

ACS 5.2 مادختساب EAP-FAST و PEAP نيوكت و WLC

تايوتحمل

- [عمدقمل](#)
- [عيساسأل تابلطمل](#)
- [تابلطمل](#)
- [عمدختسمل تانوكمل](#)
- [تاحالطصال](#)
- [نيوكتل](#)
- [كبشليل يطيختل مسرل](#)
- [تاضارتفا](#)
- [نيوكتل تاوطخ](#)
- [RADIUS مداخل نيوكت](#)
- [كبشلا دراوم نيوكت](#)
- [نيمدختسمل نيوكت](#)
- [عسايسل رصانع فيرعت](#)
- [لوصول تاسايس قيبط](#)
- [\(WLC\) عكلسلاللا عيلحمللا كبشلا يف مكحتللا رصنع نيوكت](#)
- [ليصافات مادختساب \(WLC\) عكلسلاللا عيلحمللا كبشلا يف مكحتللا رصنع نيوكتب مق](#)
- [عقداصمل مداخل](#)
- [\(VLANs\) عكيمانيدلا تاهاولا نيوكت](#)
- [WLAN \(SSID\) تاكلش نيوكت](#)
- [عدعاسمل Wireless Client عادأ نيوكت](#)
- [PEAP-MSCHAPv2 \(user1\)](#)
- [EAP-FAST \(user2\)](#)
- [عحصلل نم ققحتل](#)
- [1 \(PEAP-MSCHAPv2\) مدختسمل نم ققحتل](#)
- [2 \(EAP-FAST\) مدختسمل نم ققحتل](#)
- [اهالصل او عاطخاللا فاشكتسا](#)
- [اهالصل او عاطخاللا فاشكتسا رماوأ](#)
- [قلص تاذا تامولعم](#)

عمدقمل

- [\(WLC\) عكلسلاللا عيلحمللا كبشلا يف مكحتللا عدحو نيوكت عيفيك دننتسمل اذه حرشي](#)
- [مدخل لثم يجراخ RADIUS مداخل مادختساب \(EAP\) عسوتمللا عقداصمل لوكوتورب عقداصمل](#)
- [5.2 \(ACS\) لوصوللا يف مكحتللا](#)

عيساسأل تابلطمل

تابل طتم ل

نيوكتلا اذه ةل و احم لبق ةيلالاتلا تابل طتم ل ءافيتسا نم دكأت

- (ينث) ةطقن ذفنم نزو فيفخو WLC ل نم ةيساسأل ةفرعم يقلت ي
- AAA مداخل ةيفيظو ةفرعم
- يكلسال ل نامأل تالكشم و ةيكلسال ل تاكلابل ةلماش ةفرعم

ةمدختسم ل تانوكم ل

ةيلالاتلا ةيدام ل تانوكم ل و احم ل رادصل ل دن تسم ل اذه في ةدراول تامولعمل دن تست

- Cisco 5508 WLC رادصل ل ، تباثل احم ل رابل لغشي يذلا Cisco 5508 WLC
- Cisco 3502 Series LAP ةلسلس ل نم Lightweight عضول في لوصول ةطقن
- Intel ليغشتلا احم ل رعب عم Microsoft Windows 7 ليغشتلا ماظنل لصلأل احم ل رابل ل 14.3 رادصل ل 6300-N
- Cisco 5.2 رادصل ل لغشي يذلا Cisco نم نم آلل فيفاضل ل يوتحمل رصم
- Cisco 3560 Series Switch ل و حمل

ةصاخ ةيلمعم ةئيبي في ةدوومل ةزهجال نم دن تسم ل اذه في ةدراول تامولعمل ءاشنإ مت تناك اذ. (يضا رتفا) حوسمم نيوكتب دن تسم ل اذه في ةمدختسُم ل ةزهجال ءي م اءب رمل آل لم تحمل ريثأتلل كمهف نم دكأت ف ، ةرشابم كتك ب ش

تاحال طصال

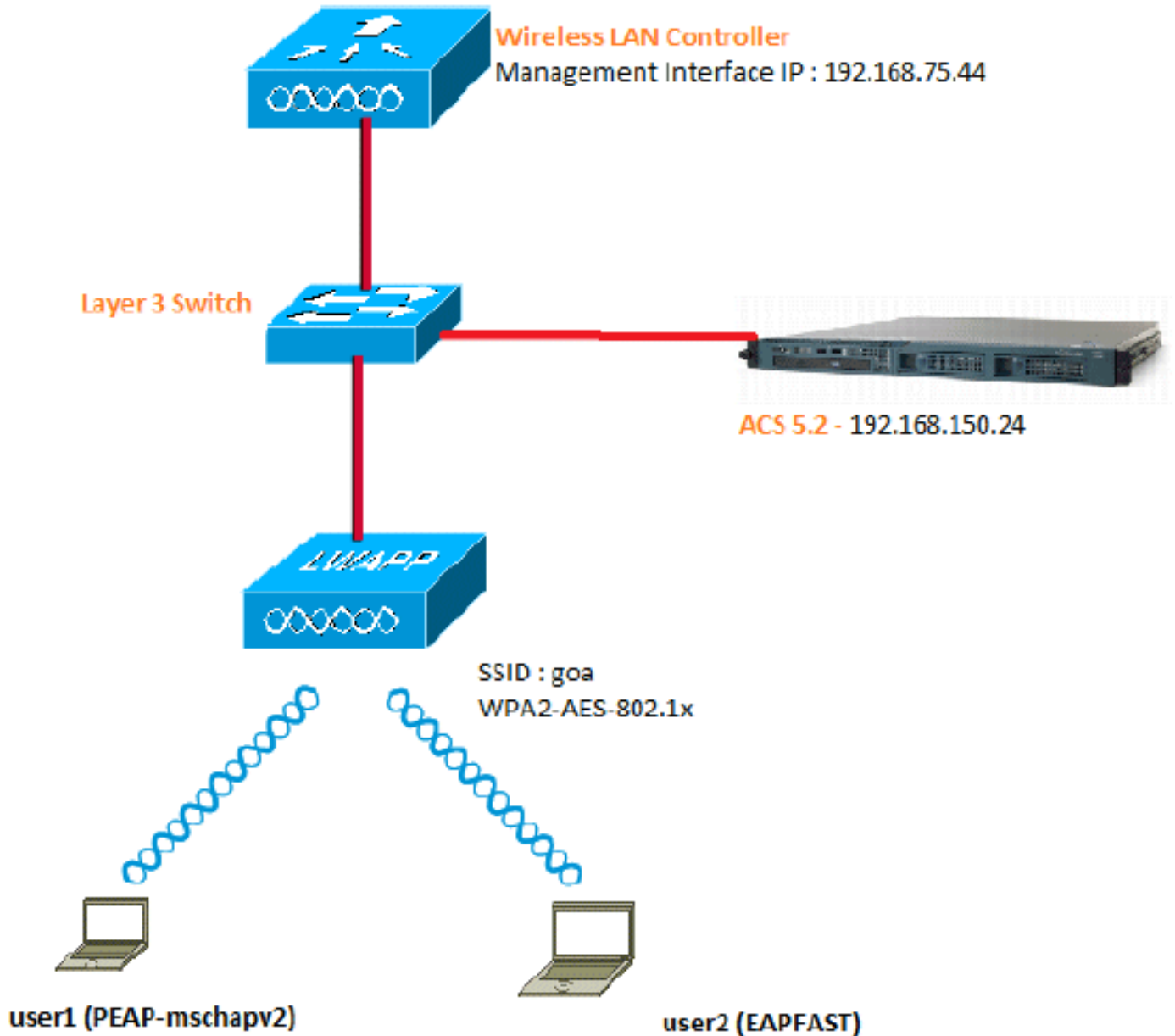
[تاحال طصال ل و احم ل عمل ل نم ديزم ل ل و صل ل ةينقتلا Cisco تاحيملت تاحال طصال عجار تادنتسمل](#)

نيوكتلا

دن تسم ل اذه في ةحضوم ل تازيمل نيوكت تامولعمل كل مّ دقت ، م سقلا اذه في نم ديزم ل ل و صل ل (طقف [نيلجسمل](#) ءالمعل) [رملوأل شحب ءادأ](#) م دختسأ : ةظالم م سقلا اذه في ةمدختسمل رملوأل ل و صل ل تامولعمل

ةكبش ل ل يطي طختلا مسرل

يلالاتلا ةكبش ل دادع دن تسم ل اذه م دختسي



ططخملا اذه يف ةمدختسملا تانوكملا نيوكت لي صافات يه هذه

- 192.168.150.24. وه ACS (RADIUS) مداخ صاخلا IP ناوع
- ةيلحملا ةكبشلا يف مكحتلا ةدحوب ةصاخلا AP-Manager و ةرادلا ةهجاو ناوع
192.168.75.44. وه (WLC) ةيكلساللا
- 192.168.150.25. DHCP مداخ ناوع
- س فنب ني مدختسملا الك لصتي. نيوكتلا اذه ربع VLAN 253 ةكبش مادختسا متي
PEAP-MSCHAPv2 و user2 مادختساب ةقداصملا 1 مدختسملا نيوكت متي، كلذ عم و SSID فرعمل "goa"
- 253: مقرر VLAN ةكبش يف ني مدختسملا نييعت متيس
- 192.168.153.1: ةباوبلا. 192.168.153.x/24: VLAN 253 ةكبش
- 192.168.75.1: ةباوبلا. 192.168.75.x/24: VLAN 75 ةكبش

تاضارتفا

- 3 VLANs ةقبط لك لحاتفم تللكش
- DHCP مداخل DHCP قاطن نييغت مت
- ةكبشلا يف ةزهجالا عيجم نيب 3 ةقبطلا لاصتا دجوي
- ةيلحمل ةكبشلا يف مكحتلا ةدحوب لعفلاب ةلصتم (LAP) لوصولا ةطقن (WLC) ةيكلساللا
- عانق /24 لىل ةكبش لك يوتحت
- ةتبتم ايتا ةعقوم ةداهش لىل ACS 5.2 يوتحي

نيوكتلا تاوطخ

يوتسمل ةيلع تاوطخ ثالث لىل نيوكتلا اذه مييسقت متي

1. [RADIUS مداخل نيوكتب مق](#)
2. [WLC لىل تللكش](#)
3. [يكلساللا ليملل ةدعاسملا ةادالا نيوكتب مق](#)

RADIUS مداخل نيوكت

تاوطخ عبرا لىل RADIUS مداخل نيوكت مييسقت متي

1. [ةكبشلا دراوم نيوكتب مق](#)
2. [نيمدختسمل نيوكتب مق](#)
3. [ةسايسلا رصانع فيرعت](#)
4. [لوصولا تاسايس قيبت](#)

جذومن مدختسي ACS 5.x نأ ي. ةسايسلا لىل ةمئاق لوصولا يف مكحتلل ماطن وه ACS 5.x تارادصا يف مدختسمل ةعومجم لىل دننتسمل جذومنلا نم ال دب دعاوق لىل دننتسم ةسايس 4.x.

نم ديزمب مستت لوصولا لىل ةرطيسي ACS 5.x دعاوق لىل ةمئاقلا تاسايسلا جذومن رفويو. تاوعومجم لىل ةمئاقلا ميذللا جهنلاب ةنراقم ةنورملاو ةوقلا

عاونأ ةثالث لىل يوتحت اهانل جهنلا ةعومجم دحت، ةعومجم لىل دننتسمل مدقألا جذومنلا يف اهانب طبرتو تامولعمل نم

- وأ AD تاوعومجم يف ةيوضعلا لىل تامولعمل اذه دننتست نأ نكمي - ةيوهلا تامولعمل نييلخادلا ACS يمدختسمل تباث نييغت وأ LDAP

• كلذى الامو ءزهجألا دويقو تقولا دويق - ىرخأ طورش وأ دويق

• Cisco IOS® تازايتما تايوتسم وأ VLAN تاكبش - تانوذألا

جذومنلا دعاوق ىلا ACS 5.x ءسايس جذومن دننسي

• ءچيتن ءلاجل تناك اذا

ءوعومج ىلا دننسملا جذومنلل ءفوصوملا تامولعملل مدختسن ،لاثلما لىبس ىلع

• لىوختلا فىرت فلم مئ دىقت طرش وأ ءوه ءلاحو ءوحو ءلاحو فى

ىلا لوصولاب مدختسملل حمسي يتلا طورشلل دىحتل ءنورم اءه انل رفوي ،كلذل ءچيتنو ءنيعم طورش ءافيتسا دنن ءه حومسملا لىوختلا يوتسم ىلا ءفاضلااب ءكبشلا

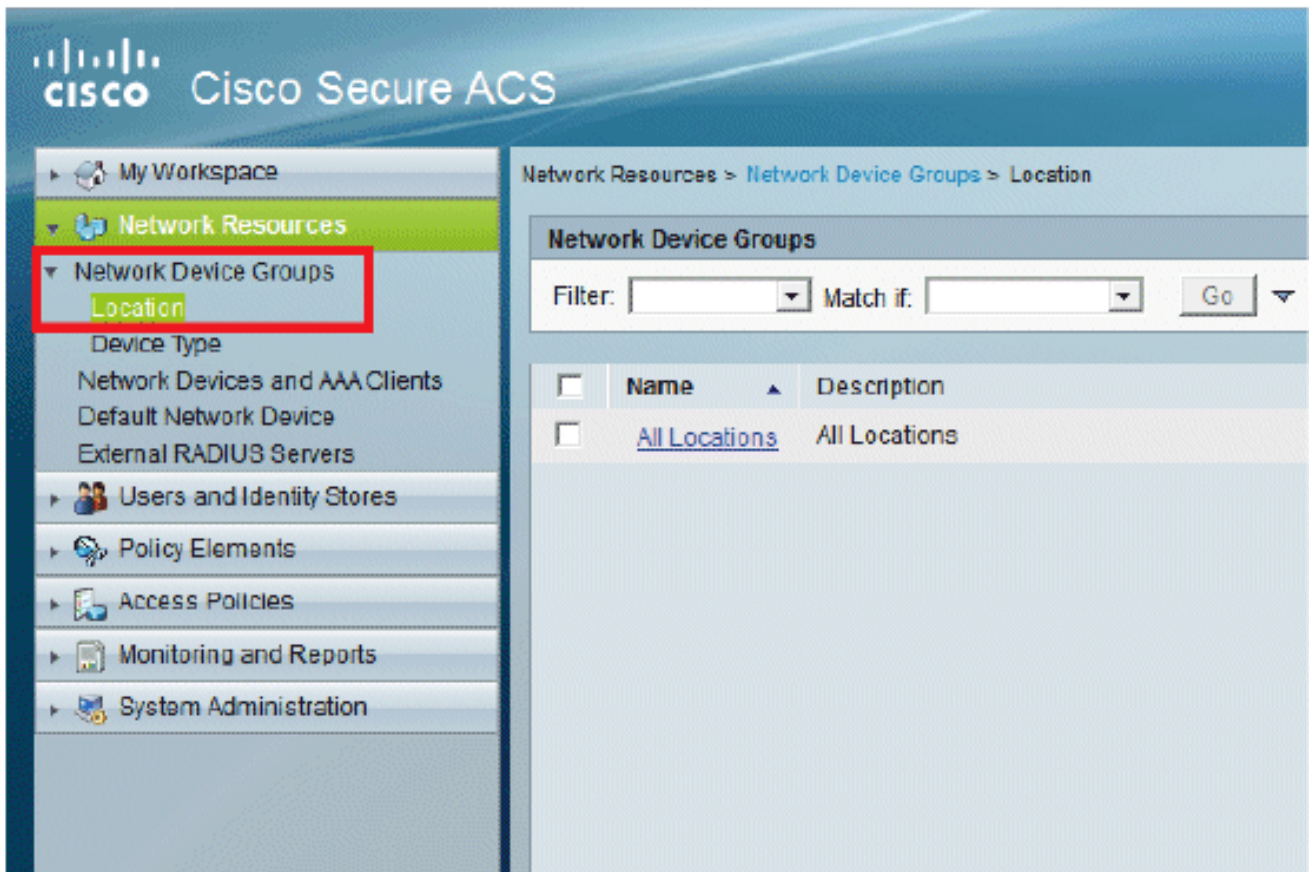
ءكبشلا دراوم نيوكت

RADIUS مءاخ ىلع WLC ل AAA لىم ءنيوكتب موقن ،مسللا اءه فى

(WLC) ءىكلساللا ءىلحملا ءكبشلا فى مءحتلا رصنع ءفاضل ءىففى ءارجلا اءه حرشى ءىلحملا ءكبشلا فى مءحتلا رصنع ررمت نأ نكمى ىتح RADIUS مءاخ ىلع AAA لىمءك RADIUS مءاخ ىلا مدختسملا ءامتعا تانايب (WLC) ءىكلساللا

ءىلاتلا تاوطلال لمكأ

1. ءزهجأ تاعومجم > ءكبشلا دراوم ىلا لقتنا ،(ACS) ءىموسرلا مدختسملا ءهجاو نم (لفسألا فى) ءاشنأ قوف رقناو ،ءقوملا ءكبشلا



2. لاسرا قوف رقناو، ةبولطملا لوقحلا ةفاضاب مق

Network Resources > Network Device Groups > Location > Create

Device Group - General

Name:

Description:

Parent:

☼ = Required fields

ةشاشلا هذه نآلا ىرتس:

CISCO Cisco Secure ACS

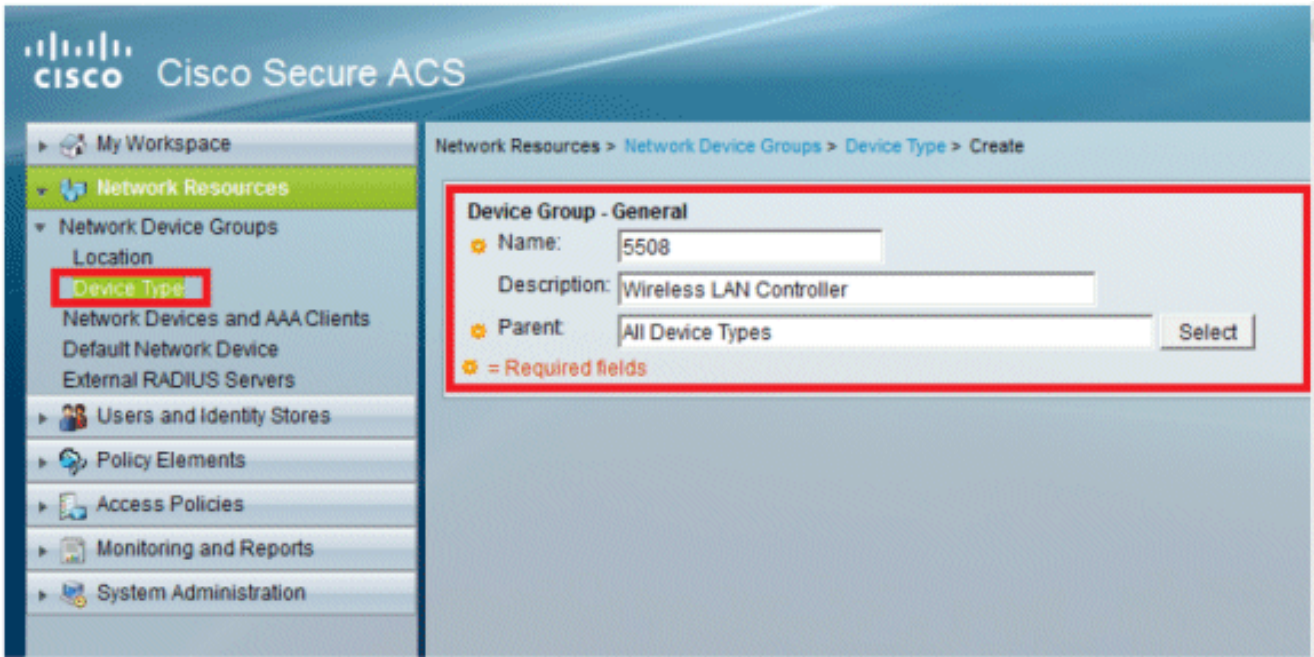
Network Resources > Network Device Groups > Location

Network Device Groups

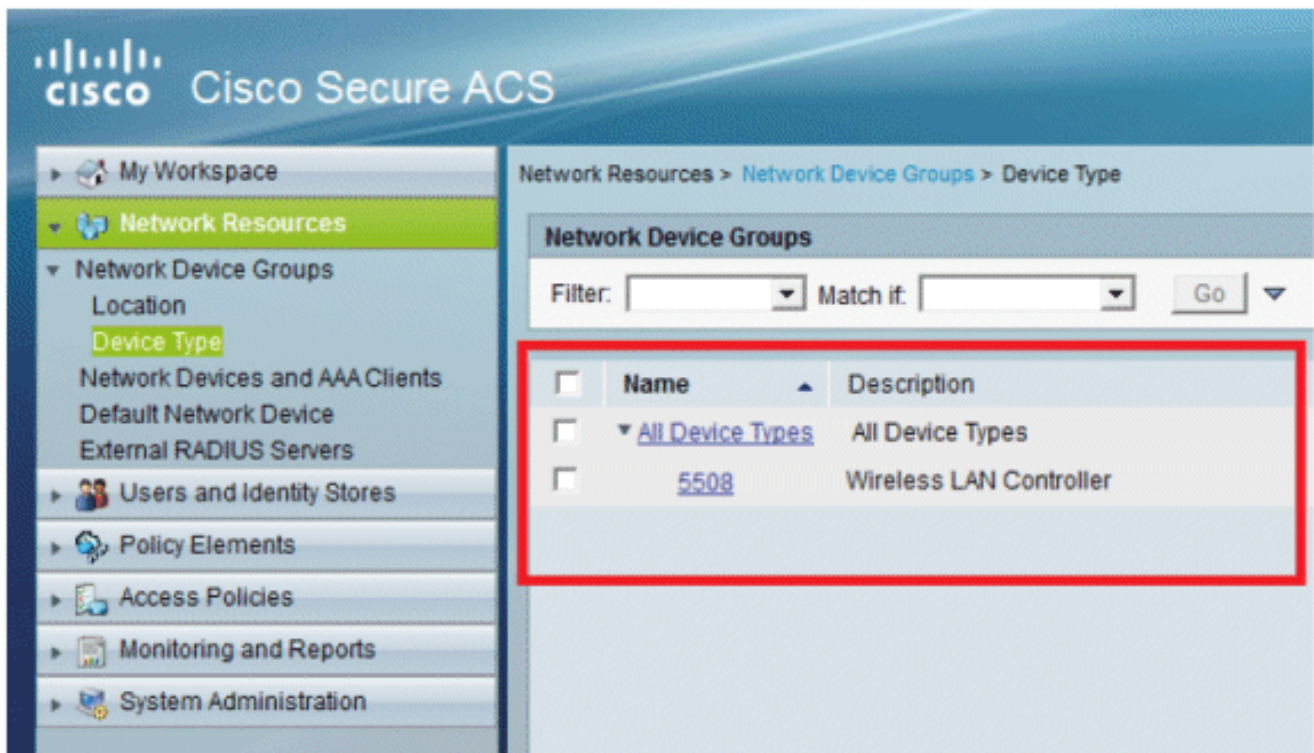
Filter: Match if:

<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	▼ All Locations	All Locations
<input type="checkbox"/>	LAB	LAB Devices

3. ءاشنإ > زاھجلا عون قوف رقنا



4: شاشة الالهة نآلآ ىرتس .لاسرا ىلع رقنا



5. AAA ءالمعو ءكباشلا ءزهجأ > ءكباشلا دراوم ىلآ لقتنا

6: انه حضوم وه امك لىصافتلا ءئبعتب مقو ،ءاشنا قوف رقنا

My Workspace

Network Resources

Network Device Groups

Location

Device Type

Network Devices and AAA Clients

Default Network Device

External RADIUS Servers

Users and Identity Stores

Policy Elements

Access Policies

Monitoring and Reports

System Administration

Network Resources > Network Devices and AAA Clients > Create

Name: WLC-5508

Description: Wireless LAN Controller

Network Device Groups

Location: All Locations:LAB [Select]

Device Type: All Device Types:5508 [Select]

IP Address

Single IP Address IP Range(s)

IP: 192.168.75.44

Authentication Options

TACACS+

RADIUS

Shared Secret: cisco

CoA port: 1700

Enable KeyWrap

Key Encryption Key: []

Message Authenticator Code Key: []

Key Input Format ASCII HEXADECIMAL

Required fields

7: ةشاشلا هذه نآلا ىرتس .لاسرلا ىلع رقنا

Network Resources > Network Devices and AAA Clients

Network Devices

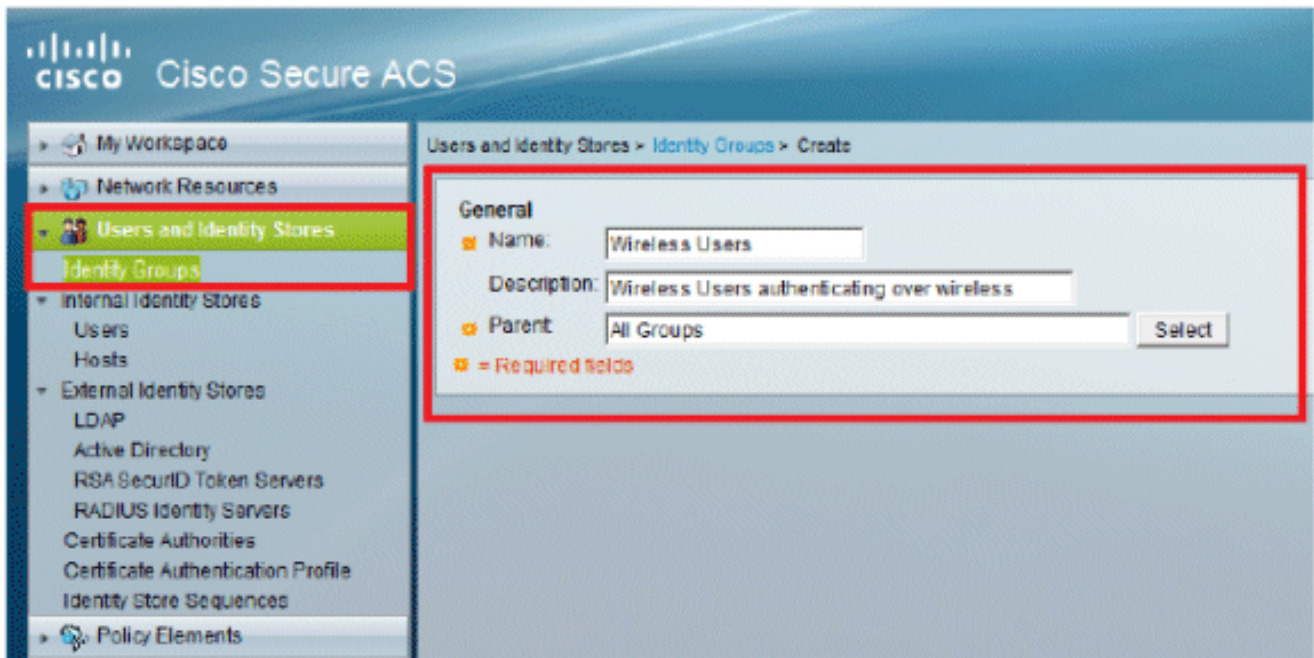
Filter: [] Match it: [] Go: []

<input type="checkbox"/>	Name	IP / Mask	NDG:Location	NDG:Device Type	Description
<input type="checkbox"/>	WLC-5508	192.168.75.44/32	All Locations:LAB	All Device Types 5508	Wireless LAN Controller

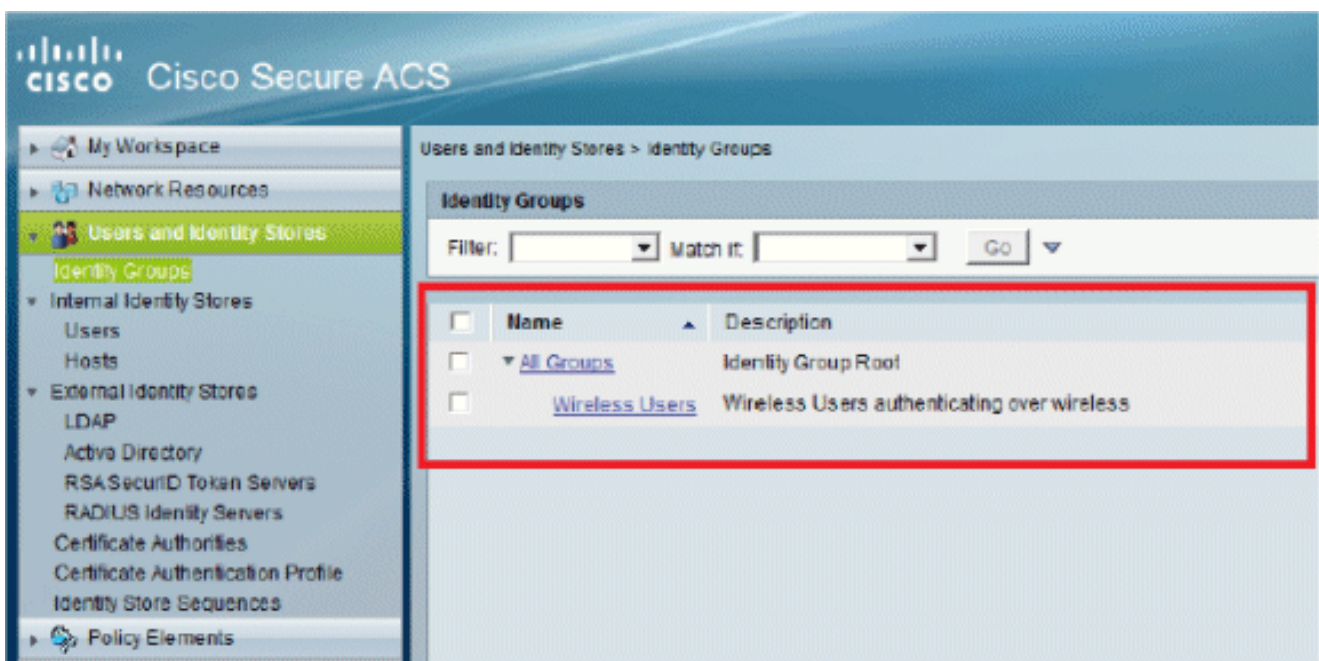
نيم دختسم لال نيوكت

نيم دختسم لال الك نييعت مت ACS. ىلع نييلحم نيم دختسم ئشننس ،مسقلا اذه يف "نويكلساللا نوم دختسم لال" ىمست ةومجم يف (user1 و user2).

1. ءاشنإ > ةيوهلا تاعومجم > ةيوهلا نزاخم و نيم دختسم لال ىلا لقتنا



2. يلى امك ءحفص لى وءبءس ، لاسرل قوف رقنلا ءرءم



3. نىءءءءس لى ءومءم ل مهنىىءءب مق و ، user1 و user2 نىءءءءس مءشنل مق "نىىكلس لى".

Create.a > نىءءءءس لى > ءىوه لى ءاعومءم > ءىوه لى نءءم و نىءءءءس لى قوف رقنل

Cisco Secure ACS

Users and Identity Stores > Internal Identity Stores > Users > Create

General

- Name: user1 Status: Enabled
- Description: PEAP:mschapv2 users
- Identity Group: All Groups:Wireless Users

Password Information

Password must:

- Contain 4 - 32 characters

Change password on next login

User Information

There are no additional identity attributes defined for user records

* = Required fields

user2.b. عاشناب مق، لثملاب

Cisco Secure ACS

Users and Identity Stores > Internal Identity Stores > Users > Create

General

- Name: user2 Status: Enabled
- Description: EAPFAST user
- Identity Group: All Groups:Wireless Users

Password Information

Password must:

- Contain 4 - 32 characters

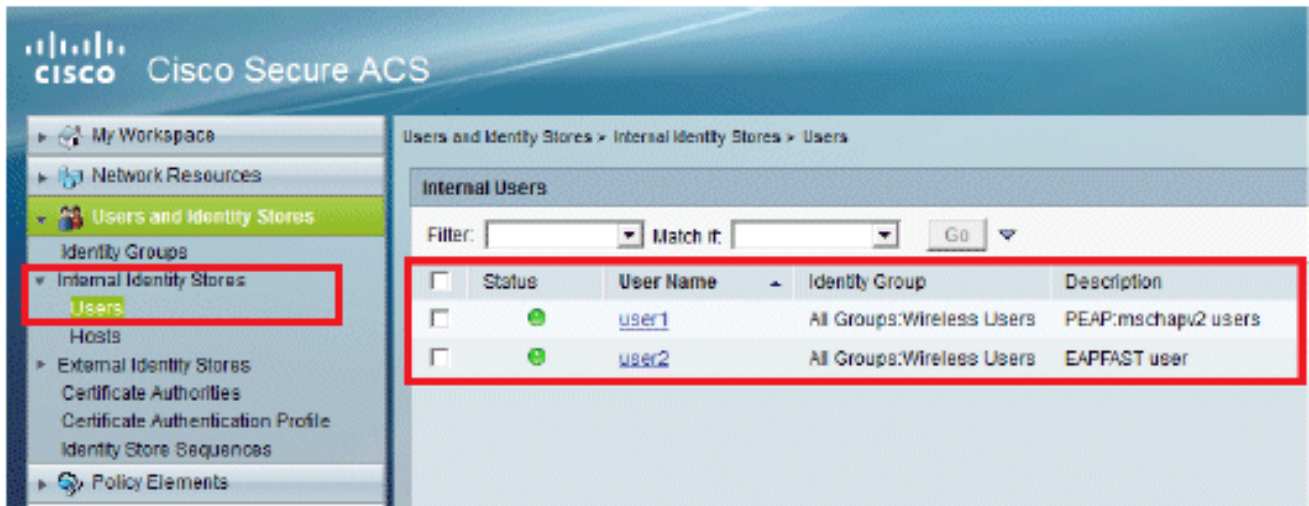
Change password on next login

User Information

There are no additional identity attributes defined for user records

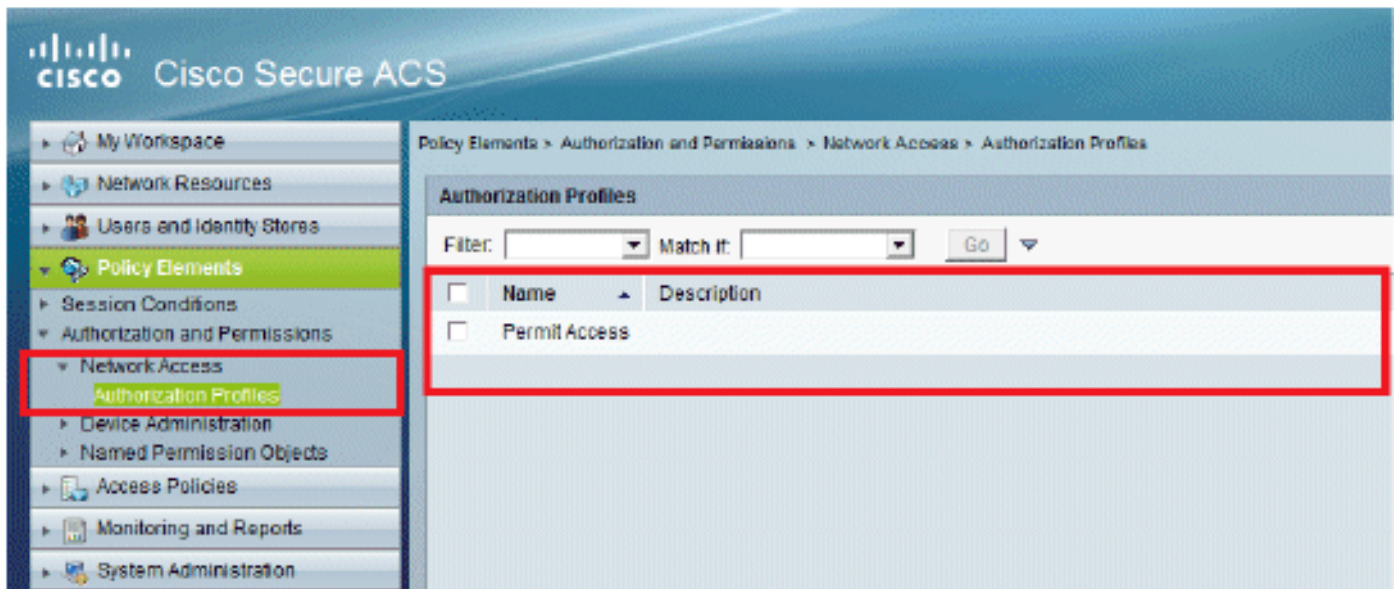
* = Required fields

يولي امك ةشاشلا ودبتس:



ةساي سلال رصانع فيرعت

لوصولاب حام سلال نييعت نم ققحت

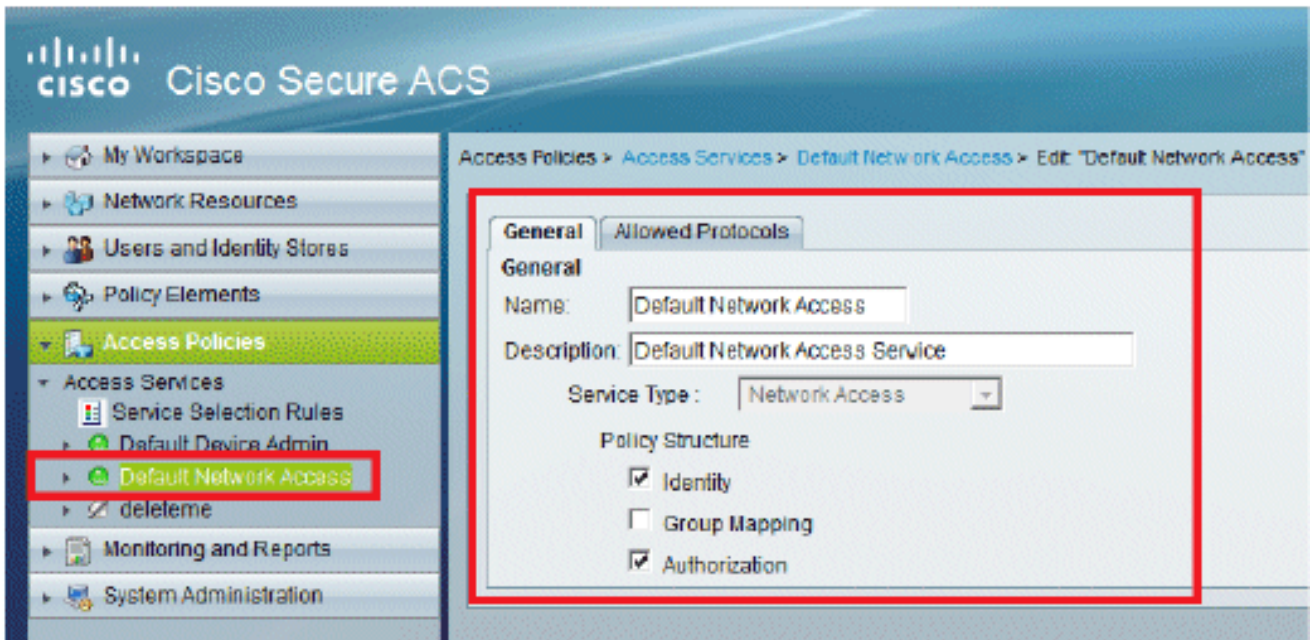


لوصولا تاسايس قي ببط

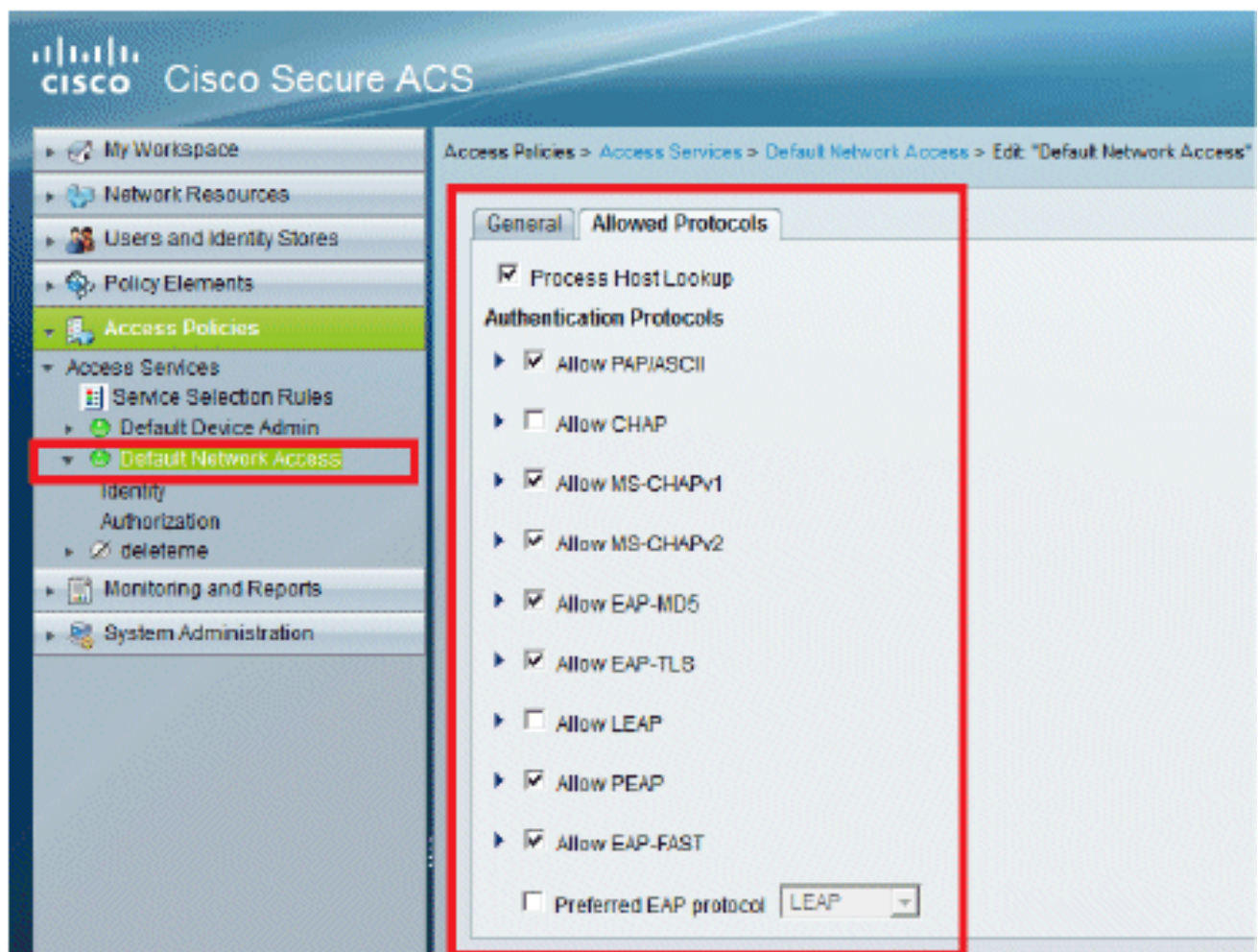
ئشننس. دعاوقلا نيوك تة فيكي واهم ادختس ا دارملا ةقداصلما قرط ددحنس، مسقلا اذ في ةقباسلا تاوطخلا لىل دن تست دعاوق

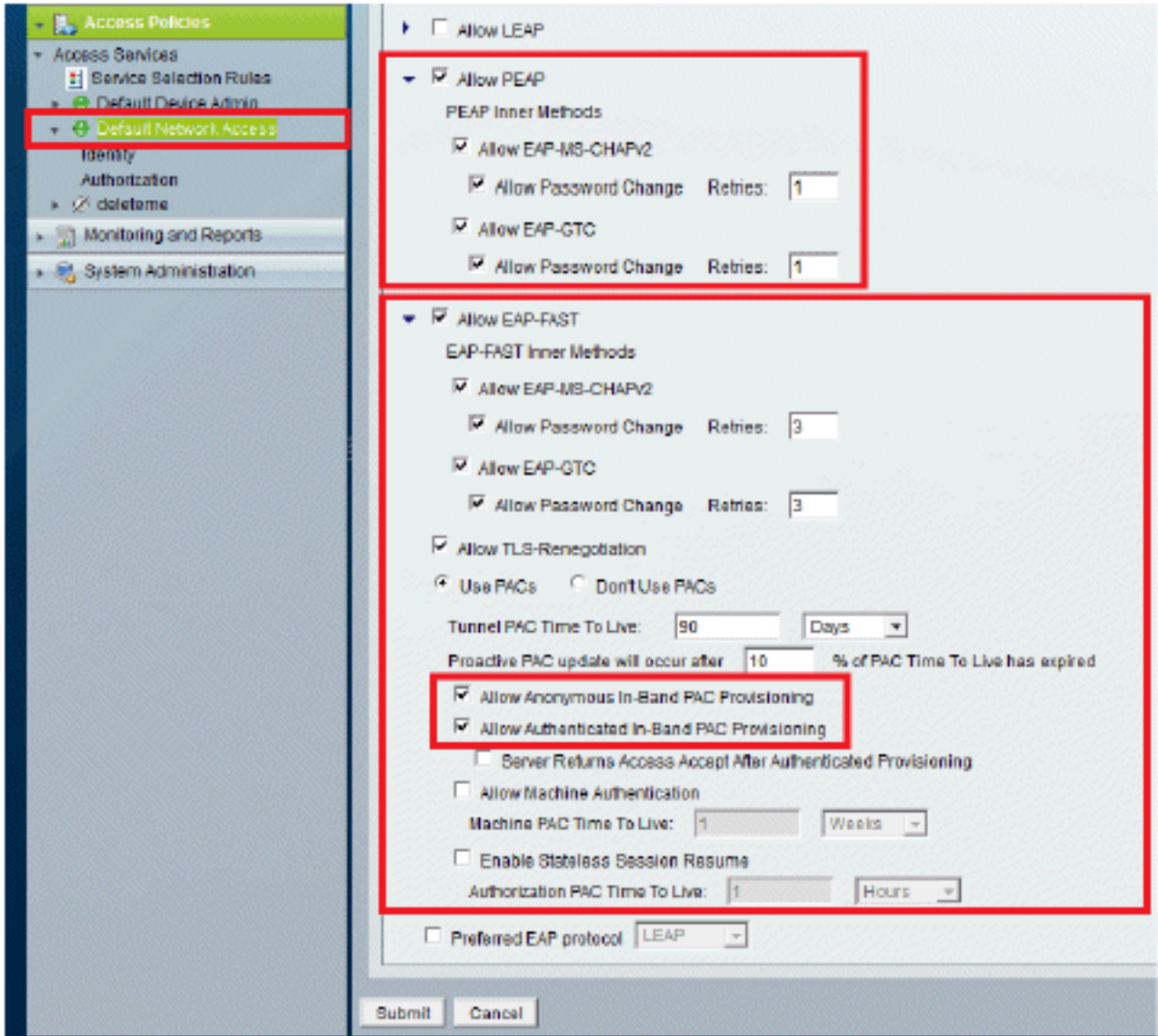
ةيلاتلا تاوطخلا لمكأ

1. لىل يضا رتفالا لوصولا > لوصولا تامدخ > لوصولا تاسايس لىل لقتنا "ةكبشلا لىل يضا رتفالا لوصولا": ريرحت > ةكبشلا



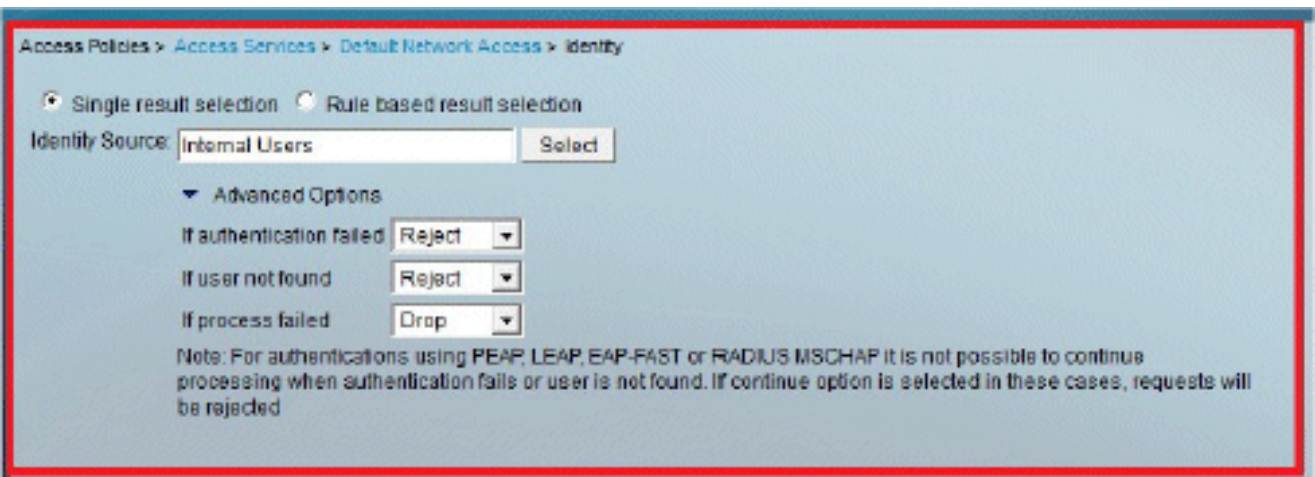
2. لثاملا اذه في .هيلع نيكيكلساللا عالمعلا ةقداصم ديرت يذلا EAP بولسأ دح
EAP-FAST و PEAP-MSCHAPv2 مدختسن





3. لاسر اىل عرقنا

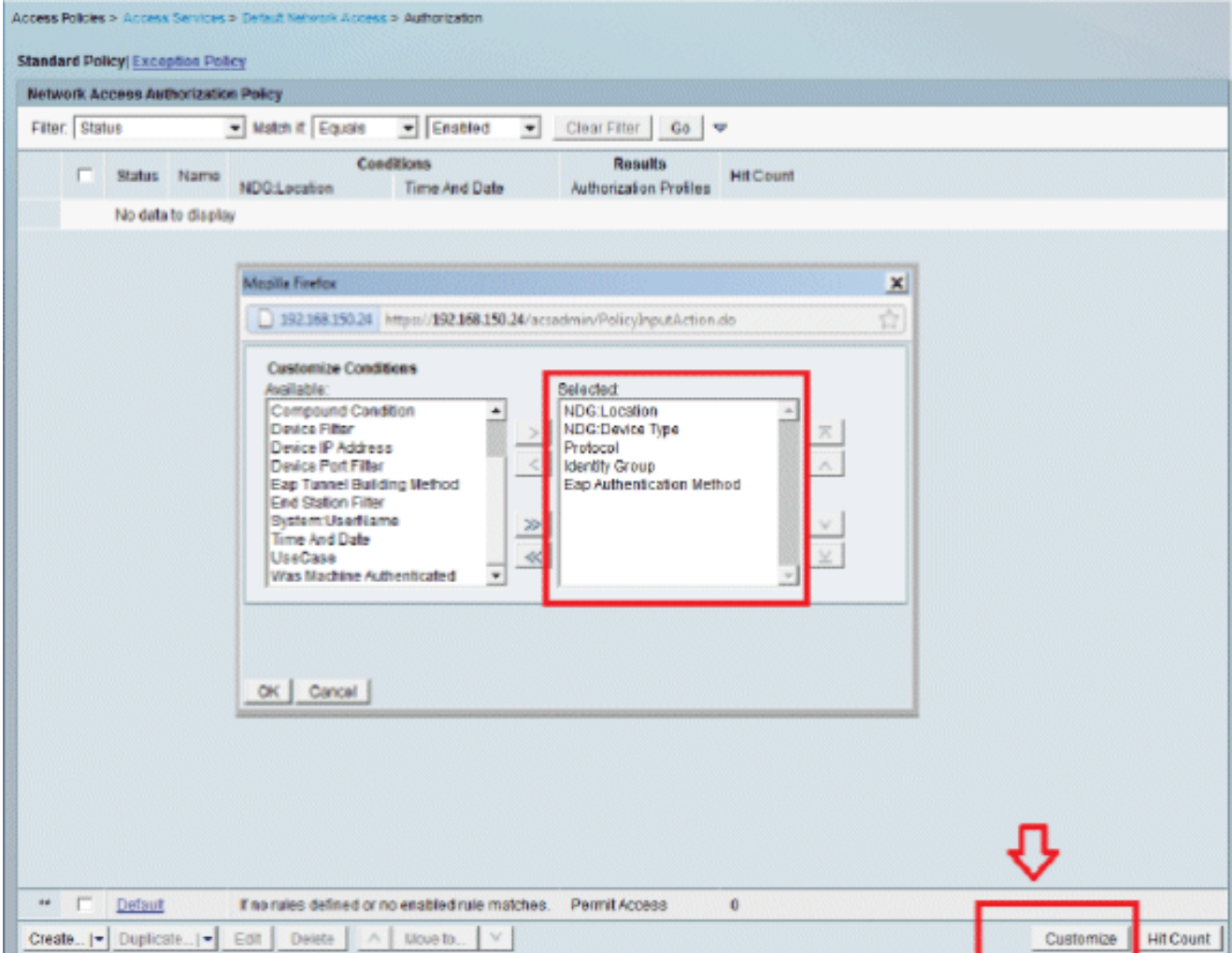
4. نى مدخست سمل مدختسن، لالم اذ ف. اهتدح يتلا ةيوهال ةومجم نم ققحت تاريغتل ظفح ب مق ACS. لىل هاناشنأ يذلا، نىلخالدا



5. ماتدخ > لوصول تاسايس لىل لقتنا، لىل وختل فىرعت فلم نم ققحتلل

ليوختلا > كة بشلا لى لى اضارت فالال ووصولال ووصولال

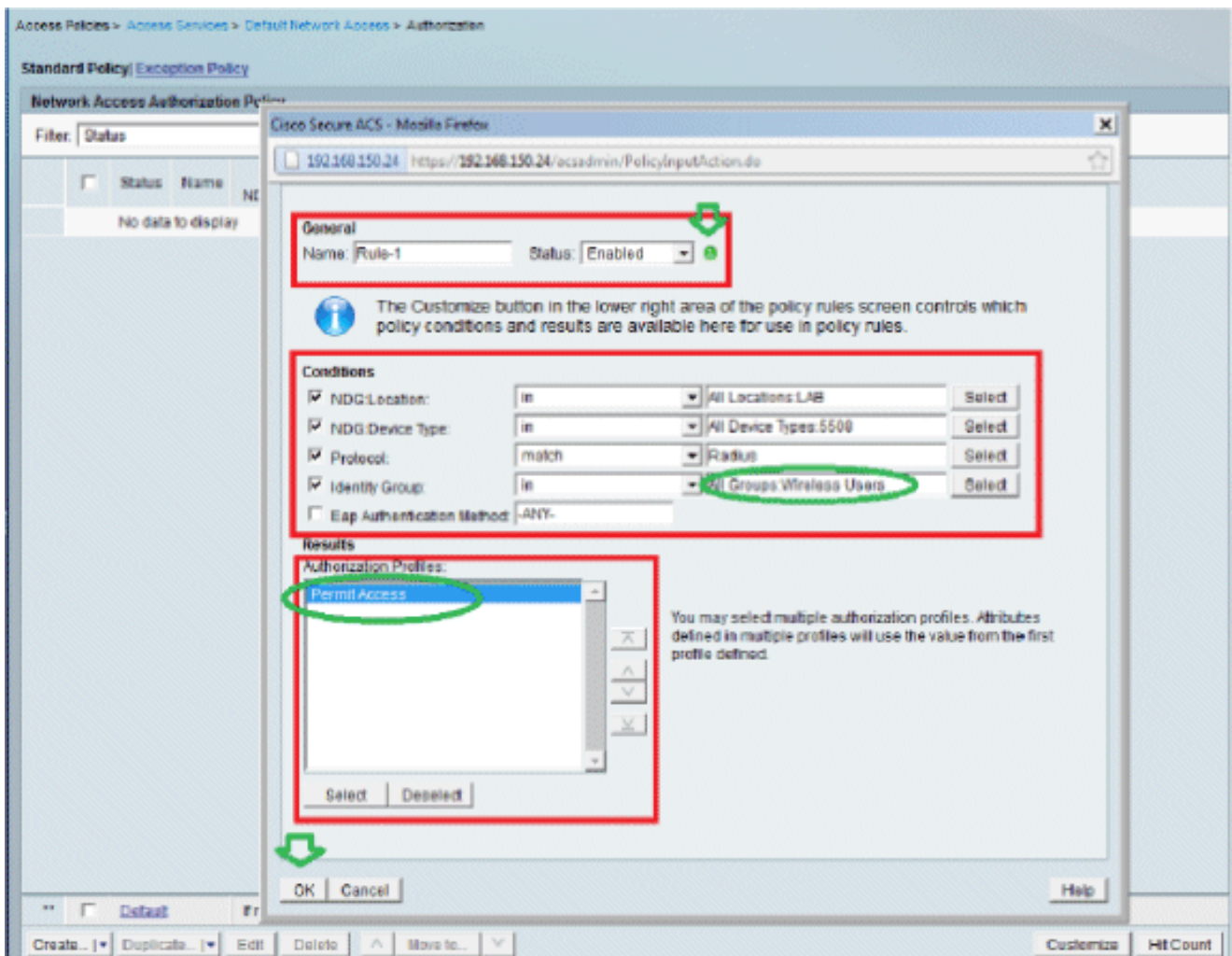
ياو كة بشلا لى لى ووصولال مدختس ملل حيتتس طورش يا تحت صيصختلا كنكمي
ةيلبالا هذه رفوتت الو. هيلع ةقداصلال درجمب هررمتس (تامس) ليوخت فيصوت
زاهجال عونو، عقومال ديحتب انمق، لاثمال اذف ACS 5.x في الال ليدعتلل
EAP ةقداصلم بولسأو، ةيوهال ةعومجم، لوكوتوربال



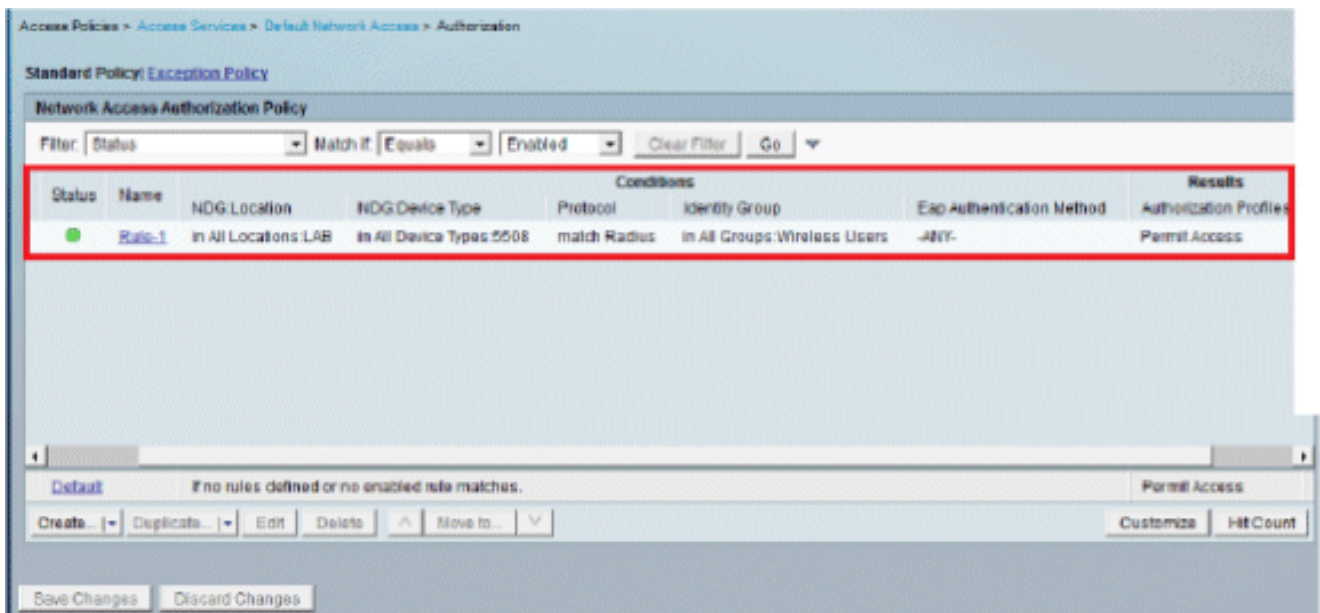
6. تاريغتلال ظفحالمث، قفاوم قوف رقنا

7. حامسلا متي، دعاوق ةيا فيرعت متي مل اذ. ةدعاق عاشنل يا في ةيلالاتلا ةوطخلال لثمتت
طورش ةيا نود لوصولال ليمعلل

ةعومجم في ني مدختس ملاب ةصاخ ةدعاقلال هذه 1- ةدعاقلال > عاشنل قوف رقنا
"نيكلسالال ني مدختس ملال"



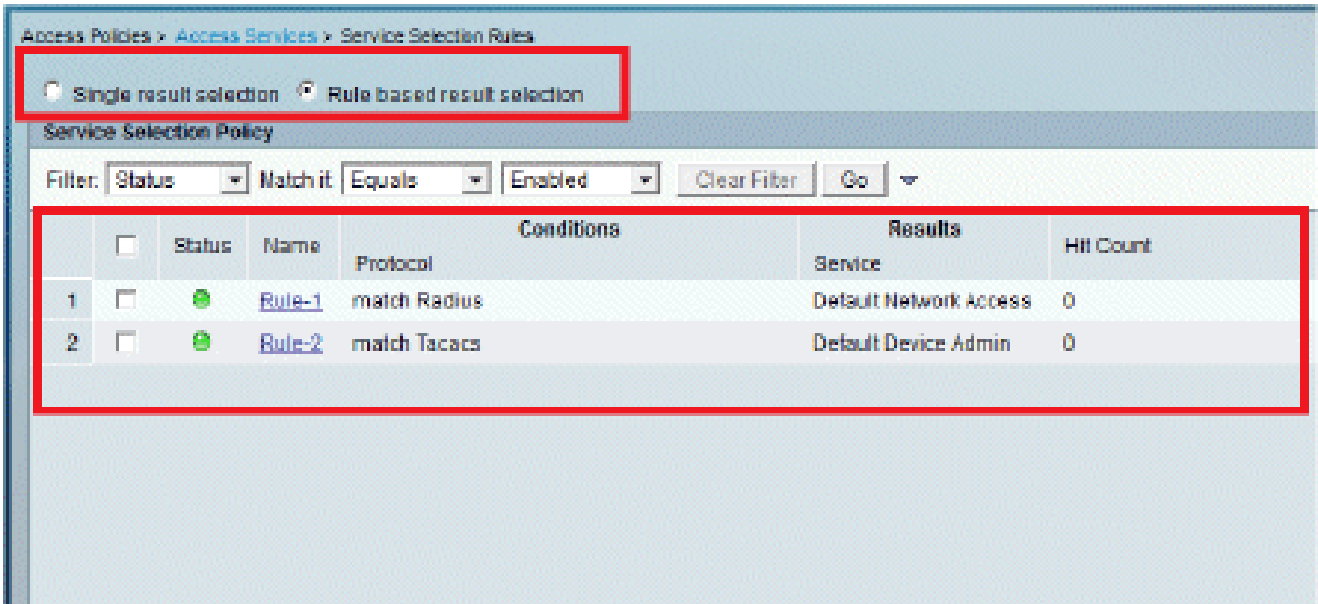
8: يلى امك ءشاشلا ودبت س . تاريغيغلا ظفح ب مق



ريحت ب مق ف ، طورشلا عم نوقباطتي ال نى ذل نى مدخت س م ل ا ض ف ر ي ف ب غرت تنك اذ ا
 "لوصول ا ض ف ر" لوقلل ءيضا رت ف ال ا ءءاق ل ا

9: و ا ط ي س ب ح ن ن ي و ك ت ل ء ح ف ص ل ا ه ذ ه م د خ ت س ا . ء م د خ ل ل ر ا ي ت خ ا ء ع ا و ق ء ي د ح ت ب ن ا ل ا م و ق ن س

اذه يف .ة دراوالا تا بل لطلال ىلع اهق يبطت متيس يتلا ةمدخلال ديحتل دعاقو ىل دنتم دعاقو ىل دنتم ةسايس مادختسا متي ،لا ثمل



ةيكل سلالا ةيحلح ملاء ةكبشلا يف مكحتلا رصنع نيوكت (WLC)

ةيلالاتلا تاوطخال نيوكتلا اذه بلطتي

1. [مادختساب \(WLC\) ةيكل سلالا ةيحلح ملاء ةكبشلا يف مكحتلا رصنع نيوكت مق ةقداصملا مداخل ليصافت](#)

2. [\(VLANs\) ةيكل يمانيدلا تاهاجاولا نيوكت مق](#)

3. [WLAN \(SSID\) تاكبش نيوكت](#)

(WLC) ةيكل سلالا ةيحلح ملاء ةكبشلا يف مكحتلا رصنع نيوكت مق ةقداصملا مداخل ليصافت مادختساب

هنكمي ىتح (WLC) ةيكل سلالا ةيحلح ملاء ةكبشلا يف مكحتلا رصنع نيوكت يرورضلا نم ىرخأ تاكح يأل كلذكو ،ءالمعلا ةقداصم RADIUS مداخل لاصتالا

ةيلالاتلا تاوطخال لمكأ

1. نامألا قوف رقنا ،مكحتلا ةدحول (GUI) ةيموسرلا مدختسملا ةهجاو نم

2. مداخل نيپ مدختسملا كرتشملا ىرسلا حاتفملاو RADIUS مداخل صاخلا IP ناو نع لخدأ RADIUS و WLC.

مداخل يف هنيوكت مت يذلا هسفن وه كرتشملا ىرسلا حاتفملا اذه نوكي نا بجي RADIUS.

The screenshot shows the Cisco WLC configuration interface for adding a new RADIUS Authentication Server. The page is titled "RADIUS Authentication Servers > New". The configuration fields are as follows:

- Server Index (Priority): 1
- Server IP Address: 192.168.150.24
- Shared Secret Format: ASCII
- Shared Secret: [Redacted]
- Confirm Shared Secret: [Redacted]
- Key Wrap: (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
- Port Number: 1812
- Server Status: Enabled
- Support for RFC 3576: Enabled
- Server Timeout: 2 seconds
- Network User: Enable
- Management: Enable
- IPSec: Enable

(VLANs) ةيكيما نيدلا تاهجاو ال نيوكت

WLC ال ىلع يكرح نراق لكشي نأ فيك عارج اذه فصبي

ةةلاتلا تاوطخلا لمكأ

1. ةدحوب ةصاخلا (GUI) ةيموسرلا مدختسملا ةهجاو نم ةيكيما نيدلا ةهجاو ال نيوكت مت تاهجاو ال > مكحتلا ةذفان في ، مكحتلا

The screenshot shows the Cisco WLC configuration interface for adding a new interface. The page is titled "Interfaces > New". The configuration fields are as follows:

- Interface Name: vlan253
- VLAN Id: 253

2. قېبىت قوف رونا

(انه 253 VLAN) يكر نراق اذه نم ءذفان ريرحتلا لىل كللقني اذه

3. ءيكي مانيدلا ءه جاولا هذهل ءيضا رتفالا ءباول او IP ناووع لخدأ

The screenshot shows the Cisco Controller configuration interface for the 'CONTROLLER' tab. The left sidebar lists navigation options like General, Inventory, Interfaces, etc. The main content area is titled 'Interfaces > Edit' and shows configuration for 'vlan253'. The 'Interface Address' section is highlighted with a red border and contains the following fields:

Interface Address	
VLAN Identifier	253
IP Address	192.168.153.81
Netmask	255.255.255.0
Gateway	192.168.153.1

Below this, the 'DHCP Information' section shows:

DHCP Information	
Primary DHCP Server	192.168.150.25
Secondary DHCP Server	

The 'Access Control List' section shows:

Access Control List	
ACL Name	none

A note at the bottom states: 'Note: Changing the interface parameters causes the VLANs to be temporarily disabled and thus may result in loss of connectivity for some clients.'

4. قېبىت قوف رونا

5. يلى امك اهنوك مت ي تلال تاه جاولا و دبتس

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management
management	75	192.168.75.44	Static	Enabled
service-port	N/A	0.0.0.0	Static	Not Supported
virtual	N/A	1.1.1.1	Static	Not Supported
vlan253	253	192.168.153.81	Dynamic	Disabled

WLAN (SSID) تاكل بش نيوكت

ةي لحم لة اك بش لة ي ف مكحت لة رصنع ي ف WLAN تاكل بش نيوكت ةي فية ك ءارجل ا اذ حرش ي (WLC) ةي ك لس لة لة

ة: لة لة لة ا واطخ لة لم ك ا

1. WLAN تاكل بش لة لة لة قتنا ، مكحت لة ة دحوب ة صاخ لة (GUI) ةي م و سر لة مدخت س م لة ة ه ا و نم ة دي دج لة WLAN تاكل بش ة ذفان ضرع م تي . ة دي دج WLAN ة اك بش ءاش ن لة دي دج ءاش ن لة

2. WLAN SSID تام و لعم و WLAN فرعم ل خ د ا

ة اك بش لة SSID فرعم ك GOA ل ا ث م لة اذ مدخت سي . WLAN SSID م ساب م سا ي ا ل ا خ د ا ك ن ك م ي WLAN.

WLANs > New	
Type	<input type="text" value="WLAN"/>
Profile Name	<input type="text" value="goa"/>
SSID	<input type="text" value="goa"/>
ID	<input type="text" value="1"/>

3. WLAN goa لة نم ة ذفان edit لة لة لة تبه ذ in order to قبطي ة ققط

CISCO MONITOR **WLANS** CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

WLANS

- WLANS
- Advanced
 - AP Groups

WLANS > Edit 'goa'

General Security QoS Advanced

Profile Name goa
Type WLAN
SSID goa
Status Enabled

Security Policies [WPA2][Auth(802.1X + CCKM)]
(Modifications done under security tab will appear after applying the changes.)

Radio Policy All
Interface/Interface Group(G) vlan253

Multicast Man Feature Enabled
Broadcast SSID Enabled

CISCO MONITOR **WLANS** CONTROLLER WIRELESS SECURITY

WLANS

- WLANS
- Advanced

WLANS > Edit 'goa'

General **Security** QoS Advanced

Layer 2 Layer 3 AAA Servers

Layer 2 Security WPA+WPA2
 802.1X Filtering

WPA+WPA2 Parameters

WPA Policy
WPA2 Policy
WPA2 Encryption AES TKIP
Auth Key Mgmt 802.1X+CCKM

WLANs > Edit 'goa'

General Security QoS Advanced

Layer 2 Layer 3 AAA Servers

Select AAA servers below to override use of default servers on this WLAN

Radius Servers

Radius Server Overrides interface Enabled

	Authentication Servers	Accounting Servers
Server 1	<input checked="" type="checkbox"/> Enabled IP:192.168.150.24, Port:1812	<input checked="" type="checkbox"/> Enabled None
Server 2	None	None
Server 3	None	None

LDAP Servers

Server 1 None

Server 2 None

Server 3 None

Local EAP Authentication

Local EAP Authentication Enabled

Authentication priority order for web-auth user

Not Used Order Used For Authentication

WLANs > Edit 'goa'

General Security QoS Advanced

Allow AAA Override Enabled

Coverage Hole Detection Enabled

Enable Session Timeout

Aironet IE Enabled

Diagnostic Channel Enabled

IPv6 Enable

Override Interface ACL None

P2P Blocking Action Disabled

Client Exclusion Enabled

Maximum Allowed Clients 0

Static IP Tunneling Enabled

Off Channel Scanning Defer

Scan Defer Priority 0 1 2 3 4 5 6 7

Scan Defer Time(msecs) 100

DHCP

DHCP Server Override

DHCP Addr. Assignment Required

Management Frame Protection (MFP)

MFP Client Protection Disabled

DTIM Period (in beacon intervals)

802.11a/n (1 - 255) 1

802.11b/g/n (1 - 255) 1

NAC

NAC State None

Load Balancing and Band Select

Client Load Balancing

Client Band Select

Passive Client

ةدعاسملا Wireless Client ةادأ نيوكت

PEAP-MSCHAPv2 (user1)

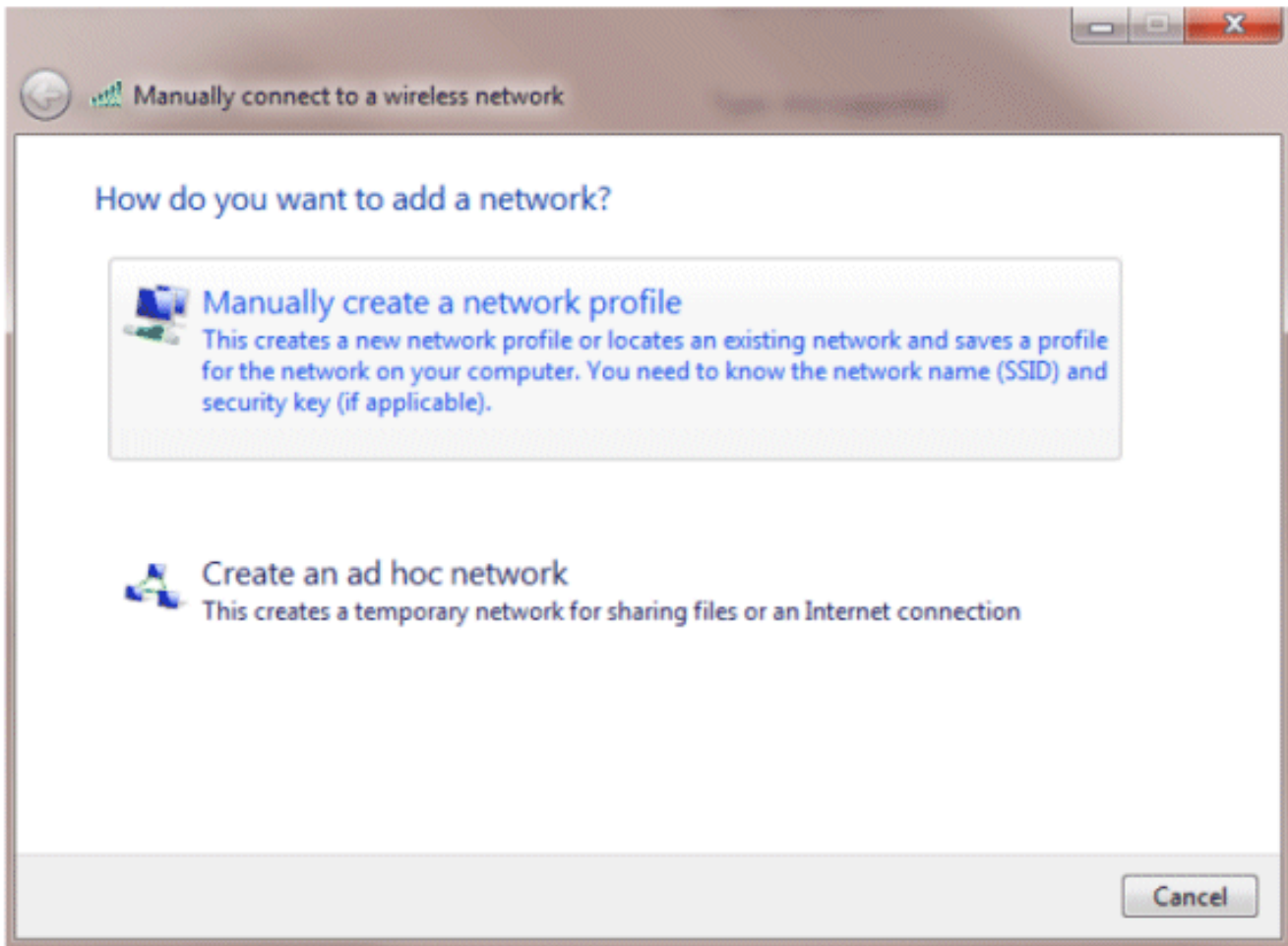
موظنبة لصل الة مكنحتلا ءءو مءءءسن اننإف؁ هكل من ىءلا لىمعل رابءءال زاآ ىف
14.3 لىءشء ءم انرب راءصا لءشء Intel نم 6300-N زارء ءقائب عم Windows 7 لىءشءلا
نءءروملا نم لىءشءلا ءمارب ءءءا ماءءءسا ب رابءءا ءارءاب ىصوى

Windows Zero Config (WZC): ىف فىرءء فلم ءاشنإل ءىلءالءا ءاوظءلا لمءا

1. ءىكللسالءا ءاكبشلا ءراءا > ءنرءنإلءا ءكبشلا > مكنحتلا ءءول لىل لءءنا

2. ءفاضا بىوبءلءا ءمالء قوف رءنا

3. اىوءى ءكبش فىصوء ءاشنإلءىلء رءنا



4. ءىلءملاء ءكبشلا ىف مكنحتلا رصنع لىلء اهنىوءءءمءامك لىصافءلءا فضا
(WLC) ءىكللسالءا

فءءالءلءالء اساسء SSID ءعى: ءظءالم

5. (ىلءلءا) Next قوف رءنا

Manually connect to a wireless network

Enter information for the wireless network you want to add

Network name:

Security type:

Encryption type:

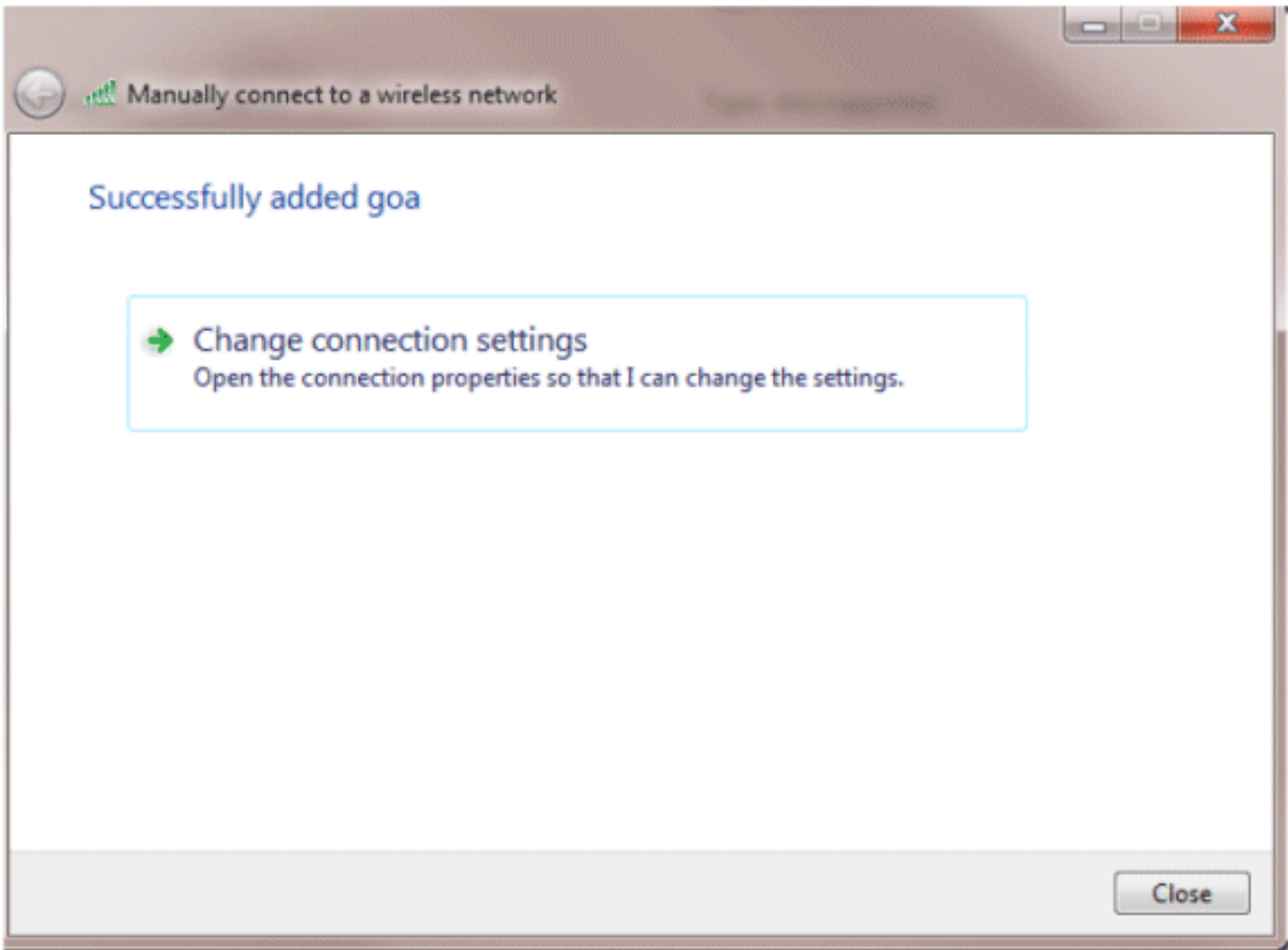
Security Key: Hide characters

Start this connection automatically

Connect even if the network is not broadcasting

Warning: If you select this option, your computer's privacy might be at risk.

6. اداع | ةلمعلا تققو | اداع | ةلمع لىصوت ريغي ةقطق



7. PEAP نېكمت نم دكأت

goa Wireless Network Properties



Connection Security

Security type: WPA2-Enterprise

Encryption type: AES

Choose a network authentication method:

Microsoft: Protected EAP (PEAP)

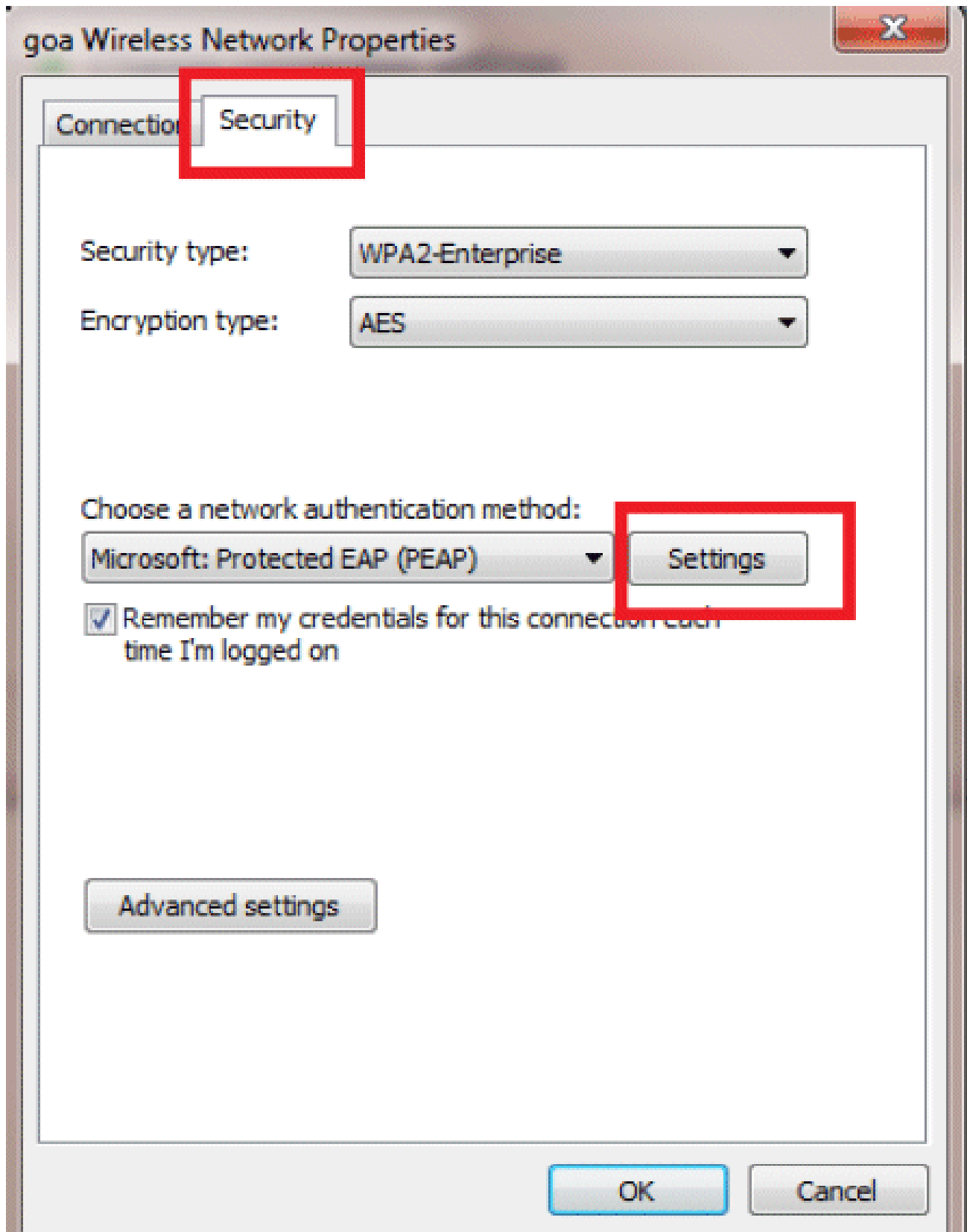
Settings

Remember my credentials for this connection each time I'm logged on

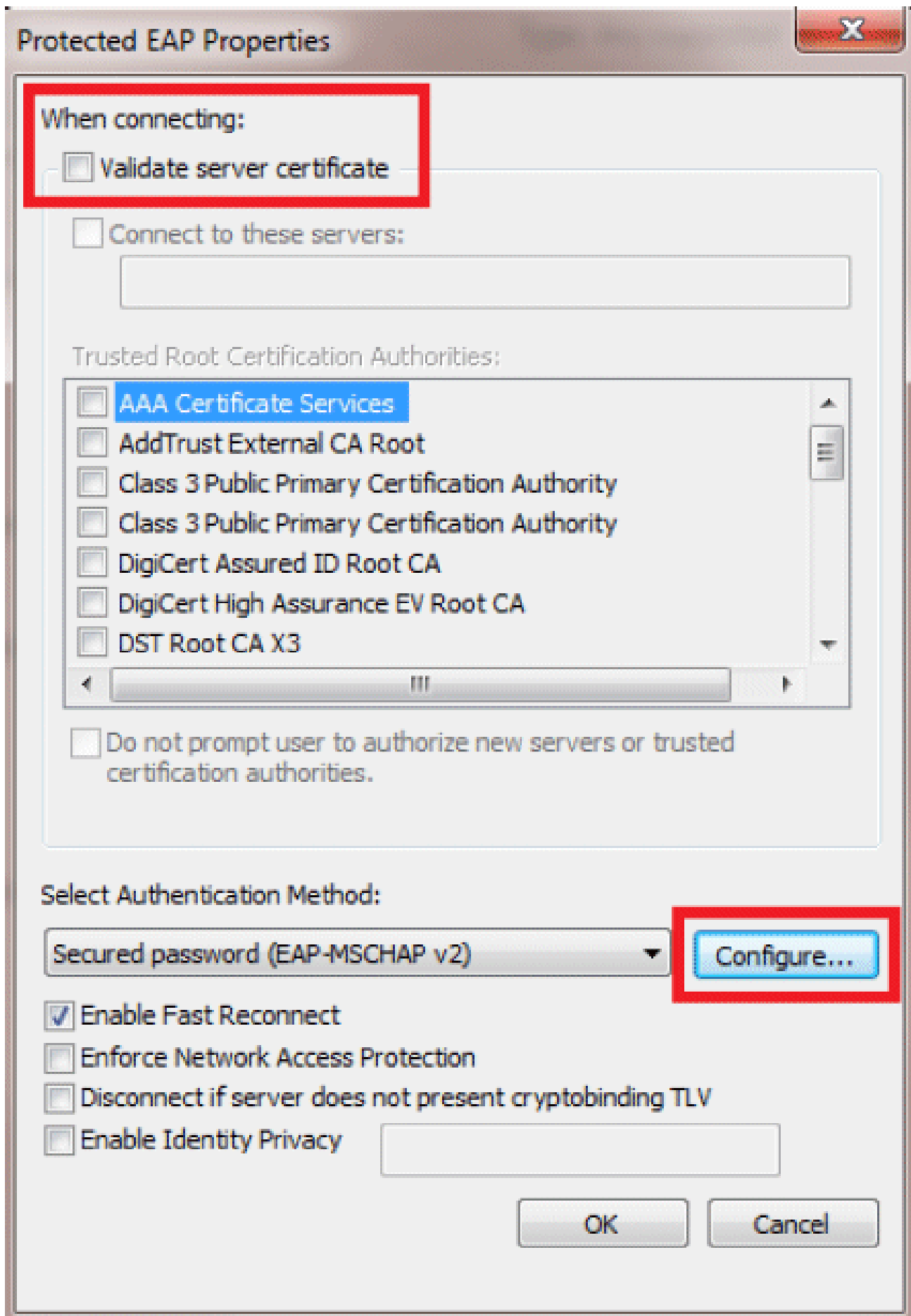
Advanced settings

OK

Cancel

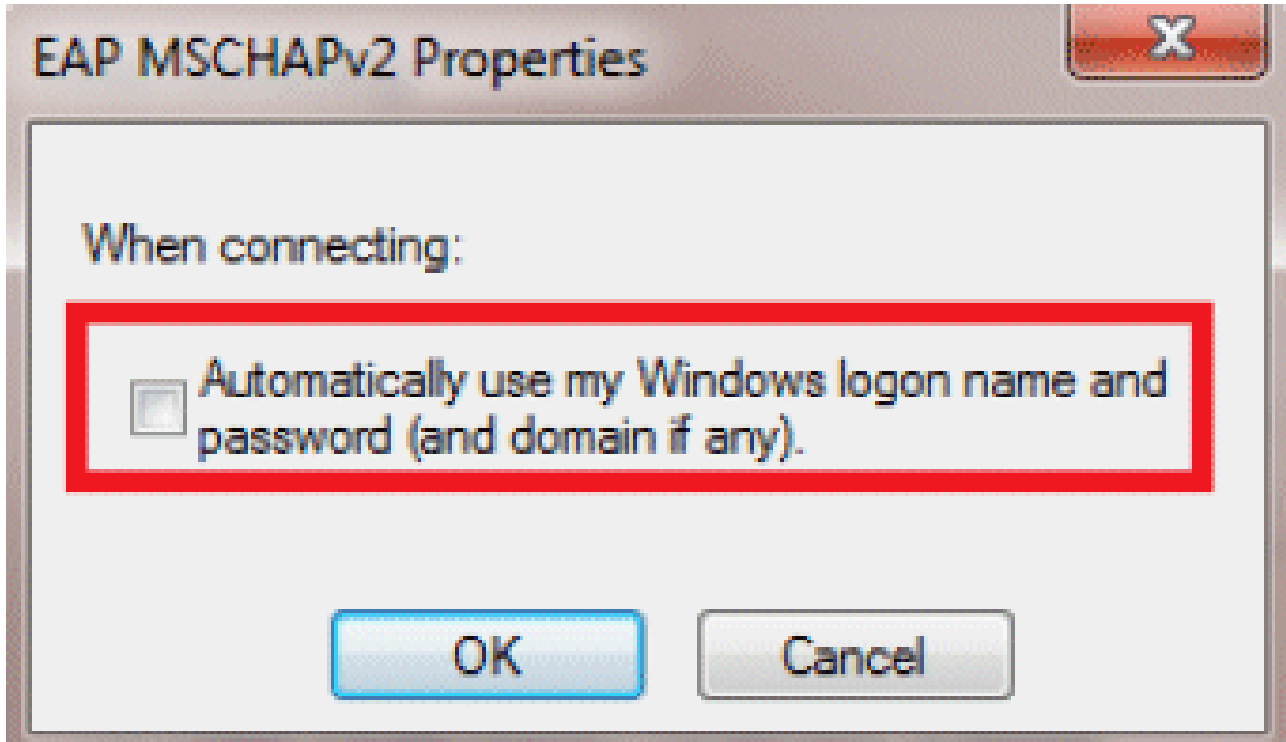


8. نكمت ملو عبرملا اذه تدح اذا. مداخال ادهاش ةحص نم ققحتلاب موقن ال، لاثملا اذه يف
يرخا ةرم رابتخاللا مثةزيملا ليطعت لواحف، لاصتالا نم



9. لاج يا ىلع .لوخدلا ليجستل Windows دامتعا تانايب مادختسا كنكمي ،كلذ نم الوب

OK قوف رقناو. كلذ مدختسن نل لاثملا اذه يف



10. ةملاك و username تلاكش in order to دادعإ ةيلمع مدقتم تقطوط

goa Wireless Network Properties



Connection Security

Security type: WPA2-Enterprise

Encryption type: AES

Choose a network authentication method:

Microsoft: Protected EAP (PEAP)

Settings

Remember my credentials for this connection each time I'm logged on

Advanced settings

OK

Cancel

Advanced settings



802.1X settings

802.11 settings

Specify authentication mode:

User authentication

Save credentials

Delete credentials for all users

Enable single sign on for this network

Perform immediately before user logon

Perform immediately after user logon

Maximum delay (seconds):

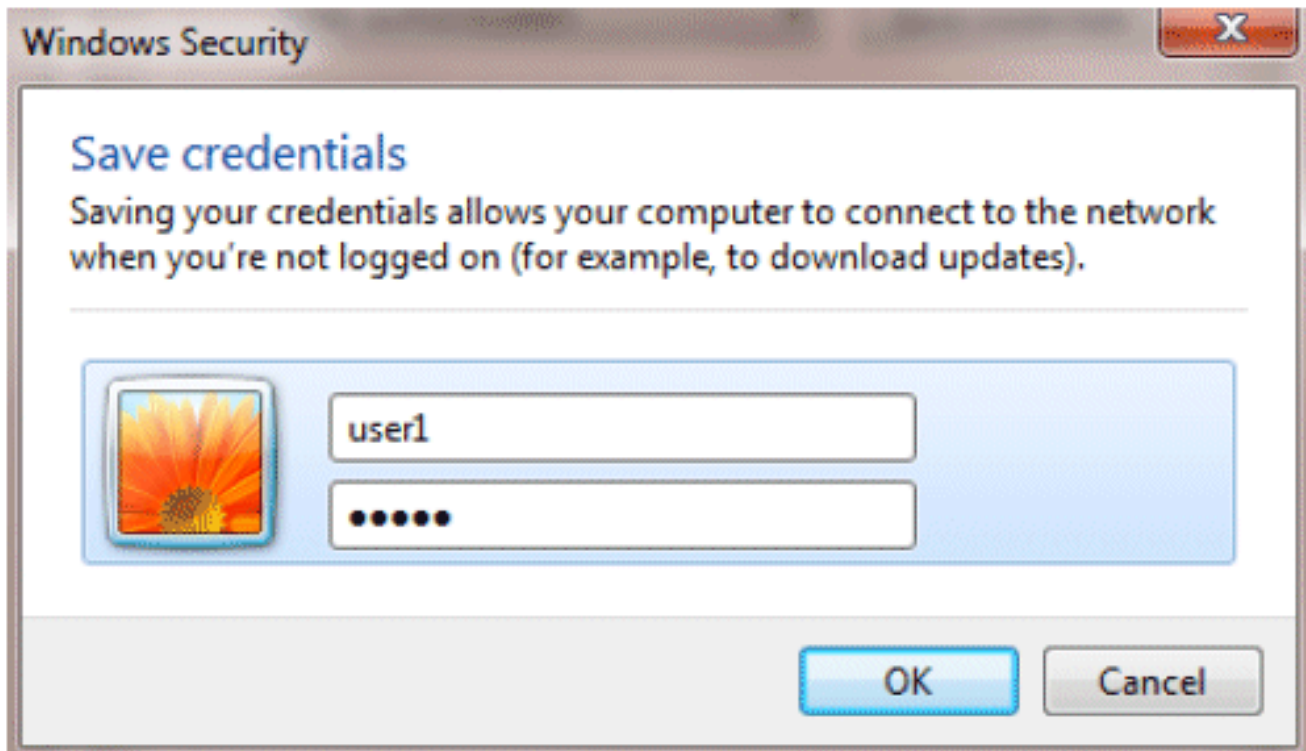
10

Allow additional dialogs to be displayed during single sign on

This network uses separate virtual LANs for machine and user authentication

OK

Cancel



للاصتال ل نآلة زهاج ليمع لل ةدعاسم لة أدال.

EAP-FAST (user2)

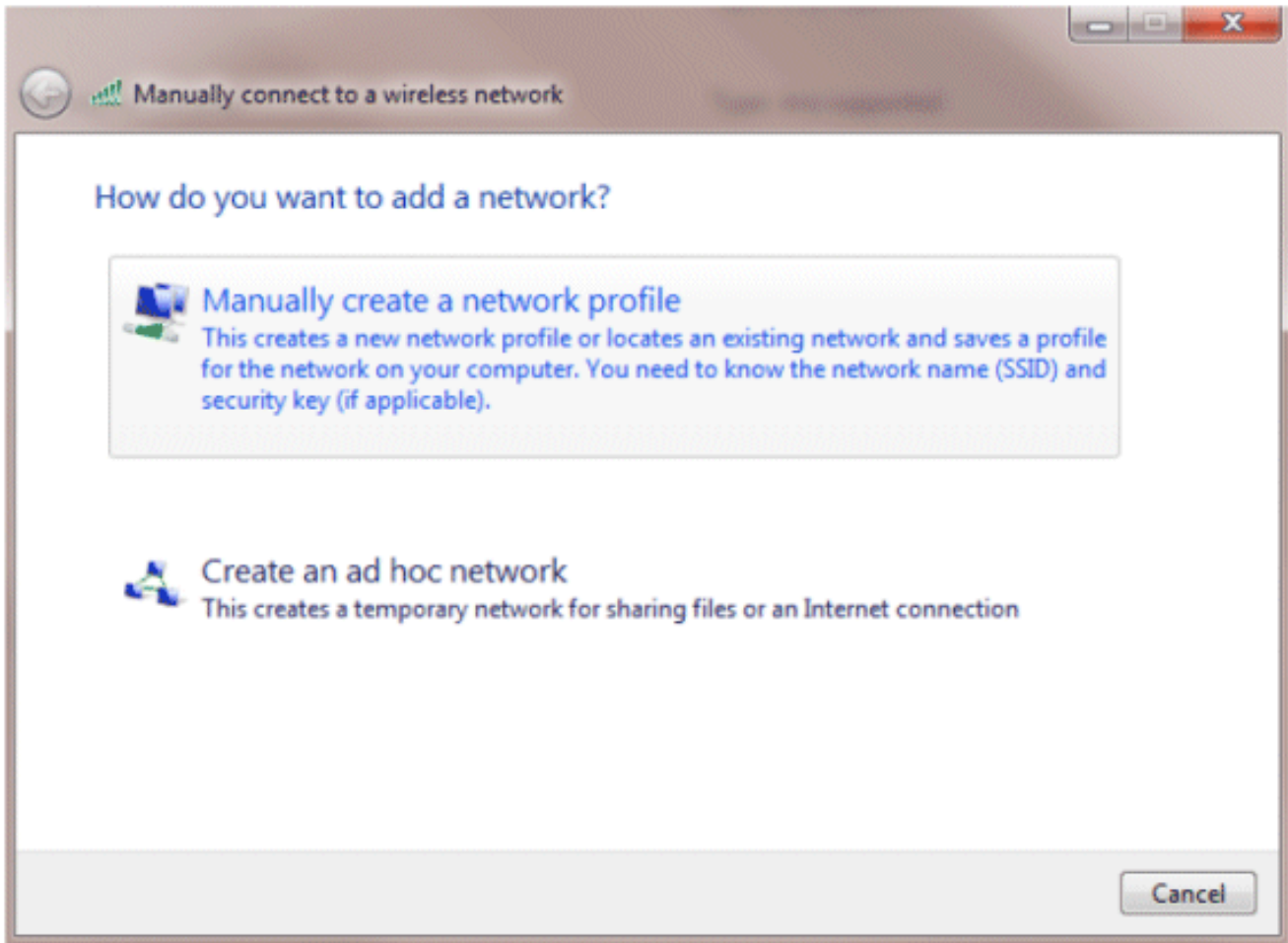
ماظن بة لصلأال مكحتللا ةدحو مدختسن اننإف، هكلمن يذلا ليمع ل رابتخال زاهاج يف
14.3 ل يغشت جم انرب رادصل لغشت Intel نم 6300-N زارط ةقاطب عم Windows 7 ل يغشت ل
نيدرولم ل نم ل يغشت ل جم ارب ثدحأ مادختساب رابتخال اءارجاب ي صوي

WZC: يف في صوت عاشن إلة لالات ل تاوطلخ ل لمكأ

1. ةيكل لسلال ل تاكبش ل ةرادإ > تنرتن إل او ةكبش ل > مكحتللا ةحول ل ل لقتنا

2. ةفاضا بيوبتللا ةمالع قوف رقنا

3. ايودي ةكبش في صوت عاشن إل ل رقنا



4. لملحمة الشللا في مكحتلا رصنع لىع انه نوكت مت امك لىصافتلا فضا
ة (WLC) لىكلساللا

ف. لال لال لاساسح SSID دعي: لظالم

5. (للاللا) Next قوف رونا

Manually connect to a wireless network

Enter information for the wireless network you want to add

Network name: goa

Security type: WPA2-Enterprise

Encryption type: AES

Security Key: Hide characters

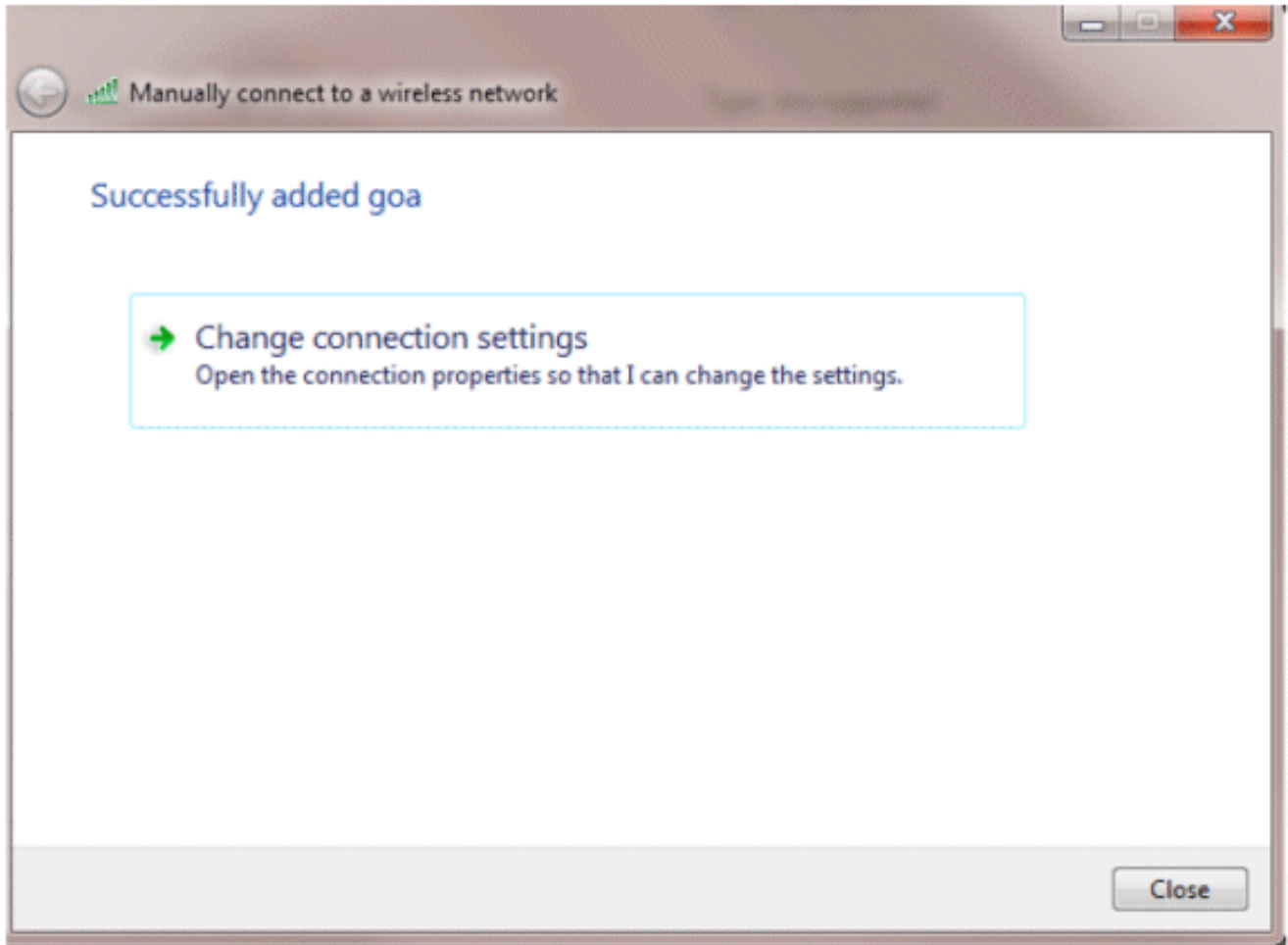
Start this connection automatically

Connect even if the network is not broadcasting

Warning: If you select this option, your computer's privacy might be at risk.

Next Cancel

6. اداع |ة لملعلا تقق د in order to اداع |ة لملع ليصوت ريغي ة ققط



7. EAP-FAST نيكمت نم دكأت

بجي. ةقداصم ةقيرطك EAP-FAST ىلع يضا رتفا لكشب WZC يوتحي ال: ةظالم
Intel، ةقاطب اهنأ امب، لاثملا اذه يف. ةيجراخ ةهجل عبات دروم نم ةدعاسملا ةادألا ليزنت
م. اظنلا ىلع ةتبتثم Intel PROSet انيدلف

goa Wireless Network Properties

Connection

Security

Security type:

WPA2-Enterprise

Encryption type:

AES

Choose a network authentication method:

Cisco: EAP-FAST

Microsoft: Smart Card or other certificate

Microsoft: Protected EAP (PEAP)

Cisco: LEAP

Cisco: PEAP

Cisco: EAP-FAST

Intel: EAP-SIM

Intel: EAP-TTLS

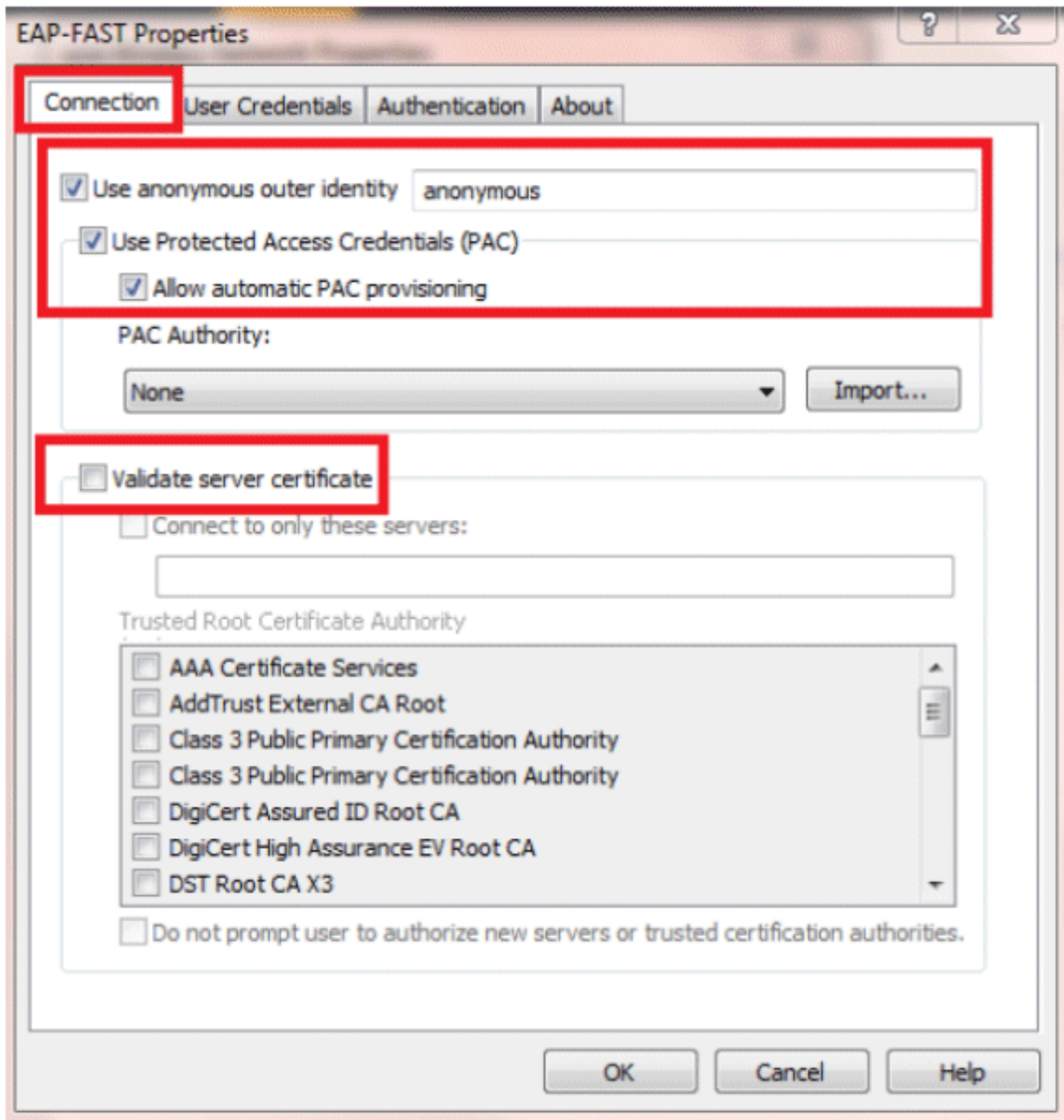
Intel: EAP-AKA

Settings

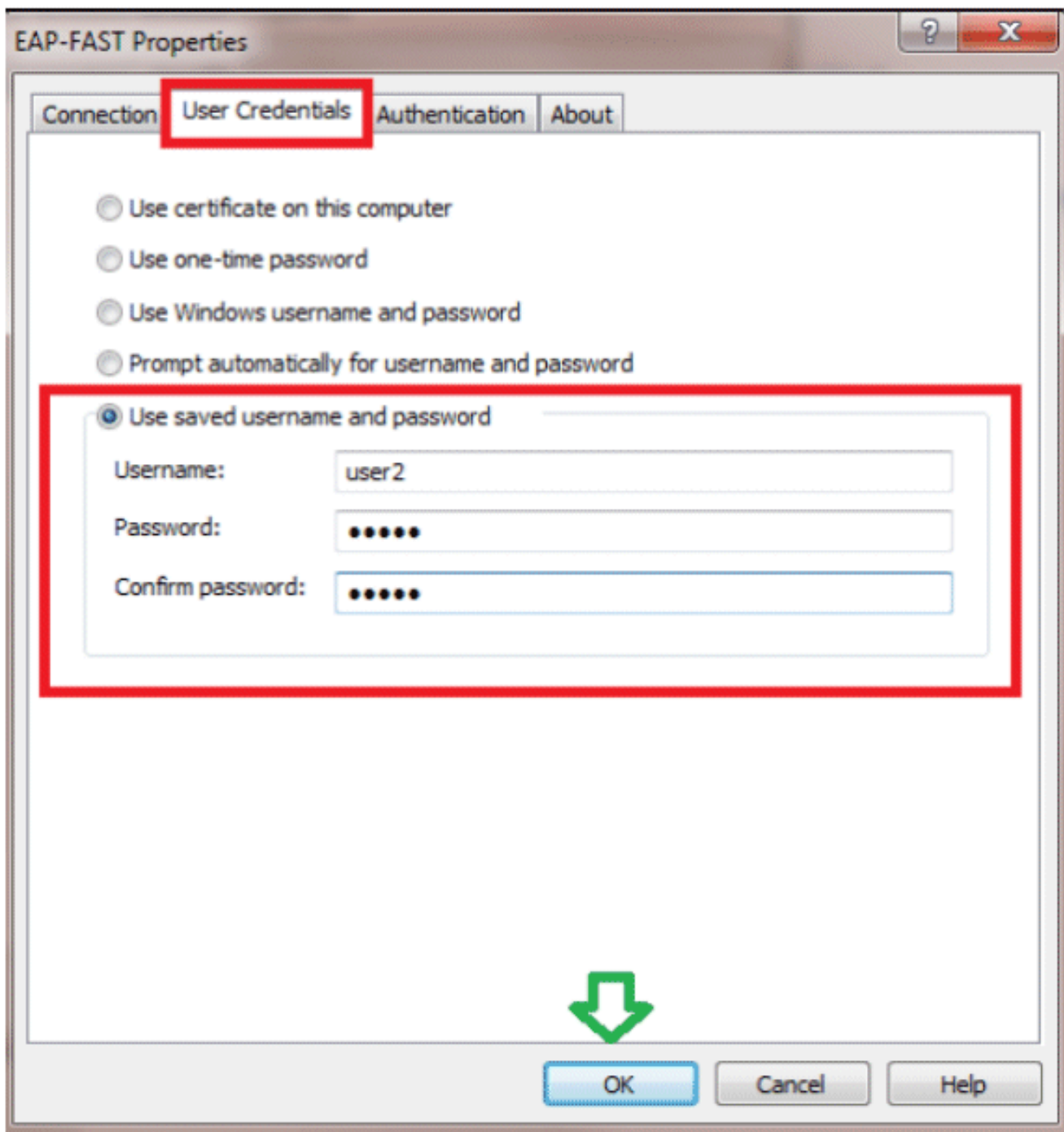
Advanced settings

OK

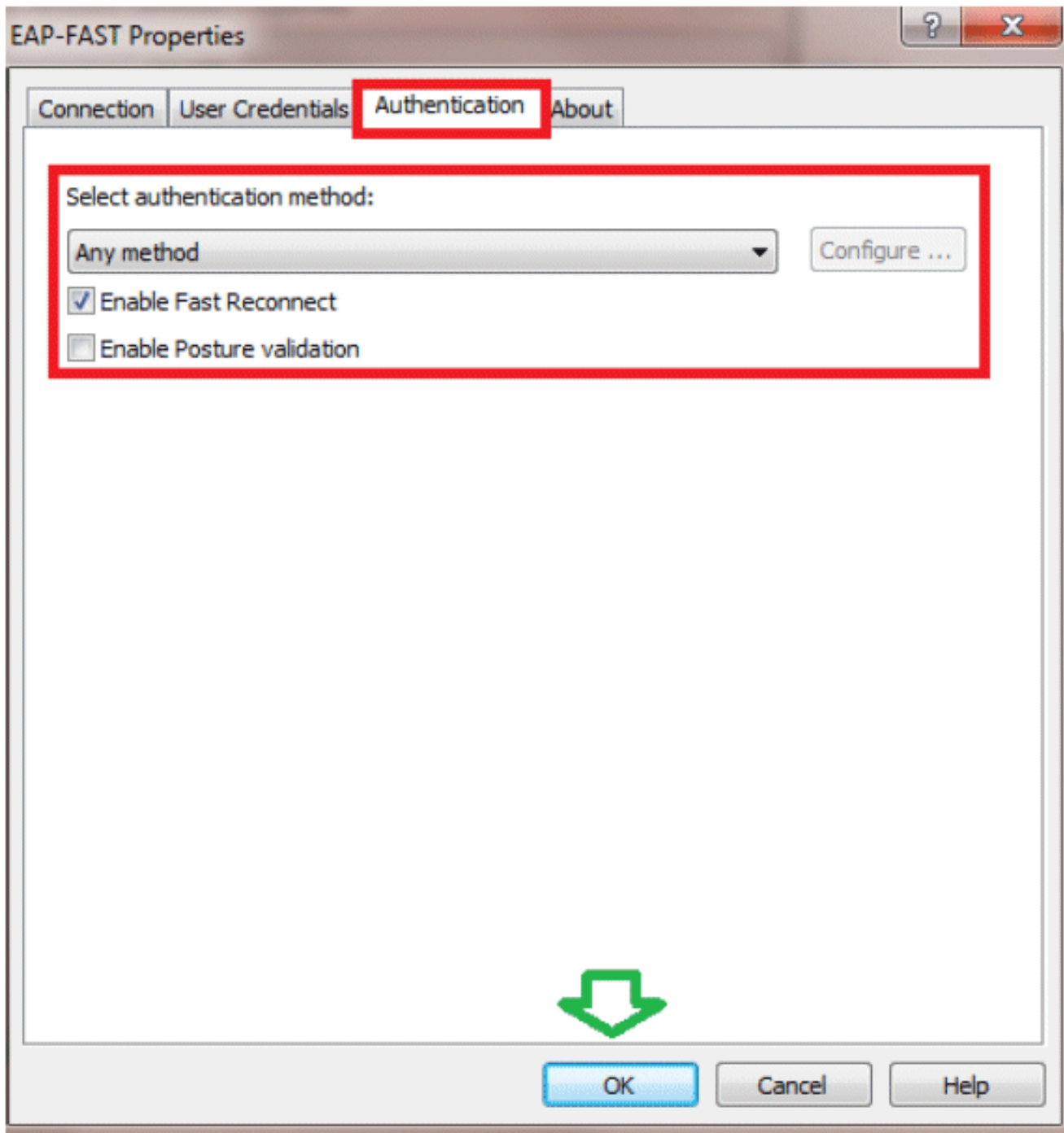
Cancel



9. نم ال د ب . 2 م د خ ت س م ل ا ت ا غ و س م ل خ د ا و ، م د خ ت س م ل ا ت ا غ و س م ب ي و ب ت ل ا ة م ا ل ع ق و ف ر ق ن ا ا ذ ه ي ف ، ل ا ح ي ا ي ل ع . ل و خ د ل ا ل ي ج س ت ل W i n d o w s د ا م ت ع ا ت ا ن ا ي ب م ا د خ ت س ا ك ن ك م ي ، ك ل ذ ك ل ذ م د خ ت س ن ن ل ل ا ث م ل ا



10. OK قوف رقناو



2. م دختسم ل ل لاصتال ن آلا ةزهاج ل لمعلل ةدعاسم ل ةادألا

PAC. يمحم لوصو غوسم RADIUS م داخ لسري ، ةقداصم ل 2م دختسم ل ةلواحم دنع : ةظالم
ةقداصم ل لامكتسال (PAC) يمحم ل لوصول تاغوسم لوبق

EAP-FAST



Automatic PAC provisioning is enabled for this profile. However, a valid PAC that matches the server to which the client is connecting could not be found. Do you wish to obtain a new security credential (PAC)?



Yes

No

ةحصلال نم ققحتال

ححص لكشب نيوكتال لمع ديكأتل مسقلا اذه مدختسا

مجرتم ةادأ مدختسا . show [رماواضعب \(طقف نيلجس ملءالمعلل\) جارخالا مجرتم ةادأ](#) معدت
show رمالا جَرْم ليلحت ضرعل (OIT) جارخالا

1 مدختس مل نم ققحتال (PEAP-MSCHAPv2)

ةيلحمل ةكبشلا يف مكحتال ةدحوب ةصاخلا (GUI) ةيموسرلا مدختس مل ةهجاو نم
MAC ناو نع ددحو، ءالمعلا > ةشاشلا ىلا لقتنا، (WLC) ةيكلساللا

Clients > Detail

Client Properties

MAC Address	00:24:d7:aa:f1:08
IP Address	192.168.153.107
Client Type	Regular
User Name	user1
Port Number	13
Interface	vlan253
VLAN ID	253
CCX Version	CCXv4
E2E Version	E2Ev1
Mobility Role	Local
Mobility Peer IP Address	N/A
Policy Manager State	RLN
Management Frame Protection	No
UpTime (Sec)	12
Power Save Mode	OFF
Current TxRateSet	6.0,9.0,12.0,18.0,24.0,36.0,48.0,34.0
Data RateSet	0

AP Properties

AP Address	2c:3f:38:c1:3c:f0
AP Name	3502e
AP Type	802.11an
WLAN Profile	gold
Status	Associated
Association ID	1
802.11 Authentication	Open System
Reason Code	1
Status Code	0
CF Pollable	Not Implemented
CF Poll Request	Not Implemented
Short Preamble	Not Implemented
PBCC	Not Implemented
Channel Agility	Not Implemented
Re-authentication timeout	86365
Remaining Re-authentication timeout	0
WEP State	WEP Enable

Security Information

Security Policy Completed	Yes
Policy Type	REN (WPA2)
Encryption Cipher	CCMP (AES)
EAP Type	PEAP
SNMP NAC State	Access
Radius NAC State	RLN

WLC RADIUS: تالاح

<#root>

(Cisco Controller) >

show radius auth statistics

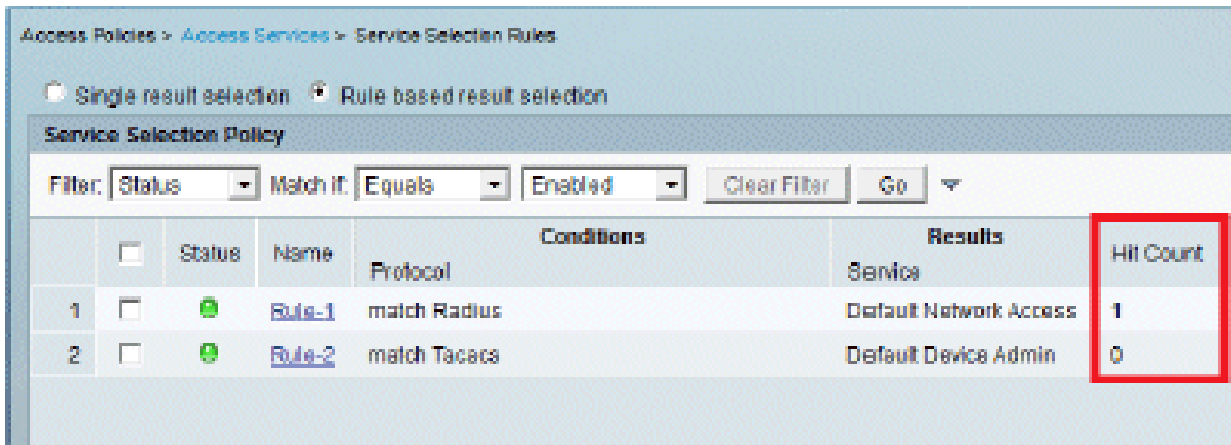
```
Authentication Servers:
  Server Index..... 1
  Server Address..... 192.168.150.24
  Msg Round Trip Time..... 1 (msec)
  First Requests..... 8
  Retry Requests..... 0
  Accept Responses..... 1
  Reject Responses..... 0
  Challenge Responses..... 7
  Malformed Msgs..... 0
  Bad Authenticator Msgs..... 0
```

Pending Requests..... 0
 Timeout Requests..... 0
 Unknowntype Msgs..... 0
 Other Drops..... 0

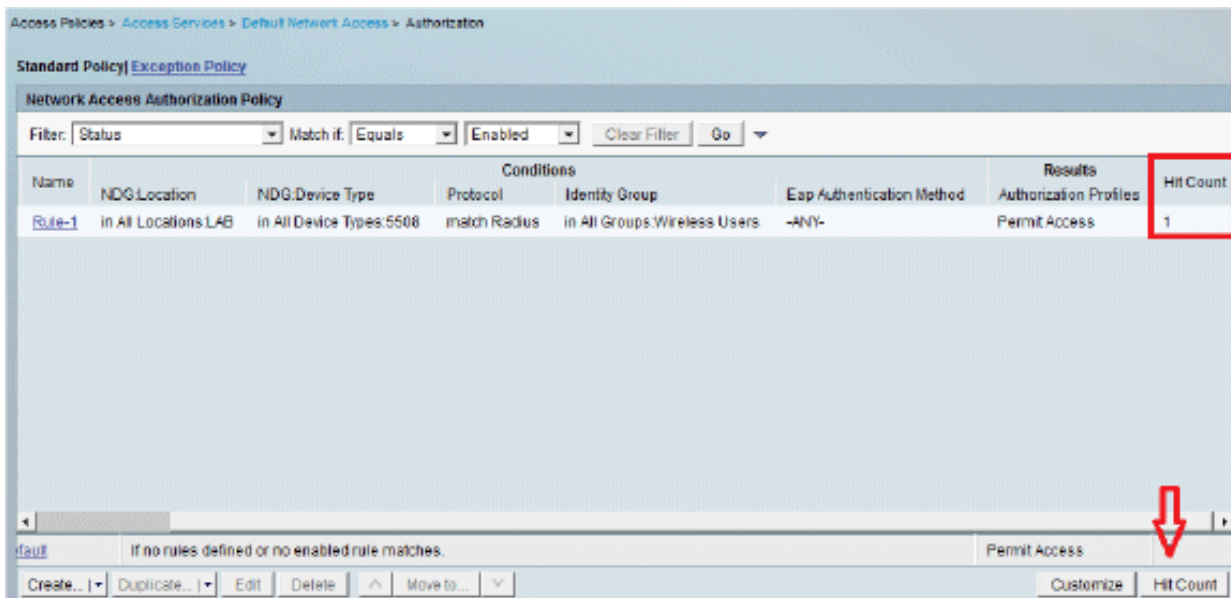
ACS تالچس

1:دع برض ل تدهاش steps in order to اذه تم تاً

a.تارم ددع شي دجت نم دكأت ف ،ةقداصم ل نم ةقوي قد 15 ل لالخ تالچس ل ا صرغب تمق اذ ا لوصول.



b.ةحفص ل س فن ل فسأ يف لوصول تارم ددع ل بيوبت ةمالع كيدل



2- تاقداصم ل ا ل لقتنا .ةديج ةقث بنم ةذفان رهظيو and Reporting ةقطق يتل ةمدخل ا ددجت ةدعاق نم ققحتل ل Details قوف رقنل ااضيأ كنكمي .موي ل- RADIUS اةقبيبطت م

Showing Page 1 of 1 | [Home](#) | [Print](#) | [Back](#) | [List](#) | [Go](#) | [Launch Interactive Viewer](#)

AAA Protocol > RADIUS Authentication

Authentication Status : Pass or Fail
 Date : January 29, 2012 05:49 PM - January 29, 2012 06:10 PM ([Last 30 Minutes](#) | [Last Hour](#) | [Last 12 Hours](#) | [Today](#) | [Yesterday](#) | [Last 7 Days](#) | [Last 30 Days](#))

Generated on January 29, 2012 6:10:42 PM EST

Selected

Pass
 Fail
 Click for details
 Mouse over item for additional information

Logged At	RADIUS Status	NAS Failure	Details	Username	MAC/IP Address	Access Service	Authentication Method	Network Device	NAS IP Address	NAS Port ID	CTS Security Group	ACS Instance
Jan 29, 12 6:07:37:943 PM	✓			asa01	00:24:67:1a:ef1:98	Default_Network_Access	PEAP (EAP-MSCHAPv2)	WLC5508	192.168.153.111			SAULACS02

2 مداخلتسمل نم ققحتلا (EAP-FAST)

ةيحلحلملة كةبشلال يف مكحتلا ءدحوب ءصاخلا (GUI) ءيموسرلا مءختسمل ءهءاوم نم MAC. ناونع ءدحو، ءالمءلا > ءشاشلال ىلل لقتنا، (WLC) ءيكلساللا.

Clients > Detail

Client Properties

MAC Address	00:24:67:1a:ef1:98
IP Address	192.168.153.111
Client Type	Regular
User Name	user2
Port Number	13
Interface	vlan253
VLAN ID	253
CCX Version	CCXv4
E2E Version	E2Ev1
Mobility Role	Local
Mobility Peer IP Address	N/A
Policy Manager State	RUN
Management Frame Protection	No
UpTime (Sec)	29
Power Save Mode	OFF
Current TxRateSet	m13
Data RateSet	6.0,9.0,12.0,18.0,24.0,36.0,48.0,54.0

AP Properties

AP Address	2c:3f:38:c1:3c:f0
AP Name	3502a
AP Type	802.11an
WLAN Profile	gpa
Status	Associated
Association ID	1
802.11 Authentication	Open System
Reason Code	1
Status Code	0
CF Pollable	Not Implemented
CF Poll Request	Not Implemented
Short Preamble	Not Implemented
PBCC	Not Implemented
Channel Agility	Not Implemented
Re-authentication timeout	86302
Remaining Re-authentication timeout	0
WEP State	WEP Enable

Security Information

Security Policy Completed	Yes
Policy Type	RSN (WPA2)
Encryption Cipher	CCMP (AES)
EAP Type	EAP-FAST
SNMP NAC State	Access
Radius NAC State	RUN

ACS: ءالءس

1: ددع برض ل ا تدهاش steps in order to اذه تم تاً

a. تارم ددع شي دحت نم دكأتف ،ةقداصم ل نم ةقوي قد 15 ل لالخ تال ج س ل ا ص ح ف ب تم ق اذا م اظن ل ا ل ا ل و ص و ل ا .

Access Policies > Access Services > Service Selection Rules

Single result selection Rule based result selection

Service Selection Policy

Filter: Status Match it: Equals Enabled Clear Filter Go

	<input type="checkbox"/>	Status	Name	Conditions	Results	Hit Count
				Protocol	Service	
1	<input type="checkbox"/>		Rule-1	match Radius	Default Network Access	3
2	<input type="checkbox"/>		Rule-2	match Tacacs	Default Device Admin	0

b. ؤح ف ص ل ا س ف ن ل ف س أ ي ف ل و ص و ل ا تارم ددع ل ب ي و ب ت ة م ا ل ع ك ي د ل .

Access Policies > Access Services > Default Network Access > Authorization

Standard Policy | Exception Policy

Network Access Authorization Policy

Filter: Status Match it: Equals Enabled Clear Filter Go

Name	NDG:Location	NDG:Device Type	Conditions	Eap Authentication Method	Results	Hit Count	
			Protocol	Identify Group	Authorization Profiles		
Rule-1	In All Locations:LAB	In All Device Types:5500	match Radius	In All Groups:Wireless Users	-ANY-	Permit Access	2

If no rules defined or no enabled rule matches. Permit Access

Create... Duplicate... Edit Delete Move to... Customize Hit Count

2- ت ا ق د ا ص م ل ا ل ا ل ق ت ن ا . ة د ي د ج ة ق ت ب ن م ة ذ ف ا ن ر ه ظ ي و m o n i t o r e a n d R e p o r t i n g ة ق ط و ق ي ت ل ا ة م د خ ل ا د ي د ح ت ة د ع ا ق ن م ق ق ح ت ل ل D e t a i l s ق و ف ر ق ن ل ا ض ي أ ك ن ك م ي . م و ي ل ا - R A D I U S ا ه ق ي ب ط ت م ت .

Showing Page 1 of 1 Goto Page: Go

AAA Protocol > RADIUS Authentication

Authentication Status: Pass or Fail

Date: January 29, 2012 06:53 PM - January 29, 2012 06:23 PM (Last 30 Minutes | Last Hour | Last 12 Hours | Today | Yesterday | Last 7 Days | Last 30 Days)

Generated on January 29, 2012 6:23:17 PM EST

Refresh

Pass Fail Click for details Focus over item for additional information

Logged At	RADIUS Status	NAS Failure	Details	Username	MAC/IP Address	Access Service	Authentication Method	Network Device	NAS IP Address	NAS Port ID	CTS Security Group	ACS Ins
Jan 29, 12 6:19:27 PM	✓			user2	00-26-d7-ae-f1-90	Default Network Access	EAP-FAST (EAP-MSCHAPv2)	WLC-5500	192.168.75.44			SALLA
Jan 29, 12 6:07:37 PM	✓			user1	00-24-d7-ae-f1-90	Default Network Access	PEAP (EAP-MSCHAPv1)	WLC-5500	192.168.75.44			SALLA

اهحالصإو عاطخأل افاشكتسا

اهحالصإو نيوكتل اعاطخأ افاشكتسا ال امدختسا كنكمي تامولعم مسقلا اذه رفوي

اهحالصإو عاطخأل افاشكتسا رم اوأ

مجرتم ةادأ مدختسا . show [رماوإ ضعب \(طقف ني لچس مل اءالمعلل\) جارخال ا مجرتم ةادأ](#) معدت
show رمال جَرْم ليلحت ضرعل (OIT) جارخال

debug رماوإ م ادختسا لباق [حي حصتلا رماوإ لوح ةمه م تامولعم](#) ىل ا عجرا :ةظحالم

WLC:1 لىل ع رما اذه تردصأ ، ةلكشم يأ تنأ هجاوي نا

• <mac add of client> ليمعل اعاطخأ حي حصت

• debug aaa all enable

• جهنلا ريدم ةلاح نم ققحتلا - <mac addr> ليمعل لىل صافات راهظا

• ببس لشفال تقود - show radius auth statistics

• اعاطخأل احي حصت ليغشت فاقيا - debug disable-all

• رصنع ىل ع رطقلا فصن تا يئاصحا حسم - لكلا رطقلا فصن ةقداصم تالاح حسم
(WLC) ةيكلساللا ةيلحمل ا ةكبشلا ي ف مكحتلا

2. لشفال ببس ظحالو ACS ي ف ةدوجوملا تالجال نم ققحت

ةلص تاذا تامولعم

• [Cisco Systems - تادنتس مل او ينقتلا معدلا](#)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسمل اذ ه Cisco ت مچرت
ملاعلاء ان ا عي مچ ي ف ن ي م دخت سمل ل معد ي و تح م مي دقت ل ة ي رش ب ل و
امك ة ق ي قد ن و ك ت ن ل ة ي ل ة مچرت ل ض ف ا ن ا ة ظ حال م ي ج ر ي . ة ص ا خ ل م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م 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 (رف و ت م ط بار ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا دن تسمل ا