

# TME-recreate-attempt 2017-Oct-21

## Setup Info

- ISE 2.3 Patch 1
- ASAv with ASA 9.7(1)
- AC VPN 4.3.02039
- Cisco Temporal Agent Windows 4.5.01043

## Create the User Custom Attributes

Attribute Name	Description	Data Type	Parameters	Default Value
acPostureUnknown		String	String Max length <input type="text"/>	asaPostureReme
acPostureCompliant		String	String Max length <input type="text"/>	PERMIT_ALL_TF

## Create a NA user

**Network Access User**

\* Name

Status  Enabled

Email

---

▶ Passwords

---

▶ User Information

---

▶ Account Options

---

▶ Account Disable Policy

---

**User Custom Attributes**

acPostureUnknown	=	asaPostureRemediation
acPostureCompliant	=	PERMIT_ALL_TRAFFIC

# Authorization Profile -- iuPostureRemediation

Access Type = ACCESS\_ACCEPT



DACL = InternalUser:acPostureUnknown

## Authorization Profile


\* Name


Description

\* Access Type

Network Device Profile   

Service Template

Track Movement  

Passive Identity Tracking  

### ▼ Common Tasks

DACL Name  

# Authorization Profile -- iuCompliantAccess

Access Type = ACCESS\_ACCEPT

DACL = InternalUser:acPostureCompliant

## Authorization Profile

\* Name

Description

\* Access Type

Network Device Profile

Service Template

Track Movement

Passive Identity Tracking

### Common Tasks

DACL Name

## Authorization Policy for VPN

Status	Rule Name	Conditions	Profiles
	Compliant Access	Session-PostureStatus EQUALS Compliant	<input type="text" value="* iuCompliantAccess"/>
	Default		<input type="text" value="* iuPostureRemediation"/>

## RADIUS Live Logs

	Status	Identity	Endpoint ID	Authorization Profiles	IP Address
' 04:33:47.444 PM		#ACSACL#-IP-PERMIT_ALL_TRAFFIC-57f6b0d3			
' 04:33:47.438 PM			10.1.60.10	iuCompliantAccess	
' 04:33:45.420 PM		tt01	00:50:56:BD:FC:15	iuPostureRemediation	10.1.100.201
' 04:32:25.386 PM		#ACSACL#-IP-asaPostureRemediation-59eb6f98			
' 04:32:25.381 PM		tt01	00:50:56:BD:FC:15	iuPostureRemediation	

## TCPDUMP between ISE and ASAv

Note that the CoA-Request after posture compliant includes the DACL name.

No.	Time	Source	Destination	Protocol	Length	User-Name	Info
1	16:32:25.344898	10.1.100.254	10.1.100.21	RADIUS	629	tt01	Access-Request(1) (id=29, l=587)
2	16:32:25.381793	10.1.100.21	10.1.100.254	RADIUS	277	tt01	Access-Accept(2) (id=29, l=235)
3	16:32:25.385509	10.1.100.254	10.1.100.21	RADIUS	265	#ACSACL#-IP-asaPostureRemediation-59eb6f98	Access-Request(1) (id=30, l=223)
4	16:32:25.386721	10.1.100.21	10.1.100.254	RADIUS	1309	#ACSACL#-IP-asaPostureRemediation-59eb6f98	Access-Accept(2) (id=30, l=1267)
5	16:32:25.393039	10.1.100.254	10.1.100.21	RADIUS	673	tt01	Accounting-Request(4) (id=31, l=631)
6	16:32:25.400013	10.1.100.21	10.1.100.254	RADIUS	62		Accounting-Response(5) (id=31, l=20)
7	16:32:27.565487	10.1.100.254	10.1.100.21	RADIUS	703	tt01	Accounting-Request(4) (id=32, l=661)
8	16:32:27.569204	10.1.100.21	10.1.100.254	RADIUS	62		Accounting-Response(5) (id=32, l=20)
9	16:33:47.435990	10.1.100.21	10.1.100.254	RADIUS	238		CoA-Request(43) (id=5, l=196)
10	16:33:47.438282	10.1.100.254	10.1.100.21	RADIUS	62		CoA-ACK(44) (id=5, l=20)
11	16:33:47.443671	10.1.100.254	10.1.100.21	RADIUS	262	#ACSACL#-IP-PERMIT_ALL_TRAFFIC-57f6b0d3	Access-Request(1) (id=33, l=220)
12	16:33:47.444571	10.1.100.21	10.1.100.254	RADIUS	247	#ACSACL#-IP-PERMIT_ALL_TRAFFIC-57f6b0d3	Access-Accept(2) (id=33, l=205)
13	16:34:17.982414	10.1.100.254	10.1.100.21	RADIUS	715	tt01	Accounting-Request(4) (id=34, l=673)
14	16:34:17.986009	10.1.100.21	10.1.100.254	RADIUS	62		Accounting-Response(5) (id=34, l=20)

```

Frame 9: 238 bytes on wire (1904 bits), 238 bytes captured (1904 bits)
Ethernet II, Src: Vmware_bd:32:65 (00:50:56:bd:32:65), Dst: Vmware_bd:91:54 (00:50:56:bd:91:54)
Internet Protocol Version 4, Src: 10.1.100.21 (10.1.100.21), Dst: 10.1.100.254 (10.1.100.254)
User Datagram Protocol, Src Port: 38184 (38184), Dst Port: 1700 (1700)
Radius Protocol

```

```

Code: CoA-Request (43)
Packet identifier: 0x5 (5)
Length: 196
Authenticator: 1a5a2b3176dd114e0b507f2e9cab494e
[The response to this request is in frame 10]
Attribute Value Pairs
AVP: l=6 t=NAS-IP-Address(4): 10.1.100.254
AVP: l=12 t=Calling-Station-Id(31): 10.1.60.10
AVP: l=10 t=Acct-Session-Id(44): 5F100005
AVP: l=6 t=Event-Timestamp(55): Oct 21, 2017 16:33:47.000000000 Coordinated Universal Time
AVP: l=18 t=Message-Authenticator(80): d239c6f54be92295540344289f383911
AVP: l=75 t=Vendor-Specific(26) v=ciscoSystems(9)
VSA: l=69 t=Cisco-AVPair(1): ACS:CiscoSecure-Defined-ACL=#ACSACL#-IP-PERMIT_ALL_TRAFFIC-57f6b0d3
AVP: l=49 t=Vendor-Specific(26) v=ciscoSystems(9)

```

## ASAv Console Logging

```
ASAv# show vpn-sessiondb detail anyconnect
```

```
INFO: There are presently no active sessions
```

```
ASAv# %ASA-6-113004: AAA user authentication Successful : server = 10.1.100.21 : user = tt01
```

```
%ASA-6-113009: AAA retrieved default group policy (ANYCONNECT-ISE) for user = tt01
```

```
%ASA-6-113008: AAA transaction status ACCEPT : user = tt01
```

```
%ASA-6-113039: Group <ANYCONNECT-ISE> User <tt01> IP <10.1.60.10> AnyConnect parent session started.
```

```
%ASA-6-113004: AAA user accounting Successful : server = 10.1.100.21 : user = tt01
```

```
%ASA-6-113004: AAA user accounting Successful : server = 10.1.100.21 : user = tt01
```

```
ASAv# show vpn-sessiondb detail anyconnect
```

```
Session Type: AnyConnect Detailed
```

```
Username : tt01 Index : 8
```

```
Assigned IP : 10.1.100.201 Public IP : 10.1.60.10
```

```
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
```

```
License : AnyConnect Premium
```

```
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES128 DTLS-Tunnel: (1)AES128
```

Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1

Bytes Tx : 33561 Bytes Rx : 26122

Pkts Tx : 153 Pkts Rx : 206

Pkts Tx Drop : 0 Pkts Rx Drop : 0

Group Policy : ANYCONNECT-ISE Tunnel Group : ANYCONNECT-ISE

Login Time : 16:32:25 UTC Sat Oct 21 2017

Duration : 0h:00m:16s

Inactivity : 0h:00m:00s

VLAN Mapping : N/A VLAN : none

Audt Sess ID : 0a0164fe0000800059eb7699

Security Grp : none

AnyConnect-Parent Tunnels: 1

SSL-Tunnel Tunnels: 1

DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:

<--- More --->

Tunnel ID : 8.1

Public IP : 10.1.60.10

Encryption : none Hashing : none

TCP Src Port : 49648 TCP Dst Port : 443

Auth Mode : userPassword

Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes

Client OS : win

Client OS Ver: 6.1.7601 Service Pack 1

Client Type : AnyConnect

Client Ver : Cisco AnyConnect VPN Agent for Windows 4.3.02039

Bytes Tx : 7859 Bytes Rx : 0

Pkts Tx : 6 Pkts Rx : 0

Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:

Tunnel ID : 8.2

Assigned IP : 10.1.100.201 Public IP : 10.1.60.10

Encryption : AES128 Hashing : SHA1

Ciphersuite : AES128-SHA

Encapsulation: TLSv1.2 TCP Src Port : 49651

TCP Dst Port : 443                    Auth Mode : userPassword  
Idle Time Out: 30 Minutes            Idle TO Left : 29 Minutes  
Client OS : Windows  
<--- More --->

Client Type : SSL VPN Client  
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.3.02039  
Bytes Tx : 7859                    Bytes Rx : 0  
Pkts Tx : 6                        Pkts Rx : 0  
Pkts Tx Drop : 0                    Pkts Rx Drop : 0  
**Filter Name : #ACSACL#-IP-asaPostureRemediation-59eb6f98**

DTLS-Tunnel:

Tunnel ID : 8.3  
Assigned IP : 10.1.100.201            Public IP : 10.1.60.10  
Encryption : AES128                  Hashing : SHA1  
Ciphersuite : AES128-SHA  
Encapsulation: DTLSv1.0              UDP Src Port : 51480  
UDP Dst Port : 443                  Auth Mode : userPassword  
Idle Time Out: 30 Minutes            Idle TO Left : 30 Minutes  
Client OS : Windows  
Client Type : DTLS VPN Client  
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.3.02039  
Bytes Tx : 18003                    Bytes Rx : 27932  
Pkts Tx : 145                        Pkts Rx : 222  
Pkts Tx Drop : 0                    Pkts Rx Drop : 0  
**Filter Name : #ACSACL#-IP-asaPostureRemediation-59eb6f98**

ASAv# %ASA-6-113004: AAA user authorization Successful : server = 10.1.100.21 : user = tt01  
%ASA-6-113009: AAA retrieved default group policy (ANYCONNECT-ISE) for user = tt01  
%ASA-6-113008: AAA transaction status ACCEPT : user = tt01  
%ASA-6-109100: Received CoA update from 10.1.100.21 for user 'tt01', with session ID 0a0164fe0000800059eb7699,  
changing authorization attributes.

ASAv# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : tt01 Index : 8  
Assigned IP : 10.1.100.201 Public IP : 10.1.60.10  
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel  
License : AnyConnect Premium  
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES128 DTLS-Tunnel: (1)AES128  
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1  
Bytes Tx : 14468755 Bytes Rx : 511821  
Pkts Tx : 10703 Pkts Rx : 11158  
Pkts Tx Drop : 0 Pkts Rx Drop : 0  
Group Policy : ANYCONNECT-ISE Tunnel Group : ANYCONNECT-ISE  
Login Time : 16:32:25 UTC Sat Oct 21 2017  
Duration : 0h:01m:35s  
Inactivity : 0h:00m:00s  
VLAN Mapping : N/A VLAN : none  
Audt Sess ID : 0a0164fe0000800059eb7699  
Security Grp : none  
AnyConnect-Parent Tunnels: 1  
SSL-Tunnel Tunnels: 1  
DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:

<--- More --->

Tunnel ID : 8.1  
Public IP : 10.1.60.10  
Encryption : none Hashing : none  
TCP Src Port : 49648 TCP Dst Port : 443  
Auth Mode : userPassword  
Idle Time Out: 30 Minutes Idle TO Left : 28 Minutes  
Client OS : win  
Client OS Ver: 6.1.7601 Service Pack 1  
Client Type : AnyConnect  
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.3.02039  
Bytes Tx : 7859 Bytes Rx : 0  
Pkts Tx : 6 Pkts Rx : 0  
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:

Tunnel ID : 8.2  
Assigned IP : 10.1.100.201      Public IP : 10.1.60.10  
Encryption : AES128      Hashing : SHA1  
Ciphersuite : AES128-SHA  
Encapsulation: TLSv1.2      TCP Src Port : 49651  
TCP Dst Port : 443      Auth Mode : userPassword  
Idle Time Out: 30 Minutes      Idle TO Left : 28 Minutes  
Client OS : Windows

<--- More --->

Client Type : SSL VPN Client  
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.3.02039  
Bytes Tx : 7859      Bytes Rx : 0  
Pkts Tx : 6      Pkts Rx : 0  
Pkts Tx Drop : 0      Pkts Rx Drop : 0

Filter Name : #ACSACL#-IP-PERMIT\_ALL\_TRAFFIC-57f6b0d3

DTLS-Tunnel:

Tunnel ID : 8.3  
Assigned IP : 10.1.100.201      Public IP : 10.1.60.10  
Encryption : AES128      Hashing : SHA1  
Ciphersuite : AES128-SHA  
Encapsulation: DTLSv1.0      UDP Src Port : 51480  
UDP Dst Port : 443      Auth Mode : userPassword  
Idle Time Out: 30 Minutes      Idle TO Left : 29 Minutes  
Client OS : Windows  
Client Type : DTLS VPN Client  
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.3.02039  
Bytes Tx : 14453037      Bytes Rx : 511821  
Pkts Tx : 10691      Pkts Rx : 11158  
Pkts Tx Drop : 0      Pkts Rx Drop : 0

Filter Name : #ACSACL#-IP-PERMIT\_ALL\_TRAFFIC-57f6b0d3

ASAv# %ASA-4-113019: Group = ANYCONNECT-ISE, Username = tt01, IP = 10.1.60.10, Session disconnected. Session Type: SSL, Duration: 0h:01m:52s, Bytes xmt: 28921792, Bytes rcv: 1023642, Reason: User Requested



%ASA-6-113004: AAA user accounting Successful : server = 10.1.100.21 : user = tt01

ASAv# show vpn-sessiondb detail anyconnect

INFO: There are presently no active sessions