

# ISE RADIUS J Secure Firewall Chassis Manager (FCM) ةقداصم نيوكت

## تايوتحملا

### ةمدقملا

ةنمآلة ةيامحلا رادج مزح ةرادال RADIUS ةقداصم/ضيوفت نيوكت ةيلمع دنتسملا اذه فصوي ISE مادختساب.

### ةيساسال تابلطتملا

#### تابلطتملا

ةيلالتل ةيضاملاب ةفرعم دوجوب Cisco ي صوت:

- FCM (FCM) نمآلة ةيامحلا رادج لكيه ري دم
- Cisco (ISE) نم ةيوهلا تامدخ كرحم
- RADIUS ةقداصم

#### ةمدختسملا تانوكملا

- Cisco Firepower 4110 FXOS v2.12 نامآلا زاهج
- Cisco Identity Services Engine (ISE) v3.2 patch 4

ةيلمع ةئيبي يف ةدوجوملا ةزهجال نم دنتسملا اذه يف ةدراول تامولعمل عاشنإ م اذإ. (يضارتفا) حوسمم نيوكتب دنتسملا اذه يف ةمدختسملا ةزهجال ةيمح تادب. ةصاخ رما يال لم تحملا ري ثأتلل كمهف نم دكأتف، لئغشتلا ديق كتكبش تناك.

## نيوكتلا

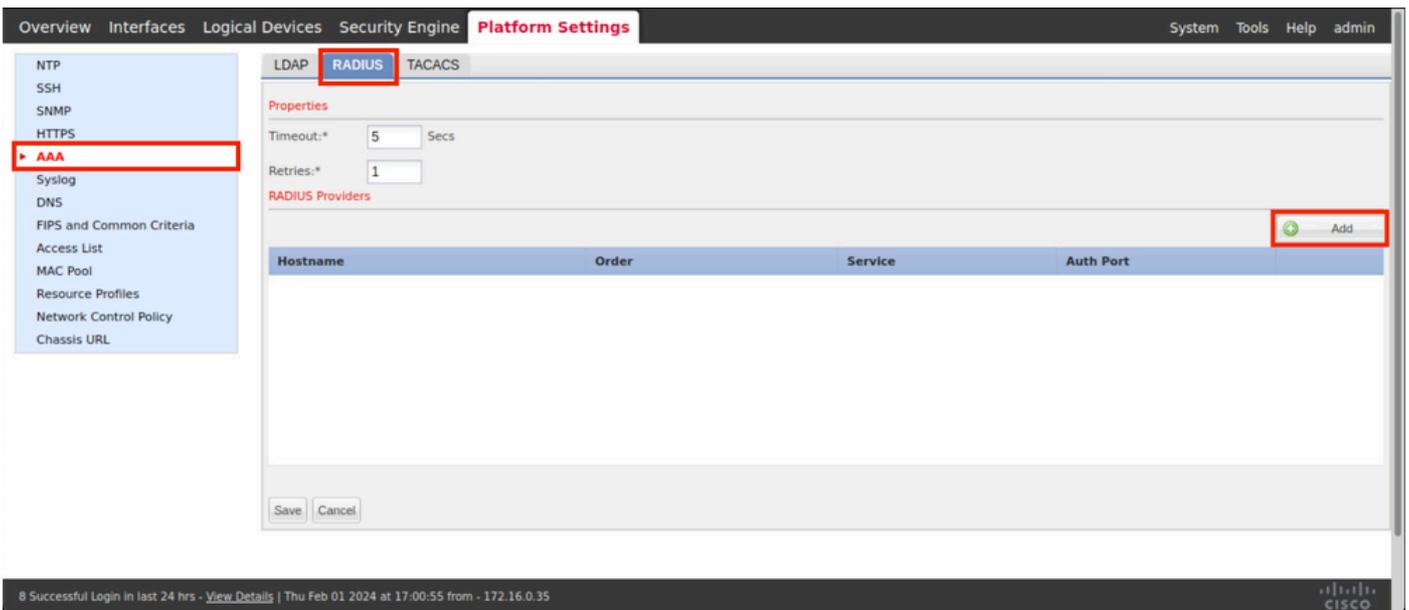
### تانويوكتلا

#### نمآلة ةيامحلا رادج لكيه ري دم

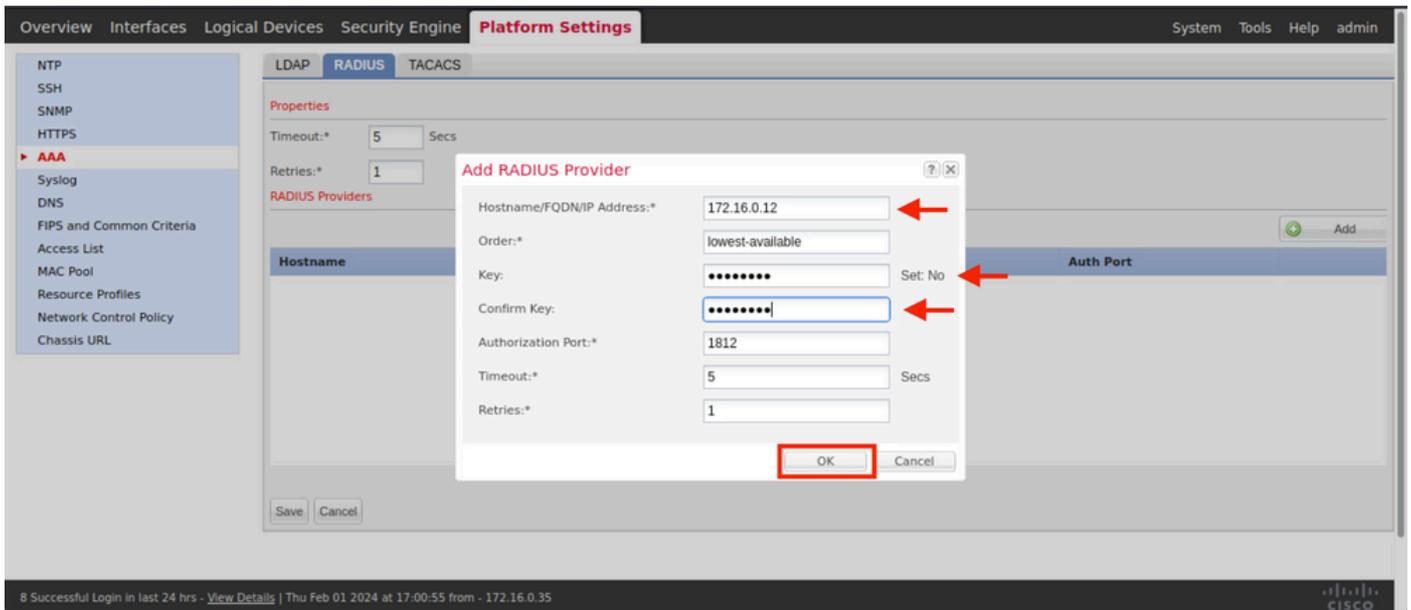
Firepower Chassis Manager ةيموسررلا م دختسملا ةهجاو ىلإ لوخدلا لئجستب مق 1. ةوطخلا  
يساسال ماظنلا تادادع ىلإ لقتنا 2. ةوطخلا



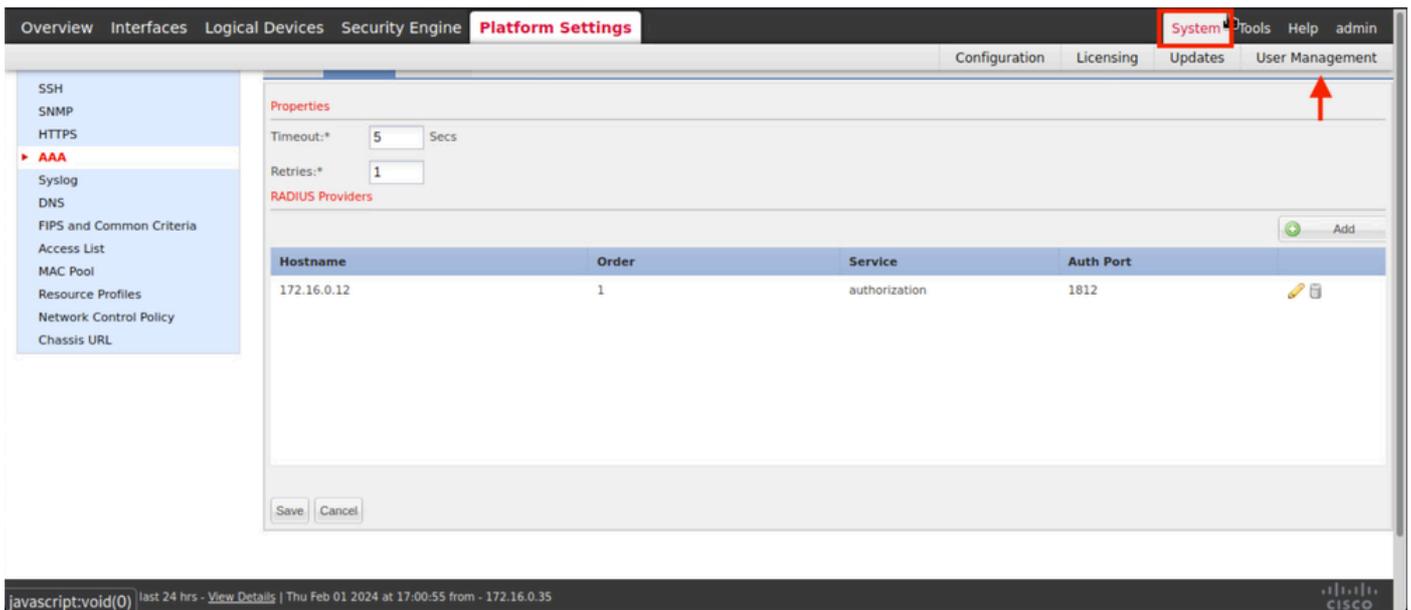
ديج RADIUS رفوم ةفاضاب مقو RADIUS دج. AAA قوف رقنا ىرسىلا ةمئاقلا نم 3. ةوطخلا



OK قوف رقناو. RADIUS رفوم نم ةبولطملا تامولعملاب رمألا هجوم ةمئاق ألاما 4. ةوطخلا



مدخست سمل ةرادإ > ماظنلإ ىلإ لقتنا 5. ةوطخل



ةمئاقلا نم ةيضارتفالا ةقداصملا طبضاو "تادادع" بيوبتلا ةمالع قوف رقنا 6. ةوطخل  
نيوكتلا ظفحاً مث لفسأل ريرمتلاب مق مٲ، Radius ىلإ ةلدسنملا

Overview Interfaces Logical Devices Security Engine Platform Settings **System** Tools Help admin

Configuration Licensing Updates **User Management**

Local Users **Settings**

**Default Authentication**

Local  \*Local is fallback authentication method

Local  
RADIUS   
LDAP  
TACACS  
None  
No-Login

Console Authentication

**Remote User Settings**

Remote User Role Policy

**Local User Settings**

Password Strength Check  Enable

History Count  (0-disabled,1-15)

Change Interval   (1-730 hours)

Change Count  (1-10)

No Change Interval   (1-730 hours)

Days until Password Expiration  (0-never,1-9999 days)

Password Expiration Warning Period  (0-9999 days)

Expiration Grace Period  (0-9999 days)

Password Reuse Interval  (0-disabled,1-365 days)

Session Timeout(web UI,ssh,telnet)  (0-never,3600 seconds)

8 Successful Login in last 24 hrs - [View Details](#) | Thu Feb 01 2024 at 17:00:55 from - 172.16.0.35

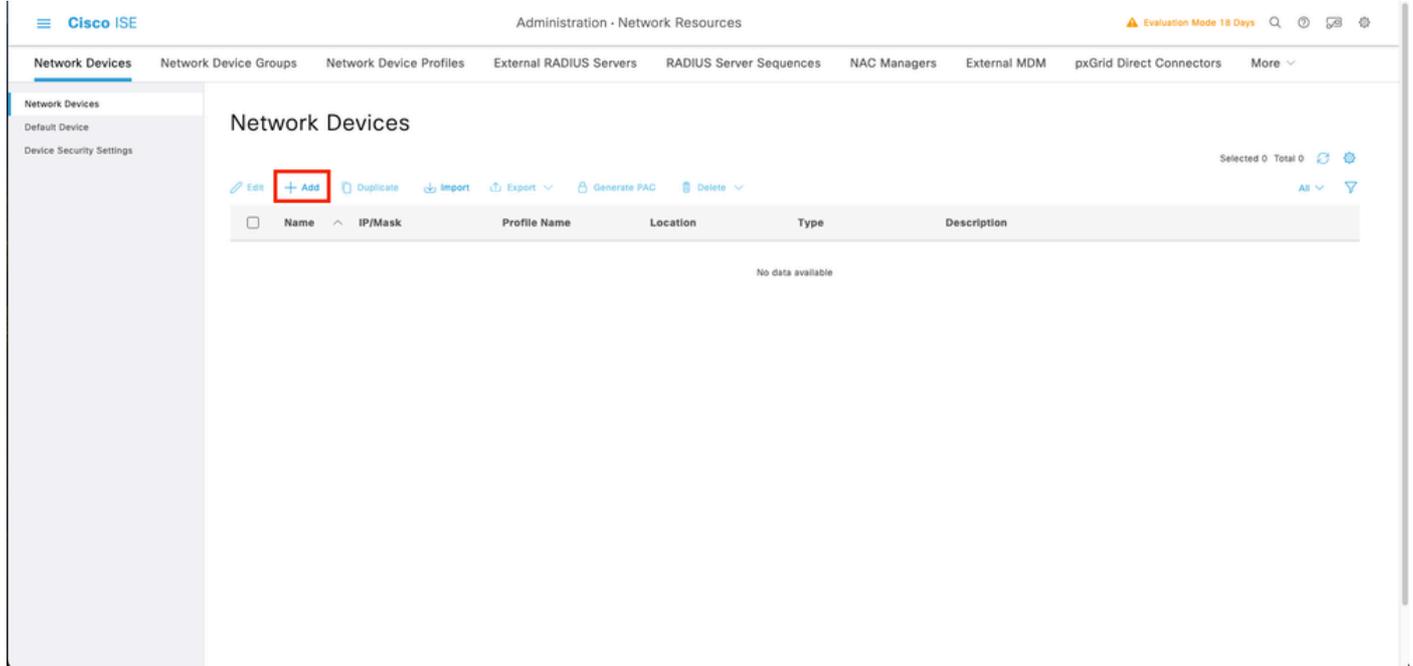
CISCO

ةطقنللا هذه دنع FCM نيوكت ةيلمع تهتنا :ةظحالم

## ةي وهلا ةمدخ كرحم

دي دج ةكبش زاغ ةفاضل 1. ةوطخل

> ةكبشلا دراوم > ةرادا > ىرسلا ةيولعلا ةيوازلا ≡ يف ةدوجوملا Burger ةنوقيا ىلا لقتنا ةفاضلا + > ةكبشلا ةزهجا

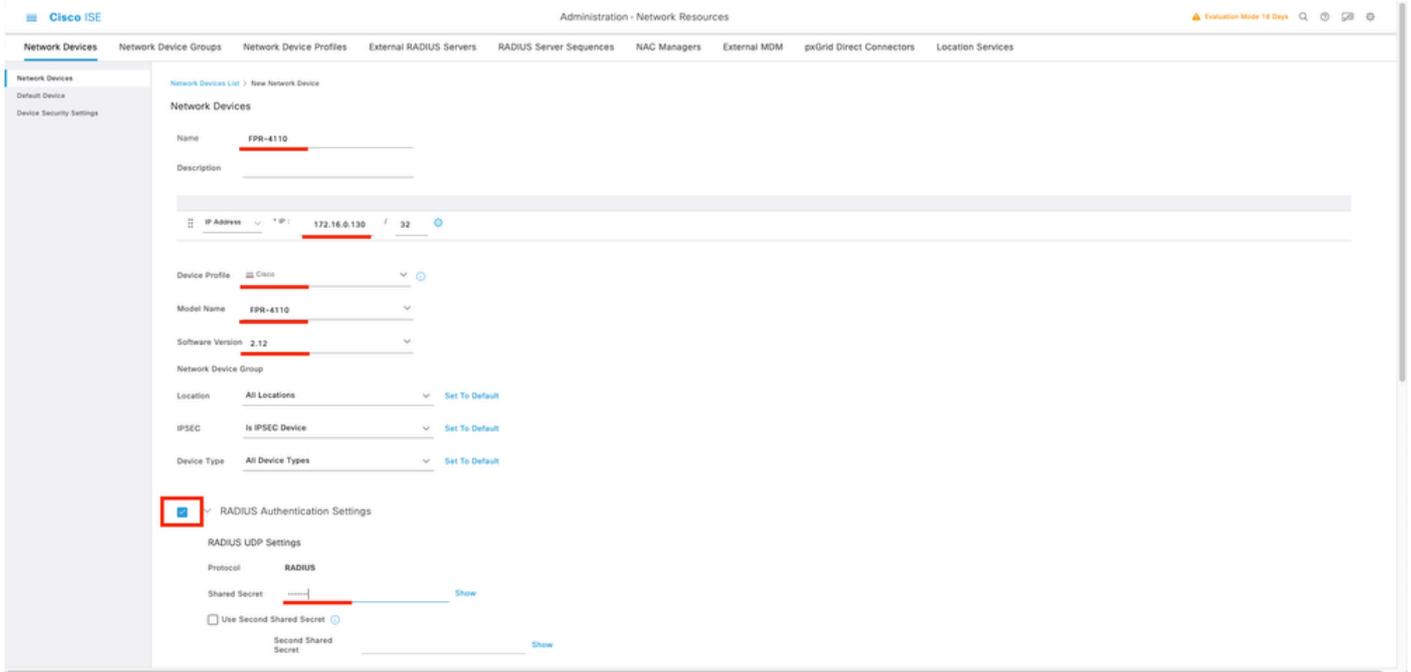


ةدي دجال ةكبشلا ةزهجا تامولعم لوح ةبولطملا تاملعمل ةئبعتب مق 2. ةوطخل

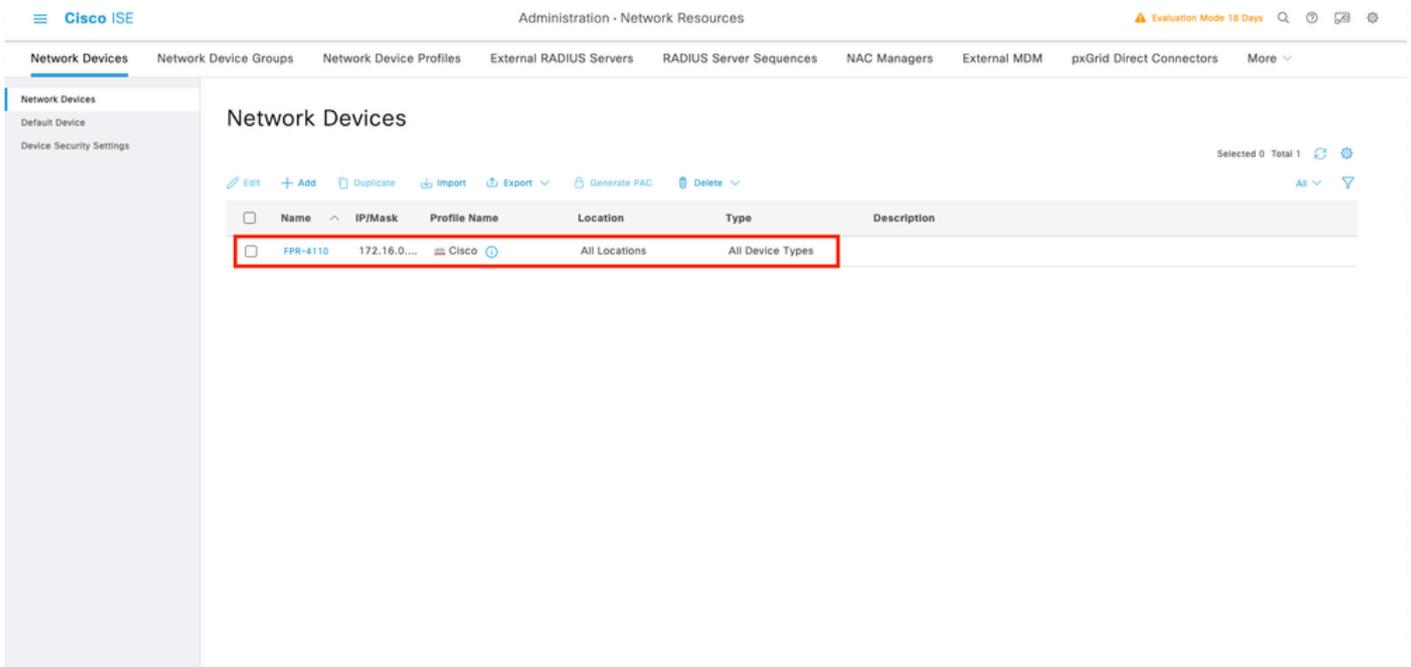
2.1 RADIUS رايتخاللا ةناخ ددح

2.2 FCM RADIUS نيوكت يف لالحلا وه امك كرتشملا ىرسلا حاتفملا سفن نيوكتب مق

2.1 لاسرا قوف رقناو لفسأل ري رمتلاب مق



ةكبشلا ةزهجأ نمض ديدجلا زاهجلا ةحص نم ققحتلا ضرع متي .3 ةوطخلا



≡ رغربلا ةنوقيأ ىلإ لقتنا .ةبولطملا مدختسملا ةيوه تاعومجم ءاشناب مق .4 ةوطخلا  
 ةيوه تاعومجم > تاعومجم > ةيوهلا ةرادا > ةرادا > ىرسلا ةيولعلا ةيوازلا يف ةدوجوملا  
 ةفاضلا + > مدختسملا

The screenshot shows the Cisco ISE Administration interface for Identity Management. The 'Groups' tab is selected. On the left, a sidebar shows the navigation menu with 'User Identity Groups' expanded. The main area displays a table of existing user identity groups. At the top of this table, the '+ Add' button is highlighted with a red box. Other buttons like 'Edit', 'Delete', 'Import', and 'Export' are also visible.

Name	Description
<input type="checkbox"/> ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group
<input type="checkbox"/> Employee	Default Employee User Group
<input type="checkbox"/> GROUP_ACCOUNTS (default)	Default GROUP_ACCOUNTS (default) User Group
<input type="checkbox"/> GuestType_Contractor (default)	Identity group mirroring the guest type
<input type="checkbox"/> GuestType_Daily (default)	Identity group mirroring the guest type
<input type="checkbox"/> GuestType_SocialLogin (default)	Identity group mirroring the guest type
<input type="checkbox"/> GuestType_Weekly (default)	Identity group mirroring the guest type
<input type="checkbox"/> OWN_ACCOUNTS (default)	Default OWN_ACCOUNTS (default) User Group

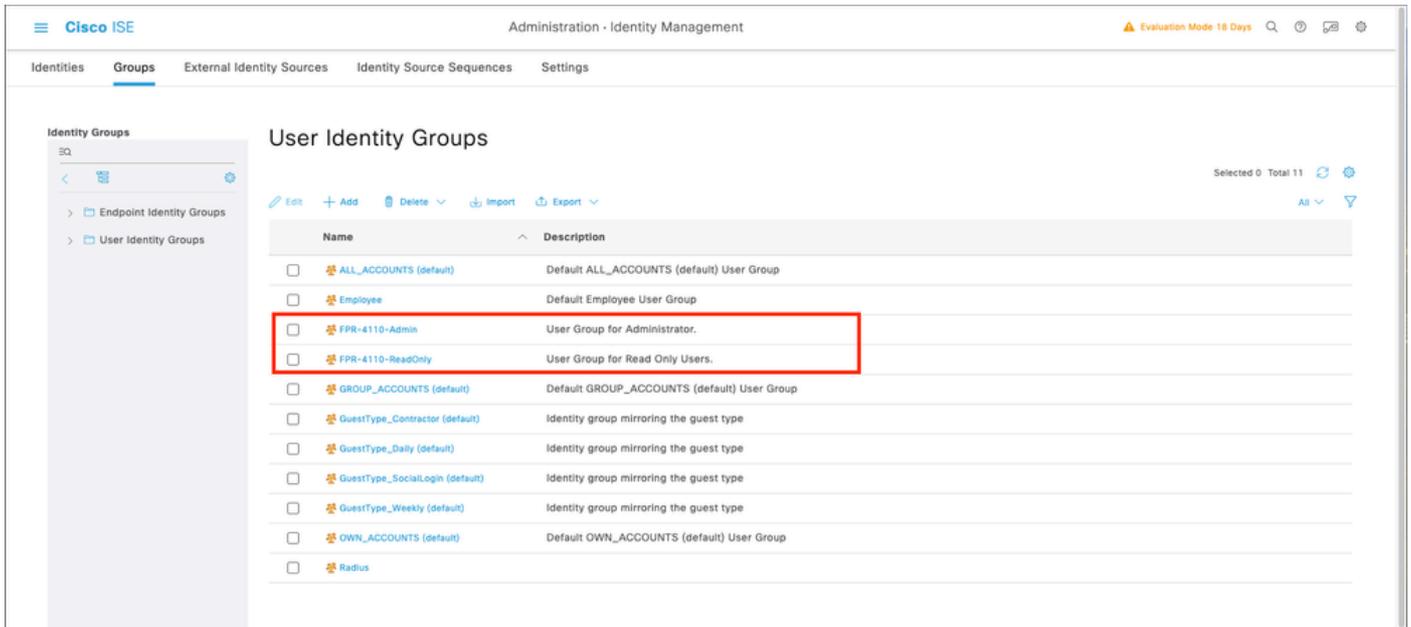
ظفحل لاسرراقوف رقن او لوؤس مل مدختسم فيرعت ةومجمل مسا نييعتب مق 5 ةوطخل نيوكتل.

The screenshot shows the 'New User Identity Group' form in Cisco ISE. The 'Name' field is filled with 'FPR-4110-Admin' and is highlighted with a red box. Below it is a text area for the description, currently containing 'User Group for Administrator.'. At the bottom right, the 'Submit' button is highlighted with a red box, and a 'Cancel' button is also visible.

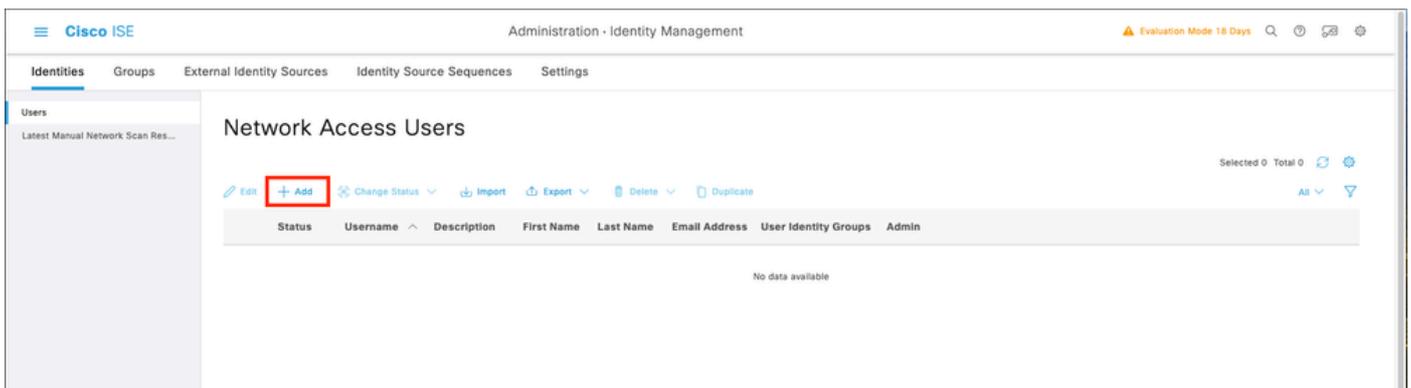
5.1 ReadOnly يمدختسمل ةيلمعال سفن ررك.

The screenshot shows the 'New User Identity Group' form in Cisco ISE. The 'Name' field is filled with 'FPR-4110-ReadOnly' and is highlighted with a red box. Below it is a text area for the description, currently containing 'User Group for Read Only Users.'. At the bottom right, the 'Submit' button is highlighted with a red box, and a 'Cancel' button is also visible.

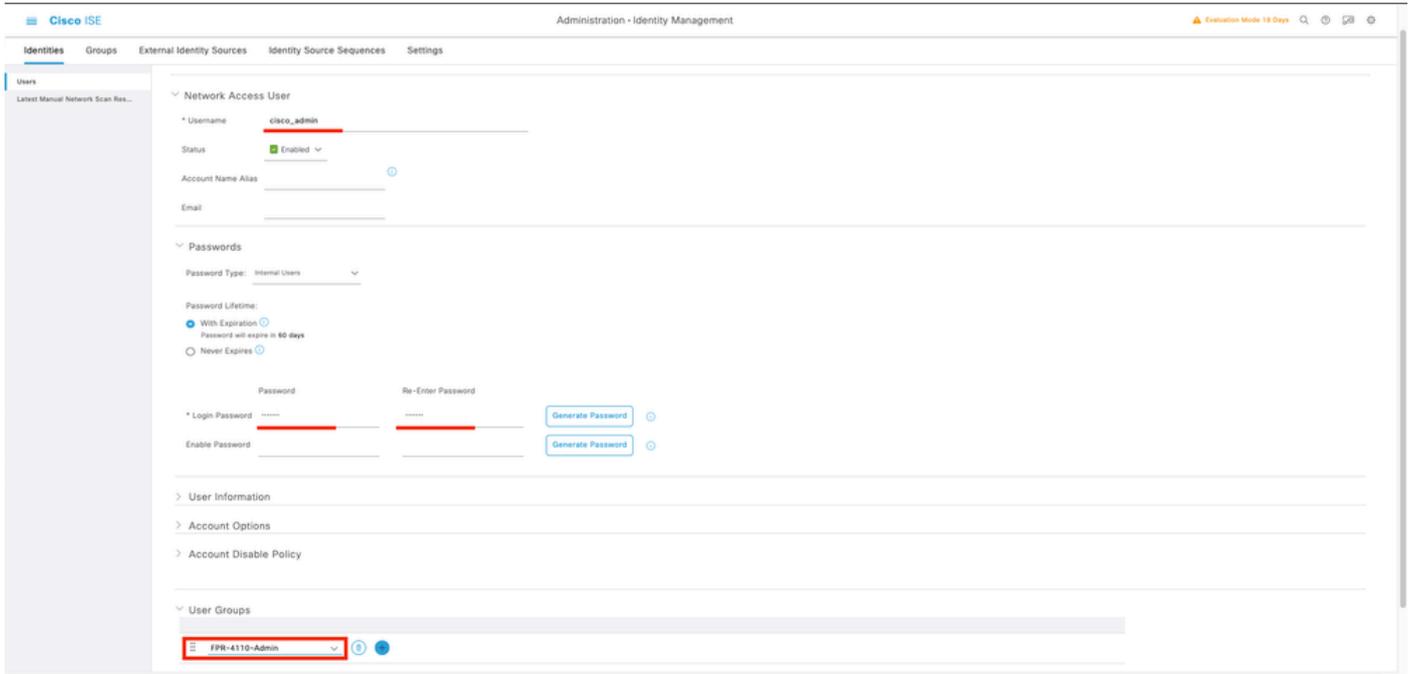
ةيوه ةاومجم نمض ةديجل ني مدختسمل ةاومجم روهظ ةحص نم ققحتلا 6 ةوطخل مدختسمل.



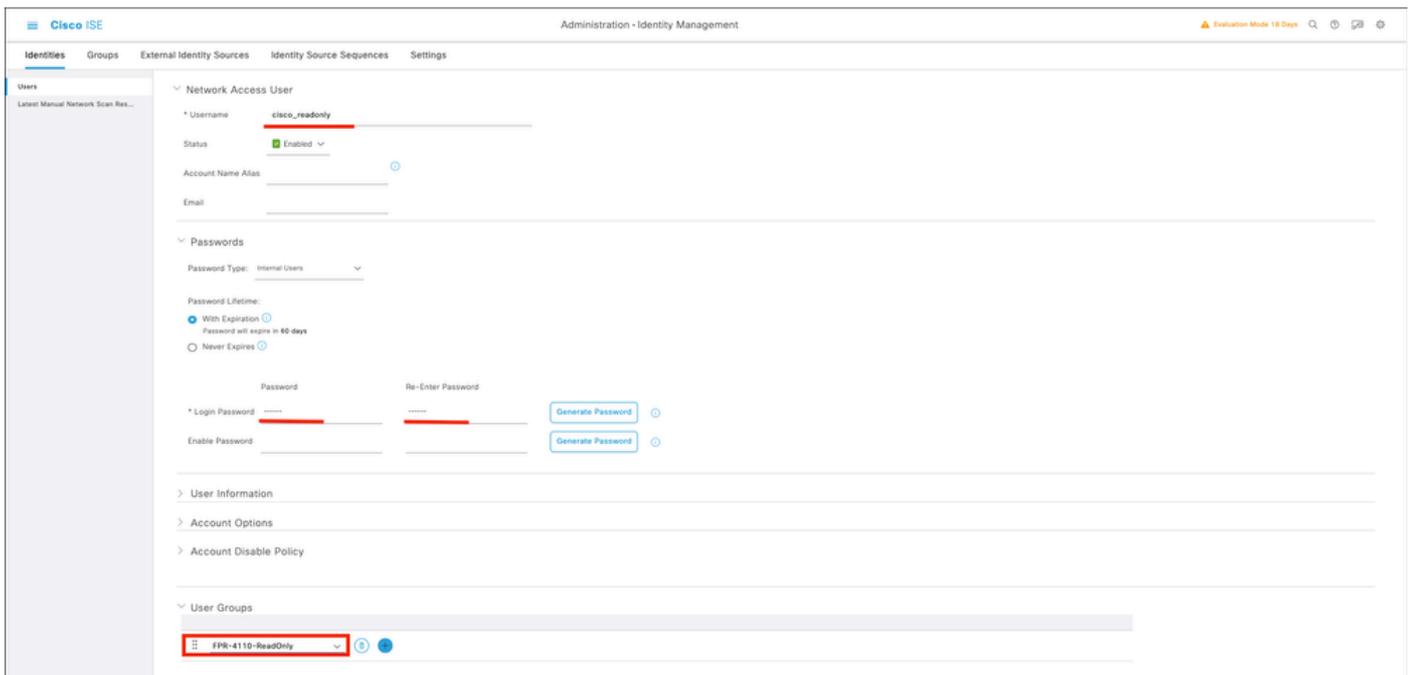
إلى لقتنا. مهيلسارم ةومجم إلى مهتفاضإو نييلحمال نيمدختسمل اءاشنإب مق 7. ةوطخال ةفاضإ + > تايوهال > ةيوهال ةرادإ > ةرادإ > ≡ رجب ةنوقى



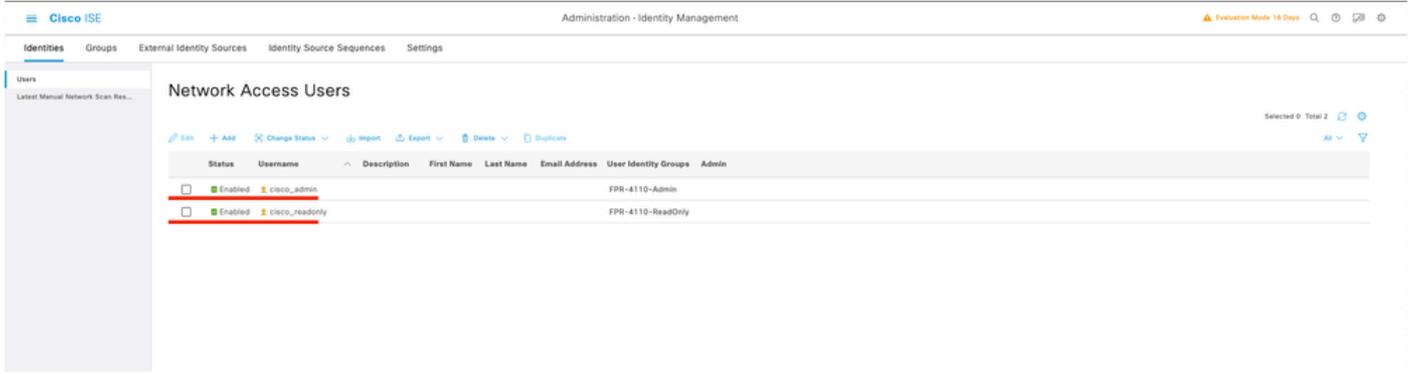
FPR-4110-Admin لىل ةنبيىءورورم ةملكومسا نييىءب مق . لوؤسمل قوقحب مدختسمل افضأ 7.1. تاريىءلالظفحل لاسرارقنوا لفسأ لىل ريرم تلاب مق ،



7.2 يلى ع هنيي عت و رورم ةم لك و مسا نهيي عت ب مق . ReadOnly قو قح عم مدخت سمل افضأ 7.2  
 4110-ReadOnly، تاريي غتلا ظفحل لاسرا رقن او لفسأ يلى ريرمت لابل مق .



7.3 يم مدخت سمل Network Access. نمض نهيي مدخت سمل افضأ نم ققحتلا 7.3



لوؤس مالم دختس ملل لي وختل في رعت فلم عاشن اب مق 8. ة وطلخا

ة لالتل دختس مالم راودأ FXOS لك يه نمضتي

- رودلا اذه ني عت متي . لمك لابل ماظنلا لى ل ة باتك لال ة عارق ل لمك لوصو - لوؤس مالم هريغت نكمي الو يضارت فالو لوؤس مالم باسحل يضارت فا لكش ب
- ة ل ل يدعتل تازايتما نودب ماظنلا ني وكت لى ل طقف ة عارق ل لوصو - طقف ة عارق ل ل ماظنلا
- Call Home ل كذل نيوكت لالو ، NTP ني وكت لى ل ة باتك لال ة عارق ل لوصولا - تايل لمعلا لوصولا ة عارق . لاطع أل او syslog مداوخ لك لذي ف امب ، ماظنلا تال جسو ، ي كذل صيخرتل ل ماظنلا يقاب لى ل
- لى ل ة باتك لال ة عارق ل لوصو - (AAA) ة بساح مالم وضيوفت لال ة قداص مالم لى ل لوصولا لوصولا ة عارق . (AAA) ة بساح مالم وضيوفت لال ة قداص مالم ني وكت و راودأل او ني دختس مالم ماظنلا يقاب لى ل

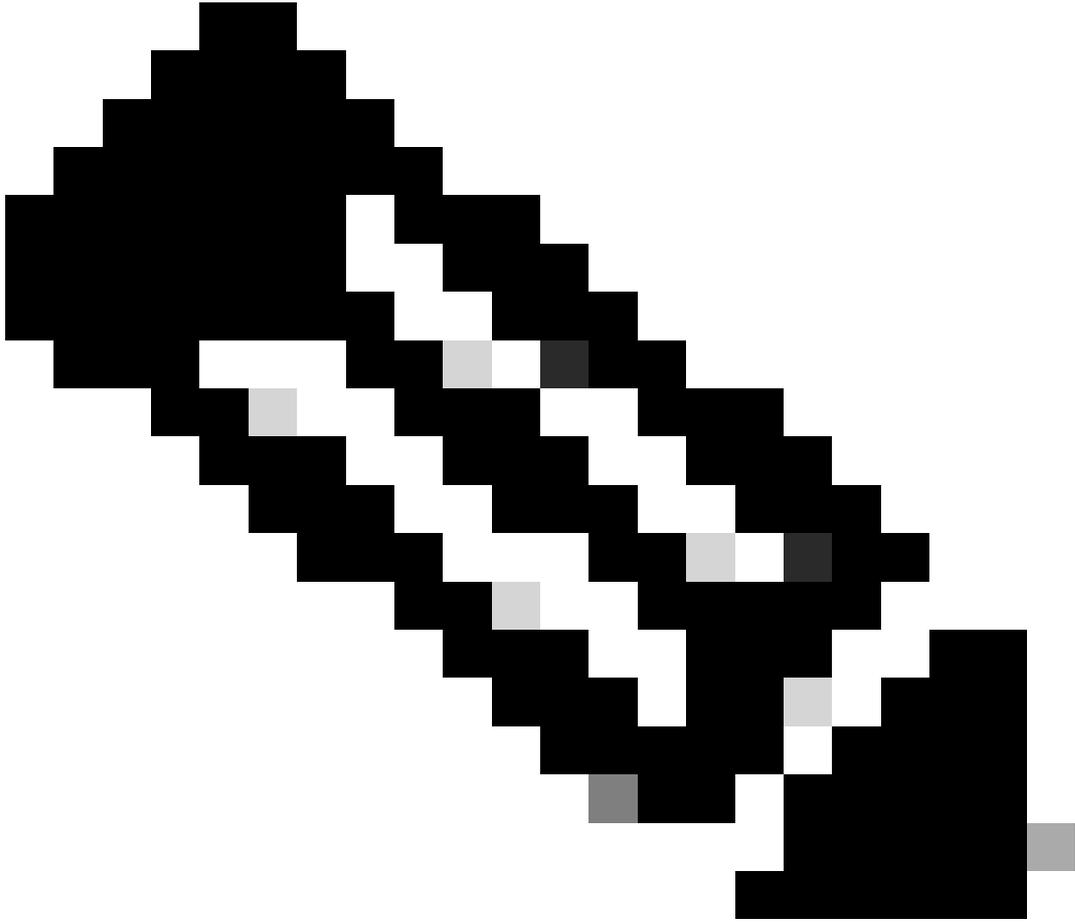
رود لك ب ة صاخلا تامسلا

cisco-av-pair=shell:roles="admin"

cisco-av-pair=shell:roles="aaa"

cisco-av-pair=shell:roles="operations"

cisco-av-pair=shell:roles="read-only"



طوق ةءارقلاو لوؤسملل تامس قئاثولا هذو ددحت :ةظحالم

---

> ضيوفتلا > جئاتنلا > ةسايسلا رصانع > ةسايسلا > Burger ةنوقيأ لىل لقتنا  
ةفاضا+ > ضيوفتلا صيصخت تافللم

ةئيه لىل لوصولو عون كرتاو ،ضيوفتلا فيرعت فلمل مسافيرعتب مق  
عم cisco-av-pair=shell:roles="admin" فضأ ةمدقتمل تامسلل تاداعل تحتو ACCESS\_ACCEPT  
قوف رقناو لاسرالا

Cisco ISE Policy - Policy Elements

Authentication Profiles > FPR-4110-Admins

Authorization Profile

\* Name: FPR-4110-Admins

Description:

\* Access Type: ACCESS\_ACCEPT

Network Device Profile: Cisco

Service Template:

Track Movement:

Agentless Posture:

Passive Identity Tracking:

ACL IPv6 (Filter-ID):

Advanced Attributes Settings

Cisco:cisco-av-pair shell:roles=\*admin\*

Attributes Details

Access Type = ACCESS\_ACCEPT  
cisco-av-pair = shell:roles=\*admin\*

Submit Cancel

8.1 عاشن اب مق ReadOnly م دخت س مل ل لي وخت ل ل في رت فلم عاشن ال ة ق با س ل ل ة و ط خ ل ل ر ر ك ة ر م ل ل ه ذ ل ل و ؤ س م ك ط ق ة ع ا ر ق ل ل ة م ي ق ل ل م ا د خ ت س ا ب RADIUS ة ئ ف

Cisco ISE Policy - Policy Elements

Authentication Profiles > New Authorization Profile

Authorization Profile

\* Name: FPR-4110-ReadOnly

Description:

\* Access Type: ACCESS\_ACCEPT

Network Device Profile: Cisco

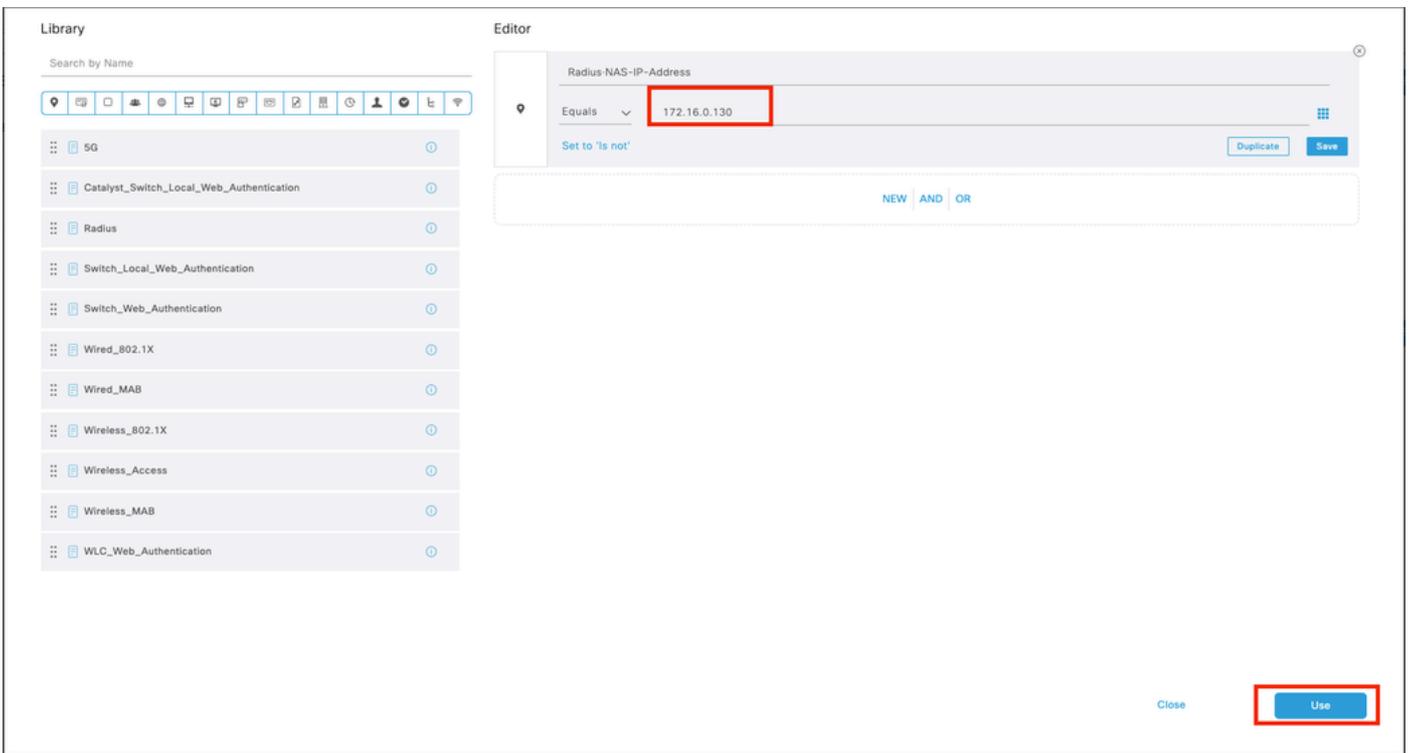
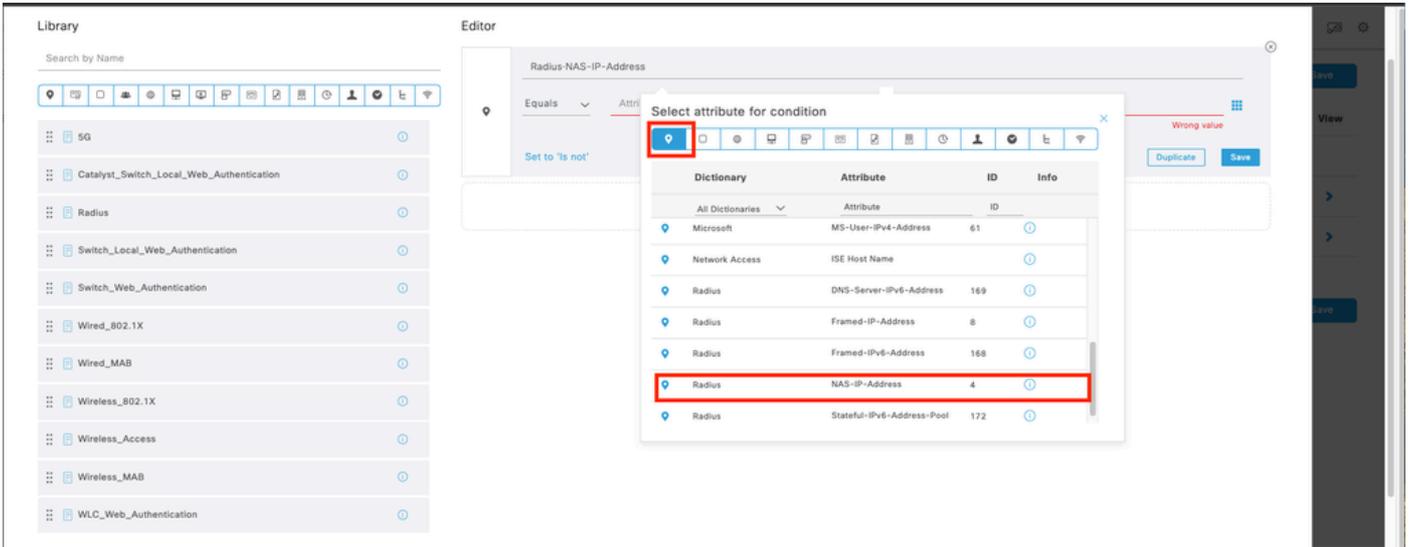
Service Template:

Track Movement:

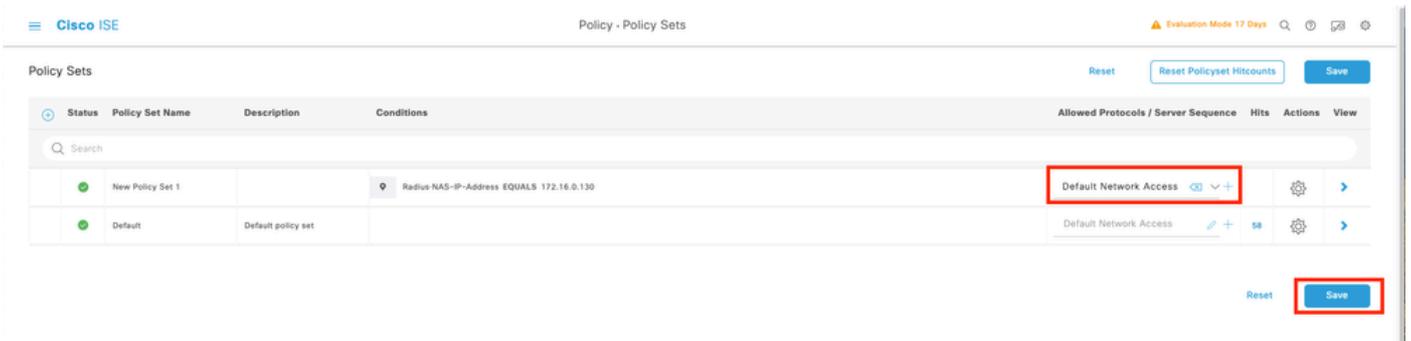
Agentless Posture:

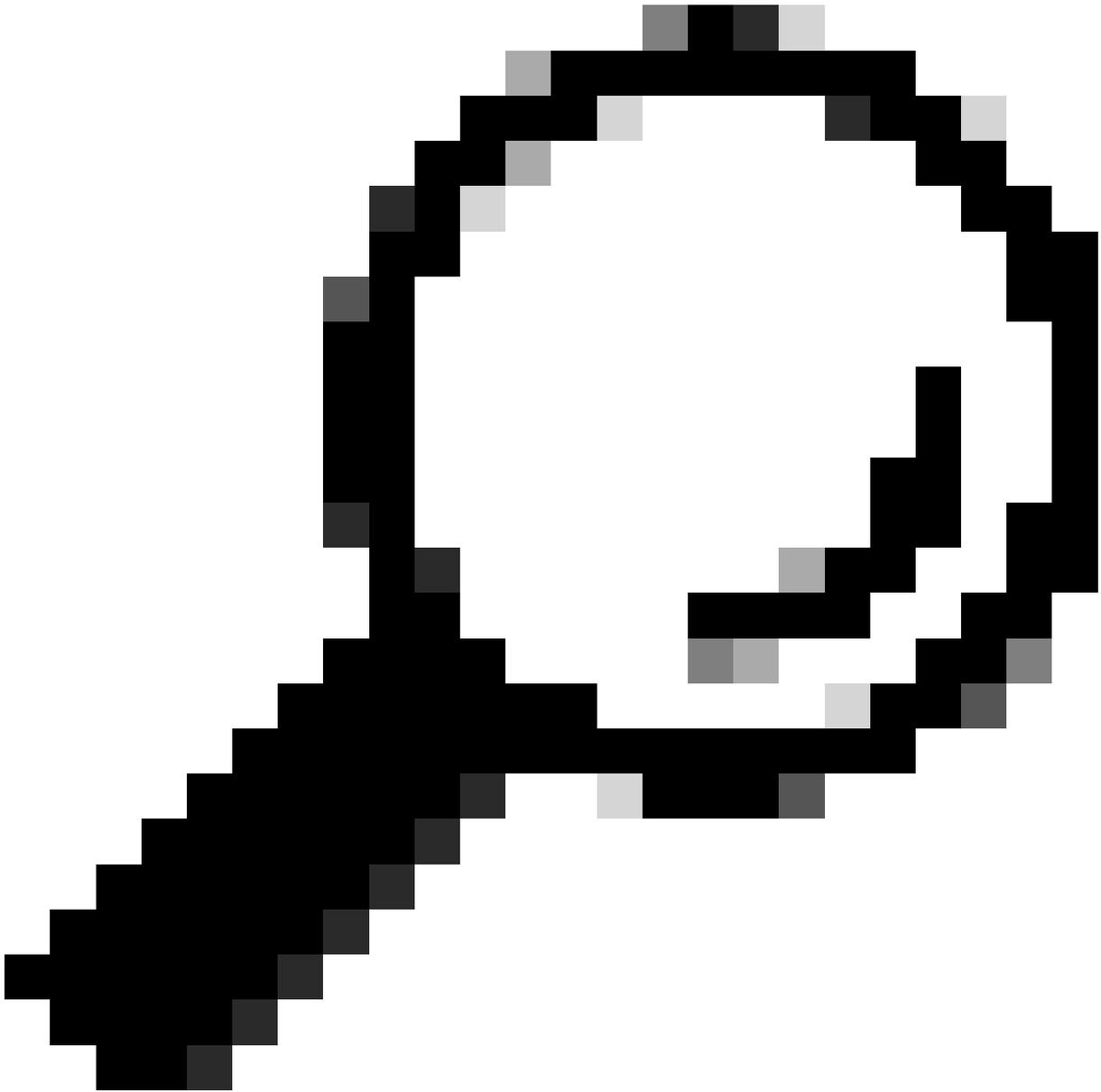
Passive Identity Tracking:





### 9.3. طيف قوف رقنا، اهل امتك ادرج م 9.3.





هذه الصورة هي لوصول التالوكوتورب عملاق بة لملعمل هذه انحمس دقل :حملت  
ة.احال بسح اهقطن قبيضتو ةديج عملاق عاشن انكمي .ةيضارتفال

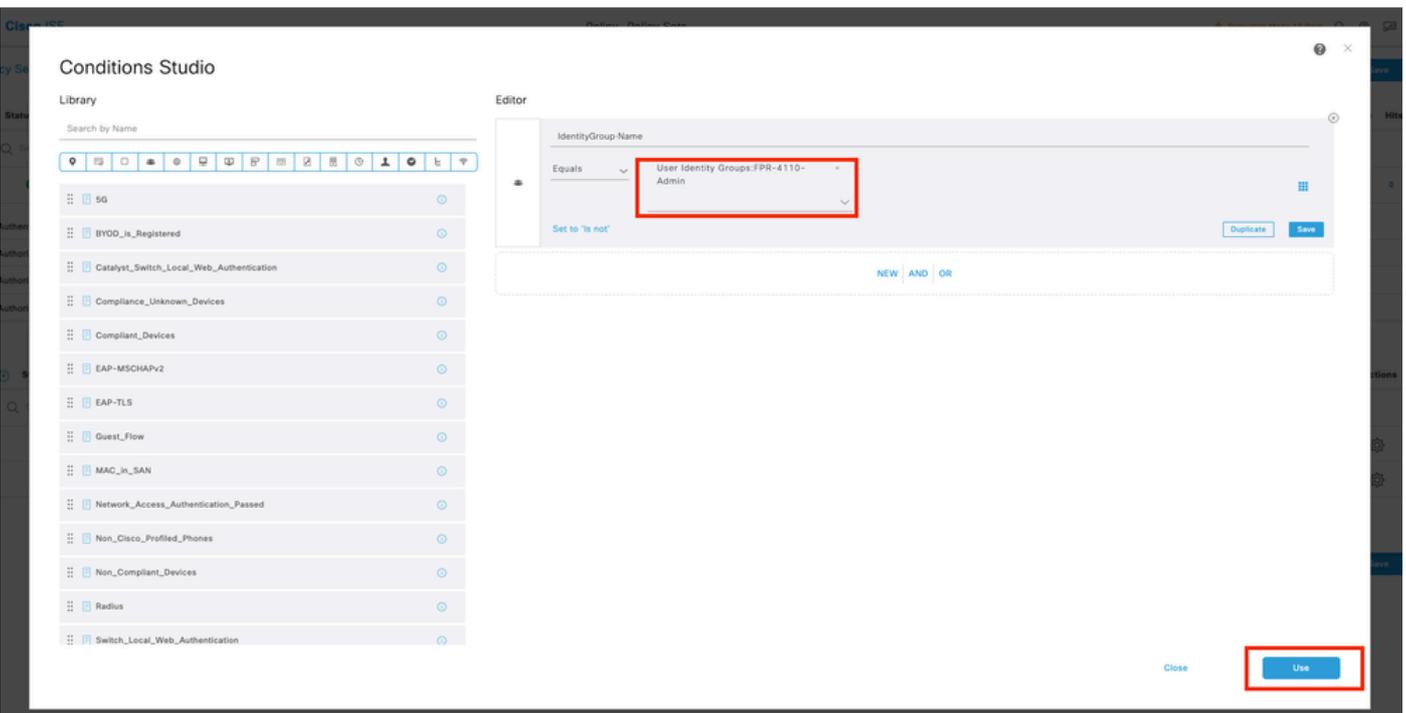
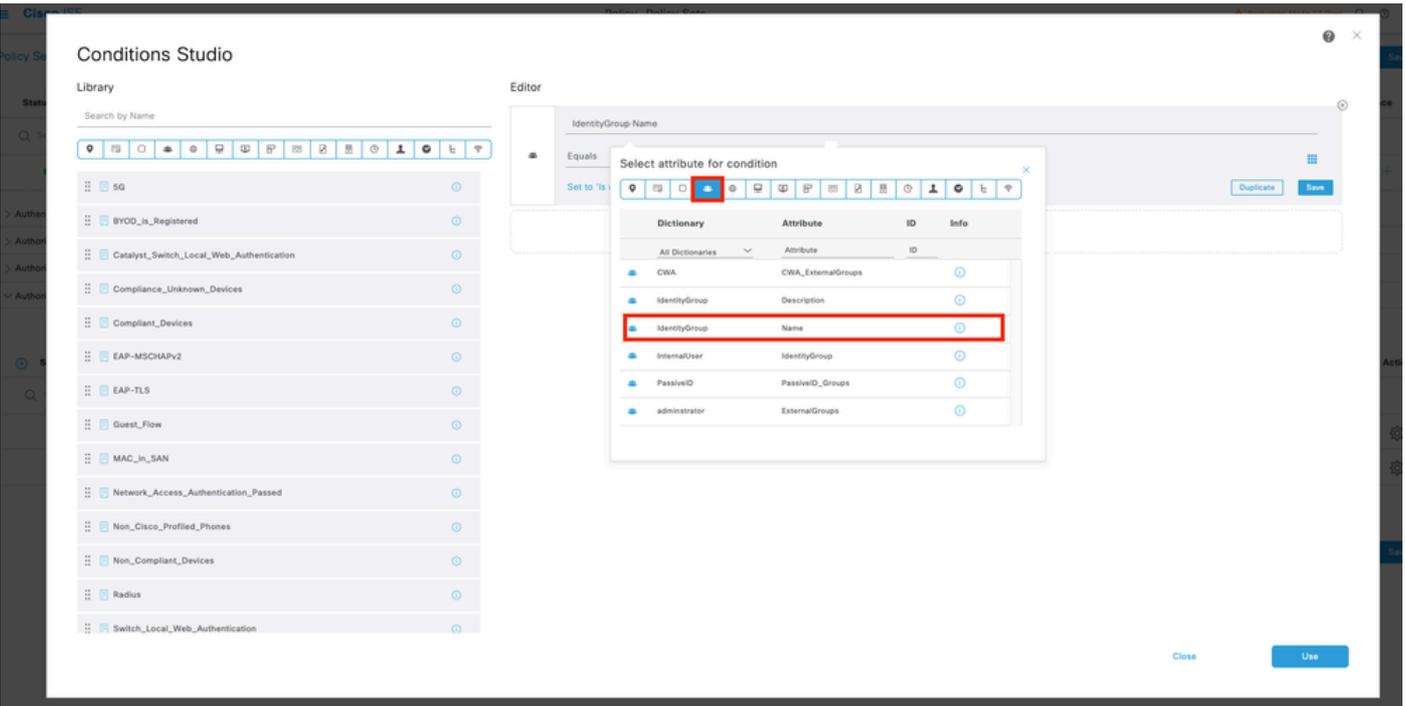
ةياهن يف دوجوملا > زمر لوصول قيرط نع ةديجال "جهنلا ةومجم" ضرع 10. ةوطخلا  
فصلا



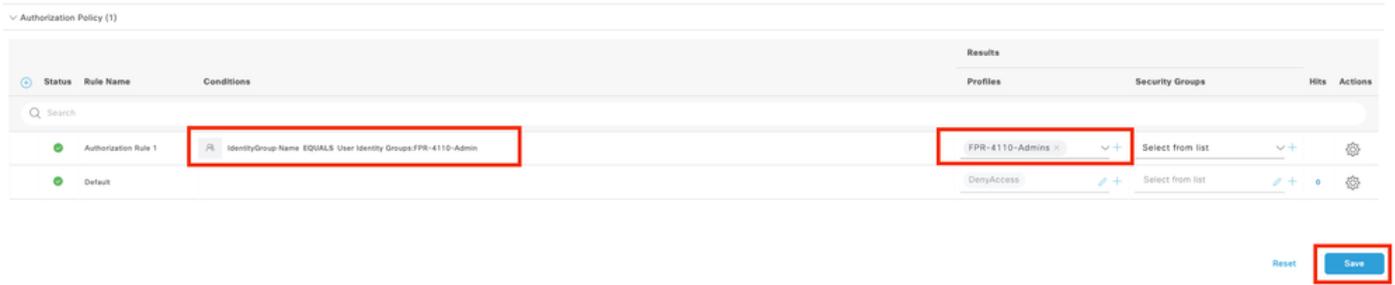
ديج طارش ةفاضل (+) قوف رقن او ليوختل جهن عملاق عيسوتب مق 10.1



في هؤاشنإ مت يذلا ةعومجم لاسا) FPR-4110-Admins: م دختس م ل ةي وه تاعومجم يواسي  
 م ادختس إ قوف ر قناو (7 ةوطخلال



في رعت فلم فضا م ث ، لي وختلا جهن في دي دجالا طرشلال ني وكت نم دكأت 10.3 ة وطلال  
في رعتلا تافل نمض مدختسم



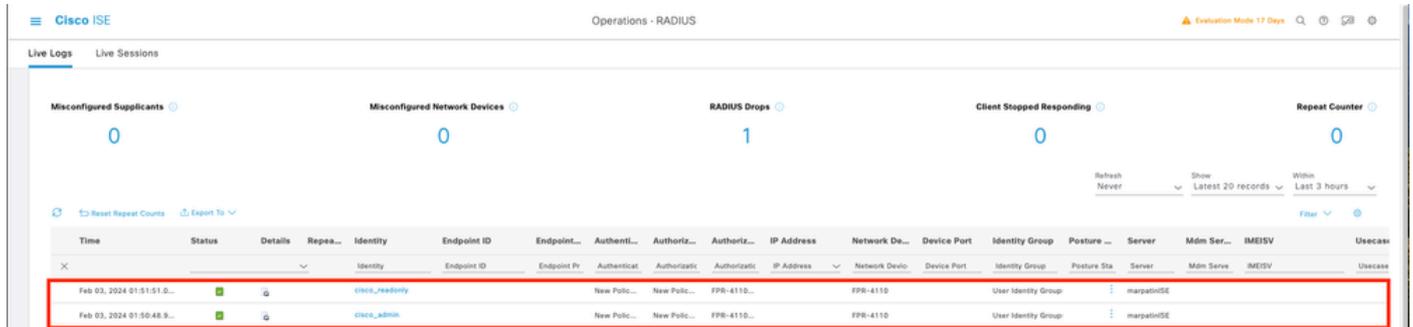
ظفح قوف رقناو طقف ةءارق لل ني مدختسم لل 9 ة وطلال في ةي لمعل س فن ررك 11 ة وطلال

ةحصلا نم ققحتلا

1. مادختساب FCM ب ةصاخلا (GUI) ةي م و سرلا مدختسملا ةهجاو لي لوخدلا لي جست ةل ولام 1.

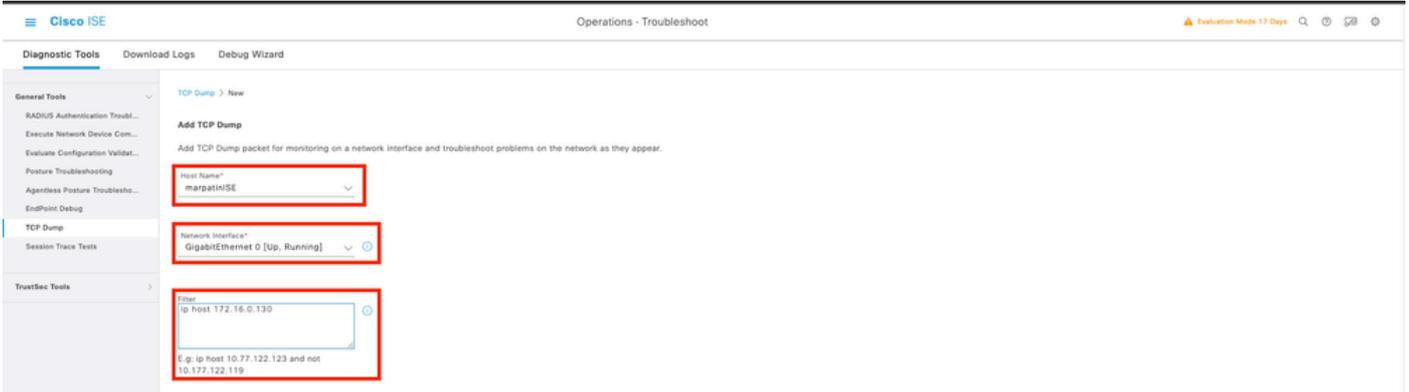
2. ةرشابملا تال جسلال RADIUS > تاي لمعلال > ررب ةنوقي لي لقتنا.

3. حاجنب لوخدلا لي جست ب مدختسملا ما اذا ام ة ضرورعمل تامولعمل رهظت.

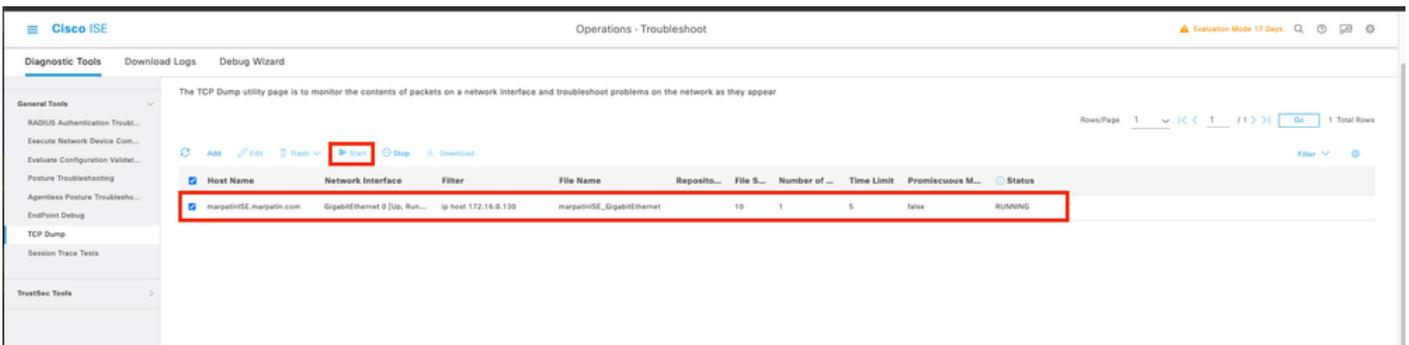


4. لك به ةصاخلا (CLI) رم اوألا رطس ةهجاو نم ني لجسملال ني مدختسملا رود ةحص نم ققحتلا.  
نم آل ةي امحل رادج





2.2 هلي غشت أدباو طاقت لال ددح .



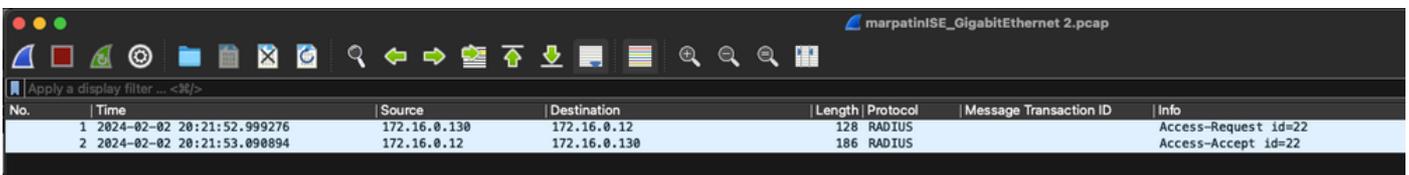
2.3 ISE طاقت لال لي غشت ءانثأ نم آلا ءي امحل رادج لك يه يلى لوخدلا لي جس ت ءل و احم 2.3

2.4 ي.لحم زا هج يلى فلم لال لي زنت ب مقو ISE ي TCP غي رقت فوقاً 2.4

2.5 رورم لال ءك رح تا ج رخم ءع جارم 2.5

ءقوت مل ج ت ان لال :

1812 (RADIUS) ذفن مل لال خ نم ISE م داخ يلى نم آلا ءي امحل رادج نم بل ط 1 م قر ءم زحل  
 ي.لصلأال بل ط لال لوبق ب ISE م داخ در 2 م قر ءم زحل



ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذہ Cisco تچرت  
ملاعلاء انءمچي فني مدختسمل معدى وتحم مي دقتل ةيرشبل او  
امك ةقيقد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچري. ةصاغل مهتغب  
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحل وه  
ىل إأمئاد ةوچرلاب ي صؤت وتامچرتل هذه ةقدنع اهتيلوئسم Cisco  
Systems (رفوتم طبارل) يلصلأل يزي لچنل دن تسمل