관리 사용자를 인증하도록 WLC 및 ACS 구성

목차

소개

이 문서에서는 AAA 서버가 컨트롤러의 관리 사용자를 인증할 수 있도록 WLC 및 Cisco Secure ACS를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 컨피그레이션을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

- WLC에서 기본 매개변수를 구성하는 방법에 대한 지식
- Cisco Secure ACS와 같은 RADIUS 서버를 구성하는 방법에 대한 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 버전 7.0.216.0을 실행하는 Cisco 4400 무선 LAN 컨트롤러
- 소프트웨어 버전 4.1을 실행하고 이 컨피그레이션에서 RADIUS 서버로 사용되는 Cisco Secure ACS.

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

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

배경 정보

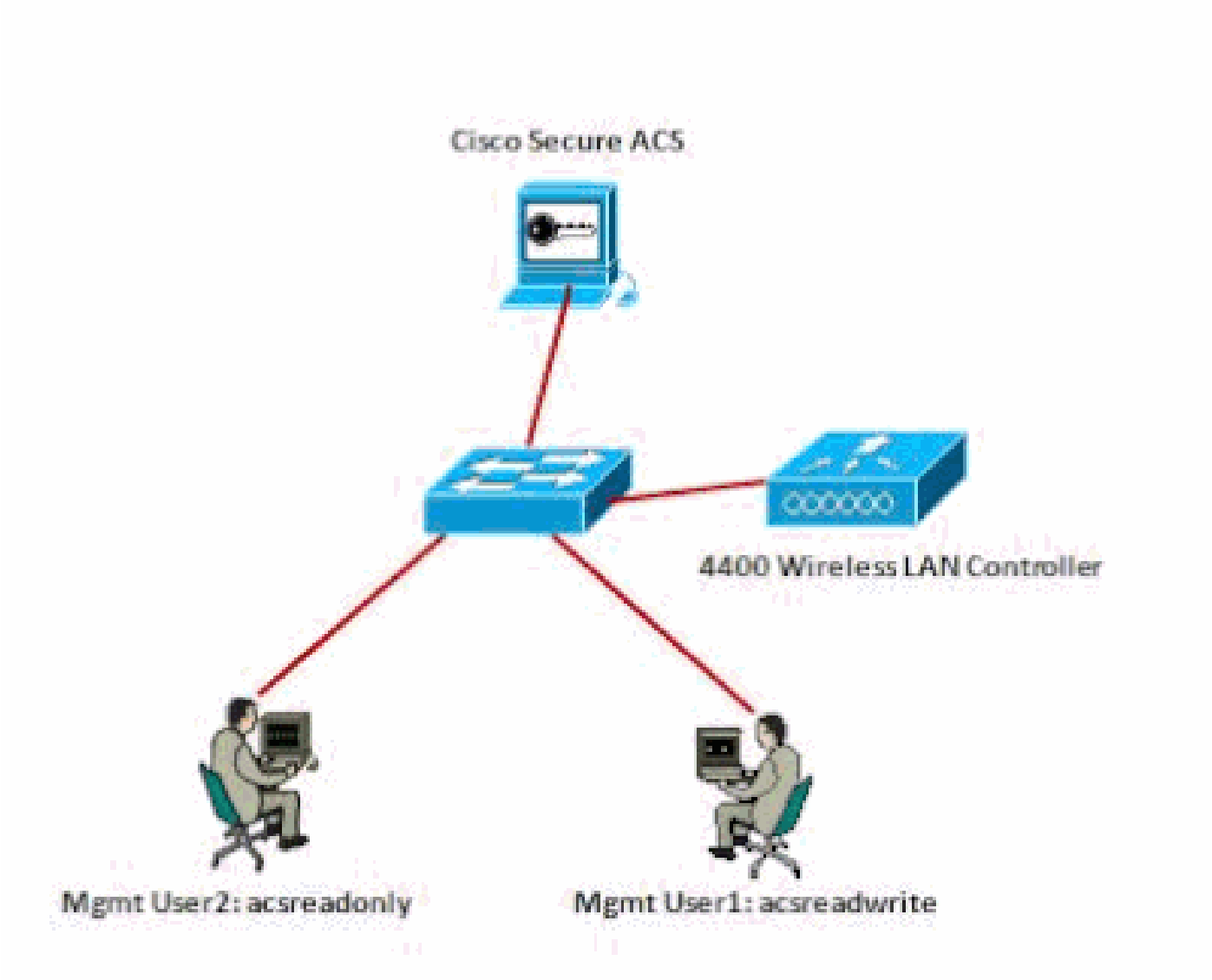
이 문서에서는 AAA(Authentication, Authorization, and Accounting) 서버가 컨트롤러의 관리 사용자를 인증할 수 있도록 WLC(Wireless LAN Controller) 및 Cisco Secure ACS(Access Control Server)를 구성하는 방법에 대해 설명합니다. 또한 이 문서에서는 여러 관리 사용자가 Cisco Secure ACS RADIUS 서버에서 반환된 VSA(Vendor-Specific Attributes)를 사용하여 어떻게 다양한 권한을 받을 수 있는지도 설명합니다.

구성

이 섹션에서는 이 문서에 설명된 목적을 위해 WLC 및 ACS를 구성하는 방법에 대한 정보를 제공합니다.

네트워크 다이어그램

이 문서에서는 이 네트워크 설정을 사용합니다.



네트워크 다이어그램

이 컨피그레이션 예에서는 다음 매개변수를 사용합니다.

- Cisco Secure ACS의 IP 주소 —172.16.1.1/255.255.0.0
- 컨트롤러의 관리 인터페이스 IP 주소—172.16.1.30/255.255.0.0
- 액세스 포인트(AP) 및 RADIUS 서버에서 사용되는 공유 암호 키(asdf1234)
- 다음은 이 예제가 ACS에서 구성하는 두 사용자의 자격 증명입니다.
    - 사용자 이름 - acsreadwrite

      비밀번호 - acsreadwrite
    - 사용자 이름 - acsreadonly

      비밀번호 - acsreadonly

다음을 수행하려면 WLC 및 Cisco Secure Cisco Secure ACS를 구성해야 합니다.

- acsreadwrite로 사용자 이름과 비밀번호를 사용하여 WLC에 로그인하는 모든 사용자는 WLC에 대한 전체 관리 액세스 권한을 부여받습니다.
- 사용자 이름과 비밀번호를 acsreadonly로 사용하여 WLC에 로그인하는 사용자는 WLC에 대한 읽기 전용 액세스 권한을 부여받습니다.

설정

이 문서에서는 다음 설정을 사용합니다.

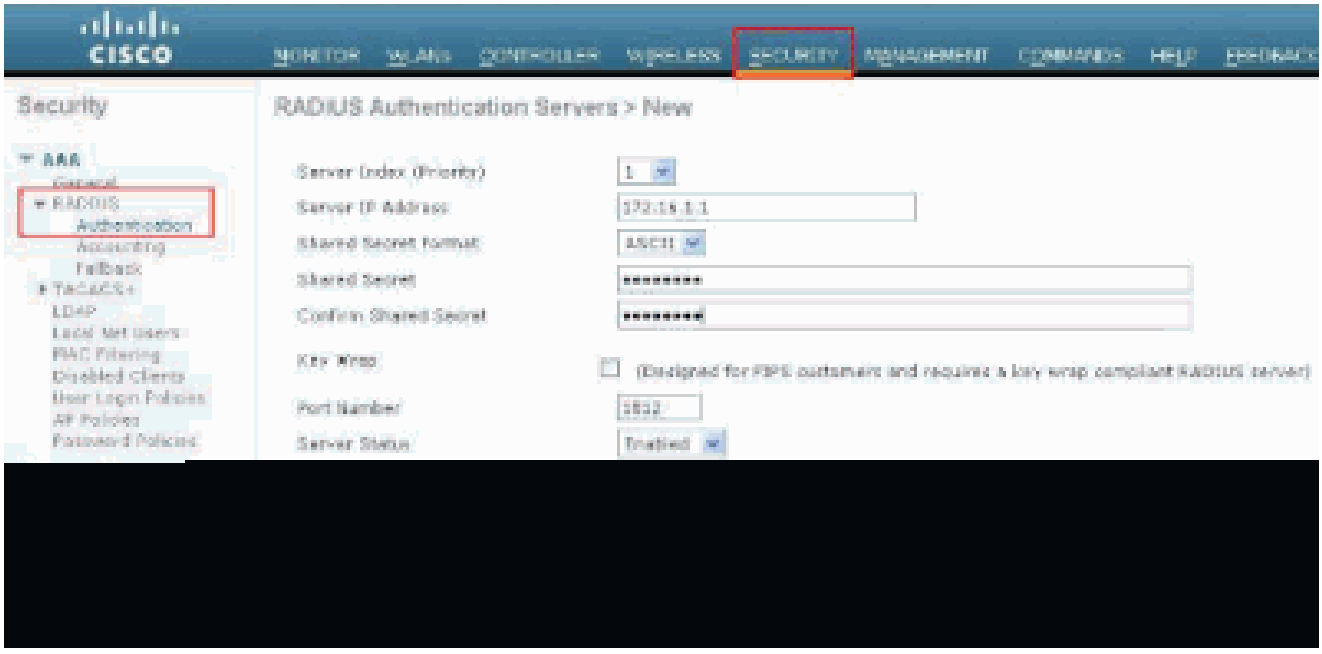
- WLC 컨피그레이션
- Cisco Secure ACS 컨피그레이션

WLC 컨피그레이션

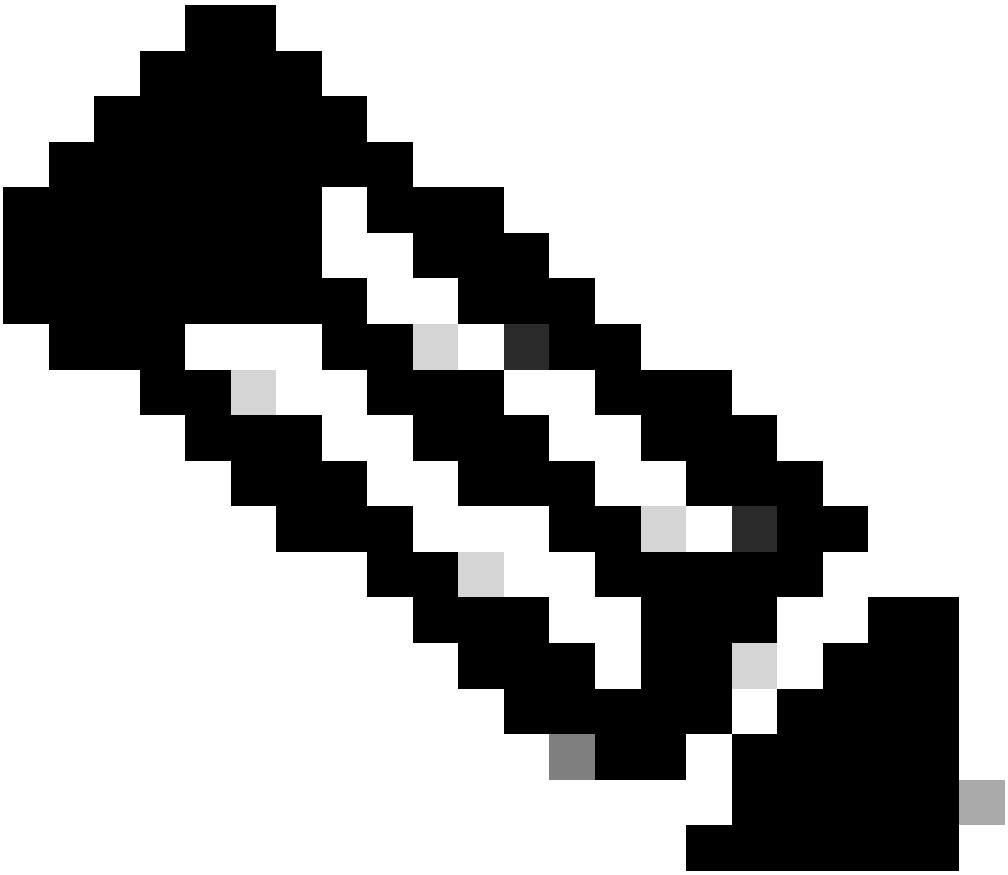
Cisco Secure ACS Server를 통한 관리를 허용하도록 WLC 구성

RADIUS 서버와 통신하도록 WLC를 구성하려면 다음 단계를 완료하십시오.

1. WLC GUI에서 Security(보안)를 클릭합니다. 왼쪽의 메뉴에서 RADIUS > Authentication(인증)을 클릭합니다. RADIUS Authentication servers(RADIUS 인증 서버) 페이지가 나타납니다. 새 RADIUS 서버를 추가하려면 New를 클릭합니다. RADIUS Authentication Servers(RADIUS 인증 서버) > New(새) 페이지에서 RADIUS 서버와 관련된 매개변수를 입력합니다. 이제 DDoS 공격의 실제 사례를 살펴보겠습니다.

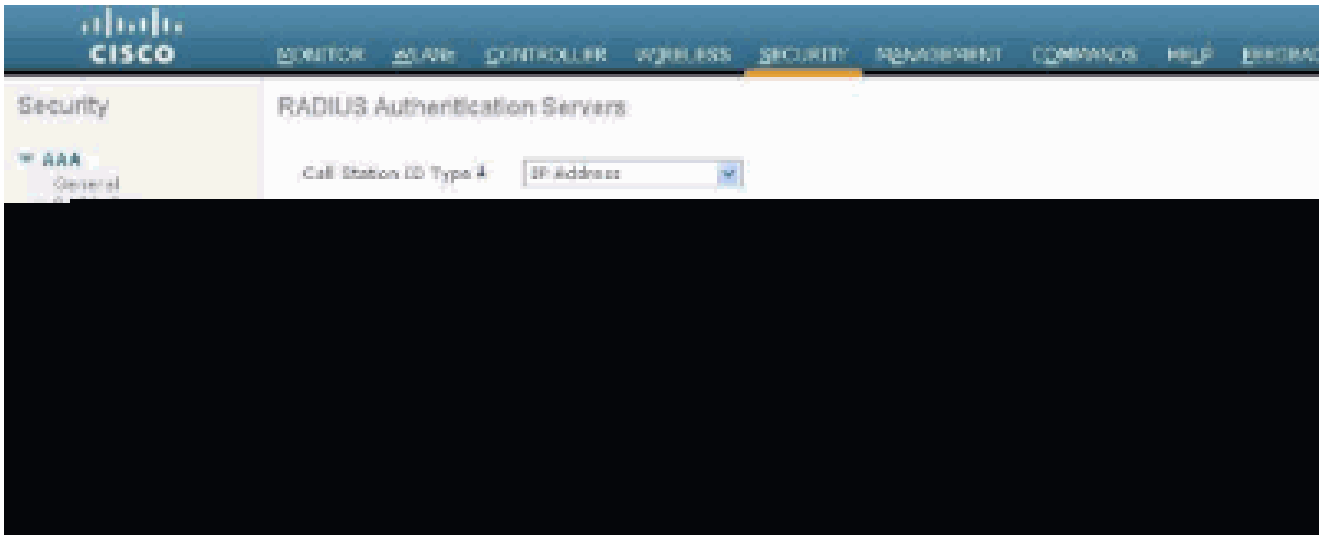


2. RADIUS 서버가 WLC에 로그인하는 사용자를 인증하도록 하려면 Management(관리) 라디오 버튼을 선택합니다.



참고: 이 페이지에 구성된 공유 암호가 RADIUS 서버에 구성된 공유 암호와 일치하는지 확인하십시오. 그런 다음 WLC가 RADIUS 서버와 통신할 수 있습니다.

3. WLC가 Cisco Secure ACS에서 관리되도록 구성되었는지 확인합니다. 이렇게 하려면 WLC GUI에서 Security(보안)를 클릭합니다. 결과 GUI 창이 이 예와 유사하게 나타납니다.



RADIUS 서버 172.16.1.1에 대해 Management(관리) 확인란이 활성화되어 있음을 확인할 수 있습니다. 이는 ACS가 WLC에서 관리 사용자를 인증할 수 있음을 보여줍니다.

Cisco Secure ACS 컨피그레이션

ACS를 구성하려면 다음 섹션의 단계를 완료합니다.

1. RADIUS 서버에 AAA 클라이언트로 WLC를 추가합니다.
2. 사용자 및 해당 RADIUS IETF 특성을 구성합니다.
3. 읽기-쓰기 액세스 권한이 있는 사용자를 구성합니다.
4. 읽기 전용 액세스 권한이 있는 사용자를 구성합니다.

RADIUS 서버에 AAA 클라이언트로 WLC 추가

Cisco Secure ACS에서 WLC를 AAA 클라이언트로 추가하려면 다음 단계를 완료합니다.

1. ACS GUI에서 Network Configuration(네트워크 컨피그레이션)을 클릭합니다.
2. AAA Clients 아래에서 Add Entry를 클릭합니다.
3. Add AAA Client(AAA 클라이언트 추가) 창에서 WLC 호스트 이름, WLC의 IP 주소 및 공유 비밀 키를 입력합니다.

   이 예에서는 다음과 같은 설정을 사용합니다.

   - AAA 클라이언트 호스트 이름은 WLC-4400입니다.
   - 172.16.1.30/16은 AAA 클라이언트 IP 주소이며, 이 경우에는 WLC입니다.
   - 공유 비밀 키는 "asdf1234"입니다.

AAA 클라이언트 추가 창

이 공유 비밀 키는 WLC에서 구성하는 공유 비밀 키와 같아야 합니다.

4. Authenticate Using(사용하여 인증) 드롭다운 메뉴에서 RADIUS(Cisco Airespace)를 선택합니다.
5. 컨피그레이션을 저장하려면 Submit(제출) + Restart(재시작)를 클릭합니다.

사용자 및 해당 RADIUS IETF 특성 구성

RADIUS 서버를 통해 사용자를 인증하려면 컨트롤러 로그인 및 관리를 위해 IETF RADIUS 특성 Service-Typeset을 사용하여 사용자 권한에 따라 적절한 값으로 RADIUS 데이터베이스에 사용자를 추가해야 합니다.

- 사용자에 대한 읽기/쓰기 권한을 설정하려면 Service-TypeAttribute를 Administrative로 설정합니다.
- 사용자에 대한 읽기 전용 권한을 설정하려면 Service-TypeAttribute를 NAS-Prompt로 설정합니다.

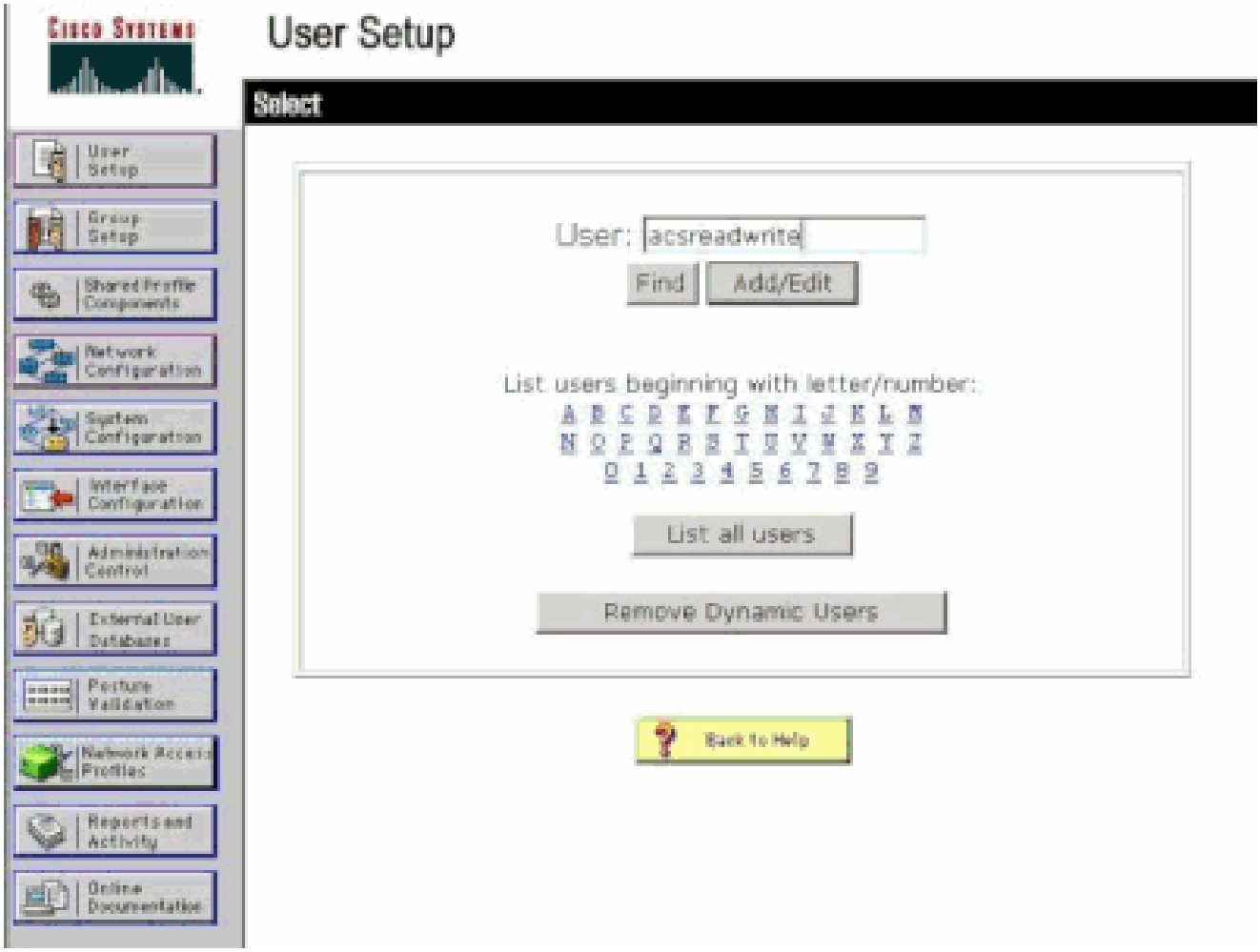
읽기-쓰기 액세스 권한이 있는 사용자 구성

첫 번째 예에서는 WLC에 대한 전체 액세스 권한을 가진 사용자의 컨피그레이션을 보여줍니다. 이 사용자가 컨트롤러에 로그인을 시도하면 RADIUS 서버가 인증하고 이 사용자에게 전체 관리 액세스를 제공합니다.

이 예에서 사용자 이름과 비밀번호는 acsreadwrite입니다.

Cisco Secure ACS에서 다음 단계를 완료합니다.

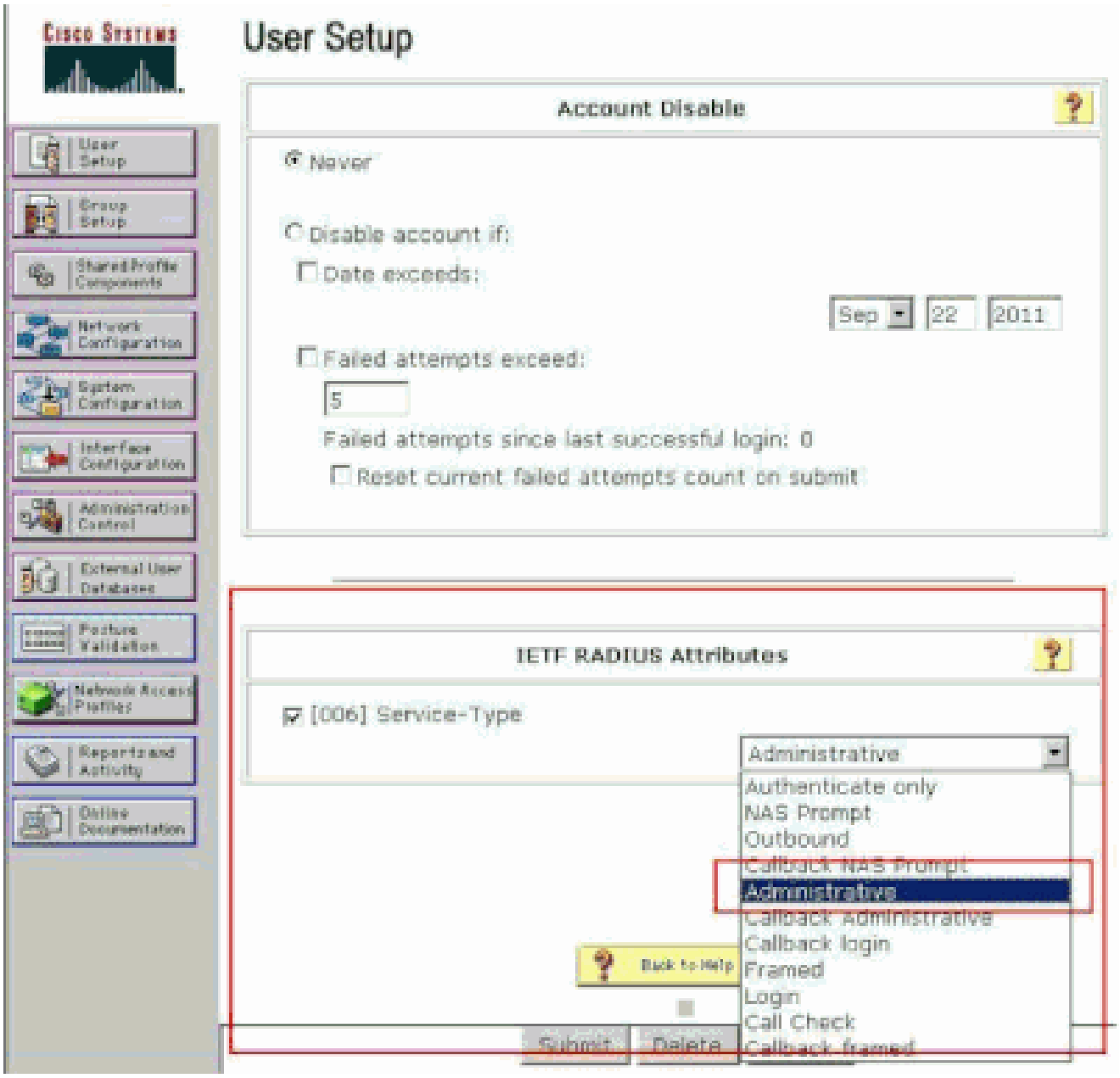
1. ACS GUI에서 User Setup(사용자 설정)을 클릭합니다.
2. 이 예제 창에 표시된 대로 ACS에 추가할 사용자 이름을 입력합니다.



사용자 설정 창

3. Add/Edit(추가/수정)를 클릭하여 User Edit(사용자 수정) 페이지로 이동합니다.
4. User Edit(사용자 수정) 페이지에서 이 사용자의 Real Name(실제 이름), Description(설명) 및 Password(비밀번호) 세부사항을 제공합니다.
5. 아래로 스크롤하여 IETF RADIUS Attributes(IETF RADIUS 특성) 설정으로 이동한 다음 Service-Type Attribute(서비스 유형 특성)를 선택합니다.
6. 이 예에서는 사용자 acsreadwrite에 전체 액세스 권한을 부여해야 하므로 Service-Type(서비스 유형) 풀다운 메뉴에 대해 Administrative(관리)를 선택하고 Submit(제출)을 클릭합니다.

   이렇게 하면 이 특정 사용자가 WLC에 대한 읽기-쓰기 액세스 권한을 갖게 됩니다.



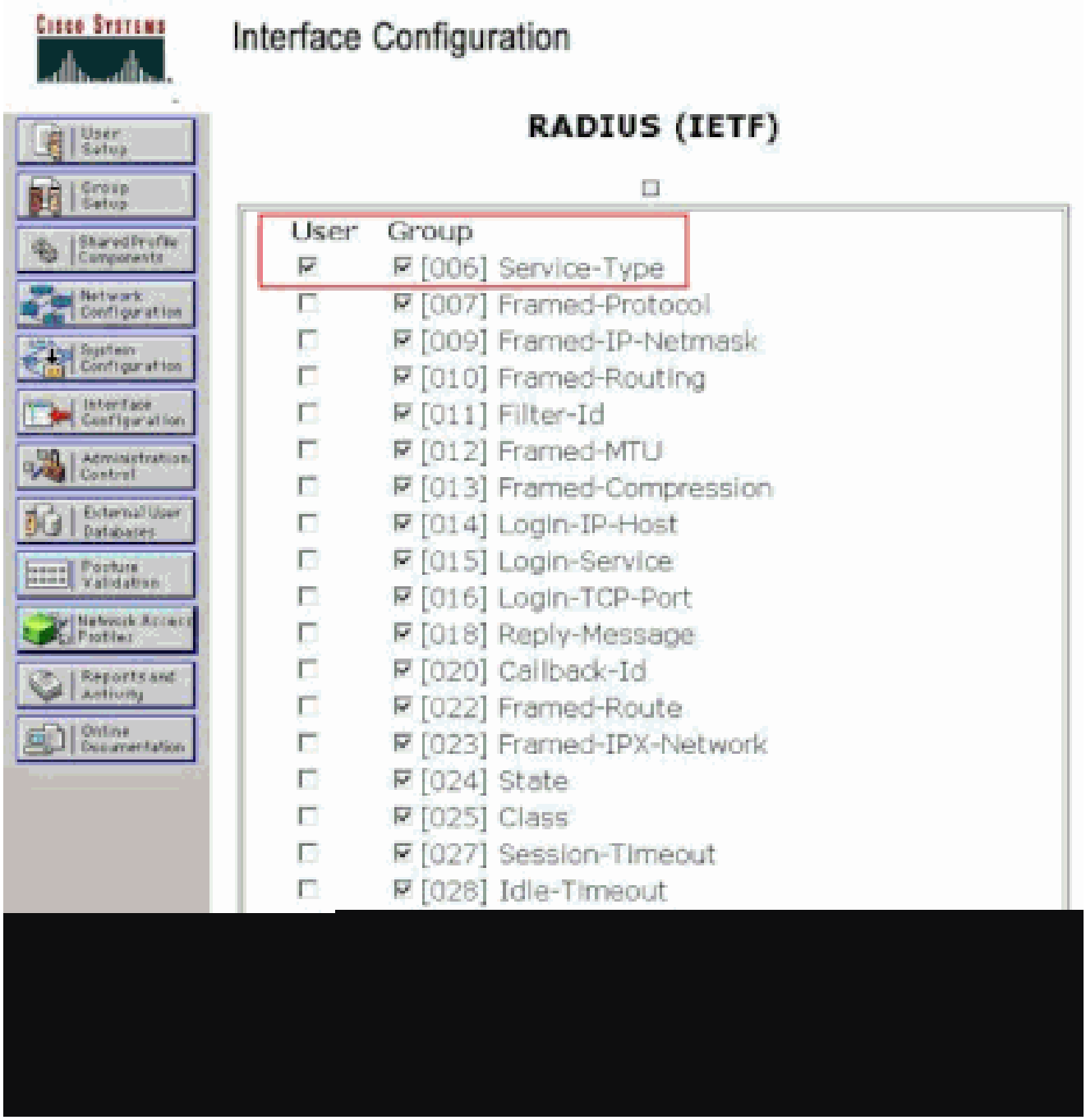
ETF RADIUS 특성 설정

사용자 설정에서 이 Service-Type 특성이 표시되지 않는 경우가 있습니다. 이러한 경우 다음 단계를 완료하여 가시성을 확보하십시오.

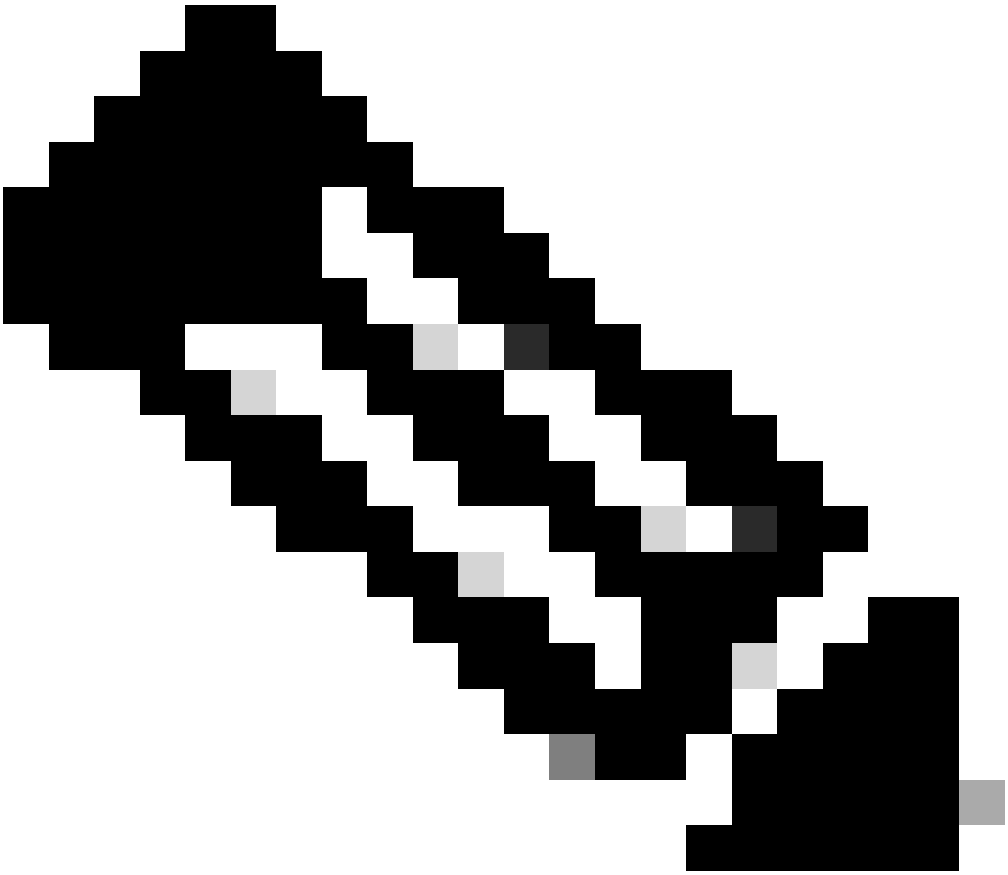
1. ACS GUI에서 Interface Configuration(인터페이스 컨피그레이션) > RADIUS(IETF)를 선택하여 User Configuration(사용자 컨피그레이션) 창에서 IETF 특성을 활성화합니다.

   그러면 RADIUS(IETF) Settings(RADIUS(IETF) 설정) 페이지로 이동합니다.

2. RADIUS (IETF) Settings(IETF 설정) 페이지에서 사용자 또는 그룹 설정에서 표시해야 하는 IETF 특성을 활성화할 수 있습니다. 이 컨피그레이션에서는 User(사용자) 열의 Service-Type(서비스 유형)을 선택하고 Submit(제출)을 클릭합니다. 이 창에는 예가 나와 있습니다.



RADIUS(IETF) 설정 페이지



참고: 이 예에서는 사용자 단위로 인증을 지정합니다. 특정 사용자가 속한 그룹을 기반으로 인증을 수행할 수도 있습니다. 이 경우 Group(그룹) 확인란을 활성화하여 Group settings(그룹 설정)에서 이 특성을 볼 수 있도록 합니다. 또한 인증이 그룹 기반인 경우 사용자를 특정 그룹에 할당하고 해당 그룹의 사용자에게 액세스 권한을 제공하도록 그룹 설정 IETF 특성을 구성해야 합니다. 그룹을 구성하고 관리하는 방법에 대한 자세한 내용은 그룹 관리를 참조하십시오.

읽기 전용 액세스 권한이 있는 사용자 구성

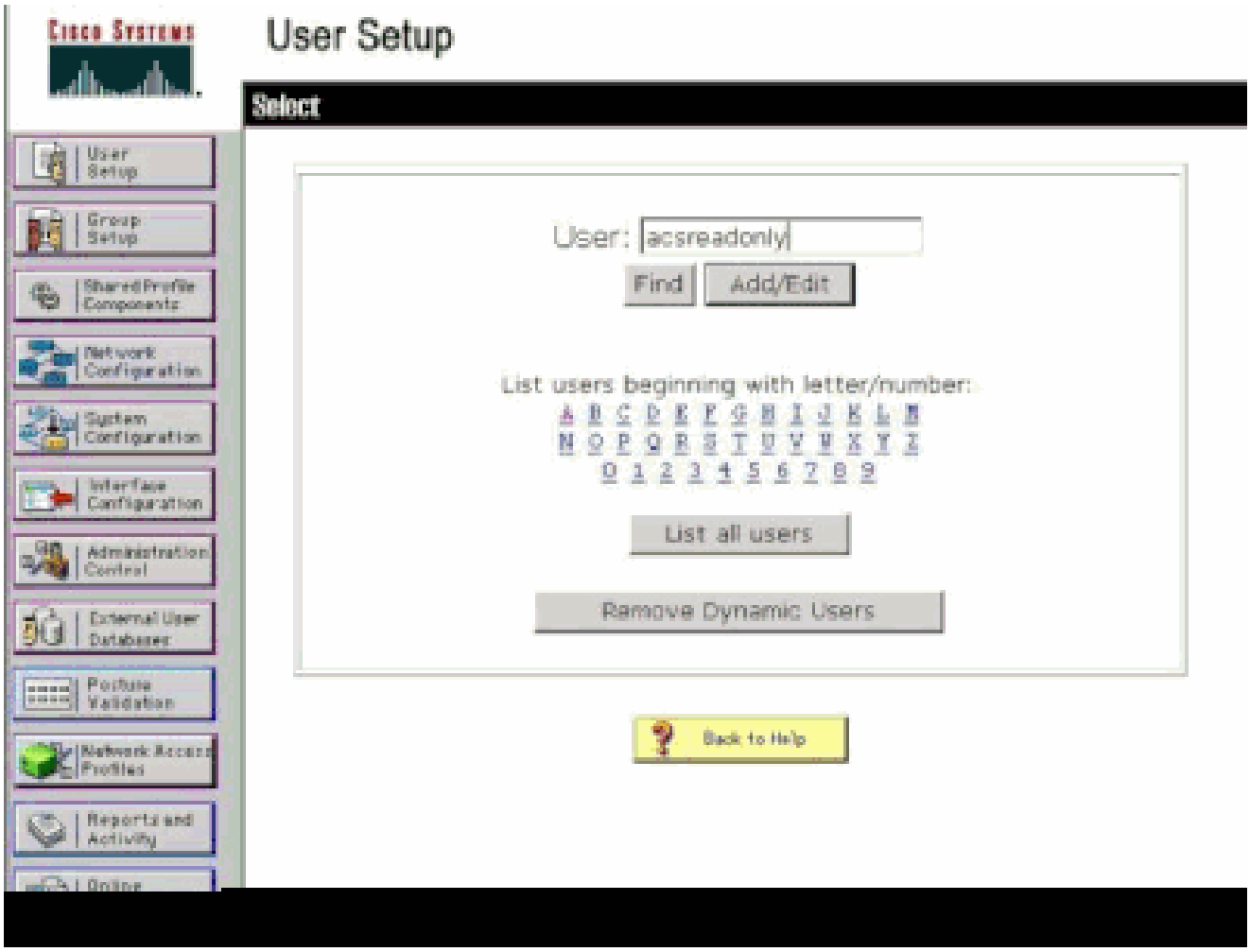
이 예에서는 WLC에 대한 읽기 전용 액세스 권한이 있는 사용자의 컨피그레이션을 보여줍니다. 이 사용자가 컨트롤러에 로그인을 시도하면 RADIUS 서버가 인증하고 이 사용자에게 읽기 전용 액세스를 제공합니다.

이 예에서 사용자 이름과 비밀번호는 acsreadonly입니다.

Cisco Secure ACS에서 다음 단계를 완료합니다.

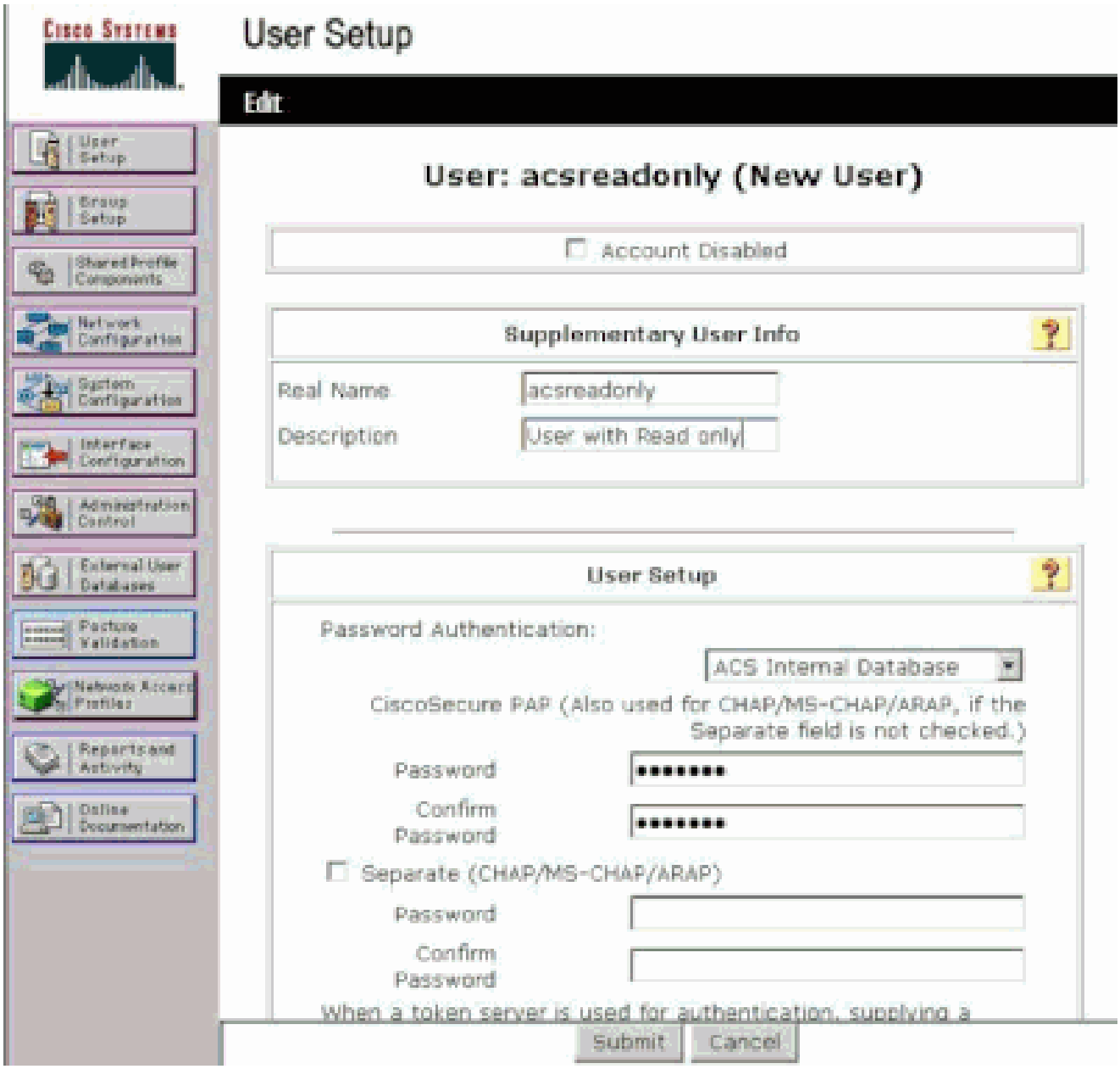
1. ACS GUI에서 User Setup(사용자 설정)을 클릭합니다.

2. ACS에 추가할 사용자 이름을 입력하고 Add/Edit(추가/수정)를 클릭하여 User Edit(사용자 수정) 페이지로 이동합니다.



사용자 이름 추가

3. 이 사용자의 실제 이름, 설명 및 암호를 제공합니다. 이 창에는 예가 나와 있습니다.

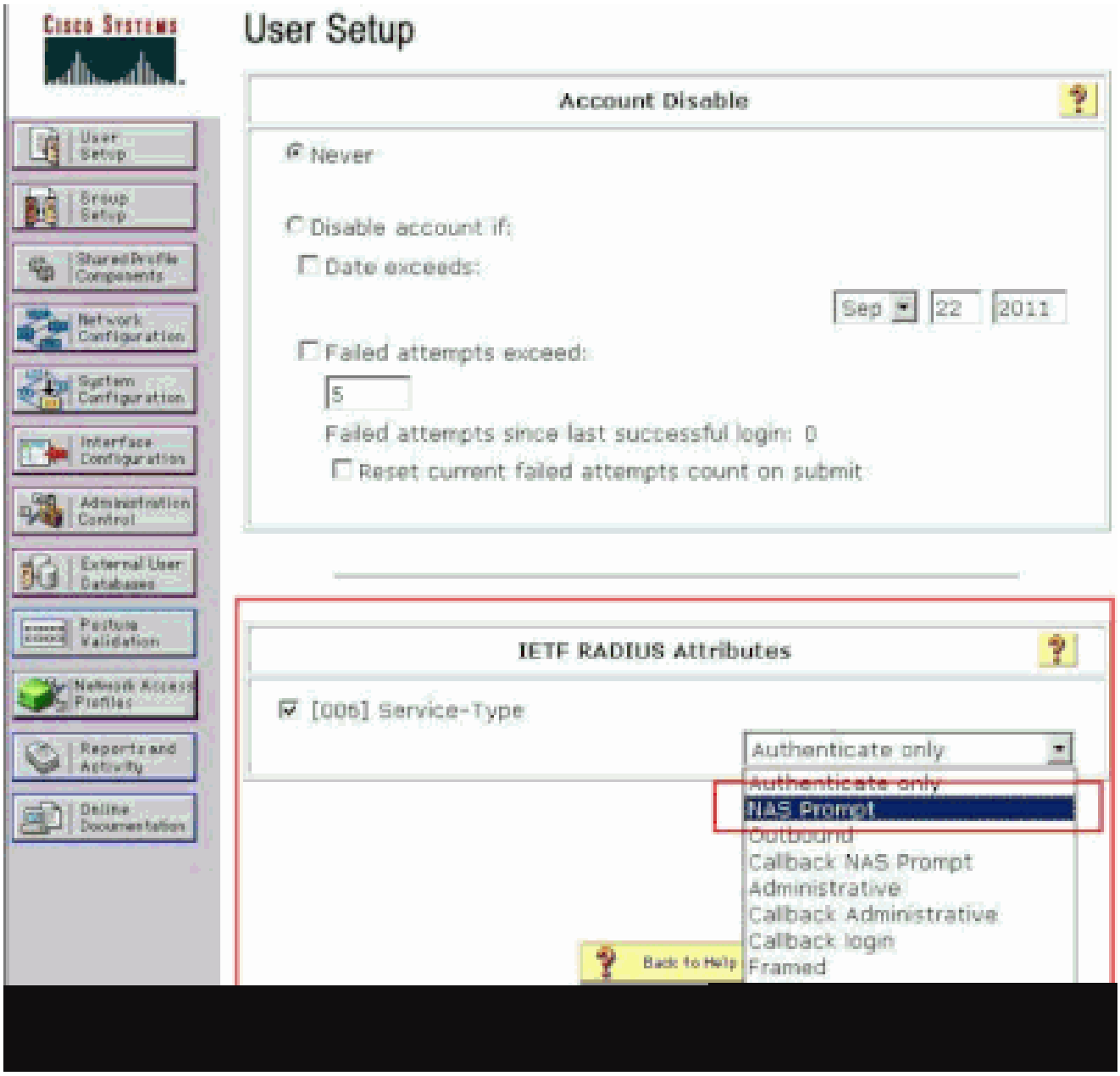


추가된 사용자의 실명, 설명 및 비밀번호 입력

4. 아래로 스크롤하여 IETF RADIUS Attributes(IETF RADIUS 특성) 설정으로 이동한 다음 Service-Type Attribute(서비스 유형 특성)를 선택합니다.

5. 이 예에서는 사용자 acsreadonly가 읽기 전용 액세스 권한을 가져야 하므로 Service-Type 풀다운 메뉴에서 NAS Prompt(NAS 프롬프트)를 선택하고 Submit(제출)을 클릭합니다.

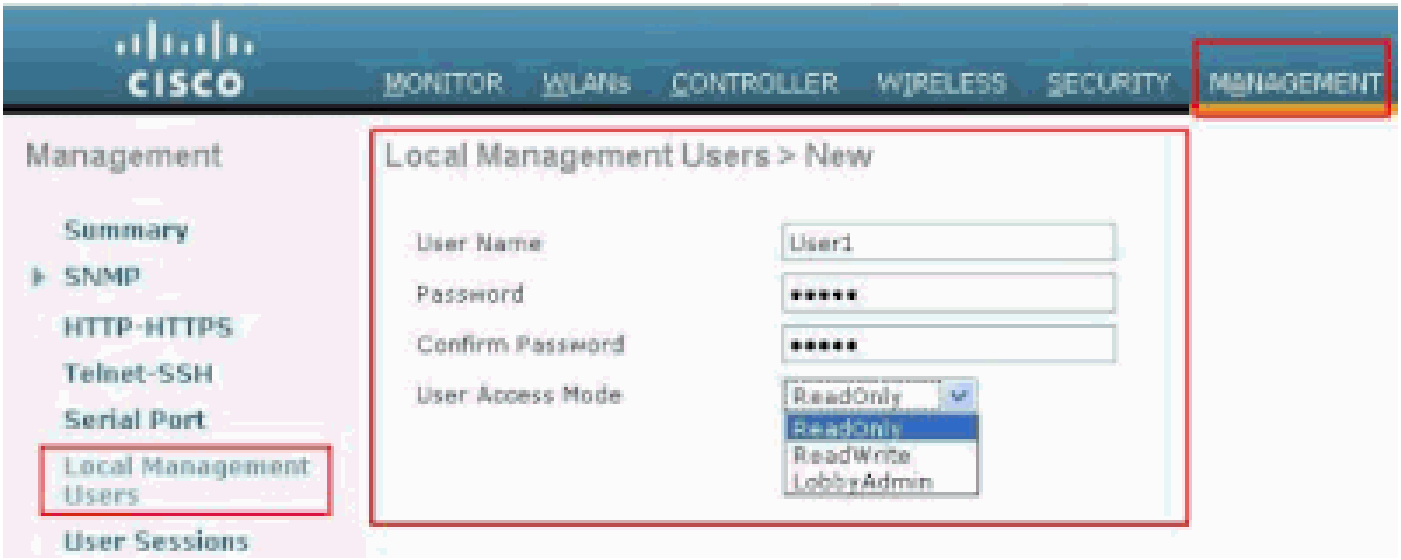
   이렇게 하면 이 특정 사용자가 WLC에 대한 읽기 전용 액세스 권한을 갖게 됩니다.



Service-Type 특성 확인

로컬로 및 RADIUS 서버를 통해 WLC 관리

WLC에서 로컬로 관리 사용자를 구성할 수도 있습니다. 이 작업은 컨트롤러 GUI의 Management(관리) > Local Management Users(로컬 관리 사용자)에서 수행할 수 있습니다.



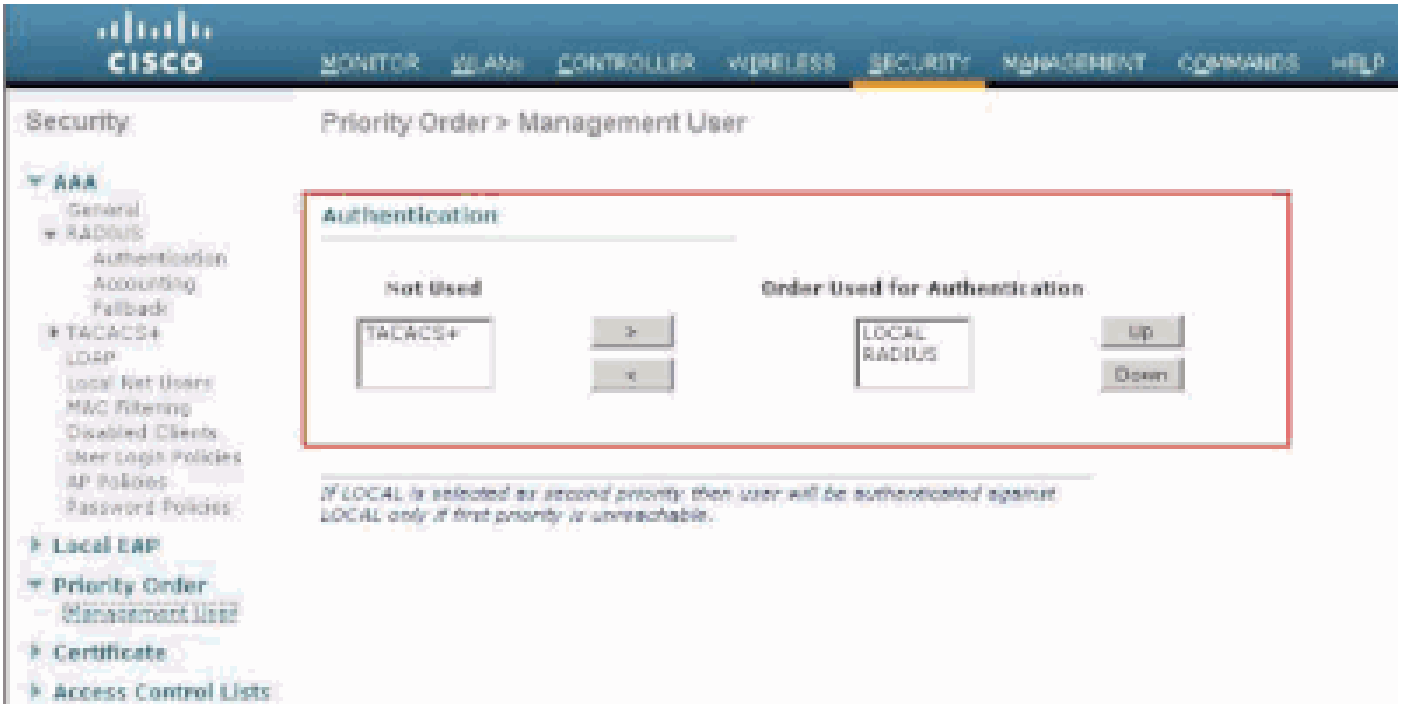
WLC에서 로컬로 관리 사용자 구성

WLC가 로컬뿐 아니라 Management(관리) 확인란이 활성화된 RADIUS 서버에서도 관리 사용자로 구성되어 있다고 가정합니다. 이러한 시나리오에서 기본적으로 사용자가 WLC에 로그인을 시도하면 WLC는 다음과 같은 방식으로 동작합니다.

1. WLC는 먼저 사용자를 검증하기 위해 정의된 로컬 관리 사용자를 확인합니다. 사용자가 로컬 목록에 있는 경우 이 사용자에 대한 인증을 허용합니다. 이 사용자가 로컬에 나타나지 않으면 RADIUS 서버를 찾습니다.

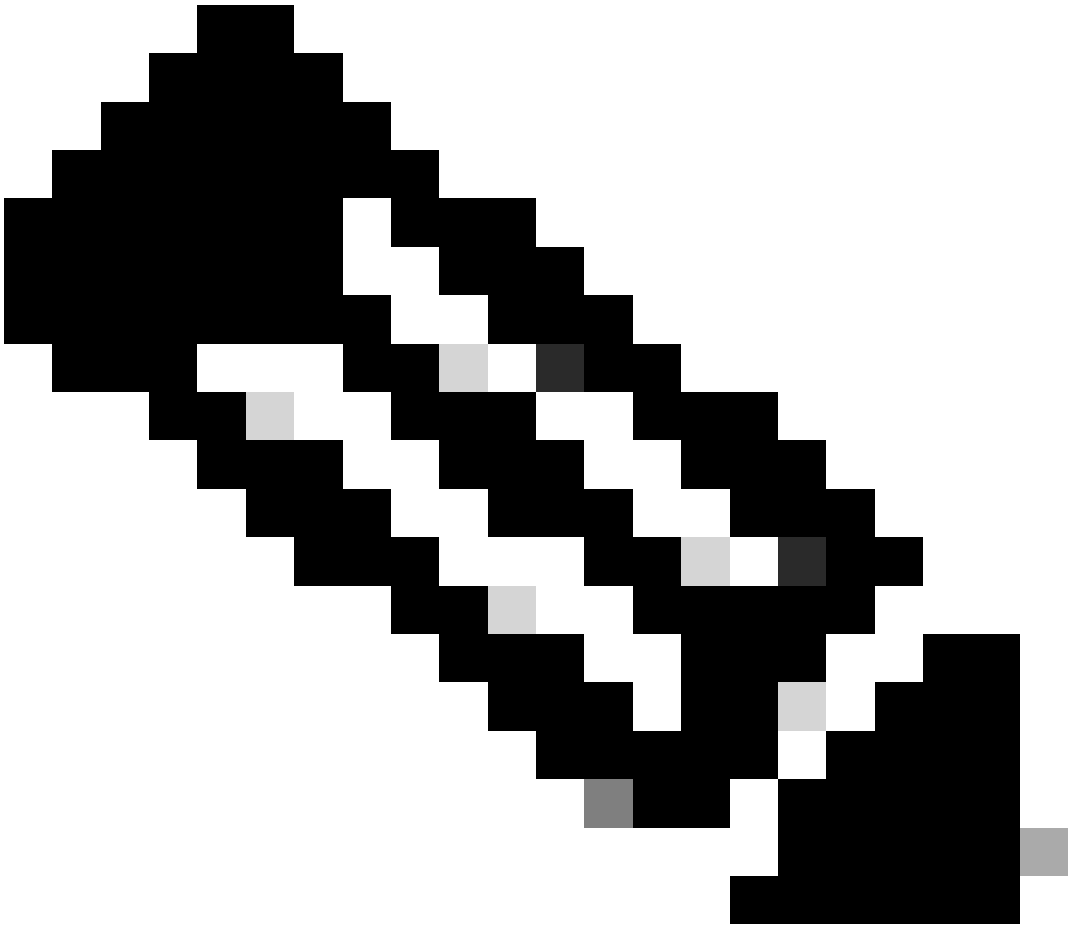
2. 동일한 사용자가 RADIUS 서버에 있을 뿐 아니라 로컬에 모두 존재하지만 액세스 권한이 다른 경우, WLC는 로컬로 지정된 권한으로 사용자를 인증합니다. 즉, WLC의 로컬 컨피그레이션은 RADIUS 서버와 비교할 때 항상 우선합니다.

관리 사용자에 대한 인증 순서는 WLC에서 변경할 수 있습니다. 이렇게 하려면 WLC의 Security(보안) 페이지에서 Priority Order(우선순위 순서) > Management User(관리 사용자)를 클릭합니다. 이 페이지에서 인증 순서를 지정할 수 있습니다. 이제 DDoS 공격의 실제 사례를 살펴보겠습니다.



Management User Selection(관리 사용자 선택)" />

Priority Order(우선순위 순서) > Management User Selection(관리 사용자 선택)



참고: LOCAL을 두 번째 우선 순위로 선택하면 첫 번째 우선 순위로 정의된 방법(RADIUS/TACACS)에 연결할 수 없는 경우에만 이 방법으로 사용자가 인증됩니다.

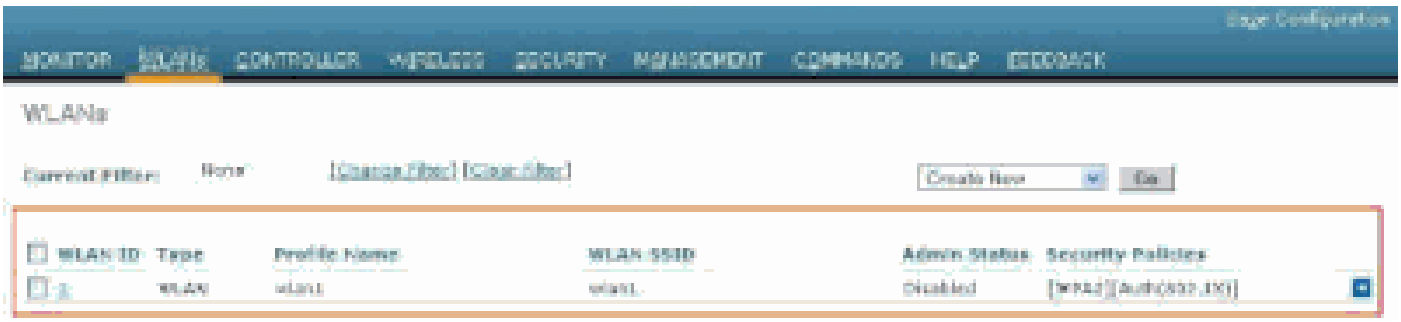
다음을 확인합니다.

컨피그레이션이 제대로 작동하는지 확인하려면 CLI 또는 GUI(HTTP/HTTPS) 모드를 통해 WLC에 액세스합니다. 로그인 프롬프트가 나타나면 Cisco Secure ACS에 구성된 대로 사용자 이름 및 비밀번호를 입력합니다.

컨피그레이션이 올바르면 WLC에 성공적으로 인증됩니다.

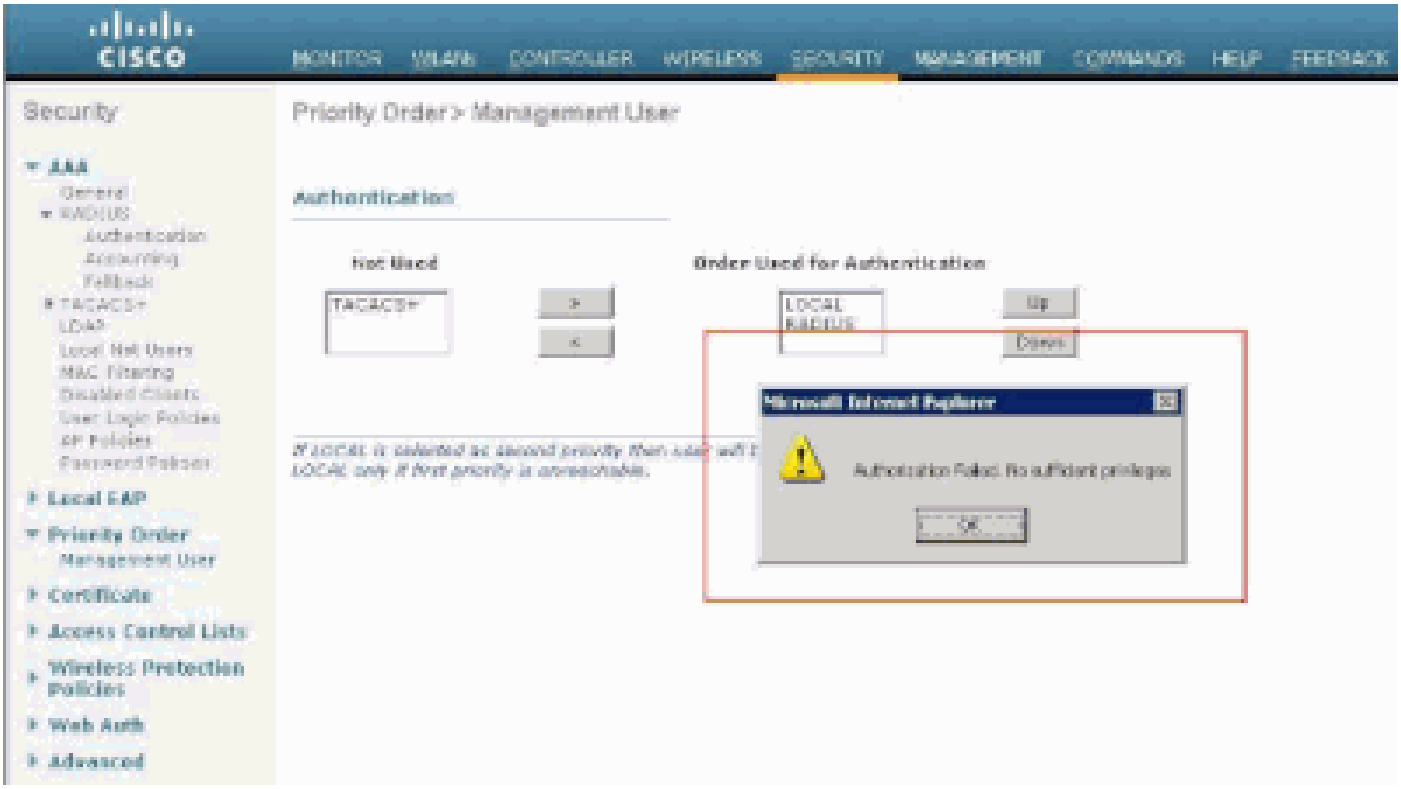
또한 ACS에서 지정한 대로 인증된 사용자에게 액세스 제한이 제공되는지 확인할 수 있습니다. 이렇게 하려면 HTTP/HTTPS를 통해 WLC GUI에 액세스합니다(WLC에서 HTTP/HTTPS를 허용하도록 구성되었는지 확인).

ACS에서 읽기-쓰기 액세스 권한이 설정된 사용자는 WLC에서 몇 가지 구성 가능한 권한을 가집니다. 예를 들어 읽기-쓰기 사용자는 WLC의 WLANs 페이지 아래에 새 WLAN을 생성할 수 있는 권한을 가집니다. 이 창에는 예가 나와 있습니다.



WLC에서 구성 가능한 권한

읽기 전용 권한이 있는 사용자가 컨트롤러의 컨피그레이션을 변경하려고 하면 이 메시지가 표시됩니다.



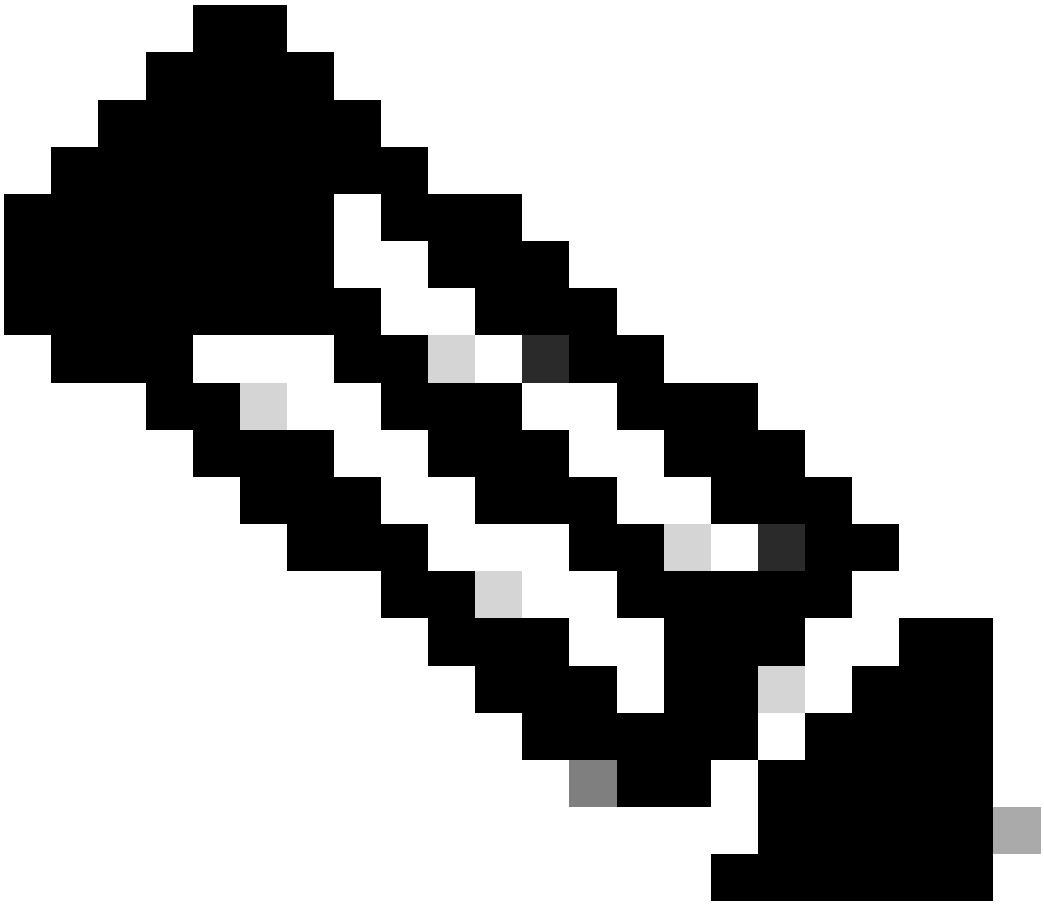
읽기 전용 액세스로 컨트롤러를 변경할 수 없습니다.

이러한 액세스 제한은 WLC의 CLI를 통해서도 확인할 수 있습니다. 이 출력은 예를 보여줍니다.

```
<#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.
```

이 예제 출력에서 볼 수 있듯이, 컨트롤러 CLI에서 는 현재 사용자에 대해 사용 가능한 명령 목록을 표시합니다. 또한 이 예제 출력에서 **config** 명령을 사용할 수 없습니다. 이는 읽기 전용 사용자에게 WLC에서 어떤 컨피그레이션도 수행할 수 있는 권한이 없음을 나타냅니다. 반면 읽기/쓰기 사용자는 컨트롤러에서 컨피그레이션을 수행할 수 있는 권한이 있습니다(GUI 및 CLI 모드 모두).



참고: RADIUS 서버를 통해 WLC 사용자를 인증한 후에도 페이지 간에 이동할 때마다 HTTP[S] 서버가 클라이언트를 완전히 인증합니다. 각 페이지에서 인증 프롬프트가 표시되지 않는 유일한 이유는 브라우저가 자격 증명을 캐시하고 재생하기

때문입니다.

문제 해결

컨트롤러가 ACS를 통해 관리 사용자를 인증하면 인증이 성공적으로 완료되고(access-accept) 컨트롤러에서 권한 부여 오류가 표시되지 않는 경우가 있습니다.그러나 사용자에게 인증을 다시 묻는 메시지가 표시됩니다.

그러한 경우, 당신은 무엇이 잘못 해석 할 수 없습니다 왜 사용자가 단지 명령만으로 WLC에 로그인 할 수 **debug aaa events enable** 없습니다. 대신 컨트롤러는 인증을 위해 다른 프롬프트를 표시합니다.

한 가지 가능한 이유는 ACS에서 사용자 이름과 비밀번호가 올바르게 구성되었지만 ACS가 특정 사용자 또는 그룹에 대한 Service-Type 특성을 전송하도록 구성되지 않았기 때문입니다.

AAA 서버에서 **access-accept**가 다시 전송되더라도 명령**debug aaa events enable** 의 출력은 사용자에게 필요한 특성(예: Service-Type 특성)이 없음을 나타내지 않습니다. 이 예제 **debug aaa events enable** 명령 출력은 예를 보여줍니다.

<#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:
```

이 첫 번째 예 **debug aaa events enable** 명령 출력에서는 RADIUS 서버에서 Access-Accept를 성공적으로 수신했지만 Service-Type 특성이 WLC에 전달되지 않았음을 확인할 수 있습니다. 이는 특정 사용자가 ACS에서 이 속성으로 구성되지 않았기 때문입니다.

사용자 인증 후 Service-Type 특성을 반환하도록 Cisco Secure ACS를 구성해야 합니다. Service-Type 특성 값은 사용자 권한에 따라 **Administrative** 또는 **NAS**-Prompt로 설정해야 합니다.

두 번째 예에서는 명령 **debug aaa events enable**출력을 다시 보여줍니다. 그러나 이번에는 Service-Type 특성이 ACS에서 **Administrative**로 설정됩니다.

```
    <#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)

이 이전 예제 출력에서 Service-Type 특성이 WLC에 전달되는 것을 확인할 수 있습니다.

관련 정보

- **Wireless LAN Controller 구성 - 컨피그레이션 가이드**
- **무선 LAN 컨트롤러에서 VLAN 구성**
- **동적 VLAN 할당을 위한 RADIUS 서버 및 WLC 구성**
- **무선 LAN 컨트롤러 및 경량형 액세스 포인트 기본 설정**
- **무선 LAN 컨트롤러로 AP 그룹 VLAN 구성**
- **Cisco 기술 지원 및 다운로드**

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.