

ASA 8.3: TACACS مادختساب ٰقادصم

تاي وتحمل

ةمدقملا

[ةيساسألا تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكمل](#)

[تاجالطصلالا](#)

[نيوكتللا](#)

[ةكبشللي طي طختلا مسلا](#)

[\(رم أول ارتس ٰههجاو\) CLI مادختساب ACS مداخ نم ٰقادصملل ASA نيوك](#)

[ASDM مادختساب ACS مداخ نم ٰقادصملل ASA نيوك](#)

[مداخك ACS نيوك](#)

[ةحصلا نم ققحتلا](#)

[ماحالص او عاطخألا فاشكتسا](#)

[لش ف من أيلع tacacs server x.x.x يف AAA زييمت: أطاخ](#)

[قلص تاذنامولعم](#)

ةمدقملا

نيمدختسملا ٰقادصمل نامألا زاهج نيوك ئيفيك لوح تامولعم دنتسملا اذه مدقى.
ةكبشلا ىلا لوصولل

ةيساسألا تابلطتملا

تابلطتملا

متولماكللا ليغشتلا ديق (ASA) فيكتلل لباقلا نامألا زاهج نأ دنتسملا اذه ضرتفي
تارييغت عارجاب Cisco نم CLI وـ (ASDM) ئلدعملما نامألا ٰزهجأ ريدمل حامسلل هنيوك
لا.

ةيفيك لوح تامولعملا نم ديزم ىلع لوصحلل [HTTPS ASDM لوصوب حامسلا](#) عجار: ظحال
مةطساوب دعب نع زاهجلما نيوكتب حامسلا ASDM.

ةمدختسملا تانوكمل

: ئيلاتلا ئيداملما تانوكمل او جماربلما تارادصلما ىلا دنتسملا اذه يف ئدراولما تامولعملا دنتس

- تارادصلالا او 8.3 رادصلالا Cisco Adaptive Security Appliance، ئلدعملما نامألا ٰزهجأ جمانرب
ثدحألا

- ثدحألا تارادصلالا او 6.3 رادصلالا Cisco Adaptive Security Device Manager.

• Cisco ماحتلا موصولا آلا نم 5.x

هـصـاخـ ةـيـلـمـعـمـ ةـيـبـ يـفـ ةـدـوـجـوـمـلـاـ ةـزـهـجـأـلـاـ نـمـ دـنـتـسـمـلـاـ اـذـهـ يـفـ ةـدـرـاـوـلـاـ تـامـوـلـعـمـلـاـ عـاـشـنـاـ مـتـ
تـنـاـكـ اـذـاـ (ـيـضـارـتـفـاـ)ـ حـوـسـمـمـ نـيـوـكـرـتـبـ دـنـتـسـمـلـاـ اـذـهـ يـفـ ةـمـدـخـتـسـمـلـاـ ةـزـهـجـأـلـاـ عـيـمـجـ تـأـدـبـ
رـمـأـ يـأـلـ لـمـتـحـمـلـاـ رـيـثـأـتـلـلـ كـمـهـفـ نـمـ دـكـأـتـفـ،ـقـرـشـاـبـمـ كـتـكـبـشـ

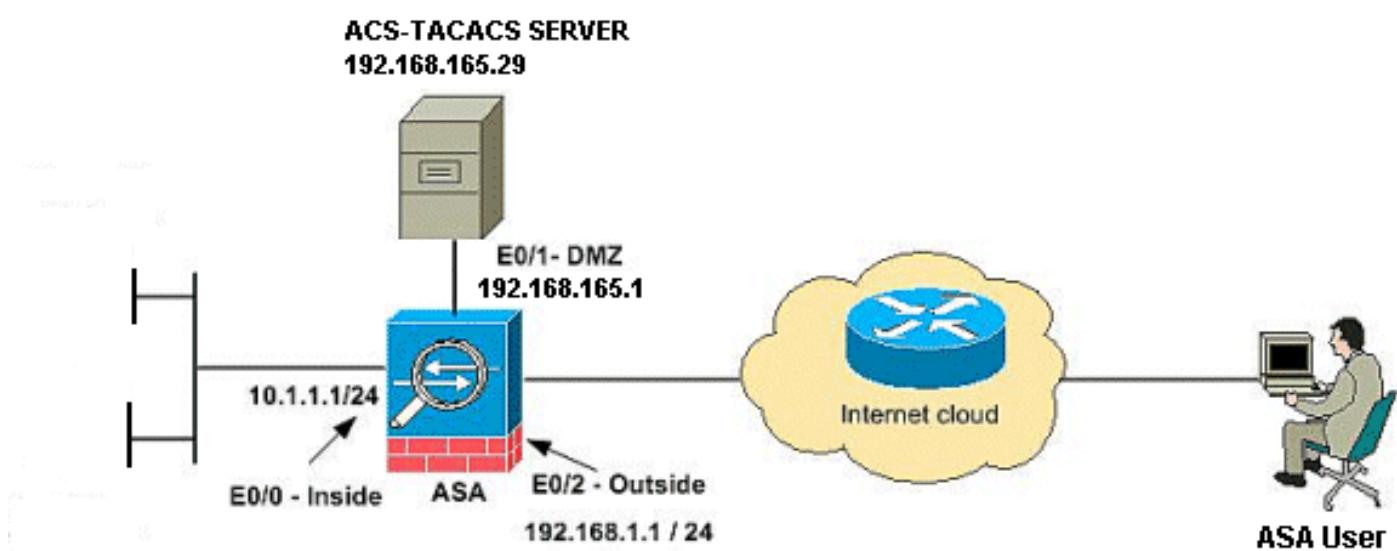
الطقس حالات

تاجحالطصا لوح تامول عملانم ديزم ىلע لوصح حلل ئينقتلا Cisco تاجيملت تاجحالطصا عجارتادنتسىملا

نیوکرک

دنتس ملا اذه يف ٰ حض ومل ا تازيملا نيوكت تامولعم كل مدقُّت ، مسقلا اذه يف
نم ديزم ىلع لوصحلل (طقف [نيلجس ملا](#) ئالمعلل) [رماؤلا شحب قادأ](#) مدخلتساً : ئطحالم
مسقلا اذه يف ٰ مدخلتس ملا رماؤلا لوح تامولعملا

ةكبس للى طختلا مسرلا



تەنرتنىلا ئىلۇر اىنوناق لىكىشت اذە يىف لەمعتسىي ئەطخ بەطاخى سىيل ip لە ئەظحالم
ھەئىب ربىت خەم يىف تەلمىعتسا ناك يىأ ناونىع 1918 rfc 5

(رم اوالا رطس ٰ وجاو) CLI مادختس اب ACS مداخ نم ٰ قداص ملل ASA نیوکت

لدان ACS لانم قدصي نأ ASA لال ليكشت اذه تزجنأ

```

ASA(config)# aaa-server cisco protocol tacacs+
ASA(config-aaa-server-group)# exit

!---- Define the host and the interface the ACS server is on.

ASA(config)# aaa-server cisco (DMZ) host 192.168.165.29
ASA(config-aaa-server-host)# key cisco

!---- Configuring the ASA for HTTP and SSH access using ACS and fallback method as LOCAL authentication.

ASA(config)#aaa authentication ssh console cisco LOCAL
ASA(config)#aaa authentication http console cisco LOCAL

```

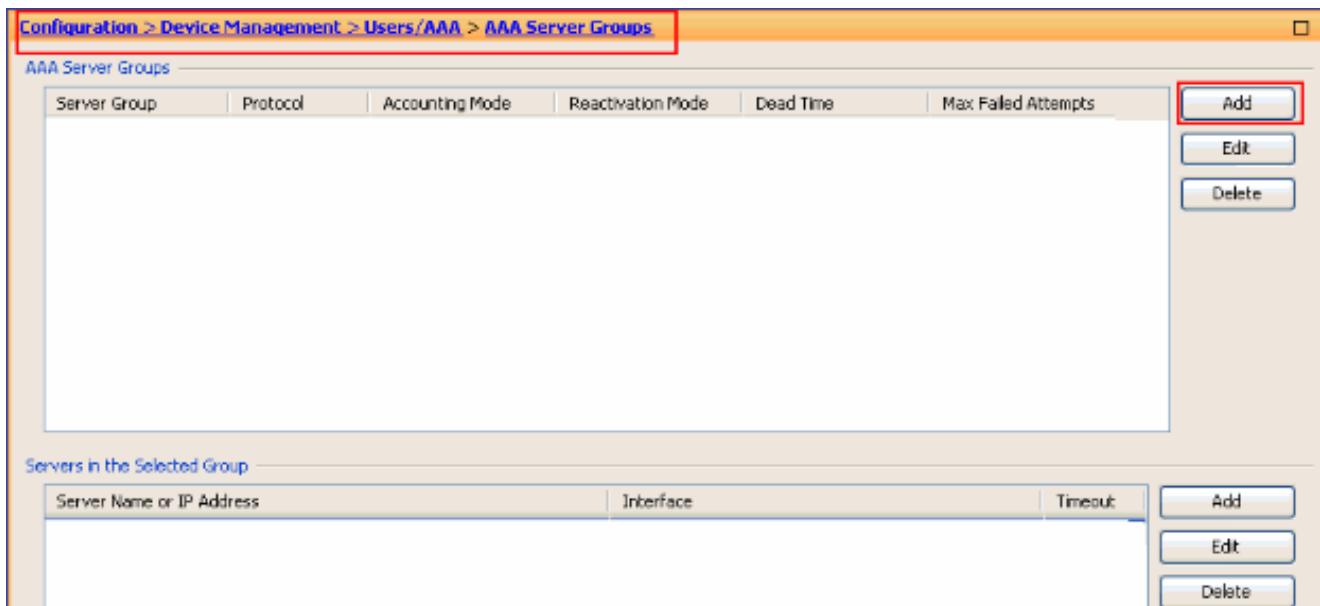
رملأا مادختس اب ASA ىلع يلح مدخلتس معاشناب مق :ةظحالم
ارفوتم ACS نوكى ال امدنع ٰيلحمل ا مادختس اب ASDM ىل ا لوصولل [privilege 15](#)

مادختس اب ACS مداخن مقداصملل ASA نيوكت

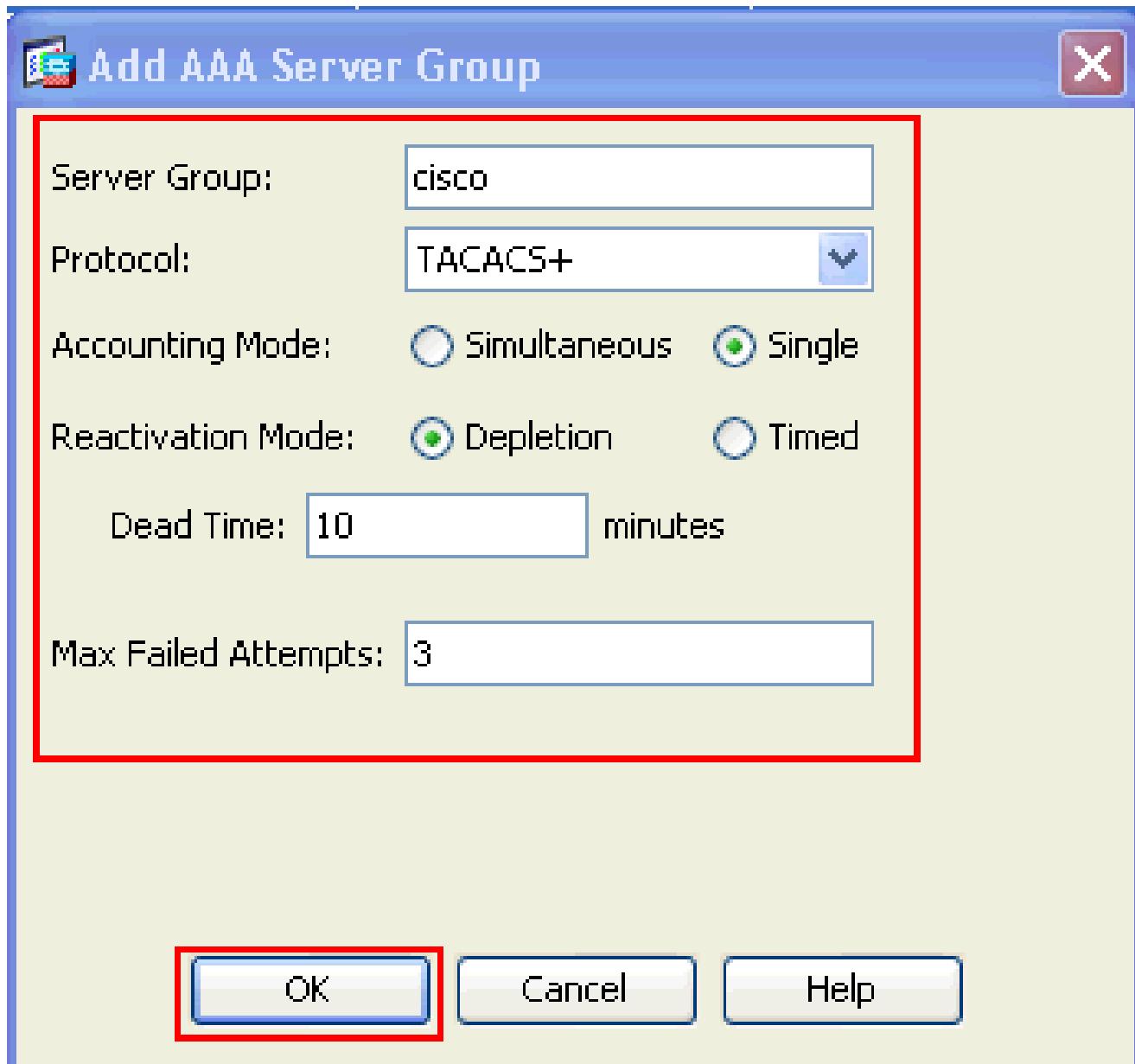
عارج ASDM

لدان acs ل ا نم مقداصملل ASA ل ا تلکش اذاه تمتأ steps in order to:

1. ةعومجم عاشنال ٰفاضا > Users/AAA > مداخن اورادا > نيوكت رتخد
مداخن AAA.



2. امك AAA مداخن ةعومجم ٰفاضا ٰذفان يف مداخن ةعومجم ليصافت ريفوتب مق
ي ه اهؤاشن ا مت يتلا مداخن ةعومجم و TACACS+ و مادختس مل ا لوكوتوربل Cisco.



وقوف رقين او

3. لدان تخت فيضي نقطط وفعومجم لدان AAA>AAA/لمعتسم<ةراداً>لديكشت ترتخأ
لدان AAA لـ تفضي in order to في دفعه ملا فعومجملا.

Server Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Attempts	
cisco	TACACS+	Single	Depletion	10	3	Edit

Servers in the Selected Group

Server Name or IP Address	Interface	Timeout	
			Add

4. مدخلات عوامجم حضوره امك AAA مدخله ظفاضاً راطلا يف AAA مدخله ليصافت ريفوتب مق
يـه ظـمـدـخـتـسـمـلـا Cisco.

Add AAA Server

Server Group:	cisco									
Interface Name:	dmz									
Server Name or IP Address:	192.168.165.29									
Timeout:	10 seconds									
TACACS+ Parameters										
Server Port:	49									
Server Secret Key:	*****									
SDI Messages										
Message Table <table border="1"> <tr><td> </td><td> </td><td> </td><td> </td><td> </td><td> </td><td> </td><td> </td><td> </td></tr> </table>										
<input type="button" value="OK"/> <input type="button" value="Cancel"/> <input type="button" value="Help"/>										

قبطي ظقط ط كل ذ دعـب، ok، ظقط ط

ىـلـعـهـنـيـوـكـتـمـتـيـذـلـاـAAAـمـداـخـلـهـعـوـمـجـمـىـرـتـسـ

5. قـيـبـطـتـقـوفـرـقـنـاـ

Configuration > Device Management > Users/AAA > AAA Server Groups

AAA Server Groups

Server Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Attempts
cisco	TACACS+	Single	Depletion	10	3

Servers in the Selected Group

Server Name or IP Address	Interface	Timeout
192.168.165.29	dmz	

LDAP Attribute Map

Apply

Reset

6. قوف رقناو ئقادىمىلارا > AAA > Users/AAA > ئىللىنىمىلارا > Cisco HTTP/ASDM و SSH دىرىجىمىك رتىخىنىمىلارا تاناخ قىيىبت قوف.

Authentication Authorization Accounting

Enable authentication for administrator access to the ASA.

Require authentication to allow use of privileged mode commands

Enable Server Group: LOCAL Use LOCAL when server group fails

Require authentication for the following types of connections

HTTP/ASDM Server Group: cisco Use LOCAL when server group fails

Serial Server Group: LOCAL Use LOCAL when server group fails

SSH Server Group: cisco Use LOCAL when server group fails

Telnet Server Group: tac Use LOCAL when server group fails

Apply

Reset

ACS نیوکت مداخل

ACS نیوکت مداخل از این طریق ایجاد می‌شود:

1. ASA لی تفرض این قلخی آنرا در درون کپش ترتیب داده و AAA نوبزن طبق قلخی آنرا در ACS لی ایجاد کرد.

Cisco Secure ACS

The screenshot shows the Cisco Secure ACS interface. The left sidebar has a 'Network Resources' section with 'Network Device Groups' expanded, showing 'Location' and 'Device Type'. Under 'Network Devices and AAA Clients', 'Default Network Device' and 'External RADIUS Servers' are listed. The main panel title is 'Network Resources > Network Devices and AAA Clients'. It contains a 'Network Devices' table with columns: Name, IP / Mask, NDG:Location, NDG:Device Type, and Description. A message says 'No data to display'. Below the table are buttons: Create (highlighted with a red box), Duplicate, Edit, Delete, File Operations, and Export.

2. لاسرا قوف رقناو (انه ليمعلا و هو ASA) ليجعلها لوح وبولطملا تامولعملا ريفوتب مق IP ناونع ليصافتلا نمضتتو. مداخل ASA هتفاضا متت نأ ل رايحلا اذه حيتحي مداخل ASA ليصافت تو TACACS.

Cisco Secure ACS

The screenshot shows the 'Create' dialog for a new network device. The 'Name' field is set to 'Cisco' and 'Description' is 'ACS to ASA'. In the 'Network Device Groups' section, 'Location' is 'All Locations' and 'Device Type' is 'All Device Types'. Under 'IP Address', 'Single IP Address' is selected and the IP address is '192.168.185.3'. In the 'Authentication Options' section, 'TACACS+' is checked and 'Shared Secret' is 'cisco'. Other options like 'Single Connect Device', 'Legacy TACACS+ Single Connect Support', and 'TACACS+ Draft Compliant Single Connect' are available. At the bottom are 'Submit' and 'Cancel' buttons.

مداخل هتفاضا متت ليمعلا Cisco دهاشتس.

Cisco Secure ACS

The screenshot shows the Cisco Secure ACS interface. The left sidebar has a tree view with 'Network Resources' selected. Under 'Network Resources', 'Network Device Groups' is expanded, showing 'Location' and 'Device Type'. 'Device Type' is further expanded to show 'Network Devices and AAA Clients', which contains 'Default Network Device', 'External RADIUS Servers', and 'Cisco'. The main panel displays a table titled 'Network Devices' with one row. The row for 'Cisco' is highlighted with a red border. The table columns are: Name, IP / Mask, NDG:Location, NDG:Device Type, and Description. The data for the Cisco entry is: Name = Cisco, IP / Mask = 192.168.166.3/32, NDG:Location = All Locations, NDG:Device Type = All Device Types, and Description = ACS to ASA.

Name	IP / Mask	NDG:Location	NDG:Device Type	Description
Cisco	192.168.166.3/32	All Locations	All Device Types	ACS to ASA

3. قوف رقناو نيم دختسملاء > ئيلخادلا ئي وهلا نزاخم > ئي وهلا نزاخم و نيم دختسملاء رت خا
دي دج مدختسملاء عاشن إل عاشنإ.

Cisco Secure ACS

The screenshot shows the Cisco Secure ACS interface. The left sidebar has a tree view with 'Users and Identity Stores' selected. Under 'Users and Identity Stores', 'Internal Identity Stores' is expanded, showing 'Users'. The main panel displays a table titled 'Internal Users' with one message: 'No data to display'. At the bottom of the table are several buttons: 'Create' (highlighted with a red box), 'Duplicate', 'Edit', 'Delete', 'Change Password', 'File Operations', and 'Export'.

4. ئاسرا قوف رقنا، عاهتنالا دنع . يراي تخا رورملاء تامولعم ريفوتب مق
اهل نيك متل او رورملاء قمل كومسا ل او رورملاء قمل ك.

Cisco Secure ACS

My Workspace Network Resources Users and Identity Stores Internal Identity Stores Users Create

General

- Name: Status:
- Description: Test User
- Identity Group:

Password Information

- Password must:
 - Contain 4 - 32 characters
- >Password:
- Confirm Password:
- Change password on next login

Enable Password Information

- Password must:
 - Contain 4 - 32 characters
- Enable Password:
- Confirm Password:

User Information

There are no additional identity attributes defined for user records.

Submit **Cancel**

مدادخ لى هتفضل ا مرتت cisco مدخلت سمل دهاشتس.

Cisco Secure ACS

My Workspace Network Resources Users and Identity Stores Internal Identity Stores Users

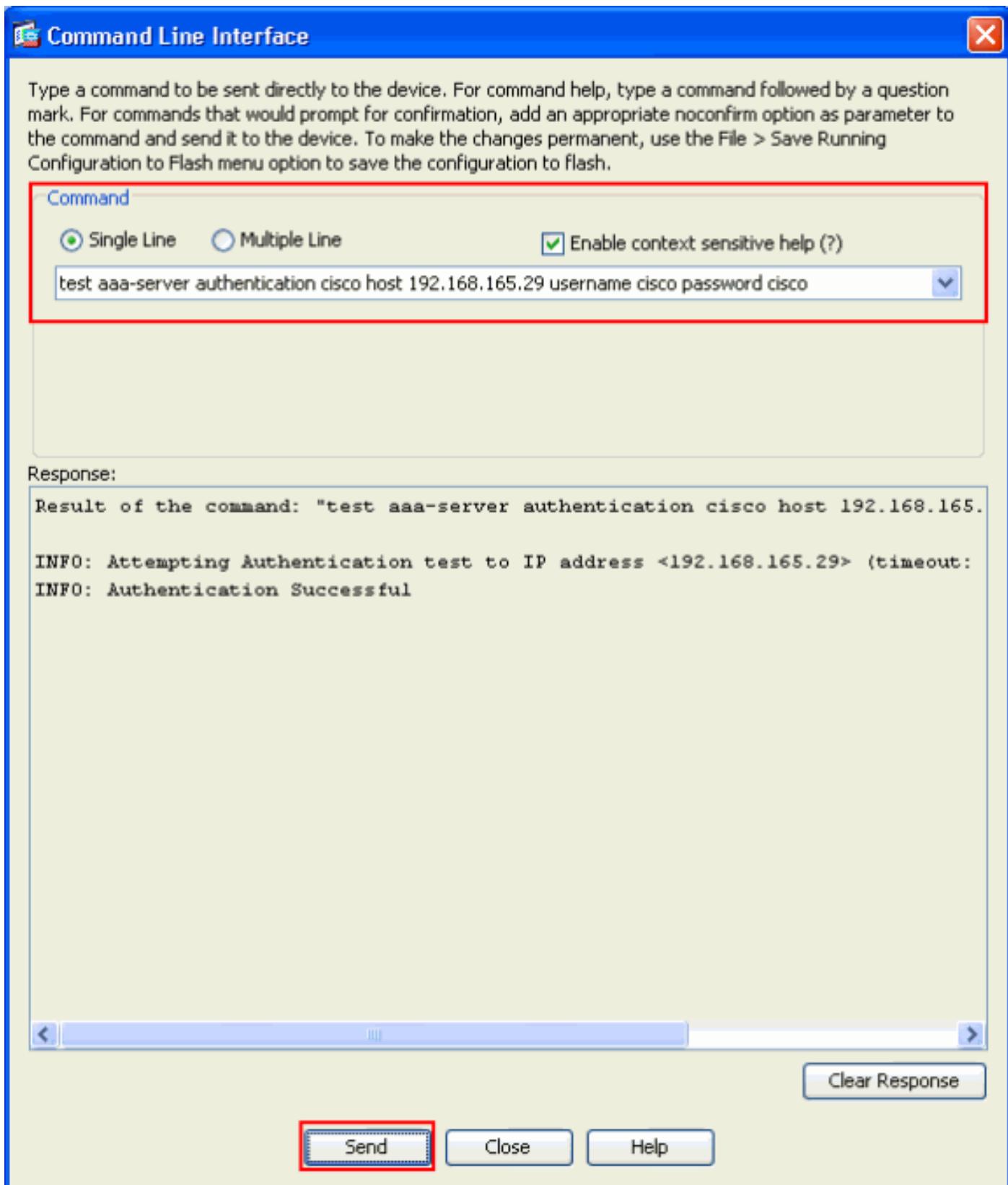
Internal Users

	Status	User Name	Identity Group	Description
<input type="checkbox"/>		cisco	All Groups	Test User

وحصلنا م ققحتل

حيحص لكشب نيكوتل ا لمع دي كأتل مسقل ا اذه مدخلتسا

ملک 192.168.165.29 username cisco فیض م cisco وہ حصہ لدان-aaa رابتخالا تلمعتسا ناً روصلا هذھ حضوت .جیحص لکشب لمعی لیکشتلا نا ققحتی ناً رمأ cisco cisco cisco ACS مداخ طس اوپ ASA ب لصتی يذلا مدختسملأا ۃقداصم تمت دق منأو ۃحجان ۃقداصملأا



مجرتم ڈادا مدختسا show رہماً ضعوب (طقف نیل جس مل اعالم علل) جارخ الامجرتمن ڈادا مع دت show رم الیا جرخُم لیلحت ضرعل (OIT) جارخ الیا

اھالص او ءاطخآل افاشڪتسا

هناك طرق متعددة لتنفيذ AAA، منها استخدام TACACS+ server x.x.x tacacs if يف زويي مل server AAA مداو خة ومجمل اطخ لش ف

حلاص لاصتا كي دل نأ نم دكأت x.x.x.x مداخل لاصتا تدقول Cisco ASA نأ ظل اس رلا هذه ينعت
نـم TACACS+ مداخل ASA ئـلـع ئـلـهـمـلـا ئـدـايـزـ اـضـيـأـ كـنـكـمـيـ . ASA نـم x.x.x.x مـاـخـلـابـ TCP 49 ئـلـع
بلـطـ ASA لـسـريـ نـلـ . ئـكـبـشـلـلـ لـاقـتـنـاـ نـمـزـ دـوـجـ وـقـلـاحـ يـفـ يـنـاوـثـلـاـ نـمـ بـوـغـرـمـلـاـ دـدـعـلـاـ ئـلـاـ 5
يـفـ يـلـاتـلـاـ مـاـخـلـاـ مـدـخـلـتـسـيـسـ هـنـإـفـ ،ـكـلـذـعـمـ وـx.x.x.x لـشـافـلـاـ مـاـخـلـاـ ئـلـاـ ئـقـداـصـ tacacs
مـداـخـلـ ئـعـومـجـمـلـ aaa.

ةلص تاذ تامولع

- Cisco نم فیکتلل قلباقلا نامآلا ۆزهجأ مع دەھفص Cisco ASA 5500 Series Adaptive Security Appliances
 - Cisco نم ۆلەدەنەنامآلە لولح ۆزهجأ رىدم Cisco ASA 5500 Series Command References
 - IKE تالوکوتورب/IPsec ۆضواقام مع دەھفص Cisco نم ۆلەدەنەنامآلە لولح ۆزهجأ رىدم
 - Windows ليغشتلا ۆمظنآل Cisco نم نەمآلە لوصولاييف مەكتىلا مداخ تاقىلىعتلا تابلط (RFCs)
 - Cisco Systems - تادىنسىسسەملەوينقىتلا مع دەل Cisco ASA 5500 Series Adaptive Security Appliances

هـ لـ وـ لـ جـ رـ تـ لـ اـ هـ ذـ هـ

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