

# ههجاول ةيچراخ ةقداصمك ISE نيوكت DNAC ل (GUI) ةيموسرلا مدختسمل

## تايوتحمل

---

[ةمدقملا](#)

[ةيساسال تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسمل تانوكملا](#)

[عدبلال بق](#)

[نيوكتل](#)

[RADIUS مادختساب ةيچراخل DNAC ةقداصم نيوكت \(1 رايخ\)](#)

[RADIUS ل ISE نيوكت مق \(1 رايخ\)](#)

[TACACS+ مادختساب ةيچراخل DNAC ةقداصم نيوكت \(2 رايخل\)](#)

[TACACS+ ل ISE نيوكت \(2 رايخل\)](#)

[فحصل نم ققحتلا](#)

[RADIUS نيوكت نم ققحتلا](#)

[TACACS+ نيوكت نم ققحتلا](#)

[اهجالص او عاطخل افاشكتسا](#)

[عجارملا](#)

---

## ةمدقملا

cisco ل ةيچراخ ةقداصمك (ISE) Cisco Identity Services Engine ل كشي نأ فيك ةقيثو اذه فصوي  
GUI زكرم DNA.

## ةيساسال تابلطتملا

### تابلطتملا

عوضوم اذه نم ةفرعم تنأ يقلتني نأ ي صوي cisco:

- RADIUS و TACACS+ تالوكوتورب.
- Cisco نم (DNA) ةيمقرلا ةكبشلا ةينب زكرم عم Cisco ISE جمدم.
- Cisco ISE ةسايس مبيقت.

### ةمدختسمل تانوكملا

ةيلالل ةيدامل تانوكملا او جماربل تارادصا ل دننتسمل اذه في ةدراولا تامولعمل دننتست:

- Cisco Identity Services Engine (ISE)، رادصإلا 3.4 Patch1.
- Cisco، رادصإلا 2.3.5.5 نم ةيمقرلا ةكبشلا ةينب زكرم.

ةصاخ ةي لمعم ةئيب يف ةدوجوملا ةزهجالا نم دنتسملا اذه يف ةدراوللا تامولعمللا ءاشنإ مت تناك اذا .(يضارتفا) حوسمم نيوكتب دنتسملا اذه يف ةمدختسُملا ةزهجالا عيمج تادب رما يأل لم تحملا ريثأتلل كمهف نم دكأتف ،لغشتلا ديقتك تكبش

## ءدبلا لبق

- > تاداعإل اظنلا ىلع هنيوكت مت لقألا ىلع دحاو RADIUS ةقداصم مداخ دوجو نم دكأت ةسايسلا ةقداصملا مداوخ > ةيجراخلا تامدخل
- ءارجإلا اذه ذيفنت DNAC ىلع SUPER-Admin-Role تانودأ هيدل مدختسمل طقف نكمي
- ةيجراخلا ةقداصملا ةيطايتحالا ةقيرطاللا نييعت نيكمت

 ةينب زكرم عجري ،ةيجراخلا ةقداصملا نيكمت دنع ، 2.1.x نم مدقألا تارادصلإا يف :ريذحت لباق ريغ AAA مداخ ناك اذا نييني لحملا نيمدختسمللا ىلإ Cisco نم ةيمقرلا ةكبشلا زكرم عجري ال ،يلاحلا رادصلإا يف .فورعم ريغ مدختسمل مسأ AAA مداخ ضفر وأ لوصول ريغ AAA مداخ ناك اذا نييني لحملا نيمدختسمللا ىلإ Cisco نم ةيمقرلا ةكبشلا ةينب نييعت نيكمت دنع .فورعم ريغ مدختسمل مسأ AAA مداخ ضفر وأ لوصول لباق نييني لحملا نيمدختسمللا نكمي ،ةيجراخلا ةقداصملا ةيطايتحالا ةقيرطاللا نم (DNA) ةيمقرلا ةكبشلا ةينب زكرم ىلإ لوخدلا ليحست نييني لحملا ني لوؤسمل او Cisco.

زكرم ليثم لاخدا ىلع SSH لوكتورب لمعي ،ةيجراخلا ةيطايتحالا ةقداصملا ةزيم نيكمتل (MAGCTL rbac external\_auth\_backback enable) اذه (CLI) رماوأل رطس ةهجاو رما لخدأو Cisco نم (DNA) ةيمقرلا ةكبشلا ةينب (external\_auth\_backback enable).

## نيوكتلا

### RADIUS مادختساب ةيجراخلا DNAC ةقداصم نيوكت (1 رايخ)

ةصصخم راودأ ديذحتب مق (يرايختإ) 1. ةوطخلا راودأ مادختسإ كنكمي ،كلذ نم ادب ،كتابلطتمب يفت يتلا ةصصخملا راودألا نيوكتب مق نومدختسمللا > بيوبتلا تامالع ماظن نم كلذب مايقلا نكمي .ةيضارتفاللا مدختسمللا رودلا ىلإ دنتسمللا لوصوللا يف مكحتلا > راودألا

### ءارجإلا

ديج رود ءاشنإ أ.

### Create a New Role

Define the name of the role, and then provide an optional description. To make it easier to assign roles down the road, describe the role as clearly as possible.

1

Role Name\*  
**DevOps-Role**

Describe the role (optional)

2

Next

رود DevOps

لوصول في رتب مق. ب.

### Define the Access

These permissions enable different capabilities in Cisco DNA Center, some of which are inter-dependent. Before making the selections, please ensure you understand the details of what each of these permissions allow. Click here to [Learn More](#).

1

Define the **DevOps-Role** role. Custom roles permit or restrict user access to certain Cisco DNA Center functions. By default, roles are configured with Read permission, which is an Observer role. If a role is configured with Deny permission, all related content for that capability is removed from the GUI.

Access	Permission	Description
> Assurance	<input checked="" type="radio"/> Deny <input type="radio"/> Read <input type="radio"/> Write	Assure consistent service levels with complete visibility across all aspects of your network.
> Network Analytics	<input type="radio"/> Deny <input checked="" type="radio"/> Read <input type="radio"/> Write	Access to Network Analytics related components.
> Network Design	<input checked="" type="radio"/> Deny <input type="radio"/> Read <input type="radio"/> Write	Set up network hierarchy, update your software image repository, and configure network profiles and settings for managing your sites and network devices.
> Network Provision	<input checked="" type="radio"/> Deny <input type="radio"/> Read <input type="radio"/> Write	Configure, upgrade, provision and manage your network devices.
> Network Services	<input checked="" type="radio"/> Deny <input type="radio"/> Read <input type="radio"/> Write	Configure additional capabilities on the network beyond basic network connectivity and access.
> Platform	<input type="radio"/> Deny <input checked="" type="radio"/> Read <input type="radio"/> Write	Open platform for accessible intent-based workflows, data exchange, notifications, and third-party app integrations.
> Security	<input checked="" type="radio"/> Deny <input type="radio"/> Read <input type="radio"/> Write	Manage and control secure access to the network.

2

Next

رود DevOps لوصول

دي رول اءاشن ا ج.

Cisco DNA Center Create a User Role

**Summary**  
Review the **DevOps-Role** role. Make sure all the details are as you expect them to be. If you need to change something, clicking edit will take you back to that section

Role Name & Description **Edit**  
Role Name DevOps-Role  
Role Description

Role Capability **Edit**

**ASSURANCE**  
Monitoring and Troubleshooting Deny  
Monitoring Settings Deny  
Troubleshooting Tools Deny

**NETWORK ANALYTICS**  
Data Access Read

**NETWORK DESIGN**  
Advanced Network Settings Deny  
Image Repository Deny  
Network Hierarchy Deny  
Network Profiles Deny  
Network Settings Deny  
Virtual Network Deny

Exit Back Create Role

رود صخلم DevOps

Cisco DNA Center Create a User Role

network Device Deny  
Port Management Deny  
Topology Deny  
License Deny  
Network Telemetry Deny  
PnP Deny  
Provision Deny

**NETWORK SERVICES**  
App Hosting Deny  
Bonjour Deny  
Stealthwatch Deny  
Umbrella Deny

**PLATFORM**  
APIs Write  
Bundles Write  
Events Write  
Reports Write

**SECURITY**  
Group-Based Policy Deny  
IP Based Access Control Deny  
Security Advisories Deny

**SYSTEM**  
Machine Reasoning Deny  
System Management Deny

Exit Back Create Role

هؤاشن او DevOps رود ةعجارم

RADIUS مادختساب ةيجراخال ةقداصم لن يوكتب مق 2. ةوطخال

ةيجراخال ةقداصم ل > راودأل او نومدختسم ل > بيوبتل تامال ع ماظن نم كلذب مايقل لنكم ي

ءارخال

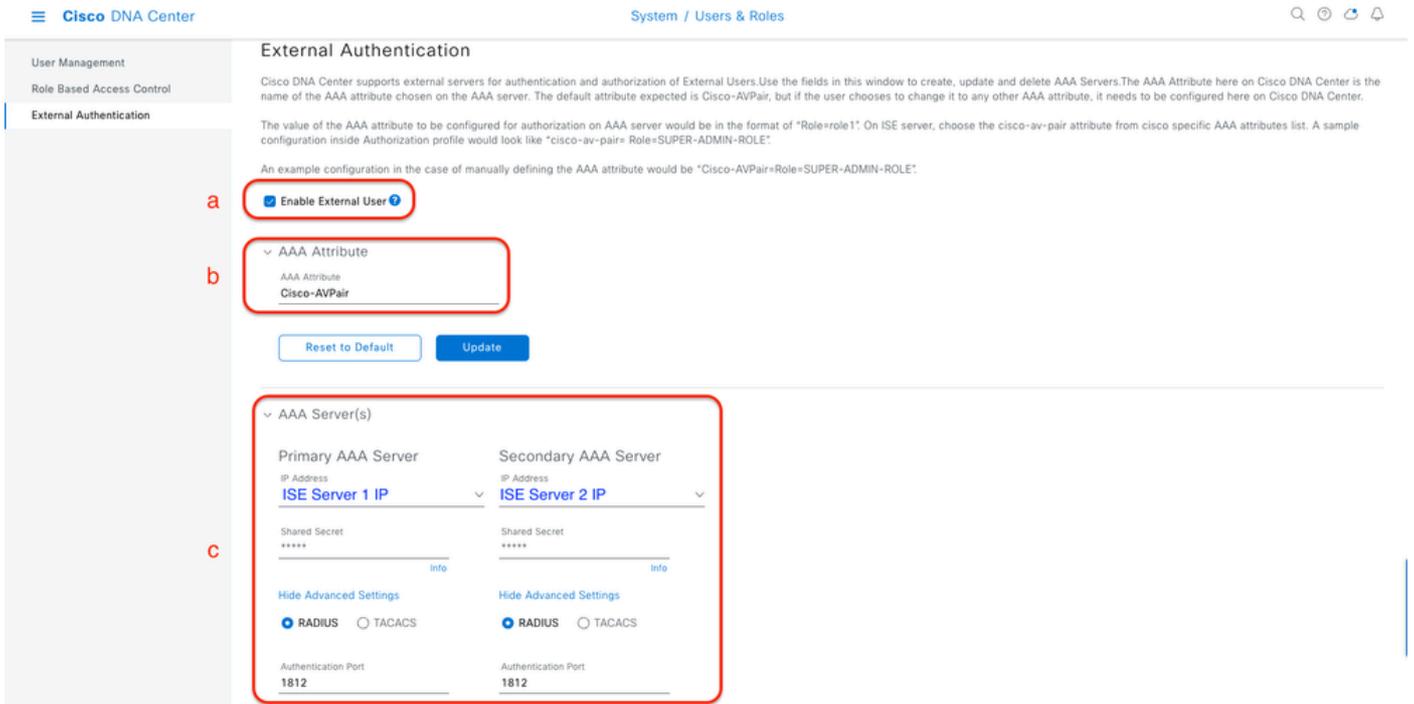
ةناخ دح، Cisco نم (DNA) ةيمقرلة ةكبشلة ةينب زكرم يفة يجراخال ةقداصم لن يكمتل أ. يجراخال مدختسم لن يكمتل رايخال

ب. AAA تامس طبض.

ل. اجم راعش aaa ل ي في cisco-AVPair تلخد.

ي. وناث لاو يس اساس ال AAA م داخ ني وكت ب مق (ي رايتخا). ج.

م داخ لا نم لك ىلع وا، لقا ال ىلع يس اساس ال AAA م داخ ىلع RADIUS لوكوتورب ني كمت نم دكأت ي. وناث لا م داخ لاو يس اساس ال.



ة ج راخ لا ل ق داصم لا ني وكت تاوطخ (RADIUS)

## ISE ل RADIUS ني وكت ب مق (1 رايتخ)

ISE. ىلع ةكبش زاكج DNAC م داخ ةفاض ا. 1 ةوطخ لا

ةكبش لا ةزهجأ > ةكبش لا دراوم > ب ي وبت لا ةمالع ةرادا نم لك لذب مايق لا نكمي

ءارح لا

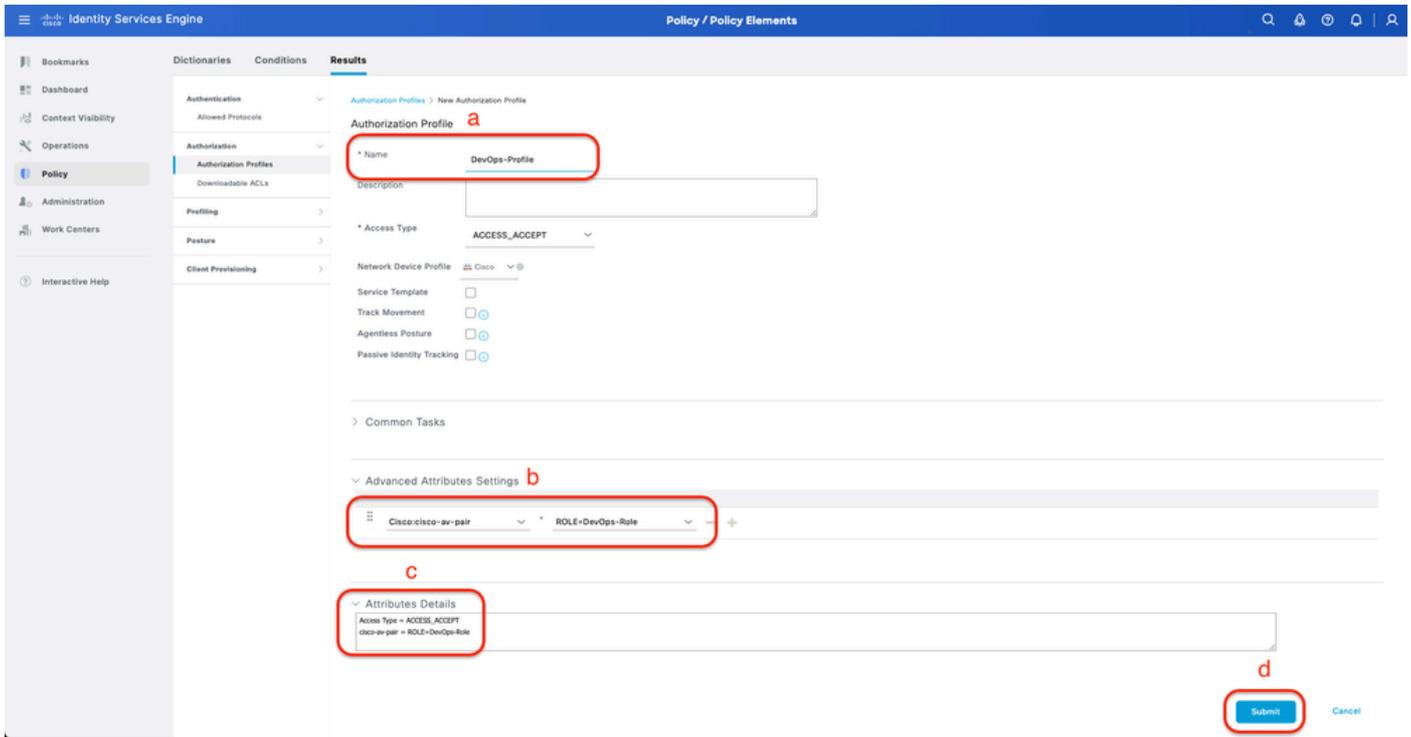
أ. IP و ةكبش لا زاكج مسا (DNAC) في رعت ب مق.

ب. جهن لا ةعومجم طرشل زاكج لا عون في نصت (ي رايتخا).

ج. RADIUS ةق داصم تااداع ني كمت.

د. كرتشم لا RADIUS رس طبض.





ضيوفتال فيرعت فلم عاشن

نيم دختسم ةعومجم عاشن 3. ةوطخال

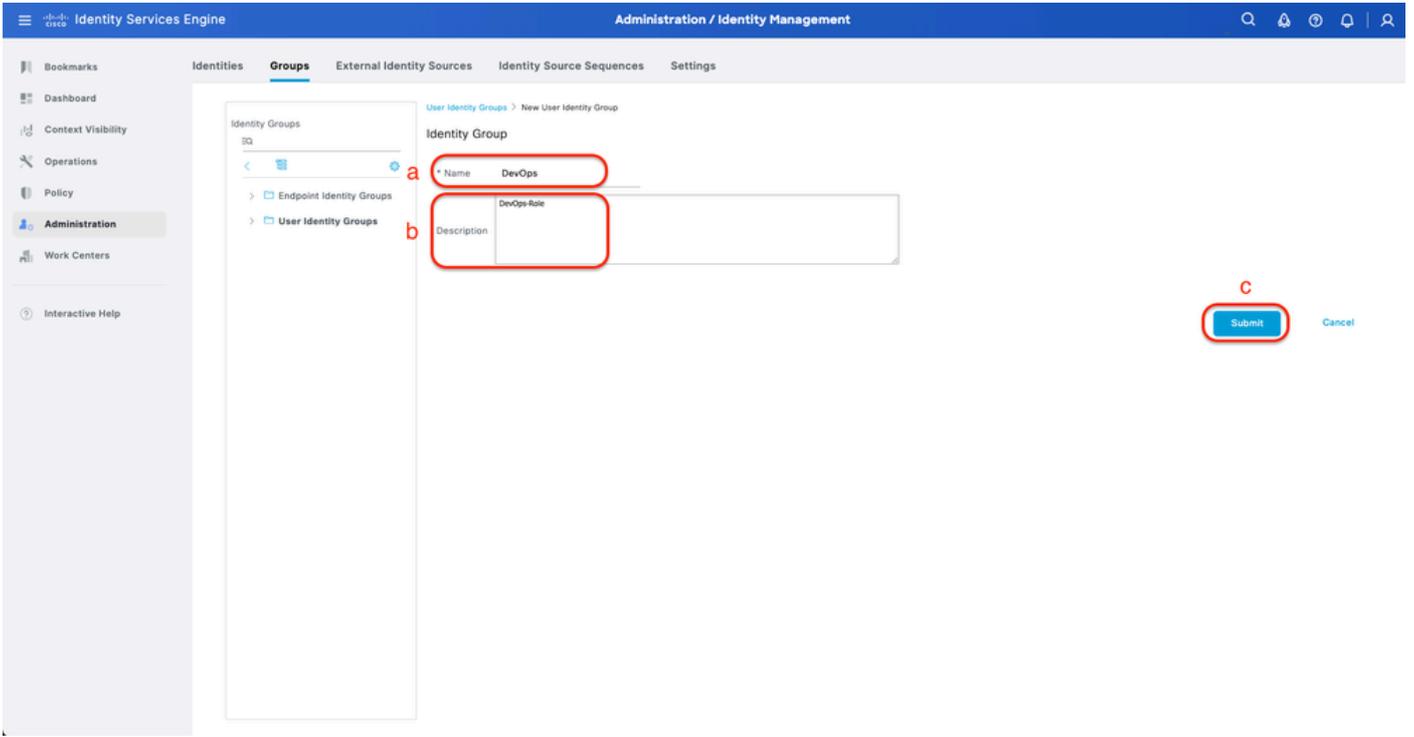
م دختسم لةي وه ةاعومجم ل > ةي وه ل ةراد > بي وبتال ةراد نم كلذب ماي قلال نكمي

ءارجال

ةي وه لةعومجم مسا دحو ةفاضا قوف رقنا أ.

فصولا فيرعت ب مق (ي رايتخا) ب.

ل اسرا قوف رقنا ج.



مدخستسمل ةيوة ةومجم ءاشن

ي.لحم مدخستسم ءاشن. 4 ةوطخل

ن.مدخستسمل > تايوهال > ةيوهال ةرادا > ةلودجال ةرادا نم كلذ متي نأ نكمي

ءارجال

أ. ل username ل نيءي و فيضي ةق طقط.

ب. ل و خدل ليجست رورم ةم لك نيءي عتب مق.

ج. ةلصل تا ذ ني مدخستسمل ةومجم ل مدخستسمل ةفاضا.

د. ل اسرا قوف رونا.

1-2 ي ل ح م م د خ ت س م ء ا ش ن ا

2-2 ي ل ح م م د خ ت س م ء ا ش ن ا

RADIUS جهن ة و م ح م ء ا (ي ر ا ي ت خ ا). 5 ة و ط خ ل ا

جهن ل ا ت ا و م ح م > جهن ل ا ب ي و ب ت ل ا ة م ا ل ع ن م ك ل ذ ب م ا ي ق ل ل ن ك م ي

ء ا ر ج ا ل ا

(ه ا ل ع ا ء ي د ج ف ص ج ا ر د ا) ر ت خ ا و ت ا ي ل م ع ق و ف ر ق ن ا ا.

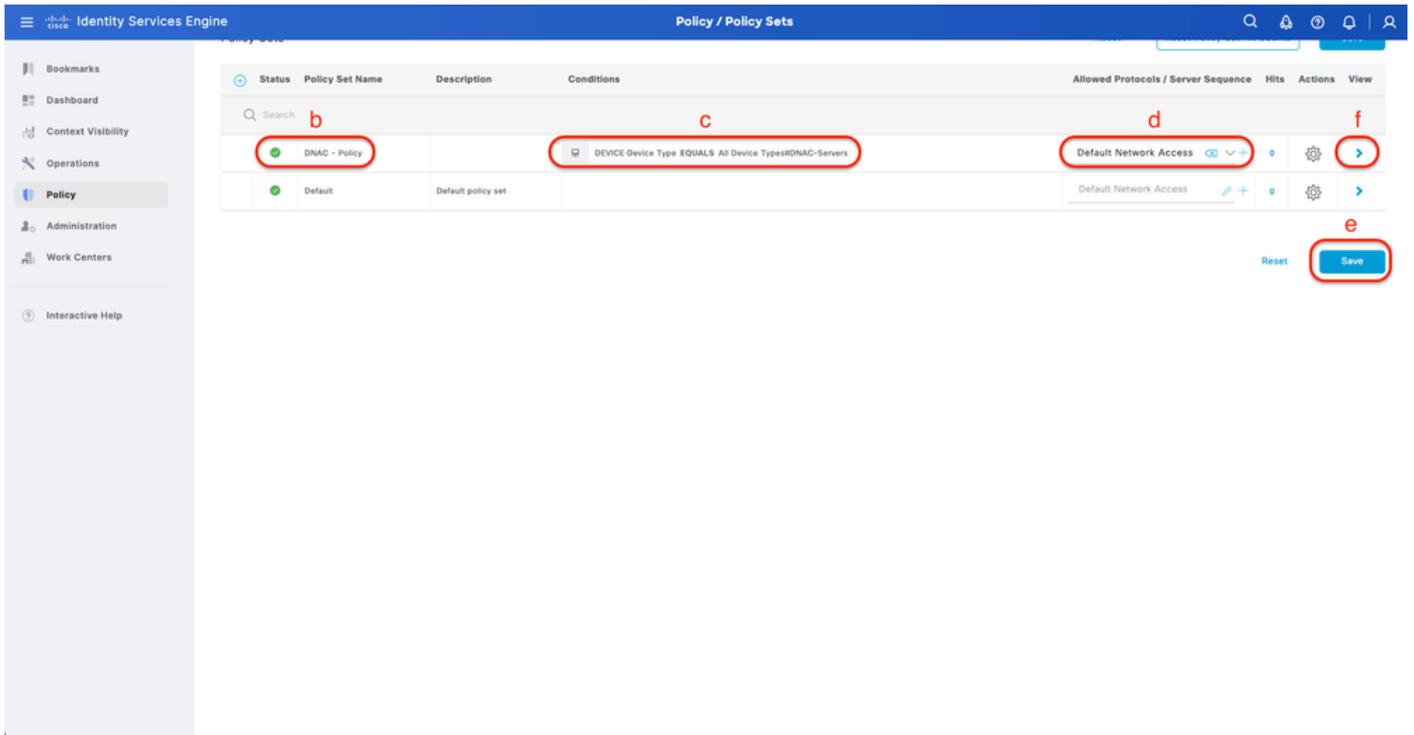
ج. ه ن ل ا ة و م ج م س ا د ي ح ت ب م ق .

ي ف ا ق ب س م ه ئ ا ش ن ا ب ت م ق ي ذ ل ا ز ا ه ج ل ا ع و ن د ي ح ت ل ت ا س ا ي س ل ا ة و م ج م ط ر ش ن ي ي ع ت ب م ق . ج .  
( $1 > b$ ) ة و ط خ ل ل ا .

د. ا ه ب ح و م س م ل ا ت ا ل و ك و ت و ر ب ل ا ن ي ي ع ت ب م ق .

ه. ظ ف ح ق و ف ر ق ن ا .

و. ض ي و ف ت ل ا و ة ق د ا ص م ل ا د ع ا و ق ن ي و ك ت ل ت ا س ا ي س ل ا ة و م ج م ض ر ع ة ق ي ر ط (>) ق و ف ر ق ن ا .



RADIUS ج ه ن ة و م ج م ة ف ا ض ا |

RADIUS ة ق د ا ص م ة س ا ي س ن ي و ك ت . 6 ة و ط خ ل ل ا .

(>) ق و ف ر ق ن ا > ج ه ن ل ا ت ا ع و م ج م > ج ه ن ل ا ب ي و ب ت ل ا ة م ا ل ع ن م ك ل ذ ب م ا ي ق ل ل ن ك م ي

ء ا ر ج ل ا

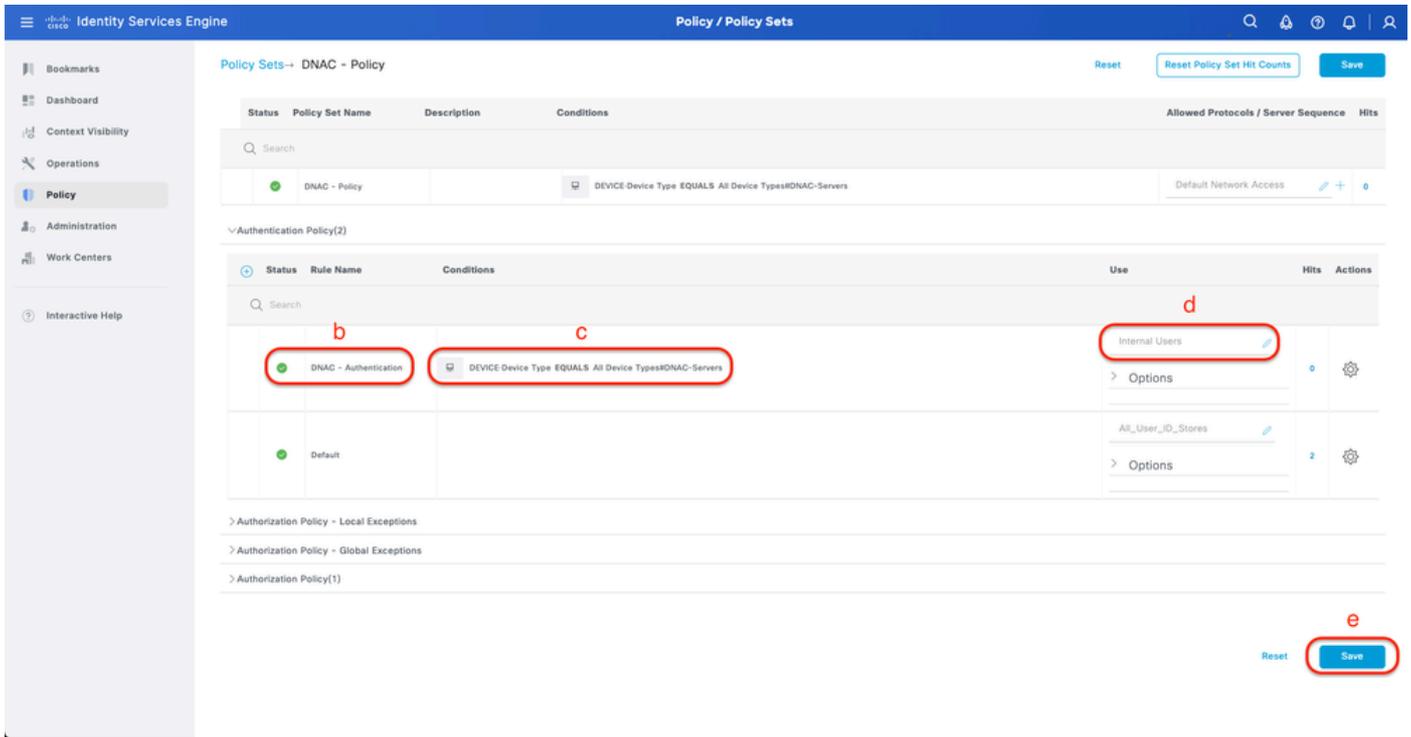
أ. (ه ا ل ع ا د ي د ج ف ص ج ا ر د ا) ر ت خ ا و ت ا ي ل م ع ق و ف ر ق ن ا .

ب. ة ق د ا ص م ل ا ج ه ن م س ا د ي ح ت ب م ق .

ي ف ا ق ب س م ه ئ ا ش ن ا ب ت م ق ي ذ ل ا ز ا ه ج ل ا ع و ن د ح و ة ق د ا ص م ل ا ة س ا ي س ط ر ش ن ي ي ع ت ب م ق . ج .  
( $1 > b$ ) ة و ط خ ل ل ا .

د. ة ي و ه ل ر د ص م ل ة ق د ا ص م ل ا ج ه ن م ا د خ ت س ا ن ي ي ع ت .

ه. ظ ف ح ق و ف ر ق ن ا .



RADIUS ةقداصم ةسايس ةفاضل

RADIUS ضيوفت ةسايس نيوكت 7 ةوطخلال

(>) قوف رقنا > جهنل اتاعومجم > جهنل بيوبتل ةمالع نم كلذب مايقل نكمي

مدختسم رود لكل ليوخت جهن عاشنال ةوطخلال هذه

- Super-admin-Role
- Network-admin رود
- DevOps رود

ءارجال

(هالعا دي دج فص جاردا) رتخاو تايلمع قوف رقنا أ.

ليوختل جهن مسا دي دحتب مق ب.

هئاشناب تمق يتل نيمدختسم ل ةومجم دي دحتو ليوختل ةسايس طارش نيبيعتب مق ج. (3 ةوطخلال) في

تمق يذل ليوختل فيرعت فلم دي دحتو ليوختل جهن فيرعت تافلماجئاتن نيبيعتب مق د. (2 ةوطخلال) في هئاشناب

ظفح قوف رقنا هـ.

The screenshot displays the Cisco ISE Policy / Policy Sets configuration interface. The main table shows the 'DNAC - Policy' set with a search filter 'DEVICE-Device Type EQUALS All Device Types#DNAC-Servers'. Below, a detailed view of a rule is shown with columns for Status, Rule Name, Conditions, Profiles, Security Groups, Hits, and Actions. Red boxes highlight specific elements: 'b' highlights the rule name 'Super Admin', 'c' highlights the condition 'IdentityGroup-Name EQUALS User Identity Groups: SUPER-ADMIN', 'd' highlights the profile 'Super-Admin\_Role\_Pr...', and 'a' highlights the gear icon in the Actions column. A 'Save' button is highlighted with 'e'.

ليوختال جهن ةفاضل

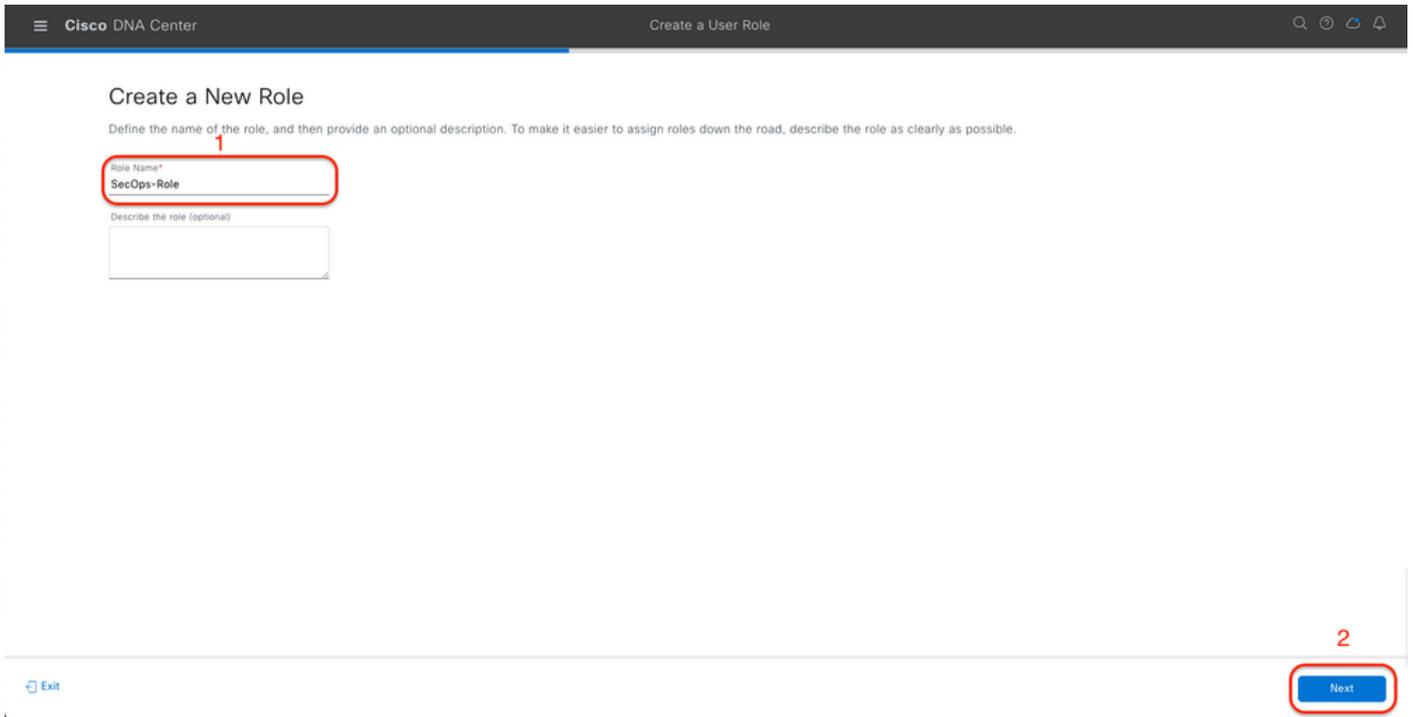
## TACACS+ مادختساب ةي ج راخال DNAC ةق داصم نيوكت (2 رايخال)

ةصصخم راودأ دي دحتب مق (ي رايخا). 1 ةوطخلا

راودأ مادختساب كنكمي، كلذ نم ال دب، كتابلطتمب يفت يتال ةصصخمملا راودألا نيوكت ب مق نوم دختسملا > بيوبتال تامالع ماظن نم كلذب مايقلال نكمي. ةيضارتفالال مدختسملا رودلا يلإ دن تسملا لوصولا يف مكحتال > راودألاو

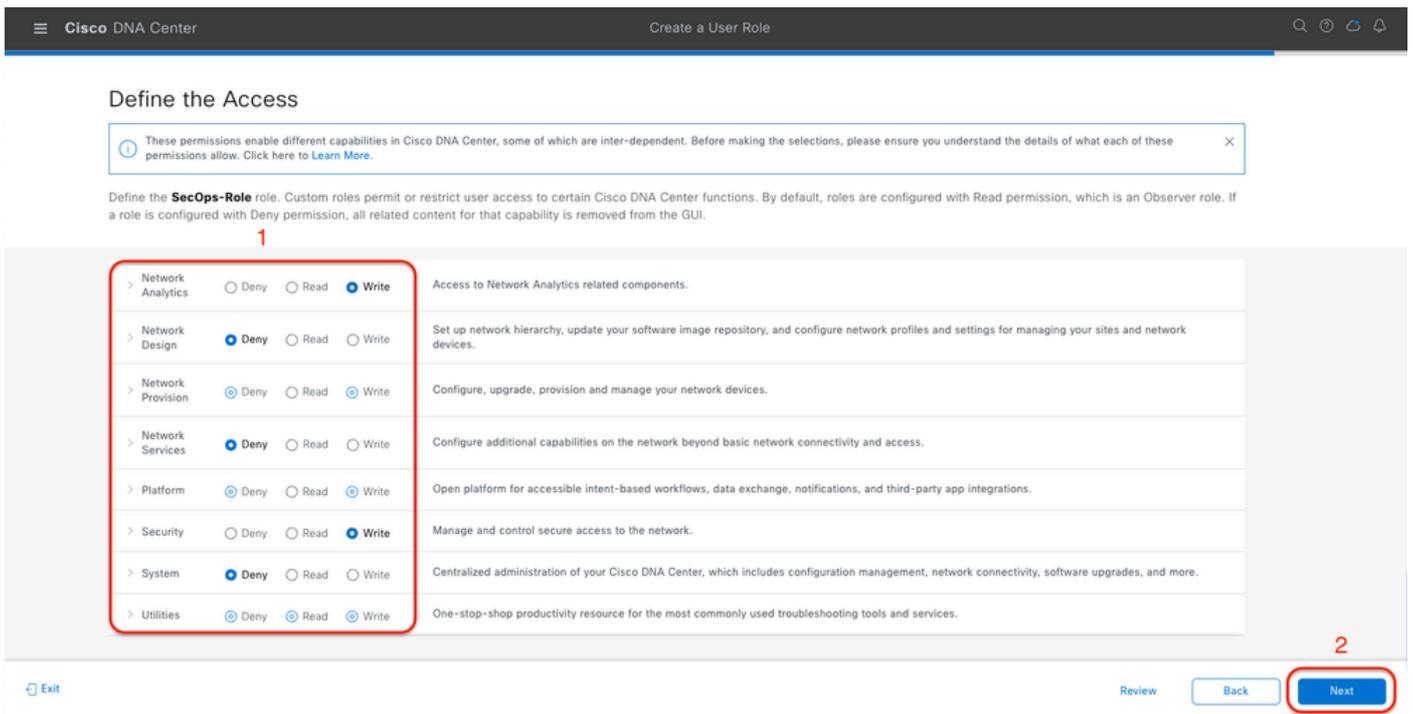
ءارجال

دي دج رود ءاشنإ أ.



SecOps رود مس

لوصول في رعب مق ب.



SecOPS رود لوصول

دي رول لوصول اشن ج.

Cisco DNA Center Create a User Role

### Summary

Review the **SecOps-Role** role. Make sure all the details are as you expect them to be. If you need to change something, clicking edit will take you back to that section.

Role Name & Description [Edit](#)

Role Name	SecOps-Role
Role Description	

Role Capability [Edit](#)

**ASSURANCE**

Monitoring and Troubleshooting	Deny
Monitoring Settings	Deny
Troubleshooting Tools	Deny

**NETWORK ANALYTICS**

Data Access	Write
-------------	-------

**NETWORK DESIGN**

Advanced Network Settings	Deny
Image Repository	Deny
Network Hierarchy	Deny
Network Profiles	Deny
Network Settings	Deny
Virtual Network	Deny

[Exit](#) [Back](#) [Create Role](#)

SecOps رود صخلم

Cisco DNA Center Create a User Role

PnP	Deny
Provision	Deny

**NETWORK SERVICES**

App Hosting	Deny
Bonjour	Deny
Stealthwatch	Deny
Umbrella	Deny

**PLATFORM**

APIs	Write
Bundles	Deny
Events	Deny
Reports	Deny

**SECURITY**

Group-Based Policy	Write
IP Based Access Control	Write
Security Advisories	Write

**SYSTEM**

Machine Reasoning	Deny
System Management	Deny

**UTILITIES**

Audit Log	Deny
Event Viewer	Read
Network Reasoner	Read

[Exit](#) [Back](#) [Create Role](#) <sup>1</sup>

هؤاشنإو SecOps رود ةعجارم

TACACS+ مادختساب ةيجراخلال ةقداصملا نيوكت 2 ةوطخلال ةيجراخلال ةقداصملا > راودأل او نومدختسملا > بيوبتلا تامالع ماظن نم كلذب مايقلا نكمي.

ةناخ ددح، Cisco نم (DNA) ةيمقرلا ةكبشللا ةينب زكرم يف ةيجراخلال ةقداصملا نيكمتل أ. ةيجراخلال مدختسملا نيكمت رايختالا.

AAA تامس طبض ب.

ل.اجم راعش aaa ل يف cisco-AVPair تلخد.

يوناثال او ياساس ال AAA م داخ نيوك ت ب مق (يراي خا) ج.

نم لك ىلع وا ،لق ال ىلع ياساس ال AAA م داخ ىلع TACACS+ لوكوت ورب نيكم ت نم دك ات  
يوناثال م داخ ل او يلوال م داخ ل

The screenshot shows the 'External Authentication' configuration page in Cisco DNA Center. The page is titled 'System / Users & Roles'. The left sidebar shows 'User Management', 'Role Based Access Control', and 'External Authentication'. The main content area has a heading 'External Authentication' and a sub-heading 'External Authentication'. Below this, there is a section 'Enable External User' with a checked checkbox. Below that is a section 'AAA Attribute' with a dropdown menu set to 'Cisco-AVPair'. Below that are two sections for 'AAA Server(s)', each with a dropdown menu for 'IP Address' (set to 'ISE Server 1 IP' and 'ISE Server 2 IP' respectively) and a 'Shared Secret' field. There are also radio buttons for 'RADIUS' and 'TACACS+' and a 'Port' field set to '49'. The page has a 'Reset to Default' button and an 'Update' button.

ةيخراخ لاق داصم ل نيوك ت تاوطخ (TACACS+)

## تازاخ ل ةرادا ةم داخ نيكم ت ب مق 1. ةوطخ ل

زهج ل ةرادا ةم داخ نيكم ت ب مق 1. ةوطخ ل  
> ريرحت > رشن ل > ماظن ل > بيوبت ل تامال ةرادا نم لك لذب مايق ل نكم ي  
ةزهج ل ةرادا ةم داخ نيكم ت ب مق 1. ةوطخ ل

The screenshot shows the 'Administration / System' page in Identity Services Engine. The page has a sidebar with 'Bookmarks', 'Dashboard', 'Context Visibility', 'Operations', 'Policy', 'Administration', 'Work Centers', and 'Interactive Help'. The main content area has a heading 'Administration / System' and a sub-heading 'Administration / System'. Below this, there are several sections: 'Administration' (checked), 'Monitoring' (checked), 'Policy Service' (checked), and 'pxGrid' (checked). The 'Enable Device Admin Service' checkbox is highlighted with a red box and labeled '1'. The 'Save' button is highlighted with a red box and labeled '2'.

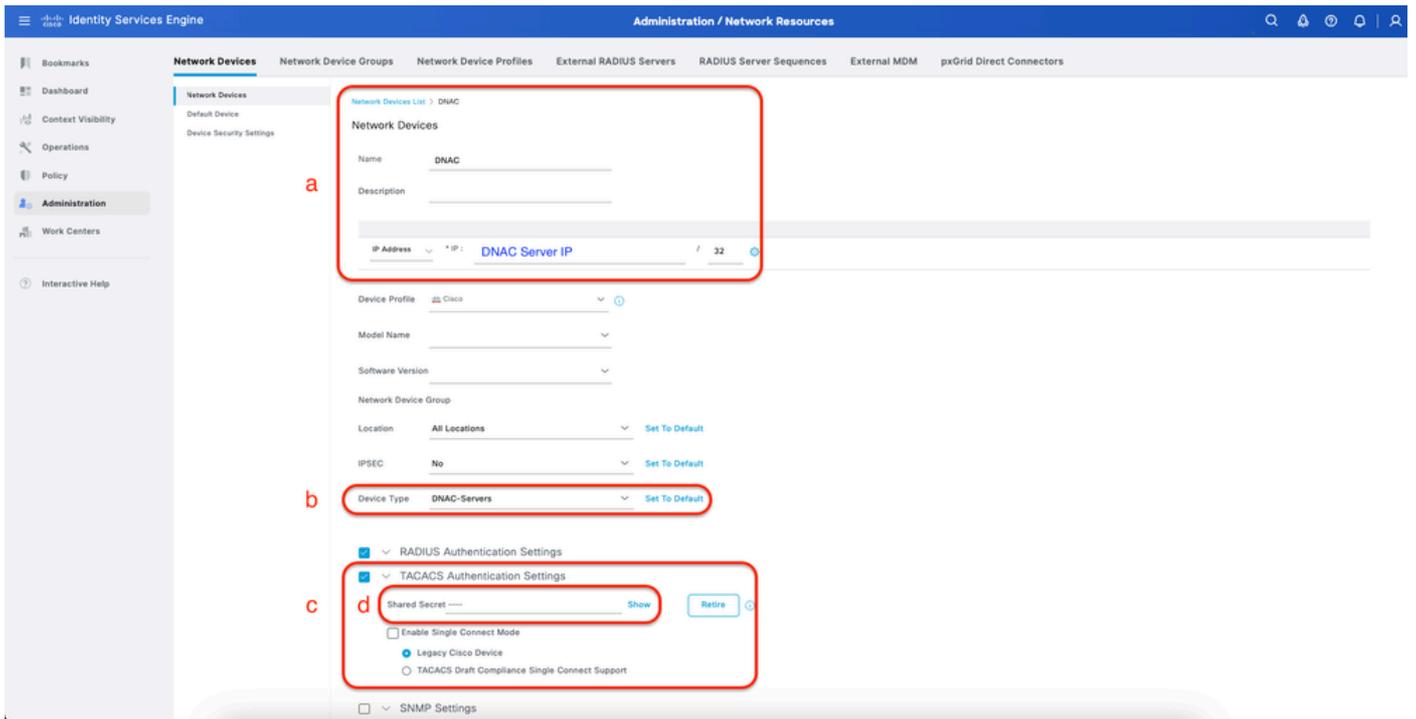
زاهجلا ةرادا ةمدخ نيكم ت

ISE ىل ةكبش زاهجك DNAC مداخل ةفاضلا 2. ةوطخل

ةكبشلا ةزهجا > ةكبشلا دراوم > بيوبتلا ةمالع ةرادا نم كلذب مايقلا نكمي

ءارجالا

- أ. IP و ةكبشلا زاهج مسا (DNAC) فيرعتب مق.
- ب. جهنلا ةومجم طرشل زاهجلا عون فينصت (ياري تخا).
- ج. TACACS+ ةقداصم تاداعلا نيكم ت ج.
- د. كرتشمل TACACS+ رس طبض د.



TACACS+ ل (DNAC) ISE ةكبش زاهج

DNAC رود لكل TACACS+ تافي صوت ءاشنلا 3. ةوطخل

> ةسايسلا رصانع > زاهجلا ةرادا > لمعلا زكارم بيوبتلا ةمالع نم كلذب مايقلا نكمي  
TACACS+ فيرعت تافل م > جئاتنلا

رود لكل في صوت عقاوب، فاعضا 3 ل دعمب TACACS+ تافي صوت ئشنأ: ةظحالم  
مدختسم.

ءارجالا

TACACS+ فيرعت فلم مسا ددحو ةفاضلا ىل رقنا أ.

م.اخ ضرع بيوبتلا ةمالع قوف رقنا ب.

ج.حيصلال مدختسمل رود علمب مق و Cisco-AVPair=ROLE= لخدأ c.

- م دختسم لارودل ةبسن لابل (SecOps-Role)، لخدأ Cisco-AVPair=ROLE=SecOps-Role.
- م دختسم لارودل ةبسن لابل (network-admin-role)، لخدأ Cisco-AVPair=ROLE=network-admin-role.
- م دختسم لارودل ةبسن لابل (super-admin-role)، لخدأ Cisco-AVPair=ROLE=super-admin-role.

نم دكأت و فرحألا ةلأجل ةساسح يه (Cisco-AVPair=ROLE=) AVPair ةميق ركذت: ةظالم DNAC. م دختسم لارودل اهتق باطم.

## د. ظفح قوف رقنا.

نإش ففرفعت TACACS (SecOps\_Role) ففلم ءاشن

نم دختسم لارودل ةبسن لابل ءاشن. 4 ةوطخل

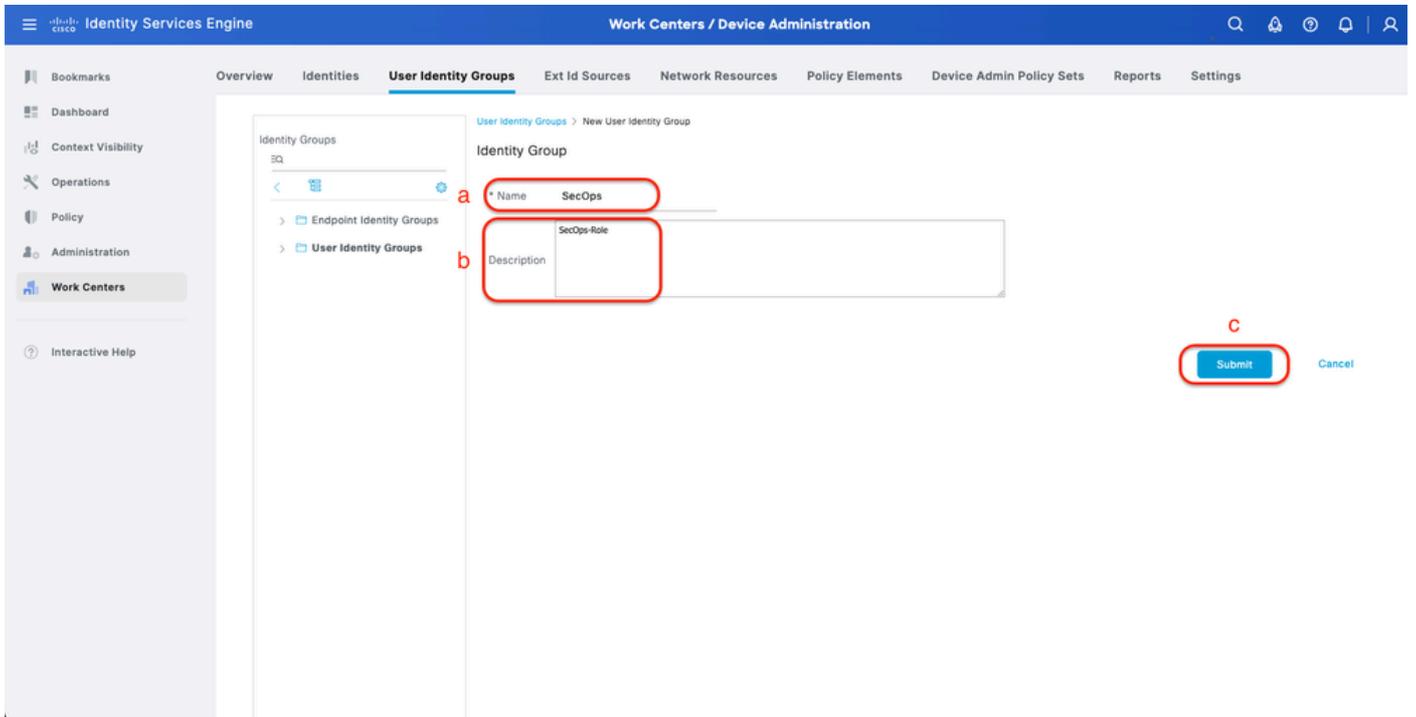
م دختسم لارودل ءاشن ءاعومجم > زاهجلا ةرادإ > لم ءال زكارم ببيو بتلا ءمالع نم لكذب مايقلا نكمي

ءارجلال

ءاشن لارودل ءاعومجم مسا ددحو ءفاضا قوف رقنا أ.

فصولا ففرفعت ب مق (فراي تخا) ب.

لارودل قوف رقنا ج.



مدخستسملا ةيوه ةعومجم عاشن

يحلحم مدخستسم عاشن 5. ةوطخل

نمدخستسملا > تايوهلا > زاهجال ةرادا > لمعال زكارم ةلودج نم كلذ متي نا نكمي

ءارجلإ

أ. username ل نيعي و فيضي ةق طقط.

ب. لودخل ليجست رورم ةملك نيعتت مق.

ج. ةلصل تاذنمدخستسملا ةعومجم ل مدخستسملا ةفاضل.

د. لاسرا قوف رقنا.

1-2 يلحم مدخستسم عاشن

2-2 يلحم مدخستسم عاشن

TACACS+ جهن ةوعومجم فضا (يراي تخا). 6 ةوطخلا

تاعومجم > ةزهجال ةرادا > (لمعال زكارم) Work Center بيوبتل طاقن نم كلذب مايقل نكمي ةزهجال ةرادا جهن

ءارجال

(هالعا ديذ فص جاردا) رتخاو تايلمع قوف رقنا أ.

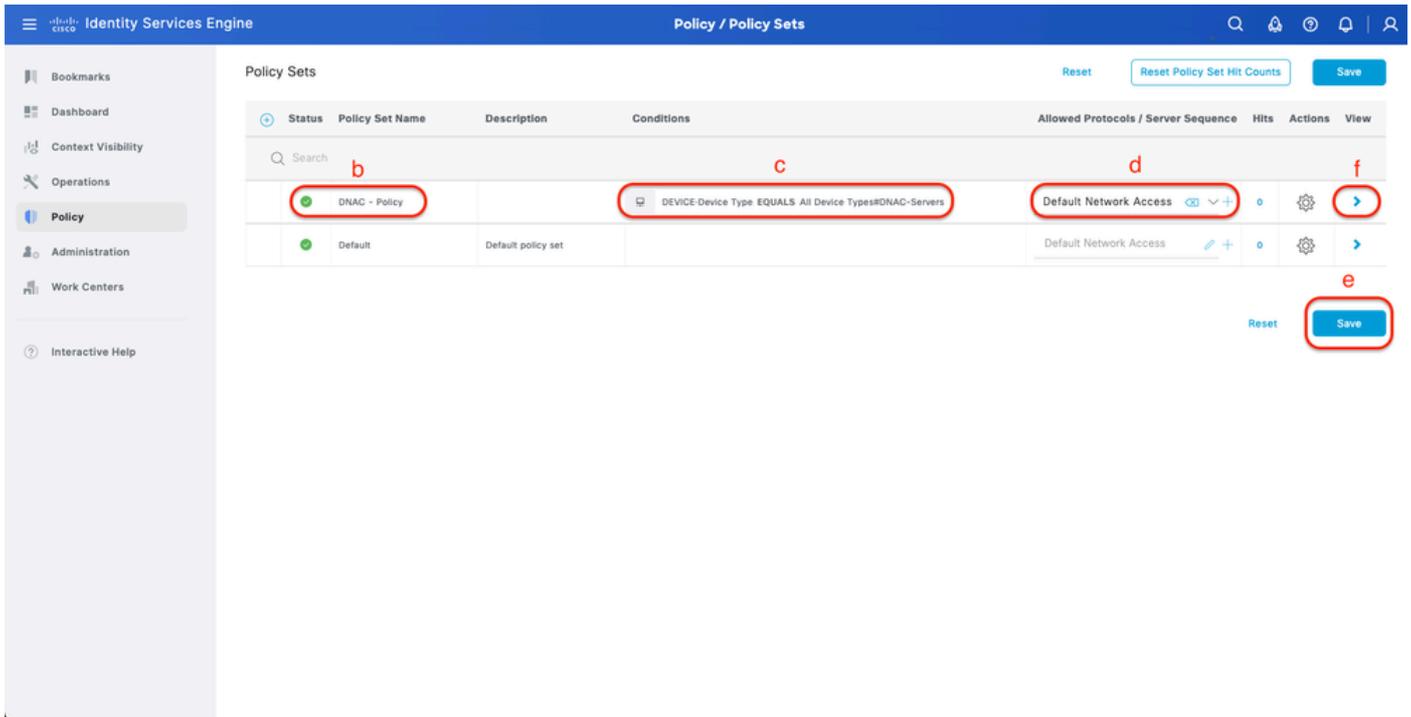
ج. ه ن ل ل ة و م ج م س ا د ي ح ت ب م ق . ب

ي ف ا ق ب س م ه ئ ا ش ن ا ب ت م ق ي ذ ل ا ز ا ه ج ل ا ع و ن د ي ح ت ل ت ا س ا ي س ل ل ة و م ج م ط ر ش ن ي ي ع ت ب م ق . ج  
( $2 > b$  ة و ط خ ل ل).

د. ا ه ب ح و م س م ل ا ت ا ل و ك و ت و ر ب ل ا ن ي ي ع ت ب م ق . د

ه. ظ ف ح ق و ف ر ق ن ا . ه

و. ض ي و ف ت ل ا و ة ق د ا ص م ل ا د ع ا و ق ن ي و ك ت ل ت ا س ا ي س ل ل ة و م ج م ض ر ع ة ق ي ر ط (>) ق و ف ر ق ن ا . و



TACACS+ ج ه ن ة و م ج م ة ف ا ض ا |

TACACS+ ة ق د ا ص م ة س ا ي س ن ي و ك ت . 7 ة و ط خ ل ل

ة ر ا د ا ت ا س ا ي س ت ا ع و م ج م > ز ا ه ج ل ا ة ر ا د ا > ل م ع ل ا ز ك ا ر م ب ي و ب ت ل ا ة م ا ل ع ن م ك ل ذ ب م ا ي ق ل ل ن ك م ي  
(>) ق و ف ر ق ن ا > ة ز ه ج ا ل ا

ء ا ر ج ا ل ا

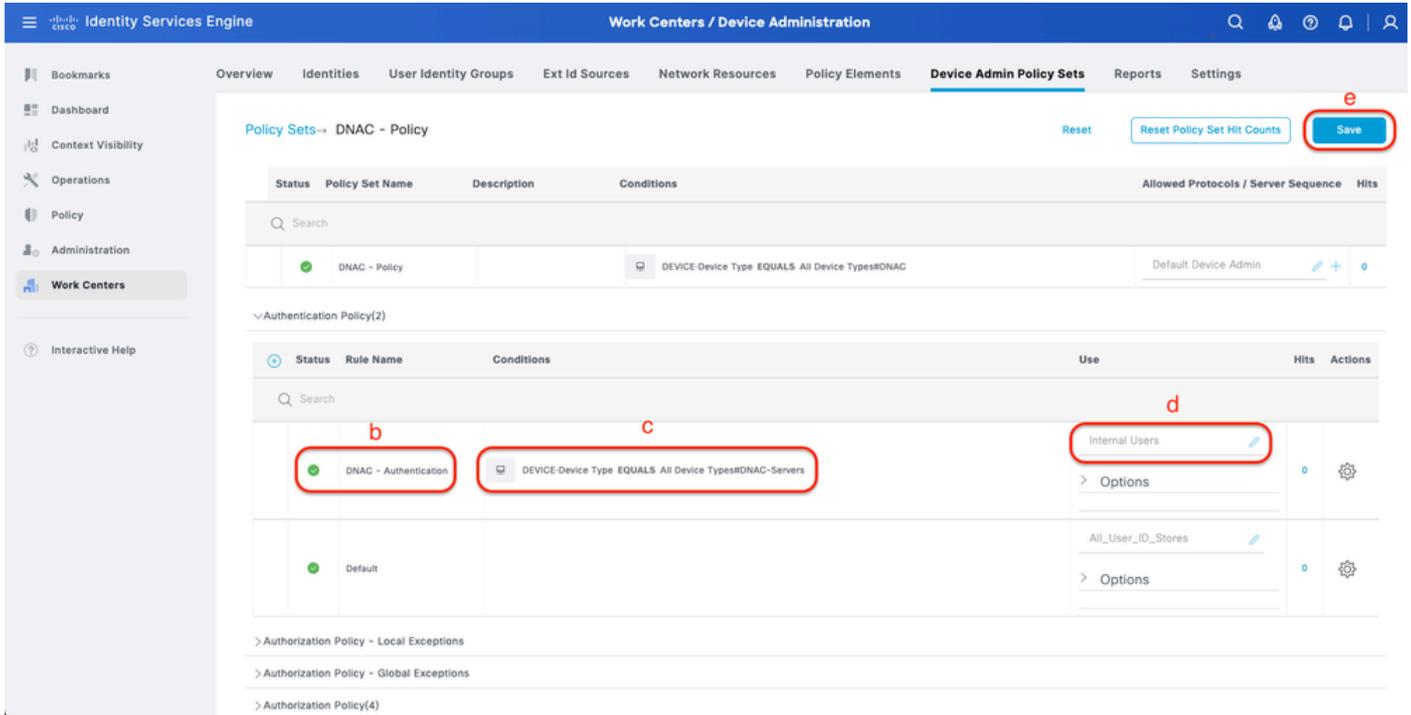
أ. (ه ا ل ع ا د ي د ج ف ص ج ا ر د ا) ر ت خ ا و ت ا ي ل م ع ق و ف ر ق ن ا . أ

ب. ة ق د ا ص م ل ا ج ه ن م س ا د ي ح ت ب م ق . ب

ي ف ا ق ب س م ه ئ ا ش ن ا ب ت م ق ي ذ ل ا ز ا ه ج ل ا ع و ن د و ة ق د ا ص م ل ا ة س ا ي س ط ر ش ن ي ي ع ت ب م ق . ج  
( $2 > b$  ة و ط خ ل ل).

د. ة ي و ه ل ا ر د ص م ل ة ق د ا ص م ل ا ج ه ن م ا د خ ت س ا ن ي ي ع ت . د

ه. ظ ف ح ق و ف ر ق ن ا . ه



TACACS+ ةقداصم ةسايس ةفاضل

TACACS+ ضيوفت ةسايس نيوكت 8 ةوطخلال

ةرادإ تاسايس تاعومجم > زاهجلا ةرادا > لمعلا زكارم بيوبتلا ةمالع نم كلذب مايقلا نكمي (>) قوف رقنا > ةزهجالا

مذختسم رود لكل ليخت جهن ءاشنال ةوطخلال هذه

- Super-admin-Role
- Network-admin رود
- SecOps-Role

ءارجالا

أ. (هالعا ديج فص جاردإ) رتخاوا تاي لمع قوف رقنا.

ب. ليختلا جهن مسا ديختب مق.

ج. هئاشناب تمق يتلا ني مذختسم الة ةومجم ديختو ليختلا ةسايس طرش نيي عتب مق. (4 ةوطخلال) ف

د. تمق يذلا TACACS فيرعت فلم ديختو ليختلا جهن Shell تافي صوت نيي عتب مق. (3 ةوطخلال) ف هئاشناب

ه. ظفح قوف رقنا..

Identity Services Engine Work Centers / Device Administration

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

Search

DNAC - Policy DEVICE Device Type EQUALS All Device Types#DNAC Default Device Admin

> Authentication Policy(2)  
> Authorization Policy - Local Exceptions  
> Authorization Policy - Global Exceptions  
v Authorization Policy(1)

Status	Rule Name	Conditions	Command Sets	Shell Profiles	Hits	Actions
+	Super Admin	IdentityGroup-Name EQUALS User Identity Groups:SUPER-ADMIN	Select from list	SUPER_ADMIN_ROLE	0	+
+	Network Admin	IdentityGroup-Name EQUALS User Identity Groups:NETWORK-ADMIN	Select from list	NETWORK_ADMIN_ROLE	0	+
+	SecOps	IdentityGroup-Name EQUALS User Identity Groups:SecOps	Select from list	SecOps_Role	0	+
+	Default		DenyAllCommands	Deny All Shell Profile	0	+

Reset Save

ليوختل جهن ةفاضل

## ةحصلال نم ققحتلال

### RADIUS نيوكت نم ققحتلال

> ةقداصلال > راودأل او نومدختسمل > نييچراخلال نيومدختسملال ماظن ضرع - DNAC 1-  
 نوويچراخلال نومدختسملال  
 لوأل RADIUS ربع لوخدلال ليچستب اوماق نيذل نييچراخلال نيومدختسملال ةمئاق ضرع كنكمي  
 راودأل او نيومدختسملال ةامسأ ةضورعملال تامولعملال نمضتتو .

Cisco DNA Center System / Users & Roles

User Management  
Role Based Access Control  
External Authentication

### External Authentication

Cisco DNA Center supports external servers for authentication and authorization of External Users. Use the fields in this window to create, update and delete AAA Servers. The AAA Attribute here on Cisco DNA Center is the name of the AAA attribute chosen on the AAA server. The default attribute expected is Cisco-AVPair, but if the user chooses to change it to any other AAA attribute, it needs to be configured here on Cisco DNA Center.

The value of the AAA attribute to be configured for authorization on AAA server would be in the format of "Role=role1". On ISE server, choose the cisco-av-pair attribute from cisco specific AAA attributes list. A sample configuration inside Authorization profile would look like "cisco-av-pair Role=SUPER-ADMIN-ROLE".

An example configuration in the case of manually defining the AAA attribute would be "Cisco-AVPair=Role=SUPER-ADMIN-ROLE".

Enable External User

AAA Attribute  
Cisco-AVPair

Reset to Default Update

AAA Server(s)

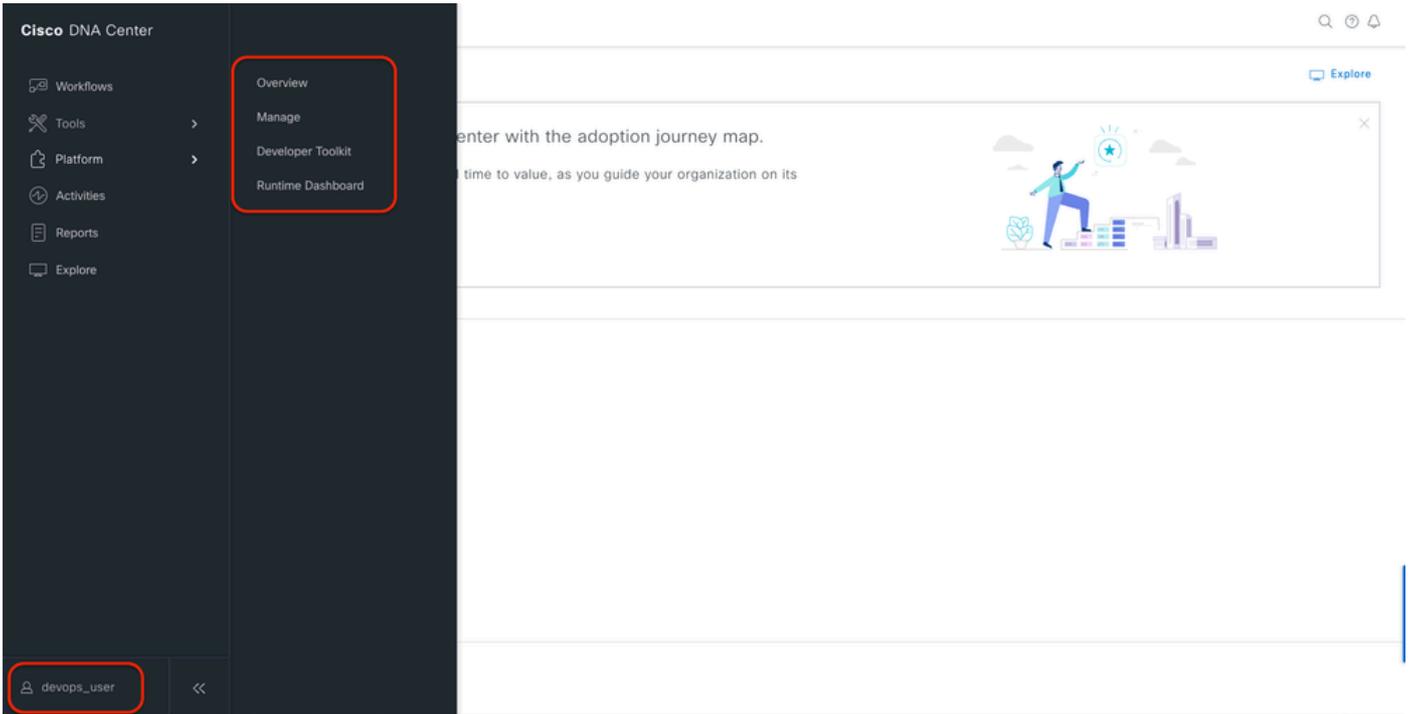
External Users

Username	Role	Action
devops_user	DevOps-Role	Delete

Showing 1 of 1

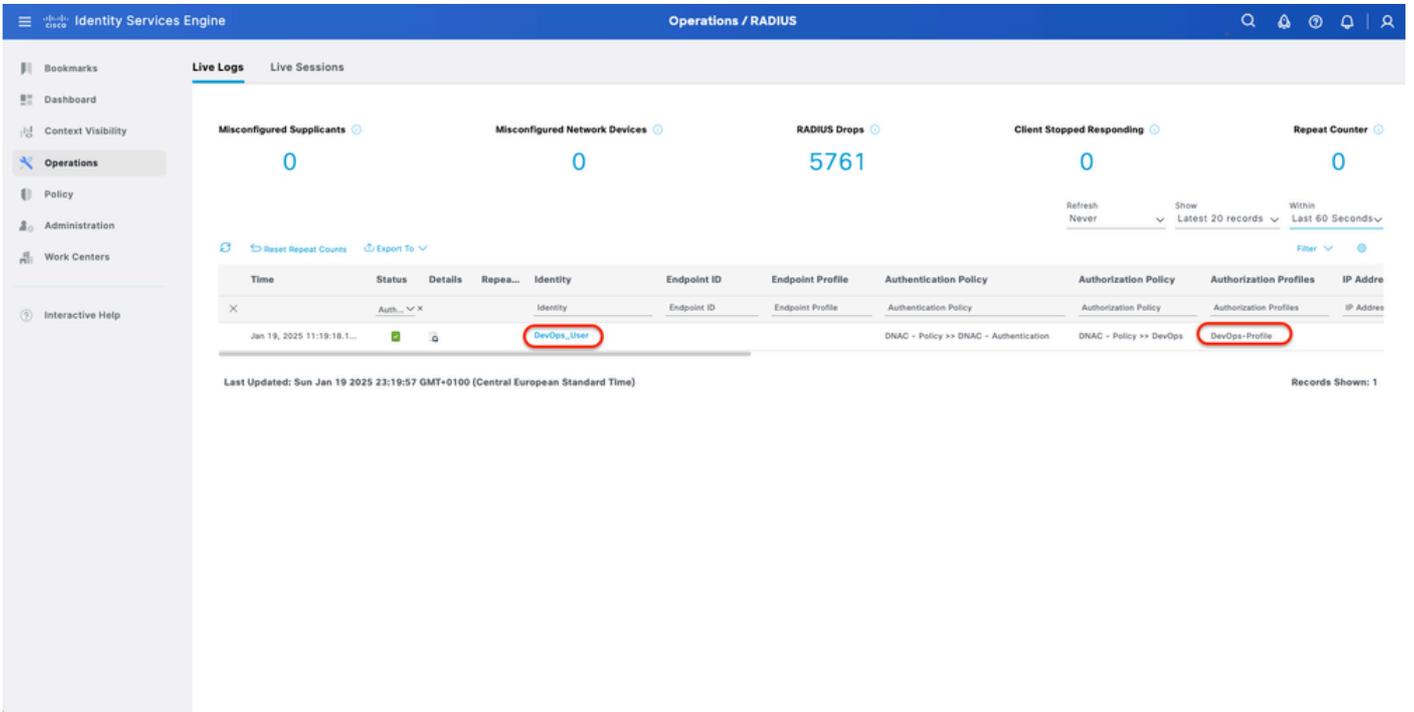
نويج راخال نوم دخت سمل

## 2. DNAC - لوصو ديكات -



مدخت سمل لودوم لوصو

## 3.a ISE - ةرشابم لالجس ل RADIUS > RADIUS > ةرشابم لالجس ل تاي لمع



ةرشابم لالجس ل RADIUS

## 3.b ISE - رونا > ةرشابم لالجس ل RADIUS > RADIUS > ةرشابم لالجس ل تاي لمع (لوصو لالجس ل لوصو لالجس ل)



Cisco DNA Center System / Users & Roles

User Management  
Role Based Access Control  
External Authentication

AAA Attribute  
Cisco-AVPair

Reset to Default Update

AAA Server(s)

Primary AAA Server  
IP Address  
Shared Secret \*\*\*\*\*  
View Advanced Settings  
Update

Secondary AAA Server  
IP Address  
Shared Secret \*\*\*\*\*  
View Advanced Settings  
Update

External Users

Filter

Username	Role	Action
secops_user	SecOps-Role	Delete

Showing 1 of 1

نوچراخال نومدختسملا

## 2. DNAC - م دختسملا لوصو ديكأت -

Cisco DNA Center

Policy >  
Workflows >  
Tools >  
Platform >  
Activities >  
Explore

Group-Based Access Control  
IP & URL Based Access Control

Network Bug Identifier  
Identify bugs in the network

secops\_user

مدختسملا ل دودحم لوصو

## 3.a ISE - TACACS LiveLog > عماع قرظن > ةزهجالا قرادإ > TACACS+ ل ةيحلل تالچسلا لمع زكارم -

Identity Services Engine Operations / TACACS

Live Logs

Refresh Never Show Latest 20 records Within Last 60 Seconds

Export To Filter

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Shell Profile	Device Type	Lo
Jan 19, 2025 05:12:4...	✓		SecOps_User	Authorization		DNAC - Policy >> SecOps	SecOps_Role	Device Type#A8I Device Types#DNAC...	Lo
Jan 19, 2025 05:12:4...	✓		SecOps_User	Authentication	DNAC - Policy >> DNAC - Authentication			Device Type#A8I Device Types#DNAC...	Lo

Last Updated: Sun Jan 19 2025 17:16:38 GMT+0100 (Central European Standard Time) Records Shown: 2

TACACS لةيحلل تالجلسل

ةماع ةرطن > ةزهأل ةرادإ > ةي لةيصف الت TACACS+ ةيحلل تالجلسل لمع زكارم - ISE 3.b لةيولل لجلسل (لےي صافت) رقنا > TACACS livelog

Cisco ISE

Overview

Request Type: Authorization  
 Status: Pass  
 Session Key: ise34/526427220/13958  
 Message Text: Device-Administration: Session Authorization succeeded  
 Username: SecOps\_User  
 Authorization Policy: DNAC - Policy >> SecOps  
 Shell Profile: SecOps\_Role  
 Matched Command Set  
 Command From Device

Authorization Details

Generated Time: 2025-01-19 17:12:43.368 +1:00  
 Logged Time: 2025-01-19 17:12:43.368  
 Epoch Time (sec): 1737303163  
 ISE Node: ise34  
 Message Text: Device-Administration: Session Authorization succeeded  
 Failure Reason  
 Resolution  
 Root Cause  
 Username: SecOps\_User  
 Network Device Name: DNAC

Steps

Step ID	Description	Latency (ms)
13005	Received TACACS+ Authorization Request	
15049	Evaluating Policy Group	1
15008	Evaluating Service Selection Policy	1
15048	Queried PIP - DEVICE.Device Type	4
15041	Evaluating Identity Policy	7
15013	Selected Identity Source - Internal Users	5
24210	Looking up User in Internal Users IDStore	1
24212	Found User in Internal Users IDStore	4
22037	Authentication Passed	0
15036	Evaluating Authorization Policy	0
15048	Queried PIP - Network Access.UserName	10
15048	Queried PIP - IdentityGroup.Name	2
15017	Selected Shell Profile	2
22081	Max sessions policy passed	1
22080	New accounting session created in Session cache	0
13034	Returned TACACS+ Authorization Reply	0

TACACS+ 1-2 لةيصف مةيحلل تالجلس

Service-Argument	cas-service
NetworkDeviceProfileId	b0699505-3150-4215-a80e-6753d45bf56c
AuthenticationIdentityStore	Internal Users
AuthenticationMethod	Lookup
SelectedAccessService	Default Device Admin
RequestLatency	38
IdentityGroup	User Identity Groups:SecOps
SelectedAuthenticationIdentityStores	Internal Users
AuthenticationStatus	AuthenticationPassed
UserType	User
CPMSessionID	13004827410.62.150.14628131Authorization130048274
IdentitySelectionMatchedRule	DNAC - Authentication
StepLatency	1=1;2=1;3=4;4=7;5=5;6=1;7=4;8=0;9=0;10=10;11=2;12=2;13=1;14=0;15=0
TotalAuthnLatency	38
ClientLatency	0
Network Device Profile	Cisco
IPSEC	IPSEC#Is IPSEC Device#No
Name	User Identity Groups:SecOps
EnableFlag	Enabled
Response	{Author-Reply-Status=PassAdd; AVPair=Cisco-AVPair=ROLE+SecOps-Role; }

2-2 ةيليصفتل ةرشابملا تالجتسلا TACACS+

## اهحالص او ءاطخال افاشكتسا

للكشت اذه ل رفوتى ةددحم صيخش تاملولعم نم ام ايلالكانه

## عجارملا

- [زاهجلا ةرادا > 3.4 رادصلا، Cisco نم ةيوهلا تامدخ كرحم لوؤسم ليلد](#)
- [2.3.5 رادصلا، Cisco نم ةيمقرلا ةكبشلا ةينب زكرم لوؤسم ليلد](#)
- [رودلا ىلا دننتملا لوصوللا يف مكحتلا: Cisco نم ةيمقرلا ةكبشلا ةينب زكرم ةيخراخلا ةقداصملا مادختساب](#)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن مة و مچم مادختساب دن تسمل اذ ه Cisco ت مچرت  
ملاعلاء نأ عي مچ ي ف ني مدختسمل م عد ي وتحم مي دقتل ل ي رش بل او  
امك ة قيق د نوك ت نل ةلأل ة مچرت ل ض ف أن ة ظ حال م ي ج ر ي . ة ص ا خ ل م ه ت غ ل ب  
Cisco ي ل خ ت . ف ر ت ح م م چ ر ت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة م چ ر ت ل ا ع م ل ا ح ل ا و ه  
ى ل ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا م چ ر ت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco  
Systems (رف و ت م ط بار ل ا) ي ل ص أ ل ا ي ز ي ل ج ن ا ل ا دن تسمل ا