ISEでのRADIUS認証とグループポリシーマッピングを使用したリモートアクセスVPNの設定

内容

はじめに

このドキュメントでは、Cisco Identity Services Engine(ISE)とのグループポリシーマッピング用のリモートアクセスVPN(RVPN)の設定について説明します。

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。

- Cisco Secure Client(AnyConnect)
- Cisco ISE
- Cisco適応型セキュリティアプライアンス(ASA)でのリモートアクセスVPN

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 ASA 5506
- AnyConnect バージョン 4.8

- 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、クリアな（デフォルト）設定で作業を開始しています。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

この設定例では、Cisco Secure Client(AnyConnect)を使用してVPN経由でASAに接続するリモートユーザは、ドロップダウンメニューから接続プロファイル(tunnel-group)を選択できません。Cisco ISEは、設定されたポリシーに基づいて接続プロファイルを特定のグループポリシーにマッピングするためです。

この設定では、ISE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。ユーザはトンネルグループを選択するオプションがないため、最初にDefaultWEBVPNGroup tunnel-groupおよびDfltGrpPolicyグループポリシーに接続されます。認証後、RADIUSクラス属性（グループポリシー）が認証応答内でISEから送信される場合、ユーザは対応するグループポリシーに割り当てられ、それによって適切な権限が付与されます。ISEがクラス属性を返さない場合、またはASAで設定されていないグループラベルを返す場合、ユーザはDfltGrpPolicyに割り当てられたままになります。グループポリシーが割り当てられていないユーザがVPN経由で接続するのを防ぐには、DfltGrpPolicyグループポリシーの下でvpn-simultaneous-logins 0コマンドを設定します。

コンフィギュレーション

ASA

aaa-server

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

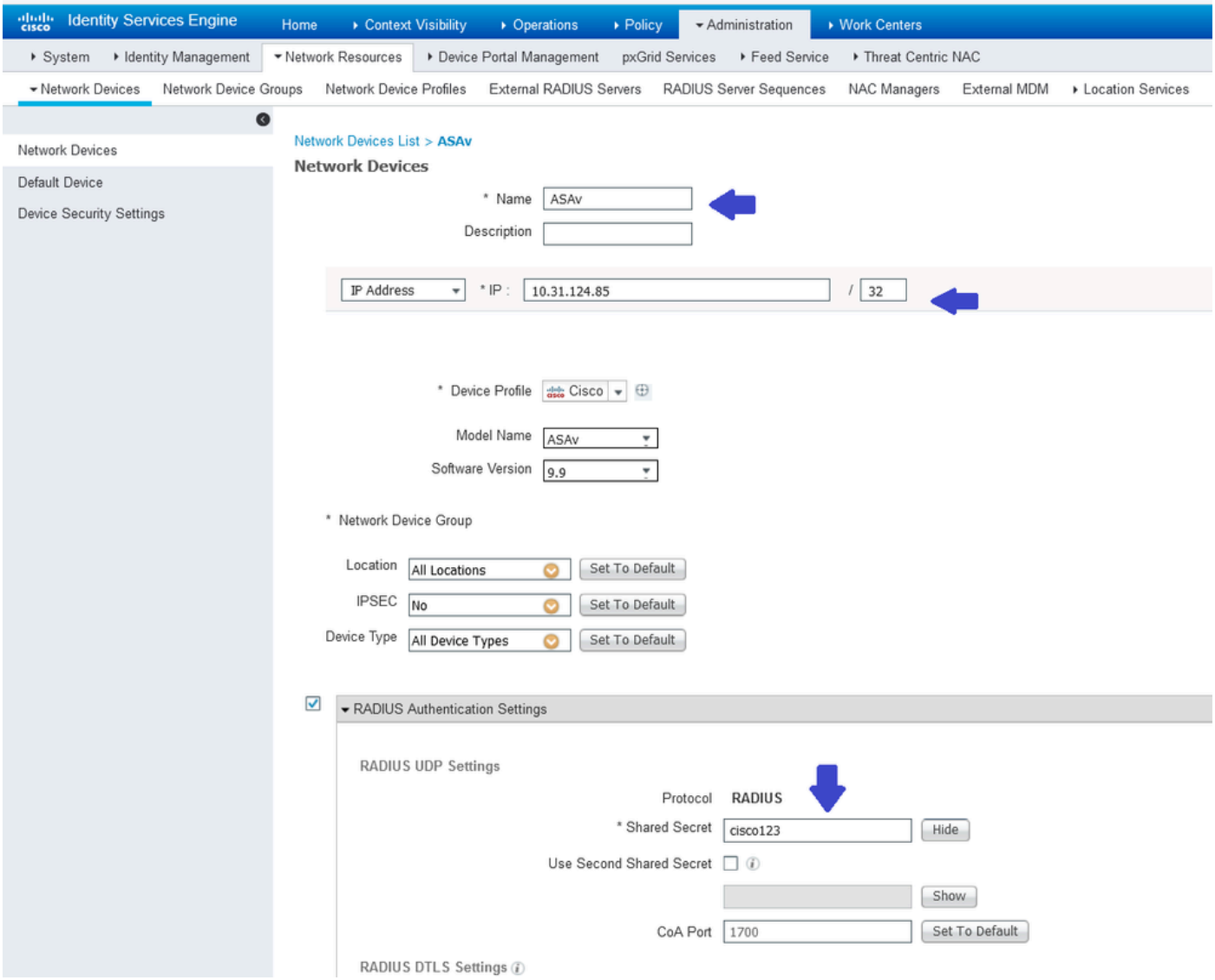
リモートアクセスVPNの設定

```
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
```

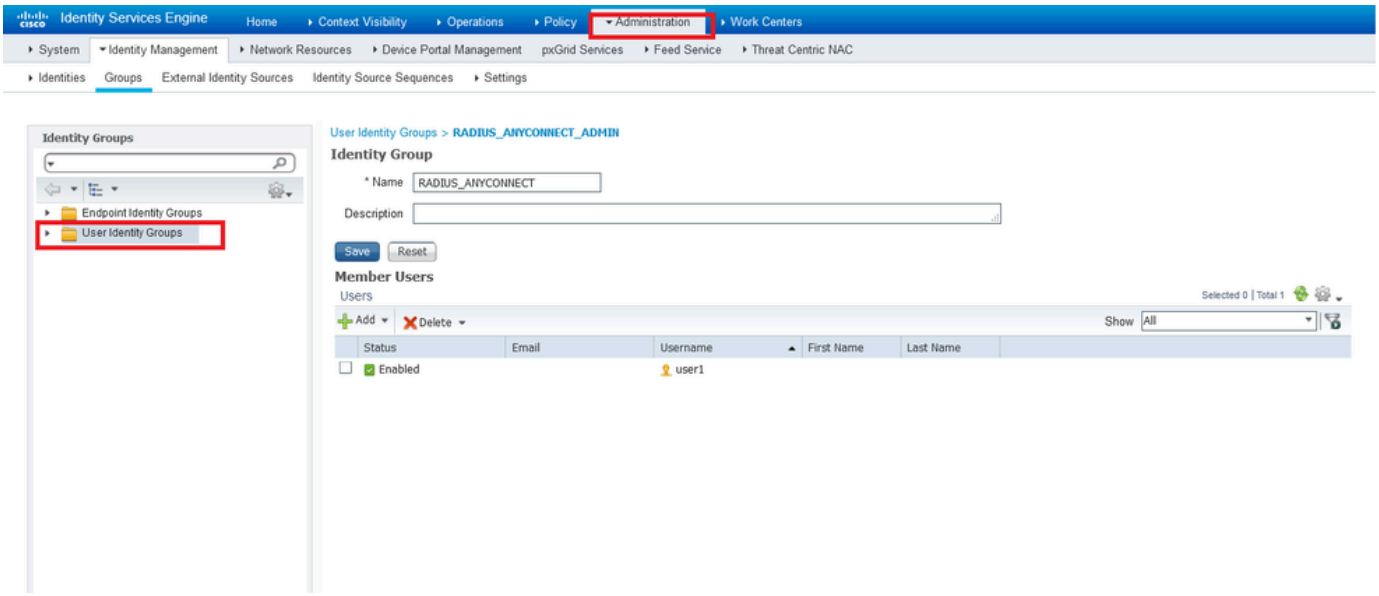
ISE

手順 1：ASAをISE上の有効なネットワークデバイスとして登録し、RADIUSの共有秘密キーを設定します。このためには、Administration > Network Resources > Network Devicesの順に選択します。



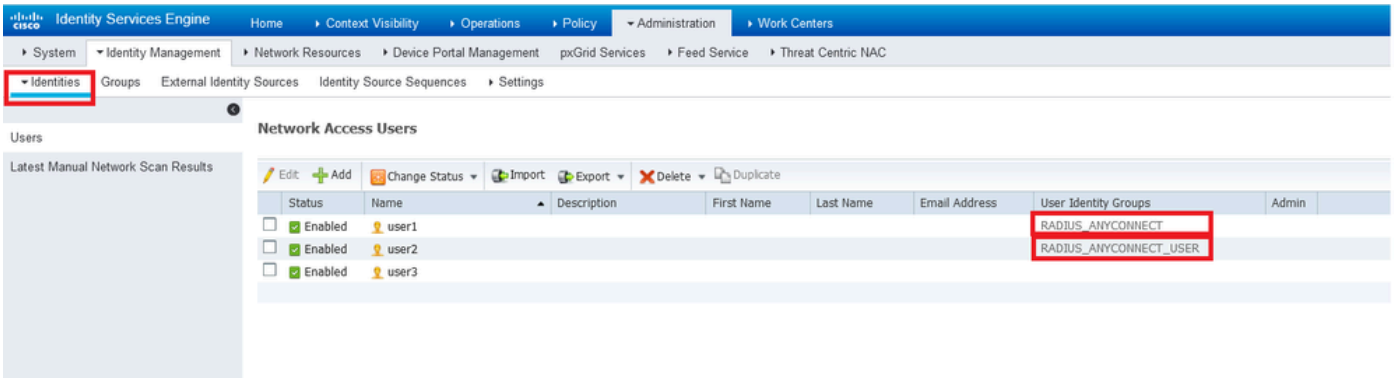
ステップ 2：IDグループを作成します。

IDグループを定義して、同様の特性を持つユーザと同様の権限を共有するユーザを関連付けます。これらは次の手順で使用します。Administration > Groups > User Identity Groupsの順に移動します。



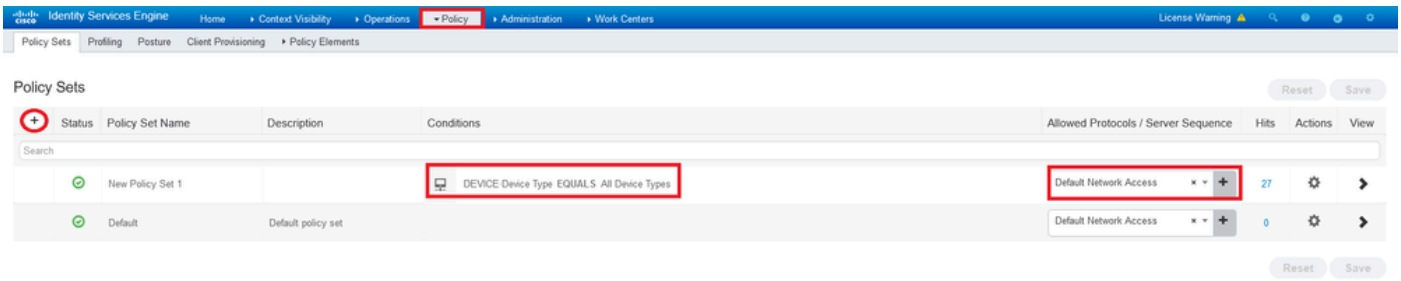
ステップ 3：ユーザをIDグループに関連付けます。

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



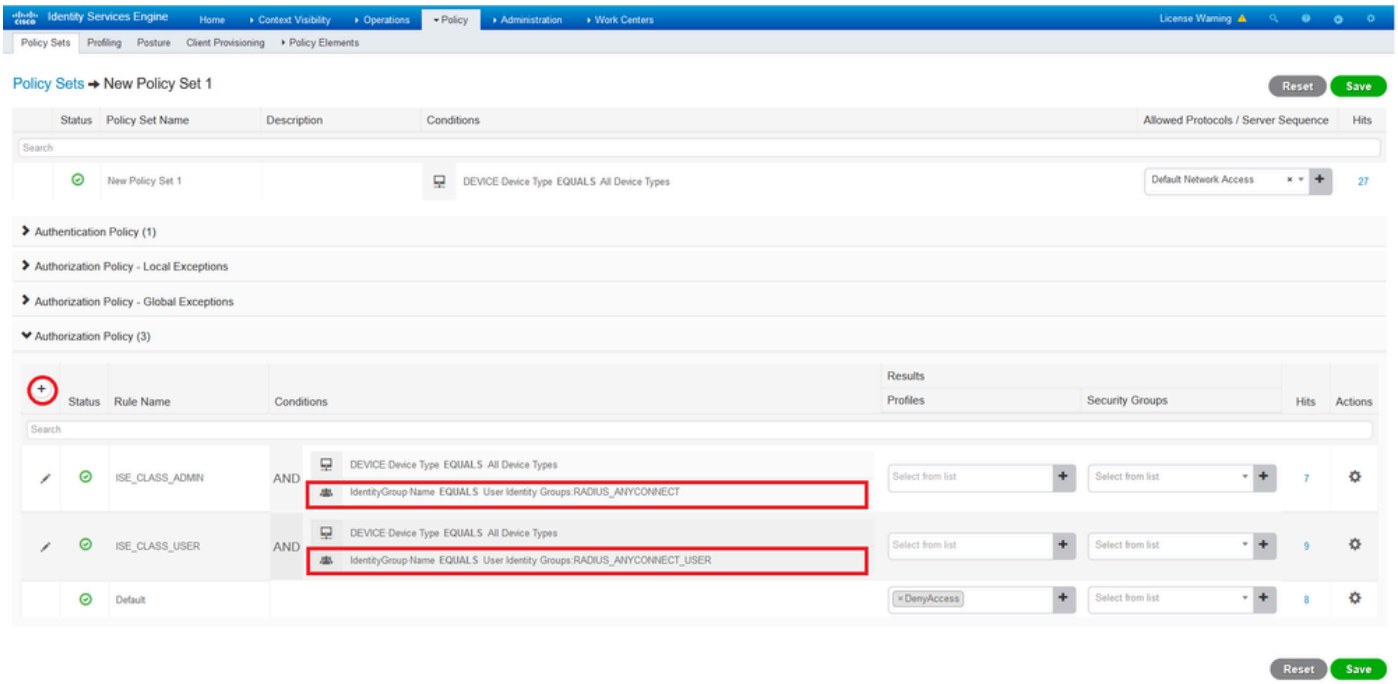
ステップ 4：ポリシーセットを作成します。

新しいポリシーセットを定義し、ポリシーに一致する条件を定義します。この例では、条件の下ですべてのデバイスタイプが許可されます。それには、Policy > Policy setsの順に移動します。



ステップ 5：認可ポリシーの作成.

ポリシーに一致するために必要な条件を使用して、新しい認可ポリシーを定義します。ステップ2で作成したIDグループを条件として含めてください。

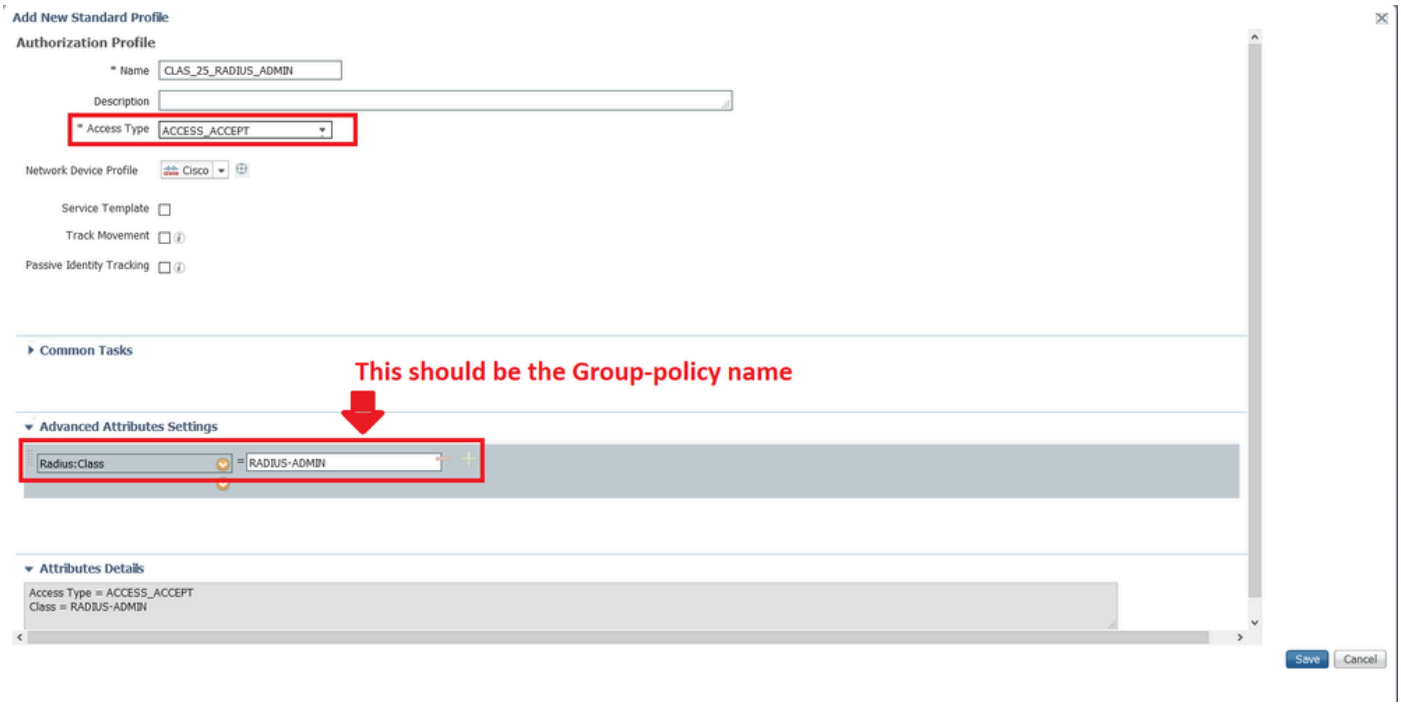


手順 6：許可プロファイルを作成します。

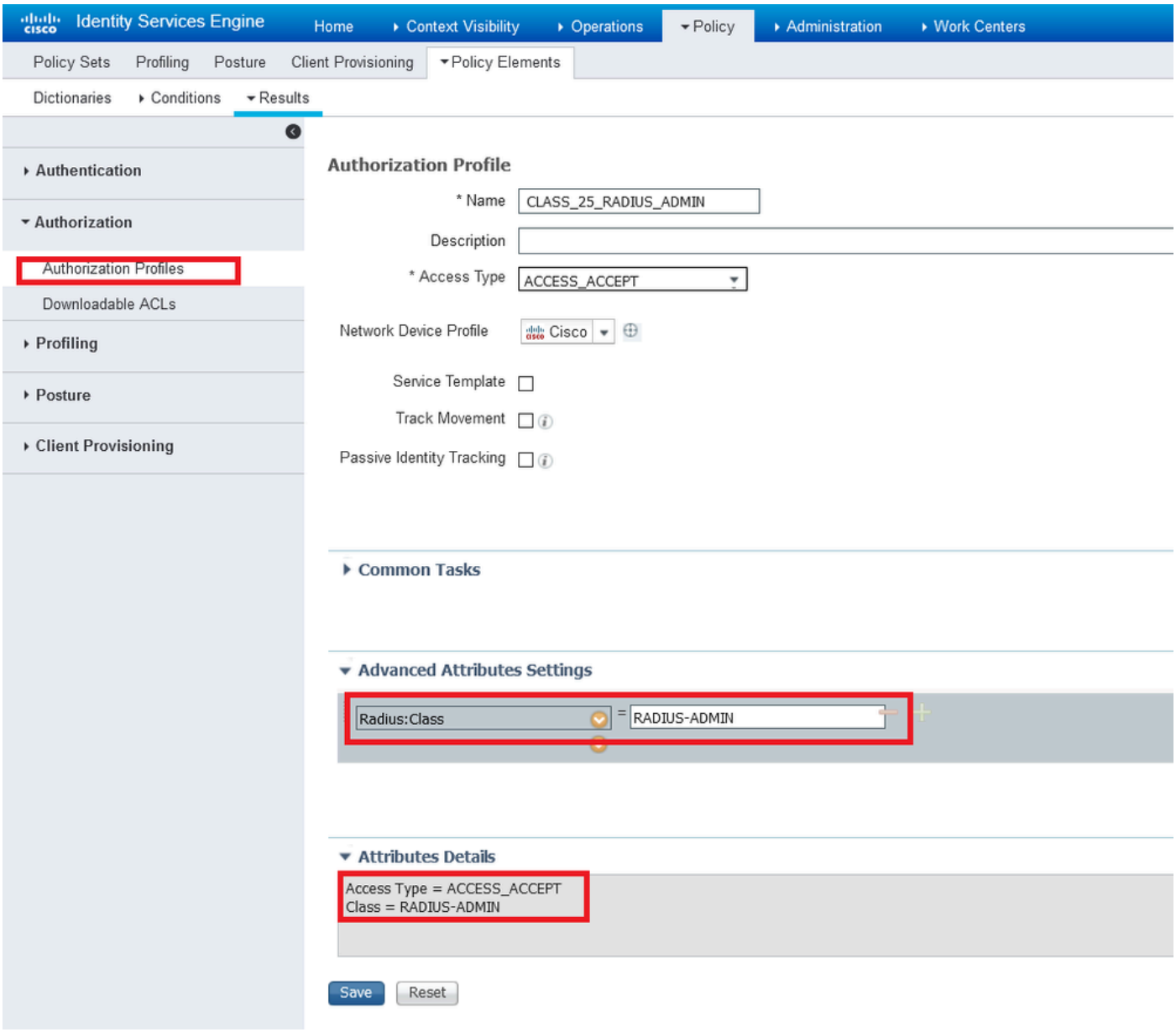
認可プロファイルには、認可ポリシーが一致した場合に実行されるアクションが含まれます。次の属性を含む新しい認可プロファイルを作成します。

- RADIUSクラス= <グループポリシーASA>
- アクセスタイプ： ACCESS_ACCEPT。

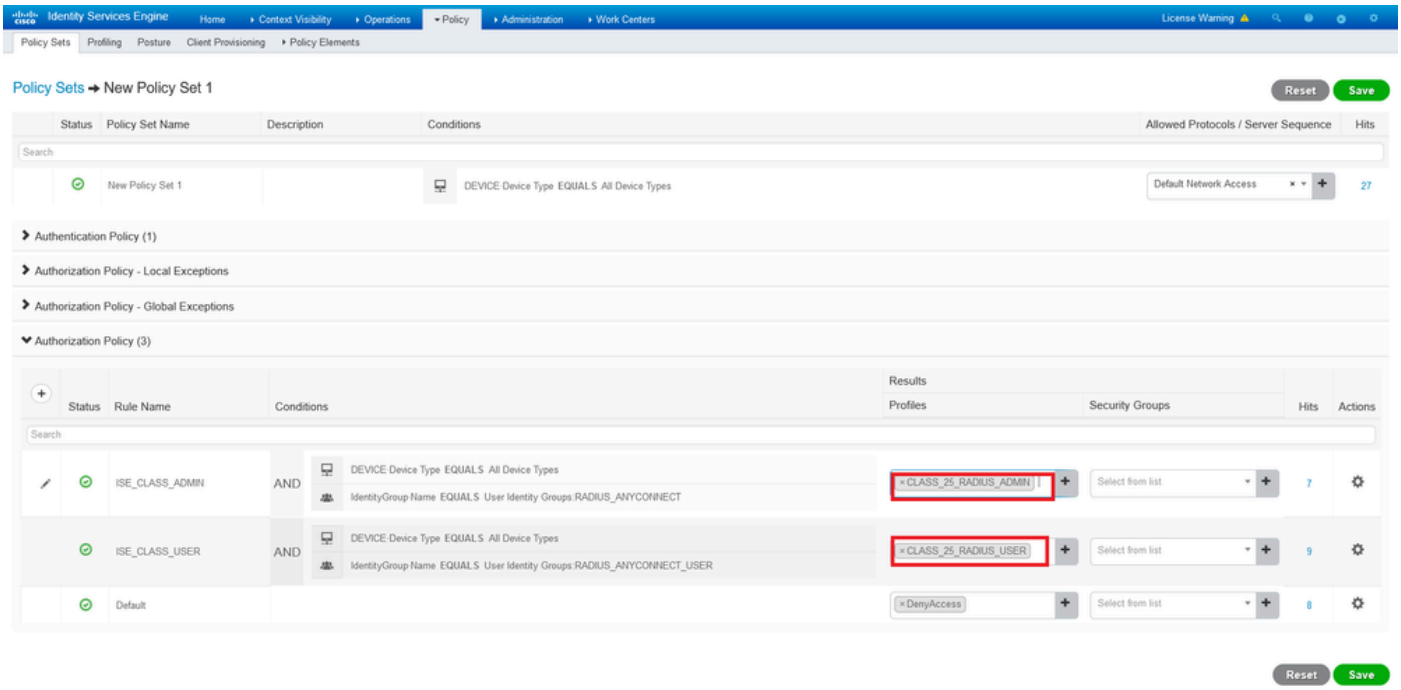
注：前の図に表示された設定を編集して、ASA設定で定義したグループポリシーの名前と一致させる必要があります。



手順 7：認可プロファイルの設定を確認します。



注：同じポリシーセット内に、各IDグループをASAで定義された特定のグループポリシーにマッピングするn個の許可ポリシーを設定できます。



この設定例では、ユーザが属するIDグループに基づいて、ISE設定を介して各セキュアクライアントユーザにグループポリシーを動的に割り当てることができます。

確認

最も役立つデバッグの1つは、debug radiusです。AAAサーバ(ISE)とASAの間の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。認証がACCEPTEDかREFUSEDか、および認証プロセスで交換された属性（この例では「class」属性）が表示されます。

```
test aaa-server authentication

        [host

        |

         ] username

           password
```

正常動作シナリオ

前述の設定例では、user1はISE設定ごとにRADIUS-ADMINグループポリシーに属しています。これは、test aaa-serverを実行して、ASAでradiusデバッグを有効にすると確認できます。デバッグからの関連する行は太字で示されています。

<#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

show vpn-sessiondb anyconnectコマンドを使用して、Secure Client経由で接続したときにISEによってuser1に正しいグループポリシーが割り当てられているかどうかを確認する方法もあります。

<#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
```

トラブルシュート

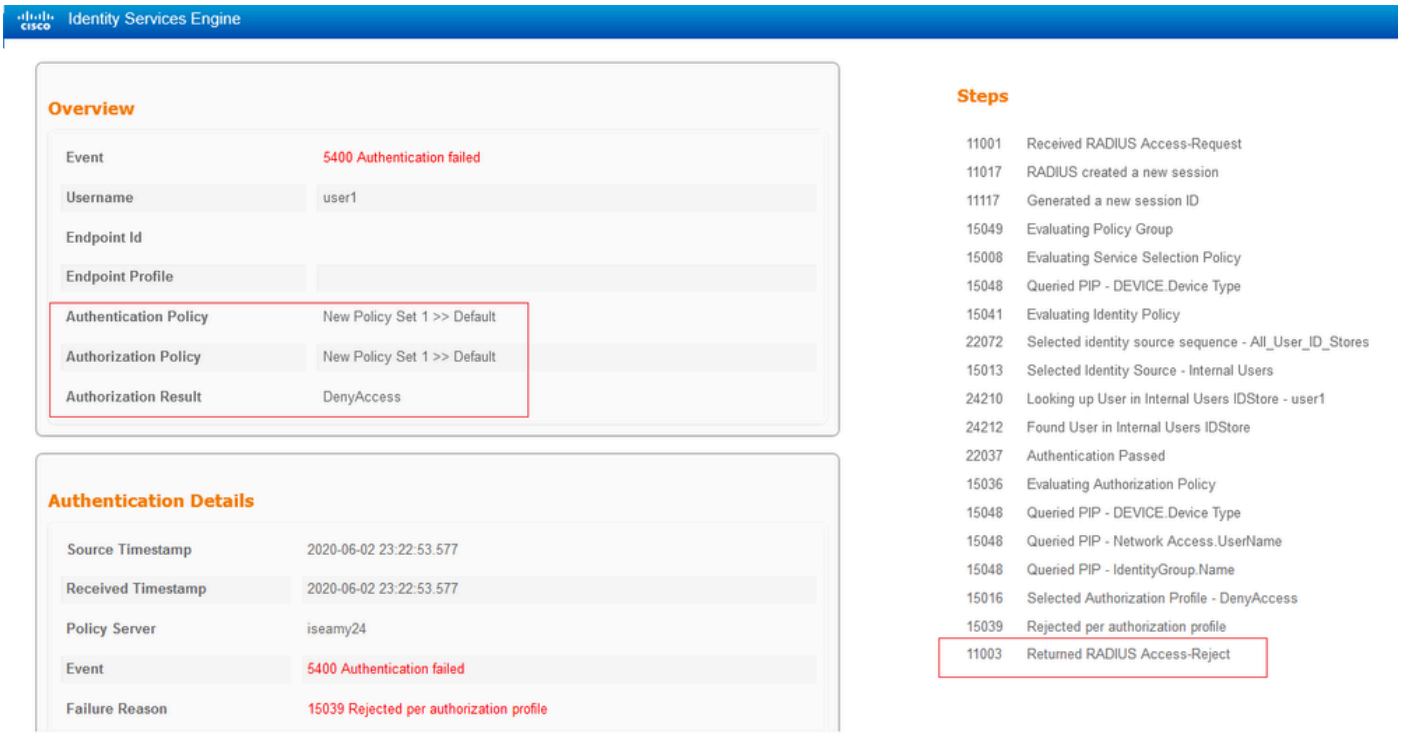
また、debug radiusコマンドとtest aaa-serverコマンドを使用して、問題が発生した場合のトラブルシューティングを行うこともできます。最も一般的な問題については、次で説明します。

正常に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。ユーザがユーザIDグループに関連付けられているか、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の順に移動します。

<#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
```



注：この例では、user1はユーザIDグループに関連付けられていません。したがって、DenyAccessアクションを含む新しいポリシーセット1の下のデフォルトの認証ポリシーと認可ポリシーにヒットします。このアクションを変更して、デフォルトの認可ポリシー内のPermitAccesに設定し、認証に関連付けられたユーザIDグループを持たないユーザを許可できます。

非稼働シナリオ2

Anyconnectで認証が失敗し、デフォルトの許可ポリシーがPermitAccessの場合、認証は受け入れられます。ただし、class属性はRadius応答には表示されないため、ユーザはDfltGrpPolicyに配置されており、設定されたコマンドvpn-simultaneous-logins 0が原因で接続しません。

<#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#
```

vpn-simultaneous-logins 0が「1」に変更された場合、ユーザは次の出力に示すように接続します。

<#root>

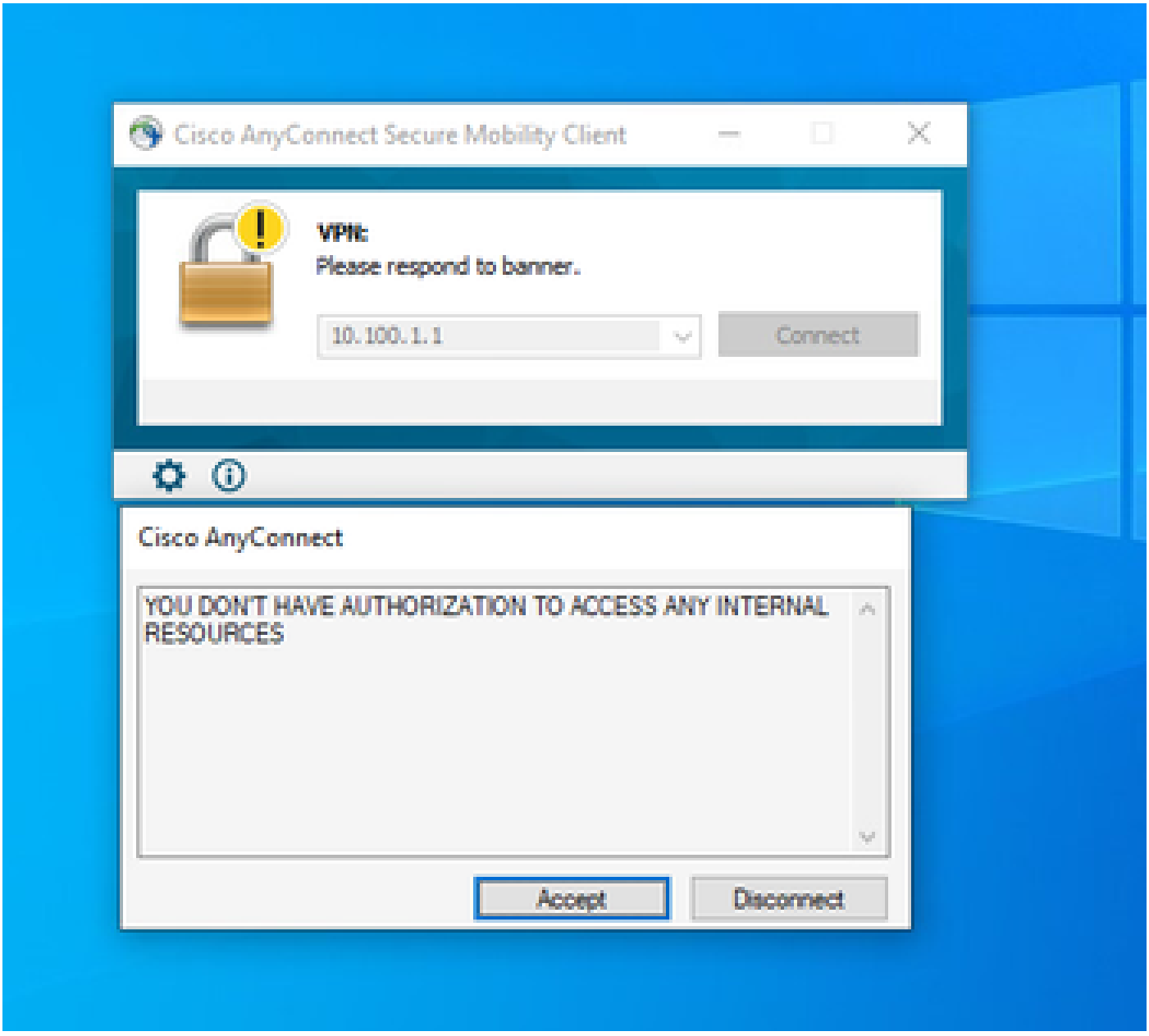
```
ASAv# show vpn-sessiondb anyconnect

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
```



非稼働シナリオ3

認証に成功してもユーザに適切なポリシーが適用されない場合、たとえば、接続されているグループポリシーに、必要に応じてフルトンネルではなくスプリットトンネルが設定されている場合です。ユーザが間違ったユーザIDグループに属している可能性があります。

<#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
```

ビデオ

このビデオでは、ISE認証とグループポリシーマッピング用のクラス属性を使用してSSL Anyconnectを設定する手順について説明します。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。