# 為組策略對映配置SSL Anyconnect的ISE身份驗證和類屬性

## 目錄

## 簡介

本文檔介紹如何使用思科身份服務引擎(ISE)配置安全套接字層(SSL)Anyconnect，以便使用者對映到特定組策略。

作者：思科TAC工程師Amanda Nava。

## 必要條件

### 需求

思科建議您瞭解以下主題：

- AnyConnect安全行動化使用者端版本4.7
- Cisco ISE 2.4
- Cisco ASA 9.8或更高版本。

### 採用元件

本文檔的內容基於這些軟體和硬體版本。

- 採用軟體版本9.8.1的調適型安全裝置(ASA)5506
- Microsoft Windows 10 64位版上的AnyConnect安全移動客戶端4.2.00096。
- ISE版本2.4。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設

）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

# 設定

在示例中，Anyconnect使用者直接連線，而無需從下拉選單中選擇隧道組的選項，因為思科ISE會根據他們的屬性將它們分配給特定組策略。

## ASA

### AAA伺服器

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

### Anyconnect

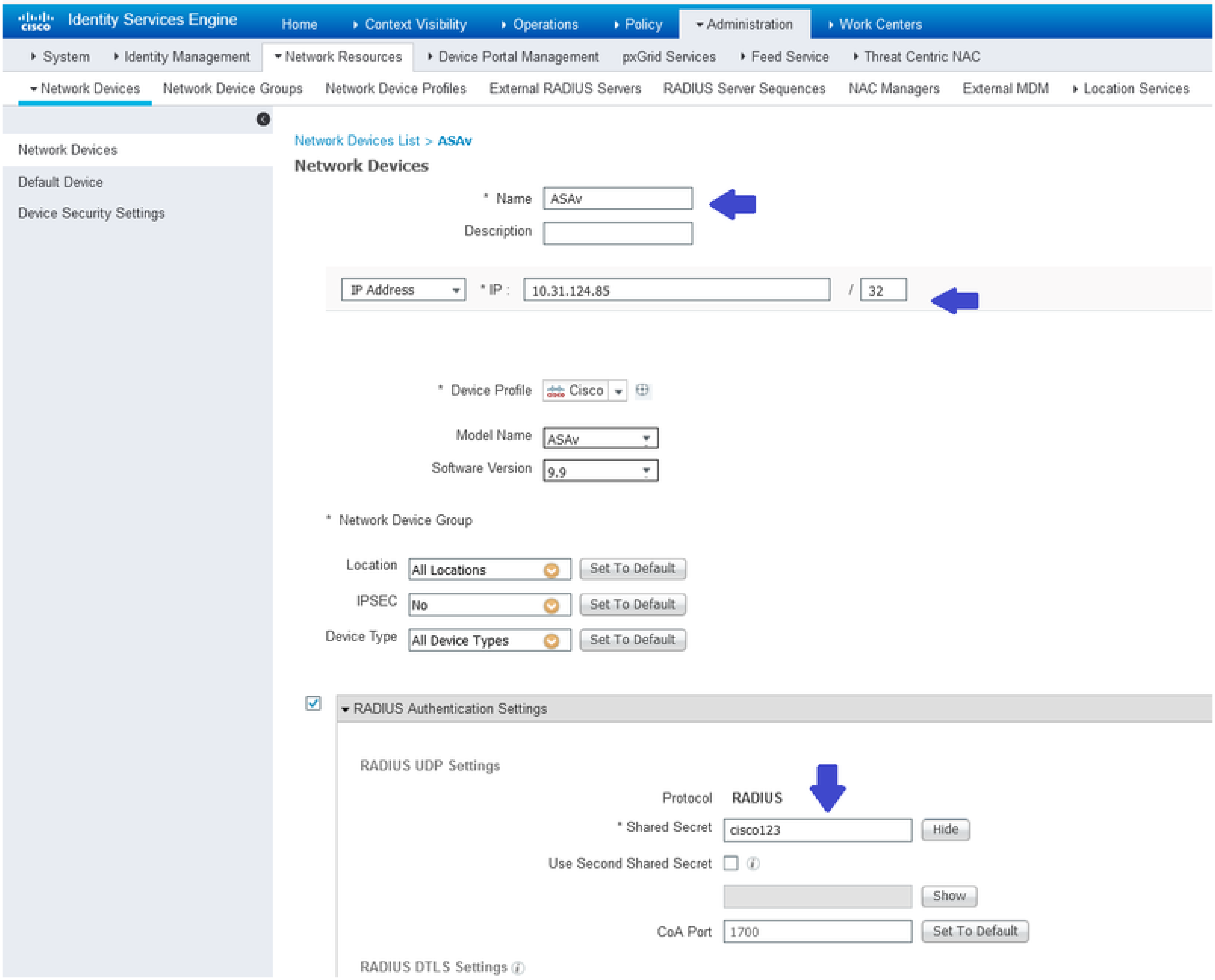
```
webvpn
enable outside
anyconnect image disk0:/anyconnect-win-4.7.01076-webdeploy-k9.pkg 1
anyconnect enable

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
```

> **附註**：在此配置示例中，您可以通過ISE配置將組策略分配給每個Anyconnect使用者。由於使用者沒有選擇隧道組的選項，因此他們連線到DefaultWEBVPNGroup tunnel-group和DfltGrpPolicy。身份驗證發生後，Class屬性(Group-policy)在ISE身份驗證響應中返回後，將使用者分配到相應的組。如果使用者沒有應用Class屬性，則此使用者仍保留在DfltGrpPolicy中。您可以在DfltGrpPolicy組下配置**vpn-simultaneous-logins 0**，以避免沒有組策略的使用者通過VPN進行連線。

# ISE

步驟1.將ASA新增到ISE。

在此步驟中，導覽至**管理>網路資源>網路裝置。**



* Name: ASAv

Description:

IP Address * IP : 10.31.124.85 / 32

* Device Profile: Cisco

Model Name: ASAv

Software Version: 9.9

* Network Device Group

Location: All Locations — Set To Default

IPSEC: No — Set To Default

Device Type: All Device Types — Set To Default

☑ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol: RADIUS

* Shared Secret: cisco123 — Hide

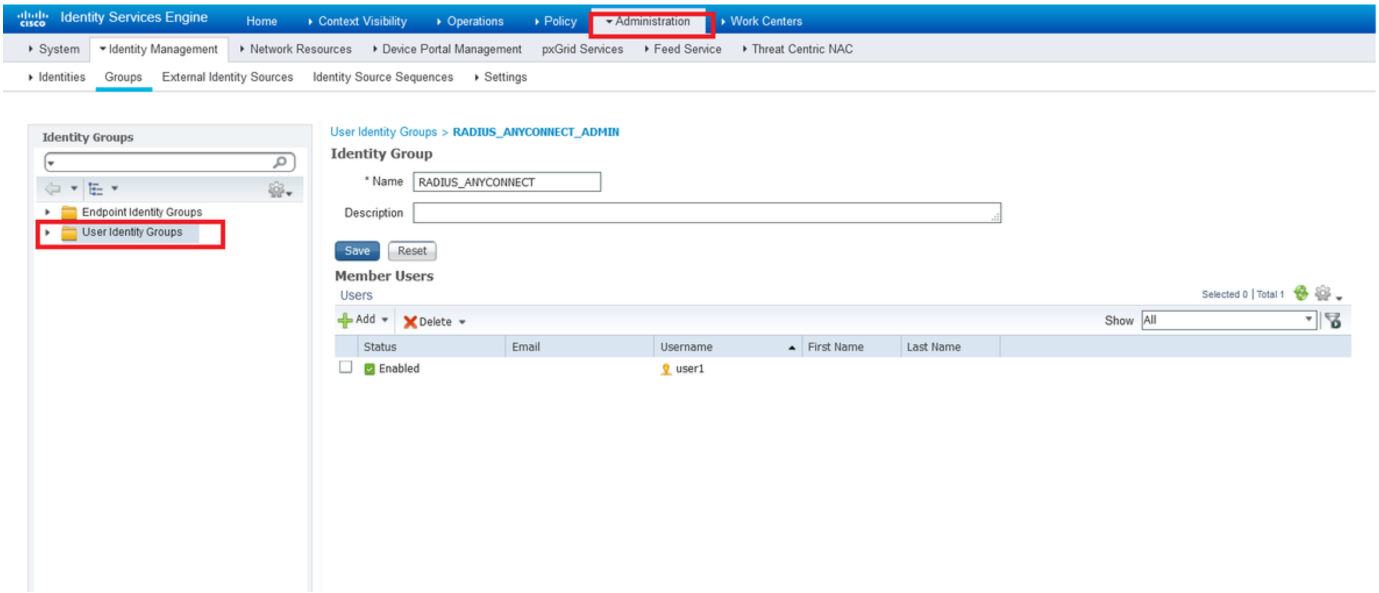
Use Second Shared Secret □ — Show

CoA Port: 1700 — Set To Default

RADIUS DTLS Settings

步驟2.建立身份組。

定義身份組，以便在後續步驟中將每個使用者與正確的使用者相關聯。導航到**管理>組>使用者身份組。**



User Identity Groups > RADIUS_ANYCONNECT_ADMIN

Identity Group

* Name: RADIUS_ANYCONNECT

Description:

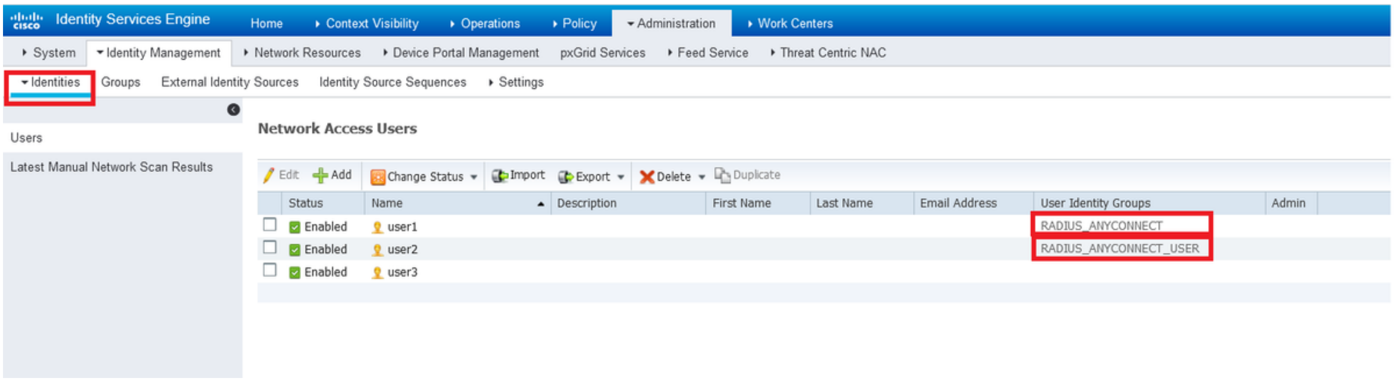
Member Users

Users

| | Status | Email | Username | First Name | Last Name |
|---|---|---|---|---|---|
| ☐ | Enabled | | user1 | | |

步驟3.將使用者與身份組關聯。

將使用者關聯到正確的身份組。導航到**管理>身份>使用者。**

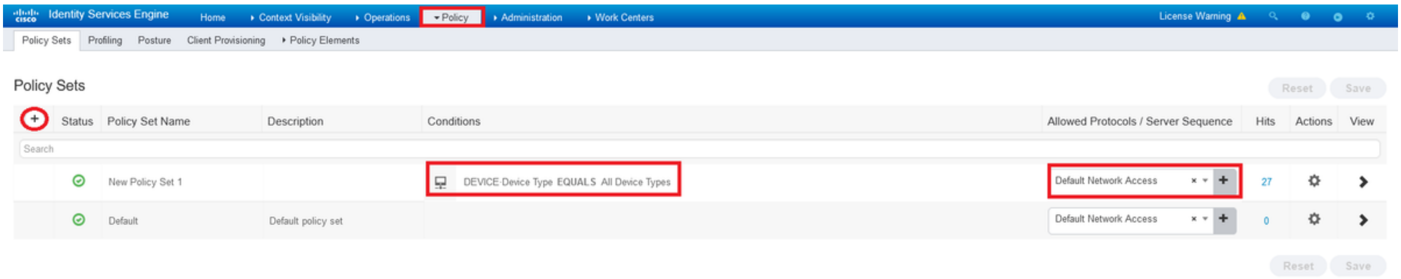


Network Access Users

| | Status | Name | Description | First Name | Last Name | Email Address | User Identity Groups | Admin |
|---|---|---|---|---|---|---|---|---|
| ☐ | Enabled | user1 | | | | | RADIUS_ANYCONNECT | |
| ☐ | Enabled | user2 | | | | | RADIUS_ANYCONNECT_USER | |
| ☐ | Enabled | user3 | | | | | | |

步驟4.建立策略集。

在條件下定義新的策略集，如示例（所有裝置型別）所示。導航到**Policy>Policy sets。**

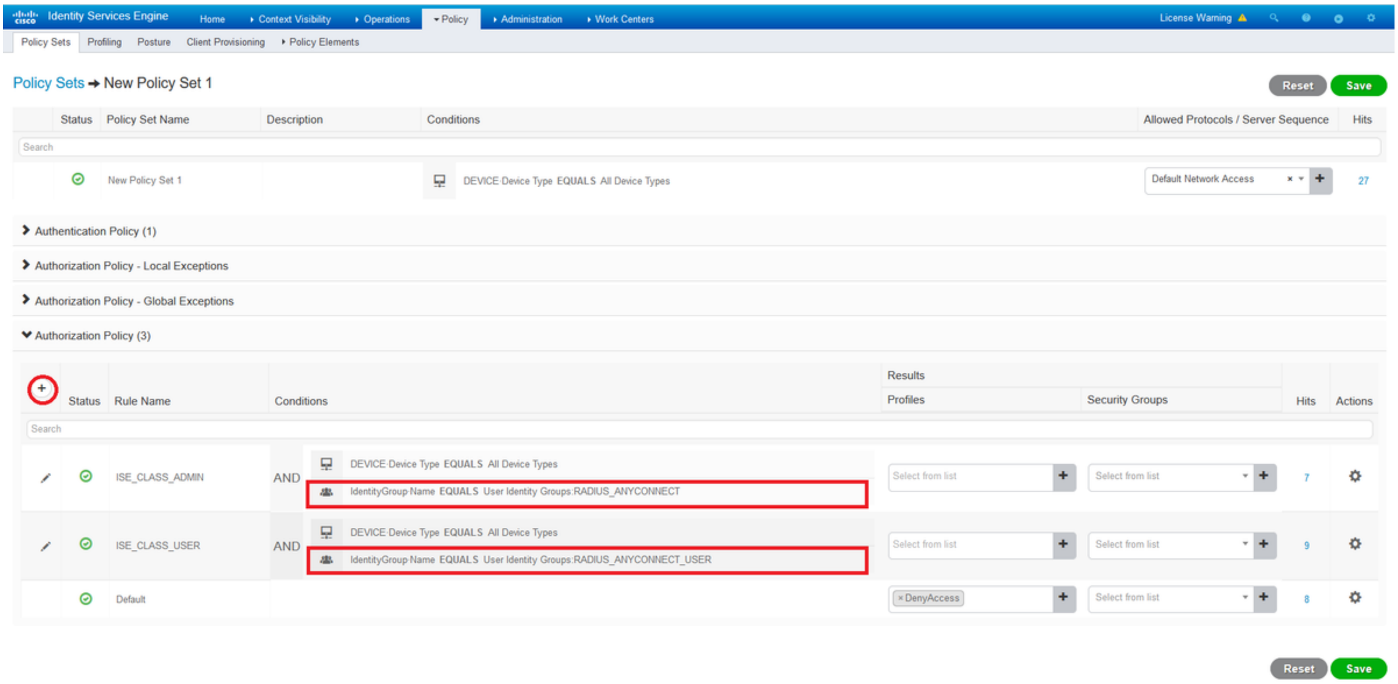


Policy Sets

| + | Status | Policy Set Name | Description | Conditions | Allowed Protocols / Server Sequence | Hits | Actions | View |
|---|---|---|---|---|---|---|---|---|
| | ✓ | New Policy Set 1 | | DEVICE·Device Type EQUALS All Device Types | Default Network Access | 27 | ⚙ | > |
| | ✓ | Default | Default policy set | | Default Network Access | 0 | ⚙ | > |

步驟5.建立授權策略。

建立具有適當條件的新授權策略以匹配身份組。

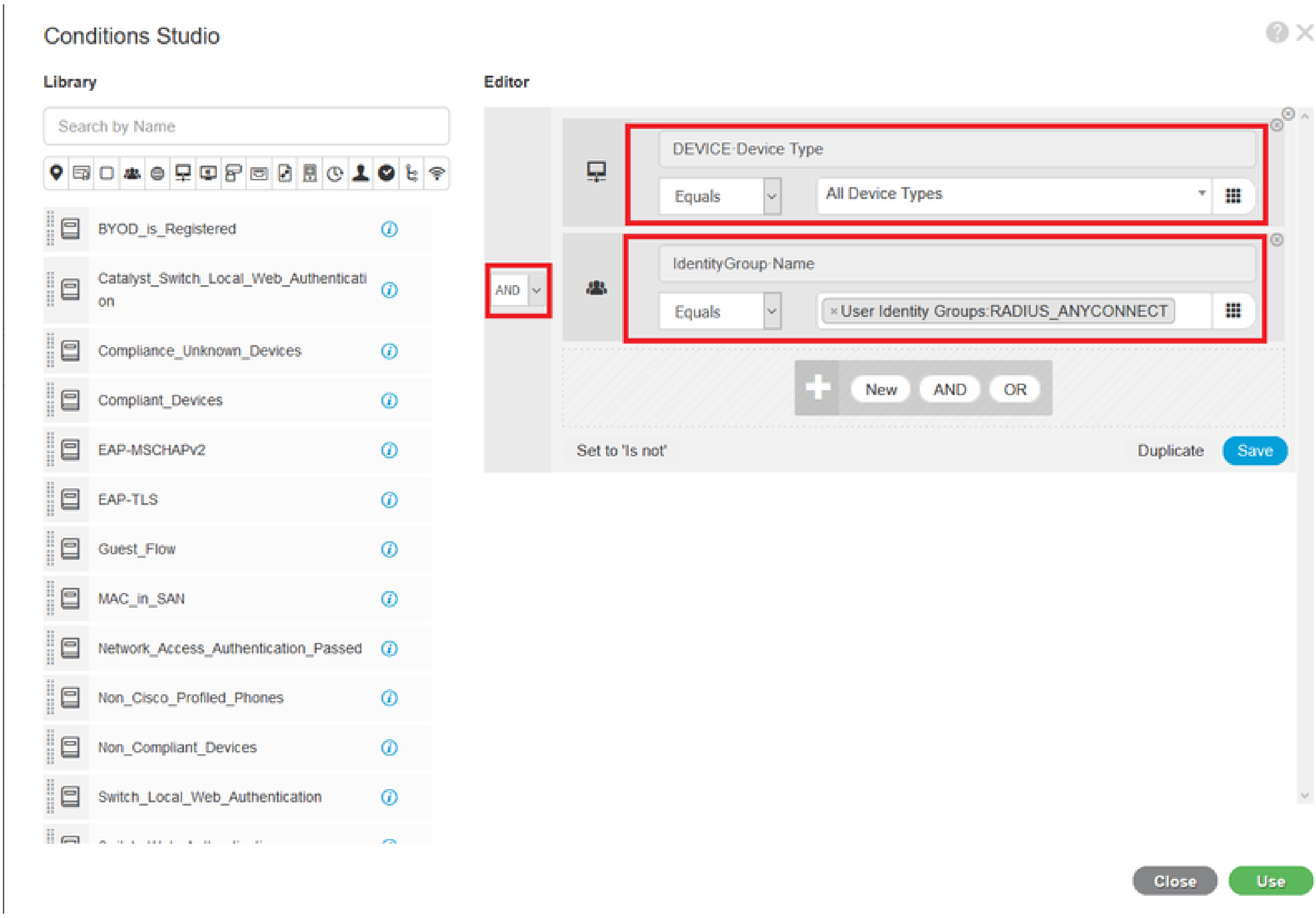


Policy Sets → New Policy Set 1

| Status | Policy Set Name | Description | Conditions | Allowed Protocols / Server Sequence | Hits |
|---|---|---|---|---|---|
| ✓ | New Policy Set 1 | | DEVICE·Device Type EQUALS All Device Types | Default Network Access | 27 |

- Authentication Policy (1)
- Authorization Policy - Local Exceptions
- Authorization Policy - Global Exceptions
- Authorization Policy (3)

| | Status | Rule Name | Conditions | | Results | | Hits | Actions |
|---|---|---|---|---|---|---|---|---|
| | | | | | Profiles | Security Groups | | |
| | ✓ | ISE_CLASS_ADMIN | AND | DEVICE·Device Type EQUALS All Device Types<br>IdentityGroup·Name EQUALS User Identity Groups:RADIUS_ANYCONNECT | Select from list | Select from list | 7 | ⚙ |
| | ✓ | ISE_CLASS_USER | AND | DEVICE·Device Type EQUALS All Device Types<br>IdentityGroup·Name EQUALS User Identity Groups:RADIUS_ANYCONNECT_USER | Select from list | Select from list | 9 | ⚙ |
| | ✓ | Default | | | × DenyAccess | Select from list | 8 | ⚙ |



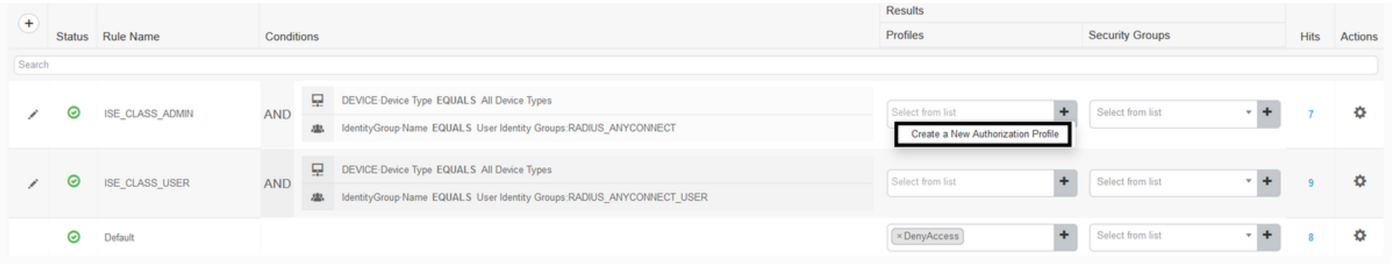
AND

DEVICE·Device Type Equals All Device Types

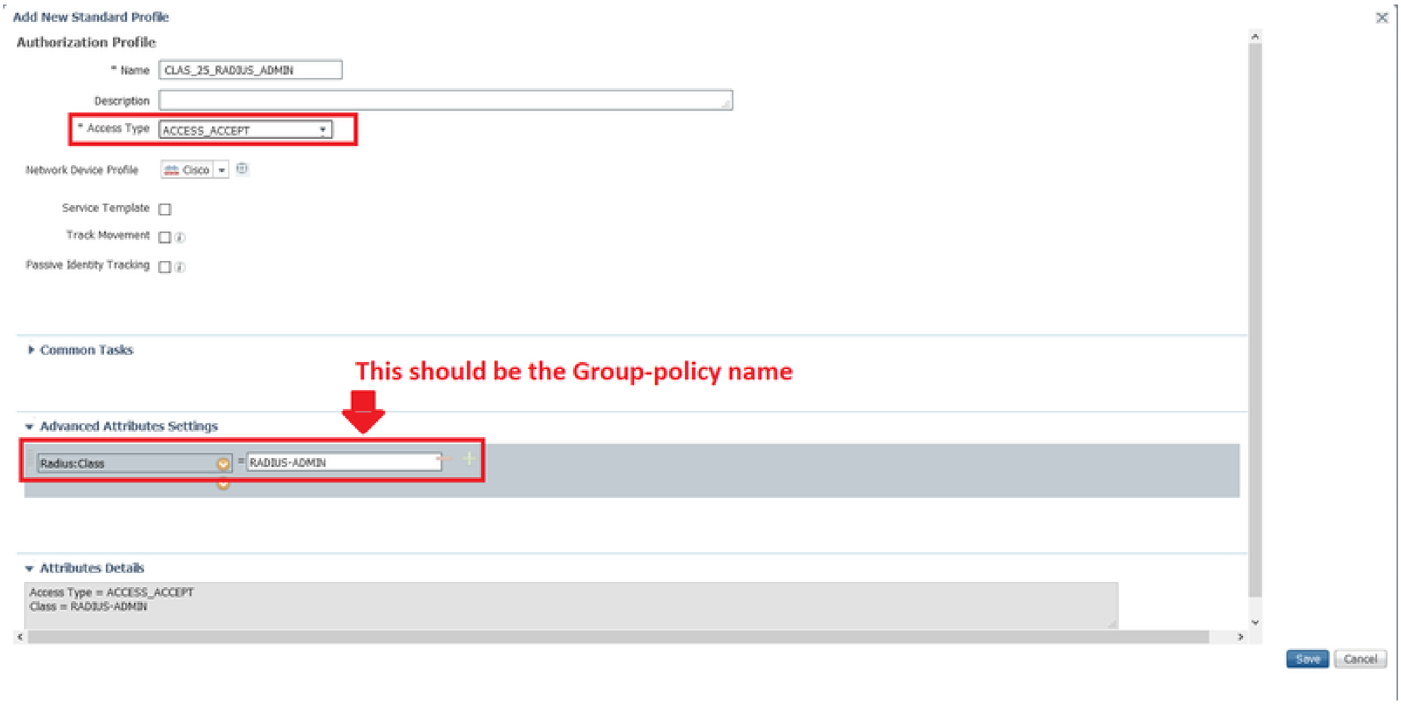
IdentityGroup·Name Equals × User Identity Groups:RADIUS_ANYCONNECT

步驟6.建立授權配置檔案。

使用RADIUS建立新授權設定檔：Class<Group-policy-ASA>屬性和*Access Type:ACCESS_ACCEPT。



|  | Status | Rule Name | Conditions |  | Results<br>Profiles | Results<br>Security Groups | Hits | Actions |
|---|---|---|---|---|---|---|---|---|
|  |  | ISE_CLASS_ADMIN | AND | DEVICE·Device Type EQUALS All Device Types<br>IdentityGroup·Name EQUALS User Identity Groups:RADIUS_ANYCONNECT | Select from list<br>Create a New Authorization Profile | Select from list | 7 |  |
|  |  | ISE_CLASS_USER | AND | DEVICE·Device Type EQUALS All Device Types<br>IdentityGroup·Name EQUALS User Identity Groups:RADIUS_ANYCONNECT_USER | Select from list | Select from list | 9 |  |
|  |  | Default |  |  | × DenyAccess | Select from list | 8 |  |



Add New Standard Profile

Authorization Profile

* Name: CLAS_25_RADIUS_ADMIN

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template □

Track Movement □

Passive Identity Tracking □

Common Tasks

This should be the Group-policy name

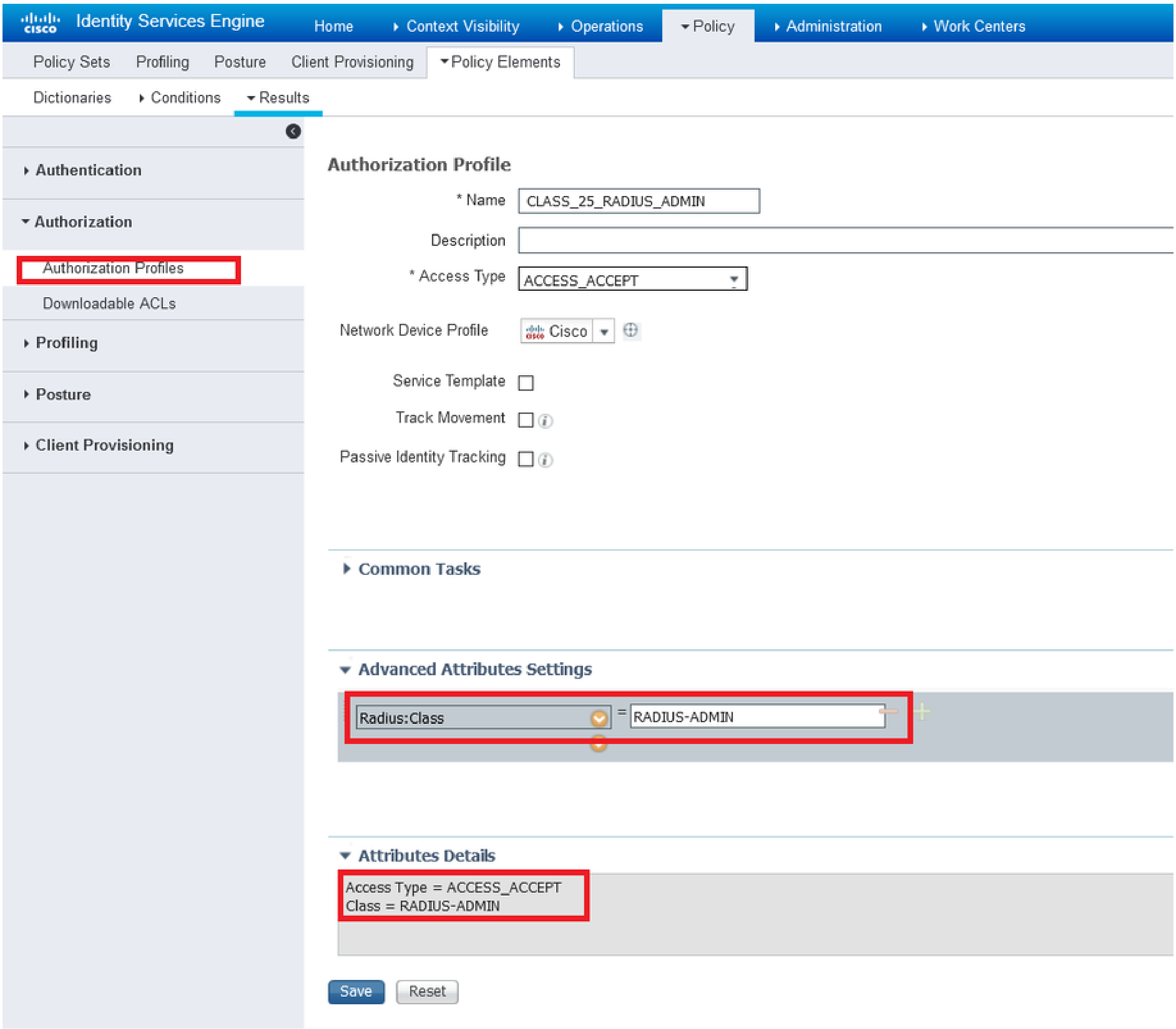
Advanced Attributes Settings

Radius:Class = RADIUS-ADMIN

Attributes Details

```
Access Type = ACCESS_ACCEPT
Class = RADIUS-ADMIN
```

步驟7.檢查授權配置檔案配置。



Authorization Profile

* Name: CLASS_25_RADIUS_ADMIN

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template □

Track Movement □

Passive Identity Tracking □

Advanced Attributes Settings

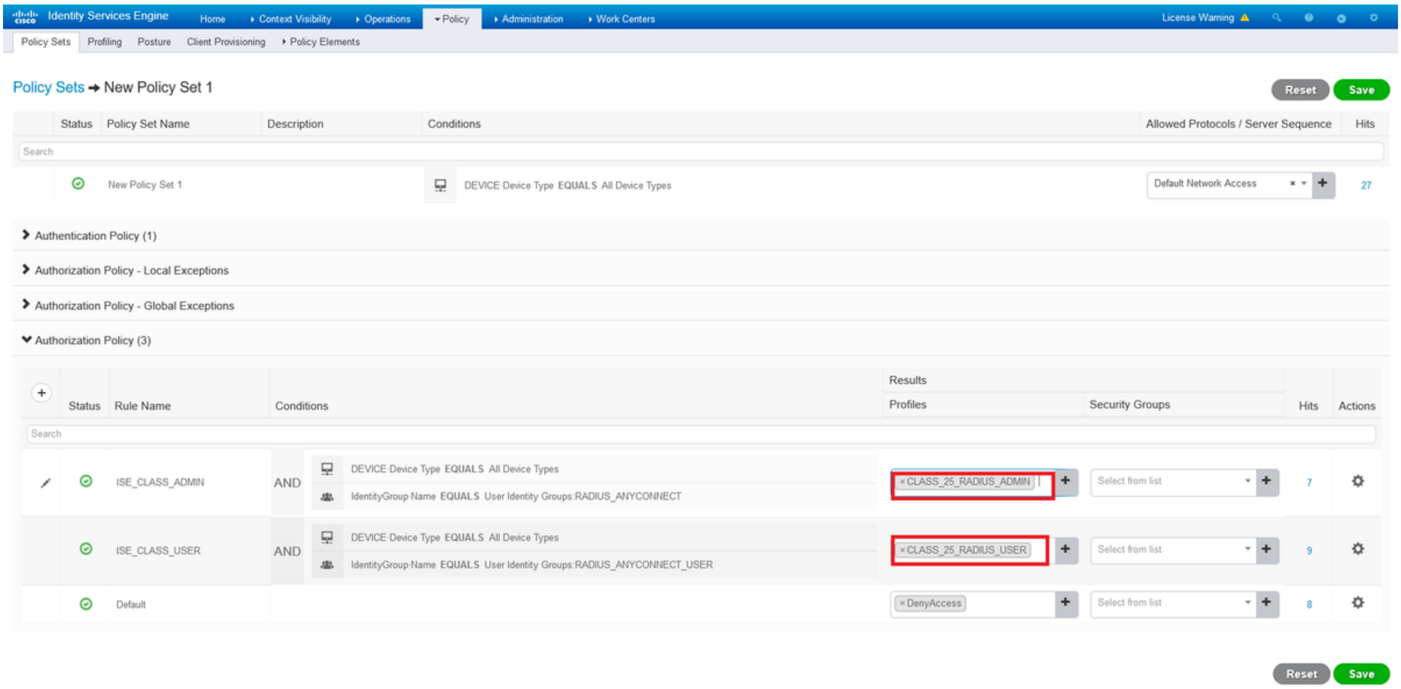
Radius:Class = RADIUS-ADMIN

Attributes Details

Access Type = ACCESS_ACCEPT
Class = RADIUS-ADMIN

**附註**：請按照上一個映像Access_Accept， Class—[25]中所示的配置進行操作，RADIUS-ADMIN是組策略的名稱（可以更改）。

該圖顯示了配置必須達到的外觀。在同一策略集上，您有n個授權策略，每個策略都與***conditions***部分中所需的身份組匹配，並使用您在ASA上的***profile***部分中的組策略**。**



Policy Sets → New Policy Set 1

| Status | Policy Set Name | Description | Conditions | Allowed Protocols / Server Sequence | Hits |
|---|---|---|---|---|---|
| ✓ | New Policy Set 1 | | DEVICE·Device Type EQUALS All Device Types | Default Network Access | 27 |

Authentication Policy (1)

Authorization Policy - Local Exceptions

Authorization Policy - Global Exceptions

Authorization Policy (3)

| | | | Results | | | |
|---|---|---|---|---|---|---|
| Status | Rule Name | Conditions | Profiles | Security Groups | Hits | Actions |
| ✓ | ISE_CLASS_ADMIN | AND DEVICE·Device Type EQUALS All Device Types<br>IdentityGroup·Name EQUALS User Identity Groups:RADIUS_ANYCONNECT | ×CLASS_25_RADIUS_ADMIN | Select from list | 7 | ⚙ |
| ✓ | ISE_CLASS_USER | AND DEVICE·Device Type EQUALS All Device Types<br>IdentityGroup·Name EQUALS User Identity Groups:RADIUS_ANYCONNECT_USER | ×CLASS_25_RADIUS_USER | Select from list | 9 | ⚙ |
| ✓ | Default | | ×DenyAccess | Select from list | 8 | ⚙ |

在此配置示例中，您可以根據類屬性通過ISE配置將組策略分配給每個Anyconnect使用者。

# 疑難排解

最有用的偵錯功能之一是**debug radius**。它顯示了AAA和ASA進程之間的radius身份驗證請求和身份驗證響應的詳細資訊。

```
debug radius
```

另一個有用的工具是命令test aaa-server。現在您可以看到身份驗證是ACCEPTED還是REFLECTED，以及身份驗證過程中交換的屬性（在本示例中為'class'屬性）。

```
test aaa-server authentication
```

## 工作場景

在上述**user1**配置示例中，根據ISE配置，屬於**RADIUS-ADMIN**組策略，如果運行測試aaa-server並調試radius，則可以驗證該配置。突出顯示需要驗證的線路。

```
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
```

另一種驗證在user1通過Anyconnect連線時是否工作的方法，使用**show vpn-sessiondb anyconnect**命令瞭解由ISE類屬性分配的組策略。

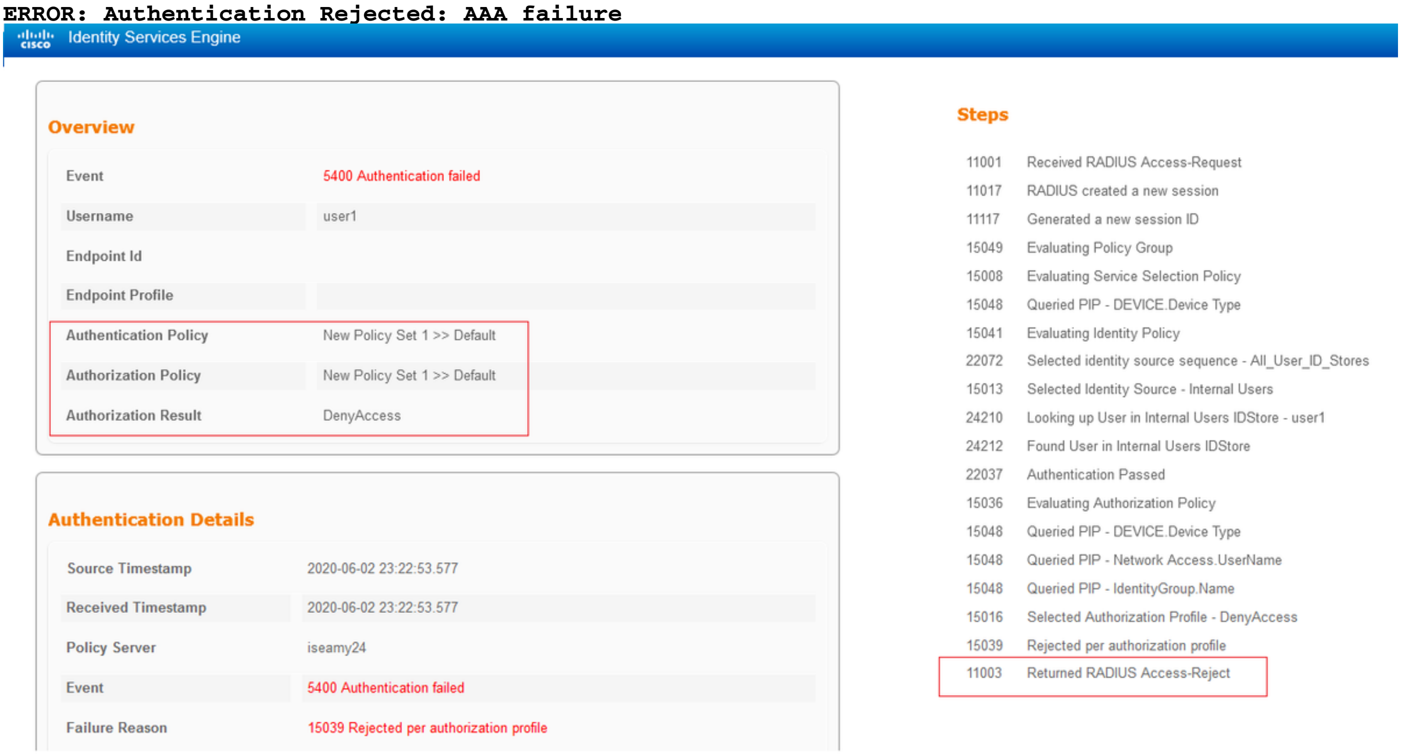
```
ASAv# show vpn-sessiondb anyconnect Session Type: AnyConnect  Username : user1                  Index
: 28
Assigned IP  : 10.100.2.1             Public IP    : 10.100.1.3
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  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
```

## 非工作場景1

如果Anyconnect上的身份驗證失敗，並且ISE使用REJECT回覆。您需要驗證使用者是否與**使用者**

**身份組**關聯，或者密碼是否不正確。 導航到**操作>即時日誌>詳細資訊。**

```
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
```



**Overview**

| | |
|---|---|
| Event | 5400 Authentication failed |
| Username | user1 |
| Endpoint Id | |
| Endpoint Profile | |
| Authentication Policy | New Policy Set 1 >> Default |
| Authorization Policy | New Policy Set 1 >> Default |
| Authorization Result | DenyAccess |

**Authentication Details**

| | |
|---|---|
| Source Timestamp | 2020-06-02 23:22:53.577 |
| Received Timestamp | 2020-06-02 23:22:53.577 |
| Policy Server | iseamy24 |
| Event | 5400 Authentication failed |
| Failure Reason | 15039 Rejected per authorization profile |

**Steps**

| | |
|---|---|
| 11001 | Received RADIUS Access-Request |
| 11017 | RADIUS created a new session |
| 11117 | Generated a new session ID |
| 15049 | Evaluating Policy Group |
| 15008 | Evaluating Service Selection Policy |
| 15048 | Queried PIP - DEVICE.Device Type |
| 15041 | Evaluating Identity Policy |
| 22072 | Selected identity source sequence - All_User_ID_Stores |
| 15013 | Selected Identity Source - Internal Users |
| 24210 | Looking up User in Internal Users IDStore - user1 |
| 24212 | Found User in Internal Users IDStore |
| 22037 | Authentication Passed |
| 15036 | Evaluating Authorization Policy |
| 15048 | Queried PIP - DEVICE.Device Type |
| 15048 | Queried PIP - Network Access.UserName |
| 15048 | Queried PIP - IdentityGroup.Name |
| 15016 | Selected Authorization Profile - DenyAccess |
| 15039 | Rejected per authorization profile |
| 11003 | Returned RADIUS Access-Reject |

**附註**：在本示例中，**user1**未與任何使用者身份組**相關聯。**因此，它會使用**DenyAccess**操作在**New Policy Set 1下觸發**預設身份驗證和**授權**策略。可以在預設授權策略中將此操作修改為**PermitAccess**，以允許沒有關聯使用者身份組的使用者進行身份驗證。

## 非工作場景2

如果Anyconnect上的身份驗證失敗且預設授權策略為PermitAccess，則接受身份驗證。但是，Radius響應中未顯示class屬性，因此使用者位於DfltGrpPolicy中，並且由於**vpn-simultaneous-logins 0而無法連線。**

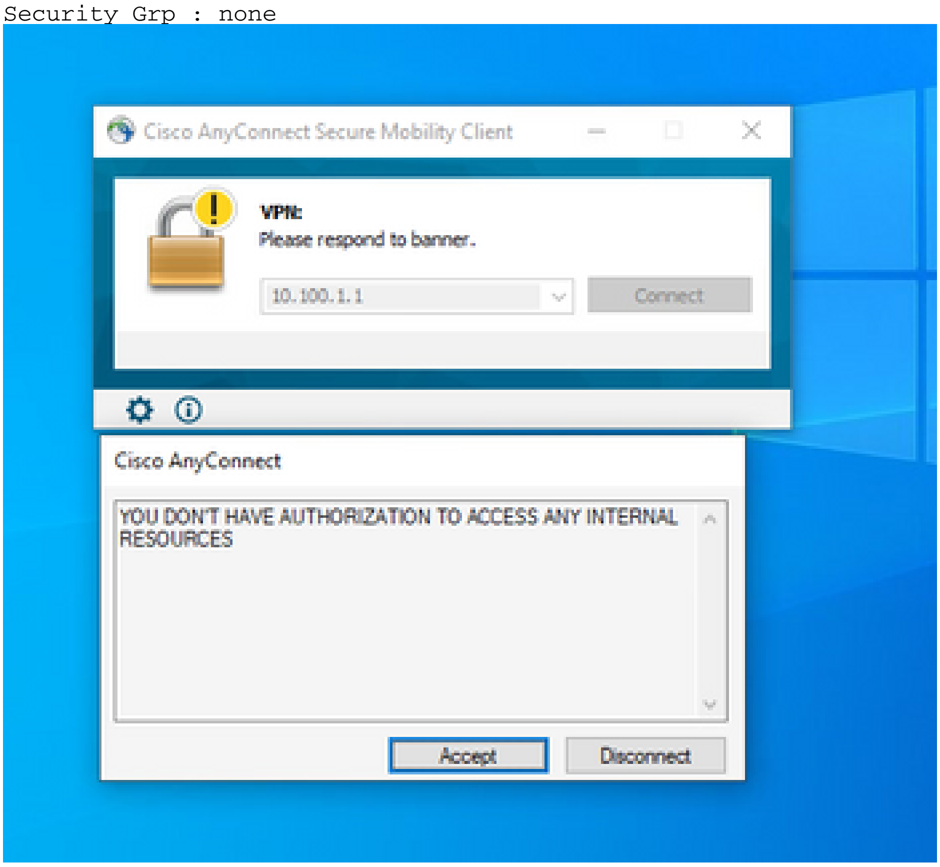
```
RADIUS packet decode (response)

--------------------------------------
```

```
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#
```

如果vpn-simultaneous-logins 0更改為'1'，則使用者連線如下輸出所示：

```
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
```



Cisco AnyConnect Secure Mobility Client
VPN:
Please respond to banner.
10.100.1.1
Connect
Cisco AnyConnect
Accept
Disconnect

YOU DON'T HAVE AUTHORIZATION TO ACCESS ANY INTERNAL RESOURCES

## 非工作場景3

如果身份驗證通過，但使用者沒有應用正確的策略，例如，如果連線的組策略有拆分隧道，而不是必須的全隧道。使用者可能位於錯誤的使用者身份組中。

```
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
```

# 影片

此影片提供了為組策略對映配置帶ISE身份驗證和類屬性的SSL Anyconnect的步驟。