9800 WLC에서 GUI & CLI 인증을 위한 RADIUS & TACACS+ 구성

목차

소개

이 문서에서는 RADIUS 또는 TACACS+ 외부 인증을 위해 Catalyst 9800을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Catalyst Wireless 9800 구성 모델
- AAA, RADIUS 및 TACACS+ 개념

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- C9800-CL v17.9.2
- ISE 3.2.0

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.

배경 정보

사용자가 WLC의 CLI 또는 GUI에 액세스하려고 하면 사용자 이름과 비밀번호를 입력하라는 메시지가 표시됩니다. 기본적으로 이러한 자격 증명은 디바이스 자체에 있는 사용자의 로컬 데이터베이스와 비교됩니다. 또는 입력 자격 증명을 원격 AAA 서버와 비교하도록 WLC에 지시할 수 있습니다. WLC는 RADIUS 또는 TACACS+를 사용하여 서버와 통신할 수 있습니다.

구성

이 예에서는 AAA 서버(ISE)에서 각각 및 의 두 가지 adminuser유형의 사용자를 helpdeskuser 구성합니다. 이러한 사용자는 각각 및admin-group 그룹의helpdesk-group 일부입니다. 의 일부인adminuser 사용자에게 admin-group WLC에 대한 전체 액세스 권한이 부여되어야 합니다. 반면, 의 helpdeskuser 일부인 는helpdesk-group WLC에 대한 모니터 권한만 부여됩니다. 따라서 컨피그레이션 액세스가 없습니다.

이 문서에서는 먼저 RADIUS 인증을 위해 WLC 및 ISE를 구성하고 나중에 TACACS+에 대해서도 동일한 작업을 수행합니다.

읽기 전용 사용자 제한

9800 WebUI 인증에 TACACS+ 또는 RADIUS를 사용하는 경우 다음과 같은 제한이 있습니다.

- 권한 수준이 0인 사용자가 있지만 GUI에 액세스할 수 없습니다.
- 권한 수준이 1-14인 사용자는 모니터 탭만 볼 수 있습니다(읽기 전용 로컬 인증 사용자의 권한 수준과 동일)
- 권한 수준이 15인 사용자는 전체 액세스 권한을 갖습니다.
- 권한 수준이 15이고 특정 명령만 허용하는 명령 집합이 있는 사용자는 지원되지 않습니다. 사용자는 WebUI를 통해 컨피그레이션 변경을 실행할 수 있습니다

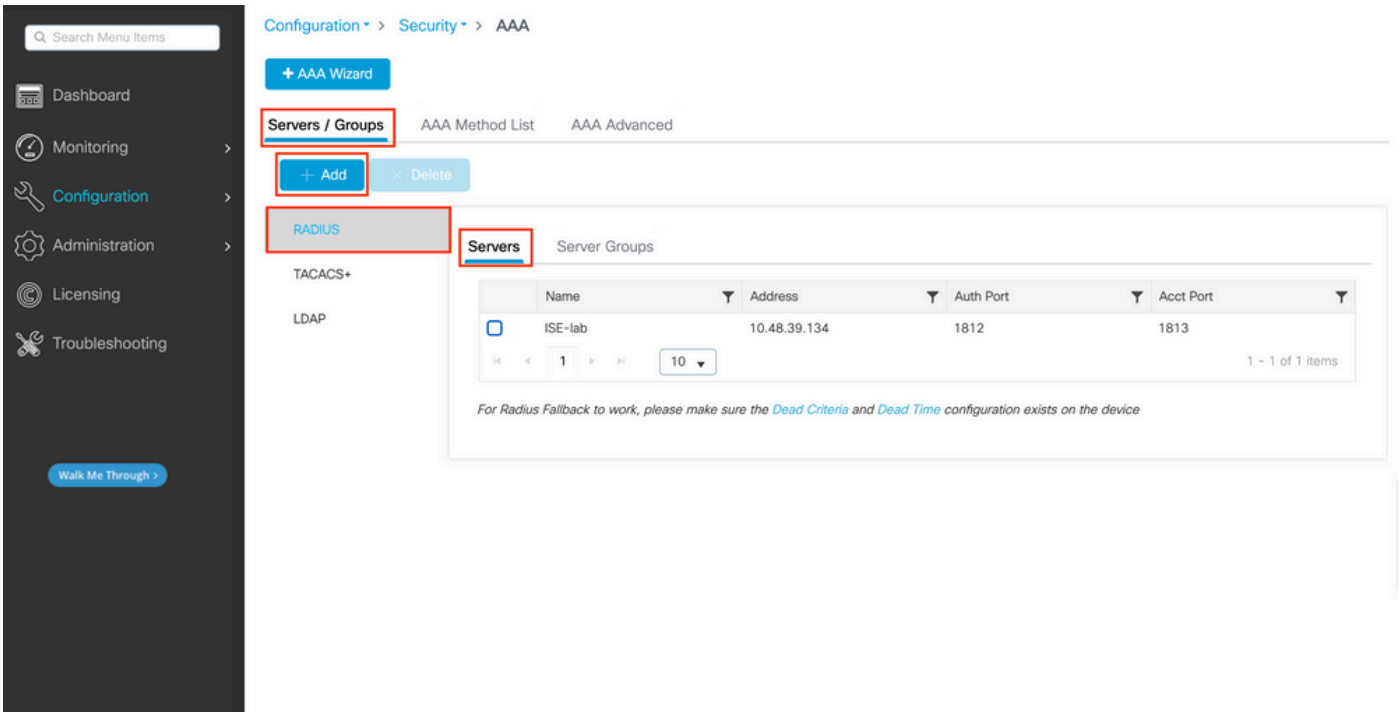
이러한 고려 사항은 변경하거나 수정할 수 없습니다.

WLC에 대한 RADIUS 인증 구성

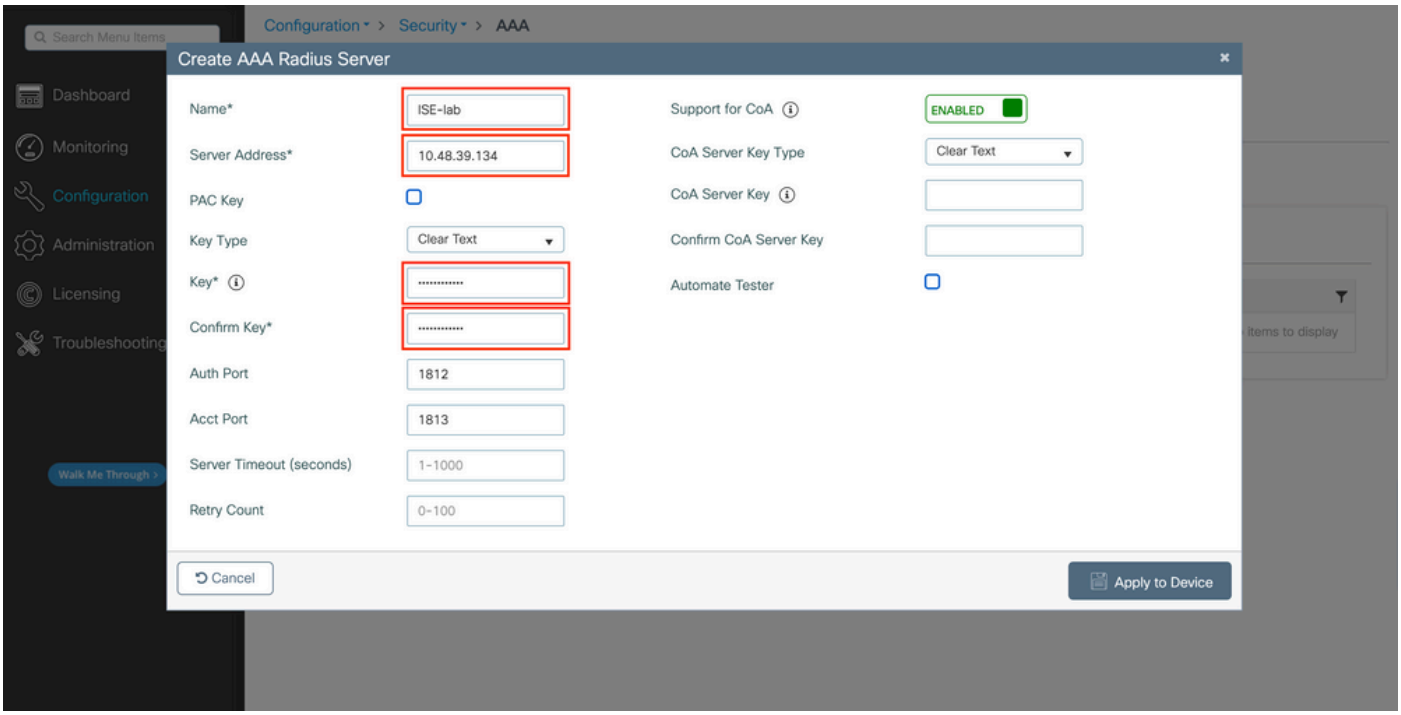
1단계. RADIUS 서버를 선언합니다.

GUI에서:

먼저 WLC에서 ISE RADIUS 서버를 생성합니다. 이 작업은 GUI WLC 페이지Servers/Groups > RADIUS > Servers에서 액세스할 수 있는 탭에서 수행할 수 있습니다https://<WLC-IP>/webui/#/aaa. 또는 로 이동하면Configuration > Security > AAA 이 이미지에 표시된 대로 수행할 수 있습니다.



WLC에 RADIUS 서버를 추가하려면 이미지의 빨간색으로 표시된 Add(추가) 버튼을 클릭합니다. 그러면 스크린샷에 표시된 팝업 창이 열립니다.



이 팝업 창에서 다음을 제공해야 합니다.

- 서버 이름(ISE 시스템 이름과 일치하지 않아도 됨)
- 서버 IP 주소
- WLC와 RADIUS 서버 간의 공유 암호

인증 및 어카운팅에 사용되는 포트와 같은 다른 매개변수를 구성할 수 있지만, 이러한 매개변수는 필수 사항이 아니며 이 설명서의 기본값으로 남겨둡니다.

CLI에서:

<#root>

WLC-9800(config)#radius server

ISE-lab

WLC-9800(config-radius-server)#address ipv4

10.48.39.134

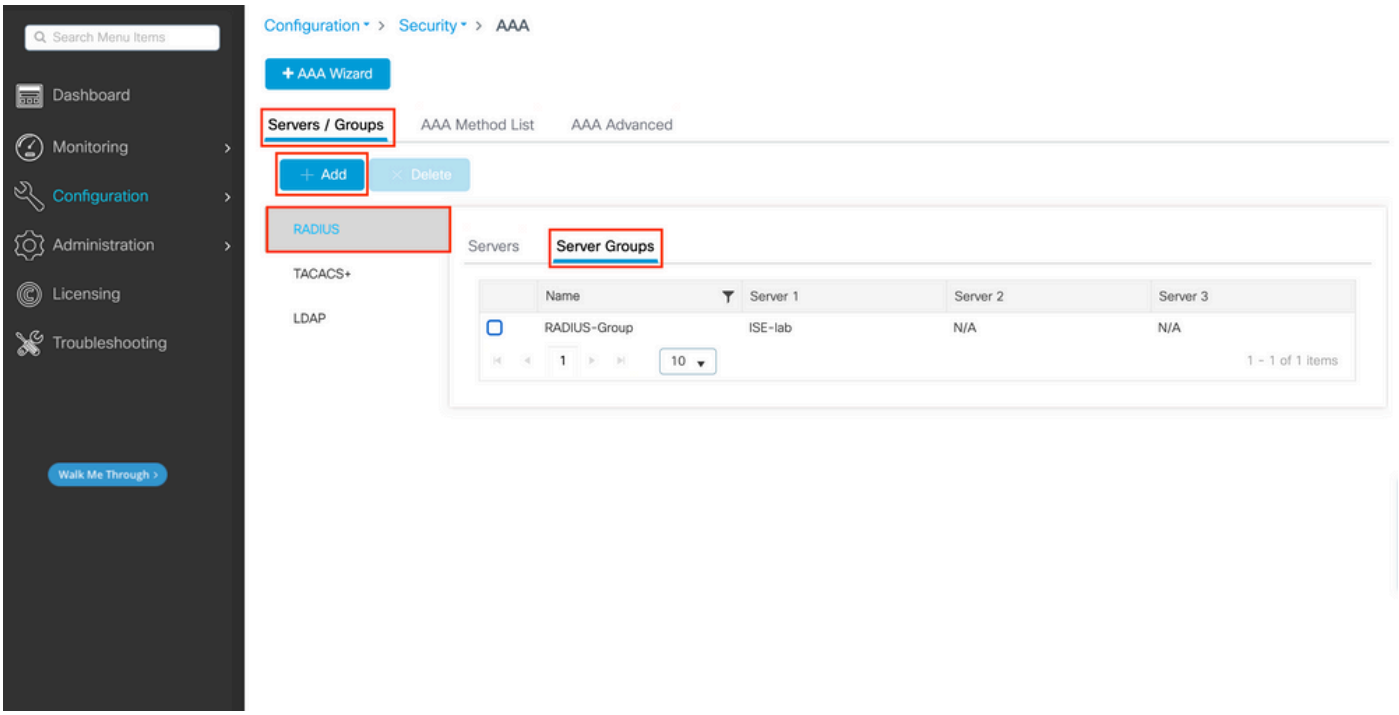
auth-port 1812 acct-port 1813
WLC-9800(config-radius-server)#key

Cisco123

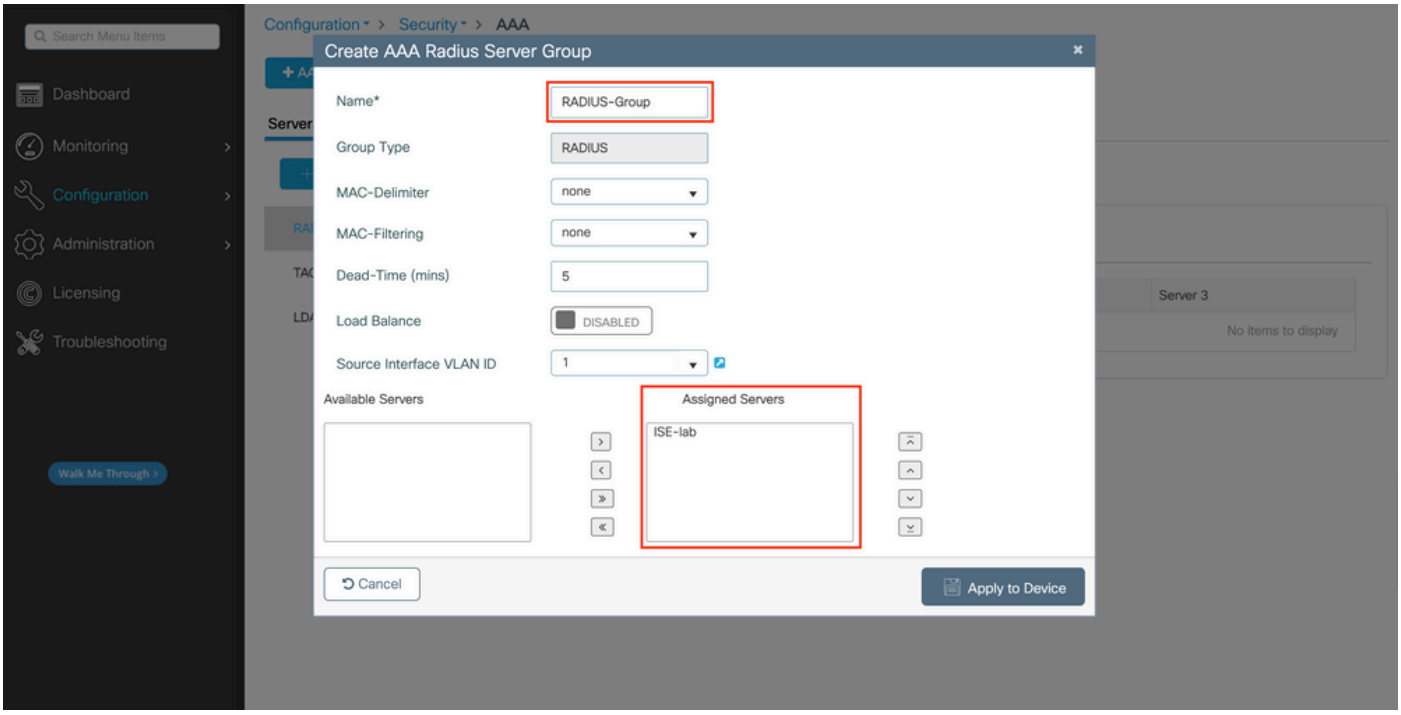
2단계. RADIUS 서버를 서버 그룹에 매핑합니다.

GUI에서:

인증에 사용할 수 있는 여러 RADIUS 서버가 있는 경우, 이러한 모든 서버를 동일한 서버 그룹에 매핑하는 것이 좋습니다. WLC는 서버 그룹의 서버 간에 로드 밸런싱과 다른 인증을 처리합니다. RADIUS 서버 그룹은 그림에Servers/Groups > RADIUS > Server Groups 표시된 대로 1단계에서 언급한 것과 동일한 GUI 페이지의 탭에서 구성됩니다.



서버 생성의 경우, 여기에 표시된 Add(추가) 버튼(이전 이미지에서 프레임)을 클릭하면 팝업 창이 나타납니다.



팝업에서 그룹에 이름을 제공하고 Assigned Servers(할당된 서버) 목록으로 원하는 서버를 이동합니다.

CLI에서:

<#root>

WLC-9800(config)# aaa group server radius

RADIUS-Group

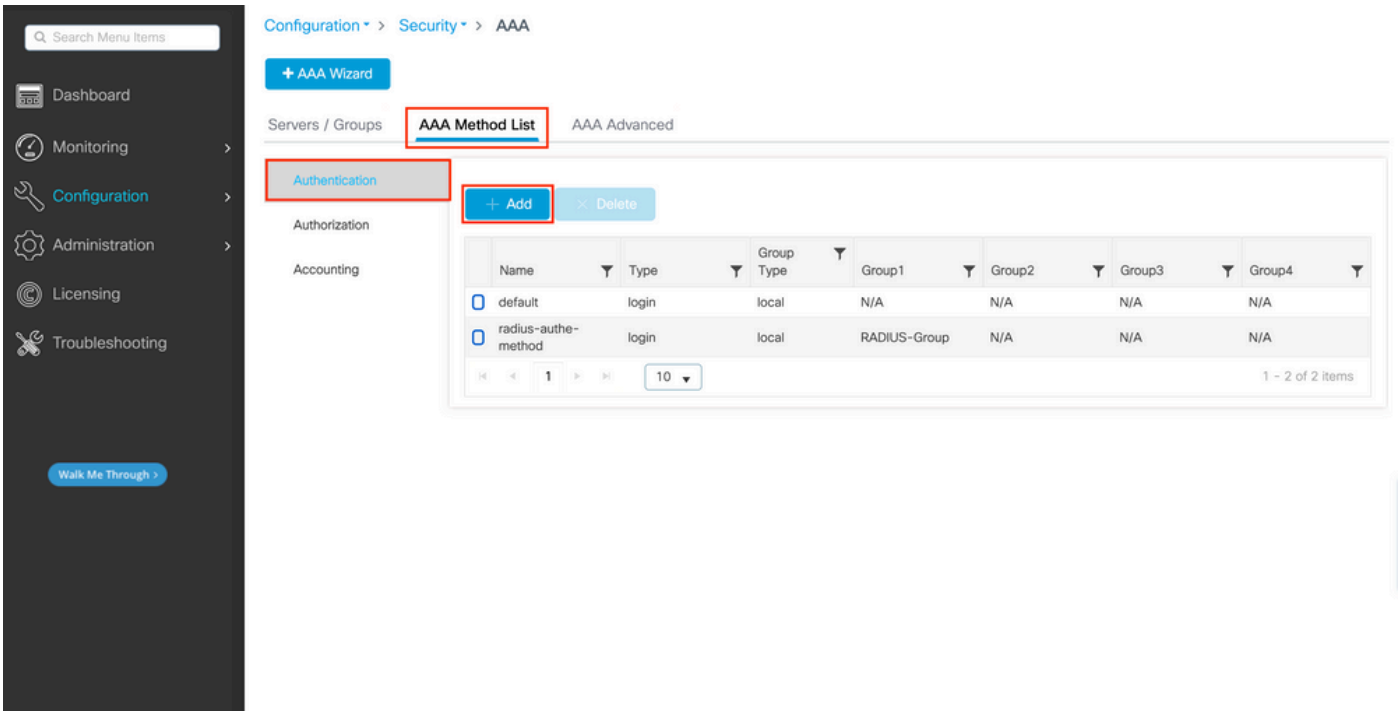
WLC-9800(config-sg-radius)# server name

ISE-lab

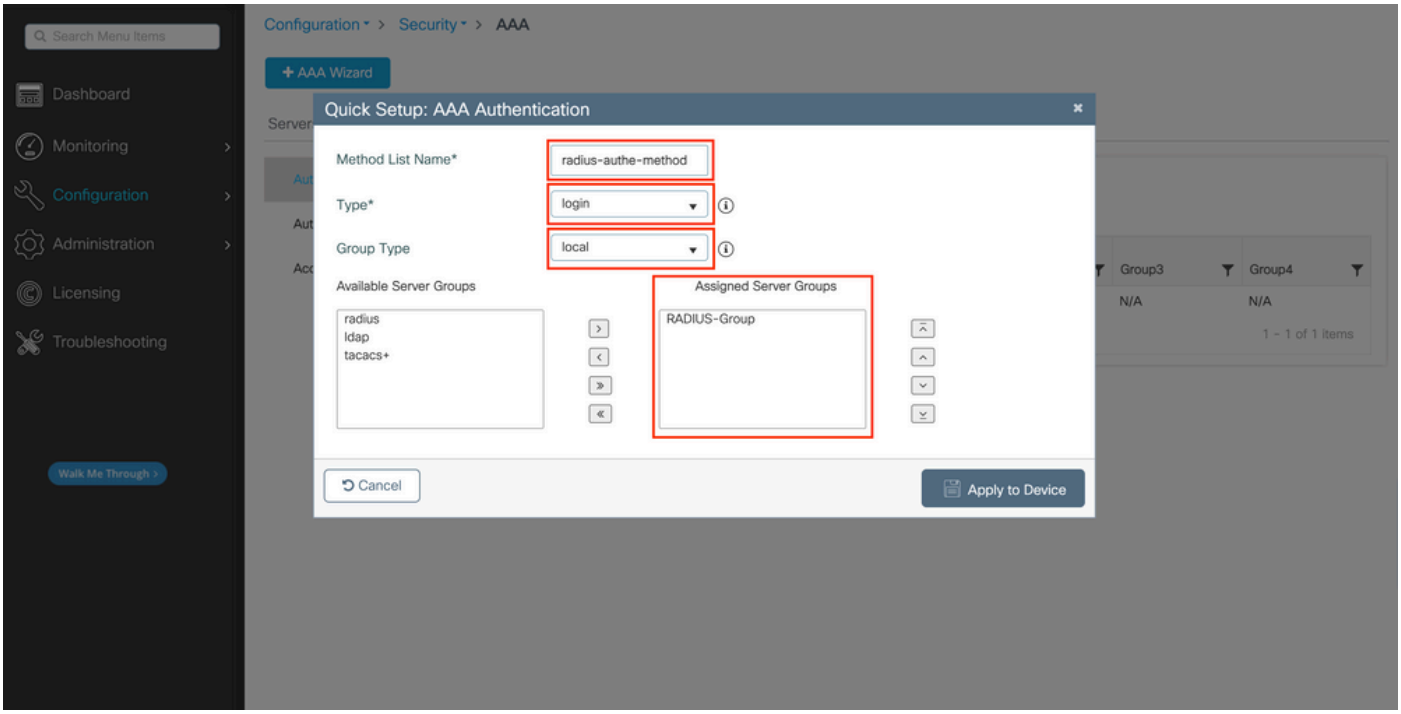
3단계. RADIUS 서버 그룹을 가리키는 방법으로 AAA 인증 로그를 생성합니다.

GUI에서:

GUI 페이지에서 https://<WLC-IP>/webui/#/aaa 탭으로 AAA Method List > Authentication 이동하여 이 이미지에 표시된 인증 방법을 생성합니다.



평소와 같이 Add(추가) 버튼을 사용하여 인증 방법을 생성하면 이 이미지에 표시된 것과 유사한 컨피그레이션 팝업 창이 나타납니다.



이 팝업 창에서 메서드의 이름을 입력합니다. 로그인으로 선택하고 Type이전 단계에서 만든 그룹 서버를 목록에 Assigned Server Groups 추가합니다. Group Type(그룹 유형) 필드에서는 여러 컨피그레이션이 가능합니다.

- Group Type(그룹 유형)을 local(로컬)로 선택하면 WLC는 먼저 사용자 자격 증명이 로컬에 존재하는지 확인한 다음 서버 그룹으로 돌아갑니다.
- Group Type(그룹 유형)을 그룹으로 선택하고 Fall back to local(로컬로 폴백) 옵션을 선택하지 않으면 WLC는 서버 그룹에 대한 사용자 자격 증명만 확인합니다.
- Group Type as a group(그룹 유형)을 선택하고 Fallback to local(로컬로 대체) 옵션을 선택하면 WLC는 서버 그룹에 대해 사용자 자격 증명을 확인하고 서버가 응답하지 않는 경우에만 로컬 데이터베이스를 쿼리합니다. 서버에서 거부를 전송하면 로컬 데이터베이스에 존재할 수 있더라도 사용자를 인증해야 합니다.

CLI에서:

사용자 자격 증명을 로컬에서 먼저 찾을 수 없는 경우에만 서버 그룹과 함께 확인하도록 하려면 다음을 사용합니다.

```
<#root>

WLC-9800(config)#aaa authentication login
```

`radius-authe-method`

```
 local group
```

RADIUS-Group

서버 그룹에서만 사용자 자격 증명을 검사하려면 다음을 사용합니다.

```
    <#root>

WLC-9800(config)#aaa authentication login
```

radius-authe-method

```
 group
```

RADIUS-Group

사용자 자격 증명을 서버 그룹과 함께 확인하려는 경우 그리고 이 마지막 항목이 로컬 엔트리와 함께 응답하지 않을 경우 다음을 사용합니다.

```
    <#root>

WLC-9800(config)#aaa authentication login
```

radius-authe-method

group

RADIUS-Group

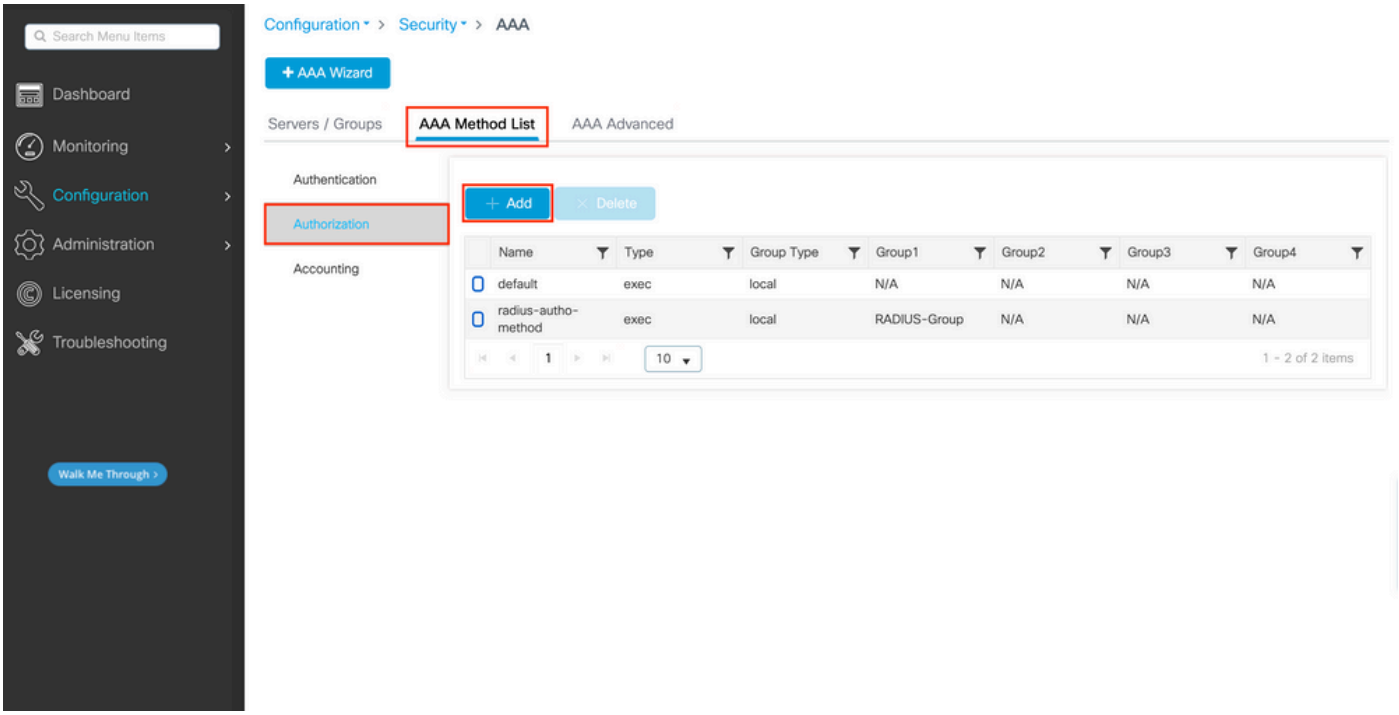
local

이 예제 설정에서는 로컬에서만 생성된 사용자가 있으며 ISE 서버에서만 생성된 사용자가 있으므로 첫 번째 옵션을 사용합니다.

4단계. RADIUS 서버 그룹을 가리키는 AAA 권한 부여 exec 방법을 생성합니다.

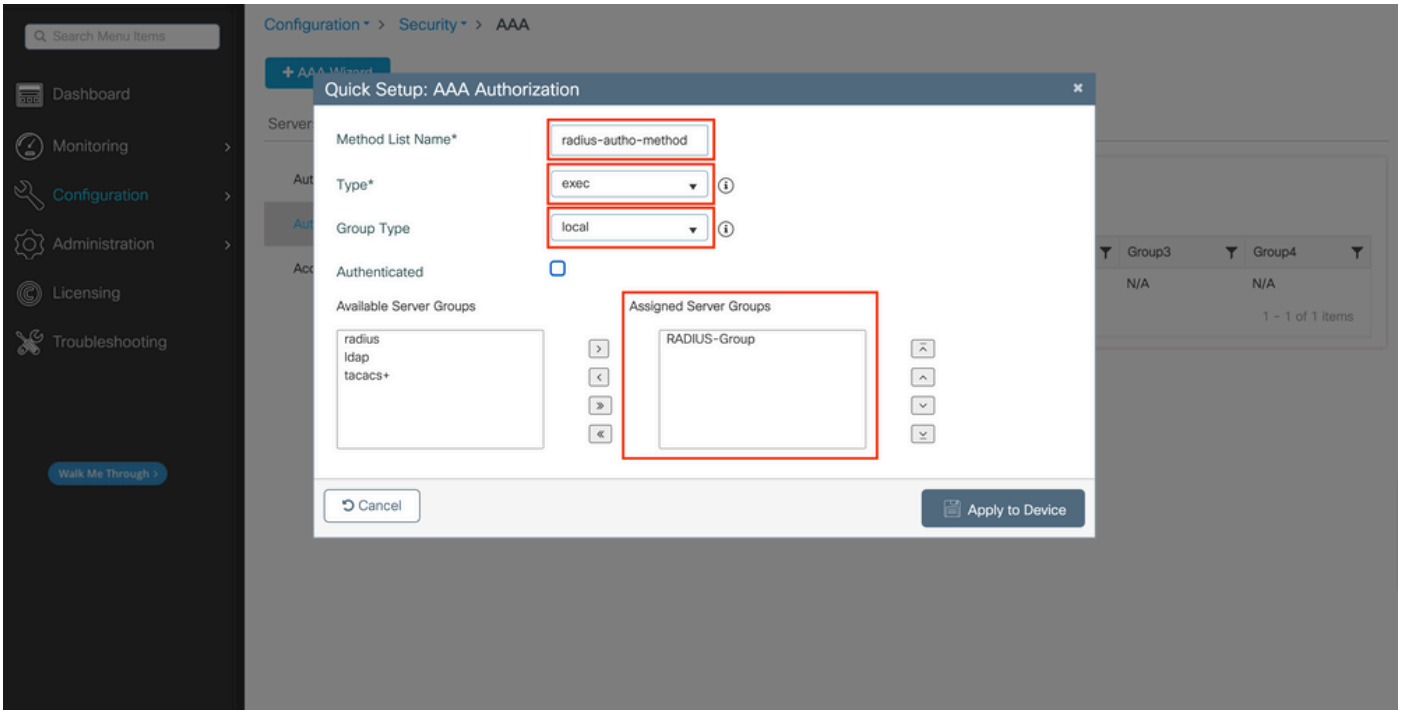
GUI에서:

사용자에게 액세스 권한을 부여하려면 권한이 있어야 합니다. 에서 GUI Page Configuration > Security > AAA 탭으로 AAA Method List > Authorization 이동한 다음 이 이미지에 표시된 대로 권한 부여 방법을 생성합니다.



인증 방법 생성

Add(추가) 버튼을 사용하여 새 방법을 추가하면 표시된 것과 유사한 권한 부여 방법 컨피그레이션 팝업이 나타납니다.



이 컨피그레이션 팝업에서 권한 부여 방법의 이름을 제공하고 Type asexec(유형)를 선택하고 3단계에서 인증 방법에 사용된 것과 동일한 그룹 유형 순서를 사용합니다.

CLI에서:

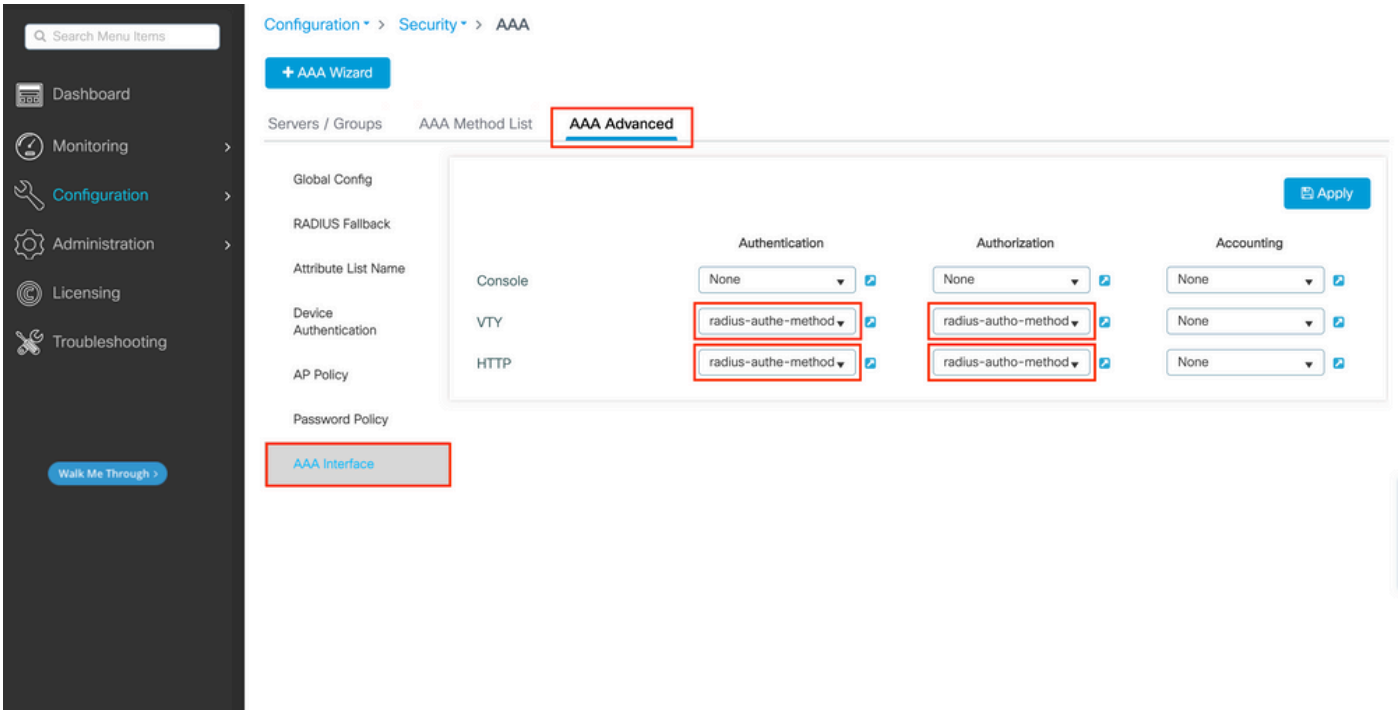
인증 방법의 경우 먼저 권한 부여가 할당되어 로컬 항목에 대해 사용자를 검사한 다음 서버 그룹의 항목에 대해 검사합니다.

```
<#root>

WLC-9800(config)#aaa authorization exec

radius-autho-method

 local group

RADIUS-Group
```

5단계. HTTP 컨피그레이션 및 텔넷/SSH에 사용되는 VTY 라인에 방법을 할당합니다.

GUI에서:

생성된 인증 및 권한 부여 방법을 HTTP 및/또는 텔넷/SSH 사용자 연결에 사용할 수 있습니다. 이 방법은 이 이미지에 표시된 것처럼 GUI WLC 페이지에서 액세스 가능한AAA Advanced > AAA Interface 탭에서https://<WLC-IP>/webui/#/aaa 계속 구성할 수 있습니다.



GUI 인증을 위한 CLI:

```
<#root>

WLC-9800(config)#ip http authentication aaa login-authentication

radius-authe-method

WLC-9800(config)#ip http authentication aaa exec-authorization

radius-autho-method
```

텔넷/SSH 인증을 위한 CLI:

<#root>

WLC-9800(config)#line vty 0 15 WLC-9800(config-line)#login authentication

radius-authe-method

WLC-9800(config-line)#authorization exec

radius-autho-method

HTTP 컨피그레이션을 변경할 경우 HTTP 및 HTTPS 서비스를 다시 시작하는 것이 가장 좋습니다. 이 작업은 다음 명령으로 수행할 수 있습니다.

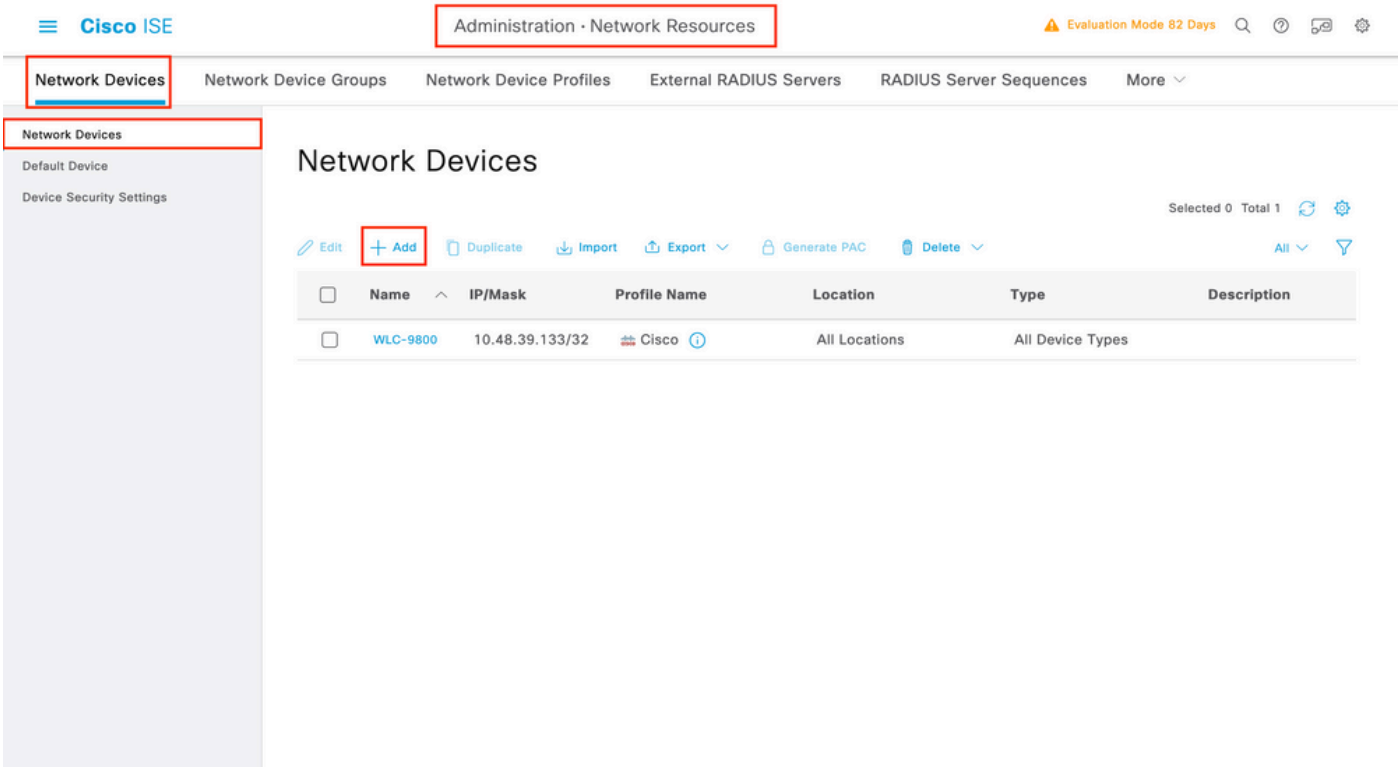
WLC-9800(config)#no ip http server WLC-9800(config)#no ip http secure-server WLC-9800(config)#ip http server WLC-9800(config)#ip http secure-serv

RADIUS를 위한 ISE 구성

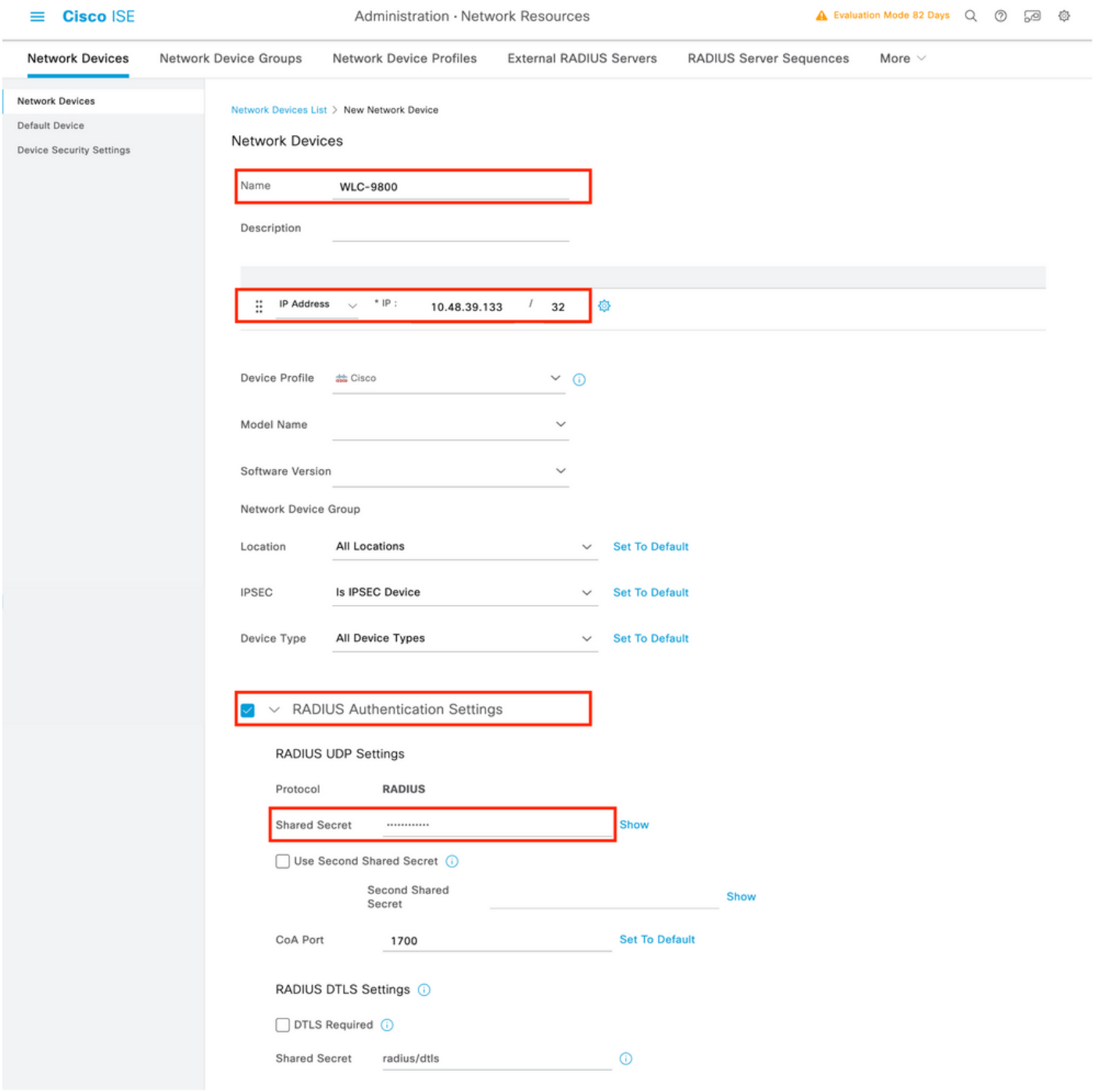
1단계. WLC를 RADIUS용 네트워크 디바이스로 구성합니다.

GUI에서:

이전 섹션에서 사용된 WLC를 ISE의 RADIUS용 네트워크 디바이스로 선언하려면 다음 이미지에 표시된 것처럼 Network devices(네트워크 디바이스) 탭으로 이동하여Administration > Network Ressources > Network Devices 엽니다.



네트워크 디바이스를 추가하려면 Add 버튼을 사용합니다. 그러면 새 네트워크 디바이스 컨피그레이션 양식이 열립니다.

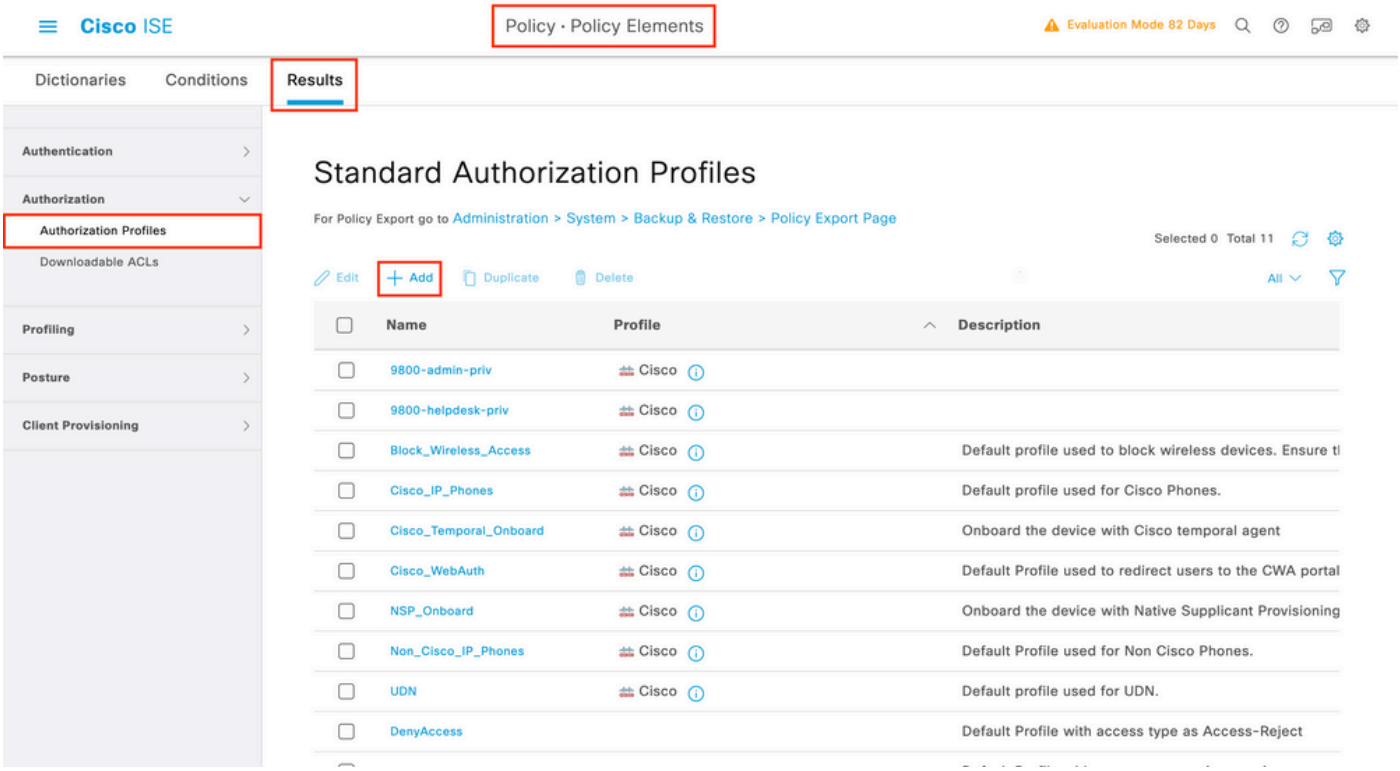


새 창에서 네트워크 디바이스의 이름을 제공하고 해당 IP 주소를 추가합니다. RADIUS Authentication Settings(RADIUS 인증 설정)를 선택하고 WLC에서 사용되는 것과 동일한 RADIUS 공유 암호를 구성합니다.

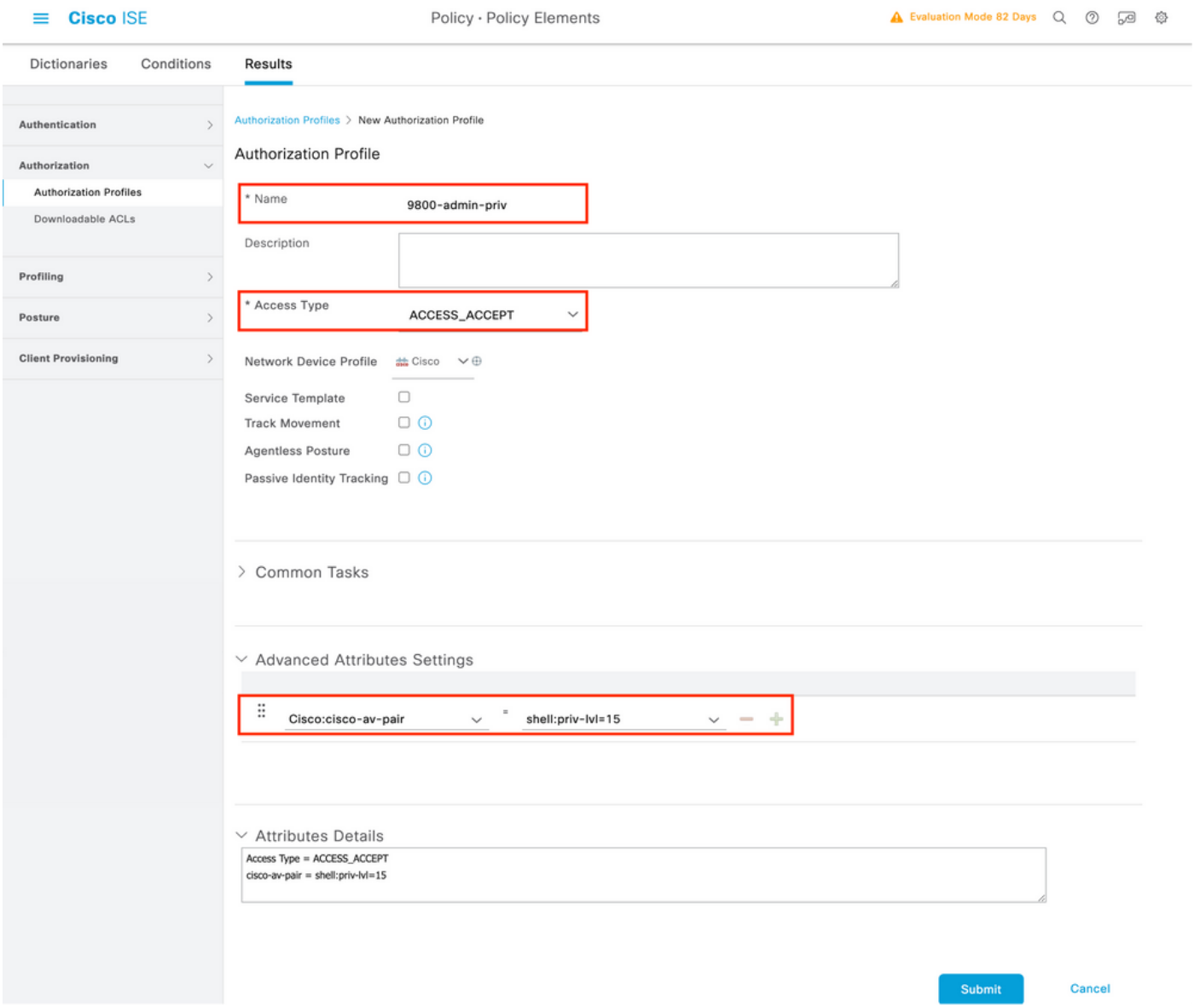
2단계. 권한 부여 결과를 생성하여 권한을 반환합니다.

GUI에서:

관리자 액세스 권한을 가지려면 는 adminuser EXEC 프롬프트 셸에 액세스할 수 있는 권한 레벨 15를 가져야 합니다. 반면 는 helpdeskuser exec 프롬프트 셸 액세스가 필요하지 않으므로 15보다 낮은 권한 레벨로 할당될 수 있습니다. 사용자에게 적절한 권한 수준을 할당하려면 권한 부여 프로파일을 사용할 수 있습니다. 다음 그림에 표시된 ISE GUI Page Policy > Policy Elements > Results 탭 Authorization > Authorization Profiles 아래에서 구성할 수 있습니다.



새 권한 부여 프로파일을 구성하려면 Add 버튼을 사용합니다. 그러면 새 권한 부여 프로파일 컨피그레이션 양식이 열립니다. 에 할당된 프로필을 구성하려면 이 양식이 특히 이와 같아야 합니다adminuser.



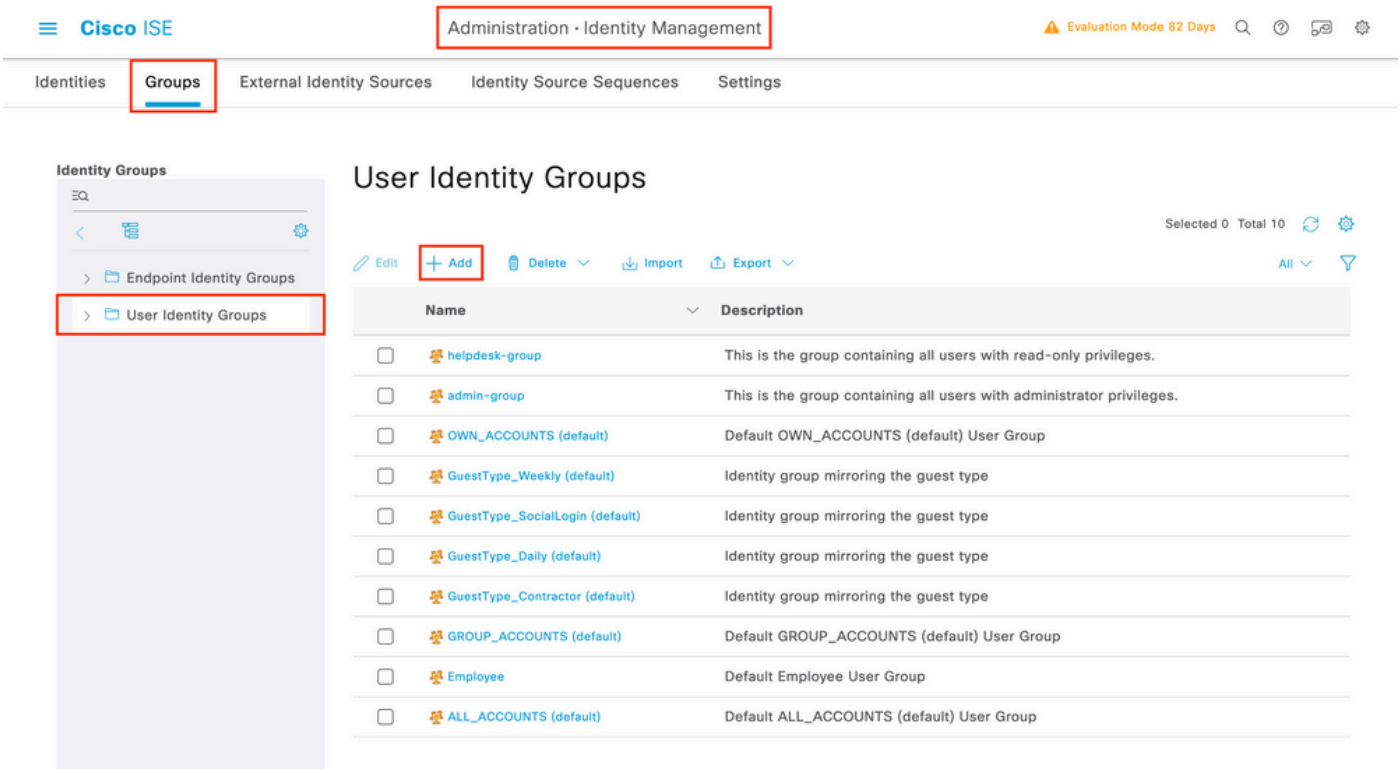
이 컨피그레이션에서는 권한 레벨 15를 연결된 모든 사용자에게 부여했습니다. 앞에서 언급했듯이 이는 다음 단계 중에adminuser 생성되는 의 예상 동작입니다. 그러나 는 helpdeskuser 더 낮은 권한 레벨을 가져야 하므로 두 번째 정책 요소를 만들어야 합니다.

의 정책 요소helpdeskusershell:priv-lvl=15 는 문자열을 로 변경하고 X를 shell:priv-lvl=X원하는 권한 레벨로 대체해야 한다는 점을 제외하고는 위에서 생성한 것과 유사합니다. 이 예에서는 1이 사용됩니다.

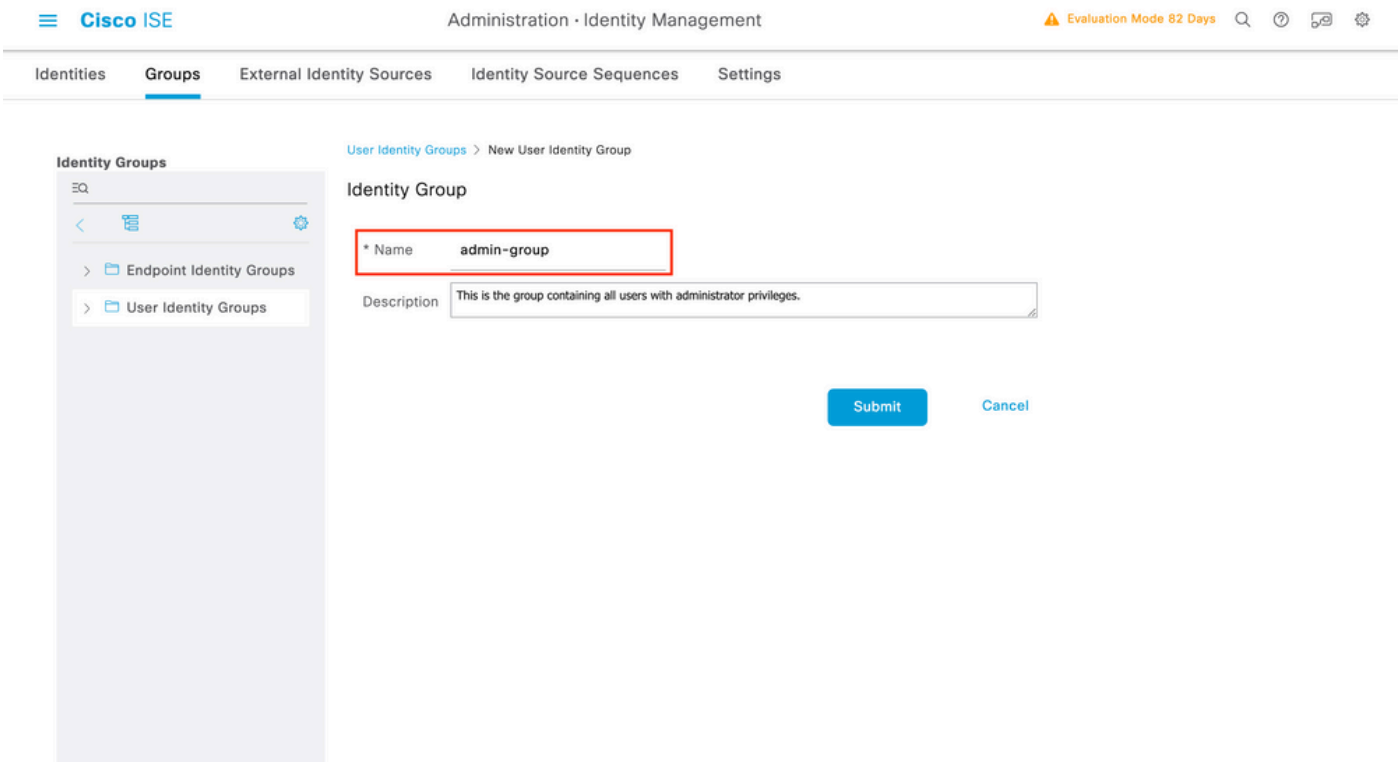
3단계. ISE에서 사용자 그룹을 생성합니다.

GUI에서 다음과 같이 표시되어야 합니다.

ISE 사용자 그룹은 의 User Identity Groups(사용자 ID 그룹) 탭에서Administration > Identity Management > Groups GUI Page 생성되며, 이는 화면 캡처에 표시됩니다.



새 사용자를 만들려면 추가 단추를 사용하여 새 사용자 ID 그룹 컨피그레이션 양식을 엽니다.

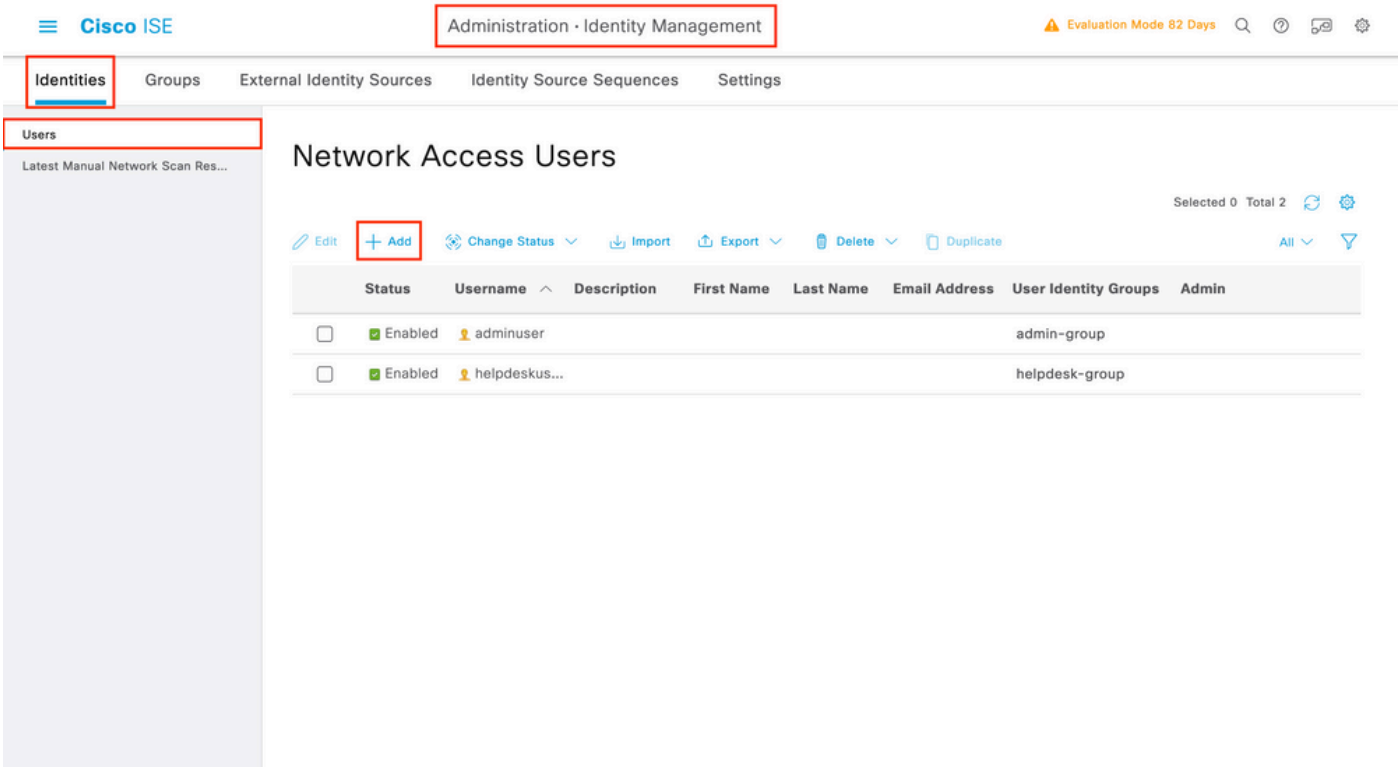


생성된 그룹의 이름을 제공합니다. 위에서 설명한 두 개의 사용자 그룹, 즉 및 을admin-group 생성합니다helpdesk-group.

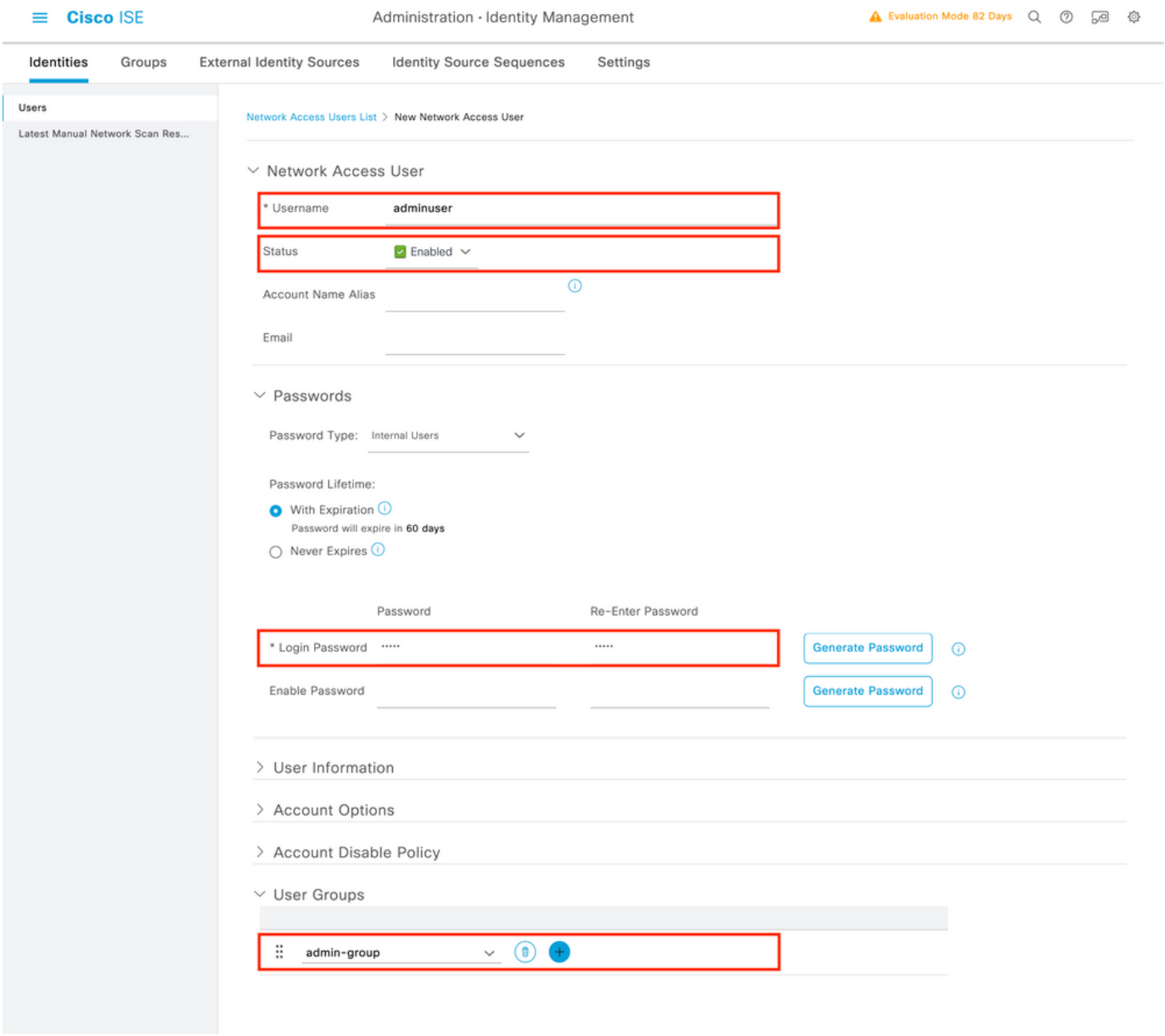
4단계. ISE에서 사용자를 생성합니다.

GUI에서 다음과 같이 표시되어야 합니다.

ISE 사용자는 의 Users(사용자) 탭Administration > Identity Management > Identities GUI Page에서 생성되며 화면 캡처에 표시됩니다.



새 사용자를 만들려면 추가 단추를 사용하여 새 네트워크 액세스 사용자 구성 양식을 엽니다.



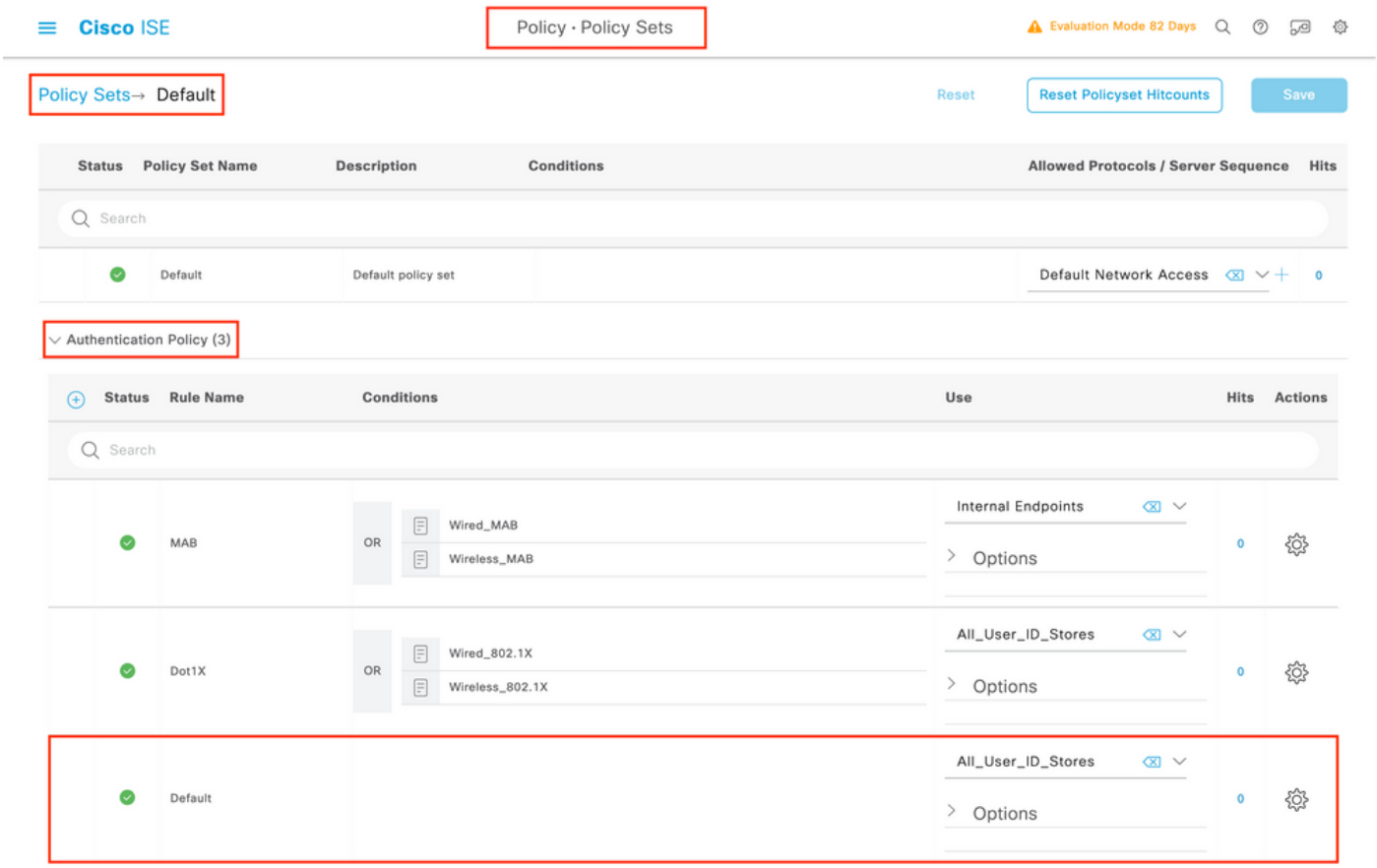
WLC에서 인증하는 데 사용되는 자격 증명, 즉 사용자 이름과 비밀번호를 사용자에게 제공합니다. 또한 사용자의 상태가 Enabled 인지 확인합니다. 마지막으로, 양식 끝에 있는 User Groups(사용자 그룹) 드롭다운 메뉴를 사용하여 4단계에서 생성된 관련 그룹에 사용자를 추가합니다.

위에서 설명한 두 사용자, 즉 및 를adminuser helpdeskuser 생성합니다.

5단계. 사용자 인증

GUI에서:

이 시나리오에서 이미 사전 구성된 ISE의 기본 정책 집합의 인증 정책은 기본 네트워크 액세스를 허용합니다. 이 정책 집합은 이 그림에Policy > Policy Sets 표시된 대로 ISE GUI 페이지에서 볼 수 있습니다. 따라서 변경할 필요가 없습니다.

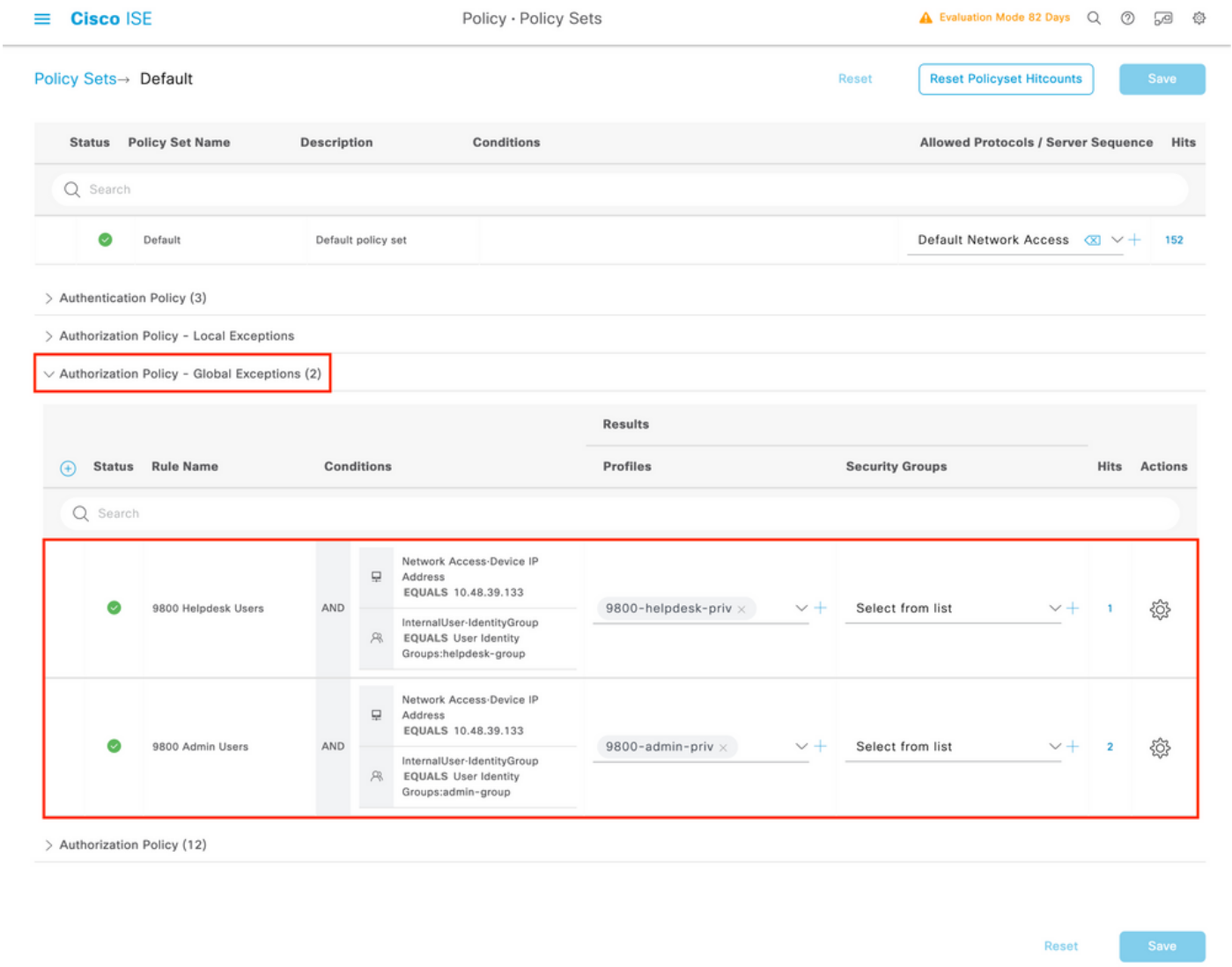


6단계. 사용자에게 권한을 부여합니다.

GUI에서:

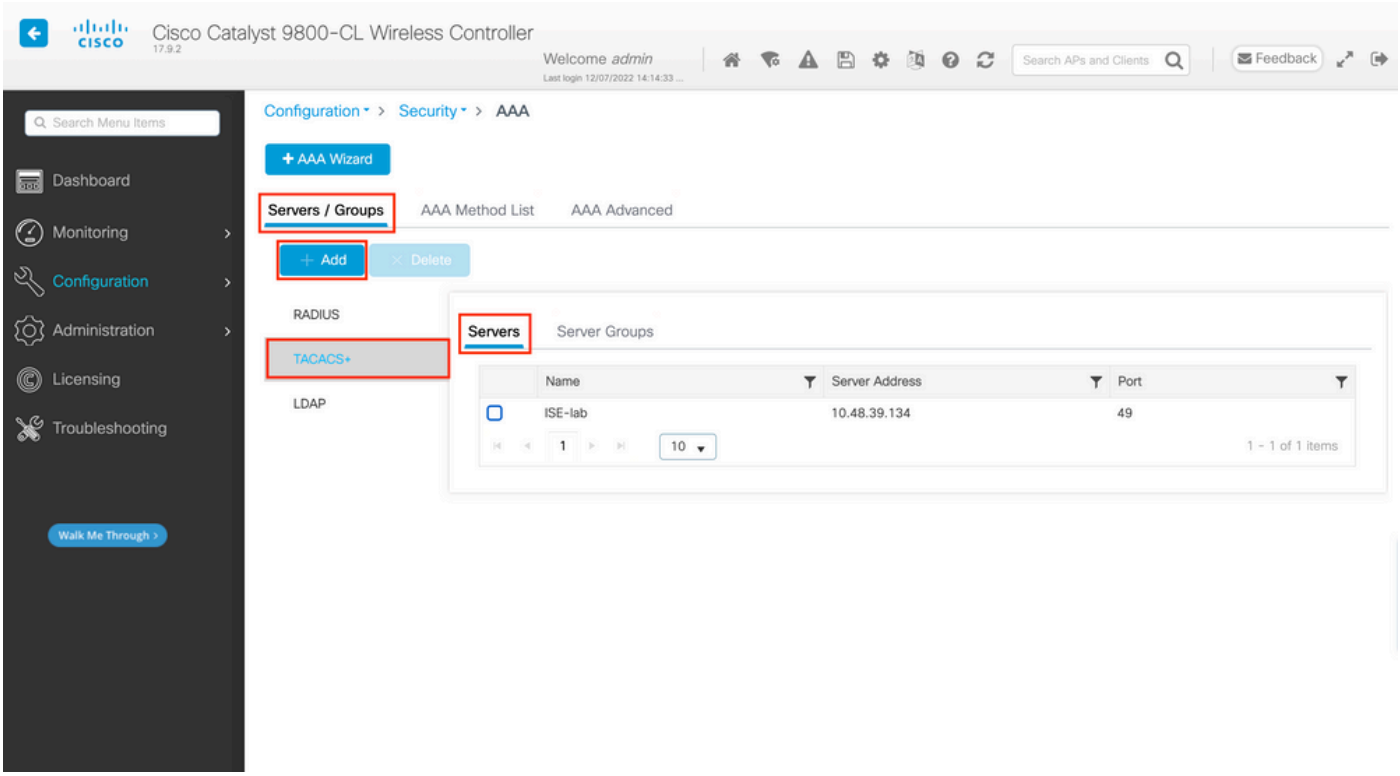
로그인 시도가 인증 정책을 통과하면 인증 정책을 승인해야 하며 ISE는 이전에 생성한 권한 부여 프로파일을 반환해야 합니다(권한 레벨과 함께 허용 수락).

이 예에서는 디바이스 IP 주소(WLC IP 주소)를 기준으로 로그인 시도가 필터링되고 사용자가 속한 그룹을 기준으로 부여할 권한 수준이 구별됩니다. 또 다른 유효한 방법은 이 예에서 각 그룹에 단일 사용자만 포함되므로 사용자 이름을 기준으로 사용자를 필터링하는 것입니다.

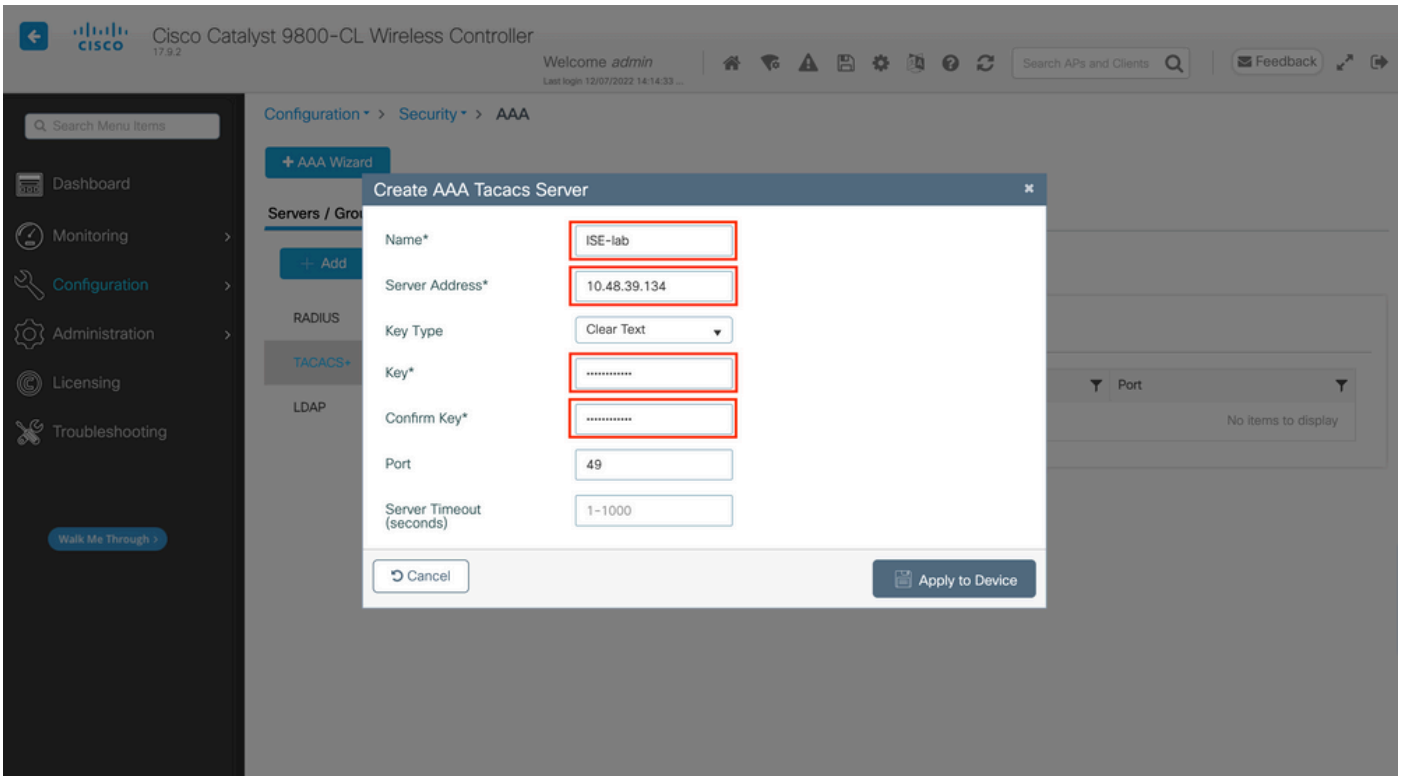


이 단계를 완료하면 및 사용자에 대해 구성된 자격 증명을adminuser helpdesk 사용하여 GUI 또는 텔넷/SSH를 통해 WLC에서 인증할 수 있습니다.

TACACS+ WLC 구성
1단계. TACACS+ 서버를 선언합니다.
GUI에서:
먼저 WLC에서 Tacacs+ 서버 ISE를 생성합니다. 이 작업은 이 이미지에 표시된 것처럼 GUI WLC 페이지Servers/Groups > TACACS+ > Servers의https://<WLC-IP>/webui/#/aaa 탭에서 수행할 수 있습니다Configuration > Security > AAA.



WLC에 TACACS 서버를 추가하려면 위의 이미지에서 빨간색으로 표시된 Add(추가) 버튼을 클릭합니다. 그러면 표시된 팝업 창이 열립니다.



팝업 창이 열리면 서버 이름(ISE 시스템 이름과 일치하지 않아도 됨), IP 주소, 공유 키, 사용된 포트 및 시간 제한을 제공합니다.

이 팝업 창에서 다음을 제공해야 합니다.

- 서버 이름(ISE 시스템 이름과 일치하지 않아도 됨)

- 서버 IP 주소
- WLC와 TACACS+ 서버 간의 공유 암호

인증 및 어카운팅에 사용되는 포트와 같은 다른 매개변수를 구성할 수 있지만, 이러한 매개변수는 필수 사항이 아니며 이 설명서의 기본값으로 남겨둡니다.

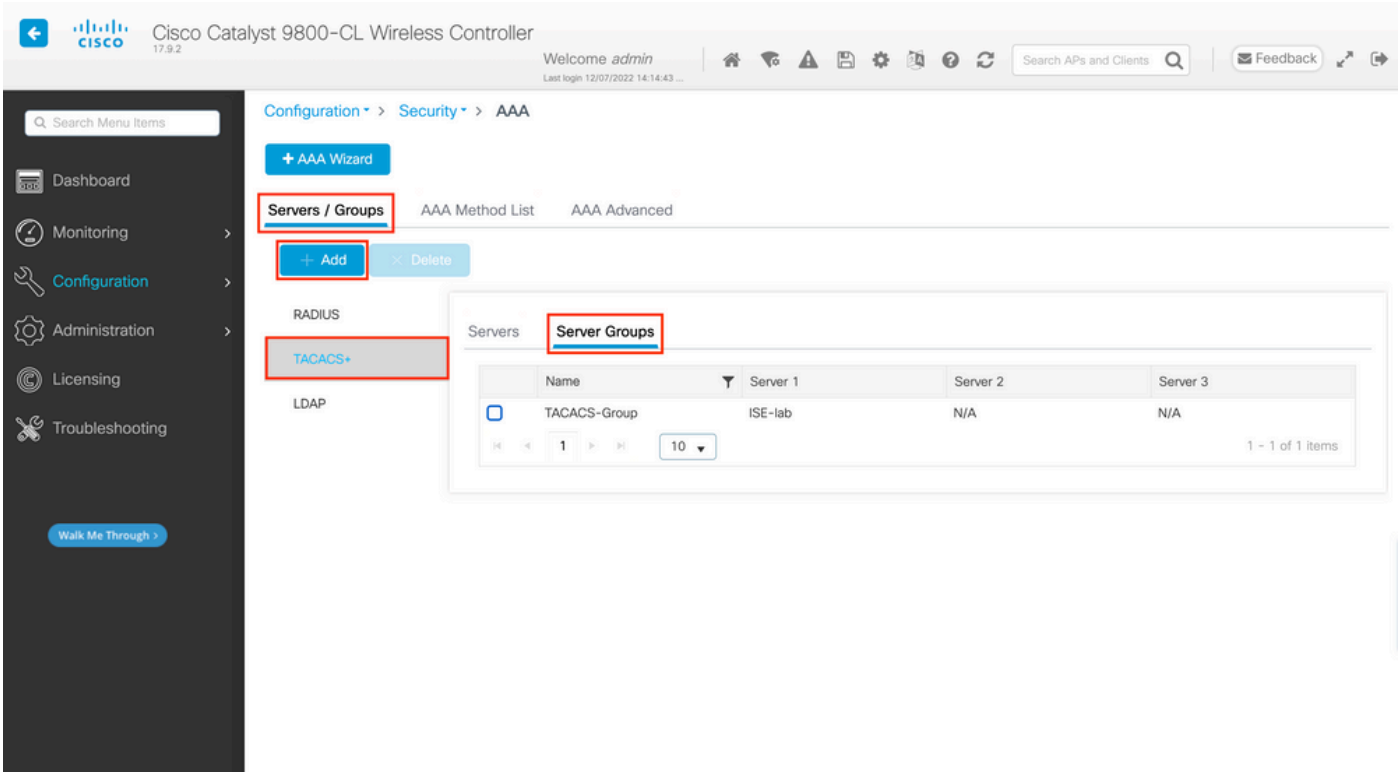
CLI에서:

```
<#root>

WLC-9800(config)#tacacs server

ISE-lab

 WLC-9800(config-server-tacacs)#address ipv4

10.48.39.134

 WLC-9800(config-server-tacacs)#key

Cisco123
```

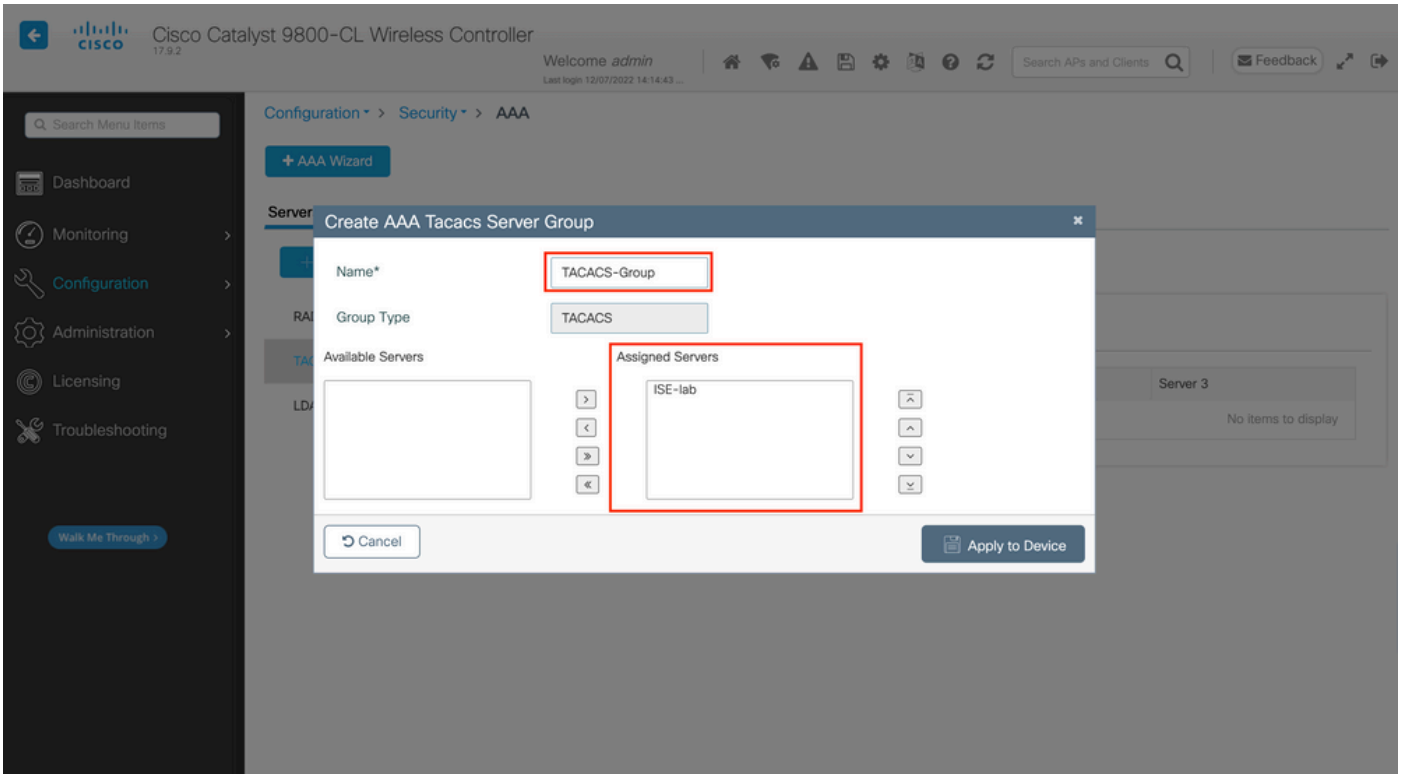
2단계. TACACS+ 서버를 서버 그룹에 매핑합니다.

GUI에서:

인증에 사용할 수 있는 여러 TACACS+ 서버가 있는 경우 이러한 모든 서버를 동일한 서버 그룹에 매핑하는 것이 좋습니다. 그런 다음 WLC는 서버 그룹의 서버 간에 로드 밸런싱을 수행합니다. TACACS+ 서버 그룹은 Servers/Groups > TACACS > Server Groups1단계에서 언급한 것과 동일한 GUI 페이지의 탭에서 구성되며, 이 GUI 페이지는 이미지에 표시됩니다.



서버 생성의 경우, 이미지에 표시된 이전 이미지의 Add(추가) 버튼을 클릭하면 팝업 창이 나타납니다.



팝업에서 그룹에 이름을 지정하고 Assigned Servers(할당된 서버) 목록으로 원하는 서버를 이동합니다.

CLI에서:

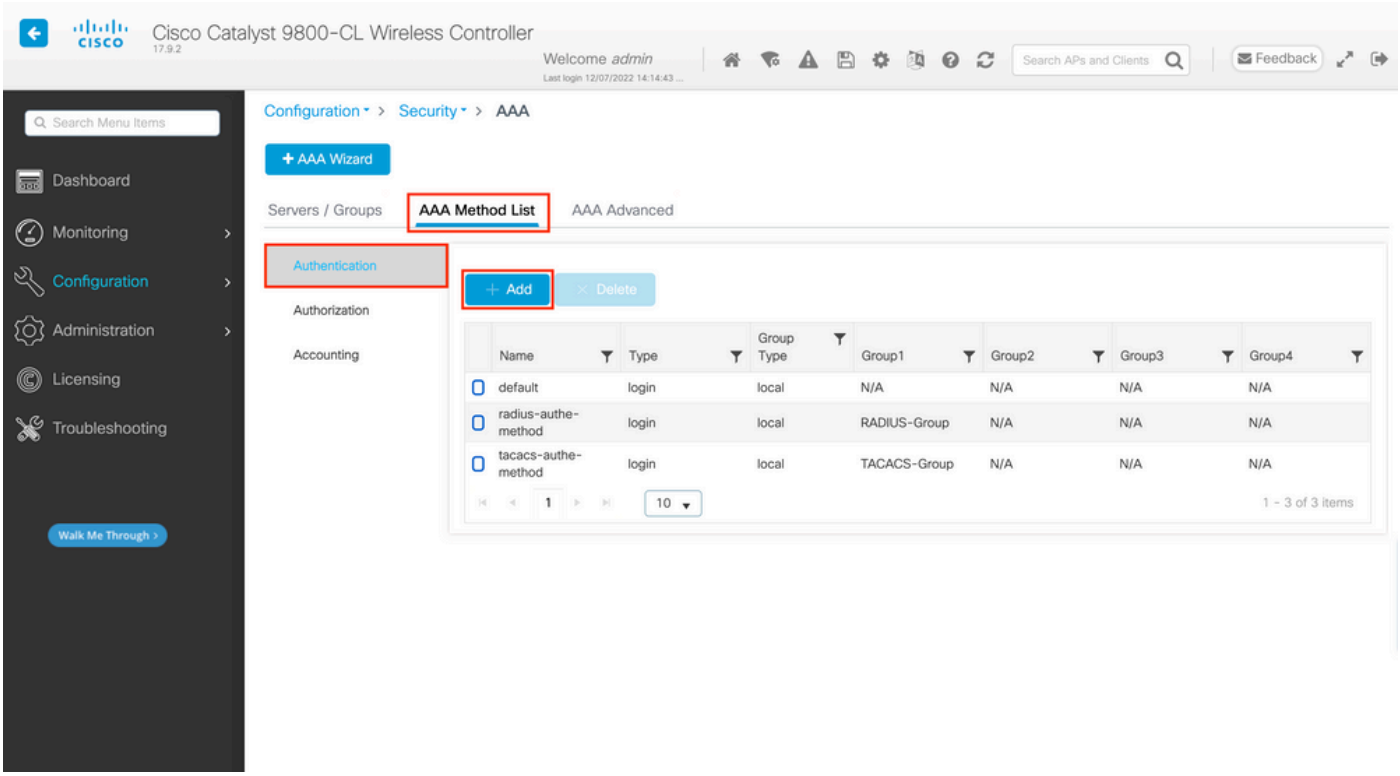
```
<#root>

WLC-9800(config)#aaa group server tacacs+
```

TACACS-Group

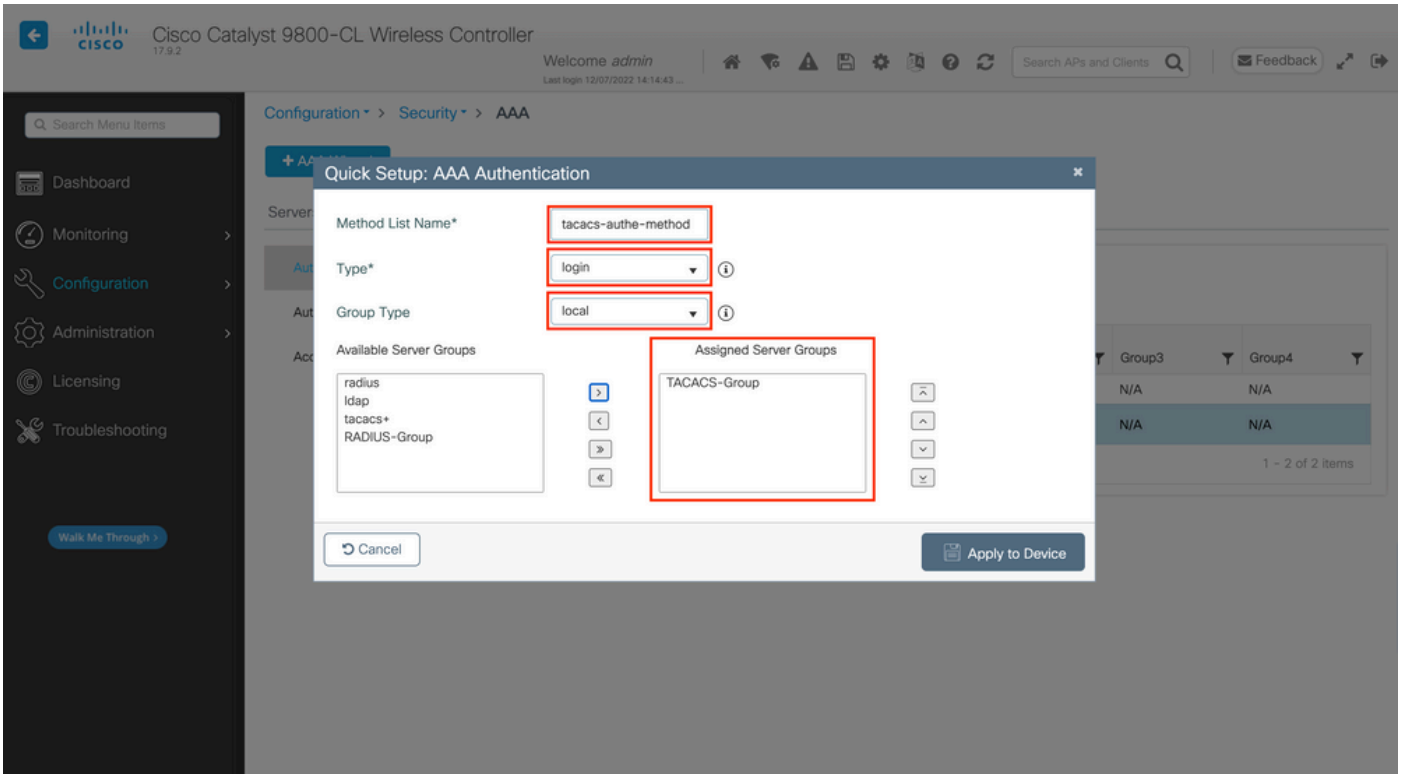
```
WLC-9800(config-sg-tacacs+)#server name
```

ISE-lab

3단계. TACACS+ 서버 그룹을 가리키는 방법으로 AAA 인증 로그를 생성합니다.
GUI에서:
여전히 GUI 페이지에서 https://<WLC-IP>/webui/#/aaa 탭으로 AAA Method List > Authentication 이동하여 이미지에 표시된 인증 방법을 생성합니다.



평소와 같이 Add(추가) 버튼을 사용하여 인증 방법을 생성하면 이 이미지에 표시된 것과 유사한 컨피그레이션 팝업 창이 나타납니다.



이 팝업 창에서 메서드의 이름을 제공하고 Type aslogin를 선택한 다음 이전 단계에서 생성한 그룹 서버를 Assigned Server Groups 목록에 추가합니다. Group Type(그룹 유형) 필드에서는 여러 컨피그레이션이 가능합니다.

- Group Type(그룹 유형)을 local(로컬)로 선택하면 WLC는 먼저 사용자 자격 증명이 로컬에 존재하는지 확인한 다음 서버 그룹으로 돌아갑니다.
- Group Type(그룹 유형)을 그룹으로 선택하고 Fall back to local(로컬로 폴백) 옵션을 선택하지 않으면 WLC는 서버 그룹에 대한 사용자 자격 증명만 확인합니다.
- Group Type as a group(그룹 유형)을 선택하고 Fallback to local(로컬로 대체) 옵션을 선택하면 WLC는 서버 그룹에 대해 사용자 자격 증명을 확인하고 서버가 응답하지 않는 경우에만 로컬 데이터베이스를 쿼리합니다. 서버에서 거부를 전송하면 로컬 데이터베이스에 존재할 수 있더라도 사용자를 인증해야 합니다.

CLI에서:

사용자 자격 증명을 로컬에서 먼저 찾을 수 없는 경우에만 서버 그룹과 함께 확인하도록 하려면 다음을 사용합니다.

```
<#root>

WLC-9800(config)#aaa authentication login
```

tacacs-authe-method

local group

TACACS-Group

서버 그룹에서만 사용자 자격 증명을 검사하려면 다음을 사용합니다.

<#root>

WLC-9800(config)#aaa authentication login

tacacs-authe-method

group

TACACS-Group

서버 그룹에서 사용자 자격 증명을 확인하려는 경우 그리고 이 마지막 항목이 로컬 항목으로 응답하지 않을 경우 다음을 사용합니다.

<#root>

WLC-9800(config)#aaa authentication login

tacacs-authe-method

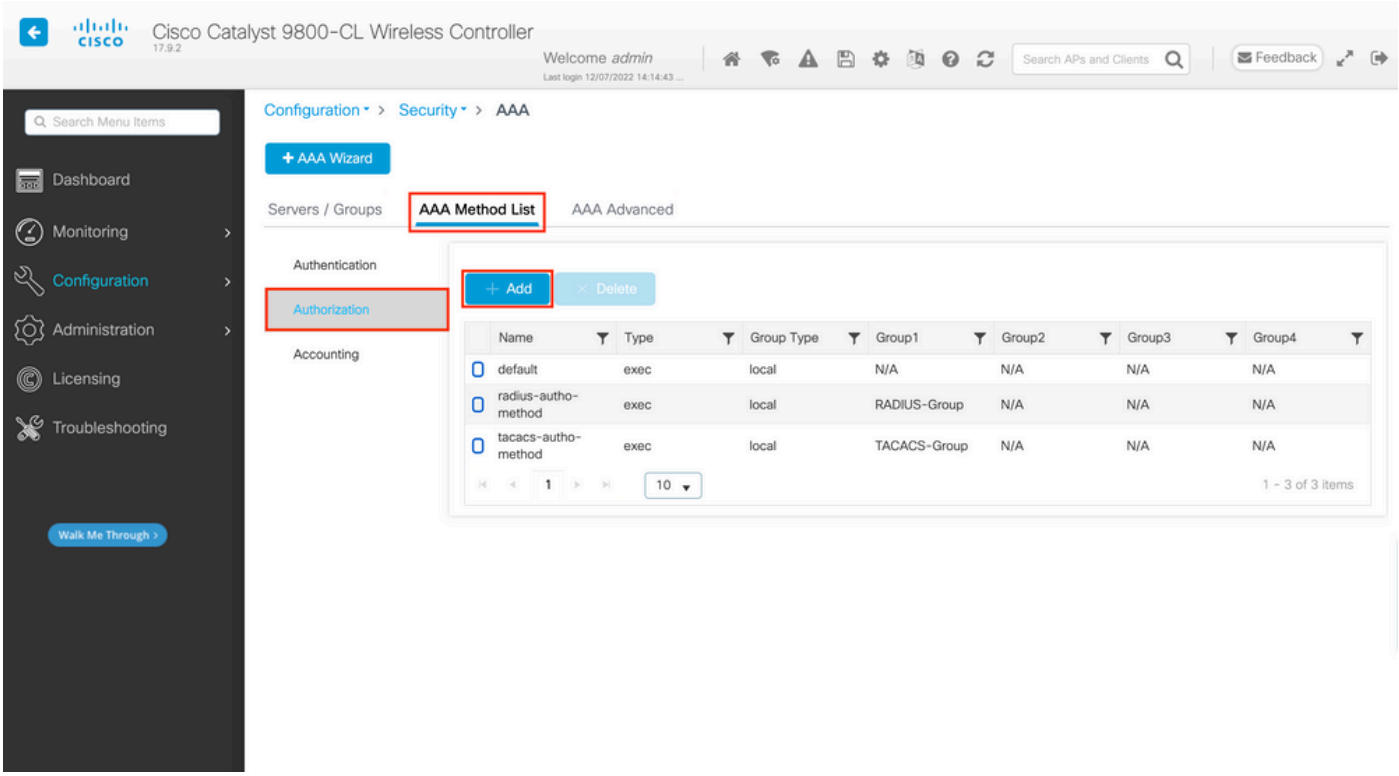
group

TACACS-Group

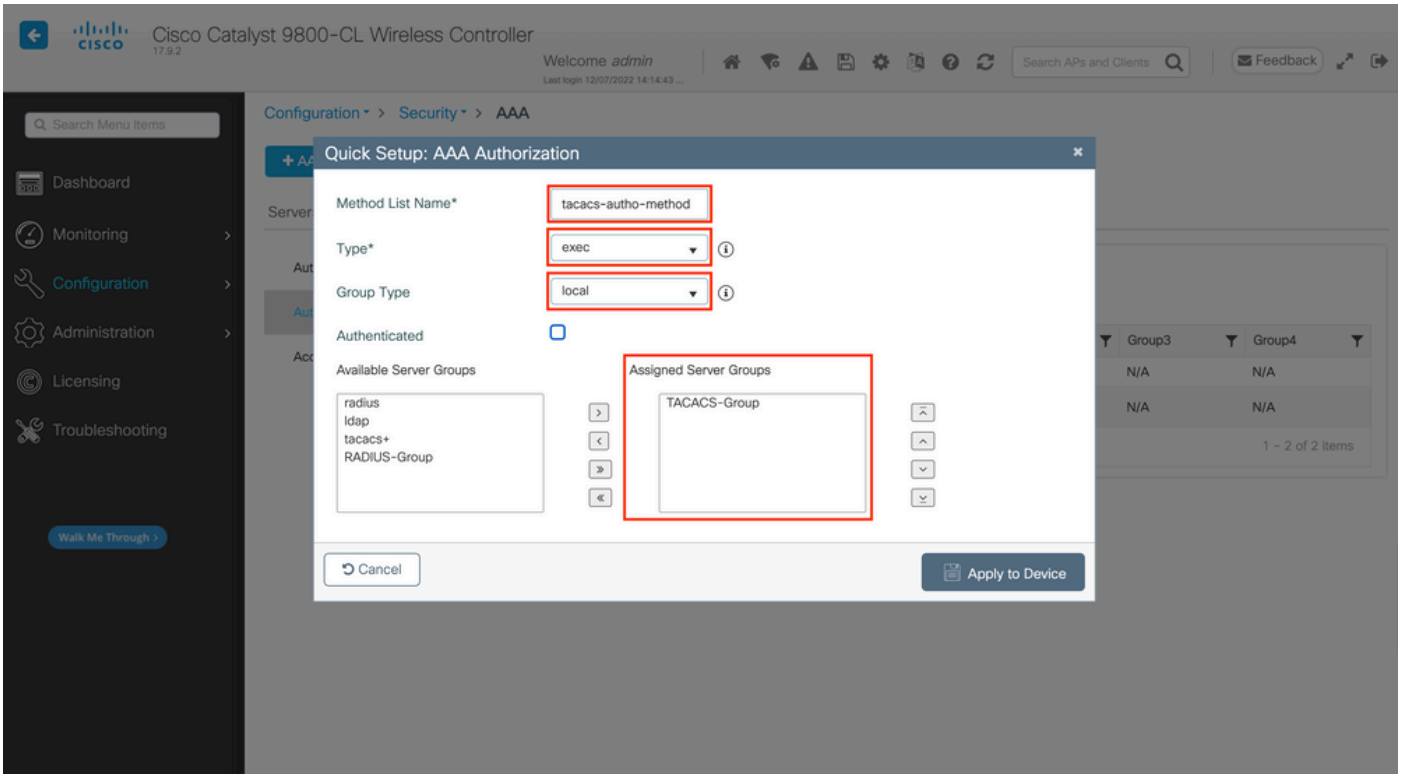
local

이 예제 설정에서는 로컬에서만 생성된 일부 사용자와 ISE 서버에서만 생성된 일부 사용자가 있으므로 첫 번째 옵션을 사용합니다.

4단계. TACACS+ 서버 그룹을 가리키는 AAA 권한 부여 exec 방법을 생성합니다.
GUI에서:
사용자에게 액세스 권한을 부여하려면 권한이 있어야 합니다. 여전히 GUI 페이지에서 Configuration > Security > AAA 탭으로 AAA Method List > Authorization 이동하고 이미지에 표시된 대로 권한 부여 방법을 생성합니다.



Add(추가) 버튼을 사용하여 새 방법을 추가하면 표시된 것과 유사한 권한 부여 방법 컨피그레이션 팝업이 나타납니다.



이 컨피그레이션 팝업에서 권한 부여 방법의 이름을 제공하고 Type asexec를 선택하고 이전 단계에서 인증 방법에 사용된 것과 동일한 Group Type 순서를 사용합니다.

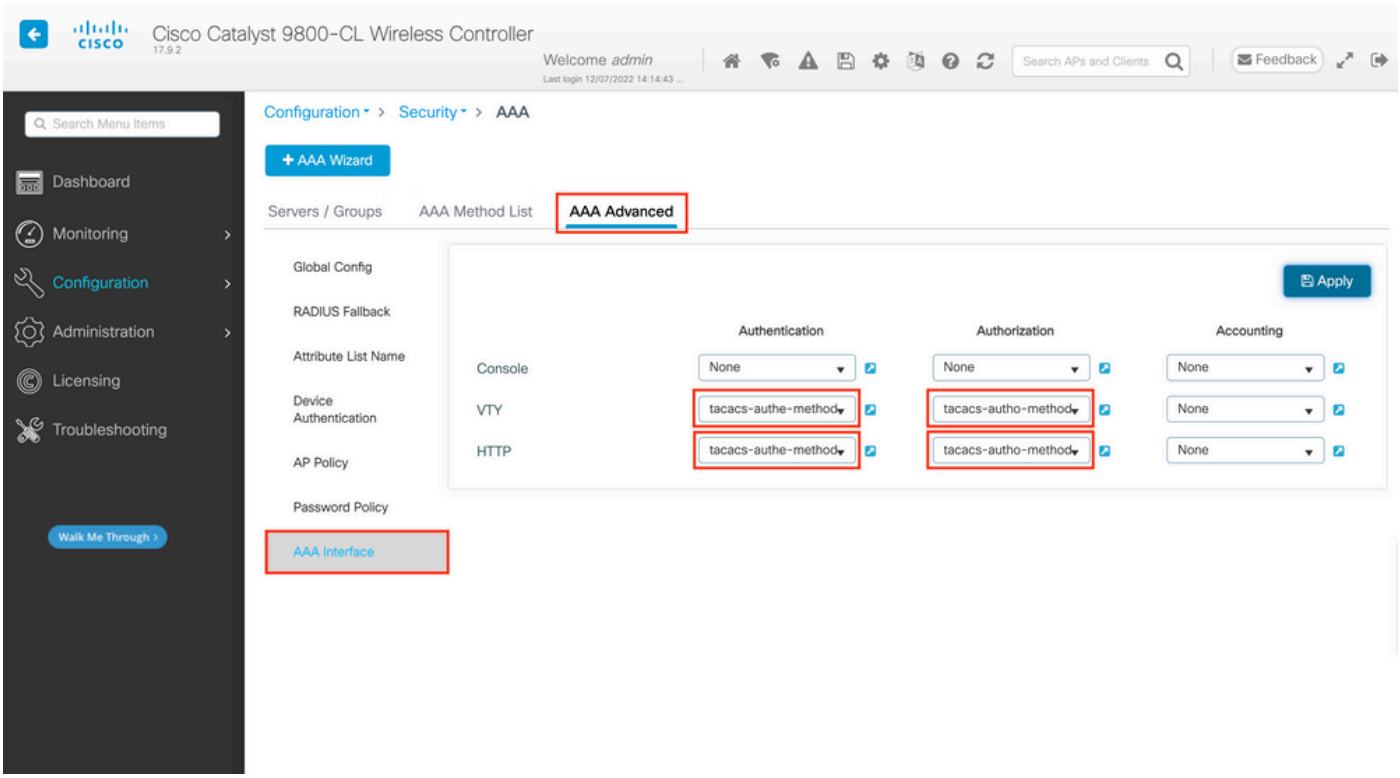
CLI에서:

```
<#root>

WLC-9800(config)#aaa authorization exec

tacacs-autho-method

 local group

TACACS-Group
```

5단계. HTTP 컨피그레이션 및 텔넷/SSH에 사용되는 VTY 라인에 방법을 할당합니다.

GUI에서:

AAA Advanced > AAA Interface 생성된 인증 및 권한 부여 방법을 HTTP 및/또는 텔넷/SSH 사용자 연결에 사용할 수 있습니다. 이 방법은 그림에 표시된 것처럼 액세스 가능한https://<WLC-IP>/webui/#/aaa GUI WLC 페이지에서 여전히 탭에서 구성할 수 있습니다.



CLI에서:

GUI 인증의 경우

<#root>

```
WLC-9800(config)#ip http authentication aaa login-authentication
```

tacacs-authe-method

```
WLC-9800(config)#ip http authentication aaa exec-authorization
```

tacacs-autho-method

텔넷/SSH 인증:

<#root>

```
WLC-9800(config)#line vty 0 15
WLC-9800(config-line)#login authentication
```

tacacs-authe-method

```
WLC-9800(config-line)#authorization exec
```

tacacs-autho-method

HTTP 컨피그레이션을 변경할 경우 HTTP 및 HTTPS 서비스를 다시 시작하는 것이 가장 좋습니다. 이 명령은 다음 명령으로 수행할 수 있습니다.

```
WLC-9800(config)#no ip http server
WLC-9800(config)#no ip http secure-server
WLC-9800(config)#ip http server
WLC-9800(config)#ip http secure-server
```

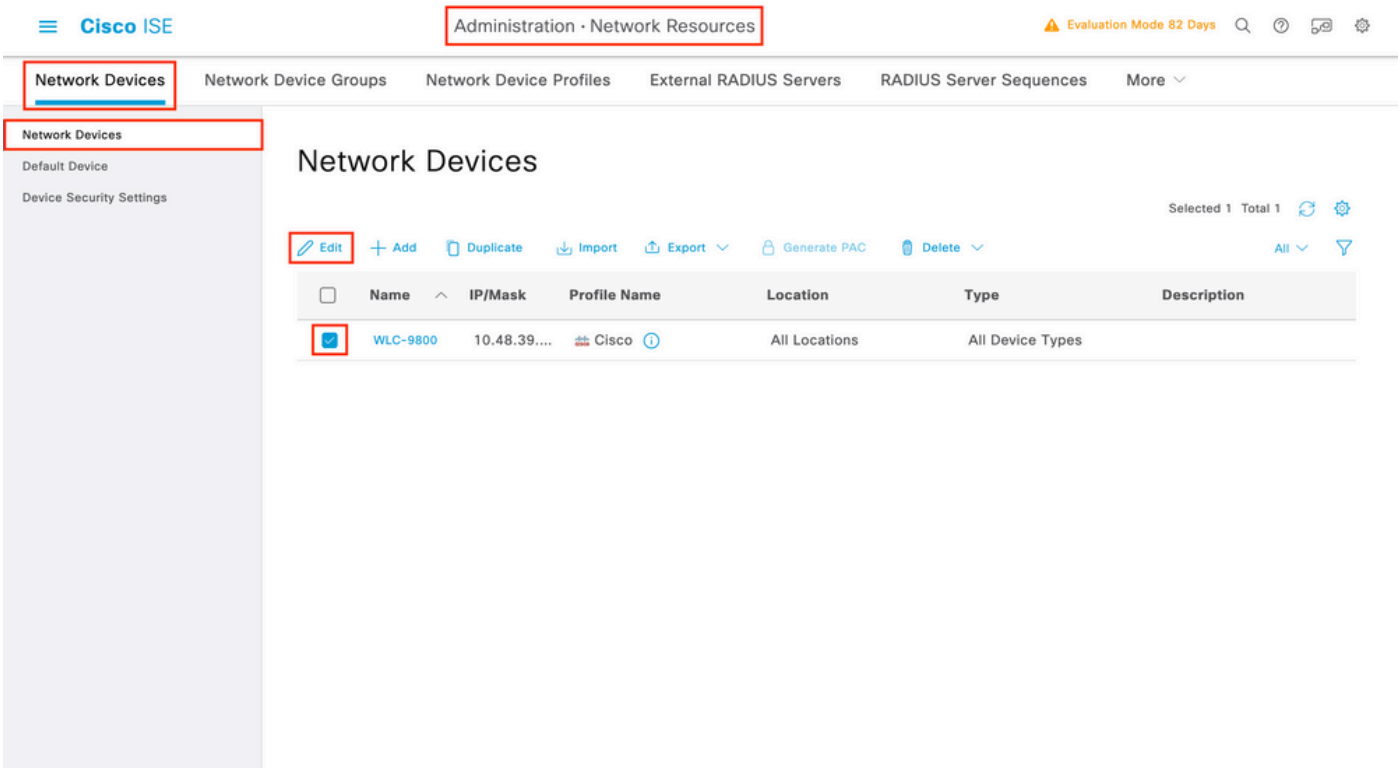
TACACS+ ISE 컨피그레이션

1단계. WLC를 TACACS+용 네트워크 디바이스로 구성합니다.

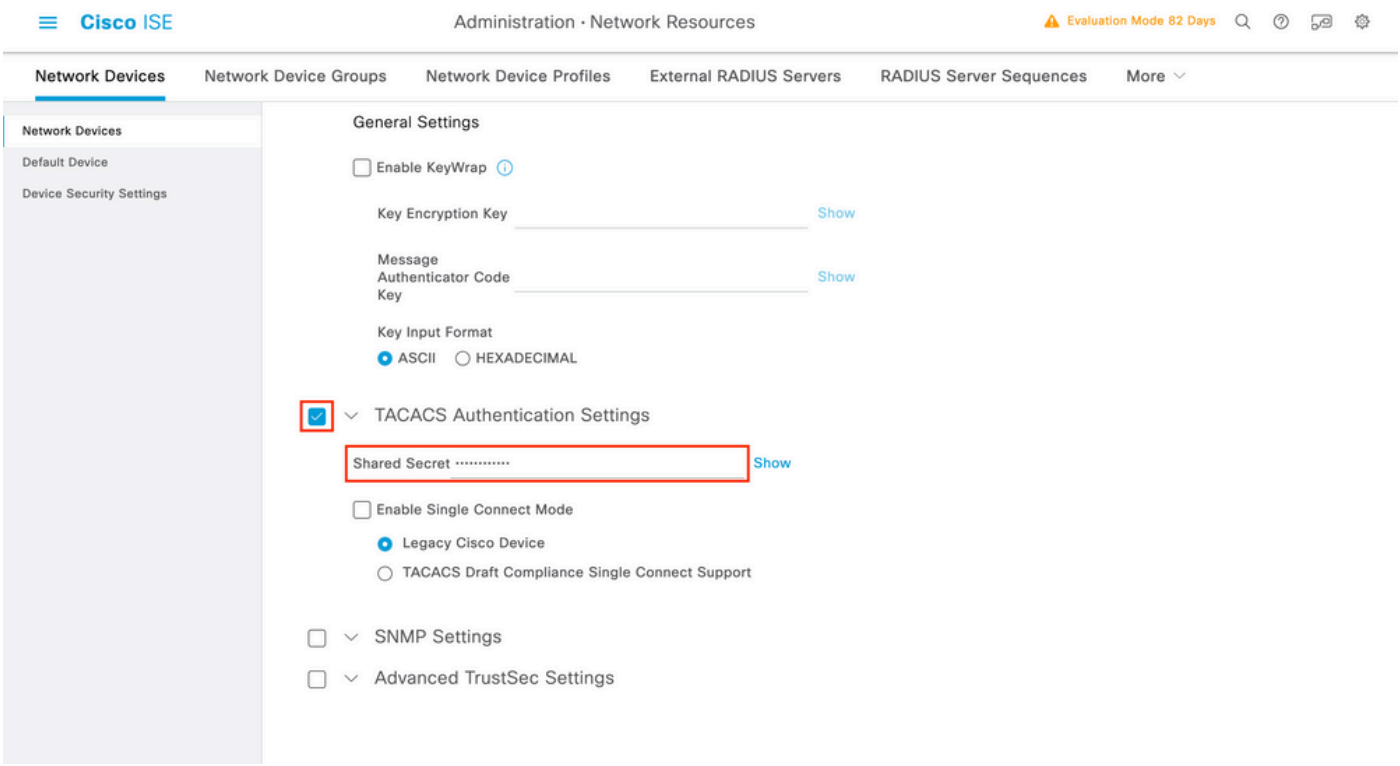
GUI에서:

이전 섹션에서 사용된 WLC를 ISE의 RADIUS용 네트워크 디바이스로 선언하려면 이 이미지에 표시된 것처럼 Network devices(네트

워크 디바이스) 탭으로 이동하여Administration > Network Resources > Network Devices 엽니다.

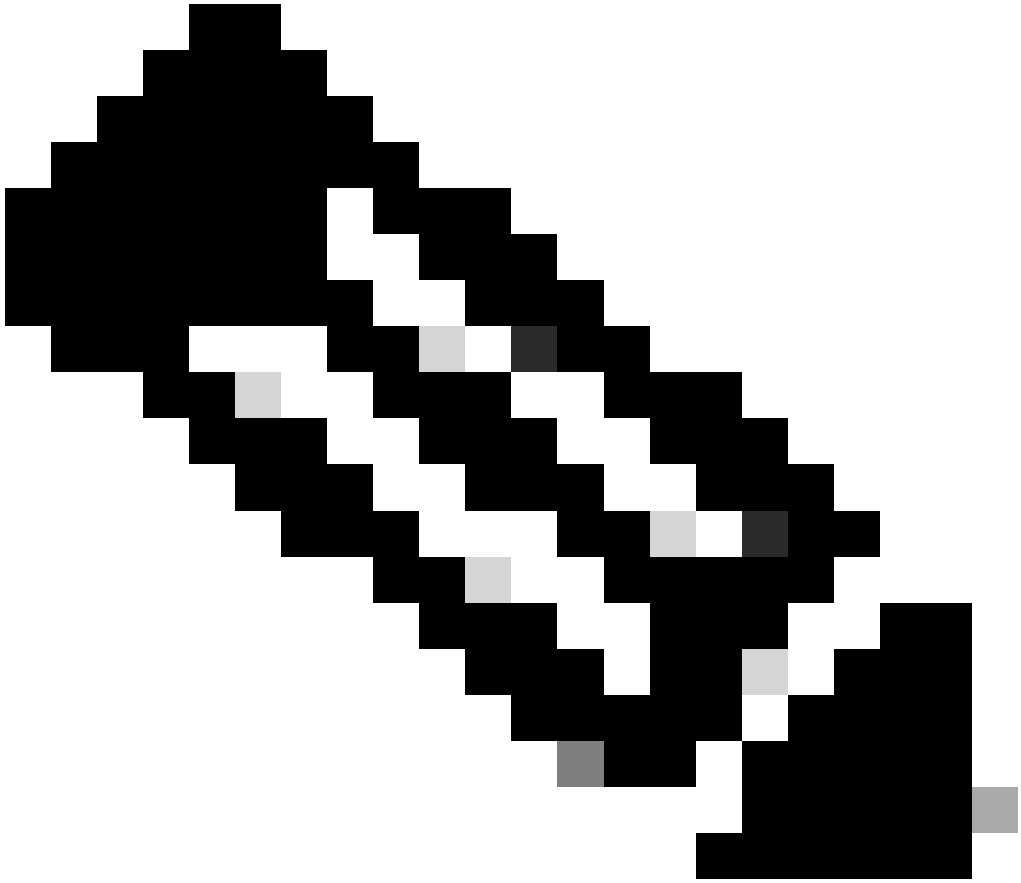


이 예에서는 RADIUS 인증을 위해 WLC가 이미 추가되었습니다(RADIUS ISE 구성 섹션의 1단계 참조). 따라서 네트워크 디바이스 목록에서 WLC를 선택하고 Edit(수정) 버튼을 클릭하면 TACACS 인증을 구성하기 위해 컨피그레이션을 수정하기만 하면 됩니다. 그러면 이 이미지에 표시된 것처럼 네트워크 디바이스 컨피그레이션 양식이 열립니다.



새 창이 열리면 아래로 스크롤하여 TACACS Authentication Settings(TACACS 인증 설정) 섹션으로 이동한 다음, 이 설정을 활성화하고 1단계에서 입력한 공유 암호를 추가합니다. Configure TACACS+ WLC(TACACS+ WLC 구성) 섹션의 일부입니다.

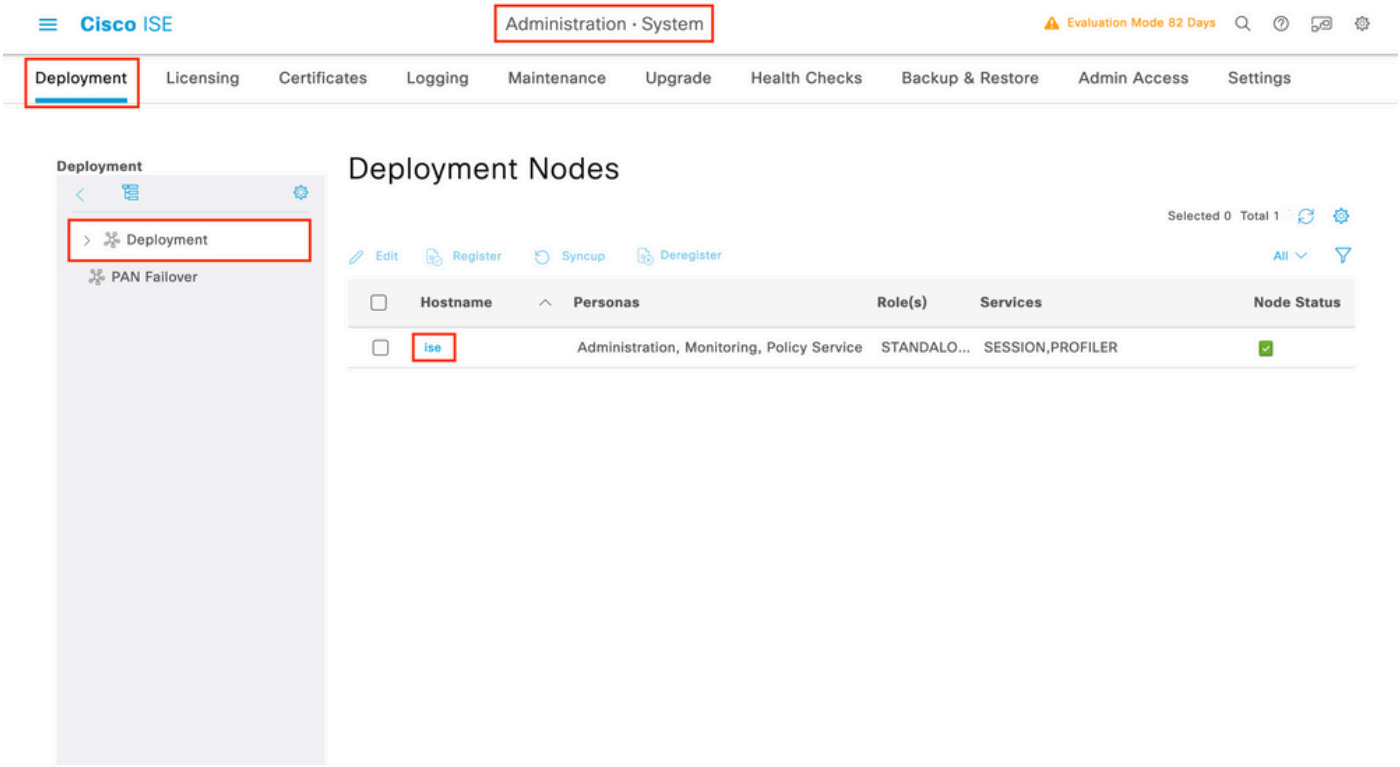
2단계. 노드에 대한 장치 관리 기능을 활성화 합니다.



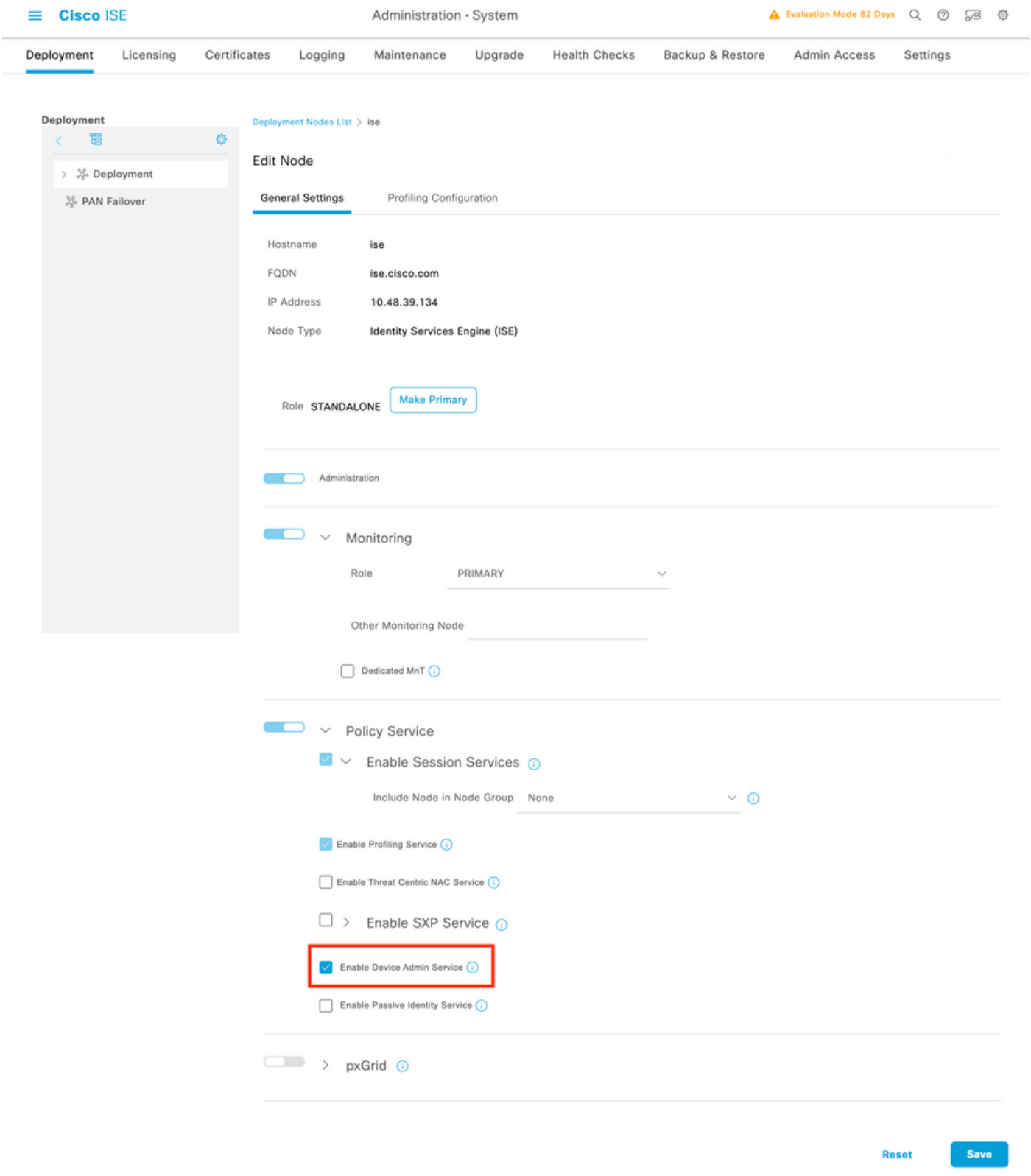
참고: ISE를 TACACS+ 서버로 사용하려면 Device Administration 라이센스 패키지와 Base 또는 Mobility 라이센스가 있어야 합니다.

GUI에서:

디바이스 관리 라이센스가 설치되면 ISE를 TACACS+ 서버로 사용하려면 노드에 대해 디바이스 관리 기능을 활성화해야 합니다. 이를 위해, 사용 된 ISE 구축 노드의 컨피그레이션을 수정 합니다. 이는 아래Administrator > Deployment에서 볼 수 있으며, 해당 이름을 클릭 하거나 버튼의 도움을 받아 Edit 그렇게 합니다.



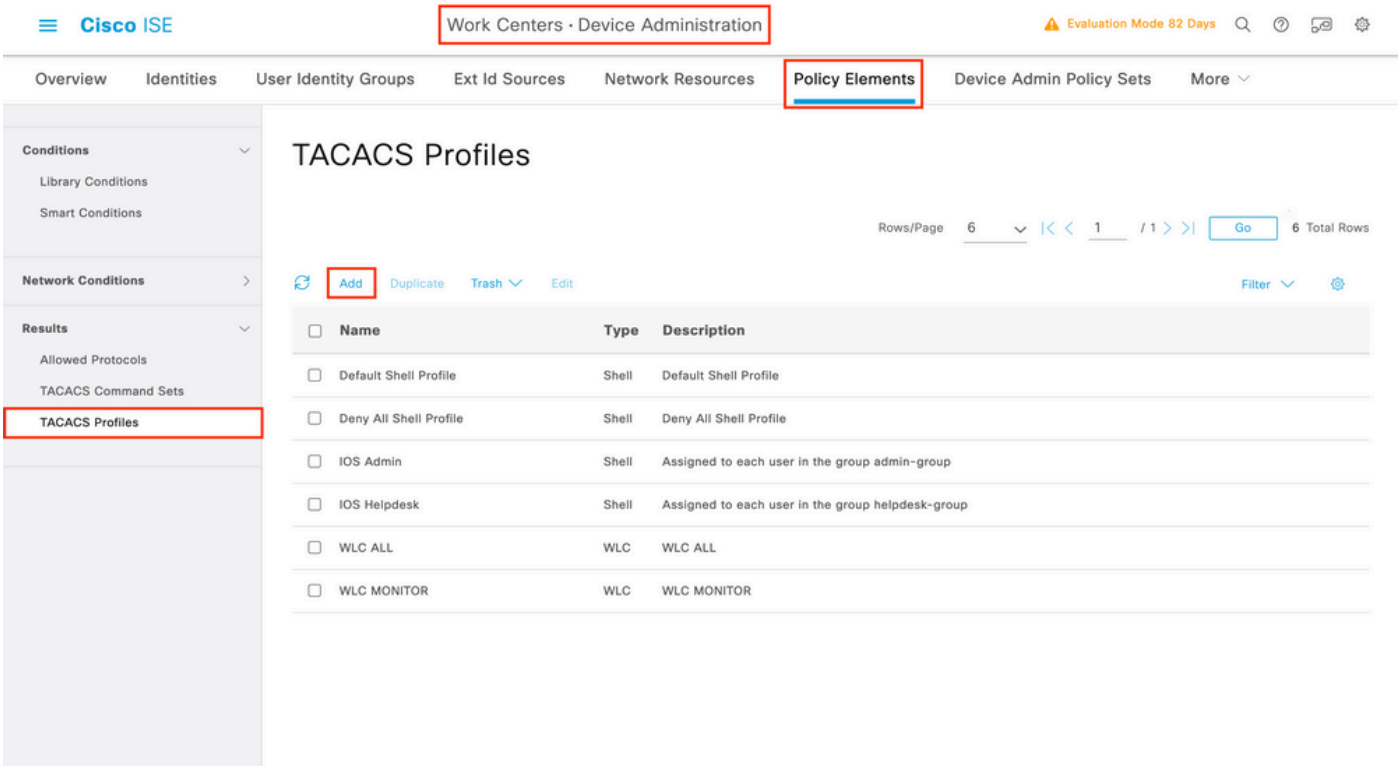
노드 컨피그레이션 창이 열리면 이 이미지에 표시된 대로 Policy Service(정책 서비스) 섹션 아래에서 Enable Device Admin Service(디바이스 관리 서비스 활성화) 옵션을 선택합니다.



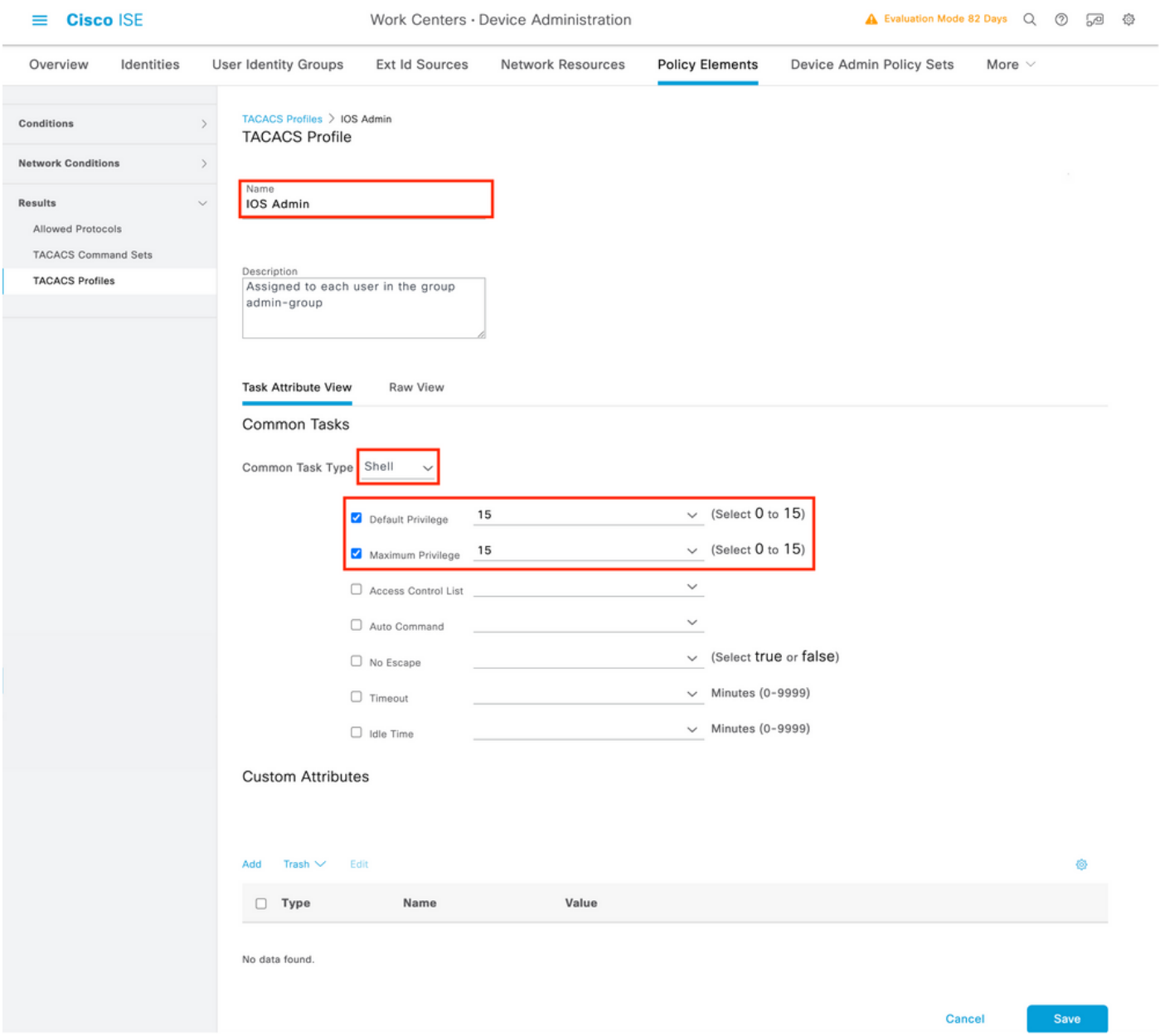
3단계. TACACS 프로파일을 생성하여 권한을 반환합니다.

GUI에서:

관리자 액세스 권한을 가지려면 는 adminuser EXEC 프롬프트 셸에 액세스할 수 있는 권한 레벨 15를 가져야 합니다. 반면 는 helpdeskuser exec 프롬프트 셸 액세스가 필요하지 않으므로 15보다 낮은 권한 레벨로 할당될 수 있습니다. 사용자에게 적절한 권한 수준을 할당하려면 권한 부여 프로파일을 사용할 수 있습니다. 다음 그림과 같이 ISE GUI 페이지Work Centers > Device Administration > Policy Elements 아래의 탭Results > TACACS Profiles에서 구성할 수 있습니다.



새 TACACS 프로파일을 구성하려면 Add 버튼을 사용합니다. 그러면 그림에 표시된 것과 유사한 새 프로파일 컨피그레이션 양식이 열립니다. 이 양식은 특히 셸 권한 레벨 15를 사용하여에adminuser 할당된 프로파일을 구성하기 위해 이와 같아야 합니다.



프로파일에 대한 작업을 helpdesk 반복합니다. 마지막 단계에서는 Default Privilege(기본 권한) 및 Maximum Privilege(최대 권한)가 모두 1로 설정됩니다.

4단계. ISE에서 사용자 그룹을 생성합니다.

이는 이 문서의 RADIUS ISE 구성 섹션의 3단계에서 설명한 것과 동일합니다.

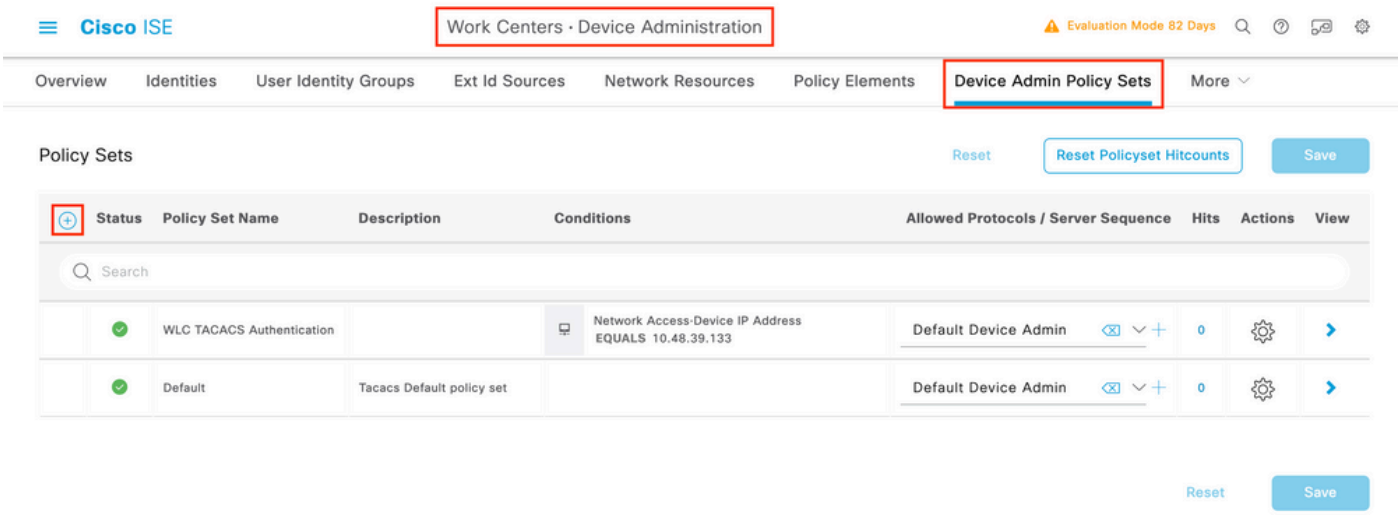
5단계. ISE에서 사용자를 생성합니다.

이 내용은 이 문서의 RADIUS ISE 구성 섹션 4단계의 내용과 동일합니다.

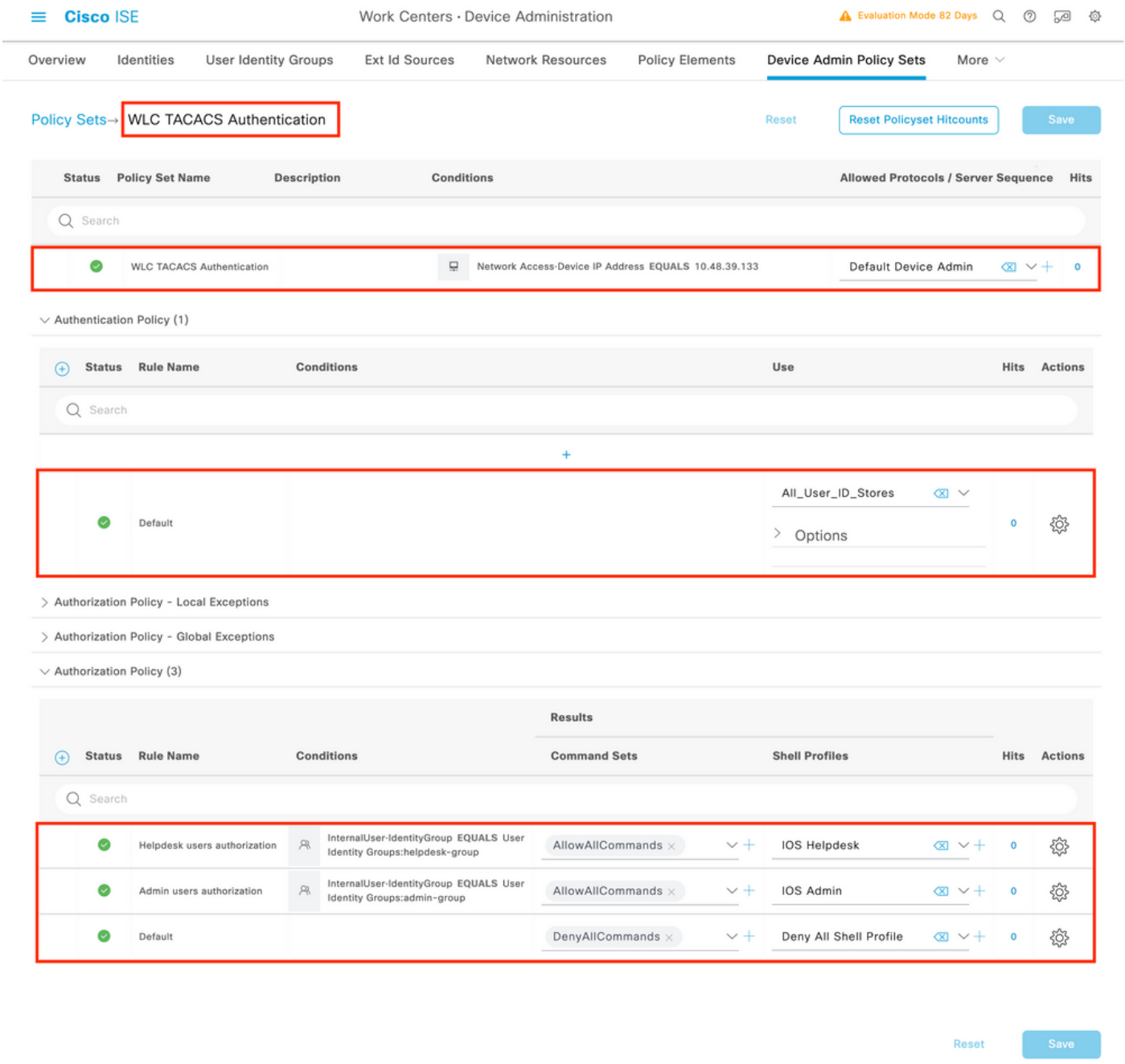
6단계. 디바이스 관리 정책 세트를 생성합니다.

GUI에서:

RADIUS 액세스의 경우, 사용자가 생성되면 적절한 액세스 권한을 부여하기 위해 ISE에서 해당 인증 및 권한 부여 정책을 정의해야 합니다. TACACS 인증은 디바이스 관리 정책 세트를 그 끝에 사용하며, 이는 표시된 대로 에서 구성할 수 Work Centers > Device Administration > Device Admin Policy Sets GUI Page 있습니다.



디바이스 관리 정책 세트를 생성하려면 이전 이미지에서 빨간색으로 프레임된 추가 버튼을 사용합니다. 그러면 정책 세트 목록에 항목이 추가됩니다. 새로 생성된 집합의 이름, 이를 적용해야 하는 조건 및 허용되는 프로토콜/서버 시퀀스(여기에서는 충분함)를 Default Device Admin 제공합니다. 이 Save 단추를 사용하여 정책 집합 추가를 완료하고 오른쪽에 있는 화살표를 사용하여 구성 페이지에 액세스합니다(그림에 나와 있는 것처럼).



이 예에서 특정 정책 집합 'WLC TACACS 인증'은 IP 주소가 C9800 WLC IP 주소 예와 동일한 요청을 필터링합니다.

인증 정책으로서 Default Rule(기본 규칙)은 사용상의 요구를 충족하므로 남겨둔 것입니다. 두 가지 권한 부여 규칙이 설정되었습니다
.

- 첫 번째 것은 사용자가 정의된 그룹에 속할 때 트리거됩니다admin-group. 모든 명령을 허용하고(기본 Permit_all 규칙을 통해) 권한 15를 할당합니다(정의된 TACACS 프로파일을 통해IOS_Admin).
- 두 번째 것은 사용자가 정의된 그룹에 속할 때 트리거됩니다helpdesk-group. 모든 명령을 허용하며(기본 규칙을 통해) Permit_all 권한 1(정의된 TACACS 프로필을 통해IOS_Helpdesk)을 할당합니다.

이 단계를 완료하면 adminuser helpdesk 및 사용자에 대해 구성된 자격 증명을 사용하여 GUI 또는 텔넷/SSH를 통해 WLC에서 인증할

수 있습니다.

문제 해결

RADIUS 서버에서 서비스 유형 RADIUS 특성을 전송해야 하는 경우 WLC에 추가할 수 있습니다.

```
radius-server attribute 6 on-for-login-auth
```

WLC CLI를 통해 WLC GUI 또는 CLI RADIUS/TACACS+ 액세스 문제 해결

WLC GUI 또는 CLI에 대한 TACACS+ 액세스의 문제를 해결하려면 터미널 모니터 1과 함께 명령을debug tacacs 실행하고 로그인이 시도될 때 라이브 출력을 확인합니다.

예를 들어, 성공적인 로그인과 사용자의 로그아웃이 이 출력을adminuser 생성합니다.

```
<#root>

WLC-9800#

terminal monitor

WLC-9800#

debug tacacs

TACACS access control debugging is on
WLC-9800#
Dec 8 11:38:34.684: TPLUS: Queuing AAA Authentication request 15465 for processing
Dec 8 11:38:34.684: TPLUS(00003C69) login timer started 1020 sec timeout Dec 8 11:38:34.684: TPLUS: pro
```

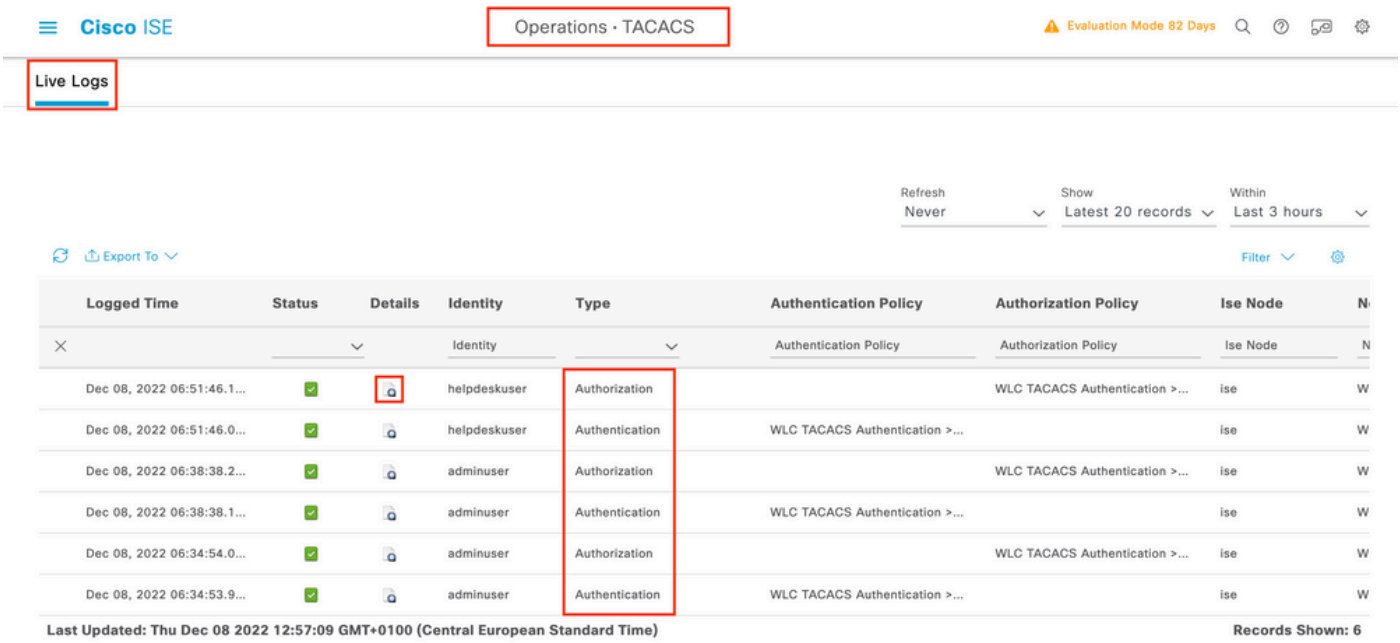
이러한 로그에서 TACACS+ 서버가 올바른 권한(즉AV priv-lvl=15)을 반환함을 확인할 수 있습니다.

RADIUS 인증을 수행할 때 RADIUS 트래픽과 관련된 유사한 디버그 출력이 표시됩니다.

명령debug aaa authentication 및 debug aaa authorization 대신 사용자가 로그인을 시도할 때 WLC에서 선택한 방법 목록을 표시합니다.

ISE GUI를 통해 WLC GUI 또는 CLI TACACS+ 액세스 문제 해결

페이지Operations > TACACS > Live Logs에서 최근 24시간까지 TACACS+로 수행한 모든 사용자 인증을 볼 수 있습니다. TACACS+ 권한 부여 또는 인증의 세부사항을 확장하려면 이 이벤트와 관련된 Details(세부사항) 버튼을 사용합니다.



를 확장하면 의 성공적인 인증 시도는 다음과helpdeskuser 같습니다.

Cisco ISE

Overview

Request Type	Authentication
Status	Pass
Session Key	ise/459637517/243
Message Text	Passed-Authentication: Authentication succeeded
Username	helpdeskuser
Authentication Policy	WLC TACACS Authentication >> Default
Selected Authorization Profile	IOS Helpdesk

Authentication Details

Generated Time	2022-12-08 06:51:46.077000 -05:00
Logged Time	2022-12-08 06:51:46.077
Epoch Time (sec)	1670500306
ISE Node	ise
Message Text	Passed-Authentication: Authentication succeeded
Failure Reason	
Resolution	
Root Cause	
Username	helpdeskuser
Network Device Name	WLC-9800
Network Device IP	10.48.39.133
Network Device Groups	IPSEC#Is IPSEC Device#No,Location#All Locations,Device Type#All Device Types
Device Type	Device Type#All Device Types
Location	Location#All Locations
Device Port	tty5
Remote Address	10.61.80.151

Steps

13013	Received TACACS+ Authentication START Request
15049	Evaluating Policy Group
15008	Evaluating Service Selection Policy
15048	Queried PIP - Network Access.Device IP Address
15041	Evaluating Identity Policy
22072	Selected identity source sequence - All_User_ID_Stores
15013	Selected Identity Source - Internal Users
24210	Looking up User in Internal Users IDStore
24212	Found User in Internal Users IDStore
13045	TACACS+ will use the password prompt from global TACACS+ configuration
13015	Returned TACACS+ Authentication Reply
13014	Received TACACS+ Authentication CONTINUE Request (⏰ Step latency=3149ms)
15041	Evaluating Identity Policy
22072	Selected identity source sequence - All_User_ID_Stores
15013	Selected Identity Source - Internal Users
24210	Looking up User in Internal Users IDStore
24212	Found User in Internal Users IDStore
22037	Authentication Passed
15036	Evaluating Authorization Policy
15048	Queried PIP - Network Access.UserName
15048	Queried PIP - InternalUser.IdentityGroup
13015	Returned TACACS+ Authentication Reply

여기에서 사용자가 인증 정책의 도움helpdeskuser을 받아 네트워크 장치WLC-9800에 성공 적으로 인증 되었음을 볼 수 있습니다WLC TACACS Authentication > Default. 또한 권한 부여 프로파일IOS Helpdesk이 이 사용자에게 할당되었으며 권한 레벨 1을 부여했습니다.

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.