# ISE 2.x에 대해 Prime 3.1 TACACS 인증 구성

녹사		
<u>소개</u>		
<u>요구 사항</u>		
<u>구성</u>		
<u>Prime 컨피그레이션</u>		
<u>ISE 구성</u>		
문제 해격		

### 소개

이 문서에서는 ISE 2.x에서 TACACS를 통해 인증하도록 Prime Infrastructure를 구성하는 방법에 대 해 설명합니다.

## 요구 사항

Cisco에서는 다음 항목에 대한 기본 지식을 갖춘 것을 권장합니다.

- Identity Services Engine(ISE)
- Prime Infrastructure

### 구성

Cisco Prime Network Control System 3.1

Cisco Identity Service Engine 2.0 이상.

(참고: ISE는 버전 2.0부터 시작하는 TACACS만 지원하지만 Prime에서 Radius를 사용하도록 구성 할 수 있습니다. Prime에는 이전 버전의 ISE 또는 서드파티 솔루션과 함께 Radius를 사용하려는 경 우 TACACS 외에도 Radius 특성 목록이 포함됩니다.)

Prime 컨피그레이션

Administration(관리) / Users(사용자)/ Users(사용자), Roles(역할) 및 AAA(AAA) 화면으로 이동합니 다(아래 참조).

그런 다음 TACACS+ Servers(TACACS+ 서버) 탭을 선택한 다음 오른쪽 상단 모서리에서 Add TACACS+ Server(TACACS+ 서버 추가) 옵션을 선택하고 go(이동)를 선택합니다.

다음 화면에서는 TACACS 서버 항목의 컨피그레이션을 사용할 수 있습니다(개별 TACACS 서버마 다 수행해야 함)

<b>n</b>	Administration /	Users /	Users,	Roles	& AAA	*
----------	------------------	---------	--------	-------	-------	---

AAA Mode Settings	Add TACACS+ Server	r
Active Sessions	IP Address	
Change Password		
Local Password Policy	O* DNS Name	
Local rabbillora rolley	* Port	49
RADIUS Servers	Shared Secret Format	ASCII
SSO Server Settings	* Shared Secret	
SSO Servers	* Confirm Shared Secret	
TACACS+ Servers	* Retransmit Timeout	5 (secs)
User Groups	* Retries	1
Users	Authentication Type	PAP T
	Local Interface IP	192.168.10.154 🔹

여기서 서버의 IP 주소 또는 DNS 주소와 공유 비밀 키를 입력해야 합니다. 또한 사용하려는 로컬 인 터페이스 IP에 유의하십시오. 나중에 ISE에서 AAA 클라이언트에 대해 동일한 IP 주소를 사용해야 합니다.

Prime에서 컨피그레이션을 완료하려면 Administration(관리)/Users(사용자)/Users(사용자)/Users(사용자), Roles(역할) 및 AAA(AAA 모드 설정) 탭 아래에서 TACACS를 활성화해야 합니다.

(참고: 특히 컨피그레이션을 테스트할 때는 Enable fallback to Local(로컬로 대체 활성화) 옵션을 ONLY on no server response(서버 응답이 없는 경우에만) 또는 On no response or failure(응답 또 는 실패 응답이 없는 경우에만) 옵션과 함께 선택하는 것이 좋습니다.)

Administration / Users /	Users, Roles & AAA 🖈	0	Ø
AAA Mode Settings	AAA Mode Settings		
Active Sessions	AAA Mode 🔞	©Local ◎RADIUS ®TACACS+ ◎SSO	
Change Password	✓ Enable fallback to Local	ONLY on no server respon:	
Local Password Policy			
RADIUS Servers	Save		
SSO Server Settings			
SSO Servers			
TACACS+ Servers			
User Groups			
Users	_		

ISE 구성

Work Centers(작업 센터)/Device Administration(디바이스 관리)/Network Resources(네트워크 리소 스)/Network Devices(네트워크 디바이스)/Add(추가)에서 ISE의 AAA 클라이언트로 Prime 구성

dentity Services Engine	Home	ty  Operations	► Policy ► Administrat	ion 🗸 Work Cente	ers	License Warning 🔺	९ 🙂	± 0
Network Access     Guest Access	TrustSec + BYOD +	Profiler IN Posture	Device Administration	-				
Overview Identities User Identity	y Groups Ext Id Sources	✓Network Resources	Network Device Groups	<ul> <li>Policy Elements</li> </ul>	Device Admin Policy Sets	Reports Settings		
0								
Network Devices	Network Devices						0.1	@ \$?
Default Devices							Selected 0   lotal 0	<b>V</b> 🕾 🗸
TACACS External Servers	/ Edit - Add Du	plicate 🔂 Import 💮	Export  Generate PAC	🔀 Delete		Show All		- 6
TACACS Server Sequence	Name 🔺 IP,	Mask Profile Na	ame	Location	Туре		Description	
INCAGO GENEL GEQUENCE				No data a	vailable			

Prime 서버에 대한 정보를 입력합니다. 포함해야 할 필수 특성은 Name(이름), IP address(IP 주소)입니다. TACACS 및 Shared Secret(공유 암호)에 대한 옵션을 선택합니다. 나중에 권한 부여 규칙 또는 기타 정보의 조건으로 사용하기 위해 Prime에 대해 Device Type(디바이스 유형)을 추가로 추 가할 수 있지만 이는 선택 사항입니다.

Network Devices     Item Interview Devices       Default Devices     • Name       TACACS External Servers     • Name       Description	
Default Devices TACACS External Servers TACACS Server Sequence       * Name	
TACACS External Servers TACACS Server Sequence	
TACACS Server Sequence	
I P Address: / 32	
* Device Profile	
Model Name  Software Version	
* Network Device Group	
Device Type All Device Types Set To Default	
Location All Locations Set To Default	
RADIUS Authentication Settings	
✓ TACACS Authentication Settings	
Shared Secret       Show         Enable Single Connect Mode	
SNMP Settings	
Advanced Teurstee Settinge	
- • Auvanceu nusicer cennigs	
Submit Cancel	

그런 다음 TACACS 프로필 결과를 생성하여 필요한 특성을 ISE에서 Prime으로 전송하여 올바른 액세스 수준을 제공합니다. Work Centers(작업 센터)/Policy Results(정책 결과)/Tacacs Profiles(Tacacs 프로필)로 이동하고 Add(추가) 옵션을 선택합니다.

dentity Services Engine	Home ► Ope	erations   Policy	Guest Access	► Administration	✓ Work Centers	1	License Warning	<u> </u>		
TrustSec     Tevice Administration										
Overview Identities User Identity	y Groups 🕨 Netw	ork Resources Netw	ork Device Groups	Policy Conditions		Device Admin Policy Sets	Reports Settin	js		
C TACACS Command Sets	TACACS Pr	ofiles		Pov			Go 6 Total Row	•		
TACACS Profiles	C Refresh	+ Add Duplica	ate 💼 Trash 🗸	C Edit			▼ Filter ▼ 🌣	•		
	Name			Description						

이름을 구성하고 Profile attributes(프로필 특성) <u>상자</u>에 특성을 입력하려면 Raw View(원시 보기) 옵 션을 사용합니다. 특성은 primer 서버 자체에서 가져옵니다.

dentity Services Engine	Home	Policy      Guest Access	► Administration	✓ Work Centers		License Warning	۹ 🔺 و	۲	4	ø
TrustSec     Tevice Administration										
Overview Identities User Identity	Groups • Network Resourc	es Network Device Groups	▶ Policy Conditions		Device Admin Policy Sets	Reports Set	tings			
TACACS Command Sets	TACACS Profiles > New									
TACACS Profiles	TACACS Profile								2	
		Name *							1	
		Description								
	Task Attribute V	Raw View								
	Profile Attributes								1	
						C	ancel	ubmit		

Administration(관리) / Users(사용자)/ Users(사용자), Roles(역할) 및 AAA(AAA) 화면에서 특성을 가져오고 User Groups(사용자 그룹) 탭을 선택합니다. 여기서 제공하려는 액세스 그룹 수준을 선택 합니다. 이 예에서는 관리자 액세스 권한이 왼쪽에 있는 적절한 작업 목록을 선택하여 제공됩니다.

#### Administration / Users / Users, Roles & AAA 🔺

User Groups

AAA Mode Settings	User Groups			
Active Sessions	Group Name	Members	Audit Trail	View Task
Change Password	Admin	JP	6	Task List
Local Password Policy	Config Managers		8	Task List
RADIUS Servers	Lobby Ambassador	User1, CostaRica, Yita	6	Task List
SSO Server Settings	Monitor Lite		e	Task List
022	NBI Credential			Task List
330 Servers	NBI Read		6	Task List
TACACS+ Servers	NBI Write		6	Task List
User Groups	North Bound API		0	Task List
Users	Root	root	1	Task List
	Super Users		6	Task List
	System Monitoring		6	Task List
	User Assistant		8	Task List
	User Defined 1		6	Task List
	User Defined 2		6	Task List
	User Defined 3		6	Task List
	User Defined 4		1	Task List
	mDNS Policy Admin		8	Task List

### 모든 TACACS 사용자 지정 특성을 복사합니다.

#### ▲ Administration / Users / Users, Roles & AAA ★

Task List AAA Mode Settings O Please copy and paste the appropriate protocol data below into the custom/vendor-specific attribute field in your AAA server. TACACS+ Custom Attributes **RADIUS** Custom Attributes Active Sessions If the size of the RADIUS attributes on your AAA server is more than 4096 bytes, Please copy ONLY role attributes, application will retrieve the associated TASKS Change Password role0=Admin NCS:role0=Admin task0=Discovery Schedule Privilege task1=Mesh Reports task2=Saved Reports List task3=Monitor Menu Access task4=Device WorkCenter NCS:task0=Discovery Schedule Privilege NCS:task1=Mesh Reports NCS:task2=Saved Reports List NCS:task3=Monitor Menu Access NCS:task4=Device WorkCenter Local Password Policy **RADIUS Servers** SSO Server Settings task5=Inventory Menu Access task6=Add Device Access NCS:task5=Inventory Menu Access NCS:task6=Add Device Access task6=Add Device Access task7=Config Audit Dashboard task8=Custom NetFlow Reports task9=Apic Controller Read Access task10=Configuration Templates Read Access task11=Alarm Policies Edit Access task12=High Availability Configuration task13=View Job task14=Incidents Alarms Events Access task15=TAC Case Management Tool task16=Configure Autonomous Access Point Templates NCS:task6=Add Device Access NCS:task7=Config Audit Dashboard NCS:task8=Custom NetFlow Reports NCS:task9=Apic Controller Read Access NCS:task10=Configuration Templates Read Access NCS:task11=Alarm Policies Edit Access NCS:task12=High Availability Configuration NCS:task12=High Availability Configuration NCS:task14=Incidents Alarms Events Access NCS:task14=Incidents Alarms Events Access NCS:task15=TAC Case Management Tool NCS:task15=Configure Autonomous Access Point Templates SSO Servers TACACS+ Servers User Groups Users task16=Contigui Templates task17=Import Policy Update task18=PnP Profile Read-Write Access task19=SSO Server AAA Mode task19=Slam Boscos Access NCS:taskl=PMP Profile Read-Write Access NCS:taskl=PMP Profile Read-Write Access NCS:taskl=SDS Server AAA Mode θv ndatory. To add cust related to Virtual Domains, please click here

그런 다음 ISE의 Profile(프로파일)의 Raw View(원시 보기) 섹션에 붙여넣습니다.

**9** Ø **1** 

isco Ideni	tity Services E	ngine	Home	<ul> <li>Operations</li> </ul>	▶ Policy	Guest Access	Administration	✓ Work Centers		License W	/aming 🔺	0,	۲	
▶ TrustSec	▼ Device Adm	ninistration												
Overview	Identities	User Identity	Groups	Network Reso	ources Net	work Device Groups	Policy Conditions	- Policy Results	Device Admin Policy Sets	Reports	Settings			
		G												
ACACS Con	nmand Sets		TAC	ACS Profiles > Ne	W									
ACACS Prof	files		TAC	CACS Profile										
					Na	me * Prime								
					Descri	ption								
				Task Attribu	te View	Raw View								
			Prof	file Attributes										
														٦
			ro	ole0=Admin		de dina na								
			ta	isku=Discovery	Schedule Pr	rivilege								
			ta ta	isk1=Mesn Rep	orte Liet									
			ta	isk2=Saveu Rep										I
			ta	sk4=Device Mo	rkCenter									I
			ta	ek5-Inventory	Annu Acces	c								I
			ta	sk5-Add Device	Access	5								I
			ta	sko=Add Device	it Dachboar	rd.								I
			ta	sk8=Custom Ne	tElow Deno	orte								
			ta	sko-Custom Ne	allor Dood A	00000								
			ta	sk10-Configura	tion Tompla	tos Boad Accoss								I
			ta	sk10-Connyura	icios Edit Ac	coss								
			ta	isk12=High Avai	Icles Eult Ad	iguration								
			ta ta	sk12=High Avai	lability Com	iguration								
			La	ISK I S-VIEW JOD									•	I
											Cancel	Su	Ibmit	
												_		

가상 도메인 사용자 지정 특성은 필수입니다. 루트 도메인 정보는 Prime Administration(기본 관리) - > Virtual Domains(가상 도메인)에서 찾을 수 있습니다.

ululu Cisco Prime										Virtual Doma	in ROOT-DOMAIN	1 1	root 🔻 🛛
cisco Infrastructure	≪d 💌 M	onitor 🔻	Configuration	٠	Inventory	<ul> <li>Map</li> </ul>	s •	Services	•	Reports 🔻	Administration	•	
Administration > Virtual Domains Virtual Domains	Virtual Domains ROOT-DOM	> ROOT-D AIN	OOMAIN										
Virtual Domains	Virtual domains Infrastructure, their assigned p	are logica ou can co art of the	al groupings of de onfigure virtual de network only.	evice omai	s and are use ns. Virtual do	d to contr main filter	ol who s allov	can admin users to c	ister a onfigu	a group. After y ire devices, vie	ou add devices t w alarms, and ge	to Pri enera	me te reports
🤄 🔹 🗄 👻 🌇	* Name	ROOT-DO	OMAIN			Time Zo	ne -	- Select Tin	ne Zoi	ne	•		
ROOT-DOMAIN	Email Address					Descript	ion [	ROOT-DOM	AIN				
	Submit	ancel											

Prime Virtual Domain의 이름을 attribute virtual-domain0="virtual domain name"으로 추가해야 합니 다.

dentity Services Engine	Home   Context Visibility	Operations	Policy + Adminis	tration · Work Centers		٩,
Network Access     Guest Access	TrustSec     BYOD     Profil	er Posture -	Device Administration	PassiveID		Click bare to do wireless setup D
Overview Identities User Identit	ity Groups Ext Id Sources • M	Network Resources		Device Admin Policy Sets	Reports Settings	Click here to do wireless setup b
Conditions	TACACS Profiles > Prime Acc	ess				
	TACACS Profile					
Network Conditions		Name Prime	Access			
✓ Results						
Allowed Protocols		Description				
TACACS Command Sets						
TACACS Profiles	Task Attribute View	Raw View				
	Profile Attributes					
	task162=Monitor Mobilit task163=Context Aware task164=Voice Diagnost task165=Configure Choi task166=RRM Dashboa task166=RRM Dashboa task168=Theme Chang task169=Import Policy Li task170=Design Endpoi task170=Design Endpoi task171=Planning Mode task171=Planning Mode task172=Pick and Unpic task173=Configure Men task174=Ack and Unpic task175=Ack and Unpic task176=Auto Provision virtual-domain0=ROOT-	y Devices Reports tics ke Points rrd er Access Jpdate nt Site Association et Alerts u Access k Alerts u Access k Alerts ing DOMAIN	Access			Ŷ

그런 다음 이전 단계에서 생성한 셸 프로필을 할당하는 규칙을 Work Centers/Device Administration/Device Admin Policy Sets(작업 센터/디바이스 관리/디바이스 관리 정책 집합) 아래 에 생성하기만 하면 됩니다

(참고: "조건"은 구축에 따라 달라지지만, 이 규칙에서 요청을 제대로 필터링하도록 Prime에 대해 특 별히 "Device Type"을 사용하거나 Prime IP 주소와 같은 다른 유형의 필터를 "조건" 중 하나로 사용 할 수 있습니다.)

-the Identity Services Engine Home	Context Visibility      Operations      Policy      Administration      Work Centers     License Warning	0 ±	0
Network Access     Guest Access     TrustSec	SYOD      Profiler      Posture      Posture      Device Administration		
Overview Identities User Identity Groups	Ext Id Sources + Network Resources Network Device Groups + Policy Elements Device Admin Policy Sets Reports Settings		
Policy Sets Search policy names & descriptions. ↓ • ▷ • ↓ ↑ ↓ ↓ ↓ ↓	Define the Policy Sets by configuring rules based on conditions. Drag and drop sets on the left hand side to change the order. For Policy Export go to Administration > System > Backup & Restore > Policy Export Page Status Name Description Default Tacacs_Default		
Summary of Policies	Regular ® Proxy Sequence		
Global Exceptions Rules across entire deployment	Authentication Policy		
Default Tacacs_Default	Default Rule (If no match) : Allow Protocols : Default Device Admin and use : Internal Users		
Save Order Reset Order	* Authorization Policy		
	Exceptions (0) Standard		
	Status         Rule Name         Conditions (identity groups and other conditions)         Command Sets         Shell Profiles           Prime Rule         If         DEV/CE:Device Type ECUALS All Device         then         PermiAll AND         Prime	Edit   •	
	Tacacs_Default if no malches, then Select Profile(s) Deny All Shell Profile	Edit   +	

이 시점에서 컨피그레이션이 완료되어야 합니다.

### 문제 해결

이 컨피그레이션이 실패하고 Prime에서 로컬 폴백 옵션이 활성화된 경우 Prime의 IP 주소를 제거하 여 ISE에서 장애 조치를 강제로 수행할 수 있습니다. 그러면 ISE가 응답하지 않고 로컬 자격 증명을 강제로 사용하게 됩니다. 거부 시 로컬 폴백이 수행되도록 구성된 경우 로컬 어카운트는 여전히 작 동하며 고객에게 액세스 권한을 제공합니다.

ISE가 성공적인 인증을 표시하고 올바른 규칙과 일치하지만 Prime이 요청을 계속 거부하는 경우 프 로필에서 특성이 올바르게 구성되었으며 추가 특성이 전송되지 않았음을 다시 확인하고자 할 수 있 습니다. 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 번 역 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.