

# Cisco Unified Wireless Network TACACS+ 컨피그레이션

## 목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기 규칙](#)

[컨트롤러의 TACACS+ 구현](#)

[인증](#)

[Authorization\(권한 부여\)](#)

[회계](#)

[WLC의 TACACS+ 컨피그레이션](#)

[TACACS+ 인증 서버 추가](#)

[TACACS+ 권한 부여 서버 추가](#)

[TACACS+ 계정 관리 서버 추가](#)

[인증 순서 구성](#)

[구성 확인](#)

[Cisco Secure ACS Server 구성](#)

[네트워크 구성](#)

[인터페이스 컨피그레이션](#)

[사용자/그룹 설정](#)

[Cisco Secure ACS의 회계 기록](#)

[WCS의 TACACS+ 컨피그레이션](#)

[가상 도메인을 사용하는 WCS](#)

[WCS를 사용하도록 Cisco Secure ACS 구성](#)

[네트워크 구성](#)

[인터페이스 컨피그레이션](#)

[사용자/그룹 설정](#)

[디버깅](#)

[역할1=ALL에 대해 WLC에서 디버깅](#)

[여러 역할에 대한 WLC에서 디버깅](#)

[권한 부여 실패를 위해 WLC에서 디버깅](#)

[관련 정보](#)

## [소개](#)

이 문서에서는 Cisco WLC(Wireless LAN Controller)의 TACACS+(Terminal Access Controller Access Control System Plus) 및 Cisco 통합 무선 네트워크용 Cisco WCS(Wireless Control

System)의 컨피그레이션 예를 제공합니다. 이 문서에서는 몇 가지 기본적인 문제 해결 팁을 제공합니다.

TACACS+는 라우터 또는 네트워크 액세스 서버에 대한 관리 액세스를 시도하는 사용자에게 중앙 집중식 보안을 제공하는 클라이언트/서버 프로토콜입니다. TACACS+는 다음 AAA 서비스를 제공합니다.

- 네트워크 장비에 로그인하려는 사용자의 인증
- 사용자가 가져야 하는 액세스 수준을 결정하는 권한 부여
- 사용자가 수행한 모든 변경 사항을 추적하는 계정 관리

AAA 서비스 및 TACACS+ 기능에 대한 자세한 내용은 TACACS+ 구성을 참조하십시오.

TACACS+ 및 RADIUS의 비교는 TACACS+ 및 RADIUS 비교를 참조하십시오.

## [사전 요구 사항](#)

### [요구 사항](#)

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 기본 운영을 위해 WLC 및 LAP(Lightweight Access Point)를 구성하는 방법에 대한 지식
- LWAPP(Lightweight Access Point Protocol) 및 무선 보안 방법에 대한 지식
- 기본 지식 RADIUS 및 TACACS+
- Cisco ACS 구성에 대한 기본 지식

### [사용되는 구성 요소](#)

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Secure ACS for Windows 버전 4.0
- 버전 4.1.171.0을 실행하는 Cisco Wireless LAN Controller. WLC의 TACACS+ 기능은 소프트웨어 버전 4.1.171.0 이상에서 지원됩니다.
- 버전 4.1.83.0을 실행하는 Cisco Wireless Control System. WCS의 TACACS+ 기능은 소프트웨어 버전 4.1.83.0 이상에서 지원됩니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

### [표기 규칙](#)

문서 규칙에 대한 자세한 내용은 [Cisco 기술 팁 표기 규칙을 참고하십시오](#).

## [컨트롤러의 TACACS+ 구현](#)

### [인증](#)

사용자 이름과 비밀번호를 사용하는 로컬 데이터베이스, RADIUS 또는 TACACS+ 서버를 사용하여 인증을 수행할 수 있습니다. 구현은 완전한 모듈형이 아닙니다. 인증 및 권한 부여 서비스는 서로 연

결되어 있습니다. 예를 들어 RADIUS/로컬 데이터베이스를 사용하여 인증을 수행하는 경우 TACACS+를 사용하여 권한 부여가 수행되지 않습니다. 로컬 또는 RADIUS 데이터베이스의 사용자(예: 읽기 전용 또는 읽기-쓰기)에 대한 권한을 사용하는 반면, TACACS+를 사용하여 인증을 수행할 경우 권한 부여는 TACACS+에 연결됩니다.

여러 데이터베이스가 구성된 경우 백엔드 데이터베이스를 참조하는 순서를 지정하는 CLI가 제공됩니다.

## Authorization(권한 부여)

권한 부여는 실제 명령별 기반 권한 부여가 아닌 작업을 기반으로 합니다. 작업은 현재 웹 GUI에 있는 7개의 메뉴 모음 항목에 해당하는 다양한 탭에 매핑됩니다. 다음은 메뉴 모음 항목입니다.

- 모니터
- WLANS
- 컨트롤러
- 무선
- 보안
- 관리
- 명령을 사용합니다

이러한 매핑의 이유는 대부분의 고객이 웹 인터페이스를 사용하여 CLI 대신 컨트롤러를 구성한다는 사실에 기반을 두고 있습니다.

로비 관리자 관리(LOBBY)에 대한 추가 역할은 로비 관리자 권한만 가져야 하는 사용자에게 제공됩니다.

사용자가 자격이 있는 작업은 사용자 지정 AV(Attribute-Value) 쌍을 사용하여 TACACS+(ACS) 서버에 구성됩니다. 사용자는 하나 이상의 작업에 대한 권한을 부여할 수 있습니다. 최소 권한 부여는 MONITOR만, 최대값은 ALL입니다(7개 탭을 모두 수행할 수 있음). 사용자가 특정 작업에 대한 자격이 없는 경우 사용자는 읽기 전용 모드에서 해당 작업에 액세스할 수 있습니다. 인증이 활성화되고 인증 서버에 연결할 수 없거나 권한을 부여할 수 없는 경우 사용자는 컨트롤러에 로그인할 수 없습니다.

**참고:** TACACS+를 통한 기본 관리 인증이 성공하려면 WLC에서 인증 및 권한 부여 서버를 구성해야 합니다. 계정 설정은 선택 사항입니다.

## 회계

계정 관리는 특정 사용자가 시작한 작업이 성공적으로 수행될 때마다 발생합니다. 변경된 특성은 다음과 함께 TACACS+ 계정 관리 서버에 기록됩니다.

- 변경을 한 개인의 사용자 ID입니다.
- 사용자가 로그인한 원격 호스트
- 명령을 수행한 날짜 및 시간
- 사용자의 권한 부여 수준
- 수행된 작업 및 제공된 값에 대한 정보를 제공하는 문자열

어카운팅 서버에 연결할 수 없게 되면 사용자는 세션을 계속할 수 있습니다.

**참고:** 어카운팅 레코드는 소프트웨어 릴리스 4.1 이상에서 WCS에서 생성되지 않습니다.

# WLC의 TACACS+ 컨피그레이션

WLC 소프트웨어 릴리스 4.1.171.0 이상에서는 WLC에서 TACACS+ 기능을 활성화하기 위해 새로운 CLI 및 웹 GUI 변경 사항이 도입되었습니다. 도입된 CLI는 이 섹션에 나와 있습니다. 웹 GUI에 대한 해당 변경 사항이 보안 탭에 추가됩니다.

이 문서에서는 WLC의 기본 컨피그레이션이 이미 완료된 것으로 가정합니다.

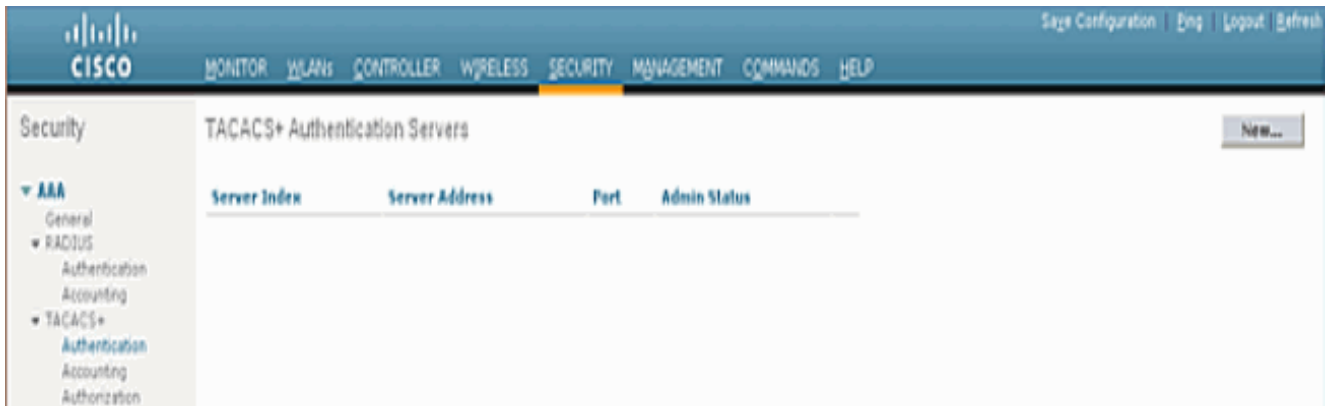
WLC 컨트롤러에서 TACACS+를 구성하려면 다음 단계를 완료해야 합니다.

1. [TACACS+ 인증 서버 추가](#)
2. [TACACS+ 권한 부여 서버 추가](#)
3. [TACACS+ 계정 관리 서버 추가](#)
4. [인증 순서 구성](#)

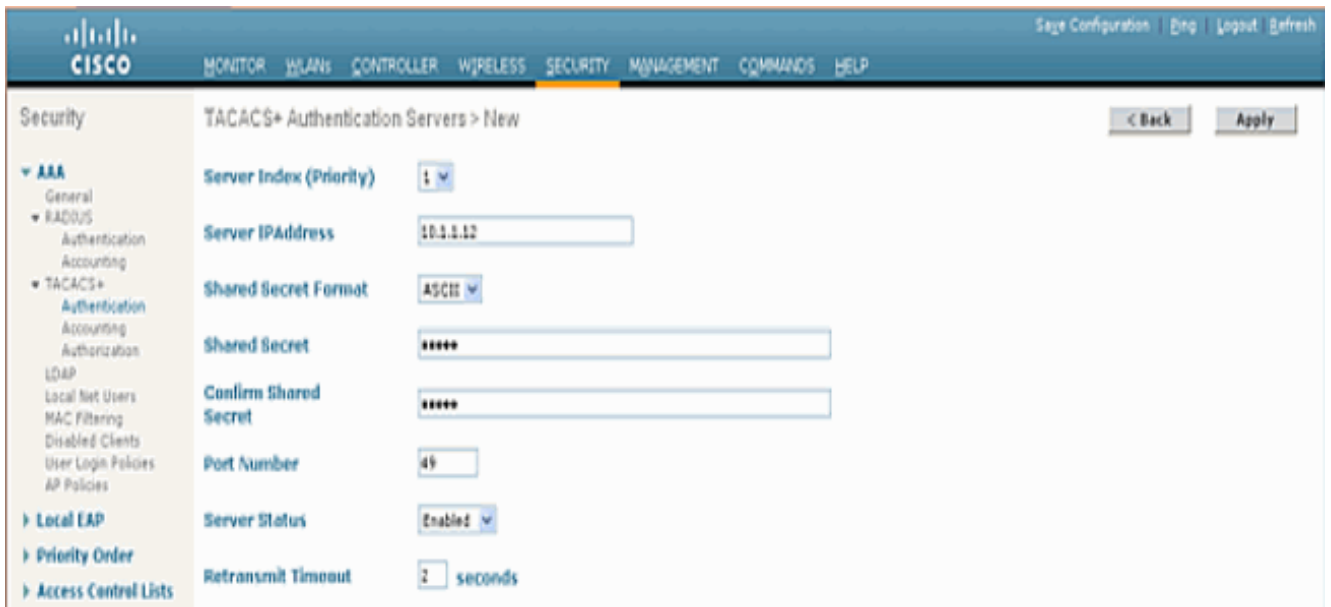
## TACACS+ 인증 서버 추가

TACACS+ 인증 서버를 추가하려면 다음 단계를 완료합니다.

1. GUI를 사용하여 Security(보안) > TACACS+ > Authentication(인증)으로 이동합니다



2. TACACS+ 서버의 IP 주소를 추가하고 공유 비밀 키를 입력합니다. 필요한 경우 TCP/49의 기본 포트를 변경합니다



3. Apply를 클릭합니다.config tacacs auth add <Server Index> <IP addr> <port> [ascii/hex] <secret> 명령을 사용하여 CLI에서 이를 수행할 수 있습니다.

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

## TACACS+ 권한 부여 서버 추가

TACACS+ 권한 부여 서버를 추가하려면 다음 단계를 완료합니다.

1. GUI에서 Security(보안) > TACACS+ > Authorization(권한 부여)으로 이동합니다.
2. TACACS+ 서버의 IP 주소를 추가하고 공유 비밀 키를 입력합니다. 필요한 경우 TCP/49의 기본 포트를 변경합니다

The screenshot shows the Cisco GUI for configuring a new TACACS+ Authorization Server. The page title is "TACACS+ Authorization Servers > New". The form includes the following fields and values:

- Server Index (Priority): 1
- Server IP Address: 10.1.1.12
- Shared Secret Format: ASCII
- Shared Secret: [masked]
- Confirm Shared Secret: [masked]
- Port Number: 49
- Server Status: Enabled
- Retransmit Timeout: 2 seconds

Navigation buttons for "< Back" and "Apply" are visible in the top right corner.

3. Apply를 클릭합니다.config tacacs를 사용하여 CLI에서 이 작업을 수행할 수 있습니다. add <Server Index> <IP addr> <port> [ascii/hex] <secret> 명령:

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

## TACACS+ 계정 관리 서버 추가

TACACS+ Accounting Server를 추가하려면 다음 단계를 완료합니다.

1. GUI를 사용하여 Security(보안) > TACACS+ > Accounting(계정 관리)으로 이동합니다.
2. 서버의 IP 주소를 추가하고 공유 비밀 키를 입력합니다. 필요한 경우 TCP/49의 기본 포트를 변경합니다



3. Apply를 클릭합니다. `config tacacs acct add <Server Index> <IP addr> <port> [ascii/hex] <secret>` 명령을 사용하여 CLI에서 이를 수행할 수 있습니다.

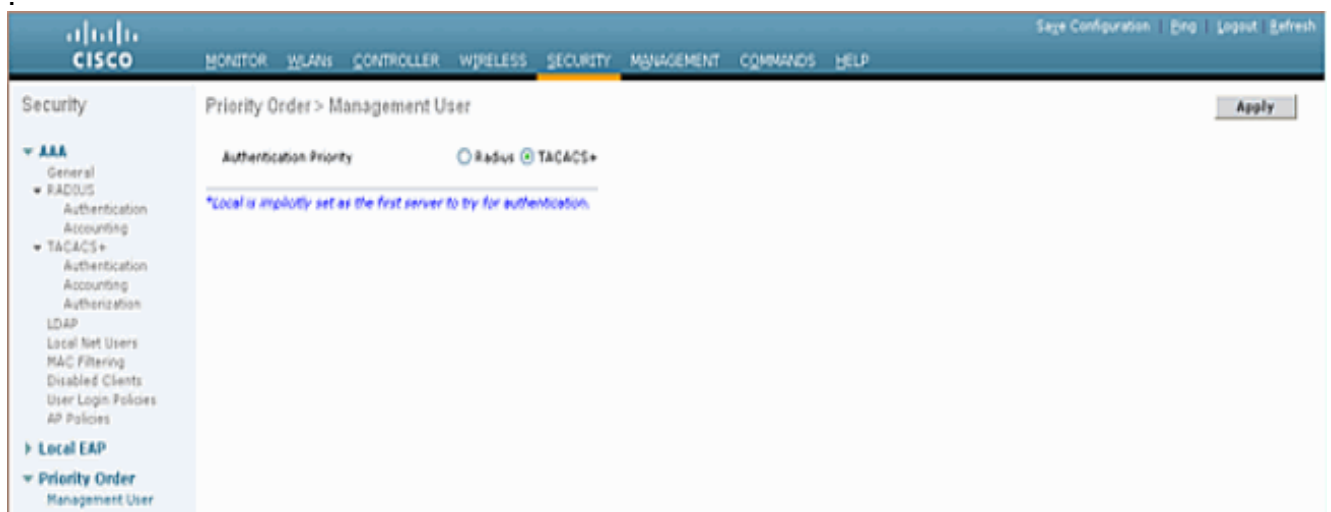
(Cisco Controller) >config tacacs acct add 1 10.1.1.12 49 ascii cisco123

## 인증 순서 구성

이 단계에서는 여러 데이터베이스가 구성된 경우 AAA 인증 순서를 구성하는 방법에 대해 설명합니다. 인증 순서는 로컬 및 RADIUS 또는 로컬 및 TACACS일 수 있습니다. 인증 순서를 위한 기본 컨트롤러 컨피그레이션은 로컬 및 RADIUS입니다.

인증 순서를 구성하려면 다음 단계를 완료합니다.

1. GUI에서 Security(보안) > Priority Order(우선순위 주문) > Management User(관리 사용자)로 이동합니다.
2. Authentication Priority(인증 우선순위)를 선택합니다. 이 예에서는 TACACS+가 선택되었습니다.
3. 적용을 클릭하여 선택합니다



`config aaa auth mgmt <server1> <server2>` 명령을 사용하여 CLI에서 이 작업을 수행할 수 있습니다.

(Cisco Controller) >config aaa auth mgmt tacacs local

## 구성 확인

이 섹션에서는 WLC에서 TACACS+ 컨피그레이션을 확인하는 데 사용되는 명령에 대해 설명합니다. 다음은 컨피그레이션이 정확한지 확인하는 데 도움이 되는 몇 가지 유용한 **show** 명령입니다.

- **show aaa auth** - 인증 순서에 대한 정보를 제공합니다.

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

- **show tacacs summary** - TACACS+ 서비스 및 통계의 요약을 표시합니다.

```
(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**—TACACS+ 인증 서버 통계를 표시합니다.

```
(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**—TACACS+ 권한 부여 서버 통계를 표시합니다.

```
(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 Authenticator Msgs..... 0
Timeout Requests..... 0
Unknowntype Msgs..... 0
Other Drops..... 0

```

- **show tacacs acct stats**—TACACS+ 계정 관리 서버 통계를 표시합니다.

```

(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

```

## Cisco Secure ACS Server 구성

이 섹션에서는 TACACS+ ACS Server에서 서비스 및 사용자 지정 특성을 생성하고 사용자 또는 그룹에 역할을 할당하는 단계에 대해 설명합니다.

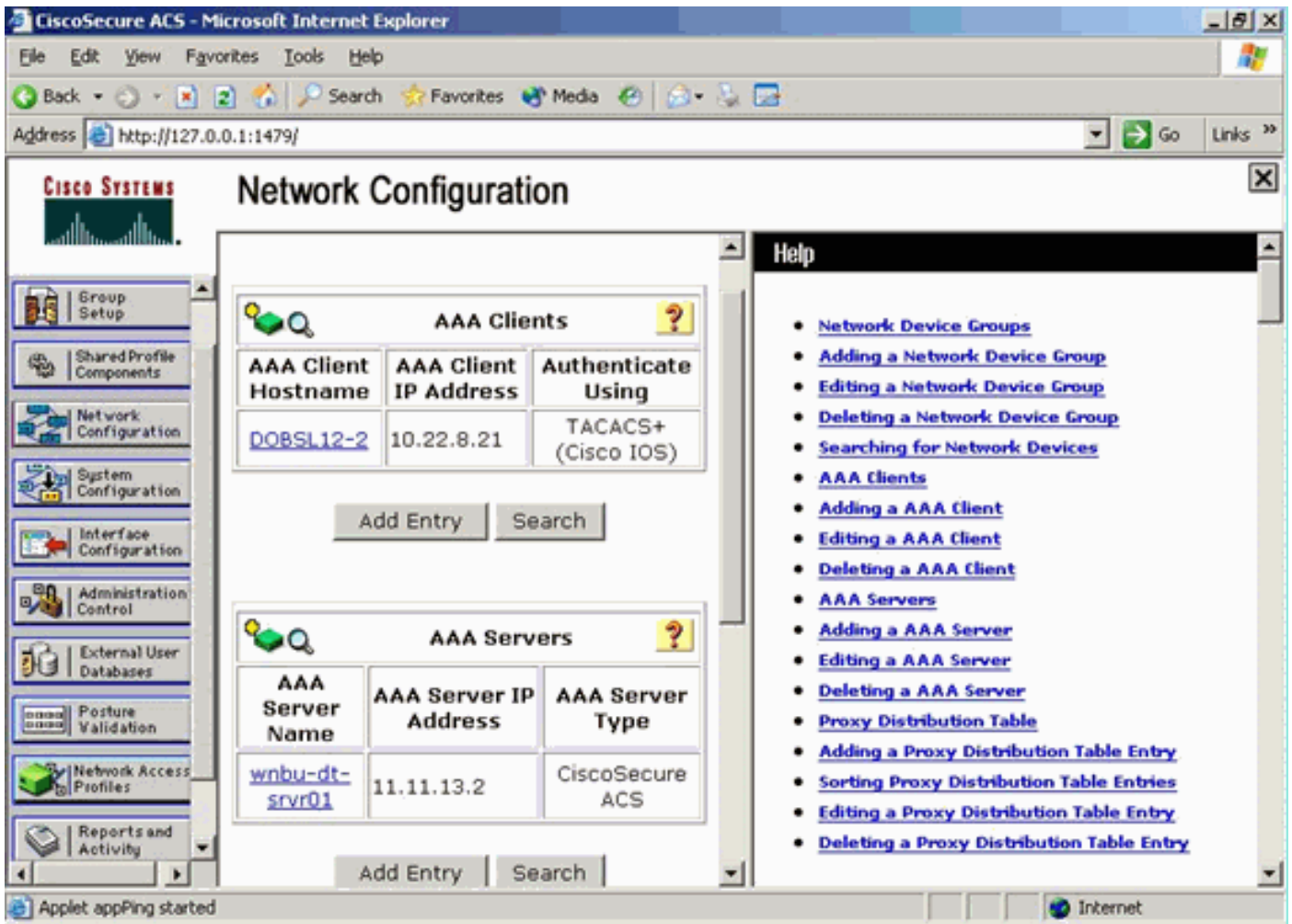
이 섹션에서는 사용자 및 그룹 생성에 대해 설명하지 않습니다. 사용자 및 그룹이 필요에 따라 생성되었다고 가정합니다. 사용자 및 사용자 그룹 생성 방법에 대한 자세한 내용은 [Cisco Secure ACS for Windows Server 4.0 사용 설명서](#)를 참조하십시오.

### 네트워크 구성

이 단계를 완료합니다.

TACACS+(Cisco IOS)로 인증 메커니즘을 사용하여 컨트롤러 관리 IP 주소를 AAA 클라이언트로 추가합니다.





## 인터페이스 컨피그레이션

다음 단계를 완료하십시오.

1. Interface Configuration 메뉴에서 TACACS+(Cisco IOS) 링크를 선택합니다.
2. 새 서비스를 활성화합니다.
3. 사용자 및 그룹 확인란을 모두 선택합니다.
4. Service(서비스)에 ciscowlc를 입력하고 Protocol(프로토콜)에 common을 입력합니다.
5. 고급 TACACS+ 기능을 활성화합니다

Address http://127.0.0.1:1767/ Go Links

**CISCO SYSTEMS**

## Interface Configuration

**TACACS+ Services**

User	Group	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	PPP IP
<input type="checkbox"/>	<input type="checkbox"/>	PPP IPX
<input type="checkbox"/>	<input type="checkbox"/>	PPP Multilink
<input type="checkbox"/>	<input type="checkbox"/>	PPP Apple Talk
<input type="checkbox"/>	<input type="checkbox"/>	PPP VPDN
<input type="checkbox"/>	<input type="checkbox"/>	PPP LCP
<input type="checkbox"/>	<input type="checkbox"/>	ARAP
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Shell (exec)
<input type="checkbox"/>	<input type="checkbox"/>	PIX Shell (pixshell)
<input type="checkbox"/>	<input type="checkbox"/>	SLIP

---

**New Services**

		Service	Protocol
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	ciscowlc	common
<input type="checkbox"/>	<input type="checkbox"/>		
<input type="checkbox"/>	<input type="checkbox"/>		

---

**Advanced Configuration Options**

Advanced TACACS+ Features

Display a Time-of-Day access grid for every TACACS+ service where you can

Submit Cancel

6. Submit(제출)을 클릭하여 변경 사항을 적용합니다.

## 사용자/그룹 설정

다음 단계를 완료하십시오.

1. 이전에 생성한 사용자/그룹을 선택합니다.
2. TACACS+ 설정으로 이동합니다.
3. Interface Configuration(인터페이스 컨피그레이션) 섹션에서 생성된 ciscowlc 서비스에 해당하는 확인란을 선택합니다.
4. Custom attributes(사용자 지정 특성) 확인란을 선택합니다



## Group Setup

Jump To Access Restrictions

- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration
- System Configuration
- Interface Configuration
- Administration Control
- External User Databases
- Posture Validation
- Network Access Profiles
- Reports and Activity
- Online Documentation

### Shell Command Authorization Set

- None
- Assign a Shell Command Authorization Set for any network device
- Per Group Command Authorization
  - Unmatched Cisco IOS commands
  - Permit
  - Deny

Command:

Arguments:

Unlisted arguments

- Permit
- Deny

#### ciscowlc common

Custom attributes

role1=ALL

#### Wireless-WCS HTTP

Custom attributes

### IETF RADIUS Attributes

[006] Service-Type

Callback NAS Prompt

Submit

Submit + Restart

Cancel

5. Custom attributes(사용자 지정 특성) 아래의 텍스트 상자에 WLAN, SECURITY 및 CONTROLLER에 대한 액세스만 필요한 경우 이 텍스트를 입력합니다. **role1=WLAN role2=SECURITY role3=CONTROLLER**. 사용자가 SECURITY 탭에만 액세스해야 하는 경우 다음 텍스트를 입력합니다. **role1=보안**. 이 역할은 컨트롤러 웹 GUI의 7가지 메뉴 모음 항목에 해당합니다. 메뉴 모음 항목은 MONITOR, WLAN, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT 및 COMMAND입니다.
6. 사용자가 role1, role2 등에 필요한 역할을 입력합니다. 사용자에게 모든 역할이 필요한 경우 ALL 키워드를 사용해야 합니다. 로비 관리자 역할의 경우 키워드 **LOBBY**를 사용해야 합니다.

WLC의 TACACS+ 계정 레코드는 TACACS+ 보고서 및 활동 관리의 Cisco Secure ACS에서 사용할 수 있습니다.

The screenshot shows the 'Reports and Activity' page in Cisco Secure ACS. The main content is a table titled 'Tacacs+ Administration active.csv'. The table has columns for Date, Time, User-Name, Group-Name, cmd, grpid, service, NAS-Portname, task\_id, NAS-IP-Address, and reason. The data shows various configuration commands for WLC, such as 'wlan enable 1', 'wlan idap delete 1 position 2', 'wlan timeout 1 0', etc., all executed by 'tac' at 16:26:52 on 02/22/2007.

Date	Time	User-Name	Group-Name	cmd	grpid	service	NAS-Portname	task_id	NAS-IP-Address	reason
02/22/2007	16:26:52	tac	Tacacs Group for WLC	wlan enable 1	249	shell	...	224	10.10.80.3	...
02/22/2007	16:26:52	tac	Tacacs Group for WLC	wlan idap delete 1 position 2	249	shell	...	223	10.10.80.3	...
02/22/2007	16:26:52	tac	Tacacs Group for WLC	wlan idap delete 1 position 1	249	shell	...	222	10.10.80.3	...
02/22/2007	16:26:52	tac	Tacacs Group for WLC	wlan idap delete 1 position 0	249	shell	...	221	10.10.80.3	...
02/22/2007	16:26:52	tac	Tacacs Group for WLC	wlan timeout 1 0	249	shell	...	220	10.10.80.3	...
02/22/2007	16:26:52	tac	Tacacs Group for WLC	wlan mac-filtering disable 1	249	shell	...	219	10.10.80.3	...
02/22/2007	16:26:52	tac	Tacacs Group for WLC	wlan security is NONE for wlan-id 1	249	shell	...	218	10.10.80.3	...
02/22/2007	16:26:52	tac	Tacacs Group for WLC	wlan security WPA(WPA2) disable 1	249	shell	...	217	10.10.80.3	...
02/22/2007	16:26:52	tac	Tacacs Group for WLC	wlan aaa-override disable 1	249	shell	...	216	10.10.80.3	...
02/22/2007	16:26:52	tac	Tacacs Group for WLC	wlan qos 1 platinum	249	shell	...	215	10.10.80.3	...
02/22/2007	16:26:52	tac	Tacacs Group for WLC	wlan radio 1 all	249	shell	...	214	10.10.80.3	...
02/22/2007	16:26:52	tac	Tacacs Group for WLC	wlan dhcp_server 1 0.0.0.0 required	249	shell	...	213	10.10.80.3	...
02/22/2007	16:26:52	tac	Tacacs Group for WLC	wlan broadcast-ssid enable 1	249	shell	...	212	10.10.80.3	...
02/22/2007	16:26:52	tac	Tacacs Group for WLC	wlan exclusionlist 1 0	249	shell	...	211	10.10.80.3	...
02/22/2007	16:26:52	tac	Tacacs Group for WLC	wlan exclusionlist 1 disable	249	shell	...	210	10.10.80.3	...
02/22/2007	16:26:52	tac	Tacacs Group for WLC	wlan act 1	249	shell	...	209	10.10.80.3	...
02/22/2007	16:26:52	tac	Tacacs Group for WLC	wlan interface 1 100	249	shell	...	208	10.10.80.3	...
02/22/2007	16:26:52	tac	Tacacs Group for WLC	wlan disable 1	249	shell	...	207	10.10.80.3	...

## WCS의 TACACS+ 컨피그레이션

다음 단계를 완료하십시오.

1. GUI에서 루트 계정으로 WCS에 로그인합니다.
2. TACACS+ 서버를 추가합니다. Administration(관리) > AAA > TACACS+ > Add TACACS+ Server(TACACS+ 서버 추가)로 이동합니다



3. TACACS+ 서버 세부 정보(예: IP 주소, 포트 번호(49가 기본값) 및 공유 암호 키)를 추가합니다



4. WCS에서 관리를 위해 TACACS+ 인증을 활성화합니다. Administration(관리) > AAA > AAA Mode(AAA 모드) > Select TACACS+로 이동합니다



## 가상 도메인을 사용하는 WCS

Virtual Domain은 WCS 버전 5.1에 도입된 새로운 기능입니다. WCS 가상 도메인은 일련의 장치와 맵으로 구성되며 사용자의 보기를 이러한 디바이스 및 맵과 관련된 정보로 제한합니다. 관리자는 가상 도메인을 통해 사용자가 자신이 담당하는 디바이스와 맵만 볼 수 있도록 할 수 있습니다. 또한 가상 도메인의 필터로 인해 사용자는 네트워크의 할당된 부분에만 대해 알림을 구성, 보고 보고서를 생성할 수 있습니다. 관리자는 각 사용자에게 대해 허용되는 가상 도메인 집합을 지정합니다. 이 중 하나만 로그인 시 해당 사용자에게 대해 활성화할 수 있습니다. 사용자는 화면 상단의 Virtual Domain 드롭다운 메뉴에서 다른 허용된 가상 도메인을 선택하여 현재 가상 도메인을 변경할 수 있습니다. 이제 모든 보고서, 경보 및 기타 기능이 해당 가상 도메인에 의해 필터링됩니다.

시스템에 정의된 가상 도메인(루트)이 하나뿐이며 TACACS+/RADIUS 서버의 사용자 지정 특성 필드에 가상 도메인이 없는 경우 기본적으로 사용자에게 루트 가상 도메인이 할당됩니다.

둘 이상의 가상 도메인이 있고 사용자에게 지정된 특성이 없는 경우 사용자가 로그인할 수 없게 됩니다. 사용자가 로그인할 수 있도록 하려면 가상 도메인 사용자 지정 특성을 Radius/TACACS+ 서버로 내보내야 합니다.

Virtual Domain Custom Attributes(가상 도메인 맞춤형 특성) 창에서 각 가상 도메인에 대해 적절한 프로토콜별 데이터를 표시할 수 있습니다. Virtual Domain Hierarchy 사이드바의 Export(내보내기) 버튼은 가상 도메인의 RADIUS 및 TACACS+ 특성을 미리 포맷합니다. 이러한 특성을 복사하여 ACS 서버에 붙여넣을 수 있습니다. 그러면 해당 가상 도메인만 ACS 서버 화면에 복사할 수 있으며, 사용자는 이러한 가상 도메인에만 액세스할 수 있습니다.

미리 포맷된 RADIUS 및 TACACS+ 특성을 ACS 서버에 적용하려면 [Virtual Domain RADIUS and TACACS+ Attributes\(가상 도메인 RADIUS 및 TACACS+ 특성\)](#) 섹션에 설명된 단계를 완료합니다.

## WCS를 사용하도록 Cisco Secure ACS 구성

이 섹션에서는 TACACS+ ACS Server에 포함된 단계를 통해 서비스 및 사용자 지정 특성을 생성하고 사용자 또는 그룹에 역할을 할당합니다.

이 섹션에서는 사용자 및 그룹 생성에 대해 설명하지 않습니다. 사용자 및 그룹이 필요에 따라 생성되었다고 가정합니다.

## 네트워크 구성

이 단계를 완료합니다.

인증 메커니즘을 TACACS+(Cisco IOS)로 사용하여 WCS IP 주소를 AAA 클라이언트로 추가합니다

The screenshot shows the Cisco Network Configuration interface. The main heading is "AAA Client Setup For WCS". The configuration fields are as follows:

- AAA Client IP Address: 192.168.60.5
- Key: cisco
- Authenticate Using: TACACS+ (Cisco IOS)
- Single Connect TACACS+ AAA Client (Record stop in accounting on failure):
- Log Update/Watchdog Packets from this AAA Client:
- Log RADIUS Tunneling Packets from this AAA Client:
- Replace RADIUS Port info with Username from this AAA Client:

Buttons at the bottom include: Submit, Submit + Apply, Delete, Delete + Apply, Cancel, and a Back to Help button.

## 인터페이스 컨피그레이션

다음 단계를 완료하십시오.

1. Interface Configuration 메뉴에서 TACACS+(Cisco IOS) 링크를 선택합니다.
2. 새 서비스를 활성화합니다.
3. 사용자 및 그룹 확인란을 모두 선택합니다.
4. Wireless-WCS for Service 및 HTTP for Protocol을 입력합니다.참고: HTTP는 CAPS여야 합니다.
5. 고급 TACACS+ 기능을 활성화합니다



# Interface Configuration

- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration
- System Configuration
- Interface Configuration
- Administration Control
- External User Databases
- Posture Validation
- Network Access Profiles
- Reports and Activity
- Online Documentation

- PPP IP
- PPP IPX
- PPP Multilink
- PPP Apple Talk
- PPP VPDN
- PPP LCP
- ARAP
- Shell (exec)
- PIX Shell (pixshell)
- SLIP

## New Services

		Service	Protocol
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	ciscowlc	common
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Wireless-WCS	HTTP
<input type="checkbox"/>	<input type="checkbox"/>		

## Advanced Configuration Options

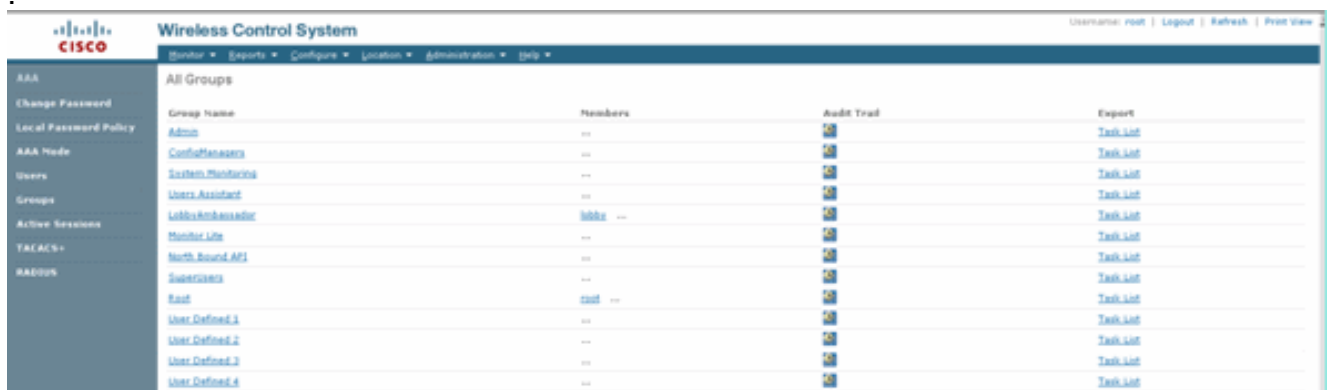
- Advanced TACACS+ Features

6. Submit(제출)을 클릭하여 변경 사항을 적용합니다.

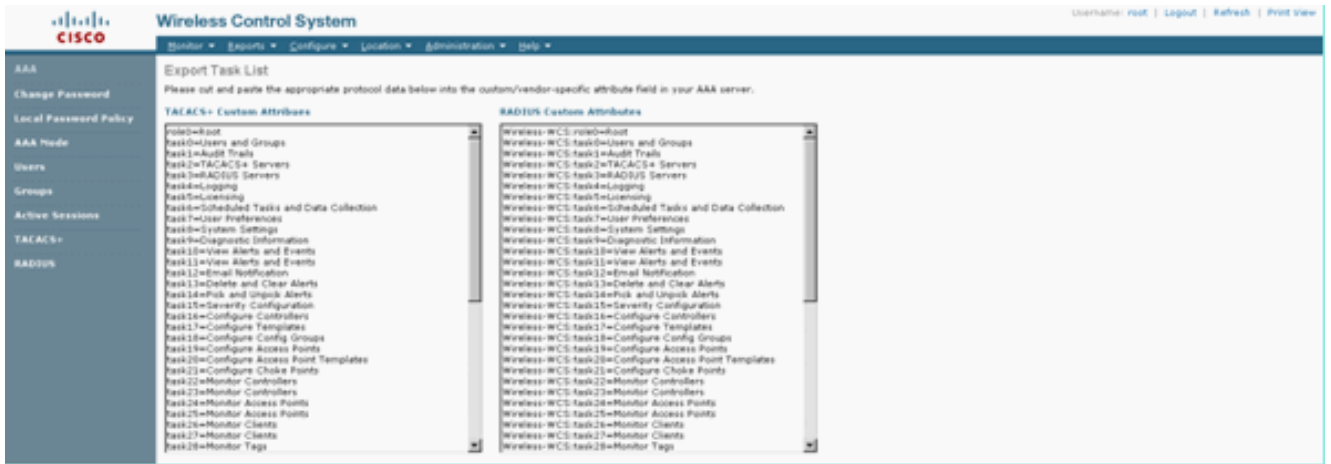
## 사용자/그룹 설정

다음 단계를 완료하십시오.

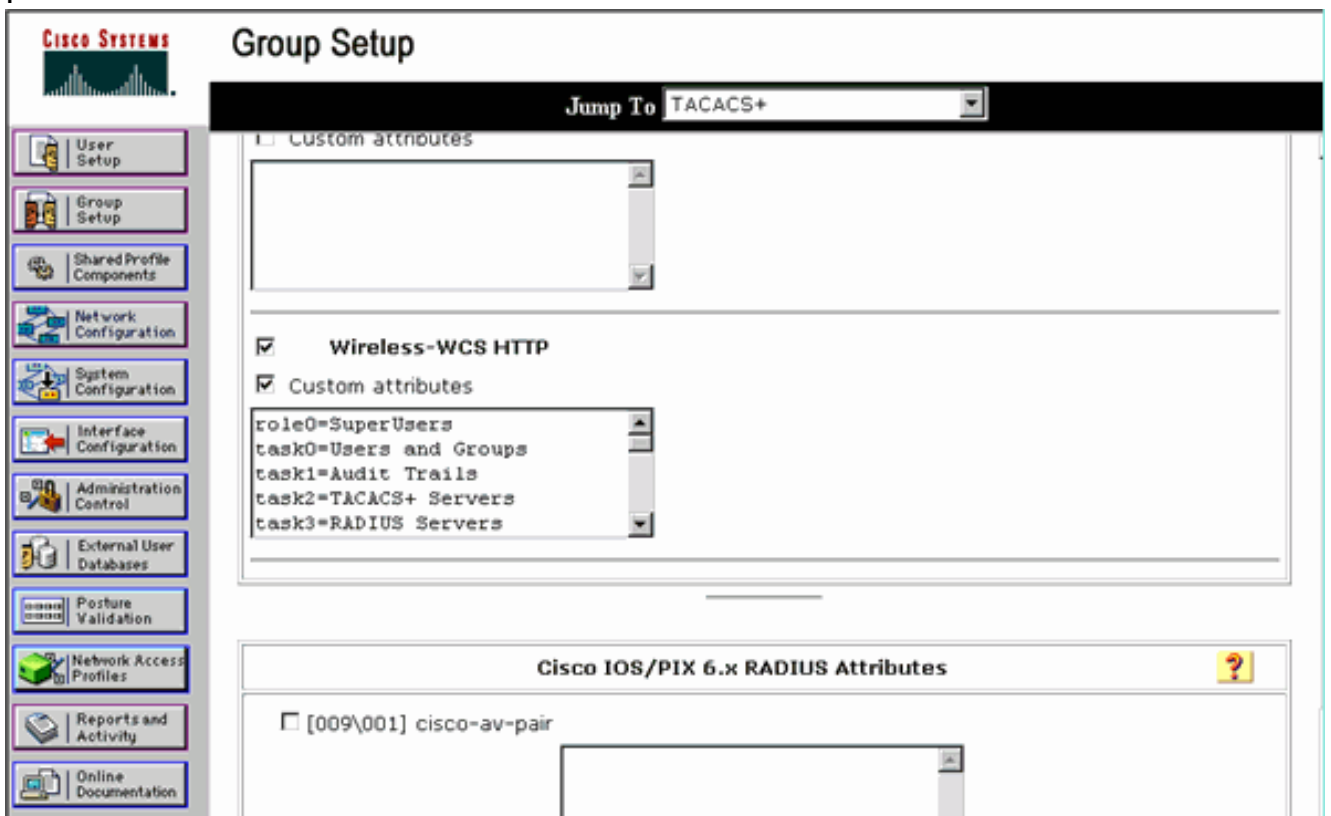
1. WCS GUI에서 **Administration(관리) > AAA > Groups(그룹)**로 이동하여 WCS의 SuperUsers와 같이 사전 구성된 사용자 그룹을 선택합니다



2. 사전 구성된 사용자 그룹에 대한 작업 목록을 선택하고 ACS에 붙여넣기를 복사합니다



3. 이전에 생성한 사용자/그룹을 선택하고 TACACS+ Settings(TACACS+ 설정)로 이동합니다.
4. ACS GUI에서 이전에 생성한 Wireless-WCS 서비스에 해당하는 확인란을 선택합니다.
5. ACS GUI에서 Custom attributes(사용자 지정 특성) 상자를 선택합니다.
6. 사용자 지정 특성 아래의 텍스트 상자에 WCS에서 복사한 이 역할 및 작업 정보를 입력합니다. 예를 들어, SuperUsers에서 허용하는 작업 목록을 입력합니다



7. 그런 다음 ACS에서 새로 생성된 사용자 이름/비밀번호를 사용하여 WCS에 로그인합니다.

## 디버깅

### 역할1=ALL에 대해 WLC에서 디버깅

```
(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 ffffffff8
```

## [여러 역할에 대한 WLC에서 디버깅](#)

```
(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
```

## [권한 부여 실패를 위해 WLC에서 디버깅](#)

```
(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
```

## [관련 정보](#)

- [웹 인증을 위한 Cisco WLC\(Wireless LAN Controller\) 및 Cisco ACS 5.x\(TACACS+\) 구성 예](#)
- [TACACS+ 구성](#)
- [ACS 5.1에서 관리자 및 비관리자 사용자에게 대한 TACACS 인증 및 권한 부여를 구성하는 방법](#)

- [TACACS+ 및 RADIUS 비교](#)
- [기술 지원 및 문서 - Cisco Systems](#)