

ةدنتسملا ضيوفتلاو مدختسملا ةقداصم تادحوو vEdge ل RADIUS و TACACS ل ISE عم مكحتلا

تايوتحمل

[ةمدقملا](#)

[ةيساسألا تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[نيوكتلا](#)

[مكحتلا تادحوو vEdge ل ليوختلاو RADIUS ل ةدنتسملا مدختسملا ةقداصم](#)

[مكحتلا تادحوو vEdge ل TACACS ل ع نيئاقلا ضيوفتلاو مدختسملا ةقداصم](#)

[ةلص تاذا تامولعم](#)

ةمدقملا

RADIUS و TACACS ل ةدنتسملا مدختسملا ةقداصم نيوكت ةيفي ك دنتسملا اذه حضوي (ISE) ةيوهلا ةمدخ كرحم مادختساب مكحتلا تادحوو vEdge ل

ةيساسألا تابلطتملا

تابلطتملا

دنتسملا اذهل ةصاخ تابلطتم دجوت ال

ةمدختسملا تانوكملا

مكحتلا تادحوو vEdge-cloud ISE. نم 2.6 رادصإلا مادختسا مت، يحيضوتلا ضرعلا ضرغلو 19.2.1 رادصإلا لمعت يتلا

ةصاخ ةيلمعم ةئيبي في ةدوجوملا ةزهجالا نم دنتسملا اذه في ةدراولا تامولعمل عاشنإ مت تناك اذا (يضا رتفا). حوسمم نيوكتب دنتسملا اذه في ةمدختسملا ةزهجالا عيمج تادب رما يال لم تحملا ريثأتلل كمهف نم دكأتف، ليغشتلا ديقتك تكبش

نيوكتلا

ةتباثلا ني مدختسملا تاعومحمل عامسأ ةثالث Viptela جم انرب رفوي **basic**، **netadmin**، **operator**، **super** ل لقالا ل ع ةدحو و عومحمل مدختسملا نييعت بجي. ةيساسألا ةومحمل في ايئاقلت يضا رتفا ل TACACS/RADIUS.

مكحتلا تادحوو vEdge ل ليوختلاو RADIUS ل ةدنتسملا مدختسملا ةقداصم

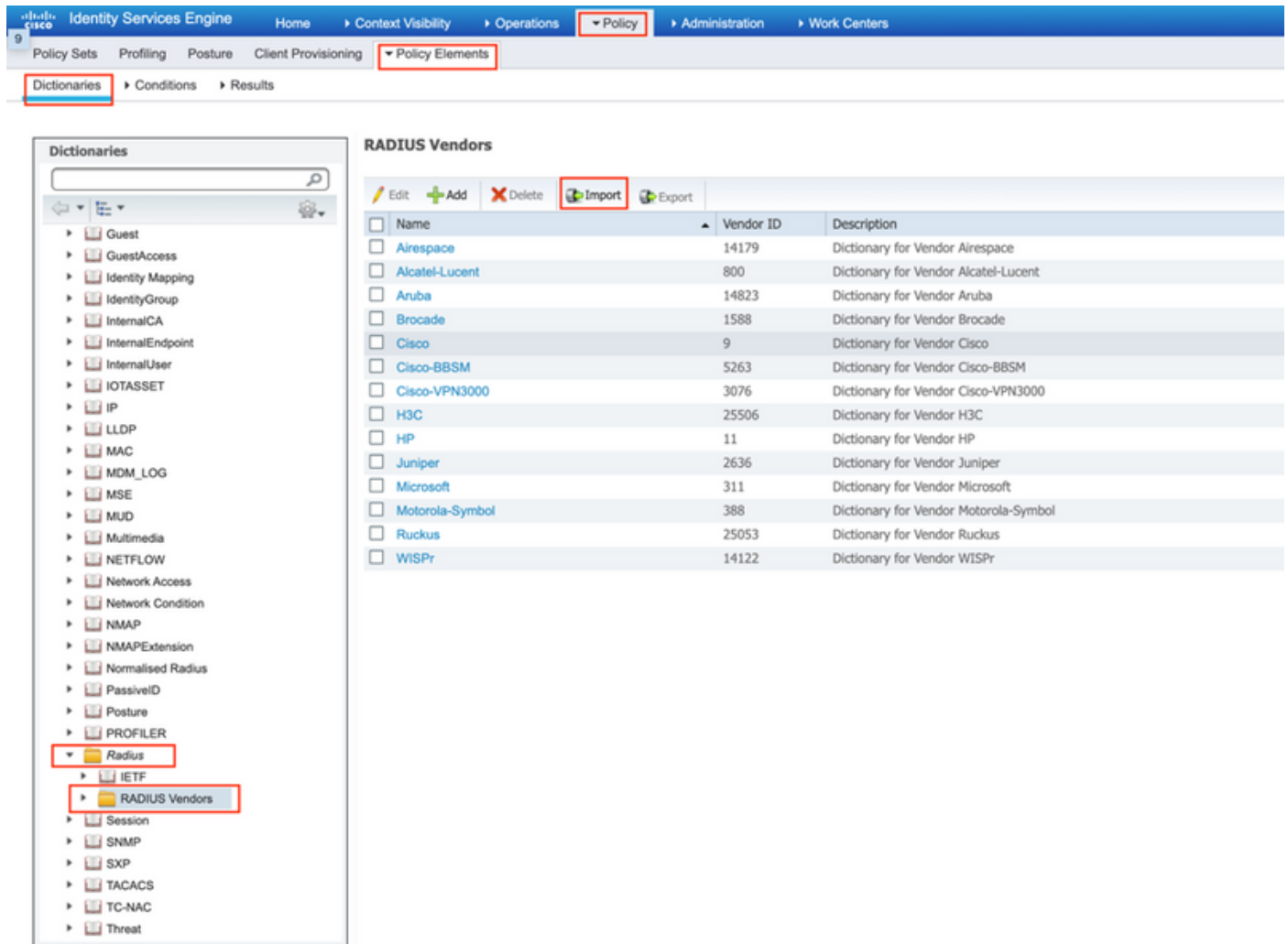
يُصنّف فلم عايشن أب مق ، كذّب مايق لل ل ISE ل Viptela radius سوماق عايشن أب مق 1. ةوطخلال
 وتحت حمل أب:

```
# -*- text -*-
#
# dictionary.viptela
#
#
# Version:      $Id$
#
VENDOR          Viptela                41916

BEGIN-VENDOR    Viptela

ATTRIBUTE       Viptela-Group-Name    1    string
```

> ةسايس لل رصانع > ةسايس لل إ ل لقتنا ، ضرغ لل اذهل إ ل إ سوماق لل ليمحت 2. ةوطخلال
 امك ، جارد إ رقتنا م رADIUS > رADIUS إ ل لقتنا نآل ، سيماق لل ةمئاق نم . سيماق لل
 ةروص حضورم وه



1. ةوطخلال ي ف هتأشنأ يذلا فلم لل ليمحتب نآل مق



Use this for to import a RADIUS Vendor. Select the file using the browser and click "Import".

* Vendor file:
 dictionary.viptela

Radius لي وخت فيرعت فلم موقية ووطخال هذه في. لي وخت فيرعت فلم عاشنإ. 3. ووطخال لقتنا، اذهل. هيلع قدصم مدختسم ل NetAdmin زايتما يوتسم، لاثملا ليبس لىع، نييغت ب نيتمدقتم ني تي صاخ دحو لي وختال صيصخت تافلم > ةسايسلا رصانع > ةسايس لىل ةروصلال في حضوم وه امك.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Policy Sets Profiling Posture Client Provisioning Policy Elements

Dictionarys Conditions Results

Authentication

Authorization

Authorization Profiles

Downloadable ACLs

Profiling

Posture

Client Provisioning

Authorization Profiles > vEdge-netadmin

Authorization Profile

Name vEdge-netadmin

Description

Access Type ACCESS_ACCEPT

Network Device Profile Cisco

Service Template

Track Movement

Passive Identity Tracking

Common Tasks

Advanced Attributes Settings

Radius:Service-Type = NAS Prompt

Viptela:Viptela-Group-Name = netadmin

Attributes Details

Access Type = ACCESS_ACCEPT

Service-Type = 7

Viptela-Group-Name = netadmin

Save Reset

ضرع ال ضارغأل .فل تخم لك شب جهن لل ةومجم و دبت دق ،يلع فال كدادع إى لع انب . 4 ةوطخل امك يف رطلال لوصولا ىم سى يذلا ةسايسال لاخذإ عاشنإ متي ،ةلاقملا هذه يف يحيضوتال ةروصلال يف حضوم وه .

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Policy Sets Profiling Posture Client Provisioning Policy Elements

Policy Sets

Reset Policyset Hitcounts Reset Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
✓	Terminal Access						
			Radius-NAS-Port-Type EQUALS Virtual				
				Default Network Access	2	⚙️	➔

ةروصلال يف حضوم وه امك ةيلالال ةشاشال رهظتو > رقنا .

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Policy Sets Profiling Posture Client Provisioning Policy Elements

Policy Sets → Terminal Access Reset Polycyset Hitcounts Reset Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Terminal Access		Radius-NAS-Port-Type EQUALS Virtual	Default Network Access	2
➤ Authentication Policy (1)					
➤ Authorization Policy - Local Exceptions					
➤ Authorization Policy - Global Exceptions					
▼ Authorization Policy (2)					

+	Status	Rule Name	Conditions	Results		Hits	Actions
				Profiles	Security Groups		
⋮	✓	vEdge-netadmin	IdentityGroup-Name EQUALS User Identity Groups:lab_admin	✖vEdge-netadmin	Select from list	1	⚙️
	✓	Default		✖DenyAccess	Select from list	0	⚙️

Reset Save

فلم ني عي و lab_admin ني مدخست سمل ة عوم جم في رعت فلم يل اذانت سا جهنلا اذ قباطتي
3. ة وطلخال يف هؤاشن مت لپوخت في رعت

ة روصلال يف حضورم وه امك (vEdge مكحت ة دحو وأ هوم) NAS في رعت ب مق 5. ة وطلخال

Identity Services Engine Administration

Network Resources

Network Devices List > vEdge-01

Network Devices

* Name: vEdge-01

Description: []

IP Address: 10.48.87.232 / 32

* Device Profile: Cisco

Model Name: []

Software Version: []

* Network Device Group

Location: All Locations [Set To Default]

IPSEC: No [Set To Default]

Device Type: All Device Types [Set To Default]

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/dtls

CoA Port: 2083 [Set To Default]

Issuer CA of ISE Certificates for CoA: Select if required (optional)

DNS Name: []

General Settings

Enable KeyWrap: []

* Key Encryption Key: [] [Show]

* Message Authenticator Code Key: [] [Show]

Key Input Format: ASCII (selected) / HEXADECIMAL

مكتمل الة دحو/vEdge ني وكت 6 ة ووطخ ل

```

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

```

ة وومجم ني عت نم دكأت و vEdge جم انرب ل ل وخذل ل ليجستب مق . ق قحت ل 7 ة ووطخ ل
دي ب ل م دختس ل ل NetAdmin

vEdgeCloud1# show users

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

تادحوو vEdge ل TACACS لى ع نيم ئاقال ضيوفت ل او مدخت س م ل ة ق داصم ل م كحت ل ل

TACACS فيرعت فلم نبيعت متي، ةوطخلال هذه في TACACS فيرعت فلم عاشن ل 1. ةوطخلال هت ق داصم تم مدخت س م ل NetAdmin زايتم اىوت س م، لاثم ل لى بس لى ع، هؤاشن ل مت يذال

- ة م س ل ل ة فاض ل ة ص ص م ل ة م س ل ل م س ق ن م ي م ا ز ل ل د د ح :
م س ل ل ع و ن ل ل ة م ي ق ل ل
Viptela Netadmin ويديف ل ل ة و م ج م م س ا ي م ا ز ل ل

The screenshot shows the Cisco Identity Services Engine (ISE) configuration page for a TACACS Profile. The page is titled "TACACS Profiles > vEdge" and "TACACS Profile". The "Name" field is set to "vEdge_netadmin" and is highlighted with a red box. Below the name field is a "Description" field. There are two tabs: "Task Attribute View" (selected) and "Raw View". Under "Common Tasks", the "Common Task Type" is set to "Shell". There are several checkboxes and dropdown menus for configuring tasks: "Default Privilege" (0 to 15), "Maximum Privilege" (0 to 15), "Access Control List", "Auto Command", "No Escape" (true or false), "Timeout" (0-9999 minutes), and "Idle Time" (0-9999 minutes). At the bottom, there is a "Custom Attributes" table with one attribute: "Mandatory" type, "Viptela-Group-Name" name, and "netadmin" value. The "Save" button is highlighted with a red box.

SD-WAN ل ة ز ه ج ة و م ج م عاشن ل 2. ةوطخلال

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM Location Services

Network Device Groups

All Groups Choose group

Refresh Add Duplicate Edit Trash Show group members Import Export Flat Table Expand All Collapse All

Name	Description	No. of Network Devices
All Device Types	All Device Types	--
SD-WAN		0
All Locations	All Locations	--
Is IPSEC Device	Is this a RADIUS over IPSEC Device	--

Add Group



Name *

SD-WAN

Description

Parent Group *

All Device Types



Cancel

Save

SD-WAN: زهجة ةوعومجم ىلإ هنييعةت وزاهجال نيوكتب مق 3. ةوطخلال

Network Devices

* Name

Description

IP Address * IP : /

* Device Profile

Model Name

Software Version

* Network Device Group

Location

IPSEC

Device Type

RADIUS Authentication Settings

TACACS Authentication Settings

Shared Secret ⓘ

Enable Single Connect Mode

Legacy Cisco Device

TACACS Draft Compliance Single Connect Support

SNMP Settings

Advanced TrustSec Settings

ةزهأل ةرادإ جهن دي دحت .4 ةوطخل

ضرعلا ضارغأل .فلتخم لكشب جهنلا ةعومجم وديت دق ،يلعفل دادعإلا ىلع ادامتعا ةسايسلا ءاشنإ متي ،دنتسما اذه يف يحيضوتلا

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Network Access Guest Access TrustSec BYOD Profiler Posture Device Administration PassiveID

Overview Identities User Identity Groups Ext Id Sources Network Resources Policy Elements Device Admin Policy Sets Reports Settings

Policy Sets

+	Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
<input type="checkbox"/>	<input checked="" type="checkbox"/>	vEdges		DEVICE Device Type EQUALS All Device Types#SD-WAN	Default Device Admin		<input type="button" value="Settings"/> <input type="button" value="Delete"/>	<input type="button" value="View"/>
<input checked="" type="checkbox"/>		Default	Tacacs Default policy set		Default Device Admin	0	<input type="button" value="Settings"/> <input type="button" value="Delete"/>	<input type="button" value="View"/>

عم جهنلا اذه قباطتي .ةروصلا هذه يف حضوم وه امك ةيلالتلا ةشاشلا رهظتو > قوف رقنا 1. ةوطخل يف ءاشنإ متي يذلا Shell فيرعت فلم نيءي و SD-WAN ىمسما زاهجال عون

Policy Sets → vEdges

Reset Policyset Hitcounts Reset Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	vEdges		DEVICE Device Type EQUALS All Device Types#SO-WAN	Default Device Admin	0
<p>Authentication Policy (1)</p> <p>Authorization Policy - Local Exceptions</p> <p>Authorization Policy - Global Exceptions</p> <p>Authorization Policy (2)</p>					

+	Status	Rule Name	Conditions	Results		Hits	Actions
				Command Sets	Shell Profiles		
+	✓	vEdge-netadmin	IdentityGroup Name EQUALS User Identity Groups:lab_admin	vEdge_netadmin		0	⚙️
+	✓	Default		DenyAllCommands	Deny All Shell Profile	0	⚙️

Reset Save

vEdge نيوكت 5. ةوطخال

```

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

```

ةومجم نيوكت نم دكأتو vEdge جم انرب ىل لوخدلا ليجستب مق. ققحتال 6. ةوطخال
ديعبال مدختسملل NetAdmin:

vEdgeCloud1# show users

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

vEdge نيوكت 5. ةوطخال

vEdge نيوكت 5. ةوطخال

vEdge نيوكت 5. ةوطخال

ةلص تاذا ماولعم

- ةزهجأة رادال يف رعتل رشنل ليلد Cisco ISE: <https://community.cisco.com/t5/security-documents/cisco-ise-device-administration-prescriptive-deployment-guide/ta-p/3738365#toc-hId-298630973>
- ةقداصل او مدختس مل لوصو نيوكت: https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/Release_18.4/02System_and_Interfaces/03Configuring_User_Access_and_Authentication

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا اذ ه Cisco ت مچرت
م ل ا ل ا ا ن ا ع مچ ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل و
ا م ك ة ق ي ق د ن و ك ت ن ل ة ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ي ل ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا دن ت س م ل ا