المصادقة المركزية للويب مع محول وماث تكوين محرك خدمات الهوية

المحتويات

المقدمة

يوضح هذا المستند كيفية تكوين مصادقة الويب المركزية مع العملاء السلكيين المتصلين بالمحولات بمساعدة محرك خدمات الهوية (ISE).

يتعارض مفهوم مصادقة الويب المركزية مع مصادقة الويب المحلية، وهي مصادقة الويب المعتادة على المحول نفسه. في هذا النظام، عند فشل dot1x/mab، سيقوم المحول بتجاوز الفشل إلى ملف تعريف مصادقة الويب وسيعيد توجيه حركة مرور العميل إلى صفحة ويب على المحول.

توفر المصادقة المركزية للويب إمكانية وجود جهاز مركزي يعمل كبوابة ويب (في المثال، ISE). يمكن الاختلاف الرئيسي مقارنة بمصادقة الويب المحلية المعتادة في أنه تم تحويلها إلى الطبقة 2 مع مصادقة MAC/dot1x. كما يختلف المفهوم في أن خادم RADIUS (ISE في هذا المثال) يرجع سمات خاصة تشير إلى المحول الذي يجب أن تحدث إعادة توجيه ويب. هذا الحل يتميز بميزة التخلص من أي تأخير كان ضروريا لمصادقة الويب. بشكل عام، إذا كان عنوان MAC الخاص بمحطة العميل غير معروف بواسطة خادم RADIUS (ولكن يمكن أيضا إستخدام معايير أخرى)، يرجع الخادم سمات إعادة التوجيه، وبأذن المحول للمحطة (عبر تجاوز مصادقة MAC [MAB]) ولكنه يضع قائمة وصول إلإعادة توجيه حركة مرور الويب إلى البوابة. بمجرد تسجيل دخول المستخدم على مدخل الضيف، من الممكن عبر CoA (تغيير التفويض) أن يرتد منفذ المحول بحيث تحدث مصادقة MAB للطبقة 2 جديدة. يمكن أن يتذكر ISE بعد

ذلك أنه كان مستخدم مصادقة ويب وتطبق سمات الطبقة 2 (مثل تعيين VLAN الديناميكي) على المستخدم. كما يمكن أن يفرض تكوين ActiveX على كمبيوتر العميل تحديث عنوان IP الخاص به.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- محرك خدمات الهوية (ISE)
- تكوين محول Cisco IOS®

المكونات المستخدمة

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

- Cisco Identity Services Engine (ISE)، الإصدار 1.1.1
- cisco مادة حفازة 3560 sery مفتاح أن يركض برمجية صيغة 12.2.55SE3

ملاحظة: الإجراء مماثل أو مماثل لنماذج محولات Catalyst الأخرى. أنت يستطيع استعملت هذا steps على كل cisco ios برمجية إطلاق لمادة حفازة ما لم يذكر خلاف ذلك.

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.

التكوين

نظرة عامة

يتكون تكوين ISE من الخطوات الخمس التالية:

1. قم بإنشاء قائمة التحكم في الوصول (ACL) القابلة للتنزيل.
2. إنشاء ملف تعريف التفويض.
3. إنشاء قاعدة مصادقة.
4. إنشاء قاعدة تخويل.
5. قم بتمكين تحديد IP (إختياري).

إنشاء قائمة التحكم في الوصول (ACL) القابلة للتنزيل

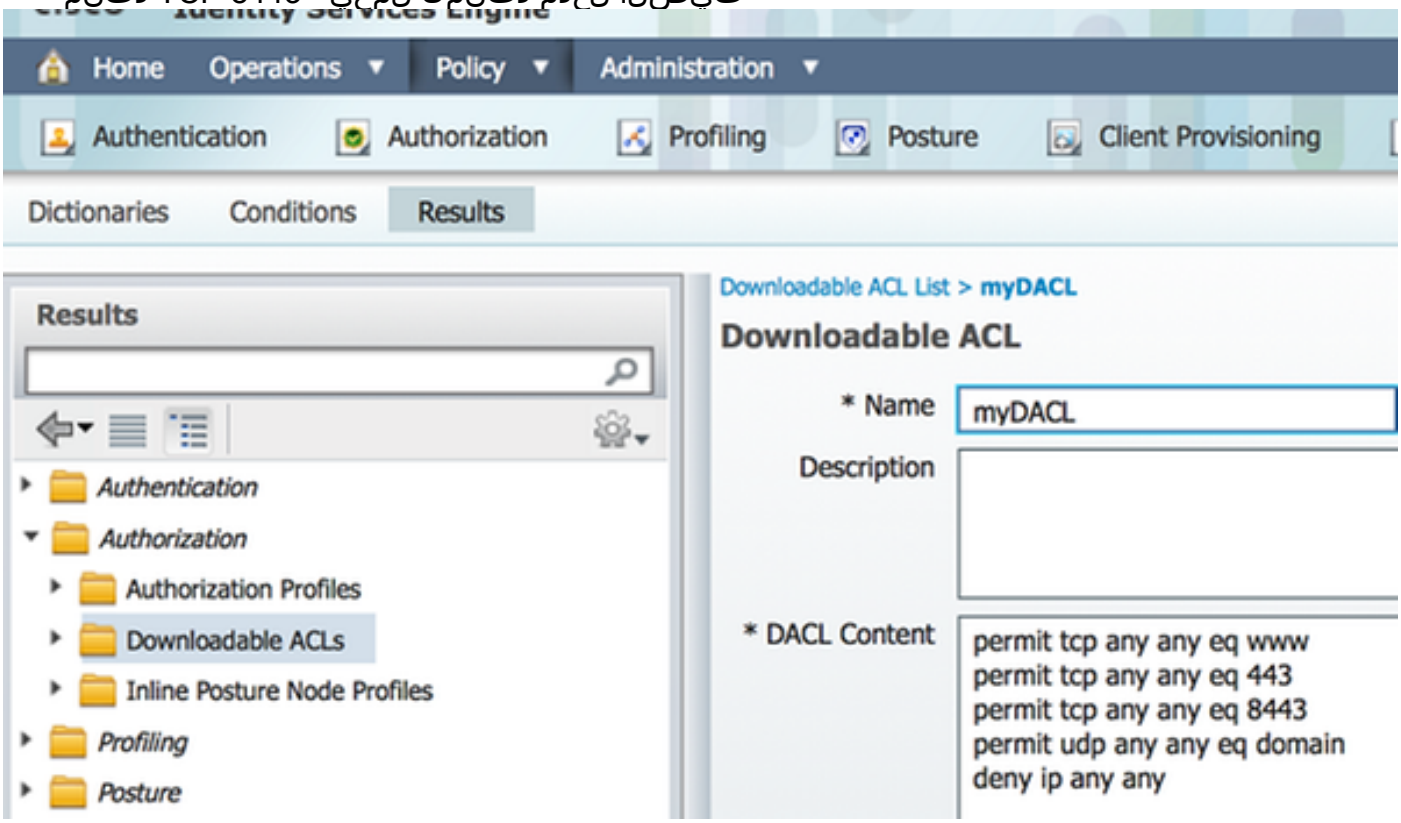
هذه ليست خطوة إلزامية. تحدد قائمة التحكم في الوصول (ACL) التي تم إرسالها مرة أخرى مع ملف تعريف مصادقة الويب المركزية حركة المرور (HTTP أو HTTPS) التي يتم إعادة توجيهها إلى ISE. تسمح كل قائمة التحكم في الوصول (ACL) القابلة للتنزيل بتحديد حركة المرور المسموح بها. يجب أن تسمح بشكل نموذجي ب DNS و HTTP(s) و 8443 ورفض البقية. وإلا، فسيعيد المحول توجيه حركة مرور HTTP ولكنه يسمح بالبروتوكولات الأخرى.

أكمل الخطوات التالية لإنشاء قائمة التحكم في الوصول (ACL) القابلة للتنزيل:

1. انقر فوق **نهج**، ثم انقر فوق **عناصر النهج**.
2. انقر فوق **النتائج**.
3. قم بتوسيع **التفويض**، وانقر فوق **قوائم التحكم في الوصول (ACL) القابلة للتنزيل**.
4. انقر فوق الزر **إضافة** لإنشاء قائمة تحكم في الوصول (ACL) جديدة قابلة للتنزيل.
5. أدخل في حقل **الاسم** اسما لقائمة التحكم بالوصول (DACL). يستخدم هذا المثال *قائمة التحكم في الوصول للبنية الأساسية (DACL)*.

تظهر هذه الصورة محتوى DACL النموذجي، والذي يسمح:

- DNS - حل اسم مضيف بوابة ISE
- HTTP و HTTPS - السماح بإعادة التوجيه
- منفذ TCP 8443 - يعمل كمنفذ مدخل الضيف



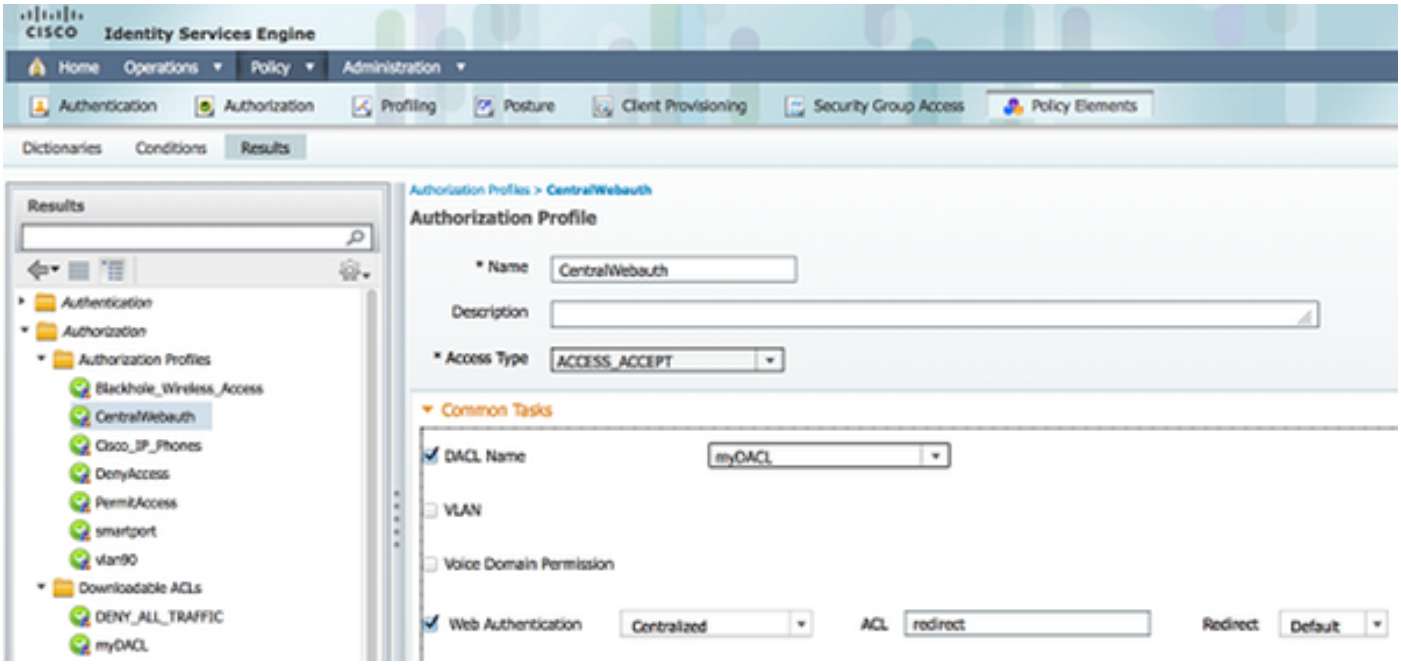
إنشاء ملف تعريف التفويض

أكمل الخطوات التالية لإنشاء ملف تعريف التخويل:

1. انقر فوق **نهج**، ثم انقر فوق **عناصر النهج**.
2. انقر فوق **النتائج**.
3. قم بتوسيع **التفويض**، وانقر فوق **ملف تعريف التفويض**.
4. انقر فوق الزر **إضافة** لإنشاء ملف تعريف تخويل جديد لـ webauth المركزي.
5. في حقل **الاسم**، أدخل اسماً لملف التعريف. يستخدم هذا المثال *CentralWebauth*.
6. اختر **ACCESS_ACCEPT** من القائمة المنسدلة نوع الوصول.
7. حدد خانة الاختيار **مصادقة الويب**، واختر **مركزي** من القائمة المنسدلة.
8. في حقل ACL، أدخل اسم ACL على المبدل الذي يحدد حركة المرور المطلوب إعادة توجيهها. تستخدم هذه الأمثلة *إعادة التوجيه*.
9. أختر **الافتراضي** من القائمة المنسدلة إعادة التوجيه.
10. حدد خانة الاختيار **اسم قائمة التحكم في الوصول الخاصة بالمنفذ (DACL)**، واختر **قائمة التحكم في الوصول الخاصة بالمنفذ (DACL) الخاصة بي** من القائمة

الدل (DACL) بالمنفذ الخاصة بالوصول في التحكم قائمة إستخدام إذا قررت المنسدلة
من قائمة التحكم في الوصول (ACL) الخاصة بالمنفذ الثابت على المحول.

تحدد سمة إعادة التوجيه ما إذا كان ISE يري مدخل ويب الافتراضي أو مدخل ويب مخصص أنشأه مسؤول ISE. على سبيل المثال، تقوم قائمة التحكم في الوصول (ACL) المعاد توجيهها في هذا المثال بتشغيل إعادة توجيه على حركة مرور HTTP أو HTTPS من العميل إلى أي مكان. يتم تحديد قائمة التحكم في الوصول (ACL) على المحول الحاقا في مثال التكوين هذا.

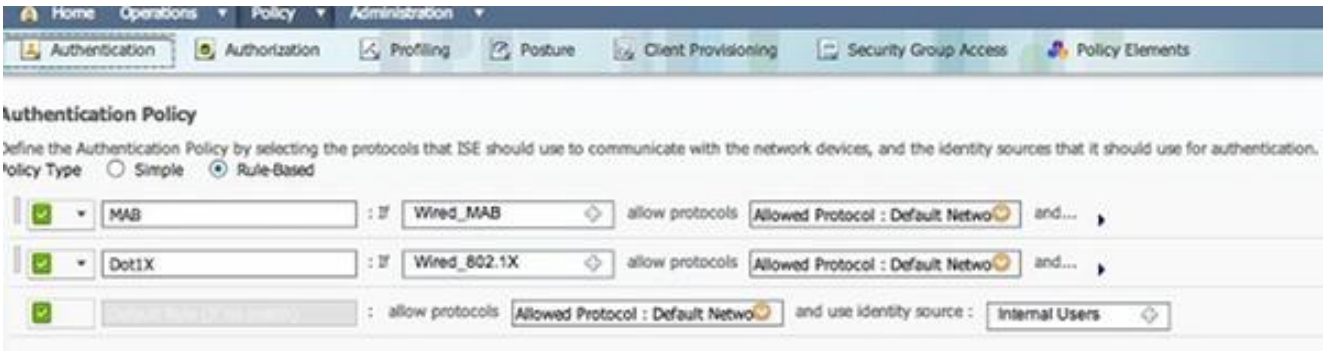


إنشاء قاعدة مصادقة

أكمل هذه الخطوات لاستخدام ملف تعريف المصادقة لإنشاء قاعدة المصادقة:

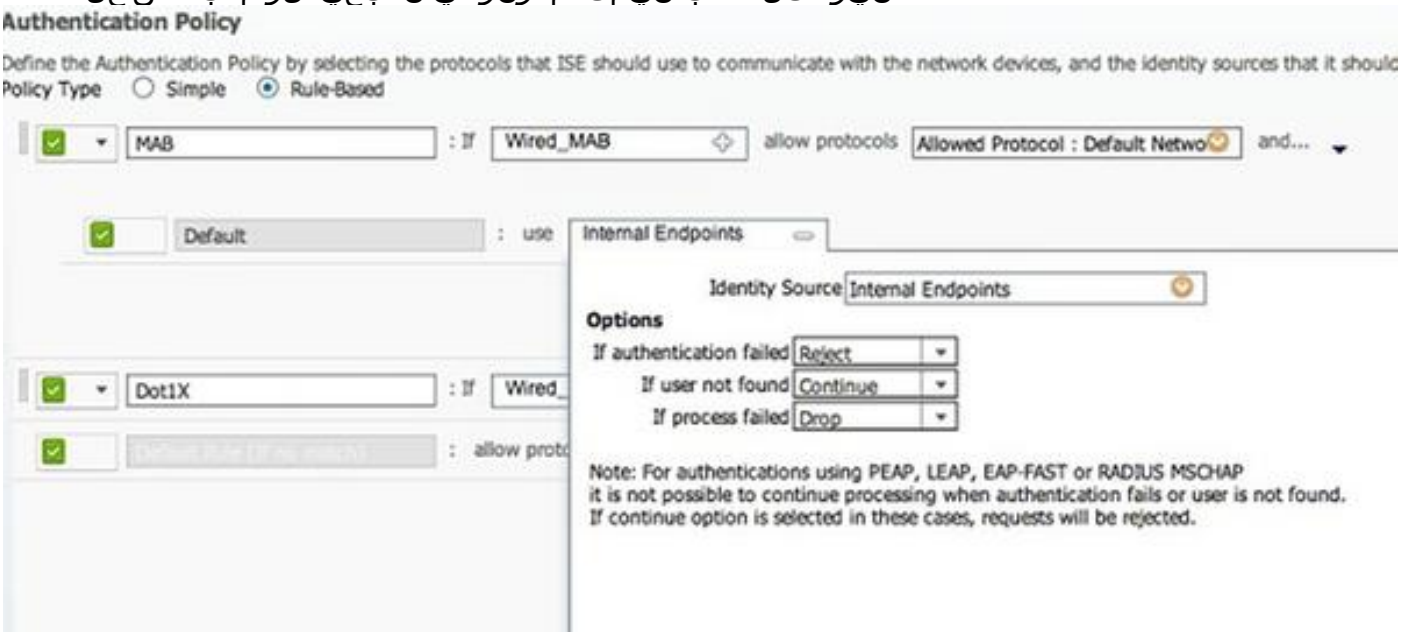
1. تحت قائمة "نهج"، انقر فوق **المصادقة**.

   توضح هذه الصورة مثال لكيفية تكوين قاعدة سياسة المصادقة. في هذا المثال ، يتم تكوين قاعدة يتم تشغيلها عند اكتشاف بروتوكول MAB.



2. أدخل اسماً لقاعدة المصادقة الخاصة بك. يستخدم هذا المثال *MAB*.
3. حدد أيقونة زائد (**+**) في حقل شرط If.
4. أختر **شرط مركب**، واختر **Wired_MAB**.
5. انقر فوق السهم الموجود بجوار **و**... لتوسيع القاعدة بشكل أكبر.
6. انقر أيقونة **+** في حقل مصدر الهوية، واختر **نقاط النهاية الداخلية**.
7. أختر **متابعة** من القائمة المنسدلة "إذا لم يتم العثور على المستخدم".

يتيح هذا الخيار مصادقة الجهاز (من خلال مصادقة الويب) حتى إذا كان عنوان MAC الخاص به غير معروف. ال يزال بإمكان عملاء dot1x المصادقة باستخدام بيانات الاعتماد الخاصة بهم والتي يجب أن يكونوا مهتمين بهذا التكوين.



إنشاء قاعدة تخويل

هناك الآن عدة قواعد للتكوين في نهج التخويل. عند توصيل الكمبيوتر، فإنه يمر عبر MAB؛ ومن المفترض أن عنوان MAC غير معروف، لذلك يتم إرجاع المصادقة على الويب وقائمة التحكم في الوصول (ACL). تظهر قاعدة *MAC غير المعروف* هذه في هذه الصورة ويتم تكوينها في هذا القسم:

أكمل الخطوات التالية لإنشاء قاعدة التخويل:

1. أنشئ قاعدة جديدة وأدخل اسماً. يستخدم هذا المثال *MAC غير المعروف*.
2. انقر أيقونة زائد (+) في حقل الشرط، واختر أن تنشئ شرط جديد.
3. قم بتوسيع القائمة المنسدلة **بالتعبير**.
4. أختر **Network Access**، وقم بتمديده.
5. انقر فوق **AuthenticationStatus**، واختر المشغل **Equals**.
6. أختر **UnknownUser** في الحقل الأيمن.
7. في صفحة التخويل العام، أختر **CentralWebauth** (ملف تعريف التخويل) في الحقل إلى يمين الكلمة *بعد ذلك*.

وهذه الخطوة تسمح باستمرار ISE حتى وإن كان المستخدم (أو MAC) غير معروف.

يتم الآن تقديم مستخدمين غير معروفين بصفحة تسجيل الدخول. ومع ذلك، بمجرد إدخال بيانات الاعتماد الخاصة بهم، يتم تقديمها مرة أخرى مع طلب مصادقة على ISE، لذلك، يجب تكوين قاعدة أخرى مع شرط يتم تلبيته إذا كان المستخدم ضيف. في هذا المثال، *إذا كان UserIdentityGroup يساوي Guest* يتم إستخدامه، ومن المفترض أن جميع الضيوف ينتمون إلى هذه المجموعة.

8. انقر زر الإجراءات الموجود في نهاية قاعدة *MAC غير المعروفة*، واختر إدراج قاعدة جديدة أعلاه.

   ملاحظة: من المهم جدا أن تأتي هذه القاعدة الجديدة قبل قاعدة *ماك غير المعروفة*.
9. أدخل اسمًا للقاعدة الجديدة. يستخدم هذا المثال *IS-Guest*.
10. اختر شرطا يتوافق مع المستخدمين الضيوف.

    يستخدم هذا المثال *InternalUser:IdentityGroup يساوي Guest* لأن جميع المستخدمين الضيوف مرتبطون بمجموعة *Guest* (أو مجموعة أخرى قمت بتكوينها في إعدادات الكفيل).
11. اختر **PermitAccess** في مربع النتائج (الموجود على يمين الكلمة *آنذاك*).

    عندما يتم تخويل المستخدم في صفحة تسجيل الدخول، يقوم ISE بإعادة تشغيل مصادقة من الطبقة 2 على منفذ المحول، ويحدث MAB جديد. في هذا السيناريو، يمكن تحديد الاختلاف بين المستخدم المجهول والمستخدم الضيف بعد تنفيذ هذه العملية. هذه القاعدة هي *المصادقة الثانية*، والشرط هو *الوصول إلى الشبكة:UseCase يساوي GuestFlow*. يتم وضع علامة على هذا الشرط عندما يقوم المستخدم بالمصادقة عبر مصادقة الويب، ويتم تعيين منفذ المحول مرة أخرى لـ MAB جديد. في هذا المثال، يتم تعيين VLAN90 حتى يتم تعيين أي سمات ترغب فيها. يمكنك تعيين الـ VLAN 90 المستعمل في مصادقة MAB ثاني له.
12. انقر فوق **إجراءات** (الموجودة في نهاية قاعدة IS-A-GUEST)، واختر **إدراج قاعدة جديدة أعلاه**.
13. أدخل **المصادقة الثانية** في حقل الاسم.
14. في حقل الشرط، انقر فوق أيقونة زائد (**+**)، واختر أن يتم إنشاء شرط جديد.
15. اختر **الوصول إلى الشبكة**، وانقر فوق **حالة الاستخدام**.
16. اختر **يساوي** كمشغل.
17. اختر **GuestFlow** كمعامل صحيح.
18. في صفحة التخويل، انقر فوق أيقونة زائد (**+**) (الموجودة بجوار *ذلك*) لاختيار نتيجة للقاعدة الخاصة بك.

    في هذا المثال، يتم تعيين ملف تعريف تم تكوينه مسبقا (VLAN90)، ولا يتم عرض هذا التكوين في هذا المستند.

    يمكنك اختيار خيار **السماح بالوصول** أو إنشاء ملف تعريف مخصص لإرجاع شبكة VLAN أو السمات التي تعجبك.

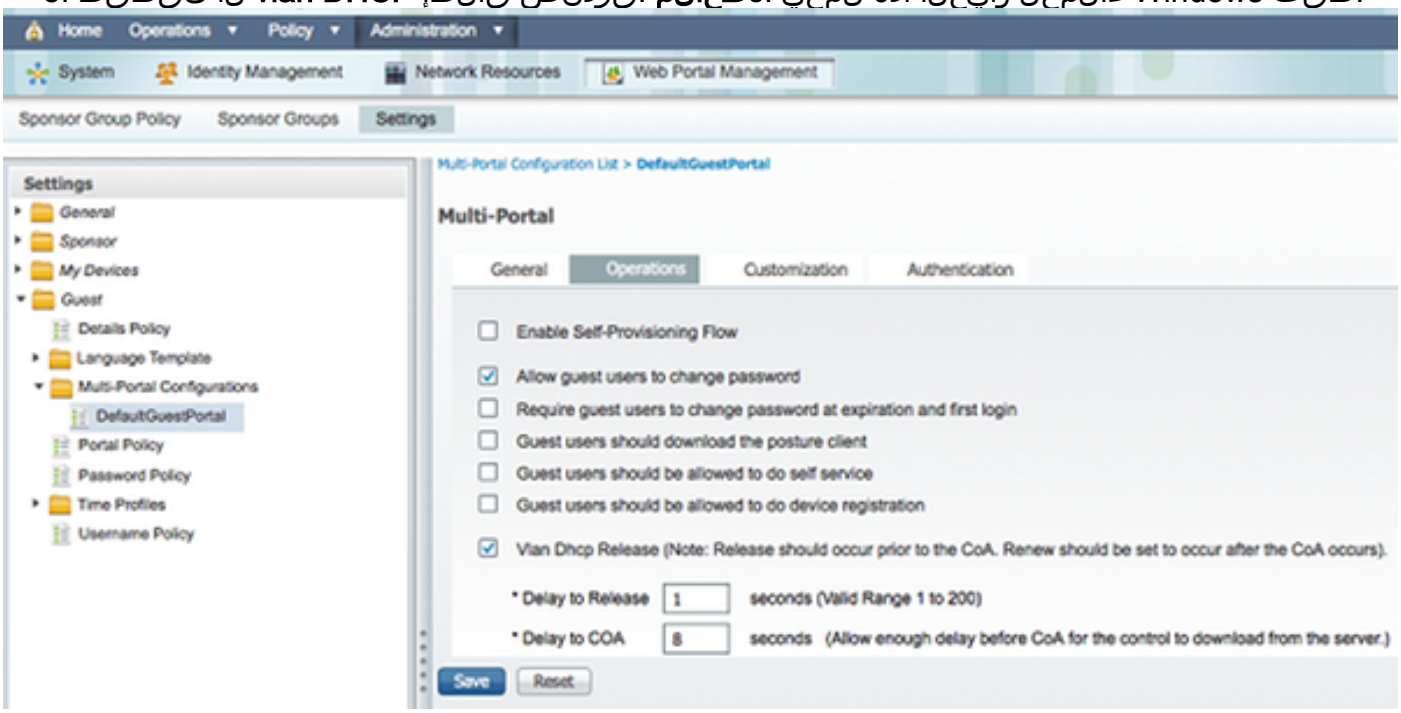
تمكين تجديد IP (اختياري)

إذا قمت بتعيين شبكة VLAN، فإن الخطوة الأخيرة هي أن يقوم جهاز الكمبيوتر الخاص بالعميل بتجديد عنوان IP الخاص به. يتم تنفيذ هذه الخطوة من خلال بوابة الضيف لعملاء Windows. إذا لم تقم بتعيين شبكة VLAN لقاعدة *AUTH الثانية* مسبقًا، فيمكنك تخطي هذه الخطوة.

إذا قمت بتعيين VLAN، أكمل هذه الخطوات لتمكين تجديد IP:

1. انقر فوق **إدارة**، وانقر فوق **إدارة الضيوف**.
2. طقطقة **عملية إعداد**.
3. قم بتوسيع **Guest**، وتوسيع **التكوين متعدد المنافذ**.
4. انقر فوق **DefaultGuestPortal** أو اسم مدخل مخصص قد قمت بإنشائه.

5. طقطقت ال **vlan DHCP** إطلاق صندوق. **ملاحظة**: يعمل هذا الخيار لعملاء Windows فقط.



تكوين المحول (مقتطف)

يزود هذا قسم قسم قسم قسم من المفاتيح تشكيل. راجع تكوين المحول (كامل) للتكوين الكامل.

يوضح هذا النموذج تكوين MAB بسيط.

```
interface GigabitEthernet1/0/12
description ISE1 - dot1x clients - UCS Eth0
switchport access vlan 100
switchport mode access
ip access-group webauth in
authentication order mab
authentication priority mab
authentication port-control auto
mab
spanning-tree portfast
end
```

VLAN 100 هي شبكة VLAN التي توفر اتصال الشبكة الكامل. يتم تطبيق قائمة التحكم في الوصول (ACL) للمنفذ الافتراضي (باسم *WebAuth*) وتعريفها كما هو موضح هنا:

```
ip access-list extended webauth
permit ip any any
```

يوفر هذا التكوين العينة الوصول الكامل إلى الشبكة حتى في حالة عدم مصادقة المستخدم؛ وبالتالي، فقد ترغب في تقييد الوصول إلى المستخدمين غير المصدق عليهم.

في هذا التكوين، ال يعمل إستعراض HTTP و HTTPS دون مصادقة (لكل قائمة التحكم في الوصول الأخرى) نظرا لتكوين ISE لاستخدام قائمة التحكم في الوصول (ACL) المعاد توجيهها (المسماة *redirect*). هنا التعريف على المفتاح:

```
ip access-list extended redirect
deny ip any host <ISE ip address>
permit TCP any any eq www
permit TCP any any eq 443
```

يجب تحديد قائمة الوصول هذه على المحول لتحديد حركة المرور التي سيقوم المحول بإجراء إعادة التوجيه عليها. (يطابق *التصريح*.) في هذا المثال، تعمل أي حركة مرور HTTP أو HTTPS يرسلها العميل على تشغيل إعادة توجيه الويب. يرفض هذا المثال أيضا عنوان IP ل ISE حركة مرور إلى ISE يذهب إلى ال ISE والو يعيد توجيه في أنشوطة. (في هذا السيناريو، لا يؤدي الرفض إلى حظر حركة المرور، ولكنه لا يعيد توجيه حركة المرور.) إذا كنت تستخدم منافذ HTTP غير عادية أو وكيل، فيمكنك إضافة منافذ أخرى.

إمكانية أخرى هي السماح ل HTTP بالوصول إلى بعض مواقع ويب وإعادة توجيه مواقع ويب أخرى. على سبيل المثال، إذا قمت بتحديد تصريح للمواقع الويب الداخلية في قائمة التحكم بالوصول (ACL) فقط، فيمكن للعملاء إستعراض الويب بدون المصادقة ولكن قد يواجهون إعادة التوجيه إذا حاولوا الوصول إلى موقع ويب خارجي.

الخطوة الأخيرة هي السماح ب CoA على المحول. وإلا، فلن يتمكن ISE من إجبار المحول على إعادة مصادقة العميل.

```
aaa server radius dynamic-author
client <ISE ip address> server-key <radius shared secret>
```

يلزم هذا الأمر للمحول لإعادة التوجيه استنادا إلى حركة مرور HTTP:

```
ip http server
```

يتطلب هذا الأمر إعادة التوجيه استنادا إلى حركة مرور بيانات HTTPS:

```
ip http secure-server
```

هذه الأوامر مهمة أيضا:

```
radius-server vsa send authentication
radius-server vsa send accounting
```

إذا لم تتم مصادقة المستخدم بعد، يرجع **show authentication session int <interface num>** هذا الإخراج:

```
01-SW3750-access#show auth sess int gi1/0/12
Interface: GigabitEthernet1/0/12
MAC Address:  000f.b049.5c4b
          IP Address:  192.168.33.201
           User-Name:  00-0F-B0-49-5C-4B
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  single-host
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  N/A
             ACS ACL:  xACSACLx-IP-myDACL-51519b43
    URL Redirect ACL:  redirect
        URL Redirect:  https://ISE2.wlaaan.com:8443/guestportal/gateway?
sessionId=C0A82102000002D8489E0E84&action=cwa
     Session timeout:  N/A
```

```
        Idle timeout:  N/A
   Common Session ID:  C0A82102000002D8489E0E84
     Acct Session ID:  0x000002FA
              Handle:  0xF60002D9

Runnable methods list:

      Method   State
      mab      Authc Success
```

ملاحظة: بالرغم من مصادقة MAB الناجحة، يتم وضع قائمة التحكم في الوصول (ACL) للمعاد توجيهها نظرا لأن عنوان MAC غير معروف من قبل ISE.

تكوين المحول (كامل)

يسرد هذا القسم تكوين المحول بالكامل. تم حذف بعض الواجهات وسطر الأوامر غير الضرورية، لذلك، يجب إستخدام هذا التكوين كمرجع فقط ويجب عدم نسخه.

```
Building configuration...

Current configuration : 6885 bytes
!
version 15.0
no service pad
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
no service password-encryption
!
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$xqtx$VPsZHbpGmLyH/EOObPpla.
!
aaa new-model
!
!
aaa group server radius newGroup
!
aaa authentication login default local
aaa authentication dot1x default group radius
aaa authorization exec default none
aaa authorization network default group radius
!
!
!
!
aaa server radius dynamic-author
client 192.168.131.1 server-key cisco
!
aaa session-id common
clock timezone CET 2 0
system mtu routing 1500
vtp interface Vlan61
udld enable

nmsp enable
ip routing
ip dhcp binding cleanup interval 600
!
```

```
!
ip dhcp snooping
ip device tracking
!
!
crypto pki trustpoint TP-self-signed-1351605760
enrollment selfsigned
subject-name cn=IOS-Self-Signed-Certificate-1351605760
revocation-check none
rsakeypair TP-self-signed-1351605760
!
!
crypto pki certificate chain TP-self-signed-1351605760
certificate self-signed 01
30820245 308201AE A0030201 02020101 300D0609 2A864886 F70D0101 04050030
31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
69666963 6174652D 31333531 36303537 3630301E 170D3933 30333031 30303033
35385A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D31 33353136
30353736 3030819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
8100B068 86D31732 E73D2FAD 05795D6D 402CE60A B93D4A88 C98C3F54 0982911D
D211EC23 77734A5B 7D7E5684 388AD095 67354C95 92FD05E3 F3385391 8AB9A866
B5925E04 A846F740 1C9AC0D9 6C829511 D9C5308F 13C4EA86 AF96A94E CD57B565
92317B2E 75D6AB18 04AC7E14 3923D3AC 0F19BC6A 816E6FA4 5F08CDA5 B95D334F
DA410203 010001A3 6D306B30 0F060355 1D130101 FF040530 030101FF 30180603
551D1104 11300F82 0D69696C 796E6173 2D333536 302E301F 0603551D 23041830
16801457 D1216AF3 F0841465 3DDDD4C9 D08E06C5 9890D530 1D060355 1D0E0416
041457D1 216AF3F0 8414653D DDD4C9D0 8E06C598 90D5300D 06092A86 4886F70D
01010405 00038181 0014DC5C 2D19D7E9 CB3E8ECE F7CF2185 32D8FE70 405CAA03

dot1x system-auth-control
dot1x critical eapol
!
!
!
errdisable recovery cause bpduguard
errdisable recovery interval 60
!
spanning-tree mode pvst
spanning-tree logging
spanning-tree portfast bpduguard default
spanning-tree extend system-id
spanning-tree vlan 1-200 priority 24576
!
vlan internal allocation policy ascending
lldp run
!
!
!
!
!
!
interface FastEthernet0/2
switchport access vlan 33
switchport mode access
authentication order mab
authentication priority mab
authentication port-control auto
mab
spanning-tree portfast
!
interface Vlan33
ip address 192.168.33.2 255.255.255.0
!
```

```
ip default-gateway 192.168.33.1
ip http server
ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.168.33.1
!
ip access-list extended MY_TEST
permit ip any any
ip access-list extended redirect
deny ip any host 192.168.131.1
permit tcp any any eq www
permit tcp any any eq 443
ip access-list extended webAuthList
permit ip any any
!
ip sla enable reaction-alerts
logging esm config
logging trap warnings
logging facility auth
logging 10.48.76.31
snmp-server community c3560public RO
snmp-server community c3560private RW
snmp-server community private RO
radius-server host 192.168.131.1 auth-port 1812 acct-port 1813 key cisco
radius-server vsa send authentication
radius-server vsa send accounting
!
!
!
privilege exec level 15 configure terminal
privilege exec level 15 configure
privilege exec level 2 debug radius
privilege exec level 2 debug aaa
privilege exec level 2 debug
!
line con 0
line vty 0 4
exec-timeout 0 0
password Cisco123
authorization commands 1 MyTacacs
authorization commands 2 MyTacacs
authorization commands 15 MyTacacs
authorization exec MyTacacs
login authentication MyTacacs
line vty 5 15
!
ntp server 10.48.76.33
end
```

تكوين وكيل HTTP

إذا كنت تستخدم وكيل HTTP لعملائك، فهذا يعني أن عملاءك:

- إستخدام منفذ غير تقليدي لبروتوكول HTTP
- إرسال كل حركة المرور الخاصة بهم إلى هذا الوكيل

in order to جعلت المفتاح يستمع على ال غير تقليدي ميناء (مثال، 8080)، استعملت هذا أمر:

```
ip http port 8080
ip port-map http port 8080
```

كما تحتاج إلى تكوين جميع العملاء لمتابعة إستخدام الوكيل الخاص بهم ولكن لعدم

إستخدام الوكيل الخاص بعنوان ISE IP. تتضمن جميع المستعرضات ميزة تسمح لك بإدخال أسماء الأجهزة المضيفة أو عناوين IP التي يجب ألا تستخدم الوكيل. إذا لم تقم بإضافة الاستثناء إلى ISE، فستواجه صفحة مصادقة تكرار حلقي.

أنت تحتاج أيضا إلى تعديل قائمة التحكم في الوصول (ACL) لإعادة التوجيه الخاصة بك للسماح على منفذ الوكيل (8080 في هذا المثال).

ملاحظة هامة حول المحولات SVIs

في هذا الوقت، يحتاج المحول إلى واجهة ظاهرية للمحول (SVI) للرد على العميل وإرسال إعادة توجيه الويب إلى العميل. لا يلزم أن يكون هذا SVI بالضرورة على الشبكة الفرعية/شبكة VLAN الخاصة بالعميل. ومع ذلك، إذا لم يكن للمحول SVI في الشبكة الفرعية للعميل/شبكة VLAN، فيجب أن يستخدم أي من SVIs الأخرى ويرسل حركة مرور البيانات كما هو محدد في جدول توجيه العميل. وهذا يعني عادة إرسال حركة المرور إلى بوابة أخرى في مركز الشبكة، وتعيد حركة المرور هذه إلى محول الوصول داخل الشبكة الفرعية للعميل.

تقوم جدران الحماية بشكل نموذجي بحظر حركة المرور من المحول نفسه وإليه، كما هو الحال في هذا السيناريو، لذلك قد لا تعمل إعادة التوجيه بشكل صحيح. تتم إستخدام الحلول في هذا السيناريو، لذلك قد لا تعمل إعادة التوجيه بشكل صحيح. الحلول للسماح بهذا السلوك على جدار الحماية أو إنشاء SVI على محول الوصول في الشبكة الفرعية للعميل.

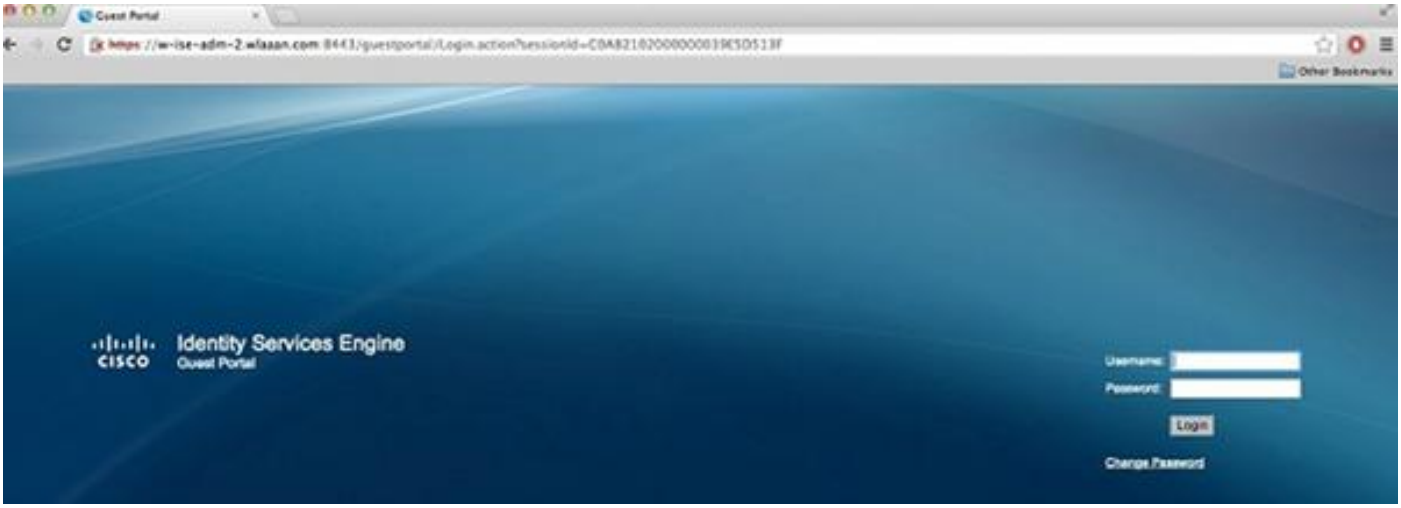
ملاحظة هامة حول إعادة توجيه HTTPS

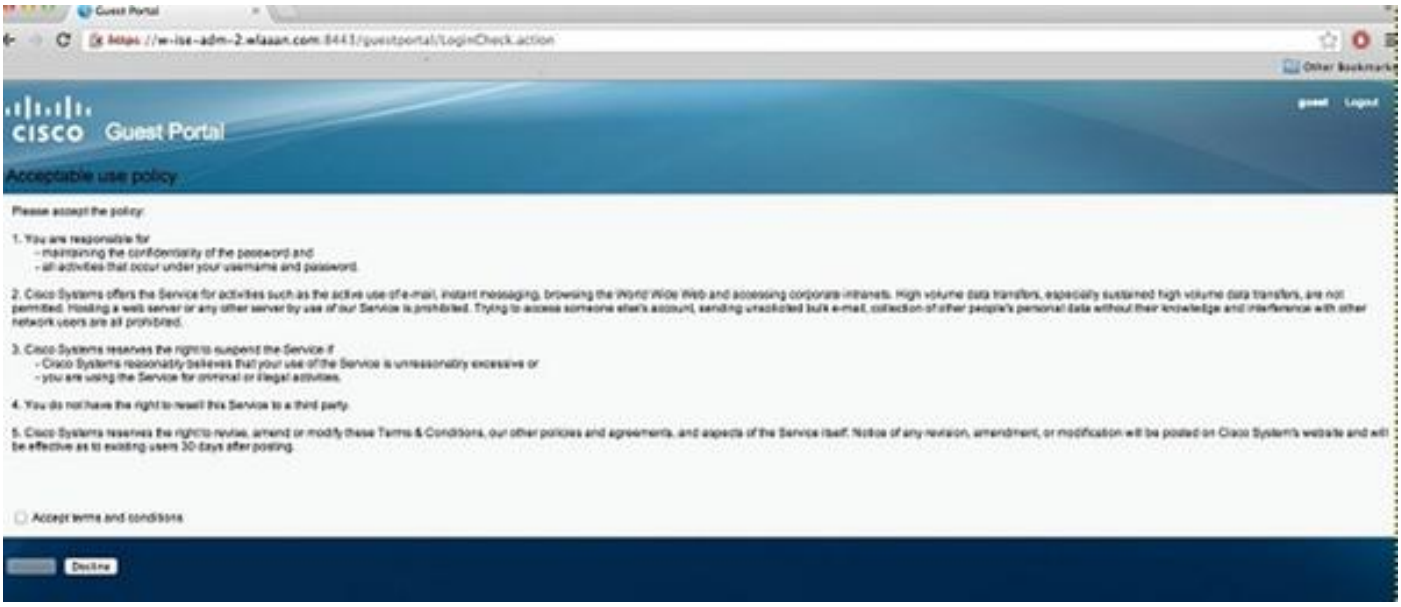
يمكن للمحولات إعادة توجيه حركة مرور بيانات HTTPS. وبالتالي، إذا كان للعميل الضيف صفحة رئيسية في HTTPS، تحدث عملية إعادة التوجيه بشكل صحيح.

يستند مفهوم إعادة التوجيه بالكامل إلى حقيقة أن جهاز (في هذه الحالة، المحول) يعترض حركة مرور المحول عنوان IP لموقع الويب. ومع ذلك، تنشأ مشكلة رئيسية عندما يعترض المحول حركة مرور HTTPS ويعيد توجيهها لأن المحول يمكن أن يقدم فقط شهادته الخاصة في مصافحة أمان طبقة النقل (TLS). نظرا لأن هذه الشهادة ليست نفس الشهادة التي طلبها موقع الويب في الأصل، فإن معظم المستعرضات تصدر تنبيهات هامة. تعامل المستعرضات بشكل صحيح مع إعادة التوجيه والعرض لشهادة أخرى كتهديد أمني. لا يوجد حل بديل لهذا الإجراء، ولا توجد طريقة للمحول لانتحال شهادة موقع الويب الأصلية.

نتيجة نهائية

موقع الكمبيوتر العميل يتوصيل MAB وتنفيذه. عنوان MAC غير معروف، لذلك يدفع ISE خصائص redirection مرة أخرى إلى المفتاح. يحاول المستخدم الانتقال إلى موقع ويب ويتم إعادة توجيهه.





عندما تكون مصادقة صفحة تسجيل الدخول ناجحة، يقوم ISE بترجيع Switchport من خلال تغيير التفويض، والذي يبدأ مرة أخرى مصادقة MAB من الطبقة 2.

ومع ذلك، تعرف إدارة التخزين (ISE) أنه عميل مصادقة ويب سابق وتخول العميل استنادا إلى بيانات اعتماد مصادقة الويب (على الرغم من أن هذه مصادقة من الطبقة 2).

في سجلات مصادقة ISE، تظهر مصادقة MAB في أسفل السجل. على الرغم من أنه غير معروف، تمت مصادقة عنوان MAC واستبعاده، وتم إرجاع سمات مصادقة الويب. وبعد ذلك، تحدث المصادقة باسم مستخدم المستخدم (أي، يقوم المستخدم بأنواع بيانات الاعتماد الخاصة به في صفحة تسجيل الدخول). مباشرة بعد المصادقة، تحدث مصادقة جديدة للطبقة 2 مع اسم المستخدم كبيانات اعتماد؛ وخطوة المصادقة هذه هي حيث يمكنك إرجاع سمات شبكة VLAN الديناميكية.

Mar 26,13 04:58:43.572 PM	✓		Nico	00:0F:80:49:5C:48	Nicoswitch	FastEthernet0/3	vlan90	Guest	NotApplicable	
Mar 26,13 04:58:43.445 PM	✓				Nicoswitch					Dynamic Author...
Mar 26,13 04:58:43.438 PM	✓		Nico	00:0F:80:49:5C:48				Guest		Guest Authentic...
Mar 26,13 04:58:37.900 PM	✓		#ACSACL#-IP-myDAC		celine					DACL Download...
Mar 26,13 04:58:36.995 PM	✓		00:1A:6C:78:56:0E	00:1A:6C:78:56:0E	celine	GigabitEthernet2/0/10	CentralWebauth		Pending	Authentication ...

التحقق من الصحة

لا يوجد حاليًا إجراء للتحقق من صحة هذا التكوين.

استكشاف الأخطاء وإصلاحها

لا تتوفر حالياً معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

معلومات ذات صلة

- محرك خدمات الهوية من Cisco
- دليل مرجع أمر محرك خدمات الهوية من Cisco
- تكامل ISE (Identity Services Engine) مع Cisco WLC (وحدة التحكم في الشبكة المحلية اللاسلكية)
- طلبات التعليقات (RFCs)
- 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).