Authentifizierung des Lobby-Administrators des Wireless LAN-Controllers über den RADIUS-Server

Inhalt

Einführung

In diesem Dokument werden die Konfigurationsschritte für die Authentifizierung eines Lobby-Administrators des WLAN-Controllers (WLC) bei einem RADIUS-Server beschrieben.

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass Sie diese Anforderungen erfüllen, bevor Sie versuchen, diese Konfiguration durchzuführen:

- Kenntnisse zum Konfigurieren von Eckparametern auf WLCs
- Kenntnisse zum Konfigurieren eines RADIUS-Servers, z. B. des Cisco Secure ACS
- Kenntnis der Gastbenutzer im WLC

Verwendete Komponenten

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

- Cisco 4400 Wireless LAN Controller mit Version 7.0.216.0
- Ein Cisco Secure ACS, der die Softwareversion 4.1 ausführt und in dieser Konfiguration als RADIUS-Server verwendet wird.

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

Ein Lobby-Administrator, auch als Lobby-Botschafter eines WLC bezeichnet, kann Gastbenutzerkonten auf dem Wireless LAN Controller (WLC) erstellen und verwalten. Der Botschafter der Lobby verfügt über eingeschränkte Konfigurationsberechtigungen und kann nur auf die Webseiten zugreifen, die zur Verwaltung der Gastkonten verwendet werden. Der Botschafter der Lobby kann angeben, wie lange die Gastbenutzer noch aktiv sind. Nach Ablauf der angegebenen Zeit laufen die Gastbenutzerkonten automatisch ab.

Weitere Informationen finden Sie im Bereitstellungsleitfaden: Cisco Guest Access Using the Cisco Wireless LAN Controller for more information on guest users.

Um ein Gastbenutzerkonto auf dem WLC zu erstellen, müssen Sie sich als Lobby-Administrator beim Controller anmelden. In diesem Dokument wird erläutert, wie ein Benutzer anhand der vom RADIUS-Server zurückgegebenen Attribute im WLC als Lobby-Administrator authentifiziert wird.

Hinweis: Die Lobby-Administrator-Authentifizierung kann auch basierend auf dem Lobby-Administratorkonto durchgeführt werden, das lokal auf dem WLC konfiguriert wurde. Unter Erstellen eines Lobby-Botschafterkontos finden Sie Informationen zum lokalen Erstellen eines Lobby-Administratorkontos für einen Controller.

Konfiguration

In diesem Abschnitt finden Sie Informationen zur Konfiguration des WLC und des Cisco Secure ACS für den in diesem Dokument beschriebenen Zweck.

Konfigurationen

In diesem Dokument werden folgende Konfigurationen verwendet:

- Die IP-Adresse der Verwaltungsschnittstelle für WLC lautet 10.77.244.212/27.
- Die IP-Adresse des RADIUS-Servers lautet 10.77.244.197/27.
- Der gemeinsam genutzte geheime Schlüssel, der auf dem Access Point (AP) und dem RADIUS-Server verwendet wird, lautet cisco123.
- Der im RADIUS-Server konfigurierte Benutzername und das Kennwort des Lobby-Administrators sind lobbyadmin.

Im Konfigurationsbeispiel dieses Dokuments wird jedem Benutzer, der sich mit Benutzername und Kennwort als lobbyadmin beim Controller anmeldet, die Rolle eines Lobby-Administrators zugewiesen.

WLC-Konfiguration

Bevor Sie die erforderliche WLC-Konfiguration starten, stellen Sie sicher, dass der Controller Version 4.0.206.0 oder höher ausführt. Dies liegt an der Cisco Bug ID CSCsg89868 (nur registrierte Kunden), in der die Webschnittstelle des Controllers falsche Webseiten für den LobbyAdmin-Benutzer anzeigt, wenn der Benutzername in einer RADIUS-Datenbank gespeichert ist. In der LobbyAdmin wird anstelle der LobbyAdmin-Schnittstelle die ReadOnly-Schnittstelle angezeigt.

Dieser Fehler wurde in WLC Version 4.0.206.0 behoben. Stellen Sie deshalb sicher, dass die Controller-Version 4.0.206.0 oder höher ist. Informationen zur Aktualisierung des Controllers auf die entsprechende Version finden Sie unter WLC-Software-Upgrade (Wireless LAN Controller).

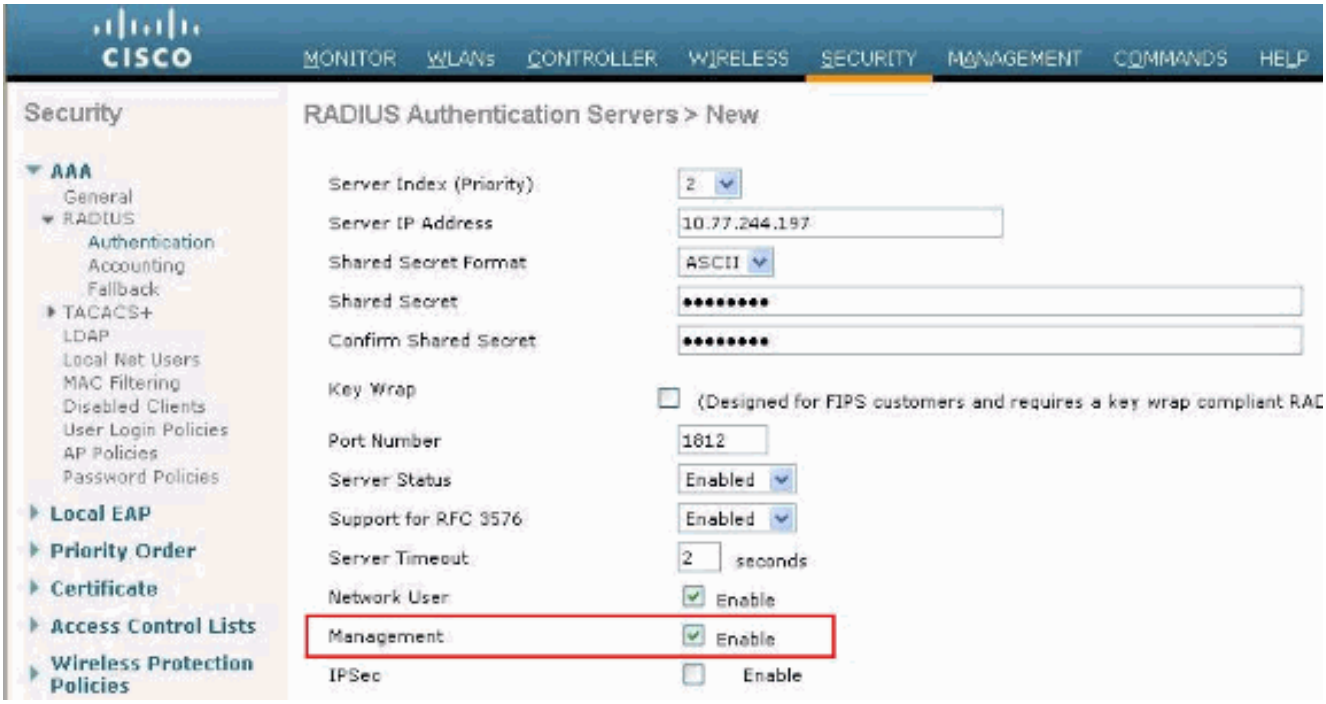
Um eine Controller-Verwaltungsauthentifizierung mit dem RADIUS-Server durchzuführen, stellen Sie sicher, dass das **Admin-auth-via-RADIUS-**Flag auf dem Controller aktiviert ist. Dies kann mithilfe der Befehlsausgabe **show radius summary** überprüft werden.

Der erste Schritt besteht in der Konfiguration der RADIUS-Serverinformationen auf dem Controller und der Einrichtung der Layer-3-Erreichbarkeit zwischen dem Controller und dem RADIUS-Server.

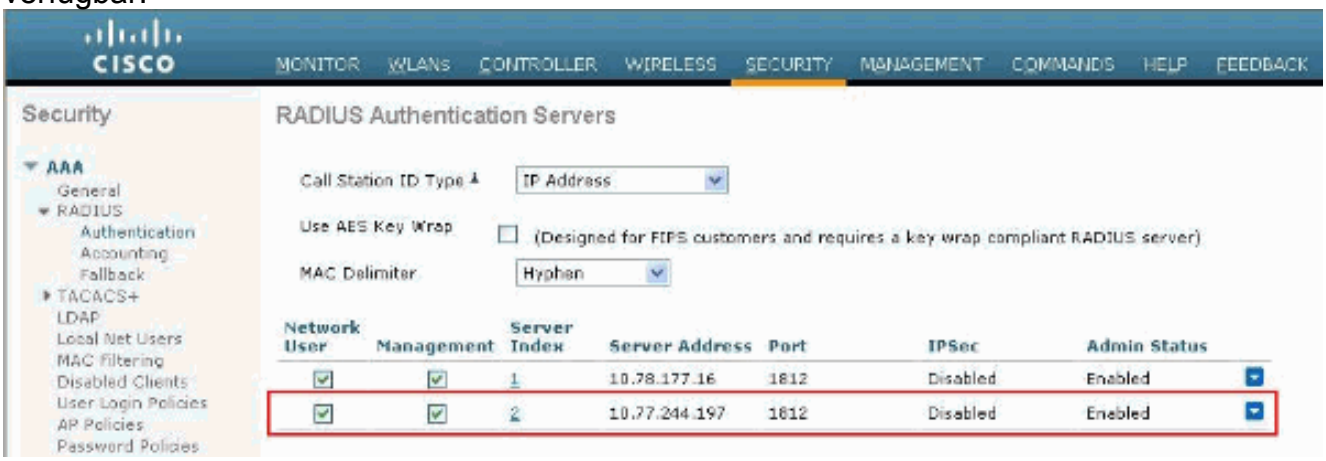
Konfigurieren der RADIUS-Serverinformationen auf dem Controller

Gehen Sie wie folgt vor, um den WLC mit Details zum ACS zu konfigurieren:

1. Wählen Sie in der WLC-GUI die Registerkarte **Security (Sicherheit)** aus, und konfigurieren Sie die IP-Adresse und den gemeinsamen geheimen Schlüssel des ACS-Servers.Dieser gemeinsame geheime Schlüssel muss auf dem ACS identisch sein, damit der WLC mit dem ACS kommunizieren kann.**Hinweis:** Beim gemeinsamen geheimen ACS wird die Groß- und Kleinschreibung beachtet. Stellen Sie deshalb sicher, dass Sie die freigegebenen geheimen Informationen korrekt eingeben.Diese Abbildung zeigt ein
   Beispiel:



2. Aktivieren Sie das Kontrollkästchen **Management**, um dem ACS die Verwaltung der WLC-Benutzer zu ermöglichen, wie in der Abbildung in Schritt 1 gezeigt. Klicken Sie anschließend auf **Übernehmen**.
3. Überprüfen Sie die Layer-3-Erreichbarkeit zwischen dem Controller und dem konfigurierten RADIUS-Server mithilfe des **Ping**-Befehls. Diese Ping-Option ist auch auf der konfigurierten RADIUS-Serverseite in der WLC-GUI der Registerkarte **Security>RADIUS Authentication** (**Sicherheit > RADIUS-Authentifizierung**) verfügbar.Dieses Diagramm zeigt eine erfolgreiche Ping-Antwort vom RADIUS-Server. Daher ist die Layer-3-Erreichbarkeit zwischen dem Controller und dem RADIUS-Server verfügbar.



RADIUS-Serverkonfiguration

Gehen Sie wie in diesen Abschnitten beschrieben vor, um den RADIUS-Server zu konfigurieren:

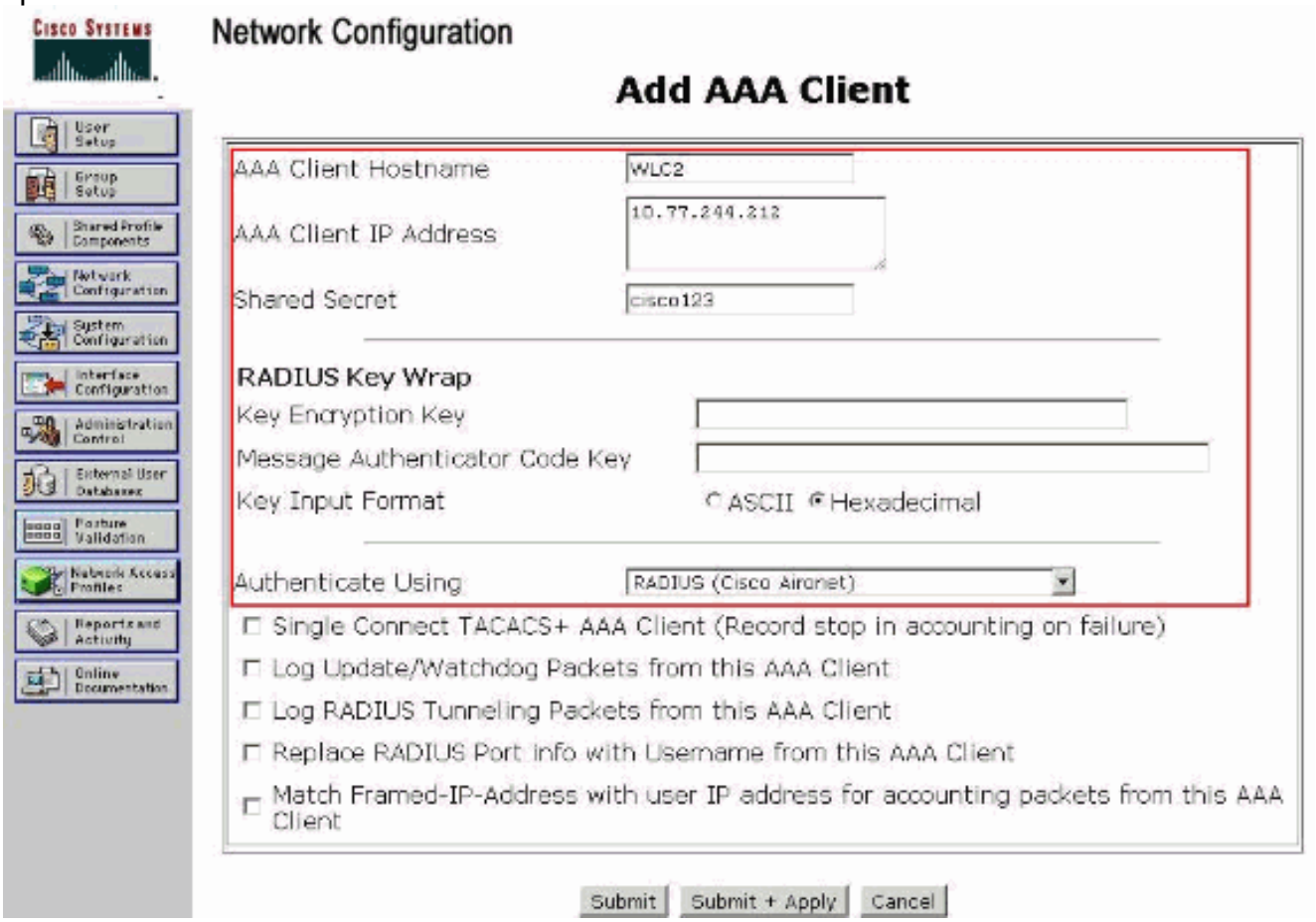
1. Hinzufügen des WLC als AAA-Client zum RADIUS-Server
2. Konfigurieren des entsprechenden RADIUS IETF-Diensttypattributs für einen Lobby-Administrator

Hinzufügen des WLC als AAA-Client zum RADIUS-Server

Führen Sie diese Schritte aus, um den WLC als AAA-Client im RADIUS-Server hinzuzufügen. Wie bereits erwähnt, verwendet dieses Dokument den ACS als RADIUS-Server. Sie können für diese Konfiguration einen beliebigen RADIUS-Server verwenden.

Gehen Sie wie folgt vor, um den WLC als AAA-Client im ACS hinzuzufügen:

1. Wählen Sie in der ACS-GUI die Registerkarte **Network Configuration (Netzwerkkonfiguration)** aus.
2. Klicken Sie unter AAA-Clients auf **Eintrag hinzufügen**.
3. Geben Sie im Fenster Add AAA Client (AAA-Client hinzufügen) den WLC-Hostnamen, die IP-Adresse des WLC und einen gemeinsamen geheimen Schlüssel ein. Siehe Beispieldiagramm unter Schritt 5.
4. Wählen Sie im Dropdown-Menü Authenticate Using (Authentifizierung über Verwendung) die Option **RADIUS (Cisco Aironet)** aus.
5. Klicken Sie auf **Senden + Neu starten**, um die Konfiguration zu speichern.

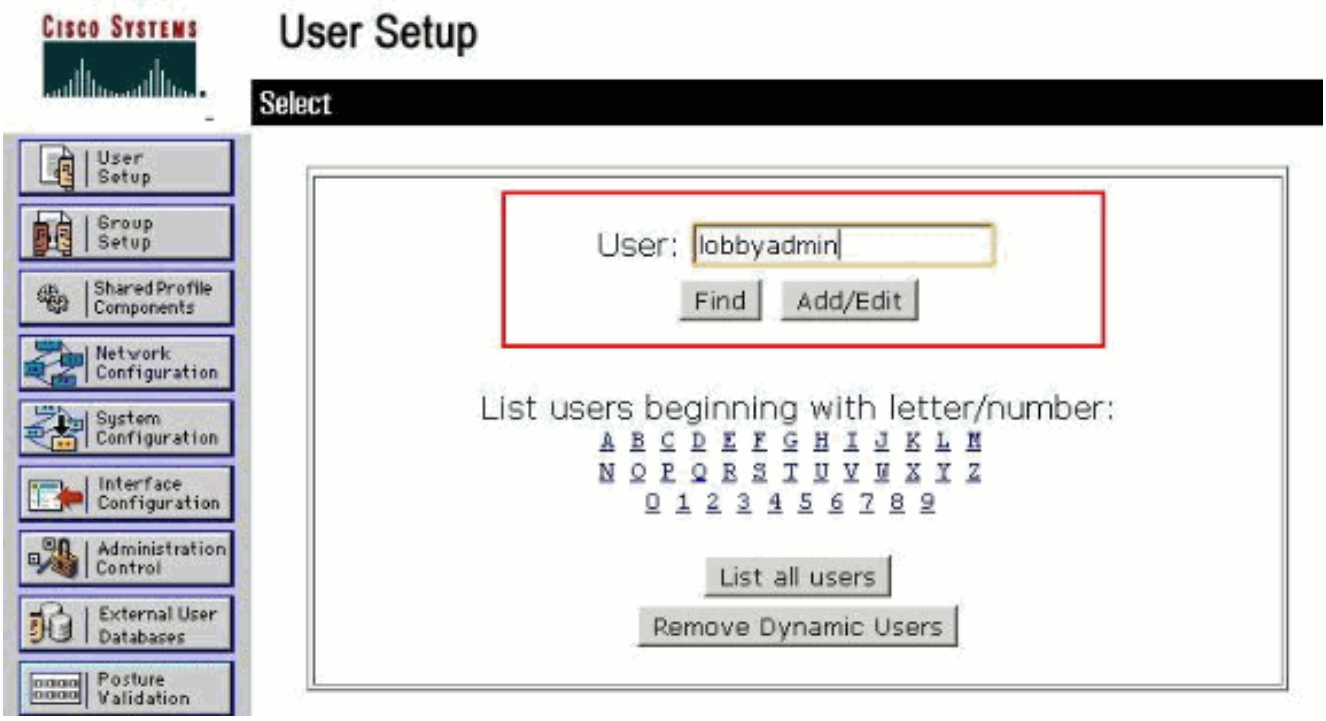


Konfigurieren des entsprechenden RADIUS IETF-Diensttypattributs für einen Lobby-Administrator

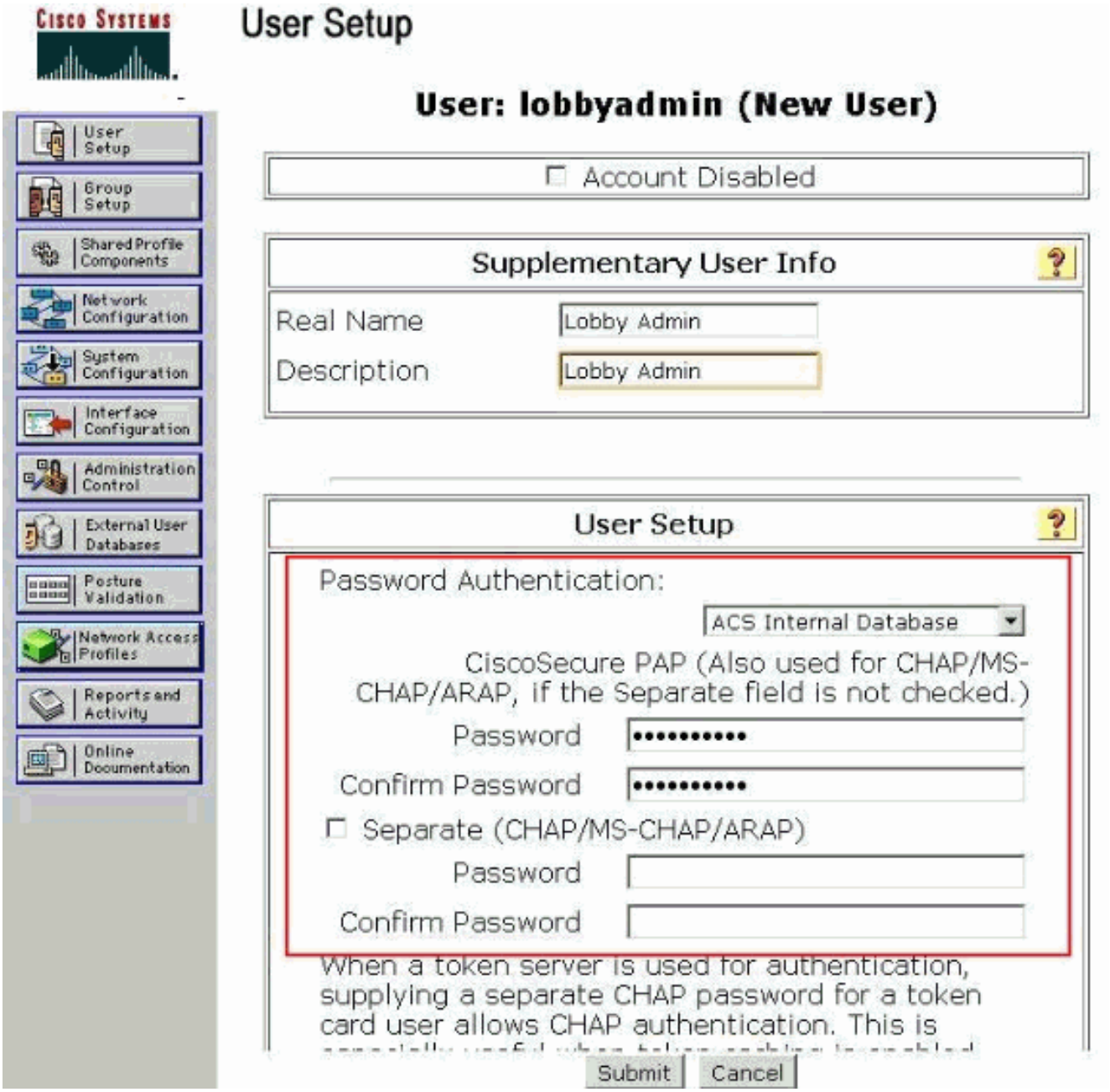
Um einen Verwaltungsbenutzer eines Controllers als Lobbyadministrator über den RADIUS-Server zu authentifizieren, müssen Sie den Benutzer der RADIUS-Datenbank hinzufügen, wobei das IETF RADIUS Service Type-Attribut auf **Callback Administrative** festgelegt ist. Dieses Attribut weist dem bestimmten Benutzer die Rolle eines Lobby-Administrators auf einem Controller zu.

Dieses Dokument zeigt das Beispiel "user lobbyadmin" als Lobby-Administrator. Gehen Sie wie folgt vor, um diesen Benutzer im ACS zu konfigurieren:

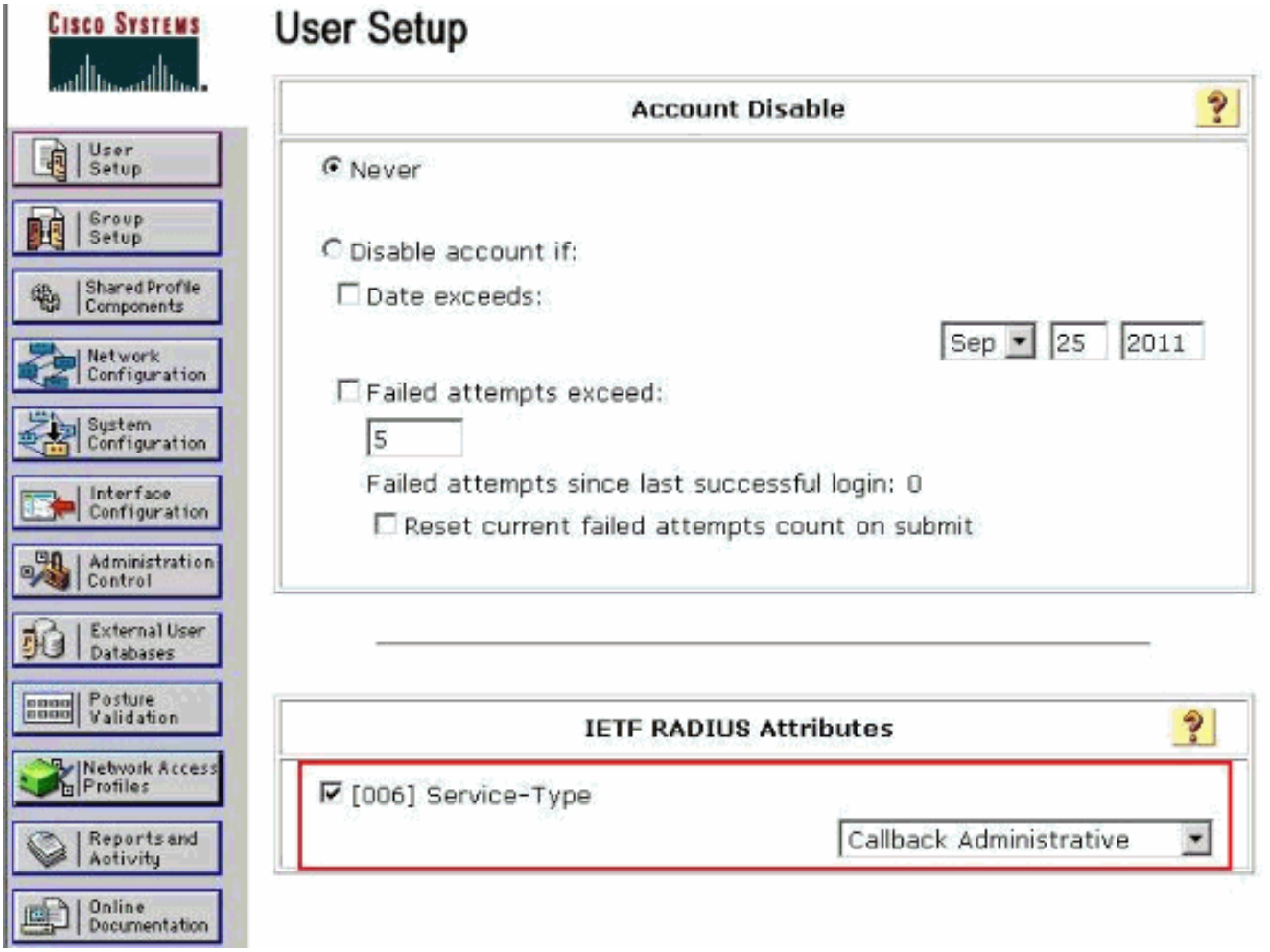
1. Wählen Sie in der ACS-GUI die Registerkarte **User Setup (Benutzereinrichtung)** aus.
2. Geben Sie den dem ACS hinzuzufügenden Benutzernamen ein, wie in diesem Beispielfenster
   gezeigt:



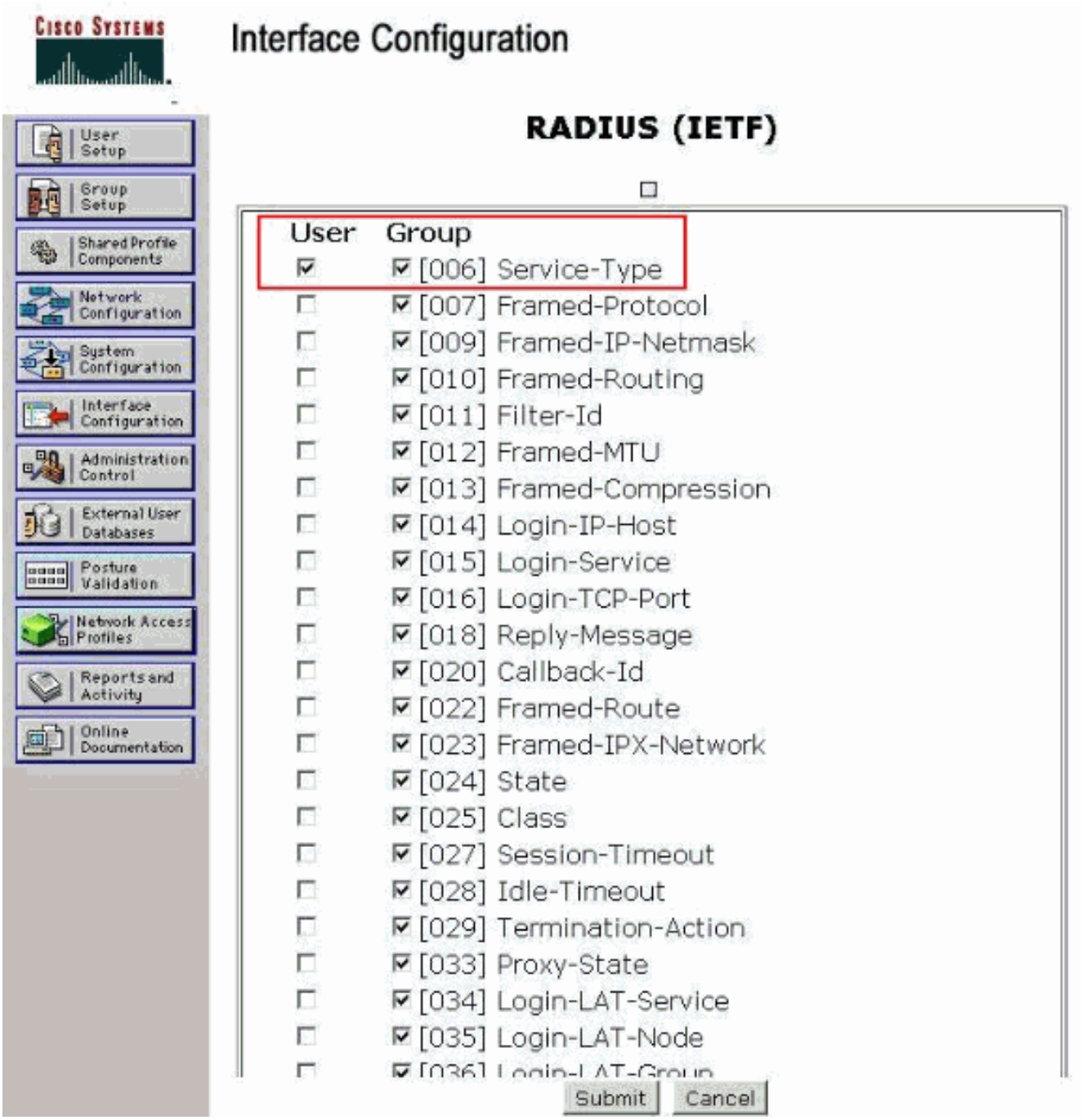
3. Klicken Sie auf **Hinzufügen/Bearbeiten**, um zur Seite Benutzerbearbeitung zu gelangen.
4. Geben Sie auf der Seite User Edit (Benutzerbearbeitung) die Details für den echten Namen, die Beschreibung und das Kennwort dieses Benutzers an.In diesem Beispiel werden Benutzername und Kennwort sowohl lobbyadmin
   verwendet.



5. Scrollen Sie nach unten zur IETF RADIUS Attributes-Einstellung, und aktivieren Sie das Kontrollkästchen **Service-Type Attribute**.
6. Wählen Sie im Dropdown-Menü "Servicetyp" die Option **Callback Administrative** aus, und klicken Sie auf **Submit (Senden)**.Dieses Attribut weist diesem Benutzer die Rolle eines Lobby-Administrators
   zu.



In manchen Fällen ist dieses Service-Type-Attribut unter den Benutzereinstellungen nicht sichtbar. Führen Sie in solchen Fällen die folgenden Schritte aus, um sie sichtbar zu machen:Wählen Sie in der ACS-GUI **Interface Configuration > RADIUS (IETF)**, um IETF-Attribute im Fenster User Configuration (Benutzerkonfiguration) zu aktivieren.Dadurch gelangen Sie zur Seite RADIUS (IETF) Settings (RADIUS-Einstellungen).Auf der Seite RADIUS (IETF) Settings (RADIUS (IETF)-Einstellungen) können Sie das IETF-Attribut aktivieren, das unter Benutzer- oder Gruppeneinstellungen sichtbar sein muss. Aktivieren Sie für diese Konfiguration die Option **Service-Type** für die Spalte User (Benutzer), und klicken Sie auf **Submit (Senden)**.Dieses Fenster zeigt ein
Beispiel:



Hinweis: In diesem Beispiel wird die Authentifizierung auf Benutzerbasis angegeben. Sie können auch eine Authentifizierung anhand der Gruppe durchführen, der ein bestimmter Benutzer angehört. Aktivieren Sie in diesem Fall das Kontrollkästchen **Gruppe**, damit dieses Attribut unter Gruppeneinstellungen angezeigt wird.**Hinweis:** Wenn die Authentifizierung auf Gruppenbasis erfolgt, müssen Sie Benutzer einer bestimmten Gruppe zuweisen und die IETF-Attribute für Gruppeneinstellungen konfigurieren, um Benutzern dieser Gruppe Zugriffsberechtigungen zur Verfügung zu stellen. Weitere Informationen zum Konfigurieren und Verwalten von Gruppen finden Sie unter Benutzergruppenverwaltung.

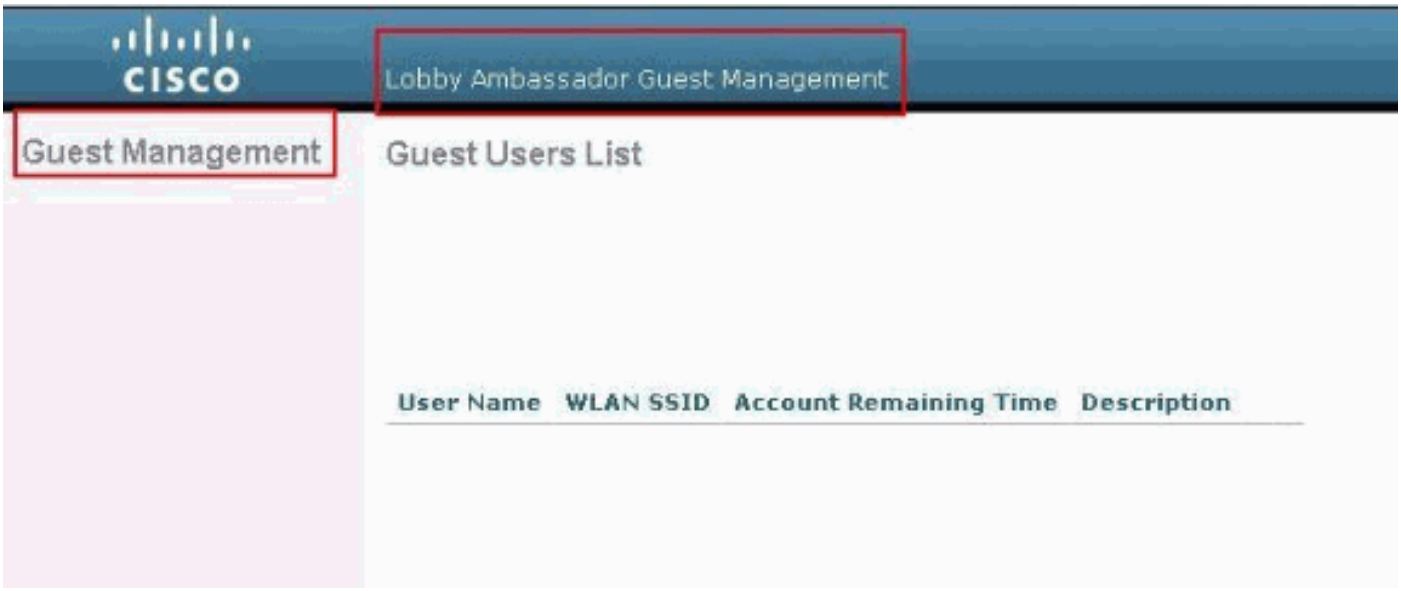
Überprüfung

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert, greifen Sie über den GUI-Modus (HTTP/HTTPS) auf den WLC zu.

Hinweis: Ein Lobby-Botschafter kann nicht auf die CLI-Schnittstelle des Controllers zugreifen und daher nur über die GUI des Controllers Gastbenutzerkonten erstellen.

Wenn die Anmeldeaufforderung angezeigt wird, geben Sie den Benutzernamen und das Kennwort wie auf dem ACS konfiguriert ein. Wenn die Konfigurationen korrekt sind, werden Sie im WLC erfolgreich als **Lobby-Administrator** authentifiziert. Dieses Beispiel zeigt, wie die GUI eines Lobby-Administrators nach erfolgreicher Authentifizierung sucht:



Hinweis: Sie können sehen, dass ein Lobby-Administrator außer der Verwaltung von Gastbenutzern keine andere Option hat.

Um diese im CLI-Modus zu überprüfen, wird Telnet als Lese- und Schreibadministrator in den Controller integriert. Führen Sie den Befehl **debug aa all enable** in der Controller-CLI aus.

```
(Cisco Controller) >debug aaa all enable

(Cisco Controller) >
*aaaQueueReader: Aug 26 18:07:35.072: ReProcessAuthentication previous proto 28,
 next proto 20001
*aaaQueueReader: Aug 26 18:07:35.072: AuthenticationRequest: 0x3081f7dc
*aaaQueueReader: Aug 26 18:07:35.072:   Callback.....................................0x10756dd0
*aaaQueueReader: Aug 26 18:07:35.072:   protocolType.................................0x00020001
*aaaQueueReader: Aug 26 18:07:35.072:
proxyState.....................................00:00:00:40:
00:00-00:00
*aaaQueueReader: Aug 26 18:07:35.072:   Packet contains 5 AVPs (not shown)
*aaaQueueReader: Aug 26 18:07:35.072: apfVapRadiusInfoGet: WLAN(0) dynamic int attributes
srcAddr:
0x0, gw:0x0, mask:0x0, vlan:0, dpPort:0, srcPort:0
*aaaQueueReader: Aug 26 18:07:35.073: 00:00:00:40:00:00 Successful transmission of
Authentication
Packet (id 39) to 10.77.244.212:1812, proxy state 00:00:00:40:00:00-00:01
*aaaQueueReader: Aug 26 18:07:35.073: 00000000: 01 27 00 47 00 00 00 00  00 00 00 00 00 00 00 00
.'.G............
*aaaQueueReader: Aug 26 18:07:35.073: 00000010: 00 00 00 00 01 0c 6c 6f  62 62 79 61 64 6d 69 6e
......lobbyadmin
*aaaQueueReader: Aug 26 18:07:35.073: 00000020: 02 12 5f 5b 5c 12 c5 c8  52 d3 3f 4f 4f 8e 9d 38
 .._[\...R.?OO..8
*aaaQueueReader: Aug 26 18:07:35.073: 00000030: 42 91 06 06 00 00 00 07  04 06 0a 4e b1 1a 20 09
B..........N....
```

```
*aaaQueueReader: Aug 26 18:07:35.073: 00000040: 57 4c 43 34 34 30 30 WLC4400
*radiusTransportThread: Aug 26 18:07:35.080: 00000000: 02 27 00 40 7e 04 6d 533d ed 79 9c b6 99
d1
f8  .'.@~.mS=.y.....
*radiusTransportThread: Aug 26 18:07:35.080: 00000010: d0 5a 8f 4f 08 06 ff ffff ff 06 06 00 00
00
0b  .Z.O............
*radiusTransportThread: Aug 26 18:07:35.080: 00000020: 19 20 43 41 43 53 3a 302f 61 65 32 36 2f
61
34  ..CACS:0/ae26/a4
*radiusTransportThread: Aug 26 18:07:35.080: 00000030: 65 62 31 31 61 2f 6c 6f62 62 79 61 64 6d
69
6e  eb11a/lobbyadmin
*radiusTransportThread: Aug 26 18:07:35.080: ****Enter processIncomingMessages: response code=2
*radiusTransportThread: Aug 26 18:07:35.080: ****Enter processRadiusResponse: response code=2
*radiusTransportThread: Aug 26 18:07:35.080: 00:00:00:40:00:00 Access-Accept received from
RADIUS
server 10.77.244.212 for mobile 00:00:00:40:00:00 receiveId = 0
*radiusTransportThread: Aug 26 18:07:35.080: AuthorizationResponse: 0x13c73d50
*radiusTransportThread: Aug 26 18:07:35.080:    structureSize.............................118
*radiusTransportThread: Aug 26 18:07:35.080:    resultCode.................................0
*radiusTransportThread: Aug 26 18:07:35.080:
protocolUsed.............................0x00000001
*radiusTransportThread: Aug 26 18:07:35.080:
proxyState.................................00:00:00:40:00:00-00:00
*radiusTransportThread: Aug 26 18:07:35.080:    Packet contains 3 AVPs:
*radiusTransportThread: Aug 26 18:07:35.080:        AVP[01] Framed-IP-
Address.....................0xffffffff (-1) (4 bytes)
*radiusTransportThread: Aug 26 18:07:35.080:        AVP[02] Service-
Type.............................0x0000000b (11) (4 bytes)
*radiusTransportThread: Aug 26 18:07:35.080:        AVP[03]
Class.....................................
CACS:0/ae26/a4eb11a/lobbyadmin (30 bytes)
*emWeb: Aug 26 18:07:35.084: Authentication succeeded for lobbyadmin
```

Die hervorgehobenen Informationen in dieser Ausgabe zeigen an, dass das Service-Type-Attribut 11 (Callback Administrative) vom ACS-Server an den Controller übergeben wird und der Benutzer als Lobby-Administrator angemeldet ist.

Diese Befehle können zusätzliche Hilfe sein:

- **debuggen aaa details aktivieren**
- **debug aaa events enable**
- **debuggen aaa pakete aktivieren**

Hinweis: Beachten Sie vor der Verwendung von **Debug-**Befehlen die Informationen zu Debug-Befehlen.

Fehlerbehebung

Wenn Sie sich bei einem Controller mit Lobby-Botschafterberechtigungen anmelden, können Sie kein Gastbenutzerkonto mit einem Lebenszeitwert "**0**" erstellen, das niemals abläuft. In diesen Situationen erhalten Sie die Fehlermeldung `Lifetime value cannot be 0`.

Dies liegt an der Cisco Bug ID CSCsf32392 (nur registrierte Kunden) , die hauptsächlich mit WLC Version 4.0 zu finden ist. Dieser Fehler wurde in WLC Version 4.1 behoben.

Zugehörige Informationen

- RADIUS-Serverauthentifizierung von Verwaltungsbenutzern im Konfigurationsbeispiel für den Controller
- Konfiguration von Cisco Unified Wireless Network TACACS+
- Konfigurationsleitfaden für Cisco Wireless LAN Controller, Version 4.0 - Verwalten von Benutzerkonten
- Konfigurationsbeispiel für ACLs in Wireless LAN-Controllern
- Häufig gestellte Fragen zum Wireless LAN Controller (WLC)
- ACLs auf Wireless LAN-Controllern: Regeln, Einschränkungen und Beispiele
- Konfigurationsbeispiel für die externe Webauthentifizierung mit Wireless LAN-Controllern
- Konfigurationsbeispiel für die Webauthentifizierung des Wireless LAN-Controllers
- Gast-WLAN und internes WLAN mit WLCs - Konfigurationsbeispiel
- Technischer Support und Dokumentation für Cisco Systeme