

- C9800-CL رادصلإا 17.9.2
- ISE 3.2.0

ةصاخ ةيلمعم ةئيب يف ةدوجوملا ةزهجالا نم دنتسملا اذه يف ةدراول تامولعمل عاشنإ مت تناك اذإ. (يضارتفا) حوسمم نيوكتب دنتسملا اذه يف ةمدختسُملا ةزهجالا عيمج تآدب رما يأل لمحتحمل ريثأتلل كمهف نم دكأتف، ليغشتلا ديق كتكبتش

ةيساسأ تامولعم

username لخدني نأ توضح مه، WLC ل نم GUI ل وأ CLI ل ذفني نأ لمعتسم لواحي ام دنع ةيلحمل تانايبلا ةدعاق عم هذه دامتعالا تانايب ةنراقم متت، يضرارتفا لكشبو. ةملاكو يف مكحتلل رصنع هيحوت نكمي، كلذ نم الادب. هسفن زاهجالا لىل ةدوجوملا، نيمدختسملل ديبب AAA مداخلباقم لاخلال دامتعا تانايب ةنراقم (WLC) ةيكللساللا ةيلحمللا ةكبشلا مداخل عم (WLC) ةيكللساللا ةيلحمللا ةكبشلا يف مكحتلل رصنع ثدحتت نأ نكمي مداخل وأ TACACS+ أو RADIUS مادختساب.

نيوكتلا

adminuser، لىل ةلاوتلا (ISE) AAA مداخل لىل نيمدختسمللا نم نيغون نيوكت مت، لاثملا اذه يف حنم عقوتمللا نم. لىل ةلاوتلا لىل تاعومحمل و helpdesk-group تاعومحمل admin-group نم عزج نومدختسمللا ءالؤه و helpdeskuser لىل لملكلا لوصول قح، (WLC) ةيكللساللا ةيلحمللا ةكبشلا يف مكحتلل رصنع admin-group نم عزج وه، و adminuser مداخل مداخل م متي نأ ينع، لىل helpdesk-group نم عزج، helpdeskuser، رخأ ةيخان نم. (WLC) ةيكللساللا ةيلحمللا ةكبشلا يف مكحتلل رصنع نيوكتلا لىل لوصول دجوي ال، لىل ءالاب و WLC لىل ءقارملا تازايتما حنم طقف.

م، RADIUS ةقداصلم ISE راي عم و (WLC) ةيكللساللا ةيلحمللا ةكبشلا يف مكحتلل رصنع نيوكتب الوأ ءلاقملا هذه موقت TACACS+ ل اقال هسفن رمالا ذيفنتب موقت.

طقف ءارقلل مداخل م دولي

ةدوجوم دولي ل هذه نوكت، WebUI 9800 ةقداصلم RADIUS أو TACACS+ مداخل ستا دنع

- مداخل م ءهجاو لىل لوصول قح مهيدل سيل نكلو 0 زايتمالا يوتسم مهيدل نيذلا نومدختسمللا دجاوتي ةيموسرلا
-
- يوتسم لداعي اذهو) "ءشاش بيوبتلا ءمالع ضرع طقف 14 لىل 1 نم تازايتما مهيدل نيذلا نيمدختسمللا نكمي (طقف ءارقلل ايلحم هتقداصلم مت مداخل م زايتمالا)
-
- لملكلا لوصول قح مهيدل 15 زايتمالا يوتسم مهيدل نيذلا نومدختسمللا
- لازي ال. طقف ءني عم رماو اءيتت لىل رماو ألة ءومحمل و 15 زايتمالا يوتسم مهيدل نيذلا نيمدختسمللا معد متي ال

WebUI لالځ نم نښوکتل تاریځت ذی فننت مدختسم لانا کماب

اهل یدعت و ا تارابتعالا هذه ریځت ن کمپ ال

WLC ل RADIUS قداصم نښوکت

RADIUS. مداخ نالعا 1. ةوطخال

نځموسرلانا مدختسم لانا ةهجاو نم

نم Servers/Groups > RADIUS > Servers بښوکتل ةمالعا نم کلذب مايقلا ن کمپي. WLC ىلعا RADIUS ISE مداخ ءاشناب مق ،الو ا لوصولا ن کمپي يتلا (GUI) ةموسرلانا مدختسم لانا ةهجاو (WLC) ةيكلسالل ةيلحمالا ةكبشلا ي ف مكحتال رصنع ةحفص ةروصلا هذه ي ف حضورم وه امك. Configuration > Security > AAA ىل لاقتنالاب تمق اذ ا و ا <https://<WLC-IP>/webui/#/aaa> ي ف اهل

Configuration > Security > AAA

+ AAA Wizard

Servers / Groups AAA Method List AAA Advanced

+ Add Delete

RADIUS

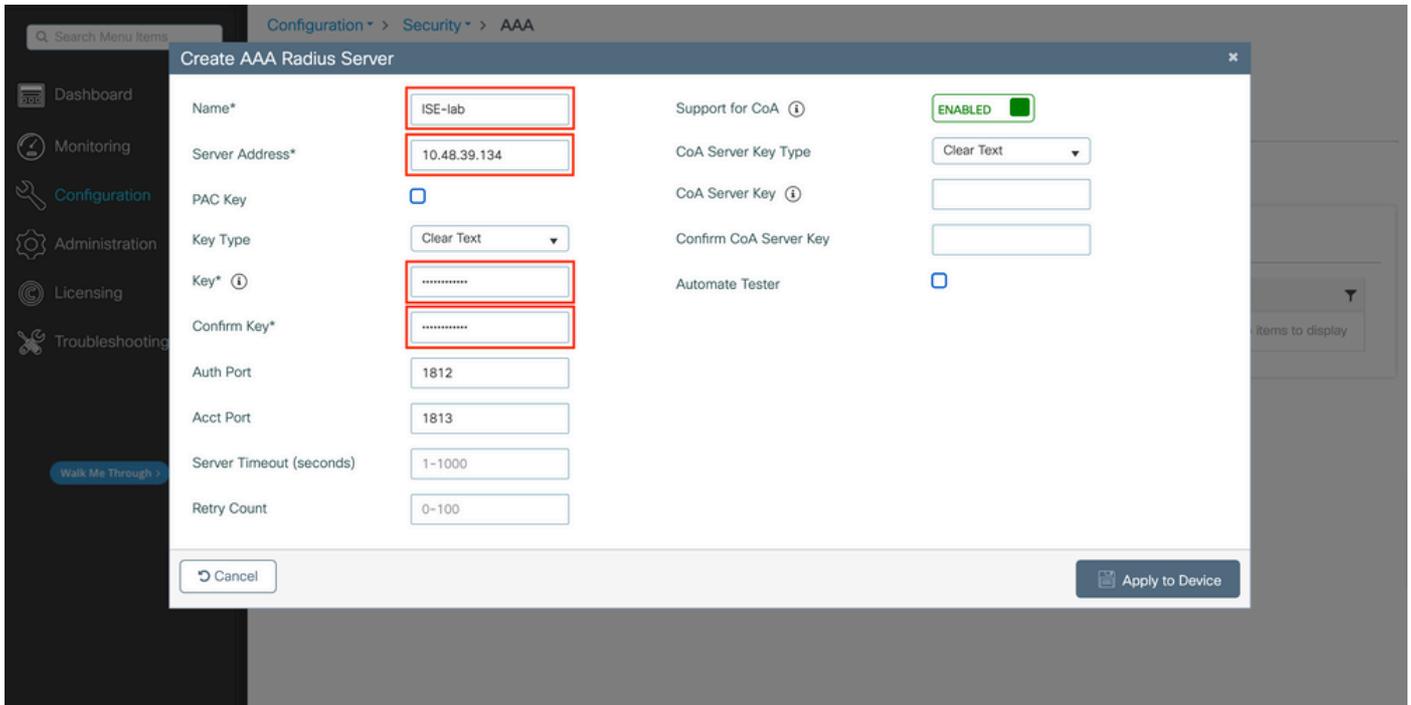
Servers Server Groups

Name	Address	Auth Port	Acct Port
ISE-lab	10.48.39.134	1812	1813

1 - 1 of 1 items

For Radius Fallback to work, please make sure the Dead Criteria and Dead Time configuration exists on the device

ي ف رمحلأاب رطؤملا ةفاضل رز رقنا ، (WLC) ةيكلسالل ةيلحمالا ةكبشلا ي ف مكحتال رصنع ىلعا RADIUS مداخ ةفاضل ةشاشلا ةطقلا ي ف ةصووعمالا ةقثب نملال ذفانلال حتف ىل اذه يدؤي. ةروصلا



رېرېفوت كېلېع بېجې، ةقثب نمل اذفانل هذه يف:

- ISE ماظن مسا قباطي نأ بېجې ال هنا اظحال) مداخل مسا
- مداخل ل IP ناونع
- RADIUS مداخل و WLC ل نېب كرتشم رسال

دادعك كرتتو ةيمازل تسيل هذه نكلو، ةبسا حملاو ةقدا صملل ةمدختس م اذفانملا لثم، يرخأ تاملعم نېوكت نكمي دنتس م اذهل يضارتفا.

رم اوأل رطس ةهجاو نم:

```
<#root>
```

```
WLC-9800(config)#radius server
```

```
ISE-1ab
```

```
WLC-9800(config-radius-server)#address ipv4
```

```
10.48.39.134
```

```
auth-port 1812 acct-port 1813
```

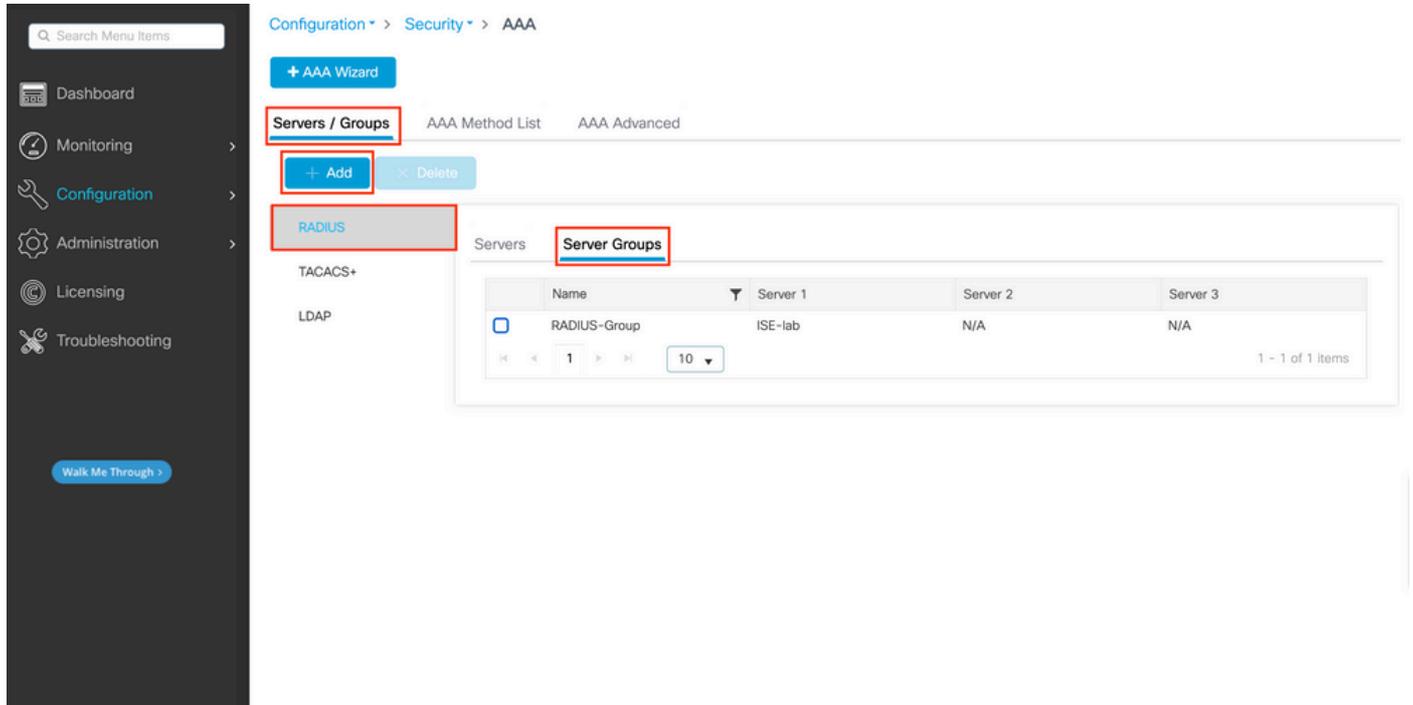
```
WLC-9800(config-radius-server)#key
```

```
Cisco123
```

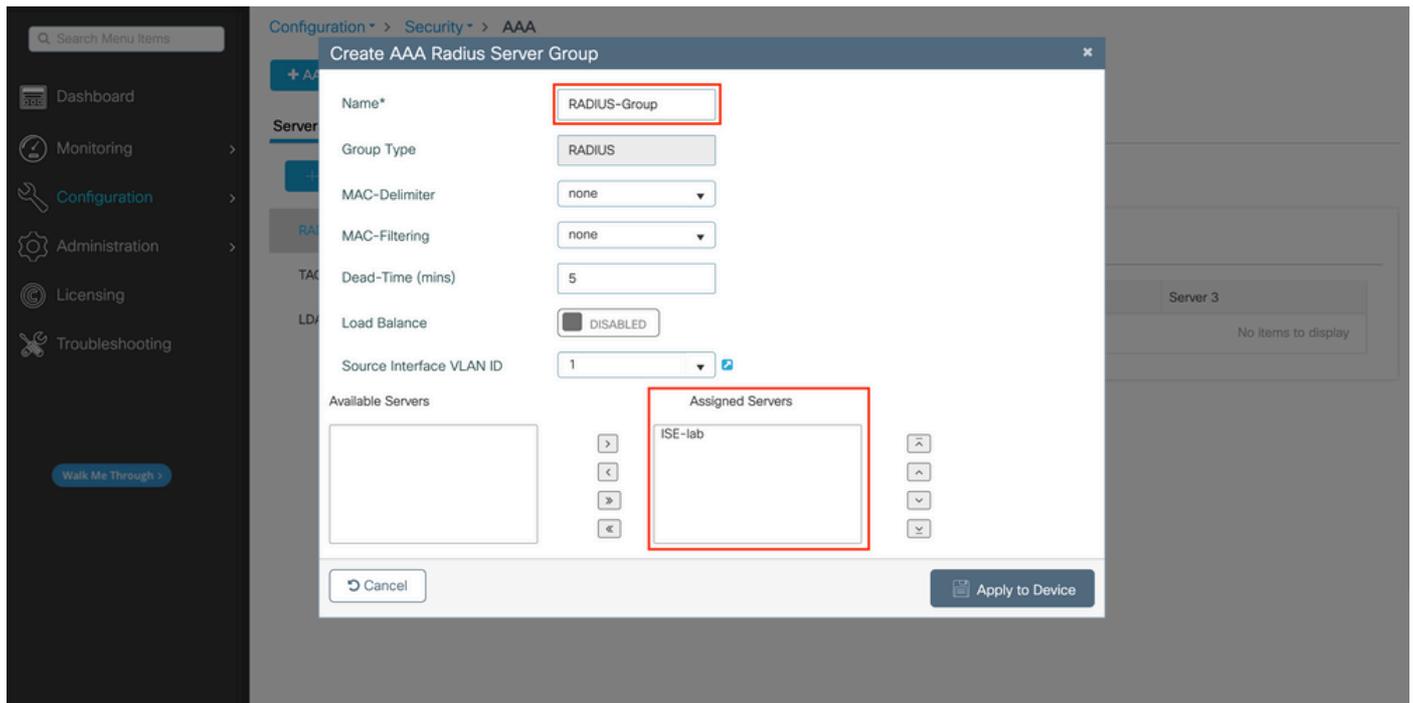
مداوخة وعومجم ىل رADIUS مداخ طي طخت 2. ةوطخل

نفة، موسرلا مداختس مل، ةهجاو نم:

مداوخة وعومجم ىل مداوخة هذه عي مج ني عت ب صوي، ةقداصل مل اهم ادختس انكم ي ةدعت م RADIUS مداوخة دوجو ةلا ح ي ةفلتخم ل ةقداصل مل تايلمع ني ب لامحال ا عيزوت ب (WLC) ةي كل ل سال ل ا ةي ل حمل ل ةك ب ش ل ا ي ف مكحت ل ا ةدحو متهت. اهس فن ةمالع Servers/Groups > RADIUS > Server Groups نم RADIUS مداوخة تاوعومجم ني وكت م تي. مداوخة وعومجم ي ف مداوخة ني ب ةروصل ل ا ي ف حضوم وه امك، 1. ةوطخل ل ا ي ف ةروك ذم ل ا (GUI) ةي موسرلا مداختس مل ةهجاو ةحفص سفن نم بي وبت ل ا



م تي يذلاو، (ةقباس ل ا ةروصل ل ا ي ف راط ل ا) ةفاض رزل قوف رقل ل ا دنع ةقثب نم ةذفان رهظت، مداخل ا ءاشنال ةب س ن ل ا ب انه ه ف ي فصت



ةنعم لمداء لةمءاء لى ءب ول طم لمداء لى لى قن ب مق مء ءوم جم لى مس ا رى فو ب مق ءق ءب نمل ءمءاء لى ف

نمءاء لى رطس ءهءاء نم

.
.
.

<#root>

WLC-9800(config)# aaa group server radius

.
.

RADIUS-Group

.
.

WLC-9800(config-sg-radius)# server name

.
.

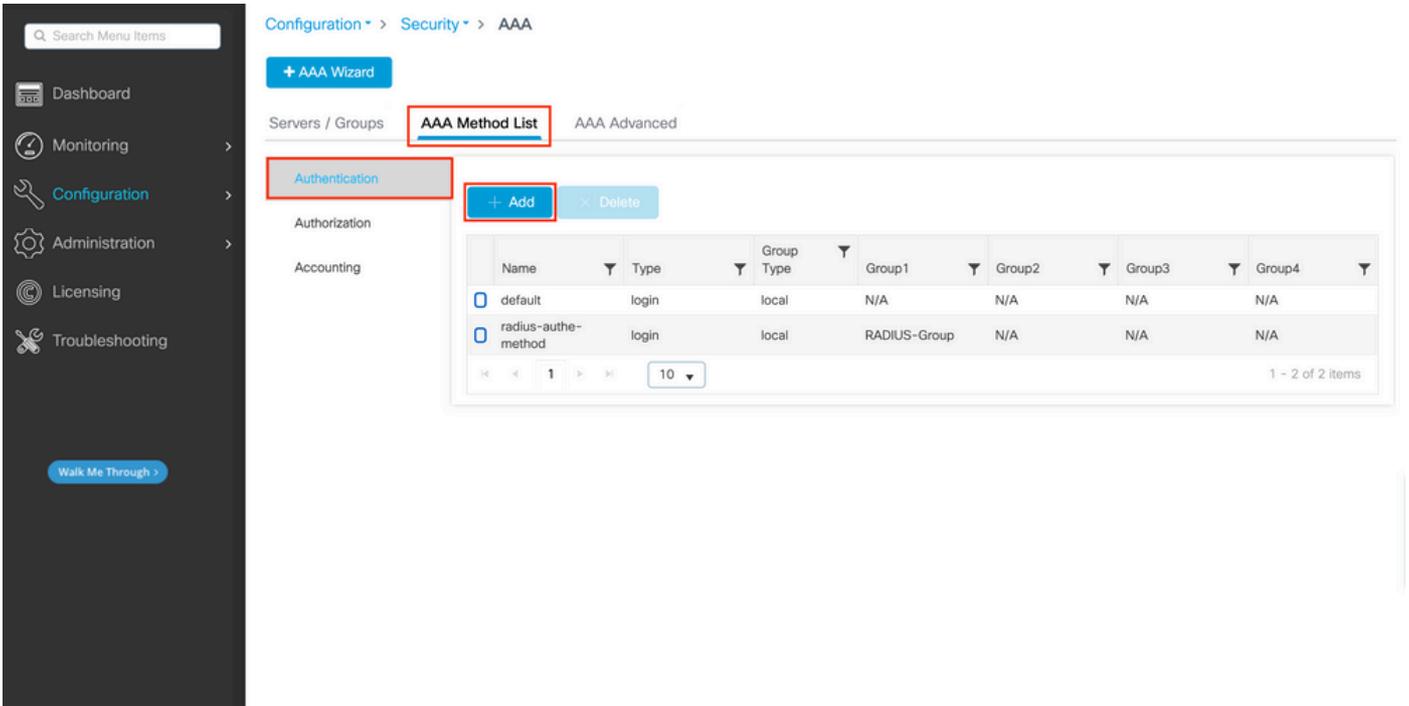
ISE-1ab

.
.
.
.
.

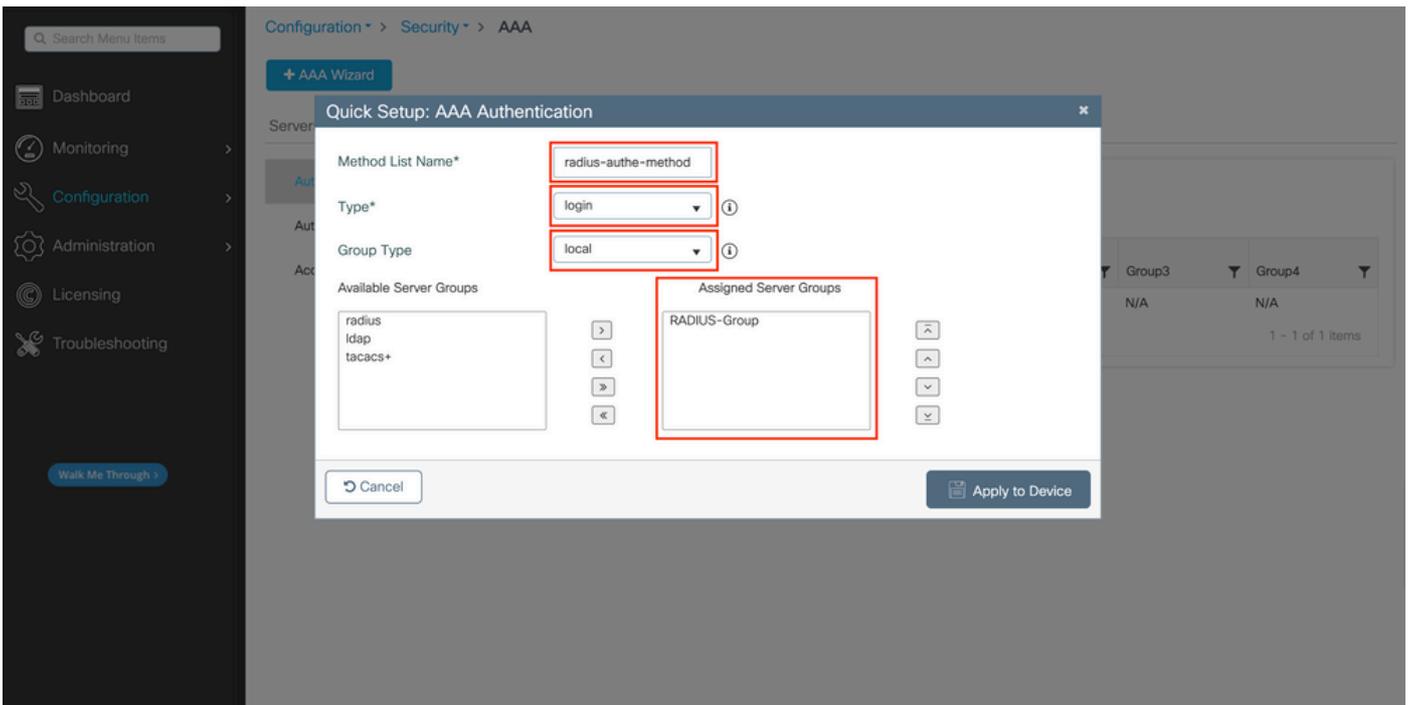
RADIUS مءاء ءوم جم لى لى رى ءء AAA ءقءاص م لوءء لى ءء ءق رط ءاش ناء مق 3 ءو طء لى

ءق مءوس رلى مءءء سمل ءهءاء نم

> AAA Method List بى وبء لى ءمء لى لى لى قنءا ءق مءوس رلى مءءء سمل ءهءاء <https://<WLC-IP>/webui/#/aaa> ءءء ءق نم ءءب ءر وء لى هءه فءءء وم وه امء ءقءاص ءق رط ءش ناء Authentication



هذه الأداة تتيح للمستخدمين إعداد قائمة طرق المصادقة، والتي يمكن استخدامها في إعدادات المصادقة، والتي يمكن استخدامها في إعدادات المصادقة.



هذه الأداة تتيح للمستخدمين إعداد قائمة طرق المصادقة، والتي يمكن استخدامها في إعدادات المصادقة، والتي يمكن استخدامها في إعدادات المصادقة.

- هناك إذا لم يتم إعداد (WLC) أي من الخوادم التي يمكن استخدامها في إعدادات المصادقة، والتي يمكن استخدامها في إعدادات المصادقة.

•

كشال في مكحتل رصنع نإف، لجم لىل عوجر رايلال نم ققحتلاب مقت ملو ةومجمك ةومجملا عون ترتخأ اذا مداوخل ةومجم لباقم مدختسمل تاغوسم نم طقف ققحتي (WLC) ةيكلسالل ةيلجملا

- كشال في مكحتل رصنع ققحتي، "لجم لىل يطايلال" رايلال تصحفو ةومجمك "ةومجملا عون" ترتخأ اذا تانايبل ةدعاق نع ملعتسيو مداوخل ةومجم لباقم مدختسمل دامتعا تانايبل نم (WLC) ةيكلسالل ةيلجملا نأ نكمي ناك ناوحت، مدختسمل ةقداصم متتس، ضفر لاسراب مداخل ما اذا. مداخل بحتسي مل اذا طقف ةيلجملا ةيلجملا تانايبل ةدعاق لىل ادوجوم نوكي.

رم اوألا رطس ةهجاو نم

مدختسأ، الوأ ايلجم اهليلع روثلعل متي مل اذا طقف مداوخل ةومجم عم مدختسمل دامتعا تانايبل نم ققحتل ديتر تنك اذا

<#root>

WLC-9800(config)#aaa authentication login

radius-auth-method

local group

RADIUS-Group

مدختسأ، طقف مداوخل ةومجم عم مدختسمل دامتعا تانايبل نم ققحتل ديتر تنك اذا

<#root>

WLC-9800(config)#aaa authentication login

radius-auth-method

group

RADIUS-Group

مذختساف، ىلحمل لادال عم رىأل اذع بحتسى مل اذو مداوع ةومجم عم مذختسمل دامتعا تاناب نم ققحتل اذرت تنك اذ:

<#root>

WLC-9800(config)#aaa authentication login

radius-auth-method

group

RADIUS-Group

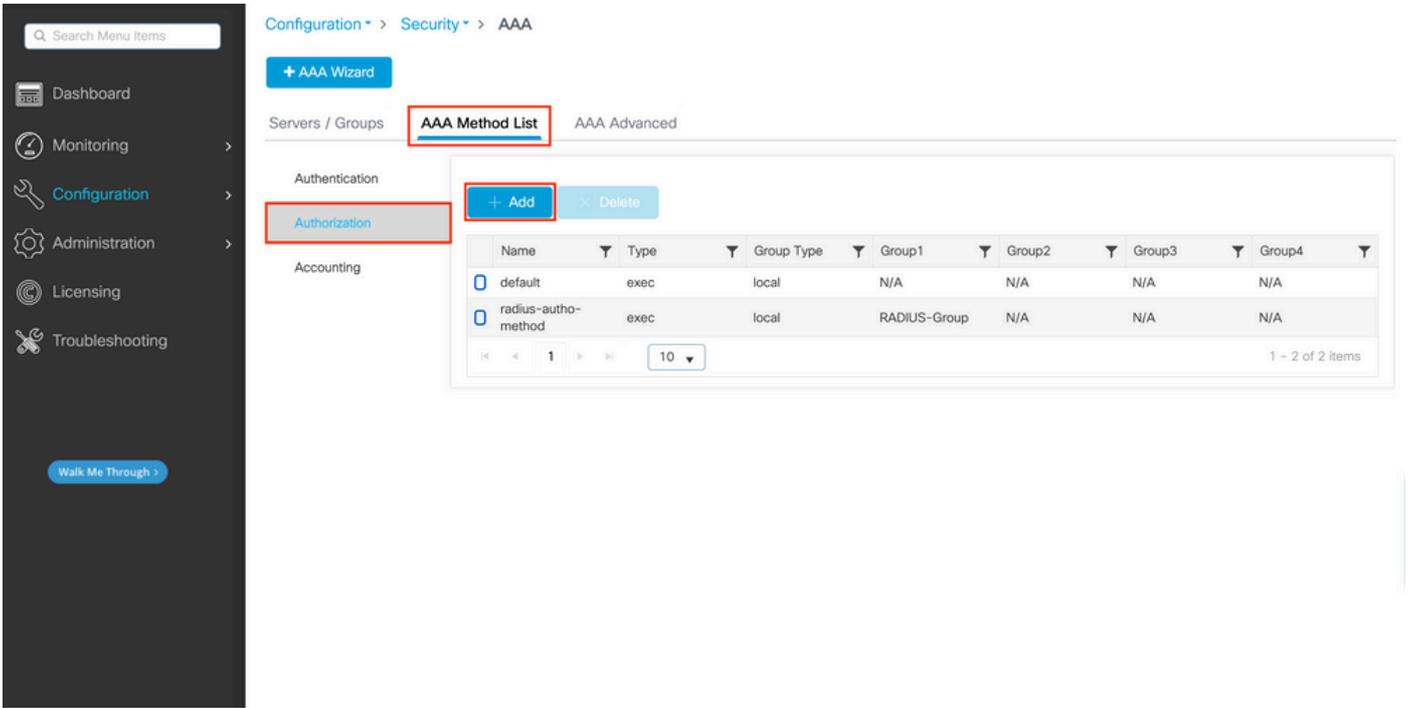
local

ISE، مداخ ىلع طقف نىمذختسمل اضعبو، طقف اىلحم مهؤاشن امت نىذل نىمذختسمل اضعب كانه، لالم اذع ىف لوأل رايال نومذختسى، ىلاتلابو.

RADIUS، مداوع ةومجم ىل رىشت AAA ضىوفتل EXEC ةقيرط عاشناب مق. 4 ةوطال

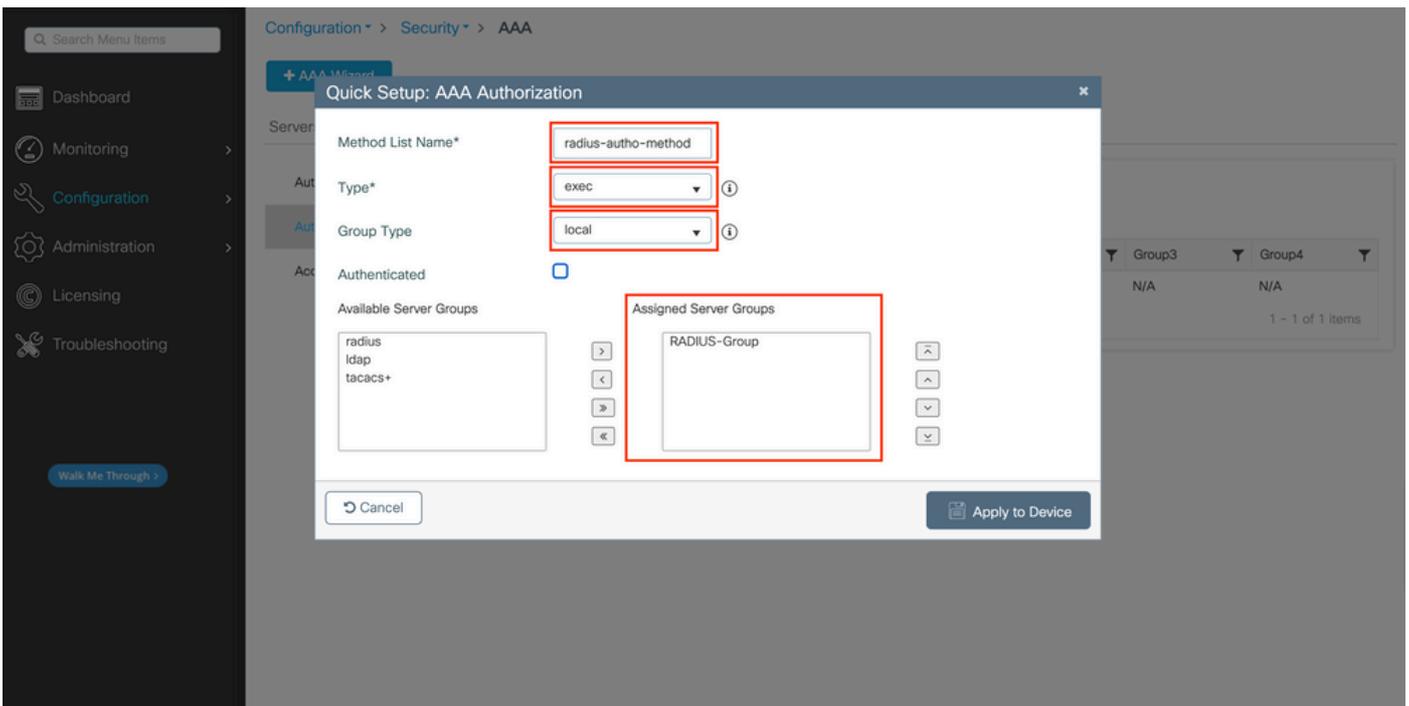
ةوموسرلما مذختسمل اةءاونم:

AAA ىل لقتنا، GUI Page Configuration > Security > AAA، نم دعب. لوصول قح هحنم متى ىتح مذختسمل لىوخت اضى بچى ةروصل هذه ىف حضوم وه امك دامتعا ةقيرط عاشناب مقو، بىوبتلا ةمالع Method List > Authorization



ليوخت الت بولسأ عاشنا

ةفاضل رزلا مادختساب ديدج بولسأ ةفاضل دنع هريوصت مت يذلا بولسألل لثامم قثبنم ليوخت بولسأ نيوكت رهظي



عونل بيترتال سفن مدختساو exec مساب عونلا رتخاو، ليوختال ةقيرطل مساري فوتب مق، قثبنم لنيوكتال اذه في ةوطخلال في ةقداصلال ةقيرطل مدختسملاك ةومجمل

نم اوألال رطس ةهجاو نم

م، ةيلحملال تالخال لباقم نيم مدختسمال نم ققحتلل الوأ ليوختال لنيوعت متي في، ةقداصلال ةقيرطل ةبسنلاب امأ م داوخل ةومجمل في تالخال لباقم

WLC-9800(config)#aaa authorization exec

radius-autho-method

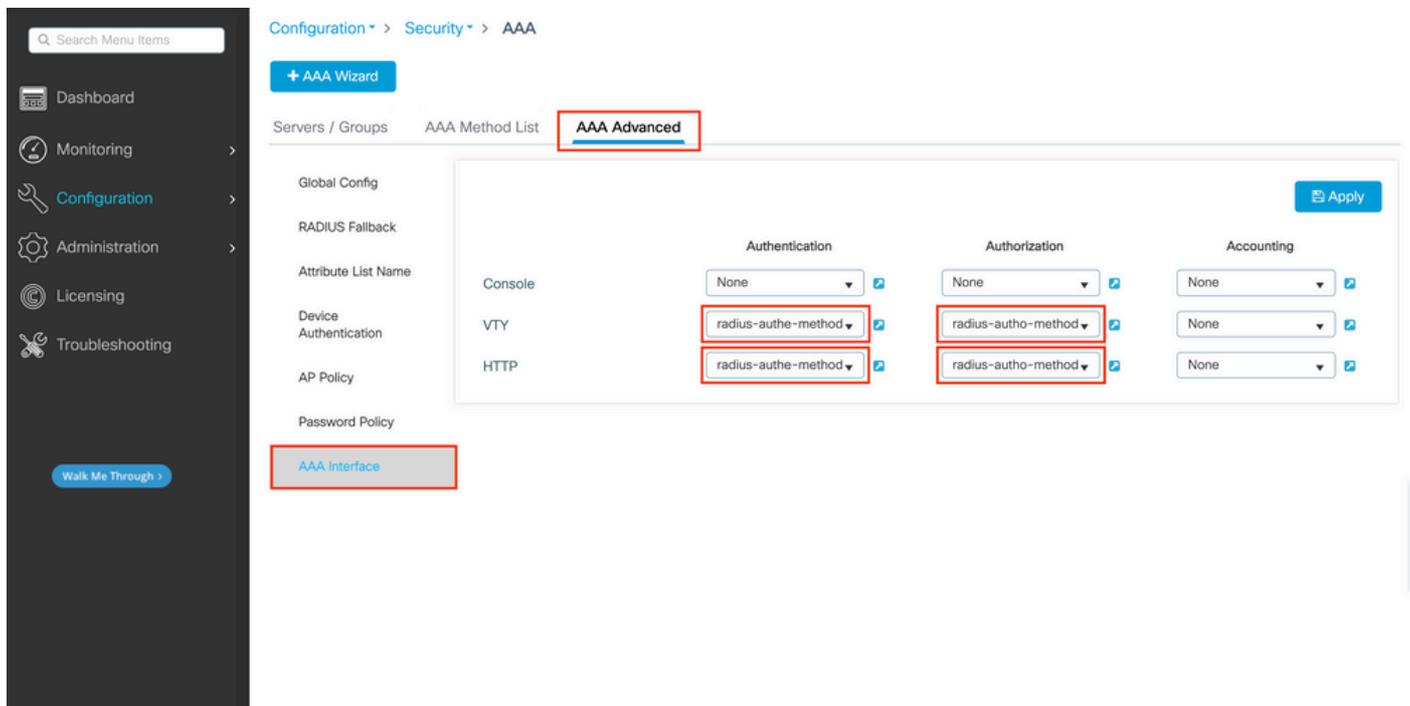
local group

RADIUS-Group

Telnet/SSH، vty طوطخ ىل و HTTP تان يوك تىل قرطال نىي عت ب مق 5. ةوطخ ال

ةي م و س ر ل ا م د خ ت س م ل ا ة ه ج ا و ن م :

ا ه ن ي و ك ت ن ك م ي ت ل ل و ، Telnet/SSH و /أو HTTP م د خ ت س م ل ا ص ت ا ل ا ه و ا ش ن ا م ت ي ت ل ا ض ي و ف ت ل ا و ة ق د ا ص م ل ا ق ر ط م ا د خ ت س ا ن ك م ي ي ف ا ه ي ل ل و و ص و ل ا ن ك م ي ي ت ل ل GUI WLC ة ح ف ص ن م ل ا ز ت ا ل ي ت ل ا ب ي و ب ت ل ا ة م ا ل ع AAA Advanced > AAA Interface ة ر و ص ل ا ه ذ ه ي ف ح ص و م و ه ا م ك :
<https://<WLC-IP>/webui/#/aaa>



ةي م و س ر ل ا م د خ ت س م ل ا ة ه ج ا و ة ق د ا ص م ل ا CLI :

<#root>

WLC-9800(config)#ip http authentication aaa login-authentication

radius-authe-method

WLC-9800(config)#ip http authentication aaa exec-authorization

radius-autho-method

CLI ةقداصم ل Telnet/SSH:

<#root>

WLC-9800(config)#line vty 0 15 WLC-9800(config-line)#login authentication

radius-authe-method

WLC-9800(config-line)#authorization exec

radius-autho-method

كلذ قيقحت نكمي. HTTP و HTTPS تامدخ ليغشت اداع لاضفأل نمف، HTTP تانيوكت لىلع تاريغيغتلا اارج دنع هنأ ظحال
ةيلاتل رماوأل مادختساب:

```
WLC-9800(config)#no ip http server WLC-9800(config)#no ip http secure-server WLC-9800(config)#ip http server WLC-9800(config)#ip http secure-server
```

تنيوكت RADIUS ل ISE

RADIUS ل ءكبش زاهجك (WLC) ءيكلساللة لىلحملة ءكبشلال يف مكحتلال رصنع ننيوكتب مق 1. ءوطخال

ةيموسرلا مدختسمللة ءهجاونم:

RADIUS ل ءكبش زاهجك قباسلال مسقلال يف (WLC) ءيكلساللة لىلحملة ءكبشلال يف مكحتلال رصنع مادختساب لىلحصول
لحصول وه امك، اءحتفاو ءكبشلال ءهجاو بىوبتلاة مالء Administration > Network Resources > Network Devices لىللقتنا، ISE يف
ةيلاتل ءروصلال يف.

The screenshot displays the Cisco ISE Administration interface. The top navigation bar shows 'Administration - Network Resources'. The left sidebar has 'Network Devices' selected. The main content area is titled 'Network Devices' and contains a table with the following data:

Name	IP/Mask	Profile Name	Location	Type	Description
WLC-9800	10.48.39.133/32	Cisco	All Locations	All Device Types	

ءىءلال ءكبشلال زاهج ننيوكت لىلحصول من ءتف يءللا ءفاضا رزلا مدختسأ، ءكبش زاهج ءفاضا ل

Network Devices

Default Device

Device Security Settings

Network Devices List > New Network Device

Network Devices

Name **WLC-9800**

Description

IP Address * IP: 10.48.39.133 / 32

Device Profile Cisco

Model Name

Software Version

Network Device Group

Location All Locations

Set To Default

IPSEC Is IPSEC Device

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

Second Shared Secret

Show

CoA Port

1700

Set To Default

RADIUS DTLS Settings

 DTLS Required

Shared Secret

radius/dtls

Show

دادع| ةي لم ة قداصم RADIUS ل| ترتخأ . هب صاخال IP ناو نع ةفاضاو ، ةكبشلا زاehl مسا ريفوتب مق ، دي دجال راطال ا يف WLC ل| لعل لمعتسي دجال نا ام رس كرتشم RADIUS هسفن ل| تل كشو

زايتمال ا عجال ، لي وخت ةجيتن عاش ناب مق . 2 ةوطخال

ةيموسرلا مدختسم ل| ةهجاو نم :

ةقبط ل| لوصولاب حمسي يذلاو ، 15 زايتمال ا يوتسم نوكي نا adminuserمزلي ، لوؤسم ل| لوصولا قوقح لعل لوصولل هنييعت نكمي ل| لالابو Shell ل| EXEC رماوا هجوم لوصول ل| رمال اجاتح helpdeskuser ل| ، رخأ ةيجان نم . exec ةبالاطم لي وختل ا فيرعت اتافل م ادختس| نكمي ، ني مدختسم ل| لباسانم ل| زايتمال ا يوتسم نييعتل . 15 نم لقا زايتمال ا يوتسم ب Authorization > بويوتل ا ةمال لفسأ ، ISE GUI Page Policy > Policy Elements > Results ، نم رصانعل ا هذو نيوكت نكمي ةيلال ا ةروصل ا يف ةحصولم ل| Authorization Profiles

Dictionaries Conditions **Results**

Authentication

Authorization

Authorization Profiles

Downloadable ACLs

Profiling

Posture

Client Provisioning

Standard Authorization Profiles

For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

Selected 0 Total 11

[Edit](#) [+ Add](#) [Duplicate](#) [Delete](#)All [Filter](#)

<input type="checkbox"/>	Name	Profile	Description
<input type="checkbox"/>	9800-admin-priv	Cisco	
<input type="checkbox"/>	9800-helpdesk-priv	Cisco	
<input type="checkbox"/>	Block_Wireless_Access	Cisco	Default profile used to block wireless devices. Ensure th
<input type="checkbox"/>	Cisco_IP_Phones	Cisco	Default profile used for Cisco Phones.
<input type="checkbox"/>	Cisco_Temporal_Onboard	Cisco	Onboard the device with Cisco temporal agent
<input type="checkbox"/>	Cisco_WebAuth	Cisco	Default Profile used to redirect users to the CWA portal
<input type="checkbox"/>	NSP_Onboard	Cisco	Onboard the device with Native Supplicant Provisioning
<input type="checkbox"/>	Non_Cisco_IP_Phones	Cisco	Default Profile used for Non Cisco Phones.
<input type="checkbox"/>	UDN	Cisco	Default profile used for UDN.
<input type="checkbox"/>	DenyAccess	Cisco	Default Profile with access type as Access-Reject

نأ بجي .ديجال لي وختال في رعت فلم ني وكت ج ذوم ن حت في يذال ة فاضا رزل ا مدخت س أ ، دي ج لي وخت في رعت فلم ني وكتل
adminuser. ه ني ي عت م تي يذال في رعتال فلم ني وكتل صوصخ ل ا ه ج و ل ع ج ذوم ن ل ا ذه و دبي

Dictionaries Conditions **Results**

Authentication > Authorization Profiles > New Authorization Profile

Authorization Profile

* Name **9800-admin-priv**

Description

* Access Type **ACCESS_ACCEPT**

Network Device Profile **Cisco**

Service Template

Track Movement ⓘ

Agentless Posture ⓘ

Passive Identity Tracking ⓘ

> Common Tasks

> Advanced Attributes Settings

Cisco:cisco-av-pair = shell:priv-lvl=15

> Attributes Details

Access Type = ACCESS_ACCEPT
 cisco-av-pair = shell:priv-lvl=15

Submit Cancel

لقب نم `adminuser` عقوت مل كولسلا وه اذه، لقب نم ركذ امك و. هب طبترم مدختسم يأل 15 حنم زايتما يوتسم نيوكتلا ضرع عاشن بجي يلاتلابو، لقا تازايتمالا يوتسم نوكتي نأ بجي `helpdeskuser`، كلذ عم و. ةيولاتلا ةوطخلل اءانثأ هؤاشن متهي يذلاو ناث ةسايس رصنع

لىل تريغ يغبني `shell:priv-lvl=15` ةلسلسلا نأ ادعام، طقف هالعأ قلخ دحاو لىل لثامم ل `helpdeskuser` ةسايسلا رصنع 1 مقرر مادختسا متهي، لاثملا اذه ي ف. بغير ب يوتسم زايتمالا عم X تلدبتسا و، `shell:priv-lvl=X`.

ISE لىل ني مدختسم تاعومجم عاشن 3. ةوطخل

ةيموسرلا مدختسم ليا ةهجاو نم:

Administration > Identity Management > Groups GUI Page في مدختسم ليا ةوه تاعومجم بيوبتلا ةمالع نم ISE في مدختسم تاعومجم عاشن متهي ةشاشلا طاقتلا في رهظي يذلاو، ةشاشلا Groups GUI Page

Network Access Users

Selected 0 Total 2

Edit + Add Change Status Import Export Delete Duplicate

All

Status	Username	Description	First Name	Last Name	Email Address	User Identity Groups	Admin
<input type="checkbox"/>	Enabled	adminuser				admin-group	
<input type="checkbox"/>	Enabled	helpdeskus...				helpdesk-group	

حضوره وه امك ديدجلا ةكبشلا لىل لوصولا مدختسم نيوكت جذومن حتفل "ةفاضل" رزلا مدختسا ،ديج مدختسم عاشنال

Users

Latest Manual Network Scan Res...

Network Access Users List > New Network Access User

Network Access User

* Username **adminuser**

Status Enabled

Account Name Alias

Email

Passwords

Password Type: Internal Users

Password Lifetime:

With Expiration
Password will expire in 60 days

Never Expires

Password Re-Enter Password

* Login Password Generate Password

Enable Password Generate Password

> User Information

> Account Options

> Account Disable Policy

User Groups

admin-group

نېم دځتسمل امه و، اه/ب هب نېصاخل رورملا ةم لك و مدځتسمل مسا ي، نېم دځتسمل دامتع ال اناي ب ريفوت ب مق اريخ. Enabled مدځتسمل انا ن اضا ي اذات (WLC) ةيكلسال ال ةيكلحال ةكبشلا ي ف مكحتل رصنع يل ع ةقداصل لل نېم دځتسمل انا وومجم ةلدسنملا ةمئاقلا عم ، 4 ةوطخلال ي اهواشن ا مت ي تالو ، ةلصل اذ هتعوومجم ال مدځتسمل انا ف جذومنلا ةياهن ي ف

مهال ع ا مهتشقانم تمت نېنذلل نېم دځتسمل اعاشنا ب مق adminuser و helpdeskuser امه و.

نېم دځتسمل انا ةقداصل م 5 ةوطخلال

ةيوسرل ا مدځتسمل انا ةهجاو نم:

اقبسم اهنېوكت مت ي تالو و، ISE ل ةيضا رتفالال جهنل انا وومجم ةصاخل ا ةقداصل م ةسايس حمست ، ويرانېنسال اذ ه ي مدځتسمل انا ةهجاو ةحفص Policy > Policy Sets نم هذ ه نل ا ةوومجم ةطحال م نكم ي . ةكبشلا ال يضا رتفالال لوصولاب ، لعفالاب هريغت ال ةحال كلذل . ةروصلال هذ ه ي ف حضوم وه امك ، ISE ب ةصاخل ال (GUI) ةيوسرل

Policy Sets → Default

Reset

Reset Policyset Hitcounts

Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Default	Default policy set		Default Network Access	0

Authentication Policy (3)

Status	Rule Name	Conditions	Use	Hits	Actions
✓	MAB	OR Wired_MAB Wireless_MAB	Internal Endpoints > Options	0	⚙️
✓	Dot1X	OR Wired_802.1X Wireless_802.1X	All_User_ID_Stores > Options	0	⚙️
✓	Default		All_User_ID_Stores > Options	0	⚙️

نېم دځت سمل لېوخت 6. ؤ وطلال

نېم وسرلېا مځت سملېا ؤه چا ونم

لېوختال فېرعت فلم عاجرا ISE لى بچې واهلېوخت بچې، ؤقداصملا ؤسايس رېرم تې لوځدلا لېچست ؤلواحم موقت نا دعب (تازايمالا يوتسم لى ؤفاضالاب، لوبقب حامسالا) اقبس مهؤاشنا مت يذلا

ف مځحتلا ؤدحوب صاخلا IP ناونع وهو زاوجلل IP ناونع لى ادا نسا لوځدلا لېچست تالواحم ؤيفصت مت، لاثملا اذه ف اه لى يمتنې يتيلا ؤومجملا لى ادا نسا حنم متيس يذلا زايمالا يوتسم زييمتو (WLC) ؤيكلساللا ؤيحمللا ؤكشلا لك يوتحت شي مهب ؤصاخلا نېمځت سملءامسا لى ادا نسا نېمځت سمل ؤيفصت ل حل اص رءآ جهن كانه. مځت سمل لاثملا اذه ف طقف دحاو مځت سمل لى ؤومجم

Policy Sets → Default

Reset

Reset Policyset Hitcounts

Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Default	Default policy set		Default Network Access	152

> Authentication Policy (3)

> Authorization Policy - Local Exceptions

> Authorization Policy - Global Exceptions (2)

Status	Rule Name	Conditions	Results		Hits	Actions
			Profiles	Security Groups		
✓	9800 Helpdesk Users	AND Network Access-Device IP Address EQUALS 10.48.39.133 InternalUser-IdentityGroup EQUALS User Identity Groups:helpdesk-group	9800-helpdesk-priv	Select from list	1	⚙️
✓	9800 Admin Users	AND Network Access-Device IP Address EQUALS 10.48.39.133 InternalUser-IdentityGroup EQUALS User Identity Groups:admin-group	9800-admin-priv	Select from list	2	⚙️

> Authorization Policy (12)

Reset

Save

يفق داصم لل helpdesk مخدم مستعمل adminuser ل اهنويوكت مت يتي التا مته الال تانايب مادختس | نكمي، ةوطخل هذه لامتك ادعب جم انرب لالخنم وأ (GUI) ةيموسررل مدمتس ملة ةهواو ربع (WLC) ةيكلسال ال ةيلحم ال ةكبش لال يف مكحتل رصنع Telnet/SSH.

تويوكت TACACS+ WLC

TACACS+ مداخنال ع | 1 ةوطخل

ةيموسررل مدمتس ملة ةهواونم:

نم كلذب مايق لال نكمي (WLC) ةيكلسال ال ةيلحم ال ةكبش لال يف مكحتل رصنع عل TACACS+ مداخنال ISE ءاشناب مق، الوأ (WLC) ةيكلسال ال ةيلحم ال ةكبش لال يف مكحتل رصنع ةحفص نم Servers/Groups > TACACS+ > Servers مديوبت ال ةمالع لاقتنالاب تمق اذ | وأ https://<WLC-IP>/webui/#/aaa، يف اهليل لوصول نكمي يتي ال (GUI) ةيموسررل مدمتس ملة ةهواو ةصاخ ال ةروصل هذه يف حضورم وه امك، Configuration > Security > AAA

Configuration > Security > AAA

+ AAA Wizard

Servers / Groups AAA Method List AAA Advanced

+ Add - Delete

RADIUS

TACACS+

LDAP

Servers Server Groups

Name	Server Address	Port
ISE-lab	10.48.39.134	49

1 - 1 of 1 items

رمحألأب رطؤمأل ةفاضل رزلأ قوف رقنا، (WLC) ةيكللساللا ةيلحمل ةكبشلا يف مكحتلأ رصنع يلع TACACS مداخل ةفاضل يف ةموسرملأ ةقثبنمأل ةذفانلأ حتف لىل اذه يدؤي. هالعأ ةروصلأ يف

Configuration > Security > AAA

+ AAA Wizard

Servers / Groups

+ Add

RADIUS

TACACS+

LDAP

Create AAA Tacacs Server

Name* ISE-lab

Server Address* 10.48.39.134

Key Type Clear Text

Key*

Confirm Key*

Port 49

Server Timeout (seconds) 1-1000

Cancel Apply to Device

حاتفمأل، هب صاخأل IP ناونع، (ISE) ماظن مسا قباطي نأ بجي أل) مداخل مسا ريفوتب مق، ةقثبنمأل ةذفانلأ حتفت امدنع ةلهملأو، مدختسمأل ذفنمأل، كرتشمأل

ريفوت كليلع بجي، ةقثبنمأل ةذفانلأ هذه يف:

ISE ماظن مسا قباطي نأ بجي ال هنا طحال) مداخل مسا

- مداخل IP ناو نع
- TACACS+ مداخلو ةيكلسالل ةيلحملا ةكبشلا يف مكحتلا رصنع نيب كرتشملا رسلا

دادعك كرتتو ةيمازلل تسيل هذه نكلو، ةبسا حمل او ةقداصلل ةمدختس مل اذفانملا لثم، يرخأ تاملعم نيوكت نكمي دنتسمل اذهل يضارتفا

رم اوألا رطس ةهجاو نم

<#root>

WLC-9800(config)#tacacs server

ISE-lab

WLC-9800(config-server-tacacs)#address ipv4

10.48.39.134

WLC-9800(config-server-tacacs)#key

Cisco123

مداوخ ةعومجم ىل TACACS+ مداخ نييعتب مق 2. ةوطخل

ةي موسرلا مدختسمل ةهجاو نم:

مداوخ ةعومجم ىل مداوخلا هذه عي مج نييعتب ىصوي، ةقداصلل اهمادختسا نكمي ةددعتم TACACS+ مداوخ دوجو ةلاح يف نييب ةفلتخم تاقداصلل لاملأال عيزوتب (WLC) ةيكلسالل ةيلحملا ةكبشلا يف مكحتلا ةدحو متهت ذئدنعو. اهسفن بيوبتلل ةمالع TACACS > Server Groups > Servers/Groups نم TACACS+ مداوخ تاعومجم نيوكت متي. مداوخ ةعومجم يف مداوخلا ةروضلا يف ةحصولو او، 1. ةوطخل يف ةروكذمل (GUI) ةي موسرلا مدختسمل ةهجاو ةحفص سفن نم

Configuration > Security > AAA

+ AAA Wizard

Servers / Groups AAA Method List AAA Advanced

+ Add - Delete

RADIUS

TACACS+

LDAP

Servers Server Groups

Name	Server 1	Server 2	Server 3
TACACS-Group	ISE-lab	N/A	N/A

1 - 1 of 1 items

يفي حضوره او، عبقاسلا ءروصل راطا يف ءفاضا رزلا قوف رقنلا دنع ءقثبنم ءذفان رهظت، مءاخال ءاشنال ءبسنلاب ءروصل.

Configuration > Security > AAA

+ AAA Wizard

Server

Create AAA Tacacs Server Group

Name* TACACS-Group

Group Type TACACS

Available Servers

Assigned Servers

ISE-lab

Cancel Apply to Device

ءنعملا مءاخال ءمءاق لىل ءبولطملا مءاخال لقناو ءعومءملا ءيمس تب مق، ءقثبنملا ءمءاق لىل يف

رم اوألا رطس ءهءاونم

<#root>

WLC-9800(config)#aaa group server tacacs+

TACACS-Group

WLC-9800(config-sg-tacacs+)#server name

ISE-lab

TACACS+ مداوخة ومجمي الى ريشة AAA ةقداصم لوخد ليجست ةقيرط عاشناب مق 3. ةوطخل

نقيموسرللا مدختسمللا ةهجاو نم

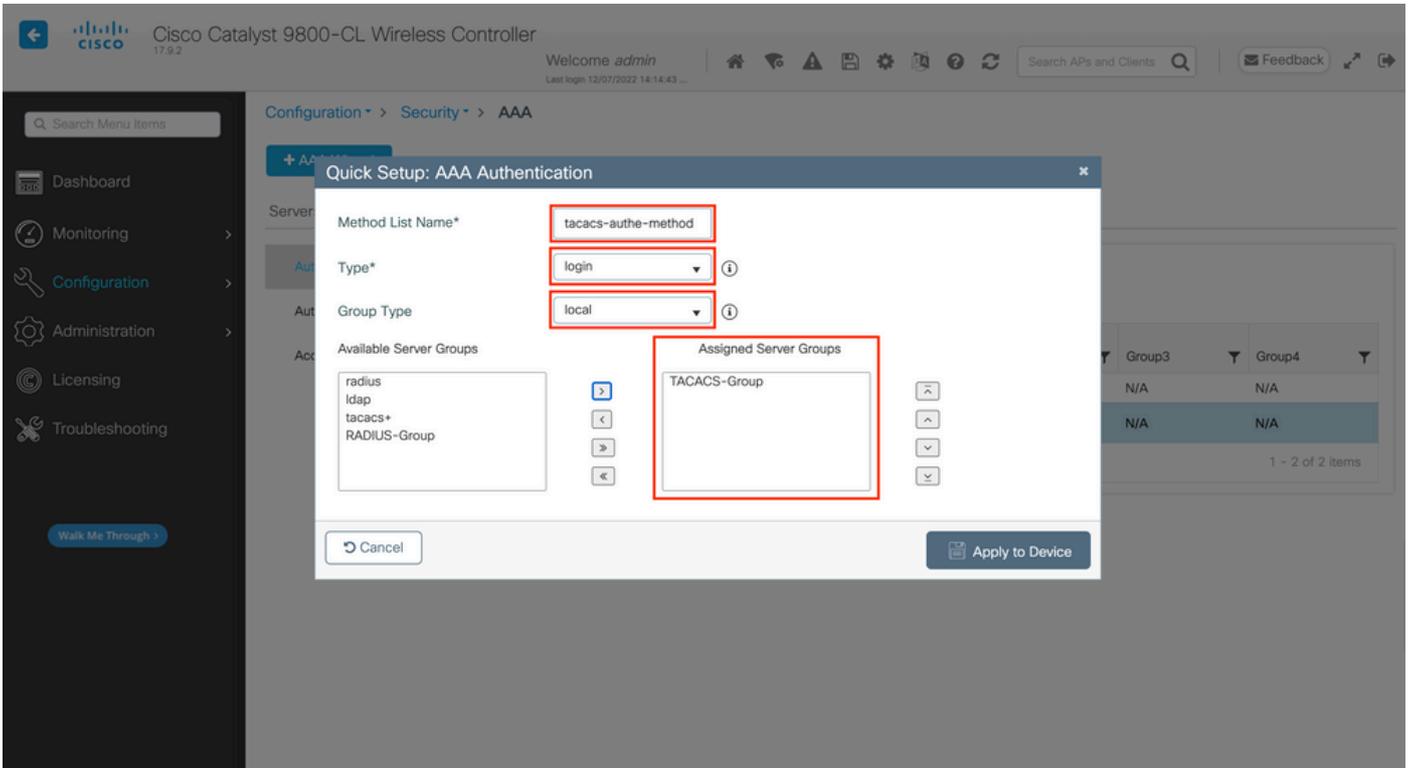
ةمالع AAA Method List > Authentication الى لقتنا ،ةيموسرللا مدختسمللا ةهجاو <https://<WLC-IP>/webui/#/aaa> ةحفص نم دعب

ةروصللا يف حضورم وه امك ةقداصم ةقيرط عاشناب مقو ،بويوبتللا

The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller web interface. The breadcrumb navigation is Configuration > Security > AAA. The 'AAA Method List' tab is selected. The 'Authentication' sub-tab is also selected. A table lists the AAA methods:

Name	Type	Group Type	Group1	Group2	Group3	Group4
default	login	local	N/A	N/A	N/A	N/A
radius-auth-method	login	local	RADIUS-Group	N/A	N/A	N/A
tacacs-auth-method	login	local	TACACS-Group	N/A	N/A	N/A

ةذفانلل ةلثامم ،نيوكتلل ةقثبنم ةذفان رهظت ،ةقداصم ةقيرط عاشناب ةفاضلا رزم دختست ام دنع ،داتعم وه امك ةروصللا هذه يف ةحضورملا



هؤاشن مت يذلا ةوعومجم لمداخ ةفاضاب مقو login مسم سابتكالك رتخاو ،بولسألل مساريفوتب مق ،قتب نمل راطلإا اذه يف نم ديدعل اءارجا نكمي ،ةوعومجم لعون لققب قلع تي اميف .ةنعم لم مداوخل تاوعومجم ةمئاق ىلإ ةقباسلا ةوطخل يف تانويكتلا .

- تانك اذا امم الؤا (WLC) ةيكل لساللا ةي لجملا ةكبشلل يف مكحتلا رصنع ققحتي ،اي لجم "ةوعومجم لعون" تترتخا اذا مداوخل ةوعومجم ىلإ ىرخا ةرم دوعي مت ،اي لجم ةدوجوم مدختسمل دامتعا تاناي ب .
- ةكبشلل يف مكحتلا رصنع ناف ،يلجم ىلإ عوجر راىخل نم ققحتلاب مقت ملو ةوعومجم ةوعومجم لعون تترتخا اذا مداوخل ةوعومجم لباقم مدختسمل تاغوسم نم طقف ققحتي (WLC) ةيكل لساللا ةي لجملا .
- ةكبشلل يف مكحتلا رصنع ققحتي ،"يلجم ىلإ يطايتحا" راىخل تصحفو ةوعومجم ك "ةوعومجم لعون" تترتخا اذا تانايبال ةدعاق نع ملعتسيو مداوخل ةوعومجم لباقم مدختسمل دامتعا تاناي ب نم (WLC) ةيكل لساللا ةي لجملا نأ نكمي ناك ناويتح ،مدختسمل ةقداصم متتس ،ضفر لاسراب مداخال ماا اذا .مداخال بجتسي مل اذا طقف ةي لجملا ةي لجملا تانايبال ةدعاق ىلإ ةدوجوم نوكتي .

رم اوأل رطس ةهجاو نم :

مدختسأ ،الؤا ايلجم اهيلع روثلعل متي مل اذا طقف مداوخل ةوعومجم عم مدختسمل دامتعا تاناي ب نم ققحتلا ديرت تانك اذا :

<#root>

WLC-9800(config)#aaa authentication login

tacacs-auth-method

local group

TACACS-Group

مدخستسأ ،طقف مداوخة وومجم عم مدخستسملل دامتعان اناي ب نم ققحتللا ديرت تنك اذا

<#root>

WLC-9800(config)#aaa authentication login

tacacs-auth-method

group

TACACS-Group

مدخستس اف ،يلجم لاخدا عم بيچتسي ال ريخال اذه ناك اذاو مداوخة وومجم عم مدخستسملل دامتعان اناي ب نم ققحتللا ديرت تنك اذا

<#root>

WLC-9800(config)#aaa authentication login

tacacs-auth-method

group

TACACS-Group

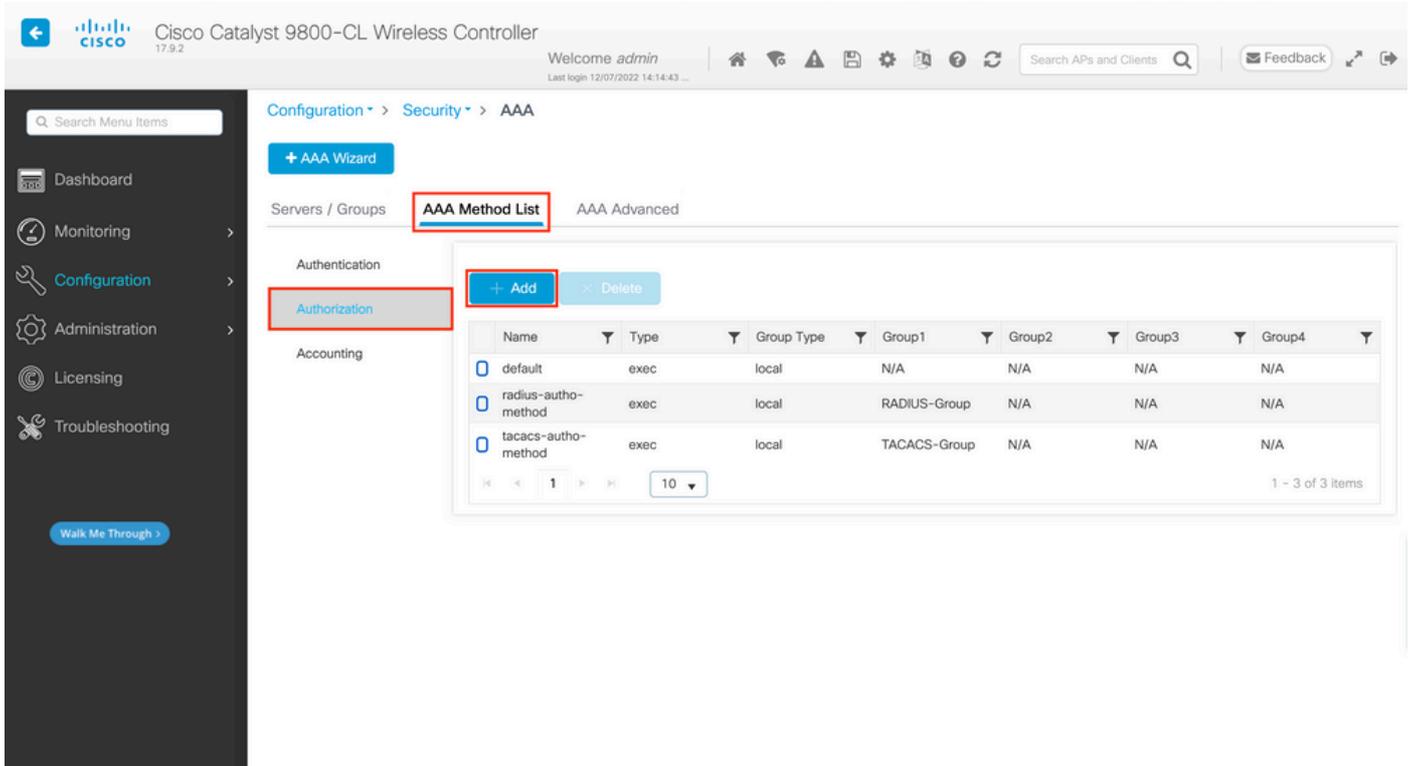
local

يلتالابو ISE، مداخل على طقف ني مداخل مستعمل وضعبو، طقف اي لحماه واوشنا مت ني ذلاني مداخل مستعمل وضعبو كانه، لثالما اذه ي لوالا رايل مداخل سا

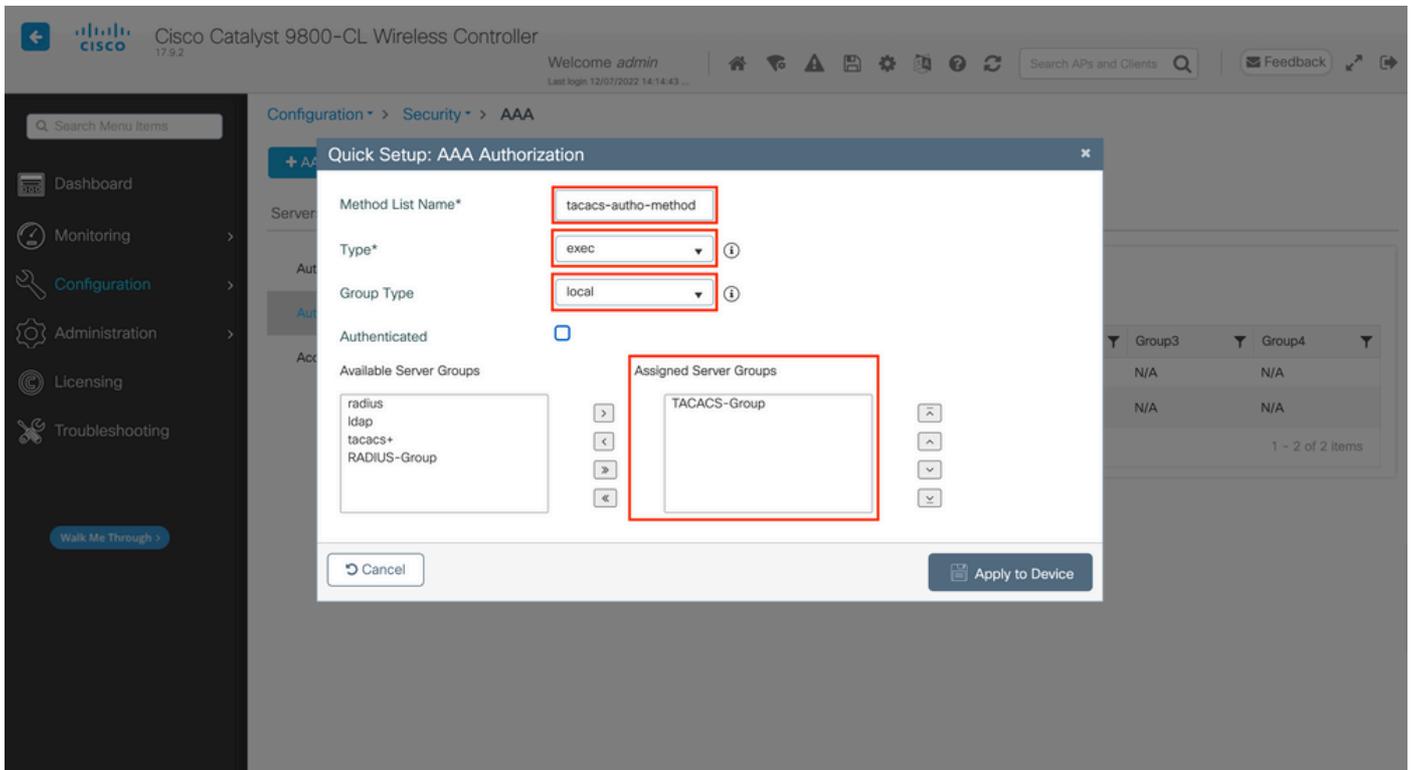
TACACS+ مداخل مستعمل اي ري شي يذلي ليوختل AAA بولسا عاشنا ب م ق 4 ة وطلخال

ة: م وسر ل مداخل مستعمل ا ق ه جاو نم

Configuration > Security > AAA، ة: م وسر ل مداخل مستعمل ا ق ه جاو ة حفص نم دعب. لوصولا ق ه جنم متي تحت مداخل مستعمل ليوخت بجي امك ة: م وسر ل ا ق ه جاو ة حفص نم دعب، بيوختل AAA Method List > Authorization ة: م وسر ل ا ق ه جاو ة حفص نم دعب، بيوختل AAA، ة: م وسر ل ا ق ه جاو ة حفص نم دعب.



ة: م وسر ل ا ق ه جاو ة حفص نم دعب، بيوختل AAA، ة: م وسر ل ا ق ه جاو ة حفص نم دعب، بيوختل AAA، ة: م وسر ل ا ق ه جاو ة حفص نم دعب، بيوختل AAA، ة: م وسر ل ا ق ه جاو ة حفص نم دعب.



عنوان بېتريال س فن مدخساو، exec مساب عونلا رتخاو، ليوختلا قيرطل مساري فوتب مق، قثبننم لانيوكتلا اذه ي قباصولا ووطخلال ي قداصولا قيرطل مدختسملاك ةومجمل.

رماولا رطس ةهجاو نم:

<#root>

WLC-9800(config)#aaa authorization exec

tacacs-autho-method

local group

TACACS-Group

Telnet/SSH ل مدختسملا vty طوطخلالو HTTP تانيوكت ل قيرطل لانييغت مق. 5 ةوطخلال

تلقوا Telnet/SSH:

```
<#root>
```

```
WLC-9800(config)#line vty 0 15
WLC-9800(config-line)#login authentication
```

```
tacacs-auth-method
```

```
WLC-9800(config-line)#authorization exec
```

```
tacacs-auth-method
```

كلذ قيقحت نكمي. HTTPS و HTTP تامدخ ليغشت اداعا لضال نمف، HTTP تانيوكت يلع تاريغيغتلا اارجا دنع هنا ظحال رماوالا هذه مادختساب.

```
WLC-9800(config)#no ip http server
WLC-9800(config)#no ip http secure-server
WLC-9800(config)#ip http server
WLC-9800(config)#ip http secure-server
```

تلقوا TACACS+ ISE نيوكت

TACACS+ ل تكبش زاك (WLC) ايكلساللا ايلحمل اكبشلا يف مكحتلا رصنع نيوكتب مق. 1. اوطخلا

اوموسرلا مادختسابلا اوجاوم:

RADIUS ل تكبش زاك قبالا مسقلا يف (WLC) ايكلساللا ايلحمل اكبشلا يف مكحتلا رصنع مادختساب ايصوتل

حضوره وه امك، اهحتفاو ةكبشلا ةزهجأ بيوبتلا ةمالع Administration > Network Resources > Network Devices لىلقنا ي ISE، ةروصلا هذو ف.

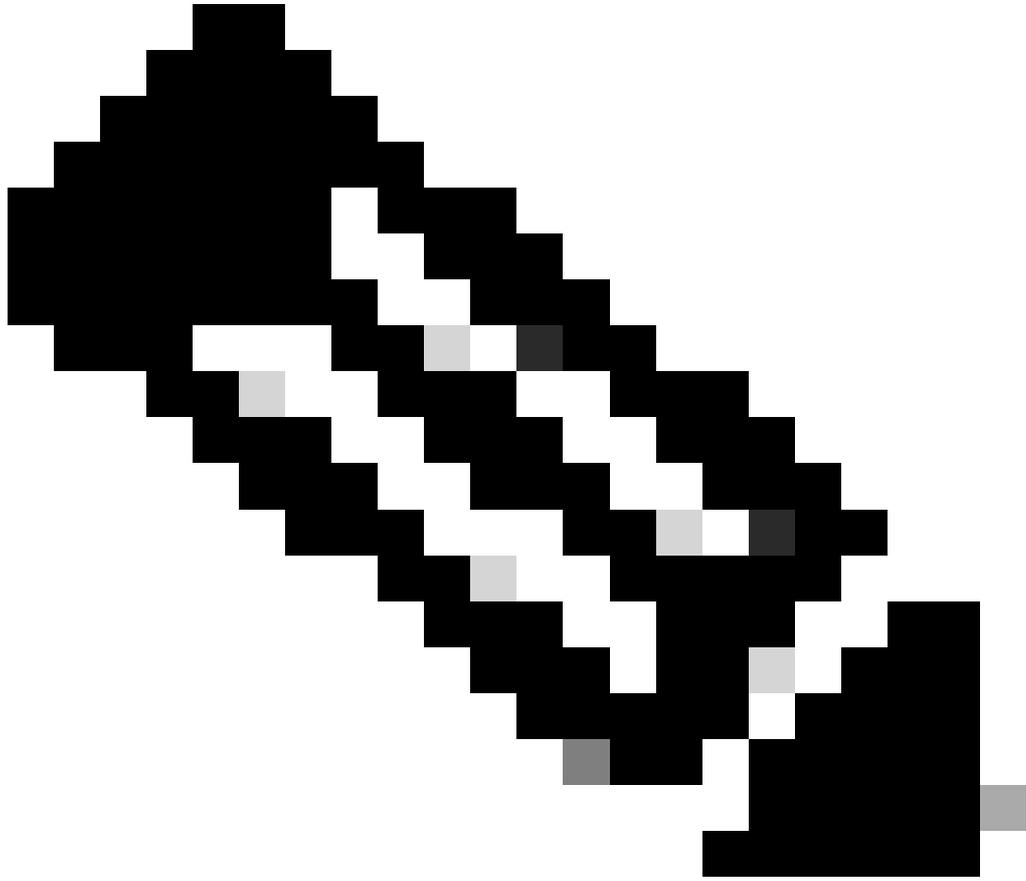
The screenshot shows the Cisco ISE Administration interface. The top navigation bar includes 'Cisco ISE', 'Administration · Network Resources', and 'Evaluation Mode 82 Days'. The main navigation menu has 'Network Devices' selected. The left sidebar shows 'Network Devices', 'Default Device', and 'Device Security Settings'. The main content area is titled 'Network Devices' and shows a table with one device: 'WLC-9800' with IP/Mask '10.48.39...', Profile Name 'Cisco', Location 'All Locations', and Type 'All Device Types'. The 'Edit' button is highlighted with a red box.

1. ةوطخلال لىلقنا عجر) RADIUS ةقداصم (WLC) ةكللساللا ةلحمل ةكبشلا ف مكحتلال رصنع ةفاضلا تمت، لالم اذو ف يذلو، TACACS ةقداصم نيوكتل هليدعت متي نأ لىلقنا ةطاسبب هنيوكتل جاتحي، كذلذ (RADIUS نيوكتل مسقلا نم زاهج نيوكتل جذومن حتف لىلقنا يدؤي اذو. ريرحت رزلا قوف رقناو ةكبشلا ةزهجأ ةمئاق ف ي WLC راتخت امدنع هلعف نكمي ةروصلا هذو ف حضوره وه امك ةكبشلا.

The screenshot shows the 'TACACS Authentication Settings' for the 'WLC-9800' device. The 'TACACS Authentication Settings' section is expanded and highlighted with a red box. The 'Shared Secret' field is also highlighted with a red box. Other settings include 'Enable KeyWrap', 'Key Encryption Key', 'Message Authenticator Code Key', 'Key Input Format' (ASCII selected), 'Enable Single Connect Mode' (Legacy Cisco Device selected), 'SNMP Settings', and 'Advanced TrustSec Settings'.

رسلا ةفاضلاو، تادادعالا هذو نيكم تو، TACACS ةقداصم تادادعالا مسق لىلقنا ريرمتلاب مق، ةديدجالا ةذفانلا حتف درجمب TACACS+ WLC نيوكتل مسقلا نم 1. ةوطخلال اناثأ هلاخدإ مت يذلا كرتشملا.

ةدقعلل "زاهجالا لوؤسم" ةريم نيكم تب مق 2. ةوطخلال



صیخرت و Base صیخرت ام، ةزهجال ةرادا صیخرت ةمزح كیدل نوکي نأ بجي، TACACS+ مداخك ISE مادختسال :تظالم
Mobility.

تفيموسرلما مدختسملما ةهجاو نم

مداخك ISE مادختسال نم نكمتتل ةدقعلل "ةزهجال ةرادا" ةزيم نيكمت كيلع بجي، ةزهجال ةرادا صيخارت تيبتت درجمب
Administrator اهيلع روثلعلا نكمي يتلاو، ةمدختسمل ISE رشن ةدقع نيوكت ريحبت مق، كلذب مايقللو. TACACS+
Edit. رزلا ةدعاسمب كلذب مق وأ اهمسا قوف رقناو، لفسأ Deployment

Deployment



Deployment Nodes

Selected 0 Total 1

Edit Register Syncup Deregister

All

<input type="checkbox"/>	Hostname	Personas	Role(s)	Services	Node Status
<input type="checkbox"/>	ise	Administration, Monitoring, Policy Service	STANDALO...	SESSION,PROFILER	<input checked="" type="checkbox"/>

هذه هي ف حضوم وه امك ، "جهنلا عم دح" مسق نمض ةزهجال ةرادا ةمدخ نيكم مت رايج نم ققحت ، ةدقعالا نيوكت ةذفان حتف درجم ب ةروصلال.

Deployment

Deployment Nodes List > ise

Edit Node

General Settings Profiling Configuration

Hostname ise

FQDN ise.cisco.com

IP Address 10.48.39.134

Node Type Identity Services Engine (ISE)

Role STANDALONE [Make Primary](#) Administration Monitoring

Role PRIMARY

Other Monitoring Node

 Dedicated MnT Policy Service Enable Session Services

Include Node in Node Group None

 Enable Profiling Service Enable Threat Centric NAC Service Enable SXP Service Enable Device Admin Service Enable Passive Identity Service pxGrid

Reset

Save

زایتمال اعجازال، TACACS تافيصوت عاشناب مق. 3 ةوطخلال

ةيموسرللا مدختسمللا ةهجاو نم:

ةقبط ىلا لوصولاب حمسي يذلاو، 15 زایتمال ىوتسم نوكي نأ adminuserمزللي، لوؤسملل لوصولا قوقح ىلع لوصولل
نهنيغت نكمي لىلاتلابو Shell لى EXEC رماو هجوم لوصولو لى رمالا جاتحي helpdeskuser، ىرخا ةيخان نم exec ةبالاطم
لليوخلتلافيرت تافل م ادختسا نكمي، نيمدختسملل بسانملا زایتمال ىوتسم نبيعتل. 15 نم لقا زایتما ىوتسم ب
(ISE) ةيموسرللا مدختسمللا ةهجاو Work Centers > Device Administration > Policy Elements ةحفض نم رصانعلا هذه نيوك نكمي
ةلىلاتلا ةروصلال ي فحوصوم وه امك Results > TACACS Profiles ةمالع لفسأ

Conditions	Library Conditions	Smart Conditions
Network Conditions		
Results	Allowed Protocols	TACACS Command Sets
TACACS Profiles		

TACACS Profiles

Rows/Page 6 << 1 >> Go 6 Total Rows

[Add](#) [Duplicate](#) [Trash](#) [Edit](#)[Filter](#) [Settings](#)

<input type="checkbox"/>	Name	Type	Description
<input type="checkbox"/>	Default Shell Profile	Shell	Default Shell Profile
<input type="checkbox"/>	Deny All Shell Profile	Shell	Deny All Shell Profile
<input type="checkbox"/>	IOS Admin	Shell	Assigned to each user in the group admin-group
<input type="checkbox"/>	IOS Helpdesk	Shell	Assigned to each user in the group helpdesk-group
<input type="checkbox"/>	WLC ALL	WLC	WLC ALL
<input type="checkbox"/>	WLC MONITOR	WLC	WLC MONITOR

لكل ذلك لثامم الال ديديج الال فيرعت الال فلم نيوكت جذومن حت في يذلا "ة فاضا" رزلا مدختسأ ،ديج TACACS فيرعت فلم نيوكتل الى هنييغت متي يذلا فيرعت الال فلم نيوكتل صاخ لكش لكالش الال اذبه جذومن الال اذبه ودي نأ بجي .ةروصلال في دوجوم الال adminuser (shell 15) تازايتما يوتسم مادختساب ،وه يذلاو).

TACACS Profiles > IOS Admin
TACACS Profile

Name
IOS Admin

Description
Assigned to each user in the group admin-group

Task Attribute View Raw View

Common Tasks

Common Task Type Shell

Default Privilege 15 (Select 0 to 15)

Maximum Privilege 15 (Select 0 to 15)

Access Control List

Auto Command

No Escape (Select true or false)

Timeout Minutes (0-9999)

Idle Time Minutes (0-9999)

Custom Attributes

Add Trash Edit

Type	Name	Value
No data found.		

Cancel Save

1. إلى تثبيت الك، زايتم maximum، زايتم ريصقتل، ريخألا اذه ل. فيرعتل helpdesk فلمل ةيلمعل رك

ISE. لىل نيمدختسم تاعومجم عاشن. 4 ةوطخل

دنتسملا اذه نم [RADIUS ISE نيوكت](#) مسقلا نم 3. ةوطخلال في ضرورعم هسفن وه اذه

ISE. لىل نيمدختسملا عاشناب مق 5 ةوطخل

دنتسملا اذه نم [RADIUS ISE نيوكت](#) مسقلا نم 4. ةوطخلال في ضرورعم هسفن وه اذه

زاهجال لوؤسم جهن ةعومجم عاشن. 6 ةوطخل

ةيموسرللا مدختسملا ةهجالو نم

ضريو فتلاو ةقداصملا تاسايس فيرعت يرورضلا نم لظي، نيمدختسملا عاشن درجمب، RADIUS لىل لوصولل ةبسنلاب ةياغلل هذهل زاهجال لوؤسم جهن تاعومجم TACACS ةقداصم مدختست. ةبسانملا لوصولل قوقح مهحنم ISE لىل مهب ةصاخلا حضوم وه امك GUI Page Device Admin Policy Sets Device Administration > Work Centers > Device Administration

Policy Sets

Reset

Reset Policyset Hitcounts

Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
	WLC TACACS Authentication		Network Access-Device IP Address EQUALS 10.48.39.133	Default Device Admin	0		
	Default	Tacacs Default policy set		Default Device Admin	0		

Reset

Save

إلى اذنه يدوي، عقب أسل الروصل في رمح أال نوللاب رطوم الأ "فأاضا" رزلا مدختسأ، ةزه أال ةرادال تاسايس ةومجم ءاشنال
هتحت اهقبطت بجي طرشو، ائيدح اهؤاشن مت يتللا ةومجم لل مسا ريفوتب مق. جهنللا تاعومجم ةمئاق إلى رصنع ةفأاضا
ةومجم ةفأاضا ءاهنال Save رزلا مدختسأ. (يفكي ام Default Device Admin، انه) هب حومسملل مداخل لس لس ت/تالوكوتوربل او
ةحفصل إلى رعظي امك، هب ةصاخلا نيوكتللا ةحفص إلى لوصولل هنيمي إلى رعومللا مهسللا سار مادختس او جهنللا
ةضورعمللا.

Policy Sets → **WLC TACACS Authentication**

Reset

Reset Policyset Hitcounts

Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	WLC TACACS Authentication		Network Access-Device IP Address EQUALS 10.48.39.133	Default Device Admin	0

Authentication Policy (1)

Status	Rule Name	Conditions	Use	Hits	Actions
✓	Default		All_User_ID_Stores	0	

Authorization Policy - Local Exceptions

Authorization Policy - Global Exceptions

Authorization Policy (3)

Status	Rule Name	Conditions	Results			Hits	Actions
			Command Sets	Shell Profiles			
✓	Helpdesk users authorization	InternalUser-IdentityGroup EQUALS User Identity Groups:helpdesk-group	AllowAllCommands	IOS Helpdesk	0		
✓	Admin users authorization	InternalUser-IdentityGroup EQUALS User Identity Groups:admin-group	AllowAllCommands	IOS Admin	0		
✓	Default		DenyAllCommands	Deny All Shell Profile	0		

Reset

Save

لا تملك أي واسي IP ناو نعب تاب لطل اية ف ص ت ب ل ا ت م ل ا ذ ه ف ي " WLC TACACS " ة ق د اص م " ة د د ح م ل ج ه ن ل ل ة و م ج م م و ق ت C9800 WLC ن ا و ن ع IP.

ض ي و ف ت ي ت د ع ا ق د ا د ع ا م ت . م ا د خ ت س ا ل ا ت ا ج ا ي ت ح ا ب ف ي ف ت ا ه ن ا ل ا ي ض ا ر ت ف ا ل ا ة د ع ا ق ا ل ك ر ت م ت ، ة ق د ا ص م ج ه ن ك :

- ر م ا و ا ل ع ي م ج ب ح م س ي و ه . ة ف ر ع م ل ا d e m o n s t r a t i o n - g r o u p ة و م ج م ل ا ل ا م د خ ت س م ل ا ي م ت ن ي ا م د ن ع ل و ا ل ر ا ي خ ل ل ا ل ي غ ش ت م ت ي (د د ح م ل TACACS_IOS_Admin ف ي ر ع ت ف ل م ر ب ع) 15 ز ا ي ت م ا ل ا ن ي ع ي و (P e r m i t _ a l l ة ي ض ا ر ت ف ا ل ا ة د ع ا ق ا ل ر ب ع) .
- ر م ا ل ك ح م س ي و ه . ة ف ر ع م ل a d m i n - g r o u p ة و م ج م ل ا ل ا م د خ ت س م ل ا ي م ت ن ي ا م د ن ع ي ن ا ث ل ر ا ي خ ل ل ا ل ي غ ش ت م ت ي (د د ح م ل TACACS_IOS_Helpdesk ف ي ر ع ت ف ل م ل ا ل خ ن م) 1 ز ا ي ت م ا ن ي ع ي و (ة ي ض ا ر ت ف ا ل ا ة د ع ا ق ا ل P e r m i t _ a l l ل ا ل خ) .

ف ي ة ق د ا ص م ل ل h e l p d e s k ن ي م د خ ت س م ل a d m i n u s e r ل ا ه ن ي و ك ت م ت ي ت ا د ا م ت ع ا ل ا ت ا ن ا ي ب م ا د خ ت س ا ل ن ك م ي ، ة و ط خ ل ه ذ ه ل ا م ت ك ا د ع ب

جما نرب مادختساب وأ (GUI) ةيموسرلا مدختسمل ةهجاو رب ع (WLC) ةيكلسالل ةيلحمل ةكبشلا يف مكحتلا رصنع Telnet/SSH.

اهالصالو اطاخال فاشكتسا

يف مكحتلا رصنع يل ع ةفاضلا كنكم يف ، ةمدخل عونل RADIUS ةمس لاسرا عقوتو ي كب صال RADIUS مداخ ناك اذا (WLC) ةيكلسالل ةيلحمل ةكبشلا :

```
radius-server attribute 6 on-for-login-auth
```

أ (WLC) ةيكلسالل ةيلحمل ةكبشلا يف مكحتلا ةدحوب ةصال (GUI) ةيموسرلا مدختسمل ةهجاو اطاخال فاشكتسا ةيكلسالل ةيلحمل ةكبشلا يف مكحتلا ةدحوب صال RADIUS/TACACS+ لوكوتورب رب ع (CLI) رماوالا رطس ةهجاو لوصو (WLC)

ةيفرطلا ةطحمل ةشاشا ل ةفاضلا اب ، رمالا رادصاب مق ، اهالصالو (WLC) ةيكلسالل ةيلحمل ةكبشلا يف مكحتلا ةدحوب ل وخذلا ليجست ةلواحم ارج دن ع رشابم ل اارخالا ةدهاشم و لوالا

جارخالا اذ ءاشناب مدختسمل adminuser نم جورخال ليجست ه عبت ي ذللا حجانل ل وخذلا ليجست موق ي ، لالم ل لابس يل ع

```
<#root>
```

```
WLC-9800#
```

```
terminal monitor
```

```
WLC-9800#
```

```
debug tacacs
```

```
TACACS access control debugging is on
```

```
WLC-9800#
```

```
Dec 8 11:38:34.684: TPLUS: Queuing AAA Authentication request 15465 for processing
```

```
Dec 8 11:38:34.684: TPLUS(00003C69) login timer started 1020 sec timeout Dec 8 11:38:34.684: TPLUS: pro
```

وهو (AV priv-lvl=15) حيث حصلنا زيارته من الالاجس الالهه نم عجره TACACS+ مداخلنا أظلالنا نمكم يو.

RADIUS رورم ةكل عتي يذالو، لثامم حيث صت جارخا ره ظي، RADIUS ةقداصمب موقت ام دنع.

مكحتال رصنع ةطساوب اهراي تخا م تي ي تال قرطال ةمئاق ضرع debug aaa authorization، كذا نم الءب و debug aaa authentication رمألأ لءولءل ليجست مءختسالم ةلءاحم دنع (WLC) ةيكلسال الءي لءالم ةكبشال ي ف.

وأ (WLC) ةيكلسال الءي لءالم ةكبشال ي ف مكحتال ةءوب ةصاخال (GUI) ةيموسرل مءختسالم ةءءاو ءاطءا فاشكسأ اءالصال ISE راي عم عم ةقفاوتمال (GUI) ةيموسرل مءختسالم ةءءاو ربع (TACACS+) رماوأل رطس ةءءاو لءل لوصول.

ءعاس 24 رخآ ىءء TACACS+ عم مءء مءختسم ةقداصم لك ضرع نمكم ي، Operations > TACACS > Live Logs ءءصال نم ءءءال اءءب لءل ءصافال رء مءختسأ، TACACS+ ةقداصم وأ ضيوفت لءل صافء عي سول.

The screenshot shows the Cisco ISE interface. At the top, there is a navigation bar with "Cisco ISE" on the left, "Operations · TACACS" in the center, and "Evaluation Mode 82 Days" on the right. Below this is a "Live Logs" tab. The main area displays a table of logs with columns for Logged Time, Status, Details, Identity, Type, Authentication Policy, Authorization Policy, Ise Node, and N. The table contains six entries, all with a status of "Success" (green checkmark) and a type of "Authorization". The first entry is for "helpdeskuser" at "Dec 08, 2022 06:51:46.1...". The second entry is for "helpdeskuser" at "Dec 08, 2022 06:51:46.0...". The third entry is for "adminuser" at "Dec 08, 2022 06:38:38.2...". The fourth entry is for "adminuser" at "Dec 08, 2022 06:38:38.1...". The fifth entry is for "adminuser" at "Dec 08, 2022 06:34:54.0...". The sixth entry is for "adminuser" at "Dec 08, 2022 06:34:53.9...". The table is updated as of "Thu Dec 08 2022 12:57:09 GMT+0100 (Central European Standard Time)".

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Ise Node	N
Dec 08, 2022 06:51:46.1...	Success	lock	helpdeskuser	Authorization	WLC TACACS Authentication >...	WLC TACACS Authentication >...	ise	W
Dec 08, 2022 06:51:46.0...	Success	lock	helpdeskuser	Authentication	WLC TACACS Authentication >...	WLC TACACS Authentication >...	ise	W
Dec 08, 2022 06:38:38.2...	Success	lock	adminuser	Authorization	WLC TACACS Authentication >...	WLC TACACS Authentication >...	ise	W
Dec 08, 2022 06:38:38.1...	Success	lock	adminuser	Authentication	WLC TACACS Authentication >...	WLC TACACS Authentication >...	ise	W
Dec 08, 2022 06:34:54.0...	Success	lock	adminuser	Authorization	WLC TACACS Authentication >...	WLC TACACS Authentication >...	ise	W
Dec 08, 2022 06:34:53.9...	Success	lock	adminuser	Authentication	WLC TACACS Authentication >...	WLC TACACS Authentication >...	ise	W

ي لءل امك ةقيرطال هءل ءءءان ةقداصم ةلءاحم helpdeskuser وءبء، عي سولال دنع:

Overview

Request Type	Authentication
Status	Pass
Session Key	ise/459637517/243
Message Text	Passed-Authentication: Authentication succeeded
Username	helpdeskuser
Authentication Policy	WLC TACACS Authentication >> Default
Selected Authorization Profile	IOS Helpdesk

Authentication Details

Generated Time	2022-12-08 06:51:46.077000 -05:00
Logged Time	2022-12-08 06:51:46.077
Epoch Time (sec)	1670500306
ISE Node	ise
Message Text	Passed-Authentication: Authentication succeeded
Failure Reason	
Resolution	
Root Cause	
Username	helpdeskuser
Network Device Name	WLC-9800
Network Device IP	10.48.39.133
Network Device Groups	IPSEC#Is IPSEC Device#No,Location#All Locations,Device Type#All Device Types
Device Type	Device Type#All Device Types
Location	Location#All Locations
Device Port	tty5
Remote Address	10.61.80.151

Steps

13013 Received TACACS+ Authentication START Request
15049 Evaluating Policy Group
15008 Evaluating Service Selection Policy
15048 Queried PIP - Network Access.Device IP Address
15041 Evaluating Identity Policy
22072 Selected identity source sequence - All_User_ID_Stores
15013 Selected Identity Source - Internal Users
24210 Looking up User in Internal Users IDStore
24212 Found User in Internal Users IDStore
13045 TACACS+ will use the password prompt from global TACACS+ configuration
13015 Returned TACACS+ Authentication Reply
13014 Received TACACS+ Authentication CONTINUE Request (Step latency=3149ms)
15041 Evaluating Identity Policy
22072 Selected identity source sequence - All_User_ID_Stores
15013 Selected Identity Source - Internal Users
24210 Looking up User in Internal Users IDStore
24212 Found User in Internal Users IDStore
22037 Authentication Passed
15036 Evaluating Authorization Policy
15048 Queried PIP - Network Access.UserName
15048 Queried PIP - InternalUser.IdentityGroup
13015 Returned TACACS+ Authentication Reply

WLC هذه دعوة اسم مة كة بشل ال WLC-9800 زاهج لىل حاجن بن helpdeskuser ممدختم اسم الة قداصم تم ت هنا ىرت نأ كنكمي ، اذه نمو ممدختم اسم ال اذهل لىل وختل لىل فى رعت فلم IOS Helpdesk نىل عىل عوالع . قداصم ال TACACS Authentication > Default .
1. زايتم الال ىوتسم هحنم متو

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