قم بتكوين ACS 5.2 للمصادقة المستندة إلى المنفذ باستخدام نقطة الوصول في الوضع Lightweight (LAP)

المحتويات

المقدمة

يصف هذا المستند كيفية تكوين نقطة وصول في الوضع Lightweight (LAP) كعميل 802.1x للمصادقة مقابل خادم RADIUS مثل خادم التحكم في الوصول (ACS) 5.2.

المتطلبات الأساسية

المتطلبات

تأكد من استيفاء المتطلبات التالية قبل محاولة هذا التكوين:

- طاقم (WLC) وحدة التحكم في الشبكة المحلية اللاسلكية (WLC) معرفة أساسية بوحدة التحكم في الوصول في الوضع Lightweight (LAPs).

- معرفة وظيفية بخادم AAA.
- دليهم معرفة كاملة بالشبكات اللاسلكية ومشكلات الأمان اللاسلكي.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- Cisco 5508 WLC الذي يشغل البرنامج الثابت، الإصدار 7.0.220.0
- نقطة الوصول في الوضع Lightweight من السلسلة Cisco 3502 Series LAP
- مصدر المحتوى الإضافي الآمن من Cisco الذي يشغل الإصدار 5.2
- المحول Cisco 3560 Series Switch

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول الاصطلاحات المستندات.

معلومات أساسية

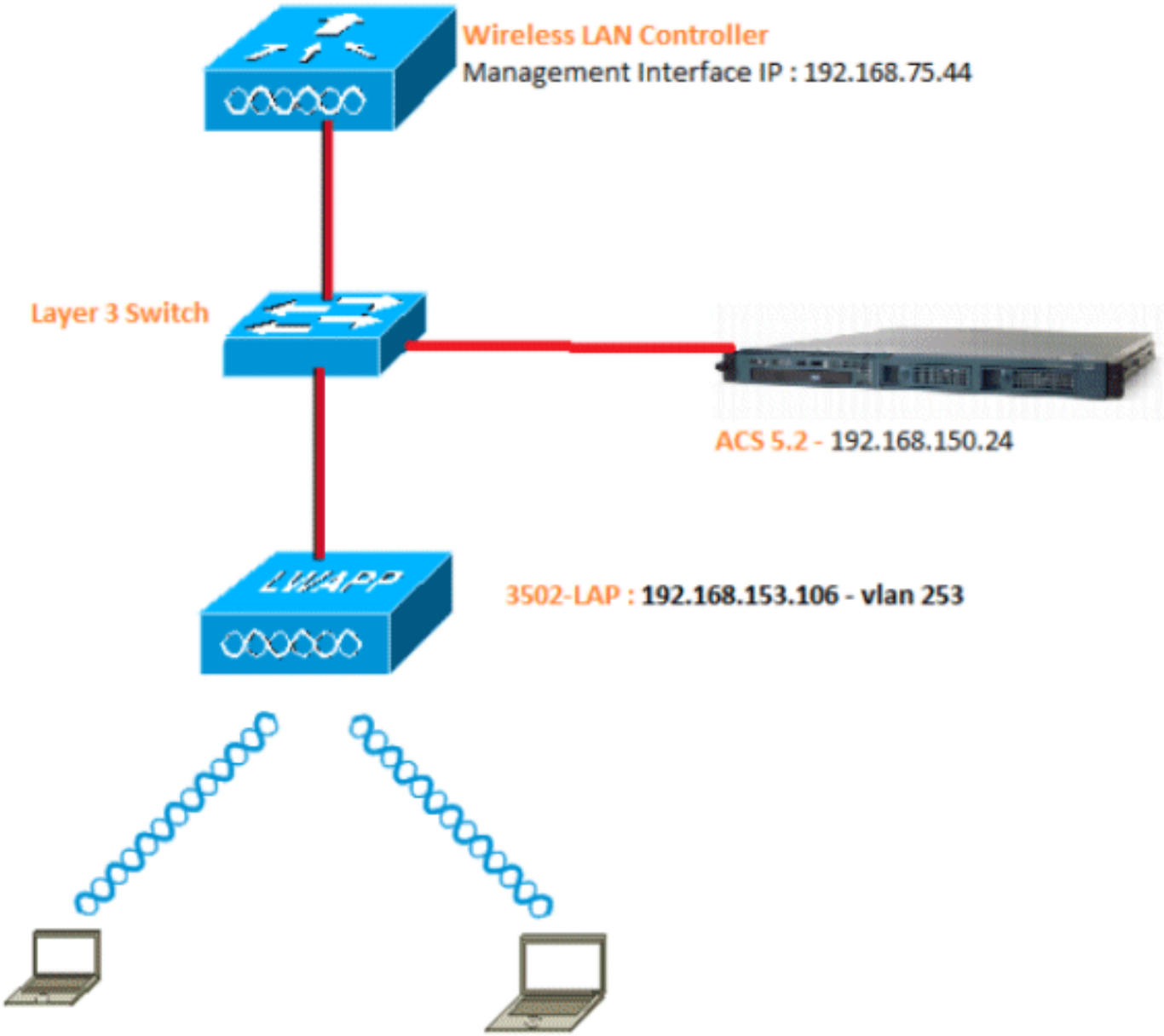
تحتوي نقاط الوصول في الوضع X.509 المثبتة في المصنع - الموقعة بواسطة مفتاح خاص - والتي يتم نسخها في الجهاز في وقت التصنيع. تستخدم نقاط الوصول في الوضع Lightweight هذه الشهادة للمصادقة مع عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) في عملية الانضمام. تصف هذه الطريقة طريقة أخرى لمصادقة نقاط الوصول في الوضع Lightweight. باستخدام برنامج WLC، يمكنك تكوين مصادقة 802.1x بين نقطة وصول Cisco Aironet (AP) ومحول Cisco. في هذه الحالة، تعمل نقطة الوصول كمحول 802.1x وتتم مصادقتها بواسطة المحول مقابل خادم RADIUS (ACS) الذي يستخدم EAP-FAST مع توفير PAC مجهول. وبمجرد تكوينها لمصادقة 802.1x، لا يسمح المحول لأي حركة مرور بخلاف حركة مرور 802.1x بالمرور عبر المنفذ حتى تتم مصادقة الجهاز المتصل بالمنفذ بنجاح. يمكن مصادقة نقطة الوصول إما قبل انضمامها إلى وحدة تحكم في الشبكة المحلية اللاسلكية (WLC) أو بعد انضمامها إلى وحدة تحكم في الشبكة المحلية اللاسلكية (WLC)، في هذه الحالة، يمكنك تكوين 802.1x على المحول بعد نقطة الوصول (LAP) تنضم إلى وحدة التحكم في الشبكة المحلية اللاسلكية (WLC).

التكوين

في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



هذه هي تفاصيل تكوين المكونات المستخدمة في هذا المخطط:

- عنوان IP الخاص بخادم ACS (RADIUS) هو 192.168.150.24.
- عنوان واجهة الإدارة و AP-Manager الخاصة بوحدة التحكم في الشبكة المحلية اللاسلكية (WLC) هو 192.168.75.44.
- عنوان خوادم DHCP 192.168.150.25.
- الثنين وضعت في VLAN 253.
- شبكة VLAN 253: 192.168.153.x/24. البوابة: 192.168.153.10
- شبكة VLAN 75: 192.168.75.x/24. البوابة: 192.168.75.1

إفتراضات

- شكلت مفتاح ل كل طبقة 3 VLANs.
- تم تعيين نطاق DHCP لخادم DHCP.
- يوجد اتصال الطبقة 3 بين جميع الأجهزة في الشبكة.
- نقطة الوصول (LAP) متصلة بالفعل بوحدة التحكم في الشبكة المحلية اللاسلكية (WLC).
- تحتوي كل شبكة VLAN على قناع /24.
- يحتوي ACS 5.2 على شهادة موقعة ذاتيا مثبتة.

خطوات التكوين

ويتم تقسيم هذا التكوين إلى ثلاث فئات:

1. تكوين نقاط الوصول في الوضع Lightweight.
2. قم بتكوين المحول.
3. قم بتكوين خادم RADIUS

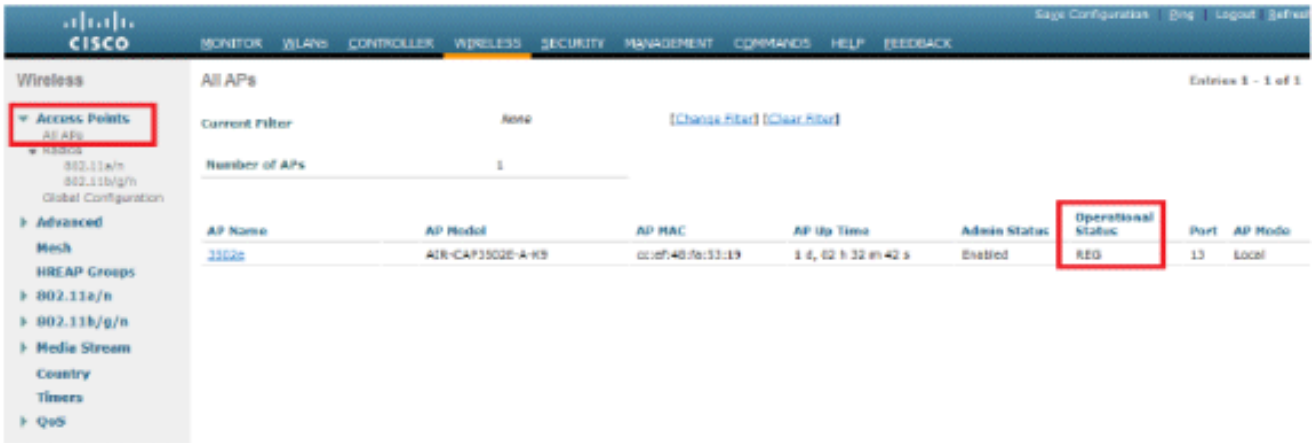
تكوين LAP

الافتراضات:

تم تسجيل نقاط الوصول في الوضع Lightweight (LAP) بالفعل إلى عنصر التحكم في شبكة المحلية اللاسلكية (WLC) باستخدام إما الخيار 43 أو DNS أو IP لواجهة إدارة WLC التي تم تكوينها بشكل ثابت.

أكمل الخطوات التالية:

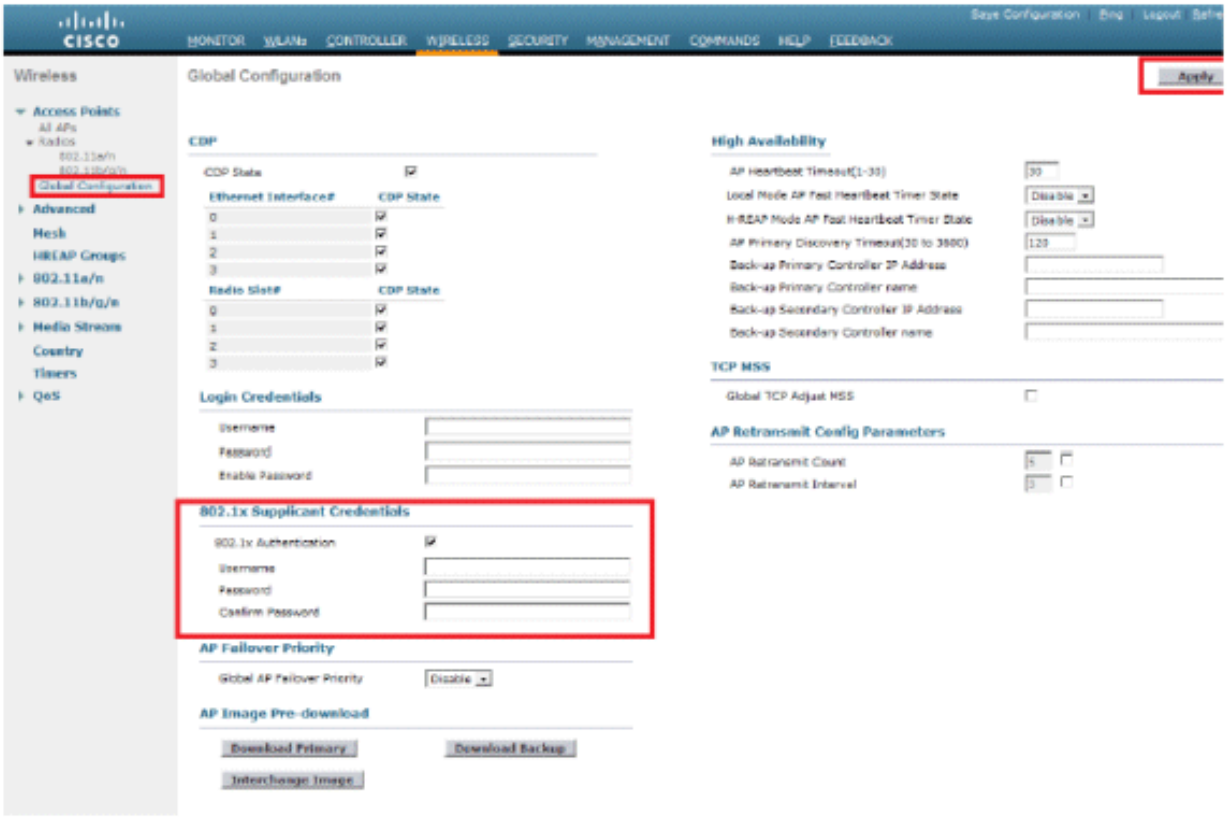
1. انتقل إلى لاسلكي > نقاط الوصول>جميع نقاط الوصول للتحقق من تسجيل نقاط الوصول في الوضع Lightweight على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC).



أنت يستطيع شكلت الـ 802.1x وقوة اعتماد (that is، username/password) لكل LAPs2. بطريقتين:

- عالمي

بالنسبة لنقاط الوصول في الوضع Lightweight المتصلة بالفعل، يمكنك تعيين بيانات الاعتماد بشكل عام حتى يرث كل نقطة وصول في الوضع Lightweight تنضم إلى عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) بيانات الاعتماد هذه.

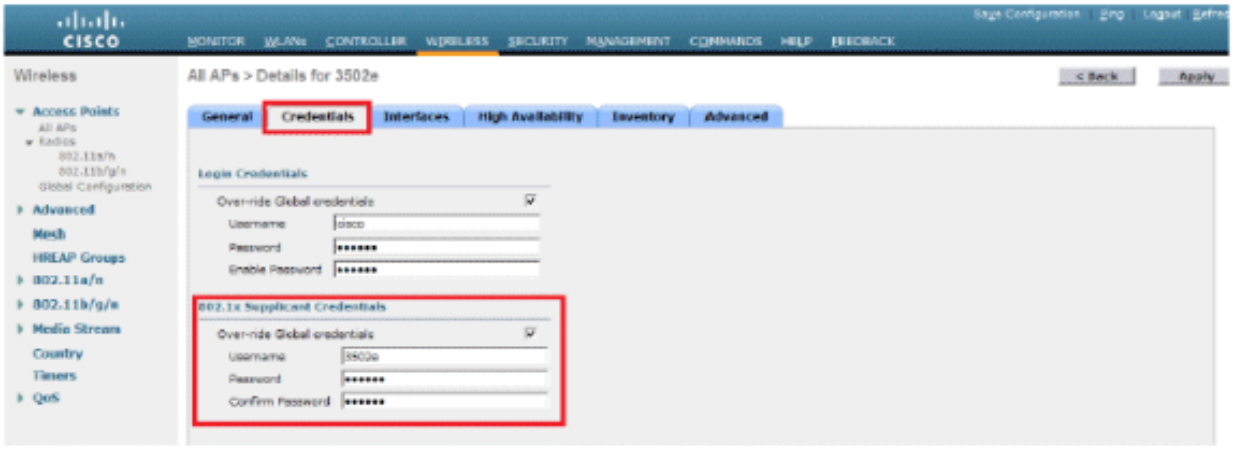


- فردي

تشكيل توصيفات 802. 1 x لكل نقطة وصول. في المثال الخاص بنا، سنقوم بتكوين بيانات الاعتماد لكل نقطة وصول.

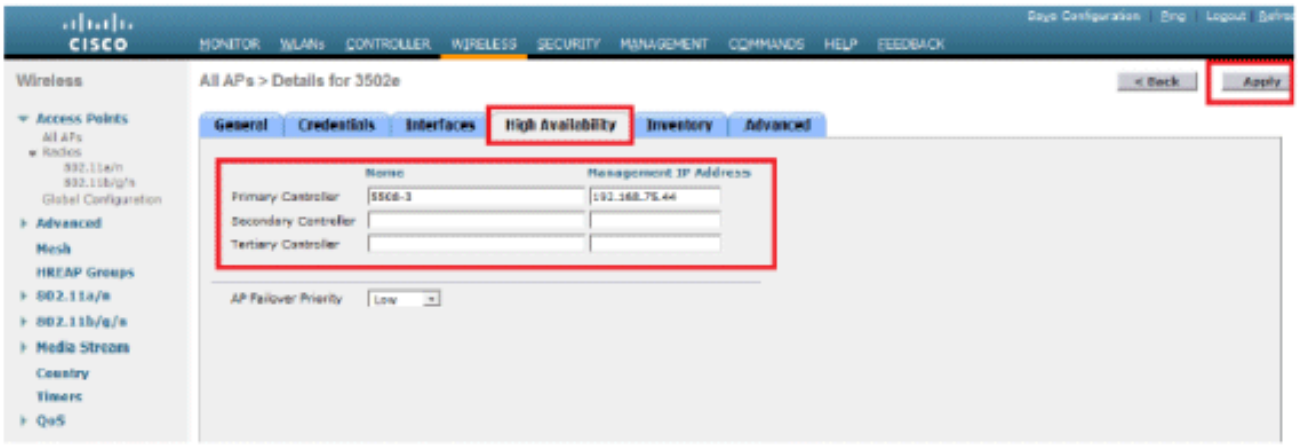
a. انتقل إلى لاسلكي > جميع نقاط الوصول، وحدد نقطة الوصول المعنية.

b. قم بإضافة اسم المستخدم وكلمة المرور في حقول بيانات اعتماد المدقق 802.1x.



ملاحظة: يتم إستخدام بيانات اعتماد تسجيل الدخول إلى Telnet أو SSH أو وحدة التحكم في نقطة الوصول.

3. قم بتكوين قسم التوفر العالي، وانقر فوق تطبيق.



ملاحظة: بمجرد حفظ بيانات الاعتماد هذه، يتم الاحتفاظ بها عبر عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) وإعادة تمهيد نقطة الوصول. تتغير بيانات الاعتماد فقط عندما تنضم نقطة الوصول في الوضع Lightweight إلى عنصر تحكم في الشبكة المحلية اللاسلكية (WLC) جديد. يفترض ال{upper}lap ال username وكلمة أن كان شكلت على ال WLC جديد.

إذا لم تنضم نقطة الوصول إلى عنصر تحكم في الشبكة المحلية اللاسلكية (WLC) في الوضع Lightweight بعد، فيجب عليك وحدة التحكم في الدخول إلى نقطة الوصول في يمكن أسلوب: لتعيين بيانات الاعتماد. أصدرت هذه CLI أمر في

lap#lwapp ap dot1x username <username> كلمة <password>

أو

lap#capwap ap dot1x username <username> كلمة <password>

ملاحظة: يتوفر هذا الأمر فقط لنقاط الوصول التي تشغل صورة الاسترداد.

التقصير username وكلمة ل ال{upper}lap `cisco` و`cisco` على التوالي.

تكوين المحول

يعمل المحول كمصدق لنقطة الوصول في الوضع Lightweight ويصادق نقطة الوصول في الوضع Lightweight. إذا لم يكن المحول يتضمن البرنامج المتوافق، قم بترقية المحول. في المحول CLI، قم بإصدار هذه الأوامر لتمكين مصادقة 802.1x على منفذ محول:

```
<#root>

switch#

configure terminal

switch(config)#

dot1x system-auth-control

switch(config)#

aaa new-model


!--- Enables 802.1x on the Switch.

switch(config)#

aaa authentication dot1x default group radius

switch(config)#

radius server host 192.168.150.24 key cisco


!--- Configures the RADIUS server with shared secret and enables switch to send !--- 802.1x information

switch(config)#

ip radius source-interface vlan 253


!--- We are sourcing RADIUS packets from VLAN 253 with NAS IP: 192.168.153.10.

switch(config)interface gigabitEthernet 0/11
     switch(config-if)switchport mode access
  switch(config-if)switchport access vlan 253
         switch(config-if)mls qos trust dscp
     switch(config-if)spanning-tree portfast


!--- gig0/11 is the port number on which the AP is connected.

switch(config-if)dot1x pae authenticator

!--- Configures dot1x authentication.

switch(config-if)dot1x port-control auto

!--- With this command, the switch initiates the 802.1x authentication.
```

802.1x، مالحظة: إذا كانت لديك نقاط وصول أخرى على المحول نفسه والتي تريدها أن تستخدم
:فيمكنك إما ترك المنفذ غير مكون لـ 802.1x أو إصدار هذا الأمر

<#root>

```
switch(config-if)authentication port-control force-authorized
```

تكوين خادم RADIUS

إذا هذه EAP طريقة تدعم يذلا RADIUS خادم أن من تأكد .EAP-FAST مع LAP يصادق
.Cisco ACS 5.2 تستخدم لم تكن

:أربع خطوات إلى RADIUS خادم تكوين يتم تقسيم

1. قم بتكوين موارد الشبكة.
2. قم بتكوين المستخدمين.
3. تعريف عناصر السياسة.
4. تطبيق سياسات الوصول.

ACS 5.x هو مصدر المحتوى الإضافي القائم على السياسات. وبمعنى آخر، يستخدم ACS 5.x نموذج سياسة مستند إلى قواعد بدلا من النموذج المستند إلى مجموعة المستخدم في إصدارات 4.x.

ويوفر نموذج السياسات القائمة على قواعد ACS 5.x سيطرة على الوصول تتسم بمزيد من القوة والمرونة مقارنة بالنهج القديم القائم على المجموعات.

في النموذج الأقدم المستند إلى مجموعة، تحدد مجموعة النهج لأنها تحتوي على ثلاثة أنواع من المعلومات وترتبط بينها:

- معلومات الهوية - يمكن أن تستند هذه المعلومات إلى العضوية في مجموعات AD أو LDAP أو تعيين ثابت لمستخدمي ACS الداخليين.
- قيود أو شروط أخرى - قيود الوقت وقيود الأجهزة وما إلى ذلك.
- أذون - شبكات VLAN أو مستويات امتيازات Cisco IOS®.

:يستند نموذج سياسة ACS 5.x إلى قواعد النموذج

إذا كانت الحالة تتجه

على سبيل المثال، نستخدم المعلومات الموصوفة للنموذج المستند إلى مجموعة:

في حالة وجود حالة هوية أو شرط تقييد ثم ملف تعريف التخويل.

وتتجه لذلك، يوفر لنا هذه مرونة لتحديد الشروط التي يسمح للمستخدم بالوصول إلى

الشبكة في ظلام وأيضا ما هو مستوى التخويل المسموح به عند استيفاء شروط معينة.

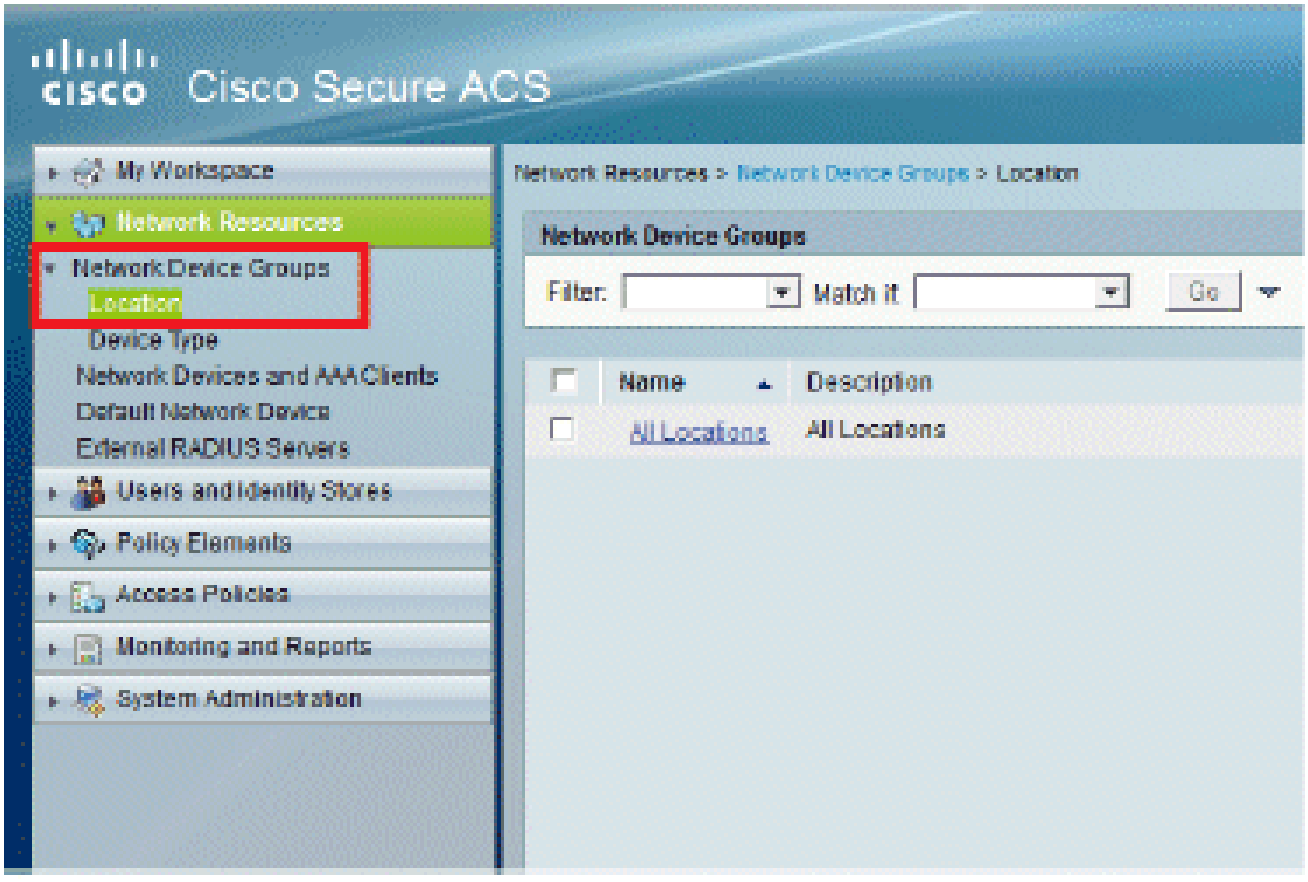
تكوين موارد الشبكة

في هذا القسم، نقوم بتكوين عميل AAA للمحول على خادم RADIUS.

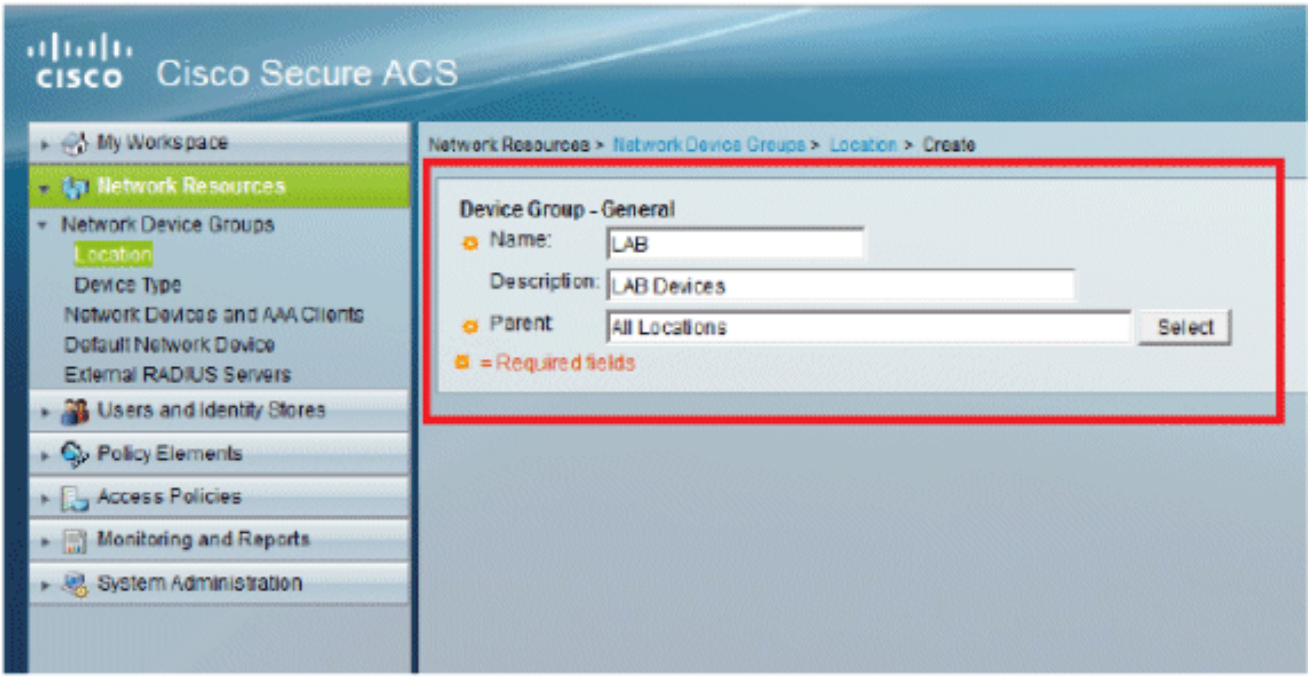
يشرح هذا الإجراء كيفية إضافة المحول كعميل AAA على خادم RADIUS حتى يمكن للمحول تمرير بيانات اعتماد المستخدم الخاصة ببروتوكول LAP إلى خادم RADIUS.

أكمل الخطوات التالية:

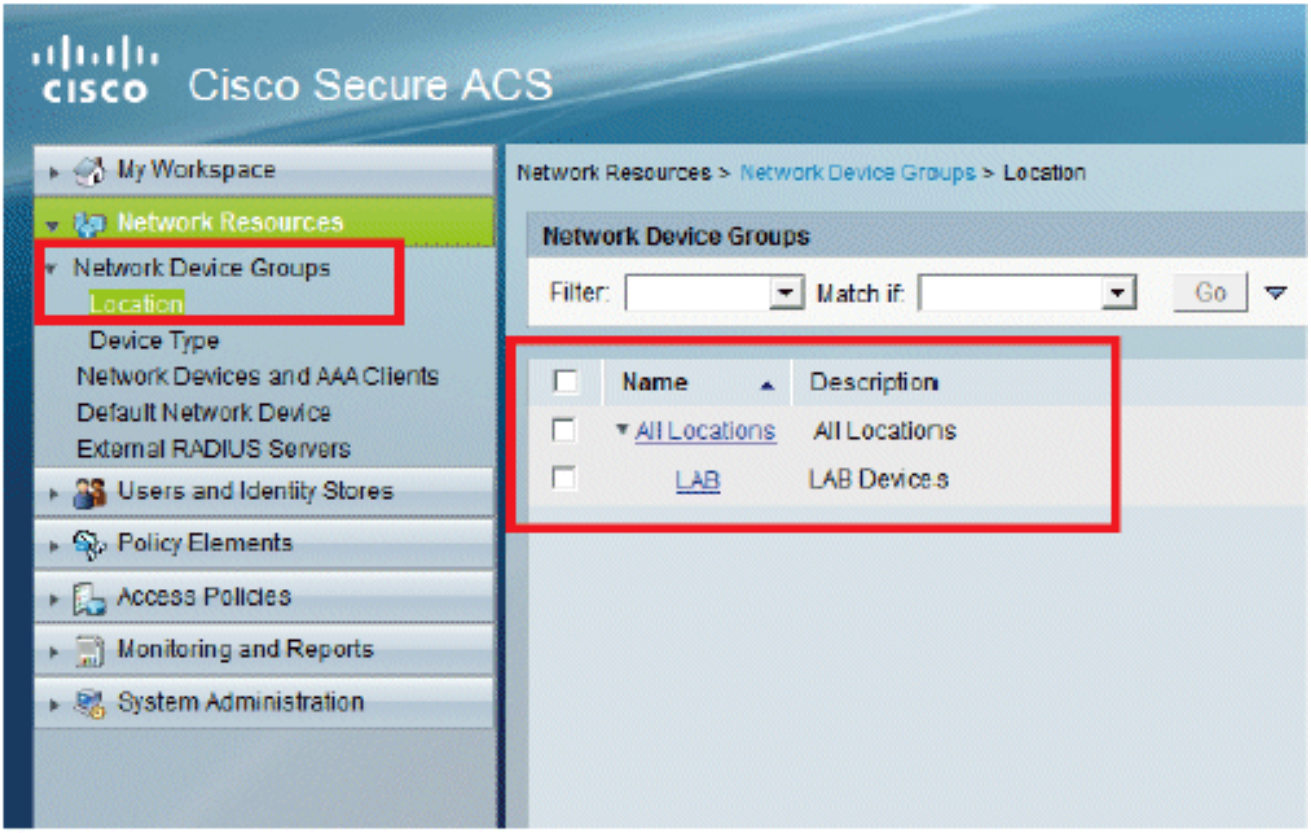
1. من واجهة المستخدم الرسومية (ACS)، انقر فوق موارد الشبكة.
2. انقر فوق مجموعات أجهزة الشبكة.
3. انتقل إلى الموقع > إنشاء (في الأسفل).



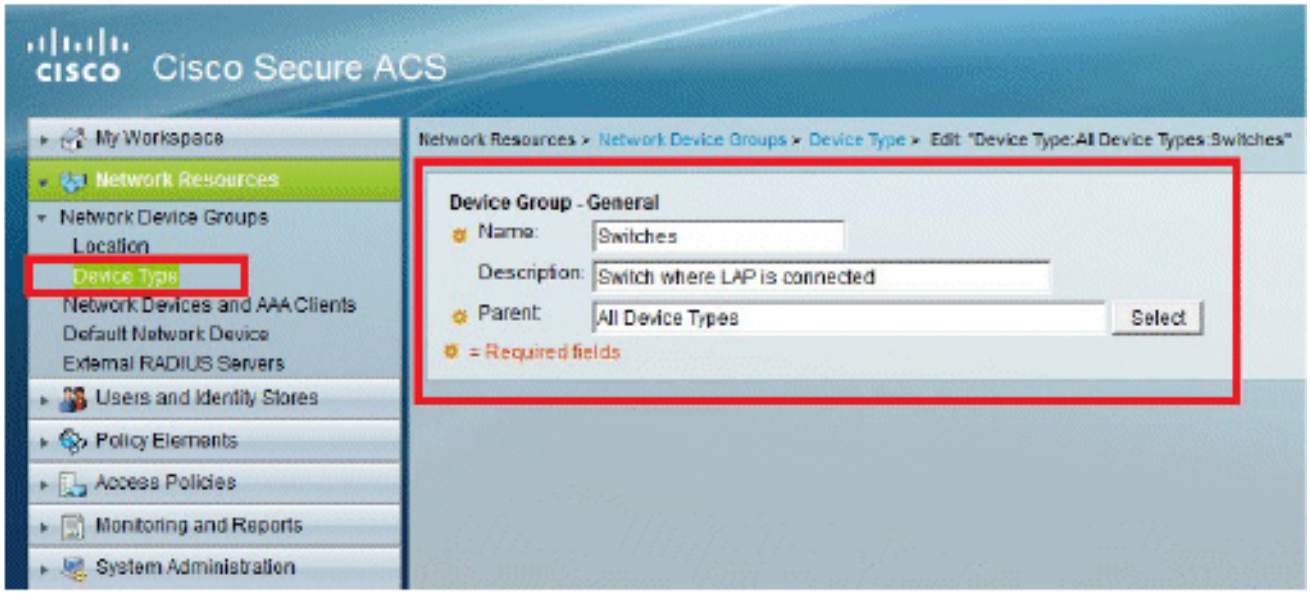
4. قم بإضافة الحقول المطلوبة وانقر فوق إرسال.



5. يتم تحديث النافذة:



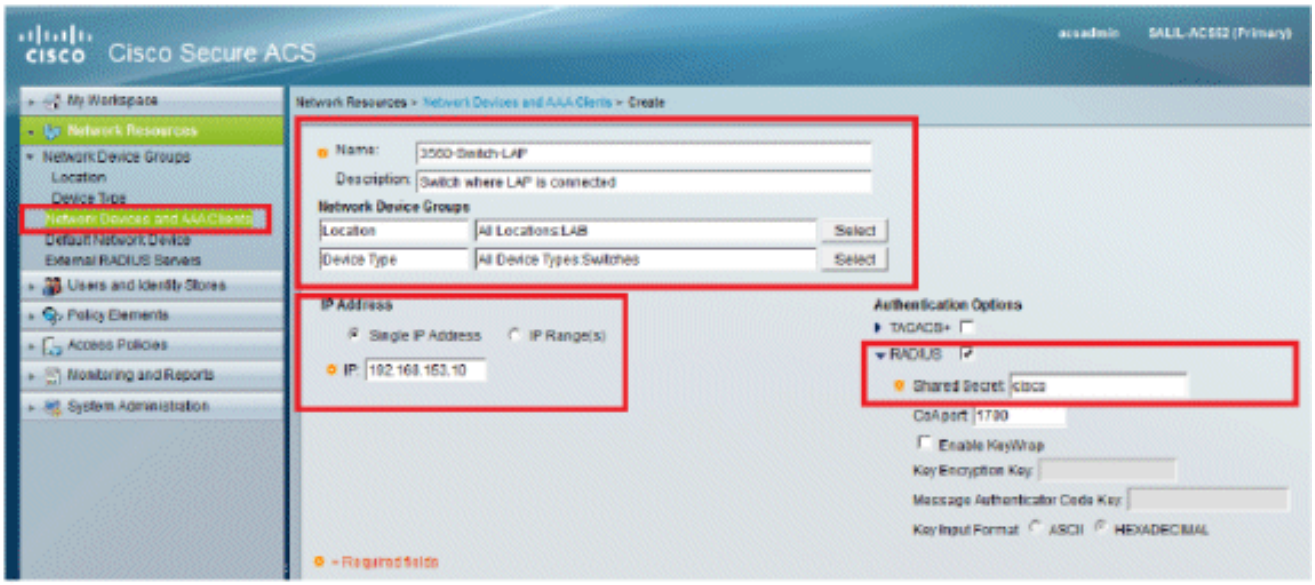
6. انقر فوق نوع الجهاز > إنشاء.



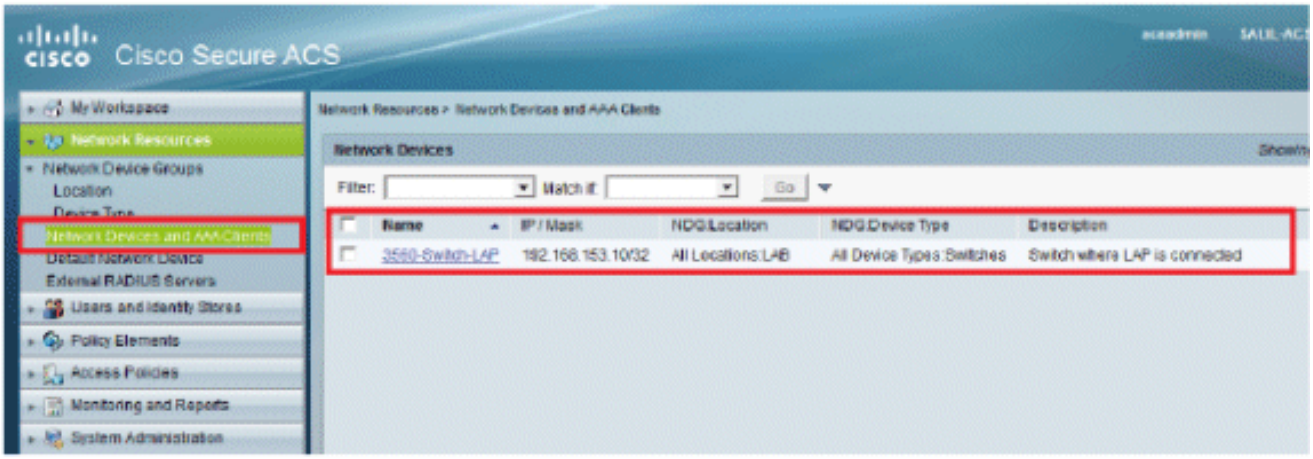
7. انقر على إرسال. بمجرد اكتمال هذه العملية، يتم تحديث النافذة:

8. انتقل إلى موارد الشبكة > أجهزة الشبكة وعملاء AAA.

9. انقر فوق إنشاء، وقم بتعبئة التفاصيل كما هو موضح هنا:



10. انقر على إرسال. يتم تحديث النافذة:

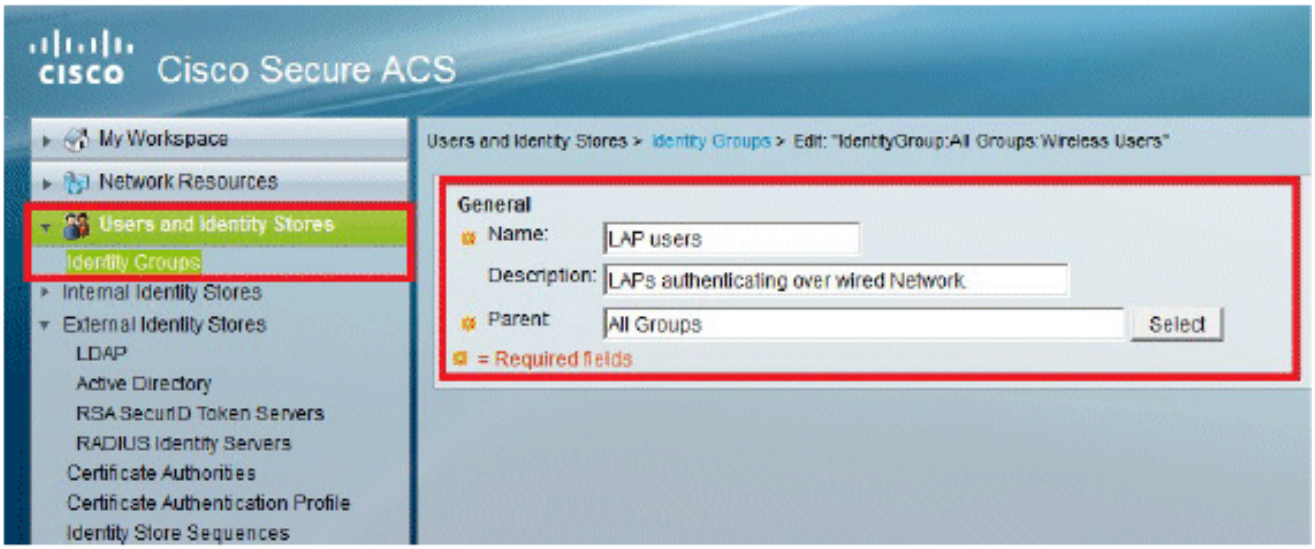


تكوين المستخدمين

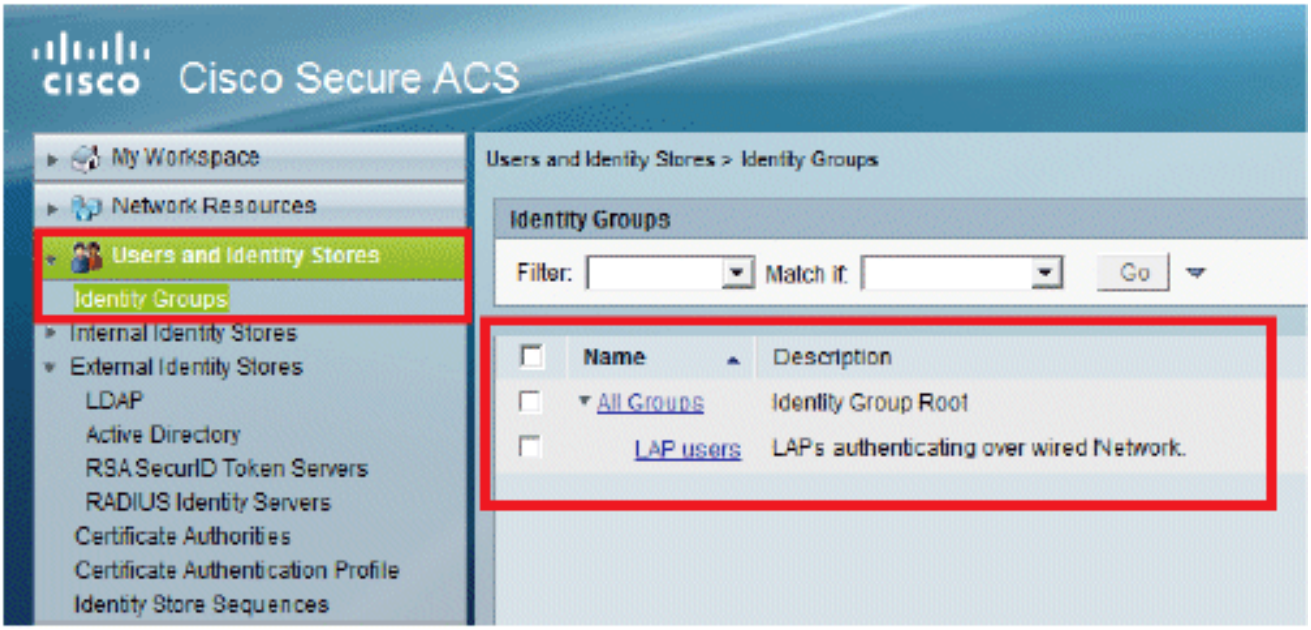
في هذا قسم، أنت سترى كيف أن يخلق مستعمل على ال ACS يشكل سابقا. ستقوم بتعيين المستخدم إلى مجموعة تسمى "مستخدمو LAP".

أكمل الخطوات التالية:

1. انتقل إلى المستخدمين ومخازن الهوية > مجموعات الهوية > إنشاء

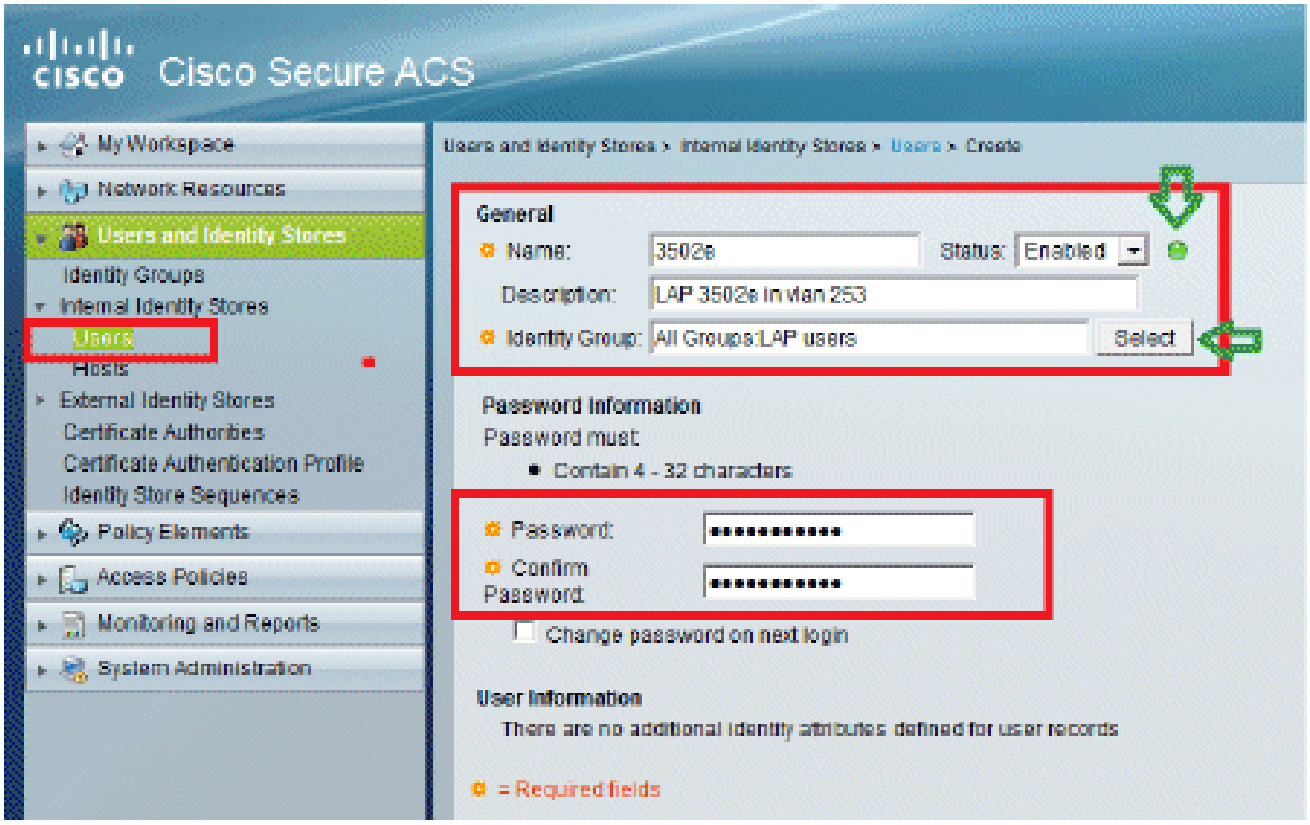


.2انقر فوق إرسال.

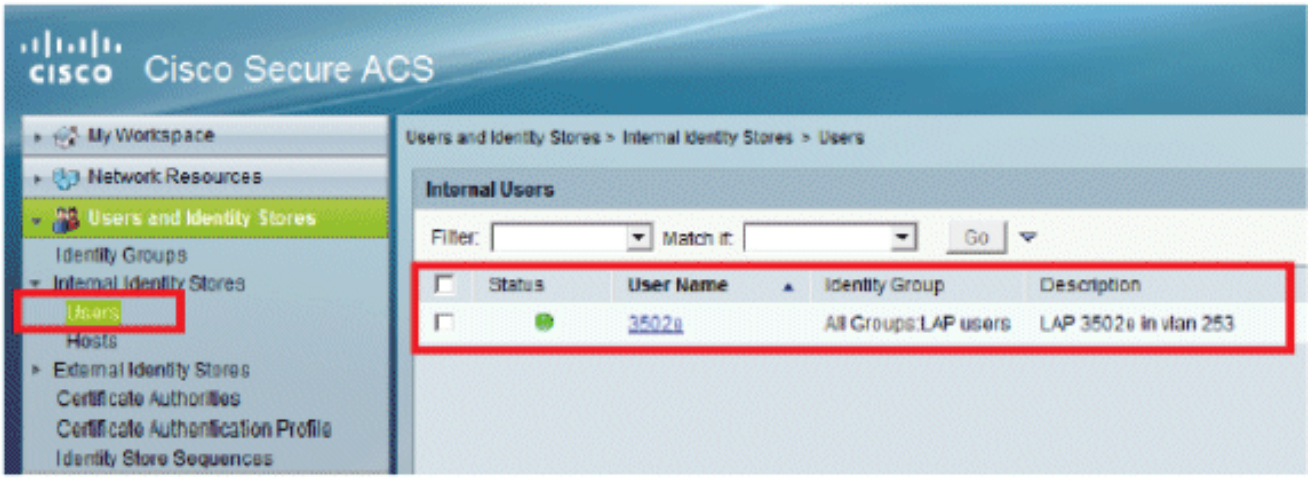


.3قم بإنشاء 3502e وتعيينه لمجموعة "مستخدمي LAP".

.4انتقل إلى المستخدمين ومخازن الهوية > مجموعات الهوية>المستخدمين>Create.

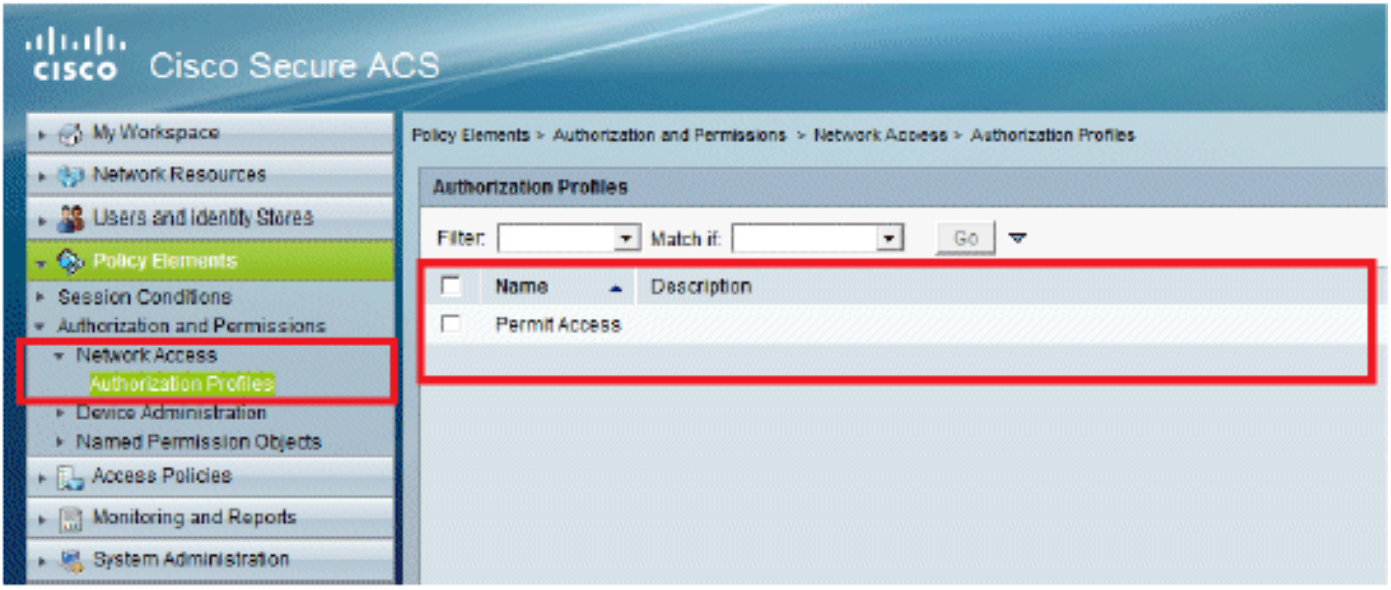


سيظهر لديك المعلومات المحدثة:5.



تعريف عناصر السياسة

تحقق من تعيين السماح بالوصول.

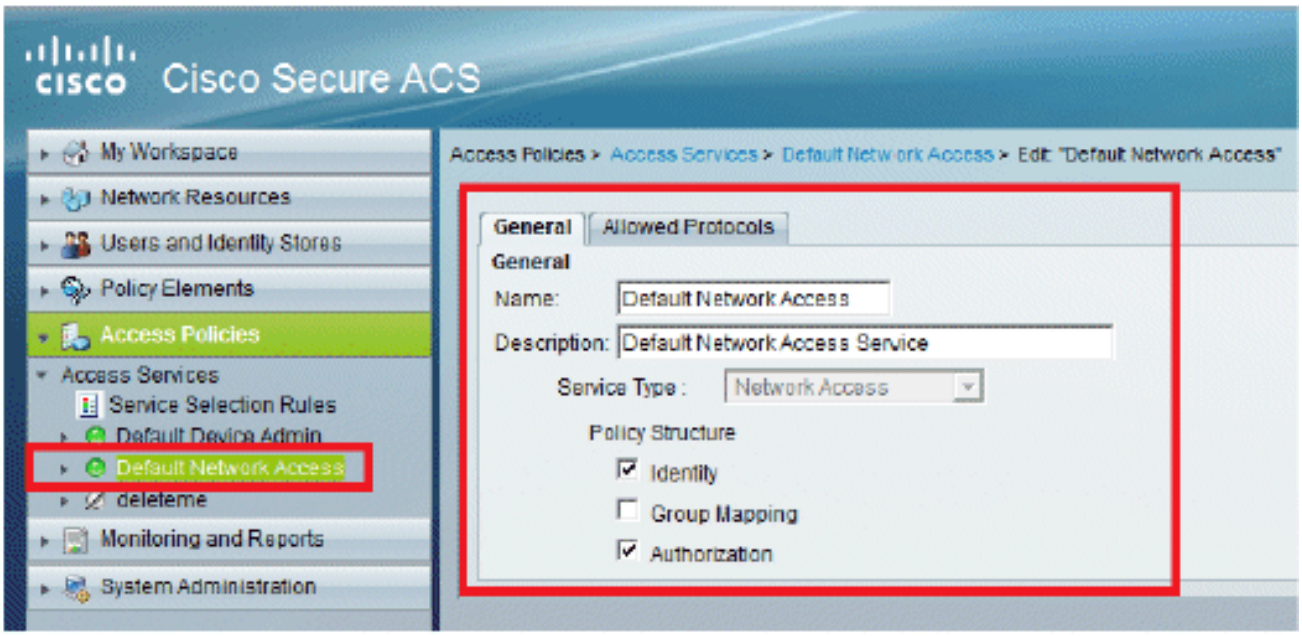


تطبيق سياسات الوصول

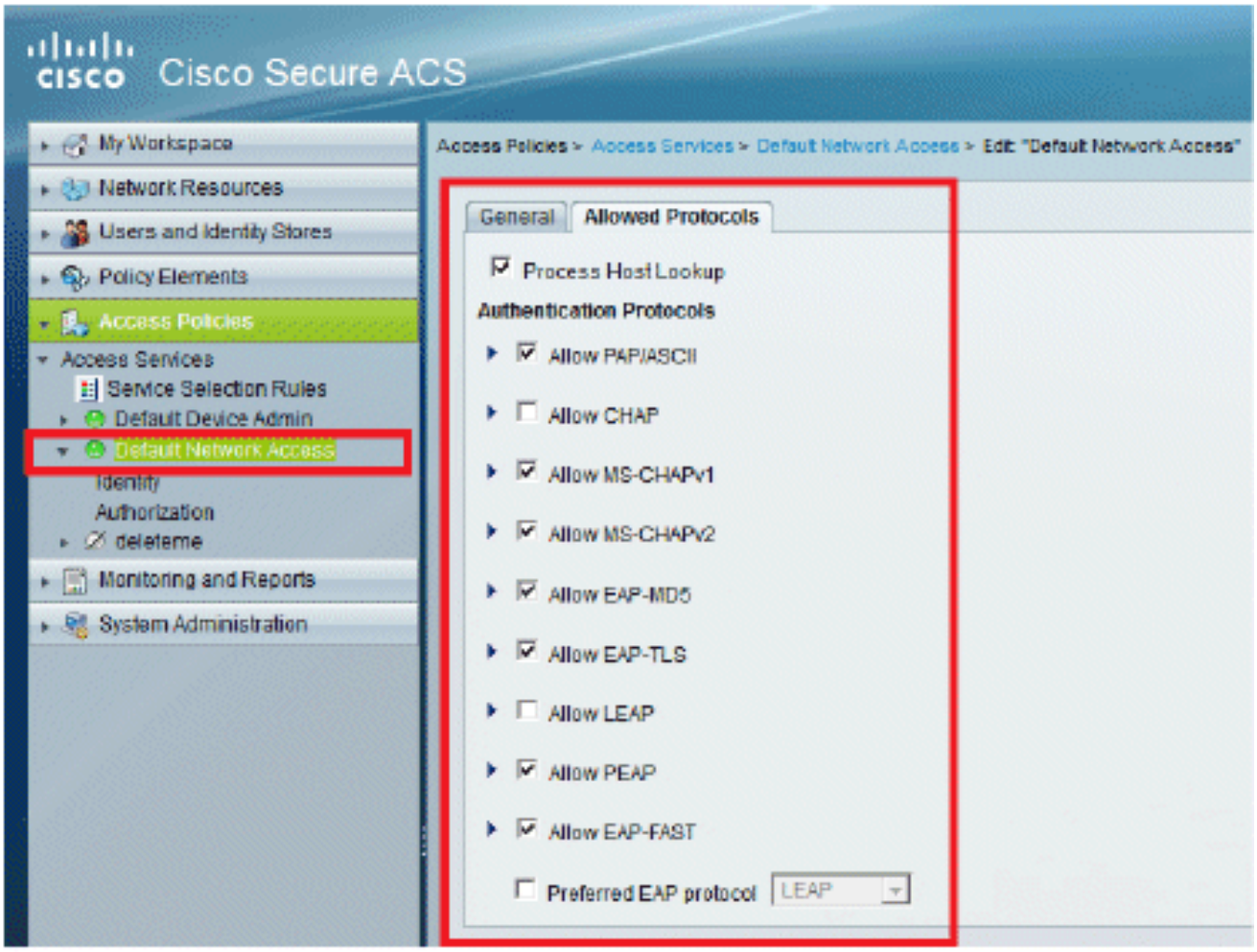
في هذا القسم، ستقوم بتحديد EAP-FAST كطريقة مصادقة تستخدم لنقاط الوصول في الوضع Lightweight للمصادقة. ستقوم بعد ذلك بإنشاء قواعد استناد إلى الخطوات السابقة.

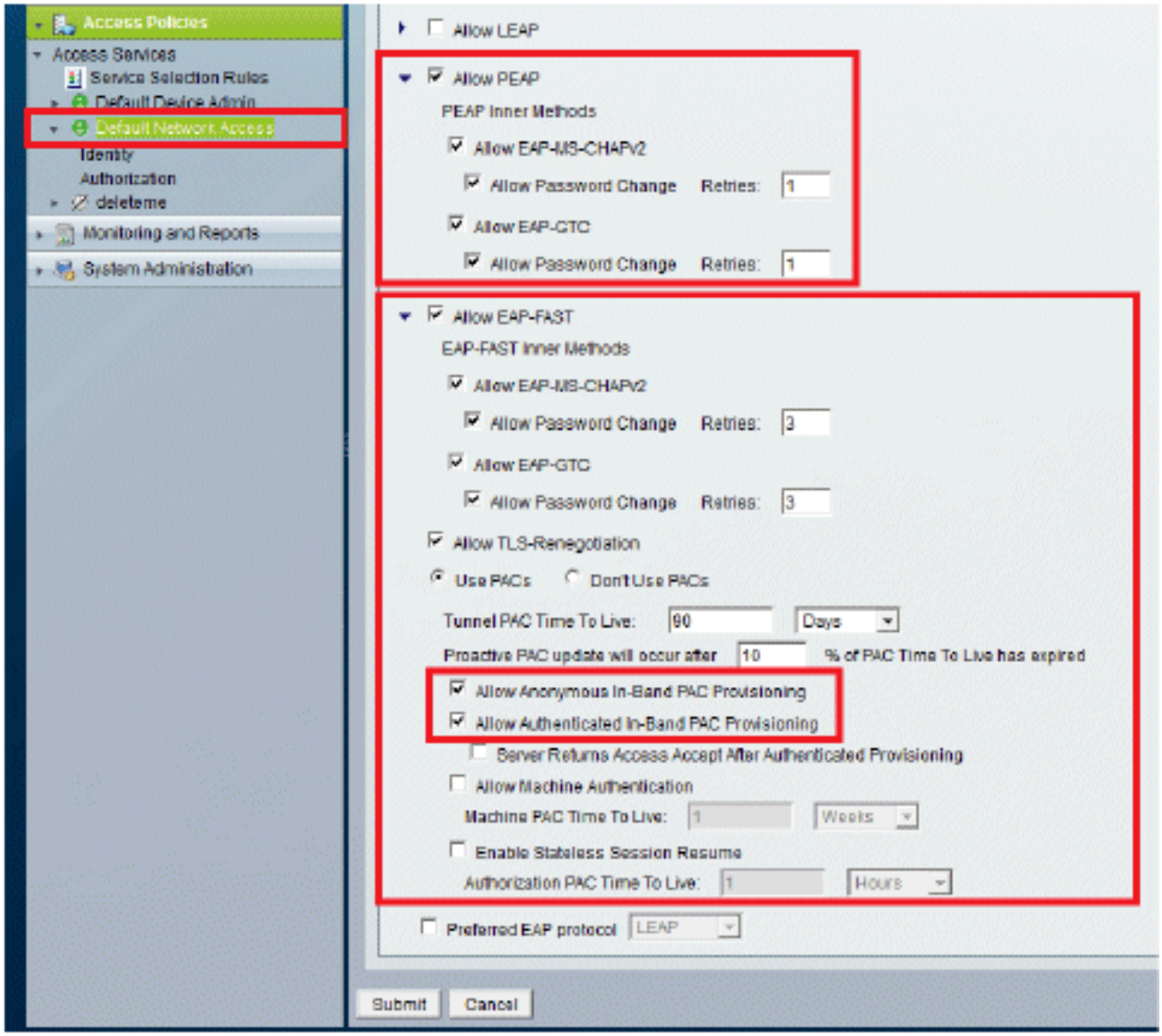
أكمل الخطوات التالية:

1. انتقل إلى سياسات الوصول>خدمات الوصول>الوصول الافتراضي إلى الشبكة>تحرير: "الوصول الافتراضي إلى الشبكة".



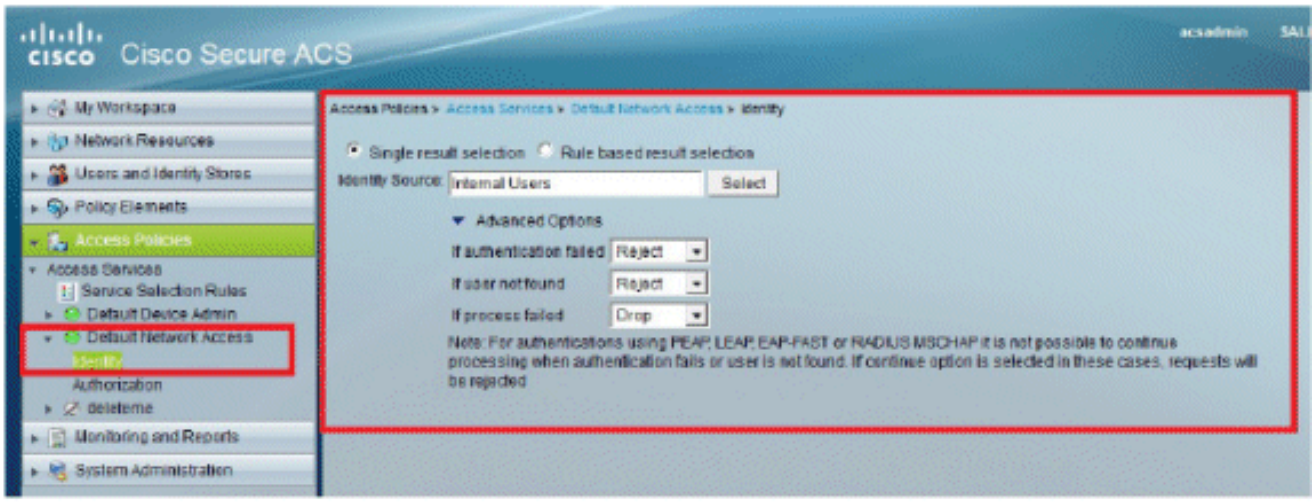
2. تأكد من تمكين EAP-FAST وتزويد PAC داخل النطاق مجهول.


Cisco Secure ACS
My Workspace
Network Resources
Users and Identity Stores
Policy Elements
Access Policies
Access Services
Service Selection Rules
Default Device Admin
Default Network Access
Identity
Authorization
deleteme
Monitoring and Reports
System Administration
Access Policies > Access Services > Default Network Access > Edit: "Default Network Access"
General
Allowed Protocols
Process Host Lookup
Authentication Protocols
Allow PAP/ASCII
Allow CHAP
Allow MS-CHAPv1
Allow MS-CHAPv2
Allow EAP-MD5
Allow EAP-TLS
Allow LEAP
Allow PEAP
Allow EAP-FAST
Preferred EAP protocol
LEAP



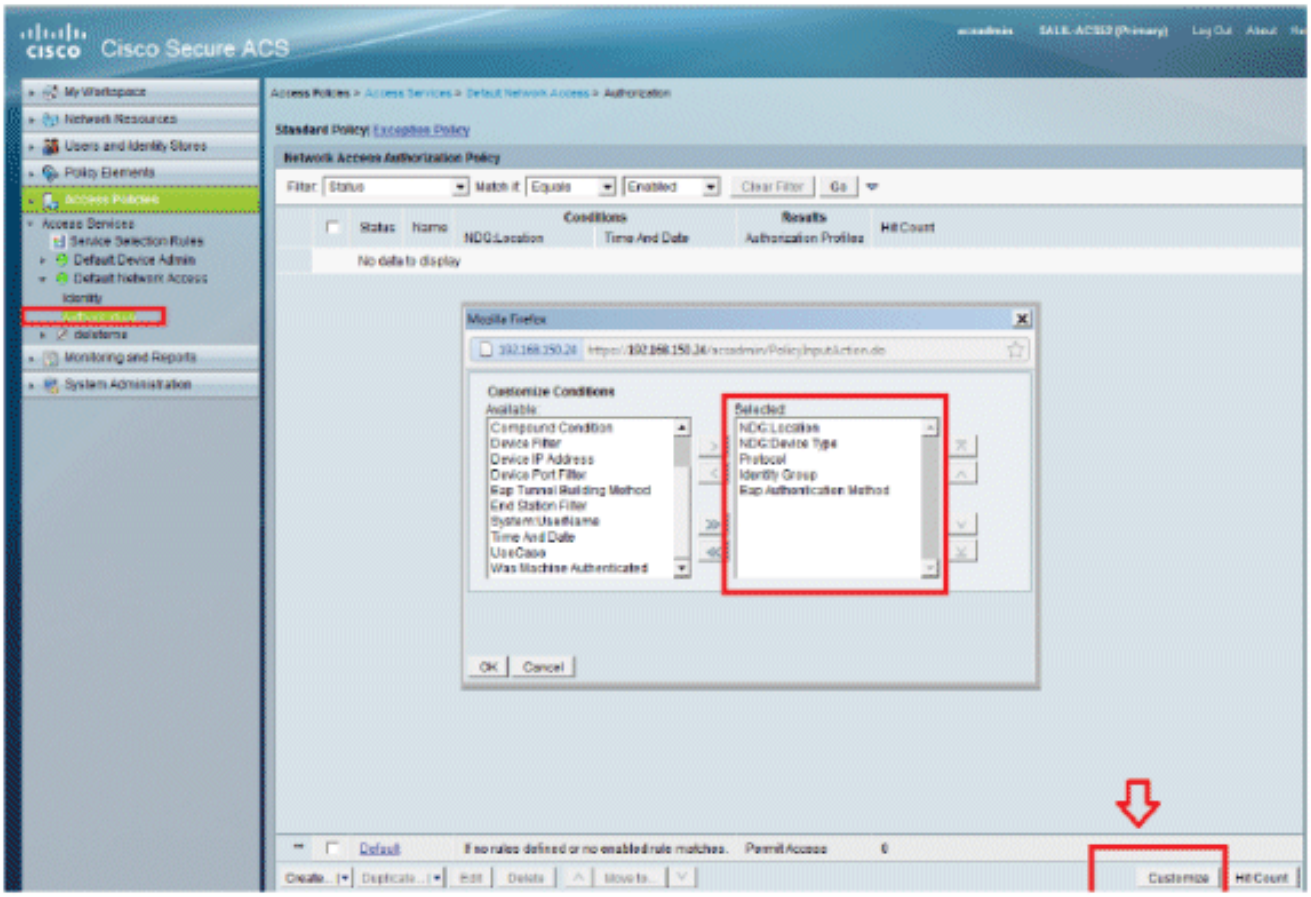
3. انقر على إرسال.

4. تحقق من مجموعة الهوية التي قمت بتحديدها. في هذا المثال، أستخدم المستخدمين الداخليين (والذي تم إنشاؤه على ACS) واحفظ التغييرات.



5. انتقل إلى سياسات الوصول>خدمات الوصول>الوصول الافتراضي إلى الشبكة>التفويض للتحقق من ملف تعريف التفويض.

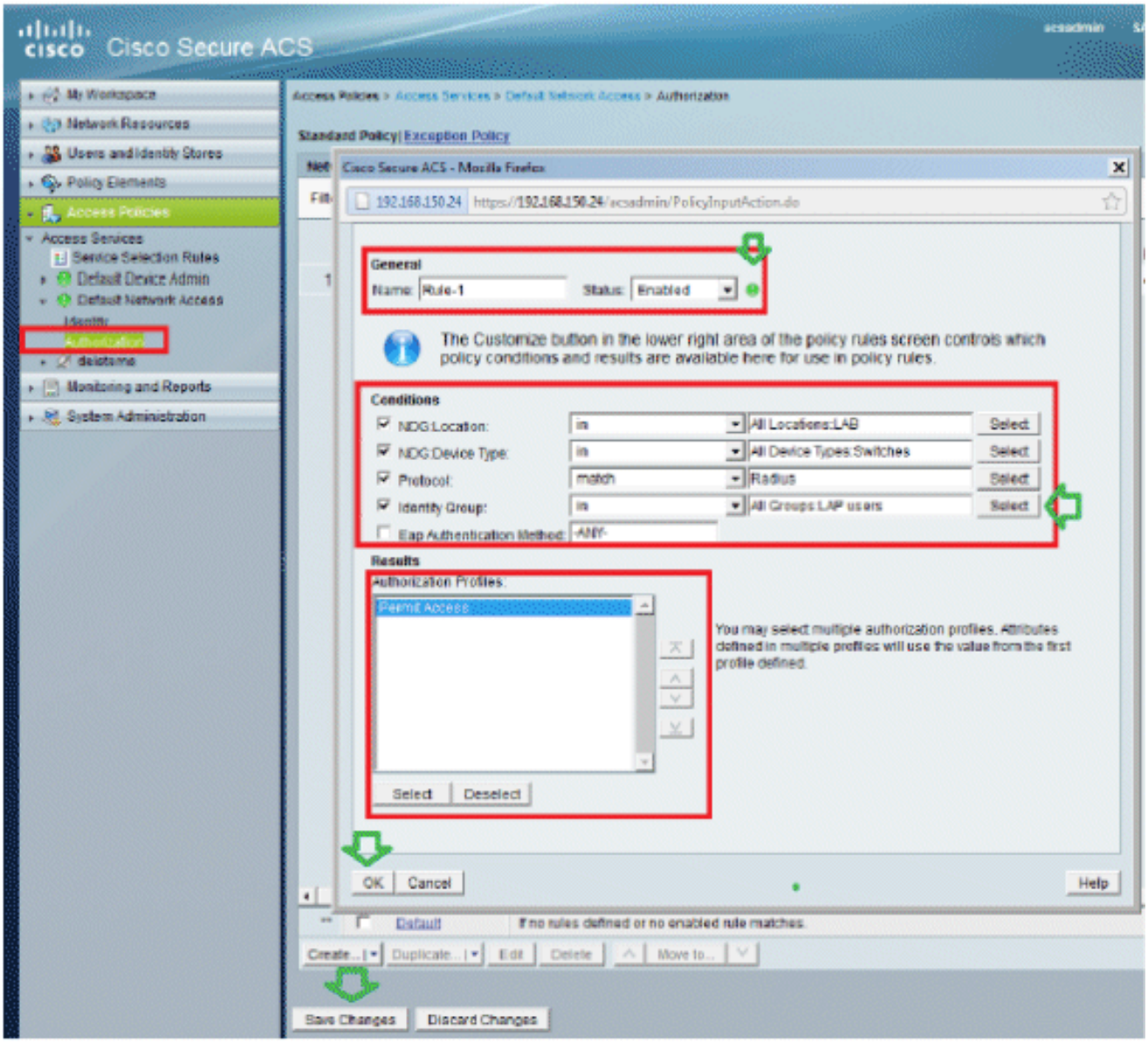
يمكنك التخصيص تحت أي شروط ستتيح لمستخدم الوصول إلى الشبكة وأي توصيف تخويل (سمات) ستتمريره بمجرد المصادقة عليه. والا تتوفر هذه القابلية للتعديل إلا في ACS 5.x. في هذا المثال، يتم تحديد الموقع، نوع الجهاز، البروتوكول، مجموعة الهوية، وأسلوب مصادقة EAP.



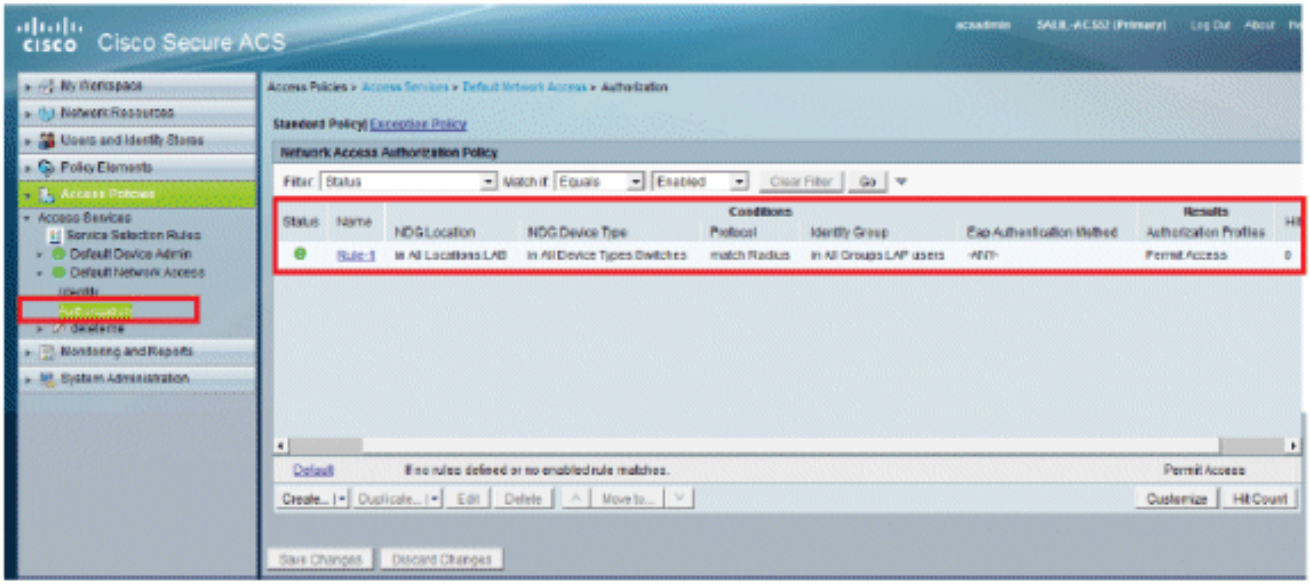
6. انقر فوق موافق، ثم احفظ التغييرات.

7. تتمثل الخطوة التالية في إنشاء قاعدة. إذا لم يتم تعريف أي قواعد، يتم السماح بوصول نقاط الوصول في الوضع Lightweight دون أي شروط.

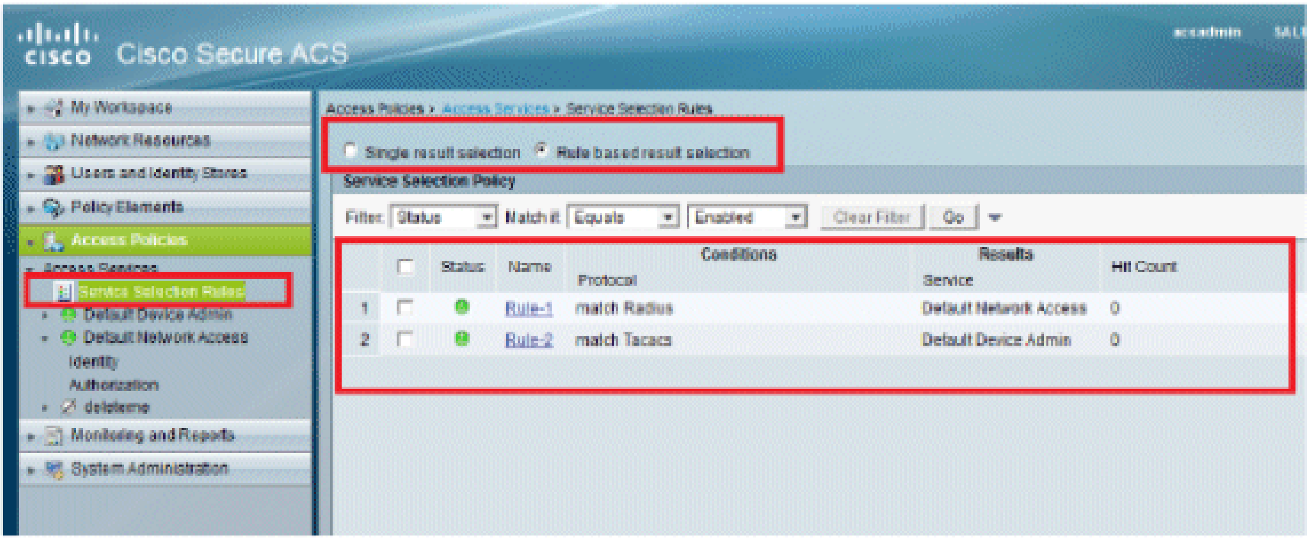
8. انقر فوق إنشاء > القاعدة-1. هذه القاعدة للمستخدمين في مجموعة "مستخدمي LAP".



انقر فوق حفظ التغييرات. إذا كنت تريد رفض المستخدمين الذين لا يتطابقون مع9. الشروط، قم بتحرير القاعدة الافتراضية لتقول "رفض الوصول".



10. تتمثل الخطوة الأخيرة في تحديد قواعد تحديد الخدمة. أستخدم هذه الصفحة لتكوين نهج بسيط أو مستند إلى قواعد لتحديد الخدمة التي سيتم تطبيقها على الطلبات الواردة. على سبيل المثال:



التحقق من الصحة

من تمكين 802.1x على المنفذ، يتم منع مرور حركة المرور كلها باستثناء مرور حركة مرور 802.1x خلال الميناء. يتم فصل نقطة الوصول (LAP)، والتي تم تسجيلها بالفعل إلى عنصر التحكم في الشبكة المحلية اللاسلكية (WLC). لا يسمح لحركة المرور الأخرى بالمرور إلا بعد مصادقة 802.1x الناجحة. يشير التسجيل الناجح لنقطة الوصول في الوضع Lightweight إلى عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) بعد تمكين معيار 802.1x على المحول إلى نجاح مصادقة نقطة الوصول Lightweight (LAP).

وحدة تحكم AP:

<#root>

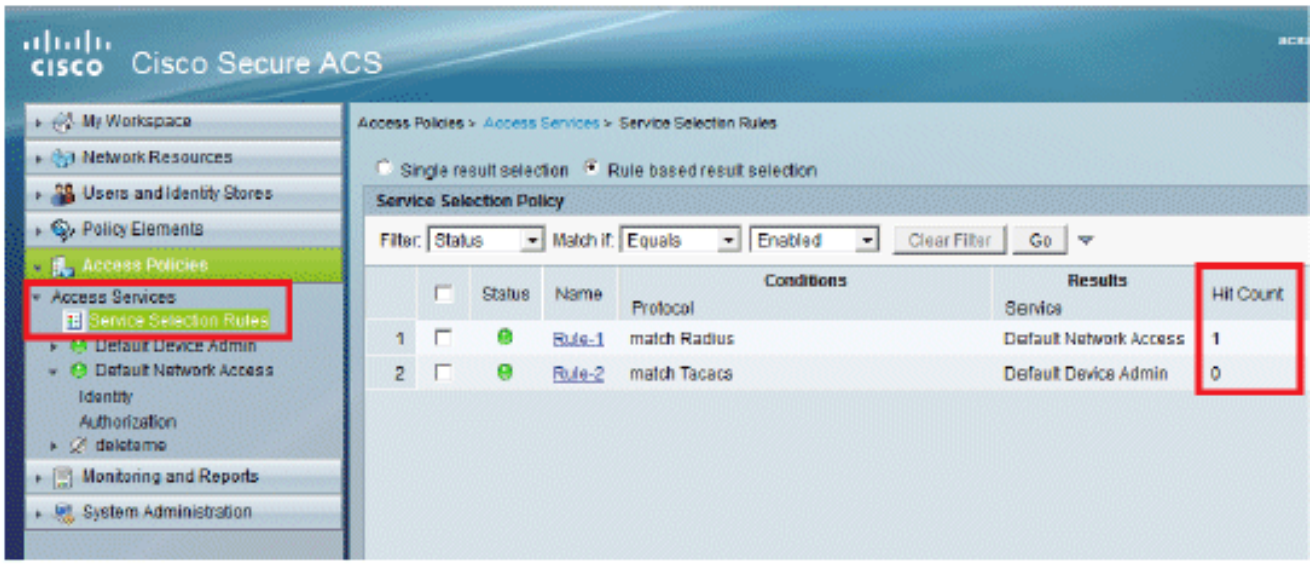
```
*Jan 29 09:10:24.048: %DTLS-5-SEND_ALERT: Send FATAL : Close notify Alert to
192.168.75.44:5246
*Jan 29 09:10:27.049: %DTLS-5-SEND_ALERT: Send FATAL : Close notify Alert to
192.168.75.44:5247

!--- AP disconnects upon adding dot1x information in the gig0/11.

*Jan 29 09:10:30.104: %WIDS-5-DISABLED: IDS Signature is removed and disabled.
*Jan 29 09:10:30.107: %CAPWAP-5-CHANGED: CAPWAP changed state to DISCOVERY
*Jan 29 09:10:30.107: %CAPWAP-5-CHANGED: CAPWAP changed state to DISCOVERY
*Jan 29 09:10:30.176: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to
administratively down
*Jan 29 09:10:30.176: %LINK-5-CHANGED: Interface Dot11Radio1, changed state to
administratively down
*Jan 29 09:10:30.186: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to
reset
*Jan 29 09:10:30.201: %LINK-3-UPDOWN: Interface Dot11Radio1, changed state to up
*Jan 29 09:10:30.211: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
*Jan 29 09:10:30.220: %LINK-5-CHANGED: Interface Dot11Radio1, changed state to
reset
```

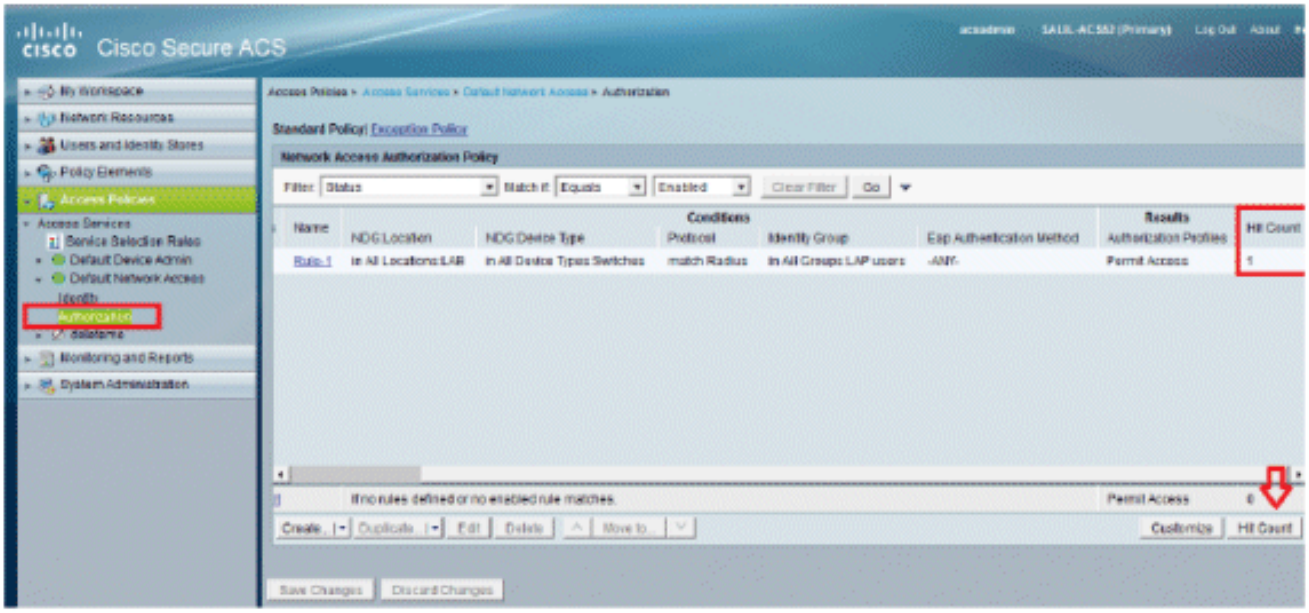
```
Translating "CISCO-CAPWAP-CONTROLLER"...domain server (192.168.150.25)
*Jan 29 09:10:36.203: status of voice_diag_test from WLC is false

*Jan 29 09:11:05.927: %DOT1X_SHIM-6-AUTH_OK: Interface GigabitEthernet0 authenticated [EAP-FAST] *Jan 29

!--- Authentication is successful and the AP gets an IP.

Translating "CISCO-CAPWAP-CONTROLLER.Wlab"...domain server (192.168.150.25)
*Jan 29 09:11:37.000: %CAPWAP-5-DTLSREQSEND: DTLS connection request sent
peer_ip: 192.168.75.44 peer_port: 5246
*Jan 29 09:11:37.000: %CAPWAP-5-CHANGED: CAPWAP changed state to
*Jan 29 09:11:37.575: %CAPWAP-5-DTLSREQSUCC: DTLS connection created
successfully peer_ip: 192.168.75.44 peer_port: 5246
*Jan 29 09:11:37.578: %CAPWAP-5-SENDJOIN: sending Join Request to 192.168.75.44

*Jan 29 09:11:37.578: %CAPWAP-5-CHANGED: CAPWAP changed state to JOIN

*Jan 29 09:11:37.748: %CAPWAP-5-CHANGED: CAPWAP chan
wmmAC status is FALSEged state to CFG
*Jan 29 09:11:38.890: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to
down
*Jan 29 09:11:38.900: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to
reset
*Jan 29 09:11:38.900: %CAPWAP-5-CHANGED: CAPWAP changed state to UP
*Jan 29 09:11:38.956: %CAPWAP-5-JOINEDCONTROLLER: AP has joined controller
5508-3
*Jan 29 09:11:39.013: %CAPWAP-5-DATA_DTLS_START: Starting Data DTLS handshake.
Wireless client traffic will be blocked until DTLS tunnel is established.
*Jan 29 09:11:39.013: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
*Jan 29 09:11:39.016: %LWAPP-3-CLIENTEVENTLOG: SSID goa added to the slot[0]
*Jan 29 09:11:39.028: %LINK-3-UPDOWN: Interface Dot11Radio1, changed state to
down
*Jan 29 09:11:39.038: %LINK-5-CHANGED: Interface Dot11Radio1, changed state to
reset
*Jan 29 09:11:39.054: %LINK-3-UPDOWN: Interface Dot11Radio1, changed state to up
*Jan 29 09:11:39.060: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to
down
*Jan 29 09:11:39.069: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to
reset
*Jan 29 09:11:39.085: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
*Jan 29 09:11:39.135: %LWAPP-3-CLIENTEVENTLOG: SSID goa added to the slot[1]DTLS
keys are plumbed successfully.
*Jan 29 09:11:39.151: %CAPWAP-5-DATA_DTLS_ESTABLISHED: Data DTLS tunnel
established.
*Jan 29 09:11:39.161: %WIDS-5-ENABLED: IDS Signature is loaded and enabled

!--- AP joins the 5508-3 WLC.
```

سجلات ACS:

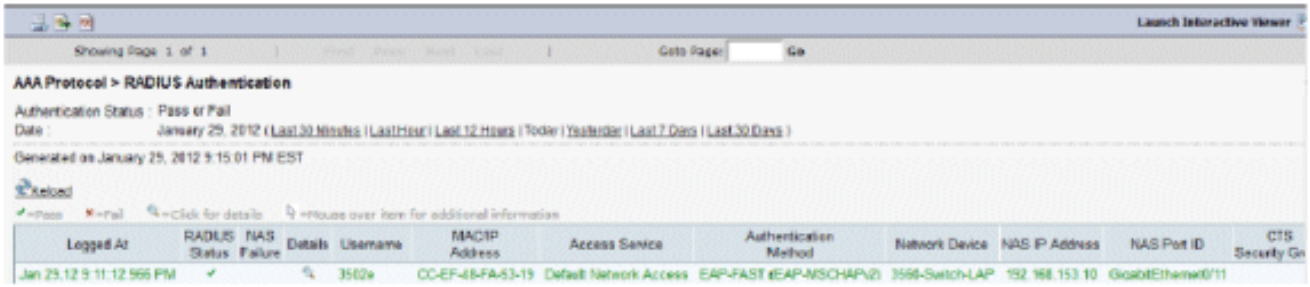
1. عرض عدد مرات الوصول:

إذا كنت تقوم بفحص السجلات خلال 15 دقيقة من المصادقة، فتأكد من تحديث عدد مرات الوصول. في نفس الصفحة، في الأسفل لديك علامة تبويب تعداد ضغطات.





طقطقة monitore and Reports ويظهر نافذة منبثقة جديد. انقر فوق مصادقة -RADIUS2. -اليوم. يمكنك أيضا النقر فوق Details للتحقق من قاعدة تحديد الخدمة التي تم تطبيقها.



استكشاف الأخطاء وإصلاحها

لا توفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

معلومات ذات صلة

- [نظام التحكم في الوصول الآمن من Cisco](#)
- [الدعم التقني والمستندات - Cisco Systems](#)

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).