Konfiguration von Cisco Unified Wireless Network TACACS+

Inhalt

Einführung

Dieses Dokument enthält ein Konfigurationsbeispiel für das Terminal Access Controller Access Control System Plus (TACACS+) in einem Cisco Wireless LAN Controller (WLC) und ein Cisco

Wireless Control System (WCS) für ein Cisco Unified Wireless Network. Dieses Dokument enthält auch einige grundlegende Tipps zur Fehlerbehebung.

TACACS+ ist ein Client-/Serverprotokoll, das zentrale Sicherheit für Benutzer bietet, die versuchen, Verwaltungszugriff auf einen Router oder einen Netzwerkzugriffsserver zu erlangen. TACACS+ bietet folgende AAA-Dienste:

- Authentifizierung von Benutzern, die versuchen, sich bei Netzwerkgeräten anzumelden
- Autorisierung zur Bestimmung der Zugriffsstufe, die Benutzer benötigen
- Buchhaltung zur Nachverfolgung aller vom Benutzer vorgenommenen Änderungen

Weitere Informationen zu AAA-Services und TACACS+-Funktionen finden Sie unter Konfigurieren von TACACS+.

Im TACACS+- und RADIUS-Vergleich finden Sie einen Vergleich von TACACS+ und RADIUS.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Kenntnisse der Konfiguration von WLCs und Lightweight Access Points (LAPs) für den Basisbetrieb
- Kenntnis der LWAPP- (Lightweight Access Point Protocol) und Wireless-Sicherheitsmethoden
- Grundkenntnisse RADIUS und TACACS+
- Grundkenntnisse der Cisco ACS-Konfiguration

Verwendete Komponenten

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

- Cisco Secure ACS für Windows Version 4.0
- Cisco Wireless LAN Controller mit Version 4.1.171.0. Die TACACS+-Funktionalität auf WLCs wird von der Softwareversion 4.1.171.0 oder höher unterstützt.
- Cisco Wireless Control System mit Version 4.1.83.0. Die TACACS+-Funktionalität für WCS wird von der Softwareversion 4.1.83.0 oder höher unterstützt.

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).

TACACS+-Implementierung im Controller

Authentifizierung

Die Authentifizierung kann mit einem lokalen Datenbank-, RADIUS- oder TACACS+-Server erfolgen, der einen Benutzernamen und ein Kennwort verwendet. Die Implementierung ist nicht vollständig modular. Authentifizierungs- und Autorisierungsdienste sind miteinander verknüpft. Wenn z. B. die Authentifizierung mithilfe der RADIUS-/lokalen Datenbank durchgeführt wird, wird die Autorisierung nicht mit TACACS+ durchgeführt. Sie verwendet die Berechtigungen, die dem Benutzer in der lokalen oder RADIUS-Datenbank zugeordnet sind, z. B. Schreibzugriff oder Schreibzugriff, während die Autorisierung bei der Authentifizierung mit TACACS+ an TACACS+ gebunden ist.

In Fällen, in denen mehrere Datenbanken konfiguriert sind, wird eine CLI bereitgestellt, um die Reihenfolge festzulegen, in der die Backend-Datenbank referenziert werden soll.

Autorisierung

Die Autorisierung basiert nicht auf einer tatsächlichen, befehlsbasierten Autorisierung, sondern auf Aufgaben. Die Tasks sind verschiedenen Registerkarten zugeordnet, die den sieben Menüleisten entsprechen, die sich derzeit in der Web-GUI befinden. Die Menüleisten sind wie folgt:

- ÜBERWACHUNG
- WLANS
- CONTROLLER
- WIRELESS
- SICHERHEIT
- MANAGEMENT
- COMMAND

Der Grund für diese Zuordnung basiert auf der Tatsache, dass die meisten Kunden die Webschnittstelle verwenden, um den Controller anstelle der CLI zu konfigurieren.

Eine zusätzliche Rolle für das Lobby-Admin-Management (LOBBY) steht Benutzern zur Verfügung, die nur über Lobby-Admin-Berechtigungen verfügen müssen.

Die Aufgabe, die einem Benutzer zugewiesen ist, wird auf dem TACACS+ (ACS)-Server mithilfe der benutzerdefinierten Attribut-Wert (AV)-Paare konfiguriert. Der Benutzer kann für eine oder mehrere Aufgaben autorisiert werden. Die minimale Autorisierung ist nur MONITOR und die maximale ist ALL (alle sieben Registerkarten können ausgeführt werden). Wenn ein Benutzer für eine bestimmte Aufgabe nicht berechtigt ist, kann er weiterhin im schreibgeschützten Modus auf diese Aufgabe zugreifen. Wenn die Authentifizierung aktiviert ist und der Authentifizierungsserver nicht erreichbar oder nicht autorisiert werden kann, kann sich der Benutzer nicht beim Controller anmelden.

Hinweis: Damit eine grundlegende Verwaltungsauthentifizierung über TACACS+ erfolgreich ist, müssen Sie Authentifizierungs- und Autorisierungsserver auf dem WLC konfigurieren. Die Konfiguration der Buchhaltung ist optional.

Buchhaltung

Die Abrechnung erfolgt immer dann, wenn eine bestimmte vom Benutzer initiierte Aktion erfolgreich ausgeführt wird. Die geänderten Attribute werden zusammen mit den folgenden Protokollen im TACACS+-Accounting-Server protokolliert:

- Die Benutzer-ID der Person, die die Änderung vorgenommen hat
- Der Remote-Host, von dem aus der Benutzer angemeldet ist
- Datum und Uhrzeit der Ausführung des Befehls
- Autorisierungsstufe des Benutzers
- Eine Zeichenfolge, die Informationen darüber bereitstellt, welche Aktion ausgeführt wurde und welche Werte bereitgestellt wurden

Wenn der Accounting-Server nicht erreichbar ist, kann der Benutzer die Sitzung trotzdem fortsetzen.

Hinweis: Buchhaltungsdatensätze werden in Softwareversion 4.1 oder höher nicht aus WCS generiert.

TACACS+-Konfiguration im WLC

In der WLC-Softwareversion 4.1.171.0 und höher werden neue CLIs und webbasierte GUI-Änderungen eingeführt, um die TACACS+-Funktionalität auf dem WLC zu aktivieren. Die eingeführten CLIs werden in diesem Abschnitt als Referenz aufgeführt. Die entsprechenden Änderungen für die Web-GUI werden unter der Registerkarte Sicherheit hinzugefügt.

In diesem Dokument wird davon ausgegangen, dass die grundlegende Konfiguration des WLC bereits abgeschlossen ist.

Um TACACS+ im WLC-Controller zu konfigurieren, müssen Sie die folgenden Schritte ausführen:

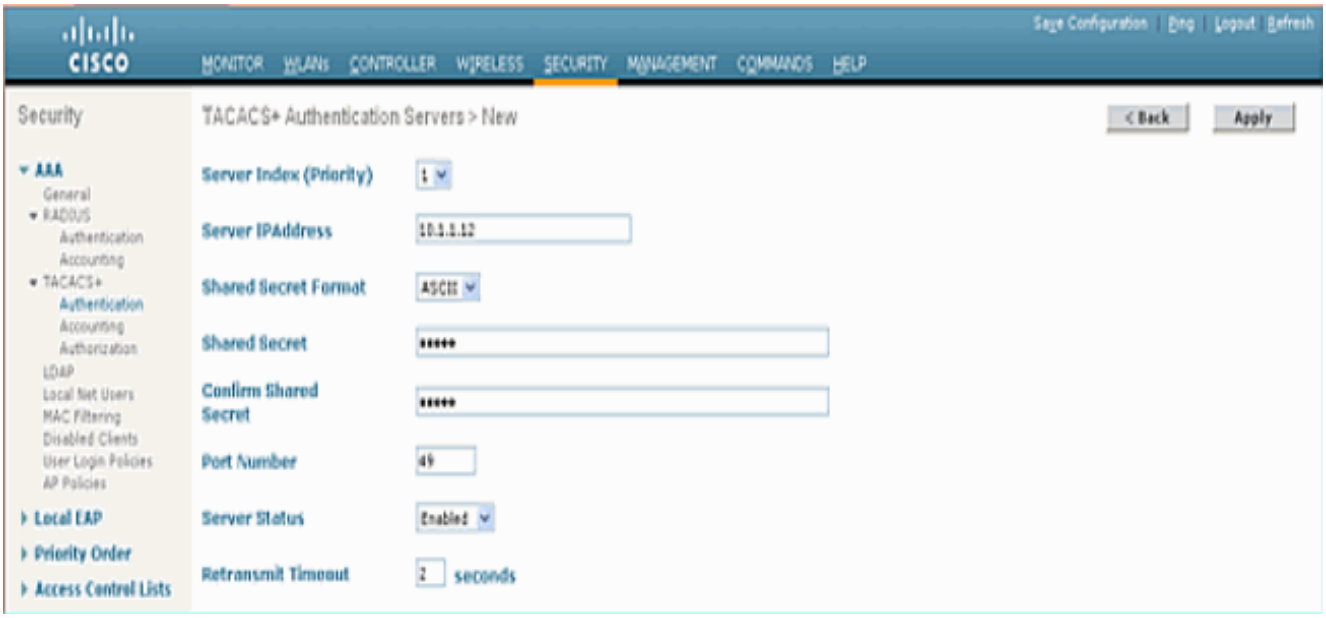
1. Hinzufügen eines TACACS+-Authentifizierungsservers
2. Hinzufügen eines TACACS+-Autorisierungsservers
3. Hinzufügen eines TACACS+-Accounting-Servers
4. Konfigurieren der Authentifizierungsreihenfolge

Hinzufügen eines TACACS+-Authentifizierungsservers

Gehen Sie wie folgt vor, um einen TACACS+-Authentifizierungsserver hinzuzufügen:

1. Klicken Sie in der GUI auf **Security > TACACS+ > Authentication (Sicherheit > TACACS+ > Authentifizierung)**.

2. Fügen Sie die IP-Adresse des TACACS+-Servers hinzu, und geben Sie den gemeinsamen geheimen Schlüssel ein. Ändern Sie ggf. den Standard-Port von TCP/49.

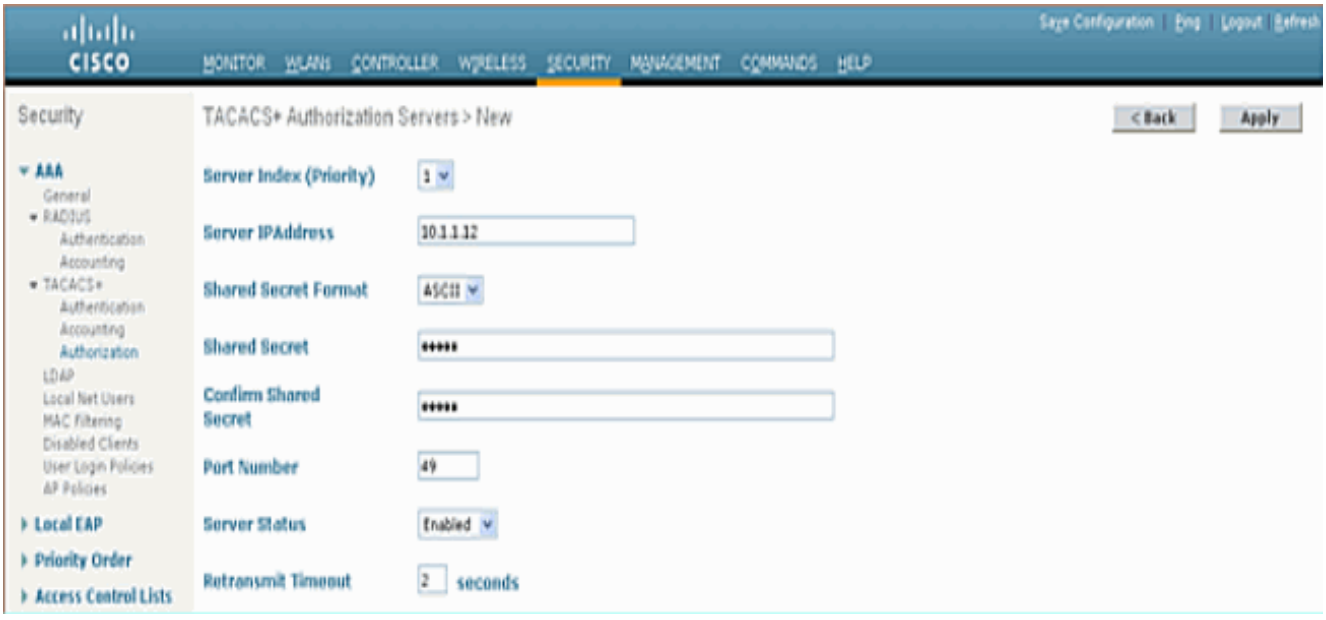


3. Klicken Sie auf **Apply** (Anwenden).Sie können dies über die CLI mit dem Befehl **config tacacs auth add** *<Server Index> <IP-Adresse> <Port> [ascii/hex]* **<secret>**-Befehl erreichen:
```
(Cisco Controller) >config tacacs auth add 1 10.1.1.12 49 ascii cisco123
```

Hinzufügen eines TACACS+-Autorisierungsservers

Gehen Sie wie folgt vor, um einen TACACS+-Autorisierungsserver hinzuzufügen:

1. Gehen Sie in der GUI zu **Security > TACACS+ > Authorization**.
2. Fügen Sie die IP-Adresse des TACACS+-Servers hinzu, und geben Sie den gemeinsamen geheimen Schlüssel ein. Ändern Sie ggf. den Standard-Port von TCP/49.



3. Klicken Sie auf **Apply** (Anwenden).Sie können dies über die CLI mithilfe der **Konfigurationstaktiken durch add** *<Server Index> <IP-Adresse> <Port> [ascii/hex]* **<secret>**-Befehl erreichen:
```
(Cisco Controller) >config tacacs athr add 1 10.1.1.12 49 ascii cisco123
```

Hinzufügen eines TACACS+-Accounting-Servers

Gehen Sie wie folgt vor, um einen TACACS+-Accounting-Server hinzuzufügen:

1. Klicken Sie in der GUI auf **Security > TACACS+ > Accounting**.
2. Fügen Sie die IP-Adresse des Servers hinzu, und geben Sie den gemeinsamen geheimen Schlüssel ein. Ändern Sie ggf. den Standard-Port von TCP/49.

3. Klicken Sie auf **Apply** (Anwenden).Sie können dies über die CLI mithilfe des **config tacacs acct add** *<Server Index> <IP-Adresse> <port> [ascii/hex]* **<secret>**-Befehls **erreichen**:

```
(Cisco Controller) >config tacacs acct add 1 10.1.1.12 49 ascii cisco123
```

Konfigurieren der Authentifizierungsreihenfolge

In diesem Schritt wird erläutert, wie die AAA-Reihenfolge für die Authentifizierung konfiguriert wird, wenn mehrere Datenbanken konfiguriert sind. Die Reihenfolge der Authentifizierung kann **lokal und RADIUS**, **lokal und TACACS** sein. Die Standardkonfiguration des Controllers für die Authentifizierungsreihenfolge ist *lokal und RADIUS*.

Gehen Sie wie folgt vor, um die Reihenfolge der Authentifizierung zu konfigurieren:

1. Gehen Sie in der GUI zu **Security > Priority Order > Management User**.
2. Wählen Sie die Authentifizierungspriorität aus.In diesem Beispiel wurde TACACS+ ausgewählt.
3. Klicken Sie auf **Apply** (Übernehmen), um die Auswahl zu treffen.

Sie können dies über die CLI mithilfe des Befehls **config aaa auth mgmt *<server1> <server2>*** **erreichen:**

```
(Cisco Controller) >config aaa auth mgmt tacacs local
```

Konfiguration überprüfen

In diesem Abschnitt werden die Befehle zum Überprüfen der TACACS+-Konfiguration auf dem WLC beschrieben. Dies sind einige nützliche **show**-Befehle, mit denen Sie feststellen können, ob die Konfiguration korrekt ist:

- **show aaa auth**: Stellt Informationen zur Reihenfolge der Authentifizierung bereit.

```
(Cisco Controller) >show aaa auth
Management authentication server order:
    1..................................... local
    2..................................... Tacacs
```

- **show tacacs summary**: Zeigt eine Zusammenfassung der TACACS+-Dienste und -Statistiken an.

```
(Cisco Controller) >show tacacs summary
Authentication Servers

Idx  Server Address    Port    State     Tout
---  ---------------  ------  --------  ----
1    10.1.1.12         49      Enabled   2

Authorization Servers

Idx  Server Address    Port    State     Tout
---  ---------------  ------  --------  ----
1    10.1.1.12         49      Enabled   2

Accounting Servers

Idx  Server Address    Port    State     Tout
---  ---------------  ------  --------  ----
1    10.1.1.12         49      Enabled   2
```

- **show tacacs auth stats**: Zeigt Statistiken des TACACS+-Authentifizierungsservers an.

```
(Cisco Controller) >show tacacs auth statistics
Authentication Servers:

Server Index..................................... 1
Server Address..................................... 10.1.1.12
Msg Round Trip Time.............................. 0 (1/100 second)
First Requests................................... 7
Retry Requests................................... 3
Accept Responses................................. 3
Reject Responses................................. 0
Error Responses.................................. 0
Restart Responses................................ 0
Follow Responses................................. 0
GetData Responses................................ 0
Encrypt no secret Responses...................... 0
Challenge Responses.............................. 0
Malformed Msgs................................... 0
Bad Authenticator Msgs........................... 0
Timeout Requests................................. 12
Unknowntype Msgs................................. 0
Other Drops...................................... 0
```

- **show tacacs athr stats**: Zeigt Statistiken des TACACS+-Autorisierungsservers an.

```
(Cisco Controller) >show tacacs athr statistics
```

```
Authorization Servers:

Server Index..................................... 1
Server Address................................... 10.1.1.12
Msg Round Trip Time.............................. 0 (1/100 second)
First Requests................................... 3
Retry Requests................................... 3
Received Responses............................... 3
Authorization Success............................ 3
Authorization Failure............................ 0
Challenge Responses.............................. 0
Malformed Msgs................................... 0
Bad Athrenticator Msgs........................... 0
Timeout Requests................................. 0
Unknowntype Msgs................................. 0
Other Drops...................................... 0
```

- **show tacacs acct state** (**takaktische Zugriffsstatistiken anzeigen**): Zeigt Statistiken des TACACS+-Accounting-Servers an.

```
(Cisco Controller) >show tacacs acct statistics
Accounting Servers:

Server Index..................................... 1
Server Address................................... 10.1.1.12
Msg Round Trip Time.............................. 0 (1/100 second)
First Requests................................... 133
Retry Requests................................... 0
Accounting Response.............................. 0
Accounting Request Success....................... 0
Accounting Request Failure....................... 0
Malformed Msgs................................... 0
Bad Authenticator Msgs........................... 0
Timeout Requests................................. 399
Unknowntype Msgs................................. 0
Other Drops...................................... 0
```

Konfigurieren des Cisco Secure ACS Servers

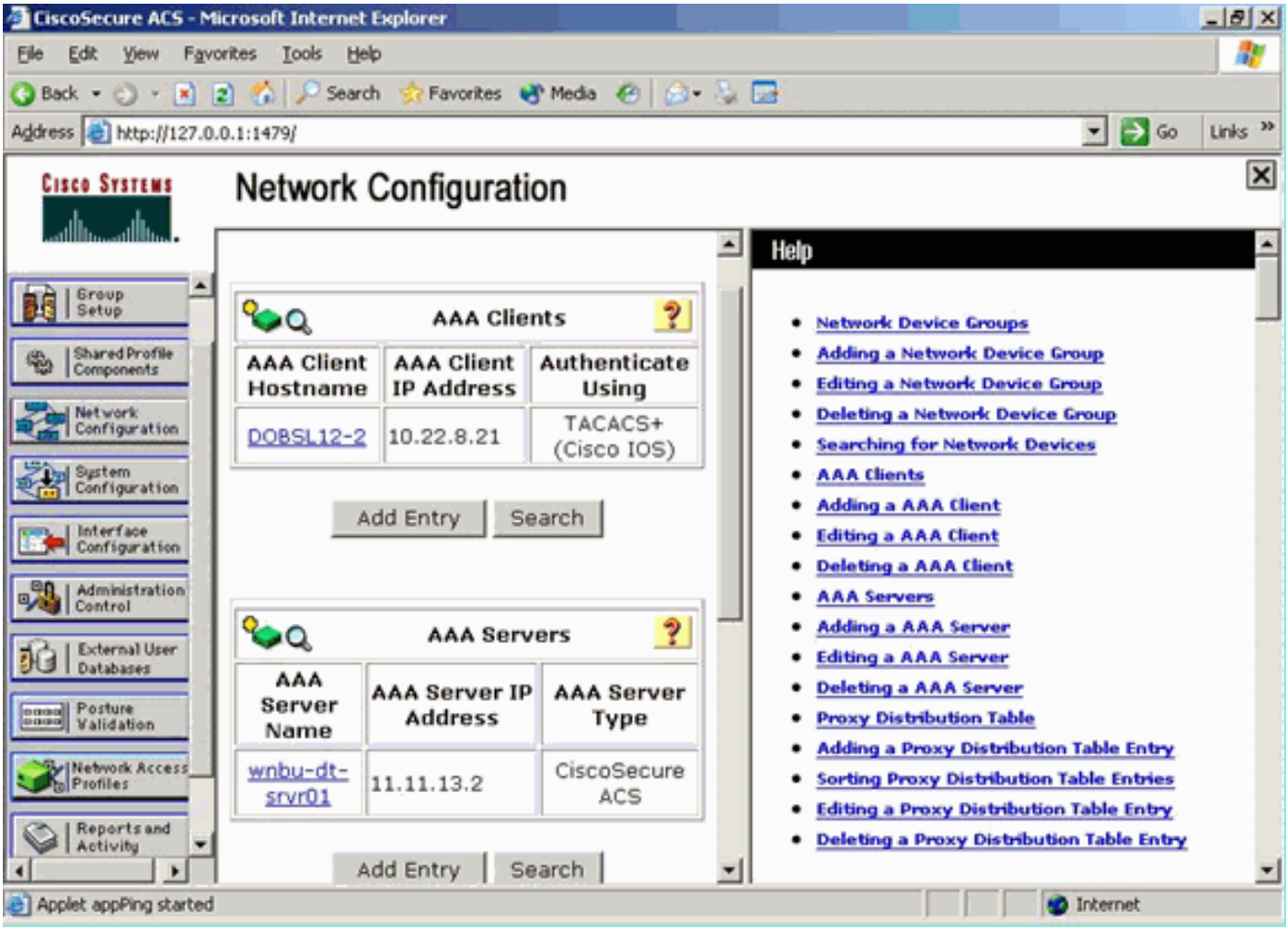
Dieser Abschnitt enthält die Schritte, die im TACACS+ ACS-Server zum Erstellen von Diensten und benutzerdefinierten Attributen und zum Zuweisen der Rollen für Benutzer oder Gruppen durchgeführt werden.

Die Erstellung von Benutzern und Gruppen wird in diesem Abschnitt nicht erläutert. Es wird davon ausgegangen, dass die Benutzer und Gruppen nach Bedarf erstellt werden. Weitere Informationen zum Erstellen von Benutzern und Benutzergruppen finden Sie im Benutzerhandbuch für Cisco Secure ACS für Windows Server 4.0.

Netzwerkkonfiguration

Führen Sie diesen Schritt aus:

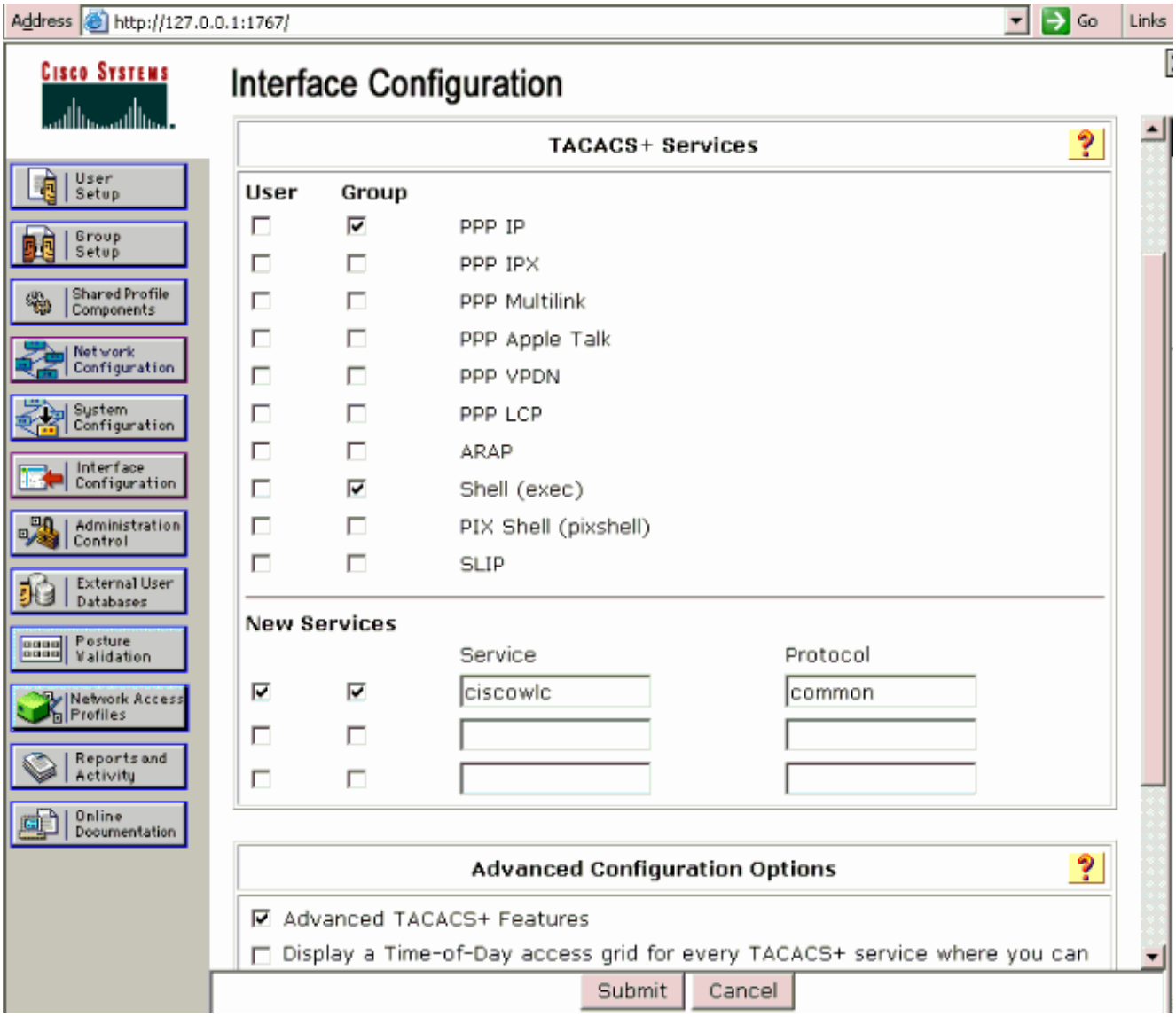
Fügen Sie die IP-Adresse für das Controller-Management als AAA-Client mit dem Authentifizierungsmechanismus TACACS+ (Cisco IOS) hinzu.



Schnittstellenkonfiguration

Führen Sie diese Schritte aus:

1. Wählen Sie im Menü Schnittstellenkonfiguration den Link **TACACS+** (Cisco IOS) aus.
2. Aktivieren Sie die **neuen Services**.
3. Aktivieren Sie die Kontrollkästchen **Benutzer** und **Gruppe**.
4. Geben Sie **ciscowlc** für Service und **common** for Protocol ein.
5. Aktivieren Sie die **erweiterten TACACS+-Funktionen**.

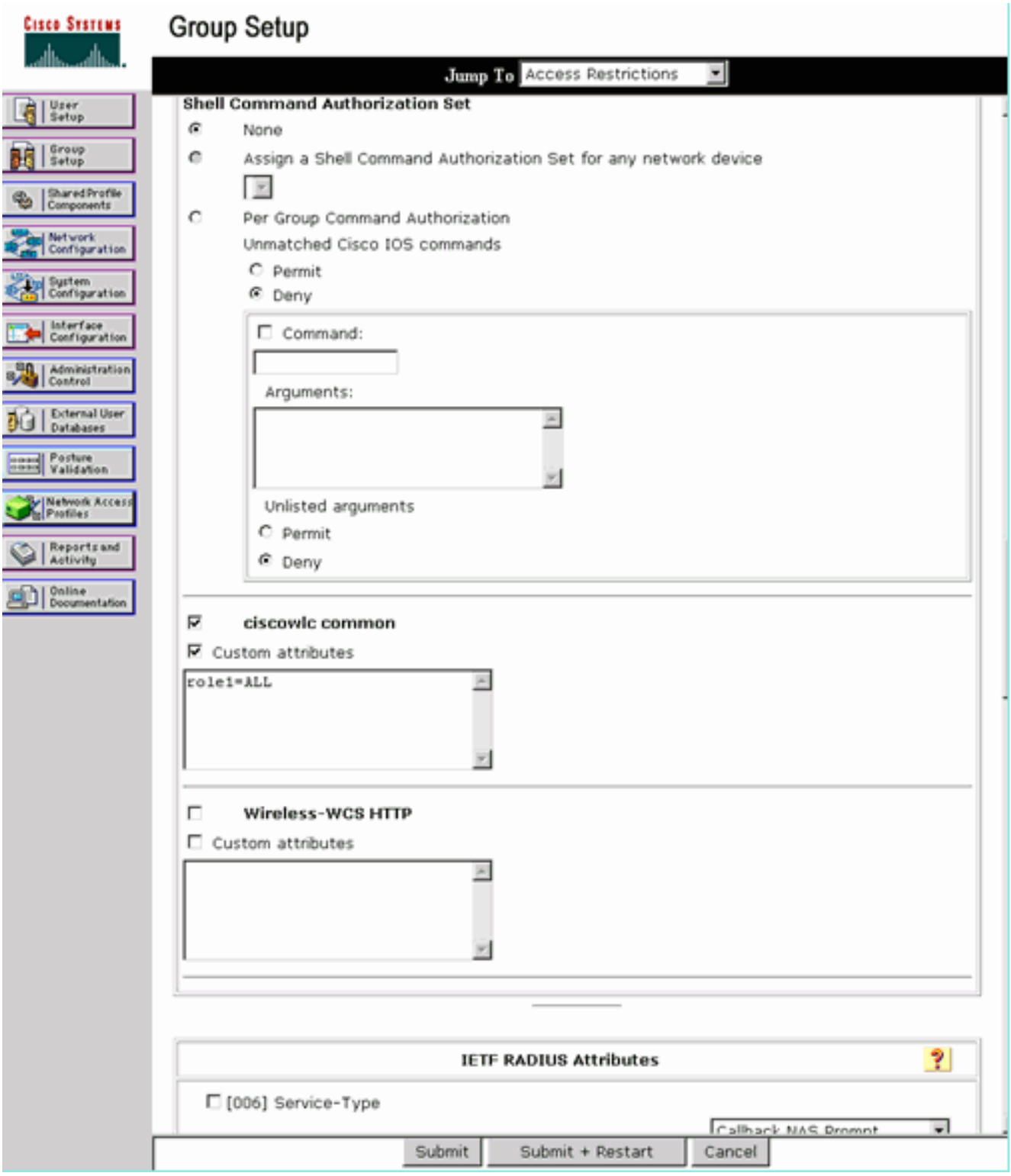


6. Klicken Sie auf **Senden**, um die Änderungen zu übernehmen.

Benutzer-/Gruppeneinrichtung

Führen Sie diese Schritte aus:

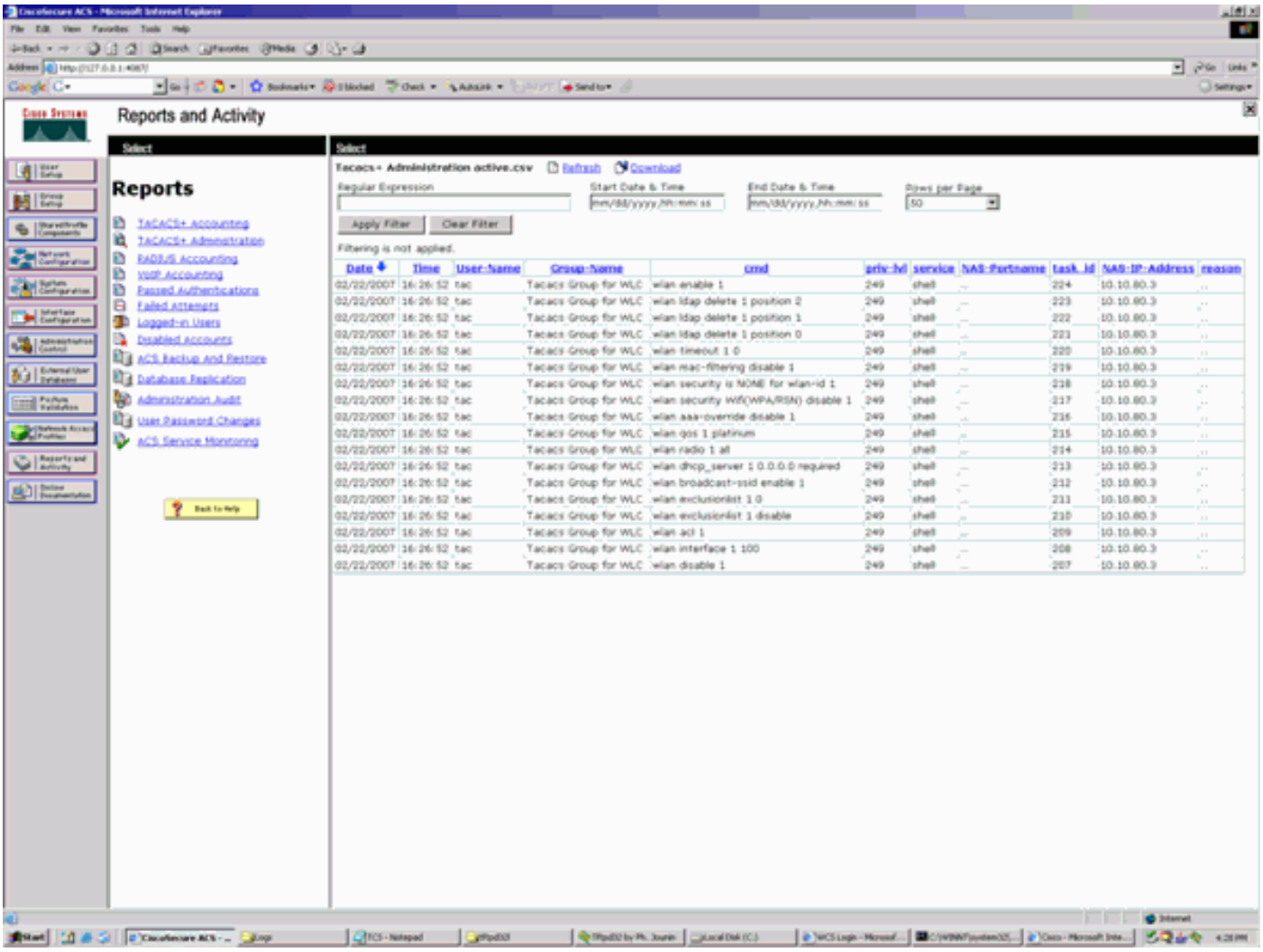
1. Wählen Sie einen zuvor erstellten Benutzer/eine Gruppe aus.
2. Gehen Sie zu **TACACS+ Settings**.
3. Aktivieren Sie das Kontrollkästchen für den *ciscowlc*-Dienst, der im Abschnitt "Schnittstellenkonfiguration" erstellt wurde.
4. Aktivieren Sie das Kontrollkästchen **Benutzerdefinierte Attribute**.



5. Geben Sie in das Textfeld unter Benutzerdefinierte Attribute diesen Text ein, wenn der erstellte Benutzer nur Zugriff auf WLAN, SECURITY und CONTROLLER benötigt: **role1=WLAN role2=SECURITY role3=CONTROLLER**.Wenn der Benutzer nur Zugriff auf die Registerkarte SICHERHEIT benötigt, geben Sie den folgenden Text ein: **role1=SECURITY**.Die Rolle entspricht den sieben Menüleisten in der grafischen Benutzeroberfläche des Controllers. Die Menüleisten sind MONITOR, WLAN, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT und COMMAND.
6. Geben Sie die Rolle ein, die ein Benutzer für Rolle 1, Rolle 2 usw. benötigt. Wenn ein Benutzer alle Rollen benötigt, sollte das Schlüsselwort **ALL** verwendet werden. Für die Rolle des Lobby-Administrators sollte das Schlüsselwort **LOBBY** verwendet werden.

Buchhaltung von Datensätzen in Cisco Secure ACS

Die TACACS+-Accounting-Datensätze des WLC sind in Cisco Secure ACS in der TACACS+-Verwaltung von Berichten und Aktivitäten verfügbar:



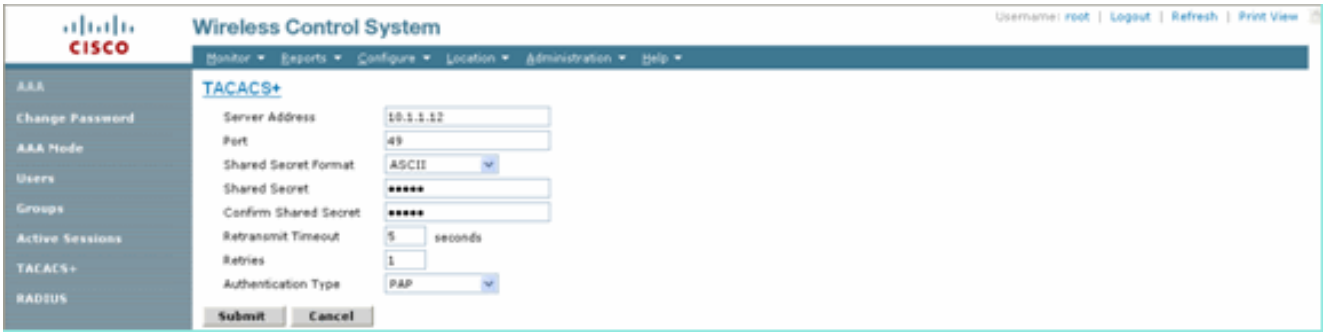
TACACS+-Konfiguration im WCS

Führen Sie diese Schritte aus:

1. Melden Sie sich über die GUI mit dem Root-Konto beim WCS an.
2. Fügen Sie den TACACS+-Server hinzu. Gehen Sie zu **Administration > AAA > TACACS+ > Add TACACS+ Server**.

3. Fügen Sie die TACACS+-Serverdetails hinzu, z. B. IP-Adresse, Portnummer (standardmäßig

49) und gemeinsam genutzter geheimer Schlüssel.



4. Aktivieren Sie die TACACS+-Authentifizierung für die Administration im WCS. Gehen Sie zu **Administration > AAA > AAA Mode > Select TACACS+**.

WCS mit virtuellen Domänen

Virtual Domain ist eine neue Funktion, die mit WCS Version 5.1 eingeführt wurde. Eine virtuelle WCS-Domäne besteht aus einer Reihe von Geräten und Zuordnungen und beschränkt die Ansicht eines Benutzers auf Informationen, die für diese Geräte und Karten relevant sind. Über eine virtuelle Domäne kann ein Administrator sicherstellen, dass Benutzer nur die Geräte und Karten anzeigen können, für die sie zuständig sind. Darüber hinaus können Benutzer dank der Filter der virtuellen Domäne Alarme konfigurieren, anzeigen und Berichte nur für den zugewiesenen Teil des Netzwerks erstellen. Der Administrator legt für jeden Benutzer einen Satz zulässiger virtueller Domänen fest. Bei der Anmeldung kann nur einer von diesen Benutzern aktiv sein. Der Benutzer kann die aktuelle virtuelle Domäne ändern, indem er im Dropdown-Menü "Virtuelle Domäne" oben im Bildschirm eine andere zulässige virtuelle Domäne auswählt. Sämtliche Berichte, Alarme und andere Funktionen werden nun von dieser virtuellen Domäne gefiltert.

Wenn im System nur eine virtuelle Domäne definiert ist (root) und der Benutzer keine virtuellen Domänen in den benutzerdefinierten Attributfeldern im TACACS+/RADIUS-Server hat, wird dem Benutzer standardmäßig die virtuelle Stammdomäne zugewiesen.

Wenn es mehrere virtuelle Domänen gibt und der Benutzer über keine angegebenen Attribute verfügt, wird die Anmeldung des Benutzers blockiert. Damit sich der Benutzer anmelden kann, müssen die benutzerdefinierten Virtual Domain-Attribute auf den Radius/TACACS+-Server exportiert werden.

Im Fenster Benutzerdefinierte Attribute für virtuelle Domänen können Sie die entsprechenden protokollspezifischen Daten für jede virtuelle Domäne angeben. Die Schaltfläche Exportieren in der Seitenleiste der virtuellen Domänenhierarchie formatiert die RADIUS- und TACACS+-Attribute der virtuellen Domäne vorab. Sie können diese Attribute kopieren und in den ACS-Server einfügen. Dadurch können Sie nur die entsprechenden virtuellen Domänen auf den ACS-Serverbildschirm kopieren und sicherstellen, dass die Benutzer nur Zugriff auf diese virtuellen

Domänen haben.

Gehen Sie wie im Abschnitt "Virtuelle Domänen-RADIUS und TACACS+-Attribute" beschrieben vor, um die vorformatierten RADIUS- und TACACS+-Attribute auf den ACS-Server anzuwenden.

Konfigurieren von Cisco Secure ACS zur Verwendung von WCS

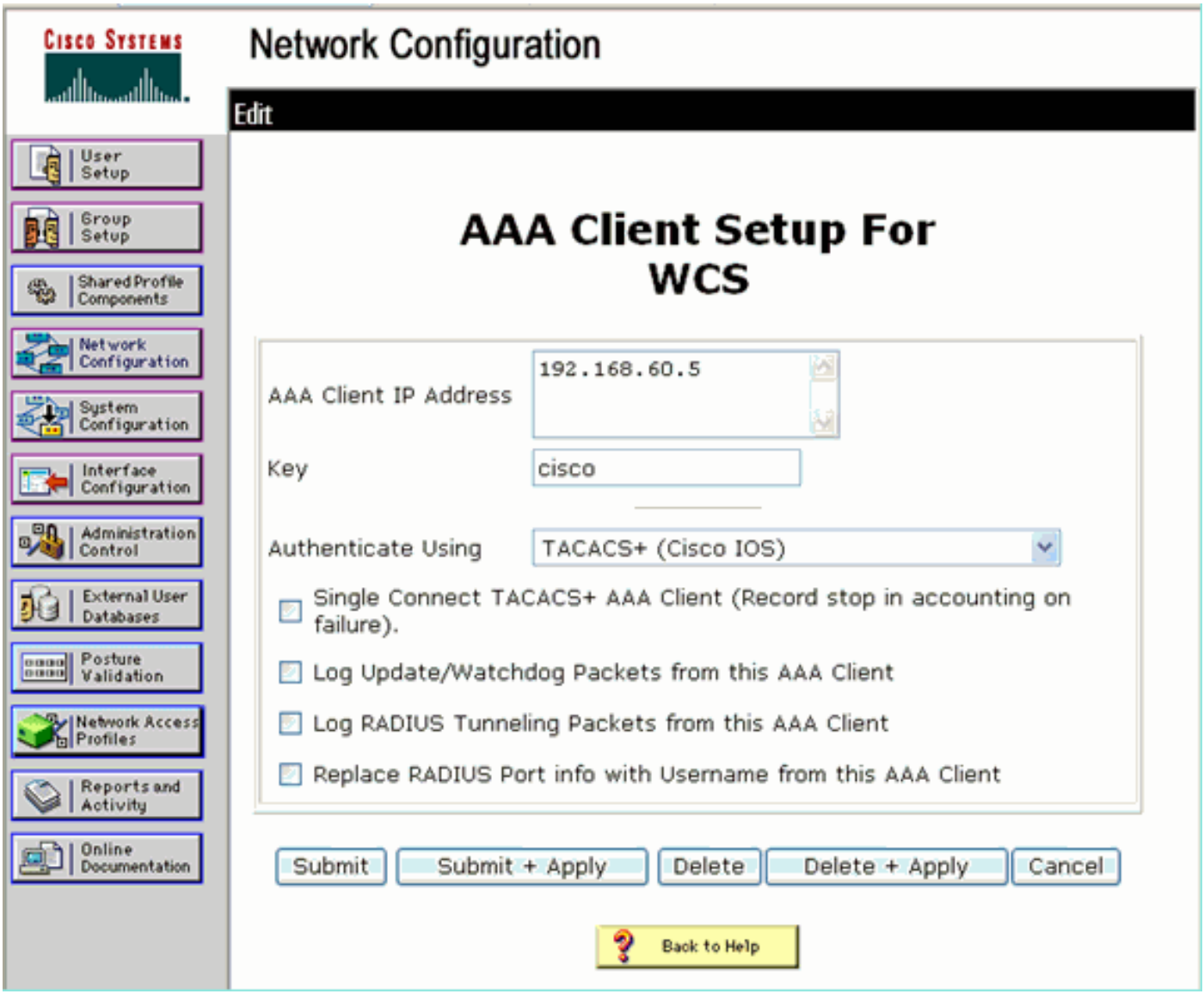
Der Abschnitt enthält die Schritte, die im TACACS+ ACS-Server zum Erstellen von Diensten und benutzerdefinierten Attributen und zum Zuweisen der Rollen für die Benutzer oder Gruppen erforderlich sind.

Die Erstellung von Benutzern und Gruppen wird in diesem Abschnitt nicht erläutert. Es wird davon ausgegangen, dass die Benutzer und Gruppen nach Bedarf erstellt werden.

Netzwerkkonfiguration

Führen Sie diesen Schritt aus:

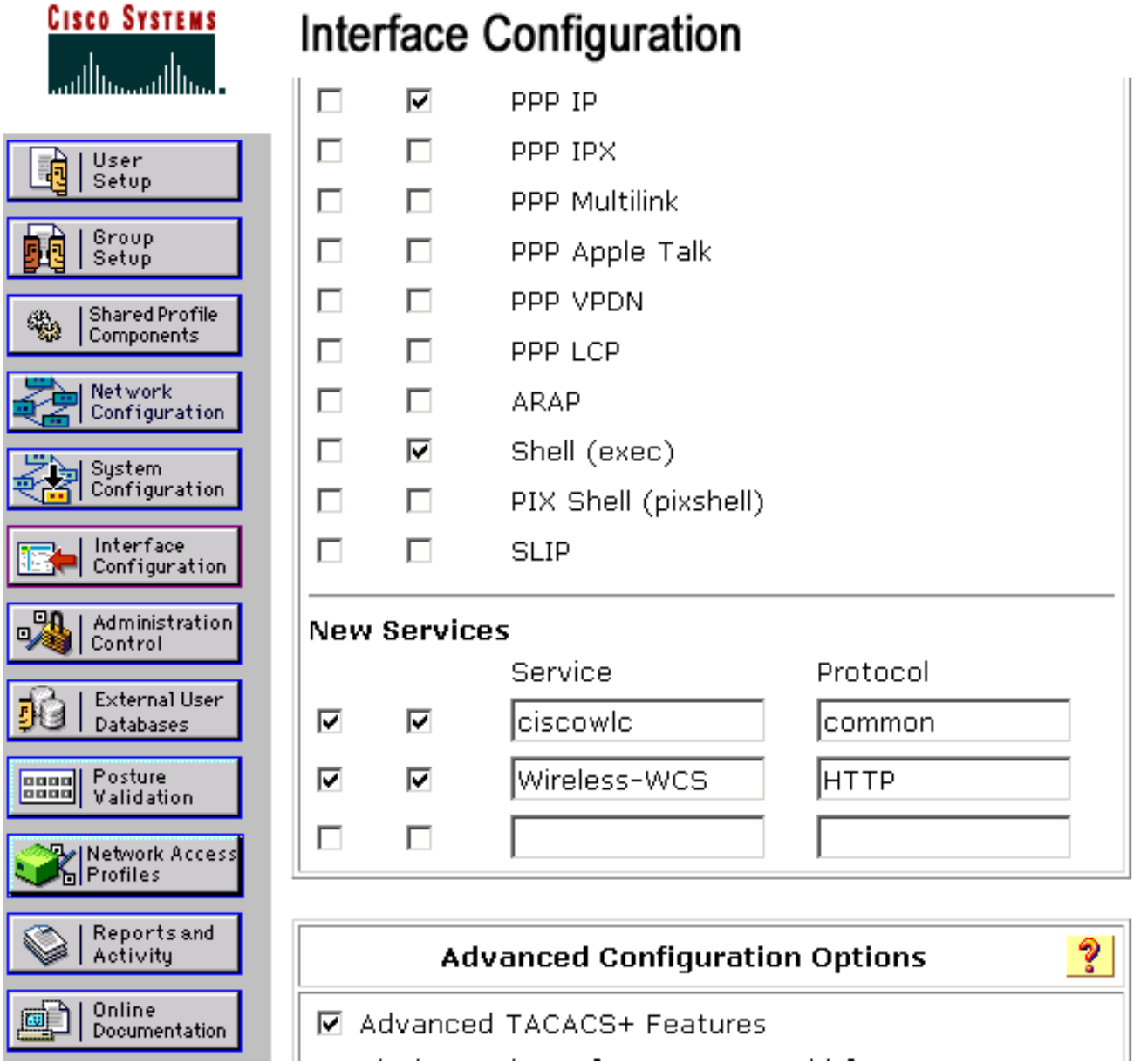
Fügen Sie die WCS-IP-Adresse als AAA-Client mit dem Authentifizierungsmechanismus TACACS+ (Cisco IOS) hinzu.



Schnittstellenkonfiguration

Führen Sie diese Schritte aus:

1. Wählen Sie im Menü Schnittstellenkonfiguration den Link **TACACS+** (Cisco IOS) aus.
2. Aktivieren Sie die **neuen Services**.
3. Aktivieren Sie die Kontrollkästchen **Benutzer** und **Gruppe**.
4. Geben Sie **Wireless-WCS** für Service und **HTTP** für Protocol ein.**Hinweis:** HTTP muss in CAPS sein.
5. Aktivieren Sie die **erweiterten TACACS+-Funktionen**.



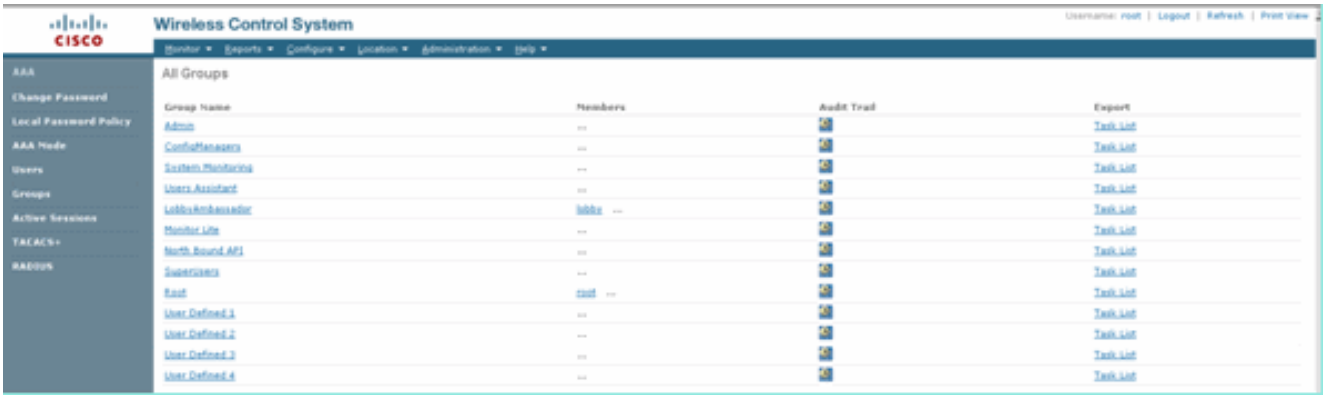
6. Klicken Sie auf **Senden**, um die Änderungen zu übernehmen.

Benutzer-/Gruppeneinrichtung

Führen Sie diese Schritte aus:

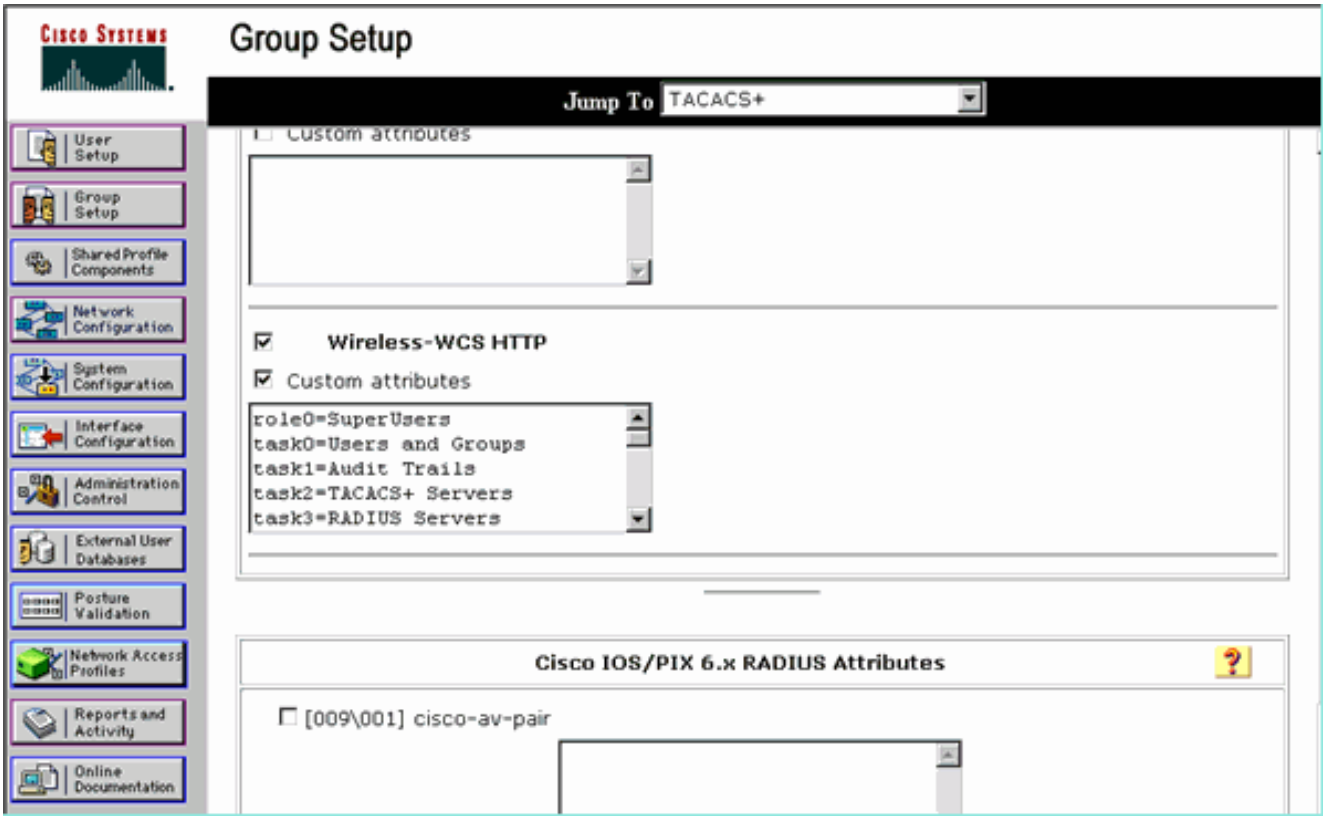
1. Navigieren Sie in der WCS-GUI zu **Administration > AAA > Groups**, um eine der vorkonfigurierten Benutzergruppen auszuwählen, z. B. SuperUsers im

WCS.



2. Wählen Sie die Aufgabenliste für die vorkonfigurierten Benutzergruppen aus, und kopieren Sie die Einfügen in den
ACS.

3. Wählen Sie einen zuvor erstellten Benutzer/eine Gruppe aus, und gehen Sie zu **TACACS+ Settings**.
4. Aktivieren Sie in der ACS-GUI das Kontrollkästchen für den zuvor erstellten Wireless-WCS-Service.
5. Aktivieren Sie in der ACS-GUI das Kontrollkästchen **Benutzerdefinierte Attribute**.
6. Geben Sie im Textfeld unter Benutzerdefinierte Attribute diese Rollen- und Aufgabeinformationen ein, die aus dem WCS kopiert werden. Geben Sie z. B. die Liste der Aufgaben ein, die von den SuperUsers zulässig
sind.



7. Melden Sie sich dann mit dem neu erstellten Benutzernamen/Kennwort im ACS beim WCS an.

Debugger

Debugger von WLC für role1=ALL

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

(Cisco Controller) >Wed Feb 28 17:36:37 2007: Forwarding request to 10.1.1.12 port=49
Wed Feb 28 17:36:37 2007: tplus response: type=1 seq_no=2 session_id=5eaa857e
length=16 encrypted=0
Wed Feb 28 17:36:37 2007: TPLUS_AUTHEN_STATUS_GETPASS
Wed Feb 28 17:36:37 2007: auth_cont get_pass reply: pkt_length=22
Wed Feb 28 17:36:37 2007: processTplusAuthResponse: Continue auth transaction
Wed Feb 28 17:36:37 2007: tplus response: type=1 seq_no=4 session_id=5eaa857e
length=6 encrypted=0
Wed Feb 28 17:36:37 2007: tplus_make_author_request() from tplus_authen_passed returns rc=0
Wed Feb 28 17:36:37 2007: Forwarding request to 10.1.1.12 port=49
Wed Feb 28 17:36:37 2007: author response body: status=1 arg_cnt=1 msg_len=0 data_len=0
Wed Feb 28 17:36:37 2007: arg[0] = [9][role1=ALL]
Wed Feb 28 17:36:37 2007: User has the following mgmtRole fffffff8
```

Debuggen aus WLC für mehrere Rollen

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

Wed Feb 28 17:59:33 2007: Forwarding request to 10.1.1.12 port=49
Wed Feb 28 17:59:34 2007: tplus response: type=1 seq_no=2
session_id=b561ad88 length=16 encrypted=0
Wed Feb 28 17:59:34 2007: TPLUS_AUTHEN_STATUS_GETPASS
Wed Feb 28 17:59:34 2007: auth_cont get_pass reply: pkt_length=22
Wed Feb 28 17:59:34 2007: processTplusAuthResponse: Continue auth transaction
```

```
Wed Feb 28 17:59:34 2007: tplus response: type=1 seq_no=4 session_id=b561ad88
length=6 encrypted=0
Wed Feb 28 17:59:34 2007: tplus_make_author_request() from tplus_authen_passed
returns rc=0
Wed Feb 28 17:59:34 2007: Forwarding request to 10.1.1.12 port=49
Wed Feb 28 17:59:34 2007: author response body: status=1 arg_cnt=4 msg_len=0 data_len=0
Wed Feb 28 17:59:34 2007: arg[0] = [11][role1=WLAN]
Wed Feb 28 17:59:34 2007: arg[1] = [16][role2=CONTROLLER]
Wed Feb 28 17:59:34 2007: arg[2] = [14][role3=SECURITY]
Wed Feb 28 17:59:34 2007: arg[3] = [14][role4=COMMANDS]
Wed Feb 28 17:59:34 2007: User has the following mgmtRole 150
```

Debuggen von einem WLC für Autorisierungsfehler

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

Wed Feb 28 17:53:04 2007: Forwarding request to 10.1.1.12 port=49
Wed Feb 28 17:53:04 2007: tplus response: type=1 seq_no=2 session_id=89c553a1
length=16 encrypted=0
Wed Feb 28 17:53:04 2007: TPLUS_AUTHEN_STATUS_GETPASS
Wed Feb 28 17:53:04 2007: auth_cont get_pass reply: pkt_length=22
Wed Feb 28 17:53:04 2007: processTplusAuthResponse: Continue auth transaction
Wed Feb 28 17:53:04 2007: tplus response: type=1 seq_no=4 session_id=89c553a1
length=6 encrypted=0
Wed Feb 28 17:53:04 2007: tplus_make_author_request() from tplus_authen_passed
returns rc=0
Wed Feb 28 17:53:04 2007: Forwarding request to 10.1.1.12 port=49
Wed Feb 28 17:53:04 2007: author response body: status=16 arg_cnt=0 msg_len=0 data_len=0
Wed Feb 28 17:53:04 2007:User has the following mgmtRole 0
Wed Feb 28 17:53:04 2007: Tplus authorization for tac failed status=16
```

Zugehörige Informationen

- Konfigurationsbeispiel für die Webauthentifizierung mit dem Cisco Wireless LAN Controller (WLC) und Cisco ACS 5.x (TACACS+)
- Konfigurieren von TACACS+
- Konfigurieren der TACACS-Authentifizierung und -Autorisierung für Admin- und Nicht-Admin-Benutzer in ACS 5.1
- TACACS+- und RADIUS-Vergleich
- Technischer Support und Dokumentation für Cisco Systeme