تكوين شبكة VPN للوصول عن بعد باستخدام مصادقة RADIUS على تخطيط ISE و Group-Policy

المحتويات

المقدمة

المتطلبات الأساسية

المتطلبات

المكونات المستخدمة

التكوين

التكوين

ASA

محرك خدمات كشف الهوية (ISE)

التحقق من الصحة

سيناريو العمل

استكشاف الأخطاء وإصلاحها

سيناريو عدم العمل 1

سيناريو عدم العمل 2

سيناريو عدم العمل 3

الفيديو

المقدمة

يصف هذا المستند تكوين شبكة VPN للوصول عن بعد لتعيين سياسة المجموعة باستخدام محرك خدمات تعريف Cisco (ISE).

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- Cisco Secure Client (AnyConnect)
- Cisco ISE
- شبكة VPN للوصول عن بعد على جهاز الأمان القابل للتكيف (ASA) من Cisco

المكونات المستخدمة

يستند محتوى هذا المستند إلى إصدارات البرامج والمكونات المادية التالية.

- ASA 5506 مع برنامج صيغة 9.8.1
- AnyConnect نم 4.8 رادصإلا
- ISE رادصإلا 2.4.

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.

التكوين

في مثال التكوين هذا، السماح للمستخدمين البعديين الذين يتصلون ب ASA عبر VPN (مجموعة أنفاق) من Cisco Secure Client (AnyConnect) باستخدام تحديد ملف تعريف اتصال بتحديد مجموعة النفق DefaultWEBvpngGroup وبنهج مجموعة DfltGrpPolicy. بعد المصادقة، إذا تم إرسال سمة فئة RADIUS (من نهج المجموعة) بواسطة ISE ضمن إستجابة المصادقة، يتم تعيين المستخدم إلى نهج المجموعة المطابق، وبالتالي يتم تلقي الأذونات المناسبة. إذا لم يقم ISE بإرجاع أي سمة من الفئة وأ إرجاع تسمية نهج مجموعة لم يتم تكوينها على ASA، فسيظل المستخدم معينا إلى DfltGrpPolicy. لمنع المستخدمين الذين ليس لديهم نهج مجموعة معين من الاتصال من خلال شبكة VPN، يمكنك تكوين الأمر vpn-synchronins 0 ضمن نهج المجموعة DfltGrpPolicy.

التكوين

ASA

مداخ AAA

```
aaa-server ISE_AAA protocol radius
aaa-server ISE_AAA (Outside) host 10.31.124.82
 key cisco123
```

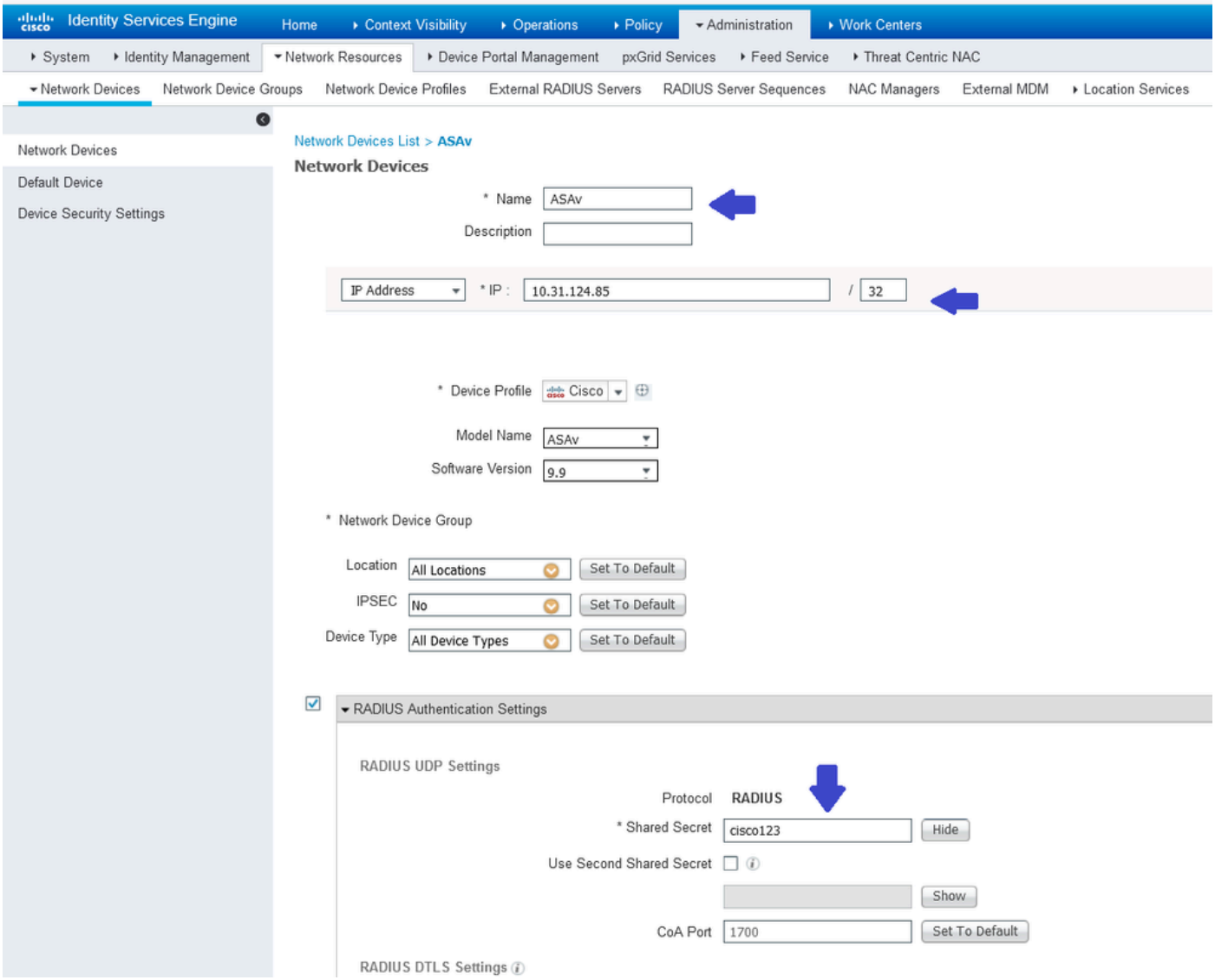
تكوين VPN للوصول عن بعد

```
webvpn
 enable outside
 anyconnect image disk0:/anyconnect-win-4.7.01076-webdeploy-k9.pkg 1
 anyconnect enable

tunnel-group DefaultWEBVPNGroup general-attributes
 address-pool Remote_users
 authentication-server-group ISE_AAA
```

```
group-policy DfltGrpPolicy attributes
 banner value ###YOU DON'T HAVE AUTHORIZATION TO ACCESS ANY INTERNAL RESOURCES###
 vpn-simultaneous-logins 0
 vpn-tunnel-protocol ssl-client

group-policy RADIUS-USERS internal
group-policy RADIUS-USERS attributes
 banner value YOU ARE CONNECTED TO ### RADIUS USER AUTHENTICATION###
 vpn-simultaneous-logins 3
 vpn-tunnel-protocol ssl-client
 split-tunnel-network-list value SPLIT_ACL

group-policy RADIUS-ADMIN internal
group-policy RADIUS-ADMIN attributes
 banner value YOU ARE CONNECTED TO ###RADIUS ADMIN AUTHENTICATION ###
 vpn-simultaneous-logins 3
 vpn-tunnel-protocol ssl-client
 split-tunnel-network-list none
```

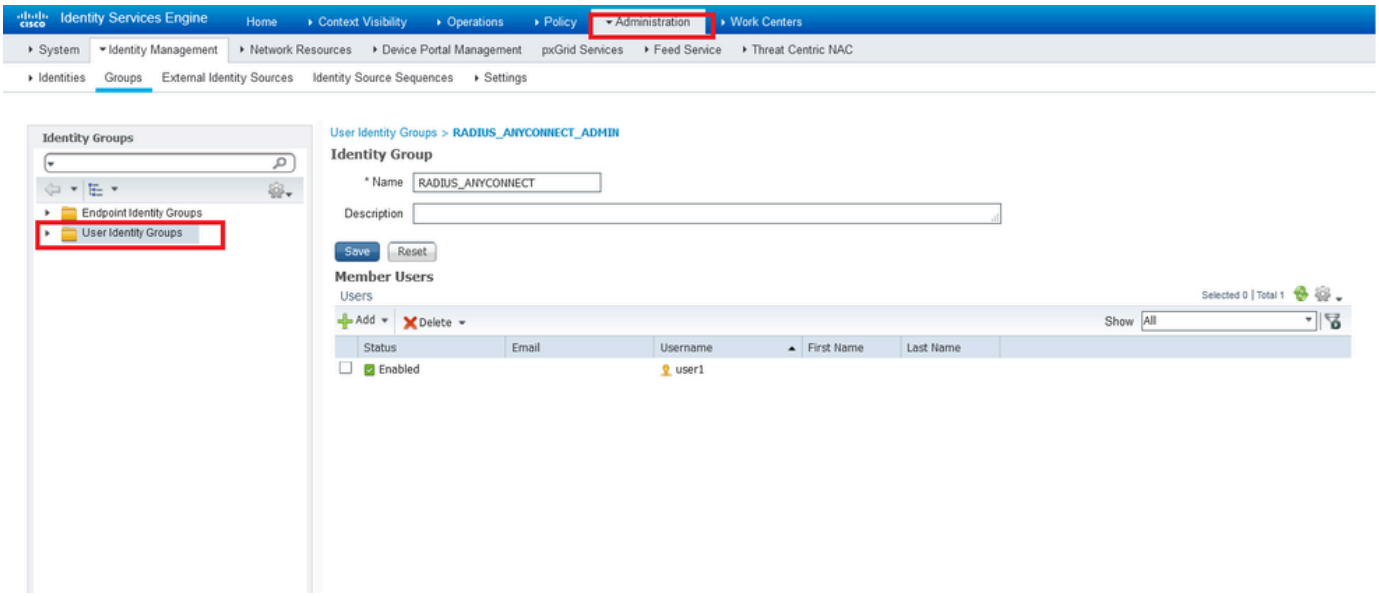
محرك خدمات كشف الهوية (ISE)

الخطوة 1. سجل ASA كجهاز شبكة صالح على ISE وقم بتكوين المفتاح السري المشترك لـ RADIUS. لهذا الغرض، انتقل إلى الإدارة>موارد الشبكة>أجهزة الشبكة.



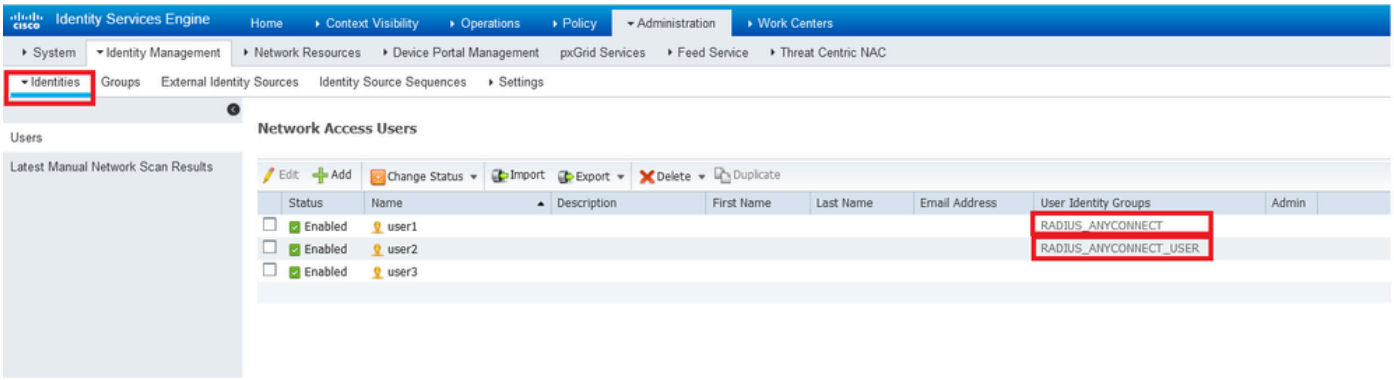
الخطوة 2. إنشاء مجموعات هوية.

قم بتعريف مجموعات الهوية لإقران المستخدمين بخصائص مماثلة والذين يتقاسمون أذون مماثلة. يتم إستخدام هذه العناصر في الخطوات التالية. انتقل إلى الإدارة>مجموعات هوية المستخدم.



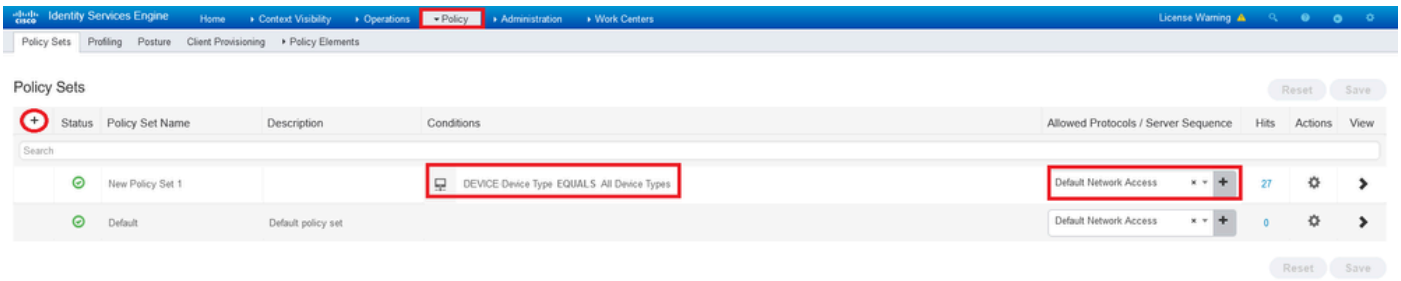
الخطوة 3. إقران المستخدمين بمجموعات الهوية.

إقران المستخدمين بمجموعة الهوية الصحيحة. انتقل إلى إدارة>هويات>المستخدمين.



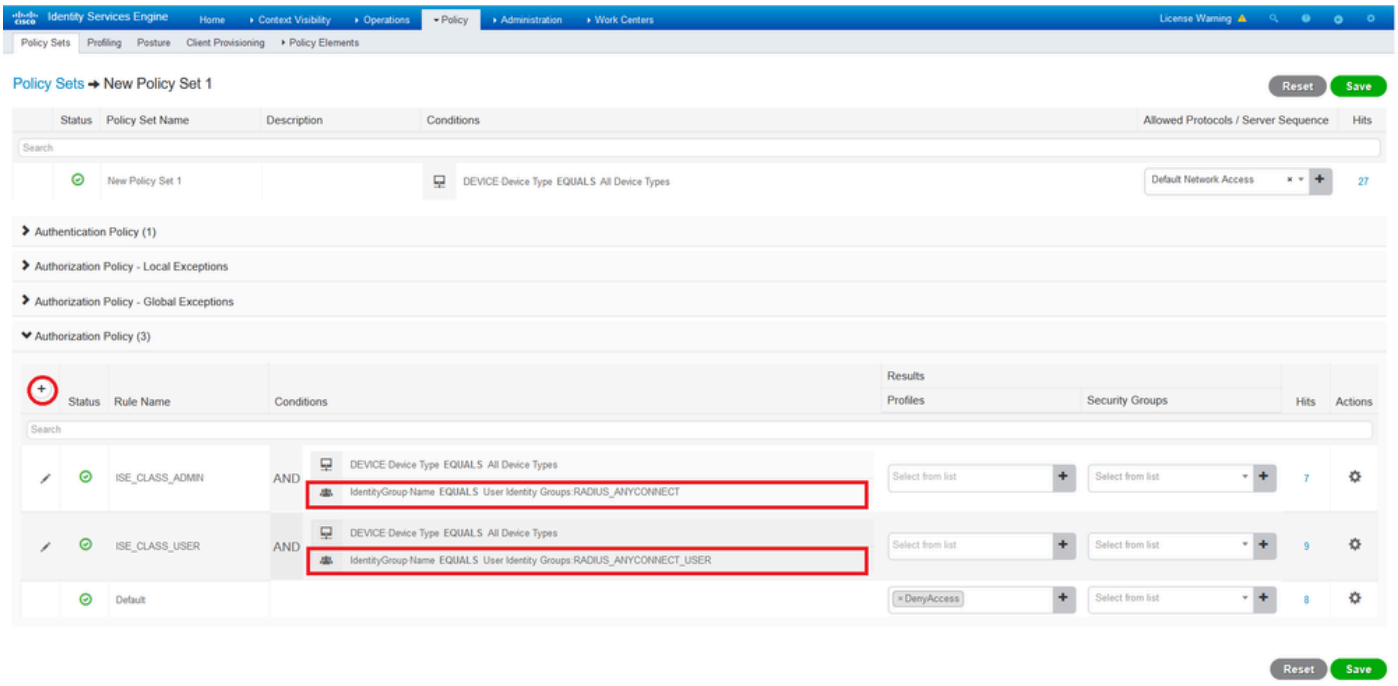
الخطوة 4. إنشاء مجموعة سياسات.

قم بتحديد مجموعة سياسات جديدة وتحديد الشروط التي تطابق السياسة. في هذا المثال، يتم السماح بجميع أنواع الأجهزة تحت الشروط. لهذا الغرض، انتقل إلى النهج>مجموعات النهج.



الخطوة 5. إنشاء سياسة تخويل.

قم بتحديد نهج تخويل جديد بالشروط المطلوبة لمطابقة النهج. تأكد من تضمين مجموعات الهوية التي تم إنشاؤها في الخطوة 2 كشرط.

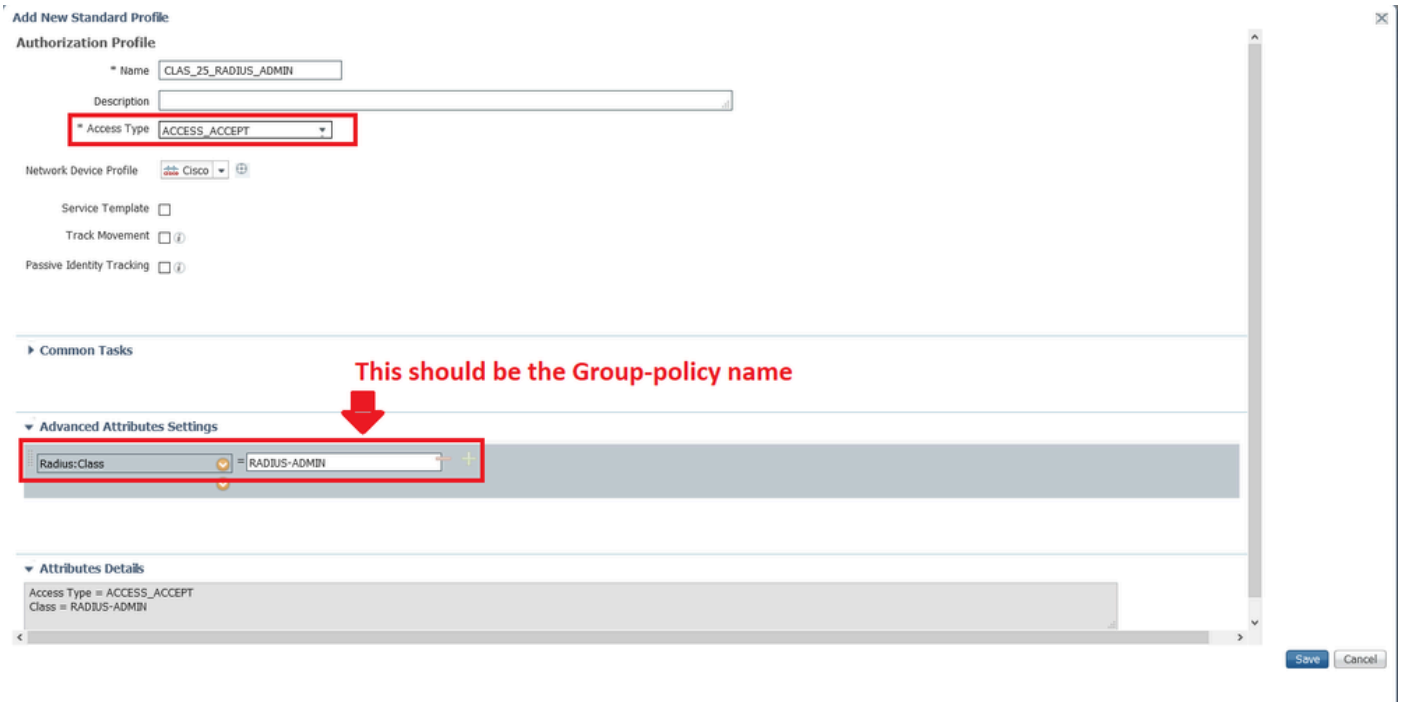


الخطوة 6. إنشاء ملف تعريف تخويل.

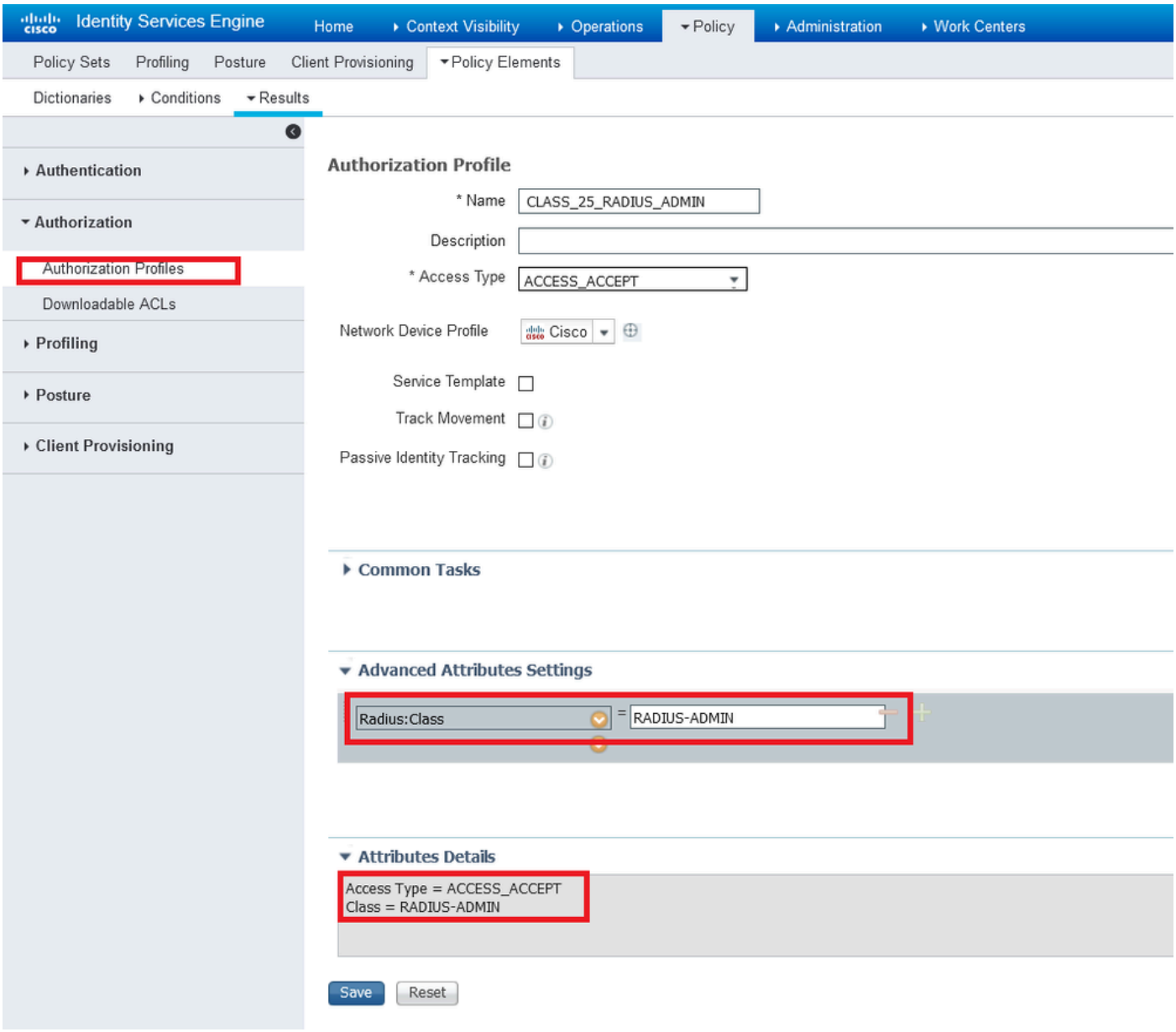
يتضمن ملف تعريف التخويل الإجراءات التي يتم إتخاذها عند مطابقة سياسة التخويل. إنشاء ملف تعريف تخويل جديد يتضمن السمات التالية:

- فئة RADIUS = <group-policy-ASA>
- نوع الوصول: ACCESS_ACCEPT.

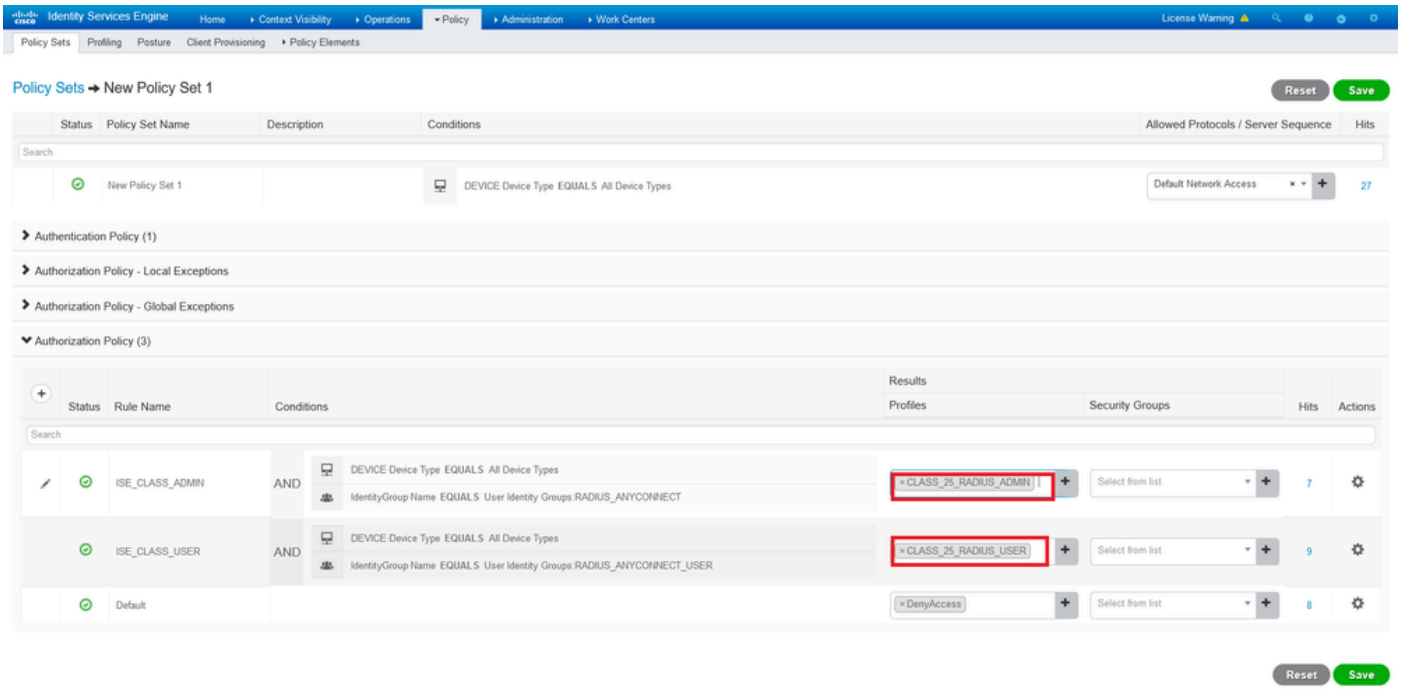
ملاحظة: يجب تحرير التكوين المعروض في الصور السابقة لمطابقة اسم نهج المجموعة التي قمت بتعريفها في تكوين ASA الخاص بك.



الخطوة 7. راجع تكوين ملف تعريف التخويل.



ملاحظة: في نفس مجموعة النهج، يمكن أن يكون لديك نهج تخويل في تعييني كل مجموعة هويّة إلى نهج مجموعة محدد محدد محدد في ASA.



باستخدام مثال التكوين هذا، يمكنك تعيين نهج المجموعة بشكل ديناميكي لكل مستخدم عميل آمن من خلال تكوين ISE استنادا إلى مجموعة الهوية التي ينتمي إليها المستخدم.

التحقق من الصحة

أحد أكثر تصحيح الأخطاء فائدة هو debug radius. وهو يعرض تفاصيل طلب مصادقة RADIUS واستجابة المصادقة بين خادم AAA (ISE) و ASA.

```
debug radius
```

أداة مفيدة أخرى هي الأمر test aaa-server. أنت الآن ترى ما إذا كانت المصادقة مقبولة أو مرفوضة والسمات ('سمة الفئة في هذا المثال) التي تم تبادلها في عملية المصادقة.

```
test aaa-server authentication

        [host

        |

         ] username

           password
```

سيناريو العمل

في مثال التكوين المذكور سابقا، ينتمي المستخدم1 إلى مجموعة RADIUS-Admin لكل تكوين ISE. يمكن التحقق من صحته إذا قمت بتشغيل الاختبار aaa-server وتمكين تصحيح أخطاء radius على ASA. يتم وضع العلامة باللون الغامق على الأسطر ذات الصلة من عمليات تصحيح الأخطاء.

<#root>

```
ASAv# debug radius
ASAv#test aaa-server authentication ISE_AAA host 10.31.124.82 username user1 password *****
INFO: Attempting Authentication test to IP address (10.31.124.82) (timeout: 12 seconds)


RADIUS packet decode (authentication request)

--------------------------------------
Raw packet data (length = 84).....
01 1e 00 54 ac b6 7c e5 58 22 35 5e 8e 7c 48 73    |  ...T..|.X"5^.|Hs
04 9f 8c 74 01 07 75 73 65 72 31 02 12 ad 19 1c    |  ...t..user1.....
40 da 43 e2 ba 95 46 a7 35 85 52 bb 6f 04 06 0a    |  @.C...F.5.R.o...
1f 7c 55 05 06 00 00 00 06 3d 06 00 00 00 05 1a    |  .|U......=......
15 00 00 00 09 01 0f 63 6f 61 2d 70 75 73 68 3d    |  .......coa-push=
74 72 75 65                                        |  true

Parsed packet data.....
Radius: Code = 1 (0x01)
Radius: Identifier = 30 (0x1E)
Radius: Length = 84 (0x0054)
Radius: Vector: ACB67CE55822355E8E7C4873049F8C74
Radius: Type = 1 (0x01) User-Name
Radius: Length = 7 (0x07)
Radius: Value (String) =
75 73 65 72 31                                     |

user1

Radius: Type = 2 (0x02) User-Password
Radius: Length = 18 (0x12)
Radius: Value (String) =
ad 19 1c 40 da 43 e2 ba 95 46 a7 35 85 52 bb 6f    |  ...@.C...F.5.R.o
Radius: Type = 4 (0x04) NAS-IP-Address
Radius: Length = 6 (0x06)
Radius: Value (IP Address) = 10.31.124.85 (0x0A1F7C55)
Radius: Type = 5 (0x05) NAS-Port
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x6
```

```
Radius: Type = 61 (0x3D) NAS-Port-Type
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x5
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 21 (0x15)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 15 (0x0F)
Radius: Value (String) =
63 6f 61 2d 70 75 73 68 3d 74 72 75 65             |  coa-push=true
send pkt 10.31.124.82/1645
rip 0x00007f03b419fb08 state 7 id 30
rad_vrfy() : response message verified
rip 0x00007f03b419fb08
 : chall_state ''
 : state 0x7
 : reqauth:
     ac b6 7c e5 58 22 35 5e 8e 7c 48 73 04 9f 8c 74
 : info 0x00007f03b419fc48
     session_id 0x80000007
     request_id 0x1e
     user 'user1'
     response '***'
     app 0
     reason 0
     skey 'cisco123'
     sip 10.31.124.82
     type 1
```

RADIUS packet decode (response)

```
--------------------------------------
Raw packet data (length = 188).....
02 1e 00 bc 9e 5f 7c db ad 63 87 d8 c1 bb 03 41    |  ....._|..c.....A
37 3d 7a 35 01 07 75 73 65 72 31 18 43 52 65 61    |  7=z5..user1.CRea
75 74 68 53 65 73 73 69 6f 6e 3a 30 61 31 66 37    |  uthSession:0a1f7
63 35 32 52 71 51 47 52 72 70 36 5a 35 66 4e 4a    |  c52RqQGRrp6Z5fNJ
65 4a 39 76 4c 54 6a 73 58 75 65 59 35 4a 70 75    |  eJ9vLTjsXueY5Jpu
70 44 45 61 35 36 34 66 52 4f 44 57 78 34 19 0e    |  pDEa564fRODWx4..
52 41 44 49 55 53 2d 41 44 4d 49 4e 19 50 43 41    |  RADIUS-ADMIN.PCA
43 53 3a 30 61 31 66 37 63 35 32 52 71 51 47 52    |  CS:0a1f7c52RqQGR
72 70 36 5a 35 66 4e 4a 65 4a 39 76 4c 54 6a 73    |  rp6Z5fNJeJ9vLTjs
58 75 65 59 35 4a 70 75 70 44 45 61 35 36 34 66    |  XueY5JpupDEa564f
52 4f 44 57 78 34 3a 69 73 65 61 6d 79 32 34 2f    |  RODWx4:iseamy24/
33 37 39 35 35 36 37 34 35 2f 33 31                |  379556745/31

Parsed packet data.....
Radius: Code = 2 (0x02)
Radius: Identifier = 30 (0x1E)
Radius: Length = 188 (0x00BC)
Radius: Vector: 9E5F7CDBAD6387D8C1BB0341373D7A35
Radius: Type = 1 (0x01) User-Name
Radius: Length = 7 (0x07)
Radius: Value (String) =
75 73 65 72 31                                     |
```

user1

```
Radius: Type = 24 (0x18) State
Radius: Length = 67 (0x43)
```

```
Radius: Value (String) =
52 65 61 75 74 68 53 65 73 73 69 6f 6e 3a 30 61    |  ReauthSession:0a
31 66 37 63 35 32 52 71 51 47 52 72 70 36 5a 35    |  1f7c52RqQGRrp6Z5
66 4e 4a 65 4a 39 76 4c 54 6a 73 58 75 65 59 35    |  fNJeJ9vLTjsXueY5
4a 70 75 70 44 45 61 35 36 34 66 52 4f 44 57 78    |  JpupDEa564fRODWx
34                                                  |  4
```

Radius: Type = 25 (0x19) Class

```
Radius: Length = 14 (0x0E)
Radius: Value (String) =
52 41 44 49 55 53 2d 41 44 4d 49 4e                |
```

RADIUS-ADMIN

```
Radius: Type = 25 (0x19) Class
Radius: Length = 80 (0x50)
Radius: Value (String) =
43 41 43 53 3a 30 61 31 66 37 63 35 32 52 71 51    |  CACS:0a1f7c52RqQ
47 52 72 70 36 5a 35 66 4e 4a 65 4a 39 76 4c 54    |  GRrp6Z5fNJeJ9vLT
6a 73 58 75 65 59 35 4a 70 75 70 44 45 61 35 36    |  jsXueY5JpupDEa56
34 66 52 4f 44 57 78 34 3a 69 73 65 61 6d 79 32    |  4fRODWx4:iseamy2
34 2f 33 37 39 35 35 36 37 34 35 2f 33 31          |  4/379556745/31
rad_procpkt: ACCEPT
```

RADIUS_ACCESS_ACCEPT

```
: normal termination
RADIUS_DELETE
remove_req 0x00007f03b419fb08 session 0x80000007 id 30
free_rip 0x00007f03b419fb08
radius: send queue empty
```

INFO: Authentication Successful

هناك طريقة أخرى للتحقق من ما إذا تم تعيين نهج المجموعة الصحيح للمستخدم 1 من قبل ISE عند الاتصال عبر العميل الآمن باستخدام الأمر show vpn-sessionDB AnyConnect.

```
<#root>

ASAv#

show vpn-sessiondb anyconnect


Session Type: AnyConnect


Username     : user1

                Index        : 28
Assigned IP  : 10.100.2.1            Public IP    : 10.100.1.3
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-256  DTLS-Tunnel: (1)AES256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA384  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 15604                 Bytes Rx     : 28706

Group Policy : RADIUS-ADMIN
```

```
Tunnel Group : DefaultWEBVPNGroup

Login Time   : 04:14:45 UTC Wed Jun 3 2020
Duration     : 0h:01m:29s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : 0a6401010001c0005ed723b5
Security Grp : none
```

استكشاف الأخطاء وإصلاحها

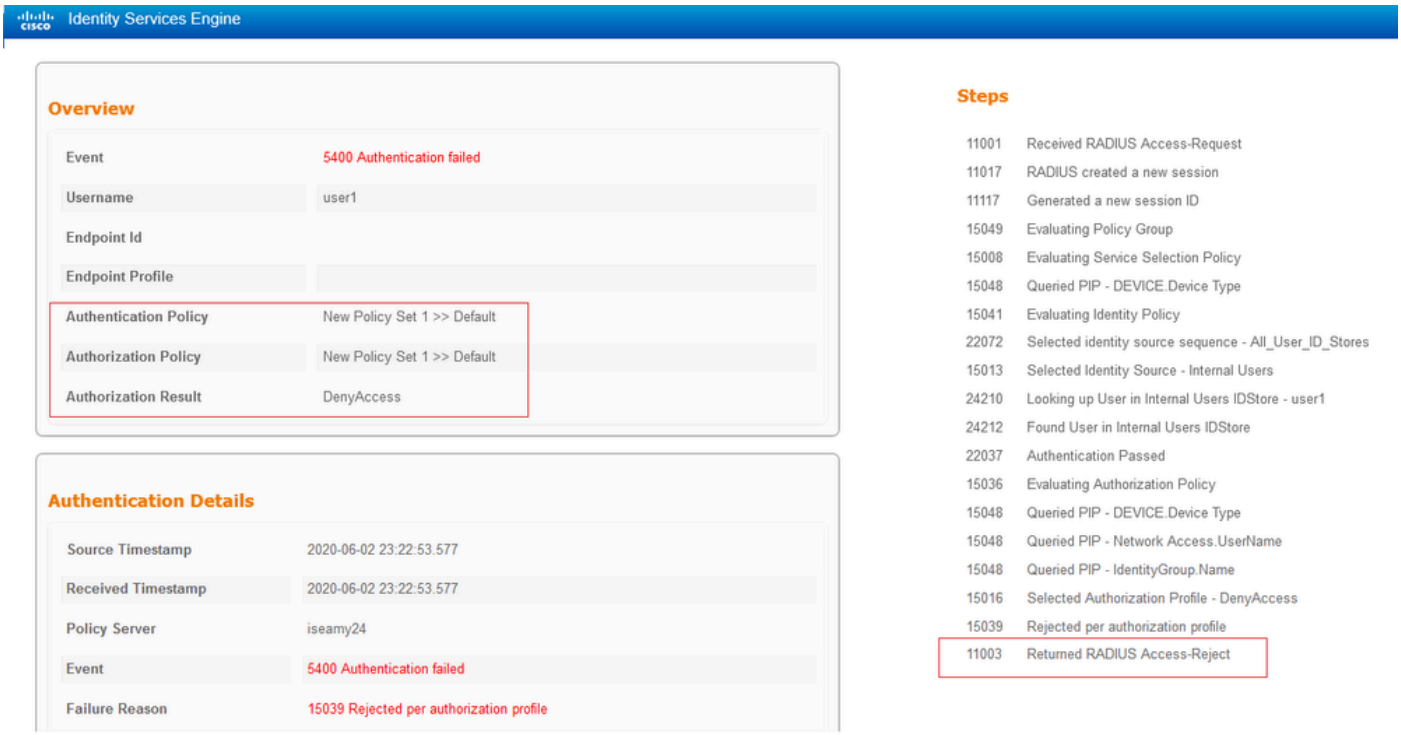
يمكنك أيضا إستخدام أوامر debug radius وtest aaa-server لاستكشاف الأخطاء وإصلاحها عند حدوث مشاكل. ثم يتم وصف القضايا الأكثر شيوعا في المستقبل.

سيناريو عدم العمل 1

إذا فشلت المصادقة على AnyConnect وكان ISE يرد برفض. يجب التحقق من اقتران المستخدم بمجموعة هوية المستخدم أو أن كلمة المرور غير صحيحة. انتقل إلى التفاصيل > السجلات المباشرة > العمليات.

<#root>

```
RADIUS packet decode (response)

--------------------------------------
Raw packet data (length = 20).....
03 21 00 14 dd 74 bb 43 8f 0a 40 fe d8 92 de 7a    |  .!...t.C..@....z
27 66 15 be                                        |  'f..

Parsed packet data.....
Radius: Code = 3 (0x03)
Radius: Identifier = 33 (0x21)
Radius: Length = 20 (0x0014)
Radius: Vector: DD74BB438F0A40FED892DE7A276615BE
rad_procpkt:

REJECT

RADIUS_DELETE
remove_req 0x00007f03b419fb08 session 0x80000009 id 33
free_rip 0x00007f03b419fb08
radius: send queue empty

ERROR: Authentication Rejected: AAA failure
```



ملاحظة: في هذا المثال، لا يقترن user1 بأي مجموعة هوية مستخدم. وبالتالي، فإنه ينفذ سياسات المصادقة والتفويض الافتراضية ضمن مجموعة السياسات الجديدة 1 باستخدام الإجراء DenyAccess. يمكنك تعديل هذا الإجراء إلى AllowedAccess في نهج التخويل الافتراضي للسماح للمستخدمين الذين لا توجد مجموعة هوية المستخدم المقترنة بالمصادقة.

سيناريو عدم العمل 2

إذا فشلت المصادقة في AnyConnect وكان نهج التخويل الافتراضي هو PermitAccess، يتم قبول المصادقة. ومع ذلك، لا يتم تقديم سمة الفئة في إستجابة RADIUS، وبالتالي يكون المستخدم موجودا في DfltGrpPolicy ولا يتصل بسبب الأمر الذي تم تكوينه: عمليات تسجيل الدخول المتزامنة لـ VPN 0.

<#root>

RADIUS packet decode (response)

```
--------------------------------------
Raw packet data (length = 174).....
02 24 00 ae 5f 0f bc b1 65 53 64 71 1a a3 bd 88    |  .$.._...eSdq....
7c fe 44 eb 01 07 75 73 65 72 31 18 43 52 65 61    |  |.D...user1.CRea
75 74 68 53 65 73 73 69 6f 6e 3a 30 61 31 66 37    |  uthSession:0a1f7
63 35 32 32 39 54 68 33 47 68 6d 44 54 49 35 71    |  c5229Th3GhmDTI5q
37 48 46 45 30 7a 6f 74 65 34 6a 37 50 76 69 4b    |  7HFE0zote4j7PviK
5a 35 77 71 6b 78 6c 50 39 33 42 6c 4a 6f 19 50    |  Z5wqkxlP93BlJo.P
43 41 43 53 3a 30 61 31 66 37 63 35 32 32 39 54    |  CACS:0a1f7c5229T
68 33 47 68 6d 44 54 49 35 71 37 48 46 45 30 7a    |  h3GhmDTI5q7HFE0z
6f 74 65 34 6a 37 50 76 69 4b 5a 35 77 71 6b 78    |  ote4j7PviKZ5wqkx
6c 50 39 33 42 6c 4a 6f 3a 69 73 65 61 6d 79 32    |  lP93BlJo:iseamy2
34 2f 33 37 39 35 35 36 37 34 35 2f 33 37          |  4/379556745/37
```

```
Parsed packet data.....
Radius: Code = 2 (0x02)
Radius: Identifier = 36 (0x24)
Radius: Length = 174 (0x00AE)
Radius: Vector: 5F0FBCB1655364711AA3BD887CFE44EB
Radius: Type = 1 (0x01) User-Name
Radius: Length = 7 (0x07)
Radius: Value (String) =
75 73 65 72 31                                  |
```

user1

```
Radius: Type = 24 (0x18) State
Radius: Length = 67 (0x43)
Radius: Value (String) =
52 65 61 75 74 68 53 65 73 73 69 6f 6e 3a 30 61    |  ReauthSession:0a
31 66 37 63 35 32 32 39 54 68 33 47 68 6d 44 54    |  1f7c5229Th3GhmDT
49 35 71 37 48 46 45 30 7a 6f 74 65 34 6a 37 50    |  I5q7HFE0zote4j7P
76 69 4b 5a 35 77 71 6b 78 6c 50 39 33 42 6c 4a    |  viKZ5wqkxlP93BlJ
6f                                                 |  o
Radius: Type = 25 (0x19) Class
Radius: Length = 80 (0x50)
Radius: Value (String) =
43 41 43 53 3a 30 61 31 66 37 63 35 32 32 39 54    |  CACS:0a1f7c5229T
68 33 47 68 6d 44 54 49 35 71 37 48 46 45 30 7a    |  h3GhmDTI5q7HFE0z
6f 74 65 34 6a 37 50 76 69 4b 5a 35 77 71 6b 78    |  ote4j7PviKZ5wqkx
6c 50 39 33 42 6c 4a 6f 3a 69 73 65 61 6d 79 32    |  lP93BlJo:iseamy2
34 2f 33 37 39 35 35 36 37 34 35 2f 33 37          |  4/379556745/37
rad_procpkt: ACCEPT
```

RADIUS_ACCESS_ACCEPT

```
: normal termination
RADIUS_DELETE
remove_req 0x00007f03b419fb08 session 0x8000000b id 36
free_rip 0x00007f03b419fb08
radius: send queue empty
```

INFO: Authentication Successful

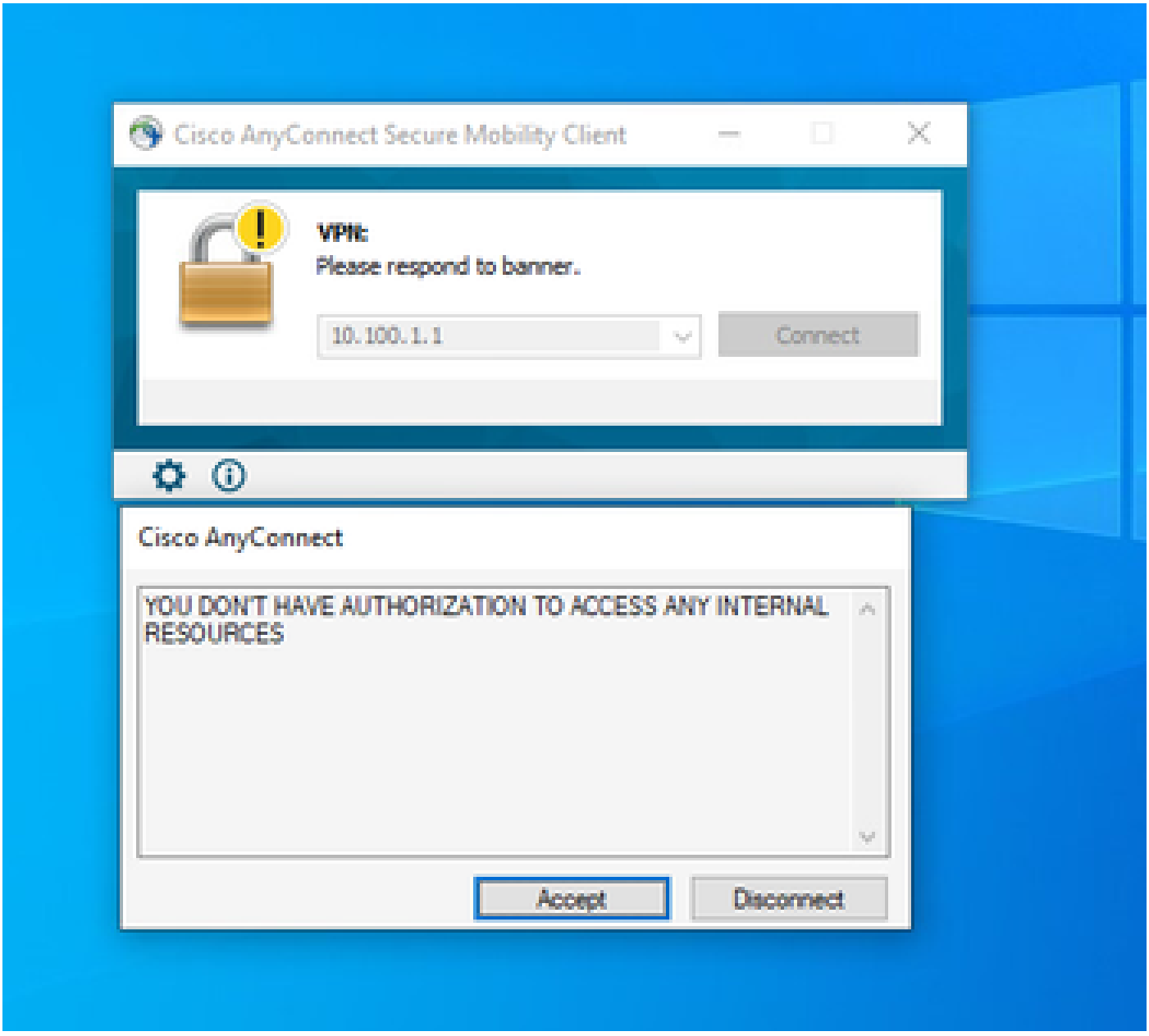
```
ASAv#
```

إذا تم تغيير عمليات تسجيل الدخول المتزامنة لـ VPN من 0 إلى "1"، يتصل المستخدم كما هو موضح في الإخراج:

<#root>

```
ASAv# show vpn-sessiondb anyconnect

Session Type: AnyConnect


Username     : user1

                 Index        : 41
Assigned IP  : 10.100.2.1             Public IP    : 10.100.1.3
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-256  DTLS-Tunnel: (1)AES256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA384  DTLS-Tunnel: (1)SHA1
```

```
Bytes Tx     : 15448                  Bytes Rx     : 15528

Group Policy : DfltGrpPolicy          Tunnel Group : DefaultWEBVPNGroup

Login Time   : 18:43:39 UTC Wed Jun 3 2020
Duration     : 0h:01m:40s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : 0a640101000290005ed7ef5b
Security Grp : none
```



سيناريو عدم العمل 3

إذا مرت المصادقة ولم يكن لدى المستخدم النهج الصحيحة المطبقة، على سبيل المثال، إذا كان نهج المجموعة المتصل يحتوي على النفق المقسم بدلا من النفق الكامل كما يجب. يمكن أن يكون المستخدم في مجموعة هوية المستخدم الخطأ.

<#root>

```
ASAv# sh vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : user1

                 Index        : 29
Assigned IP  : 10.100.2.1             Public IP    : 10.100.1.3
Protocol     : AnyConnect-Parent SSL-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA384
Bytes Tx     : 15592                  Bytes Rx     : 0

Group Policy : RADIUS-USERS

          Tunnel Group : DefaultWEBVPNGroup
Login Time   : 04:36:50 UTC Wed Jun 3 2020
Duration     : 0h:00m:20s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : 0a6401010001d0005ed728e2
Security Grp : none
```

الفيديو

يوفر هذا الفيديو الخطوات لتكوين SSL AnyConnect بمصادقة ISE وسمة الفئة لتعيين نهج المجموعة.

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).