Konfigurationsbeispiel für die Umleitung der Splash-Seite des Wireless LAN Controller

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie die Funktion zur Umleitung der Splash-Seite auf den Wireless LAN-Controllern konfigurieren.

Voraussetzungen

Anforderungen

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

- Kenntnisse der LWAPP-Sicherheitslösungen
- Informationen zur Konfiguration von Cisco Secure ACS

Verwendete Komponenten

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

- Cisco Wireless LAN Controller (WLC) der Serie 4400 mit Firmware-Version 5.0
- Cisco Lightweight Access Point der Serie 1232 (LAP)
- Cisco Aironet 802.a/b/g Wireless Client Adapter für Firmware-Version 4.1
- Cisco Secure ACS Server mit Version 4.1
- Externer Webserver von Drittanbietern

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

Splash Page Web Redirect ist eine Funktion, die mit dem Wireless LAN Controller Version 5.0 eingeführt wurde. Mit dieser Funktion wird der Benutzer auf eine bestimmte Webseite umgeleitet, nachdem die 802.1x-Authentifizierung abgeschlossen ist. Die Umleitung erfolgt, wenn der Benutzer einen Browser öffnet (konfiguriert mit einer Standard-Startseite) oder versucht, auf eine URL zuzugreifen. Nachdem die Umleitung auf die Webseite abgeschlossen ist, hat der Benutzer vollen Zugriff auf das Netzwerk.

Sie können die Umleitungsseite auf dem RADIUS-Server (Remote Authentication Dial-In User Service) angeben. Der RADIUS-Server muss so konfiguriert werden, dass das Cisco AV-pair url-redirect RADIUS-Attribut bei erfolgreicher 802.1x-Authentifizierung an den Wireless LAN Controller zurückgegeben wird.

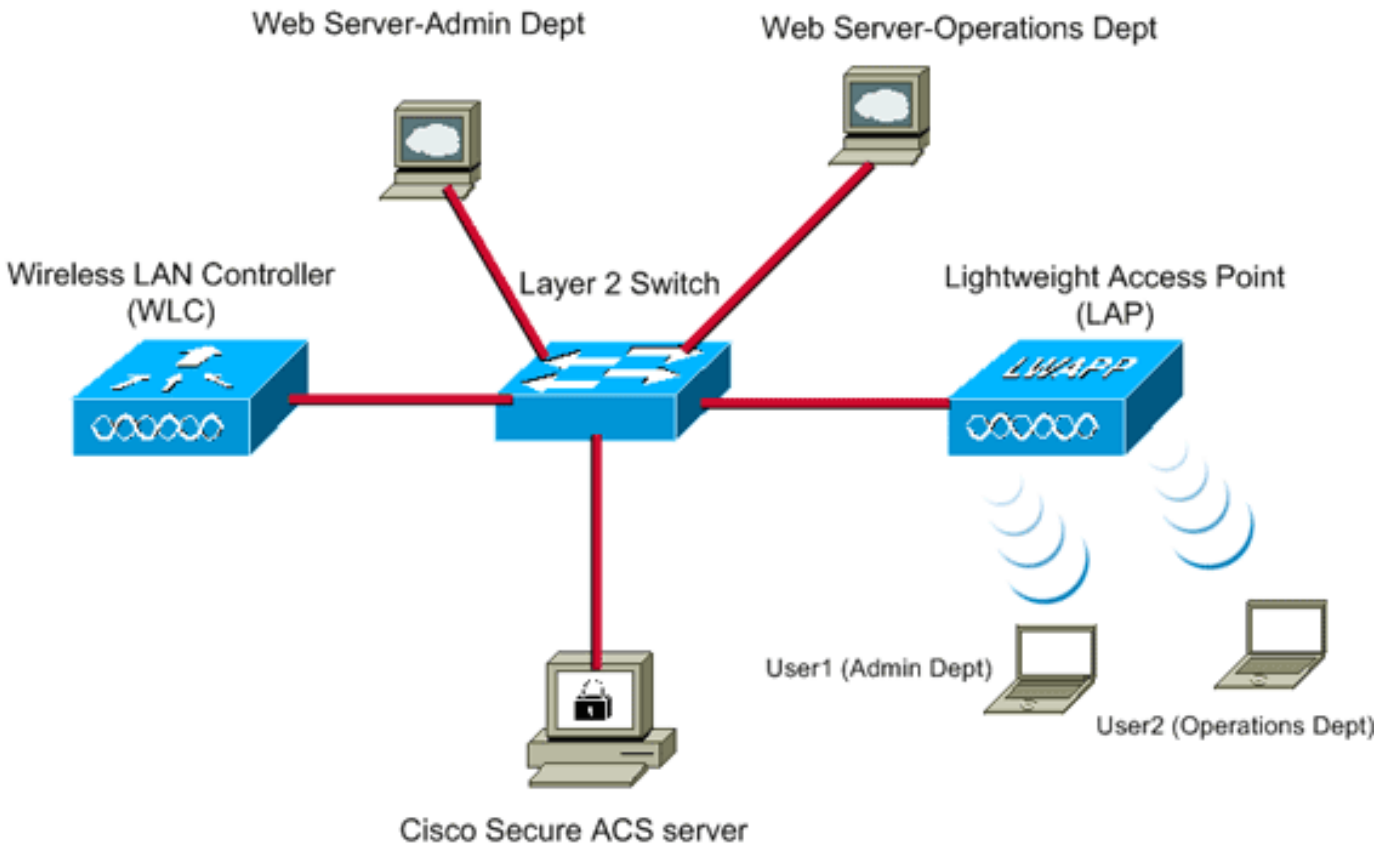
Die Splash-Page-Webumleitungsfunktion ist nur für WLANs verfügbar, die für die 802.1x- oder WPA/WPA2-Layer-2-Sicherheit konfiguriert sind.

Netzwerkeinrichtung

In diesem Beispiel sind ein Cisco 4404 WLC und ein Cisco 1232 LAP über einen Layer-2-Switch verbunden. Der Cisco Secure ACS-Server (der als externer RADIUS-Server fungiert) ist ebenfalls mit demselben Switch verbunden. Alle Geräte befinden sich im gleichen Subnetz.

Die LAP wird zunächst für den Controller registriert. Sie müssen zwei WLANs erstellen: eines für die Benutzer der **Administratorabteilung** und eines für die Benutzer der **Betriebsabteilung**. Beide WLANs verwenden WPA2/AES (EAP-FAST wird für die Authentifizierung verwendet). Beide WLANs verwenden die Funktion "Splash Page Redirect" (Umleitung der Splash-Seite), um Benutzer an die entsprechenden URLs der Startseite (auf externen Webservern) umzuleiten.

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



WLC Management IP address:	10.77.244.204
WLC AP Manager IP address:	10.77.244.205
Wireless Client IP address:	10.77.244.221
Cisco Secure ACS server IP address	10.77.244.196
Subnet Mask used in this example	255.255.255.224

Im nächsten Abschnitt wird erläutert, wie Sie die Geräte für dieses Setup konfigurieren.

Konfigurieren

In diesem Abschnitt erfahren Sie, wie Sie die in diesem Dokument beschriebenen Funktionen konfigurieren können.

Hinweis: Verwenden Sie das Tool für die Suche nach Befehlen (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Führen Sie die folgenden Schritte aus, um die Geräte für die Verwendung der Splash-Page-Umleitungsfunktion zu konfigurieren:

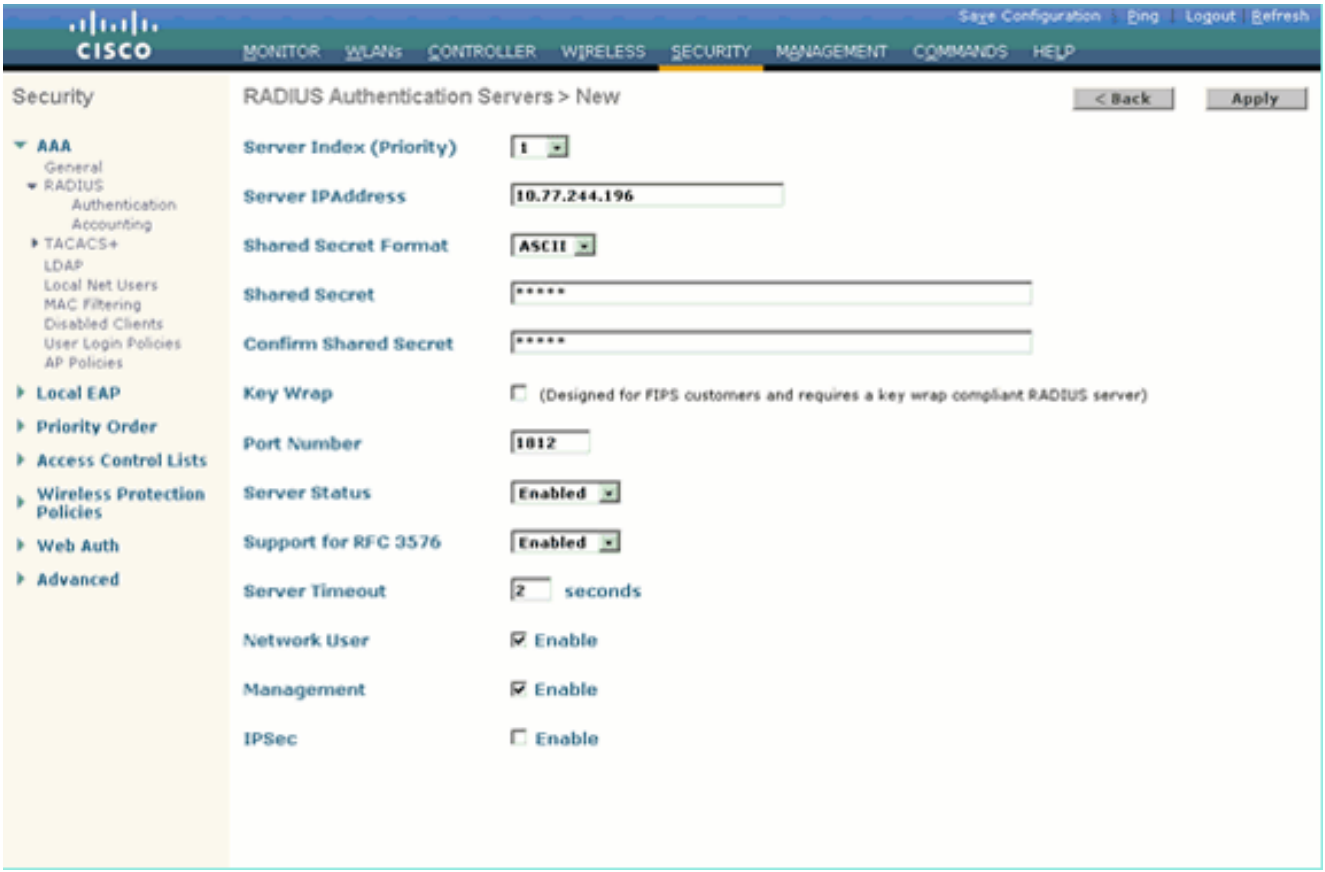
1. Konfigurieren des WLC für die RADIUS-Authentifizierung über den Cisco Secure ACS-Server
2. Konfigurieren Sie die WLANs für die Admin- und die Betriebsabteilung.
3. Konfigurieren Sie Cisco Secure ACS so, dass die Funktion zum Umleiten von Splash-Seiten unterstützt wird.

Schritt 1: Konfigurieren des WLC für die RADIUS-Authentifizierung über den Cisco Secure ACS-Server

Der WLC muss konfiguriert werden, um die Benutzeranmeldeinformationen an einen externen RADIUS-Server weiterzuleiten.

Führen Sie die folgenden Schritte aus, um den WLC für einen externen RADIUS-Server zu konfigurieren:

1. Wählen Sie **Sicherheit** und **RADIUS-Authentifizierung** in der Benutzeroberfläche des Controllers aus, um die Seite RADIUS-Authentifizierungsserver anzuzeigen.
2. Klicken Sie auf **Neu**, um einen RADIUS-Server zu definieren.
3. Definieren Sie die RADIUS-Serverparameter auf der Seite RADIUS Authentication Servers > New (RADIUS-Authentifizierungsserver > Neu).Zu diesen Parametern gehören:IP-Adresse des RADIUS-ServersGemeinsamer SchlüsselPort-NummerServerstatus



In diesem Dokument wird der ACS-Server mit der IP-Adresse 10.77.244.196 verwendet.

4. Klicken Sie auf **Apply** (Anwenden).

Schritt 2: Konfigurieren Sie die WLANs für die Abteilung Administration und Betrieb.

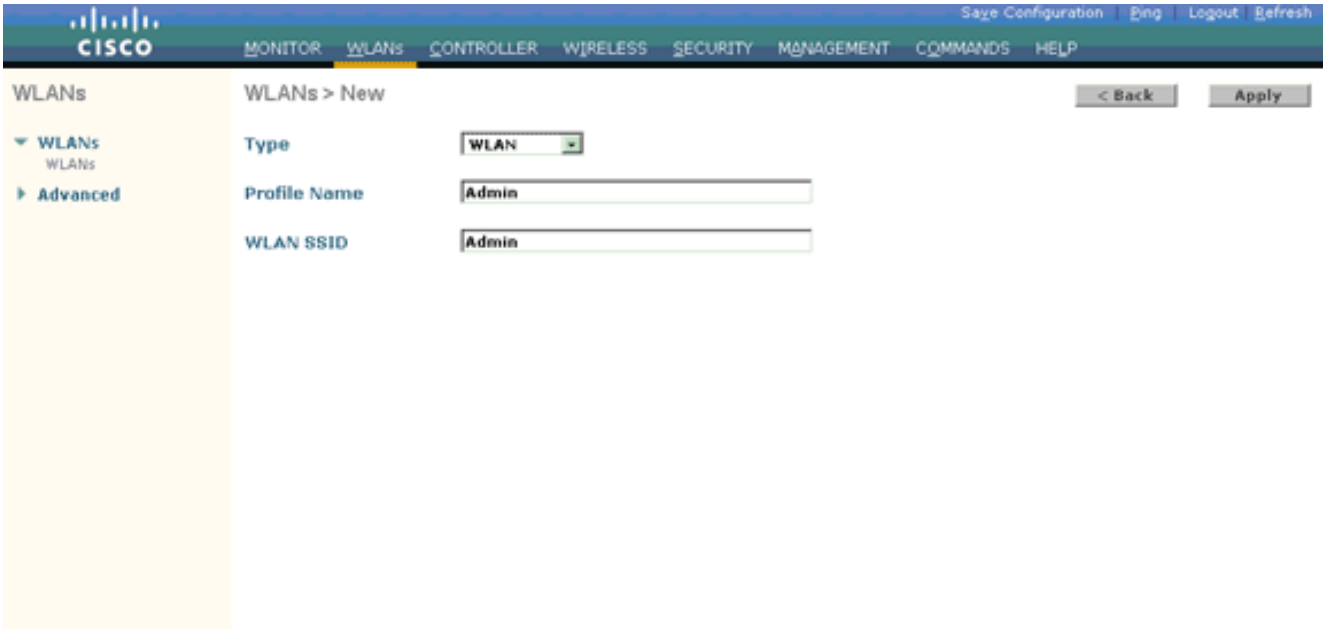
In diesem Schritt konfigurieren Sie die beiden WLANs (eines für die Admin-Abteilung und eines für die Operations-Abteilung), die die Clients für die Verbindung mit dem Wireless-Netzwerk verwenden.

Die WLAN-SSID für die Admin-Abteilung lautet *Admin*. Die WLAN-SSID für die Betriebsabteilung lautet "Operations" (Betrieb).

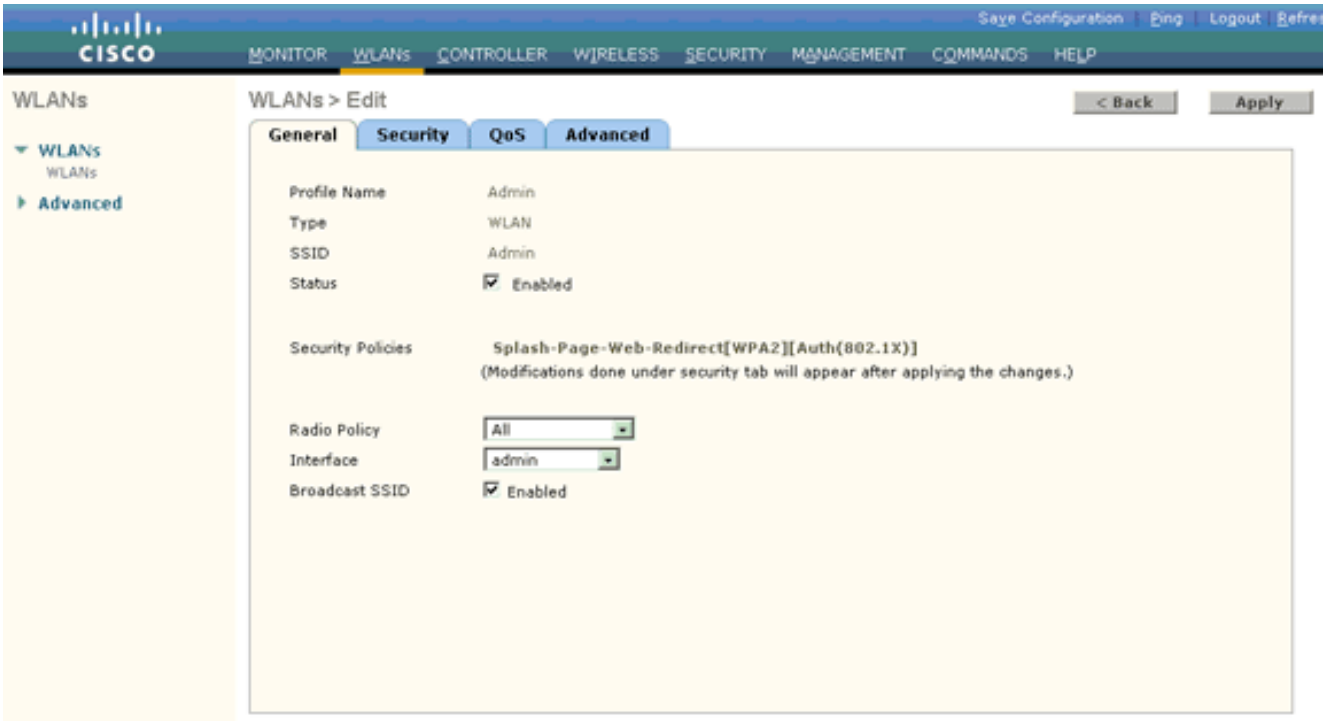
Verwenden Sie die EAP-FAST-Authentifizierung, um WPA2 als Layer-2-Sicherheitsmechanismus in beiden WLANs zu aktivieren, und die Webrichtlinie - Splash Page-Webumleitung als Layer-3-Sicherheitsmethode.

Gehen Sie wie folgt vor, um das WLAN und die zugehörigen Parameter zu konfigurieren:

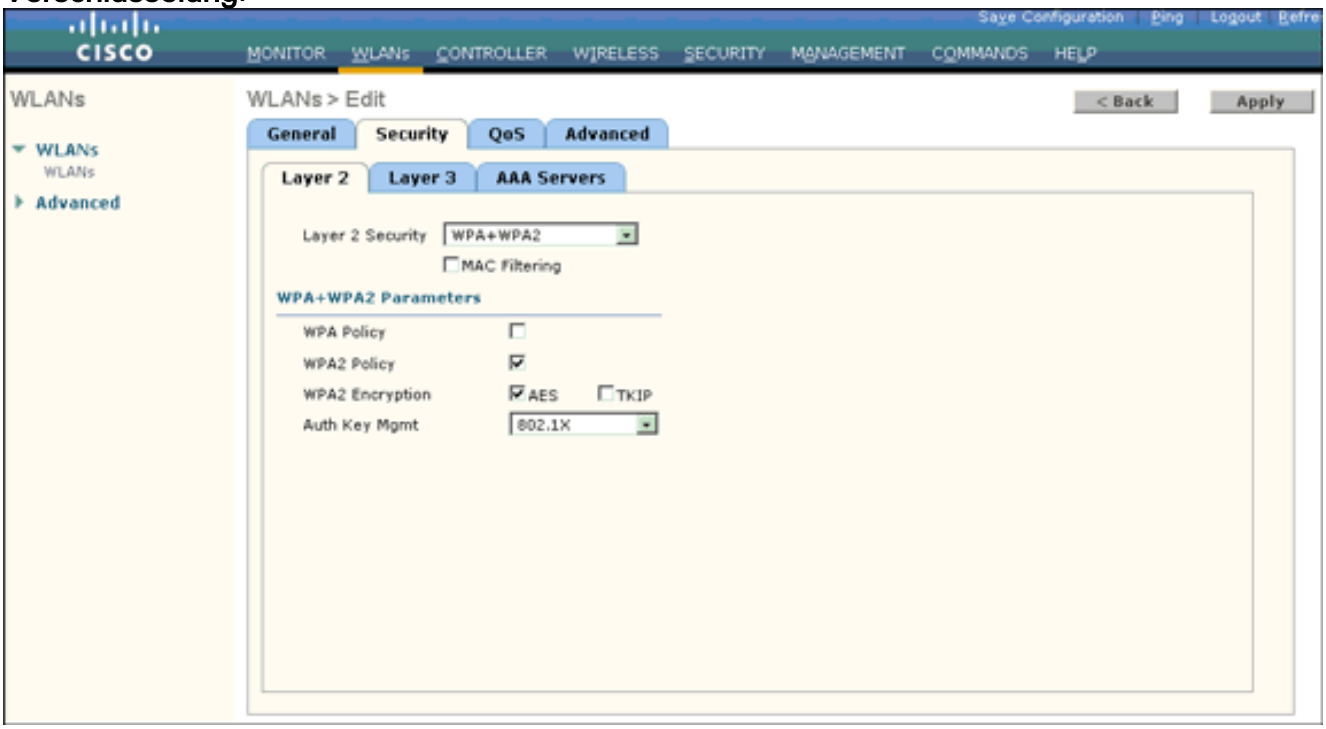
1. Klicken Sie in der GUI des Controllers auf **WLANs**, um die Seite WLANs anzuzeigen.Auf dieser Seite werden die WLANs aufgelistet, die auf dem Controller vorhanden sind.
2. Klicken Sie auf **Neu**, um ein neues WLAN zu erstellen.



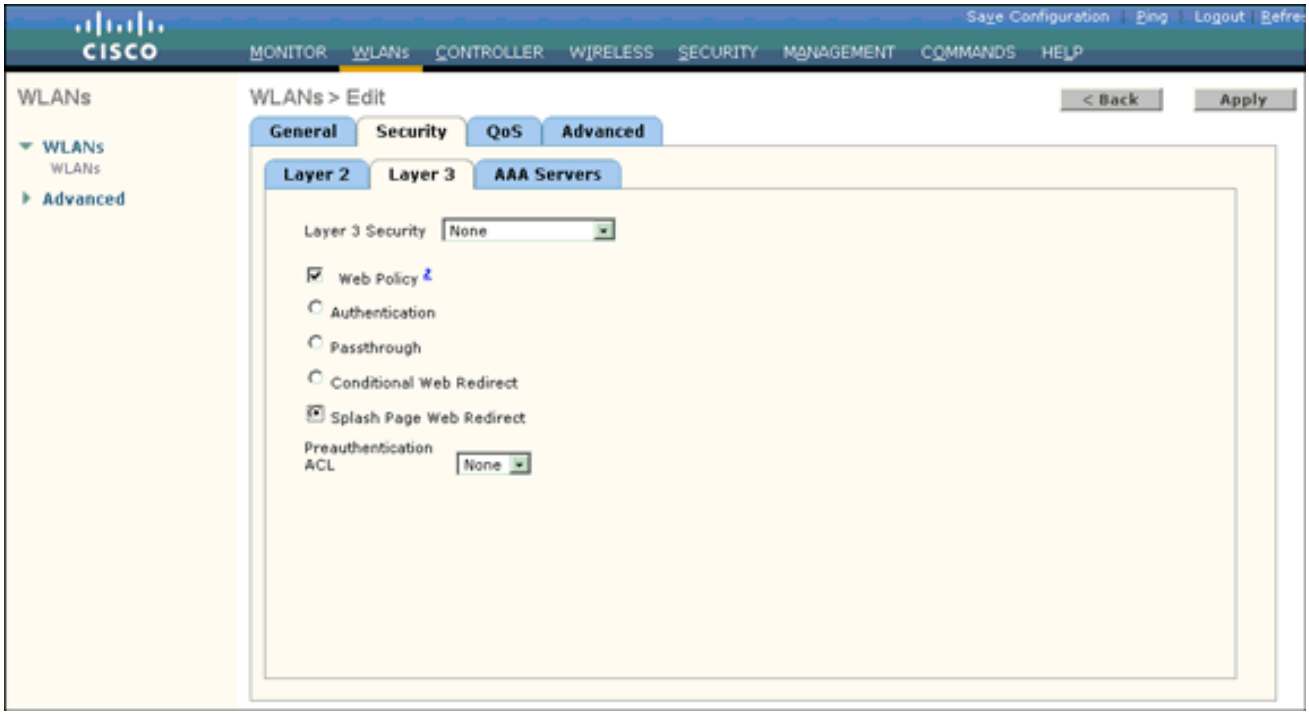
3. Geben Sie auf der Seite WLANs > New (WLAN > Neu) den WLAN-SSID-Namen und den Profilnamen ein.
4. Klicken Sie auf **Apply** (Anwenden).
5. Zunächst erstellen wir das WLAN für die Admin-Abteilung.Nach dem Erstellen eines neuen WLAN wird die Seite WLAN > Edit (WLAN > Bearbeiten) für das neue WLAN angezeigt. Auf dieser Seite können Sie verschiedene Parameter speziell für dieses WLAN definieren. Dies umfasst allgemeine Richtlinien, Sicherheitsrichtlinien, QoS-Richtlinien und erweiterte Parameter.
6. Aktivieren Sie unter General Policies (Allgemeine Richtlinien) das Kontrollkästchen **Status**, um das WLAN zu aktivieren.



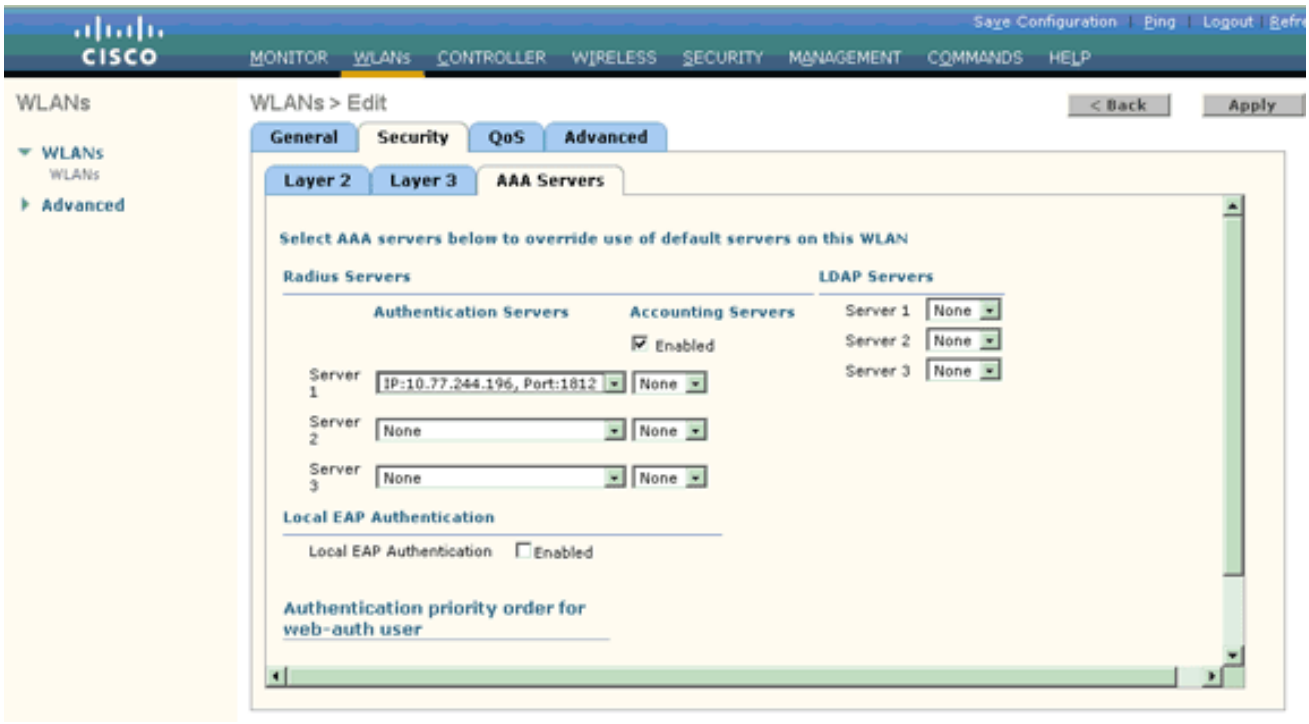
7. Klicken Sie auf die Registerkarte **Sicherheit** und dann auf die Registerkarte **Layer 2**.
8. Wählen Sie **WPA+WPA2** aus der Dropdown-Liste "Layer 2 Security" (Layer 2-Sicherheit) aus.In diesem Schritt wird die WPA-Authentifizierung für das WLAN aktiviert.
9. Aktivieren Sie unter WPA+WPA2-Parameter die Kontrollkästchen **WPA2-Richtlinie** und **AES-Verschlüsselung**.



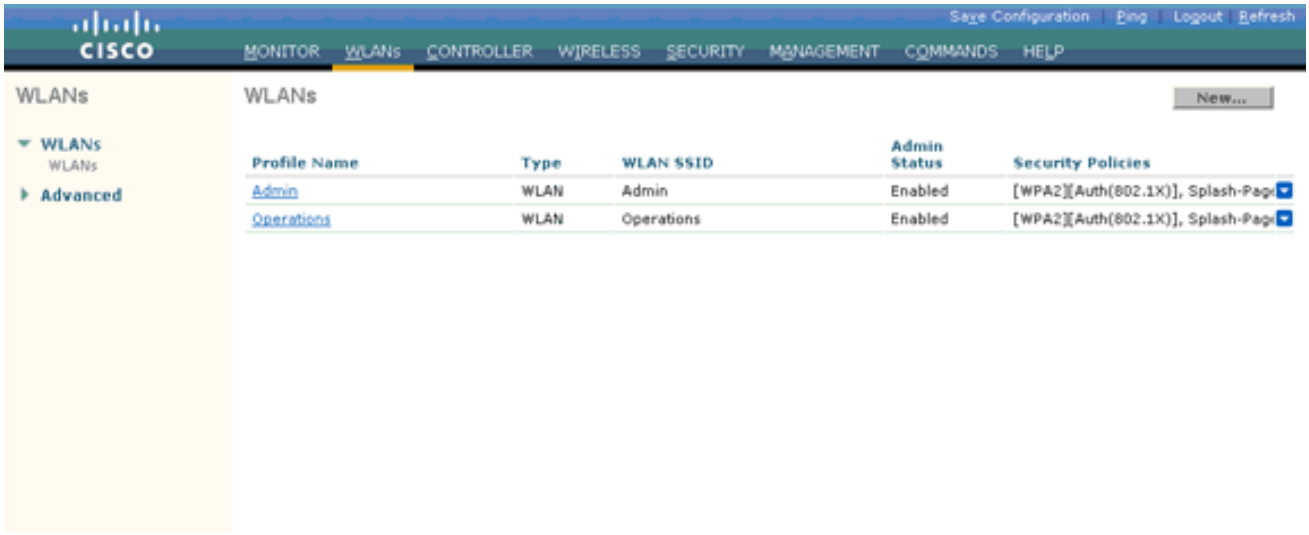
10. Wählen Sie **802.1x** aus der Dropdown-Liste "Auth Key Mgmt" (Schlüsselverwaltung für Authentifizierung) aus. Diese Option aktiviert WPA2 mit 802.1x/EAP-Authentifizierung und AES-Verschlüsselung für das WLAN.
11. Klicken Sie auf die Registerkarte **"Layer 3 Security"**.
12. Aktivieren Sie das Kontrollkästchen **Webrichtlinie**, und klicken Sie dann auf das Optionsfeld **Splash Page Web Redirect (Webumleitung für Splash-Seite)**.Mit dieser Option wird die Splash Page Web Redirect-Funktion
aktiviert.



13. Klicken Sie auf die Registerkarte **AAA-Server**.
14. Wählen Sie unter Authentication Servers (Authentifizierungsserver) in der Dropdown-Liste Server 1 die entsprechende Server-IP-Adresse
    aus.



    In diesem Beispiel wird 10.77.244.196 als RADIUS-Server verwendet.
15. Klicken Sie auf **Apply** (Anwenden).
16. Wiederholen Sie die Schritte 2 bis 15, um das WLAN für die Betriebsabteilung zu erstellen.Auf der Seite WLANs werden die beiden von Ihnen erstellten WLANs aufgeführt.



Beachten Sie, dass die Sicherheitsrichtlinien die Umleitung der Splash-Seite enthalten.

Schritt 3: Konfigurieren Sie Cisco Secure ACS so, dass die Splash-Seitenumleitungsfunktion unterstützt wird.

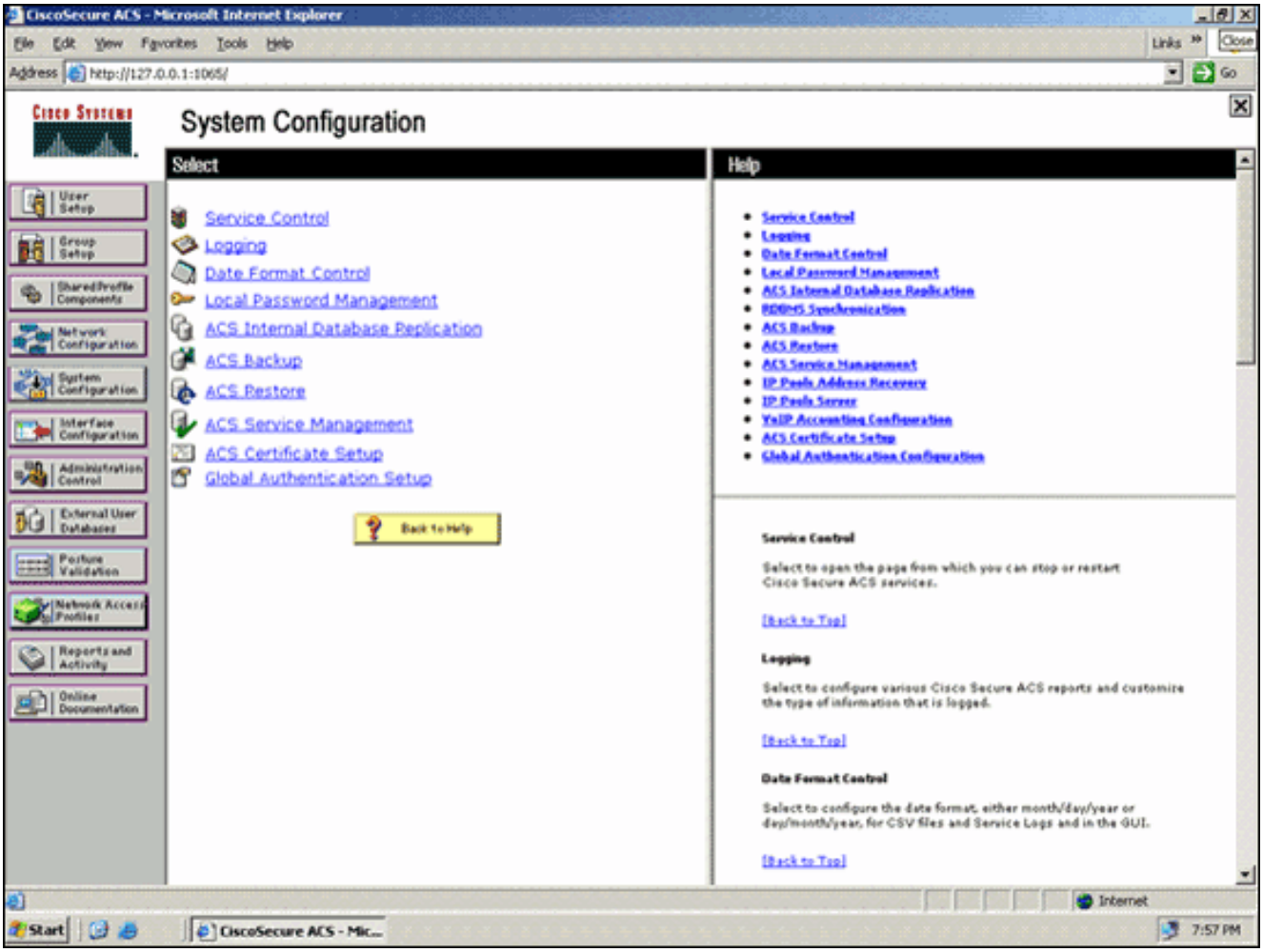
Im nächsten Schritt wird der RADIUS-Server für diese Funktion konfiguriert. Der RADIUS-Server muss eine EAP-FAST-Authentifizierung durchführen, um die Client-Anmeldeinformationen zu validieren und den Benutzer bei erfolgreicher Authentifizierung an die URL (auf dem externen Webserver) umzuleiten, die im Cisco av-pair ***url-redirect***-RADIUS-Attribut angegeben ist.

Konfigurieren von Cisco Secure ACS für die EAP-FAST-Authentifizierung

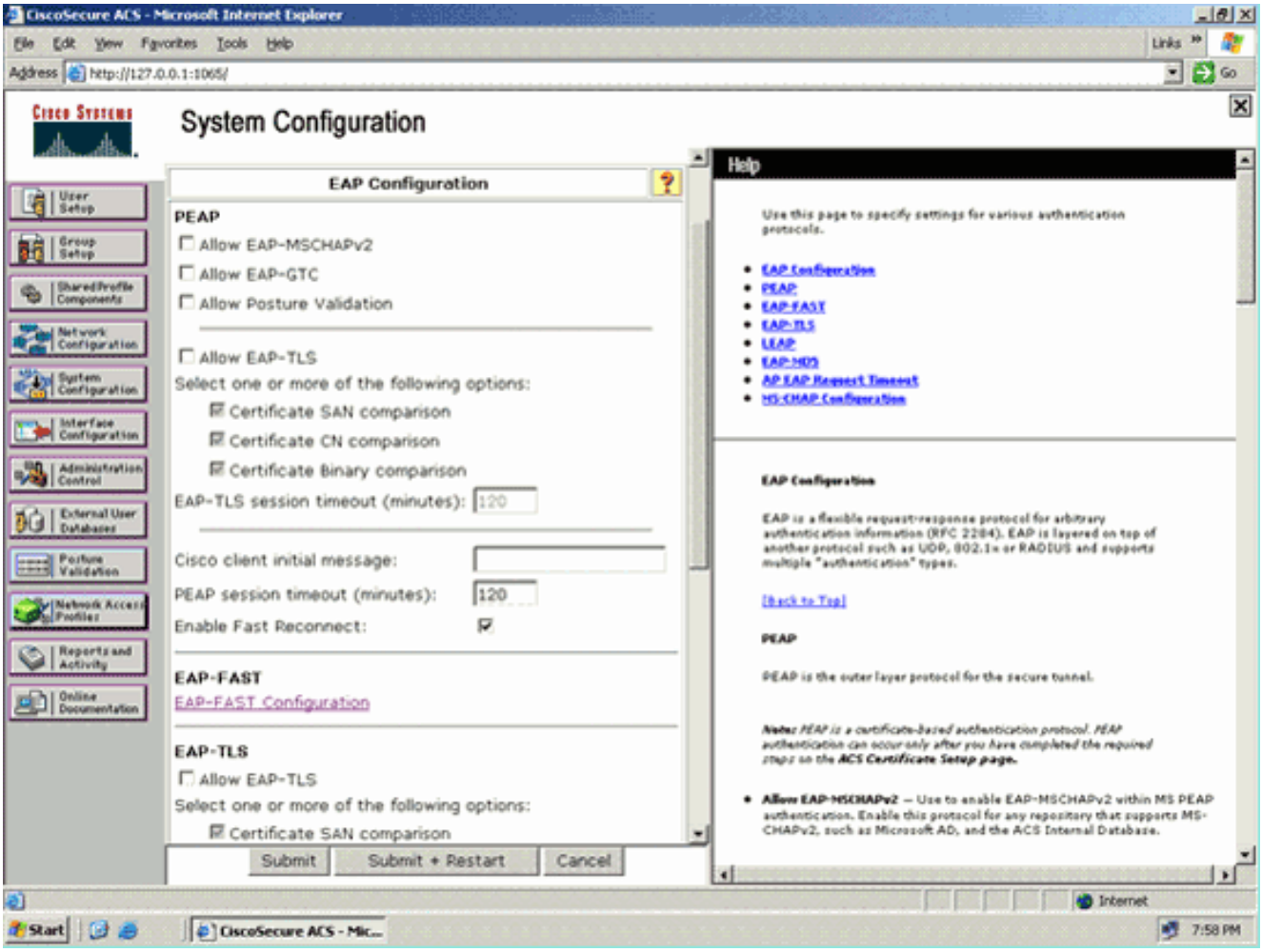
Hinweis: In diesem Dokument wird davon ausgegangen, dass der Wireless LAN Controller dem Cisco Secure ACS als AAA-Client hinzugefügt wurde.

Führen Sie die folgenden Schritte aus, um die EAP-FAST-Authentifizierung auf dem RADIUS-Server zu konfigurieren:

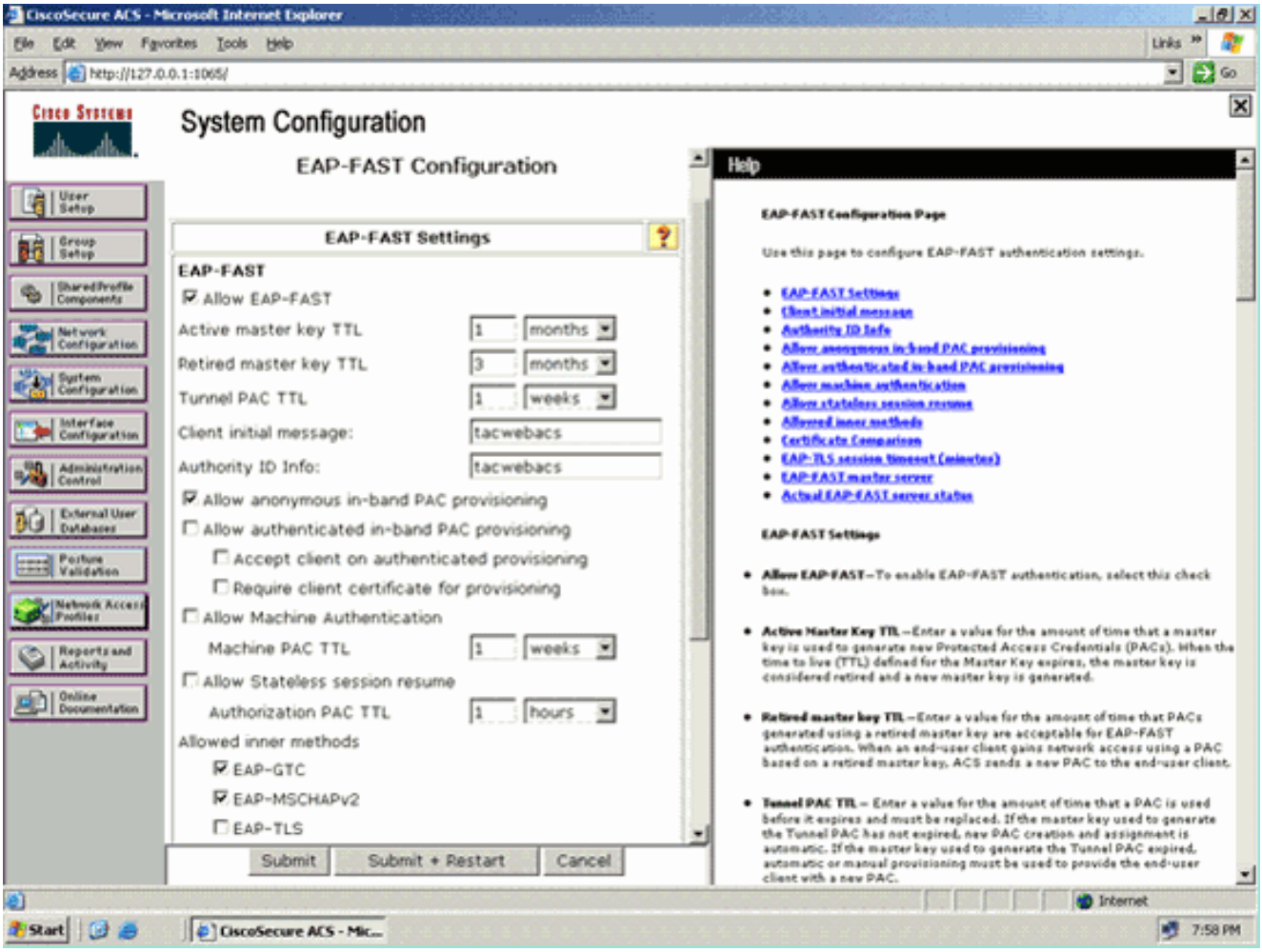
1. Klicken Sie in der RADIUS-Server-GUI auf **Systemkonfiguration**, und wählen Sie dann auf der Seite "Systemkonfiguration" die Option **Globale Authentifizierungseinrichtung** aus.



2. Klicken Sie auf der Seite "Global Authentication" auf **EAP-FAST Configuration**, um zur Seite mit den EAP-FAST-Einstellungen zu gelangen.



3. Aktivieren Sie auf der Seite "EAP-FAST Settings" das Kontrollkästchen **Allow EAP-FAST,** um EAP-FAST auf dem RADIUS-Server zu aktivieren.



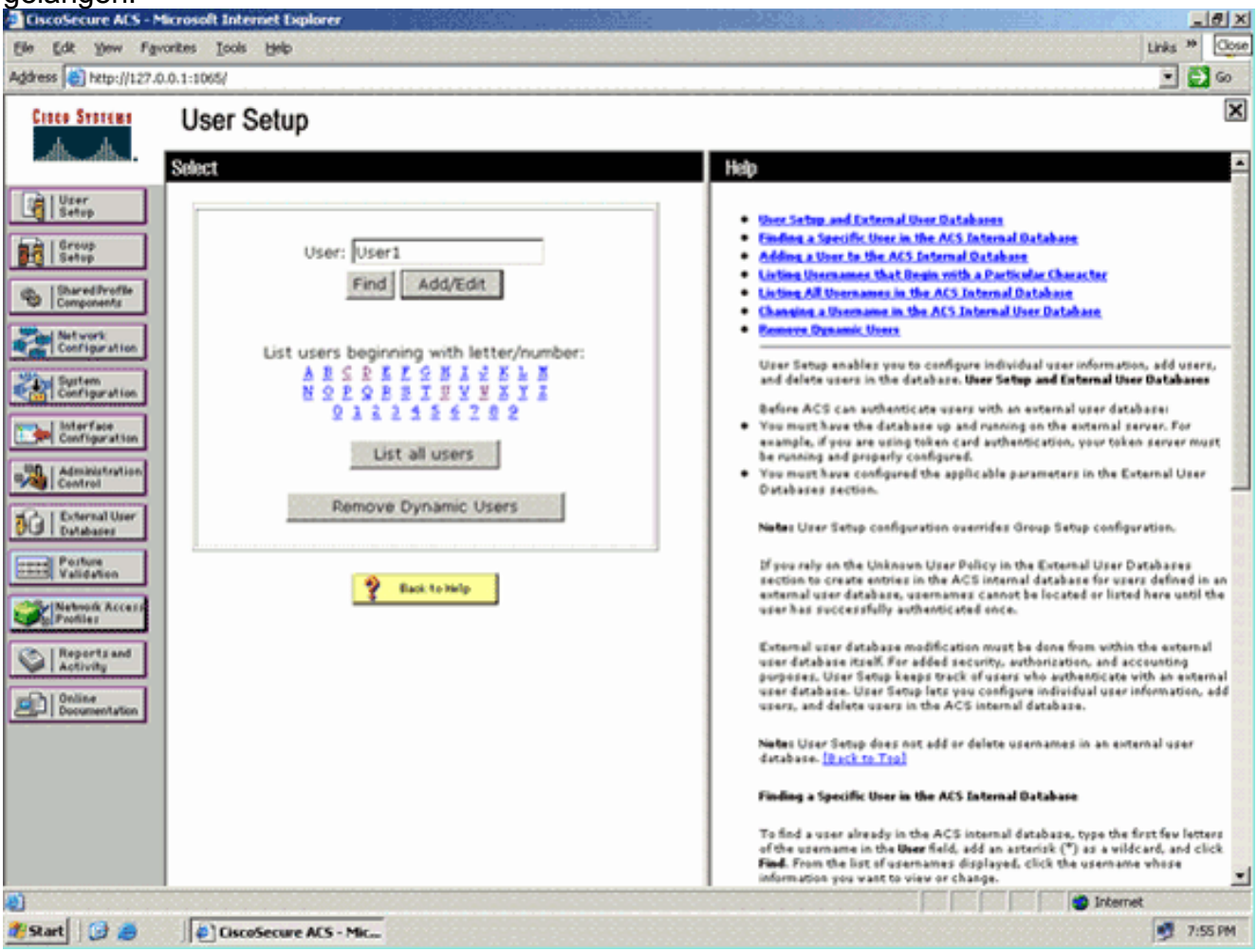
4. Konfigurieren Sie die TTL-Werte (Time-to-Live) des Master-Schlüssels "Aktiv/Abgesetzt" nach Bedarf, oder legen Sie den Standardwert fest, wie in diesem Beispiel gezeigt.Das Feld "Authority ID Info" (Autoritäts-ID-Informationen) stellt die Textidentität dieses ACS-Servers dar, über die ein Endbenutzer bestimmen kann, für welchen ACS-Server die Authentifizierung erfolgen soll. Das Ausfüllen dieses Feldes ist obligatorisch.Das Feld für die anfängliche Client-Anzeige gibt eine Nachricht an, die an Benutzer gesendet werden soll, die sich mit einem EAP-FAST-Client authentifizieren. Die maximale Länge beträgt 40 Zeichen. Die ursprüngliche Nachricht wird dem Benutzer nur angezeigt, wenn der Endbenutzer-Client die Anzeige unterstützt.
5. Wenn der ACS eine anonyme In-Band-PAC-Bereitstellung durchführen soll, aktivieren Sie das Kontrollkästchen **Anonyme In-Band-PAC-Bereitstellung zulassen**.
6. Die Option *Allowed inner methods* legt fest, welche internen EAP-Methoden im EAP-FAST TLS-Tunnel ausgeführt werden können. Für die anonyme In-Band-Bereitstellung müssen Sie EAP-GTC und EAP-MS-CHAP aus Gründen der Abwärtskompatibilität aktivieren. Wenn Sie Anonyme In-Band-PAC-Bereitstellung zulassen auswählen, müssen Sie EAP-MS-CHAP (Phase Null) und EAP-GTC (Phase Zwei) auswählen.
7. Klicken Sie auf **Senden**.**Hinweis:** Detaillierte Informationen und Beispiele zur Konfiguration von EAP FAST mit anonymer In-Band-PAC-Bereitstellung und authentifizierter In-Band-Bereitstellung finden Sie unter Konfigurationsbeispiel für EAP-FAST-Authentifizierung mit Wireless LAN-Controllern und externen RADIUS-Servern.

Konfigurieren Sie die Benutzerdatenbank und definieren Sie das RADIUS-Attribut *url-redirect.*

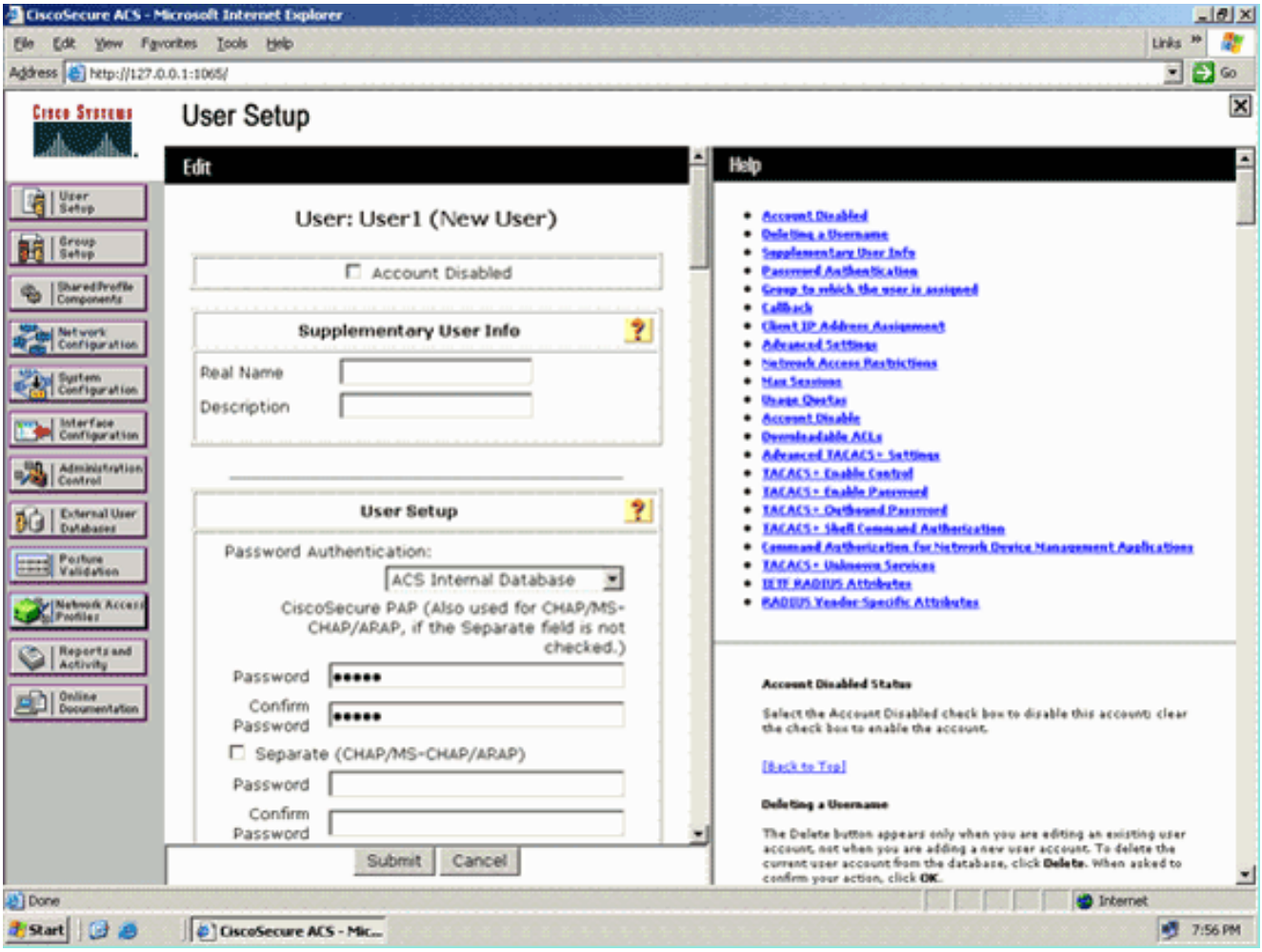
In diesem Beispiel werden der Benutzername und das Kennwort des Wireless-Clients als User1 bzw. User1 konfiguriert.

Gehen Sie wie folgt vor, um eine Benutzerdatenbank zu erstellen:

1. Wählen Sie in der Navigationsleiste in der ACS-GUI die Option **User Setup (Benutzereinrichtung)**.
2. Erstellen Sie einen neuen Wireless-Benutzer, und klicken Sie dann auf **Hinzufügen/Bearbeiten**, um zur Bearbeitungsseite dieses Benutzers zu gelangen.



3. Konfigurieren Sie auf der Seite zur Bearbeitung der Benutzereinrichtung den Namen und die Beschreibung sowie die Kennworteinstellungen, wie in diesem Beispiel gezeigt.In diesem Dokument wird die interne ACS-Datenbank für die Kennwortauthentifizierung verwendet.



4. Blättern Sie auf der Seite nach unten, um die RADIUS-Attribute zu ändern.
5. Aktivieren Sie das Kontrollkästchen **[009\001] cisco-av-pair**.
6. Geben Sie diese Cisco av-pairs im [009\001] cisco-av-pair-Bearbeitungsfeld ein, um die URL anzugeben, an die der Benutzer umgeleitet wird:url-redirect=http://10.77.244.196/Admin-Login.html

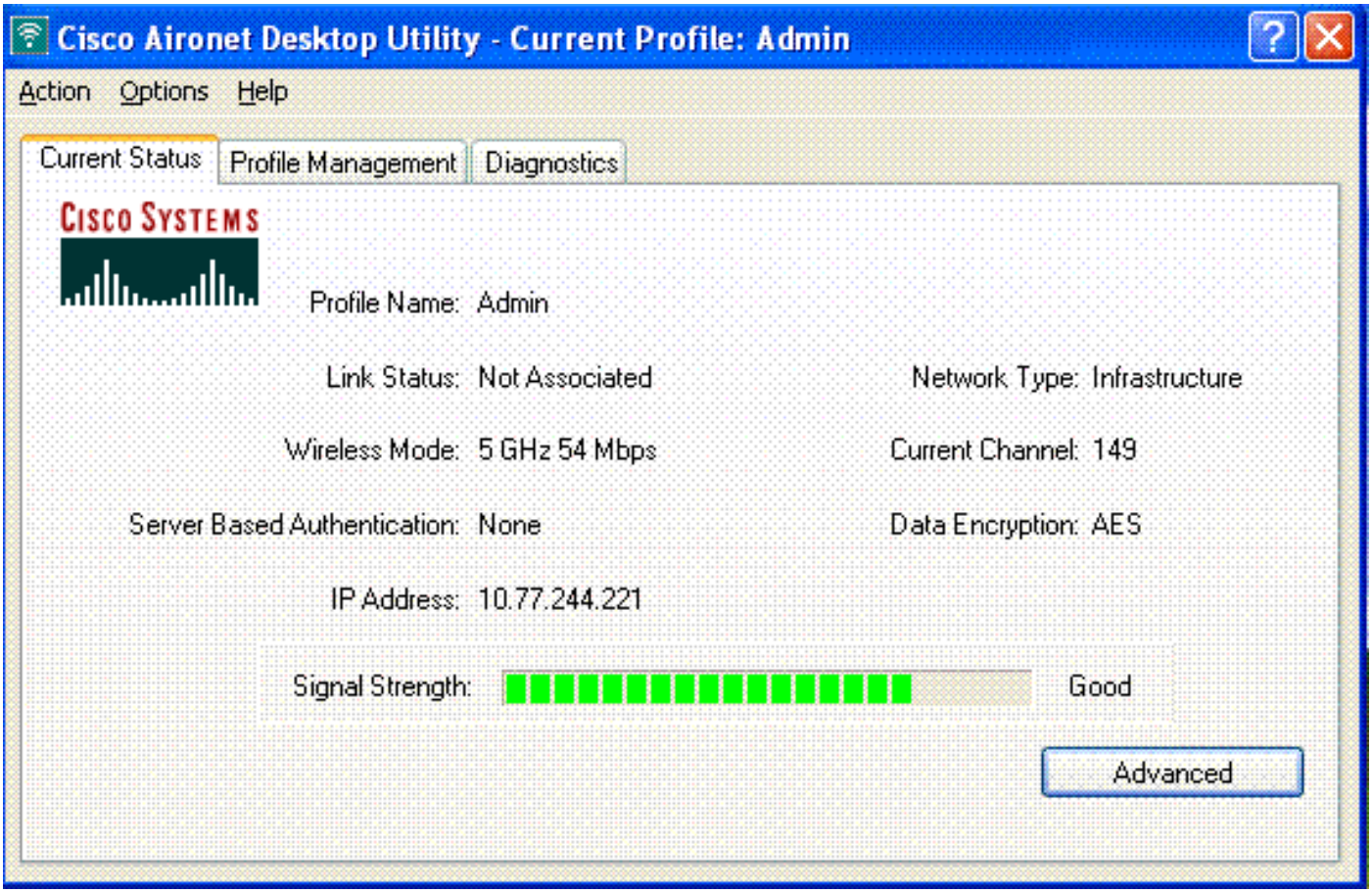
Dies ist die Homepage der Benutzer der Administratorabteilung.

7. Klicken Sie auf **Senden**.
8. Wiederholen Sie dieses Verfahren, um Benutzer 2 (Betriebsabteilung) hinzuzufügen.
9. Wiederholen Sie die Schritte 1 bis 6, um der Datenbank weitere Benutzer der Admin-Abteilung und der Operations-Abteilung hinzuzufügen.**Hinweis:** Die RADIUS-Attribute können auf Benutzer- oder Gruppenebene in Cisco Secure ACS konfiguriert werden.

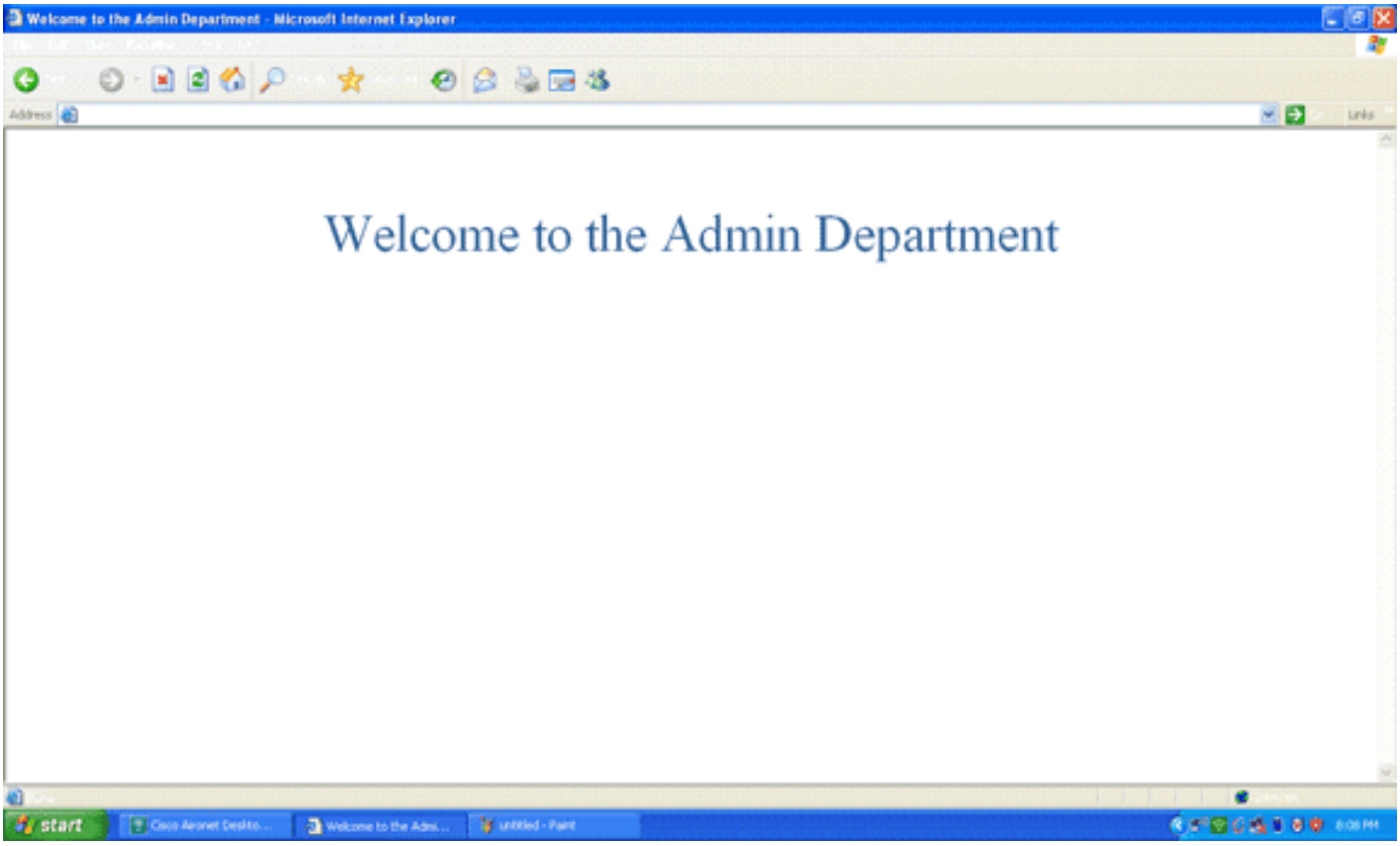
Überprüfung

Um die Konfiguration zu überprüfen, verbinden Sie einen WLAN-Client der Admin- und der Betriebsabteilung mit den entsprechenden WLANs.

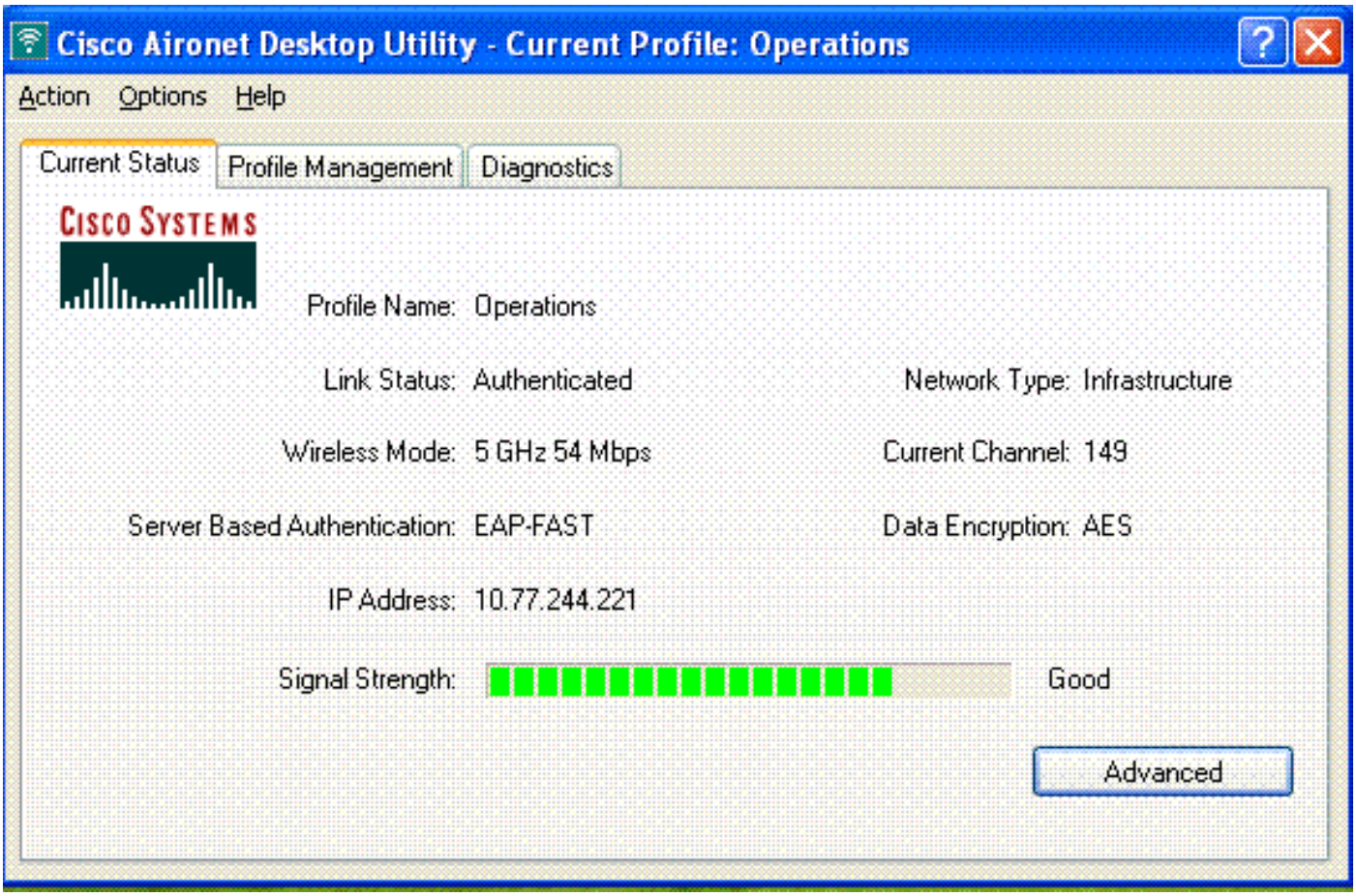
Wenn ein Benutzer der Admin-Abteilung eine Verbindung zum Wireless LAN-Administrator herstellt, wird dieser zur Eingabe von 802.1x-Anmeldedaten aufgefordert (in unserem Fall EAP-FAST-Anmeldedaten). Sobald der Benutzer die Anmeldedaten eingegeben hat, übergibt der WLC diese an den Cisco Secure ACS Server. Der Cisco Secure ACS-Server überprüft die Anmeldeinformationen des Benutzers anhand der Datenbank und gibt bei erfolgreicher Authentifizierung das url-redirect-Attribut an den Wireless LAN Controller zurück. Die Authentifizierung ist zu diesem Zeitpunkt abgeschlossen.

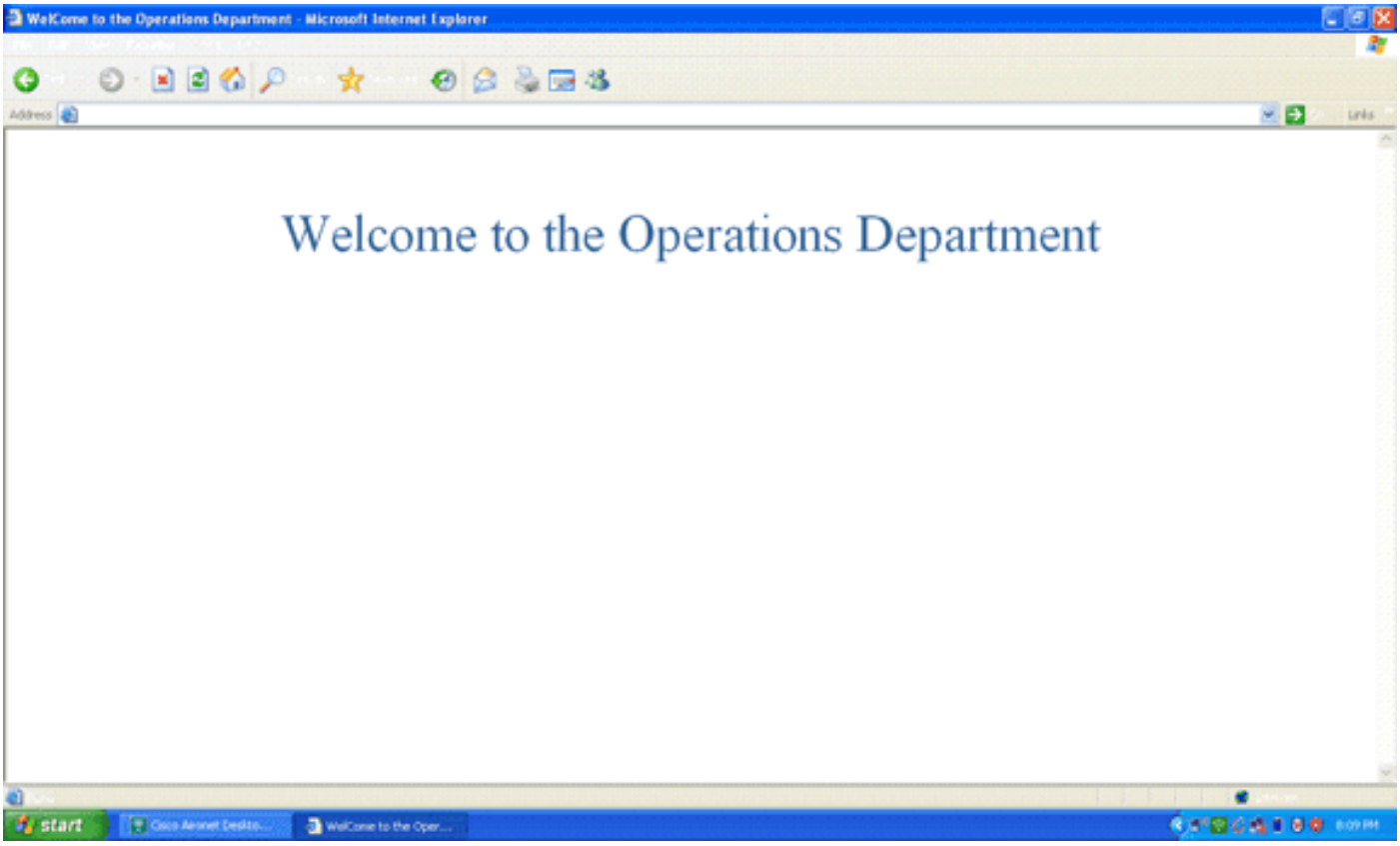


Wenn der Benutzer einen Webbrowser öffnet, wird er zur Homepage-URL der Admin-Abteilung umgeleitet. (Diese URL wird über das cisco-av-pair-Attribut an den WLC zurückgegeben.) Nach der Umleitung hat der Benutzer vollen Zugriff auf das Netzwerk. Hier sind die Screenshots:



Die gleichen Ereignisfolgen treten auf, wenn ein Benutzer der Betriebsabteilung eine Verbindung zum WLAN-Betrieb herstellt.





Fehlerbehebung

In diesem Abschnitt finden Sie Informationen zur Behebung von Fehlern in Ihrer Konfiguration.

Hinweis: Lesen Sie Wichtige Informationen zu Debug-Befehlen, bevor Sie **Debug-**Befehle verwenden.

Sie können die folgenden Befehle verwenden, um Fehler in Ihrer Konfiguration zu beheben.

- **show wlan wlan_id**: Zeigt den Status der Webumleitungsfunktionen für ein bestimmtes WLAN an.Hier ein Beispiel:

```
WLAN Identifier.................................. 1
Profile Name..................................... Admin
Network Name (SSID).............................. Admin
...
Web Based Authentication......................... Disabled
Web-Passthrough.................................. Disabled
Conditional Web Redirect......................... Disabled
Splash-Page Web Redirect......................... Enabled
```

- **debug dot1x events enable**: Aktiviert das Debuggen von 802.1x-Paketnachrichten.Hier ein Beispiel:

```
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Sending EAP Request from AAA to
    mobile 00:40:96:ac:dd:05 (EAP Id 16)
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Received EAPOL EAPPKT from
    mobile 00:40:96:ac:dd:05
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Received EAP Response from
    mobile 00:40:96:ac:dd:05 (EAP Id 16, EAP Type 43)
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Processing Access-Challenge for
    mobile 00:40:96:ac:dd:05
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Setting re-auth timeout to 1800
    seconds, got from WLAN config.
```

```
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Station 00:40:96:ac:dd:05
    setting dot1x reauth timeout = 1800
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Creating a new PMK Cache Entry
    for station 00:40:96:ac:dd:05 (RSN 2)
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Adding BSSID 00:1c:58:05:e9:cf
    to PMKID cache for station 00:40:96:ac:dd:05
Fri Feb 29 10:27:16 2008: New PMKID: (16)
Fri Feb 29 10:27:16 2008:      [0000] 79 ee 88 78 9c 71 41 f0 10 7d 31 ca
    fb fa 8e 3c
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Disabling re-auth since PMK
    lifetime can take care of same.
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Sending EAP-Success to mobile
    00:40:96:ac:dd:05 (EAP Id 17)
Fri Feb 29 10:27:16 2008: Including PMKID in M1  (16)
Fri Feb 29 10:27:16 2008:      [0000] 79 ee 88 78 9c 71 41 f0 10 7d 31 ca
    fb fa 8e 3c
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Sending EAPOL-Key Message to
    mobile 00:40:96:ac:dd:05
    state INITPMK (message 1), replay counter 00.00.00.00.00.00.00.00
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Received Auth Success while
    in Authenticating state for mobile 00:40:96:ac:dd:05
```

- **debug aaa events enable** - Aktiviert die Debug-Ausgabe aller aaa-Ereignisse.Hier ein Beispiel:

```
Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Successful transmission of
    Authentication Packet (id 103) to 10.77.244.196:1812, proxy state
    00:40:96:ac:dd:05-00:00
Thu Feb 28 07:55:18 2008: ****Enter processIncomingMessages: response code=11
Thu Feb 28 07:55:18 2008: ****Enter processRadiusResponse: response code=11
Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Access-Challenge received from
    RADIUS server 10.77.244.196 for mobile 00:40:96:ac:dd:05 receiveId = 3
Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Successful transmission of
    Authentication Packet (id 104) to 10.77.244.196:1812, proxy state
    00:40:96:ac:dd:05-00:00
Thu Feb 28 07:55:18 2008: ****Enter processIncomingMessages: response code=2
Thu Feb 28 07:55:18 2008: ****Enter processRadiusResponse: response code=2
Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Access-Accept received from
    RADIUS server 10.77.244.196 for mobile 00:40:96:ac:dd:05 receiveId = 3
Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 AAA Override Url-Redirect
    'http://10.77.244.196/Admin-login.html' set
Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Applying new AAA override for
    station 00:40:96:ac:dd:05
Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Override values for station
    00:40:96:ac:dd:05
       source: 4, valid bits: 0x0
       qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1
       dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
       vlanIfName: '', aclName: '
```

Zugehörige Informationen

- Cisco Wireless LAN Controller Configuration Guide, Release 5.0
- Konfigurationsbeispiel für Web-Authentifizierung des Wireless LAN-Controllers
- Konfigurationsbeispiel für externe Web-Authentifizierung mit Wireless LAN-Controllern
- Seite zur Wireless-Unterstützung
- 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.