디바이스 관리

TACACS+ 디바이스 관리

Cisco ISE는 네트워크 디바이스의 컨피그레이션을 제어하고 감사하기 위해 TACACS+(Terminal Access Controller Access-Control System) 보안 프로토콜을 사용하는 디바이스 관리를 지원합니다. 네트워크 디바이스는 디바이스 관리자 작업 인증 및 권한 부여를 Cisco ISE에 쿼리하고, 해당 작업을 기록하기 위해 Cisco ISE에 대한 계정 관리 메시지를 전송하도록 구성됩니다. 따라서 어떤 사용자가 어떤 네트워크 디바이스에 액세스하고 관련 네트워크 설정을 변경할 수 있는지를 세분화된 방식으로 제어할 수 있습니다. Cisco ISE 관리자는 디바이스 관리 액세스 서비스의 권한 부여 정책 규칙에서 명령 집합 및 쉘(shell) 프로파일과 같은 TACACS 결과를 선택하도록 허용하는 정책 집합을 생성할 수 있습니다. Cisco ISE 모니터링 노드는 디바이스 관리와 관련이 있는 향상된 보고서를 제공합니다. 작업 센터 메뉴에는 ISE 관리자에게 단일 시작점으로 작동하는 모든 디바이스 관리 페이지가 포함되어 있습니다.

Cisco ISE에서 TACACS+를 사용하려면 디바이스 관리 라이선스가 필요합니다.

디바이스 관리를 수행하는 관리자에는 다음 두 가지 유형이 있습니다.

- 디바이스 관리자
- Cisco ISE 관리자

디바이스 관리자는 스위치, 무선 액세스 포인트, 라우터, 게이트웨이와 같은 네트워크 디바이스에 로그인하여(일반적으로 SSH 사용) 관리 중인 디바이스의 구성 및 유지 관리를 수행하는 사용자입니다. Cisco ISE 관리자는 Cisco ISE에 로그인하여 디바이스 관리자가 로그인하는 디바이스를 구성하고 조정합니다.

Cisco ISE 관리자는 이 문서의 대상으로, 디바이스 관리자의 작업을 제어하는 설정을 구성하기 위해 Cisco ISE에 로그인합니다. Cisco ISE 관리자는 디바이스 관리 기능(Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**) > Device Administration(**디바이스 관리**)**)을 사용하여 네트워크 디바이스의 구성을 제어 및 감사합니다. 디바이스는 TACACS(Terminal Access Controller Access-Control System) 보안 프로토콜을 사용하여 Cisco ISE 서버에 쿼리하도록 구성할 수 있습니다. Cisco ISE 모니터링 노드는 디바이스 관리와 관련이 있는 향상된 보고서를 제공합니다. Cisco ISE 관리자는 다음 작업을 수행할 수 있습니다.

- TACACS+ 세부정보(공유 암호)로 네트워크 디바이스를 구성합니다.
- 디바이스 관리자를 내부 사용자로 추가하고 필요에 따라 활성화 비밀번호를 설정합니다.
- 디바이스 관리 액세스 서비스의 권한 부여 정책 규칙에서 명령 집합 및 쉘(shell) 프로파일과 같은 TACACS 결과를 선택하도록 허용하는 정책 집합을 생성합니다.
- 디바이스 관리자가 정책 집합에 따라 디바이스에 액세스할 수 있도록 Cisco ISE에서 TACACS 서버를 구성합니다.

디바이스 관리자는 Cisco ISE 서버와 통신하도록 디바이스를 설정하는 작업을 수행합니다. 디바이스 관리자가 디바이스에 로그온하면 디바이스는 Cisco ISE 서버에 쿼리합니다. 그러면 Cisco ISE 서버가 내부 또는 외부 ID 저장소에 쿼리하여 디바이스 관리자의 세부정보를 검증합니다. Cisco ISE 서버에서 검증이 수행되면 디바이스는 Cisco ISE 서버에 계정 관리 및 감사를 위해 각 세션 또는 명령 권한 부여 작업의 최종 결과를 알립니다.

Cisco ISE 관리자는 TACACS 및 Cisco ISE 2.0 이상 릴리스를 사용하여 디바이스 관리를 수행할 수 있습니다. 디바이스 관리와 관련된 구성을 Cisco Secure Access Control System(ACS) 서버 5.5, 5.6, 5.7 및 5.8 버전에서 마이그레이션할 수도 있습니다. 마이그레이션 전에 이전 버전을 5.5 또는 5.6으로 업그레이드해야 합니다.

참고 TACACS+ 작업을 활성화하려면 **Administration(**관리**) > System(**시스템**) > Deployment(**구축**) > General Settings(**일반 설정**)** 페이지에서 **Enable Device Admin Service(**디바이스 관리 서비스 활성화**)** 확인란을 선택해야 합니다. 구축의 각 PSN에서 이 옵션이 활성화되어 있는지 확인합니다.

TACACS+ 프로토콜은 스위치 또는 라우터와 Cisco ISE 간의 보안 연결을 생성하는 데 알려진 제한이 있으므로 양측 간에 IPsec 프로토콜이 구축되었는지 확인하십시오.

ISE 커뮤니티 리소스

디바이스 관리 속성에 대한 자세한 내용은 ISE Device Administration Attributes를 참고하십시오.

무선 LAN 컨트롤러, IOS 네트워크 디바이스, Cisco NX-OS 네트워크 디바이스 및 네트워크 디바이스의 TACACS+ 구성에 대한 자세한 내용은 ISE Device Administration(TACACS+)을 참고하십시오.

디바이스 관리 작업 센터

작업 센터 메뉴에는 Cisco ISE 관리자에게 단일 시작점으로 작동하는 모든 디바이스 관리 페이지가 포함되어 있습니다. 그러나 Users(사용자), User Identity Groups(사용자 ID 그룹), Network Devices(네트워크 디바이스), Default Network Devices(기본 네트워크 디바이스), Network Device Groups(네트워크 디바이스 그룹), Authentication and Authorization Conditions(인증 및 권한 부여 조건) 등 디바이스 관리 조건이 없는 페이지는 다른 메뉴 옵션, 예를 들면 Administration(관리)에서도 액세스할 수 있습니다. Work Centers(작업 센터) 옵션은 올바른 TACACS+ 라이선스를 얻어 설치한 경우에만 사용할 수 있습니다.

Device Administration(디바이스 관리) 메뉴에는 Overview(개요), Identities(ID), User Identity Groups(사용자 ID 그룹), Ext ID Stores(Ext ID 저장소), Network Resources(네트워크 리소스 그룹), Policy Elements(정책 요소), Device Admin Policy Sets(디바이스 관리 정책 집합), Reports(보고서) 및 Settings(설정) 메뉴 옵션이 포함되어 있습니다.

디바이스 관리 구축 설정

Device Administration Deployment(디바이스 관리 구축 페이지)(Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Device Administration(**디바이스 관리**)** > **Overview(**개요**)** > **Deployment(**구축**)**)에서 Cisco ISE 관리자가 구축 섹션의 각 노드를 참조하지 않고 디바이스 관리 시스템을 중앙에서 볼 수 있습니다.

Device Administration Deployment(디바이스 관리 구축) 페이지에는 구축의 PSN이 나열됩니다. 이렇게 하면 구축의 각 PSN에서 개별적으로 디바이스 관리 서비스를 활성화하는 작업이 간소화됩니다. 아래의 옵션을 선택하여 여러 PSN에 대해 디바이스 관리 서비스를 한꺼번에 활성화할 수 있습니다.

옵션	설명
없음	기본적으로 디바이스 관리 서비스는 모든 노드에 대해 비활성화되어 있습니다.
모든 정책 서비스 노드	모든 PSN에서 디바이스 관리 서비스를 활성화합니다. 이 옵션을 사용하면 새 PSN이 추가될 때 디바이스 관리자에 대해 자동으로 활성화됩니다.
특정 노드	구축의 모든 PSN을 나열하는 ISE 노드 섹션을 표시합니다. 디바이스 관리 서비스를 활성화해야 하는 필수 노드를 선택할 수 있습니다.

참고 구축에 TACACS+용 라이선스가 없으면 위의 옵션은 비활성화됩니다.

TACACS Ports(TACACS 포트) 필드에서는 최대 4개의 TCP 포트를 쉼표로 구분하여 입력 할 수 있으며 포트 값 범위는 1 ~ 65535입니다. Cisco ISE 노드 및 해당 인터페이스는 지정된 포트에서 TACACS+

요청을 수신하며, 지정된 포트가 다른 서비스에서 사용되지 않도록해야 합니다. 기본 TACACS+ 포트값은 49입니다.

Save(저장**)**를 클릭하면 **Administration(**관리**)** > **System(**시스템**)** > **Deployment Listing(**구축 목록**)**창에 지정된 노드와 변경 사항이 동기화됩니다.

디바이스 관리 정책 집합

Device Admin Policy Sets(디바이스 관리 정책 집합) 창에는(Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)> Device Administration(**디바이스 관리**) > Device Admin Policy Sets(**디바이스 관리 정책 집합**))**에는 Cisco ISE 관리자가 TACACS+ 디바이스 관리자의 인증 및 권한 부여를 제어하기 위해 관리하는 정책 집합 목록이 포함되어 있습니다. 각 정책은 일반 및 프록시 시퀀스의 두 가지 모드 중 하나일 수 있습니다.

일반 정책 집합은 인증 규칙 표과 권한 부여 규칙 표로 구성됩니다. 인증 규칙 표에는 네트워크 디바이스를 인증하는 데 필요한 작업을 선택하기 위한 규칙 집합이 포함되어 있습니다.

권한 부여 규칙 표에는 권한 부여 비즈니스 모델을 구현하는 데 필요한 특정 권한 부여 결과를 선택하는 규칙 집합이 포함되어 있습니다. 각 권한 부여 규칙은 참여할 규칙에 대해 일치해야 하는 하나 이상의 조건, 권한 부여 프로세스를 제어하기 위해 선택된 명령 집합 및/또는 셸 프로파일로 구성됩니다. 각 규칙 표은 특정 상황에서 규칙을 재정의하는 데 사용할 수 있는 예외 정책이 있으며, 종종 예외 표이 임시 상황에 사용됩니다.

참고 TACACS+ CHAP 아웃 바운드 인증은 지원되지 않습니다.

프록시 시퀀스 정책 집합에는 선택한 단일 프록시 시퀀스가 포함되어 있습니다. 정책 집합이 이 모드에 있으면 요청을 처리하는 데 하나 이상의 원격 프록시 서버가 사용됩니다(프록시 시퀀스에서 로컬 어카운팅을 구성할 수는 있음).

디바이스 관리 정책 집합 생성

디바이스 관리 정책 집합을 생성하려면 다음 단계를 수행합니다.

시작하기 전에

- TACACS + 작업에 대해 **Work Centers(**작업 센터**)** > **Device Administration(**디바이스 관리**)** > **Overview(**개요**)** > **Deployment(**구축**)** 창의 디바이스 관리가 활성화되어 있는지 확인합니다.
- 정책에 필요한 모든 사용자 ID 그룹(예: System_Admin, Helpdesk)이 생성되었는지 확인합니다. (Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Device Administration(**디바이스 관리**)** > **User Identity Groups(**사용자 **ID** 그룹**)** 페이지). 멤버 사용자(예: ABC, XYZ)가 해당 그룹에 할당되었는지 확인합니다. (Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Device Administration(**디바이스 관리**)** > **Identities(ID)** > **Users(**사용자**)**창).

- 관리해야 하는 디바이스에서 TACACS 설정을 구성해야 합니다. (Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Device Administration(**디바이스 관리**)** > **Network Resources(**네트워크 리소스**)** > **Network Devices(**네트워크 디바이스**)** > **Add(**추가**)** > **TACACS Authentication Settings(TACACS+** 인증 설정**)** 확인란이 활성화되고 TACACS 및 디바이스의 공유 암호가 동일하여 디바이스가 Cisco ISE를 쿼리하도록 지원합니다.)
- 디바이스 유형 및 위치를 기반으로 네트워크 디바이스 그룹이 생성되었는지 확인합니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Device Administration(**디바이스 관리**)** > **Network Device Groups(**네트워크 디바이스 그룹**)** 창)

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Device Administration(**디바이스 관리**)** > **Device Admin Policy Sets(**디바이스 관리자 정책 집합**)**.

단계 **2** 아무 행의 **Actions(**작업**)** 열에서 톱니바퀴 아이콘을 클릭한 다음 드롭다운 메뉴에서 필요에 따라 삽입 또는 복제 옵션을 선택하여 새 정책 집합을 삽입합니다.
정책 집합 표에 새 행이 표시됩니다.

단계 **3** 정책 집합의 이름과 설명을 입력합니다.

단계 **4** 필요한 경우 Allowed Protocols/Server Sequence(허용되는 프로토콜/서버 시퀀스) 열에서 (+) 기호를 클릭하고 다음 중 하나를 선택합니다.

a) 새 허용되는 프로토콜 생성
b) TACACS 서버 시퀀스 생성

단계 **5** **Conditions(**조건**)** 열에서 (+) 기호를 클릭합니다.

단계 **6** **Conditions Studio** 페이지에 필수 조건을 생성합니다. **Editor(**편집기**)** 섹션에서 **Click To Add an Attribute(**클릭해서 속성 추가**)** 텍스트 상자를 클릭하고 필수 사전 및 속성(예: Device-Location Equals Europe)을 선택합니다.

Click To Add An Attribute(클릭해서 속성 추가**)** 텍스트 상자에 라이브러리 조건을 끌어다 놓을 수 있습니다.

단계 **7** **Use**를 클릭합니다.

단계 **8** View(보기) 열에서 › 표시를 클릭하여 모든 정책 집합 세부정보에 액세스하고 인증 및 권한 부여 정책과 정책 예외를 생성합니다.

단계 **9** 필요 인증 정책을 생성합니다(예: Rule Name: ATN_Internal_Users, Conditions: DEVICE:Location EQUALS Location #All Locations#Europe—정책이 유럽 위치에 존재하는 디바이스에만 일치됨).

단계 **10** **Save(**저장**)**를 클릭합니다.

단계 **11** 필수 권한 부여 정책을 만듭니다.

예 1: 규칙 이름: Sys_Admin_rule, 조건: if SysAdmin and TACACS User Equals ABC then cmd_Sys_Admin AND Profile_priv_8—이 정책은 시스템 관리자를 사용자 이름 ABC와 일치시키고 지정된 명령을 실행하며 권한 레벨 8을 할당합니다.

예 2: 규칙 이름: HelpDesk AND TACACS User EQUALS XYZ then cmd_HDesk_show AND cmd_HDesk_ping AND Profile_priv_1—이 정책은 시스템 관리자와 사용자 이름 XYZ를 매칭하고 지정된 명령을 실행하도록 허용하며 권한 레벨 1을 할당합니다.

위의 예에서

- 명령 집합 cmd_Sys_Admin 및 cmd_HDesk는 **Work Centers(**작업 센터**)** > **Device Administration(**디바이스 관리**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **TACACS Command Sets(TACACS** 명령 집합**)** > **Add(**추가**)** 창에 생성됩니다.
- TACACS 프로파일 Profile_Priv_1 및 Profile_priv_8은 **Work Centers(**작업 센터**)** > **Device Administration(**디바이스 관리**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **TACACS Command Sets(TACACS** 명령 집합**)** > **Add(**추가**)** 창에 생성됩니다.

참고 인증 및 권한 부여 정책에 사용되는 조건에서 디바이스 IP 주소 속성에 대해 IPv4 또는 IPv6 단일 주소를 추가할 수 있습니다.

단계 **12** **Save(**저장**)**를 클릭합니다.

TACACS+ 인증 설정 및 공유 암호

다음 표에서는 네트워크 디바이스에 대한 TACACS+ 인증 설정을 구성하는 데 사용할 수 있는 Network Devices(네트워크 디바이스) 창의 필드를 설명합니다. 탐색 경로는 다음과 같습니다.

- (네트워크 디바이스의 경우) Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Device Administration(**디바이스 관리**)** > **Network Resources(**네트워크 리소스**)** > **Network Devices(**네트워크 디바이스**)** > **Add(**추가**)** > **TACACS Authentication Settings(TACACS** 인증 설정**)**입니다.
- (기본 디바이스의 경우) Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Device Administration(**디바이스 관리**)** > **Network Resources(**네트워크 리소스**)** > **Default Devices(**기본 디바이스**)** > **TACACS Authentication Settings(TACACS** 인증 설정**)**입니다. 자세한 내용은 의 "Cisco ISE의 기본 네트워크 디바이스 정의"를 참조하십시오.

필드 이름	사용 지침
Shared Secret(공유 암호**)**	TACACS+ 프로토콜을 활성화할 때 네트워크 디바이스에 할당된 텍스트 문자열입니다. 네트워크 디바이스가 사용자 이름과 비밀번호를 인증하기 전에 사용자가 텍스트를 입력해야 합니다. 사용자가 공유 암호를 제공할 때까지는 연결이 거부됩니다. 이것은 필수 항목이 아닙니다.
Retired Shared Secret is Active(사용 중단된 공유 암호가 활성 상태임**)**	사용 중단 기간이 활성인 경우 표시됩니다.
Retire(사용 중단**)**	기존 공유 암호를 종료하는 대신 사용 중단합니다. Retire(사용 중단)를 클릭하면 메시지 상자가 표시됩니다. **Yes(**예**)** 또는 **No(**아니요**)**를 클릭할 수 있습니다.

필드 이름	사용 지침
Remaining Retired Period(남은 사용 중단 기간**)**	(위의 메시지 상자에서 **Yes(**예**)**를 선택한 경우에만 사용 가능함) Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Device Administration(**디바이스 관리**)** > **Settings(**설정**)** > **Connection Settings(**연결 설정**)** > **Default Shared Secret Retirement Period(**기본 공유 암호 사용 중단 기간**)** 탐색 경로에 지정되어 있는 기본값이 표시됩니다. 기본값은 변경할 수 있습니다. 그러면 새 공유 암호를 입력할 수 있으며, 이전 공유 암호는 지정된 기간(일) 동안 활성 상태로 유지됩니다.
End(종료**)**	(위의 메시지 상자에서 **Yes(**예**)**를 선택한 경우에만 사용 가능함) 사용 중단 기간을 종료하고 이전 공유 암호 사용을 중단합니다.
Enable Single Connect Mode(단일 연결 모드 활성화**)**	네트워크 디바이스와의 모든 TACACS+ 통신에 단일 TCP 연결을 사용하려면 선택합니다. 다음 중 하나를 선택합니다. • 레거시 Cisco 디바이스 • 또는 TACACS+ 초안 규정 준수 단일 연결 지원. Single Connect Mode(단일 연결 모드)를 비활성화하면 ISE는 모든 TACACS+ 요청에 대해 새 TCP 연결을 사용합니다.

요약하면,

- 사용 종료 기간을 일수(범위: 1 ~ 99)로 지정하여 이전 공유 암호를 사용 종료하고 동시에 새 공유 암호를 설정합니다.
- 사용 종료 기간에는 이전 및 새 공유 암호를 사용합니다.
- 만료 기간이 만료되기 전에 이를 연장합니다.
- 이전 공유 암호는 사용 종료 기간이 끝날 때까지만 사용합니다.
- 만료되기 전에 사용 종료 기간을 종료합니다(End(종료)를 클릭한 다음 Submit(제출)을 클릭).

참고 Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 창에서 TACACS+ 인증 설정 옵션에 액세스할 수 있습니다.

디바이스 관리-권한 부여 정책 결과

Cisco ISE 관리자는 TACACS+ 명령 집합 및 TACACS+ 프로파일(정책 결과)을 사용하여 디바이스 관리자에게 부여되는 권한 및 명령을 제어할 수 있습니다. 이 정책은 네트워크 디바이스와 함께 동작하므로 네트워크 디바이스에 대한 우발적 혹은 의도적인 구성 변경을 방지합니다. 만약 이런 상황이 발생한 경우, 디바이스 관리 감사 보고서를 사용하여 특정 명령이 실행된 네트워크 디바이스의 관리자가 누구인지를 확인할 수 있습니다.

TACACS + 디바이스 관리를 위해 **FIPS** 및 비 **FIPS** 모드에서 허용되는 프로토콜

Cisco ISE가 정책 결과를 생성하기 위해 제공하는 여러 허용되는 인증 프로토콜 서비스가 있습니다. 그러나 TACACS + 프로토콜에 적용할 수 있는 PAP/ASCII, CHAP 및 MS-CHAPv1과 같은 인증 프로토콜 서비스는 RADIUS용 FIPS 지원 Cisco ISE 어플라이언스에서 비활성화됩니다. 따라서 FIPS 지원 (**Administration(**관리**)** > **System Settings(**시스템 설정**)** > **FIPS Mode(FIPS** 모드**)**) Cisco ISE 어플라이언스를 사용하는 경우 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **Allowed Protocols(**허용된 프로토콜**)** 창에서 프로토콜을 활성화하여 디바이스를 관리할 수 없습니다.

결과적으로 FIPS 및 비 FIPS 모드 모두에 대해 디바이스 관리 정책 결과에 PAP/ASCAP, CHAP 및 MS-CHAPv1 프로토콜을 구성하려면 **Work Centers(**작업 센터**)** > **Device Administration(**디바이스 관리**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **Allowed Protocols(**허용된 프로토콜**)** 창으로 이동해야 합니다. FIPS 모드가 활성화된 경우 기본 디바이스 관리자가 허용하는 프로토콜 설정만 사용할 수 있습니다. 이 옵션은 RADIUS에서 허용되지 않습니다.

TACACS+ 명령 집합

명령 집합은 디바이스 관리자가 실행할 수 있는 지정된 명령 목록을 적용합니다. 디바이스 관리자가 네트워크 디바이스에서 작동 명령을 실행하면 관리자가 이러한 명령을 실행할 권한이 있는지를 확인하기 위해 Cisco ISE가 쿼리됩니다. 이를 명령 권한 부여라고도 합니다.

명령 집합의 와일드카드 및 **Regex**

명령줄은 명령과 0개 이상의 인수로 구성됩니다. Cisco ISE는 명령줄(요청)을 수신하면 명령과 해당 인수를 다양한 방식으로 처리합니다.

- 이 명령은 와일드카드 일치 패러다임을 사용하여 명령 집합 목록에 지정된 명령과 요청의 명령을 일치시킵니다.

  예: Sh?? 또는 S*

- 정규식(regex) 일치 패러다임을 사용하여 요청의 인수를 명령 집합 목록에 지정된 인수와 일치시킵니다.

  예: Show interface[1-4] port[1-9]:tty*

명령 줄 및 명령 집합 목록 일치

요청된 명령 줄을 와일드카드 및 regex를 포함하는 명령 집합 목록에 일치시키려면 다음을 따릅니다.

1. 명령 집합 목록을 반복하여 일치하는 명령을 탐지합니다.

   와일드카드 일치는 다음을 허용합니다.

   - 대소문자 구분 안 함
   - 명령 집합에 있는 명령의 모든 문자는 "?"일 수 있으며, 이는 요청된 명령에 있어야 하는 모든 개별 문자와 일치함
   - 명령 집합에 있는 명령의 모든 문자는 "*"일 수 있으며, 이는 요청된 명령에 있는 0개 이상의 문자와 일치함

     예:

요청	명령 집합	일치	코멘트
show	show	예	—
show	표시	예	대소문자 구분 안 함
show	Sh??	예	모든 문자와 일치
show	Sho??	N	두 번째 "?" 존재하지 않는 문자와 교차
show	S*	예	"*" 문자는 모든 문자와 일치
show	S*w	예	"*"는 "ho" 문자와 일치
show	S*p	N	문자 "p"는 일치하지 않음

2. Cisco ISE는 일치하는 각 명령에 대해 인수를 검증합니다.

   명령 집합 목록에는 각 명령에 대해 공백으로 구분된 인수 집합이 포함됩니다.

   예: Show interface[1-4] port[1-9]:tty.*

   이 명령에는 두 개의 인수가 있습니다.

   1. 인수 1: interface[1-4]

   2. 인수 2: port[1-9]:tty. *

   이 요청의 명령 인수는 패킷에 나타나는 위치 중요 순서로 가져옵니다. 명령 정의의 모든 인수가 요청의 인수와 일치할 때 이 명령/인수가 일치한다고 합니다. 참고로 요청에서 관련 없는 인수는 모두 무시됩니다.

참고 표준 Unix 정규식을 인수에 사용합니다.

복수 명령 집합 처리 규칙

1. 명령 집합에 명령 및 해당 인수에 대한 일치가 포함되어 있고 일치에 Deny Always(항상 거부)가 있는 경우 Cisco ISE는 해당 명령 집합을 Commandset-DenyAlways로 지정합니다.
2. 명령 집합의 명령 일치에 Deny Always(항상 거부)가 없으면 Cisco ISE는 첫 번째 일치 항목에 대해 명령 집합의 모든 명령을 순차적으로 확인합니다.
    1. 첫 번째 일치 항목이 Permit(허용)인 경우 Cisco ISE는 명령 집합을 Commandset-Permit으로 지정합니다.
    2. 첫 번째 일치 항목이 Deny(거부)인 경우 Cisco ISE는 명령 집합을 Commandset-Deny로 지정합니다.
3. Cisco ISE는 모든 명령 집합을 분석한 후 다음 명령을 승인합니다.
    1. Cisco ISE가 Commandset-DenyAlways로 설정된 명령을 지정한 경우 Cisco ISE는 해당 명령을 거부합니다.
    2. Commandset-DenyAlways가 없는 경우 명령 집합이 Commandset-Permit이면 Cisco ISE는 해당 명령을 허용하고, 그렇지 않으면 Cisco ISE에서 명령을 거부합니다. 단, **Unmatched(**일치하지 않음**)** 확인란이 선택된 경우는 예외입니다.

TACACS+ 명령 집합 생성

TACACS + 명령 집합 정책 결과를 사용하여 정책 집합을 생성하려면,

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Device Administration(**디바이스 관리**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **TACACS Command Sets(TACACS** 명령 집합**)**

TACACS 명령 집합을 **Work Centers(**작업 센터**)** > **Device Administration(**디바이스 관리**)** > **Device Admin Policy Sets(**디바이스 관리 정책 집합**)** 페이지에서도 구성할 수 있습니다.

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** 이름과 설명을 입력합니다.

단계 **4** 부여 권한, 명령 및 인수를 지정하려면 **Add(**추가**)**를 클릭합니다.

단계 **5** **Grant(**부여**)** 드롭다운 목록에서 다음을 선택합니다.

- **Permit(**허용**)**: 지정된 명령을 허용합니다(예: permit show, permit con * Argument terminal).
- **Deny(**거부**)**: 지정된 명령을 거부합니다(예: deny mtrace).
- **Deny Always(**항상 거부**)**: 다른 명령 집합에서 허용된 명령을 재정의합니다(예: clear auditlogs).

참고 작업 아이콘을 클릭하여 권한 부여, 명령 및 인수 필드의 열 너비를 늘리거나 줄입니다.

단계 **6** **Permit any command that is not listed below(**아래에 나열되지 않은 명령 허용**)** 확인란을 선택하여 Grant(허용) 열에서 Permit(허용), Deny(거부) 또는 Deny Always(항상 거부)로 지정되지 않은 명령 및 인수를 허용합니다.

TACACS+ 프로파일

TACACS+ 프로파일은 디바이스 관리자의 초기 로그인 세션을 제어합니다. 세션은 각 개별 인증, 권한 부여 또는 계정 관리 요청을 나타냅니다. 네트워크 디바이스에 대한 세션 권한 부여 요청은 Cisco ISE 응답을 유발합니다. 응답에는 네트워크 디바이스에서 해석되는 토큰이 포함되며, 이는 세션 기간 동안 실행될 수 있는 명령을 제한합니다. 디바이스 관리 액세스 서비스에 대한 권한 부여 정책은 단일 셸 프로파일 및 여러 명령 집합을 포함할 수 있습니다. TACACS+ 프로파일 정의는 두 가지 구성 요소로 나뉩니다.

- 공통 작업
- 사용자 맞춤화 속성

TACACS+ 프로파일 창(Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Device Administration(**디바이스 관리**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **TACACS Profiles(TACACS** 프로파일**)**)에는 작업 속성 보기와 원시 보기의 두 가지 보기가 있습니다. 작업 속성 보기를 사용하여 일반 작업을 입력할 수 있으며, 작업 속성 보기 및 원시 보기에서 사용자 맞춤화 속성을 생성할 수 있습니다.

Common Tasks(일반 작업**)** 섹션에서는 프로파일에 대해 자주 사용되는 속성을 선택하고 구성할 수 있습니다. 여기에 포함된 속성은 TACACS+ 프로토콜 초안 사양에 정의된 속성입니다. 그러나 다른 서비스의 요청을 승인할 때 이 값을 사용할 수 있습니다. 작업 속성 보기에서 Cisco ISE 관리자는 디바이스 관리자에게 할당할 권한을 설정할 수 있습니다. 일반적인 작업 유형은 다음과 같습니다.

- Shell
- WLC
- Nexus
- Generic

Custom Attributes(사용자 맞춤화 속성**)** 섹션에서 추가 속성을 구성할 수 있습니다. 이 섹션은 **Common Tasks(**일반 작업**)** 섹션에서 인식되지 않는 속성 목록을 제공합니다. 각 정의는 속성 이름, 속성이 필수인지 아니면 선택인지에 대한 표시 및 속성의 값으로 구성됩니다.

참고 TACACS 사용 네트워크 디바이스에 대해 총 24개의 작업 속성을 정의 할 수 있습니다. 작업 속성을 24개보다 많이 정의하는 경우 TACACS 지원 네트워크 디바이스로 하나도 전송되지 않습니다.

Raw View(원시 보기**)**에서는 속성 이름과 해당 값 사이에 등호(=) 기호를 사용하여 필수 속성을 입력할 수 있으며, 선택 속성은 속성 이름과 해당 값 사이에 별표(*)를 사용하여 입력합니다. **Raw View(**원

시 보기) 섹션에 입력한 속성은 **Task Attribute View(**작업 속성 보기)의 **Custom Attributes(**사용자 맞춤화 속성) 섹션에 반영되며 그 반대의 경우도 마찬가지입니다. **Raw View(**원시 보기) 섹션은 클립 보드의 속성 목록(예 : 다른 제품의 속성 목록)을 복사하여 Cisco ISE에 붙여 넣는 데에도 사용됩니다. 비-셸 서비스에 대해 사용자 맞춤화 속성을 정의할 수 있습니다.

TACACS+ 프로파일 생성

TACACS+ 프로파일을 생성하려면

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터) > **Device Administration(**디바이스 관리) > **Policy Elements(**정책 요소) > **Results(**결과) > **TACACS Profiles(TACACS** 프로파일).

TACACS 명령 집합을 **Work Centers(**작업 센터) > **Device Administration(**디바이스 관리) > **Device Admin Policy Sets(**디바이스 관리 정책 집합) 페이지에서도 구성할 수 있습니다.

단계 **2** **Add(**추가)를 클릭합니다.

단계 **3** **TACACS Profile(TACACS** 프로파일) 섹션에서 프로파일 이름과 설명을 입력하십시오.

단계 **4** **Task Attribute View(**작업 속성 보기) 탭에서 필요한 **Common Tasks(**일반 작업)를 확인합니다. 일반 작업 설정, 12 페이지 페이지를 참조하십시오.

단계 **5** **Task Attribute View(**작업 속성 보기) 탭의 **Custom Attributes(**사용자 맞춤화 속성) 섹션에서 **Add(**추가)를 클릭하여 필요한 속성을 입력합니다.

일반 작업 설정

일반 작업 설정 창을 보려면 Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터) > **Device Administration(**디바이스 관리) > **Policy Elements(**정책 요소) > **Results(**결과) > **TACACS Profiles(TACACS** 프로파일) > **Add(**추가)로 이동합니다. 일반 작업 유형은 셸, WLC, Nexus 및 일반입니다.

Shell

Cisco ISE 관리자가 디바이스 관리자 권한을 설정하는 데 사용할 수 있는 옵션은 다음과 같습니다.

옵션	설명
기본 권한	셸 권한 부여에 대해 디바이스 관리자의 기본(초기) 권한 수준을 활성화합니다. 다음 옵션 중 하나를 선택합니다. • 0~15의 범위 내에서 값을 선택합니다. • 필요한 ID 저장소 속성을 선택합니다.
최대 권한	인증 활성화에 대해 최대 권한 수준을 활성화합니다. 0~15의 범위 내에서 값을 선택할 수 있습니다.

옵션	설명
ACL(Access Control List)	ASCII 문자열(1-251*) 또는 필요한 ID 저장소 속성을 선택합니다.
자동 명령	ASCII 문자열(1-248*) 또는 필요한 ID 저장소 속성을 선택합니다.
이스케이프 없음	이스케이프 문자에 대해 다음 옵션 중 하나를 선택합니다. • True: 이스케이프 방지가 활성화되도록 지정합니다. • False: 이스케이프 방지가 활성화되지 않도록 지정합니다. • 필요한 ID 저장소 속성을 선택합니다.
시간 초과	0~9999의 범위 내에서 값을 선택하거나 필요한 ID 저장소 속성을 선택합니다.
유휴 시간	0~9999의 범위 내에서 값을 선택하거나 필요한 ID 저장소 속성을 선택합니다.

WLC

Cisco ISE 관리자는 다음 옵션을 사용해 WLC 애플리케이션 탭에 대한 디바이스 관리자의 액세스를 제어할 수 있습니다. WLC 애플리케이션에는 WLAN, Controller(컨트롤러), Wireless(무선), Security(보안), Management(관리), Commands(명령) 탭이 포함되어 있습니다.

옵션	설명
All(모두)	디바이스 관리자는 모든 WLC 애플리케이션 탭에 대한 전체 액세스 권한을 갖습니다.
모니터링	디바이스 관리자는 WLC 애플리케이션 탭에 대한 읽기 전용 액세스만 가능합니다.
로비	디바이스 관리자는 제한된 컨피그레이션 권한만 갖습니다.
선택됨	디바이스 관리자는 WLAN, Controller(컨트롤러), Wireless(무선), Security(보안), Management(관리), Commands(명령) 확인란에서 Cisco ISE 관리자가 선택한 대로 탭에 액세스 할 수 있습니다.

Nexus

Cisco ISE 관리자는 다음 옵션을 사용해 Cisco Nexus 스위치에 대한 디바이스 관리자의 액세스를 제어할 수 있습니다.

옵션	설명
다음으로 속성 값 설정	Cisco ISE 관리자는 일반 작업에서 생성된 Nexus 속성을 Optional(선택 사항) 또는 Mandatory(필수)로 지정할 수 있습니다.
네트워크 역할	Nexus가 Cisco ISE를 사용하여 인증하도록 구성된 경우 디바이스 관리자는 기본적으로 읽기 전용 액세스 권한을 갖습니다. 디바이스 관리자는 다음의 역할 중 하나에 할당될 수 있습니다. 각 역할은 허용되는 작업을 정의합니다. • 없음: 권한이 없습니다. • 운영자(읽기 전용): 전체 NX-OS 디바이스에 대해 전체 읽기 액세스가 가능합니다. • 관리자(읽기/쓰기): 전체 NX-OS 디바이스에 대해 전체 읽기 및 쓰기 액세스가 가능합니다.
VDC(Virtual Device Context)	없음: 권한이 없습니다. 운영자(읽기 전용): 읽기 액세스가 VDC로 제한됩니다. 관리자(읽기/쓰기): 읽기 및 쓰기 액세스가 VDC로 제한됩니다.

Generic

Cisco ISE 관리자는이 옵션을 사용하여, 일반 작업에서 사용할 수 없는 맞춤형 속성을 지정할 수 있습니다.

커맨드라인 인터페이스에 액세스하여 활성화 비밀번호 변경

활성화 비밀번호를 변경하려면 다음 단계를 수행하십시오.

시작하기 전에

일부 명령은 권한 모드로 할당됩니다. 따라서 이들 명령은 디바이스 관리자가 이 모드로 인증한 경우에만 실행될 수 있습니다.

디바이스 관리자가 권한 모드를 시작하려고 하면 디바이스에서 특수 활성화 인증 유형을 전송합니다. Cisco ISE는 이 특수 활성화 인증 유형을 검증하기 위해 별도의 활성화 비밀번호를 지원합니다. 별도의 활성화 비밀번호는 디바이스 관리자가 내부 ID 저장소로 인증될 때 사용됩니다. 외부 ID 저장소를 통한 인증의 경우 일반 로그인과 동일한 비밀번호가 사용됩니다.

단계 **1** 스위치에 로그인합니다.

단계 **2** Enter 키를 누르면 다음 프롬프트가 표시됩니다.

```
Switch>
```

단계 **3** 다음 명령을 실행하여 활성화 비밀번호를 설정합니다.

```
Switch> enable
Password: (Press Enter to leave the password blank.)
Enter Old Password: (Enter the old password.)
Enter New Password: (Enter the new password.)
Enter New Password Confirmation: (Confirm the new password.)
```

참고 로그인 비밀번호 및 활성화 비밀번호에 사용 기간이 설정된 경우, 지정된 기간 내에 비밀번호가 변경되지 않으면 사용자 계정이 비활성화됩니다. Cisco ISE가 TACACS+ 서버로 설정되어 있고 **Enable Bypass(**우회 활성화**)** 옵션이 네트워크 디바이스에 설정된 경우 CLI에서(텔넷을 통해) 활성화 비밀번호를 변경할 수 없습니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **Identities(ID)** > **Users(**사용자**)**를 선택해서 활성화 비밀번호를 변경합니다.

전역 **TACACS+** 설정 구성

전역 TACACS + 설정을 구성하려면 다음 단계를 따르십시오.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Device Administration(**디바이스 관리**)** > **Settings(**설정**)**를 선택합니다.

Connection Settings(연결 설정**)** 탭에서 필수 필드의 기본값을 변경할 수 있습니다.

- **Authorization cache timeout(**권한 부여 캐시 시간 초과**)** 필드에서 내부 사용자의 특정 속성이 첫 번째 권한 부여 요청 시 캐시되는 TTL(Time-To-Live) 값을 설정할 수 있습니다. 캐시된 속성에는 사용자 이름 및 UserGroup과 같은 사용자별 속성이 포함됩니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **System Administration(**시스템 관리**)** > **Configuration(**컨피그레이션**)** > **Dictionaries(**사전**)** > **Identity(ID)** > **Internal Users(**내부 사용자**)**를 선택하여 속성을 생성합니다. 기본값은 0이며, 이는 권한 부여 캐시가 비활성화되었음을 의미합니다.
- **Single Connect Support(**단일 연결 지원**)**: 단일 연결 모드를 비활성화하면 ISE는 모든 TACACS + 요청에 대해 새 TCP 연결을 사용합니다.

단계 **2** **Password Change Control(**비밀번호 변경 제어**)** 탭에서 TACACS+를 통해 비밀번호 업데이트를 허용할지를 제어하는 데 필요한 필드를 정의합니다.

Enable Telnet Change Password(Telnet 비밀번호 변경 활성화**)** 섹션의 프롬프트는 이 옵션을 선택한 경우에만 활성화됩니다. 아니면 **Disable Telnet Change Password(Telnet** 비밀번호 변경 비활성화**)**에서 프롬프트가 활성화됩니다. 비밀번호 프롬프트는 맞춤 설정이 가능하며 필요에 따라 수정할 수 있습니다.

새 비밀번호가 지정된 기준과 일치하지 않을 경우 **Password Policy Violation Message(**비밀번호 정책 위반 메시지**)** 필드에 내부 사용자가 설정한 비밀번호 관련 적절한 오류 메시지를 표시할 수 있습니다.

단계 **3** **Session Key Assignment(**세션 키 할당**)** 탭에서 TACACS+ 요청을 세션에 연결하는 데 필요한 필드를 선택합니다.

세션 키는 모니터링 노드에서 클라이언트의 AAA 요청을 연결하는 데 사용됩니다. 기본 설정은 NAS-주소, 포트, 원격-주소 및 사용자 필드를 활성화하는 것입니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

관련 항목

TACACS+ 인증 설정 및 공유 암호, 6 페이지

Cisco Secure ACS에서 Cisco ISE로의 데이터 마이그레이션

마이그레이션 툴을 사용하여 ACS 5.5 이상에서 데이터를 가져오고, 모든 네트워크 디바이스에 대해 기본 TACACS + 암호를 설정할 수 있습니다. **Work Centers(**작업 센터**)** > **Device Administration(**디바이스 관리**)** > **Overview(**개요**)**Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Prepare(**준비**)** 섹션에서 소프트웨어 다운로드 웹페이지를 클릭하여 마이그레이션 툴을 다운로드합니다. 툴을 PC에 저장하고 migTool 폴더에서 migration.bat 파일을 실행하여 마이그레이션 프로세스를 시작합니다. 마이그레이션과 관련된 전체 정보는 Cisco ISE 버전에 대한 마이그레이션 가이드를 참조하십시오.

디바이스 관리 활동 모니터링

Cisco ISE는 TACACS+로 구성된 디바이스의 계정 관리, 인증, 권한 부여 및 명령 계정 관리와 관련된 정보를 볼 수 있는 다양한 보고서 및 로그를 제공합니다. 온디맨드 또는 예약 방식으로 이러한 보고서를 실행할 수 있습니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Device Administration(**디바이스 관리**)** > **Reports(**보고서**)** > **ISE Reports(ISE** 보고서**)**를 선택합니다. .

다른 위치에서 보고서를 볼 수도 있습니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(**운영**)** > **Reports(**보고서**)** > **Reports(**보고서**)**페이지를 클릭하십시오.

단계 **2** **Report Selector(**보고서 선택기**)**에서 **Device Administration(**디바이스 관리**)**을 확장하여 **Authentication Summary(**인증 요약**)**, **TACACS Accounting(TACACS** 계정 관리**)**, **TACACS Authentication(TACACS** 인증**)**, **TACACS Authorization(TACACS** 권한 부여**)** **TACACS Command Accounting(TACACS** 명령 계정 관리**)**, **Top N Authentication by Failure Reason(**실패 이유별 상위 **N** 인증**)**, **Top N Authentication by Network Device(**네트워크 디바이스별 상위 **N** 인증**)**, **Top N Authentication by User(**사용자별 상위 **N** 인증**)** 보고서를 확인합니다.

단계 **3** 보고서를 선택하고 **Filters(**필터**)** 드롭다운 목록을 사용하여 검색할 데이터를 선택합니다.

단계 **4** 데이터를 확인할 **Time Range(**시간 범위**)**를 선택합니다.
단계 **5** **Run(**실행**)**을 클릭합니다.

TACACS 라이브 로그

다음 표에서는 TACACS+ AAA 세부정보가 표시되는 TACACS Live Logs(TACACS 라이브 로그) 페이지의 필드에 대해 설명합니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(**운영**)** > **RADIUS** > **Live Logs(**라이브 로그**)**입니다. 기본 PAN에서만 TACACS 라이브 로그를 볼 수 있습니다.

표 ***1: TACACS*** 라이브 로그

필드 이름	사용 지침
생성 시간	특정 이벤트가 트리거된 시간을 기준으로 시스템 로그 생성 시간을 표시합니다.
Logged Time(기록된 시간**)**	모니터링 노드에서 시스템 로그를 처리하고 저장한 시간을 표시합니다. 이 열은 필수 항목이므로 선택을 취소할 수 없습니다.
Status(상태**)**	인증 성공 여부를 표시합니다. 이 열은 필수 항목이므로 선택을 취소할 수 없습니다. 인증이 통과한 경우 녹색으로 표시되고, 인증이 실패한 경우 빨간색으로 표시됩니다.
Details(세부정보**)**	돋보기를 클릭하면 표시되는 보고서를 드릴다운하여 선택한 인증 시나리오에 대한 추가 세부정보를 확인할 수 있습니다. 이 열은 필수 항목이므로 선택을 취소할 수 없습니다.
Session Key(세션 키**)**	ISE가 네트워크 디바이스에 반환하는 세션 키(EAP 성공 또는 EAP 장애 메시지에서 확인 가능)를 표시합니다.
Username(사용자 이름**)**	디바이스 관리자의 사용자 이름을 표시합니다. 이 열은 필수 항목이므로 선택을 취소할 수 없습니다.
Type(유형**)**	두 가지 유형인 Authentication(인증)과 Authorization(권한 부여)으로 구성됩니다. 인증, 권한 부여 또는 둘 다에서 통과했거나 장애가 발생한 사용자 이름을 표시합니다. 이 열은 필수 항목이므로 선택을 취소할 수 없습니다.
Authentication Policy(인증 정책**)**	특정 인증에 대해 선택한 정책의 이름을 표시합니다.

필드 이름	사용 지침
권한 부여 정책	특정 권한 부여에 대해 선택한 정책의 이름을 표시합니다.
ISE Node(ISE 노드**)**	액세스 요청이 처리되는 ISE 노드의 이름을 표시합니다.
Network Device Name(네트워크 디바이스 이름**)**	네트워크 디바이스의 이름을 표시합니다.
Network Device IP(네트워크 디바이스 **IP)**	액세스 요청이 처리되는 네트워크 디바이스의 IP 주소를 표시합니다.
네트워크 디바이스 그룹	네트워크 디바이스가 속한 해당 네트워크 디바이스 그룹의 이름을 표시합니다.
디바이스 유형	다른 네트워크 디바이스의 액세스 요청을 처리하는 데 사용되는 디바이스 유형 정책을 표시합니다.
Location(위치**)**	네트워크 디바이스의 액세스 요청을 처리하는 데 사용되는 위치 기반 정책을 표시합니다.
Device Port(디바이스 포트**)**	액세스 요청을 수행하는 디바이스 포트 번호를 표시합니다.
Failure Reason(실패 이유**)**	네트워크 디바이스에서 수행한 액세스 요청을 거부하는 이유를 표시합니다.
Remote Address(원격 주소**)**	최종 무선국을 고유하게 식별하는 IP 주소, MAC 주소 또는 기타 문자열을 표시합니다.
Matched Command Set(일치하는 명령 집합**)**	MatchedCommandSet 속성 값이 있으면 표시하고, MatchedCommandSet 속성 값이 비어 있거나 속성 자체가 시스템 로그에 없으면 빈 값을 표시합니다.
Shell Profile(셸 프로파일**)**	네트워크 디바이스에서 명령을 실행하기 위해 디바이스 관리자에게 부여된 권한을 표시합니다.

TACACS Live Logs(TACACS 라이브 로그) 페이지에서는 다음을 수행할 수 있습니다.

- 데이터를 csv 또는 pdf 형식으로 내보냅니다.
- 요건에 따라 열을 보이거나 숨깁니다.
- 빠른 필터 또는 맞춤형 필터를 사용하여 데이터를 필터링합니다. 나중에 사용하기 위해 필터를 저장할 수도 있습니다.
- 열을 다시 정렬하고 열의 폭을 조정합니다.

- 열 값을 정렬합니다.

참고 모든 사용자 맞춤 설정은 사용자 기본 설정으로 저장됩니다.