

ههجاوول TACACS+؛ AMP؛ RADIUS ةئيهت ةقداصم AMP؛ و (GUI) ةيموسرلا مدختسملا 9800 WLCs ىلع CLI

تايوتحمل

[ةمدقملا](#)

[ةيساسألا تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[ةيساسأ تامولعم](#)

[نئيوكتلا](#)

[طقف ةعارقلل مدختسملا دويق](#)

[WLC ل RADIUS ةقداصم نئيوكت](#)

[RADIUS ل ISE نئيوكت](#)

[TACACS+ WLC نئيوكت](#)

[TACACS+ ISE نئيوكت](#)

[اهجالصاو عااخالأ افاشكتسلا](#)

[ةهجاو لوصو وأ \(WLC\) تاموسرلا مدختسم ةهجاو ب ةصاخلا \(GUI\) تاهجاو ل عااخالأ افاشكتسأ
ةصاخلا \(CLI\) رماوألأ رطس ةهجاو ل لالخ نم TACACS+/RADIUS لوكوتورب رب ع \(CLI\) رماوألأ رطس
\(WLC\) تاموسرلا مدختسم ةهجاو ب](#)

[مدختسملا ةهجاو رب ع TACACS+ لوصو وأ \(GUI\) ةيموسرلا تاهجاو ل عااخالأ افاشكتسأ
اهجالصاو ISE راي عم عم ةقفافوتملا \(GUI\) ةيموسرلا](#)

ةمدقملا

ةيجراخ ةيوه ةحص TACACS+ وأ RADIUS ل 9800 ةزافح ةدام لكشي نأ فيك ةقيثو اذه فص ي.

ةيساسألا تابلطتملا

تابلطتملا

ةيلاتلا عيضاوملاب ةفرعم كي دل نوكت نأب Cisco ي صوت:

- Catalyst Wireless 9800 نئيوكت جذومن
- TACACS+ و RADIUS و (AAA) ةبساحملاو ضيوفتلاو ةقداصملا ميهافم

ةمدختسملا تانوكملا

ةيلاتلا ةيداملا تانوكملاو جماربلا تارادصا ىلا دنتسملا اذه في ةدراولا تامولعمل دنتست

- C9800-CL رادصلإا 17.9.2
- ISE 3.2.0

ةصاخ ةي لمعم ةئي ب ي ف ةدوجومل ةزهجال نم دنتسمل اذه ي ف ةدراول تامولعمل عاشنإ مت تناك اذا .(يضا رتفا) حوسمم نيوكتب دنتسمل اذه ي ف ةمدختسمل ةزهجال عيمج تأدب رما يأل لمحتمل ريثأتلل كمهف نم دكأتف ،ليغشتلا دي قكتكبش

ةيساسأ تامولعم

username لخدي 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 ،يضا رتفا لكشبو .ةملكو ي ف مكحتل رصنع هي جوت نكمي ،كلذ نم الدب .هسفن زاهجلا ىلع ةدوجومل ،نيمدختسملل :ديعب AAA مداخلباقم لاخلال دامتعا تانايب ةنراقمل (WLC) ةيكلساللا ةيلحمل ةكبشلل ةقداصلم اتقيرط امه ناذه .TACACS+ وأ RADIUS مادختساب مداخللا ىل WLC ثدحتت نأ نكمي (لاثلل ليبس ىلع LDAP دجوي ال) لوؤسمل يمدختسمل ناتديحولل ناتيجراخل

نيوكتلا

adminuser، لاوتلا ىلع ،(ISE) AAA مداخل ىلع نيمدختسمل نم نيغون نيوكت مت ،لاثلل اذه ي .لاوتلا ىلع تاعومجمل helpdesk-group وتاعومجمل admin-group نم عزج نومدختسمل الؤه .helpdeskuser، مكحتل رصنع ىللا لملكلا لوصول قح ،admin-group نم عزج وه ،مدختسمل حنم عقوتمل adminuser نم ينعي ،helpdesk-group نم عزج ،helpdeskuser، ىرخأ ةيخان نم .(WLC) ةيكلساللا ةيلحمل ةكبشلل ي ف نيوكتلا ىللا لوصول دجوي ال ،يلا تلابو .WLC ىللا ةبقارمل تازاي تما حنم طقف متي نأ

(WLC) ةيكلساللا ةيلحمل ةكبشلل ي ف مكحتل رصنع نيوكتب الؤا ةلاقمل هذه موقت TACACS+ ل اقحال هسفن رمالا ذيفنتب موقت مث ،RADIUS ةقداصلم ISE رايعمو

طقف ةعارقلل ممدختسمل دويق

:ةدوجوم دويقل هذه نوكت ،WebUI 9800 ةقداصلم RADIUS وأ TACACS+ مادختسا دنع

- لوصول قح مهيدل سيل نكلو 0 زايتمالا ىوتسم مهيدل نيذل نومدختسمل دجاوتي ةيموسرل ممدختسمل ةهجاو ىللا
- بيبوتللا ةمالع ضرع طقف 14 ىل 1 نم تازاي تما مهيدل نيذل نيمدختسمل نكمي (طقف ةعارقلل ايلحم هتقداصم متت ممدختسمل زايتمالا ىوتسم لداعي اذهو) "ةشاش
- لملكلا لوصول قح مهيدل 15 زايتمالا ىوتسم مهيدل نيذل نومدختسمل
- حيتت يتلل رمالا ةعومجمو 15 زايتمالا ىوتسم مهيدل نيذل نيمدختسمل معد متي ال لالخنم نيوكتلا تاريغيغت ذيفنت ممدختسمل ناكمإ لازي ال .طقف ةنيغم رمالا WebUI

.اهل يدعت وأ تارابتعالا هذه ريغيغت نكمي ال

WLC ل RADIUS ةقداصلم نيوكت

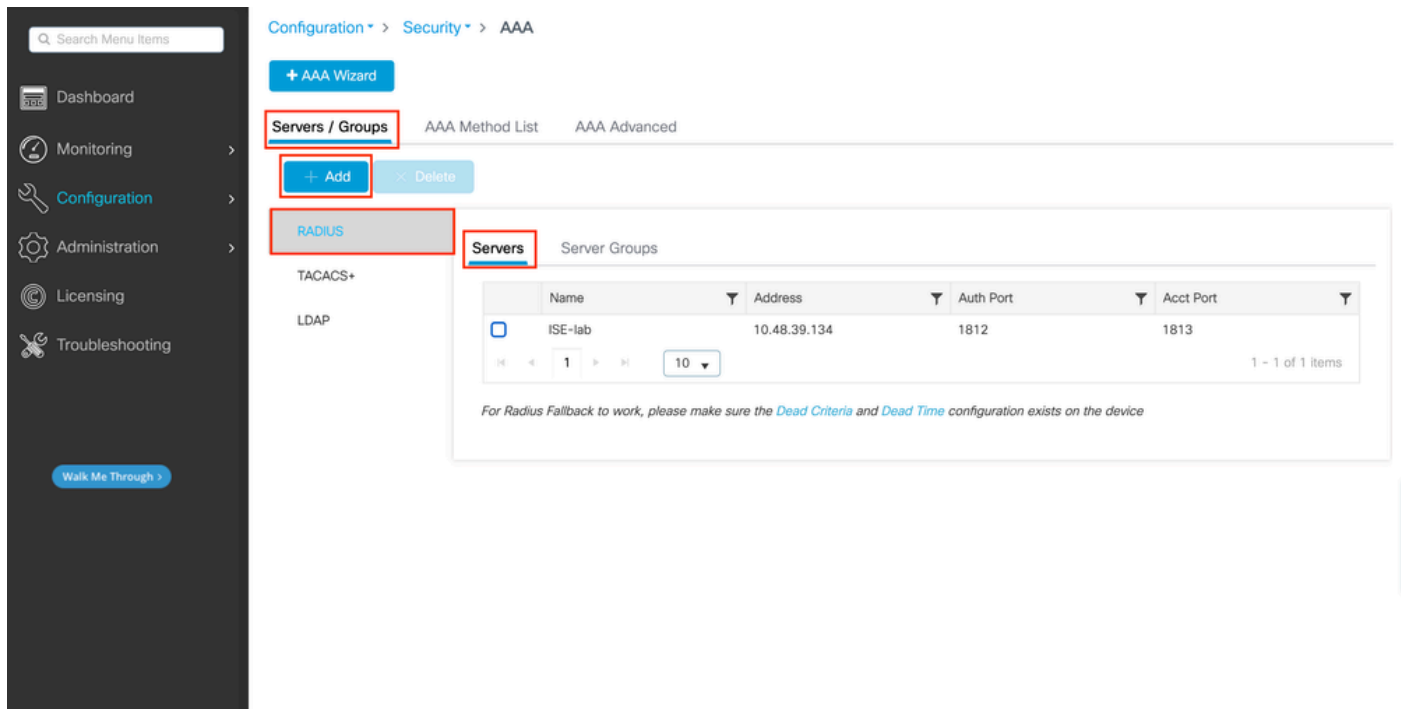
RADIUS. مداخل نالعا 1. ةوطخلا

ةيموسرلا مدختس مل اة جاو نم

هذه هي الطريقة التي يتم بها إعداد خادم الـ ISE RADIUS لمعالجة طلبات الـ WLC (WLAN Controller) من أجل التحقق من هوية المستخدمين وإدارة الوصول إلى الشبكة. يتم إعداد الخادم ليخدم مجموعة من الخوادم (Servers/Groups) والتي تكون عادةً خوادم الـ WLC. يتم إعداد الخادم ليخدم مجموعة من الخوادم (Servers/Groups) والتي تكون عادةً خوادم الـ WLC. يتم إعداد الخادم ليخدم مجموعة من الخوادم (Servers/Groups) والتي تكون عادةً خوادم الـ WLC.

```
/webui/#/aaa
```

• **الوصول** هذه في حضوره امك ، Configuration > Security > AAA، **تصلت** اذا و ،



رزرقنا، (WLC) ةيكلسالل ةيلحمل ةكبشلل يف مكحتل رصنع ىلع RADIUS مداخ ةفاضل
يف ةضورعمل ةقثبنمل ةذفانل حتف ىل اذه يدؤي. ةروصلل يف رمحلأاب رطؤمل ةفاضل
ةشاشل ةطقل.

ري فو ت ك ي ل ع ب ج ي ، ة ق ث ب ن م ل ا ذ ف ا ن ل ا ه ذ ه ي :

- ISE م ا ط ن م س ا ق ب ا ط ي ن ا ب ج ي ا ل ه ن ا ط ح ا ل م د ا خ ل م س ا
- م د ا خ ل ل IP ن ا و ن ع
- RADIUS م د ا خ و WLC ل ا ن ي ب ك ر ت ش م ل ر س ل ا

ه ذ ه ن ك ل و ، ة ب س ا ح م ل ا و ة ق د ا ص م ل ل ة م د خ ت س م ل ا ذ ف ا ن م ل ا ل ث م ، ي ر خ ا ت ا م ل ع م ن ي و ك ت ن ك م ي د ن ت س م ل ا ذ ه ل ي ض ا ر ت ف ا د ا د ع ا ك ك ر ت ت و ة ي م ا ز ل ا ت س ي ل

ر م ا و ا ل ر ط س ة ه ج ا و ن م :

<#root>

WLC-9800(config)#radius server

ISE-lab

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

10.48.39.134

auth-port 1812 acct-port 1813

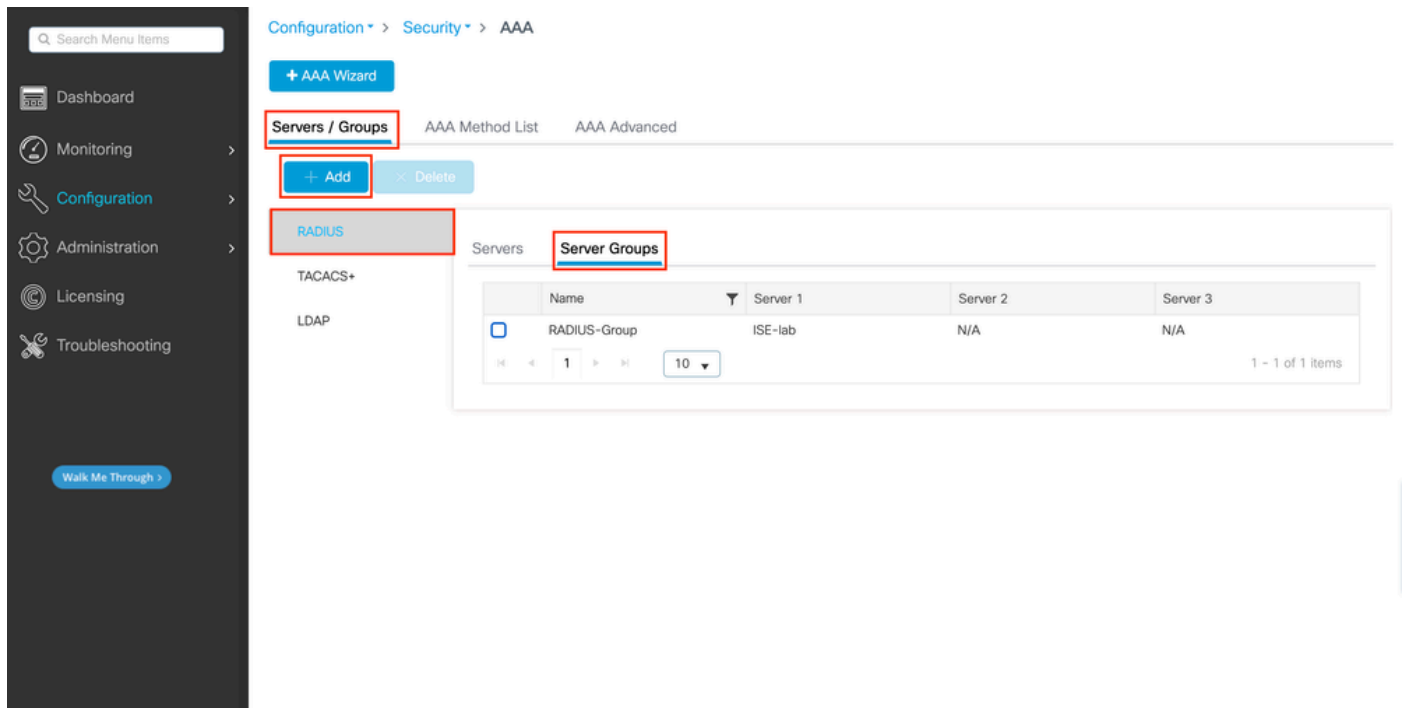
WLC-9800(config-radius-server)#key

Cisco123

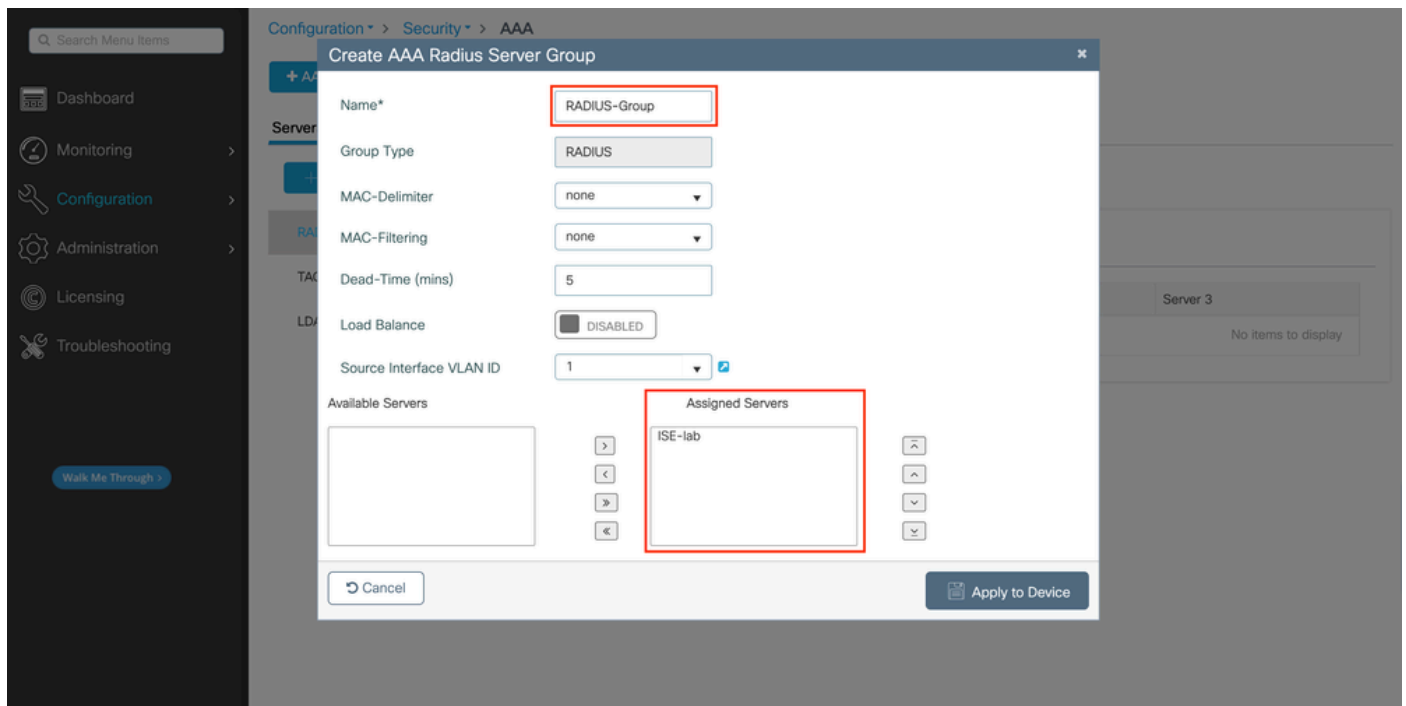
م د ا و خ ة و م ح م ي ل ا RADIUS م د ا خ ن ي ي ع ت ب م ق 2. ة و ط خ ل ا

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

هذه عي مج ني عتب ي صوي ،ةق داصم لل اهم ادختسإ نكمي ةددعتم RADIUS مداوخ دوجو ةلاحي في
 ةيكلسالل ةيلحملا ةكبشلا في مكحتلا ةدحو متت .اهسفن مداوخلا ةعومجم يلا مداوخلا
 مداوخلا ةعومجم في مداوخلا ني ب ةفلتخملا ةق داصملا تايلمع ني ب لامحالآ عيزوتب (WLC)
 سفن نم بيوبتلا ةمالع Servers/Groups > RADIUS > Server Groups مداوخ تا عومجم ني وكت متي
 ةروصللا في حضوم وه امك ، 1. ةوطخللا في ةروكذملا (GUI) ةي موسرلا مدختسمللا ةهجاو ةحفص



في رابطال) ةفاضل رزلا قوف رقلال دنع ةقثب نم ةذفان رهظت ،مداخال ءاشنإل ةبسنلاب
 انه هفيفصت متي يذلاو ،(ةقباسلا ةروصللا



إلا ةبولطملا مداوخلا لقنب مق م ،ةعومجم لل مسا ريفوتب مق ،ةقثب نملا ةمئاقلا في
 ةني عمل مداوخلا ةمئاق

ریم اوآل رطس ةهچ او نم

<#root>

WLC-9800(config)# aaa group server radius

RADIUS-Group

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

ISE- lab

RADIUS م داوخ ةومجم ىلإ رىشت AAA ةقداصم لوخد لىجست ةقيرط عاشنإب مق 3. ةوطخل

ةيموسرللا مدختسملا ةهچ او نم

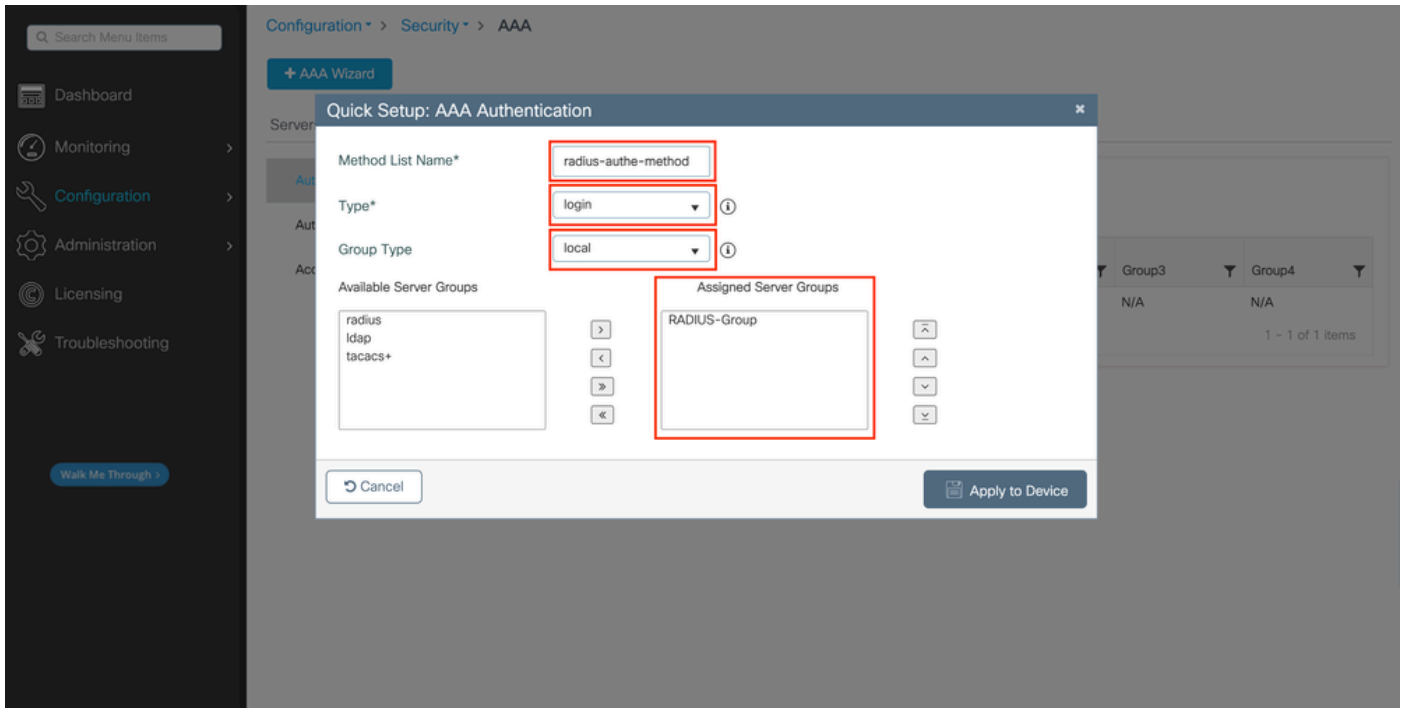
https:// ةحفص نم دعب

/webui/#/aaa

ئشنأو Authentication > AAA Method List بىوبتللا ةمالع ىلإ لقتنا ،ةيموسرللا مدختسملا ةهچ او ةروصللا هذه يف حضوم وه امك ةقداصم ةقيرط

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

ةقثبنم ةذفان رهظت ،ةقداصم ةقيرط عاشنإل ةفاضل رز مدختست ام دنع ،داتعم وه امك ةروصللا هذه يف ةحضوملا ةذفانلل ةلثامم ،نىوكتلل



ةفاضاب مقو، لوخذ لجسكTypeرتخأ. بولسألل مساري فوتب مق، ةقثبنملا ةذفانللا هذه يف اميف. ةمئاقلا Assigned Server Groups إلى ةقباسلا ةوطخل يف هؤاشنإ مت يذلا ةعومجملا مداخل تانيوكتلا نم ديدعلا عارجإ نكمي، ةعومجملا عون لقحب قلع تي.

- ةلحمللا ةكبشللا يف مكحتلا رصنع ققحتي، ايلحم "ةعومجملا عون" ترتخأ اذا ةرم دوعي مت، ايلحم ةدوجوم مدختسملا دامتعا تانايب تناك اذا امم الوأ (WLC) ةيكللساللا مداخللا ةعومجم إلى ىرخأ.
- نإف، ايلحم إلى عوجر رايلخللا نم ققحتلاب مقت ملو ةعومجمك ةعومجملا عون ترتخأ اذا تاغوسم نم طقف ققحتي (WLC) ةيكللساللا ةلحمللا ةكبشللا يف مكحتلا رصنع مداخللا ةعومجم لباقم مدختسملا.
- رصنع ققحتي، "ايلحم إلى يطايتحا" رايلخللا تصحفو ةعومجمك "ةعومجملا عون" ترتخأ اذا لباقم مدختسملا دامتعا تانايب نم (WLC) ةيكللساللا ةلحمللا ةكبشللا يف مكحتلا اذا. مداخللا بحتسي مل اذا طقف ةلحمللا تانايبلا ةدعاق نع ملعتسيو مداخللا ةعومجم نوكي نأ نكمي ناك ناو ىتح، مدختسملا ةقداصم متتس، ضفر لاسراب مداخللا ماق ةلحمللا تانايبلا ةدعاق ىلع ادوجوم.

رم اوألا رطس ةهجاو نم:

روثعللا متي مل اذا طقف مداخللا ةعومجم عم مدختسملا دامتعا تانايب نم ققحتلا ديرت تنك اذا مدختسأ، الوأ ايلحم اهيلع:

<#root>

WLC-9800(config)#aaa authentication login

radius-auth-method

local group

RADIUS-Group

مدخستساً، طقف مداوأة ومجم عم مدختسملا دامتعا تانايب نم ققحتلا ديرت تنك اذا

<#root>

WLC-9800(config)#aaa authentication login

radius-authe-method

group

RADIUS-Group

ريأالا اذه بختسي مل اذاو مداوأة ومجم عم مدختسملا دامتعا تانايب نم ققحتلا ديرت تنك اذا
مدختساف، يلملا لاأالا عم

<#root>

WLC-9800(config)#aaa authentication login

radius-authe-method

group

RADIUS-Group

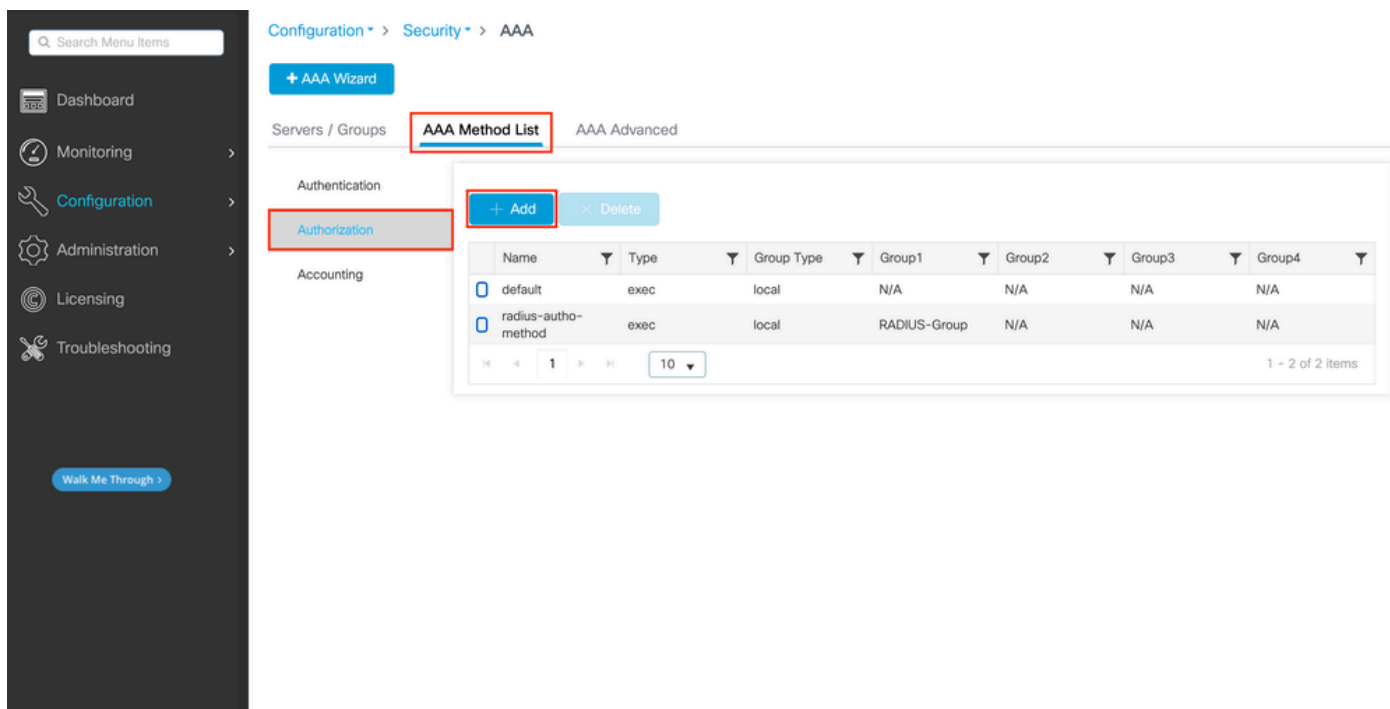
local

ضعبو، طقف ايلحم مهأاشنإ مت نذل نيمدختسملا ضعب كانه، لاثملا اذه ي
لأالا راأالا نومدختسي، يلاتلابو، ISE مداوأة طقف نيمدختسملا

RADIUS مداوأة ومجم إلى ريشت AAA ضيوفت EXEC قيرط عاشنإب مق 4. عوطأالا

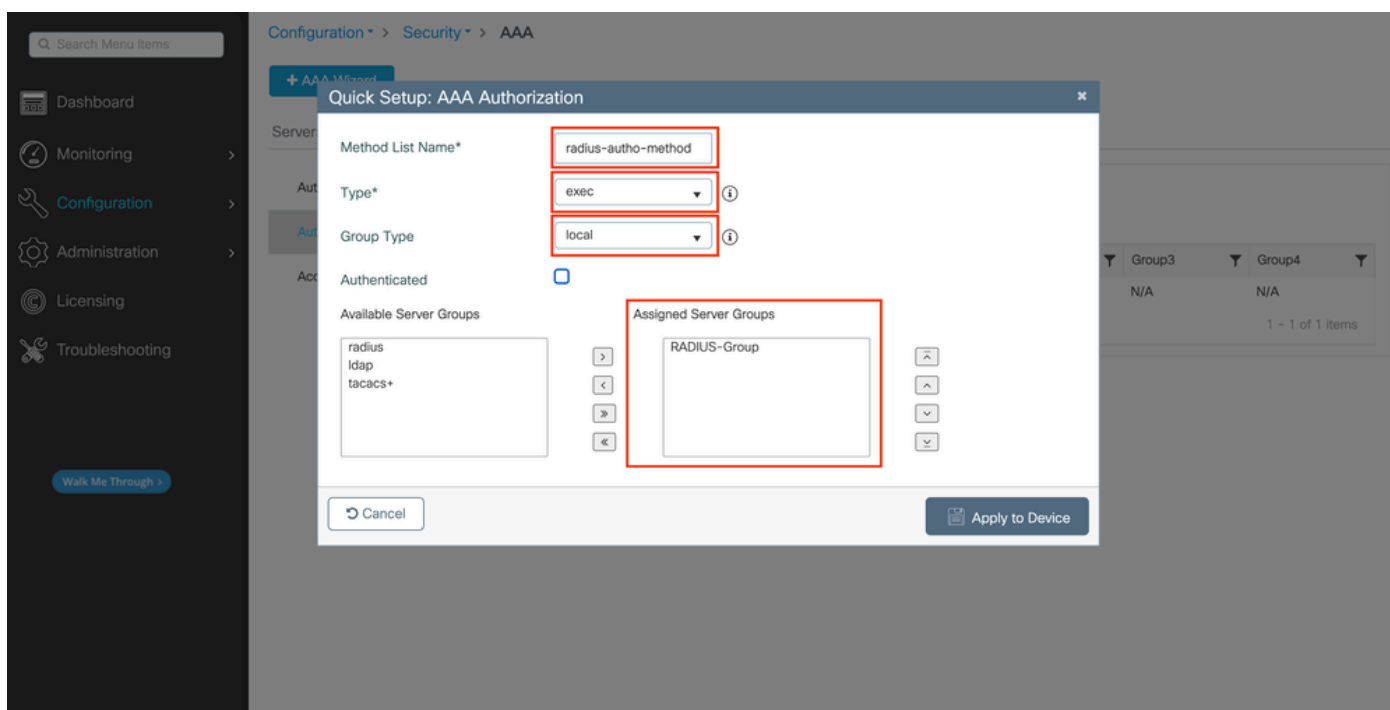
نيموسرلا مدختسملا عأاونم

GUI Page Configuration > Security > نمدعب. لوصولأ قح حنم متي ىتح مدختسملا ليوخت اضيأ بجي
وه امك دامتعا قيرط عاشنإب مقو، بيوأالا عمالء Authorization > AAA Method List إلى لقتنا، AAA
ةروصلأ هذه يفضوم.



ليوختال بولسأ عاشنا

بولسأ ةفاضل دنع هريوشت مت يذال بولسألل لثامم قثبنم ليوخت بولسأ نيوكت رهظي ةفاضل رزل مادختساب ديدج.



exec، مساب عونل رتخاو، ليوختال ةقيرطل مسا ريفوتب مق، قثبنم نيوكتال اذه في 3. ةوطخلال في ةقداصلمال ةقيرطل مدختسمالك ةعومجمل عونل بيترتل سفن مدختساو.

نم اوأال رطس ةهچاونم

ني مدختسمال نم ققحتلل الو ليوختال نييعت متيف، ةقداصلمال ةقيرطل ةبسنلاب امأ مداو ةعومجم في تالاخلال لباقم م، ةقيرطل تالاخلال لباقم.

RADIUS-Group

ةروصلا هذه يف حضوم وه امك ،

Configuration > Security > AAA

+ AAA Wizard

Servers / Groups AAA Method List **AAA Advanced**

Global Config

RADIUS Falback

Attribute List Name

Device Authentication

AP Policy

Password Policy

Walk Me Through >

AAA Interface

	Authentication	Authorization	Accounting
Console	None	None	None
VTY	radius-authen-method	radius-autho-method	None
HTTP	radius-authen-method	radius-autho-method	None

<#root>

```
WLC-9800(config)#ip http authentication aaa login-authentication  
radius-auth-method
```

```
WLC-9800(config)#ip http authentication aaa exec-authorization  
radius-auth-method
```

CLI ةقداصل مل Telnet/SSH:

<#root>

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

```
WLC-9800(config-line)#authorization exec  
radius-auth-method
```

HTTP تامدخ لي غشت ةداعإ لضفأل نمف ، HTTP تانيوكت ىلع تاريغيغتلا عارجا دنع هنا طحال ةيلاتل رماوالا مادختساب كلذ قيقتحت نكمي . HTTPS و

```
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
```

ISE ل RADIUS نيوكت

زاهك (WLC) ةيكلساللا ةيلحمل ةكبشلا في مكحتلا رصنع نيوكتب مق 1. ةوطخل RADIUS ل ةكبش

ةيموسرلا مدختسمل ةهجاو نم

مسقلا في (WLC) ةيكلساللا ةيلحمل ةكبشلا في مكحتلا رصنع مادختسا حيضوتل Administration > Network Ressources > Network ةيكلساللا ل RADIUS في ISE، ةكبش زاهك قباسلا ةيلاتلا ةروصل في حضوم وه امك ، اهتفاو ةكبشلا ةزهجا بيوتلا ةمالع Devices

 Administration • Network Resources Evaluation Mode 82 Days

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences More ▾

Network Devices

Default Device
Device Security Settings

Network Devices

Selected 0 Total 1  

 Edit  **Add**  Duplicate  Import  Export ▾  Generate PAC  Delete ▾ All ▾ 

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

ديدجال ةكبشلا زاهج نيوكت جذومن حت في يذلا ةفاضلا رزلا مدختسأ ، ةكبش زاهج ةفاضلا

Cisco ISE Administration • Network Resources Evaluation Mode 82 Days

Network Devices | Network Device Groups | Network Device Profiles | External RADIUS Servers | RADIUS Server Sequences | More

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**

لا ترتخأ. هب صاخ ال IP ناو نع ةفاضإو، ةكبشلا زاهل مسا ريفوتب مق، ديدجل راطإلا في لمعتسي دحاولا نأ امب رس كرتشم RADIUS هسفن لا ت لكشو دادعإ ةيلمع ةقداصم RADIUS ال WLC.

زايتمال اعجارال، ضيوفت ةجيتن عاشنإب مق 2. ةوطخل

نؤموسرل مدختسملا ةهجاو نم:

يذلاو 15، زايتمال يوتسم نوكي نأ adminuserمزل ي، لوؤسملل لوصول قوقح ىل لوصول EXEC جاتحي helpdeskuserال، رخأ ةيجان نم. exec. ةبلاطم ةقبط ىل لوصولاب حمسي يوتسم نييغت ل 15 نم لقأ زايتمال يوتسمب هنييغت نكمي يلاتلابو Shell ىل ليرسلا نيوك نكمي. ليوختلا فيرعت تافلم مادختسا نكمي، ني مدختسملل بسانملا زايتمالا Authorization > Authorization بويوبتلا ةمالع لفسأ، ISE GUI Page Policy > Policy Elements > Results، نم رصانعلا هذه

Profilas. ەروصلال ي ف ەحضومل

Policy · Policy Elements

⚠️ Evaluation Mode 82 Days

🔍 ? 🗨️ ⚙️

Dictionary

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

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

فلم نيوكٽ جڏوم ن حت في يذلة فاضا رزلا مدخت ساً ،ديج ليوخت فيرعت فلم نيوكٽ ل
فيرعتا فلم نيوكٽ ل صوصخا ل هجو ىلع جڏوم نلا اذه ودبي نأ بجي .ديجال ليوختا ل فيرعت
adminuser.هه نىى عت متى يذلا

Policy · Policy Elements

Authentication 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

وه اذه ،لبق نم ركذامكو .ه ب طبرت رم مدختسم يأل 15 حنم زايتما يوتسم نيوكتل ضرع
عمو .ةليلال ةوطخل اناثا هؤاشنإ متي يذلاو لبق نم adminuser عقوقوتمل كولسل
ةسايس رصنع عاشنإ بجي يلاتلابو ،لقأ تازايتمال يوتسم نوكي نأ بجي helpdeskuser ،كلذل
ناث.

shell:priv-lvl=15 ةلسلسل نأ ادعام ،طقف هالعأ قلخ دحاو لىل لثامم ل helpdeskuser ةسايس رصنع
متي ،لثامل اذه ي ف .يوتسم زايتمال عم X تلدبتساو ،shell:priv-lvl=X لىل ريغت نأ يغبني shell:priv-lvl=15
1. مقر مادختسا

ISE. لىل ني مدختسم تاعومجم عاشنإ 3. ةوطخل

ةي موسرلا مدختسملا ةهجاو نم

مدختسملا ةي وه تاعومجم بيوبتل ةمالع نم ISE ي مدختسم تاعومجم عاشنإ متي
ةشاشال طاقتال ي رهظي يذلاو ،ةشاشال Administration > Identity Management > Groups GUI Page في

Cisco ISE Administration · Identity Management Evaluation Mode 82 Days

Identities **Groups** External Identity Sources Identity Source Sequences Settings

Identity Groups

EQ

< [Icon] [Settings]

> Endpoint Identity Groups

> **User Identity Groups**

User Identity Groups

Selected 0 Total 10 [Refresh] [Settings]

[Edit] **+ Add** [Delete] [Import] [Export]

Name	Description
☐ helpdesk-group	This is the group containing all users with read-only privileges.
☐ admin-group	This is the group containing all users with administrator privileges.
☐ OWN_ACCOUNTS (default)	Default OWN_ACCOUNTS (default) User Group
☐ GuestType_Weekly (default)	Identity group mirroring the guest type
☐ GuestType_SocialLogin (default)	Identity group mirroring the guest type
☐ GuestType_Daily (default)	Identity group mirroring the guest type
☐ GuestType_Contractor (default)	Identity group mirroring the guest type
☐ GROUP_ACCOUNTS (default)	Default GROUP_ACCOUNTS (default) User Group
☐ Employee	Default Employee User Group
☐ ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group

هه وه عومجم نيوكت جذومن حت في يذلا ةفاضل رزل مدختسأ ،ديج مدختسم عاشنإل
حضوم وه امك ةديجلال مدختسملا

Cisco ISE Administration · Identity Management Evaluation Mode 82 Days

Identities **Groups** External Identity Sources Identity Source Sequences Settings

Identity Groups

EQ

< [Icon] [Settings]

> Endpoint Identity Groups

> User Identity Groups

User Identity Groups > New User Identity Group

Identity Group

* Name **admin-group**

Description This is the group containing all users with administrator privileges.

Submit Cancel

نيتللل ني مدختسملا يت عومجم عاشنإب مق .اهؤاشنإ مت يتللا ةعومجملا مساري فوتب مق
helpdesk-group و admin-group امه وه ،هالعا امهتشقانم تمت

ISE. ىلع ني مدختسم عاشنإ 4. ةوطخل

ةيموسرلا مدختسملا ةهجاونم

Administration > Identity Management > Identities GUI Page

Administration · Identity Management

Identities

Groups

External Identity Sources

Identity Source Sequences

Settings

Users

Latest Manual Network Scan Res...

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
☐	Enabled	adminuser				admin-group	
☐	Enabled	helpdesk...				helpdesk-group	

ىل لوصولا مدختسم نيوكت جذومن حتفل "ةفاضل" رزلا مدختسأ ،ديج مدختسم عاشنل
 حضوم وه امك ديجلال ةكبشلا.

Cisco ISE Administration · Identity Management Evaluation Mode 82 Days

Identities Groups External Identity Sources Identity Source Sequences Settings

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

نصائح لإصلاح رورم الة مكد و مكدتسم الم مسا يا ، نيمدختسم لل دامتعالا تانايب ريفوتب مق
 ةيكلسال الة لحد الم ةكبشال ي ف مكدتال رصنع لى لى قداصل لل نيمدختسم الم امهو ، اه/ب
 تاذ هتومجم لى لى مكدتسم الم فضا ، اريخا . Enabled مكدتسم الم ةلاح نا نم اضيا دكا ت . (WLC)
 ي ف نيمدختسم الم تاعومجم ةلدسنم الم ةمئاقال عم ، 4 ةوطخال ي افواشن مت ي تالوا ، ةلصل
 جذومنل ةياهن .

مق adminuser و helpdeskuser امهو ، هالعا امهتشقانم تمت نيل لل نيمدختسم الم عاشناب مق

نيمدختسم الم ةقداصل 5 ةوطخال

ةيموسرل مكدتسم الم ةهجاوم

ISE ل ةيضارتفالال جهنل تاعومجم ب ةصاخال ةقداصل الم ةسايس حمست ، ويرانيسال اذ ي ف
 ةطحال نمكي . ةكبشال لى لى يضارتفالال لوصولاب ، لى لى اباقبسم امنىوكت مت ي تالوا
 امك ، ISE ب ةصاخال (GUI) ةيموسرل مكدتسم الم ةهجاوم ةحفص Policy > Policy Sets نم هذ جهنل ةومجم
 هريغت لى لى ةجاح ال كلذل . ةروصل هذ ي ف حضوم وه

Cisco ISE Policy • Policy Sets Evaluation Mode 82 Days

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	⚙️

ن.ني مدختسم لايوخت 6. ةوطخل

ةيموسرلا مدختسملا ةهجاونم

ىلع بجيو اهليوخت بجي، ةقداصملا ةسايس ريرومتب لوخدلا ليحست ةلواحم موقت نأ دعب ىلا ةفاضلاب، لوبقبحامسلا) اقبس هؤاشنا مت يذلا لايوختلا فيرعت فلم عاجرا ISE (تازايمالا يوتسم).

وهو) زاهلل IP ناونع ىلا ادا نسا لوخدلا ليحست ةلواحم ةيفصت مت، لاثملا اذه ي يوتسم زيومتو (WLC) ةيكلساللا ةلحملا ةكبشلا ي ف مكحتلا ةدحوب صاخلا IP ناونع جهن كانه. مدختسملا اهلي يمتني يتلا ةومجملا ىلا ادا نسا هحنم متيس يذلا زايتمالا ثيح مهب ةصاخلا ني مدختسملا عامسأ ىلا ادا نسا ني مدختسملا ةيفصتلا خلاص رخآ لاثملا اذه ي ف طقف دحاو مدختسم ىلع ةومجم لك يوتحت.

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)

				Results				
+	Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions	
Search								
	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

اهنيوكت مت يتل دامتعالا تانايب مادختسا نكمي، ةوطخل هذه لامتك دعب
 ةيكلساللا ةيلحمل ةكبشللا يف مكحتللا رصنع يف ةقداصللل helpdesk مدختسم ال Jadminuser
 Telnet/SSH جم انرب لالخنم وأ (GUI) ةيموسرللا مدختسم ال ةهجاو ربع (WLC).

TACACS+ WLC نيوكت

TACACS+ دخال نال ع 1. ةوطخل

ةيموسرللا مدختسم ال ةهجاو نم:

ةمالع نم كلذب مايقل نكمي (WLC) ةيكلساللا ةيلحمل ةكبشللا يف مكحتللا رصنع ىل ع TACACS+ دخال ISE ءاشناب مق، الوأ
 مدختسم ال ةهجاو ب ةصاللا ةيكلساللا ةيلحمل ةكبشللا يف مكحتللا رصنع ءحفص نم Servers/Groups > TACACS+ > Servers بوبتل
 https:// ءي اهل لوصول نكمي يتل (GUI) ةيموسرللا

/webui/#/aaa

ةروصللا هذه يف حضروم وه امك، Configuration > Security > AAA ىل لالقتناب تمل اذ وأ

يؤدي هالعمل أروصلها يف رمحالاب رطوملأ ففاضل رزلأ قوف رقلأ (WLC) ةيكلساللأ ةيلحملأ ةكبشلأ يف مكحتلأ رصنع ىلع TACACS+ مداخل ففاضلأ ةموسرملأ ققثبنملأ ةذفانلأ حتف ىلأ اذه.

(ISE ماطن مسا قباطي نأ بجي ال) مداخل مسا ريفوتب مق ،ةقثبنملأ ةذفانلأ حتفت امدنع ةلهملأو ،مدختسملأ ذفنملأ ،كرتشملا حتافملأ ،هب صاخلا IP ناونع .

ريفوت كىلعل بجي ،ةقثبنملأ ةذفانلأ هذه يف:

- (ISE ماطن مسا قباطي نأ بجي ال هنأ طحال) مداخل مسا
- مداخلل IP ناونع
- TACACS+ مداخلو ةيكلساللأ ةيلحملأ ةكبشلأ يف مكحتلأ رصنع نيّب كرتشملا رسلأ

هذه نكلو، ةبساحمل او ةقداصل مل ةمدختس مل اذفان مل لثم ،ىرخأ تامل عم نيوكت نكمي
دنتس مل اذهل يضا رتفا دادعك كرتتو ةيمازل ا تسيل

رم اوأل 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

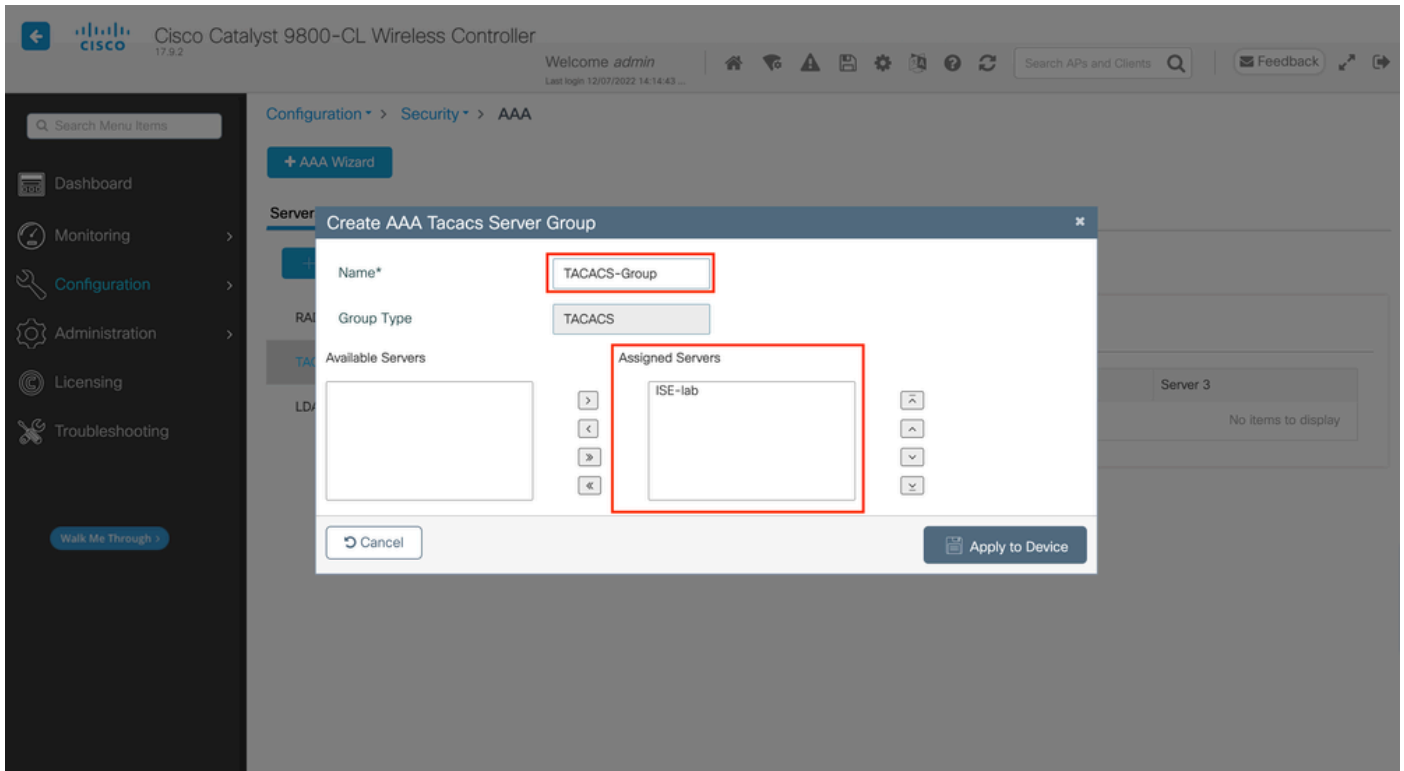
مداوخ ةعوم جم ىلإ TACACS+ مداخ ني عتب مق 2. قوطخل

ةيوسرل مدختسل ا ةهجاو نم

تدحو متهت ذئدعو .امسفن مداوخل ةعوم جم ىلإ مداوخل ا هذ عي مج ني عتب ىصوي ،ةقداصل مل امدادختس! نكمي ةددعتم TACACS+ مداوخ دوجو قلاح يف
مداوخ تاخوم جم نيوكت متي .مداوخل ةعوم جم يف مداوخل ني ب فلتخم تاقداصل مل لامجال عيزوتب (WLC) ةيكلسال ا ةيلحمل ا كلبشلا يف مكحتل
1. قوطخل يف قروكذل (GUI) ةيوسرل مدختس مل ا ةهجاو ةحفص سفن نم بيوبتل ا قمال ع Servers/Groups > TACACS > Server Groups نم TACACS+
قروصل ا يف ةحصول مل او

The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller GUI. The breadcrumb navigation is Configuration > Security > AAA. The 'Servers / Groups' tab is selected, and the 'Add' button is highlighted. The 'RADIUS' section is expanded, and the 'TACACS+' option is selected. The 'Server Groups' table is displayed with one entry: 'TACACS-Group' with 'ISE-lab' as the server address and 'Cisco123' as the key. The table has columns for Name, Server 1, Server 2, and Server 3. The 'TACACS-Group' row shows 'ISE-lab' in the Server 1 column, 'N/A' in the Server 2 column, and 'N/A' in the Server 3 column. The table is paginated to show 1 of 1 items.

قروصل ا يف حصول مل او ،تقباسل ا قروصل ا راطل يف ةفاضل رزل ا قوف رقل ا دن ع ققشب نم ةنغان رهطت ،مداوخل ا ءاشنل ا قتبسل ا ب



قن ي عمل مداوخل قمئاق ىل ا قبول طملا مداوخل لقن او عوم جملا قىم سبت مق ، ققث بنملا قمئاقلا يف

رم او الا رطس قه جاو نم

<#root>

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

TACACS-Group

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

ISE- lab

TACACS+ مداوخل عوم جم ىل ا ريش AAA ققداصم لوخذ ليجست ققيرط عاشن اب مق 3 قوطخل

قئوسرلا مدختسمل قه جاو نم

https:// قحفص نم دعب

/webui/#/aaa

قروصل ا يف حضوم وه امك ققداصم ققيرط عاشن اب مقو ، بيوبتل ا قمال Authentication > AAA Method List ىل ا لقن ا ، قئوسرلا مدختسمل قه جاو

Cisco Catalyst 9800-CL Wireless Controller 17.9.2

Welcome admin
Last login 12/07/2022 14:14:43 ...

Configuration > Security > AAA

+ AAA Wizard

Servers / Groups **AAA Method List** AAA Advanced

Authentication

Authorization

Accounting

+ Add - Delete

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

1 - 3 of 3 items

تتضمن هذه الصفحة قائمة بـ AAA Method List، والتي تحتوي على قائمة بـ AAA Method List، والتي تحتوي على قائمة بـ AAA Method List، والتي تحتوي على قائمة بـ AAA Method List.

Cisco Catalyst 9800-CL Wireless Controller 17.9.2

Welcome admin
Last login 12/07/2022 14:14:43 ...

Configuration > Security > AAA

+ AAA Wizard

Quick Setup: AAA Authentication

Method List Name* tacacs-auth-method

Type* login

Group Type local

Available Server Groups

Assigned Server Groups

TACACS-Group

Cancel Apply to Device

تتضمن هذه الصفحة قائمة بـ AAA Method List، والتي تحتوي على قائمة بـ AAA Method List، والتي تحتوي على قائمة بـ AAA Method List، والتي تحتوي على قائمة بـ AAA Method List.

- تتيح هذه الصفحة للمستخدمين إضافة طرق المصادقة الجديدة، والتي يمكن استخدامها في طرق المصادقة الحالية.
- تتيح هذه الصفحة للمستخدمين إضافة طرق المصادقة الجديدة، والتي يمكن استخدامها في طرق المصادقة الحالية.

تاغوسم نم طقف ققحتي (WLC) ةيكلسالل ةيلحمل ةكبشل ي ف مكحتل رصنع مداوخل ةعومجم لباقم مدختسمل

- رصنع ققحتي، "يلحم ىل يطايتح" رايل تصحفو ةعومجم ك "ةعومجل عون" ترتخا اذا لباقم مدختسمل دامتعا تانايب نم (WLC) ةيكلسالل ةيلحمل ةكبشل ي ف مكحتل اذا. مداخل بجتسي مل اذا طقف ةيلحمل تانايب ةدعاق نع ملعتسيو مداوخل ةعومجم نوكتي نا نكتي ناك ناو ىتح، مدختسمل ةقداصم متتس، ضفر لاسراب مداخل ماق ةيلحمل تانايب ةدعاق ىلع ادوجوم.

رم اوأل رطس ةهجاو نم:

روثعل متي مل اذا طقف مداوخل ةعومجم عم مدختسمل دامتعا تانايب نم ققحتل ديرت تنك اذا مدختسا، الو ايلحم اهيلع

<#root>

WLC-9800(config)#aaa authentication login

tacacs-auth-method

local group

TACACS-Group

مدختسا، طقف مداوخل ةعومجم عم مدختسمل دامتعا تانايب نم ققحتل ديرت تنك اذا

<#root>

WLC-9800(config)#aaa authentication login

tacacs-auth-method

group

TACACS-Group

ال ريخا اذه ناك اذاو مداوخل ةعومجم عم مدختسمل دامتعا تانايب نم ققحتل ديرت تنك اذا مدختساف، يلحم لاخدا عم بيجتسي

<#root>

WLC-9800(config)#aaa authentication login

tacacs-auth-method

group

TACACS-Group

local

ضربو، طقف اي لحم اه و اشنن مت ني ذل ني مدختسملا ضرب كانه، لاثملا اذه في لوال راغل مادختسا يلاتلابو، ISE، مداخل طقف ني مدختسملا

TACACS+ مداخل عومجم يلى ريشت AAA ضيوفتلى EXEC قيرط عاشناب مق. 4. قوطخل

ةيموسرلا مدختسملا هجاو نم:

Configuration > Security > AAA، (GUI) ةيموسرلا مدختسملا هجاو ءحفص نم لاز ام. لوصول قح حنم متي ىتح مدختسملا ليوخت اضيأ بجي ءروصل ي ف حضوم وه امك ليوخت قيرط عاشناب مق مٲ، AAA Method List > Authorization، بويوبتلا ءمالع يلى لقتنا

Cisco Catalyst 9800-CL Wireless Controller
Welcome admin
Last login 12/07/2022 14:14:43 ...

Configuration > Security > AAA

+ AAA Wizard

Servers / Groups AAA Method List AAA Advanced

Authentication

Authorization

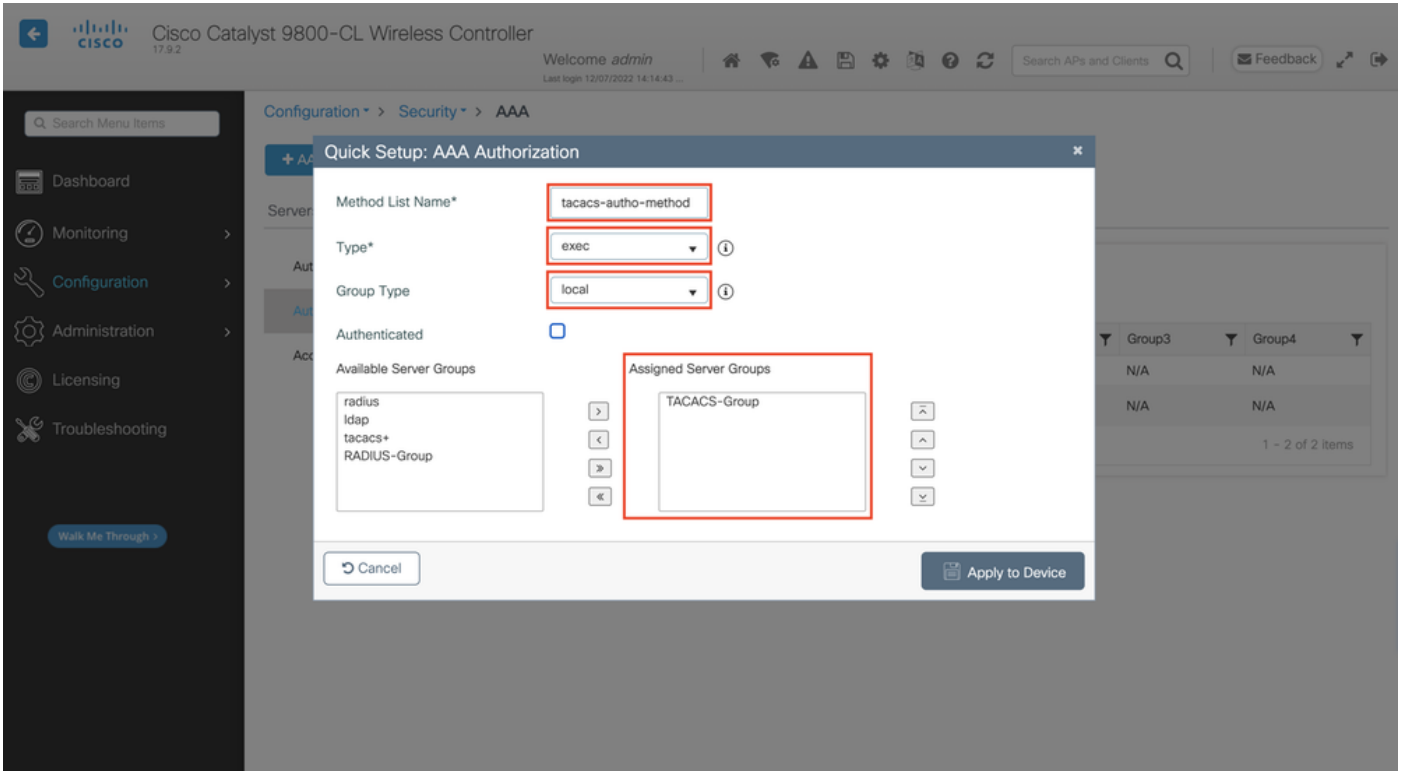
Accounting

+ Add - Delete

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

1 - 3 of 3 items

بولسأ ءفاضل دنع هريو صت مت ني ذل بولسألل لثامم قثبنم ليوخت بولسأ نيوكت رهظي ءفاضل رزلا مادختساب ديدج.



exec مساب عونل رتخاو، لېوختل ةقيرطل مسا ريفوتب مق، قثبنم لنيوكتل اذه يف ةوطخل يف ةقداصلم ل ةقيرطل مدختسم لاك ةومجمل عونل بېترتل سفن مدختساو ةقباسل.

رماوالا رطس ةهجاو نم:

<#root>

WLC-9800(config)#aaa authorization exec

tacacs-autho-method

local group

TACACS-Group

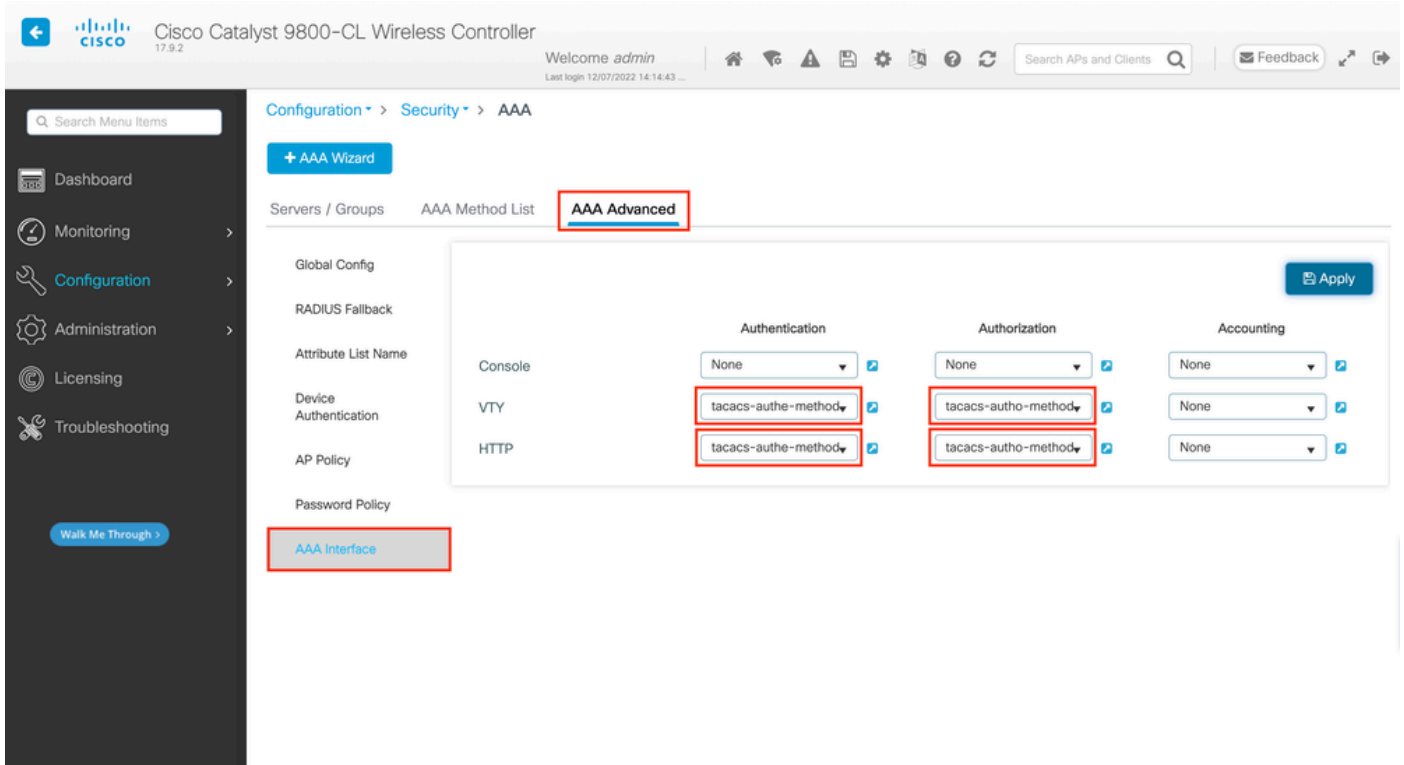
Telnet/SSH ل مدختسم ل vty طوطخ ىل او HTTP تانيوكت ىل قرطال نييعتب مق. 5 ةوطخل

ةيموسرلا مدختسم ل ةهجاو نم:

او HTTP مدختسم لاصتال اهؤاشن امت يتل اضيوفتلاو ةقداصلم ل قرط مادختسا نكمي نم لازتال يتل بېوكتل ةمالع AAA Advanced > AAA Interface نم اهنوكت نكمي يتلاو، Telnet/SSH، [https://](https://webui/#/aaa) يف اهيلي لوصولو نكمي يتل GUI WLC ةحفص

/webui/#/aaa

ةروصل يف حضوم وه امك ،



رم اوآل رطس ةهچ او نم:

(GUI): ةي موسرلا مدختسملا ةهچ او ةقداصل مل ةبسنلاب

<#root>

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

tacacs-auth-method

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

tacacs-auth-method

Telnet/SSH: ةقداصل مل

<#root>

WLC-9800(config)#line vty 0 15

WLC-9800(config-line)#login authentication

tacacs-auth-method

WLC-9800(config-line)#authorization exec

HTTP تادم دغ لي غشت ةداعإ لضأل نم ف HTTP تاني وكت ىل ع تاري غتال عارجإ دن ع هنأ ظحال رماوأل هذه مادختساب كلذ قيقحت نكمي. HTTPS و

```
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
```

TACACS+ ISE ني وكت

TACACS+ ل ءكبش زاهجك (WLC) ةيكلسالال ةيلحمل ءكبشال ي ف مكحتال رصنع ني وكتب مق 1. ةوطخال

ةي موسرل مادختسابل ةهجاو نم

مسقلال ي ف (WLC) ةيكلسالال ةيلحمل ءكبشال ي ف مكحتال رصنع مادختسابل حيضوتل Administration > Network Resources > Network Devices ءكبش زاهجك قباسل ةروصل هذه ي ف حضوم وه امك ،اهتف او ءكبشال ةزهجأ بي وبتال ةمالع Devices

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....	Cisco	All Locations	All Device Types	

The 'Edit' button for the selected device is highlighted with a red box.

(WLC) ةيكلسالال ةيلحمل ءكبشال ي ف مكحتال رصنع ةفاضل تمت ،لاثمل اذه ي هني وكت جاتحي ،كلذل (RADIUS ISE ني وكت) مسقلال نم 1. ةوطخال ىل عجارا RADIUS ةقداصل راتخت امدنع هل عف نكمي يذل او ،TACACS ةقداصل هني وكتل هلي دعت متي نأ ىل ةطاسب زاهج ني وكت جذومن حت ف ىل ي دؤي اذهو .ريحت رزل قوف رقناو ءكبشال ةزهجأ ةمئاق ي ف WLC

ةروصلال هذه يف حضوم وه امك ةكبشلل

Cisco ISE Administration · Network Resources Evaluation Mode 82 Days

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences More

Network Devices

Default Device

Device Security Settings

General Settings

☐ Enable KeyWrap ⓘ

Key Encryption Key Show

Message Authenticator Code Key Show

Key Input Format

☒ ASCII ☐ HEXADECIMAL

☒ TACACS Authentication Settings

Shared Secret Show

☐ Enable Single Connect Mode

☒ Legacy Cisco Device

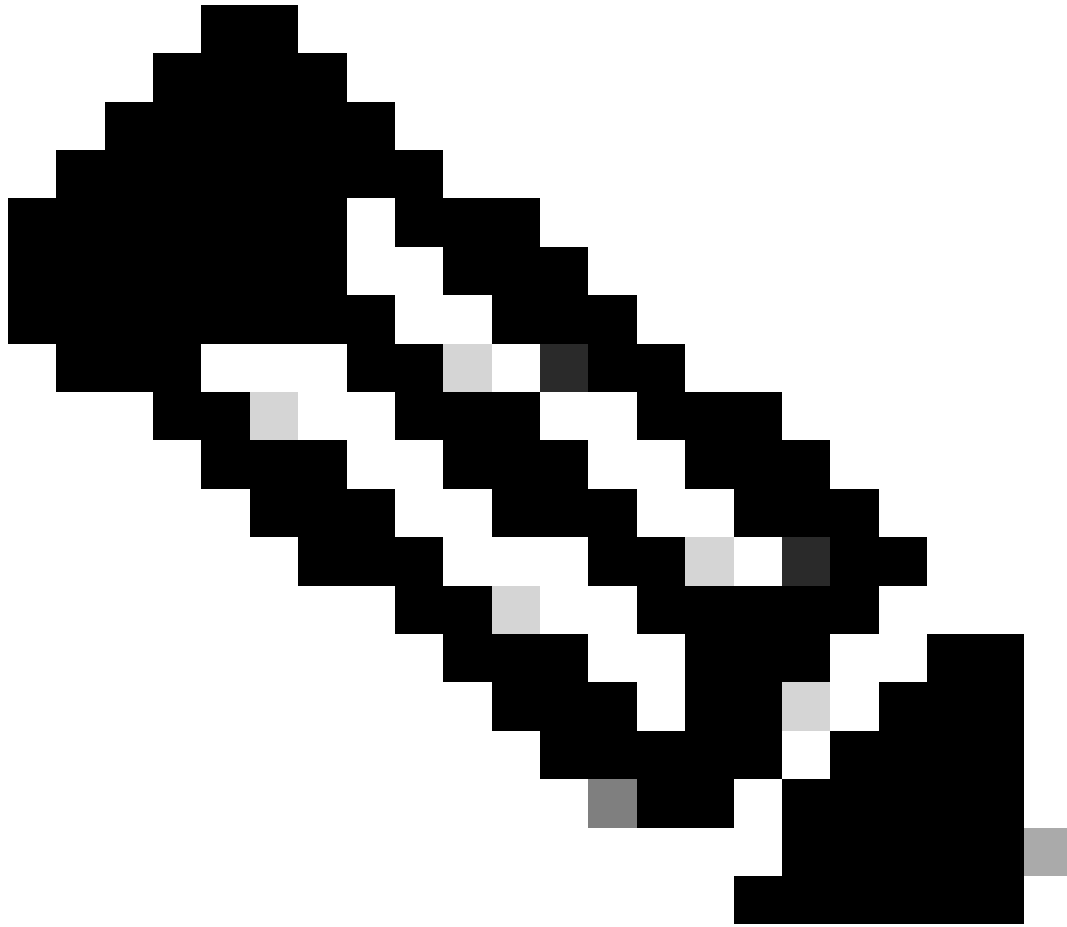
☐ TACACS Draft Compliance Single Connect Support

☐ SNMP Settings

☐ Advanced TrustSec Settings

هذه نيكمتو، TACACS ةقداصم تادادعإ مسق ىلإ ريرمتلاب مق ،ةديجلال ةذفانلال حتف درجمب
نيوكت مسقلا نم 1. ةوطخلال ءانثأ هلإخدا مت يذلا كرتشمال رسلال ةفاضإو ،تادادعإل
[TACACS+ WLC](#).

ةدقعلل "زاهجلال لوؤسم" ةزيم نيكمتب مق 2. ةوطخلال



قراڊا صيخرت ةمزح كيڊل نوكي نأ بجي ،TACACS+ مڊاڤك ISE مڊاڤتسا لڄأ نم :ةظحال م
Mobility وأ Base صيخرت اماو ةزهجألا

ةيموسرلا مڊاڤتسا ملأ ةهجاو نم

نكم تنل ةدقعلل "ةزهجألا قراڊا" ةزيم نيكم ت كيڊل ع بجي ،ةزهجألا قراڊا صيخارت تي بثت درجم ب
ISE رشن ةدقع نيوك ت ريح ت ب مق ،كلذب مايقللو .TACACS+ مڊاڤك ISE مڊاڤتسا نم
مق وأ اهمسا قوف رقناو ،لفسا Administrator > Deployment روثعلال نكمي يتلاو ،ةمڊاڤتسا ملأ
Edit. رزلا ةدعاسم ب كلذب

Cisco ISE Administration - System Evaluation Mode 82 Days

Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access Settings

Deployment

Deployment Nodes

Selected 0 Total 1

Edit Register Syncup Deregister

	Hostname	Personas	Role(s)	Services	Node Status
☐	ise	Administration, Monitoring, Policy Service	STANDALO...	SESSION,PROFILER	✓

مَدْخَلُ "مَسَقْ نَمَضْ عَزْهَجْ أَلَا عَرَادِ مَدْخَلْ نِي كَمَتْ رَايْخْ نَمْ قَقْ حَتْ، عَدَقْ عَالْ نِي وَكْتْ عَذْفَانْ حَتْ فِ دَرَجْمَبْ
عَرُوصَالْ هَذِهِ فِ حَضُومْ وَهْ أَمَكْ، "جَهْنَالْ

Cisco ISE Administration · System Evaluation Mode 82 Days

Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access Settings

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](#)

زايتم ال اعجال ،TACACS فيرعت تافل م عاشن اب مق .3 ةوطخل

ةيموسرل مدختس مل اةه او نم

يذلاو ،15 زايتم ال اوتسم نوكي ن adminuserمزل ي ،لوؤس ملل لوصول ا قوقح ىل لوصولل
 لوصول EXEC اتي helpdeskuserال ،ىرخا اتيح ان نم .exec ةبالاطم ةقبط ىل ا لوصول اب حمسي
 اوتسم نيي عتل .15 نم لقا زايتم اوتسمب هنيي عت نكمي يلاتلابو Shell ىل ا عيرسل
 نيوك نكمي .ليوختل فيرعت تافل مادختس ا نكمي ،نيمدختس ملل بس انم ال زايتم ال

هي موزرلا مدختسملا ههجاو Work Centers > Device Administration > Policy Elements ههجاو
اللاتال ةروصلال يف حضوم وه امك Results > TACACS Profiles امك بيو بئال ةمالع لفسأ (ISE).

Cisco ISE Work Centers · Device Administration Evaluation Mode 82 Days

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

Conditions Library Conditions Smart Conditions

Network Conditions

Results Allowed Protocols TACACS Command Sets TACACS Profiles

TACACS Profiles

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

Add Duplicate Trash Edit Filter

Name	Type	Description
Default Shell Profile	Shell	Default Shell Profile
Deny All Shell Profile	Shell	Deny All Shell Profile
IOS Admin	Shell	Assigned to each user in the group admin-group
IOS Helpdesk	Shell	Assigned to each user in the group helpdesk-group
WLC ALL	WLC	WLC ALL
WLC MONITOR	WLC	WLC MONITOR

فللم نيوكت جذوم نحت في يذلا "ةفاضإ" رزل مدختسأ ،ديج TACACS في رعت فلم نيوكت ل
لكشلا اذهب جذوم نال اذه وديبي نأ بجي .ةروصلال يف دوجوم لكالذل لثامم لال ديجال في رعتال
مادختساب ،وه يذلا(adminuser إلى هنيي عت متي يذلا في رعتال فلم نيوكت ل صاخ لكش ب
(shell 15) تازايتما يوتسم

Cisco ISE Work Centers · Device Administration Evaluation Mode 82 Days

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

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

الك، زايتم as maximum، زايتم ري صقتا، ريخالا اذه ل. فيرعتا helpdesk فملم ةيلمعلا رك 1. إلى تتبث

ISE. إلى نع ني مدختسم تاعومجم عاشنإ 4. ةوطخلا

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

ISE. إلى نع ني مدختسملا عاشنإ ب مق 5. ةوطخلا

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

زاهج لوؤسم جهن ةعومجم عاشنإ 6. ةوطخلا

ةيموسرلا مدختسملا ةهجاو نم

فيرعت ريورضلا نم لظي، ني مدختسملا عاشنإ درجم ب، RADIUS إلى لوصولل ةبسنلاب ةبسانملا لوصولل قوقح مهنم ISE إلى لع مهب ةصاخلا ضيوفتالو ةقداصملا تاسايس اهنويوكت نكمي يتلاو، ةياغل اذهل زاهجال لوؤسم جهن تاعومجم TACACS ةقداصم مدختست

Work Centers > Device Administration > Device Admin Policy Sets GUI Page

Cisco ISE Work Centers · Device Administration Evaluation Mode 82 Days

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

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

في رمح أال نوللاب رطؤم أا "ةفاضأ" رزلأ مدختسأ ،ةزه أال ةرادأل تاسايس ةعومجم ءاشن إل مسا ريفوتب مق .جهنلأ تاعومجم ةمئاق إلأ رصنع ةفاضأ إلأ اذه يدؤي ،ةقباسلأ ةروصلأ لسلسلأ /تالوكوتوربالأ ،هتحت اهقيبطت بجي طرشو ،اثيرح اهؤاشن إلأ متي تلأ ةعومجملل جهنلأ ةعومجم ةفاضأ ءاهن إل Save رزلأ مدختسأ .(يفكي ام Default Device Admin ،انه) هب حومسملأ مداخلأ امك ،هب ةصاخلأ نيوكتلأ ةحفص إلأ لوصولل هنيمي إلع دوجوملأ مهسلأ سار مادختساو ةضورعملأ ةحفصلأ إلع رهظي .

Cisco ISE Work Centers · Device Administration Evaluation Mode 82 Days

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

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	Options

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](#)

تابل لطل اةيفصتب لاثمل اذه في "WLC TACACS ةقداصم" ةدحمل جهنل ةومجم موقت
IP ناوع C9800 WLC لاثمل يواسي يذل IP ناوع

دادع مت .مادختسالا تاجايتحاب يفت اهنأل ةيضارتفالا ةدعاقلا كرت مت ،ةقداصم جهنك
ضيوفت يتدعاق:

- وه .ةفرعمل admin-group ةومجملا لىل مدختسمل يمتني امدنع لوأل رايل ليغشت متي
فل م ربع 15 زايتمالا نيغيو (Permit_all ةيضارتفالا ةدعاقلا ربع) رماوأل عيجمب حمسي
(دحمل TACACSIOS_Admin فيرعت).
- ةدحمل helpdesk-group ةومجملا لىل مدختسمل يمتني امدنع ةيناثلا ةزيملا ليغشت متي و
1 زايتمالا نيغيعتب موقتو (ةيضارتفالا ةدعاقلا Permit_all ربع) رماوأل عيجمب حمست يهو
(دحمل TACACSIOS_Helpdesk فيرعت فلم ربع).

اهنيوكت مت يتل دامتعالا تانايب مادختسلا نكمي ،ةوطخل هذه لامتك دع

ةي لحملا ةكبشللا يف مكحتلا رصنع يف ةقداصملا helpdesk نيف مدختسملا adminuser ل
Telnet/SSH جم ان رب مادختساب وأ (GUI) ةي موسرلا مدختسملا ةهجاو ربع (WLC) ةي كللساللا

اهحال صا واطخالا فاشكتسا

ةفاضالا كنكم يف ،ةمدخلال عونل RADIUS ةمس لاسرا عقوتي كب صاخلا RADIUS مدخالناك اذا
(WLC) ةي كللساللا ةي لحملا ةكبشللا يف مكحتلا رصنع ىلع :

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

يف مكحتلا ةدحوب ةصاخلا (GUI) ةي موسرلا مدختسملا ةهجاو واطخا فاشكتسا
ربع (CLI) رماوالا رطس ةهجاو لوصو وأ (WLC) ةي كللساللا ةي لحملا ةكبشللا
ةي لحملا ةكبشللا يف مكحتلا ةدحوب صاخلا RADIUS/TACACS+ لوكوتورب
(WLC) ةي كللساللا

رطس ةهجاو وأ (GUI) ةي موسرلا مدختسملا ةهجاو ىلا TACACS+ لوصو واطخا فاشكتسا لجا نم
(WLC) ةي كللساللا ةي لحملا ةكبشللا يف مكحتلا ةدحوب debug tacacs ةصاخلا (CLI) رماوالا
جارخالا ةدهاشمو ىلوالا ةيفرطالا ةطحمللا ةشاش ىلا ةفاضالاب ،رمالا رادصاب مق ،اهحال صا
لوخدلا ليجست ةلواحم عارجا دنع رشابملا

جورخلال ليجست هعبتي يذلا حجانلا لوخدلا ليجست موقفي ،لا ثملال لابس ىلع
جارخالا اذه عاشناب مدختسملا adminuser نم

```
<#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: processing authentication start request id 15465  
Dec 8 11:38:34.685: TPLUS: Authentication start packet created for 15465(adminuser)  
Dec 8 11:38:34.685: TPLUS: Using server 10.48.39.134  
Dec 8 11:38:34.685: TPLUS(00003C69)/0/NB_WAIT/7FD29013CA68: Started 5 sec timeout  
Dec 8 11:38:34.687: TPLUS(00003C69)/0/NB_WAIT: socket event 2  
Dec 8 11:38:34.688: TPLUS(00003C69)/0/NB_WAIT: wrote entire 45 bytes request  
Dec 8 11:38:34.688: TPLUS(00003C69)/0/READ: socket event 1  
Dec 8 11:38:34.688: TPLUS(00003C69)/0/READ: Would block while reading  
Dec 8 11:38:34.701: TPLUS(00003C69)/0/READ: socket event 1  
Dec 8 11:38:34.701: TPLUS(00003C69)/0/READ: read entire 12 header bytes (expect 15 bytes data)
```

```

Dec 8 11:38:34.701: TPLUS(00003C69)/0/READ: socket event 1
Dec 8 11:38:34.701: TPLUS(00003C69)/0/READ: read entire 27 bytes response
Dec 8 11:38:34.701: TPLUS(00003C69)/0/7FD29013CA68: Processing the reply packet
Dec 8 11:38:34.701: TPLUS: Received authen response status GET_PASSWORD (8)
Dec 8 11:38:38.156: TPLUS: Queuing AAA Authentication request 15465 for processing
Dec 8 11:38:38.156: TPLUS(00003C69) login timer started 1020 sec timeout
Dec 8 11:38:38.156: TPLUS: processing authentication continue request id 15465
Dec 8 11:38:38.156: TPLUS: Authentication continue packet generated for 15465
Dec 8 11:38:38.156: TPLUS(00003C69)/0/WRITE/7FD3796079D8: Started 5 sec timeout
Dec 8 11:38:38.156: TPLUS(00003C69)/0/WRITE: wrote entire 29 bytes request
Dec 8 11:38:38.183: TPLUS(00003C69)/0/READ: socket event 1
Dec 8 11:38:38.183: TPLUS(00003C69)/0/READ: read entire 12 header bytes (expect 6 bytes data)
Dec 8 11:38:38.183: TPLUS(00003C69)/0/READ: socket event 1
Dec 8 11:38:38.183: TPLUS(00003C69)/0/READ: read entire 18 bytes response
Dec 8 11:38:38.183: TPLUS(00003C69)/0/7FD3796079D8: Processing the reply packet
Dec 8 11:38:38.183: TPLUS: Received authen response status PASS (2)
Dec 8 11:38:38.184: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: adminuser] [Source: 10.61.80.151]
Dec 8 11:38:38.259: TPLUS: Queuing AAA Authorization request 15465 for processing
Dec 8 11:38:38.260: TPLUS(00003C69) login timer started 1020 sec timeout
Dec 8 11:38:38.260: TPLUS: processing authorization request id 15465
Dec 8 11:38:38.260: TPLUS: Protocol set to None .....Skipping
Dec 8 11:38:38.260: TPLUS: Sending AV service=shell
Dec 8 11:38:38.260: TPLUS: Sending AV cmd*
Dec 8 11:38:38.260: TPLUS: Authorization request created for 15465(adminuser)
Dec 8 11:38:38.260: TPLUS: using previously set server 10.48.39.134 from group TACACS-Group
Dec 8 11:38:38.260: TPLUS(00003C69)/0/NB_WAIT/7FD3796079D8: Started 5 sec timeout
Dec 8 11:38:38.260: TPLUS(00003C69)/0/NB_WAIT: socket event 2
Dec 8 11:38:38.260: TPLUS(00003C69)/0/NB_WAIT: wrote entire 64 bytes request
Dec 8 11:38:38.260: TPLUS(00003C69)/0/READ: socket event 1
Dec 8 11:38:38.260: TPLUS(00003C69)/0/READ: Would block while reading
Dec 8 11:38:38.285: TPLUS(00003C69)/0/READ: socket event 1
Dec 8 11:38:38.285: TPLUS(00003C69)/0/READ: read entire 12 header bytes (expect 18 bytes data)
Dec 8 11:38:38.285: TPLUS(00003C69)/0/READ: socket event 1
Dec 8 11:38:38.285: TPLUS(00003C69)/0/READ: read entire 30 bytes response
Dec 8 11:38:38.285: TPLUS(00003C69)/0/7FD3796079D8: Processing the reply packet
Dec 8 11:38:38.285: TPLUS: Processed AV priv-lvl=15
Dec 8 11:38:38.285: TPLUS: received authorization response for 15465: PASS
Dec 8 11:38:44.225: %SYS-6-LOGOUT: User adminuser has exited tty session 7(10.61.80.151)
Dec 8 11:38:44.225: Socket I/O cleanup message sent to TACACS
TPLUS Proc:SOCKET IO CLEANUP EVENT
Dec 8 11:38:44.226: %HA_EM-6-LOG: catchall: logout
Dec 8 11:39:18.689: %SYS-6-LOGOUT: User admin has exited tty session 5(10.61.80.151)
Dec 8 11:39:18.690: Socket I/O cleanup message sent to TACACS
TPLUS Proc:SOCKET IO CLEANUP EVENT

```

اهرأى خإ مآى ىل قرطال ةمئاق ضرع debug aaa authorization، كلذ نم الدب و debug aaa authentication رمرأل

م دختسمل ةلواحم دنع (WLC) ةىكلسلال ةىلحمل ةكبشلل فى مكحتل رصنع ةطساوب رورم ةكرب قلعتى يذلاو، لثامم حىحصت جارخا رهظى، RADIUS ةقداصمب موقت ام دنع RADIUS.

اهرأى خإ مآى ىل قرطال ةمئاق ضرع debug aaa authorization، كلذ نم الدب و debug aaa authentication رمرأل

فى مكحتل ةدحوب ةصاخال (GUI) ةىموسرل م دختسمل ةهجاو عا طخأ فاشكتسأ

رم اوأال رطس ةهجاو ىلإ لوصولا وأ (WLC) ةيكلسالل ةيلحمل ةكبشلا
ISE راي عم عم ةقفاوتملا (GUI) ةيموسرل مدختسملا ةهجاو ربع (TACACS+)
اهحالصإو

TACACS+ عم مت مدختسم ةقداصم لك ضرع نكمي، Operations > TACACS > Live Logs ةحفصلال نم
ليصافتلا رز مدختسأ، TACACS+ ةقداصم وأ ضيوفت ليصافت عيسوتل. ةعاس 24 رخآ ىتح
ثدحل اذهب قلعتملا.

Cisco ISE

Operations · TACACS

Evaluation Mode 82 Days

Live Logs

Refresh

Never

Show

Latest 20 records

Within

Last 3 hours

Export To

Filter

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

Last Updated: Thu Dec 08 2022 12:57:09 GMT+0100 (Central European Standard Time)

Records Shown: 6

يلي امك ةقيرطال هذهل ةحجان ةقداصم ةلواح helpdeskuser وذب، عيسوتل دن ع

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

```

ةكبشال WLC-9800 زاهج ىلع حاجن ب helpdeskuser م دخت سمل ةق داصم تم ت هنا ىرت نأ كنكمي ، اذه نمو
فل م IOS Helpdesk ن يي عت مت ، كلذ ىلع ةوالع . ةق داصم ل WLC TACACS Authentication > Default ج هن ةدعاس م ب
1. زاي ت م ا ل ا ي و ت س م ه ح ن م م ت و ، م دخت سمل ا اذه ل ل ي و خ ت ل ا في ر ع ت

ةمچرتل هذه ل و ح

ةيلآل ا تاي ن ق ت ل ا ن م ة و م ج م ا د خ ت س ا ب د ن ت س م ل ا ا ذ ه Cisco ت م چ ر ت م ل ا ع ل ا ا ح ن ا ع م ج 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 ا و ا م ك ة ق ي ق د ن و ك ت ن ل ة ي ل آ ة م چ ر ت ل ض ف ا ن ا ة ط 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 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 ي ل ا 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 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 د ن ت س م ل ا