Externe Web-Authentifizierung mit WLCs konfigurieren

Inhalt

Einleitung

In diesem Dokument wird die Verwendung eines externen Webservers zum Einrichten eines Wireless LAN-Controllers (WLC) für die Webauthentifizierung erläutert.

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass die folgenden Anforderungen erfüllt sind, bevor Sie diese Konfiguration ausprobieren:

- Grundkenntnisse der Konfiguration von Lightweight Access Points (LAPs) und Cisco WLCs
- Grundkenntnisse von LWAPP (Lightweight Access Point Protocol) und CAPWAP (Control and Provisioning of Wireless Access Points)

- Kenntnisse zum Einrichten und Konfigurieren eines externen Webservers
- Kenntnisse zum Einrichten und Konfigurieren von DHCP- und DNS-Servern

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco 4400 WLC mit Firmware-Version 7.0.116.0
- Cisco Serie 1131AG - LAP
- Cisco 802.11a/b/g Wireless Client Adapter für Firmware-Version 3.6
- Externer Webserver, der die Anmeldeseite für die Webauthentifizierung hostet
- DNS- und DHCP-Server für Adressauflösung und IP-Adresszuweisung an Wireless-Clients

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

Hintergrundinformationen

Die Webauthentifizierung ist eine Sicherheitsfunktion auf Layer 3, die den Controller veranlasst, IP-Datenverkehr (mit Ausnahme von DHCP- und DNS-bezogenen Paketen) von einem bestimmten Client erst zuzulassen, wenn dieser einen gültigen Benutzernamen und ein gültiges Kennwort eingegeben hat. Web-Authentifizierung ist eine einfache Authentifizierungsmethode, ohne dass eine Komponente oder ein Client-Dienstprogramm erforderlich ist.

Die Webauthentifizierung kann wie folgt durchgeführt werden:

- Standard-Anmeldefenster des WLC
- Geänderte Version des Standard-Anmeldefensters auf dem WLC
- Ein benutzerdefiniertes Anmeldefenster, das Sie auf einem externen Webserver konfigurieren (externe Webauthentifizierung).
- Ein benutzerdefiniertes Anmeldefenster, das Sie auf den Controller herunterladen

Dieses Dokument enthält ein Konfigurationsbeispiel für die Konfiguration des WLC zur Verwendung eines Anmeldeskripts von einem externen Webserver.

Externer Webauthentifizierungsprozess

Bei der externen Webauthentifizierung wird die für die Webauthentifizierung verwendete Anmeldeseite auf einem externen Webserver gespeichert. Dies ist die Abfolge von Ereignissen, wenn ein Wireless-Client versucht, auf ein WLAN-Netzwerk zuzugreifen, in dem die externe Web-Authentifizierung aktiviert ist:

1. Der Client (Endbenutzer) stellt eine Verbindung mit dem WLAN her, öffnet einen

Webbrowser und gibt eine URL ein, z. B. www.cisco.com.
2. Der Client sendet eine DNS-Anfrage an einen DNS-Server, um www.cisco.com in eine IP-Adresse aufzulösen.
3. Der WLC leitet die Anfrage an den DNS-Server weiter, der wiederum www.cisco.com in IP-Adresse auflöst und eine DNS-Antwort sendet. Der Controller leitet die Antwort an den Client weiter.
4. Der Client versucht, eine TCP-Verbindung mit der IP-Adresse www.cisco.com herzustellen, indem er das TCP-SYN-Paket an die IP-Adresse www.cisco.com sendet.
5. Der WLC verfügt über Regeln, die für den Client konfiguriert sind, und kann daher als Proxy für www.cisco.com fungieren. Es sendet ein TCP-SYN-ACK-Paket zurück an den Client, dessen Quelle die IP-Adresse www.cisco.com ist. Der Client sendet ein TCP-ACK-Paket zurück, um den Drei-Wege-TCP-Handshake abzuschließen, und die TCP-Verbindung ist vollständig hergestellt.
6. Der Client sendet ein HTTP GET-Paket an www.google.com. Der WLC fängt dieses Paket ab und sendet es zur Weiterleitungsbehandlung. Das HTTP-Anwendungs-Gateway bereitet einen HTML-Text vor und sendet diesen als Antwort auf die vom Client angeforderte HTTP GET-Anforderung zurück. Dieser HTML-Code veranlasst den Client, zur Standard-Webseite-URL des WLC zu wechseln, z. B. http://<Virtual-Server-IP>/login.html.
7. Der Client startet dann die HTTPS-Verbindung mit der Umleitungs-URL, die sie an 1.1.1.1 sendet. Dies ist die virtuelle IP-Adresse des Controllers. Der Client muss das Serverzertifikat validieren oder ignorieren, um den SSL-Tunnel zu öffnen.
8. Da die externe Webauthentifizierung aktiviert ist, leitet der WLC den Client an den externen Webserver um.
9. Die externe Webauthentifizierungs-Anmelde-URL wird mit Parametern wie "AP_Mac_Address", "client_url" (www.cisco.com) und "action_URL" angehängt, die der Client benötigt, um den Controller-Webserver zu kontaktieren.**Hinweis:** Action_URL teilt dem Webserver mit, dass Benutzername und Passwort auf dem Controller gespeichert sind. Die Anmeldeinformationen müssen an den Controller zurückgesendet werden, um authentifiziert zu werden.
10. Die externe Webserver-URL führt den Benutzer zu einer Anmeldeseite.
11. Auf der Anmeldeseite werden die Benutzeranmeldeinformationen eingegeben, und die Anforderung wird an die action_URL, z. B. http://1.1.1.1/login.html, des WLC-Webservers zurückgesendet.
12. Der WLC-Webserver sendet den Benutzernamen und das Kennwort zur Authentifizierung ein.
13. Der WLC initiiert die RADIUS-Serveranforderung oder verwendet die lokale Datenbank auf dem WLC und authentifiziert den Benutzer.
14. Wenn die Authentifizierung erfolgreich ist, leitet der WLC-Webserver den Benutzer entweder an die konfigurierte Umleitungs-URL oder an die URL weiter, mit der der Client begonnen hat, z. B. www.cisco.com.
15. Wenn die Authentifizierung fehlschlägt, leitet der WLC-Webserver den Benutzer zurück zur Anmelde-URL des Kunden.

Hinweis: Führen Sie den folgenden Befehl aus, um die externe Webauthentifizierung für die Verwendung anderer Ports als HTTP und HTTPS zu konfigurieren:

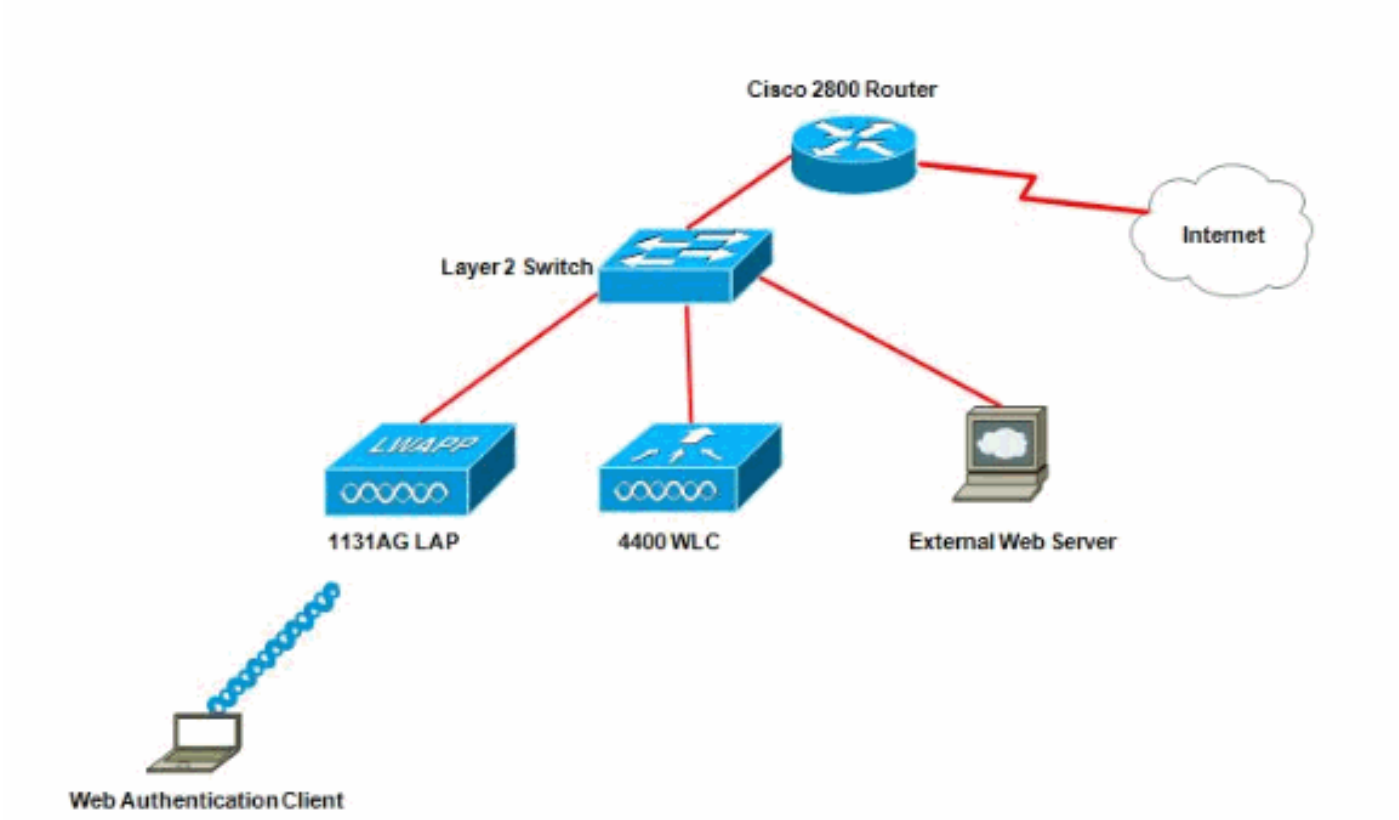
```
(Cisco Controller) >config network web-auth-port

<port>          Configures an additional port to be redirected for web authentication.
```

Netzwerkeinrichtung

Im Konfigurationsbeispiel wird diese Konfiguration verwendet. Beim WLC ist ein LAP registriert. Sie müssen einen WLAN-**Gast** für die Gastbenutzer konfigurieren und die Webauthentifizierung für die Benutzer aktivieren. Sie müssen außerdem sicherstellen, dass der Controller den Benutzer zur externen Webserver-URL umleitet (für die externe Webauthentifizierung). Der externe Webserver hostet die Web-Anmeldeseite, die für die Authentifizierung verwendet wird.

Die Benutzeranmeldeinformationen müssen mit der lokalen Datenbank auf dem Controller abgeglichen werden. Nach erfolgreicher Authentifizierung sollten die Benutzer Zugriff auf den WLAN-Gast erhalten. Der Controller und andere Geräte müssen für diese Einrichtung konfiguriert werden.

Hinweis: Sie können eine benutzerdefinierte Version des Anmeldeskripts verwenden, die für die Webauthentifizierung verwendet wird. Sie können ein Web-Authentifizierungs-Beispielskript von der Seite Cisco Software-Downloads herunterladen. Navigieren Sie für die Controller der Serie 4400 beispielsweise zu **Products > Wireless > Wireless LAN Controller > Standalone Controllers > Cisco Wireless LAN Controller der Serie 4400 > Cisco 4404 Wireless LAN Controller > Software on Chassis > Wireless LAN Controller Web Authentication Bundle-1.0.1,** und laden Sie die **webauth_bundle.zip-**Datei herunter.



Hinweis: Das benutzerdefinierte Web-Authentifizierungspaket darf maximal 30 Zeichen für Dateinamen enthalten. Stellen Sie sicher, dass keine Dateinamen im Paket mehr als 30 Zeichen enthalten.

Hinweis: In diesem Dokument wird davon ausgegangen, dass DHCP, DNS und externe Webserver konfiguriert sind. Weitere Informationen zur Konfiguration von DHCP, DNS und externen Webservern finden Sie in der entsprechenden Dokumentation des Drittanbieters.

Konfigurieren

Bevor Sie den WLC für die externe Webauthentifizierung konfigurieren, müssen Sie den WLC für den Basisbetrieb konfigurieren und die LAPs beim WLC registrieren. In diesem Dokument wird davon ausgegangen, dass der WLC für den Basisbetrieb konfiguriert ist und dass die LAPs beim WLC registriert sind. Wenn Sie ein neuer Benutzer sind, der versucht, den WLC für den Basisbetrieb mit den LAPs einzurichten, lesen Sie Lightweight AP (LAP) Registration to a Wireless LAN Controller (WLC).

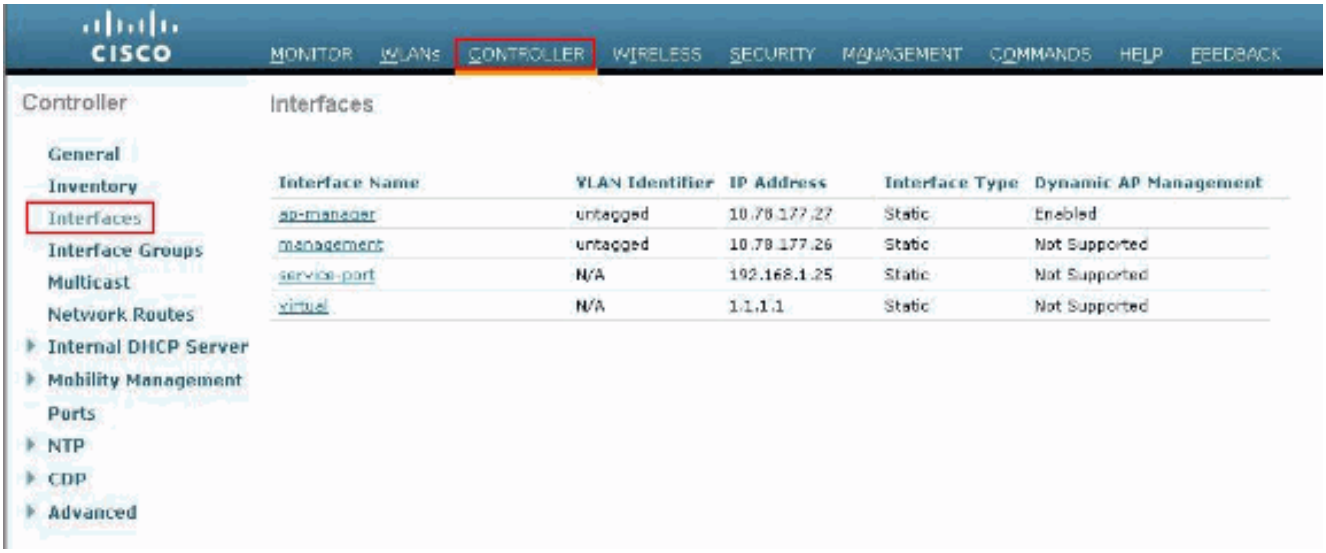
Gehen Sie wie folgt vor, um die LAPs und den WLC für diese Einrichtung zu konfigurieren:

1. Erstellen einer dynamischen Schnittstelle für Gastbenutzer
2. Erstellen einer Vorauthentifizierungs-ACL
3. Erstellen einer lokalen Datenbank auf dem WLC für Gastbenutzer
4. Konfigurieren des WLC für die externe Webauthentifizierung
5. WLAN für Gastbenutzer konfigurieren

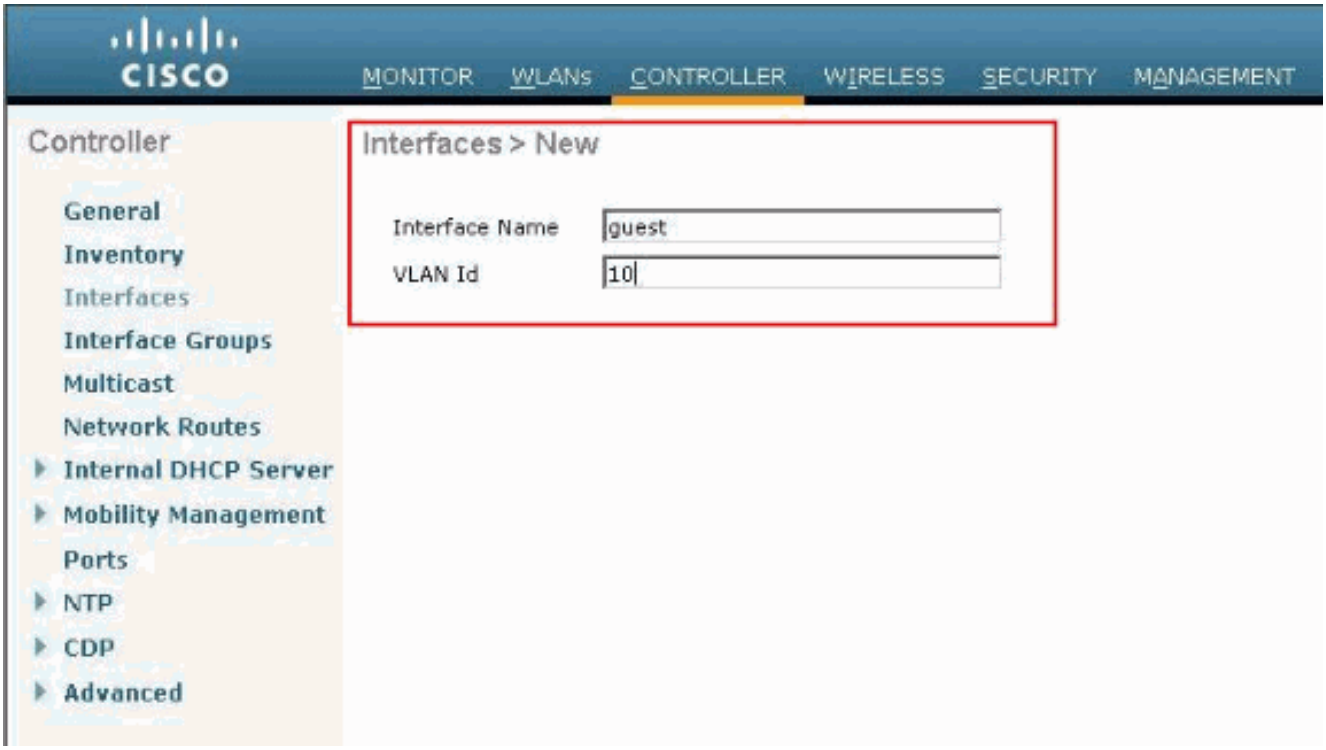
Erstellen einer dynamischen Schnittstelle für Gastbenutzer

Führen Sie die folgenden Schritte aus, um eine dynamische Schnittstelle für Gastbenutzer zu erstellen:

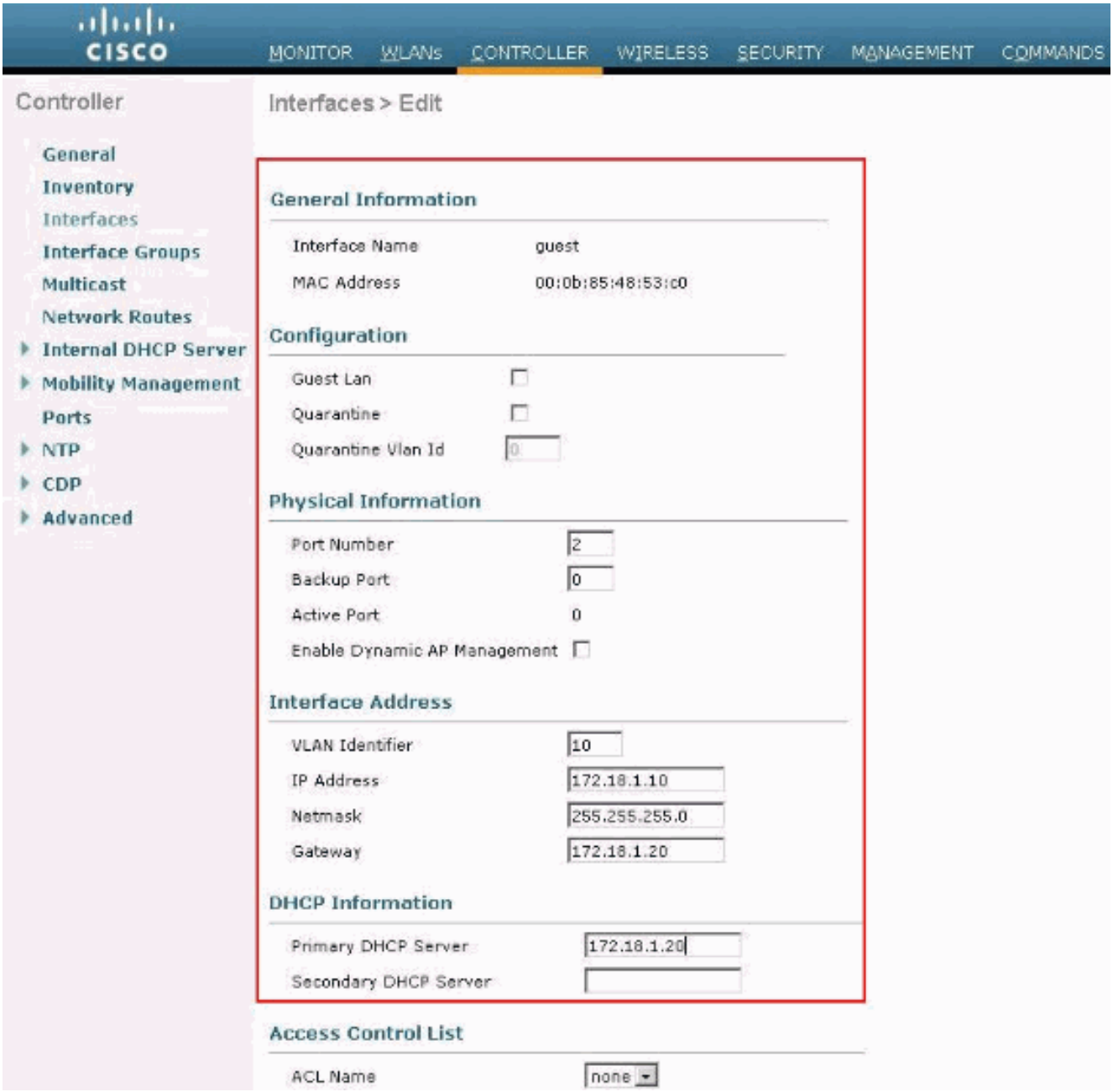
1. Wählen Sie in der WLC-GUI **Controller > Interfaces (Controller > Schnittstellen) aus**.Das Fenster Interfaces (Schnittstellen) wird angezeigt. In diesem Fenster werden die Schnittstellen aufgeführt, die auf dem Controller konfiguriert sind. Dies umfasst die Standardschnittstellen, d. h. die Management-Schnittstelle, die Schnittstelle "ap-manager", die virtuelle Schnittstelle und die Service-Port-Schnittstelle sowie die benutzerdefinierten dynamischen
   Schnittstellen.



2. Klicken Sie auf **Neu**, um eine neue dynamische Schnittstelle zu erstellen.
3. Geben Sie im Fenster **Schnittstellen > Neu** den Schnittstellennamen und die VLAN-ID ein. Klicken Sie dann auf **Anwenden**.In diesem Beispiel lautet der Name der dynamischen Schnittstelle **guest,** und die VLAN-ID lautet
   10.



4. Geben Sie im Fenster **Interfaces > Edit (Schnittstellen > Bearbeiten)** für die dynamische Schnittstelle die IP-Adresse, die Subnetzmaske und das Standard-Gateway ein. Weisen Sie ihn einem physischen Port am WLC zu, und geben Sie die IP-Adresse des DHCP-Servers ein. Klicken Sie anschließend auf
Apply.



Erstellen einer Vorauthentifizierungs-ACL

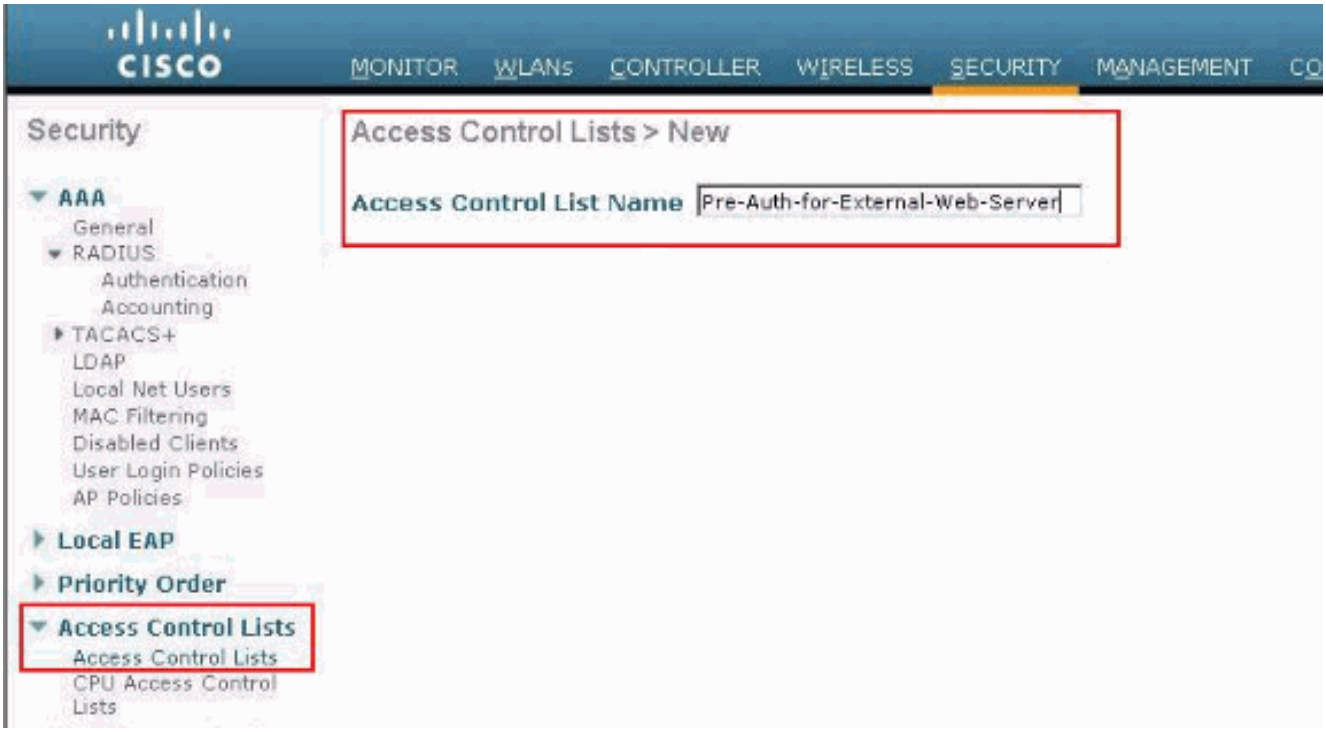
Wenn ein externer Webserver für die Webauthentifizierung verwendet wird, benötigen einige WLC-Plattformen eine Pre-Authentication-ACL für den externen Webserver (Cisco Controller der Serie 5500, Cisco Controller der Serie 2100, Cisco Controller der Serie 2000 und das Controller-Netzwerkmodul). Für die anderen WLC-Plattformen ist die ACL vor der Authentifizierung nicht obligatorisch.

Es ist jedoch empfehlenswert, bei Verwendung der externen Webauthentifizierung eine Vorauthentifizierungs-ACL für den externen Webserver zu konfigurieren.

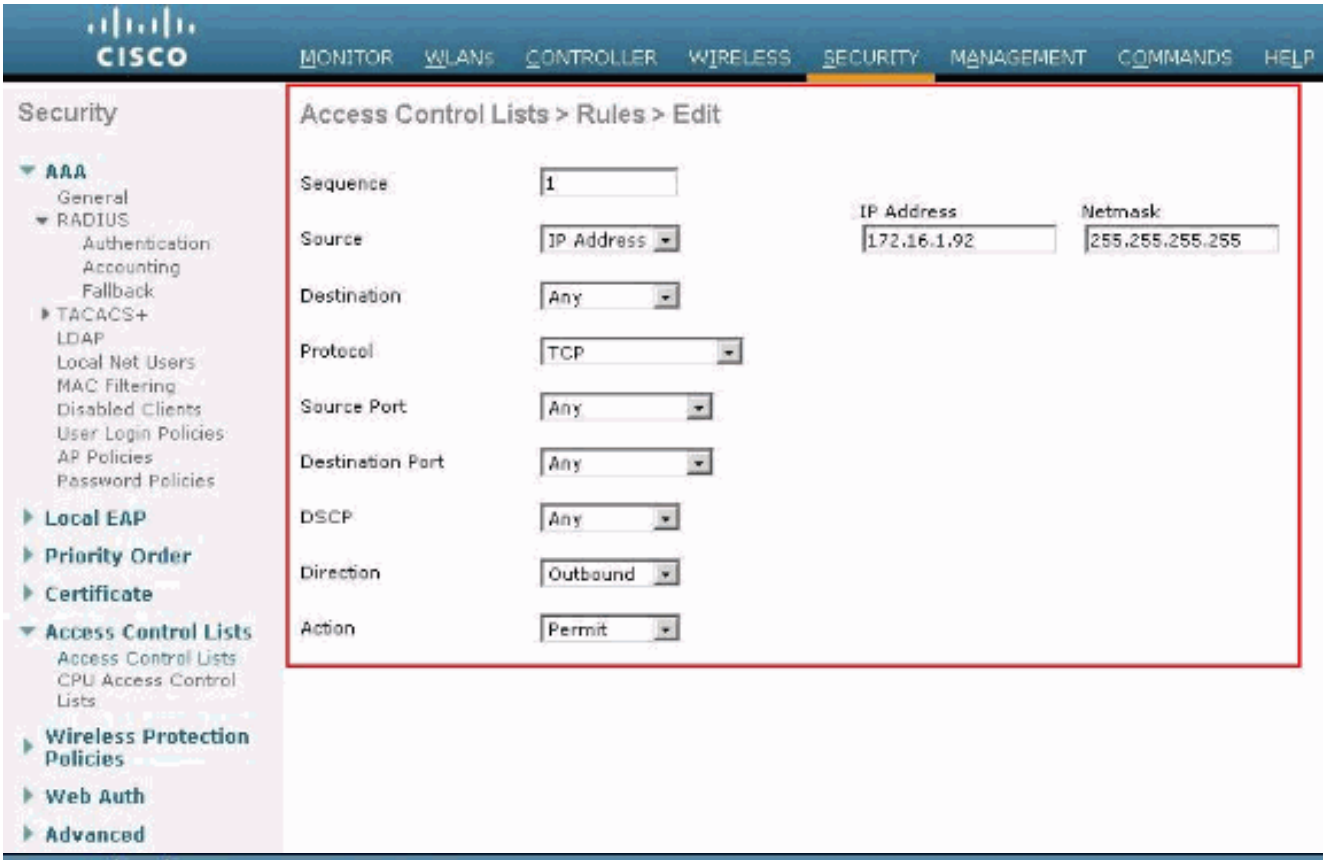
Gehen Sie wie folgt vor, um die Zugriffskontrollliste vor der Authentifizierung für das WLAN zu konfigurieren:

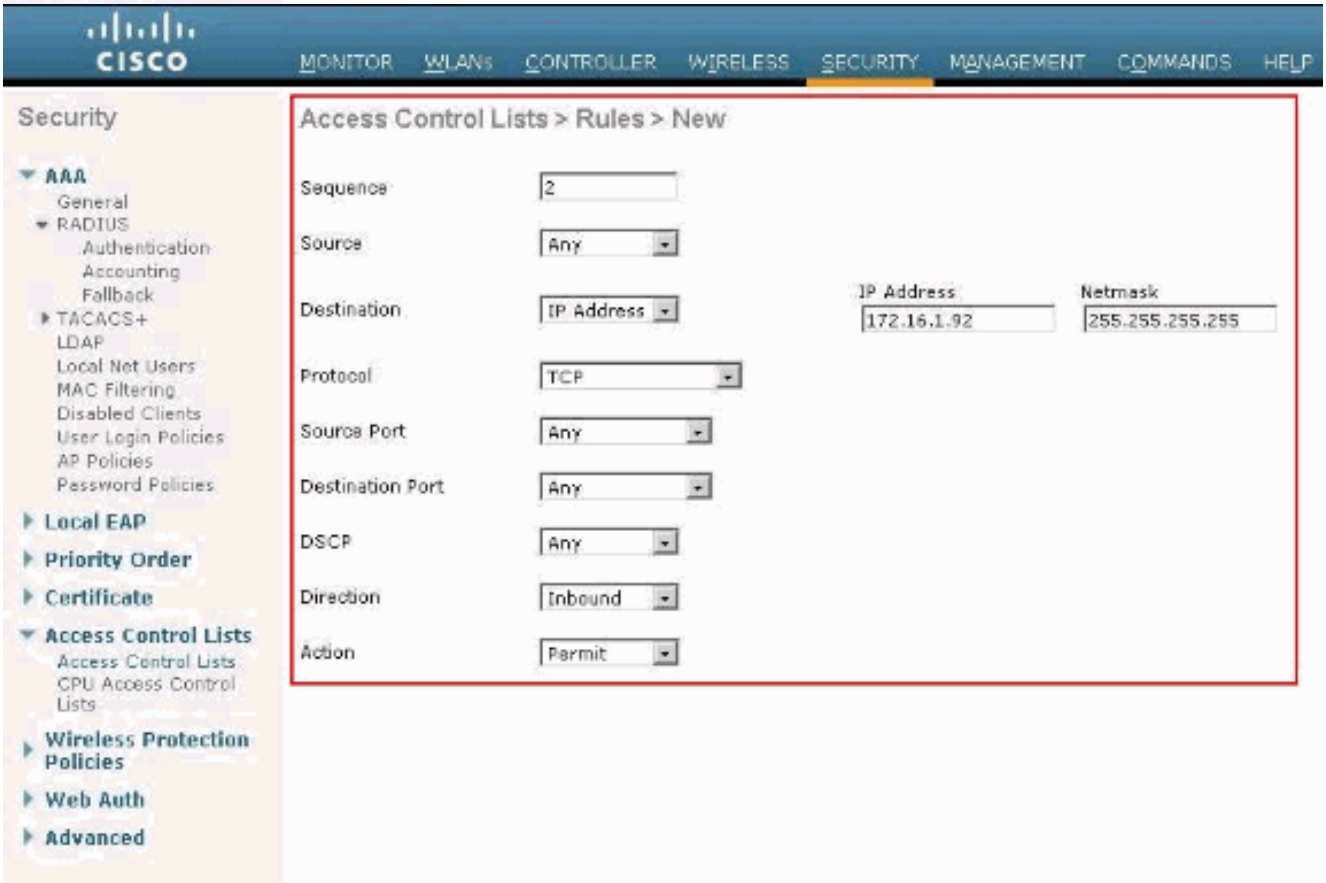
1. Wählen Sie in der WLC-GUI **Security > Access Control Lists (Sicherheit > Zugriffskontrolllisten)**.In diesem Fenster können Sie die aktuellen ACLs anzeigen, die den standardmäßigen Firewall-ACLs ähneln.

2. Klicken Sie auf **Neu**, um eine neue ACL zu erstellen.
3. Geben Sie den Namen der ACL ein, und klicken Sie auf **Apply**.In diesem Beispiel hat die ACL den Namen **Pre-Auth-for-External-Web-Server**.

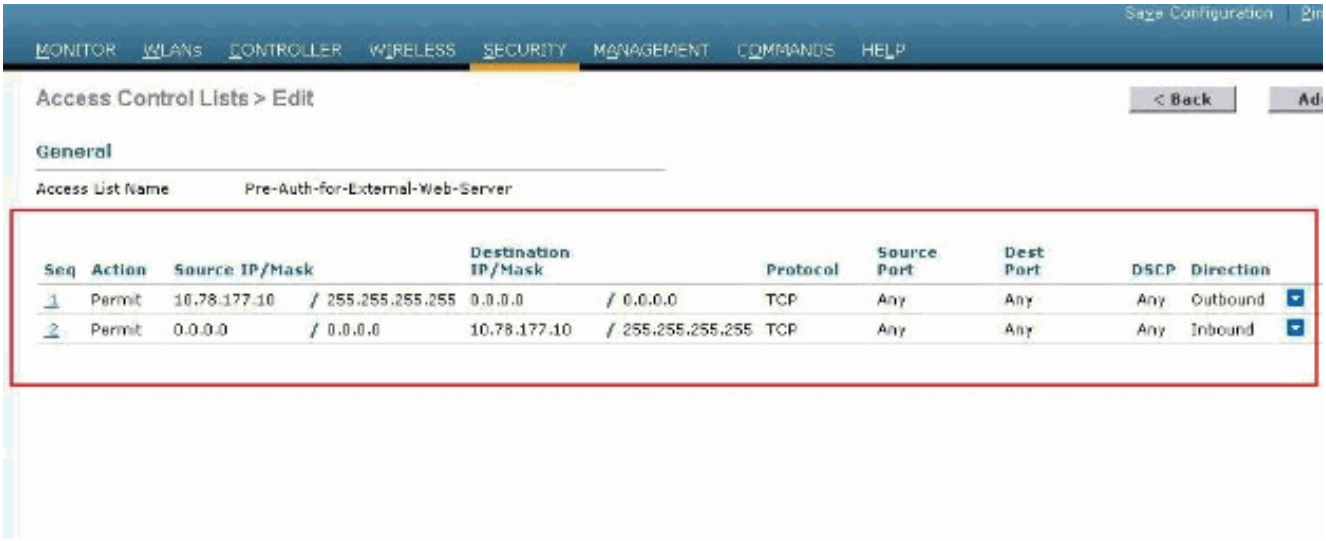


4. Klicken Sie für die neu erstellte ACL auf **Edit**.Das Fenster ACL > Edit (ACL > Bearbeiten) wird angezeigt. In diesem Fenster kann der Benutzer neue Regeln definieren oder vorhandene Regeln der ACL ändern.
5. Klicken Sie auf **Neue Regel hinzufügen**.
6. Definieren Sie eine ACL-Regel, die den Zugriff der Clients auf den externen Webserver ermöglicht.In diesem Beispiel ist 172.16.1.92 die IP-Adresse des externen Webservers.





7. Klicken Sie auf **Apply**, um die Änderungen zu übernehmen.

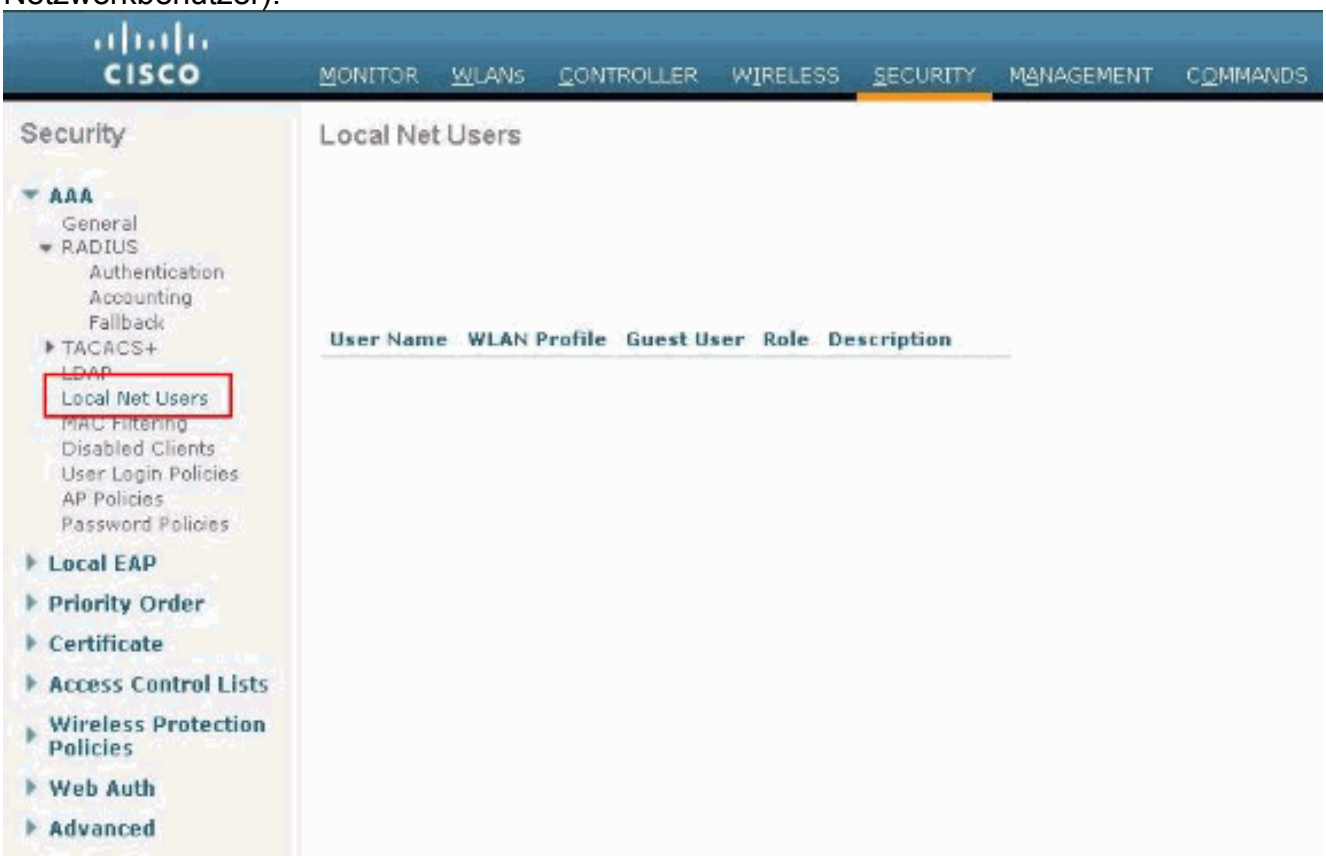


Erstellen einer lokalen Datenbank auf dem WLC für Gastbenutzer

Die Benutzerdatenbank für die Gastbenutzer kann entweder in der lokalen Datenbank des Wireless LAN-Controllers oder außerhalb des Controllers gespeichert werden.

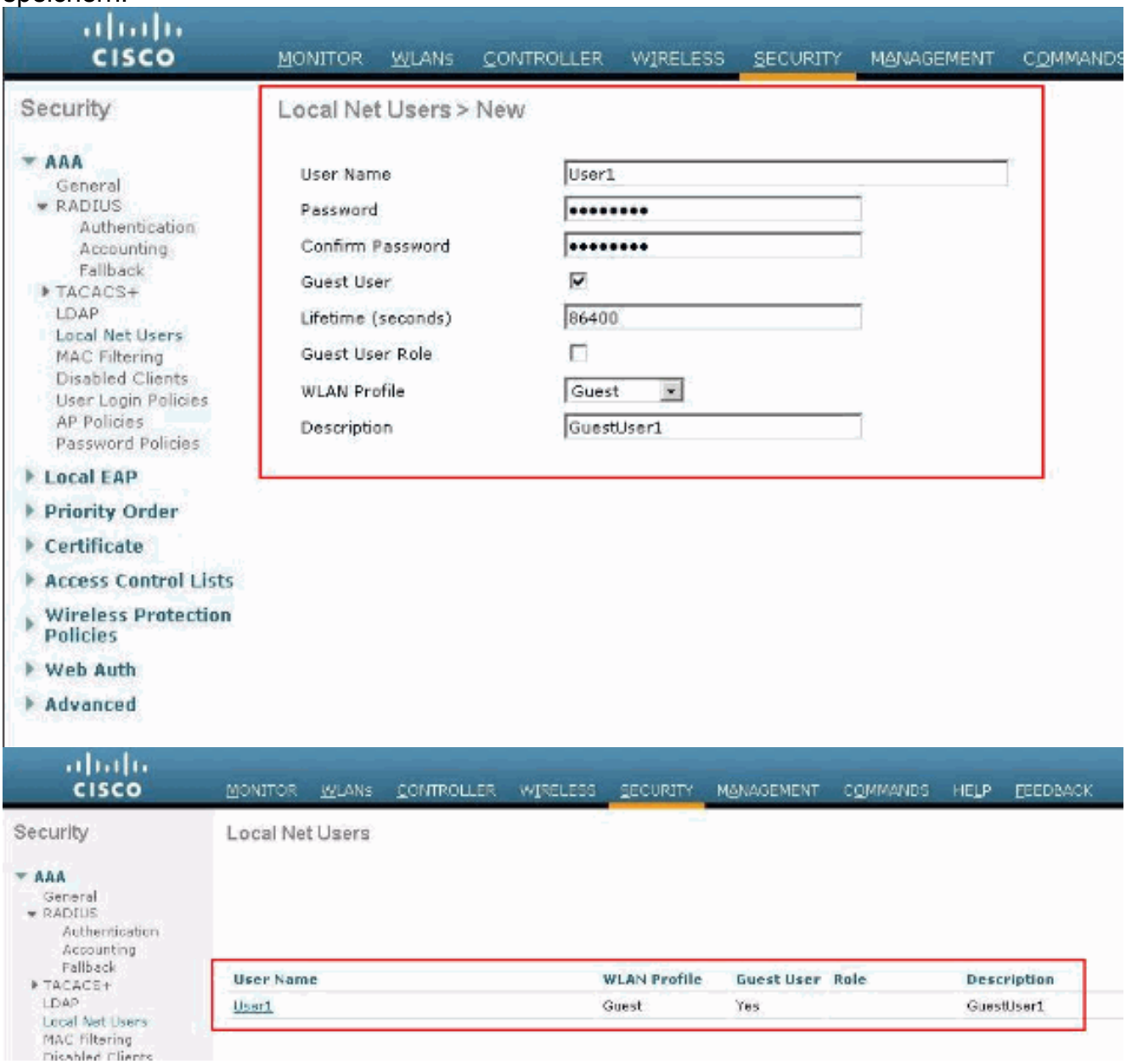
In diesem Dokument wird die lokale Datenbank auf dem Controller zur Benutzerauthentifizierung verwendet. Sie müssen einen Local Net User erstellen und ein Kennwort für die Client-Anmeldung für die Webauthentifizierung definieren. Gehen Sie wie folgt vor, um die Benutzerdatenbank auf dem WLC zu erstellen:

1. Wählen Sie in der WLC-GUI die Option **Security** (**Sicherheit)**.
2. Klicken Sie im Menü AAA auf **Local Net Users** (Lokale Netzwerkbenutzer).



3. Klicken Sie auf **Neu**, um einen neuen Benutzer zu erstellen.Es wird ein neues Fenster angezeigt, in dem Sie nach Benutzername- und Kennwortinformationen gefragt werden.

4. Geben Sie einen Benutzernamen und ein Kennwort ein, um einen neuen Benutzer zu erstellen, und bestätigen Sie dann das Kennwort, das Sie verwenden möchten.In diesem Beispiel wird der Benutzer mit dem Namen **User1** erstellt.
5. Fügen Sie ggf. eine Beschreibung hinzu.In diesem Beispiel wird **Guest User1** verwendet.
6. Klicken Sie auf **Apply**, um die neue Benutzerkonfiguration zu speichern.



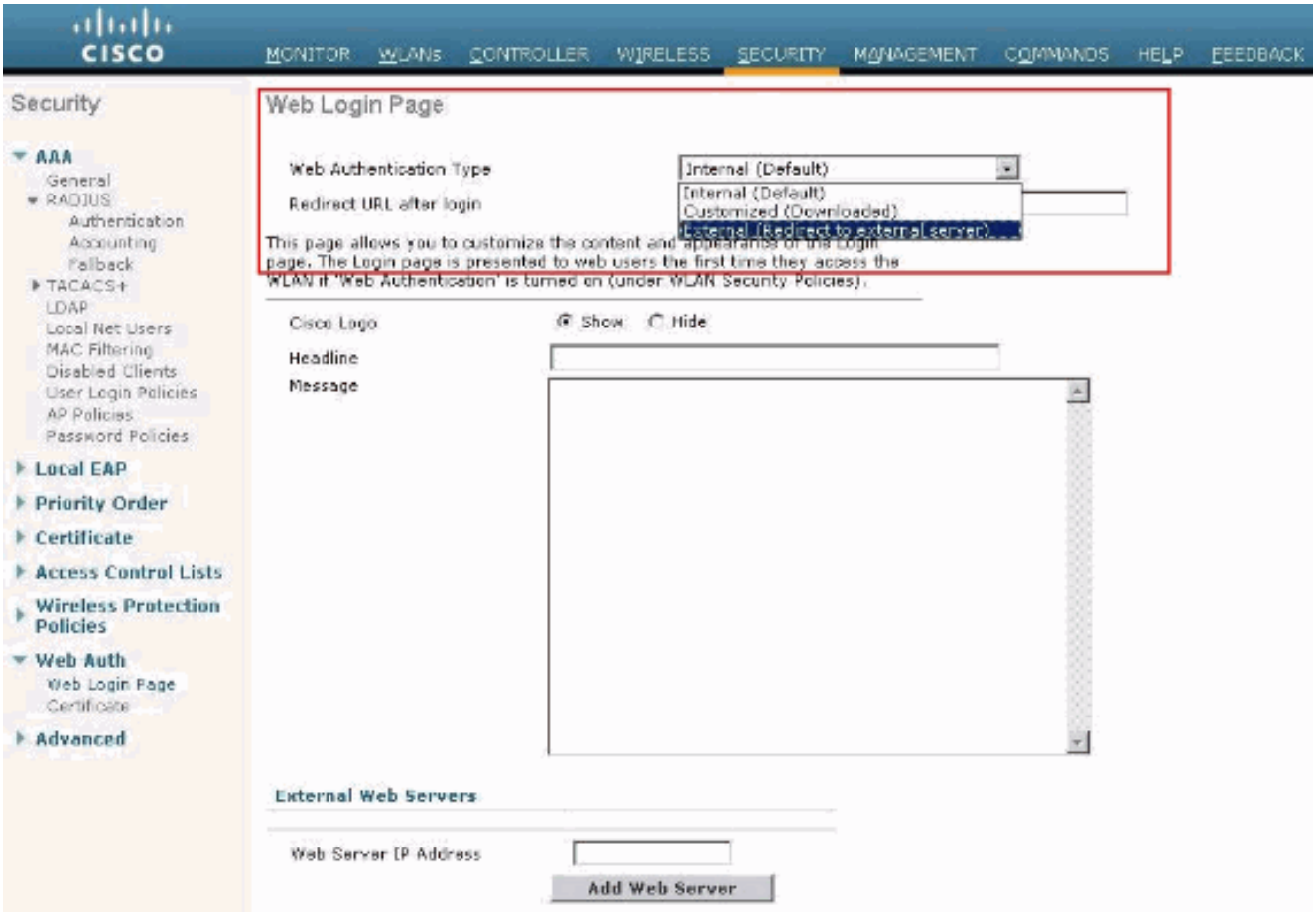
7. Wiederholen Sie die Schritte 3-6, um der Datenbank weitere Benutzer hinzuzufügen.

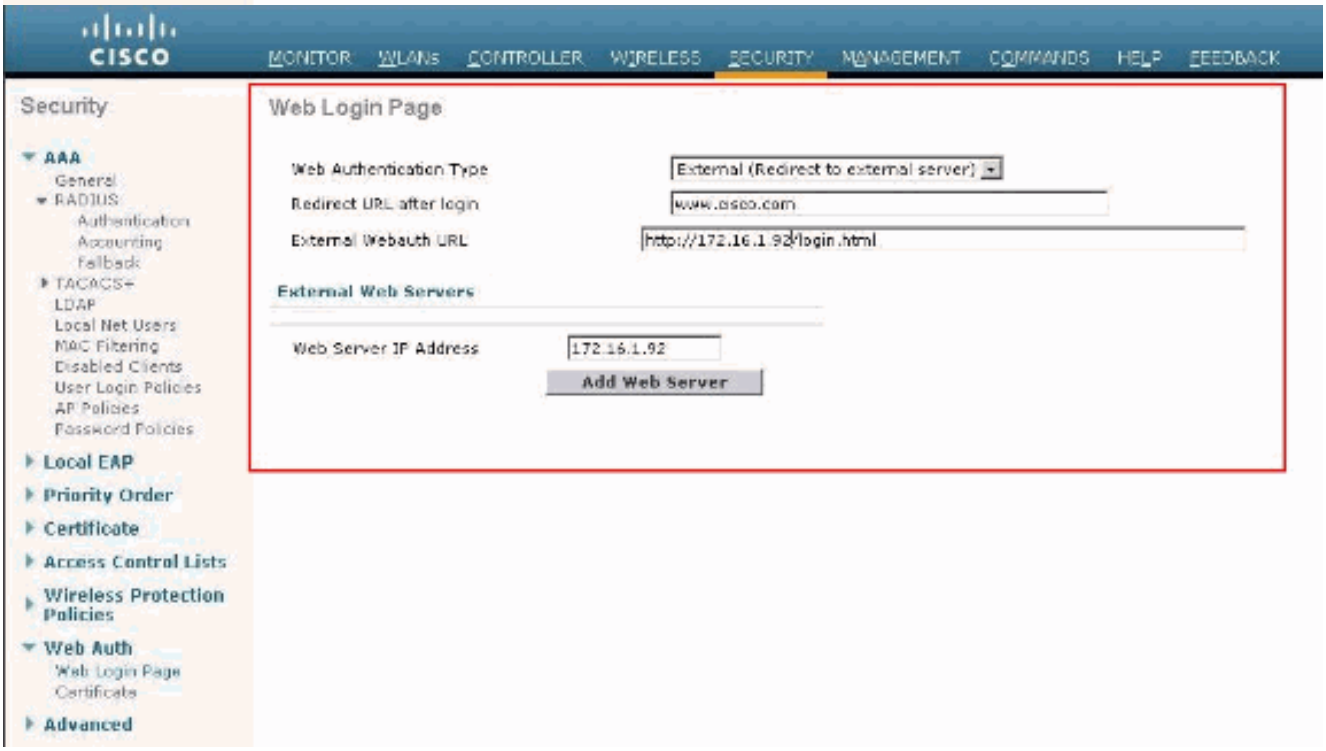
Konfigurieren des WLC für die externe Webauthentifizierung

Im nächsten Schritt wird der WLC für die externe Webauthentifizierung konfiguriert. Führen Sie diese Schritte aus:

1. Wählen Sie in der GUI des Controllers **Security > Web Auth > Web Login Page** aus, um auf die Web Login Page zuzugreifen.
2. Wählen Sie im Dropdown-Feld "Web Authentication Type" die Option **External (Redirect to external server) aus**.
3. Fügen Sie im Abschnitt **Externer Webserver** den neuen externen Webserver hinzu.
4. Geben Sie im Feld **Redirect URL after login (URL nach Anmeldung umleiten)** die URL der

Seite ein, an die der Endbenutzer bei erfolgreicher Authentifizierung umgeleitet wird. Geben Sie im Feld **Externe Webauthentifizierungs-URL** die URL ein, unter der die Anmeldeseite auf dem externen Webserver gespeichert
ist.



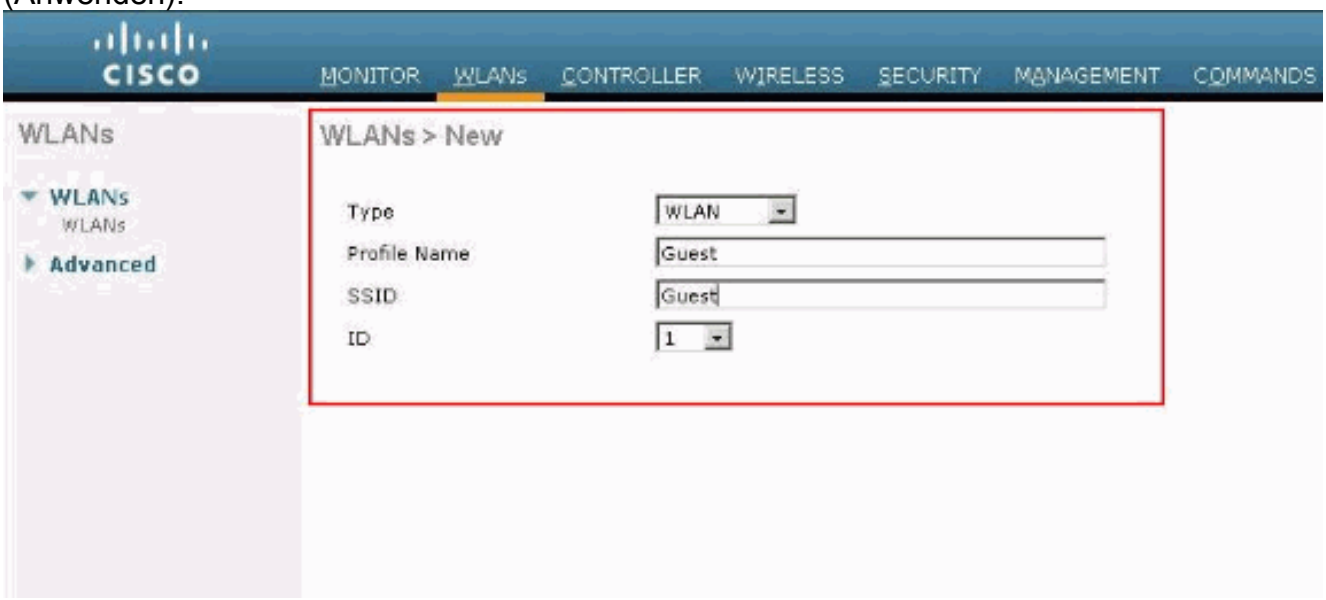


Hinweis: In WLC Version 5.0 und höher kann die Logout-Seite für die Web-Authentifizierung ebenfalls angepasst werden. Weitere Informationen zur Konfiguration finden Sie im Abschnitt Assign Login (Anmelden), Login Failure (Anmeldefehler) und Logout (Abmelden pro WLAN) im *Wireless LAN Controller Configuration Guide*, *5.2* .

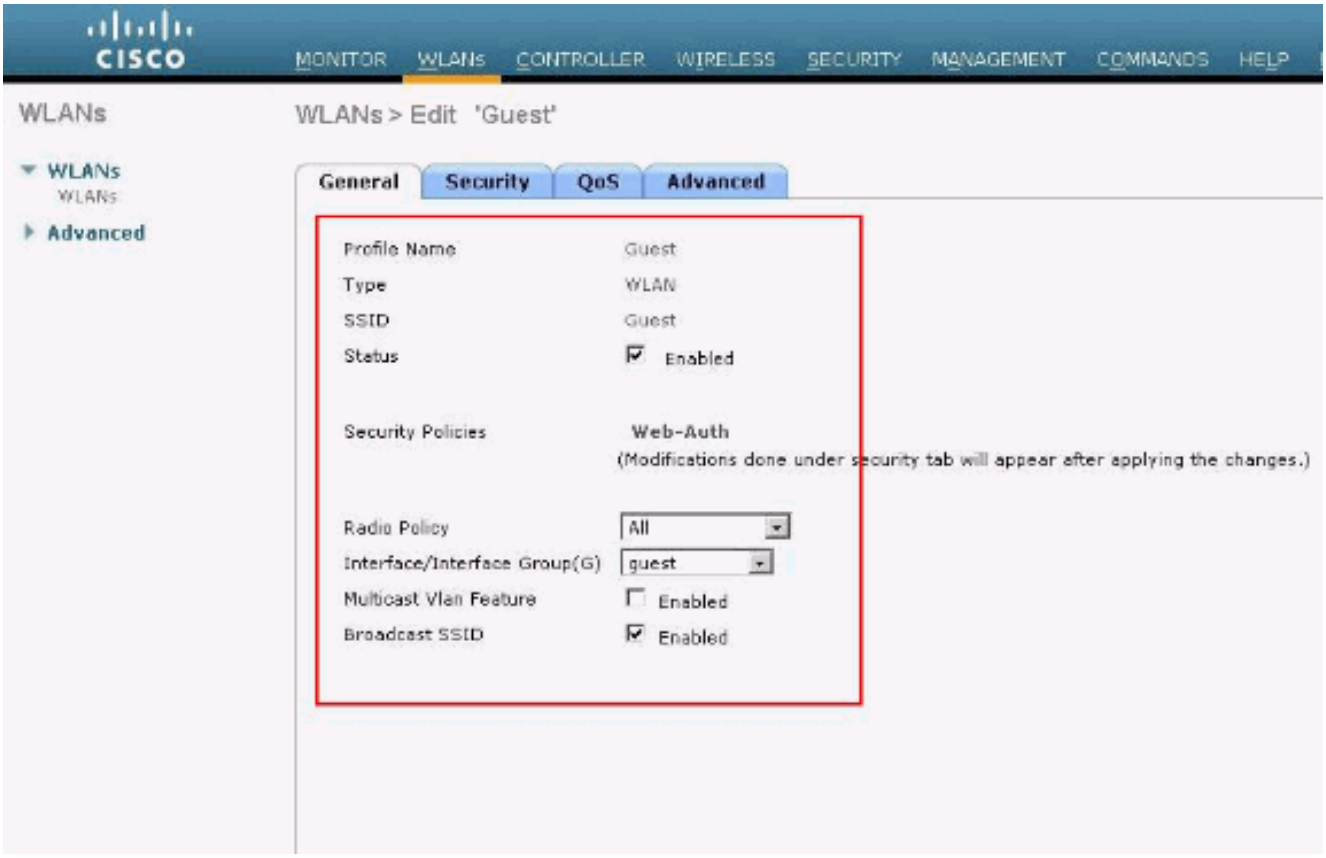
WLAN für Gastbenutzer konfigurieren

Der letzte Schritt besteht in der Erstellung von WLANs für die Gastbenutzer. Führen Sie diese Schritte aus:

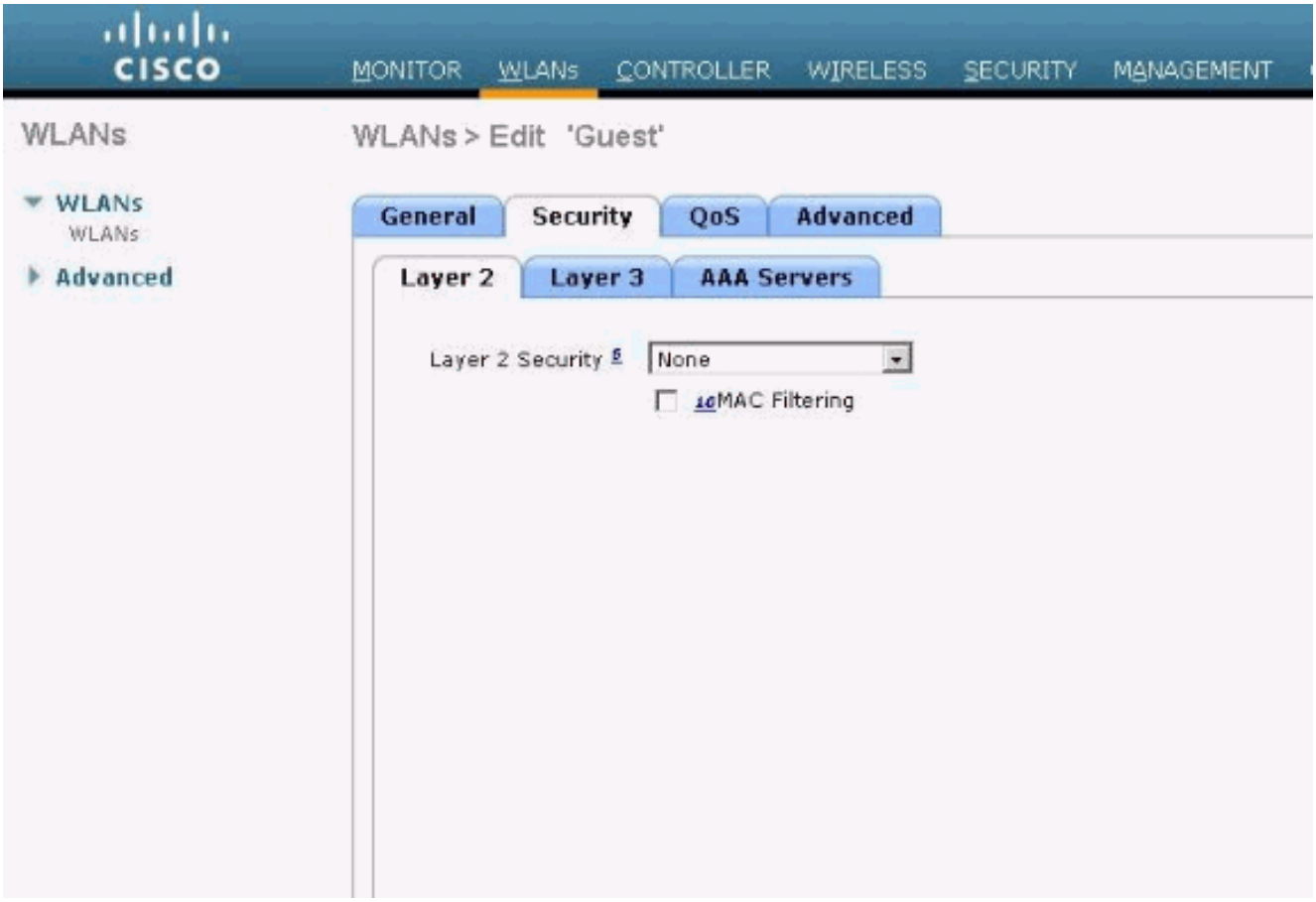
1. Klicken Sie in der Controller-GUI auf **WLANs**, um ein WLAN zu erstellen.Das Fenster WLANs wird angezeigt. In diesem Fenster werden die auf dem Controller konfigurierten WLANs aufgeführt.
2. Klicken Sie auf **Neu**, um ein neues WLAN zu konfigurieren.In diesem Beispiel lautet die WLAN-ID **Guest** und die WLAN-ID **1**.
3. Klicken Sie auf **Apply**
   (Anwenden).



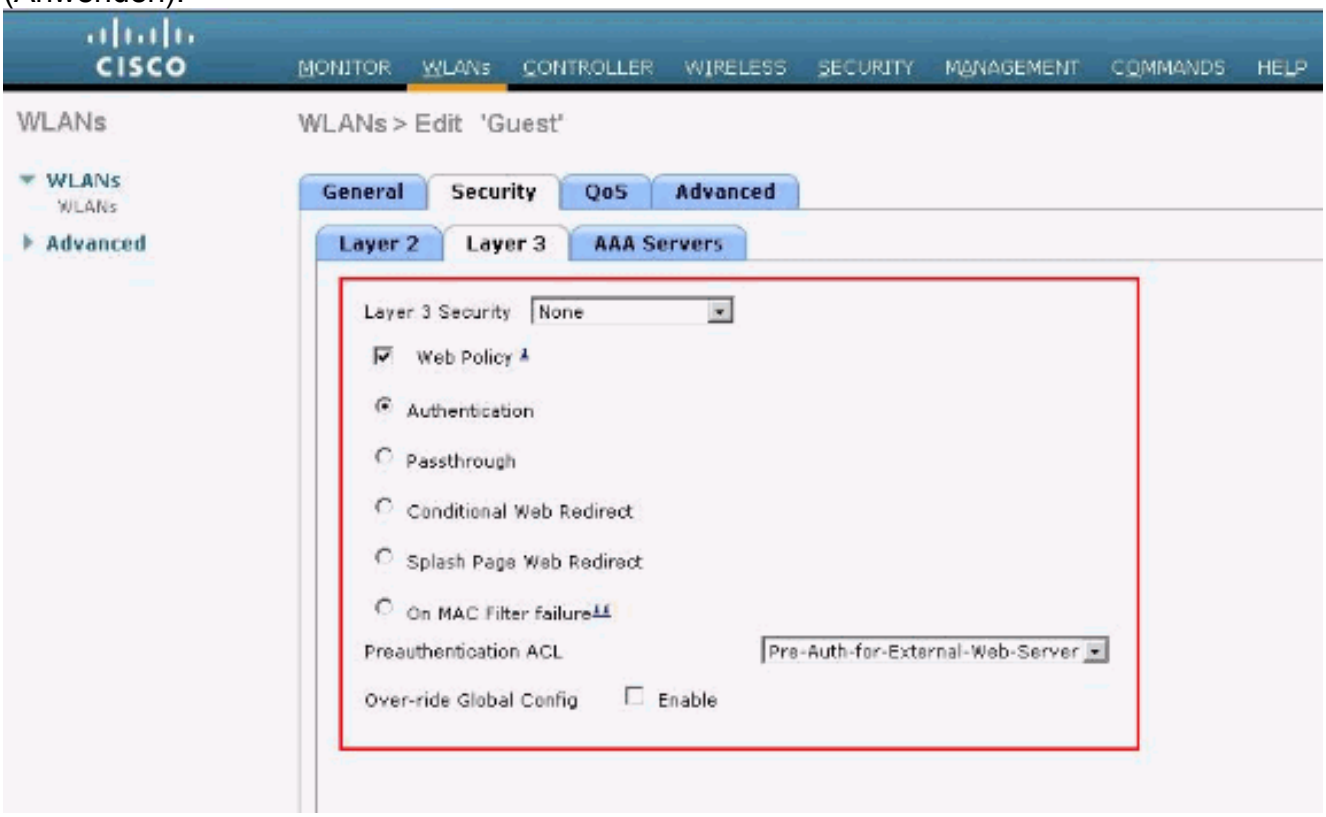
4. Definieren Sie im Fenster WLAN > Edit (WLAN > Bearbeiten) die WLAN-spezifischen Parameter.Wählen Sie für das Gast-WLAN auf der Registerkarte General (Allgemein) im Feld Interface Name (Schnittstellenname) die entsprechende Schnittstelle aus.In diesem Beispiel wird die zuvor erstellte dynamische Schnittstelle **guest** dem WLAN guest zugeordnet.



Wechseln Sie zur Registerkarte Sicherheit. In diesem Beispiel ist unter Layer-2-Sicherheit **Keine** ausgewählt.**Hinweis:** 802.1x-Authentifizierung unterstützt keine Webauthentifizierung. Dies bedeutet, dass Sie bei der Webauthentifizierung nicht 802.1x oder WPA/WPA2 mit 802.1x als Layer-2-Sicherheit auswählen können.Die Webauthentifizierung wird mit allen anderen Layer-2-Sicherheitsparametern
unterstützt.



Aktivieren Sie im Feld Layer 3-Sicherheit das Kontrollkästchen **Webrichtlinie,** und wählen Sie die Option **Authentifizierung**.Diese Option wird gewählt, da die Wireless-Gast-Clients mithilfe der Webauthentifizierung authentifiziert werden.Wählen Sie im Dropdown-Menü die entsprechende ACL für die Vorauthentifizierung aus.In diesem Beispiel wird die zuvor erstellte ACL für die Vorauthentifizierung verwendet.Klicken Sie auf **Apply** (Anwenden).

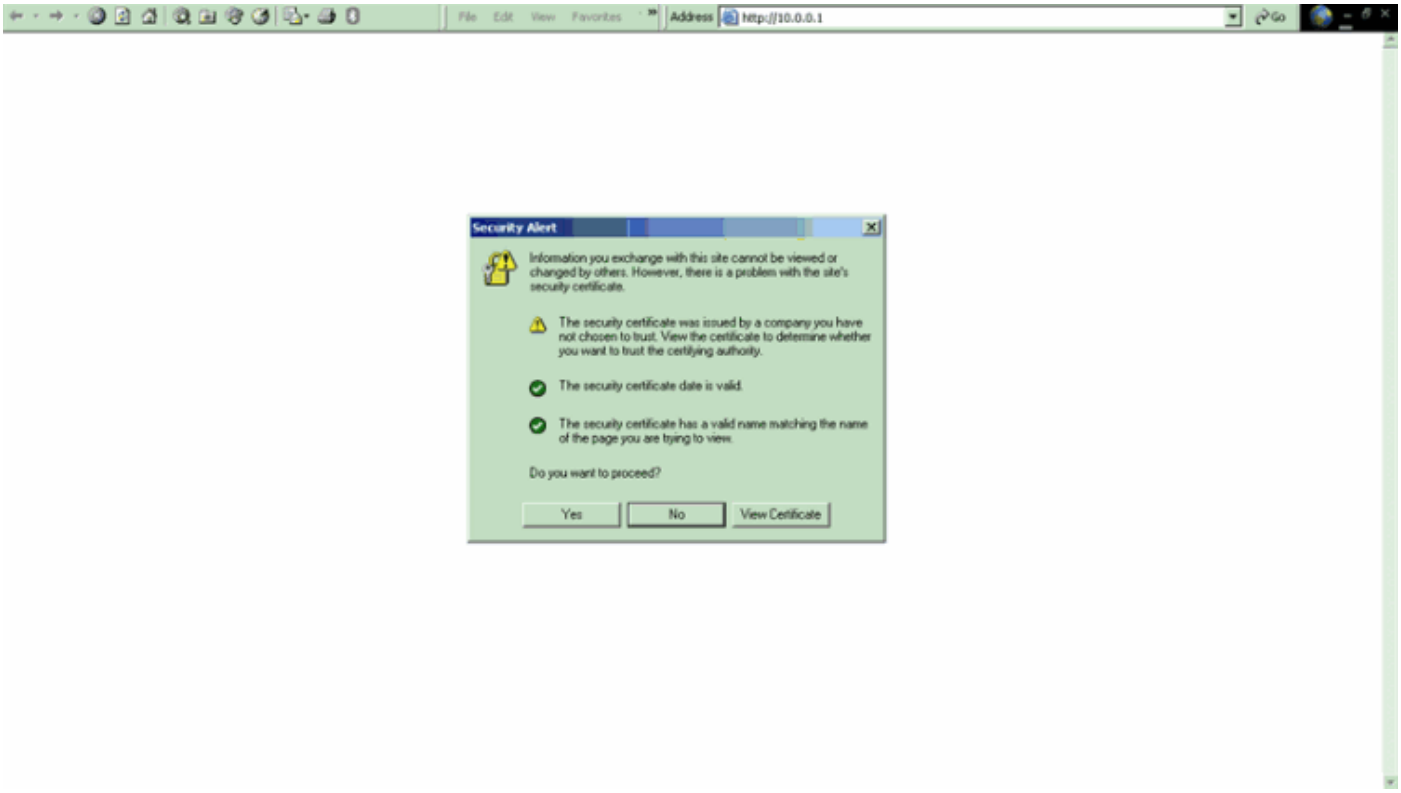


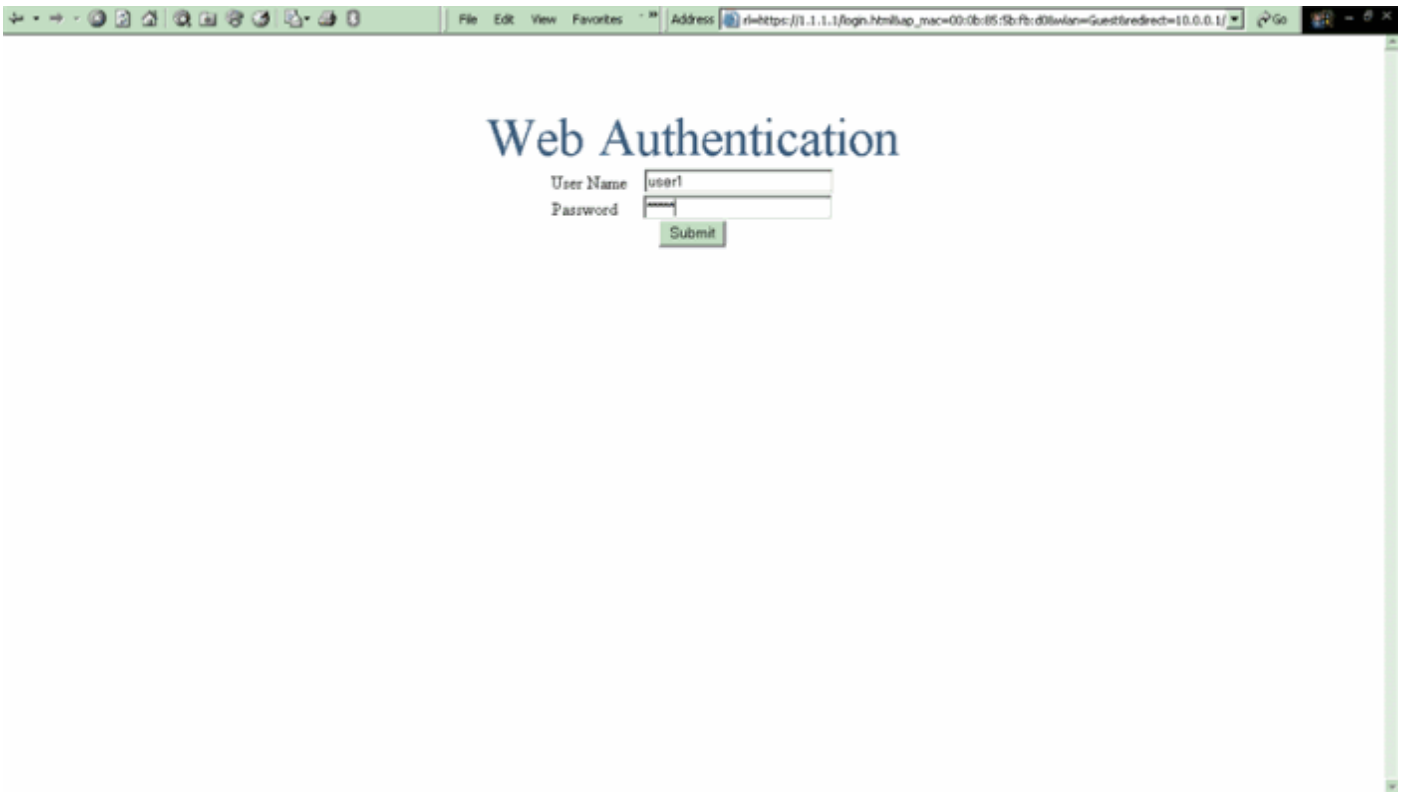
Überprüfung

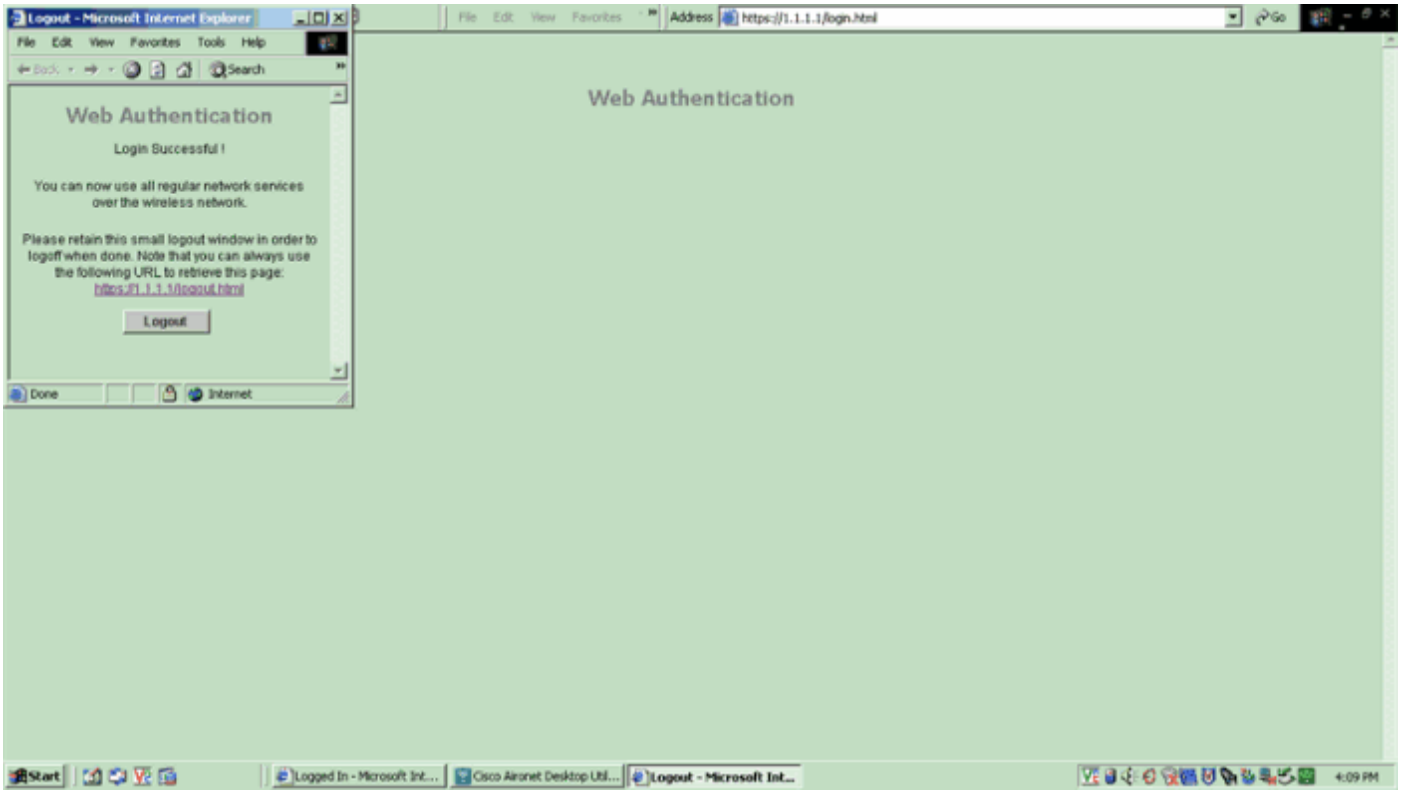
Der Wireless-Client wird geöffnet, und der Benutzer gibt die URL (z. B. www.cisco.com) in den Webbrowser ein. Da der Benutzer nicht authentifiziert wurde, leitet der WLC den Benutzer an die externe Web-Anmelde-URL um.

Der Benutzer wird zur Eingabe der Anmeldeinformationen aufgefordert. Nachdem der Benutzer den Benutzernamen und das Kennwort eingegeben hat, werden auf der Anmeldeseite die Benutzeranmeldeinformationen eingegeben und die Anforderung beim Senden an das action_URL-Beispiel http://1.1.1.1/login.html des WLC-Webservers zurückgesendet. Dieser wird als Eingabeparameter für die Kundenumleitungs-URL bereitgestellt, wobei 1.1.1.1 die virtuelle Schnittstellenadresse auf dem Switch ist.

Der WLC authentifiziert den Benutzer anhand der auf dem WLC konfigurierten lokalen Datenbank. Nach erfolgreicher Authentifizierung leitet der WLC-Webserver den Benutzer entweder an die konfigurierte Umleitungs-URL oder an die URL weiter, mit der der Client begonnen hat, z. B. www.cisco.com.


File Edit View Favorites
Address http://10.0.0.1
Security Alert
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
The security certificate date is valid.
The security certificate has a valid name matching the name of the page you are trying to view.
Do you want to proceed?
Yes
No
View Certificate


File Edit View Favorites
Address rl=https://1.1.1.1/login.html&ap_mac=00:0b:85:5b:fb:d0&wlan=Guest&redirect=10.0.0.1/
Web Authentication
User Name user1
Password
Submit



Fehlerbehebung

Verwenden Sie diese Befehle zum Debuggen, um Fehler in Ihrer Konfiguration zu beheben.

- debug mac addr <client-MAC-Adresse xx:xx:xx:xx:xx:xx>
- debug aaa all enable
- debug pem state enable
- debug pem events enable
- debug dhcp message enable
- debug dhcp packet enable
- debug pm ssh-appgw enable
- debug pm ssh-tcp enable

Verwenden Sie diesen Abschnitt, um Probleme mit Ihrer Konfiguration zu beheben.

Clients, die an den externen Webauthentifizierungsserver umgeleitet werden, erhalten eine Zertifikatwarnung.

Problem: Wenn Clients an den externen Web-Authentifizierungsserver von Cisco umgeleitet werden, erhalten sie eine Zertifikatswarnung. Auf dem Server befindet sich ein gültiges Zertifikat, und wenn Sie sich direkt mit dem externen Webauthentifizierungsserver verbinden, wird die Zertifikatwarnung nicht empfangen. Liegt dies daran, dass die virtuelle IP-Adresse (1.1.1.1) des WLC dem Client anstelle der tatsächlichen IP-Adresse des externen Web-Authentifizierungsservers, der mit dem Zertifikat verknüpft ist, angezeigt wird?

Lösung: Ja. Unabhängig davon, ob Sie eine lokale oder externe Webauthentifizierung durchführen, wird der interne Webserver auf dem Controller immer noch erreicht. Wenn Sie eine Umleitung zu einem externen Webserver durchführen, erhalten Sie weiterhin die Zertifikatswarnung vom Controller, es sei denn, Sie verfügen über ein gültiges Zertifikat auf dem Controller selbst. Wenn die Umleitung an https gesendet wird, erhalten Sie die Zertifikatswarnung

vom Controller und vom externen Webserver, es sei denn, beide verfügen über ein gültiges Zertifikat.

Um die Zertifikatswarnungen vollständig loszuwerden, benötigen Sie ein Zertifikat auf Stammebene, das ausgestellt und auf Ihren Controller heruntergeladen wird. Das Zertifikat wird für einen Hostnamen ausgestellt, und Sie geben diesen Hostnamen in das Feld für den DNS-Hostnamen unter der virtuellen Schnittstelle auf dem Controller ein. Sie müssen außerdem den Hostnamen zu Ihrem lokalen DNS-Server hinzufügen und ihn auf die virtuelle IP-Adresse (1.1.1.1) des WLC verweisen.

Weitere Informationen finden Sie unter Certificate Signing Request (CSR) Generation for a Third Party Certificate on a WLAN Controller (WLC).

Fehler: "Seite kann nicht angezeigt werden"

Problem: Nach dem Upgrade des Controllers auf 4.2.61.0 wird die Fehlermeldung "Seite kann nicht angezeigt werden " angezeigt, wenn Sie eine heruntergeladene Webseite für die Webauthentifizierung verwenden. Dies funktionierte vor dem Upgrade gut. Die interne Standardwebseite wird problemlos geladen.

Lösung: Ab der WLC Version 4.2 und höher wird eine neue Funktion eingeführt, bei der Sie mehrere benutzerdefinierte Anmeldeseiten für die Webauthentifizierung haben können.

Damit die Webseite ordnungsgemäß geladen wird, reicht es nicht aus, den Web-Authentifizierungstyp in **Security > Web Auth > Web Login (Sicherheit > Webauthentifizierung > Webanmeldung)** global **anzupassen**. Es muss auch auf einem bestimmten WLAN konfiguriert werden. Führen Sie hierzu die folgenden Schritte aus:

1. Melden Sie sich bei der GUI des WLC an.
2. Klicken Sie auf die Registerkarte **WLANs**, und greifen Sie auf das Profil des für die Webauthentifizierung konfigurierten WLAN zu.
3. Klicken Sie auf der Seite WLAN > Edit (WLAN > Bearbeiten) auf die Registerkarte **Security (Sicherheit)**. Wählen Sie anschließend **Layer 3 aus.**
4. Wählen Sie auf dieser Seite als Layer 3 Security (Layer-3-Sicherheit) **None** (**Keine**) aus.
5. Aktivieren Sie das Kontrollkästchen **Webrichtlinie**, und wählen Sie die Option **Authentifizierung** aus.
6. Aktivieren Sie das Kontrollkästchen "Globale Konfiguration überschreiben **aktivieren"**, wählen Sie "**Benutzerdefiniert (Heruntergeladen)**" als Web Auth Type (Webauthentifizierungstyp) aus, und wählen Sie die gewünschte Anmeldeseite aus dem Dropdown-Menü **Anmeldeseite**. Klicken Sie auf **Apply** (Anwenden).

Zugehörige Informationen

- Konfigurationsbeispiel für Web-Authentifizierung des Wireless LAN-Controllers
- Video: Web-Authentifizierung auf Cisco Wireless LAN-Controllern (WLCs)
- Konfigurationsbeispiel für VLANs auf einem Wireless LAN Controller
- Wireless LAN-Controller und Lightweight Access Point - Konfigurationsbeispiel
- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.