Cisco ASA용 ISE TACACS+ 컨피그레이션 가이드

보안 액세스 방법 사용자 시리즈

작성자: Cisco Systems의 보안 비즈니스 그룹, 정책 및 액세스, 기술 마케팅 팀

날짜: 2016년 2월

목차

가이드 정보 4

개요 4

가이드 사용 4

사용되는 구성 요소 4

디바이스 관리를 위한 ISE 컨피그레이션 5

ISE에서의 라이센싱 디바이스 관리 5

ISE에서의 디바이스 관리 활성화 5

디바이스 관리 작업 센터 7

네트워크 디바이스 및 네트워크 디바이스 그룹 7

ID 저장소 9

TACACS 프로파일 10

ASA 모니터링 전용 11

ASA 읽기 전용 12

ASA 관리 12

TACACS 명령 집합 13

HelpDesk 명령 13

Permit All 명령 14

ASA Basic 14

ASA ReadOnly Extra 15

디바이스 관리 정책 집합 15

ASDM Authz 16

ASA Regular 17

TACACS+를 위한 ASA 컨피그레이션 20

TACACS+ 인증 및 대체 21

명령 권한 부여 22

EXEC 권한 부여 22
로컬 명령 권한 부여 22
ASDM에서 정의된 사용자 역할 22
TACACS+ 명령어 권한 부여 24
TACACS+ 계정 관리 25
다음 단계는 무엇인가요? 26

가이드 정보

개요

TACACS+(Terminal Access Controller Access Control System Plus)는 라우터 및 다른 여러 유형의 네트워크 액세스 디바이스에 대한 관리 액세스를 중앙 집중식으로 보안 제어할 수 있는 클라이언트 서버 프로토콜입니다. TACACS+는 다음의 AAA 서비스를 제공합니다.

- 인증 – 사용자는 누구인가
- 권한 부여 – 사용자는 어떤 작업을 수행할 수 있는가
- 계정 관리 – 누가 무엇을, 언제 수행했는가

이 문서는 Cisco ISE(Identity Services Engine)를 TACACS+ 서버로 사용하고 Cisco ASA(Adaptive Security Appliance)를 TACACS+ 클라이언트로 사용하는 TACACS+ 컨피그레이션에 대한 예시를 제공합니다.

가이드 사용

이 가이드에서는 ISE를 Cisco ASA에 대한 관리 액세스를 관리하도록 활성화하기 위한 작업을 2개의 파트로 나누어 설명합니다.

- 파트 1 – 디바이스 관리를 위한 ISE 구성
- 파트 2 – TACACS+를 위한 Cisco ASA 구성

사용되는 구성 요소

이 문서의 정보는 아래의 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- ISE VMware 가상 어플라이언스, 릴리스 2.0
- Cisco ASAv(Adaptive Security Virtual Appliance), Cisco ASA 소프트웨어 버전 9.5(2) 및 ASDM(Adaptive Security Device Manager) 버전 7.5(2)
- Oracle Java™ SE Runtime Environment, build 1.7.0_40-b43

이 문서의 내용은 랩 환경의 디바이스를 토대로 작성되었습니다. 여기에 포함된 모든 디바이스는 초기화된(기본) 컨피그레이션에서 시작합니다.

디바이스 관리를 위한 ISE 컨피그레이션

ISE에서의 라이센싱 디바이스 관리

디바이스 관리(TACACS+)는 설치를 기준으로 라이센스가 부여되지만 여기에는 기존의 유효한 ISE Base 또는 Mobility 라이센스가 필요합니다.

ISE에서의 디바이스 관리 활성화

디바이스 관리 서비스(TACACS+)는 ISE 노드에서 기본적으로 활성화되지 않습니다. 첫 번째 단계는 이 서비스를 활성화하는 것입니다.

1 단계 지원되는 브라우저 중 하나를 사용하여 ISE 관리 웹 포털에 로그인합니다.

2 단계 **Administration(관리) > System(시스템) > Deployment(설치)**로 이동합니다. ISE 노드 옆에 있는 확인란을 선택하고 **Edit(수정)**를 클릭합니다.

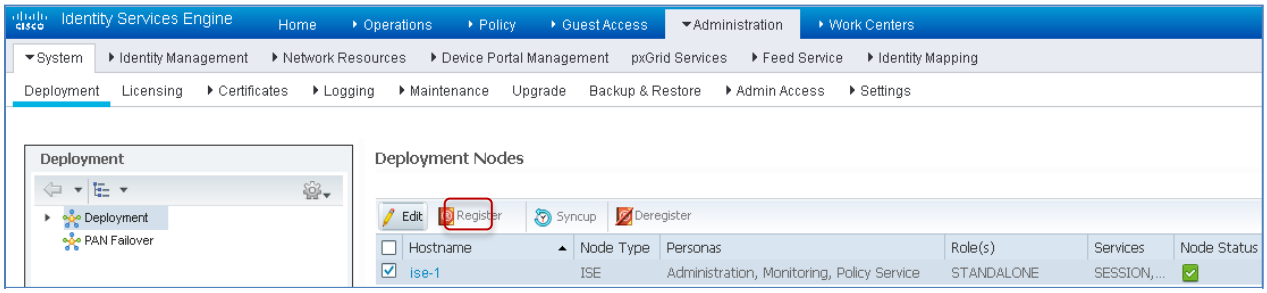

그림 1. ISE 설치 페이지

3 단계 **General Settings(일반 설정)**에서 아래로 스크롤하여 **Enable Device Admin Service(디바이스 관리 서비스 활성화)** 옆에 있는 확인란을 선택합니다.

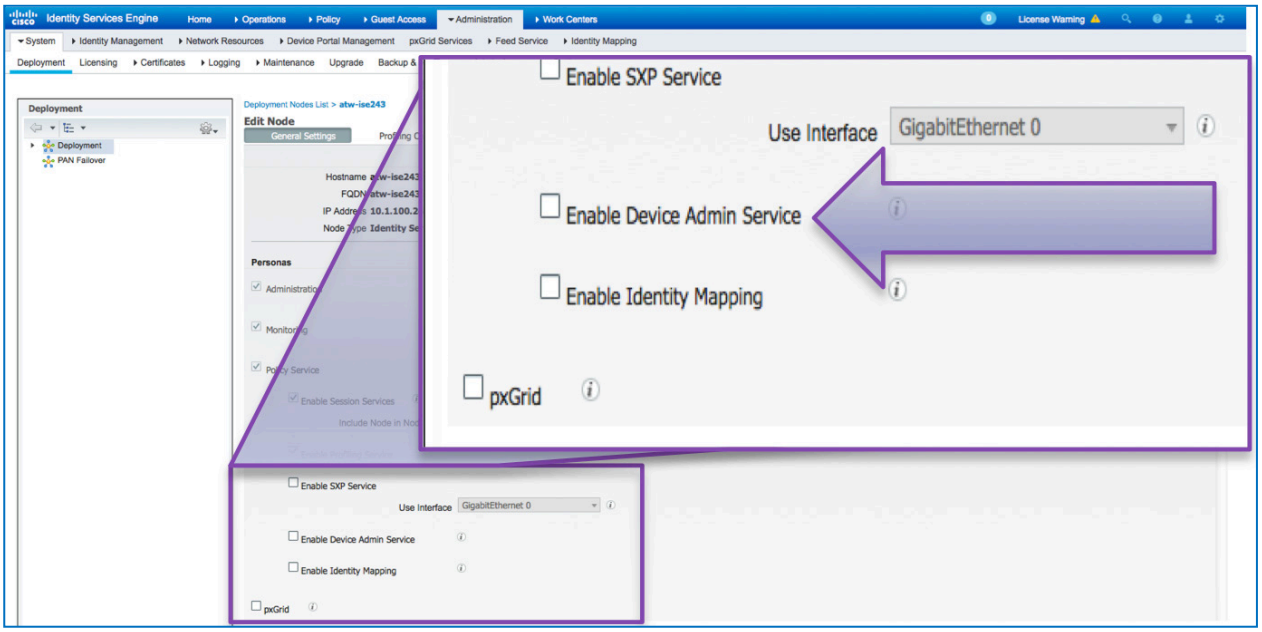

그림 2. ISE 설치 일반 설정

4 단계 컨피그레이션을 **저장**합니다. 이제 디바이스 관리 서비스가 ISE 에서 활성화됩니다.

디바이스 관리 작업 센터

ISE 2.0에서는 작업 센터마다 특정 기능에 대한 모든 요소를 포함하는 작업 센터가 도입되었습니다.

1 단계 **Work Centers(작업 센터) > Device Administration(디바이스 관리) > Overview(개요)**로 이동합니다.

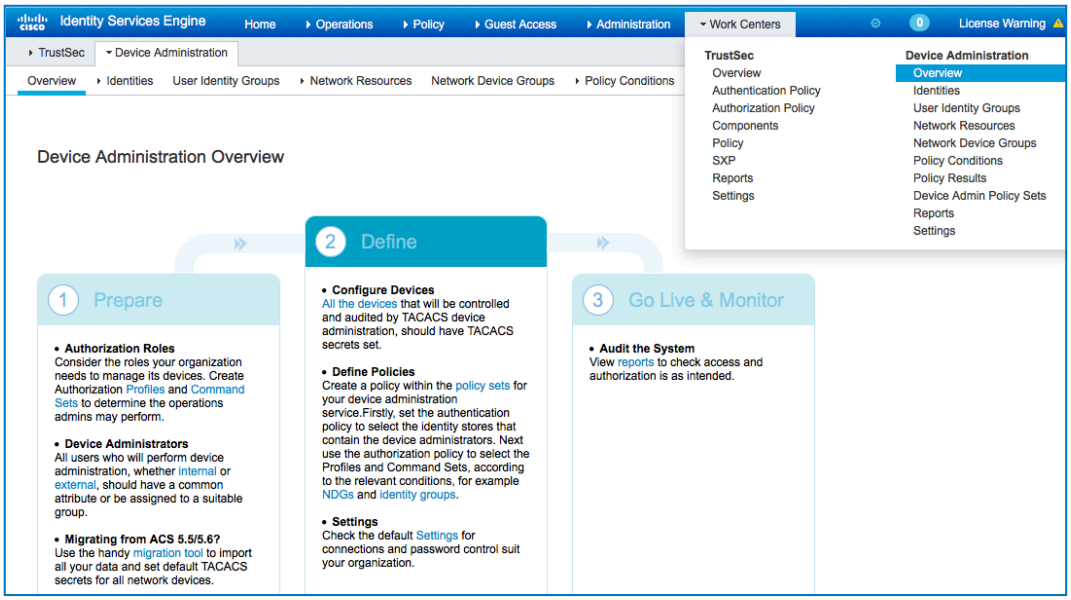

그림 3. 디바이스 관리 개요

디바이스 관리 개요에서는 디바이스 관리 활용 사례에 필요한 단계를 상세하게 설명합니다.

네트워크 디바이스 및 네트워크 디바이스 그룹

ISE는 여러 디바이스 그룹 계층으로 분류되는 강력한 디바이스를 제공합니다. 각 계층 구조는 네트워크 디바이스를 개별적이면서 독립적으로 분류한 것을 나타냅니다.

1 단계 **Work Centers(작업 센터) > Device Administration(디바이스 관리) > Network Device Groups(네트워크 디바이스 그룹)**로 이동합니다.

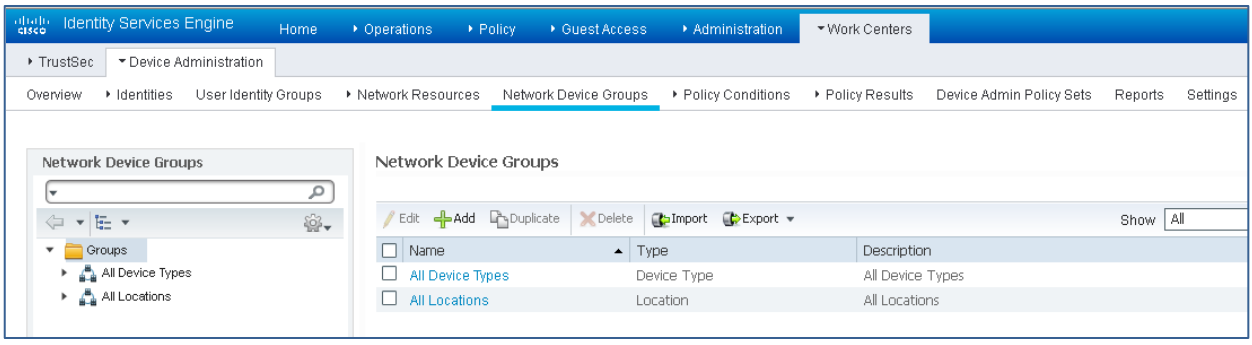

그림 4. 네트워크 디바이스 그룹

모든 디바이스 유형과 모든 위치는 ISE에서 제공하는 기본 계층 구조입니다. 향후 정책 조건에 사용할 수 있는 네트워크 디바이스를 식별할 때 고유한 계층 구조를 추가하고 다양한 구성 요소를 정의할 수 있습니다.

2 단계 계층 구조를 정의하면 네트워크 디바이스 그룹이 다음과 유사하게 나타납니다.

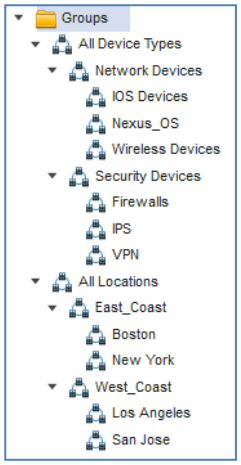

그림 5. 네트워크 디바이스 그룹 트리 보기

3 단계 이제, ASAv 를 네트워크 디바이스로 추가합니다. **Work Centers(작업 센터) > Device Administration(디바이스 관리) > Network Resources(네트워크 리소스)**로 이동합니다. 새 네트워크 디바이스 **DMZ_BLDO_ASAv** 를 추가하려면 **+Add(추가)**를 클릭합니다.

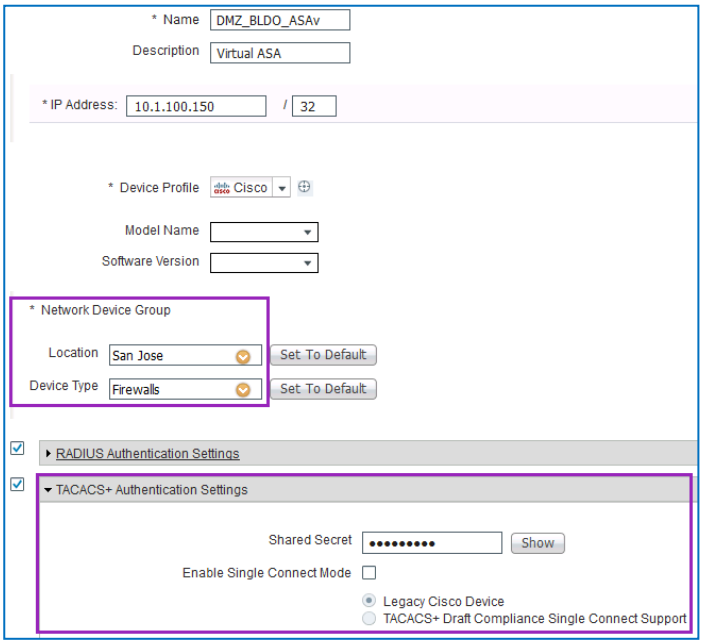

그림 6. 네트워크 디바이스 추가

디바이스의 IP 주소를 입력하고 디바이스의 위치와 디바이스 유형을 매핑합니다. 마지막으로, **TACACS+ Authentication Settings(TACACS+ 인증 설정)**를 활성화하고 공유 암호를 지정합니다.

ID 저장소

이 섹션에서는 디바이스 관리자의 ID 저장소를 정의합니다. 디바이스 관리자는 ISE 내부 사용자 및 지원되는 모든 외부 ID 소스가 될 수 있습니다. 여기에서는 외부 ID 소스 중 하나인 AD(Active Directory)를 사용합니다.

1 단계 **Administration(관리) > Identity Management(ID 관리) > External Identity Stores(외부 ID Active Directory)**로 이동합니다. 새 AD 조인 지점을 정의하려면 **Add(추가)**를 클릭합니다. 조인 지점 이름 및 AD 도메인 이름을 지정하고 **Submit(제출)**을 클릭합니다.

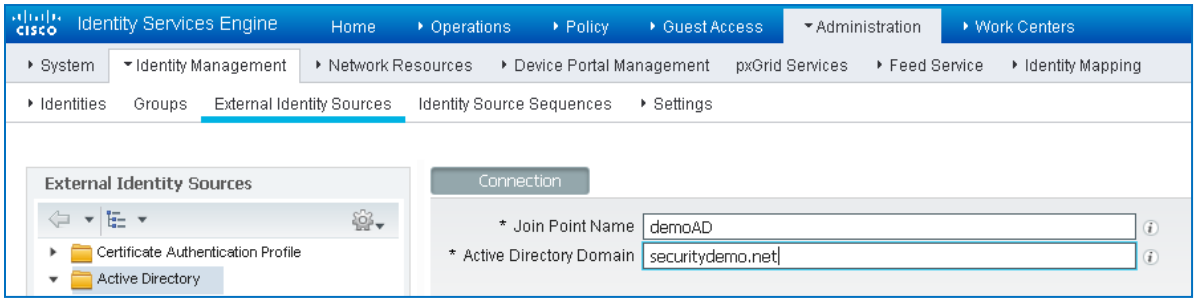

그림 7. AD 조인 지점 추가

2 단계 "모든 ISE 노드를 이 Active Directory 도메인에 조인하시겠습니까?"라는 프롬프트가 표시되면 **Yes(예)**를 클릭합니다. AD 조인 권한이 있는 크리덴셜을 입력하고 ISE 를 AD 에 **조인**합니다. 작동되는지 확인하기 위해 Status(상태)를 확인합니다.

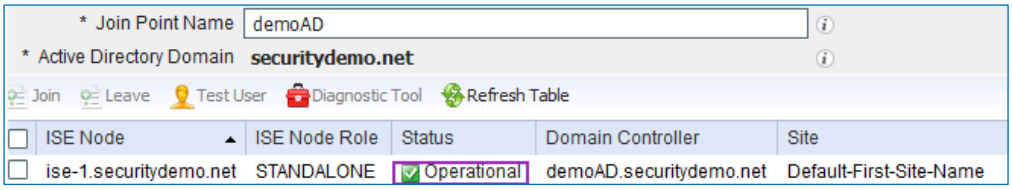

그림 8. AD에 ISE 조인

3 단계 **Groups(그룹)** 탭으로 이동하고 디바이스 액세스 권한이 있는 사용자에 따라 필요한 모든 그룹을 가져오려면 **Add(추가)**를 클릭합니다. 다음 예는 이 가이드의 권한 부여 정책에 사용된 그룹을 보여줍니다.

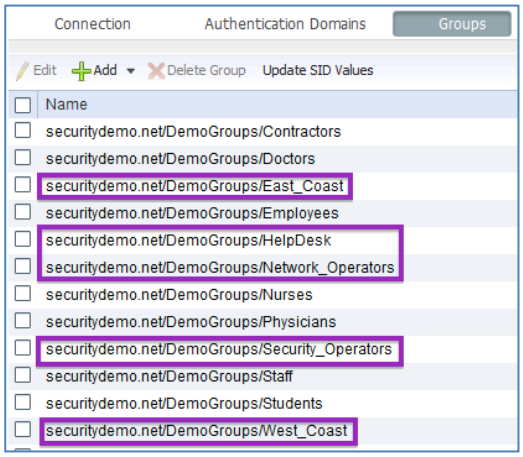

그림 9. AD 그룹

TACACS 프로파일

Cisco ASA는 명령 권한 부여를 위해 16가지 레벨로 구성된 액세스 권한을 제공합니다. 다음 3가지 레벨은 기본으로 정의되어 있습니다.

권한 레벨 0 – *show checksum, show curpriv, show history, show version, enable, help, login, logout, pager, show pager, clear pager* 및 *quit* 명령 허용 로그인 이후 최소 액세스 가능 레벨이 1이므로 이 레벨 0의 모든 명령은 모든 사용자가 사용할 수 있습니다.

권한 레벨 1 – 권한이 없는 모드 또는 사용자 EXEC 모드는 로그인한 사용자의 기본 권한 레벨입니다. 셸 프롬프트는 디바이스 이름 뒤에 꺾쇠괄호가 옵니다(예: “ciscoasa>”).

권한 레벨 15 – 권한 EXEC 모드는 enable 명령 다음의 권한 레벨입니다. 셸 프롬프트는 디바이스 호스트 이름 뒤에 우물 정(#) 기호가 옵니다(예: “ciscoasa#”).

기본적으로 ASA의 모든 명령의 권한 레벨은 0, 1 또는 15입니다. ASDM 역할 기반 제어는 3가지의 ASDM 사용자 역할(레벨 15(관리), 레벨 5(읽기 전용) 및 레벨 3(모니터링 전용))을 사전 정의합니다. 여기서는 이러한 역할을 ISE 정책에 사용하며 이후에 ASDM이 정의된 사용자 역할에서 설정합니다.

EXEC 권한 부여의 경우 ASA 디바이스는 사용자가 셸(EXEC) 세션을 시작할 수 있는지를 확인하기 위해 인증이 끝난 직후에 TACACS+ 권한 부여 요청을 AAA 서버로 전송합니다. ISE는 사용자별로 특성을 맞춤화하기 위해 다음의 2가지 특성을 푸시할 수 있습니다.

기본 권한: 셸 세션에 대해 최초(기본) 권한 레벨을 지정합니다. 권한이 부여된 사용자는 레벨 1 대신 이 레벨을 획득합니다.

최대 권한: 해당 셸 세션에 허용된 최대 레벨을 지정합니다. 권한이 부여된 사용자는 더 낮은 기본 레벨로 로그인하고 enable 명령을 사용하여 이 특성에서 할당된 더 높은 레벨의 최대값으로 이동할 수 있습니다. 외부 AAA 서버의 경우, ASA는 값 15만 사용하도록 허용합니다.

ASA 모니터링 전용

이 기능은 ASDM에서 사용자 권한을 홈 및 모니터링 창으로 제한하기 위한 것입니다.

1 단계 ISE 관리 웹 포털에서 **Work Centers(작업 센터) > Device Administration(디바이스 관리) > Policy Results(정책 결과) > TACACS Profiles(TACACS 프로파일)**로 이동합니다. 새로운 TACACS 프로파일 추가하고 이름을 **ASA Monitor Only** 로 지정합니다.

2 단계 아래로 스크롤하여 **Common Tasks(공통 작업)** 섹션으로 이동합니다. 드롭다운 선택기에서 값 3 을 선택하여 기본 권한을 활성화하고 드롭다운에서 값 4 를 선택하여 최대 권한을 활성화합니다.

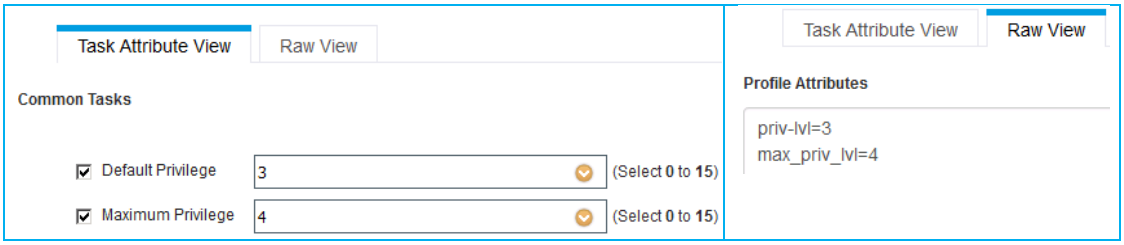

그림 10. ASA 모니터링 전용 TACACS 프로파일

값이 4인 최대 권한은 예시를 위한 것으로 여기서는 사용되지 않습니다. 그 이유는 외부 AAA 서버를 사용할 때만 ASA에 대해 값 15가 허용되기 때문입니다.

3 단계 프로파일을 저장하려면 **Submit(제출)**을 클릭합니다.

ASA 읽기 전용

이 기능은 ASDM에서 사용자에게 읽기 전용 액세스 권한을 제공하기 위한 것입니다.

4 단계 새로운 TACACS 프로파일 추가하고 이름을 **ASA Read Only** 로 지정합니다.

5 단계 아래로 스크롤하여 **Common Tasks(공통 작업)** 섹션으로 이동합니다. 드롭다운 선택기에서 값 5 를 선택하여 기본 권한을 활성화하고 드롭다운에서 값 7 을 선택하여 최대 권한을 활성화합니다.

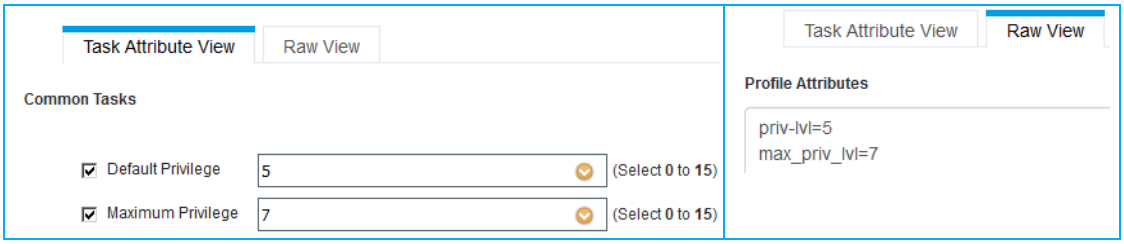

그림 11. ASA 읽기 전용 TACACS 프로파일

값이 7인 최대 권한은 예시를 위한 것으로 여기서는 사용되지 않습니다. 그 이유는 외부 AAA 서버를 사용할 때만 ASA에 대해 값 15가 허용되기 때문입니다.

6 단계 프로파일을 저장하려면 **Submit(제출)**을 클릭합니다.

ASA 관리

이 기능은 ASDM에서 무제한 액세스 권한을 제공하기 위한 것입니다.

7 단계 다른 프로파일을 추가하고 이름을 **ASA Admin** 으로 지정합니다.

8 단계 아래로 스크롤하여 **Common Tasks(공통 작업)** 섹션으로 이동합니다. 드롭다운 선택기에서 값 15 를 선택하여 기본 권한을 활성화하고 드롭다운에서 값 15 를 선택하여 최대 권한을 활성화합니다.

그림 12. ASA 관리용 TACACS 프로파일

최대 권한 값인 15는 사용자가 사용자 EXEC 모드에서 “enable”을 실행할 때 ASA CLI에서 사용됩니다.

9 단계 프로파일을 저장하려면 **Submit(제출)**을 클릭합니다.

TACACS 명령 집합

ASA 명령 권한 부여는 권한 레벨과 관계없이 디바이스 관리자가 명령을 실행할 권한을 부여받았는지 여부를 확인하기 위해 구성된 TACACS+ 서버를 쿼리합니다.

여기서는 HelpDesk_Commands, Permit_All_Commands, ASA Basic 및 ASA_ReadOnly_Extra의 4가지 명령 집합을 정의합니다.

HelpDesk 명령

이 명령은 IOS 디바이스용 설명서에 있는 명령과 동일합니다. 명령이 이미 정의되어 있는 경우 이 섹션을 건너뜁니다.

1 단계 ISE GUI 에서 **Work Centers(작업 센터) > Device Administration(디바이스 관리) > Policy Results(정책 결과) > TACACS Command Sets(TACACS 명령 집합)**로 이동합니다. 새로운 집합을 추가하고 이름을 **HelpDesk_Commands** 로 지정합니다.

2 단계 해당 집합에 항목을 구성하려면 **+Add(추가)**를 클릭합니다.

권한 부여	명령어	인수
허용	debug	
허용	undebug	
허용	traceroute	
거부	ping	^([0-9]{1,3})\.([0-9]{1,3})\.([0-9]{1,3})\.255$
허용	ping	
허용	show	

여기서는 HelpDesk 분석가가 debug, undebug, traceroute 및 show를 수행할 수 있습니다. Ping의 경우, 브로드캐스트 Ping이 제한되며, 인수 열에 있는 정규식에 보이는 것과 같이 브로드캐스트 주소가 있는 네트워크 서브넷이 255로 끝난다고 가정합니다.

3 단계 행을 유지하려면 각 항목 끝에 있는 확인 표시인 √를 클릭합니다.

4 단계 명령 집합을 그대로 유지하려면 **Submit(제출)**을 클릭합니다.

Permit All 명령

이 명령은 IOS 디바이스용 설명서에 있는 명령과 동일합니다. 명령이 이미 정의되어 있는 경우 이 섹션을 건너뜁니다.

5 단계 새로운 집합을 추가하고 이름을 **Permit_All_Commands** 로 지정합니다.

6 단계 **Permit any command that is not listed below ☑**(아래에 나열되지 않은 모든 명령 허용) 옆에 있는 확인란을 선택하고 명령 목록을 비워둡니다.

권한 부여	명령어	인수

7 단계 명령 집합을 그대로 유지하려면 **Submit(제출)**을 클릭합니다.

ASA Basic

8 단계 새로운 집합을 추가하고 이름을 **ASA Basic** 으로 지정합니다.

9 단계 해당 집합에 항목을 구성하려면 **+Add(추가)**를 클릭합니다.

권한 부여	명령어	인수
허용	show	`checksum|curpriv|history|pager|version`
허용	enable	
허용	help	
허용	login	
허용	logout	
허용	pager	
허용	clear	`pager`
허용	quit	
허용	exit	

첫 번째 항목은 **show** 명령 다음에 오는 허용 가능한 인수의 목록을 보여줍니다. 이 항목은 `show checksum`, `show curpriv`, `show history`, `show pager` 및 `show version` 중 하나와 일치합니다.

10 단계 행을 유지하려면 각 항목 끝에 있는 확인 표시인 **√**를 클릭합니다.

11 단계 명령 집합을 그대로 유지하려면 **Submit(제출)**을 클릭합니다.

ASA ReadOnly Extra

12 단계 새로운 집합을 추가하고 이름을 **ASA ReadOnly Extra** 로 지정합니다.

13 단계 해당 집합에 항목을 구성하려면 **+Add(추가)**를 클릭합니다.

권한 부여	명령어	인수
허용	more	
허용	dir	
허용	export	

14 단계 행을 유지하려면 각 항목 끝에 있는 확인 표시인 √를 클릭합니다.

15 단계 명령 집합을 그대로 유지하려면 **Submit(제출)**을 클릭합니다.

디바이스 관리 정책 집합

정책 집합은 디바이스 관리에 대해 기본적으로 활성화됩니다. 정책 집합은 TACACS 프로파일을 쉽게 적용할 수 있도록 디바이스 유형에 기반하여 정책을 구분할 수 있습니다. 예를 들어, Cisco ASA 디바이스는 권한 레벨 및/또는 명령 집합을 사용하는 반면, WLC 디바이스는 맞춤형 특성을 사용합니다.

ASDM은 메뉴 및 기타 그래픽 사용자 인터페이스 요소로 조작하므로 ASDM 액세스는 ASA CLI에 비해 허용되는 명령이 더 많이 필요합니다.

여기서는 2개의 정책 집합을 정의합니다. 하나는 ASDM 액세스 권한 부여를 위한 정책 집합이며 나머지 하나는 ASA 관리 액세스를 위한 정책 집합입니다.

ASDM Authz

1 단계 **Work Centers(작업 센터) > Device Administration(디바이스 관리) > Device Admin Policy Sets(디바이스 관리 정책 설정)**로 이동합니다. 새 정책 집합 ASDM Authz 를 추가합니다.

S	이름	설명	조건
√	ASDM Authz		DEVICE:Device Type EQUALS Device Type#All Device Types#Network Devices#Firewalls AND TACACS:Type EQUALS Authorization AND TACACS:Port EQUALS 443

그림 13. ASDM Authz에 대한 정책 집합 조건

ASDM 권한 부여 요청은 기본 HTTPS 포트를 사용할 때 TACACS 포트 번호 443을 통해 전송됩니다. ASDM에서 대체 포트를 사용하는 경우 이 조건의 값을 맞춤형 포트로 업데이트합니다.

2 단계 인증 정책을 생성합니다. 인증의 경우 AD 를 ID 저장소로 사용하며 권한 부여 요청에서 사용자 이름을 식별할 때도 사용됩니다.

인증 정책	
√	기본 규칙(일치하는 항목이 없는 경우) : 프로토콜 허용 : 기본 디바이스 관리 및 사용: demoAD

그림 14. ASDM Authz에 대한 인증 정책

3 단계 권한 부여 정책을 정의합니다. ASDM 액세스는 3 개의 사전 정의된 권한 레벨을 사용하여 제어되므로 간소화하기 위해 모든 인증된 관리자에게 Permit_All_Commands 를 제공합니다.

S	규칙 이름	조건	명령 집합	셸 프로파일
√	HelpDesk West	DEVICE:Location CONTAINS All Locations#West_Coast AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/West_Coast AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/HelpDesk	Permit_All_Commands	ASA 모니터링 전용
√	HelpDesk East	DEVICE:Location CONTAINS All Locations#East_Coast AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/East_Coast AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/HelpDesk	Permit_All_Commands	ASA 모니터링 전용

S	규칙 이름	조건	명령 집합	셸 프로파일
√	Security West	DEVICE:Location CONTAINS All Locations#West_Coast AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/West_Coast AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/Security_Operators	Permit_All_Commands	ASA 관리
√	Security East	DEVICE:Location CONTAINS All Locations#East_Coast AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/East_Coast AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/Security_Operators	Permit_All_Commands	ASA 관리
√	Admin West	DEVICE:Location CONTAINS All Locations#West_Coast AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/West_Coast AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/Network_Operators	Permit_All_Commands	ASA 읽기 전용
√	Admin East	DEVICE:Location CONTAINS All Locations#East_Coast AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/East_Coast AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/Network_Operators	Permit_All_Commands	ASA 읽기 전용
√	기본	일치하는 항목이 없는 경우	DenyAllCommands	

그림 15. ASDM Authz에 대한 권한 부여 정책

ASA Regular

4 단계 **Work Centers(작업 센터) > Device Administration(디바이스 관리) > Device Admin Policy Sets(디바이스 관리 정책 설정)**로 이동합니다. 기존 정책 집합인 ***ASDM Authz*** 를 선택하고 [아래에 복제]합니다. 새 정책 집합이 이전 정책 집합보다 등급이 낮기 때문에 조건이 덜 세분화될 수 있습니다. 중복 사본을 업데이트하고 아래와 같이 디바이스 유형에 대해서만 조건을 설정합니다.

S	이름	설명	조건
√	ASA Regular		DEVICE:Device Type EQUALS Device Type#All Device Types#Network Devices#Firewalls

그림 16. ASA Regular에 대한 정책 집합 조건

5 단계 인증 정책을 생성합니다. 인증 시 AD 를 ID 저장소로 사용합니다.

인증 정책
√ 기본 규칙(일치하는 항목이 없는 경우) : 프로토콜 허용 : 기본 디바이스 관리 및 사용: demoAD

그림 17. ASA Regular에 대한 인증 정책

6 단계 권한 부여 정책을 정의합니다. 여기서는 AD 의 사용자 그룹과 디바이스 위치를 기반으로 권한 부여 정책을 정의합니다. 예를 들어, AD 그룹 West Coast 사용자는 West Coast 에 위치한 디바이스에만 액세스할 수 있습니다. ASA. 셸 프로파일은 ASA 에서 로컬 명령 권한 부여를 사용하는 ASA CLI 및 ASDM 액세스에 주로 사용됩니다.

S	규칙 이름	조건	명령 집합	셸 프로파일
√	HelpDesk West	DEVICE:Location CONTAINS All Locations#West_Coast AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/West_Coast AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/HelpDesk	ASA_Basic AND HelpDesk_Commands	ASA 모니터링 전용
√	HelpDesk East	DEVICE:Location CONTAINS All Locations#East_Coast AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/East_Coast AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/HelpDesk	ASA_Basic AND HelpDesk_Commands	ASA 모니터링 전용
√	Security West	DEVICE:Location CONTAINS All Locations#West_Coast AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/West_Coast AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/Security_Operators	Permit_All_Commands	ASA 관리

S	규칙 이름	조건	명령 집합	셸 프로파일
√	Security East	DEVICE:Location CONTAINS All Locations#East_Coast AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/East_Coast AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/Security_Operators	Permit_All_Commands	ASA 관리
√	Admin West	DEVICE:Location CONTAINS All Locations#West_Coast AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/West_Coast AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/Network_Operators	ASA_Basic AND HelpDesk_Commands AND ASA_ReadOnly_Commands	ASA 읽기 전용
√	Admin East	DEVICE:Location CONTAINS All Locations#East_Coast AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/East_Coast AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/Network_Operators	ASA_Basic AND HelpDesk_Commands AND ASA_ReadOnly_Commands	ASA 읽기 전용
√	기본	일치하는 항목이 없는 경우	DenyAllCommands	

그림 18. ASA Regular에 대한 권한 부여 정책

이제 ASA 디바이스의 디바이스 관리를 위한 ISE 컨피그레이션을 마쳤습니다.

TACACS+를 위한 ASA 컨피그레이션

TACACS+를 구성하기 전에 IP 주소 지정 및 적절한 원격 연결 프로토콜을 먼저 구성해야 합니다. 다음은 ASA CLI 액세스를 위해 SSH를 활성화하고 ASDM 액세스를 위해 HTTP를 활성화하는 방법에 대한 예시입니다.

```
hostname ASAv
domain-name securitydemo.net

crypto key generate rsa modulus 2048 noconfirm

console timeout 0

interface Management0/0
 management-only
 nameif management
 security-level 100
 ip address 10.1.100.150 255.255.255.0
 no shutdown

route management 0.0.0.0 0.0.0.0 10.1.100.1 1

ssh 10.1.100.0 255.255.255.0 management
ssh timeout 30
ssh version 2

http server enable
http 10.1.100.0 255.255.255.0 management

username sec-admin password ISEisC00L privilege 15

aaa authentication ssh console LOCAL
aaa authentication enable console LOCAL
aaa authorization exec LOCAL auto-enable
```

이 단계에서 샘플 네트워크 디바이스에 유효한 IP 주소가 있으므로 콘솔 로그인이 인증되지 않은 상태에서 10.1.100.0/24의 클라이언트에서 SSH를 활성화할 수 있습니다. AAA 컨피그레이션 중에 발생할 수 있는 액세스 문제를 방지하려면 콘솔에 대한 EXEC 타임아웃을 비활성화하십시오.

버전 9.5(1)부터 ASA는 관리 전용 인터페이스에 대해 별도의 라우팅 테이블을 가집니다. 여기서는 모든 연결된 서브넷에 없는 파일 서버를 연결하기 위해 기본 경로를 추가합니다.

ASA에서의 활성화 동작을 Cisco IOS와 매우 유사하게 만들기 위해 EXEC 권한 부여를 위한 *auto-enable* 옵션이 ASA 버전 9.2(1)에 추가되었습니다. 그 결과 충분한 권한이 있는 디바이스 관리자는 비밀번호를 두 번 입력할 필요가 없습니다.

ASDM을 사용하려면 ASDM 이진 파일을 ASA의 disk0에 업로드해야 합니다. 예를 들어 다음과 같습니다.

```
copy http://a.web.file.server/path/to/asdm-752.bin disk0:/
```

Cisco ASDM-IDM 시작 관리자가 아직 설치되지 않은 경우 웹 브라우저를 사용하여 https://10.1.100.150/admin 으로 이동하고 [Install ASDM Launcher(ASDM 시작 관리자 설치)] 또는 [Run ASDM(ASDM 실행)]을 클릭합니다. 전역 활성화 비밀번호 없이, 여기서는 ASDM-IDM 시작 관리자가 10.1.100.150을 가리키도록 하고 비어 있는 사용자 이름 및 비밀번호를 사용하거나 로컬 관리자 크리덴셜을 사용하여 로그인합니다.

Cisco ASA 디바이스의 TACACS+ AAA는 다음 순서로 구성될 수 있습니다.

1. TACACS+ 인증 및 대체 활성화
2. TACACS+ 명령 권한 부여 활성화
3. TACACS+ 명령 계정 관리 활성화

TACACS+ 인증 및 대체

TACACS+ 인증은 다음과 유사한 컨피그레이션으로 활성화될 수 있습니다.

```
aaa-server demoTG protocol tacacs+
aaa-server demoTG (management) host 10.1.100.21
 key ISEisC00L

clear configure aaa

aaa authentication ssh console demoTG LOCAL
aaa authentication enable console demoTG LOCAL
aaa authentication http console demoTG LOCAL
aaa authentication secure-http-client
```

따라서 여기서는 SSH 및 ASDM에 대한 액세스를 인증하기 위해 TACACS+로 전환했습니다. SSH용 TACACS+를 사용하여 로그인에 성공한 경우 권한 레벨이 1이며 ASDM 로그인에 성공한 경우에는 권한 레벨이 15입니다.

“enable” 인증 행은 모든 유형의 연결을 위한 것이므로 VTY 및 CONSOLE 모두 “enable” 액세스를 인증하기 위해 TACACS+를 사용합니다. “enable”에 대한 AAA 인증은 인수 없이 수행되며 기본값이 15로 설정되어 있으므로 최대 권한 레벨이 15인 관리자만 “enable”을 성공적으로 실행할 수 있습니다.

구성된 TACSACS+ 서버를 사용할 수 없게 된 경우, 로그인하여 “로컬” 사용자 데이터베이스를 사용하도록 인증 대체를 활성화합니다. 액세스 대체가 허용된 사용자는 투명한 액세스를 위해 자신의 로컬 비밀번호를 외부 AAA 서버와 동기화해야 합니다.

명령 권한 부여

EXEC 권한 부여

EXEC 권한 부여는 특별한 형식의 명령 권한 부여입니다. 이 작업은 사용자가 로그인한 후에 바로 수행되며 다음을 추가하여 활성화할 수 있습니다.

```
aaa authorization exec authentication-server auto-enable
```

앞에서 언급한 것과 같이, ASA 9.2(1)에 **auto-enable**이 추가되었으므로 ASA에서 이전 코드를 실행 중인 경우 이 옵션을 건너뛰십시오. 이 시점에서 ***default*** 권한 특성을 사용하는 셸 프로파일은 새 SSH 세션에 적용됩니다.

9.4(1) 버전부터 ASA는 다른 유형의 연결에서 ASDM에 대한 EXEC 권한을 분리합니다. 따라서 여기서는 다음을 추가합니다.

```
aaa authorization http console demoTG
```

로컬 명령 권한 부여

로컬 명령 권한 부여를 통해 관리자는 자신의 권한 레벨 이하로 할당된 명령을 사용할 수 있습니다. 명령은 다음과 같이 구성됩니다.

```
aaa authorization command LOCAL
```

ASDM에서 정의된 사용자 역할

ASDM에서 정의된 사용자 역할은 ASDM 액세스를 위한 3가지 권한 레벨(3, 5, 15)을 나타냅니다. 이 레벨을 설정하기 위해 ASDM은 3가지 권한 레벨에 명령을 재할당합니다. 이 권한 레벨은 이후 로컬 명령 권한 부여에서 직접 사용되거나 TACACS+ 명령 권한 부여에 대한 대체로 사용됩니다.

전체 액세스가 가능한 ASA 관리자로 ASDM에 로그인하고 **Configuration(컨피그레이션) > Device Management(디바이스 관리) > Users/AAA(사용자 및 AAA) > AAA Access(AAA 액세스) > Authorization(권한 부여)**으로 이동하고 [Set ASDM Defined User Roles...(ASDM에서 정의된 사용자 역할 설정...)] 버튼을 클릭합니다. **ASDM Defined User Roles Setup(ASDM에서 정의된 사용자 역할 설정)** 팝업 창에서 [Yes(예)]를 클릭합니다.

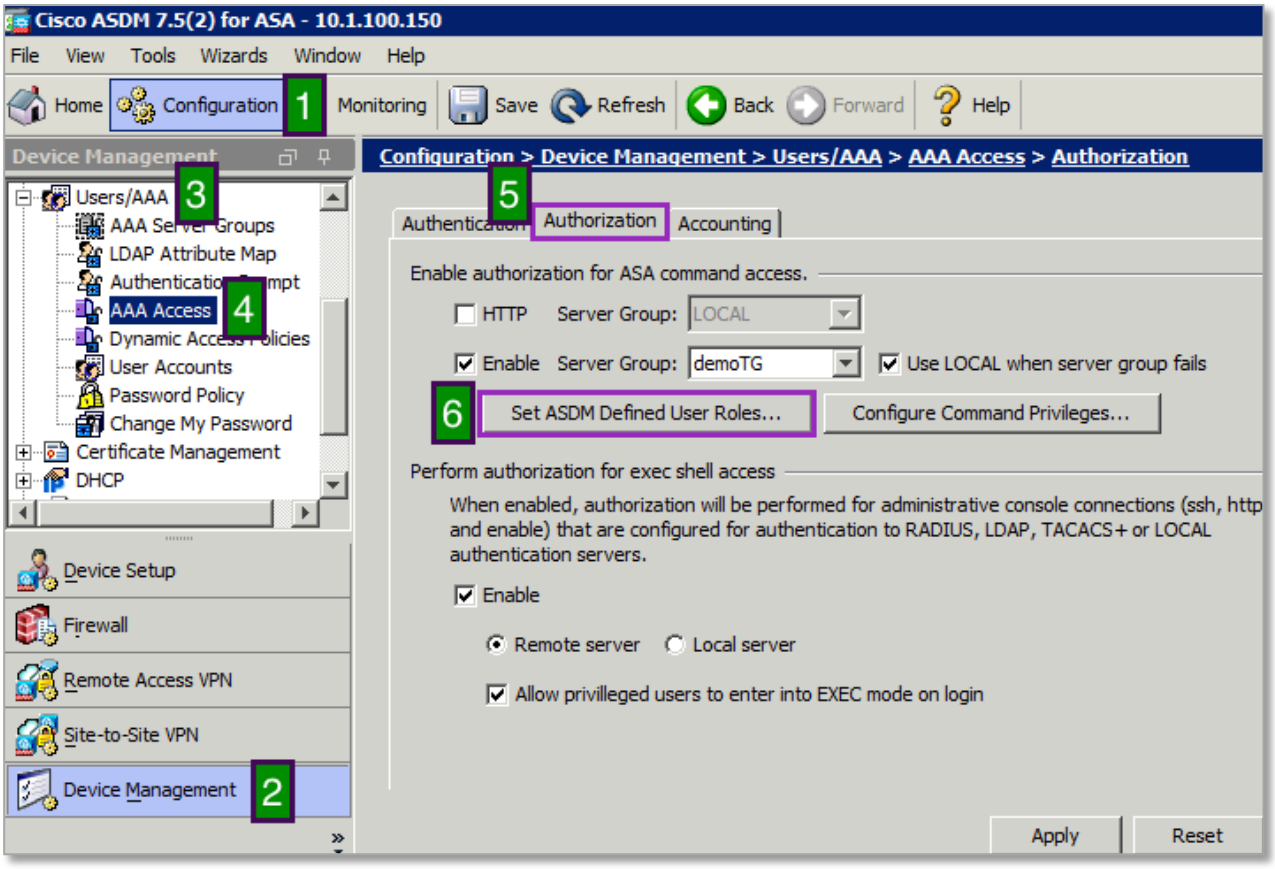

그림 19. ASDM에서 정의된 사용자 역할 설정

구성된 권한 명령 목록을 보기 위해 여기서는 ASDM 기본 설정에서 [☑Preview commands before sending them to the device(명령을 디바이스에 전송하기 전에 미리보기)] 옵션을 설정할 수 있습니다(아래 그림 16 참조). 컨피그레이션을 ASA에 전송하려면 [Apply(적용)]를 누릅니다. 미리 보기 옵션이 활성화된 경우 ***Preview CLI Commands(CLI 명령 미리 보기)*** 팝업 창에서 [Send(전송)]를 클릭합니다.

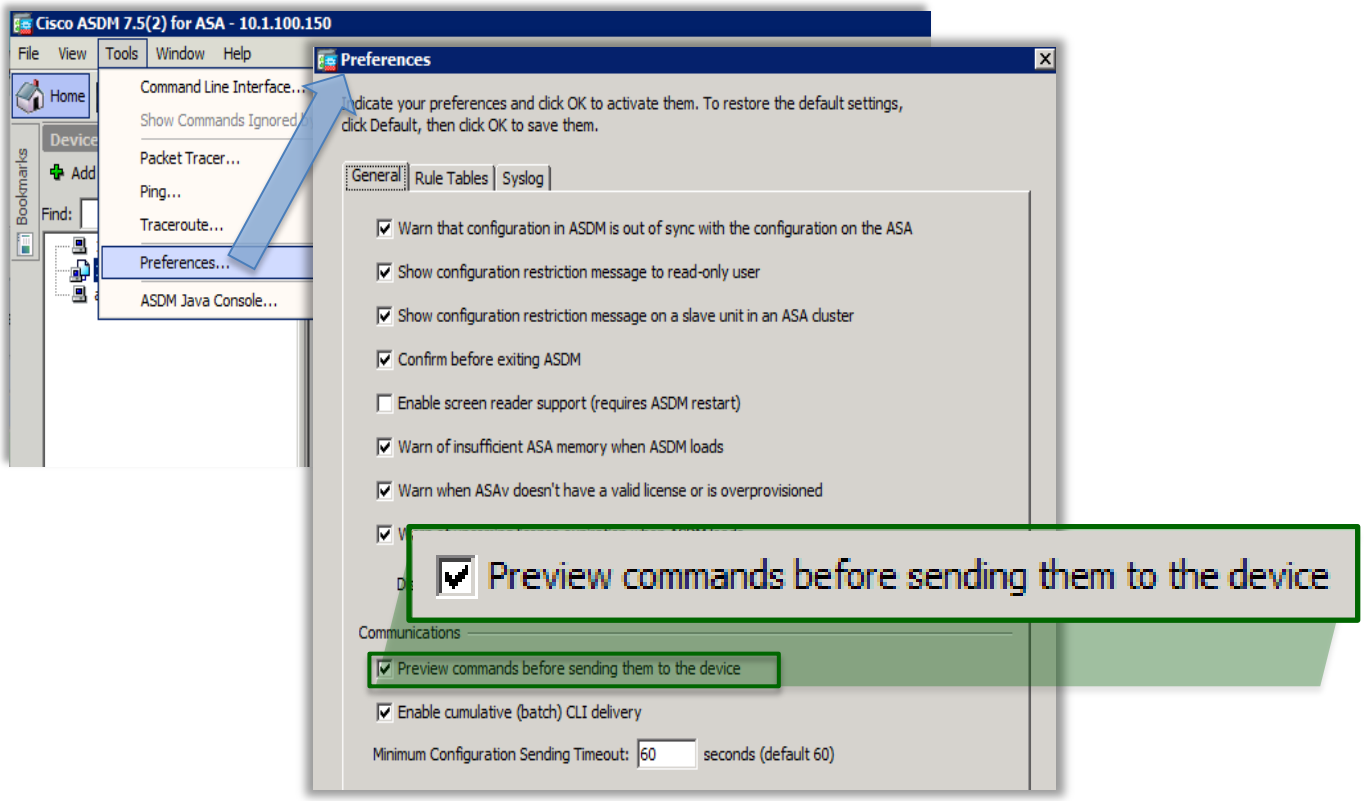

그림 20. ASA로 전송하기 전에 명령을 미리 보기 위한 ASDM 기본 설정

TACACS+ 명령어 권한 부여

TACACS+ 명령 권한 부여를 사용하려면 다음을 구성합니다.

```
aaa authorization command demoTG LOCAL
```

이렇게 하면 각 권한 레벨에 사용 가능한 목록이 재정의되며 TACACS+ 서버의 명령 목록에 관리자의 현재 권한 레벨보다 높은 권한 레벨의 명령을 포함할 수 있습니다.

TACACS+ 계정 관리

ASA는 다음을 사용하여 TACACS+ 서버 그룹에 관리 사용자 활동을 로그하도록 활성화될 수 있습니다.

```
aaa accounting ssh console demoTG
aaa accounting serial console demoTG
aaa accounting enable console demoTG
```

명령 계정 관리는 실행된 각 명령에 대한 정보를 전송하며 이 정보에는 명령, 날짜 및 사용자 이름이 포함됩니다. 다음은 이전 컨피그레이션 예를 추가하여 이 계정 관리 기능을 활성화합니다.

```
aaa accounting command demoTG
```

이 명령은 “show” 명령을 제외한 임의의 명령에 대한 계정 관리 메시지를 전송합니다. 최소 권한 레벨을 지정하려면 선택 사항인 권한 키워드를 사용할 수 있습니다. 예를 들어, “`aaa accounting command privilege 3 demoTG`”는 “show”를 제외하고 레벨이 3 이상인 권한에 대한 명령 계정 관리를 전송합니다.

이제 TACACS+용 ASA 컨피그레이션을 마쳤습니다.

다음 단계는 무엇인가요?

Cisco ASA용 디바이스 관리를 위한 컨피그레이션을 완료했습니다. 이제 컨피그레이션을 검증해야 합니다.

1 단계 SSH 를 활성화하고 다양한 역할로 ASA 디바이스에 로그인합니다.

2 단계 디바이스 CLI(Command Line Interface)에서 한 번 사용자가 적절한 명령에 액세스할 수 있는지 확인합니다. 예를 들어, HelpDesk 사용자는 일반 IP 주소(예 10.1.10.1)를 Ping 할 수 있어야 하지만 브로드캐스트 주소(예 10.1.10.255)의 Ping 은 거부됩니다.

3 단계 사용자 연결을 보려면 다음을 실행합니다.

```
show ssh sessions
show asdm sesssions
show curpriv
```

샘플 출력은 아래와 같습니다.

```
ASAv# show ssh sessions

SID Client IP       Version Mode Encryption Hmac     State            Username
2   10.1.100.6      2.0     IN   aes256-ctr sha1     SessionStarted   hellen
                            OUT  aes256-ctr sha1     SessionStarted   hellen
ASAv# show asdm sessions
0 10.1.100.6
AASAv# show curpriv
Username : hellen
Current privilege level : 3
Current Mode/s : P_PRIV
…
```

4 단계 다음 디버그는 TACACS+ 문제 해결에 유용합니다.

```
debug aaa common
debug tacacs
```

다음은 샘플 디버그 출력입니다.

```
mk_pkt - type: 0x1, session_id: 495
 user: neo
 Tacacs packet sent
Sending TACACS Start message. Session id: 495, seq no:1
Received TACACS packet. Session id:1117437566  seq no:2
tacp_procpkt_authen: GETPASS
mk_pkt - type: 0x1, session_id: 495
mkpkt_continue - response: ***
 Tacacs packet sent
Sending TACACS Continue message. Session id: 495, seq no:3
Received TACACS packet. Session id:1117437566  seq no:4
tacp_procpkt_authen: PASS
TACACS Session finished. Session id: 495, seq no: 3
```

```
mk_pkt - type: 0x2, session_id: 496
mkpkt - authorize user: neo
 Tacacs packet sent
Sending TACACS Authorization message. Session id: 496, seq no:1
Received TACACS packet. Session id:63315798  seq no:2
tacp_procpkt_author: PASS_ADD
tacp_procpkt_author: PASS_REPL
Attributes = priv-lvl
TACACS Session finished. Session id: 496, seq no: 1

mk_pkt - type: 0x2, session_id: 498
mkpkt - authorize user: neo
cmd=ping
cmd-arg=10.1.1.255  Tacacs packet sent
Sending TACACS Authorization message. Session id: 498, seq no:1
Received TACACS packet. Session id:244563180  seq no:2
tacp_procpkt_author: FAIL
TACACS Session finished. Session id: 498, seq no: 1
…
```

5 단계 ISE GUI 에서 **Operations(작업) > TACACS Livelog** 로 이동합니다. 모든 TACACS 인증 및 권한 부여 요청은 여기에서 캡처되며 세부사항 버튼을 누르면 특정 트랜잭션이 통과 및 실패한 원인에 대한 자세한 정보를 확인할 수 있습니다.

Username	Type	Authorization Policy	Device Port	Remote Address	Matched Command Set	Shell Profile
	All					
neo	Authorization	ASA Regular >> NetOps	22	10.1.100.6	HelpDesk Commands	
neo	Authorization	ASA Regular >> NetOps	0	10.1.100.6		ASA Read Only
neo	Authentication		87	10.1.100.6		
sean	Authorization	ASA Regular >> SecOps	22	10.1.100.6	Permit All Commands	
sean	Authorization	ASA Regular >> SecOps	22	10.1.100.6	Permit All Commands	
sean	Authorization	ASA Regular >> SecOps	0	10.1.100.6		ASA Admin
sean	Authentication		86	10.1.100.6		
hellen	Authorization	ASA Regular >> HelpDesk	22	10.1.100.6		
neo	Authorization	ASDM Authz >> NetOps	443	10.1.100.6	Permit All Commands	

그림 21. TACACS Livelogs

6 단계 내역 리포트의 경우 인증, 권한 부여 및 계정 관리 리포트를 가져오려면 **Work Centers(작업 센터) > Device Administration(디바이스 관리) > Reports(리포트) > Device Administration(디바이스 관리)**로 이동합니다.

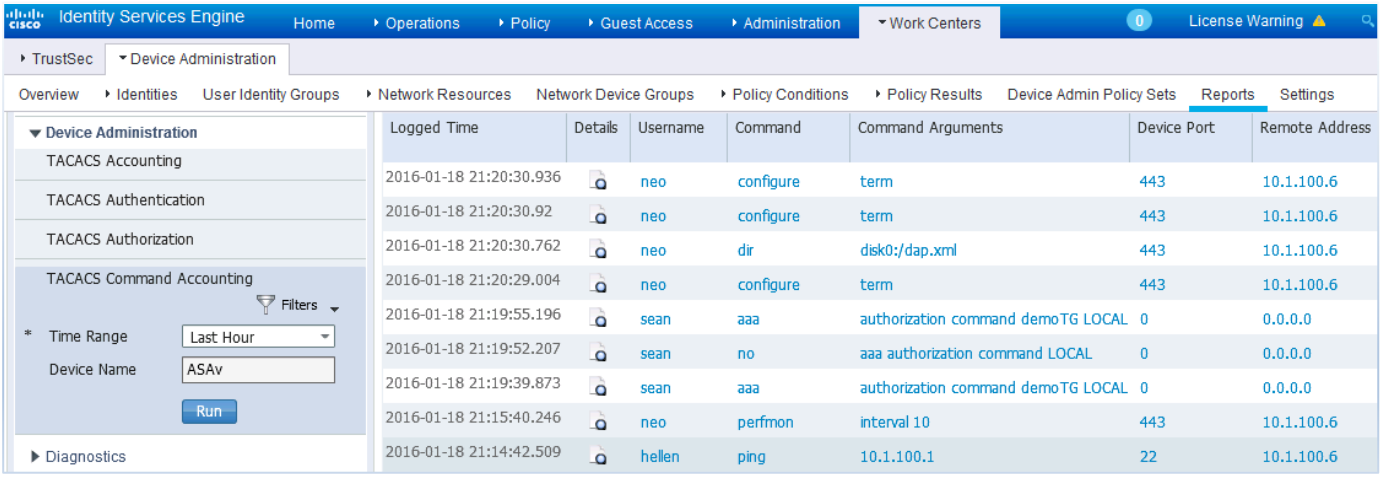

그림 22. TACACS 리포트