# Konfigurieren eines WLC und eines ACS zur Authentifizierung von Managementbenutzern

## Inhalt


- Einleitung
- Voraussetzungen
  - Anforderungen
  - Verwendete Komponenten
  - Konventionen
- Hintergrundinformationen
- Konfigurieren
  - Netzwerkdiagramm
  - Konfigurationen
  - WLC-Konfiguration
    - Konfigurieren des WLC zum Akzeptieren der Verwaltung über den Cisco Secure ACS Server
  - Cisco Secure ACS-Konfiguration
    - Hinzufügen des WLC als AAA-Client zum RADIUS-Server
    - Konfigurieren der Benutzer und der entsprechenden RADIUS IETF-Attribute
    - Konfigurieren eines Benutzers mit Lese- und Schreibzugriff
    - Konfigurieren eines Benutzers mit schreibgeschütztem Zugriff
  - Verwalten des WLC lokal und über den RADIUS-Server
- Überprüfung
- Fehlerbehebung
- Zugehörige Informationen


## Einleitung

In diesem Dokument wird beschrieben, wie ein WLC und ein Cisco Secure ACS konfiguriert werden, damit der AAA-Server die Management-Benutzer auf dem Controller authentifizieren kann.

## Voraussetzungen

### Anforderungen

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

- Grundlegende Informationen zum Konfigurieren von WLC-Basisparametern
- Kenntnisse der Konfiguration eines RADIUS-Servers wie Cisco Secure ACS

### 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 Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

### Konventionen

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

## Hintergrundinformationen

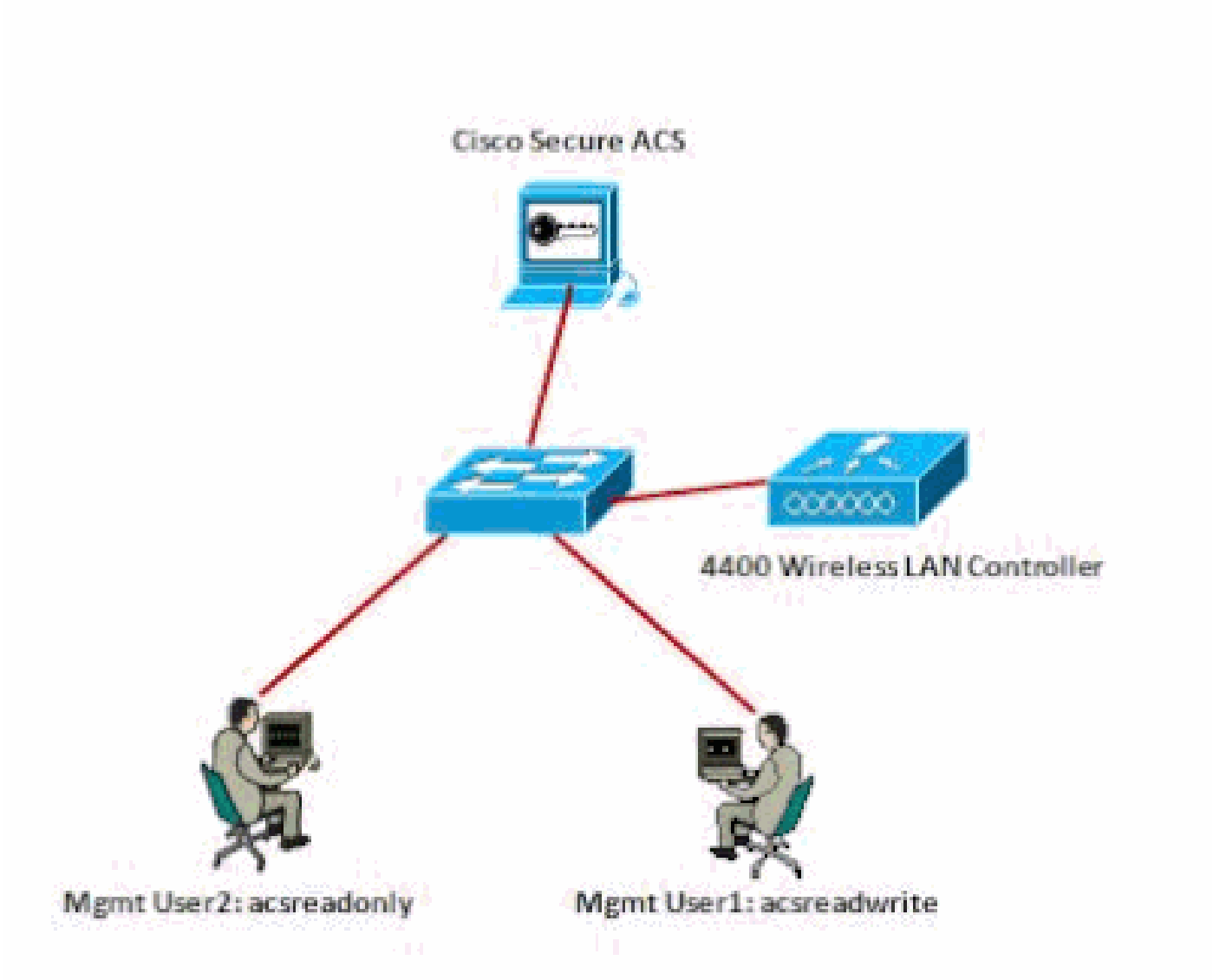
In diesem Dokument wird erläutert, wie ein Wireless LAN Controller (WLC) und ein Zugriffssteuerungsserver (Cisco Secure ACS) konfiguriert werden, sodass der AAA-Server (Authentication, Authorization, and Accounting) Verwaltungsbenutzer auf dem Controller authentifizieren kann. In diesem Dokument wird außerdem erläutert, wie verschiedene Managementbenutzer unterschiedliche Berechtigungen mit anbieterspezifischen Attributen (VSAs) erhalten können, die vom Cisco Secure ACS RADIUS-Server zurückgegeben werden.

## Konfigurieren

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

### Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:




Netzwerkdiagramm

In diesem Konfigurationsbeispiel werden folgende Parameter verwendet:

- IP-Adresse des Cisco Secure ACS - 172.16.1.1/255.255.0.0
- IP-Adresse der Management-Schnittstelle des Controllers: 172.16.1.30/255.255.0.0
- Gemeinsamer geheimer Schlüssel, der auf dem Access Point (AP) und dem RADIUS-Server verwendet wird - asdf1234
- Dies sind die Anmeldeinformationen der beiden Benutzer, die in diesem Beispiel auf dem ACS konfiguriert werden:
    - Benutzername - acsreadwrite

      Kennwort - acsreadwrite
    - Benutzername - acsreadonly

      Kennwort - acsreadonly

Sie müssen den WLC und Cisco Secure Cisco Secure ACS konfigurieren, um:

- Jeder Benutzer, der sich mit Benutzername und Kennwort als acsreadwrite beim WLC anmeldet, erhält vollen Administratorzugriff auf den WLC.
- Jeder Benutzer, der sich mit Benutzername und Kennwort als acsreadonly beim WLC anmeldet, erhält schreibgeschützten Zugriff auf den WLC.

## Konfigurationen

In diesem Dokument werden folgende Konfigurationen verwendet:

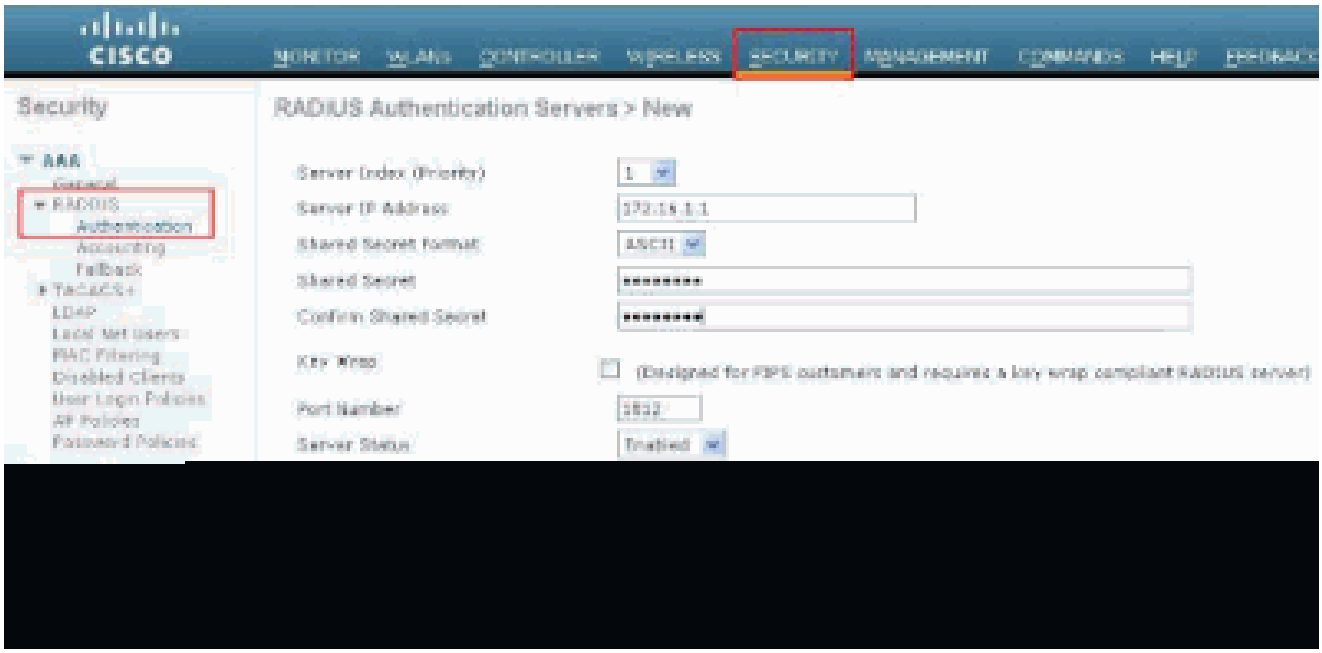
- WLC-Konfiguration
- Cisco Secure ACS-Konfiguration

## WLC-Konfiguration

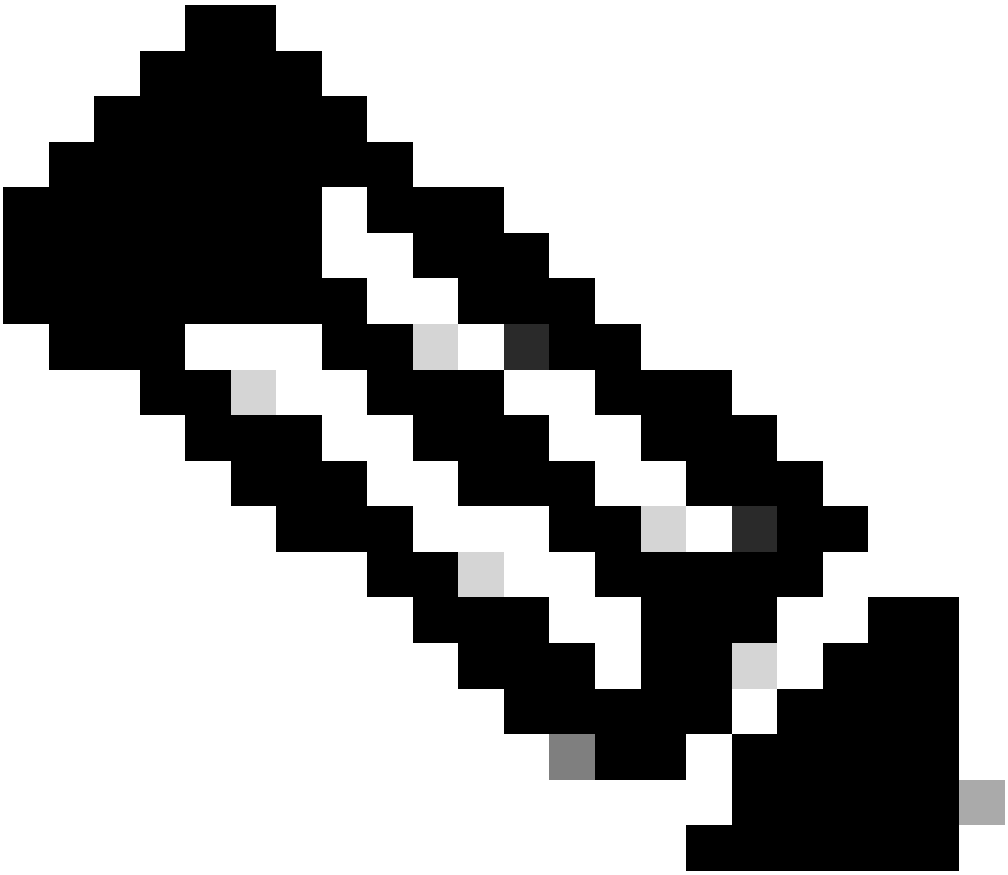
Konfigurieren des WLC zum Akzeptieren der Verwaltung über den Cisco Secure ACS Server

Gehen Sie wie folgt vor, um den WLC so zu konfigurieren, dass er mit dem RADIUS-Server kommuniziert:

1. Klicken Sie in der WLC-GUI auf Sicherheit.  Klicken Sie im Menü auf der linken Seite auf RADIUS > Authentication (RADIUS > Authentifizierung).  Die Seite RADIUS Authentication Servers wird angezeigt. Um einen neuen RADIUS-Server hinzuzufügen, klicken Sie auf Neu. Geben Sie auf der Seite RADIUS Authentication Servers > New (RADIUS-Authentifizierungsserver > Neu) die für den RADIUS-Server spezifischen Parameter ein. Hier ein Beispiel.

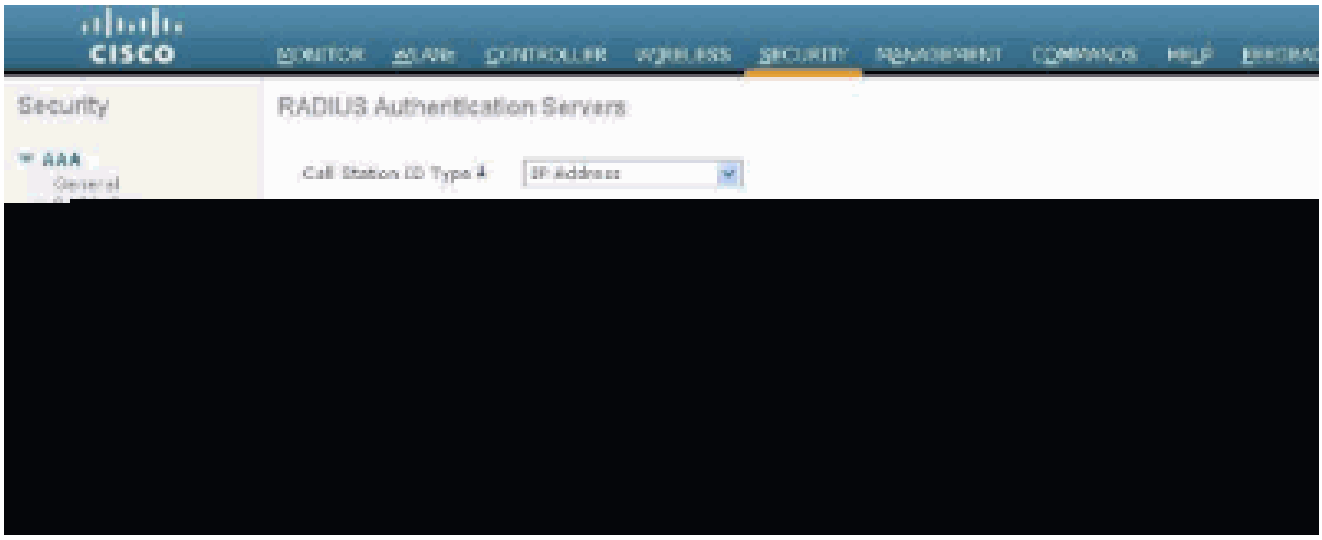



2. Aktivieren Sie das Optionsfeld Management, damit der RADIUS-Server Benutzer authentifizieren kann, die sich beim WLC anmelden.



Hinweis: Stellen Sie sicher, dass der auf dieser Seite konfigurierte geheime Schlüssel mit dem auf dem RADIUS-Server konfigurierten geheimen Schlüssel übereinstimmt. Nur dann kann der WLC mit dem RADIUS-Server kommunizieren.

3. Überprüfen Sie, ob der WLC für die Verwaltung durch Cisco Secure ACS konfiguriert ist. Klicken Sie dazu in der WLC-GUI auf Security (Sicherheit). Das resultierende GUI-Fenster wird ähnlich wie in diesem Beispiel angezeigt.




Wie Sie sehen, ist das Kontrollkästchen Verwaltung für den RADIUS-Server 172.16.1.1 aktiviert. Dies zeigt, dass der ACS die Verwaltungsbenutzer auf dem WLC authentifizieren kann.

## Cisco Secure ACS-Konfiguration

Führen Sie die Schritte in diesen Abschnitten aus, um den ACS zu konfigurieren:

1. Fügen Sie den WLC als AAA-Client zum RADIUS-Server hinzu.
2. Konfigurieren von Benutzern und der entsprechenden RADIUS IETF-Attribute
3. Konfigurieren eines Benutzers mit Lese- und Schreibzugriff.
4. Konfigurieren eines Benutzers mit schreibgeschütztem Zugriff

Hinzufügen des WLC als AAA-Client zum RADIUS-Server

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

1. Klicken Sie in der ACS-GUI auf Network Configuration.
2. Klicken Sie unter AAA Clients auf Add Entry (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.

   In diesem Beispiel sind dies die Einstellungen:

   - AAA-Client-Hostname: WLC-4400
   - 172.16.1.30/16 die IP-Adresse des AAA-Clients, in diesem Fall der WLC.
   - Der gemeinsame geheime Schlüssel lautet "asdf1234".

Fenster "AAA-Client hinzufügen"

Dieser Schlüssel muss mit dem Schlüssel für den gemeinsamen geheimen Schlüssel übereinstimmen, den Sie auf dem WLC konfigurieren.

4. Wählen Sie im Dropdown-Menü Authenticate Using (Authentifizieren über) die Option RADIUS (Cisco Airspace) aus.

5. Klicken Sie auf Submit + Restart, um die Konfiguration zu speichern.

Konfigurieren der Benutzer und der entsprechenden RADIUS IETF-Attribute

Um einen Benutzer über einen RADIUS-Server zu authentifizieren, müssen Sie den Benutzer für die Controller-Anmeldung und -Verwaltung der RADIUS-Datenbank mit dem IETF RADIUS-Attribut "Service-Type" hinzufügen, das auf der Grundlage der Benutzerberechtigungen auf den entsprechenden Wert festgelegt wurde.

- Um Lese- und Schreibberechtigungen für den Benutzer festzulegen, legen Sie das Service-TypeAttribute auf Administrative fest.
- Um schreibgeschützte Berechtigungen für den Benutzer festzulegen, legen Sie das Service-TypeAttribute auf NAS-Prompt fest.

Konfigurieren eines Benutzers mit Lese- und Schreibzugriff

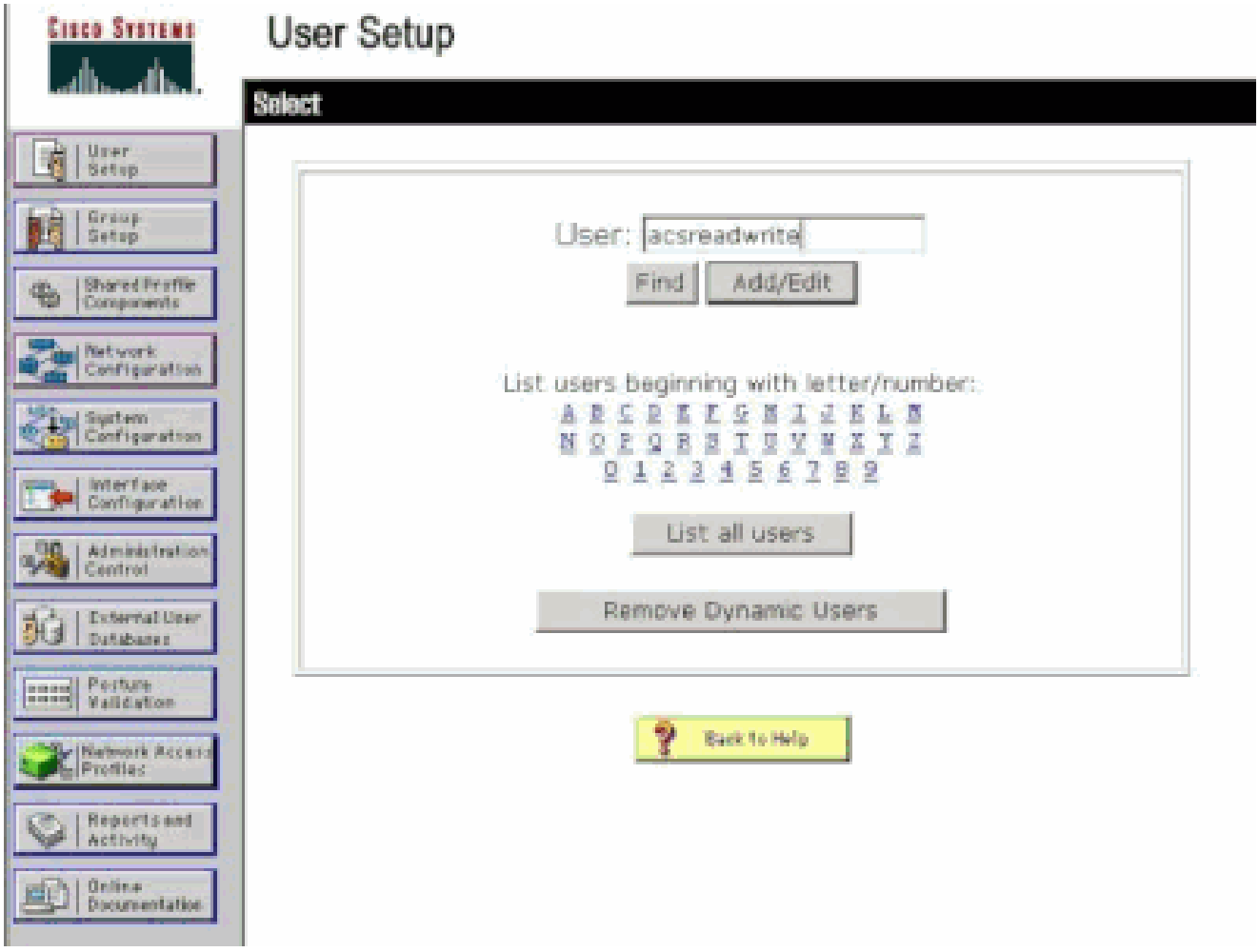
Das erste Beispiel zeigt die Konfiguration eines Benutzers mit vollem Zugriff auf den WLC. Wenn dieser Benutzer versucht, sich beim Controller anzumelden, authentifiziert sich der RADIUS-

Server und gewährt diesem Benutzer vollständigen Administratorzugriff.

In diesem Beispiel lautet der Benutzername und das Kennwort acsreadwrite (acsreadwrite).

Gehen Sie wie folgt vor: Cisco Secure ACS.

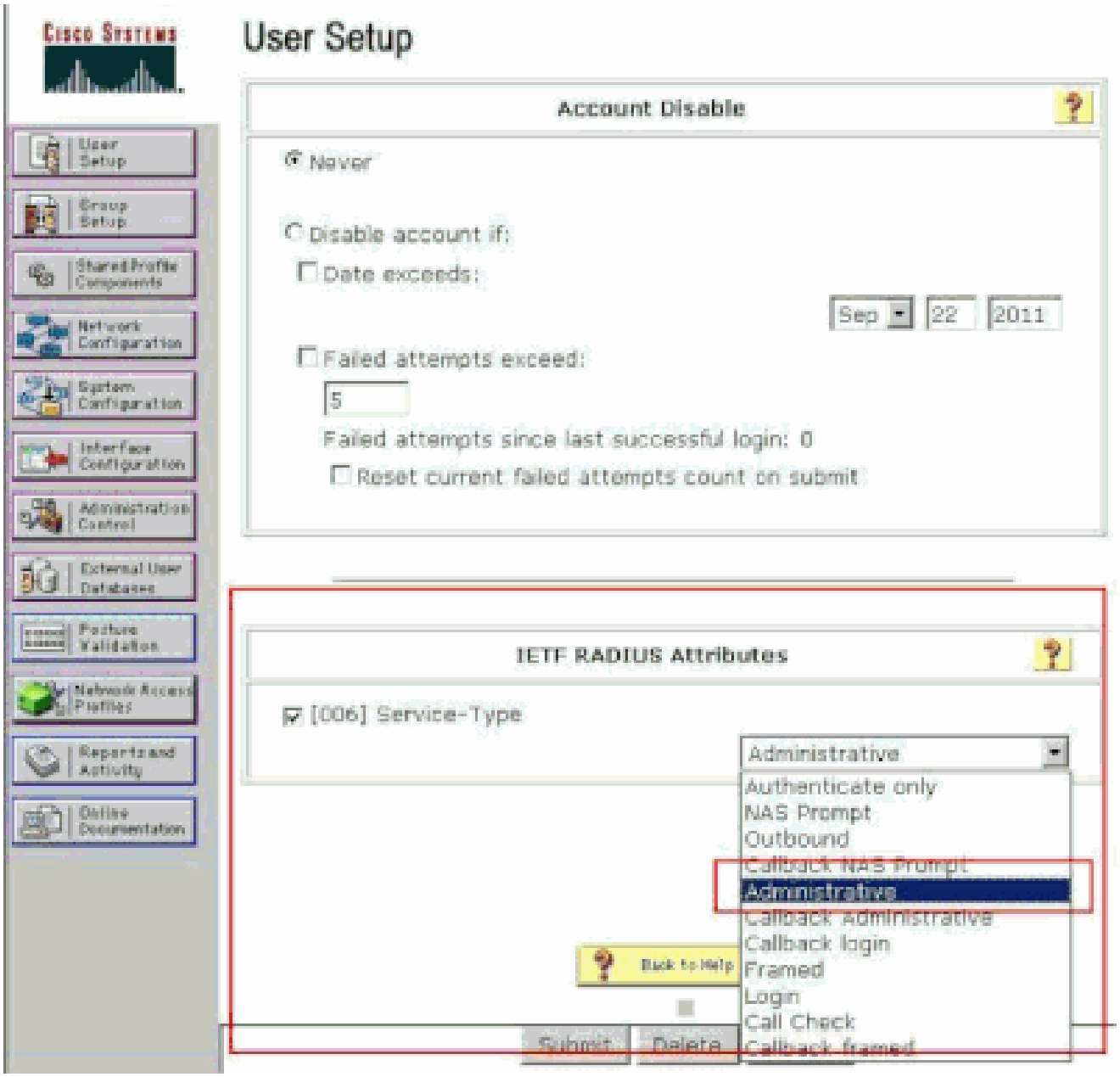
1. Klicken Sie in der ACS-GUI auf User Setup (Benutzereinrichtung).
2. Geben Sie den Benutzernamen ein, der dem ACS hinzugefügt werden soll, wie in diesem Beispielfenster dargestellt.




Fenster "User Setup"

3. Klicken Sie auf Hinzufügen/Bearbeiten, um zur Seite Benutzerbearbeitung zu gelangen.
4. Geben Sie auf der Seite "User Edit" (Benutzerbearbeitung) den Real Name, die Beschreibung und das Password dieses Benutzers an.
5. Blättern Sie nach unten zur Einstellung IETF RADIUS Attributes (IETF RADIUS-Attribute), und aktivieren Sie Service-Type Attribute (Servicetyp-Attribut).
6. Da in diesem Beispiel der Benutzer acsreadwrite vollständigen Zugriff erhalten muss, wählen Sie im Pulldown-Menü "Service-Type" die Option Administrative aus, und klicken Sie auf Submit (Senden).

Dadurch wird sichergestellt, dass dieser Benutzer Lese- und Schreibzugriff auf den WLC hat.



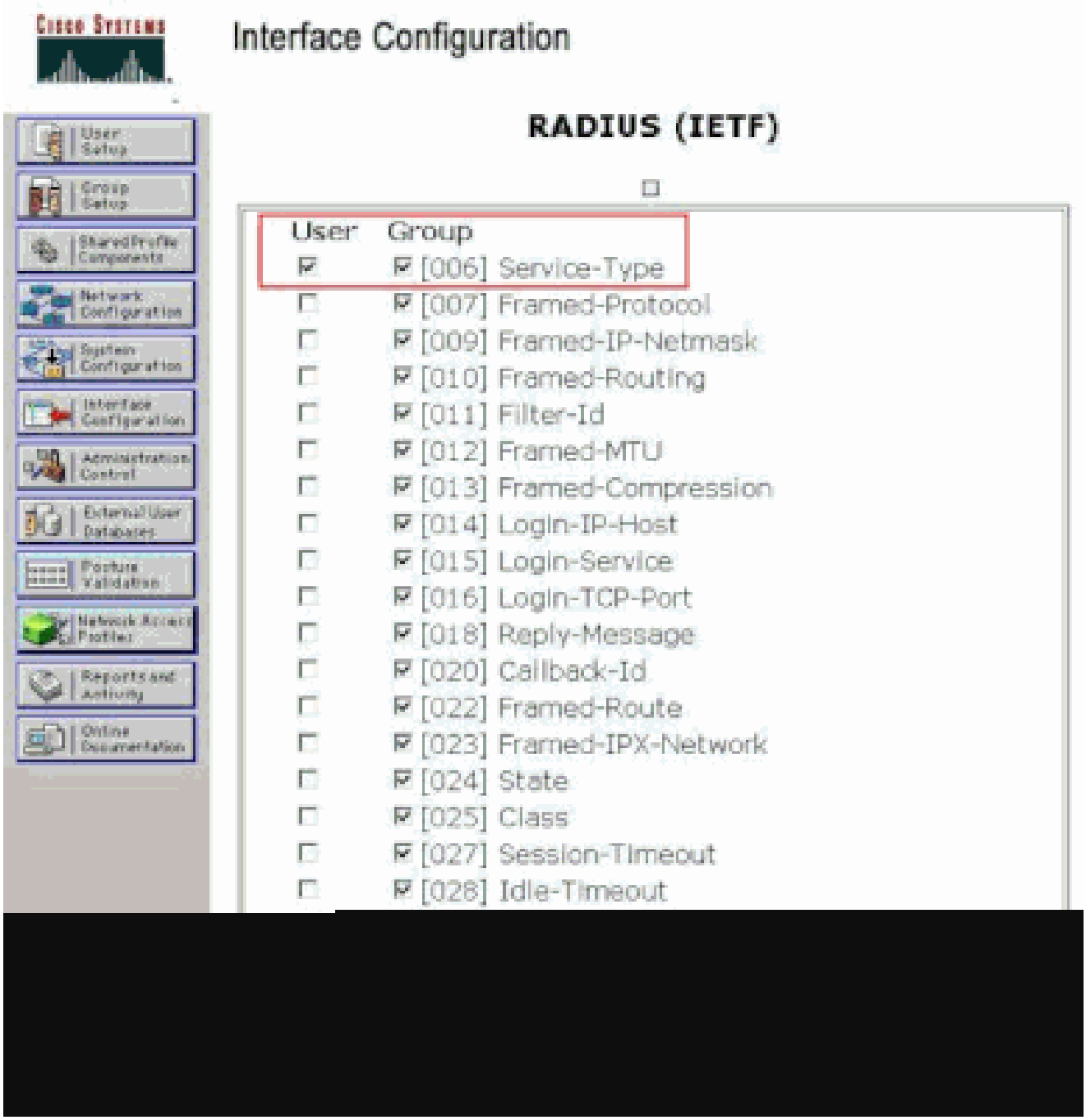

Einstellungen für ETF-RADIUS-Attribute

In manchen Fällen ist dieses Servicetyp-Attribut unter den Benutzereinstellungen nicht sichtbar. Führen Sie in diesen Fällen diese Schritte aus, um sie sichtbar zu machen.

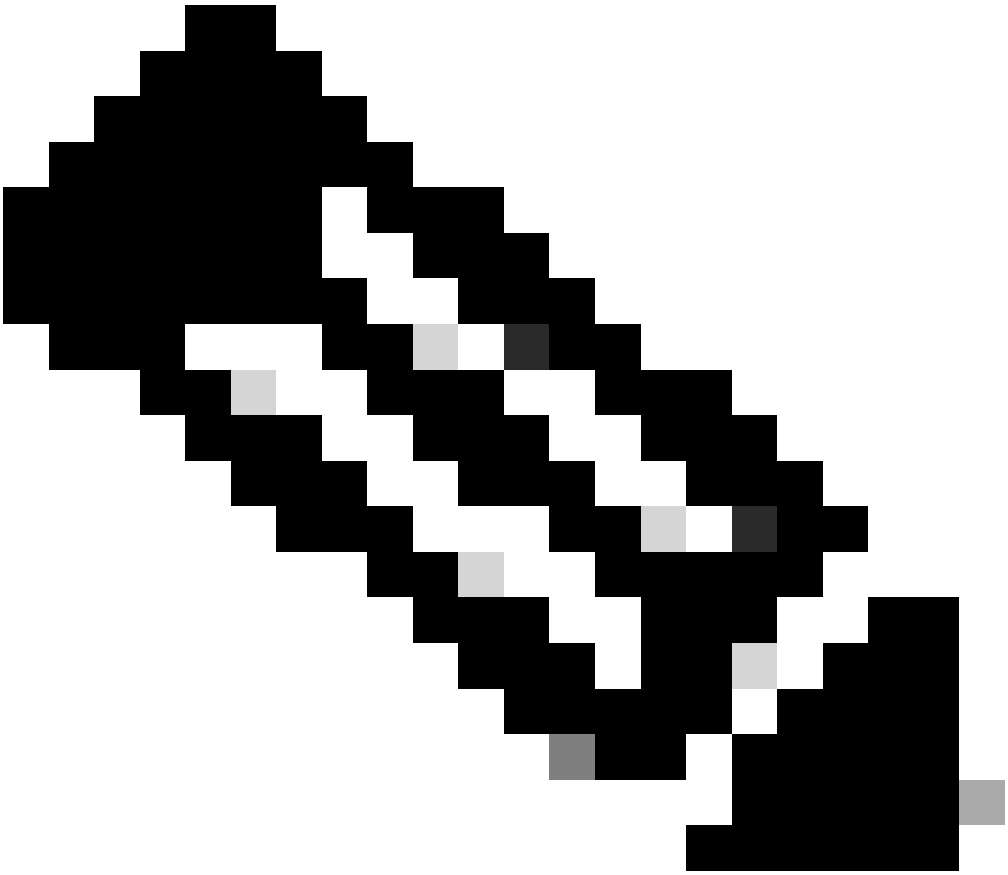
1. Wählen Sie in der ACS-GUI Interface Configuration > RADIUS (IETF) aus, um die IETF-Attribute im Fenster User Configuration zu aktivieren.

   Dadurch gelangen Sie zur Seite RADIUS (IETF) Settings (RADIUS- (IETF)-Einstellungen).

2. Auf der Seite RADIUS (IETF) Settings (RADIUS (IETF)-Einstellungen) können Sie das IETF-Attribut aktivieren, das unter Benutzer- oder Gruppeneinstellungen angezeigt werden muss. Aktivieren Sie für diese Konfiguration in der Spalte "Benutzer" das Kontrollkästchen "Servicetyp", und klicken Sie auf Senden.  Dieses Fenster zeigt ein Beispiel.




RADIUS (IETF)-Einstellungsseite



Hinweis: In diesem Beispiel wird die Authentifizierung auf Benutzerbasis angegeben. Sie können die Authentifizierung auch basierend auf der Gruppe durchführen, zu der ein bestimmter Benutzer gehört. Aktivieren Sie in diesem Fall das Kontrollkästchen Gruppe, damit dieses Attribut unter Gruppeneinstellungen angezeigt wird. 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 zuzuweisen. Detaillierte Informationen zum Konfigurieren und Verwalten von Gruppen finden Sie unter Gruppenverwaltung.

Konfigurieren eines Benutzers mit schreibgeschütztem Zugriff

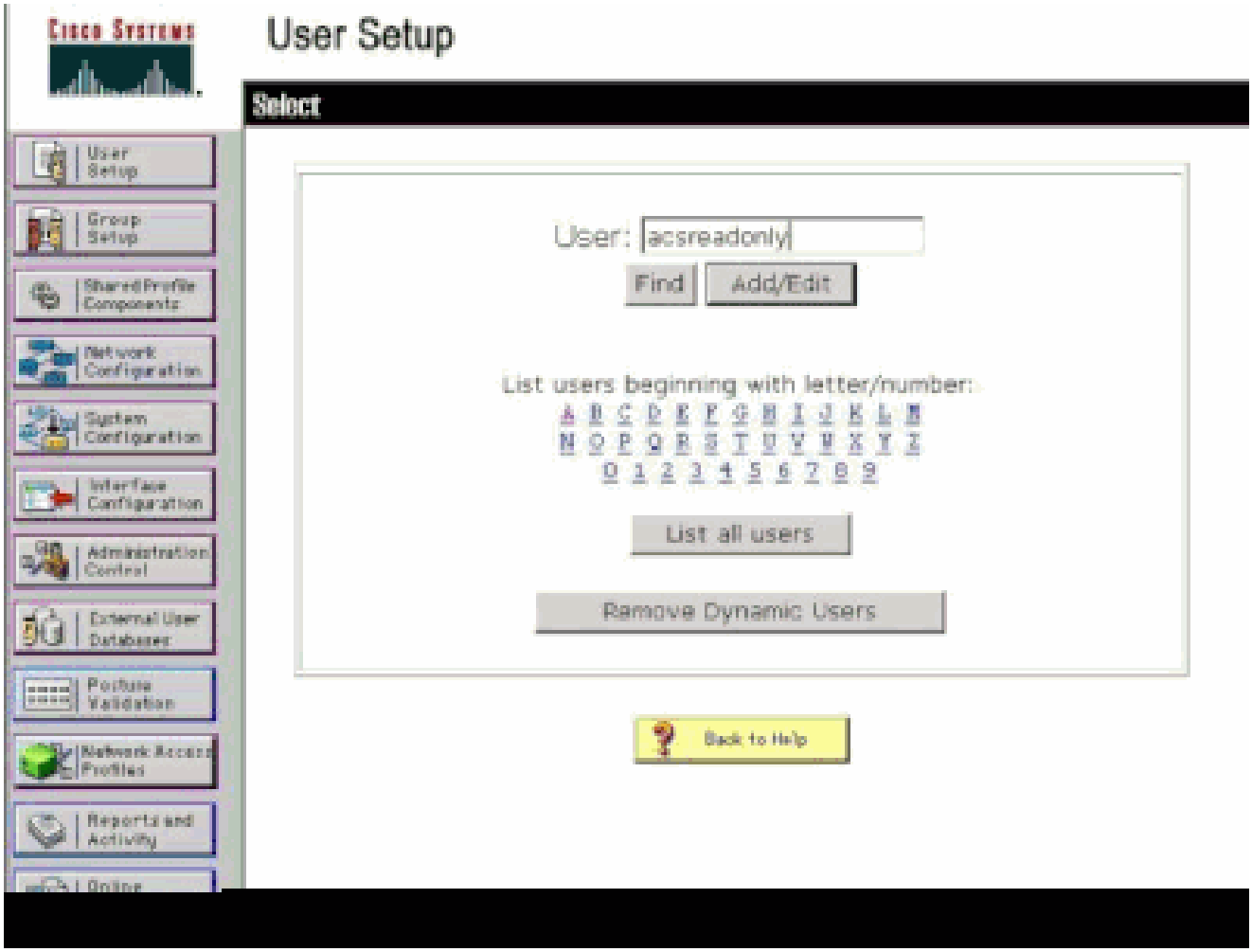
Dieses Beispiel zeigt die Konfiguration eines Benutzers mit schreibgeschütztem Zugriff auf den WLC. Wenn dieser Benutzer versucht, sich beim Controller anzumelden, authentifiziert sich der RADIUS-Server und gewährt diesem Benutzer schreibgeschützten Zugriff.

In diesem Beispiel sind der Benutzername und das Kennwort acsreadonly.

Gehen Sie wie folgt vor, um Cisco Secure ACS:

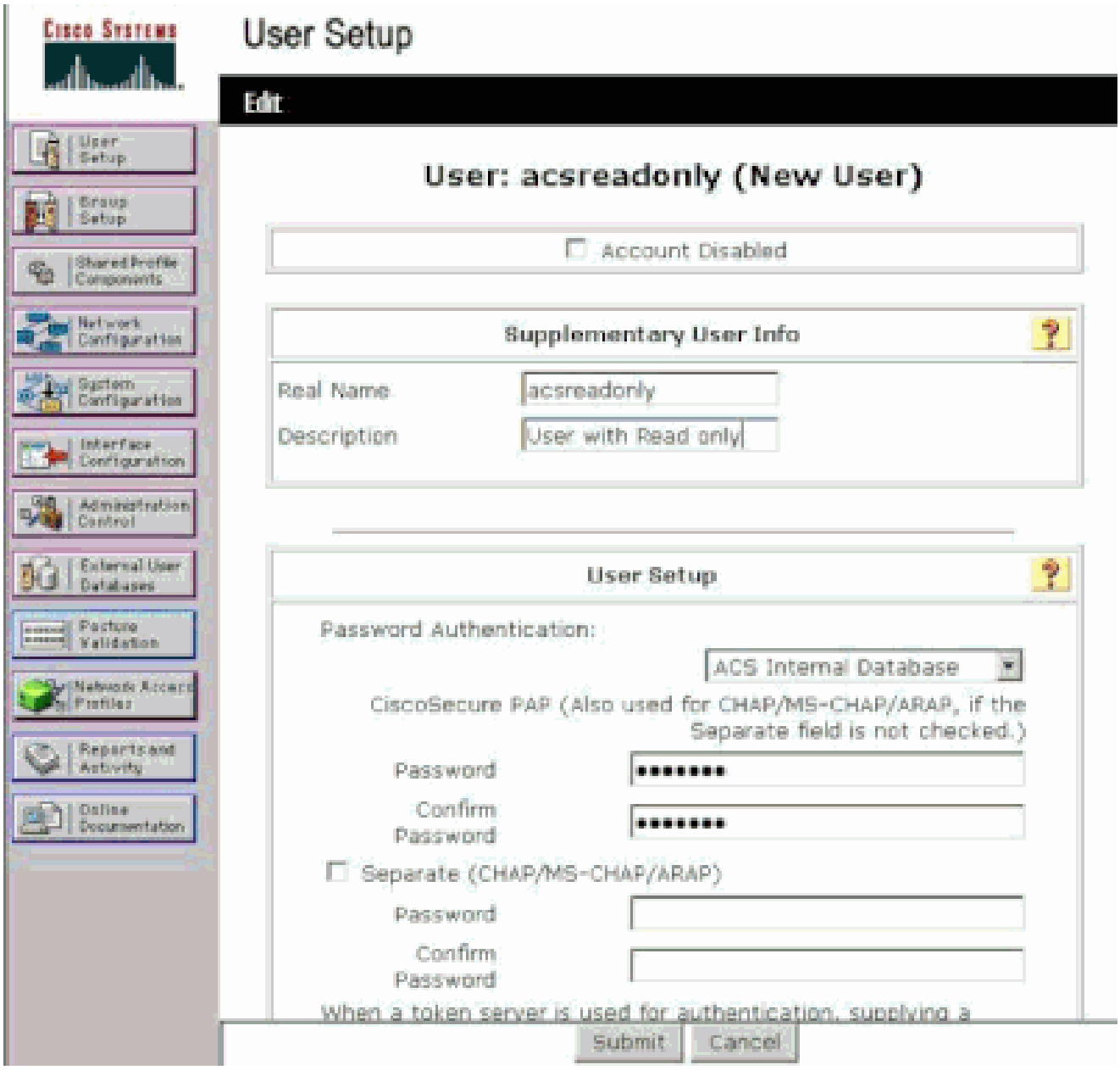
1. Klicken Sie in der ACS-GUI auf User Setup (Benutzereinrichtung).

2. Geben Sie den Benutzernamen ein, den Sie dem ACS hinzufügen möchten, und klicken Sie auf Hinzufügen/Bearbeiten, um zur Seite "Benutzerbearbeitung" zu gelangen.




Hinzufügen eines Benutzernamens

3. Geben Sie den richtigen Namen, die richtige Beschreibung und das richtige Passwort für diesen Benutzer an. Dieses Fenster zeigt ein Beispiel.

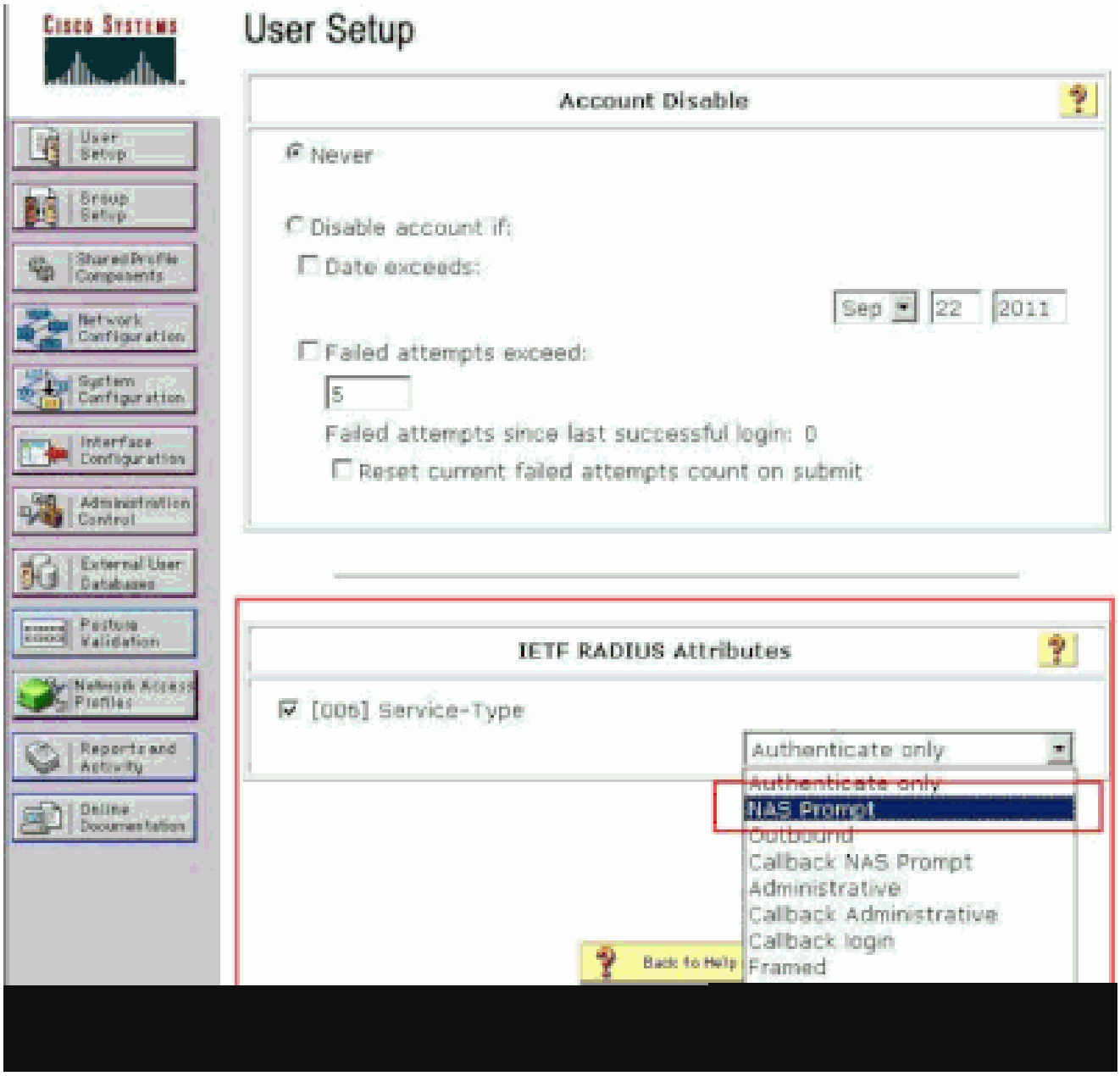



Geben Sie den wahren Namen, die Beschreibung und das Passwort des hinzugefügten Benutzers an.

4. Blättern Sie nach unten zur Einstellung IETF RADIUS Attributes (IETF RADIUS-Attribute), und aktivieren Sie Service-Type Attribute (Servicetyp-Attribut).

5. Da in diesem Beispiel für den Benutzer acsreadonly schreibgeschützten Zugriff benötigt, wählen Sie NAS Prompt aus dem Dropdown-Menü Service-Type (Servicetyp) aus, und klicken Sie auf Submit (Senden).

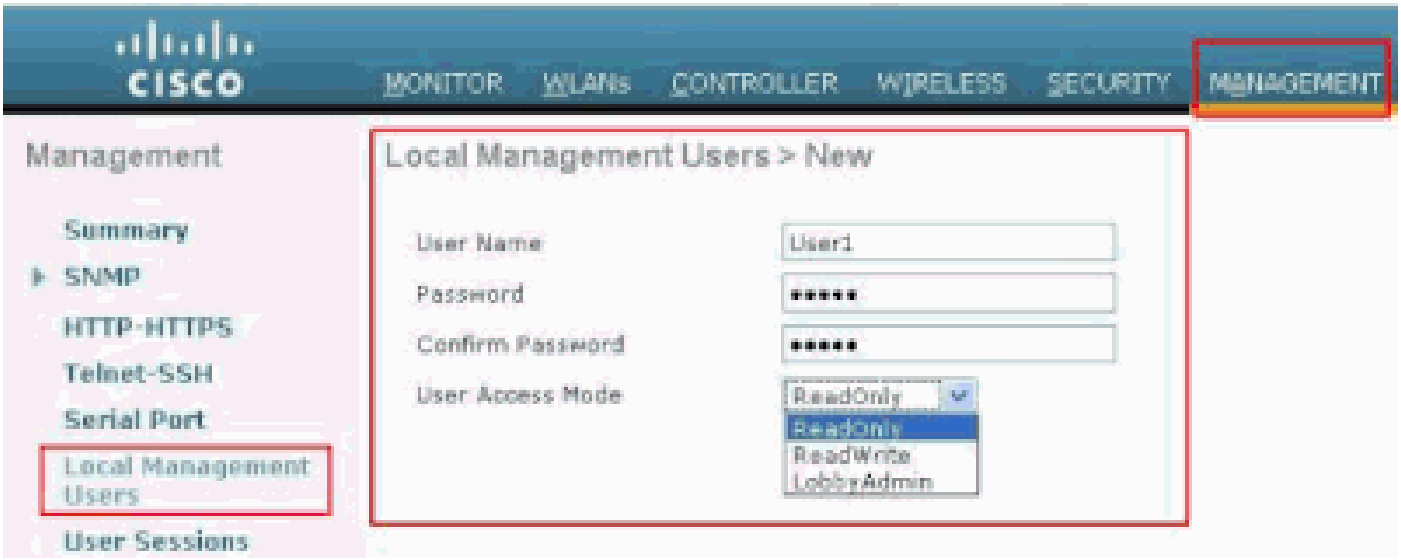
   Dadurch wird sichergestellt, dass dieser spezielle Benutzer schreibgeschützten Zugriff auf den WLC hat.




Servicetyp-Attribut überprüfen

## Verwalten des WLC lokal und über den RADIUS-Server

Sie können die Management-Benutzer auch lokal auf dem WLC konfigurieren. Dies kann über die Controller-GUI unter Management > Local Management Users (Verwaltung > Lokale Verwaltungsbenutzer) durchgeführt werden.



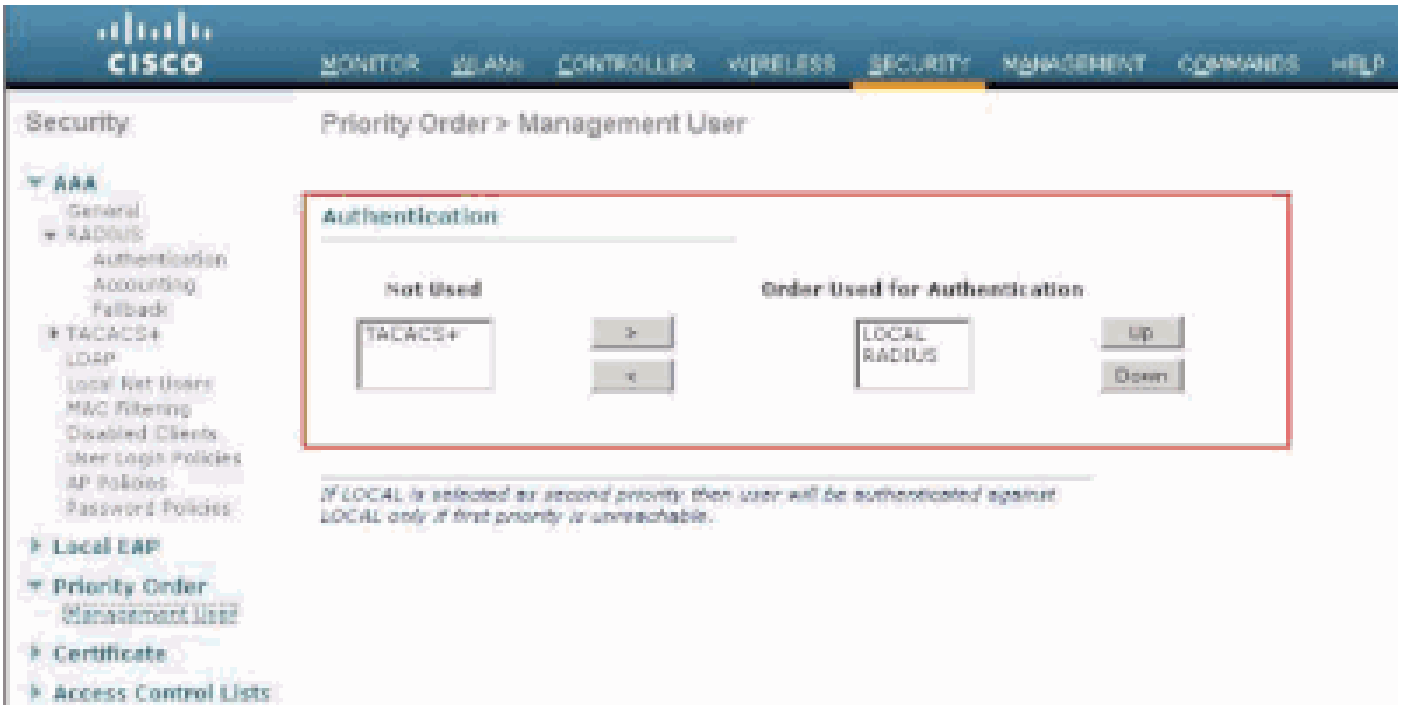

Lokale Konfiguration der Management-Benutzer auf dem WLC

Es wird davon ausgegangen, dass der WLC mit Managementbenutzern sowohl lokal als auch auf dem RADIUS-Server konfiguriert ist, wobei das Kontrollkästchen "Management" aktiviert ist. Wenn ein Benutzer versucht, sich beim WLC anzumelden, verhält sich der WLC in einem solchen Szenario standardmäßig wie folgt:

1. Der WLC untersucht zunächst die lokalen Management-Benutzer, die zur Validierung des Benutzers definiert wurden. Wenn der Benutzer in der lokalen Liste vorhanden ist, kann er für diesen Benutzer authentifiziert werden. Wenn dieser Benutzer nicht lokal angezeigt wird, ruft er den RADIUS-Server auf.

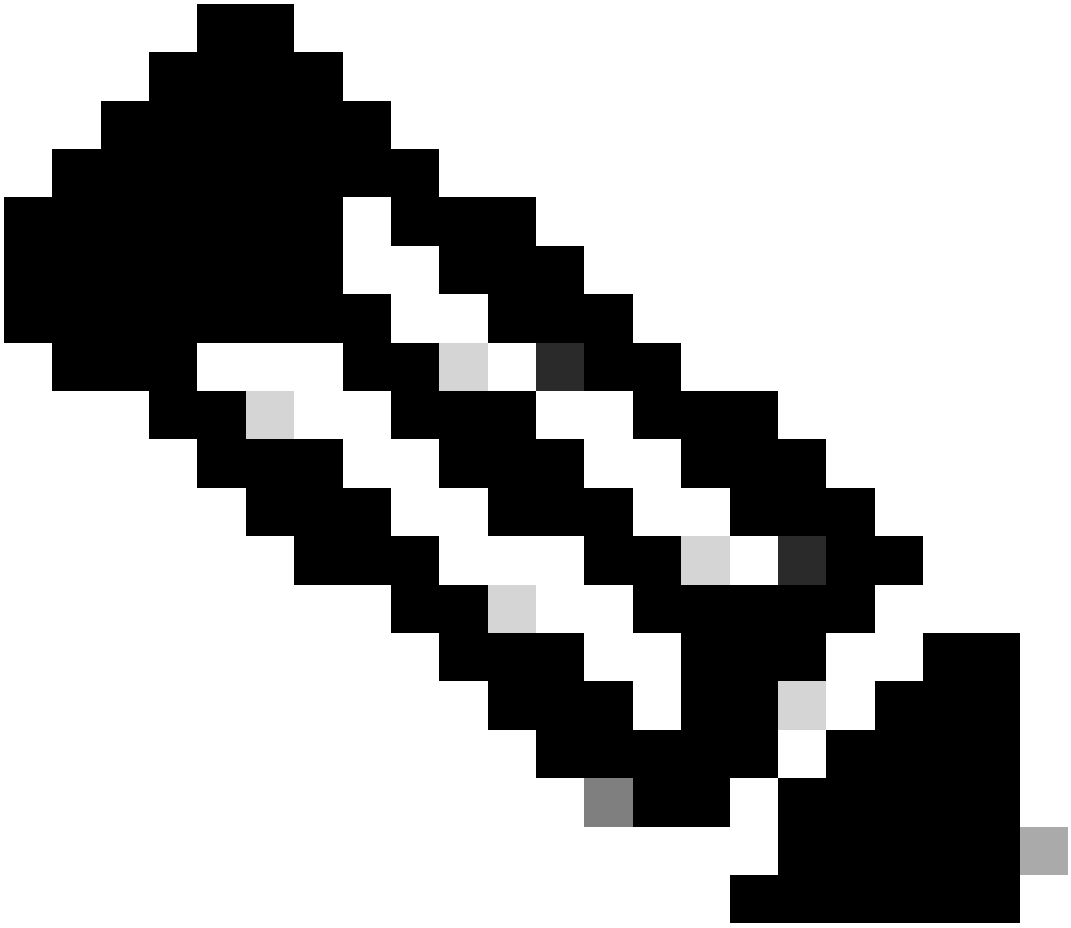
2. Wenn derselbe Benutzer sowohl lokal als auch auf dem RADIUS-Server vorhanden ist, aber unterschiedliche Zugriffsberechtigungen hat, authentifiziert der WLC den Benutzer mit den lokal festgelegten Berechtigungen. Mit anderen Worten, die lokale Konfiguration auf dem WLC hat im Vergleich zum RADIUS-Server immer Vorrang.

Die Reihenfolge der Authentifizierung für Managementbenutzer kann auf dem WLC geändert werden. Klicken Sie dazu auf der Seite Security (Sicherheit) des WLC auf Priority Order (Prioritätsreihenfolge) > Management User (Verwaltungsbenutzer).  Auf dieser Seite können Sie die Reihenfolge der Authentifizierung festlegen. Hier ein Beispiel.




Management User Selection" />

Priority Order > Management User Selection



Hinweis: Wenn LOCAL als zweite Priorität ausgewählt ist, wird der Benutzer mit dieser Methode nur authentifiziert, wenn die als erste Priorität definierte Methode (RADIUS/TACACS) nicht erreichbar ist.

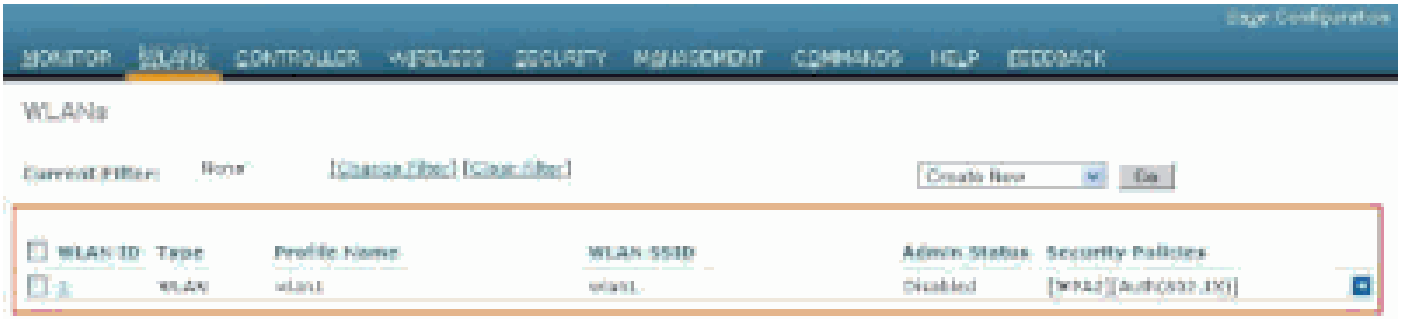
## Überprüfung

Um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert, greifen Sie über die CLI oder den GUI-Modus (HTTP/HTTPS) auf den WLC zu. Wenn die Anmeldeaufforderung angezeigt wird, geben Sie den auf Cisco Secure ACS konfigurierten Benutzernamen und das Kennwort ein.

Wenn die Konfigurationen korrekt sind, wird die Authentifizierung im WLC erfolgreich durchgeführt.

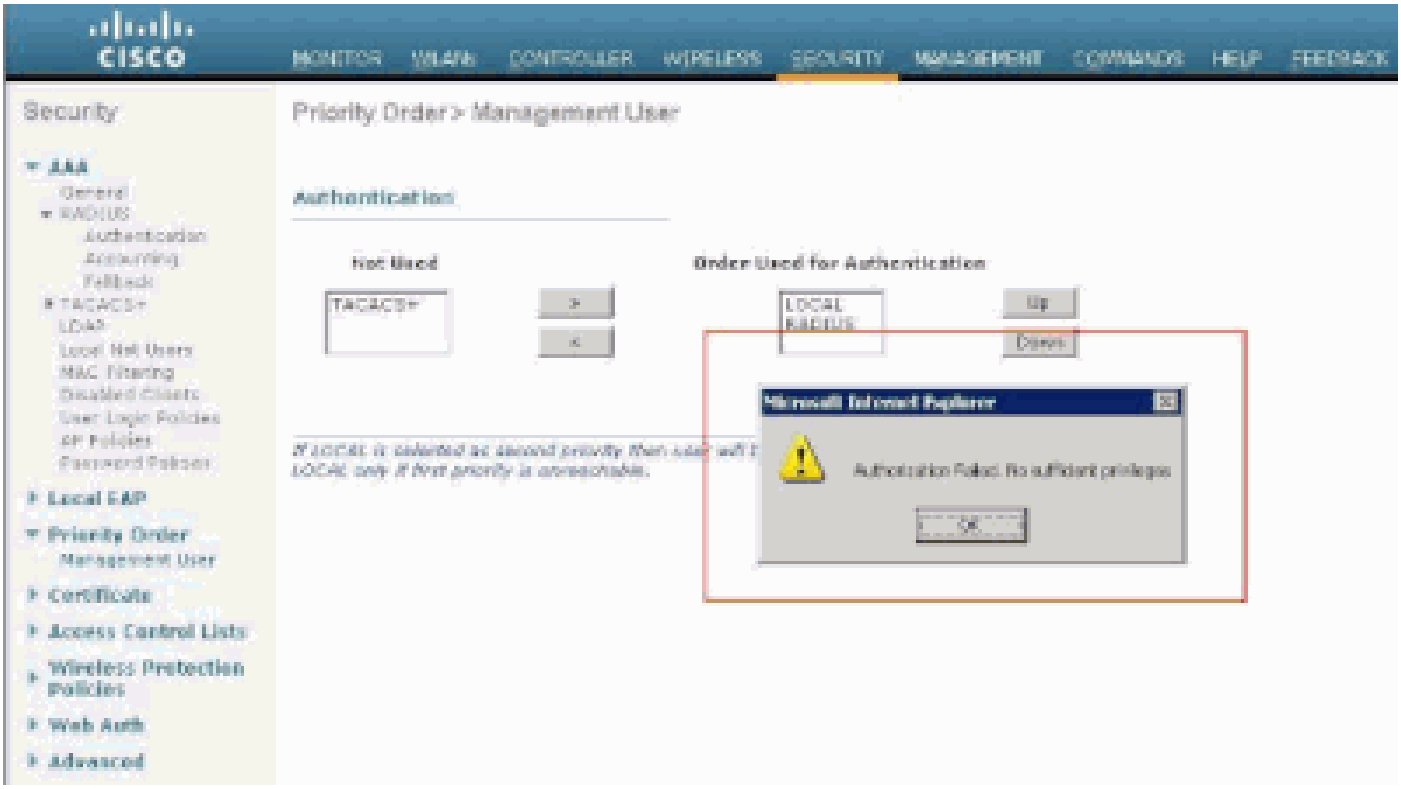
Sie können auch sicherstellen, dass dem authentifizierten Benutzer die vom ACS festgelegten Zugriffsbeschränkungen gewährt werden. Greifen Sie hierzu über HTTP/HTTPS auf die WLC-GUI zu (stellen Sie sicher, dass WLC so konfiguriert ist, dass HTTP/HTTPS zulässig ist).

Ein Benutzer mit im ACS festgelegtem Lese-/Schreibzugriff verfügt über mehrere konfigurierbare Berechtigungen im WLC. Beispielsweise verfügt ein Benutzer mit Lese-/Schreibzugriff über die Berechtigung, auf der Seite "WLANs" des WLC ein neues WLAN zu erstellen. Dieses Fenster zeigt ein Beispiel.




Konfigurierbare Berechtigungen im WLC

Wenn ein Benutzer mit schreibgeschütztem Zugriff versucht, die Konfiguration auf dem Controller zu ändern, wird diese Meldung angezeigt.




Controller kann nicht mit schreibgeschütztem Zugriff geändert werden

Diese Zugriffsbeschränkungen können auch über die CLI des WLC überprüft werden. Diese Ausgabe zeigt ein Beispiel.

```
<#root>

(Cisco Controller) >

?

debug           Manages system debug options.
```

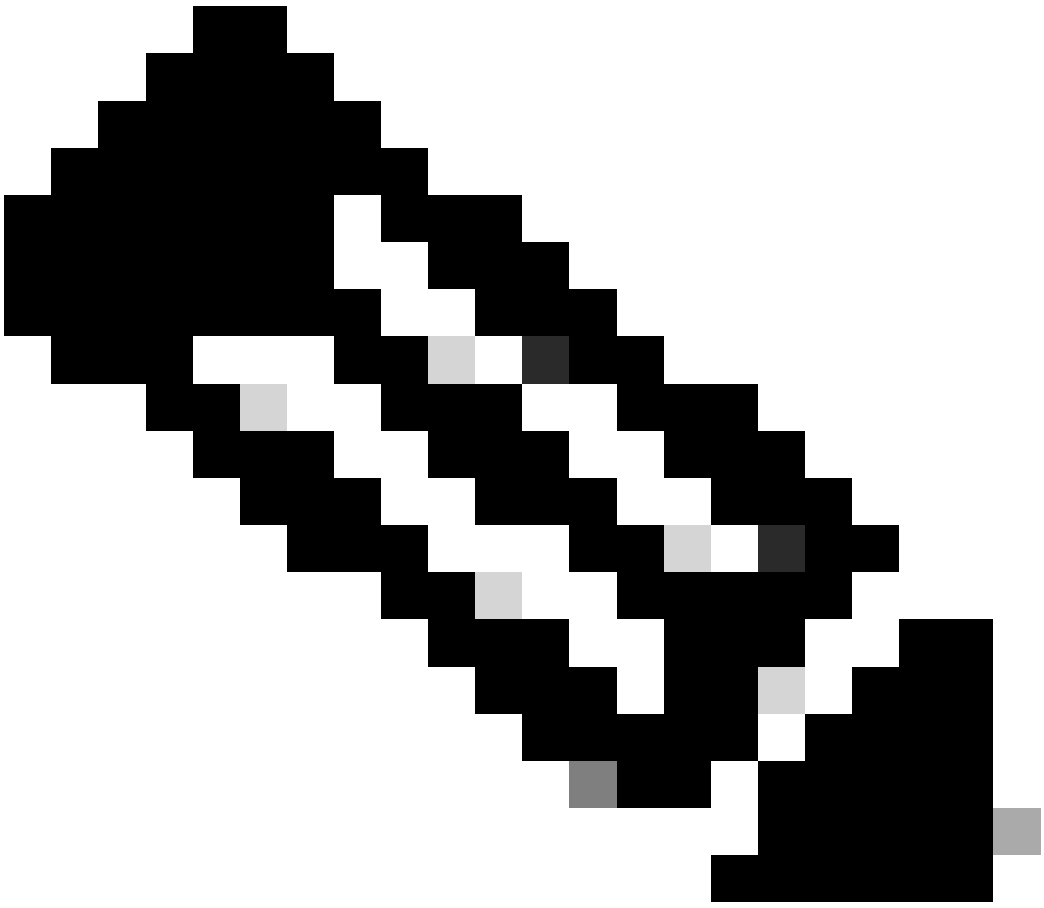
```
help            Help
linktest        Perform a link test to a specified MAC address.
logout          Exit this session. Any unsaved changes are lost.
show            Display switch options and settings.

(Cisco Controller) >config

Incorrect usage.  Use the '?' or <TAB> key to list commands.
```

Wie dieses Beispiel zeigt, zeigt ein ? in der CLI des Controllers eine Liste der Befehle an, die für den aktuellen Benutzer verfügbar sind. Beachten Sie außerdem, dass der **config** Befehl in dieser Beispielausgabe nicht verfügbar ist. Dies zeigt, dass ein schreibgeschützter Benutzer nicht über die Berechtigung verfügt, Konfigurationen auf dem WLC durchzuführen. Ein Benutzer mit Lese-/Schreibzugriff hat hingegen die Berechtigung, Konfigurationen auf dem Controller auszuführen (sowohl im GUI- als auch im CLI-Modus).

---



---

**Hinweis:** Auch wenn Sie einen WLC-Benutzer über den RADIUS-Server authentifizieren, während Sie von Seite zu Seite navigieren, authentifiziert der HTTP[S]-Server den Client jedes Mal vollständig. Sie werden auf jeder Seite nur deshalb nicht zur Authentifizierung aufgefordert, weil Ihr Browser Ihre Anmeldeinformationen zwischenspeichert und wiedergibt.

## Fehlerbehebung

Unter bestimmten Umständen authentifiziert ein Controller Management-Benutzer über den ACS, die Authentifizierung wird erfolgreich abgeschlossen (access-accept), und Sie sehen keinen Autorisierungsfehler auf dem Controller.*Der Benutzer wird jedoch erneut zur Authentifizierung aufgefordert.*

In solchen Fällen können Sie nicht interpretieren, was falsch ist und warum sich der Benutzer nicht nur mit dem **debug aaa events enable** Befehl beim WLC anmelden kann. Stattdessen zeigt der Controller eine weitere Aufforderung zur Authentifizierung an.

Ein möglicher Grund hierfür ist, dass der ACS nicht für die Übertragung des Servicetyp-Attributs für diesen Benutzer oder diese Gruppe konfiguriert ist, obwohl Benutzername und Kennwort auf dem ACS korrekt konfiguriert sind.

Die Ausgabe des **debug aaa events enable** Befehls gibt nicht an, dass ein Benutzer nicht über die erforderlichen Attribute (in diesem Beispiel das Service-Type-Attribut) verfügt, obwohl ein **Accept-Accept** vom AAA-Server zurückgesendet wird. Dieses Beispiel **debug aaa events enable** zeigt ein Beispiel.

```
<#root>

(Cisco Controller) >


debug aaa events enable


Mon Aug 13 20:14:33 2011: AuthenticationRequest: 0xa449a8c
Mon Aug 13 20:14:33 2011: Callback.....................................0x8250c40
Mon Aug 13 20:14:33 2011: protocolType.................................0x00020001
```

```
Mon Aug 13 20:14:33 2011: proxyState.....................1A:00:00:00:00:00-00:00

Mon Aug 13 20:14:33 2011: Packet contains 5 AVPs (not shown)

Mon Aug 13 20:14:33 2011: 1a:00:00:00:00:00 Successful transmission of
Authentication Packet (id 8) to 172.16.1.1:1812, proxy state
1a:00:00:00:00:00-00:00

Mon Aug 13 20:14:33 2011: ****Enter processIncomingMessages: response code=2

Mon Aug 13 20:14:33 2011: ****Enter processRadiusResponse: response code=2
```

```
Mon Aug 13 20:14:33 2011: 1a:00:00:00:00:00 Access-Accept
received from RADIUS server 172.16.1.1 for mobile 1a:00:00:00:00:00 receiveId = 0
```

```
Mon Aug 13 20:14:33 2011: AuthorizationResponse: 0x9802520

Mon Aug 13 20:14:33 2011: structureSize..............................28

Mon Aug 13 20:14:33 2011: resultCode.................................0

Mon Aug 13 20:14:33 2011: protocolUsed...............................0x00000001

Mon Aug 13 20:14:33 2011: proxyState.....................1A:00:00:00:00:00-00:00

Mon Aug 13 20:14:33 2011: Packet contains 0 AVPs:
```

In diesem ersten Beispiel **debug aaa events enable** wird angezeigt, dass Access-Accept erfolgreich vom RADIUS-Server empfangen wurde, das Service-Type-Attribut jedoch nicht an den WLC übergeben wird. Dies liegt daran, dass der jeweilige Benutzer nicht mit diesem Attribut im ACS konfiguriert ist.

Cisco Secure ACS muss so konfiguriert werden, dass das Servicetyp-Attribut nach der Benutzerauthentifizierung zurückgegeben wird. Der Wert für das Attribut "Service-Type" muss je nach Benutzerberechtigungen entweder auf "**Administrative"** oder "**NAS-Prompt"** gesetzt werden.

In diesem zweiten Beispiel wird die **debug aaa events enable**Befehlsausgabe erneut veranschaulicht. Diesmal ist das Service-Type-Attribut im ACS jedoch auf **Administrative** festgelegt.

```
    <#root>

(Cisco Controller)>
```

**debug aaa events enable**

Mon Aug 13 20:17:02 2011: AuthenticationRequest: 0xa449f1c

Mon Aug 13 20:17:02 2011: Callback.....0x8250c40

Mon Aug 13 20:17:02 2011: protocolType.....0x00020001

Mon Aug 13 20:17:02 2011: proxyState.....1D:00:00:00:00:00-00:00

Mon Aug 13 20:17:02 2011: Packet contains 5 AVPs (not shown)

Mon Aug 13 20:17:02 2011: 1d:00:00:00:00:00 Successful transmission of
Authentication Packet (id 11) to 172.16.1.1:1812, proxy state
1d:00:00:00:00:00-00:00

Mon Aug 13 20:17:02 2011: ****Enter processIncomingMessages: response code=2

Mon Aug 13 20:17:02 2011: ****Enter processRadiusResponse: response code=2

**Mon Aug 13 20:17:02 2011: 1d:00:00:00:00:00 Access-Accept received
from RADIUS server 172.16.1.1 for mobile 1d:00:00:00:00:00 receiveId = 0**

Mon Aug 13 20:17:02 2011: AuthorizationResponse: 0x9802520

Mon Aug 13 20:17:02 2011: structureSize.....100

Mon Aug 13 20:17:02 2011: resultCode.....0

Mon Aug 13 20:17:02 2011: protocolUsed.....0x00000001

Mon Aug 13 20:17:02 2011: proxyState.....1D:00:00:00:00:00-00:00

Mon Aug 13 20:17:02 2011: Packet contains 2 AVPs:

**Mon Aug 13 20:17:02 2011: AVP[01] Service-Type.....0x00000006 (6) (4 bytes)**

Mon Aug 13 20:17:02 2011: AVP[02] Class.....

```
CISCOACS:000d1b9f/ac100128/acsserver (36 bytes)
```

In der Ausgabe des vorherigen Beispiels sehen Sie, dass das Service-Type-Attribut an den WLC übergeben wird.

## Zugehörige Informationen

- **Konfigurieren des Wireless LAN-Controllers - Konfigurationsleitfaden**
- **Konfigurieren von VLANs auf Wireless LAN-Controllern**
- **Konfigurieren eines RADIUS-Servers und eines WLC für die dynamische VLAN-Zuweisung**
- **Konfigurieren von Wireless LAN-Controllern und Lightweight Access Point Basic**
- **Konfigurieren der AP-Gruppen-VLANs mithilfe von Wireless LAN Controllern**
- **Technischer Support und Downloads von Cisco**

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.