# Konfigurieren der Prime 3.1 TACACS-Authentifizierung für ISE 2.x

### Inhalt

Einführung Anforderungen Konfigurieren Prime-Konfiguration ISE-Konfiguration Fehlerbehebung

## Einführung

In diesem Dokument wird beschrieben, wie die Prime-Infrastruktur für die Authentifizierung über TACACS mit ISE 2.x konfiguriert wird.

## Anforderungen

Cisco empfiehlt, dass Sie über grundlegende Kenntnisse in folgenden Bereichen verfügen:

- Identity Services Engine (ISE)
- Prime-Infrastruktur

## Konfigurieren

Cisco Prime Network Control System 3.1

Cisco Identity Service Engine 2.0 oder höher

(Hinweis: Die ISE unterstützt nur TACACS ab Version 2.0. Es ist jedoch möglich, Prime für die Verwendung von Radius zu konfigurieren. Prime enthält zusätzlich zu TACACS eine Liste mit Radius-Attributen, wenn Sie Radius verwenden möchten. Dies gilt auch für eine ältere Version der ISE oder einer Drittanbieterlösung.)

### **Prime-Konfiguration**

Navigieren Sie zum folgenden Bildschirm: Administration/Benutzer/Benutzer, Rollen und AAA wie unten dargestellt.

Wählen Sie dort die Registerkarte TACACS+ Servers (TACACS+-Server) aus, wählen Sie anschließend in der rechten oberen Ecke die Option Add TACACS+ Server (TACACS+-Server hinzufügen) aus, und wählen Sie Go (Los) aus.

Auf dem nächsten Bildschirm ist die Konfiguration des TACACS-Servereintrags verfügbar (dies muss für jeden einzelnen TACACS-Server erfolgen).

Administration / Users /	Users, Roles & AAA 🔺		0 Ø 🛛
AAA Mode Settings	Add TACACS+ Server		
Active Sessions	IP Address		
Change Password	O* DNS Name		
Local Password Policy	* 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		
Users	Authentication Type		
	Local Interface IP	192,168,10,154	
	Save Cancel		

Hier müssen Sie entweder die IP-Adresse oder die DNS-Adresse des Servers sowie den gemeinsamen geheimen Schlüssel eingeben. Bitte beachten Sie auch die IP-Adresse der lokalen Schnittstelle, die Sie verwenden möchten, da diese IP-Adresse später für den AAA-Client in der ISE verwendet werden muss.

Um die Konfiguration auf Prime abzuschließen. Sie müssen TACACS unter Administration / Users / Users, Roles & AAA unter der Registerkarte AAA Mode settings (AAA-Modus-Einstellungen) aktivieren.

(Hinweis: Es wird empfohlen, die Option Enable fallback to Local (Fallback auf Lokal aktivieren) zu aktivieren, wobei entweder NUR auf Keine Serverantwort oder die Option On no response (Keine Antwort oder Fehler), insbesondere beim Testen der Konfiguration, verwendet werden sollte.



#### **ISE-Konfiguration**

Konfigurieren Sie Prime als AAA-Client auf der ISE in Work Centers/Device Administration/Network Resources/Network Devices/Add



Geben Sie die Informationen für den Prime-Server ein. Die erforderlichen Attribute, die Sie einschließen müssen, sind Name, IP-Adresse, wählen Sie die Option für TACACS und den Shared Secret aus. Sie können zusätzlich einen Gerätetyp, speziell für Prime, hinzufügen, um später als Bedingung für die Autorisierungsregel oder andere Informationen verwendet zu werden. Dies ist jedoch optional.

0	
Network Devices	Network Devices List > New Network Device
Default Devices	
TACACS External Servers	
TACACS Server Sequence	Description
	* IP Address: / 32
	* Device Profile 📾 Cisco 🔻 🕀
	Model Name  Software Version
	* Network Device Group
	Device Type       All Device Types       Set To Default         Location       All Locations       Set To Default
	RADIUS Authentication Settings         Image: TACACS Authentication Settings
	Shared Secret Show
	<ul> <li>Legacy Cisco Device</li> <li>TACACS Draft Compliance Single Connect Support</li> </ul>
	SNMP Settings
	Advanced TrustSec Settings
	Submit Cancel

Erstellen Sie anschließend ein TACACS-Profilergebnis, um die erforderlichen Attribute von der ISE an Prime zu senden, um die richtige Zugriffsebene bereitzustellen. Navigieren Sie zu Work Center/Policy Results/Tacacs Profiles, und wählen Sie die Option Add (Hinzufügen) aus.

dentity Services Engine	Home	<ul> <li>Operations</li> </ul>	Policy	Guest Access	► Administration	✓ Work Centers	1	License Wa	arning 🔺	Q,	0	2	ø
TrustSec     Tevice Administration													
Overview Identities User Identit	y Groups	Network Resource	es Networ	rk Device Groups	<ul> <li>Policy Conditions</li> </ul>		Device Admin Policy Sets	Reports	Settings				
TACACS Command Sets	TAC/	ACS Profiles			Rov	vs/Page 6 🔻	⊲ ⊲ 1/1 ⊳ ⊳	Go 6 To	otal Rows				
	CI	Refresh 🕂 Add	Duplicate	e 💼 Trash 🕶	🕑 Edit			▼ Filter ▼	۰.				
		Name			Description								

Konfigurieren Sie den Namen, und geben Sie die Attribute unter dem Feld Profile attribute (Profile-Attribute) mithilfe der Option <u>Raw View</u> (<u>Raw-Ansicht</u>) ein. Die Attribute werden vom Primärserver

#### selbst übernommen.

	Home • Open	rations + Pol	icy → Guest Access	► Administration	✓ Work Centers	•	License Wa	aming 🔺	٩	۲	4 0
TrustSec     TrustSec											
Overview Identities User Identity	Groups • Netwo	ork Resources	Network Device Groups	Policy Conditions		Device Admin Policy Sets	Reports	Settings			
TACACS Command Sets	TACACS Profil	es > New									
TACACS Profiles	TACACS Profi	le								_	
			Name *								
		De	scription								
		A4-0-1-1-									
	Task	Attribute View	Raw View								
	Profile Attribu	tes								_	

Rufen Sie die Attribute im Bildschirm Administration / Users / Users, Roles & AAA ab, und wählen Sie die Registerkarte User Groups (Benutzergruppen) aus. Hier wählen Sie die Zugriffsebene Gruppe aus, die Sie bereitstellen möchten. In diesem Beispiel wird der Administratorzugriff durch Auswahl der entsprechenden Aufgabenliste auf der linken Seite gewährt.

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			Task List
RADIUS Servers	Lobby Ambassador	User1, CostaRica, Yita	6	Task List
SSO Server Settings	Monitor Lite		8	Task List
SEO Samara	NBI Credential			Task List
550 Servers	NBI Read			Task List
TACACS+ Servers	NBI Write		6	Task List
User Groups	North Bound API		1	Task List
Users	Root	root		Task List
	Super Users		8	Task List
	System Monitoring			Task List
	User Assistant		8	Task List
	User Defined 1		8	Task List
	User Defined 2			Task List
	User Defined 3		6	Task List
	User Defined 4		8	Task List
	mDNS Policy Admin			Task List

### Kopieren Sie alle benutzerdefinierten TACACS-Attribute.

#### ▲ Administration / Users / Users, Roles & AAA ★ Task List AAA Mode Settings 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 role@=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:task0=Discovery Schedule Privilege NCS:task2=Saved Reports List NCS:task2=Nonitor Menu Access NCS:task4=Device WorkCenter Local Password Policy **RADIUS Servers** task4=Device WorkCenter task5=Inventory Menu Access task5=Add Device Access task5=Config Audit Dashboard task8=Custom NetFlow Reports task3@=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 NCS:task4=Device WorkCenter NCS:task5=Inventory Menu Access NCS:task5=Add Device Access NCS:task8=Custom NetFlow Reports NCS:task9=Apic Controller Read Access NCS:task10=Configuration Templates Read Access NCS:task10=Apic Edit Access NCS:task11=Alarm Policies Edit Access NCS:task12=High Availability Configuration NCS:task13=View Job NCS:task14=Incidents Alarms Events Access NCS:task15=TAC Case Management Tool **SSO Server Settings** SSO Servers TACACS+ Servers User Groups Users task14=inCleents Alarms Events Access task15=TAC Case Management Tool task16=Configure Autonomous Access Point Templates task17=Import Policy Update task18=PnP Profile Read-Write Access task19=S0 Server AA Mode NCS:task15=TAC Case Management Tool NCS:task16=Configure Autonomous Access Point NCS:task16=Com age: C Templates NCS:task17=Import Policy Update NCS:task18=PnP Profile Read-Write Access NCS:task19=S50 Server AAA Mode θv rtual Domain cu s are mandatory To add custom a es related to Virtual Domains, please click here

Fügen Sie sie dann im Abschnitt "Raw View" des Profils auf der ISE ein.

sco lucinity Sel	vices Engine	Home	<ul> <li>Operations</li> </ul>	Policy	<ul> <li>Guest Access</li> </ul>	Administration	✓ Work Centers		License W	arning 🔺	Q	•	
TrustSec • De	vice Administration												
verview 🕨 Ider	tities User Identity	/ Groups	Network Reso	ources Net	work Device Groups	Policy Conditions	✓ Policy Results	Device Admin Policy Sets	Reports	Settings			
	0	TACA	ACS Profiles > Net	w									
ACS Command S	Sets		1001101100-1101										
ACS Profiles		TACA	ACS Profile										
				Na	me * Prime								
				Descrip	ption								
			Task Attribut	le View	Raw View								
		Profi	le Attributes										10
		rol	le0=Admin									-	1
		tas	sk0=Discovery S	Schedule Pr	ivilene								
		tas	sk1=Mesh Repo	orts	Micge								
		tas	sk2=Saved Rep	orts List									
		tas	sk3=Monitor Me	anu Access									
		tas	sk4=Device Wou	rkCenter									
		tas	sk5=Inventory N	Aenu Acces	9								
		tas	sk6=Add Device	Access									
		tac	sko-Add Device	it Daebboar									
		tas	sk7=Custom Ne	tElow Depo	urte								
		tas	sko-Custom Ne	allor Dood A	115								
		lds	sk9-Apic Contro	Jiel Redu A	ICLESS								
		las	sk to=Conligura	uon rempia	tes Read Access								
		tas	sk11=Alarm Poli	cies Edit Ac	cess								
		tas	sk12=High Avail	ability Confi	guration								
		tas	sk13=View Job									•	
										Cancol	911	umit	

Benutzerdefinierte Attribute virtueller Domänen sind obligatorisch. Informationen zur Root-Domain finden Sie unter Prime Administration -> Virtual Domains (Prime-Verwaltung -> virtuelle Domänen).

uluulu. Cisco Prime							Virtual	Domain ROOT-DOMAIN	N   root 🕶
cisco Infrastructure	<b>∉</b> d I ▼ M	onitor 🔻	Configuration	Inventory	<ul> <li>Maps</li> </ul>	Services	s <b>T</b> Reports	Administration	n 💌
Administration > Virtual Domains Virtual Domains	Virtual Domains	> ROOT-I AIN	OOMAIN						
Virtual Domains	Virtual domains Infrastructure, their assigned	are logic you can c part of the	al groupings of devi onfigure virtual don e network only.	ices and are us nains. Virtual de	ed to control v omain filters a	who can admin Ilow users to o	nister a group. Af configure devices	ter you add devices , view alarms, and g	to Prime Jenerate reports
(= * ) 🖽 * 🍕 🌇	* Name	ROOT-D	OMAIN		Time Zone	Select Tir	me Zone	•	
ROOT-DOMAIN	Email Address				Description	ROOT-DOM	1AIN		
	Submit	ancel							

Der Name der Prime Virtual Domain muss als Attribut **virtual-domain0=**"virtual domain name" hinzugefügt werden.

	Home  Context Visibility  Operations  Policy  Administration  Work Centers	٩
Network Access     Guest Access	TrustSec      BYOD      Profiler      Posture      Cevice Administration      PassiveID	Click here to do wireless setup C
Overview      Identities     User Identity      Conditions      Network Conditions      Results     Allowed Protocols     TACACS Command Sets	ty Groups Ext Id Sources   Network Resources  Policy Elements Device Admin Policy Sets Reports Settings  TACACS Profile  Name Prime Access Description	Click here to do wireless setup D
IACACS Profiles	Task Attribute View       Raw View         Profile Attributes         task162=Monitor Mobility Devices         task163=Context Aware Reports         task163=Context Aware Reports         task164=Voice Diagnostics         task165=Configure Choke Points         task165=Configure Choke Points         task165=RRM Dashboard         task165=Rhm Dashboard         task167=Swim Delete         task168=Theme Changer Access         task169=Import Policy Update         task170=Design Endpoint Site Association Access         task171=Planning Mode         task173=Configure Menu Access         task173=Configure Menu Access         task174=Ack and Unack Security Index Issues	^

Danach müssen Sie nur noch eine Regel erstellen, um das im vorherigen Schritt erstellte Shell-Profil unter Work Center/Device Administration/Device Admin Policy Sets (Work Center/Device Administration/Device Admin-Richtliniensätze) zuzuweisen.

(Hinweis: "Bedingungen" variieren je nach Bereitstellung. Sie können jedoch "Gerätetyp" speziell für Prime oder einen anderen Filtertyp wie die IP-Adresse von Prime verwenden, um Anfragen entsprechend zu filtern.

-de-the Identity Services Engine Home	Context Visibility > Operations	Policy      Administration	Work Centers	License Warning 🔺 👘 🤗	
Network Access      Guest Access      TrustSec	BYOD      Profiler      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. Search policy names & descriptions. Search policy names & descriptions. Supervised Second Seco	Define the Policy Sets by configuring in For Policy Export go to Administration 2 Status Name Default Regular ® Proxy Sequence Authentication Policy Default Rule (if no math	ules based on conditions. Drag and dn - System > Backup & Restore > Policy Description Tacacs_Default (kh) : Allow Protocols : Default De	op sets on the left hand side to change the Export Page evice Admin and use : Internal Us	order. ers	Edz   •
Tacacs_Default	* Authorization Policy				
(anten) (Antens)	Exceptions (0)     Standard				
	Status Rule Name	Conditions (identity grou	ps and other conditions) Comman	Stell Profiles	1
	Prime Rule	If DEVICE:Device Type EQ Types#Prime	UALS All Device then PermitAll	AND Prime	Edit  •
	Tacacs_Default	if no matches, then Selec	t Profile(s) Deny All Shell Profile		Edit   +

Zu diesem Zeitpunkt sollte die Konfiguration abgeschlossen sein.

## Fehlerbehebung

Wenn diese Konfiguration nicht erfolgreich ist und die lokale Rückfalloption auf Prime aktiviert wurde, können Sie einen Failover von der ISE erzwingen, indem Sie die IP-Adresse von Prime entfernen. Dies führt dazu, dass die ISE nicht reagiert und die Verwendung lokaler Anmeldeinformationen erzwingt. Wenn für eine Ablehnung ein lokaler Fallback konfiguriert ist, funktionieren die lokalen Konten weiterhin und ermöglichen dem Kunden Zugriff.

Wenn die ISE eine erfolgreiche Authentifizierung anzeigt und mit der richtigen Regel übereinstimmt, Prime jedoch die Anforderung noch ablehnt, können Sie überprüfen, ob die Attribute im Profil korrekt konfiguriert sind und keine weiteren Attribute gesendet werden.