

Konfigurieren von SSL AnyConnect mit ISE-Authentifizierung und Klassenattribut für Gruppenrichtlinienzuordnung

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[ASA](#)

[ISE](#)

[Fehlerbehebung](#)

[Arbeitsszenario](#)

[Nichterwerbstätiges Szenario 1](#)

[Nichterwerbstätiges Szenario 2](#)

[Nichterwerbstätiges Szenario 3](#)

[Video](#)

Einführung

In diesem Dokument wird beschrieben, wie Secure Sockets Layer (SSL) AnyConnect mit der Cisco Identity Services Engine (ISE) für die Zuordnung von Benutzern zu bestimmten Gruppenrichtlinien konfiguriert wird.

Unterstützt von Amanda Nava, Cisco TAC Engineer.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- AnyConnect Secure Mobility Client Version 4.7
- Cisco ISE 2.4
- Cisco ASA Version 9.8 oder höher

Verwendete Komponenten

Der Inhalt dieses Dokuments basiert auf diesen Software- und Hardwareversionen.

- Adaptive Security Appliance (ASA) 5506 mit Softwareversion 9.8.1
- AnyConnect Secure Mobility Client 4.2.00096 unter Microsoft Windows 10 64-Bit.

- ISE Version 2.4

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

Im Beispiel stellen AnyConnect-Benutzer eine direkte Verbindung her, ohne dass die Option zur Auswahl der Tunnelgruppe im Dropdown-Menü verfügbar ist, da sie von der Cisco ISE gemäß ihren Attributen bestimmten Gruppenrichtlinien zugewiesen werden.

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
```

Hinweis: Mit diesem Konfigurationsbeispiel können Sie die Gruppenrichtlinie jedem AnyConnect-Benutzer über die ISE-Konfiguration zuweisen. Da die Benutzer nicht die Möglichkeit haben, die Tunnelgruppe auszuwählen, sind sie mit der Tunnelgruppe

DefaultWEBVPNGroup und der DfltGrpPolicy verbunden. Nach der Authentifizierung und der Rückgabe des Class-Attributs (Gruppenrichtlinie) in der ISE-Authentifizierungsantwort wird der Benutzer der entsprechenden Gruppe zugewiesen. Wenn für den Benutzer kein Class-Attribut angewendet wurde, bleibt dieser Benutzer weiterhin in der DfltGrpPolicy. Sie können die **vpn-simultane-Anmeldungen 0** unter der DfltGrpPolicy-Gruppe konfigurieren, um zu verhindern, dass Benutzer ohne Gruppenrichtlinie über das VPN eine Verbindung herstellen.

ISE

Schritt 1: Hinzufügen der ASA zur ISE

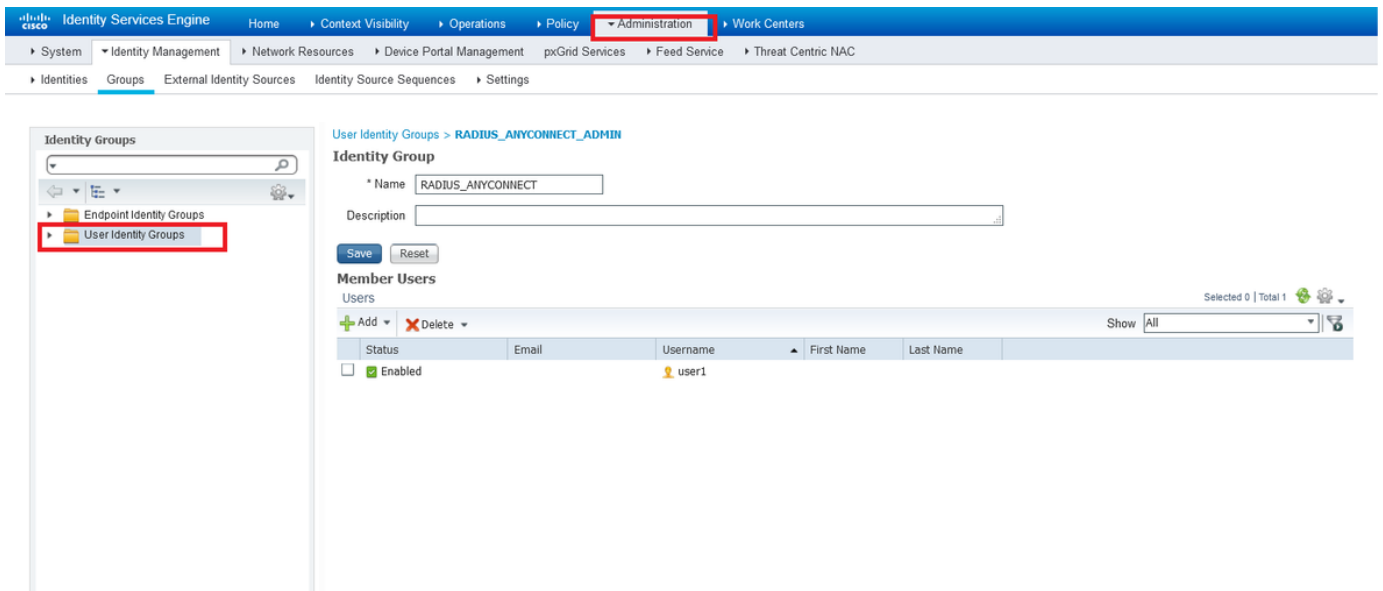
Navigieren Sie in diesem Schritt zu **Administration>Network Resources>Network Devices** (**Verwaltung > Netzwerkressourcen > Netzwerkgeräte**).

The screenshot displays the Cisco Identity Services Engine (ISE) interface for configuring a new network device. The breadcrumb navigation is **Administration > Network Resources > Network Devices**. The page title is **Network Devices List > ASAv**. The configuration form includes the following fields and options:

- 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:** (empty field)
- Location:** All Locations (Set To Default)
- IPSEC:** No (Set To Default)
- Device Type:** All Device Types (Set To Default)
- RADIUS Authentication Settings:** (checked)
 - RADIUS UDP Settings:**
 - Protocol:** RADIUS (indicated by a blue arrow)
 - Shared Secret:** cisco123 (Hide button)
 - Use Second Shared Secret:** (unchecked)
 - CoA Port:** 1700 (Set To Default)
 - RADIUS DTLS Settings:** (info icon)

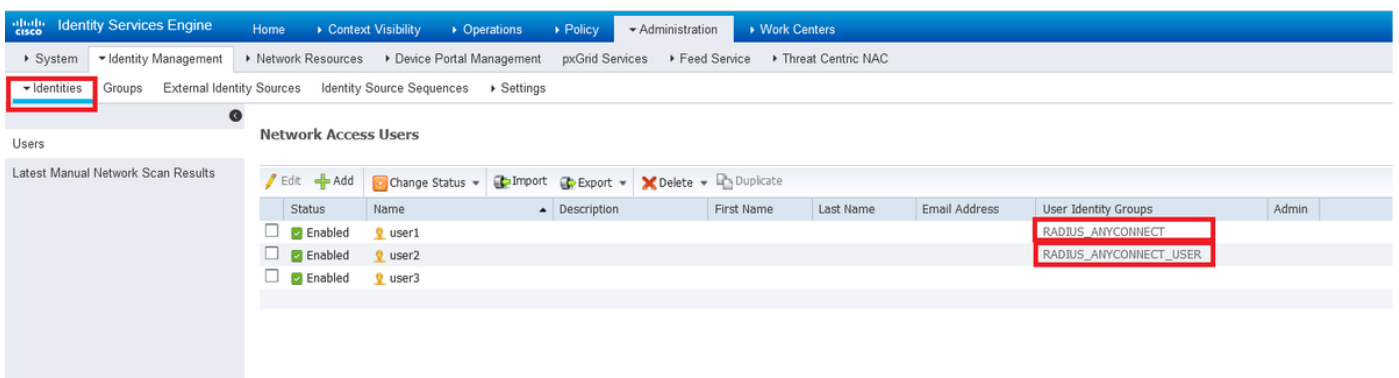
Schritt 2: Erstellen Sie Identitätsgruppen.

Identitätsgruppen definieren, um jeden Benutzer in den nächsten Schritten dem richtigen zuzuordnen. Navigieren Sie zu **Administration>Groups>User Identity Groups** (**Administration > Gruppen > Benutzeridentitätsgruppen**).



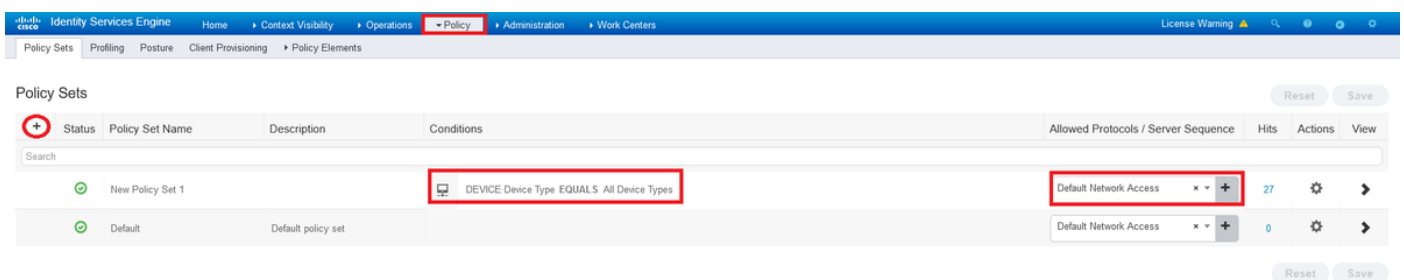
Schritt 3: Verknüpfen Sie Benutzer mit Identitätsgruppen.

Ordnen Sie Benutzer der richtigen Identitätsgruppe zu. Navigieren Sie zu **Administration>Identities>Users**.



Schritt 4: Policy-Set erstellen.

Definieren Sie einen neuen Richtlinienatz, wie im Beispiel gezeigt (alle Gerätetypen) unter Bedingungen. Navigieren Sie zu **Richtlinien > Richtlinien-Sets**.



Schritt 5: Erstellen einer Autorisierungsrichtlinie.

Erstellen Sie eine neue Autorisierungsrichtlinie mit der richtigen Bedingung, um die Identitätsgruppe abzugleichen.

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	Profiles	Security Groups	Hits	Actions
✓	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

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

Schritt 6: Erstellen eines Autorisierungsprofils

Erstellen eines neuen Autorisierungsprofils mit RADIUS: Class<Group-policy-ASA> Attribut und *Zugriffstyp: 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

Schritt 7: Überprüfen der Konfiguration des Autorisierungsprofils

The screenshot displays the Cisco Identity Services Engine (ISE) configuration interface for an Authorization Profile. The navigation menu on the left includes Authentication, Authorization, and Client Provisioning. The main configuration area is titled 'Authorization Profile' and contains the following fields:

- * Name: CLASS_25_RADIUS_ADMIN
- Description: (empty)
- * Access Type: ACCESS_ACCEPT
- Network Device Profile: Cisco
- Service Template:
- Track Movement:
- Passive Identity Tracking:

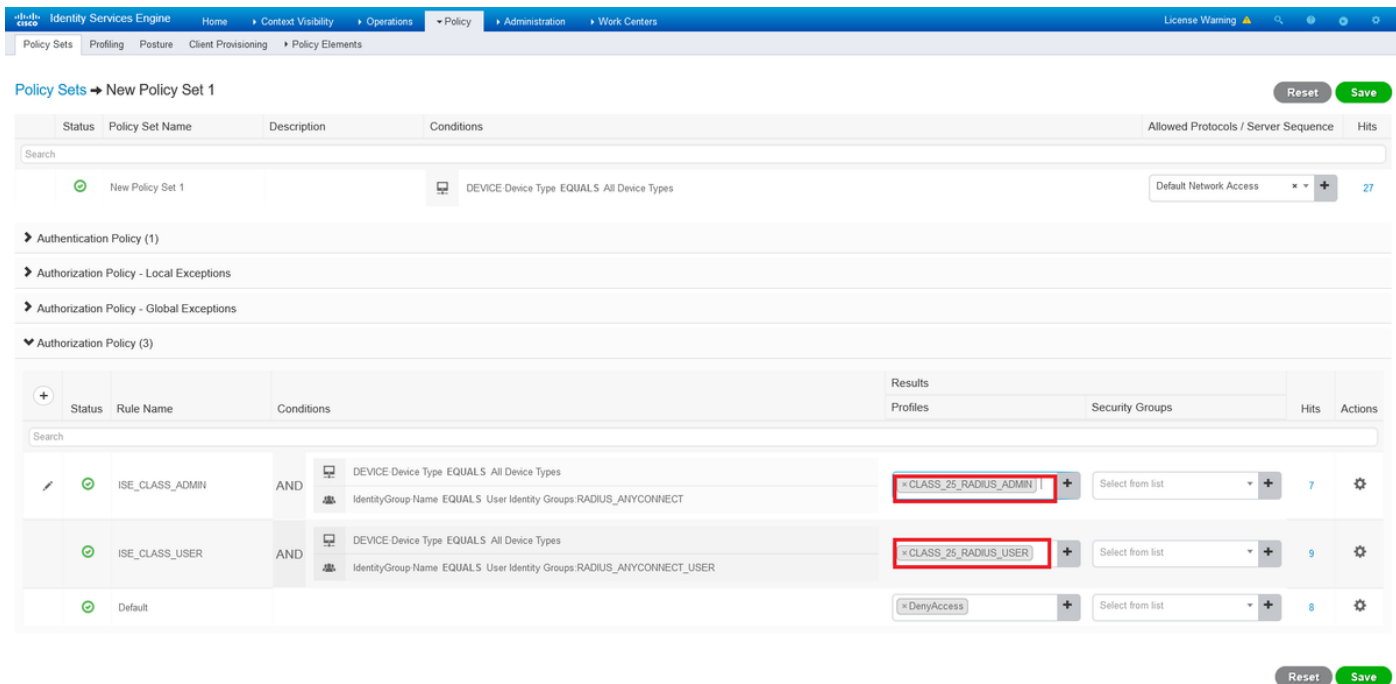
Below the configuration fields, there are sections for 'Common Tasks', 'Advanced Attributes Settings', and 'Attributes Details'. The 'Advanced Attributes Settings' section shows a configuration for 'Radius:Class' set to 'RADIUS-ADMIN'. The 'Attributes Details' section shows the following configuration:

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

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

Hinweis: Folgen Sie der Konfiguration, wie sie im vorherigen Bild angezeigt wird: Access_Accept, Class—[25], der RADIUS-ADMIN ist der Name Ihrer Gruppenrichtlinie (kann geändert werden).

Das Bild zeigt, wie die Konfiguration aussehen muss. Im gleichen Richtlinienatz verfügen Sie über keine Autorisierungsrichtlinien. Jede dieser Richtlinien entspricht der im Abschnitt "**Bedingungen**" erforderlichen Identitätsgruppe und verwendet die Gruppenrichtlinie, die Sie für die ASA im Abschnitt "**Profil**" haben.



In diesem Konfigurationsbeispiel können Sie die Gruppenrichtlinie jedem AnyConnect-Benutzer mithilfe der ISE-Konfiguration zuweisen, die auf dem Klassenattribut basiert.

Fehlerbehebung

Einer der nützlichsten Debugger ist der **Debugradius**. Es enthält Details zur RADIUS-Authentifizierungsanfrage und der Authentifizierungsantwort zwischen AAA- und ASA-Prozess.

```
debug radius
```

Ein weiteres nützliches Tool ist der Befehl `test aaa-server authentication`. Sie sehen nun, ob die Authentifizierung AKZEPTIERT oder ABGELEHNT ist und die Attribute ('class'-Attribut in diesem Beispiel) im Authentifizierungsprozess ausgetauscht werden.

```
test aaa-server authentication
```

Arbeitsszenario

Im oben erwähnten Konfigurationsbeispiel gehört **user1** zur Gruppenrichtlinie **RADIUS-ADMIN** entsprechend der ISE-Konfiguration. Es kann überprüft werden, ob der Testaa-Server und der Debugradius ausgeführt werden. Markieren Sie die zu verifizierenden Posten.

```
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

| 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

Eine andere Möglichkeit zu überprüfen, ob es funktioniert, wenn Benutzer1 über AnyConnect eine Verbindung herstellt, verwenden Sie den Befehl **show vpn-sessiondb anyconnect**, um die vom ISE-Klassenattribut zugewiesene Gruppenrichtlinie zu kennen.

```

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

```

Nichterwerbstitiges Szenario 1

Wenn bei AnyConnect die Authentifizierung fehlschlgt und die ISE mit einem REJECT antwortet. Sie mssen berprfen, ob der Benutzer einer **Benutzeridentittsgruppe** zugeordnet ist oder ob das Kennwort falsch ist. Navigieren Sie zu **Operations > Live logs > Details**.

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

Hinweis: In diesem Beispiel ist **user1** keiner **Benutzeridentittsgruppe** zugeordnet. Daher trifft er auf die Standardauthentifizierungs- und Autorisierungsrichtlinien unter dem **New Policy Set 1** mit der Aktion **DenyAccess**. Sie knnen diese Aktion in der Standardautorisierungsrichtlinie auf **PermitAccess** ändern, um Benutzern ohne die zugeordnete Benutzeridentittsgruppe die Authentifizierung zu ermoglichen.

Nichterwerbstitiges Szenario 2

Wenn bei AnyConnect die Authentifizierung fehlschlägt und die standardmäßige Autorisierungsrichtlinie PermitAccess lautet, wird die Authentifizierung akzeptiert. Das class-Attribut wird jedoch nicht in der RADIUS-Antwort angezeigt, daher befindet sich der Benutzer in der DfltGrpPolicy, und die Verbindung wird aufgrund der **vpn-simultanen Anmeldungen 0** nicht hergestellt.

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:0alf7
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:0alf7c5229T
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:0alf7c5229T
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#

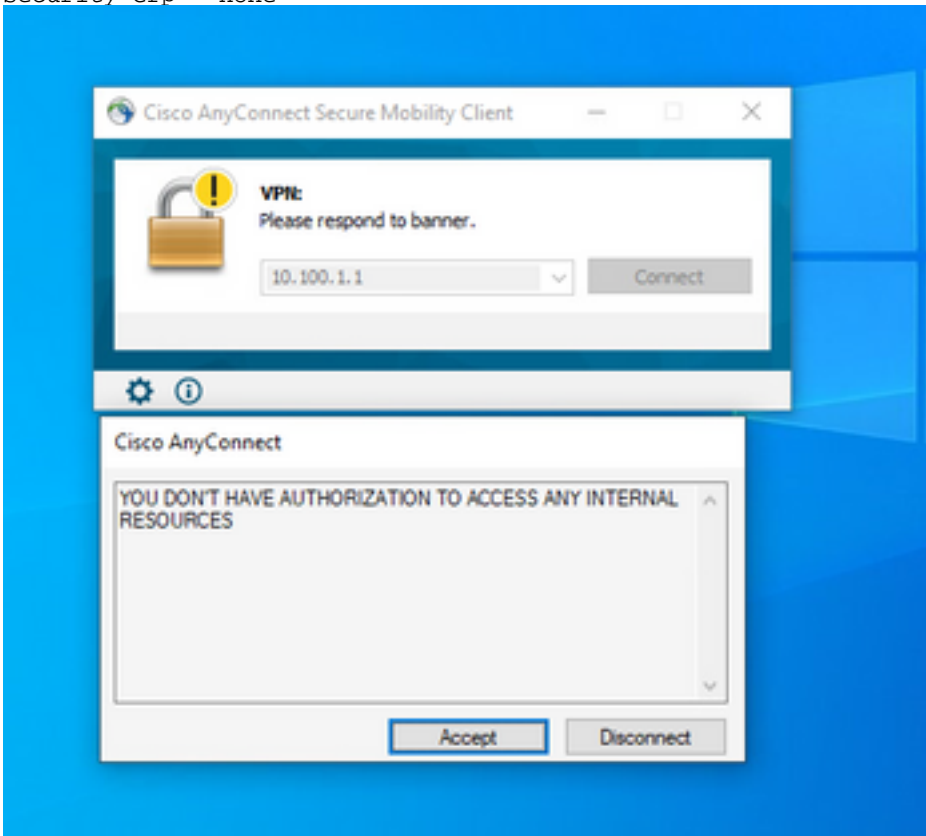
```

Wenn die **vpn-simultane-Anmeldungen 0** auf '1' geändert wird, stellt der Benutzer eine Verbindung her, wie in der Ausgabe dargestellt:

```

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

```



Nichterwerbstätiges Szenario 3

Wenn die Authentifizierung erfolgreich verläuft, der Benutzer aber nicht über die richtigen Richtlinien verfügt, z. B. wenn die Gruppenrichtlinie verbunden ist, den Split Tunnel anstelle des vollständigen Tunnels hat, wie er sein muss. Der Benutzer kann sich in der falschen Benutzeridentitätsgruppe befinden.

```
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

Video

Dieses Video enthält die Schritte zur Konfiguration von SSL AnyConnect mit ISE-Authentifizierung und Klassenattribut für die Gruppenrichtlinienzuordnung.