

# グループポリシーマッピングのISE認証とクラス属性を使用したSSL Anyconnectの設定

## 内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[ASA](#)

[ISE](#)

[トラブルシューティング](#)

[正常動作シナリオ](#)

[動作しないシナリオ1](#)

[動作しないシナリオ2](#)

[動作しないシナリオ3](#)

[ビデオ](#)

## 概要

このドキュメントでは、特定のグループポリシーへのユーザマッピングのために、Cisco Identity Services Engine(ISE)を使用してSecure Sockets Layer(SSL)Anyconnectを設定する方法について説明します。

著者 : Cisco TACエンジニア、Amanda Nava

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- AnyConnectセキュアモバイルクライアントバージョン4.7
- Cisco ISE 2.4
- Cisco ASA バージョン 9.8 以降.

### 使用するコンポーネント

このドキュメントの内容は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ソフトウェアバージョン9.8.1が稼働する適応型セキュリティアプライアンス(ASA)5506
- Microsoft Windows 10 64ビット上のAnyConnectセキュアモバイルクライアント 4.2.00096。

- ISE バージョン 2.4.

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## 設定

この例では、Anyconnectユーザは、属性に応じてCisco ISEによって特定のグループポリシーに割り当てられるため、ドロップダウンメニューからトンネルグループを選択するオプションなしで直接接続します。

## ASA

### aaa-server

```
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
```

**注：**この設定例では、ISE設定を使用して各Anyconnectユーザにグループポリシーを割り当てることができます。ユーザにはトンネルグループを選択するオプションがないため、ユーザはDefaultWEBVPNGroup tunnel-groupとDfltGrpPolicyに接続されます。認証が発生し、

ISE認証応答でクラス属性 (グループポリシー) が戻ると、ユーザは対応するグループに割り当てられます。ユーザにクラス属性が適用されていない場合でも、このユーザは DfltGrpPolicyに残ります。VPN経由で接続するグループポリシーのないユーザを回避するために、DfltGrpPolicyグループの下にvpn-simultaneous-logins 0を設定できます。

## ISE

ステップ1:ASAをISEに追加します。

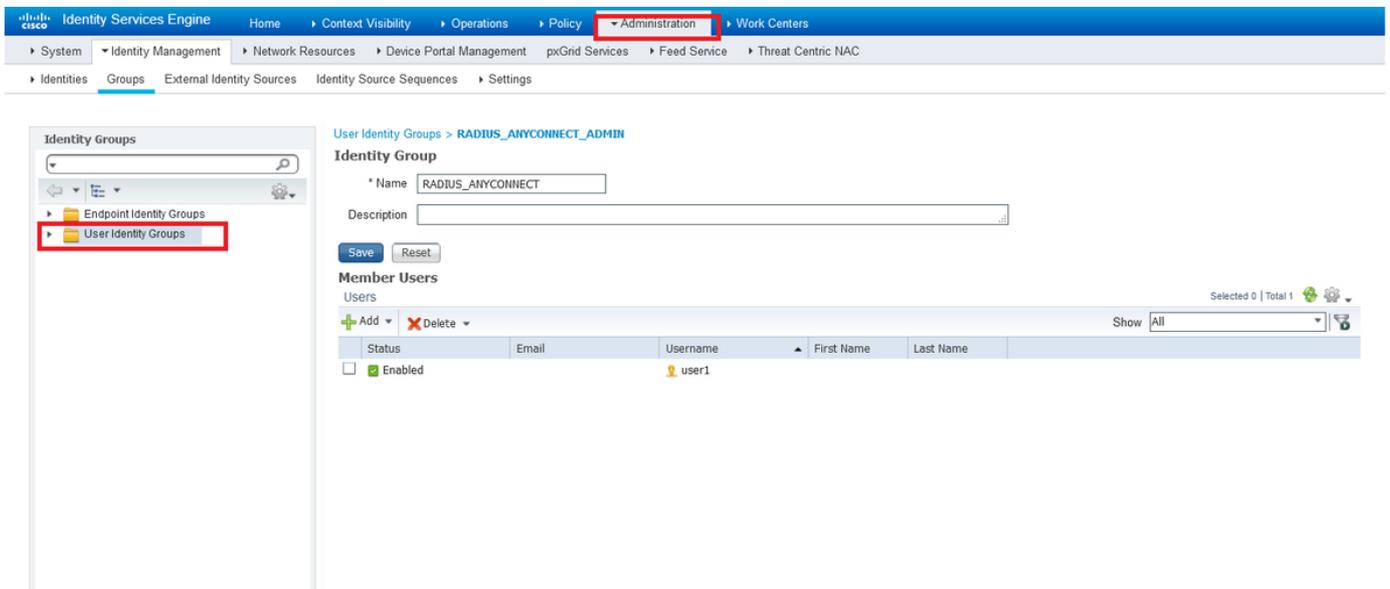
この手順を実行するには、[Administration] > [Network Resources] > [Network Devices]に移動します。

The screenshot displays the Cisco Identity Services Engine (ISE) configuration interface for a Network Device. The breadcrumb navigation is Administration > Network Resources > Network Devices. The main configuration area is titled 'Network Devices List > ASAv'. The configuration fields are as follows:

- Name:** ASAv
- Description:** (empty)
- IP Address:** 10.31.124.85 / 32
- Device Profile:** Cisco
- Model Name:** ASAv
- Software Version:** 9.9
- Network Device Group:** (empty)
- Location:** All Locations
- IPSEC:** No
- Device Type:** All Device Types
- RADIUS Authentication Settings:**
  - Protocol:** RADIUS
  - Shared Secret:** cisco123
  - Use Second Shared Secret:** (unchecked)
  - CoA Port:** 1700

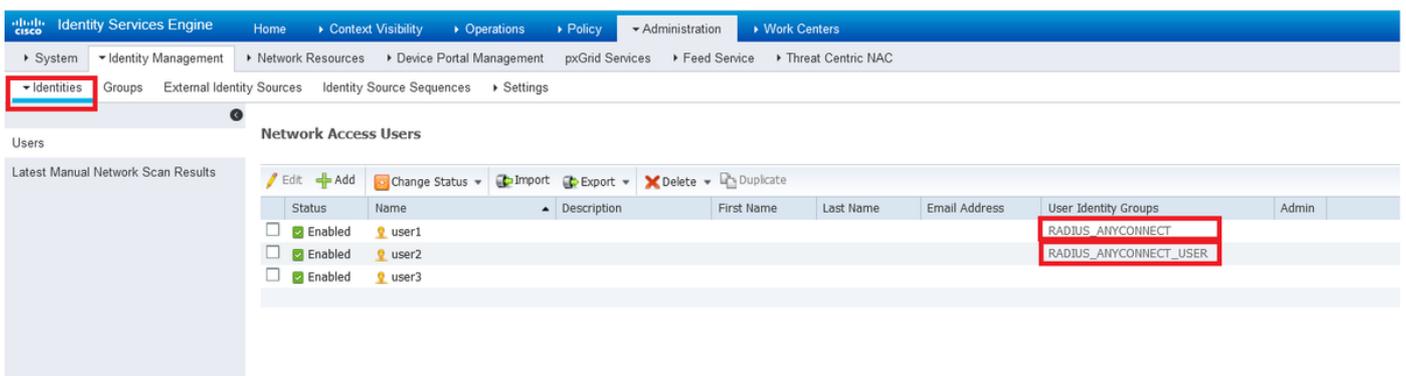
ステップ2:IDグループを作成します。

次の手順で、各ユーザを正しいユーザに関連付けるアイデンティティグループを定義します。  
[Administration] > [Groups] > [User Identity Groups]に移動します。



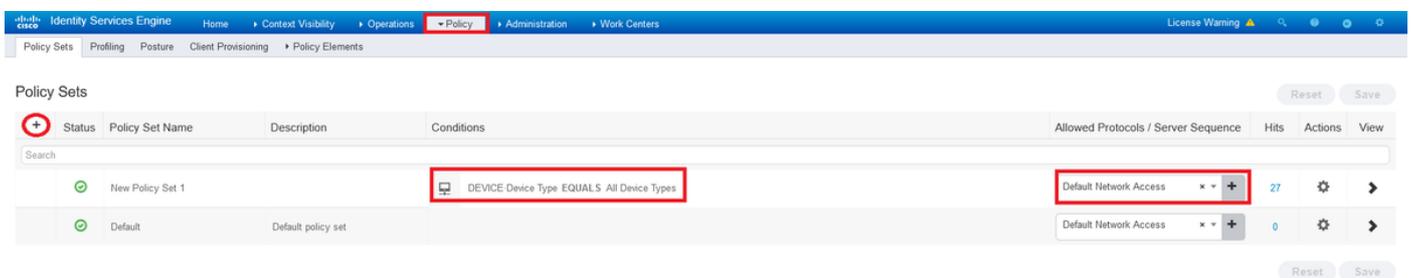
ステップ3 : ユーザをアイデンティティグループに関連付けます。

ユーザを適切なIDグループに関連付けます。[Administration] > [Identities] > [Users]に移動します。



ステップ4 : ポリシーセットの作成

条件の下で、例 (すべてのデバイスタイプ) に示すように新しいポリシーセットを定義します。[Policy] > [Policy sets]に移動します。



ステップ5 : 許可ポリシーを作成します。

IDグループに一致する適切な条件で新しい許可ポリシーを作成します。



+	Status	Rule Name	Conditions	Results		Hits	Actions
				Profiles	Security Groups		
Search							
✎	🟢	ISE_CLASS_ADMIN	AND DEVICE Device Type EQUALS All Device Types IdentityGroup Name EQUALS User Identity Groups:RADIUS_ANYCONNECT	Select from list +	Select from list +	7	⚙️
				Create a New Authorization Profile			
✎	🟢	ISE_CLASS_USER	AND DEVICE Device Type EQUALS All Device Types 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

▼ Advanced Attributes Settings

Radius:Class = RADIUS-ADMIN

▼ Attributes Details

Access Type = ACCESS\_ACCEPT  
Class = RADIUS-ADMIN

Save Cancel

This should be the Group-policy name

ステップ7：許可プロファイルの設定を確認します。

The screenshot displays the Cisco Identity Services Engine (ISE) configuration interface for an Authorization Profile. The left-hand navigation pane shows the 'Authorization Profiles' menu item selected. The main configuration area is titled 'Authorization Profile' and contains the following fields and options:

- \* Name:** CLASS\_25\_RADIUS\_ADMIN
- Description:** (empty text field)
- \* Access Type:** ACCESS\_ACCEPT
- Network Device Profile:** Cisco
- Service Template:**
- Track Movement:**
- Passive Identity Tracking:**

Below the main configuration area, there are sections for 'Common Tasks', 'Advanced Attributes Settings', and 'Attributes Details'. The 'Advanced Attributes Settings' section shows a configuration entry: 'Radius:Class = RADIUS-ADMIN'. The 'Attributes Details' section shows the resulting configuration: 'Access Type = ACCESS\_ACCEPT' and 'Class = RADIUS-ADMIN'. At the bottom of the page, there are 'Save' and 'Reset' buttons.

注：前の図に示されているように、設定に従います。Access\_Accept、Class—[25]、RADIUS-ADMINはグループポリシーの名前です（変更可能）。

次の図は、設定の外観を示しています。同じポリシーセットに許可ポリシーが存在し、それぞれが[conditions]セクションで必要なIDグループに一致し、[In the profile]セクションでASAに設定したグループポリシーを使用します。

The screenshot shows the Cisco ISE Policy Sets configuration interface. At the top, there are navigation tabs for Policy Sets, Profiling, Posture, Client Provisioning, and Policy Elements. The main content area is titled 'Policy Sets → New Policy Set 1'. It features a search bar and a table of policy sets. The table has columns for Status, Policy Set Name, Description, Conditions, Allowed Protocols / Server Sequence, and Hits. Below this, there are sections for Authentication Policy (1), Authorization Policy - Local Exceptions, Authorization Policy - Global Exceptions, and Authorization Policy (3). The Authorization Policy (3) section contains a detailed table of rules. The first rule is 'ISE\_CLASS\_ADMIN' with conditions 'DEVICE Device Type EQUALS All Device Types' and 'IdentityGroup Name EQUALS User Identity Groups RADIUS\_ANYCONNECT'. Its result is 'CLASS\_25\_RADIUS\_ADMIN'. The second rule is 'ISE\_CLASS\_USER' with conditions 'DEVICE Device Type EQUALS All Device Types' and 'IdentityGroup Name EQUALS User Identity Groups RADIUS\_ANYCONNECT\_USER'. Its result is 'CLASS\_25\_RADIUS\_USER'. The third rule is 'Default' with result 'DenyAccess'. Each rule has a 'Hits' column showing the number of hits (7, 9, and 8 respectively). At the bottom right, there are 'Reset' and 'Save' buttons.

この設定例では、class属性に基づくISE設定を介して、各Anyconnectユーザにグループポリシーを割り当てることができます。

## トラブルシューティング

最も便利なデバッグの1つがdebug radiusです。AAAプロセスとASAプロセス間のRADIUS認証要求および認証応答の詳細が表示されます。

```
debug radius
```

もう1つの便利なツールは、test aaa-serverコマンドです。これで、認証がACCEPTEDまたはREFUSEDで、属性(この例では「class」属性)が認証プロセスで交換されたかどうかを確認されます。

```
test aaa-server authentication
```

### 正常動作シナリオ

上記の設定例でuser1は、ISE設定に従ってRADIUS-ADMINグループポリシーに属していますが、test aaa-serverおよびdebug radiusを実行すれば確認できます。確認する必要がある行を強調表示します。

```
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 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:0alf7

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

| 1f7c52RqQGRp6Z5

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**

user1がAnyconnect経由で接続する際に機能するかどうかを確認するもう1つの方法として、**show vpn-sessiondb anyconnect**コマンドを使用して、ISEクラス属性によって割り当てられたグループポリシーを確認します。

```

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

```

## 動作しないシナリオ1

Anyconnectで認証が失敗し、ISEがREJECTで応答する場合。ユーザーがユーザーIDグループに関連付けられていることを確認する必要があるか、パスワードが正しくないことを確認する必要があります。[Operations] > [Live logs] > [Details]に移動します。

### 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**

Identity Services Engine

### 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

注：この例では、user1はユーザーIDグループに関連付けられていません。したがって、DenyAccessアクションを使用して、新しいポリシーセット1の下のDefault Authentication and Authorizationポリシーにヒットします。デフォルトの承認ポリシーでこのアクションをPermitAccessに変更し、ユーザーIDグループが関連付けられていないユーザーに認証を許可することができます。

## 動作しないシナリオ2

Anyconnectで認証が失敗し、デフォルトの認可ポリシーがPermitAccessの場合、認証が受け入れられません。ただし、class属性はRadius応答に表示されないため、ユーザはDfltGrpPolicyに配置され、vpn-simultaneous-logins 0が原因で接続に成功しませんでした。

**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 | Z5wqkx1P93BlJo.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

| viKZ5wqkx1P93BlJ

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#

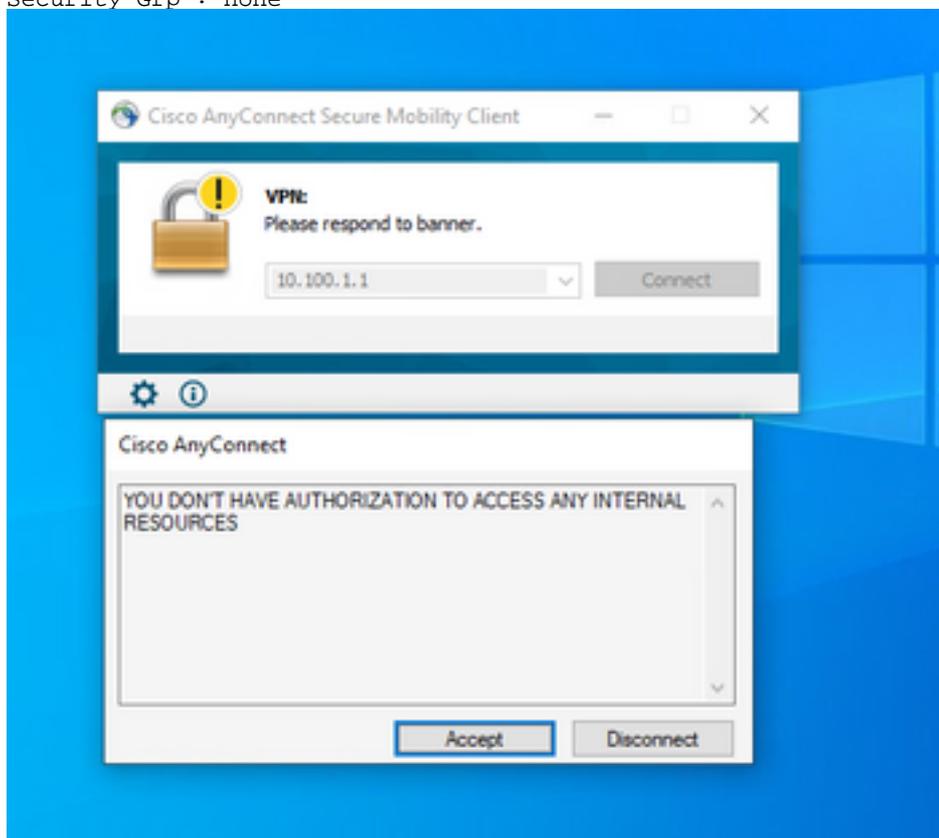
vpn-simultaneous-logins 0が'1'に変更された場合、出力に示すようにユーザが接続します。

```
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

```



### 動作しないシナリオ3

認証に合格しても、ユーザに適切なポリシーが適用されていない場合（たとえば、接続されたグループポリシーに必要な完全なトンネルではなくスプリットトンネルがある場合）。ユーザが誤ったユーザIDグループに属している可能性があります。

```
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

## ビデオ

このビデオでは、ISE認証とクラス属性を使用したSSL Anyconnectのグループポリシーマッピングの設定手順について説明します。