ISE 서버를 사용하여 UCS Manager에서 TACACS+ 인증 도메인 구성

목차

소개

이 문서에서는 UCSM(Unified Compute System Manager)에서 TACACS+(Terminal Access Controller Access-Control System Plus) 인증의 컨피그레이션에 대해 설명합니다. TACACS+는 AAA(Authentication, Authorization and Accountability Services)에 사용되는 네트워크 프로토콜로서, 서버를 통해 규칙을 관리하고 생성할 수 있는 NAD(Network Access Devices)를 관리하기 위한 중앙 집중식 방법을 제공합니다. 이 활용 사례에서는 ISE(Identity Services Engine)를 사용합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco UCS Manager(UCSM)
- TACACS+(Terminal Access Controller Access-Control System Plus)
- Identity Services Engine(ISE)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- UCSM 4.2(3d)
- Cisco ISE(Identity Services Engine) 버전 3.2

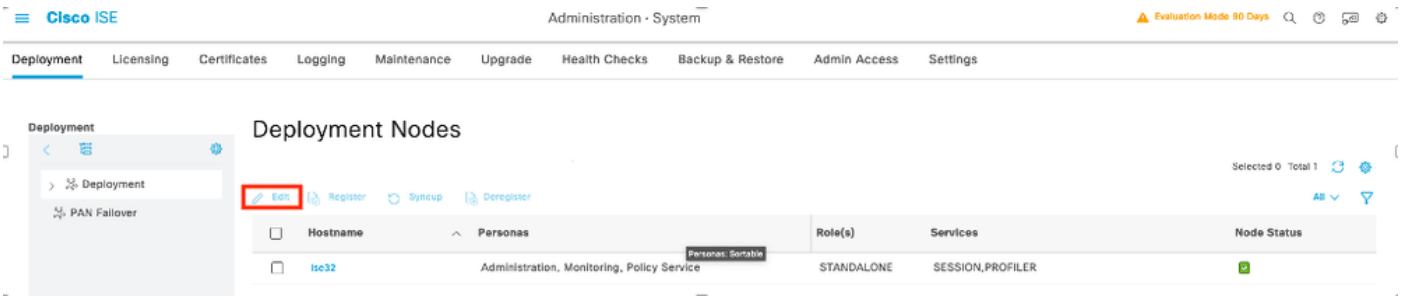
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

설정

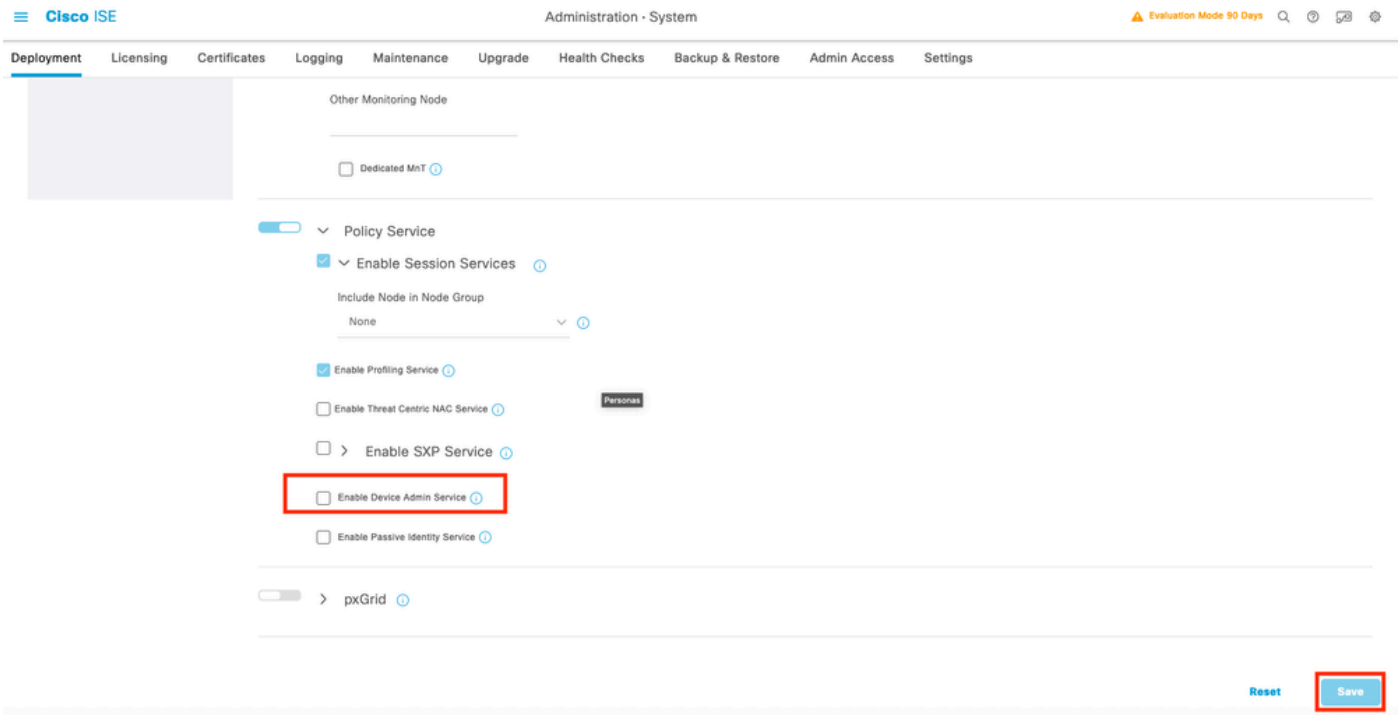
ISE의 TACACS+ 컨피그레이션

ISE의 TACACS+ 설정

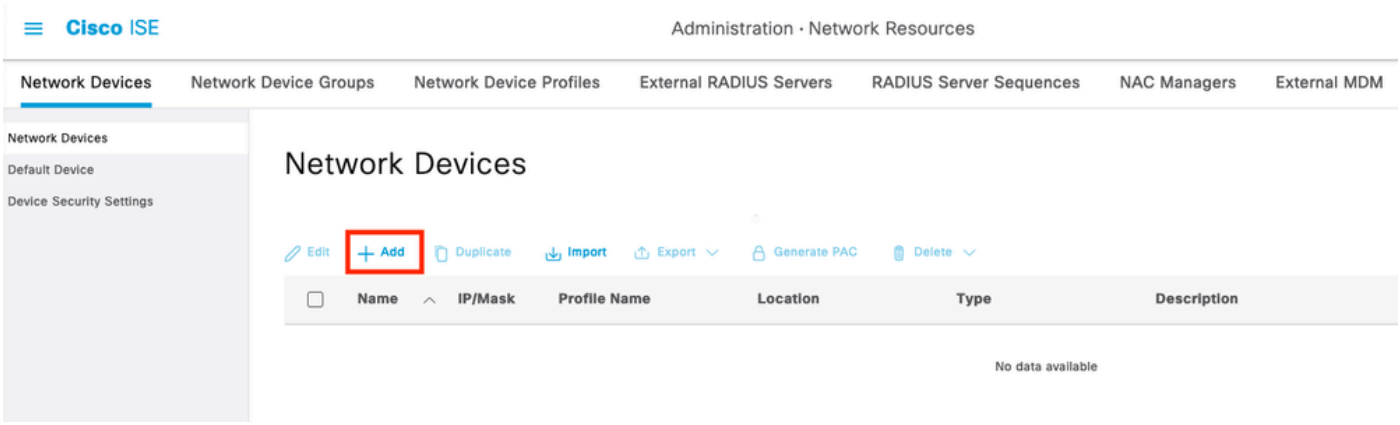
1단계. 첫 번째 작업은 ISE에 TACACS+ 인증을 처리할 수 있는 올바른 기능이 있는지 검토하는 것입니다. 따라서 PSN(Policy Service Node) 내에서 Device Admin Service(디바이스 관리 서비스) 기능을 원하는지 확인하고, Administration(관리) > System(시스템) > Deployment(구축) 메뉴를 탐색하고, ISE가 TACACS+를 수행하는 노드를 선택한 다음 버튼 편집을 선택해야 합니다.



2단계. Device Administration Service라는 해당 기능이 표시될 때까지 아래로 스크롤합니다(이 기능을 활성화하려면 먼저 노드에서 Policy Server 페르소나를 활성화해야 하며 구축에서 TACACS+에 대한 라이센스를 사용할 수 있어야 함). 해당 확인란을 선택한 다음 컨피그레이션을 저장합니다.

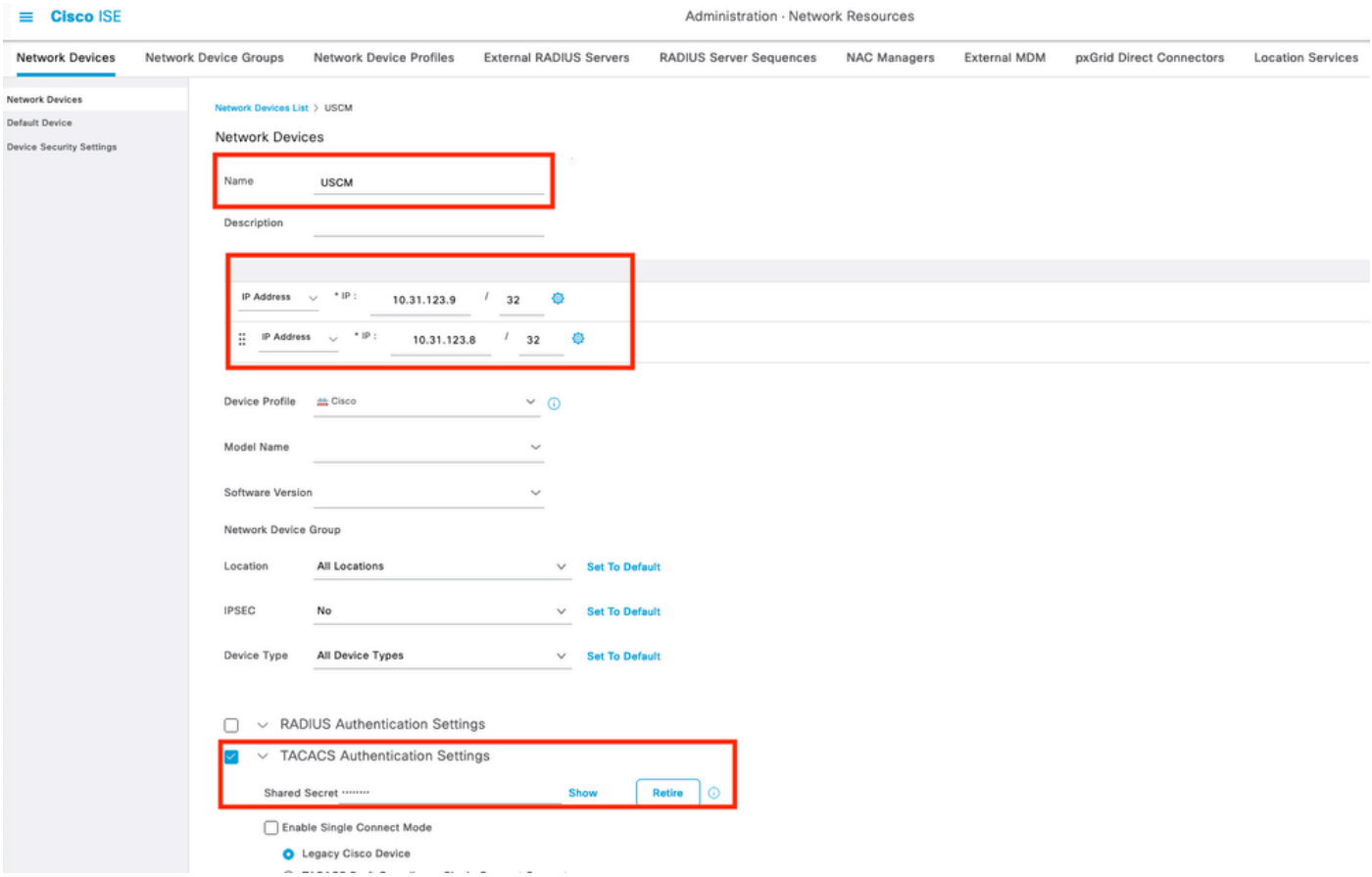


3단계. ISE를 TACACS+로 서버로 사용하는 NAD(Network Access Device)를 구성하고 Administration(관리) > Network Resources(네트워크 리소스) > Network Devices(네트워크 디바이스) 메뉴로 이동한 다음 +Add(추가) 버튼을 선택합니다.



4단계. 이 섹션에서는 다음을 구성합니다.

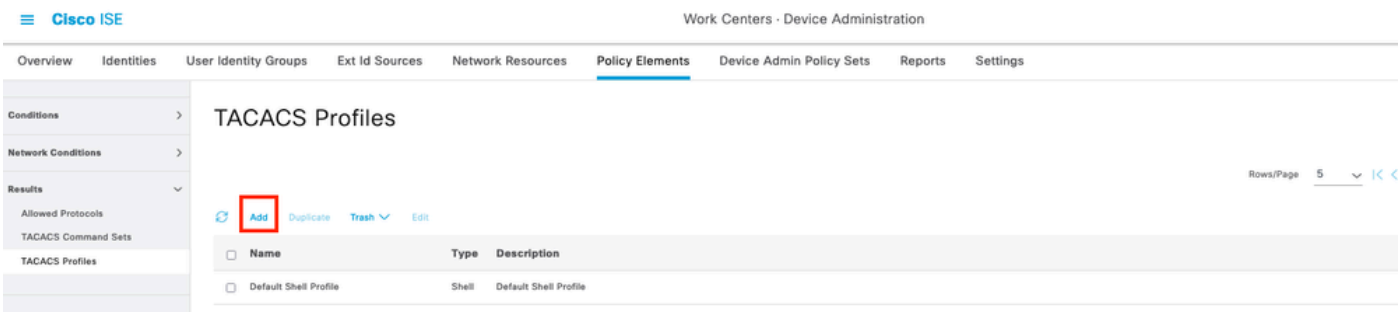
- TACACS+ 클라이언트가 될 UCSM의 이름.
- UCSM에서 ISE에 요청을 보내는 데 사용하는 IP 주소.
- TACACS+ 공유 암호 - UCSM과 ISE 간의 패킷을 암호화하는 데 사용되는 암호입니다.



참고: 클러스터 컨피그레이션의 경우 두 패브릭 인터커넥트에 대한 관리 포트 IP 주소를 추가합니다. 이 컨피그레이션을 통해 첫 번째 패브릭 인터커넥트에 장애가 발생하고 시스템이 두 번째 패브릭 인터커넥트로 장애 조치될 경우 원격 사용자가 계속 로그인할 수 있습니다. 모든 로그인 요청은 Cisco UCS Manager에서 사용하는 가상 IP 주소가 아니라 이러한 IP 주소에서 소싱됩니다.

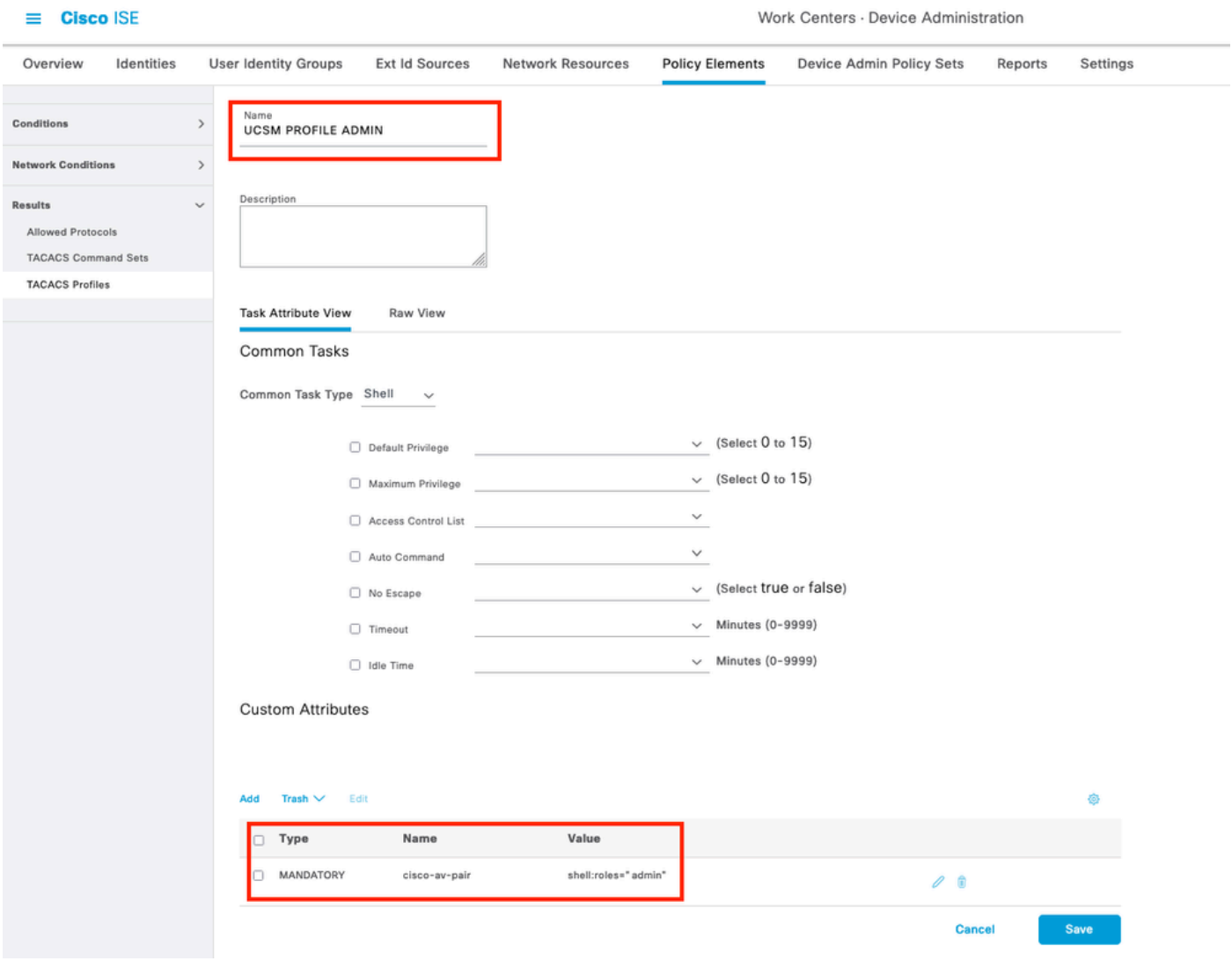
ISE에서 특성 및 규칙 구성

1단계. TACACS+ 프로필을 생성하고 Work Centers(작업 센터) > Device Administration(디바이스 관리) > Policy Elements(정책 요소) > Results(결과) > TACACS Profiles(TACACS 프로필) 메뉴로 이동한 다음 Add(추가)를 선택합니다

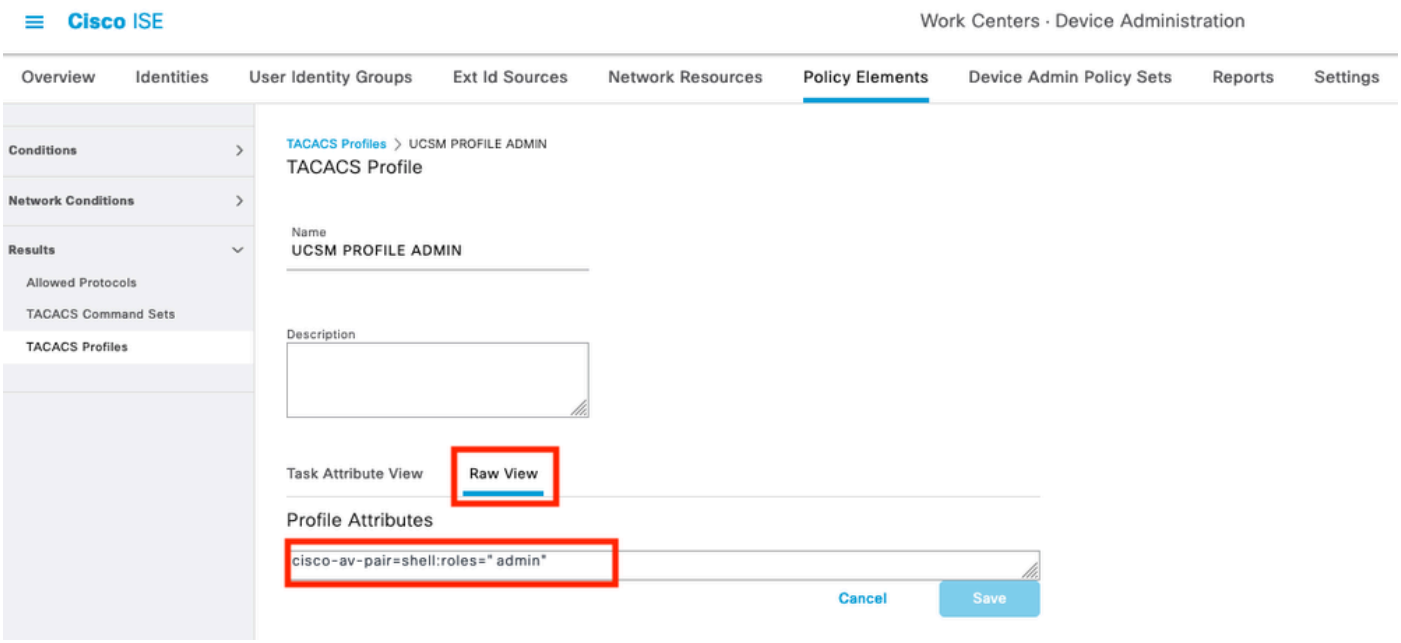


2단계. 이 섹션에서 이름으로 프로파일을 구성하고 Custom Attributes 섹션에서 Add를 선택한 다음 특성 MANDATORY의 특성을 하나 만들고 이름을 cisco-av-pair로 지정하고 값에서 UCSM에서 사

용 가능한 역할 중 하나를 선택하고 해당 역할을 셸 역할로 입력합니다. 이 예에서는 admin 역할을 사용하고 있으며 선택한 입력은shell:roles="admin"입니다.



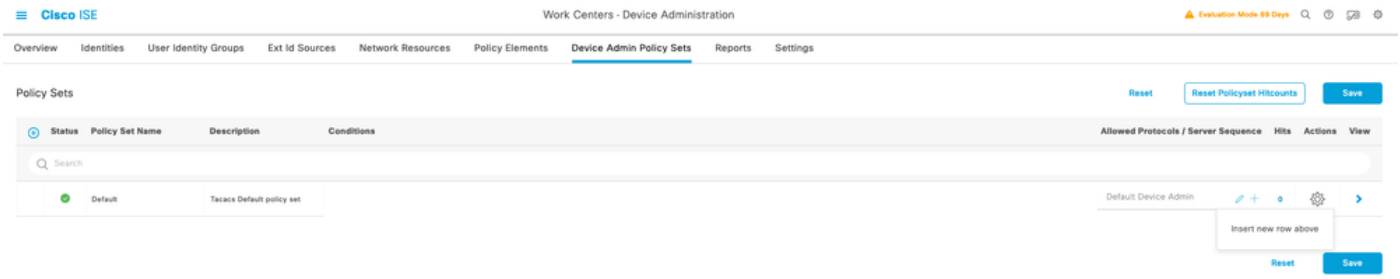
동일한 메뉴에서 TACACS 프로필에 대한 Raw View를 선택하면 ISE를 통해 전송할 특성의 해당 컨피그레이션을 확인할 수 있습니다.



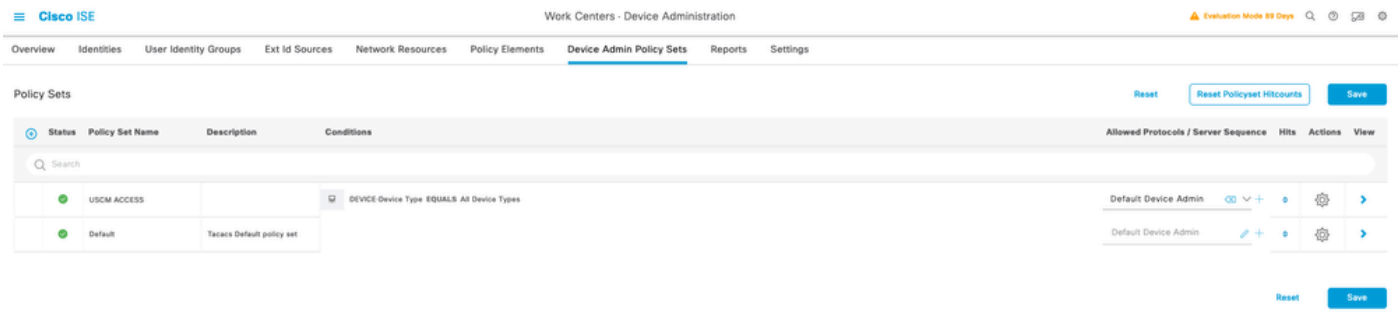
참고: cisco-av-pair 이름은 TACACS+ 제공자에 대한 특성 ID를 제공하는 문자열입니다.

3단계. 틱 마크에서 선택하고 컨피그레이션을 저장합니다.

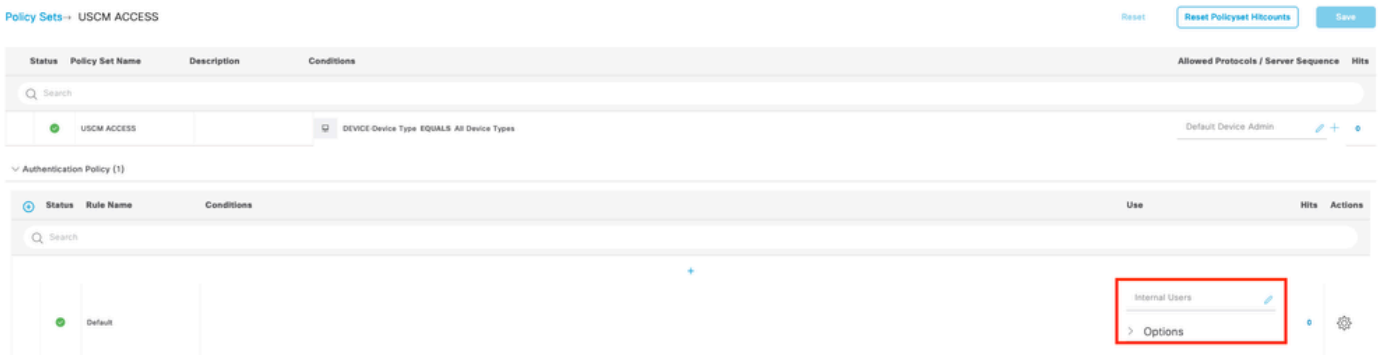
4단계. UCSM에 사용할 Device Admin Policy Set(디바이스 관리 정책 집합)를 생성하고 Work Centers(작업 센터) > Device Administration(디바이스 관리) > Device Admin Policy Sets(디바이스 관리 정책 집합) 메뉴를 탐색한 다음, 기존 정책 집합에서 기어 아이콘을 선택하여 Insert new row(새 행 삽입)를 선택합니다



5단계. 이 새 정책 집합의 이름을 지정하고, UCSM 서버에서 진행되는 TACACS+ 인증의 특성에 따라 조건을 추가하고, Allowed Protocols(허용되는 프로토콜) > Default Device Admin(기본 디바이스 관리)으로 선택하여 컨피그레이션을 저장합니다.

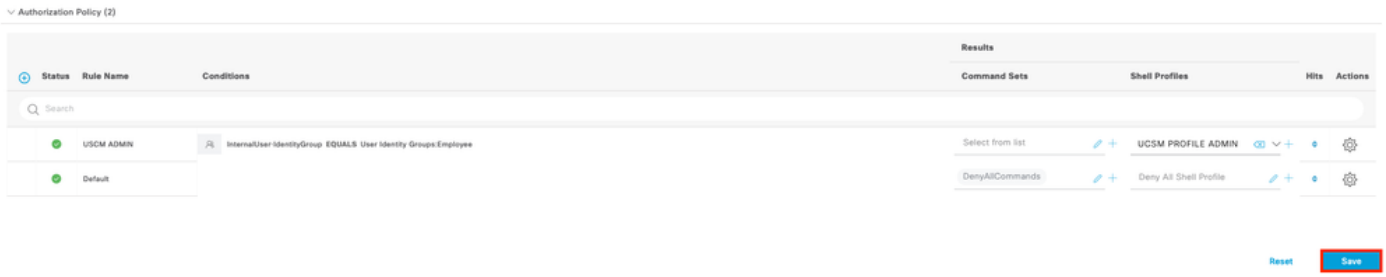


6단계. > 보기 옵션에서 선택하고 인증 정책 섹션에서 외부 ID 소스를 선택합니다. 여기서 ISE는 UCSM에 입력된 사용자 이름 및 자격 증명을 쿼리합니다. 이 예에서는 자격 증명이 ISE에 저장된 내부 사용자에 해당합니다.



7단계. Authorization Policy(권한 부여 정책)라는 섹션이 Default(기본) 정책에 도달할 때까지 아래로 스크롤하여 톱니바퀴 아이콘을 선택한 다음 하나의 규칙을 삽입합니다.

8단계. 새 Authorization Rule(권한 부여 규칙)의 이름을 지정하고 이미 그룹 멤버십으로 인증된 사용자에 대한 조건을 추가하고 Shell Profiles(셸 프로필) 섹션에서 이전에 구성한 TACACS 프로필을 추가하고 컨피그레이션을 저장합니다.



UCSM의 TACACS+ 컨피그레이션

관리자 **Cisco UCS Manager**권한이 있는 사용자를 사용하여 GUI에 로그인합니다.

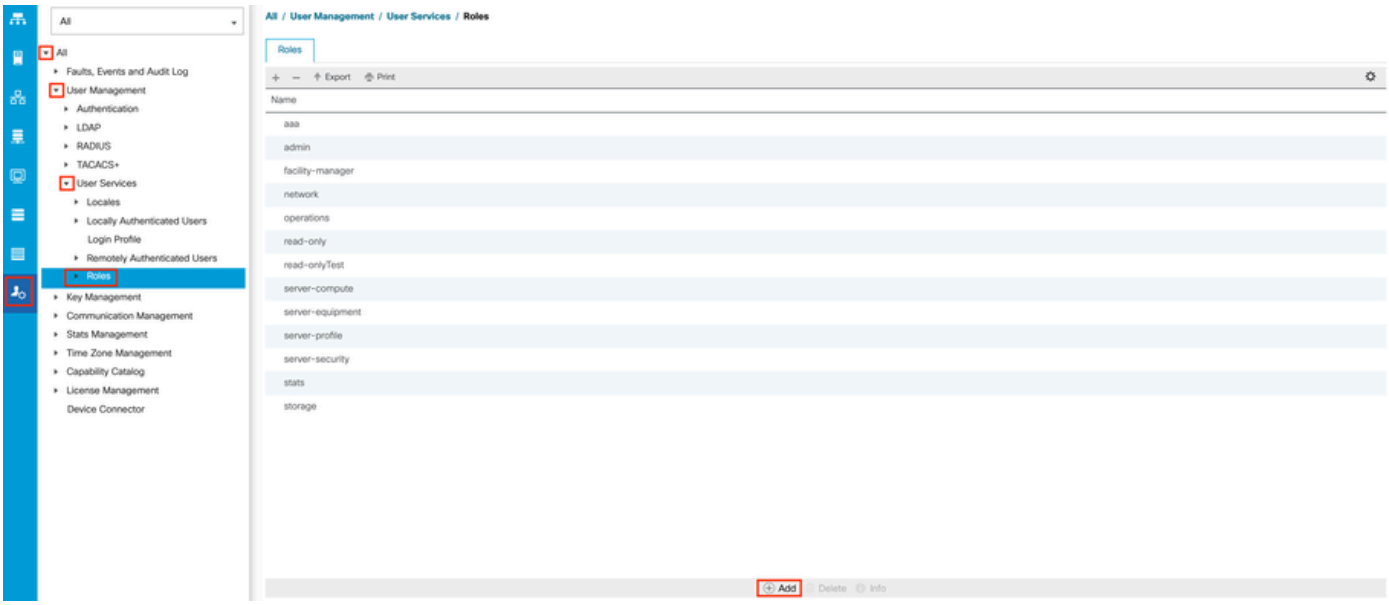
사용자에 대한 역할 생성

1단계. Navigation(탐색) 창에서 Admin(관리) 탭을 선택합니다.
2단계. Admin(관리) 탭에서 All(모두) > User Management(사용자 관리) > User Services(사용자 서비스) > Roles(역할)를 확장합니다.

3단계. 창**Work**에서 탭을**General**선택합니다.

4단계. 사용자 지정 역할에 대해 Add를 선택합니다. 이 샘플은 기본 역할을 사용합니다.

5단계. 이전에 TACACS 프로파일에서 구성된 이름과 역할 일치를 확인합니다.

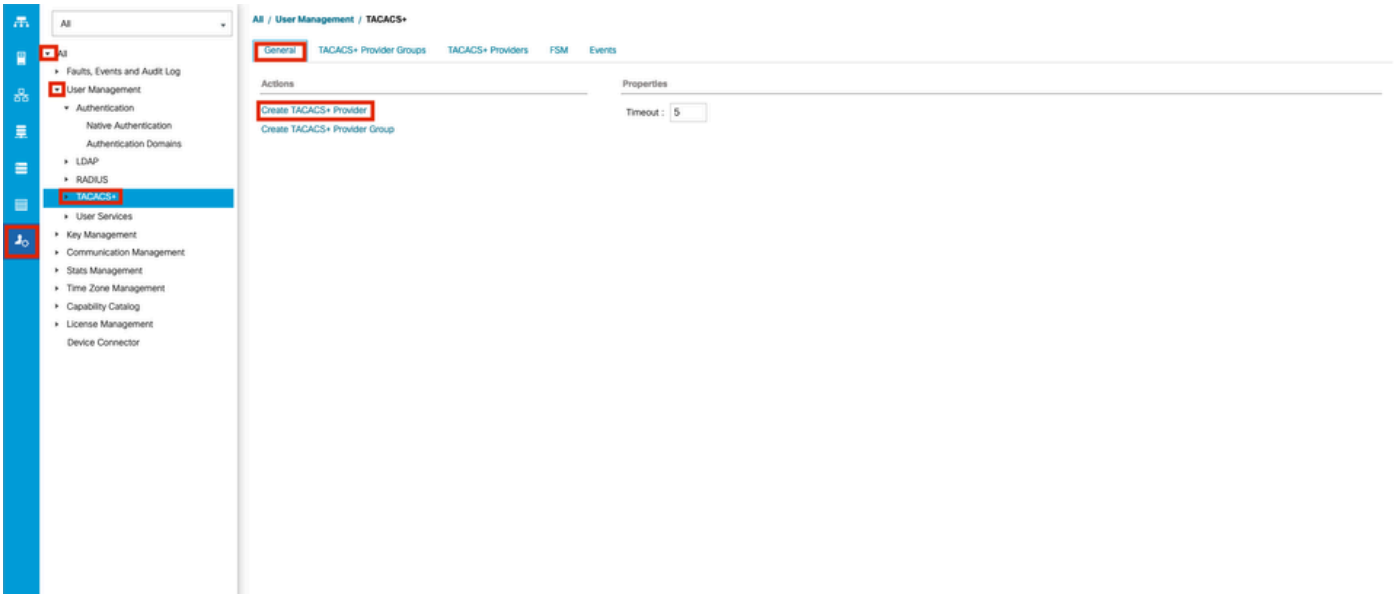


TACACS+ 제공자 생성

1단계. Navigation(탐색) 창에서 Admin(관리) 탭을 선택합니다.
2단계. Admin(관리) 탭에서 All(모두) > User Management(사용자 관리) > TACACS+를 확장합니다.

3단계. 창**Work**에서 탭을**General** 선택합니다.

4단계. 영역에서**Actions**다음을 선택합니다**Create TACACS+ Provider.**



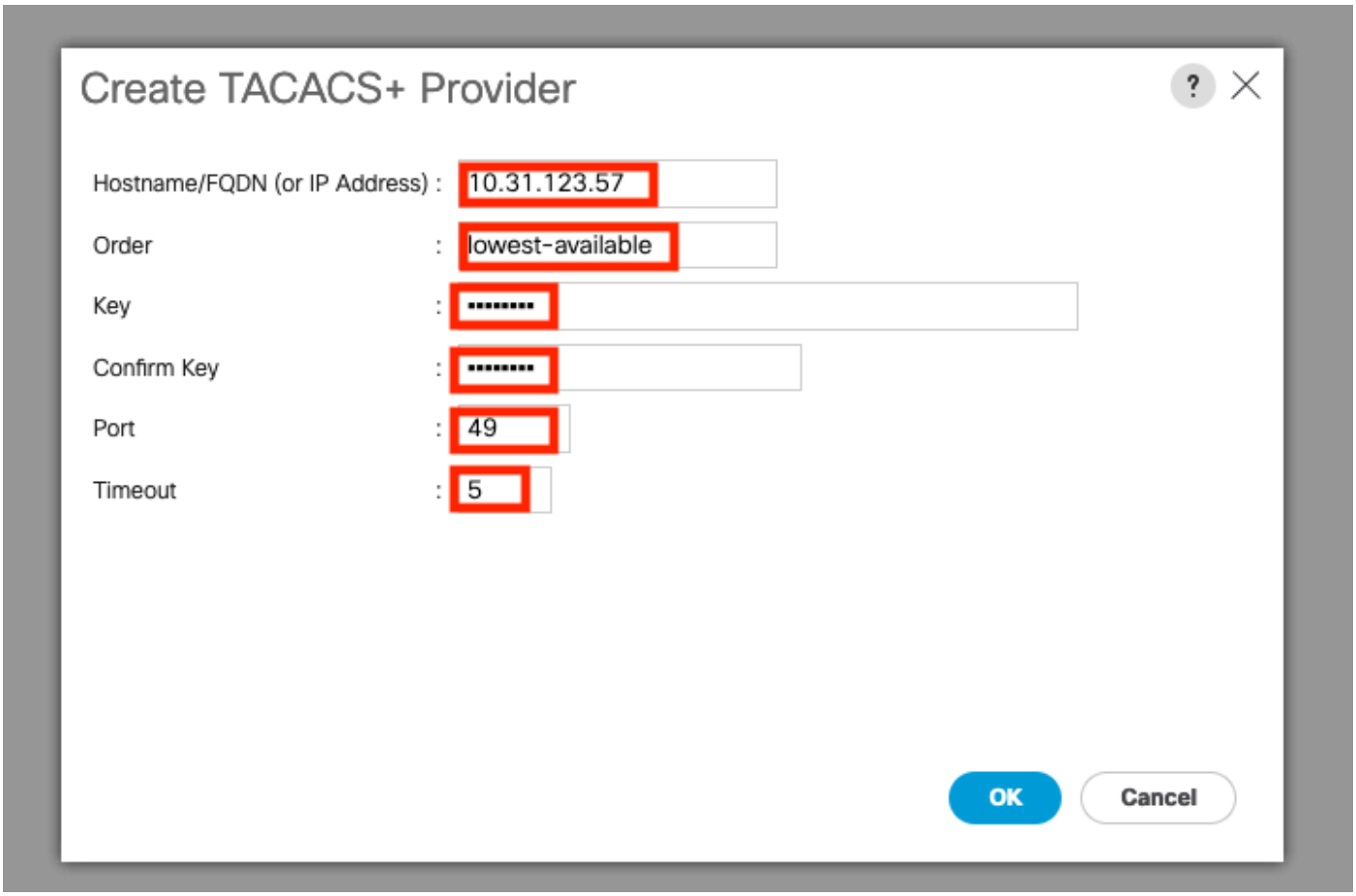
5단계. 마법사**Create TACACS+ Provider**에서 적절한 정보를 입력합니다.

- Hostname(호스트 이름) 필드에 TACACS+ 서버의 IP 주소 또는 호스트 이름을 입력합니다.
- Cisco UCS에서 사용자를 인증하는 데 이 공급자를 사용하는 순서입니다.

  Cisco UCS가 이 Cisco UCS 인스턴스에 정의된 다른 공급자를 기준으로 다음 사용 가능한 주문을 할당하도록 하려면 1에서 16 사이의 정수를 입력하거나, 최저 가용성 또는 0(영)을 입력

합니다.

- Key(키) 필드에서 데이터베이스에 대한 SSL 암호화 키입니다.
- Confirm Key 필드에서 SSL 암호화 키가 확인을 위해 반복됩니다.
- Port(포트) 필드에서 Cisco UCS가 TACACS+ 데이터베이스와 통신하는 데 사용되는 포트(포트 49 기본 포트).
- Timeout 필드에서는 시간 초과되기 전에 시스템이 TACACS+ 데이터베이스에 연결을 시도하는 데 보낸 시간(초)입니다.



6단계. 확인을 선택합니다.

참고: IP 주소가 아닌 호스트 이름을 사용하는 경우 Cisco UCS Manager에서 DNS 서버를 구성해야 합니다.

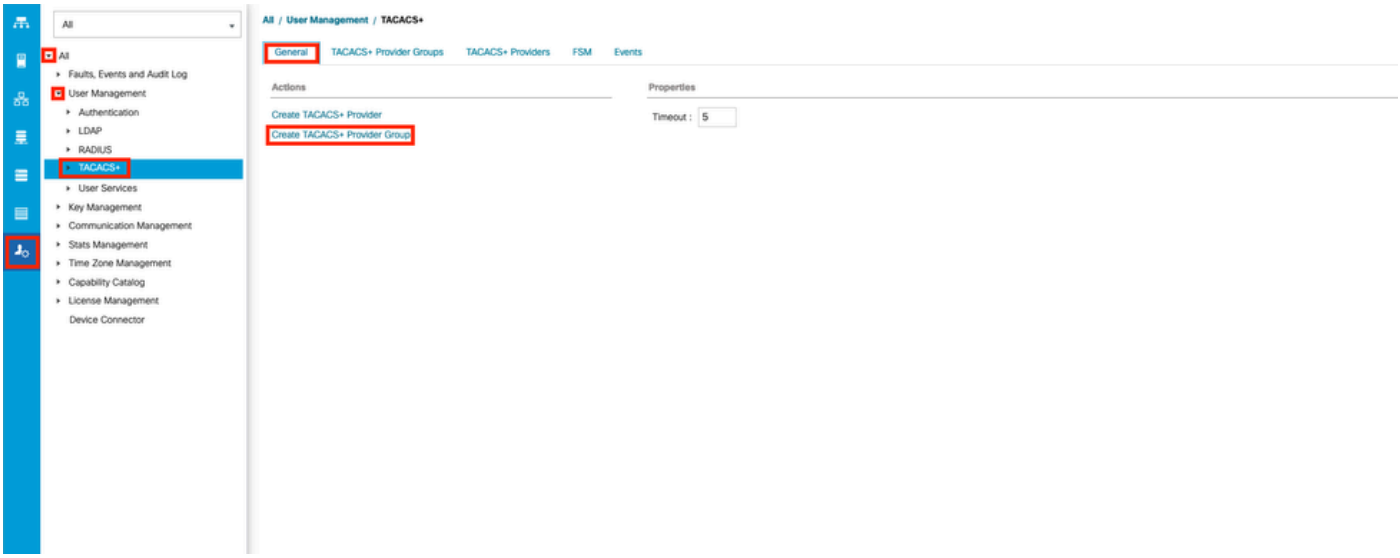
TACAC+ 제공 기관 그룹 생성

1단계.창**Navigation**에서 탭을 **Admin** 선택합니다.

2단계. 탭**Admin**에서 를 확장합니다**All** > **User Management** > **TACACS+**.

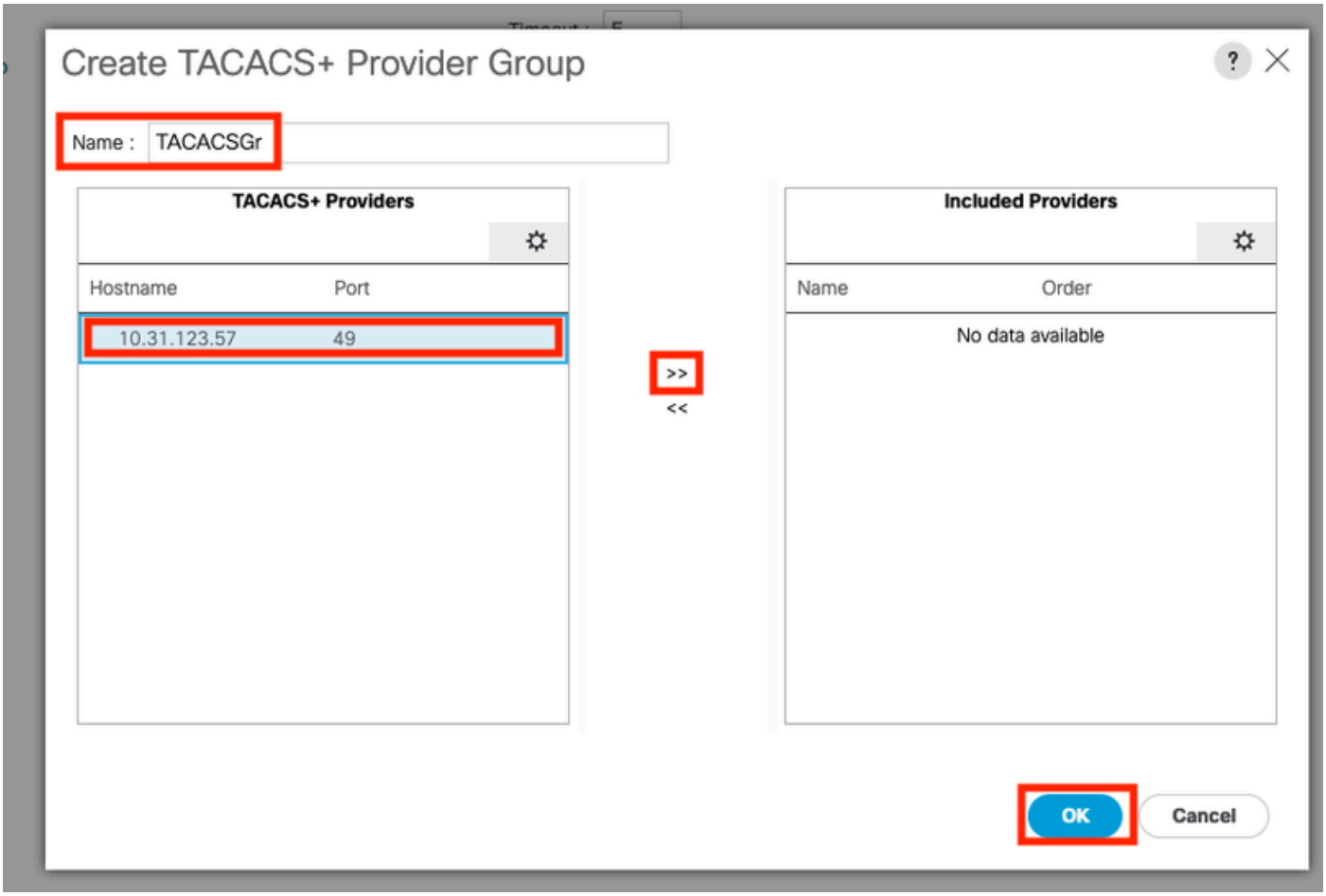
3단계. 창**Work**에서 탭을 **General** 선택합니다.

4단계. 영역에서**Actions**그룹을 Create TACACS+ Provider선택합니다.



5단계. Create TACACS+ Provider Group(TACACS+ 제공자 그룹 생성) 대화 상자에서 요청한 정보를 입력합니다.

- Name(이름) 필드에 그룹의 고유한 이름을 입력합니다.
- TACACS+ Providers(TACACS+ 제공자) 테이블에서 그룹에 포함할 제공자를 선택합니다.
- 제공자를 >> 버튼을 선택하여 포함된 제공자 테이블에 추가합니다.



6단계. 확인을 선택합니다.

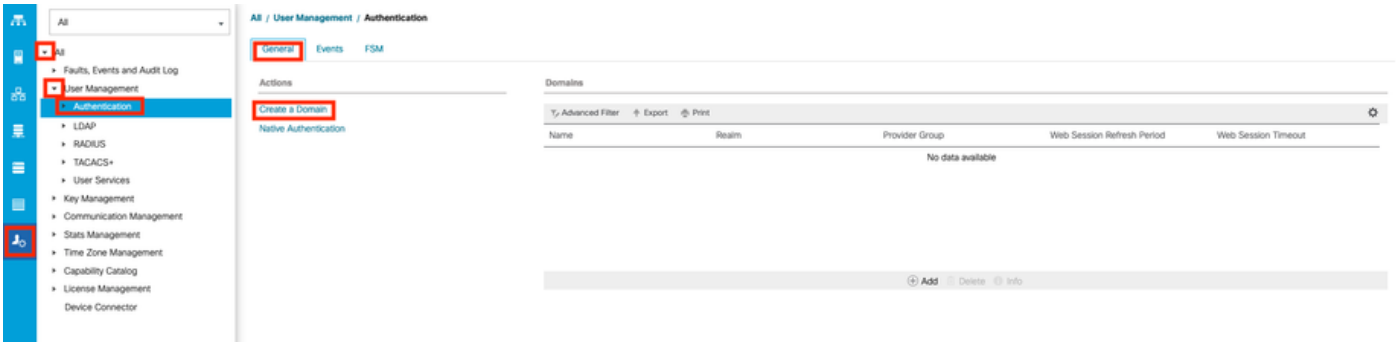
인증 도메인 생성

1단계. 창에서 **Navigation** 탭을 **Admin** 선택합니다.

2단계. 탭에서 **Admin** 다음을 확장합니다. **All** > **User Management** > **Authentication**

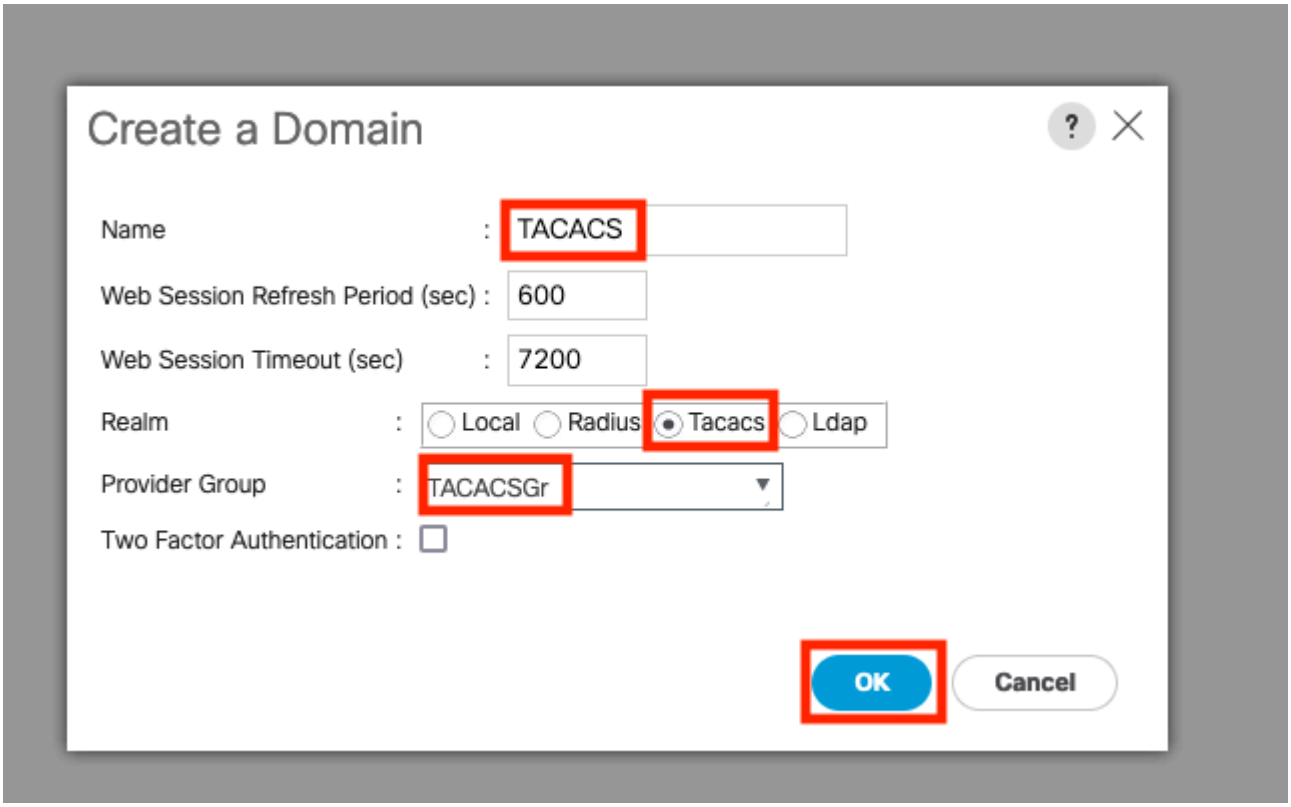
3단계. 창**Work**에서 탭을 **General** 선택합니다.

4단계. 영역에서**Actions**다음을 선택합니다.**Create a Domain.**



5단계. Create Domain(도메인 생성) 대화 상자에 요청한 정보를 입력합니다.

- Name(이름) 필드에 도메인의 고유한 이름을 입력합니다.
- Realm에서 Tacacs 옵션을 선택합니다.
- Provider Group 드롭다운 목록에서 이전에 생성한 TACACS+ 제공자 그룹을 선택하고 OK를 선택합니다



문제 해결

UCSM의 일반적인 TACACS+ 문제

- 잘못된 키 또는 잘못된 문자입니다.
- 잘못된 포트.
- 방화벽 또는 프록시 규칙으로 인해 공급자와 통신하지 않습니다.
- FSM은 100%가 아닙니다.

UCSM TACACS+ 컨피그레이션 확인:

UCSM에서 FSM(Finite State Machine)의 상태를 확인하는 컨피그레이션이 100% 완료로 표시되었는지 확인해야 합니다.

UCSM 명령줄에서 컨피그레이션을 확인합니다

<#root>

UCS-A#

scope security

UCS-A /security #

scope tacacs

UCS-A /security/tacacs #

show configuration

```
UCS-AS-MXC-P25-02-A# scope security
UCS-AS-MXC-P25-02-A /security # scope tacacs
UCS-AS-MXC-P25-02-A /security/tacacs # show configuration
 scope tacacs
     enter auth-server-group TACACSGr
         enter server-ref 10.31.123.57
             set order 1
         exit
     exit
     enter server 10.31.123.57
         set order 1
         set port 49
         set timeout 5
 !       set key
     exit
     set timeout 5
 exit
```

<#root>

UCS-A /security/tacacs #

show fsm status

```
[UCS-AS-MXC-P25-02-A /security/tacacs # show fsm status

    FSM 1:
        Status: Nop
        Previous Status: Update Ep Success
        Timestamp: 2023-06-24T20:54:05.021
        Try: 0
        Progress (%): 100
        Current Task:
```

NXOS에서 Tacacs 컨피그레이션을 확인합니다.

<#root>

UCS-A#

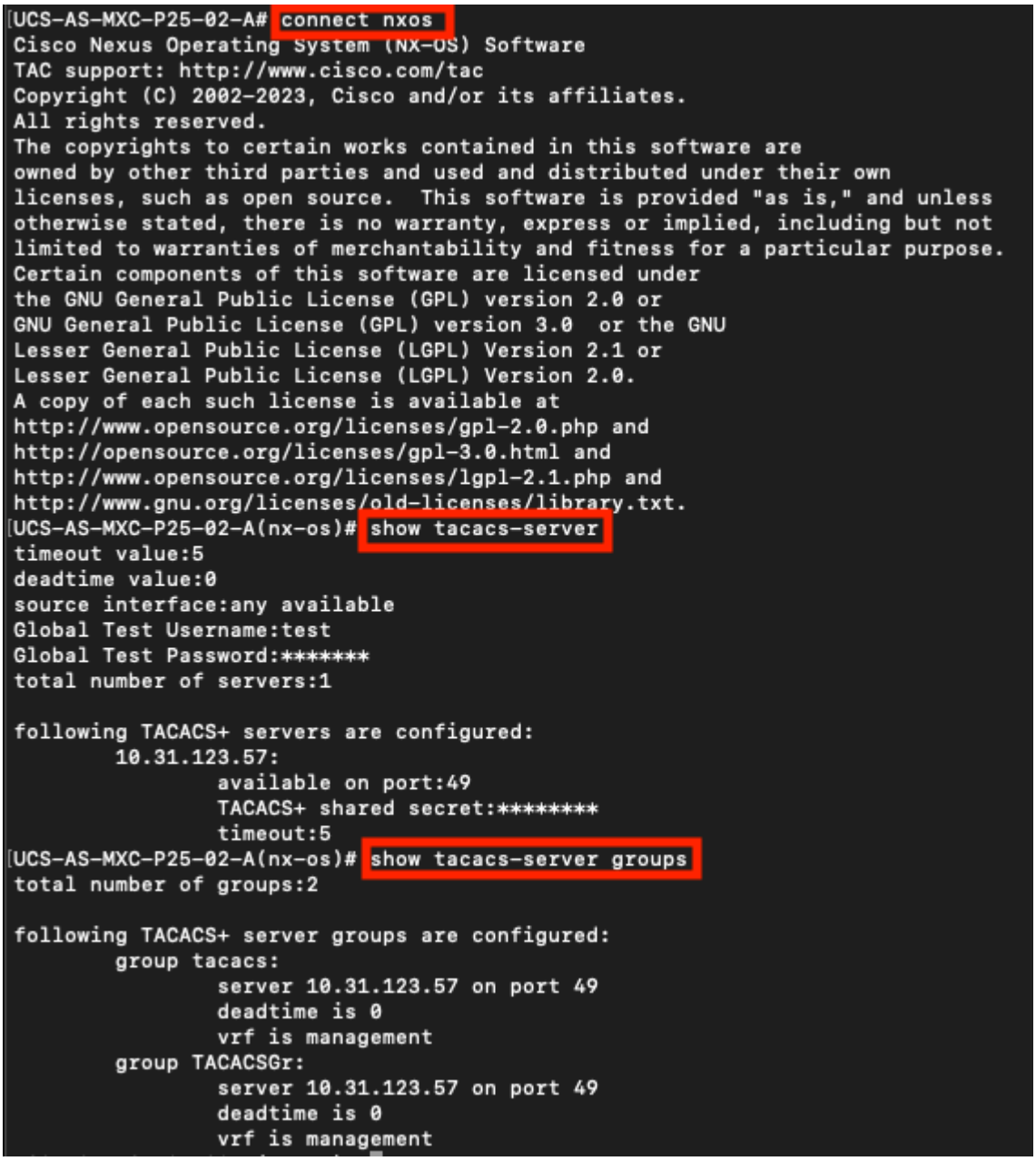
connect nxos

UCS-A(nx-os)#

show tacacs-server

UCS-A(nx-os)#

show tacacs-server groups



NX-OS에서 인증을 테스트하려면 명령을 사용합니다(**test aaa**NXOS에서만 사용 가능).

서버의 구성을 확인합니다.

<#root>

UCS-A(nx-os)#

test aaa server tacacs+

<TACACS+-server-IP-address or FQDN> <username> <password>

```
UCS-AS-MXC-P25-02-A# connect nxos
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2023, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their own
licenses, such as open source.  This software is provided "as is," and unless
otherwise stated, there is no warranty, express or implied, including but not
limited to warranties of merchantability and fitness for a particular purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0  or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.
UCS-AS-MXC-P25-02-A(nx-os)# test aaa server tacacs+ 10.31.123.57 operator Cisc0123
```

UCSM 검토

연결 가능성 확인

<#root>

UCS-A#

connect local-mgmt

UCS-A(local-mgmt)#

ping

 <TACACS+-server-IP-address or FQDN>

```
UCS-AS-MXC-P25-02-A# connect local-mgmt
pCisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2009, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php

UCS-AS-MXC-P25-02-A(local-mgmt)# ping 10.31.123.57
PING 10.31.123.57 (10.31.123.57) from 10.31.123.8 : 56(84) bytes of data.
64 bytes from 10.31.123.57: icmp_seq=1 ttl=64 time=0.347 ms
64 bytes from 10.31.123.57: icmp_seq=2 ttl=64 time=0.309 ms
```

포트 확인

<#root>

UCS-A#

connect local-mgmt

UCS-A(local-mgmt)#

telnet

<TACACS+-server-IP-address or FQDN> <Port>

```
UCS-AS-MXC-P25-02-A# connect local-mgmt
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2009, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php

UCS-AS-MXC-P25-02-A(local-mgmt)# telnet 10.31.123.57 49
Trying 10.31.123.57...
Connected to 10.31.123.57.
Escape character is '^]'.
```

오류를 확인하는 가장 효과적인 방법은 NXOS 디버그를 활성화하는 것입니다. 이 출력으로 그룹, 연결 및 잘못된 통신을 유발하는 오류 메시지를 볼 수 있습니다.

- UCSM에 대한 SSH 세션을 열고 관리자 권한이 있는 권한이 있는 모든 사용자(로컬 사용자 권장)와 로그인하고 NX-OS CLI 컨텍스트로 변경한 다음 터미널 모니터를 시작합니다.

<#root>

UCS-A#

connect nxos

UCS-A(nx-os)#

terminal monitor

- 디버그 플래그를 활성화하고 로그 파일에 대한 SSH 세션 출력을 확인합니다.

<#root>

UCS-A(nx-os)#

debug aaa all

UCS-A(nx-os)#

```
debug aaa aaa-request

UCS-A(nx-os)#
debug tacacs+ aaa-request

UCS-A(nx-os)#
debug tacacs+ aaa-request-lowlevel

UCS-A(nx-os)#
debug tacacs+ all
```

```
UCS-AS-MXC-P25-02-A# connect nxos
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2023, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their own
licenses, such as open source.  This software is provided "as is," and unless
otherwise stated, there is no warranty, express or implied, including but not
limited to warranties of merchantability and fitness for a particular purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0  or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.
UCS-AS-MXC-P25-02-A(nx-os)# terminal monitor
UCS-AS-MXC-P25-02-A(nx-os)# debug tacacs+ all
2023 Jun 26 04:42:22.104286 tacacs: event_loop(): calling process_rd_fd_set
2023 Jun 26 04:42:22.104311 tacacs: process_rd_fd_set: calling callback for fd 6
2023 Jun 26 04:42:22.104341 tacacs: fsrv didnt consume 182 opcode
2023 Jun 26 04:42:22.104994 tacacs: mts_message_handler: sdwrap_process_msg
2023 Jun 26 04:42:22.105011 tacacs: process_rd_fd_set: callback returned for fd 6
UCS-AS-MXC-P25-02-A(nx-os)# debug aaa all
```

- 이제 새 GUI 또는 CLI 세션을 열고 원격 사용자(TACACS+)로 로그인을 시도합니다.
- 로그인 실패 메시지가 표시되면 세션을 닫거나 이 명령을 사용하여 디버그를 끕니다.

```
UCS-A(nx-os)# undebug all
```

ISE의 일반적인 TACAC 문제

- ISE에서 이 동작은 UCSM이 admin 또는 기타 역할에 해당하는 역할을 할당하는 데 필요한 특성에서 tacacs 프로필을 구성하는 동안 표시되며, save(저장) 버튼을 선택하면 이 동작이 표시됩니다.

이 오류는 다음 버그 때문에 발생합니다. https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwc91917, 이 결함이 해결된 위치를 확인하십시오.

ISE 검토

1단계. TACACS+ 서비스 가용성이 실행 중인지 검토합니다. 다음을 체크 인할 수 있습니다.

- GUI: Administration > System > Deployment에서 서비스 DEVICE ADMIN과 함께 나열된 노드가 있는지 검토합니다.
- CLI: show ports 명령을 실행합니다 | TACACS+에 속하는 TCP 포트에 연결이 있는지 확인하려면 49를 포함합니다.

<#root>

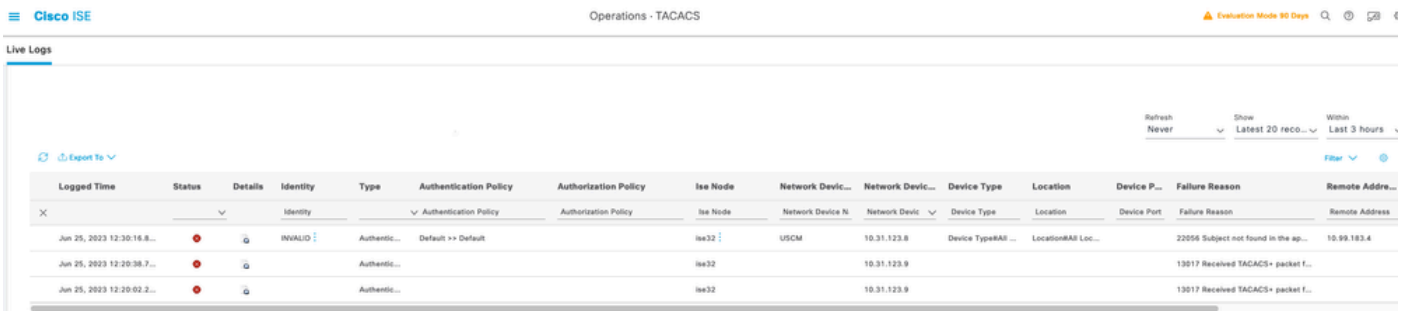
```
ise32/admin#
```

show ports | include 49

```
tcp: 169.254.4.1:49, 169.254.2.1:49, 169.254.4.1:49, 10.31.123.57:49
```

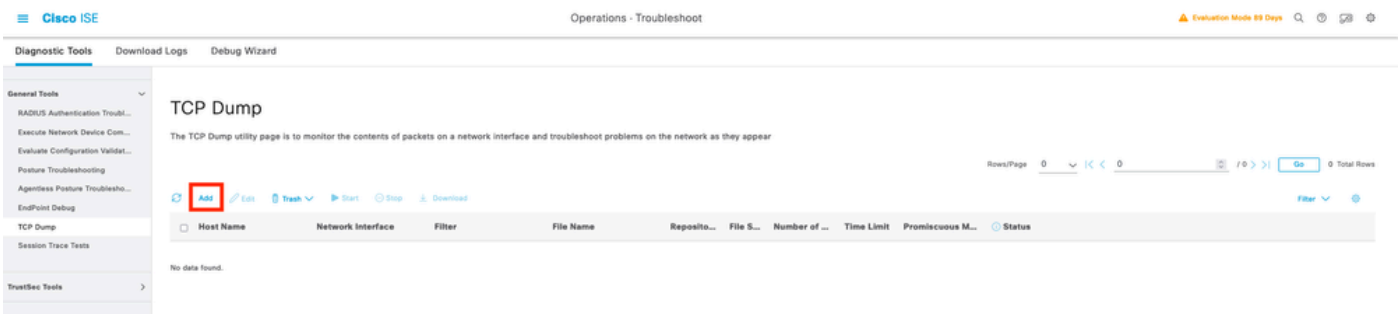
2단계. TACACS+ 인증 시도와 관련된 livelogs가 있는지 확인합니다. 이는 Operations(작업) > TACACS > Live logs(라이브 로그) 메뉴에서 확인할 수 있습니다.

실패 사유에 따라 컨피그레이션을 조정하거나 실패 원인을 해결할 수 있습니다.

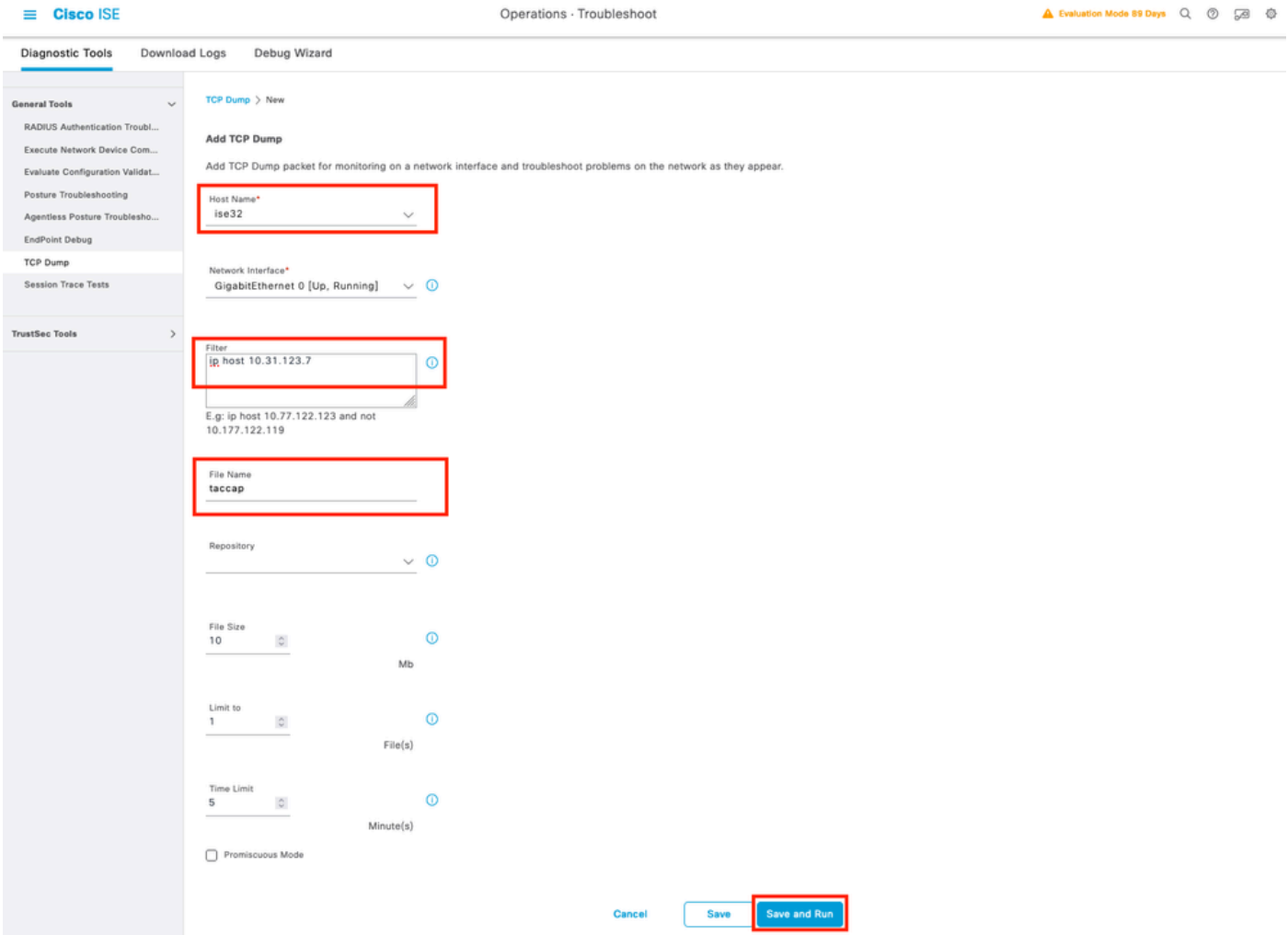


3단계. 라이브로그가 표시되지 않는 경우 패킷 캡처를 진행하려면 Operations(운영) > Troubleshoot(문제 해결) > Diagnostic Tools(진단 도구) > General Tools(일반 도구) > TCP

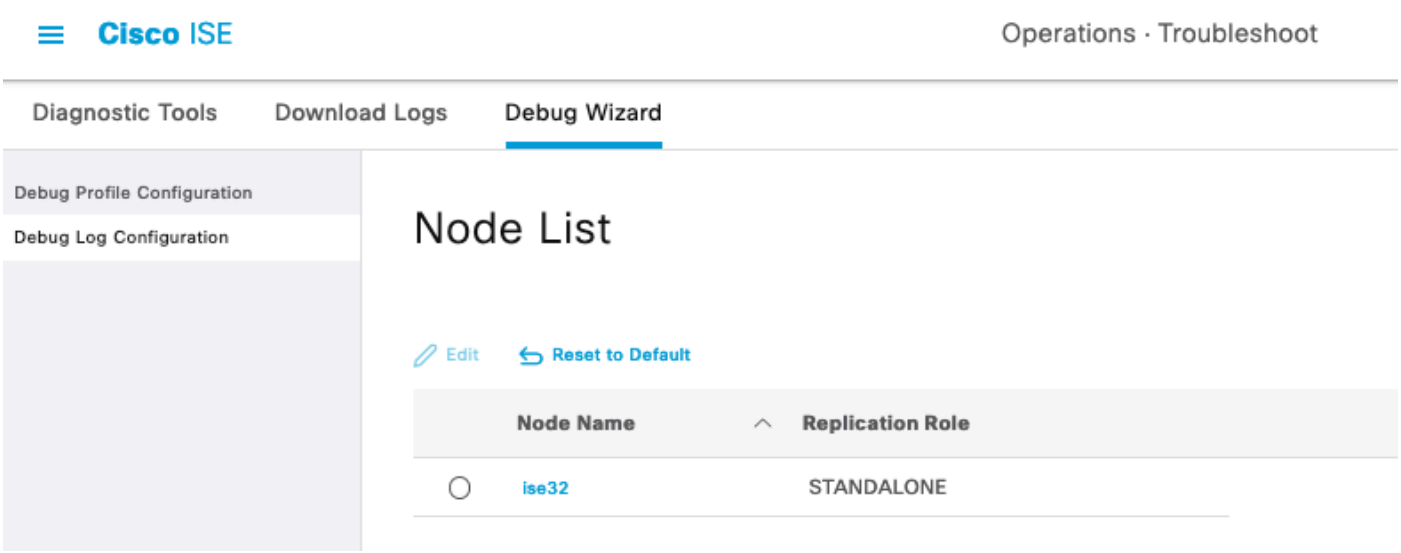
Dump(TCP 덤프) 메뉴로 이동합니다.



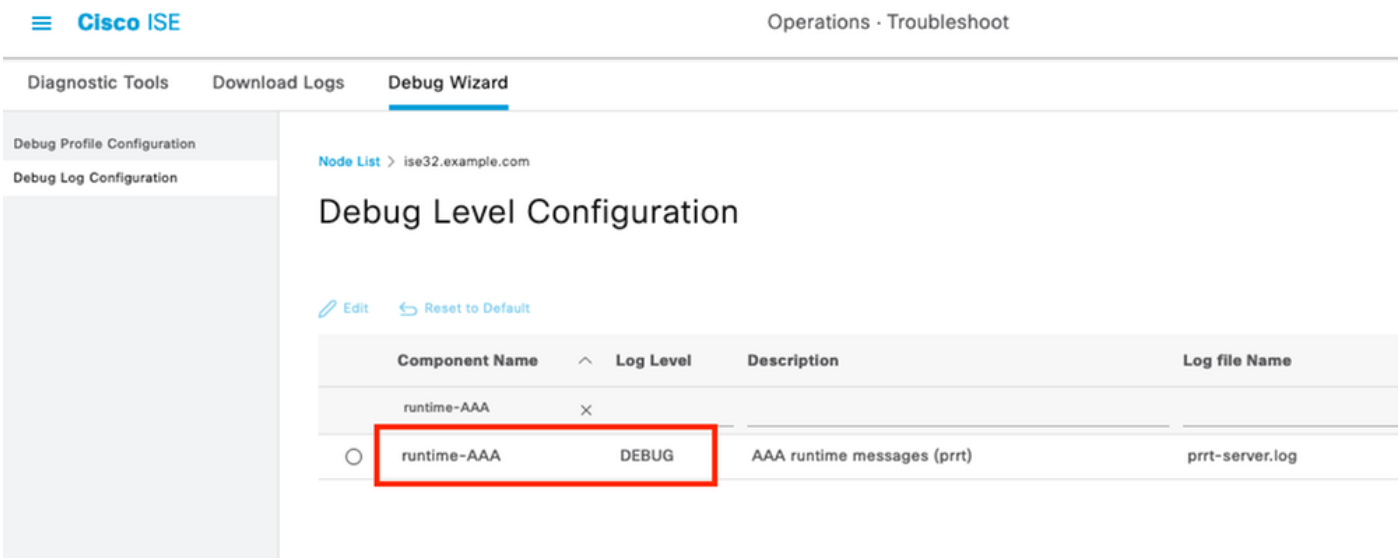
UCSM에서 인증을 보내는 정책 서비스 노드를 선택한 다음 필터에서 인증이 전송되는 UCSM의 IP에 해당하는 ip 호스트 X.X.X.X를 입력하고 캡처 이름을 지정한 다음 아래로 스크롤하여 저장하고 , 캡처를 실행한 다음 UCSM에서 로그인합니다.



4단계. Operations(운영) > Troubleshoot(문제 해결) > Debug Wizard(디버그 마법사) > Debug log configuration(디버그 로그 컨피그레이션)에서 인증이 수행되는 PSN 내의 디버그에서 구성 요소 runtime-AAA를 활성화하고, PSN 노드를 선택한 후 edit(편집) 버튼에서 next(다음)를 선택합니다.



런타임 AAA 구성 요소를 찾아 그 수준을 debug로 변경하여 문제를 다시 재현하고 로그 분석을 진행합니다.



참고: 자세한 내용은 Cisco Youtube 채널 How to Enable Debugs on ISE 3.x Versions https://www.youtube.com/watch?v=E3USz8B76c8의 비디오를 참조하십시오.

관련 정보

Cisco UCS Manager 관리 가이드

Cisco UCS CIMC 컨피그레이션 가이드 TACACS+

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.