Captive Portal auf dem WAP561 und WAP551 erstellen

Ziel

Über ein Captive Portal können Sie den Zugriff auf Ihr Netzwerk einschränken, bis die Wireless-Benutzer verifiziert wurden. Wenn ein Benutzer seinen Webbrowser öffnet, wird er auf eine Anmeldeseite umgeleitet, auf der er seinen Benutzernamen und sein Kennwort eingeben muss. Zwei Arten von Benutzern können 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 ein Captive Portal für WAP561 und WAP551 erstellt wird.

Um ein Captive Portal am Wireless Access Point (WAP) zu erstellen, müssen Sie mehrere Schritte ausführen:

·Global aktivieren Captive Portale auf dem WAP. Dadurch können Captive Portale wirksam werden.

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

·Zuordnen einer Captive Portal-Instanz zu einem VAP Benutzer, die versuchen, auf den VAP zuzugreifen, müssen die für die Instanz konfigurierten Parameter befolgen.

·Webportal anpassen Das Webportal ist die Webseite, auf die Benutzer zugreifen, wenn sie versuchen, sich beim VAP anzumelden.

·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.

Anwendbare Geräte

WAP551
WAP561

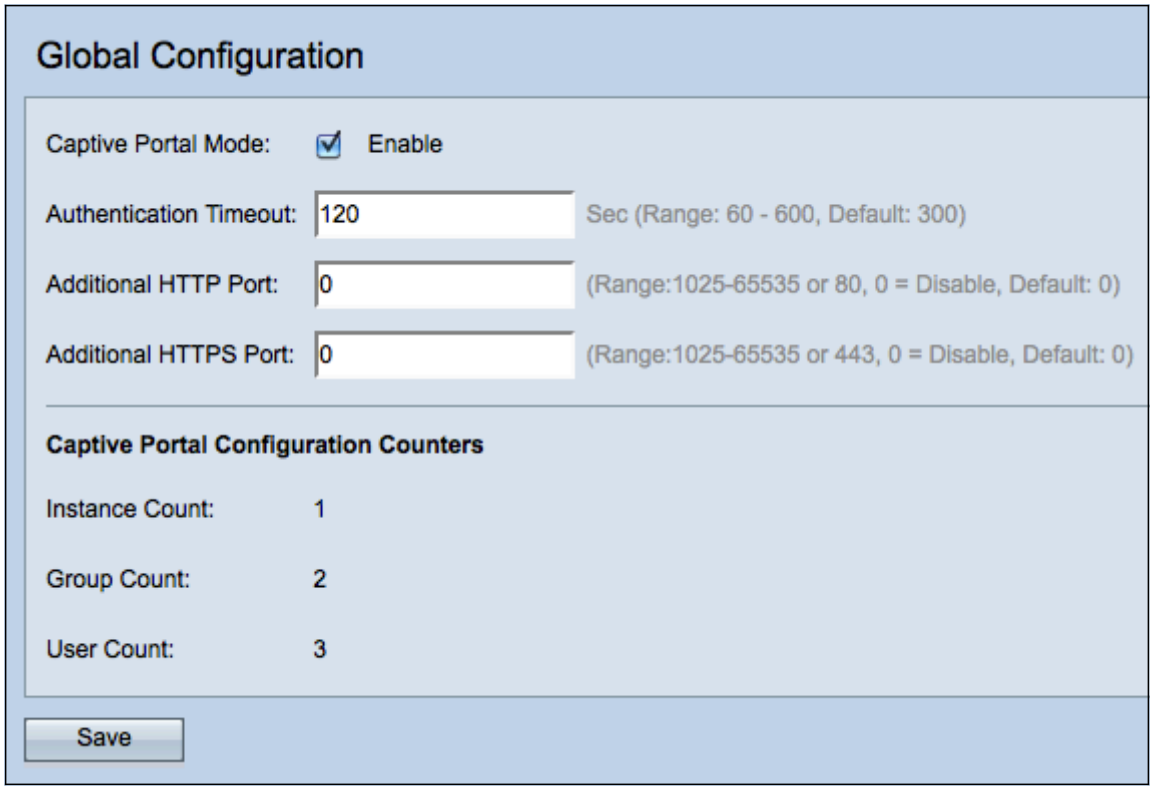
Softwareversion

·v1.0.4.2

Captive Portal für Gastbenutzer erstellen

Globale Konfiguration aktivieren

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, um **Captive Portal > Global Configuration** auszuwählen. Die Seite *Globale* Konfiguration wird geöffnet:



Schritt 2: Aktivieren Sie das Kontrollkästchen **Aktivieren** im Feld *Captive Portal Mode (Captive Portal Mode*), um das Captive Portal (CP) für den WAP zu aktivieren.

Schritt 3: Geben Sie die Anzahl der Sekunden ein, die der Benutzer Authentifizierungsinformationen eingeben muss, bevor der WAP die Authentifizierungssitzung im Feld *Authentifizierungs-Timeout* schließt.

Schritt 4: (Optional) Wenn HTTP-Informationen zwischen dem WAP und dem Client verwendet werden sollen, um neben der Standardeinstellung einen anderen Port zu verwenden, 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 5: (Optional) Wenn HTTP-Informationen zwischen dem WAP und dem Client verwendet werden sollen, um neben der Standardeinstellung einen anderen Port zu verwenden, 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 Feld *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.

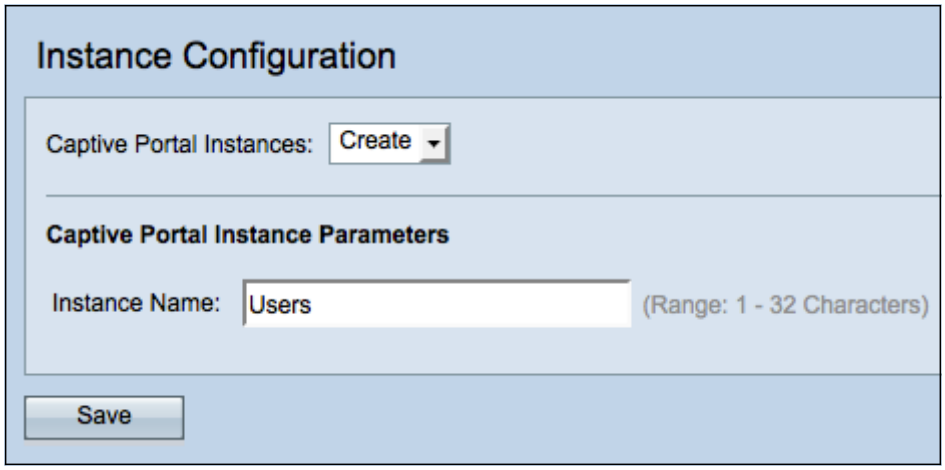
·Gruppenanzahl - Die Anzahl der CP-Gruppen, die auf dem WAP-Gerät konfiguriert wurden. Es können bis zu zwei Gruppen konfiguriert werden. Die Standardgruppe kann nicht gelöscht werden.

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

Schritt 6: Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Instanzkonfiguration

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Captive Portal > Instance Configuration aus**. Die Seite *Instanzkonfiguration* wird geöffnet:

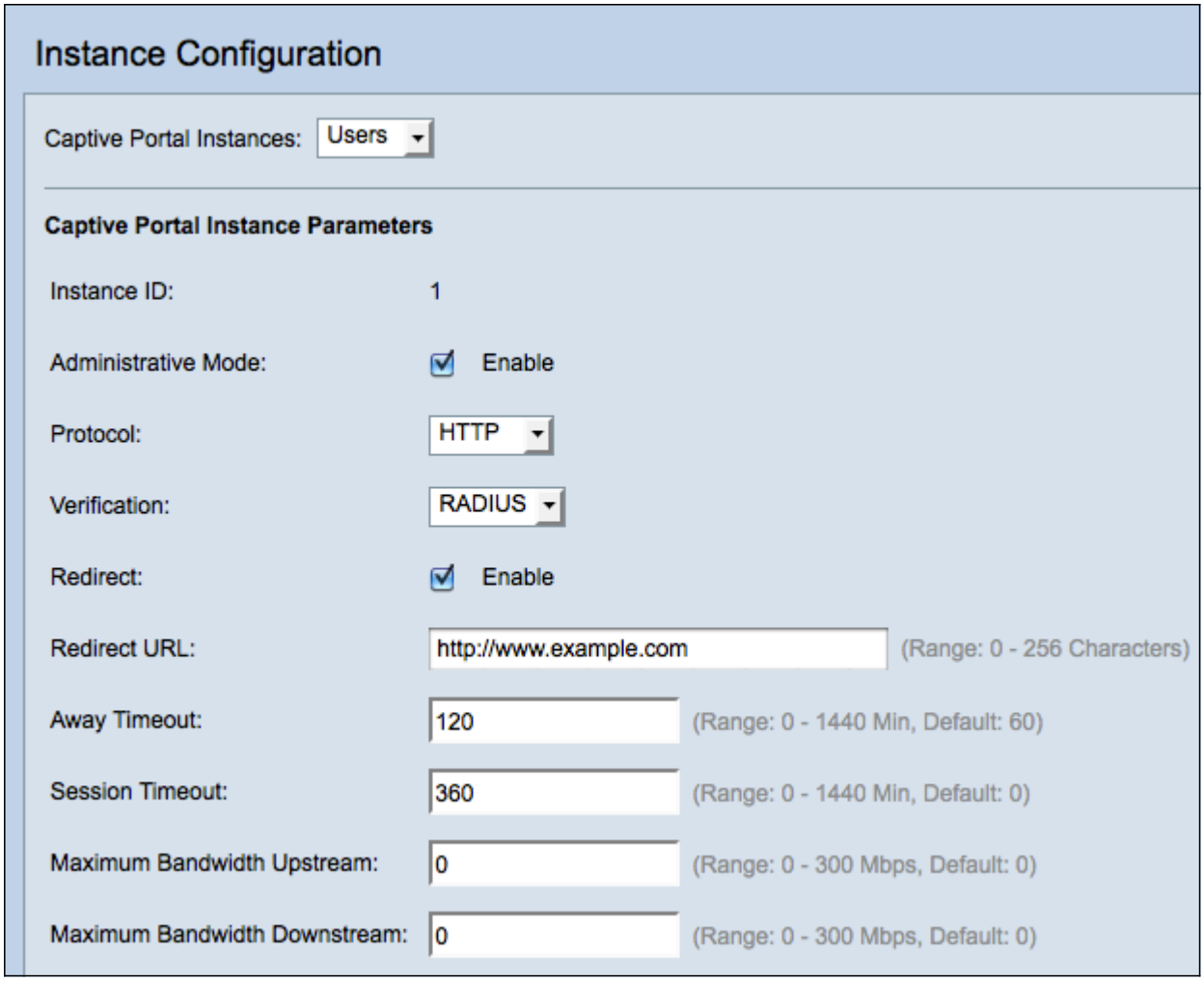


Schritt 2: Wählen Sie **Erstellen** aus der Dropdown-Liste *Captive Portal Instances* aus, um eine neue Instanz zu erstellen.

Schritt 3: Geben Sie im Feld *Instanzname* einen Namen für die Konfiguration ein.

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

Schritt 4: Klicken Sie auf **Speichern**, um die Instanz zu erstellen. Auf der Seite *Instanzkonfiguration* werden zusätzliche Informationen angezeigt. Die Instanz-ID ist ein nicht konfigurierbares Feld, das die Instanz-ID der aktuellen Instanz anzeigt.



Schritt 5: (Optional) Wählen Sie aus der Dropdown-Liste *Captive Portal Instances (*Instanzen *des Captive Portals)* eine andere Instanz aus, die konfiguriert werden soll.

Schritt 6: Aktivieren Sie das Kontrollkästchen **Aktivieren** im Feld *Verwaltungsmodus*, um die CP-Instanz zu aktivieren.

Schritt 7: 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.

Schritt 8: Wählen Sie aus der Dropdown-Liste *Überprüfung* eine Authentifizierungsmethode für den 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.

Schritt 9: (Optional) Wenn Sie Benutzer, die für eine konfigurierte URL verifiziert sind, umleiten möchten, aktivieren Sie das Kontrollkästchen **Aktivieren** im Feld *Umleiten*. Wenn diese Option deaktiviert ist, wird für verifizierte Benutzer eine länderspezifische Willkommensseite angezeigt.

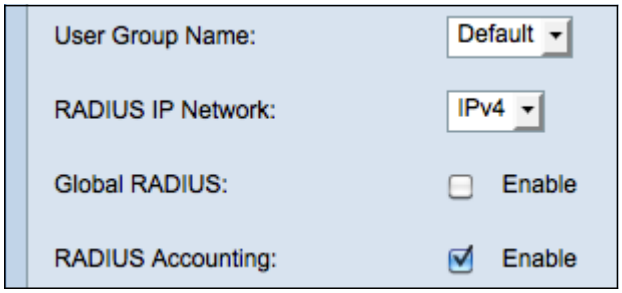
Schritt 10: Geben Sie die URL ein, an die Sie geprüfte Benutzer umleiten möchten. Dieser Schritt ist nur anwendbar, wenn Sie in Schritt 9 **Redirect** aktiviert haben.

Schritt 11: 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 der *Away Timeout*-Wert, muss er erneut autorisiert werden, bevor er den WAP verwenden kann.

Schritt 12: 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 13: 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 14: Geben Sie im Feld *Maximum Bandwidth Downstream* (Downstream-Bandbreite für maximale Bandbreite) die maximale Download-Geschwindigkeit (in Mbit/s) ein, die ein Client über das Captive Portal empfangen kann.



Schritt 15: 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 8 muss entweder Local (Lokal) oder RADIUS (RADIUS) sein, um eine Gruppe zuzuweisen.

Zeitgeber: Wenn Sie in Schritt 8 **Lokal** oder **Gast** als Verifizierung ausgewählt haben, fahren Sie mit Schritt 23 fort.

Schritt 16: Wählen Sie im Feld *RADIUS IP Network (RADIUS-IP-Netzwerk*) den Typ des Internetprotokolls aus, der vom RADIUS-Client verwendet wird.

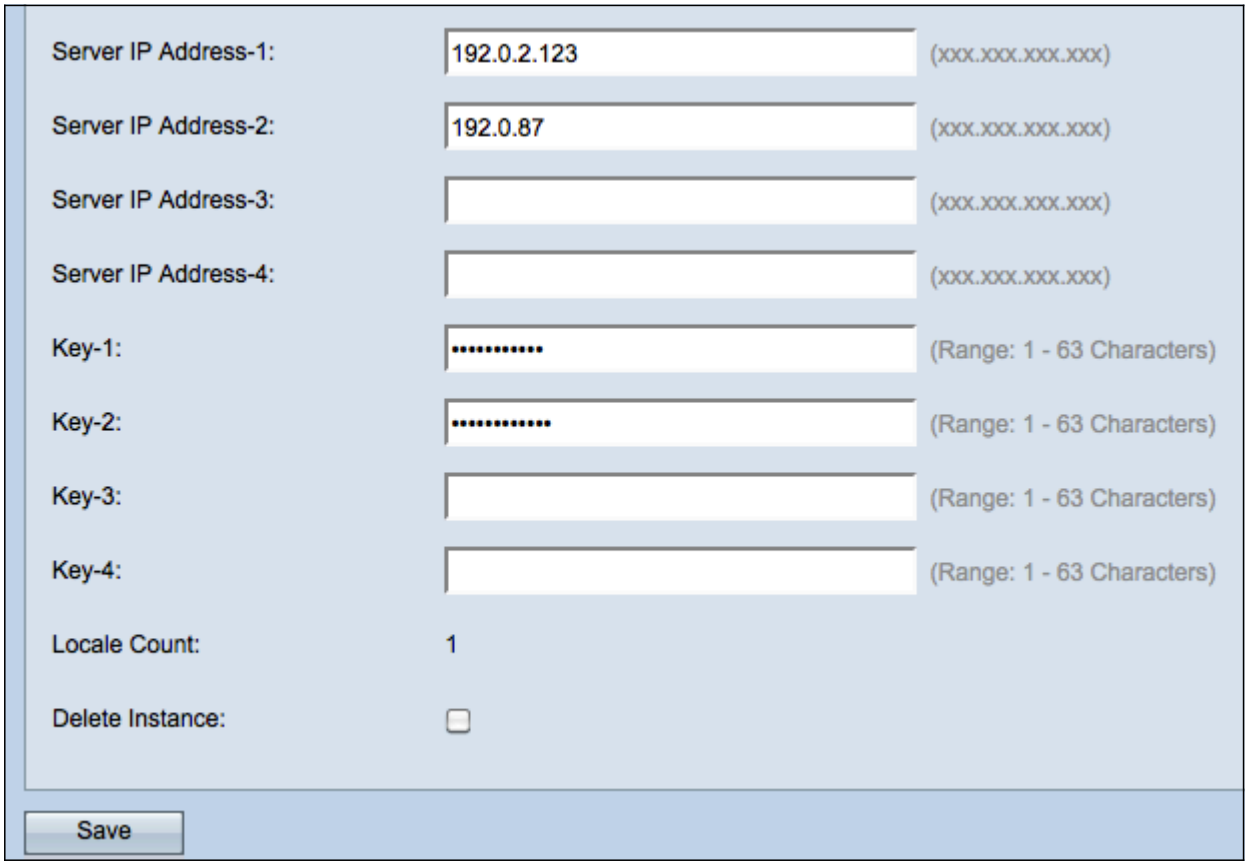
·IPv4 - Die Adresse des RADIUS-Clients hat das Format xxx.xxx.xxx.xxx (192.0.2.10).

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

Schritt 17: Aktivieren Sie im Feld *Global RADIUS* das **Kontrollkästchen Enable (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 23 fort, wenn Sie **Global RADIUS** aktivieren.

Schritt 18: Aktivieren Sie im Feld *RADIUS Accounting (RADIUS Accounting*) das **Kontrollkästchen Enable (Aktivieren)**, wenn Sie die Zeit- und Datenauslastung der Clients im WAP-Netzwerk nachverfolgen und messen möchten.



Hinweis: Wenn das Kontrollkästchen **Global RADIUS** in Schritt 17 aktiviert wurde, müssen keine zusätzlichen RADIUS-Server konfiguriert werden.

Schritt 19: 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 20: (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 21: 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 22: Geben Sie in den übrigen *Schlüsselfeldern (2-4)* den gemeinsamen geheimen Schlüssel ein, den das WAP-Gerät für die Authentifizierung bei den entsprechenden Backup-Radius-Servern verwendet.

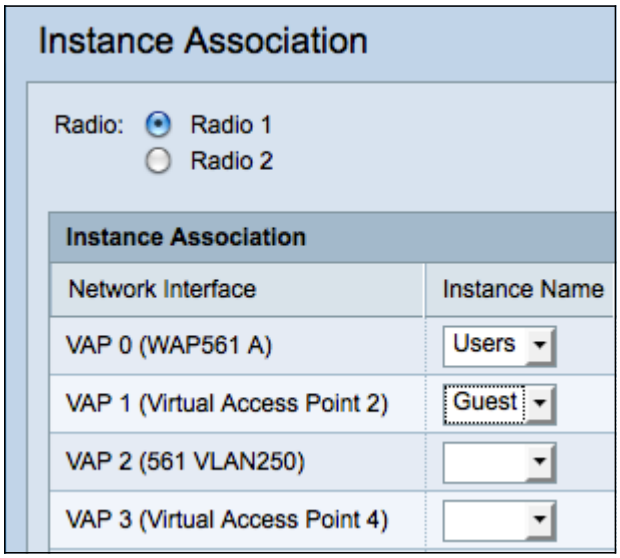
Hinweis:*Locale Count* ist ein nicht konfigurierbares Feld, das die Anzahl der Gebietsschemas anzeigt, die dieser Instanz zugeordnet sind.

Schritt 23: (Optional) Aktivieren Sie das Kontrollkästchen **Instanz löschen**, um die aktuelle Instanz zu löschen.

Schritt 24 Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Zuordnen der Instanz zu VAP

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Captive Portal > Instance Association (Captive Portal > Instanzzuordnung)**. Die Seite *Instanzzuordnung* wird geöffnet:



Schritt 2: Klicken Sie auf das Optionsfeld des Radios, dem Sie eine Instanz im Feld *Radio (Funkübertragung)* zuordnen möchten.

Hinweis: Schritt 2 gilt nur für den WAP561, da der WAP551 nur über eine Funkeinheit verfügt.

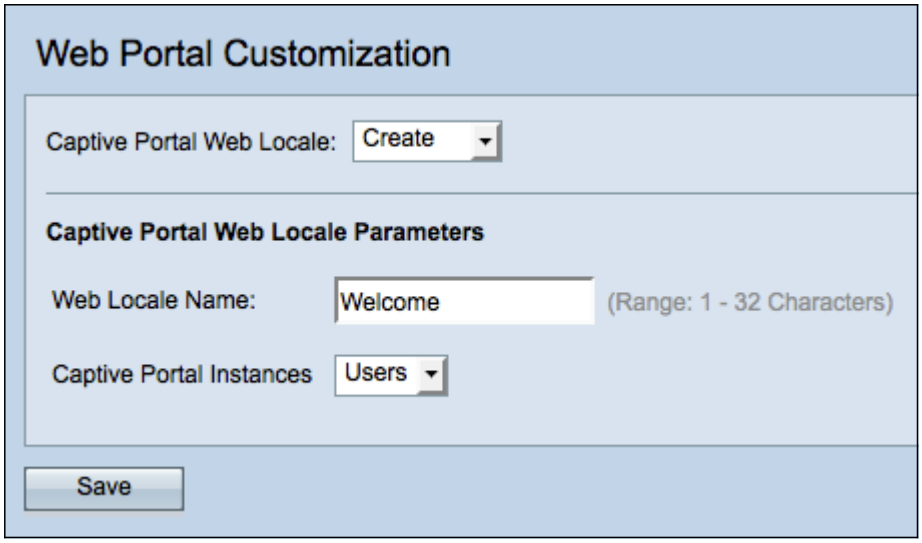
Schritt 3: Wählen Sie aus der Dropdown-Liste *Instanzname* eine Instanzkonfiguration aus, um eine Verknüpfung mit dem angegebenen VAP herzustellen.

Schritt 4: Klicken Sie auf **Speichern**, um die Änderungen zu 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 *Web Portal Customization* können Sie ein Gebietsschema anpassen und einer Captive Portal-Instanz zuweisen.

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Captive Portal > Web Portal Customization aus**. Die Seite *"Webportal-Anpassung"* wird geöffnet:

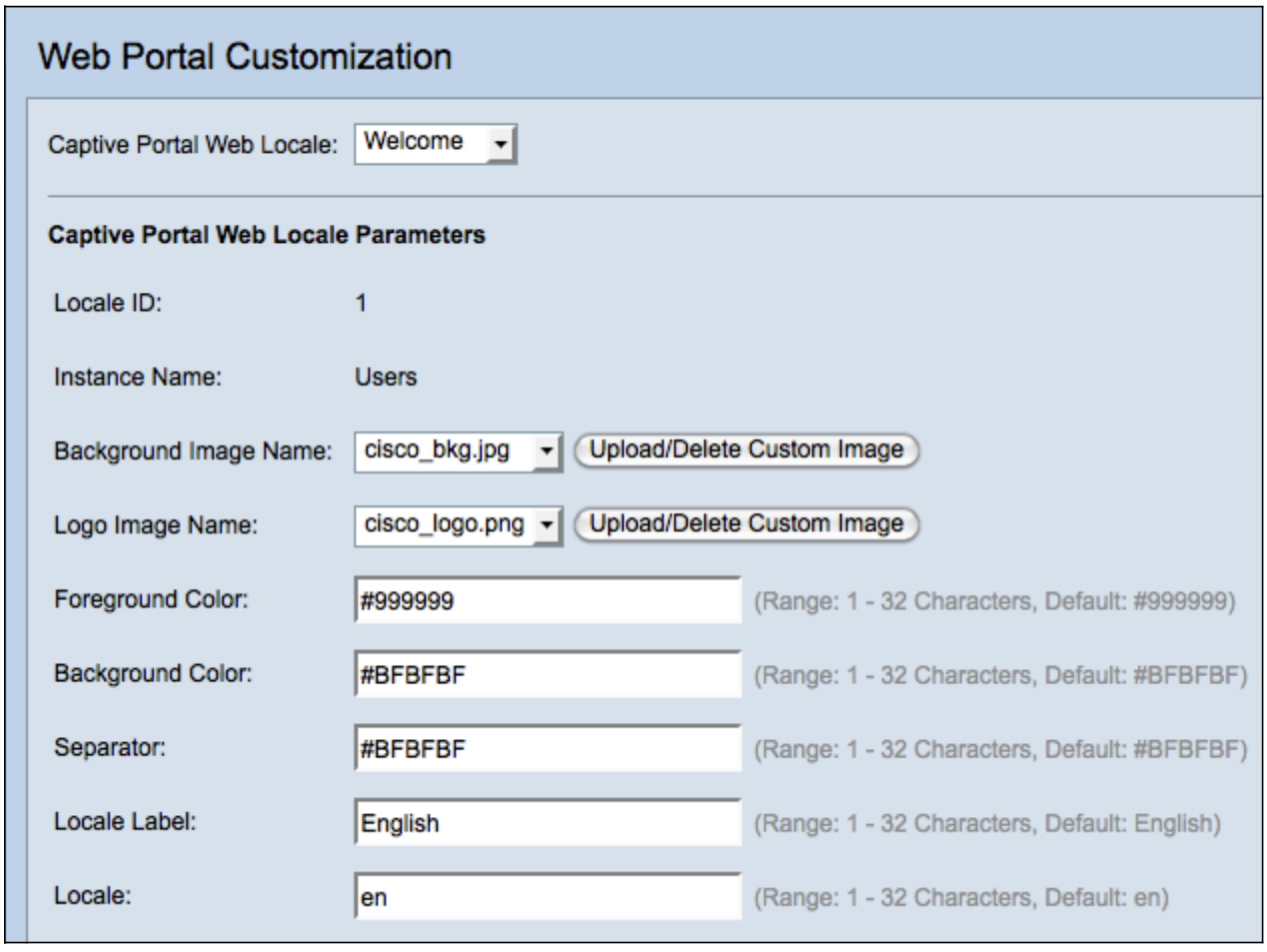


Schritt 2: Wählen Sie **Erstellen** aus der *Captive Portal Web Locale*-Dropdown-Liste aus, um ein neues Gebietsschema zu erstellen.

Schritt 3: Geben Sie den Namen des Gebietsschemas in das Feld *Web Locale Name* ein.

Schritt 4: Wählen Sie aus der Dropdown-Liste *Captive Portal Instances* 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 5: Klicken Sie auf **Speichern**, um ein neues Gebietsschema zu erstellen. Auf der Seite *Web Portal Customization* werden zusätzliche Informationen angezeigt.



Hinweis: Die Gebietsschemas-ID ist ein nicht konfigurierbares Feld, das die ID-Nummer des

aktuellen Gebietsschemas anzeigt.

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

Schritt 6: Wählen Sie aus der Dropdown-Liste *Background Image Name (Hintergrundbildname*) ein Bild für die Anzeige im Hintergrund für das Gebietsschema aus. Klicken Sie auf **Benutzerdefiniertes Bild hochladen/löschen**, um ein eigenes Bild hinzuzufügen. Weitere Informationen erhalten Sie im Abschnitt *Benutzerdefiniertes Bild hochladen/löschen*.

Schritt 7: Wählen Sie aus der Dropdown-Liste *Logo Image Name (Logo-Abbildname*) ein Bild, das in der oberen linken Ecke angezeigt werden soll.

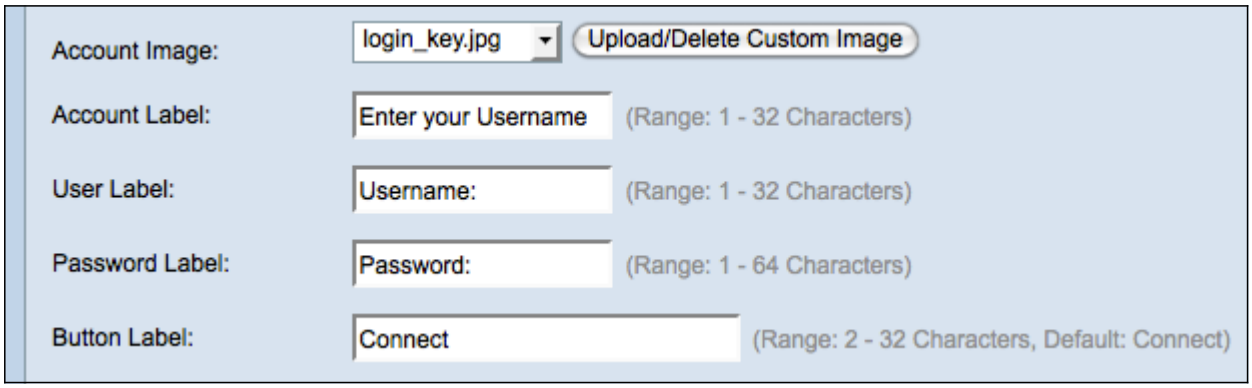
Schritt 8: Geben Sie im Feld *Vordergrundfarbe* den sechsstelligen HTML-Code für die Vordergrundfarbe des Gebietsschemas ein.

Schritt 9: Geben Sie im Feld *Hintergrundfarbe* den sechsstelligen HTML-Code für die Hintergrundfarbe des Gebietsschemas ein.

Schritt 10: Geben Sie im Feld *Trennzeichen* den sechsstelligen HTML-Code für die Farbe der horizontalen Zeile ein, die die Seitenkopfzeile vom Seitentext trennt.

Schritt 11: 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 12: Geben Sie im Feld *Gebietsschema* eine Abkürzung für das Gebietsschema ein.



Schritt 13: Wählen Sie aus der Dropdown-Liste *Account Image* (Kontobild) ein Bild aus, das über dem Anmeldefeld angezeigt werden soll.

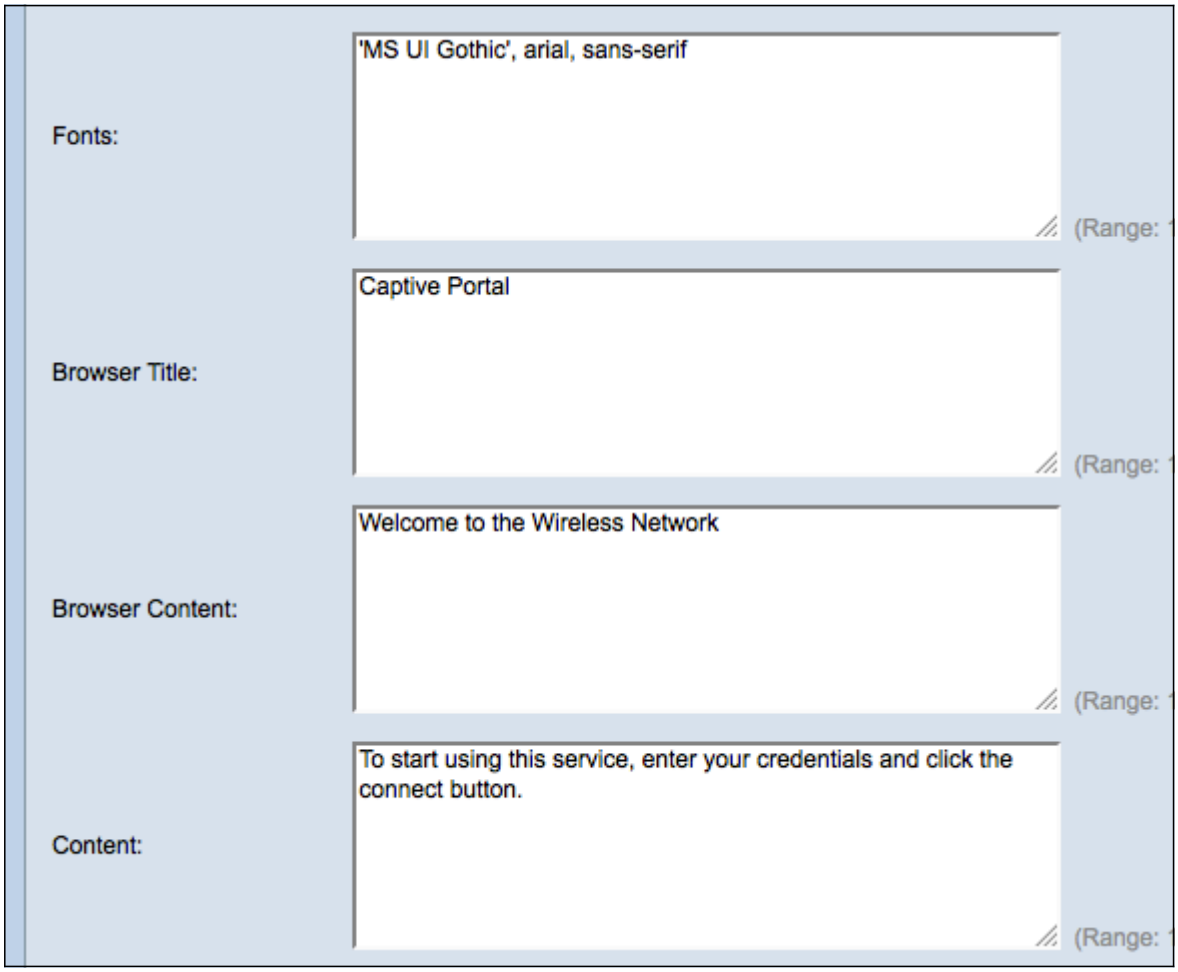
Schritt 14: Geben Sie im Feld *Kontonamen* die Anweisungen ein, die den Benutzer auffordern, seinen Benutzernamen einzugeben.

Schritt 15: Geben Sie im Textfeld *User Label* (Benutzerbezeichnung) das Label für das Textfeld User Name (Benutzername) ein.

Schritt 16: Geben Sie im Feld *Password Label (Kennwortbezeichnung)* die Bezeichnung für das Kennworttextfeld ein.

Schritt 17: 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 einzureichen.

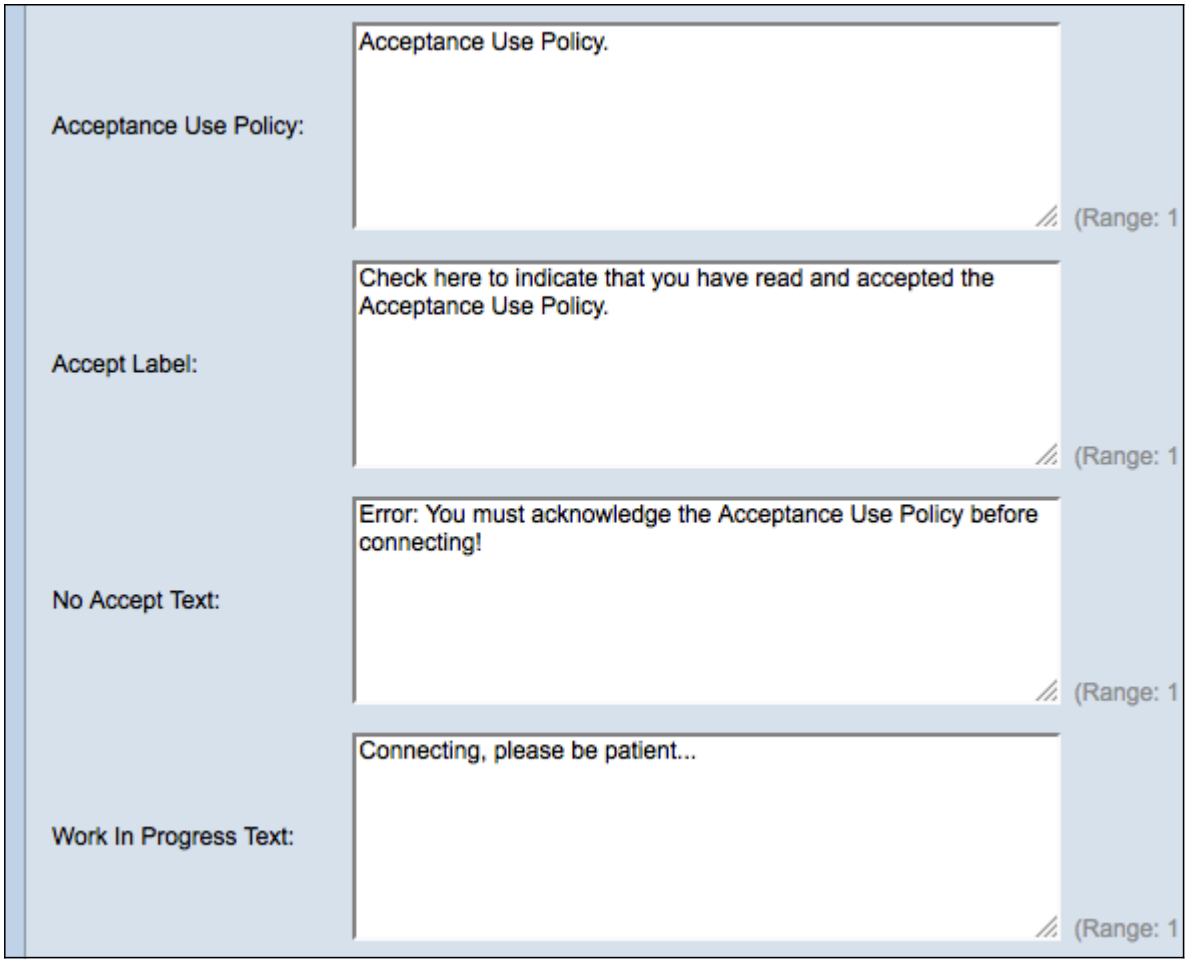


Schritt 18: Geben Sie im Feld *Schriftarten* den für das Gebietsschema verwendeten Schriftartnamen ein. Sie können mehrere Schriftarten eingeben, die durch ein Komma getrennt sind. Wenn der erste Schriftstil vom Client-Gerät nicht gefunden wird, wird die nächste Schriftart verwendet. Wenn ein Schriftartname mehrere Wörter durch Leerzeichen voneinander getrennt hat, können Sie einen einzelnen Anführungszeichen um den Schriftnamen herum verwenden.

Schritt 19: Geben Sie im Feld *Browser Title* (Browsertitel) den Text ein, den Sie in der Titelleiste des Browsers anzeigen möchten.

Schritt 20: Geben Sie im Feld *Browserinhalt* den Text ein, den Sie in der Seitenüberschrift anzeigen möchten.

Schritt 21: Geben Sie im *Content*-Feld den Text ein, der den Benutzer anweist, zu handeln. Dieses Feld wird unter den Textfeldern Benutzername und Kennwort angezeigt.

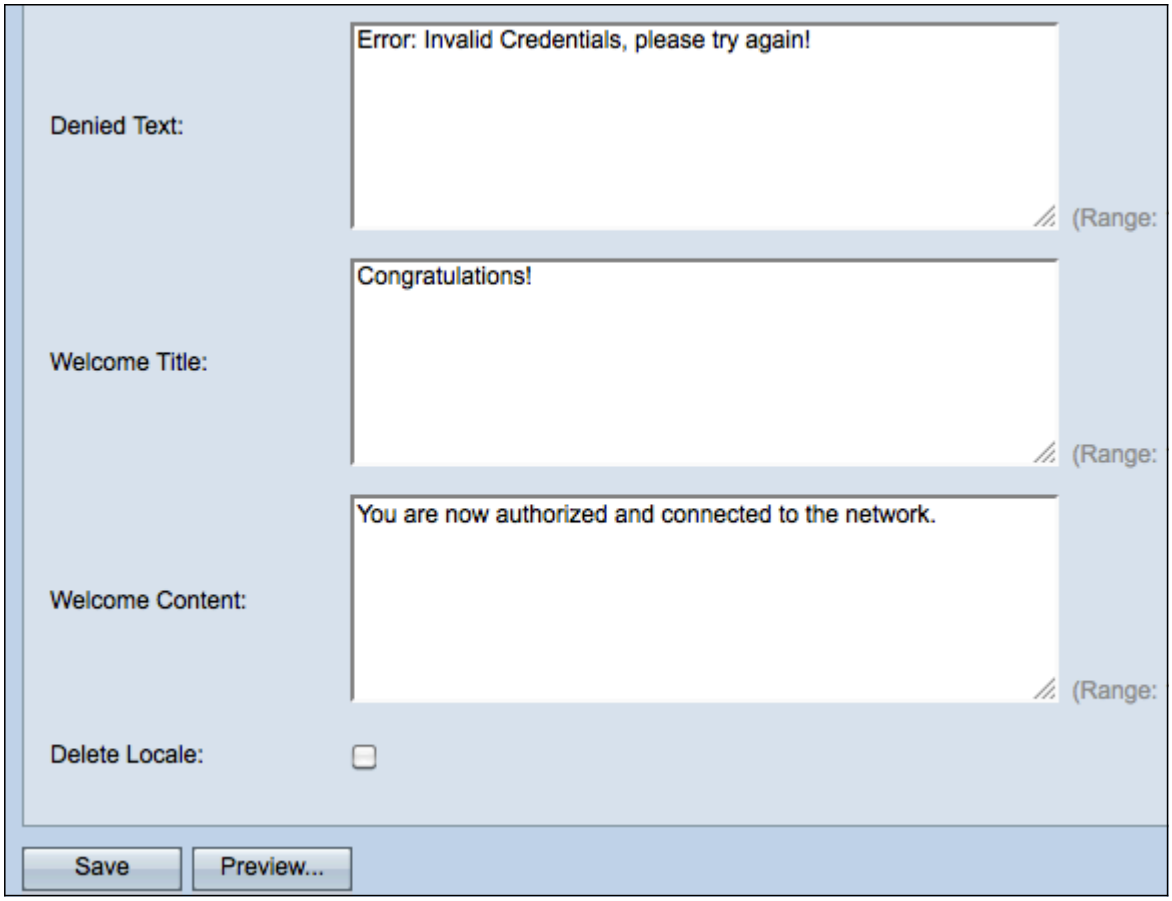


Schritt 22: Geben Sie in der *Acceptance Use Policy (Richtlinie zur Akzeptanznutzung*) die Bedingungen ein, denen Benutzer zustimmen müssen, wenn sie auf den WAP zugreifen möchten.

Schritt 23: Geben Sie im Feld *Accept Label (Label akzeptieren*) den Text ein, der Benutzer anweist, zu überprüfen, ob sie die Richtlinie zur Akzeptanznutzung gelesen und akzeptiert haben.

Schritt 24: Geben Sie im Feld *No Accept Test* (Test ohne Akzeptanz) den Text ein, der einen Benutzer warnt, wenn er Anmeldeinformationen einreicht, aber die Richtlinie zur Akzeptanznutzung nicht akzeptiert.

Schritt 25: Geben Sie im Feld *Text in Bearbeitung* den Text ein, der angezeigt wird, während der WAP die angegebenen Anmeldeinformationen überprüft.



Schritt 26: Geben Sie im Feld *Denied Text* (Text *verweigern*) den Text ein, der angezeigt wird, wenn die Authentifizierung eines Benutzers fehlschlägt.

Schritt 27: Geben Sie im Feld *Welcome Title* (Willkommenstitel) den Titeltext ein, der angezeigt wird, wenn ein Client erfolgreich authentifiziert wurde.

Schritt 28: Geben Sie im Feld *Welcome Content* (Willkommensinhalte) den Text ein, der einem Client angezeigt wird, der mit dem Netzwerk verbunden ist.

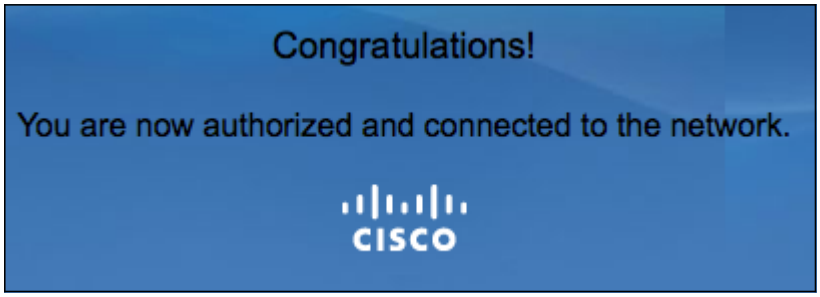
Schritt 29: (Optional) Aktivieren Sie das Kontrollkästchen **Gebietsschema löschen**, um das Gebietsschema zu löschen.

Schritt 30: Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Schritt 31: (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:

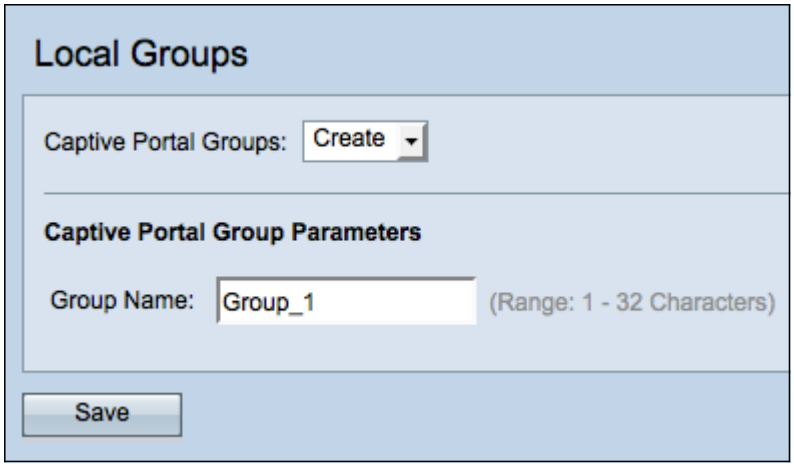
Hinweis: Wenn das Captive Portal erfolgreich abgeschlossen wurde, sollte ein Fenster angezeigt werden, das dem folgenden ähnelt:



Lokale Gruppe erstellen

Hinweis: 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 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Captive Portal > Local Groups (Captive Portal > Lokale Gruppen)**. Die Seite *Lokale Gruppen* wird geöffnet:



Schritt 2: Wählen Sie **Erstellen** aus der Dropdown-Liste *Captive Portal Groups (Captive Portal-Gruppen*) aus.

Schritt 3: Geben Sie den Namen der lokalen Gruppe im Feld *Gruppenname ein*.

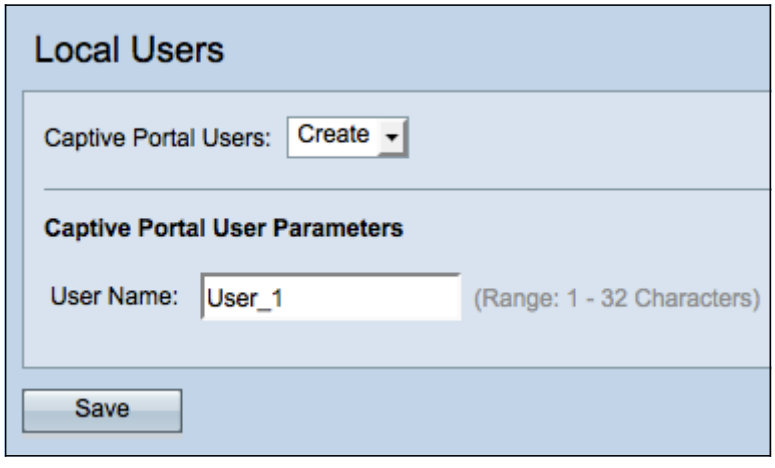
Schritt 4: Klicken Sie auf **Speichern**, um die Gruppe zu speichern.

Hinweis: Sie weisen einer Instanz in Schritt 15 des Abschnitts *Instanzkonfiguration* eine lokale Gruppe zu.

Lokalen Benutzer erstellen

Hinweis: 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.

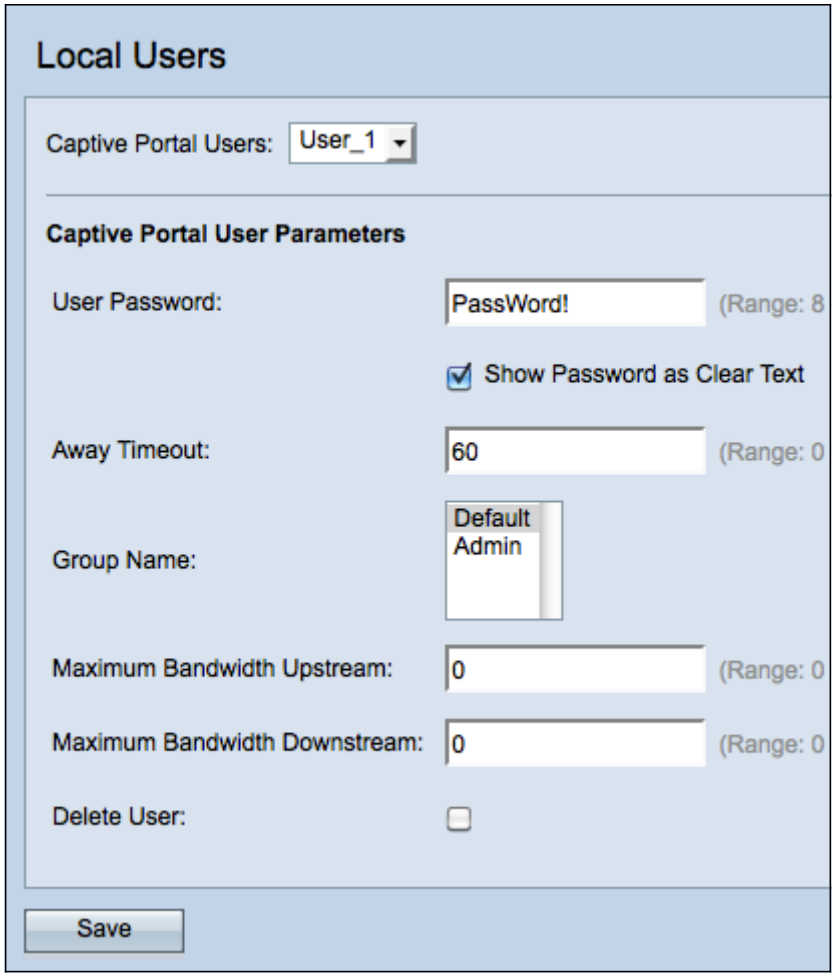
Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Captive Portal > Local Users aus**. Die Seite *Lokale Benutzer* wird geöffnet:



Schritt 2: Wählen Sie **Erstellen** aus der Dropdown-Liste *Captive Portal Users aus*.

Schritt 3: Geben Sie im Feld *Benutzername* den Benutzernamen ein, den Sie hinzufügen möchten.

Schritt 4: Klicken Sie auf **Speichern**, um den neuen Benutzer zu erstellen. Auf der Seite *Lokale Benutzer* werden zusätzliche Informationen angezeigt.



Schritt 5: Geben Sie im Feld *User Password* (Benutzerkennwort) das dem Benutzer zugeordnete Kennwort ein.

Schritt 6: (Optional) Um das Kennwort im Klartext anzeigen zu lassen, aktivieren Sie das Kontrollkästchen **Kennwort als Klartext anzeigen**. Wenn das Kontrollkästchen nicht aktiviert ist, wird das Kennwort maskiert.

Schritt 7: Geben Sie im Feld *Away Timeout* (Abwesenheitszeit) die Zeitdauer 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 8: Klicken Sie im Feld *Gruppenname* auf die lokale Gruppe, der der Benutzer beitreten soll.

Schritt 9: 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.

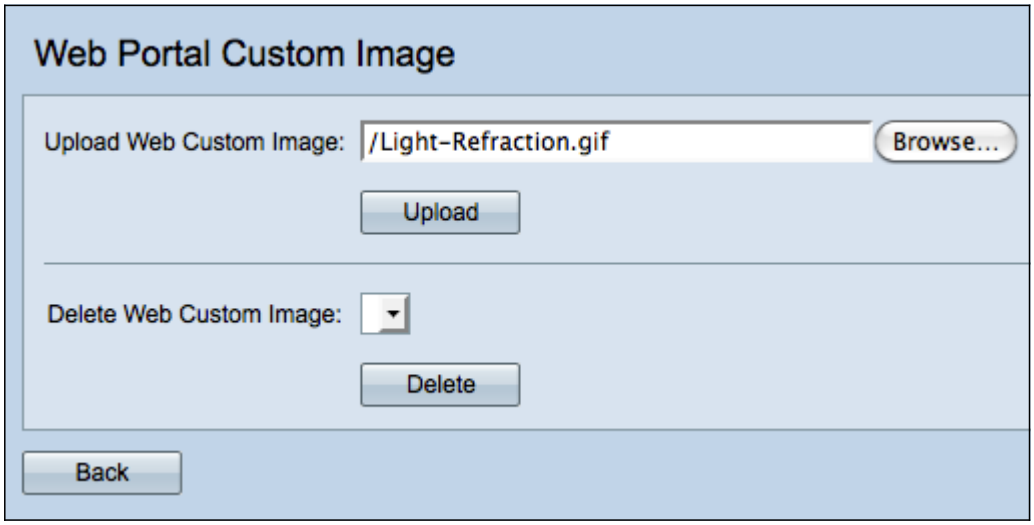
Schritt 10: Geben Sie im Feld *Maximum Bandwidth Downstream* (Downstream-Bandbreite für maximale Bandbreite) die maximale Downloadgeschwindigkeit in Mbit/s ein, die ein Client über das Captive Portal empfangen kann.

Schritt 11: (Optional) Um einen lokalen Benutzer zu löschen, aktivieren Sie das Kontrollkästchen **Benutzer löschen**.

Schritt 12: Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Benutzerdefiniertes Bild hochladen/löschen

Wenn Sie im Feld *Hintergrundbildname, Logo-Abbildname* oder *Kontobild* **auf die** Schaltfläche **Benutzerdefiniertes Bild hochladen/löschen** geklickt haben, wird die Seite für *Benutzerdefinierte Webportal* geöffnet:



Schritt 1: Klicken Sie im Feld *Benutzerdefiniertes Web-Image hochladen auf* **Durchsuchen**, um in Ihrem Verzeichnis nach einem GIF- oder JPG-Bild zu suchen. Bilder dürfen maximal 5 Kilobyte groß sein.

Schritt 2: Klicken Sie auf **Hochladen**, um Ihr Bild hochzuladen.

Schritt 3: (Optional) Um ein Bild zu löschen, wählen Sie ein Bild aus der Dropdown-Liste *Benutzerdefiniertes Webbild löschen*, und klicken Sie auf **Löschen**.

Schritt 4: Klicken Sie auf **Zurück**, um zur *Webportal-*Anpassungsseite zurückzukehren.

Sehen Sie sich ein Video zu diesem Artikel an..

Klicken Sie hier, um weitere Tech Talks von Cisco anzuzeigen.