

为组策略映射配置SSL AnyConnect的ISE身份验证和类属性

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[ASA](#)

[ISE](#)

[故障排除](#)

[工作场景](#)

[非工作场景1](#)

[非工作场景2](#)

[非工作场景3](#)

[视频](#)

简介

本文档介绍如何配置安全套接字层(SSL)Anyconnect与思科身份服务引擎(ISE)，以使用户映射到特定组策略。

作者：思科TAC工程师Amanda Nava。

先决条件

要求

Cisco 建议您了解以下主题：

- AnyConnect安全移动客户端版本4.7
- 思科ISE 2.4
- Cisco ASA 9.8版或更高版本。

使用的组件

本文档的内容基于这些软件和硬件版本。

- 自适应安全设备(ASA)5506，软件版本9.8.1
- Microsoft Windows 10 64位版上的AnyConnect安全移动客户端4.2.00096。
- ISE版本2.4。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原

始 (默认) 配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

在示例中，Anyconnect用户直接连接，而不具有从下拉菜单中选择隧道组的选项，因为Cisco ISE根据其属性将他们分配到特定组策略。

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
```

注意：通过此配置示例，您可以通过ISE配置将组策略分配给每个Anyconnect用户。由于用户没有选择隧道组的选项，因此他们连接到DefaultWEBVPNGroup隧道组和DfltGrpPolicy。在进行身份验证并在ISE身份验证响应中返回Class属性(Group-policy)后，用户将分配到相应的组。在这种情况下，用户未应用Class属性，此用户仍保留在DfltGrpPolicy中。您可以在DfltGrpPolicy组下配置vpn-simulatenous-logins 0，以避免没有组策略的用户通过VPN连接。

ISE

步骤1.将ASA添加到ISE。

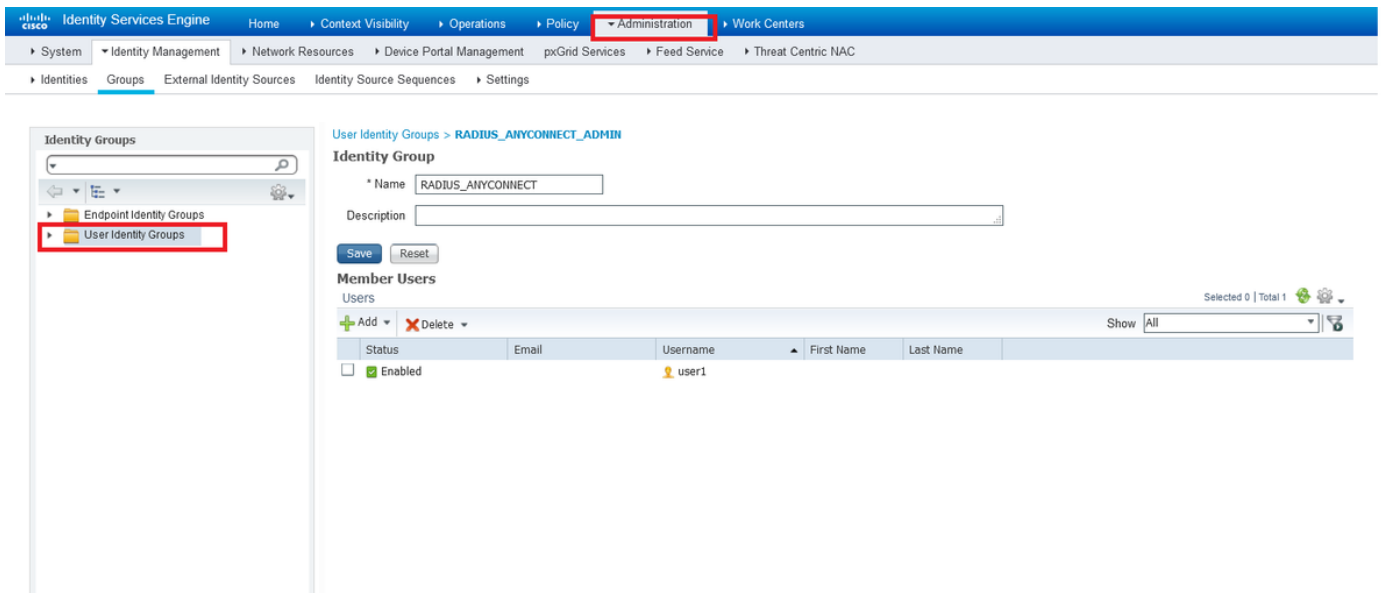
对于此步骤，请导航至Administration>Network Resources>Network Devices。

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 left sidebar shows 'Network Devices', 'Default Device', and 'Device Security Settings'. The main content area is titled 'Network Devices List > ASAv' and contains the following configuration sections:

- Name:** ASAv
- Description:** (empty)
- IP Address:** 10.31.124.85 / 32
- 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:**
 - Protocol: RADIUS
 - Shared Secret: cisco123
 - Use Second Shared Secret: (unchecked)
 - CoA Port: 1700

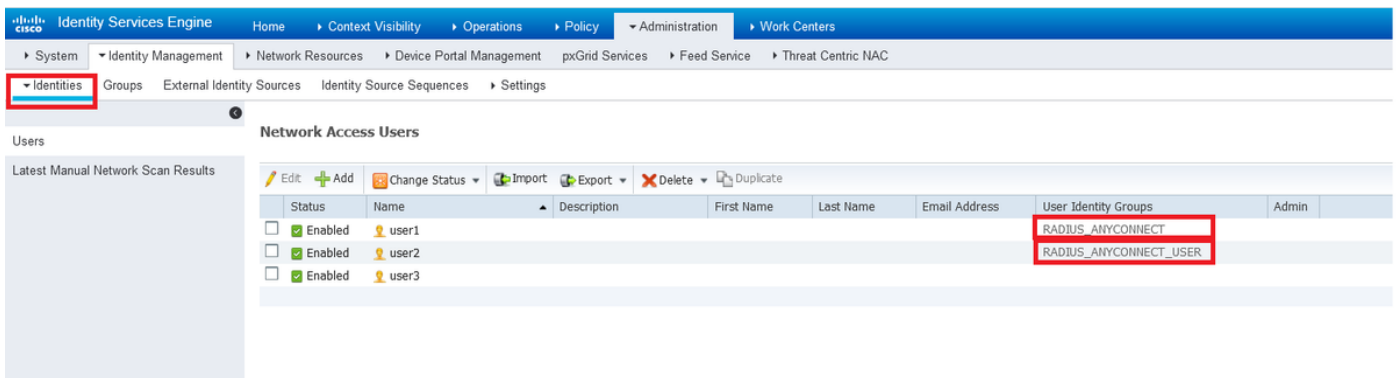
步骤2.创建身份组。

在后续步骤中，定义身份组，将每个用户关联到正确的用户。导航至Administration>Groups>User Identity Groups。



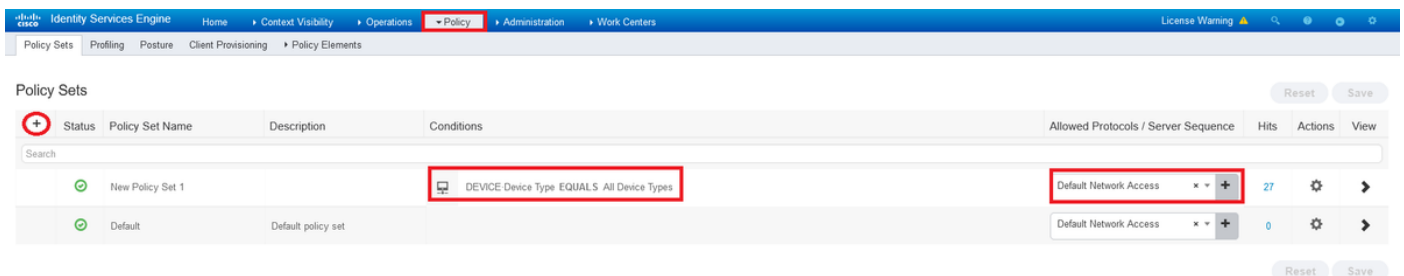
步骤3.将用户关联到身份组。

将用户关联到正确的身份组。导航至管理>身份>用户。



步骤4.创建策略集。

定义新策略集，如示例所示（所有设备类型）。导航至策略>策略集。



步骤5.创建授权策略。

创建具有适当条件的新授权策略以匹配身份组。

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers License Warning

Policy Sets Profiling Posture Client Provisioning Policy Elements

Policy Sets → New Policy Set 1 Reset Save

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 👤 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 👤 IdentityGroup Name EQUALS User Identity Groups:RADIUS_ANYCONNECT_USER	Select from list	Select from list	9	⚙️
🟢	Default			DenyAccess	Select from list	8	⚙️

Conditions Studio Reset Save ? ×

Library

Search by Name

BYOD_is_Registered ⓘ
 Catalyst_Switch_Local_Web_Authenticati on ⓘ
 Compliance_Unknown_Devices ⓘ
 Compliant_Devices ⓘ
 EAP-MSCHAPV2 ⓘ
 EAP-TLS ⓘ
 Guest_Flow ⓘ
 MAC_in_SAN ⓘ
 Network_Access_Authentication_Passed ⓘ
 Non_Cisco_Profiling_Phones ⓘ
 Non_Compliant_Devices ⓘ
 Switch_Local_Web_Authentication ⓘ

Editor

AND

🖨️ DEVICE Device Type
 Equals All Device Types

👤 IdentityGroup Name
 Equals * User Identity Groups:RADIUS_ANYCONNECT

+ New AND OR

Set to 'Is not' Duplicate Save

Close Use

步骤6. 创建授权配置文件。

使用RADIUS创建新授权配置文件：类<Group-policy-ASA>属性和*访问类型：ACCESS_ACCEPT。

+	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

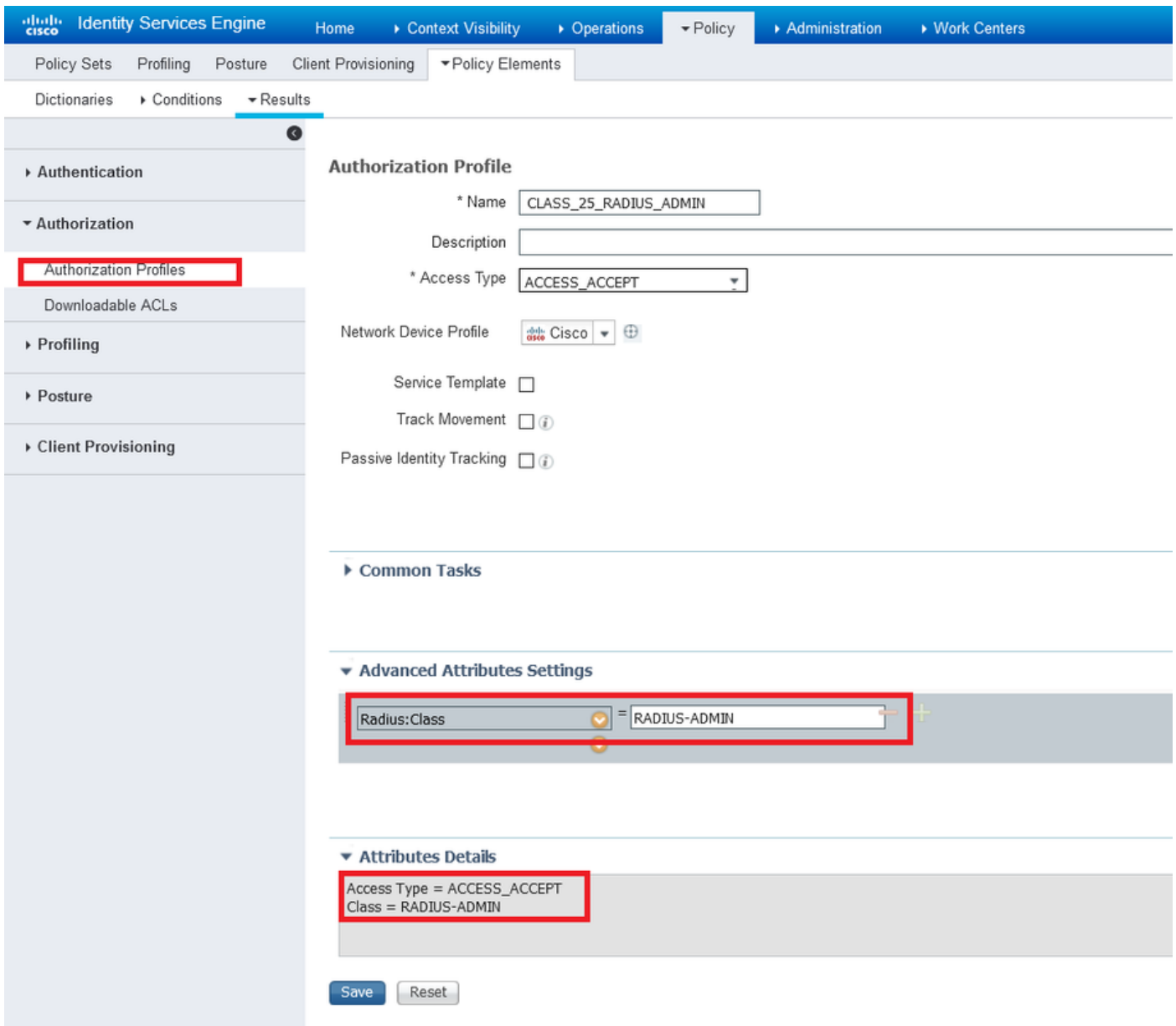
Attributes Details

Access Type = ACCESS_ACCEPT
Class = RADIUS-ADMIN

Save Cancel

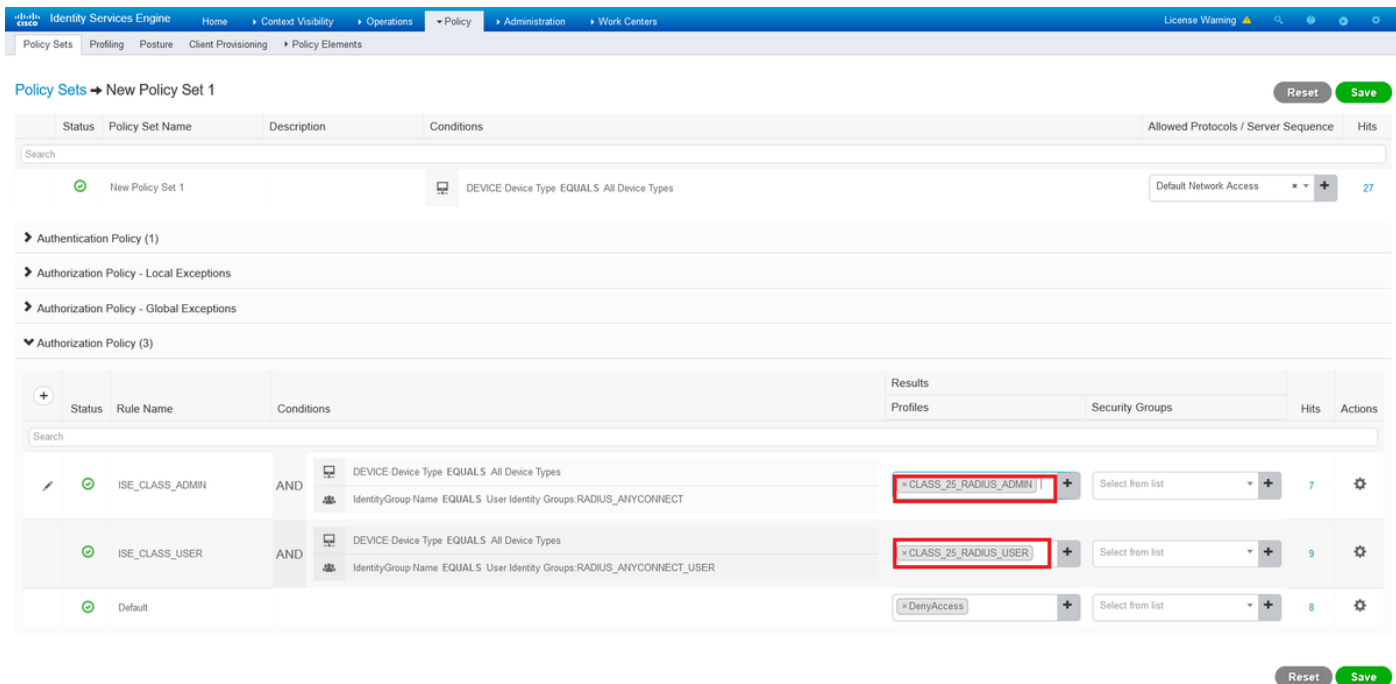
This should be the Group-policy name

步骤7.查看授权配置文件配置。



注意：按照上一映像Access_Accept、Class - [25]中所示的配置操作，RADIUS-ADMIN是组策略的名称（可以更改）。

图中显示了配置的外观。在同一策略集上，您有授权策略，每个策略都与条件部分中必需的身份组匹配，并使用您在配置文件部分的ASA上拥有的组策略。



通过此配置示例，您可以根据类属性通过ISE配置将组策略分配给每个Anyconnect用户。

故障排除

最有用的调试之一是调试radius。它显示AAA和ASA进程之间的RADIUS身份验证请求和身份验证响应的详细信息。

```
debug radius
```

另一个有用的工具是命令test aaa-server。现在您将看到身份验证是ACCEPTED还是REFUSED，以及在身份验证过程中交换的属性（本例中的“class”属性）。

```
test aaa-server authentication
```

工作场景

在上述配置示例中user1 根据ISE配置属于RADIUS-ADMIN 组策略，如果运行test aaa-server和debug radius，则可以验证它。突出显示需要验证的行。

```
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

另一种验证用户1通过Anyconnect连接时其是否工作的方法，请使用show vpn-sessiondb anyconnect命令了解由ISE类属性分配的组策略。

```
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
```

非工作场景1

如果Anyconnect上的身份验证失败，ISE回复REJECT。您需要验证用户是否与用户身份组关联或

密码不正确。 导航至“操作”>“实时日志”>“详细信息”。

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

注意：在本示例中，**user1**未与任何用户身份组关联。因此，它使用DenyAccess操作命中New Policy Set 1下的Default Authentication and Authorization策略(默认身份验证)。您可以在默认授权策略中将此操作修改为PermitAcces，以允许用户在未关联用户身份组的情况下进行身份验证。

非工作场景2

如果Anyconnect上的身份验证失败且默认授权策略为PermitAccess，则接受身份验证。但是，类属性不显示在Radius响应中，因此用户位于DfltGrpPolicy中，并且由于vpn-simultaneous-logins 0而无法连接。

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-simulate-logins 0更改为“1”，则用户连接，如输出所示：

```

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

```

