# أستكشاف مشكلات وصول الضيف الشائع وإصلاحها إلى ISE

## المحتويات



## المقدمة

يوضح هذا المستند كيفية أستكشاف أخطاء الضيوف الشائعة وإصلاحها في النشر وكيفية عزل المشكلة والتحقق منها والحلول البديلة البسيطة للمحاولة.

## المتطلبات الأساسية

### المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- تكوين ضيف ISE
- تكوين CoA على أجهزة الوصول إلى الشبكة (NAD)
- يلزم توفر أدوات التقاط على محطات العمل.

### المكونات المستخدمة

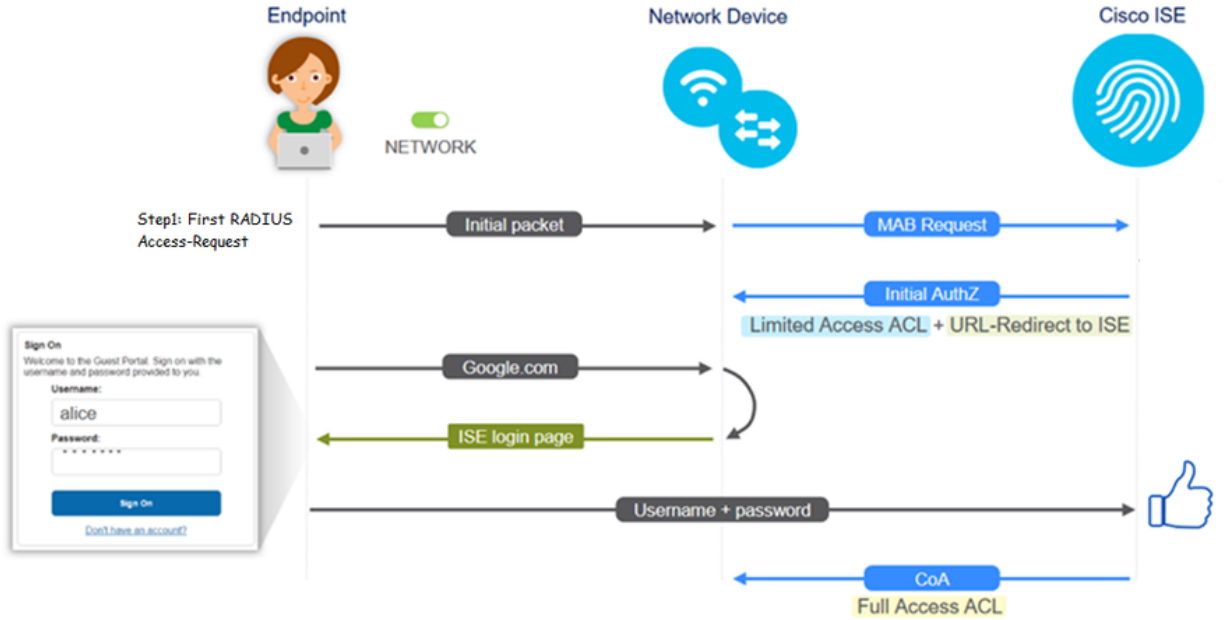
تستند المعلومات الواردة في هذا المستند إلى Cisco ISE، الإصدار 2.6، و:

- WLC 5500
- المحول Catalyst 3850 15.x version
- محطة عمل Windows 10

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 قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

# تدفق الضيف

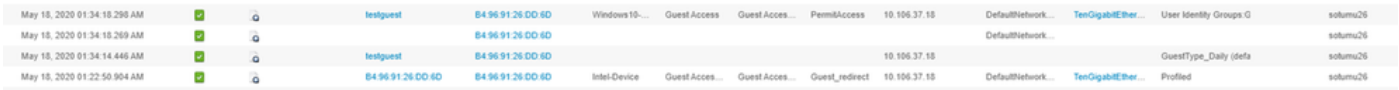
نظرة عامة على تدفق الضيف مماثلة للخيارات السلكية أو اللاسلكية. يمكن إستخدام هذه الصورة من الرسم التخطيطي للتدفق كمرجع عبر المستند. فهي تساعد على تصور الخطوة والكيان.




كما يمكن متابعة التدفق على سجلات ISE المباشرة [**العمليات > سجلات RADIUS المباشرة**] من خلال تصفية معرف نقطة النهاية:

- مصادقة MAB ناجحة- يحتوي حقل اسم المستخدم على عنوان MAC- يتم دفع URL إلى NAD - يحصل المستخدم على البوابة
- مصادقة الضيف ناجحة- يحتوي حقل اسم المستخدم على اسم المستخدم الضيف، وقد تم تعريفه باسم GuestType_Daily (أو النوع الذي تم تكوينه للمستخدم الضيف)
- الحقل CoA الذي تم بدء تشغيله- اسم المستخدم فارغ، يظهر التقرير التفصيلي "التفويض الديناميكي" بنجاح
- تم توفير وصول الضيف

تسلسل الأحداث في الصورة (من الأسفل إلى الأعلى)



# أدلة الاستخدام الشائعة

فيما يلي بعض الارتباطات للمساعدة في التكوين. بالنسبة لأي عملية أستكشاف أخطاء حالة إستخدام معينة وإصلاحها، فإنها تساعد على إدراك التهيئة المثالية أو المتوقعة.

- تكوين الضيف السلكي
- تكوين ضيف لاسلكي
- CWA Wireless Guest مع نقاط الوصول FlexAuth APs

# المشاكل التي تتم مواجهتها بشكل متكرر

يتناول هذا المستند بشكل أساسي هذه القضايا:

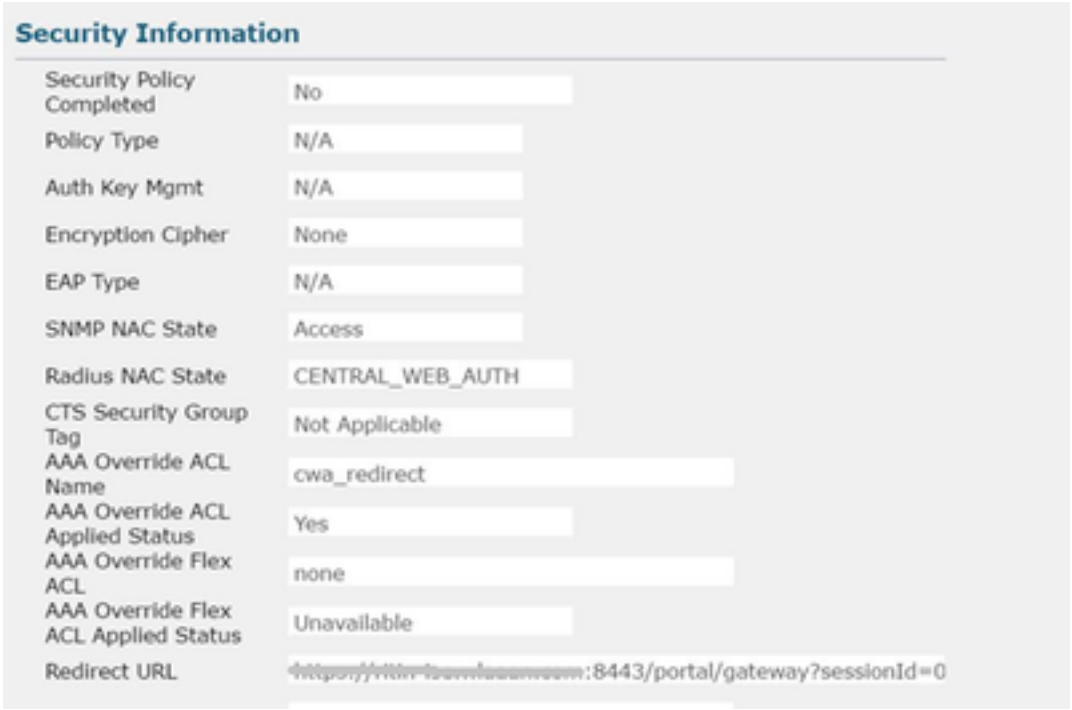
## إعادة التوجيه إلى مدخل Guest العمل

بمجرد دفع عنوان URL المعاد توجيهه وقوائم التحكم في الوصول من ISE، فتحقق مما يلي:

1. حالة العميل على المحول (في حالة وصول الضيف السلكي) باستخدام الأمر **show authentication session int <interface> تفاصيل**:

```
guestlab#sh auth sess int T1/0/48 de
           Interface:  TenGigabitEthernet1/0/48
              IIF-ID:  0x1096380000001DC
         MAC Address:  b496.9126.dd6d
        IPv6 Address:  Unknown
        IPv4 Address:  10.106.37.18
           User-Name:  B4-96-91-26-DD-6D
              Status:  Authorized
              Domain:  DATA
      Oper host mode:  single-host
    Oper control dir:  both
     Session timeout:  N/A
     Restart timeout:  N/A
    Common Session ID:  0A6A25110000012652C64B014
     Acct Session ID:  0x0000124F
              Handle:  0x5E00014D
      Current Policy:  POLICY_Te1/0/48

Local Policies:
       Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
     Security Policy:  Should Secure
     Security Status:  Link Unsecure

Server Policies:

        URL Redirect:  https://10.127.197.212:8443/portal/gateway?sessionId=0A6
A25110000012652C64B014&portal=26d19560-2e58-11e9-98fb-0050568775a3&action=cwa&tok
en=66bbfce930a43142fe26b9d9577971de
     URL Redirect ACL:  REDIRECT_ACL

Method status list:
      Method           State
      mab              Authc Success
```

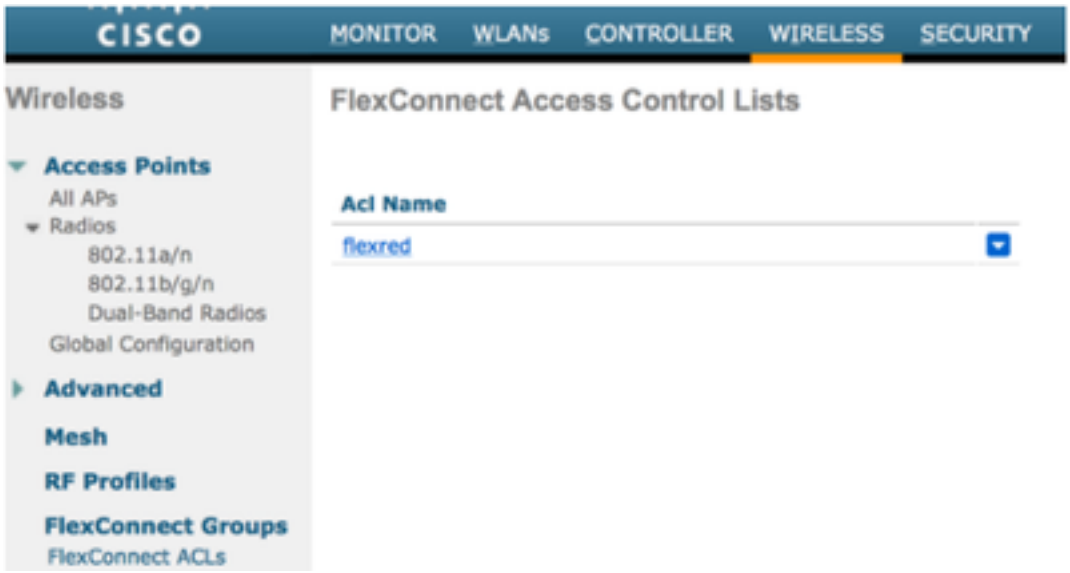
2. حالة العميل على وحدة التحكم في الشبكة المحلية اللاسلكية (في حالة وصول الضيف اللاسلكي): **شاشة > عميل > عنوان MAC**



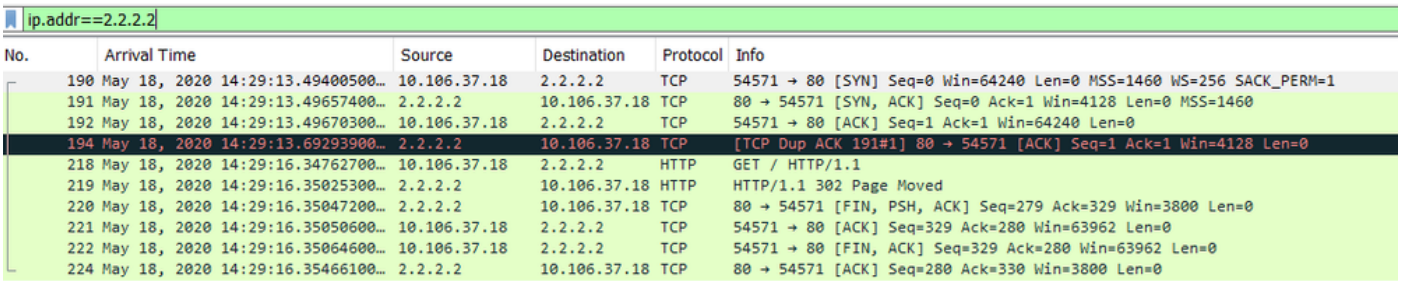

3. إمكانية الوصول من نقطة النهاية إلى ISE على منفذ TCP 8443 بمساعدة موجه الأوامر: **C:\Users\user>Telnet <ISE-IP> 8443**

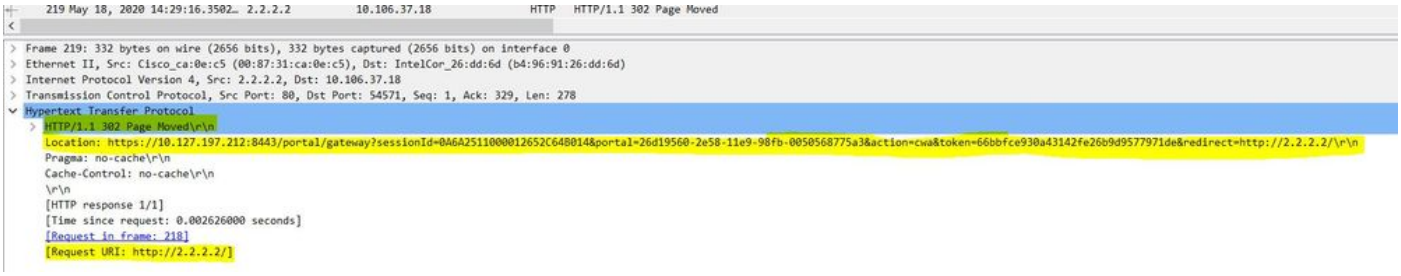
4. إذا كان عنوان URL لإعادة توجيه البوابة يحتوي على FQDN، فتحقق مما إذا كان العميل قادرا على الحل من موجه الأوامر: **C:\Users\user>nslookup guest.ise.com**

5. في إعداد الاتصال المرن، تأكد من تكوين اسم قائمة التحكم في الوصول (ACL) نفسه تحت قوائم التحكم في الوصول (ACL) وقوائم التحكم في الوصول (ACL) المرنة. تحقق أيضا من تعيين قائمة التحكم في الوصول (ACL) على نقاط الوصول (APs). راجع دليل التكوين من القسم السابق-الخطوات 7 ب و c للحصول على مزيد من المعلومات.




6. التقاط حزمة من العميل، والتحقق من إعادة التوجيه. تشير صفحة الحزمة HTTP/1.1 302 التي تم نقلها إلى URL المعاد توجيهه للموقع الذي تم الوصول إليه من قبل WLC/Switch إلى مدخل ضيف ISE (عنوان URL المعاد توجيهه):




7. تم تمكين محرك (محركات) HTTP على أجهزة الوصول إلى الشبكة:

على المُبدّل:

```
guestlab#sh run | in ip http
ip http server
ip http secure-server
```

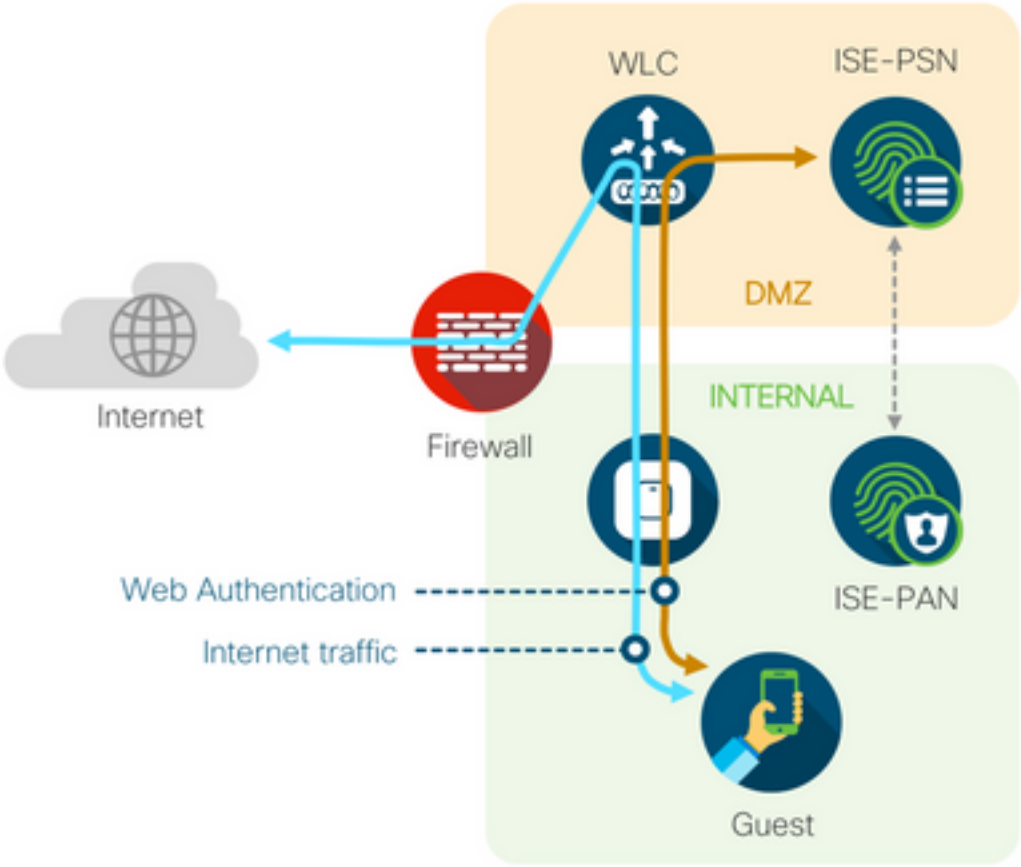
على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC):


8. إذا كان عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) في إعداد إرساء خارجي، فتحقق مما يلي:

الخطوة 1. يجب أن تكون حالة العميل هي نفسها على كل من WLCs.

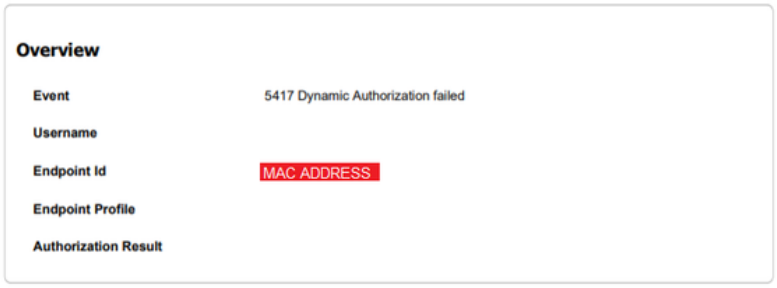
الخطوة 2. يجب رؤية عنوان URL لإعادة التوجيه على كل من وقائم التحكم في الشبكة المحلية اللاسلكية (WLCs).

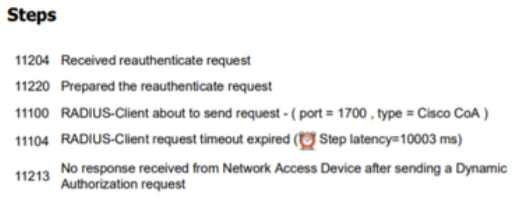
الخطوة 3. يجب تعطيل محاسبة RADIUS على عنصر الربط WLC.




## فشل التفويض الديناميكي

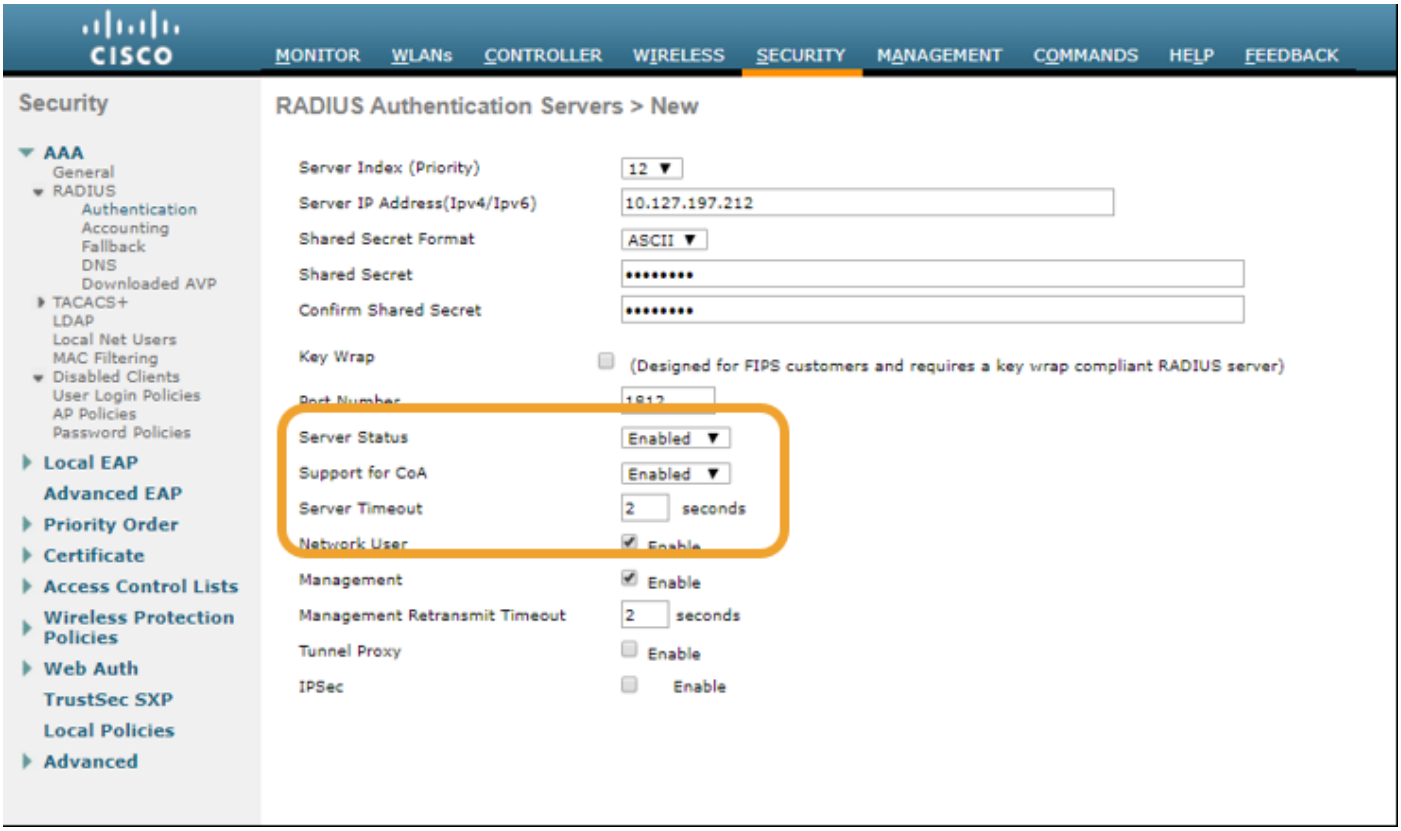
إذا كان المستخدم النهائي قادرا على الوصول إلى مدخل الضيف وتسجيل الدخول بنجاح، فإن الخطوة التالية ستكون تغيير التفويض لمنح وصول الضيف الكامل للمستخدم. إذا لم ينجح ذلك، فسترى فشل "التفويض الديناميكي" على سجلات ISE Radius Live. ولمعالجة المسألة، تحقق مما يلي:



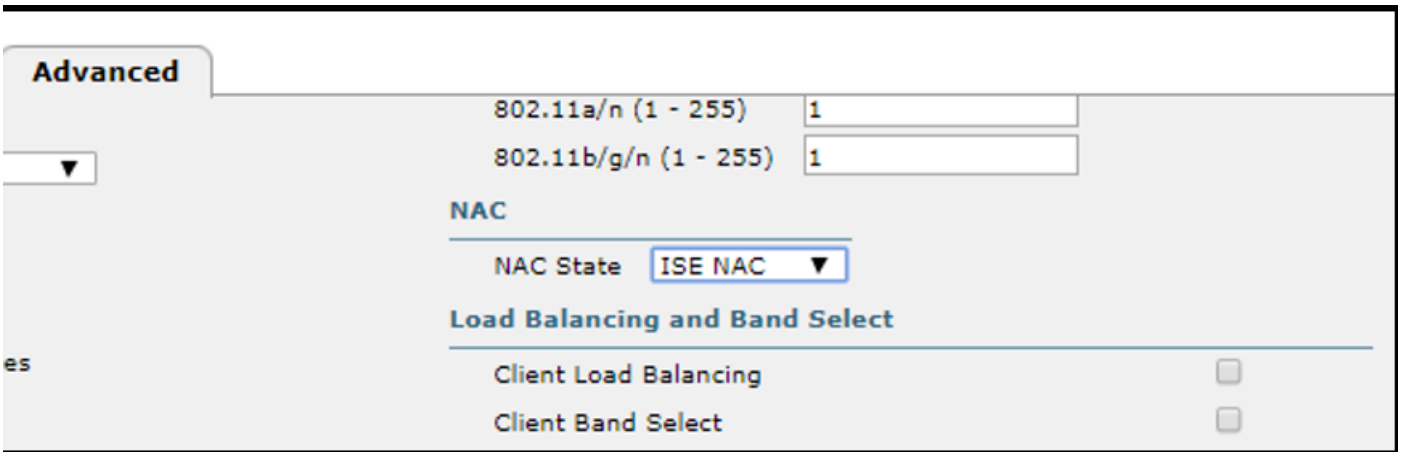

1. يجب تمكين/تكوين تغيير التفويض (CoA) على NAD:

```
!
aaa server radius dynamic-author
 client 10.127.197.209 server-key cisco123
 client 10.127.197.212 server-key cisco123
!
```




2. يجب السماح بمنفذ UDP 1700 على جدار الحماية.

3. حالة NAC على WLC غير صحيحة. تحت إعدادات متقدمة على **WLC GUI>WLAN** يغير **NAC** دولة إلى ISE NAC.

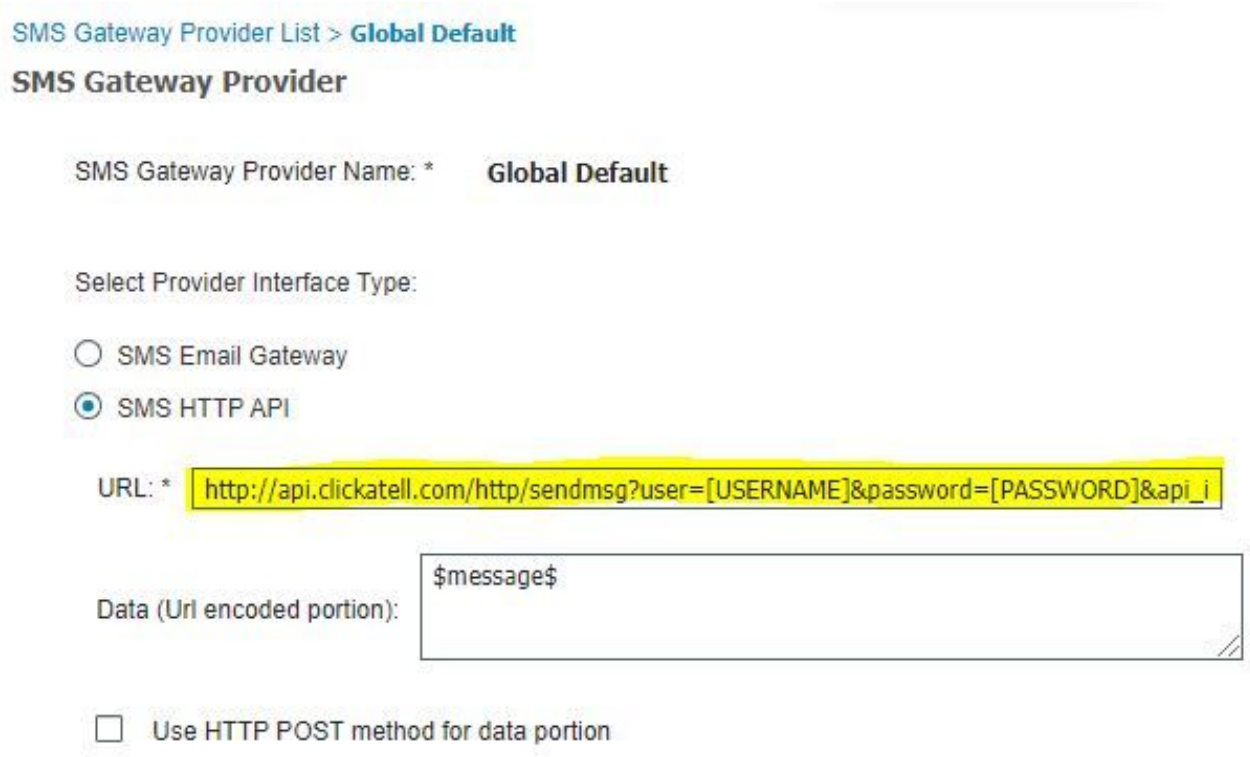



## لم يتم إرسال إعلامات البريد الإلكتروني/SMS

1. تحقق من تكوين SMTP تحت **الإدارة > النظام > الإعدادات > SMTP**.

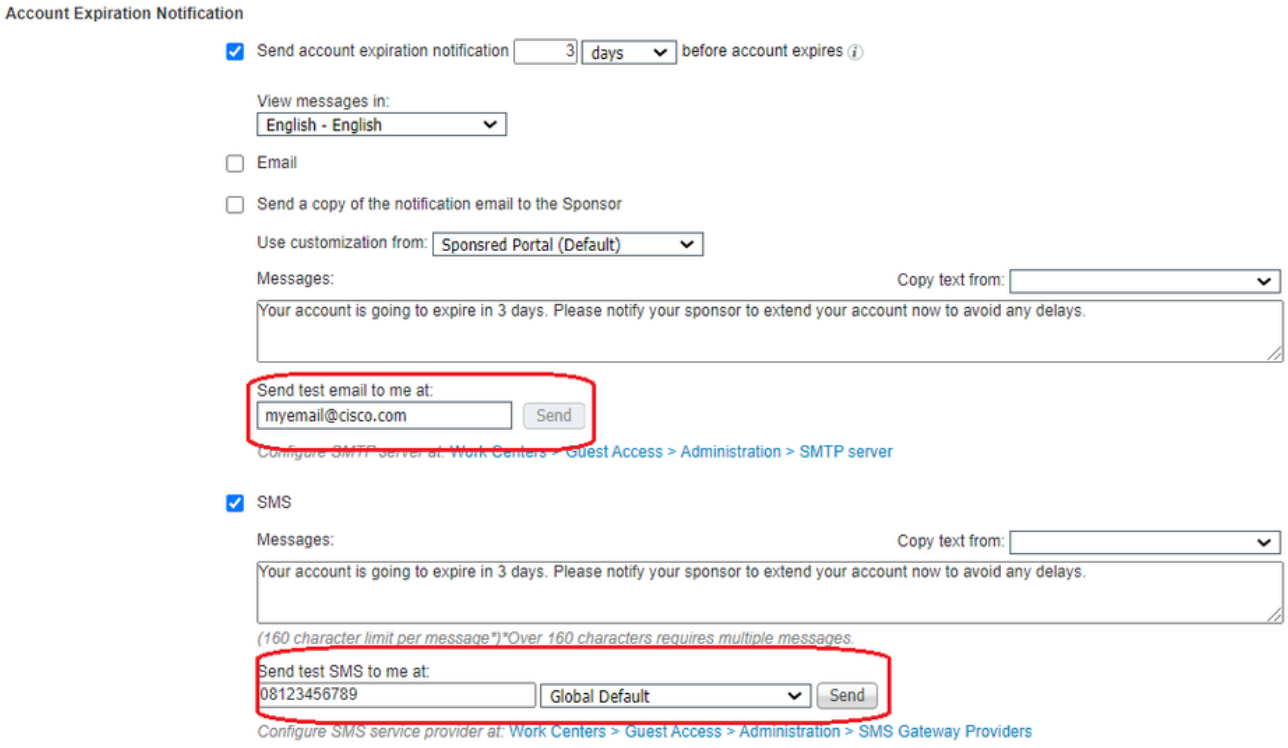
2. التحقق من واجهة برمجة التطبيقات (API) بحثا عن بوابات رسائل SMS/البريد الإلكتروني خارج ISE:

اختبر عنوان (عناوين) URL التي يوفرها المورد على عميل API أو متصفح، واستبدل المتغيرات مثل أسماء المستخدمين وكلمات المرور ورقم الهاتف المحمول واختبر قابلية الوصول. **[الإدارة > النظام > الإعدادات > بوابات SMS]**




بدلا من ذلك، إذا قمت بالاختبار من مجموعات مقدمي خدمة ISE [**مراكز العمل > الوصول الضيف > البوابات والمكونات > أنواع الضيوف**]، فعليك التقاط حزمة على ISE وبوابة SMS/SMTP للتحقق مما إذا

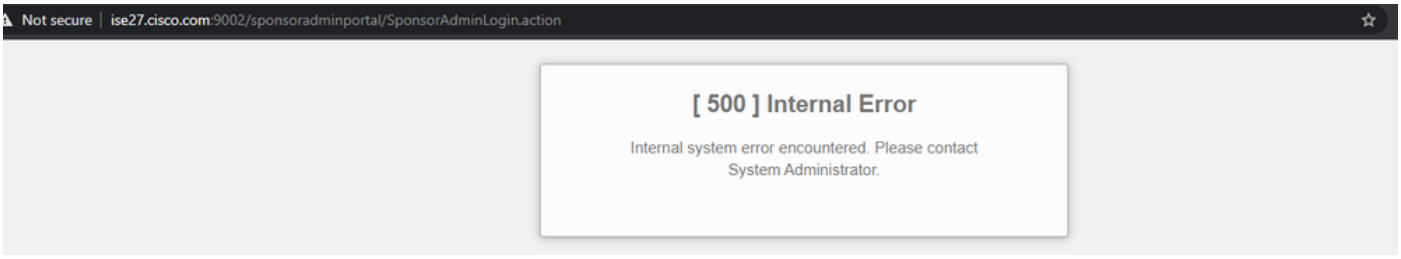
1. تصل حزمة الطلب إلى الخادم دون تغيير.
2. يحتوي خادم ISE على الأذونات/الامتيازات الموصى بها من قبل المورد للعبارة لمعالجة هذا الطلب.




## لا يمكن الوصول إلى صفحة الحسابات

1. تحت **مراكز العمل > Guest Access (وصول الضيف) > Manage Accounts** Button، يوجه زر **إدارة**

**الحسابات** إلى ISE FQDN على المنفذ 9002، لكي يتمكن مسؤول ISE من الوصول إلى بوابة الكفيل:




2. تحقق مما إذا تم حل FQDN بواسطة محطة العمل التي يتم الوصول من خلالها إلى بوابة الكفيل باستخدام الأمر **nslookup <FQDN من ISE PAN>**.

3. تحقق مما إذا كان ISE TCP ميناء 9002 مفتوحا من ال CLI من ال ISE مع الأمر **show ports | بما في ذلك 9002**.

## أفضل الممارسات لشهادة البوابة

- من أجل تجربة المستخدم السلسة، يجب أن يتم توقيع الشهادة المستخدمة في البوابات ودور المسؤول من قبل هيئات شهادات عامة معروفة (مثل GoDaddy و DigiCert و VeriSign وما إلى ذلك)، والتي عادة ما يتم الوثوق بها من قبل المستعرضين (مثل Google Chrome و Firefox وما إلى ذلك).

- ال يوصى باستخدام IP الثابت لإعادة توجيه الضيف لأن ذلك يجعل IP الخاص ل ISE مرئيا لجميع المستخدمين. ال يوفر معظم الموردين شهادات موقعة من قبل جهة خارجية لبروتوكول الإنترنت الخاص.

- عندما ينقل أنت من ISE 2.4 p6 إلى p8 أو p9، هناك خطأ معروف: cisco بق id CSCvp75207 حيث **الثقة للمصادقة داخل ISE** و **الثقة لمصادقة العميل و syslog** صندوق يجب أن يكون فحصت يدويا بعد ترقية التصحيح. وهذا يضمن أن يقوم ISE بإرسال سلسلة الشهادات الكاملة لتدفق TLS عند الوصول إلى مدخل الضيف.

إذا لم تحل هذه الإجراءات مشاكل الوصول إلى الضيف، فيرجى الوصول إلى TAC باستخدام حزمة دعم مجمعة مع إرشادات من المستند: تصحيح الأخطاء لتمكين ISE.

# معلومات ذات صلة

- الدعم التقني والتنزيلات من Cisco

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).