## Radius- und TACACS-basierte Benutzerauthentifizierung und -autorisierung für vEdge und Controller mit ISE

## Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Konfigurieren Radius-Based User Authentication and Authorization for vEdge and Controllers TACACS-basierte Benutzerauthentifizierung und -autorisierung für vEdge und Controller Zugehörige Informationen

## Einführung

In diesem Dokument wird beschrieben, wie RADIUS- und TACACS-basierte Benutzerauthentifizierung und -autorisierung für vEdge und Controller mit Identity Service Engine (ISE) konfiguriert wird.

### Voraussetzungen

#### Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

#### Verwendete Komponenten

Für die Demonstration wurde ISE Version 2.6 verwendet. vEdge-Cloud und Controller mit 19.2.1

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

### Konfigurieren

Die Viptela-Software enthält drei feste Benutzergruppennamen: **Basic**, **netadmin** und **operator**. Sie müssen den Benutzer mindestens einer Gruppe zuweisen. Der Benutzer Default TACACS/Radius wird automatisch in die Grundgruppe eingefügt.

#### Radius-Based User Authentication and Authorization for vEdge and Controllers

Schritt 1: Erstellen Sie ein Viptela-Radius-Wörterbuch für die ISE. Erstellen Sie dazu eine Textdatei mit dem Inhalt:

# #	-*- text -*-			
# # #	dictionary.v:	iptela		
# # #	Version:	\$Id\$		
VI	ENDOR	Viptela	41916	5
Bl	EGIN-VENDOR	Viptela		
A	TTRIBUTE	Viptela-Group-Name	1	string

Schritt 2: Wörterbuch auf ISE hochladen Navigieren Sie zu **Richtlinien > Richtlinienelemente > Wörterbücher**. Navigieren Sie in der Liste der Wörterbücher zu **Radius > Radius Vendors** und klicken Sie dann auf **Importieren**, wie im Bild gezeigt.

dentity Services Engine Home	Context Visibility      Operations	Policy     Administration	Work Centers
Policy Sets Profiling Posture Client Provision	ing Policy Elements		
Dictionaries + Conditions + Results			
	RADIUS Vendors		
Dictionaries	Toto venuoro		
[م	/ Edit -Add X Delete	E Import	
(□ * 圧 *	Name	Vandor ID	Description
Guest	Airespace	14179	Dictionary for Vendor Airespace
GuestAccess	Alcately ucent	800	Dictionary for Vendor Alcatel-Lucent
Identity Mapping	Anha	14823	Dictionary for Vendor Aniha
IdentityGroup	Brocade	1588	Dictionary for Vendor Produl
InternalEndopint		9	Dictionary for Ventor Diction
InternalUser	Citron-BBSM	5263	Dictionary for Vendor Cisco-BRSM
IOTASSET	Cisco-VPN3000	3076	Dictionary for Vendor Cisco-VPN3000
> 🛄 IP		25506	Dictionary for Vendor H3C
LLDP		11	Dictionary for Vendor HP
MAC		2636	Dictionary for Vendor Juniper
MDM_LOG	Microsoft	311	Dictionary for Vendor Microsoft
MSE CERTIFIC	Motorola-Symbol	388	Dictionary for Vendor Motorola-Symbol
MUD	Ruckus	25053	Dictionary for Vendor Ruckus
III NETELOW	WISPr	14122	Dictionary for Vendor WISPr
Network Access			
Network Condition			
NMAP			
NMAPExtension			
Normalised Radius			
PassivelD			
Posture			
PROFILER			
<ul> <li>Reados</li> <li>IETE</li> </ul>			
RADIUS Vendors			
Session			
SNMP			
SXP			
TACACS			
TC-NAC			
Threat			

Laden Sie jetzt die Datei hoch, die Sie in Schritt 1 erstellt haben.

cisco Identit	y Services	s Engine	Home 🕨	Context Visibility	<ul> <li>Operations</li> </ul>	▼ Policy	Administration	Work Centers
Policy Sets	Profiling	Posture	Client Provisionin	Policy Elemen	its			
Dictionaries	<ul> <li>Conditi</li> </ul>	ons • Re	esults					

Dictionaries	
Dictionaries	Use this for to import a RADIUS Vendor. Select the file using the browser and click "Import".
م	* Vendor file:
(= ▼ 1 = ▼	Choose file dictionary.viptela
Guest	
GuestAccess	
Identity Mapping	Import Cancel
IdentityGroup	
InternalCA	
InternalEndpoint	
InternalUser	
IOTASSET	
▶ 🛄 IP	
LLDP	
MAC	
MDM_LOG	
MSE	
MUD	
Multimedia	
NETFLOW	
Network Access	
Network Condition	
► LI NMAP	
MMAPExtension	
Normalised Radius	
PassiveID	
Posture	
PROFILER	
Radius	
RADIUS Vendore	
Session	
▶ III SNMP	
SXP	
TACACS	
TC-NAC	
Threat	

Schritt 3: Erstellen eines Autorisierungsprofils In diesem Schritt weist das Radius-Autorisierungsprofil einem authentifizierten Benutzer beispielsweise die Ebene der Netadmin-Berechtigungen zu. Navigieren Sie hierzu zu **Richtlinien > Richtlinienelemente > Autorisierungsprofile,** und geben Sie zwei erweiterte Attribute an, wie im Bild gezeigt.

dentity Services	vices Engin	e Hon	ne	bility	▼Policy	<ul> <li>Administration</li> </ul>	➤ Work Centers
Policy Sets Profili	ing Postu	re Client P	rovisioning Polic	y Elements			
Dictionaries + Co	nditions	<ul> <li>Results</li> </ul>					
Authentication		G Au Au	uthorization Profiles >	vEdge-netadmin ïle			
- Authorization			* Na	me vEdge-netadmin		]	
Authorization Profil	95		Descript	ion		-	
Downloadable ACL	s		* Access Ty	Pe ACCESS_ACCEPT	*		
Profiling			Network Device Profile	e Cisco 👻 🕀			
▶ Posture			Service Templ	ate 🗌			
Client Provisioning	I		Track Movem Passive Identity Track	ent ⊡ ⑧ ing □ ⑧			
		-	Common Tasks				
		_	Advanced Attrib	utes Settings			
			Radius:Service-Type	e 📀 = [	IAS Prompt	0	
			Viptela:Viptela-Grou	ıp-Name 💟 = [r	etadmin	0	- +
			<ul> <li>Attributes Detai</li> </ul>	ls			
			Access Type = ACCES Service-Type = 7 Viptela-Group-Name	S_ACCEPT = netadmin			
			Save				

Schritt 4: Abhängig von Ihrer tatsächlichen Einrichtung sieht Ihr Richtliniensatz möglicherweise anders aus. Für die Demonstration in diesem Artikel wird der Richtlinieneintrag "**Terminalzugriff**" wie im Bild gezeigt erstellt.

cisco Id	lentity Se	rvices Engine	Home	Context Visibility	Operations	▼ Policy	Administration	Work Centers		٩,	0	o o
Policy S	ets Pro	filing Posture	Client Provision	ing      Policy Elem	ents							
Policy	Sets								Reset Policyset Hitcounts		Reset	Save
+	Status	Policy Set Nar	ne	Description		Conditions			Allowed Protocols / Server Sequence	Hits	Actions	View
Search												
	Ø	Terminal Access				🗇 Rad	lius·NAS-Port-Type E	QUALS Virtual	Default Network Access × × +	2	¢	>

Klicken Sie > und der nächste Bildschirm wird angezeigt, wie im Bild gezeigt.

cisco Id	entity Ser	vices Engine	Home	Context Visibili	ty > Operations	* Policy	Administratio	n + Work Centers	5				• •
Policy S	ets Prof	fling Posture	Client Provisio	oning + Policy E	Bements								
Policy	Sets →	Terminal Ac	cess							Reset Policyse	Hitcounts	Reset	Save
	Status	Policy Set Nan	ne	Description		Conditio	ns			Allowed P	rotocols / Server	Sequence	Hits
Search													
	0	Terminal Access				D P	tadius-NAS-Port-Typ	e EQUALS Virtual		Default N	etwork Access	× • +	2
> Auth	entication	Policy (1)											
> Auth	orization	Policy - Local E	xceptions										
> Auth	orization	Policy - Global	Exceptions										
♥ Auth	orization	Policy (2)											
							Result	8					
•	Status	Rule Name		Condition	s		Profile	5	Secu	rity Groups		Hits	Actions
Searc	h												
	Ø	vEdge-netadm	in	書 Ide Gr	ntityGroup-Name EQI oups:lab_admin	JALS User	Identity ×vEc	ige-netadmin	+ Sel	act from list	× +	1	٥
	Ø	Default					×Der	yAccess	+ Sei	ect from list	- +	0	٥
													Save

Diese Richtlinie stimmt mit der Benutzergruppe "lab\_admin" überein und weist ein in Schritt 3 erstelltes Autorisierungsprofil zu.

Schritt 5: Definieren Sie NAS (vEdge-Router oder Controller), wie im Image gezeigt.

• Setem * Identify Banagemet • Neurole Resource * > Parked Revice * > Freed Service * > Treed Service * > * > Treed Service * > * > * > * > * > * > * > * > * > *	cisco Identity Services Engine	Home Context Visibility Operations Policy Administration Work Centers	
• Network Devices     Network Devices     Network Devices List > vEdged1     Devices Security Settings     • Device Profile     • Device Traine     • Device Profile     • Device Profile     • Device Traine     • Device Profile     • Device Traine	System      Identity Management	Network Resources     Device Portal Management     pxGrid Services     Feed Service     Threat Centric NAC	
Network Devices Lis > stége-01           Derive Security Settings         Image: Security Settings                • Devices Profile @ Olaco + @ · Device Trope @ Set: To Default             · Device Trope @ Device Trope @ Set: To Default             · Device Trope @ Device	Network Devices Network Device	e Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM + Location Services	
Network Devices List version         Default Device         Device Security Settings         Image: Case of the security Settings         Image: Case of the security Settings         Image: Security Secur		0	
Detail Device       Image: Methods         Device Security Settings	Network Devices	Network Devices List > vEdge-01	
Device Security Settings	Default Device	Network Devices	
Description	Device Security Settings	Name VEdge-01	
IP Address       * 'P':       10.48.87.232       / 32       %*         * Device Profile       Clasor       0         * Obvice Profile       Clasor       0         * Obvice Profile       *       *         * Obvice Profile       *       *         * Obvice Profile       *       *         * Obvice Oroup       *       *         Location       *       Model Rame         Device Type       *       Stat To Default         Device Type       *       Stat To Default         Device Type       *       Stat To Default         Ovice Type       *       Stat To Default         Use Second Shared Secret       *       Snow         CoA Port       *       Snow         CoA Port       *       Snow         CoA Port       *       Snow         CoA Port       *       Snow         Stated Secret       *       *         Stated Secret       * <td></td> <td>Description</td> <td></td>		Description	
Protocol Profile      Ison			60
Device Profile      Gaso		IP Address • 1P : 10.48.87.232 7 32	- 92.4
Device Profile Claco     Device Profile Claco     Device Profile Claco     Device Profile Claco     Device Trans     Software Version     Tectorian Mal Locations     Device Trans     Devic			
<ul> <li>Device Profile <u>Claco</u></li> <li>Device Note:</li> <li>Network Device Group</li> <li>Cocation <u>Allos</u></li> <li>Device Type <u>Allows</u></li> <li>Set To Default</li> <li>Device Type <u>Allows</u></li> <li>Set To Default</li> <li>Device Type <u>Allows</u></li> <li>Set To Default</li> <li>Device Type <u>Allows</u></li> <li>Stated Secret <u>Constant</u></li> <li>Show</li> <li>CoA Port 1700 <u>Set To Default</u></li> <li>Brow</li> <li>RADIUS DTLS Settings ()</li> <li>DTLS Required ()</li> <li>Shared Secret <u>aduations</u> ()</li> </ul>			
Model Name   Software Version  Network Device Group  Location II Locations  Set To Default  IPSEC No Set To Default  Device Type  (RADIUS Authentication Settings  RADIUS UDP Settings  Protocol RADIUS  Show CoA Port 1700 Set To Default  RADIUS DTLS Settings  DLS Required  Now		* Device Profile dia Cisco v 🕀	
Software Version		Model Name v	
Network Device Group      Location Al Locations      Set To Default     IPSEC No     Set To Default     Device Type      Set To Default      Protocol RADIUS      RADIUS UDP Settings      Protocol RADIUS      Use Second Shared Secret     imset Show     CoA Port 1700     Set To Default      RADIUS DTLS Settings ()      DTLS Required [)      Shared Secret radiualdits     ()		Software Version	
* Network Device Group Location All Locations © Set To Default IPSEC No © Set To Default Device Type II Device Types © Set To Default * RADIUS Authentication Settings RADIUS UDP Settings Protocol RADIUS Use Second Shared Secret © Show CoA Port 1700 Set To Default RADIUS DTLS Settings () DTLS Required © () Shared Secret radiualdits ()			
Location All Locations Set. To Default IPSEC No Set. To Default Device Type III Device Type S Set. To Default • RADIUS Authentication Settings RADIUS UDP Settings Protocol RADIUS Use Second Shared Secret Show Use Second Shared Secret Show CoA Port 1700 Set. To Default RADIUS DTLS Settings () DTLS Required [] () Shared Secret radius/dtls ()		* Network Device Group	
IPSEC No Set To Default Device Type All Device Types Set To Default		Location All Locations Set To Default	
Device Type     All Device Types     Image: Contraction Settings     Protocol     RADIUS     Protocol     RADIUS     Protocol     Protocol     RADIUS     Use Second Shared Secret     Show   CoA Port   1700   Set To Default     PTLS Required   ()   Shared Secret   ()     Shared Secret     ()     Show     CoA Port   1700   Set To Default     OTLS Required   ()     Shared Secret     ()     Shared Secret     ()     Shared Secret     ()     Set To Default     ()     Shared Secret         Shared Secret     Shared Secret         Shared Secret     Share		IPSEC No. Set To Default	
RADIUS Authentication Settings      RADIUS UDP Settings      Protocol RADIUS      * Shared Secret			
RADIUS Authentication Settings   RADIUS UDP Settings   Protocol   RADIUS   * Shared Secret   * Show   Use Second Shared Secret   * Show   CoA Port   1700   Set To Default   RADIUS DTLS Settings ()   DTLS Required   Shared Secret   radius/dtts		Sec to behavior	
RADIUS Authentication Settings  RADIUS UDP Settings  Protocol RADIUS  Protocol RADIUS  Show Use Second Shared Secret  Show CoA Port 1700 Set To Default  RADIUS DTLS Settings  DTLS Required  DTLS Required			
RADIUS UDP Settings     Protocol   RADIUS   * Shared Secret   * Show   Use Second Shared Secret   * CoA Port   1700   Set To Default     RADIUS DTLS Settings ()   DTLS Required   * Shared Secret   * Shared Secret		RADIUS Authentication Settings	
Protocol RADIUS  Protocol RADIUS  *Shared Secret Show Use Second Shared Secret Show CoA Port 1700 Set To Default  RADIUS DTLS Settings ()  DTLS Required ()  Shared Secret radius/dtts ()		RADIUS LIDP Settings	
* Shared Secret Show Use Second Shared Secret Show Use Second Shared Secret Show CoA Port 1700		Protocol RADIUS	
Use Second Shared Secret () Show CoA Port 1700 Set. To Default RADIUS DTLS Settings () DTLS Required () Shared Secret radius/dtls ()		* Shared Secret	
CoA Port 1700 Set To Default RADIUS DTLS Settings () DTLS Required () Shared Secret radius/dtts ()			
CoA Port 1700 Set To Default RADIUS DTLS Settings () DTLS Required () Shared Secret radius/dtts ()		Use second shared secret	
CoA Port 1700 Set. To Default RADIUS DTLS Settings () DTLS Required () Shared Secret radius/dtts ()		Snow	
RADIUS DTLS Settings () DTLS Required () Shared Secret radius/dtls ()		CoA Port 1700 Set To Default	
DTLS Required  () Shared Secret radius/dtls ()		RADIUS DTLS Settings ()	
Shared Secret radius/dtts ()		DTLS Required	
		Shared Secret radius/dts	
CoA Port 2083 Set To Default		CoA Port 2083 Set To Default	
Issuer CA of ISE Certificates for CoA Select if required (optional)		Issuer CA of ISE Certificates for CoA Select if required (optional)	
DNS Name		DNS Name	
General Settings		General Settings	
Endote Keywrap		Enable Reywrap [] ()	
Show Show		Nov Show	
* Massaga Buthasticator Code Key		Message Authenticator Code Key Show	
Show		Key Input Format	

Schritt 6: Konfigurieren Sie vEdge/Controller.

```
system

aaa

auth-order radius local

radius

server 10.48.87.210

vpn 512

key cisco

exit

!

Schrift 7: Überprüfung Moldon S
```

Schritt 7: Überprüfung. Melden Sie sich bei vEdge an, und stellen Sie sicher, dass dem Remote-Benutzer die Netadmin-Gruppe zugewiesen ist.

SESSION	USER	CONTEXT	FROM	PROTO	GROUP	LOGIN TIME
33472	ekhabaro	cli	10.149.4.155	ssh	netadmin	2020-03-09T18:39:40+00:00

# TACACS-basierte Benutzerauthentifizierung und -autorisierung für vEdge und Controller

Schritt 1: Erstellen Sie ein TACACS-Profil. In diesem Schritt wird das erstellte TACACS-Profil einem authentifizierten Benutzer zugewiesen, z. B. der Ebene der Netadmin-Berechtigungen.

• Wählen Sie **Obligatorisch** im **Custom-Attribut-**Abschnitt aus, um das Attribut wie folgt hinzuzufügen:

TypNameWertObligatorisch Viptela-Gruppenname netadmin

dentity Services Engine	Home   Context Visibility   Operative	ations + Policy + Administration	Nork Centers	
Network Access     Guest Access	TrustSec      BYOD      Profiler      Po	osture		
Overview      Identities User Ident	ity Groups Ext Id Sources   Network R	esources Policy Elements Device Admin F	Policy Sets Reports Settings	
Conditions	TACACS Profiles > vEdge			
Network Conditions	Nam	vEdge_netadmin		
Allowed Protocols	Descriptio	n		
TACACS Command Sets				
TACACS Profiles	Task Attribute View R	aw View		
	Common Tasks			
	Common Task Type Shell \$			
	Default Privilege	٥	(Select 0 to 15)	
	Maximum Privilege	0	(Select 0 to 15)	
	Access Control List	0	1	
	C Auto Command	•	J	
	Addo Command	<b>V</b>	]	
	No Escape	0	(Select true or false)	
	Timeout	0	Minutes (0-9999)	
	Idle Time	0	Minutes (0-9999)	
	Custom Attributes			
	+ Add			۰.
	Type Na	ame Value		
	Mandatory \$ Vi	ptela-Group-Name netadmin	۲	√×
				_
				Cancel Save

Schritt 2: Erstellen Sie eine Gerätegruppe für SD-WAN.

cisce reaction of the context Visibility > Operat	tions  Policy  Administration  Work Centers	~ • • • •
System      Identity Management     Vetwork Resources     Device Portal Management	agement pxGrid Service + Feed Service + Threat Centric NAC	
Network Device Stroups     Network Device Profiles     External	RADIUS Servers RADIUS Server Sequences NAC Managers External MDM   Location Services	
Network Device Groups		
All Groups Choose group *		
C Refresh 🕇 Add Duplicate 🗇 Edit 🗎 Trash 👁 Show group in	members 🛎 Import 🔮 Export - 🗮 Flat Table 🧳 Expand All 🖌 Collapse All	o-
C Refresh     + Add     Duplicate     ⊘ Edit               Trash	members 🛎 Import 🗳 Export 🕶 🖩 Flat Table 🖍 Expand All 🗡 Collapse All Description No. of Network Devices	۰.
C Refresh	Description     No. of Network Devices       All Device Types	0-
Refresh + Add Duplicate C Edit Trash      Trash      Show group      Name      All Device Types      SD-WAN	members 2 Import 2 Export  Flat Table  Collapse All Collapse All Description No. of Network Devices All Device Types - 0	0-
Refresh + Add Duplicate & Edit      Trash      Show group      Name      * All Device Types      SD-WAN      All Locations	Description     No. of Network Devices       All Device Types     -       All Locations     -	0-
Refresh + Add Duplicate © Edit      Trash      Show group      Name      All Device Types      SD-WAN      All Locations      Is IPSEC Device	Description     No. of Network Devices       All Device Types     -       All Locations     -       Is this a RADIUS over IPSEC Device     -	0-

Add Group		×
Name *	SD-WAN	
Description		
Parent Group *	All Device Types	x <b>*</b>
		Cancel Save

Schritt 3: Konfigurieren Sie das Gerät, und weisen Sie es der SD-WAN-Gerätegruppe zu:

Network Devices List > vEdge-01	
Network Devices	
Description	
IP Address         * IP :         10.48.87.232         / 32	ŵ <b>.</b>
* Device Profile data Cisco ♥ ⊕ Model Name ♥ Software Version ♥	
* Network Device Group	
Location       All Locations       Set To Default         IPSEC       No       Set To Default         Device Type       SD-WAN       Set To Default	
RADIUS Authentication Settings	
✓ TACACS Authentication Settings	
Shared Secret Show Retire ( Enable Single Connect Mode Legacy Cisco Device TACACS Draft Compliance Single Connect Support	
SNMP Settings	
Advanced TrustSec Settings	
Save Reset	

Schritt 4: Definieren Sie die Gerätemanagement-Richtlinie.

Abhängig von Ihrer tatsächlichen Einrichtung sieht Ihr Richtliniensatz möglicherweise anders aus. Für die Demonstration in diesem Dokument wird die Richtlinie erstellt.

cisco	dentity Se	rvices Engine	Home	Context Visibi	lity ⊧ (	Operations	Policy	+ Administ	tration	· Work Centers						Q,	0	• •
Netv	ork Access	Guest Access	+ TrustSec	+ BYOD	Profiler	+ Posture	- Device Adr	ninistration	+ Passi	velD								
+ Over	view + k	dentities User Ide	ntity Groups	Ext Id Sources	<ul> <li>Network</li> </ul>	ork Resources	<ul> <li>Policy E</li> </ul>	lements	Device Ad	min Policy Sets	Reports	Settings						
Policy	Sets												Rese	Policy	set Hitcount		Reset	Save
+	Status	Policy Set Nam	e	Descriptio	n		Conditions						Allowed Protocols	Server	Sequence	Hits	Actions	View
Searc	h																	
/	ø	vEdges					DEV	ICE-Device	Type EQU	JALS All Device	lypes#SD-V	NAN	Default Device Adm	'n	x • +		٥	>
	ø	Default		Tacacs Def	ault policy s	iet							Default Device Adm	'n	×* +	0	٥	>
																	Reset	Save

Klicken Sie auf > und der nächste Bildschirm wird angezeigt, wie in diesem Bild gezeigt. Diese Richtlinie stimmt mit dem Gerätetyp **SD-WAN** überein und weist dem in Schritt 1 erstellten Shell-Profil das entsprechende Shell-Profil zu.

dudu Iden	tity Sen	vices Engine	Home	<ul> <li>Context Visibility</li> </ul>	y → Operations	+ Policy	/ + Admini	stration	·Work Cer	ters							• •
<ul> <li>Network.</li> </ul>	Access	Guest Access	<ul> <li>TrustSec</li> </ul>	BYOD → F	Profiler + Posture	* Device	Administration	Passiv	Clev								
<ul> <li>Overview</li> </ul>	r ⊁lde	intities User Ident	ity Groups	Ext Id Sources	<ul> <li>Network Resource</li> </ul>	s ≯ Pol	cy Elements	Device Adr	min Policy Se	ts Reports	Settings						
Policy Se	ets 🔸 v	vEdges											Reset	Policyset Hi	itcounts	Reset	Save
s	tatus	Policy Set Name		Description		Conditio	ons						1	Allowed Prote	ocols / Server	Sequence	Hits
Search																	
	Ø	vEdges					DEVICE-Device	Type EQU	ALS AI Dev	ce Types#SD-1	MAN			Default Devic	e Admin	×* +	0
> Auther	tication	Policy (1)															
> Author	ization P	Policy - Local Exc	eptions														
> Author	ization P	Policy - Global Ex	ceptions														
* Author	ization P	Policy (2)															
										lesults							
•	Status	Rule Name		Conditions	1				(	command Se	ts		Shell Profile	5		Hits	Actions
Search																_	
	ø	vEdge-netadmin		AL Iden	ntityGroup-Name EQU	IALS User	Identity Group	s:lab_admin				+	vEdge_neta	dmin	×* +	۰	٥
	ø	Default								× DenyAllCon	nmands	+	Deny All Sh	ell Profile	x * +	0	٥

Reset Save

#### Schritt 5: Konfigurieren Sie vEdge:

```
system
aaa
auth-order tacacs local
!
tacacs
server 10.48.87.210
vpn 512
key cisco
exit
!
!
```

Schritt 6: Überprüfung. Melden Sie sich bei vEdge an, und stellen Sie sicher, dass der Remote-Benutzer zugewiesene Netadmin-Gruppe:

vEdgeCloudl# show users AUTH SESSION USER CONTEXT FROM PROTO GROUP LOGIN TIME 33472 ekhabaro cli 10.149.4.155 ssh netadmin 2020-03-09T18:39:40+00:00

Schritt 5: Konfigurieren Sie vEdge:

Schritt 5: Konfigurieren Sie vEdge:

Schritt 5: Konfigurieren Sie vEdge:

#### Zugehörige Informationen

- Cisco ISE Device Administration-Prescriptive Deployment-Guide: <u>https://community.cisco.com/t5/security-documents/cisco-ise-device-administration-prescriptive-deployment-guide/ta-p/3738365#toc-hld-298630973</u>
- Konfigurieren von Benutzerzugriff und Authentifizierung: <u>https://sdwan-</u> <u>docs.cisco.com/Product\_Documentation/Software\_Features/Release\_18.4/02System\_and\_Int</u> <u>erfaces/03Configuring\_User\_Access\_and\_Authentication</u>