

ىلإ ۋەنەتسەمىلا مىختىسىملا ۋەقداشىم نېۋەك TACACS و RADIUS

تایوتیم

مدخل

مطابق بالإنجليزية

تاتل طت ملا

ةمدختسملاتانوكمل

نیوکل

مكحـتـلـاـتـادـجـوـوـ vEdgeـلـلـيـوـخـتـلـاوـ RADIUSـىـلـاـقـدـنـتـسـمـلـاـمـدـخـتـسـمـلـاـفـقـدـاصـمـ

میکنیم که این داده ها را در TACACS+ و vEdge میگیریم.

علم و تام ذات تاذ صقل

ةمدقمل

ل TACACS و radius ىل ا ئدنتسملار مدختسملار ئق داصم نويوكت ئيفيك دنتسملار اذه حضوي vEdge مادختسالاب مكحتلى تادح وو ISE.

ةيسيس ئاسلا تاپل طت ملا

تابلطتما

دنتس ملا اذهل ڦصاخ تاپل طتم دجوت ال

ةمـدـخـتـسـمـلـاـ تـانـوـكـمـلـا

يُتَلِّا مَكْحُولًا تَادِح وَوُو ISE نِمْ 2.6 رَادِص إِلَى مَادِخْتِسَا مَتِي، وَيَحْاضِي إِلَى ضَارِعٍ أَلْلَى 19.2.1 رَادِص إِلَى لِغْشَت

ڇاخ ڦيلمعم ڦئيب یف ڏدوجوملا ڙهنجألا نم دنتسملا اذه یف ڏراولما تامولعملاءشنا مت
تناك اذا (يضارتفا) حوسمم نيوكتب دنتسملا اذه یف ڏمدختسملا ڙهنجألا عيمج تأدب
رمأ یأل لمحملاريثأتلل كمهف نم داكتف، ليغشتلا ديق كتكبش

نیوکل

مكاحتلا تادح وو vEdge ل ليوختلاو RADIUS ىلإ ًادنتسملا مدخلتسملاء قداصم

يصن فلم عاشناب مق ، كلذب مایقلل Viptela radius ایشناب مق. 1. ۋەطخىلا:

```
# -*- text -*-
#
# dictionary.viptela
#
#
# Version:      $Id$
#
VENDOR          Viptela           41916
BEGIN-VENDOR    Viptela
ATTRIBUTE       Viptela-Group-Name   1     string
```

> ئەسايىسلار رصانع > ئەسايىسلار لىلىقتنىا، ضرغىلا اذەل. ئەسايىسلار لىلىقتنىا، ضرغىلا اذەل. 2. ۋەطخىلا وە امك داريتسا رقنىامىث RADIUS يىدرۇم > RADIUS سىيم اوچىلا ئەمەنەم. سىيم اوچىلا حضۇم.

The screenshot shows the Juniper Networks Identity Services Engine (ISE) web interface. The top navigation bar includes links for Home, Context Visibility, Operations, Policy (which is highlighted with a red box), Administration, and More Centers. Below the navigation, there are tabs for Policy Sets, Profiling, Posture, Client Provisioning, and Policy Elements (also highlighted with a red box). A breadcrumb trail indicates the current location: Dictionaries > Conditions > Results.

Dictionaries

- Radius (highlighted with a red box)
- Guest
- GuestAccess
- Identity Mapping
- IdentityGroup
- InternalCA
- InternalEndpoint
- InternalUser
- KPIASSET
- IP
- LLDP
- MAC
- NEIM_UDP
- NTP
- NUD
- Multimedia
- NETFLOW
- Network Access
- Network Condition
- RRM
- RRMPElement
- Normalized Radius
- Protocol
- Posture
- PROFILER
- Radius (highlighted with a red box)
- Radius (highlighted with a red box)
- RADIUS Vendor
- Session
- SNMP
- SSO
- TACACS
- TCAP
- Threat

RADIUS Vendors

Name	Vendor ID	Description
Airspace	10279	Dictionary for Vendor Airspace
Alcatel-Lucent	900	Dictionary for Vendor Alcatel-Lucent
Anuta	14023	Dictionary for Vendor Anuta
Brocade	1200	Dictionary for Vendor Brocade
Cisco	9	Dictionary for Vendor Cisco
Cisco-BBMM	1262	Dictionary for Vendor Cisco-BBMM
Cisco-EPIC3000	3076	Dictionary for Vendor Cisco-EPIC3000
H3C	25306	Dictionary for Vendor H3C
HP	11	Dictionary for Vendor HP
Juniper	2636	Dictionary for Vendor Juniper
Microsoft	2121	Dictionary for Vendor Microsoft
Motorola-Symbol	388	Dictionary for Vendor Motorola-Symbol
Ruckus	26013	Dictionary for Vendor Ruckus
WISPr	10232	Dictionary for Vendor WISPr

1. ۋەطخلا يف ھاتشنى يىذلا فلملا لىيەمەت بىمەق

The screenshot shows the Juniper Identity Services Engine interface. The top navigation bar includes links for Home, Context Visibility, Operations, Policy, Administration, and Work Centers. Below this, a sub-navigation bar shows Policy Sets, Profiling, Posture, Client Provisioning, and Policy Elements. The 'Policy Elements' link is currently active, indicated by a blue underline.

The main content area is titled 'Dictionaries'. On the left, a tree view lists various dictionary types: Guest, GuestAccess, Identity Mapping, IdentityGroup, InternalCA, InternalEndpoint, InternalUser, iGRASSET, IP, LLDP, MAC, MDM_LOG, MH, MUO, Multimedia, NETFLOW, Network Access, Network Condition, NMAP, NMAPExtension, Normalized Radius, PassiveID, Posture, PROFILE, Radius, iETF, RADIUS Vendors, Session, SNMP, SXP, TACACS, TCG-AAC, and Threat. The 'Radius' and 'RADIUS Vendors' nodes are highlighted with orange boxes.

To the right of the tree view, there is a message: "Use this for to import a RADIUS Vendor. Select the file using the browser and click "Import"." Below this is a form field labeled "Vendor file:" with a "Choose file" button and a text input field containing "dictionary.vptlist". At the bottom of this panel are "Import" and "Cancel" buttons.

لېۋەت خەت فېرىعەت فلم موقۇي، ۋەطخلا ھەذە يف. لېۋەت خەت فېرىعەت فلم ئاشنە 3. ۋەطخلا، لقتنى، اذەل. ھېلىع قىدىم مەدختىسىم NetAdmin زايىتىم نىيىعەت بىمەق، لاثىملارلا لىيەسلىك نىيتىمىدقىتم نىيتىصاخ دەحولېۋەتلىا صىيىچەت تافلم > ئاسايىسلار رەسانىع > ئاسايىسلىك رەسىمىنەرلا يف حەضور وەمك.

Identity Services Engine > Policy > Policy Elements > Results

Authorization Profiles > vijogo-netadmin

Authorization Profile

- Name: vijogo-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	=	RAD Prompt
Vptole-Vptole-Group-Name	=	netadmin

Attributes Details

- Access Type = ACCESS_ACCEPT
- Service Type = 2
- Vptole Group Name = netadmin

Save **Reset**

ضارغأ ل. كب صاخلا يلعل دادع إلل اقفو فلتخم لكشب جهنا لةعومجم ودب دق. 4. ةوطخل
لوصولا يمسي يذلا ةسايسلالا لاخدا عاشنامتى، ءلاقملاهذه يف يحييضوتلاضرعلا
ةروصلایف حضوم وه امك يفترطلا.

Identity Services Engine > Policy > Policy Sets

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
Green	Terminal Access			Radius Host, From Type: Virtual, To: Virtual	0	Actions	View
Green	Default Network Access			Radius Host, From Type: Virtual, To: Virtual	0	Actions	View

ةروصلایف حضوم وه امك ئيلاتلاداشلارهظاتو > رقنا.

The screenshot shows the Juniper Identity Services Engine interface. The top navigation bar includes links for Home, Context Visibility, Operations, Policy, Administration, and Work Centers. Below this, a secondary navigation bar shows Policy Sets, Profiling, Posture, Client Processing, and Policy Elements. The main content area is titled "Policy Sets > Terminal Access".

Policy Set Details:

- Status: Enabled
- Policy Set Name: Terminal Access
- Description: Radius NAS-Port-Type ISDN/ISI Virtual
- Conditions: Radius NAS-Port-Type ISDN/ISI Virtual
- Allowed Protocols / Server Sequence: Default Network Access
- Hits: 0

Rule Details:

- Rule Name: vEdge-connection
- Conditions: Member/Group Name: ISDN/ISI User Identity (Groups lab_admin)
- Actions: vEdge-connection, Select from list (disabled), Delete
- Default: Default, Select from list (disabled), Delete

Buttons at the bottom right include "Reset Policyset Hitcounts", "Reset", and "Save".

فلم نيعي و lab_admin نيمدخلت سمل اوعومجم فيرعت فلم ىل ادانتسا جهنا اذه قباطتي 3. ووطخلا يف هواشن! مت ليوخت فيرعت.

ةروصلالا يف حضوم وه امك (vEdge) مكحـت ةـدـحـو وـأـهـجـومـ) فيـرـعـتـبـ مـقـ. 5. ووطخـلـا.

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 Devices

Default Device

Device Security Settings

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

IPSEC: No

Device Type: All Device Types

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol: RADIUS

* Shared Secret: ****

Use Second Shared Secret:

CoA Port: 1700

RADIUS DTLS Settings

DTLS Required:

Shared Secret: radius/dtls

CoA Port: 2083

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

DNS Name:

General Settings

Enable KeyWrap:

* Key Encryption Key:

* Message Authenticator Code Key:

Key Input Format: ASCII (selected) HEXADECIMAL

مكاحتل اودج ونيوكت 6. ووطخل.

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

نـيـعـت نـم دـكـأـت و vEdge إـلـى لـوـخـدـلـا لـيـجـسـتـب مـقـ. قـقـحـتـلـا 7. ةـوـطـخـلـا دـيـعـبـلـا مـدـخـتـسـمـلـلـ.

```
vEdgeCloud1# show users
```

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

تادحوو TACACS vEdge ىلع نيمئاقلما ضيوفتلارا مدخلتسملاء قداصم مكحتلارا

- ک ۆم سلا ۆف اض إل ۆص صخ م لا ۆم سلا م سق نم ي م از لا د د ح

عونلا	مسالا	قميقل
ايمازلا	Viptela ويديفل اوعومجم مس	Netadmin

Screenshot of the Identity Services Engine interface showing the configuration of a TACACS+ Profile.

The navigation path is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Device Administration > Policies > Policy Elements > TACACS Profiles > [selected] vigeo.

TACACS Profile: vigeo

Common Tasks:

- Task Attribute View (selected)
- Rule View

Common Task Type: User

Custom Attributes:

Type	Name	Value
Mandatory	Mobile-Group-Name	Mobile

Buttons:

- (Cancel)
- Save**

ل ڈزہجأ ڈعو و مجم عاشن| 2. ڈوطخل ا

Screenshot of the Identity Services Engine interface showing the configuration of Network Device Groups.

The navigation path is: Home > Identity Management > Network Resources > Network Device Groups > Network Device Profiles > External RADIUS Servers > RADIUS Server Sequences > MAC Managers > External NDS > Location Services.

Network Device Groups:

AI Groups:

- All Devices
- Add
- Import
- Edit
- Export
- Show group numbers
- Import
- Export
- For Today
- Expand All
- Collapse All

Name	Description	No. of Network Devices
All Device Types	All Device Types	0
Mobile		0
All Locations	All Locations	0
In This or RADIUS over IPSEC Device	In This or RADIUS over IPSEC Device	0

Add Group



Name: SD-WAN

Description:

Parent Group: All Device Types

Cancel Save

3. ۋەچىمەنچىن SD-WAN ئىچىلىقىنى تېكىنلىك بىلدىرىنىڭ زەلەتلىكىنى دەرىجەلەمك.

Network Devices List > vEdge-01

Network Devices

* Name: vEdge-01

Description:

IP Address: 192.168.87.732

Device Profile: Clear

Model Name:

Software Version:

* Network Device Group:

Location: All Locations

IPsec: No

Device Type: SD-WAN

RADIUS Authentication Settings

TACACS+ Authentication Settings

Shared Secret: Show Hide

Enable Single Connect Mode:

Legacy Cisco Device

TACACS+ Draft Compliance Single Connect Support

SNMP Settings

Advanced TrustSec Settings

Save Reset

4. ۋەچىمەنچىن دىدەتلىكىنى تېكىنلىك بىلدىرىنىڭ زەلەتلىكىنى دەرىجەلەمك.

ضرع لـا ضارغأـل . كـب صـاخـلـا يـلـعـفـلـا دـادـعـإـلـلـ اـقـفـوـ فـلـتـخـمـ لـكـشـبـ جـهـنـلـا ةـعـوـمـجـمـ وـدـبـتـ دقـةـ سـاـيـسـلـا عـاـشـنـا مـتـيـ ، دـنـتـسـمـلـا اـذـهـ يـفـ يـحـيـضـوـتـلـا

The screenshot shows the 'Policy Sets' page in the Juniper ISE web interface. A policy set named 'vEdge' is selected. In the 'Conditions' section, there is a condition 'Device Type: vEdge'. Below it, the 'Default Device Admin' dropdown is highlighted with a red box. The top navigation bar includes links for Home, Context Visibility, Operations, Policy, Administration, Work Centers, Network Access, Guest Access, Trustlets, BYOD, Posture, Device Administration, and Device Admin Policy Sets.

عـمـ جـهـنـلـا اـذـهـ قـبـاطـتـيـ . رـوـصـلـا هـذـهـ يـفـ حـضـوـمـ وـهـ اـمـكـ ةـيـلـاتـلـا ةـشـاشـلـا رـهـظـتـوـ > قـوـفـ رـقـنـاـ 1ـ ـوـطـخـلـاـ يـفـ هـؤـاشـنـاـ مـتـيـ يـذـلـاـ Shـe~l~ فـيـرـعـتـ فـلـمـ نـيـعـيـوـ SD-WANـ مـسـمـلـاـ زـاـجـلـاـ عـونـ

The screenshot shows the 'Policy Sets' page with the 'vEdge' policy set expanded. It displays two rules: 'edge_automation' and 'Default'. The 'edge_automation' rule has a condition 'IdentityGroup Name: ISGKLB' and a command set 'edge_automation'. The 'Default' rule has a condition 'Any' and a command set 'Every In (Dual Profile)'. The 'Default Device Admin' dropdown is highlighted with a red box. The interface includes sections for Authentication Policy (1), Authorization Policy - Local Exceptions, Authorization Policy - Global Exceptions, and Authorization Policy (2).

نـيـوـكـتـ 5ـ ـوـطـخـلـاـ v~E~d~g~e~:

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

6. ۋە ئەنرپ ىل اسەتىپ مۇق. قىقەتلىا لىجىEdge vEdge نىيىعت نم دكأتو جمادىلدا ۋە ئەنرپ ىل اسەتىپ مۇق. قىقەتلىا لىجى سەمىللى دىعېلما مۇختىسىملى:

```
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	

ةلص تاذ تامولۇم

- Cisco ISE: <https://community.cisco.com/t5/security-documents/cisco-ise-device-administration-prescriptive-deployment-guide/ta-p/3738365#toc-hld-298630973>
- SD-WAN: <https://sdwan-docs.cisco.com/Product Documentation/Software Features/Release 18.4/02System and Interface>

هـ لـ وـ لـ جـ رـ تـ لـ اـ هـ ذـ هـ

ةـ يـ لـ آـ لـ اـ تـ اـ يـ نـ قـ تـ لـ اـ نـ مـ مـ جـ مـ وـ عـ مـ اـ دـ خـ تـ سـ اـ بـ دـ نـ تـ سـ مـ لـ اـ اـ ذـ هـ تـ مـ جـ رـ تـ
لـ اـ عـ لـ اـ ءـ اـ حـ نـ اـ عـ يـ مـ جـ يـ فـ نـ يـ مـ دـ خـ تـ سـ مـ لـ لـ مـ عـ دـ ئـ وـ تـ حـ مـ يـ دـ قـ تـ لـ ةـ يـ رـ شـ بـ لـ اـ وـ
اـ مـ كـ ةـ قـ يـ قـ دـ نـ وـ كـ تـ نـ لـ ةـ يـ لـ آـ ةـ مـ جـ رـ تـ لـ ضـ فـ اـ نـ اـ ةـ ظـ حـ اـ لـ مـ ئـ جـ رـ يـ .ـ صـ اـ خـ لـ اـ مـ هـ تـ غـ لـ بـ
يـ لـ خـ تـ .ـ فـ رـ تـ حـ مـ مـ جـ رـ تـ مـ اـ هـ دـ قـ يـ يـ تـ لـ اـ ةـ يـ فـ اـ رـ تـ حـ اـ لـ اـ ةـ مـ جـ رـ تـ لـ اـ عـ مـ لـ اـ حـ لـ اـ وـ
ىـ لـ إـ أـ مـ ئـ اـ دـ عـ وـ جـ رـ لـ اـ بـ يـ صـ وـ تـ وـ تـ اـ مـ جـ رـ تـ لـ اـ هـ ذـ هـ ةـ قـ دـ نـ عـ اـ هـ تـ يـ لـ وـ ئـ سـ مـ
(رـ فـ وـ تـ مـ طـ بـ اـ رـ لـ اـ)ـ يـ لـ صـ أـ لـ اـ يـ زـ يـ لـ جـ نـ إـ لـ اـ دـ نـ تـ سـ مـ لـ اـ).