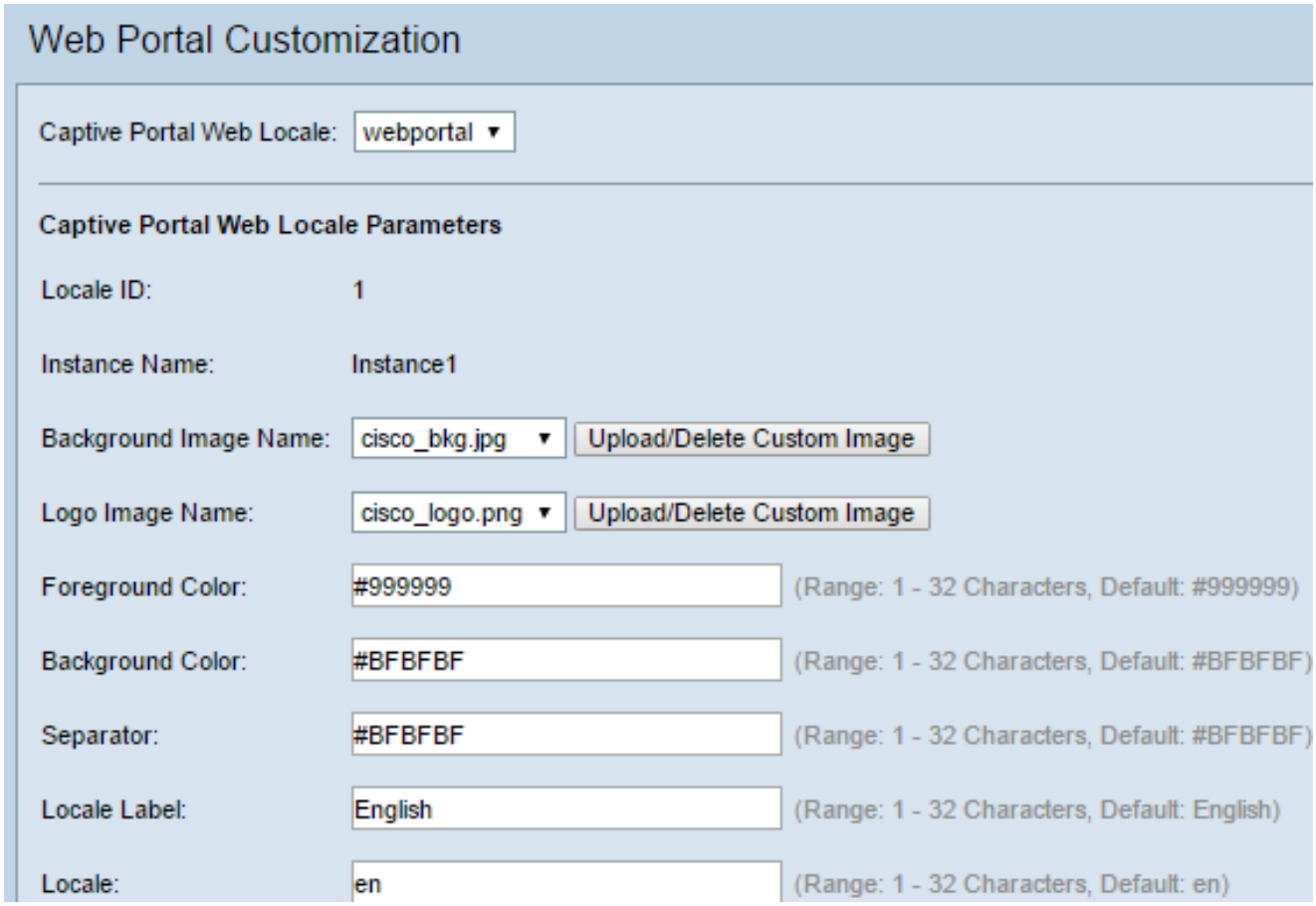


Schritt 36: Wählen Sie aus der Dropdown-Liste Captive Portal Instances (Instanzen des Captive Portals) eine Captive Portal-Instanz aus, der das Gebietsschema zugeordnet ist. Sie können mehrere Gebietsschemas einer einzelnen Captive Portal-Instanz zuordnen. Der Benutzer kann auf einen Link klicken, um zu einem anderen Gebietsschema zu wechseln.



Schritt 37: Klicken Sie auf **Speichern**, um ein neues Gebietsschema zu erstellen.

Hinweis: Auf der Seite zur Anpassung des Webportals werden zusätzliche Informationen angezeigt.



Die Gebietsschemas-ID ist ein nicht konfigurierbares Feld, das die ID-Nummer des aktuellen Gebietsschemas anzeigt.

Instanzname ist ein nicht konfigurierbares Feld, das den dem Gebietsschema zugeordneten Namen der Captive Portal-Instanz anzeigt.

Schritt 38: Wählen Sie aus der Dropdown-Liste Hintergrundbildname ein Bild aus, das im Hintergrund Gebietsschema angezeigt werden soll. Klicken Sie auf die Schaltfläche **Benutzerdefiniertes Bild hochladen/löschen**, um ein eigenes Bild hinzuzufügen. Weitere Informationen erhalten Sie im Abschnitt Benutzerdefiniertes Bild hochladen/löschen.

Schritt 39: Wählen Sie aus der Dropdown-Liste Logo Image Name (Name des Logos) ein Bild für die Anzeige in der oberen linken Ecke der Seite aus.

Schritt 40: Geben Sie im Feld *Vordergrundfarbe* den sechsstelligen HTML-Code (Hyper Text Transfer Protocol) für die Vordergrundfarbe des Gebietsschemas ein.

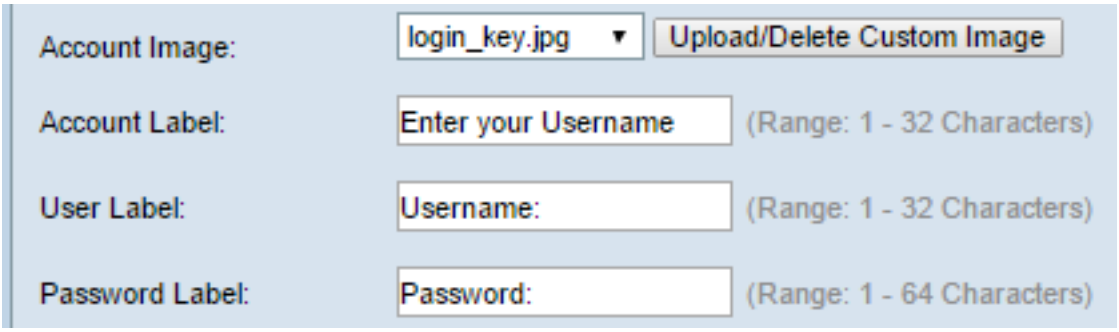
Schritt 41: Geben Sie im Feld *Hintergrundfarbe* den sechsstelligen HTML-Code für die Hintergrundfarbe des Gebietsschemas ein.

Schritt 42: Geben Sie im Feld *Trennzeichen* den sechsstelligen HTML-Code für die Farbe der horizontalen Zeile ein, die die Seitenkopfzeile vom Seitentext trennt.

Schritt 43: Geben Sie einen beschreibenden Namen für das Gebietsschema in das Feld *Locale Label (Gebietsschemabezeichnung)* ein. Wenn Sie mehrere Gebietsschemas haben, ist dies der Name des Links, auf den Sie klicken, um zwischen Gebietsschemas zu wechseln. Wenn Sie beispielsweise ein Gebietsschema für Englisch und Spanisch haben, können Sie dies in Ihrem Gebietsnamen angeben.

Schritt 44: Geben Sie im Feld *Gebietsschema* eine Abkürzung für das Gebietsschema ein.

Schritt 45: Wählen Sie aus der Dropdown-Liste Kontobild ein Bild aus, das über dem Anmeldefeld angezeigt werden soll.

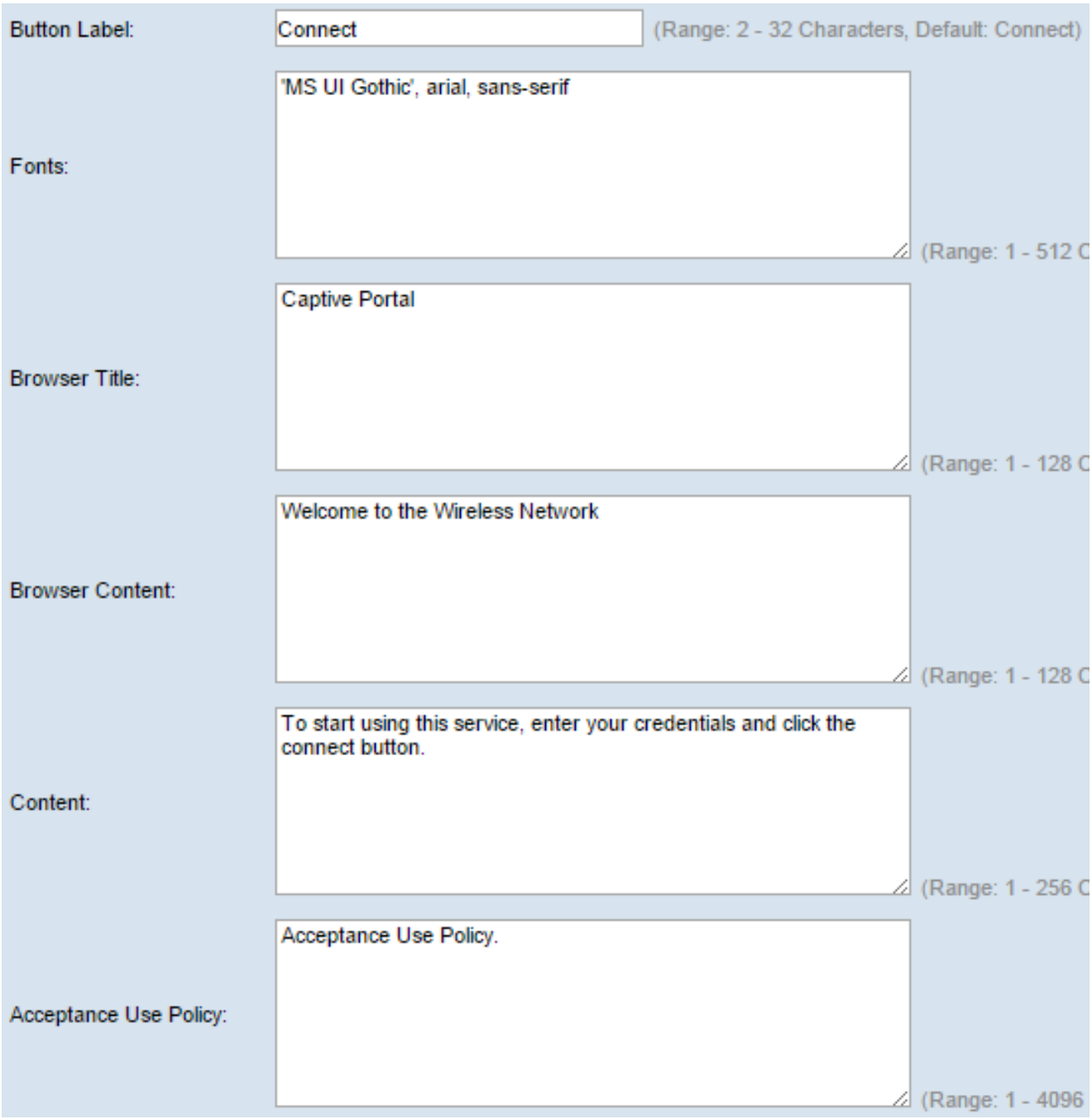


Schritt 46: Geben Sie im Feld *Kontonamen* die Anweisungen ein, die den Benutzer zur Eingabe seines Benutzernamens auffordern.

Schritt 47: Geben Sie im Textfeld *User Label* (Benutzerbezeichnung) das Label für das Textfeld User Name (Benutzername) ein.

Schritt 48: Geben Sie im Textfeld *Password Label (Passwortbezeichnung)* die Bezeichnung für das Kennwortfeld ein.

Schritt 49: Geben Sie im Feld *Button Label (Button-Bezeichnung*) die Bezeichnung für die Schaltfläche ein, auf die die Benutzer klicken, um ihren Benutzernamen und ihr Kennwort zu senden.



Schritt 50: Geben Sie im Feld *Schriftarten* den für das Gebietsschema verwendeten Schriftartnamen ein. Sie können mehrere Schriftarten eingeben, die durch ein Komma getrennt sind. Wenn der erste Schriftstil vom Client-Gerät nicht gefunden wird, wird die nächste Schriftart verwendet. Wenn ein Schriftartname mehrere Wörter durch Leerzeichen voneinander getrennt hat, können Sie einen einzelnen Anführungszeichen um den Schriftnamen herum verwenden. Beispielsweise "MS UI Gothic" , arial, sans-serif usw.

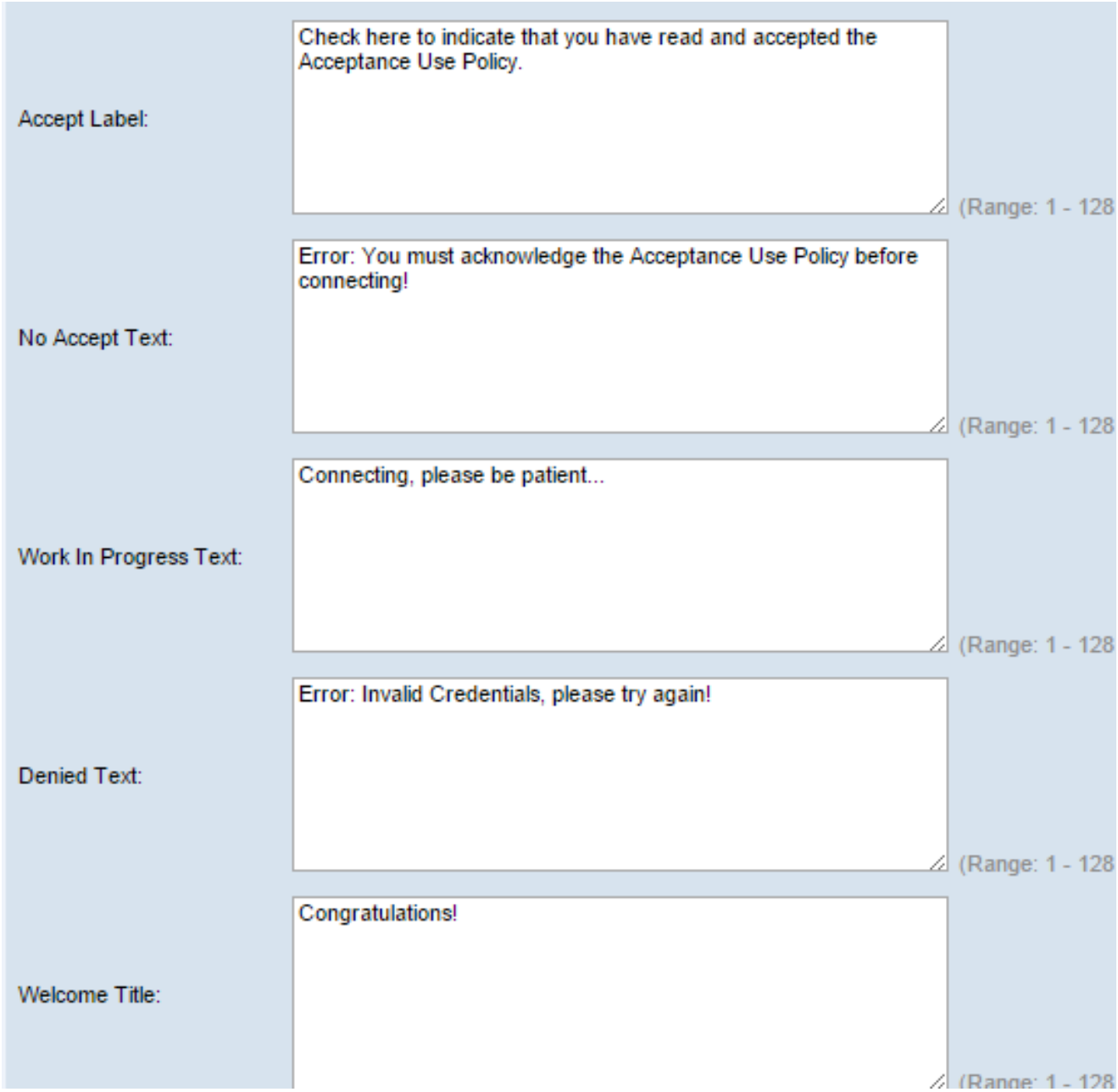
Schritt 51: Geben Sie im Feld *Browser Title* (Browsertitel) den Text ein, den Sie in der Titelleiste des Browsers anzeigen möchten.

Schritt 52: Geben Sie im Feld *Browserinhalt* den Text ein, den Sie in der Seitenüberschrift anzeigen möchten.

Schritt 53: Geben Sie im *Content*-Feld den Text ein, der den Benutzer anweist, zu handeln. Dieses Feld wird unter den Textfeldern Benutzername und Kennwort angezeigt.

Schritt 54: Geben Sie im Feld *Acceptance Use Policy* (Richtlinie zur Akzeptanznutzung) die Begriffe ein, denen Benutzer zustimmen müssen, wenn sie auf den WAP zugreifen möchten.

Schritt 55: Geben Sie im Feld *Accept Label (Label akzeptieren*) den Text ein, der Benutzer anweist, zu überprüfen, ob sie die Richtlinie zur Verwendung von Acceptance gelesen und akzeptiert haben.



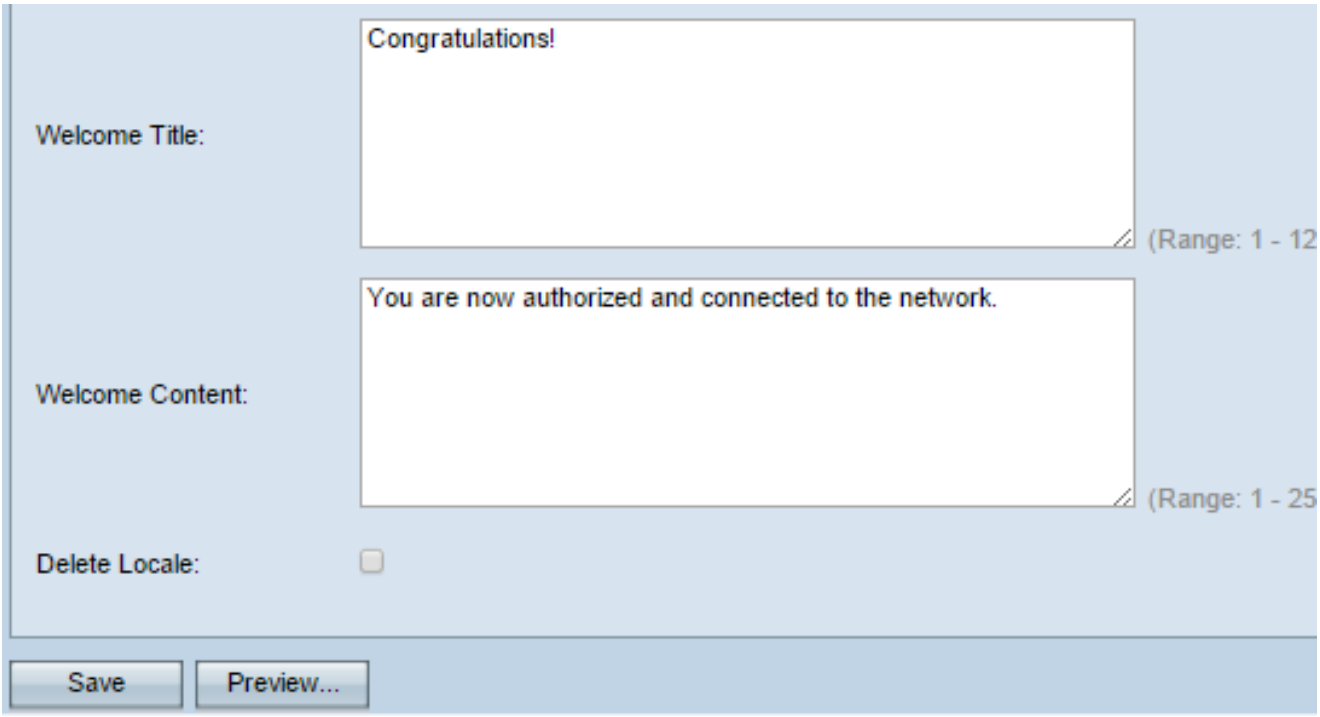
Schritt 56: Geben Sie im Feld *No Accept Text (Text ohne Zustimmung*) den Text ein, der einen Benutzer auffordert, wenn er Anmeldeinformationen einreicht, aber die Acceptance Use Policy (Richtlinie zur Akzeptanznutzung) nicht akzeptiert.

Schritt 57: Geben Sie im Feld *Text in Bearbeitung* den Text ein, der angezeigt wird, während der WAP die angegebenen Anmeldeinformationen überprüft.

Schritt 58: Geben Sie im Feld *Denied Text (Abgelehnter Text*) den Text ein, der angezeigt wird, wenn die Authentifizierung eines Benutzers fehlschlägt.

Schritt 59: Geben Sie im Feld *Welcome Title* (Willkommenstitel) den Titeltext ein, der angezeigt wird, wenn ein Client erfolgreich authentifiziert wurde.

Schritt 60: Geben Sie im *Feld Welcome Content* (Willkommensinhalte) den Text ein, der einem Client angezeigt wird, der mit dem Netzwerk verbunden ist.

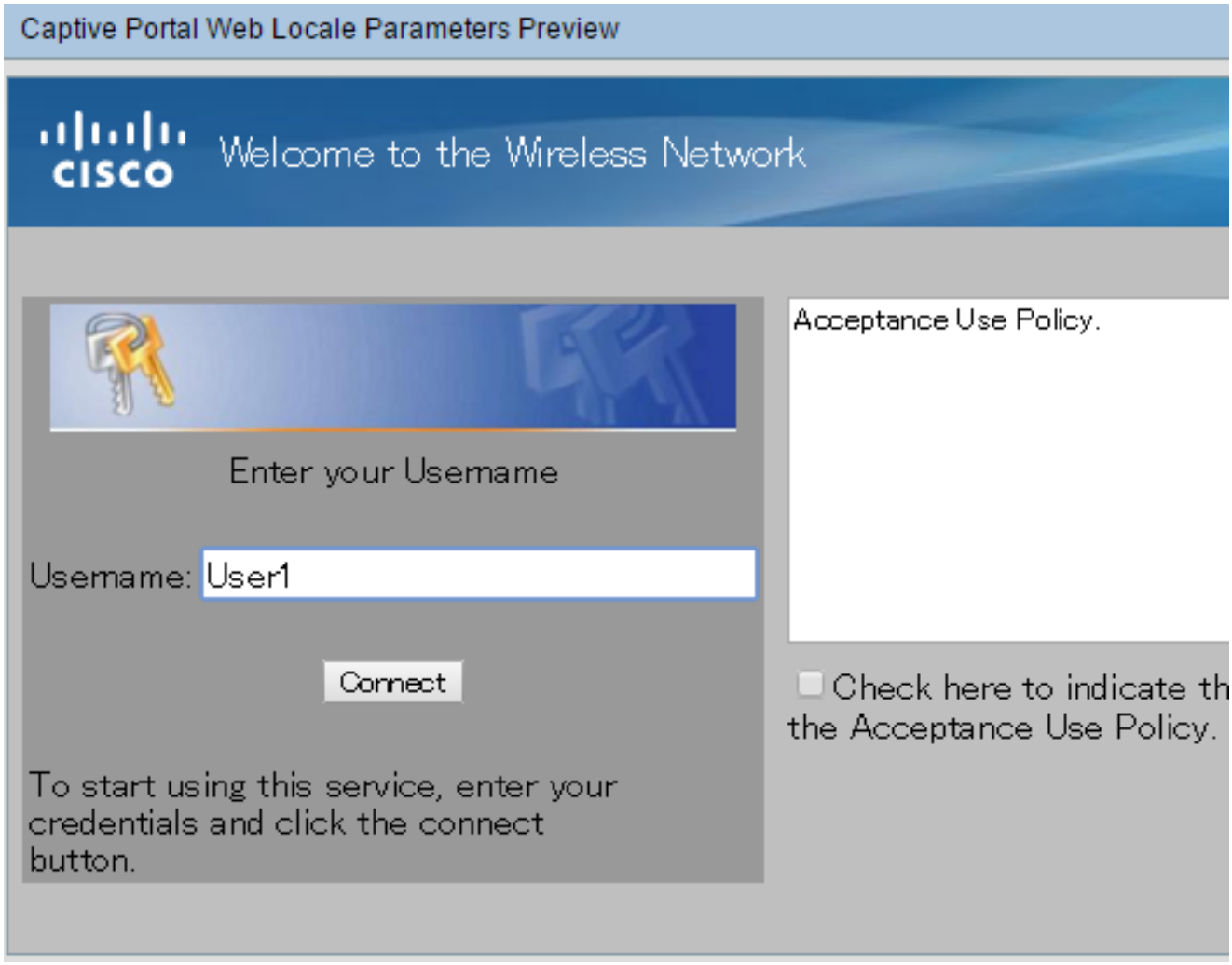


Schritt 61: (Optional) Um das aktuelle Gebietsschema zu löschen, aktivieren Sie das Kontrollkästchen **Gebietsschema löschen**.

Schritt 62: Klicken Sie auf **Speichern**.

Schritt 63: (Optional) Um Ihr aktuelles Gebietsschema anzuzeigen, klicken Sie auf **Vorschau** . Wenn Sie Änderungen vornehmen, klicken Sie vor der Vorschau auf **Speichern**, um die Änderungen zu aktualisieren.

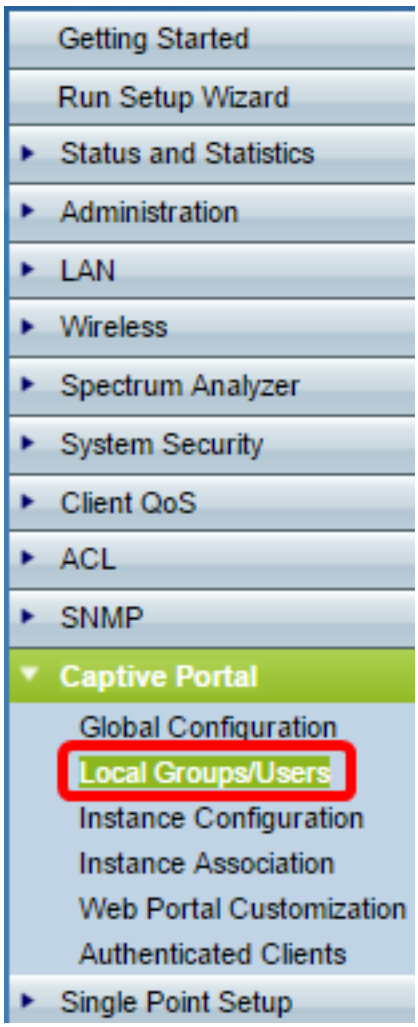
Hinweis: Der Anmeldungsbildschirm des Captive Portals ähnelt dem folgenden Bild:



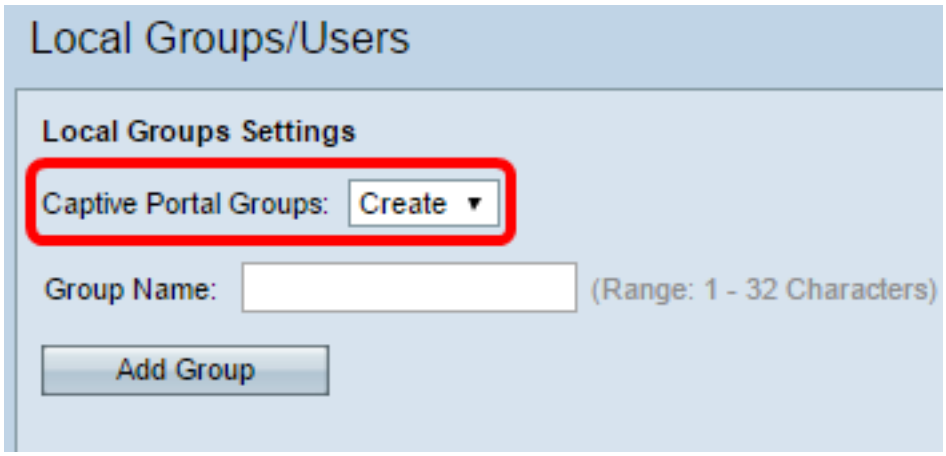
Lokale Gruppe erstellen

Bei einem Captive Portal, das keine Gastbenutzer ist, müssen sich Benutzer basierend auf ihrem Benutzernamen und Kennwort anmelden. Der WAP erstellt eine lokale Gruppe, die eine Gruppe von lokalen Benutzern enthält. Die lokale Gruppe wird dann an eine Instanz angefügt. Lokale Benutzer, die Mitglied der lokalen Gruppe sind, können über das Captive Portal auf das Portal zugreifen. Die lokale Standardgruppe ist immer aktiv und kann nicht gelöscht werden. Dem WAP können bis zu zwei zusätzliche lokale Gruppen hinzugefügt werden.

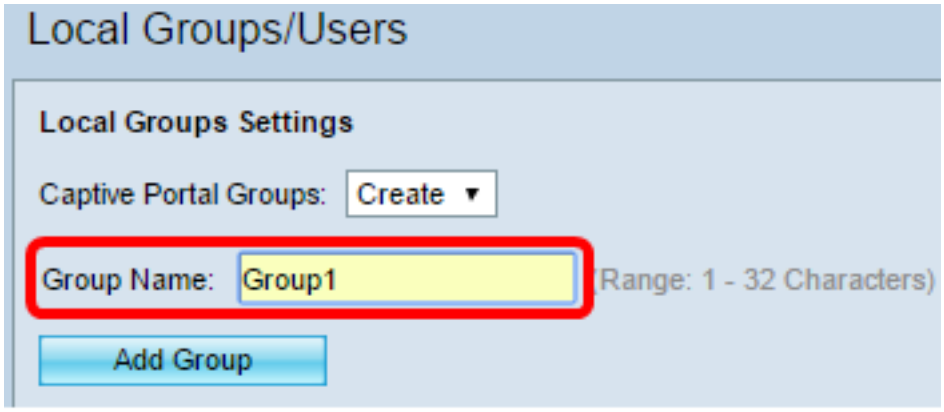
Schritt 64: Wählen Sie im webbasierten Dienstprogramm **Captive Portal > Local Groups/Users aus**.



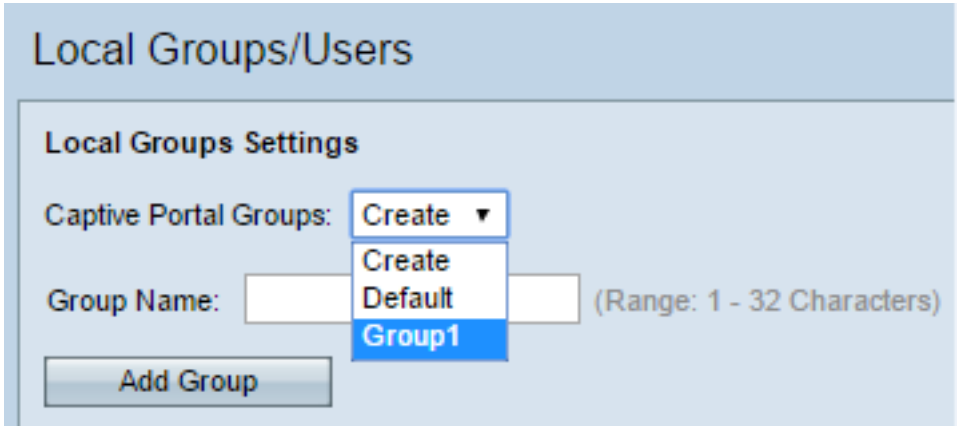
Schritt 65: Wählen Sie **Erstellen** aus der Dropdown-Liste Captive Portal Groups (Captive Portal-Gruppen) aus.



Schritt 66: Geben Sie im Feld *Gruppenname* den Namen der lokalen Gruppe ein.



Schritt 67: Klicken Sie auf **Gruppe hinzufügen**, um die Gruppe zu speichern.

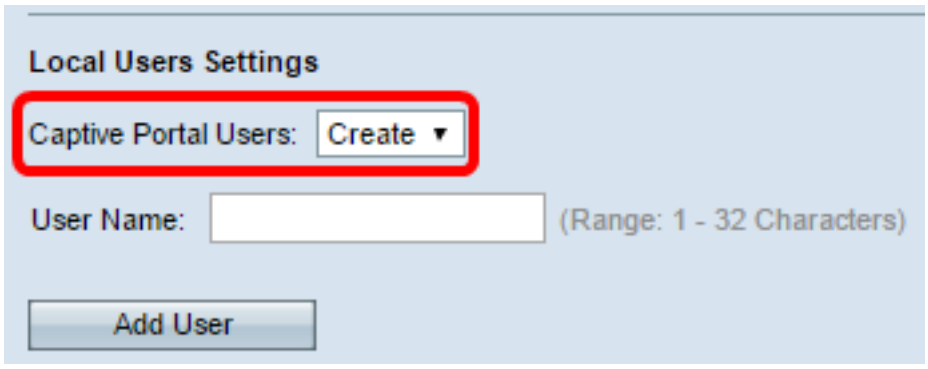


Hinweis: Sie können einer Instanz in Schritt 19 des Abschnitts "Instanzkonfiguration" eine lokale Gruppe zuweisen.

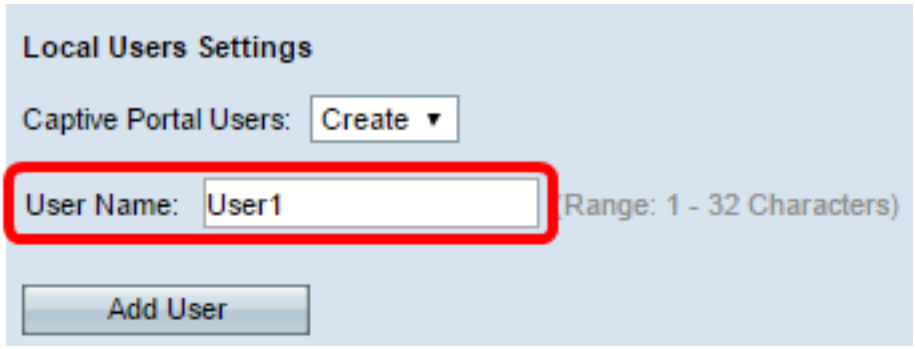
Lokalen Benutzer erstellen

Lokale Benutzer werden einer lokalen Gruppe hinzugefügt. Diese Benutzer können auf ein Captive Portal zugreifen, das über eine Instanz verfügt, deren lokale Gruppe konfiguriert ist. Einige Informationen, die auf der Seite "Lokale Benutzer" konfiguriert sind, werden auch auf der Seite "Instanzkonfiguration" konfiguriert. Der für einen lokalen Benutzer konfigurierte Wert hat Vorrang vor dem für eine Instanz konfigurierten Wert. In der lokalen Datenbank können bis zu 128 autorisierte Benutzer konfiguriert werden.

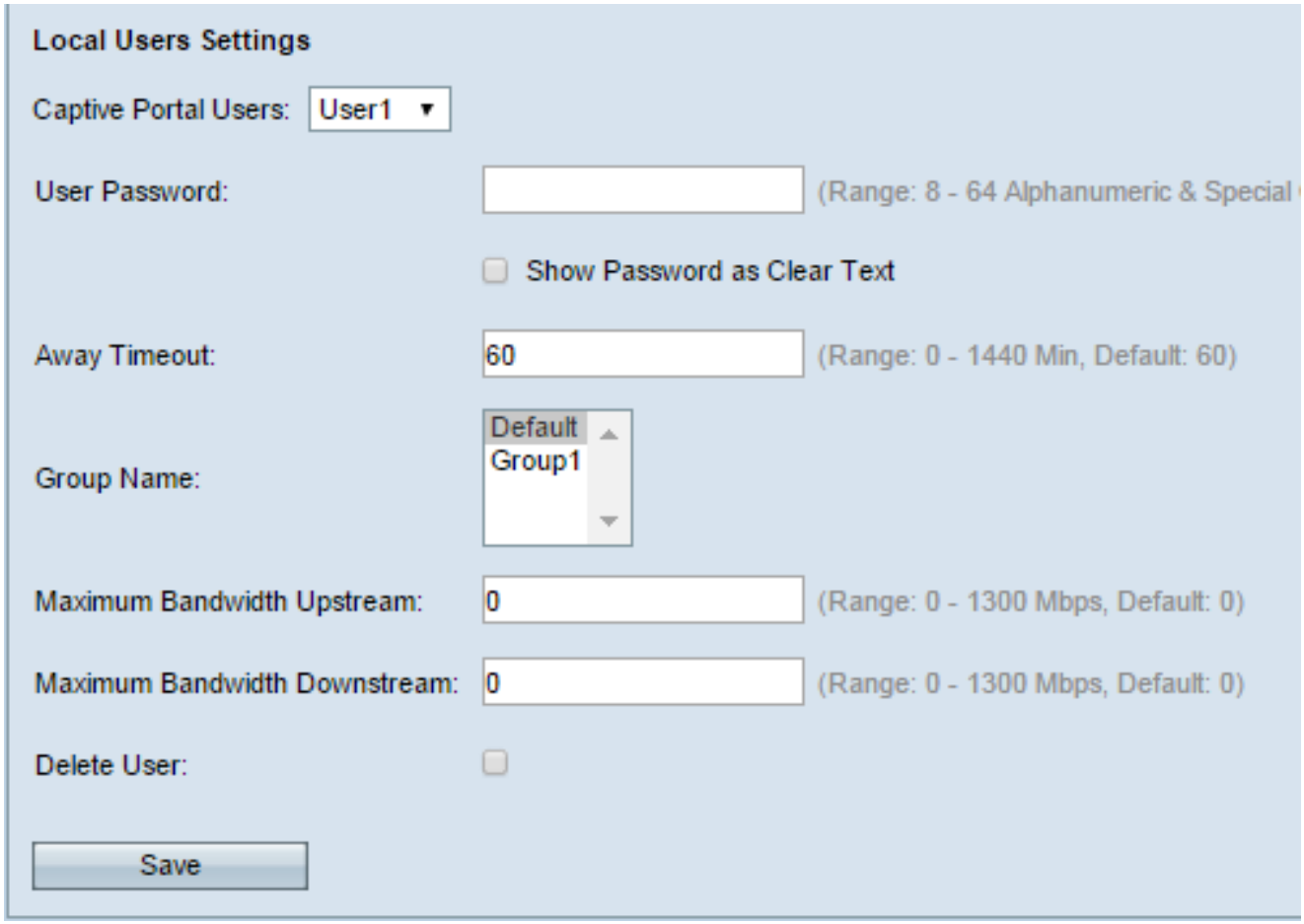
Schritt 68: Wählen Sie **Create** (Erstellen) aus der Dropdown-Liste Captive Portal Users (Captive Portal-Benutzer) aus.



Schritt 69: Geben Sie im Feld *Benutzername* den Benutzernamen ein, den Sie hinzufügen möchten.



Schritt 70: Klicken Sie auf **Benutzer hinzufügen**, um den neuen Benutzer zu erstellen. Im Fenster Lokale Benutzereinstellungen werden zusätzliche Informationen angezeigt.



Schritt 71: Geben Sie im Feld *User Password* (Benutzerkennwort) das dem Benutzer zugeordnete Kennwort ein.

Schritt 72: (Optional) Um das Kennwort im Klartext anzuzeigen, aktivieren Sie das Kontrollkästchen **Kennwort als Klartext anzeigen**. Wenn das Kontrollkästchen nicht aktiviert ist, wird das Kennwort maskiert.

Schritt 73: Geben Sie im Feld *Away Timeout* (Abwesend-Timeout) die Zeitdauer (in Minuten) ein, die ein Benutzer vom WAP trennen und in der Liste der WAP-authentifizierten Clients verbleiben kann. Wenn der Benutzer nicht länger mit dem WAP verbunden ist als mit dem Abwesenheitszeitlimit, muss er erneut autorisiert werden, bevor er den WAP verwenden kann.

Schritt 74: Klicken Sie im Feld *Gruppenname* auf die lokale Gruppe, der der Benutzer beitreten soll.

Schritt 75: Geben Sie im Feld *Maximum Bandwidth Upstream* (Maximale Upstream-Bandbreite) die maximale Upload-Geschwindigkeit in Mbit/s ein, die ein Client über das Captive Portal senden kann.

Schritt 76: Geben Sie im Feld *Maximum Bandwidth Downstream* (Downstream-Bandbreite für maximale Bandbreite) die maximale Downloadgeschwindigkeit in Mbit/s ein, die ein Client über das Captive Portal empfangen kann.

Schritt 77: (Optional) Um einen lokalen Benutzer zu löschen, aktivieren Sie das Kontrollkästchen **Benutzer löschen**.

Schritt 78: Klicken Sie auf **Speichern**.

Sie sollten jetzt die erweiterten Captive Portal-Einstellungen Ihres WAP571 oder WAP571E konfiguriert haben.