

ISE 서버를 사용하여 CIMC에서 TACACS+ 인증 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[구성](#)

[권한 연결을 위한 TACACS+ 서버측 컨피그레이션](#)

[ISE 구성 요구 사항](#)

[CIMC의 TACACS+ 컨피그레이션](#)

[다음을 확인합니다.](#)

[CIMC의 CLI에서 컨피그레이션 확인](#)

[문제 해결](#)

[ISE 문제 해결](#)

[관련 정보](#)

소개

이 문서에서는 Cisco CIMC(Integrated Management Controller)에서 TACACS+(Terminal Access Controller Access-Control System Plus) 인증을 구성하는 방법에 대해 설명합니다.

TACACS+는 일반적으로 중앙 서버에서 네트워크 디바이스를 인증하는 데 사용됩니다. 릴리스 버전 4.1(3b)부터 Cisco IMC는 TACACS+ 인증을 지원합니다. CIMC에 대한 TACACS+ 지원을 통해 디바이스에 액세스할 수 있는 여러 사용자 계정을 손쉽게 관리할 수 있습니다. 이 기능은 주기적으로 사용자의 자격 증명을 변경하고 사용자 계정을 원격으로 관리하는 데 도움이 됩니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco CIMC(Integrated Management Controller)
- TACACS+(Terminal Access Controller Access-Control System Plus)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- UCSC-C220-M4S
- CIMC 버전:4.1(3b)
- Cisco ISE(Identity Services Engine) 버전 3.0.0.458

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

구성

권한 연결을 위한 TACACS+ 서버측 컨피그레이션

사용자의 권한 레벨은 해당 사용자에 대해 구성된 **cisco-av-pair** 값을 기반으로 계산됩니다. TACACS+ 서버에 **cisco-av-pair**를 생성해야 하며 사용자는 기본 TACACS+ 특성을 사용할 수 없습니다. 아래 표시된 세 가지 구문은 **cisco-av-pair** 특성에 대해 지원됩니다.

관리자 권한:

```
cisco-av-pair=shell:roles="admin"
```

사용자 권한:

```
cisco-av-pair=shell:roles="user"
```

읽기 전용 권한:

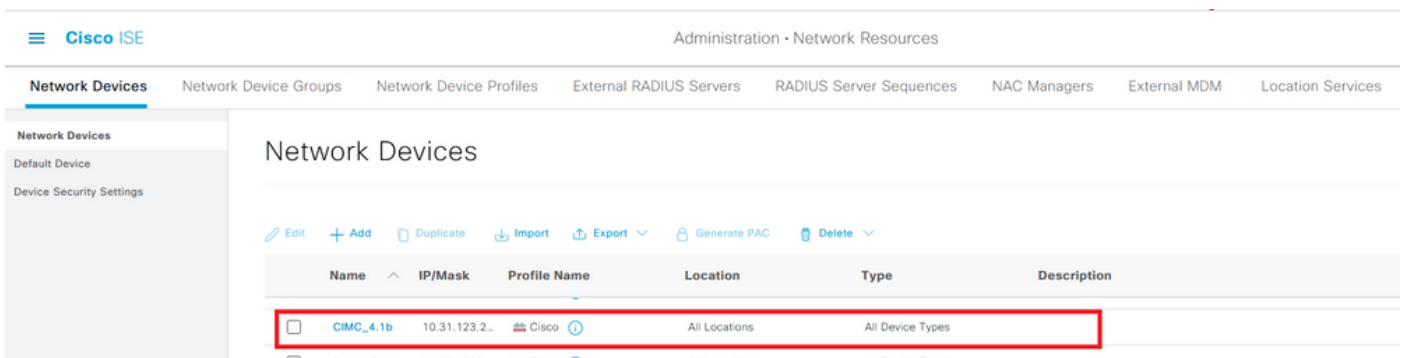
```
cisco-av-pair=shell:roles="read-only"
```

다른 디바이스를 지원하려면 다른 역할을 추가해야 하는 경우 쉼표로 구분하여 추가할 수 있습니다. 예를 들어 UCSM은 **aaa**를 지원하므로 **shell:roles="admin,aaa"**를 구성하고 CIMC가 이 형식을 수락할 수 있습니다.

참고: **cisco-av-pair**가 TACACS+ 서버에 구성되지 않은 경우 해당 서버의 사용자는 읽기 전용 권한을 갖습니다.

ISE 구성 요구 사항

서버의 관리 IP는 ISE 네트워크 디바이스에서 허용되어야 합니다.



The screenshot shows the Cisco ISE Administration console. The top navigation bar includes 'Administration · Network Resources'. Below it, a menu lists various configuration options: 'Network Devices', 'Network Device Groups', 'Network Device Profiles', 'External RADIUS Servers', 'RADIUS Server Sequences', 'NAC Managers', 'External MDM', and 'Location Services'. The 'Network Devices' section is active, displaying a table of configured devices. A red box highlights the first row of the table, which contains the following information:

Name	IP/Mask	Profile Name	Location	Type	Description
CIMC_4.1b	10.31.123.2...	Cisco	All Locations	All Device Types	

CIMC에 입력할 공유 암호

Network Devices

- Default Device
- Device Security Settings

Network Devices List > CIMC_4.1b

Network Devices

* Name

Description

IP Address /

* Device Profile

Model Name

Software Version

* Network Device Group

Location

IPSEC

Device Type

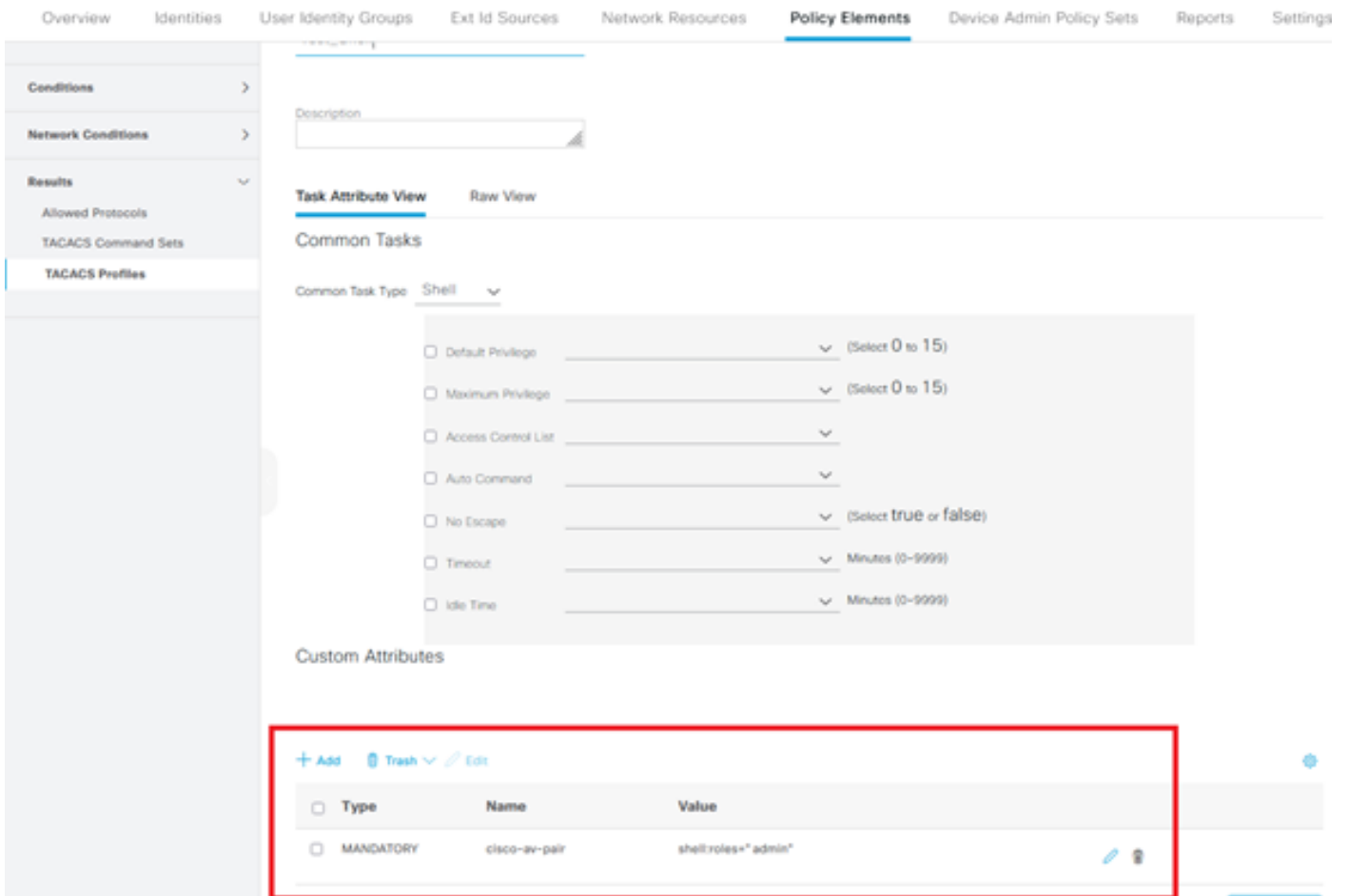
TEST

RADIUS Authentication Settings

TACACS Authentication Settings

Shared Secret

cisco-av-pair 특성과 관리자 권한이 있는 셸 프로파일



CIMC의 TACACS+ 컨피그레이션

1단계. Admin(관리) > User Management(사용자 관리) > TACACS+로 이동합니다.

2단계. TACACS+를 활성화하려면 확인란을 선택합니다.

3단계. 테이블에 지정된 6개 행 중 하나에 새 서버를 추가할 수 있습니다. 행을 클릭하거나 행을 선택하고 이 이미지에 표시된 대로 테이블 위에 있는 **편집** 단추를 클릭합니다.

TACACS+ Properties

Enabled: 1 ←

Fallback only on no connectivity:

Timeout (for each server): (5 - 30 Seconds)

Server List

Selected 0 / Total 6

ID	IP Address or Host Name	Port	Server Key
<input type="radio"/> 1			
<input type="radio"/> 2			
<input type="radio"/> 3			
<input type="radio"/> 4			
<input type="radio"/> 5			
<input type="radio"/> 6			

참고: 사용자가 연결 없음 옵션에서 TACACS+ 폴백을 활성화한 경우 CIMC는 첫 번째 인증 우선 순위를 항상 TACACS+로 설정해야 합니다. 그렇지 않으면 폴백 컨피그레이션이 적합하지 않을 수 있습니다.

4단계. IP 주소 또는 호스트 이름, 포트 및 서버 키/공유 암호를 입력하고 구성을 저장합니다.

Server List

Selected 0 / Total 6

ID	IP Address or Host Name	Port	Server Key	Confirm Server Key
1	10.31.126.220	49	*****	*****
2				
3				
4				
5				

Save | Cancel

3 ↑

Cisco IMC는 최대 6개의 TACACS+ 원격 서버를 지원합니다. 사용자가 성공적으로 인증되면 사용자 이름에 (TACACS+)가 추가됩니다.

🔔 0 tacacs_user (TACACS+)@10.24.92.202 - C220-WZP22460WCD ⚙️

Refresh | ? i

세션 관리에도 표시됩니다.

Sessions

Selected 0 / Total 1 ⚙

Terminate Session				
Session ID	User Name	IP Address	Session Type	
<input type="checkbox"/> 81	tacacs_user (TACACS+)	10.24.92.202	webgui	

다음을 확인합니다.

- CIMC에서 최대 6개의 TACACS+ 서버를 구성할 수 있습니다.
- 서버에 연결된 비밀 키는 최대 64자까지 가능합니다.
- 시간 초과는 5초~30초(LDAP와 일치할 경우 최대 180초로 평가됨) 사이로 구성할 수 있습니다.
- TACACS+ 서버가 서비스 이름을 사용하여 **cisco-av-pair**를 생성해야 하는 경우, 사용자는 **Log in**을 서비스 이름으로 사용해야 합니다.
- 컨피그레이션을 수정할 수 있는 redfish는 지원되지 않습니다.

CIMC의 CLI에서 컨피그레이션 확인

- TACACS+가 활성화되어 있는지 확인합니다.

```
C220-WZP22460WCD# scope tacacs+
C220-WZP22460WCD /tacacs+ # show detail
TACACS+ Settings:
Enabled: yes
Fallback only on no connectivity: no
Timeout(for each server): 5
```

- 서버당 컨피그레이션 세부사항을 확인합니다.

```
C220-WZP22460WCD /tacacs+ # scope tacacs-server 1
C220-WZP22460WCD /tacacs+/tacacs-server # show detail
Server Id 1:
Server IP address/Hostname: 10.31.126.220
Server Key: *****
Server Port: 49
```

문제 해결

- TACACS+ 서버 IP가 CIMC에서 연결 가능하며 포트가 올바르게 구성되었는지 확인합니다.
- TACACS+ 서버에서 **cisco-av** 쌍이 올바르게 구성되었는지 확인합니다.
- TACACS+ 서버에 연결할 수 있는지 확인합니다(IP 및 포트).
- 비밀 키 또는 자격 증명이 TACACS+ 서버에 구성된 키 또는 자격 증명과 일치하는지 확인합니다.
- TACACS+로 로그인할 수 있지만 **읽기 전용** 권한만 있는 경우 **cisco-av-pair**가 TACACS+ 서버에 올바른 구문을 가지고 있는지 확인합니다.

ISE 문제 해결

- 인증 시도 중 하나에 대해 Tacacs Live 로그를 확인합니다.상태는 전달이어야 합니다.

Overview

Request Type	Authorization
Status	Pass
Session Key	ise30baaamex/408819883/155352
Message Text	Device-Administration: Session Authorization succeeded
Username	tacacs_user
Authorization Policy	New Policy Set 1 >> Authorization Rule 1
Shell Profile	Test_Shell
Matched Command Set	
Command From Device	

- 응답에 올바른 **cisco-av-pair** 특성이 구성되었는지 확인합니다.

Other Attributes

ConfigVersionId	933
DestinationIPAddress	10.31.126.220
DestinationPort	49
UserName	tacacs_user
Protocol	Tacacs
RequestLatency	53
Type	Authorization
Service-Argument	login
NetworkDeviceProfileId	b0699505-3150-4215-a80e-6753d45bf56c
AuthenticationIdentityStore	Internal Users
AuthenticationMethod	Lookup
SelectedAccessService	Default Device Admin
IdentityGroup	User Identity Groups:ALL_ACCOUNTS (default)
SelectedAuthenticationIdenti...	Internal Users
AuthenticationStatus	AuthenticationPassed
UserType	User
CPMSessionID	50617983410.31.123.2734354Authorization506179834
IdentitySelectionMatchedRule	Default
TEST	TEST#TEST
Network Device Profile	Cisco
IPSEC	IPSEC#Is IPSEC Device#No
EnableFlag	Enabled
Response	{Author-Reply-Status=PassAdd; AVPair=cisco-av-pair=shell:roles=" admin" ; }

관련 정보

- [TACACS+ 인증 Cisco UCS-C](#)
- [기술 지원 및 문서 - Cisco Systems](#)
- [ISE 2.0 구성:AD 그룹 멤버십 기반 IOS TACACS+ 인증 및 명령 권한 부여](#)