

# ISE 인증과 함께 SSL AnyConnect 구성 및 그룹 정책 매핑에 대한 클래스 특성

## 목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용된 구성 요소](#)

[구성](#)

[ASA](#)

[ISE](#)

[문제 해결](#)

[작업 시나리오](#)

[비작동 시나리오 1](#)

[비작동 시나리오 2](#)

[비작동 시나리오 3](#)

[비디오](#)

## 소개

이 문서에서는 특정 그룹 정책에 대한 사용자 매핑을 위해 Cisco ISE(Identity Services Engine)와 SSL(Secure Sockets Layer) Anyconnect를 구성하는 방법에 대해 설명합니다.

기고자: Amanda Nava, Cisco TAC 엔지니어

## 사전 요구 사항

### 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- AnyConnect Secure Mobility Client 버전 4.7
- Cisco ISE 2.4
- Cisco ASA 버전 9.8 이상

### 사용된 구성 요소

이 문서의 내용은 이러한 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- ASA(Adaptive Security Appliance) 5506(소프트웨어 버전 9.8.1)
- Microsoft Windows 10 64비트의 AnyConnect Secure Mobility Client 4.2.00096.
- ISE 버전 2.4.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스

이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

## 구성

이 예에서 AnyConnect 사용자는 Cisco ISE에서 특성에 따라 특정 그룹 정책에 할당할 때 드롭다운 메뉴에서 터널 그룹을 선택하는 옵션 없이 직접 연결합니다.

### ASA

#### AAA-서버

```
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
```

**참고:**이 컨피그레이션 예에서는 ISE 컨피그레이션을 통해 각 Anyconnect 사용자에게 그룹 정책을 할당할 수 있습니다.사용자는 터널 그룹을 선택할 수 있는 옵션이 없으므로 DefaultWEBVPNGroup 터널 그룹 및 DfltGrpPolicy에 연결됩니다.인증이 발생하고 Class 특성(Group-policy)이 ISE 인증 응답에서 반환되면 사용자는 해당 그룹에 할당됩니다.이 경우 사용자에게 Class 특성이 적용되지 않고 이 사용자는 DfltGrpPolicy에 남아 있습니다.그룹 정책이 없는 사용자가 VPN을 통해 연결하는 것을 방지하기 위해 DfltGrpPolicy 그룹에서 **vpn-simultaneous-logins 0**을 구성할 수 있습니다.

# ISE

1단계. ISE에 ASA를 추가합니다.

이 단계에서는 Administration(관리)>Network Resources(네트워크 리소스)>Network Devices(네트워크 디바이스)로 이동합니다.

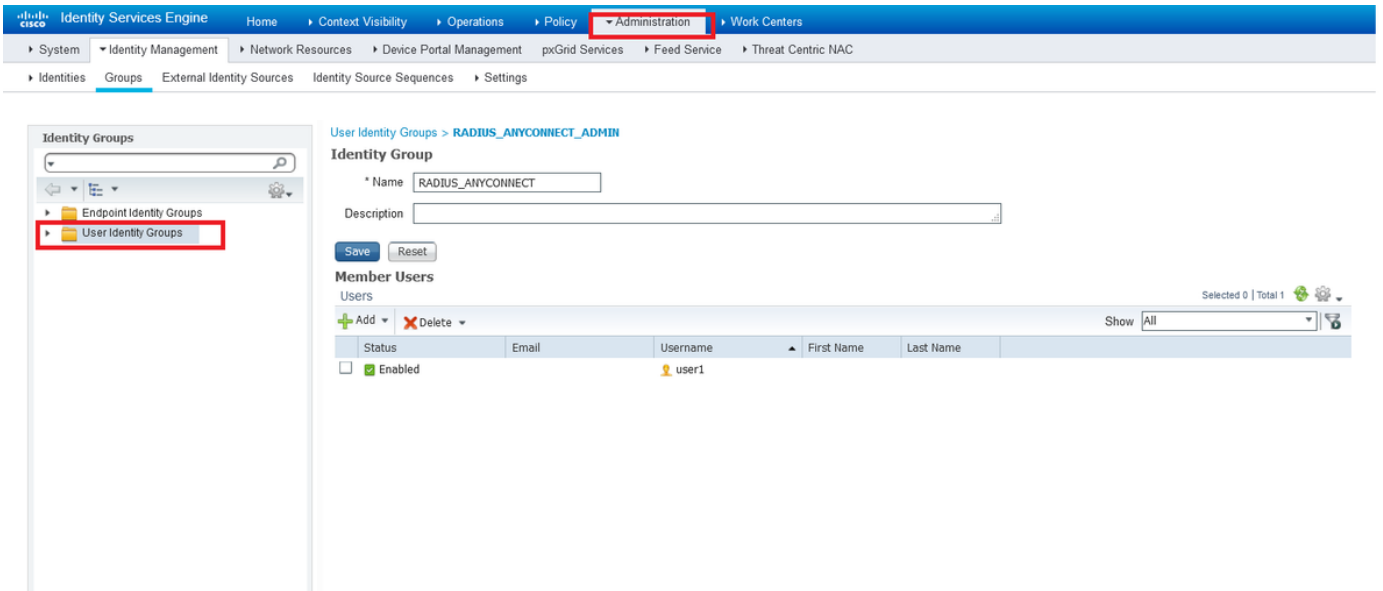
The screenshot displays the Cisco Identity Services Engine (ISE) Administration console. The navigation menu at the top includes Home, Context Visibility, Operations, Policy, Administration, and Work Centers. The main content area is titled "Network Devices List > ASAv" and "Network Devices".

Configuration fields include:

- \* Name: ASAv (indicated by a blue arrow)
- Description: (empty field)
- IP Address: 10.31.124.85 / 32 (indicated by a blue arrow)
- \* Device Profile: Cisco
- Model Name: ASAv
- Software Version: 9.9
- \* Network Device Group: Location (All Locations), IPSEC (No), Device Type (All Device Types)
- RADIUS Authentication Settings
  - RADIUS UDP Settings
    - Protocol: RADIUS (indicated by a blue arrow)
    - \* Shared Secret: cisco123 (Hide button)
    - Use Second Shared Secret:  (info icon)
    - CoA Port: 1700 (Set To Default button)
  - RADIUS DTLS Settings (info icon)

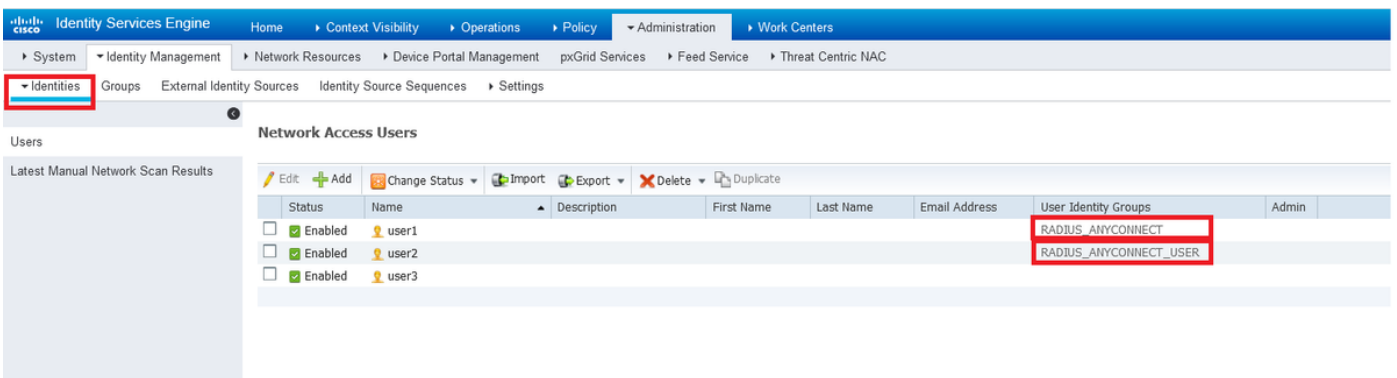
2단계. ID 그룹을 생성합니다.

각 사용자를 다음 단계의 오른쪽 그룹에 연결할 ID 그룹을 정의합니다.관리>그룹>사용자 ID 그룹으로 이동합니다.



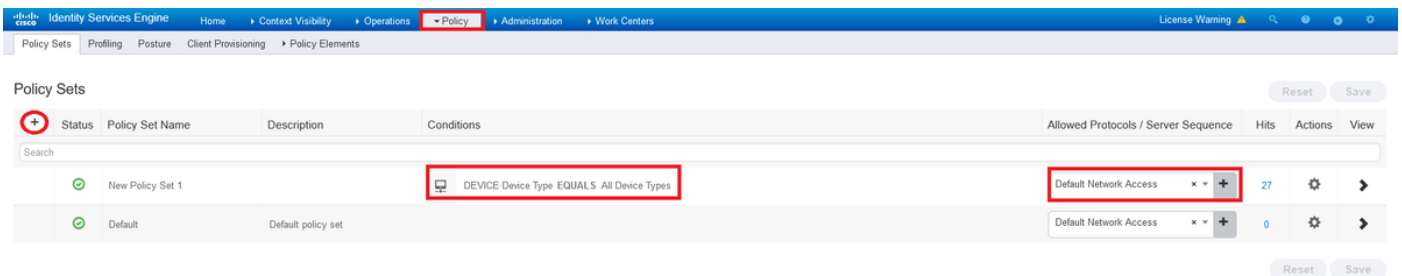
3단계. 사용자를 ID 그룹에 연결합니다.

사용자를 올바른 ID 그룹에 연결합니다.Administration(관리)>Identities(ID)>Users(사용자)로 이동합니다.



4단계. 정책 세트를 생성합니다.

조건에서 예(모든 디바이스 유형)와 같이 새 정책 세트를 정의합니다.Policy(정책) >Policy sets(정책 세트)로 이동합니다.



5단계. 권한 부여 정책을 생성합니다.

ID 그룹과 매칭할 적절한 조건을 가진 새 권한 부여 정책을 만듭니다.



+	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:  (i)

Passive Identity Tracking:  (i)

---

▶ 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

7단계. 권한 부여 프로파일 컨피그레이션을 검토합니다.

The screenshot displays the Cisco Identity Services Engine (ISE) configuration interface for an Authorization Profile. The breadcrumb navigation at the top includes: Home > Context Visibility > Operations > Policy > Administration > Work Centers. The left sidebar shows the navigation menu with 'Authorization Profiles' highlighted. The main content area is titled 'Authorization Profile' and contains the following configuration details:

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

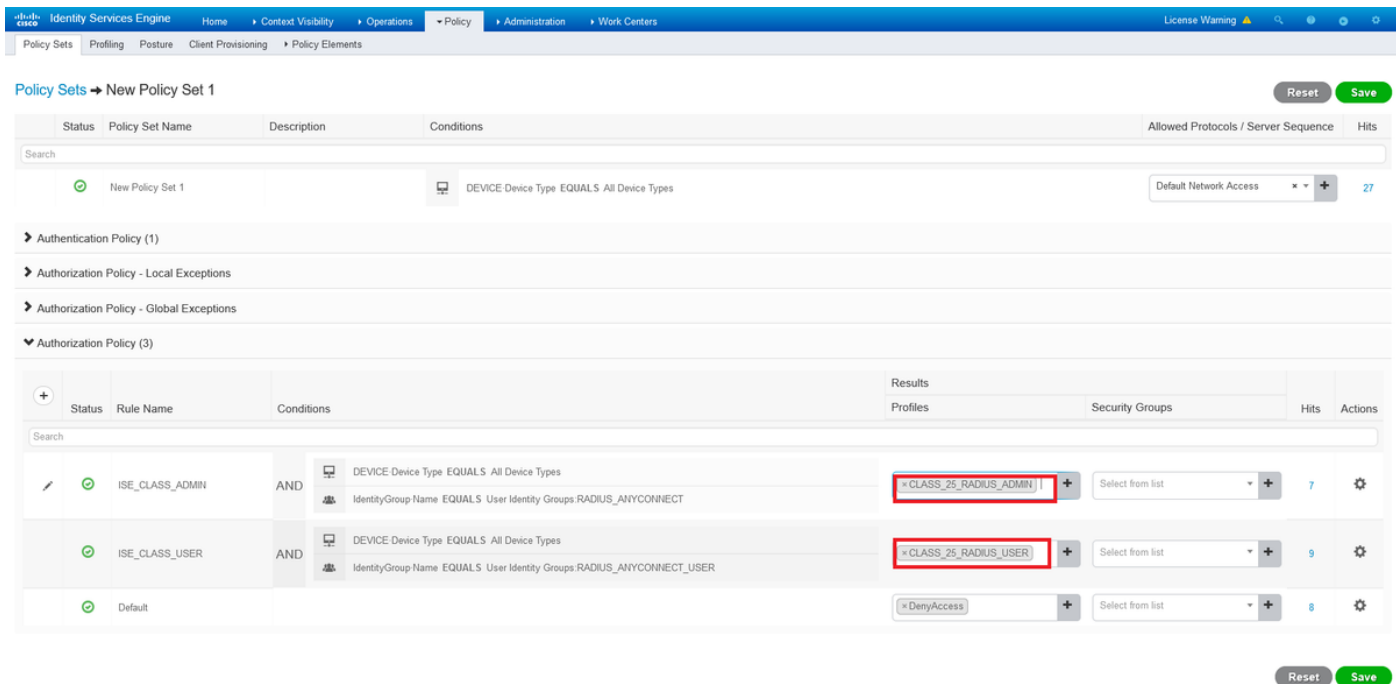
Below the configuration fields, there are sections for 'Common Tasks', 'Advanced Attributes Settings', and 'Attributes Details':

- Advanced Attributes Settings:** Shows a configuration entry for 'Radius:Class' set to 'RADIUS-ADMIN'.
- Attributes Details:** Shows the summary: 'Access Type = ACCESS\_ACCEPT' and 'Class = RADIUS-ADMIN'.

At the bottom of the configuration area, there are 'Save' and 'Reset' buttons.

**참고:**이전 이미지 Access\_Accept, Class—[25]에 표시된 대로 컨피그레이션을 수행합니다. RADIUS-ADMIN은 그룹 정책의 이름입니다(변경할 수 있음).

이 그림에서는 컨피그레이션의 모양을 보여 줍니다. 동일한 정책 집합에서 권한 부여 정책이 없으며, 각 정책은 **조건** 섹션에 필요한 ID 그룹과 일치하고 **프로필** 섹션의 ASA에 있는 그룹 정책을 사용합니다.



이 컨피그레이션 예에서는 클래스 특성을 기반으로 ISE 컨피그레이션을 통해 각 Anyconnect 사용자에게 그룹 정책을 할당할 수 있습니다.

## 문제 해결

가장 유용한 디버깅 중 하나는 디버그 반지름입니다. AAA와 ASA 프로세스 간의 RADIUS 인증 요청 및 인증 응답에 대한 세부 정보를 표시합니다.

```
debug radius
```

또 다른 유용한 툴은 명령 `test aaa-server`입니다. 이제 인증이 ACCEPTED 또는 REFUSED인지, 그리고 인증 프로세스에서 교환되는 특성('class' 특성)을 확인합니다.

```
test aaa-server authentication
```

## 작업 시나리오

위에서 언급한 컨피그레이션 예에서 **user1**은 ISE 컨피그레이션에 따라 RADIUS-ADMIN 그룹 정책에 속하며 테스트 `aaa-server`를 실행하고 디버그 반지름을 실행하는지 확인할 수 있습니다. 확인해야 할 라인을 강조 표시합니다.

```
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: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**

user1이 Anyconnect를 통해 연결할 때 작동하는지 확인하는 또 다른 방법은 **show vpn-sessiondb anyconnect** 명령을 사용하여 ISE 클래스 특성에 의해 할당된 그룹 정책을 확인합니다.

```

ASA# 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

```

## 비작동 시나리오 1

AnyConnect에서 인증이 실패하고 ISE가 REJECT로 응답하는 경우.사용자가 사용자 ID 그룹과 연결되었는지 또는 암호가 잘못되었는지 확인해야 합니다. Operations(작업) >Live logs(라이브 로그) > Details(세부 정보)로 이동합니다.

**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

**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

**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

**참고:**이 예에서 user1은 사용자 ID 그룹과 연결되지 않습니다.따라서 DenyAccess 작업을 사용하여 New Policy Set 1(새 정책 집합 1) 아래의 Default Authentication and Authorization(기본 인증 및 권한 부여) 정책에 도달합니다.이 작업을 Default Authorization Policy(기본 권한 부여 정책)에서 PermitAccess(허용 액세스)로 수정하여 User ID 그룹이 연결되지 않은 사용자를 허용할 수 있습니다.

**비작동 시나리오 2**

AnyConnect에서 인증이 실패하고 기본 권한 부여 정책이 PermitAccess인 경우 인증이 수락됩니다.그러나 클래스 특성은 Radius 응답에 표시되지 않으므로 사용자가 DfltGrpPolicy에 있으며 vpn-simultaneous-logins 0으로 인해 연결되지 않습니다.

**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 | 1P93BlJo: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 | 1P93BlJo: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

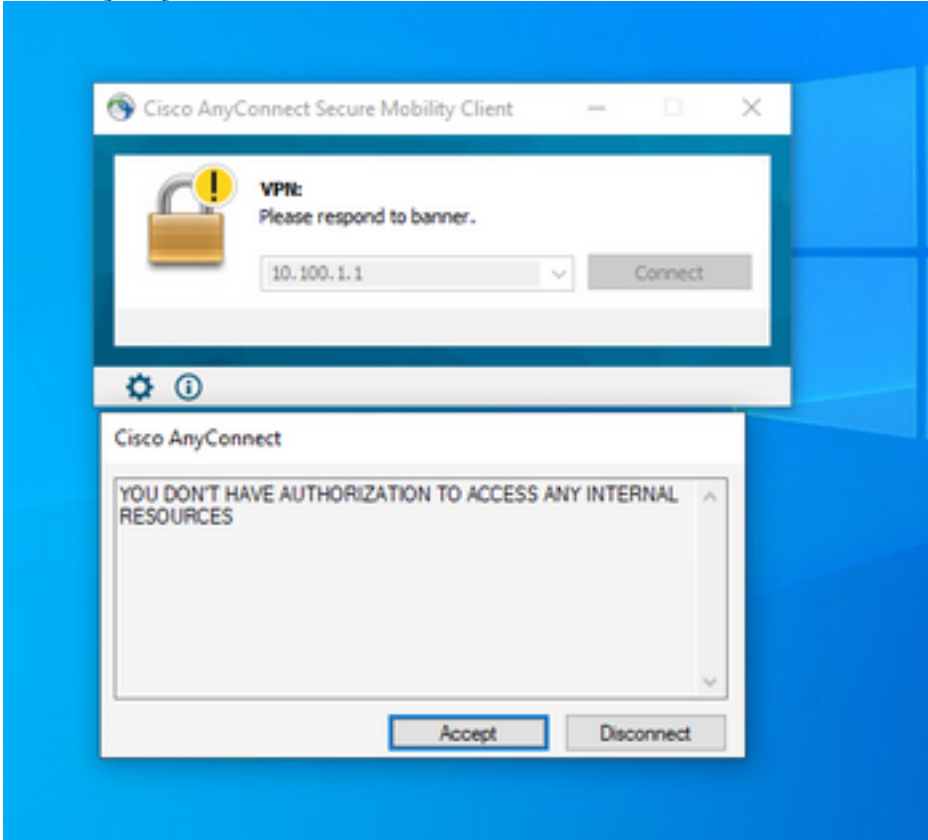
**INFO: Authentication Successful**

ASAv#

**vpn-simultaneous-logins 0이 '1'로 변경되면 사용자는 출력에 표시된 대로 연결됩니다.**

```
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



### 비작동 시나리오 3

인증이 통과되었지만 사용자에게 올바른 정책이 적용되지 않은 경우(예: 연결된 그룹 정책이 전체 터널 대신 스플릿 터널이 있어야 하는 경우)사용자가 잘못된 사용자 ID 그룹에 있을 수 있습니다.

```
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
  
```

### 비디오

이 비디오에서는 ISE 인증과 함께 SSL AnyConnect를 구성하는 단계 및 그룹 정책 매핑에 대한 클래스 특성을 제공합니다.