# **Configure ASA VPN Posture with ISE**

## Contents

Introduction
<u>Prerequisites</u>
Requirements
Components Used
Background Information
<u>Configure</u>
Network Diagram and Traffic Flow
Configurations
ASA
ISE
Periodic Reassessment
<u>Verify</u>
<u>Troubleshoot</u>
Debugs on the ISE
Debugs on the ASA
Debugs for the Agent
NAC Agent Posture failure
Related Information

## Introduction

This document describes how to configure the ASA to posture VPN users against the ISE.

## Prerequisites

## Requirements

Cisco recommends that you have knowledge of these topics:

- Basic knowledge of ASA CLI configuration and Secure Socket Layer (SSL) VPN configuration
- Basic knowledge of remote access VPN configuration on the ASA
- Basic knowledge of ISE and posture services

## **Components Used**

The information in this document is based on these software versions:

- Cisco ASA software Versions 9.16 and later
- Microsoft Windows Version 7 with Cisco AnyConnect Secure Mobility Client Version 4.10
- Cisco ISE Version 3.0

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure

that you understand the potential impact of any command.

## **Background Information**

The Cisco ASA Version 9.16 supports RADIUS Change of Authorization (CoA) (RFC 5176). This allows for posturing of VPN users against the Cisco ISE. After a VPN user logs in, the ASA redirects web traffic to the ISE, where the user is provisioned with a Network Admission Control (NAC) Agent or Web Agent. The agent performs specific checks on the user machine in order to determine its compliance against a configured set of posture rules, such as Operating System (OS), patches, AntiVirus, Service, Application or Registry rules.

The results of the posture validation are then sent to the ISE. If the machine is deemed complaint, then the ISE can send a RADIUS CoA to the ASA with the new set of authorization policies. After successful posture validation and CoA, the user is allowed access to the internal resources.

## Configure



## **Network Diagram and Traffic Flow**

Here is the traffic flow, as illustrated in the network diagram:

- 1. The remote user uses Cisco Anyconnect for VPN access to the ASA.
- 2. The ASA sends a RADIUS Access-Request for that user to the ISE.
- 3. That request hits the policy named **ASA916-posture** on the ISE. As a result, the **ASA916-posture** authorization profile is returned. The ISE sends a RADIUS Access-Accept with two Cisco Attribute-Value pairs:

- **url-redirect-acl=redirect** this is the Access Control List (ACL) name that is defined locally on the ASA, which decides the traffic that must be redirected.
- **url-redirect** this is the URL to which the remote user must be redirected.

**Tip**: The Domain Name System (DNS) servers that are assigned to the VPN clients must be able to resolve the Fully Qualified Domain Name (FQDN) that is returned in the redirect URL. If the VPN filters are configured in order to restrict access at the tunnel-group level, ensure that the client pool is able to access the ISE server on the configured port (**TCP 8443** in this example).

- 4. The ASA sends a RADIUS Accounting-Request start packet and receives a response. This is needed in order to send all of the details in regards to the session to the ISE. These details include the session\_id, external IP address of the VPN client, and the IP address of the ASA. The ISE uses the session\_id in order to identify that session. The ASA also sends periodic interim account information, where the most important attribute is the Framed-IP-Address with the IP that is assigned to the client by the ASA (**10.10.10.10** in this example).
- 5. When the traffic from the VPN user matches the locally-defined ACL (redirect). Dependent upon the configuration, the ISE provisions the NAC Agent or the Web Agent.
- 6. After the agent is installed on the client machine, it automatically performs specific checks. In this example, it searches for the c:\test.txt file. It also sends a posture report to the ISE, which can include multiple exchanges with the use of SWISS protocol and ports TCP/UDP 8905 in order to access the ISE.
- 7. When the ISE receives the posture report from the agent, it processes the authorization rules once again. This time, the posture result is known and another rule is hit. It sends a RADIUS CoA packet:
  - If the user is compliant, then a Downloadable ACL (DACL) name that permits full access is sent (AuthZ rule ASA916-compliant).
  - If the user is non-compliant, then a DACL name that permits limited access is sent (AuthZ rule ASA916-noncompliant).

**Note**: The RADIUS CoA is always confirmed; that is, the ASA sends a response to the ISE in order to confirm.

- 8. The ASA removes the redirection. If it does not have the DACLs cached, it must send an Access-Request in order to download them from the ISE. The specific DACL is attached to the VPN session.
- 9. The next time that the VPN user tries to access the web page, it can access all of the resources that are permitted by the DACL that is installed on the ASA. If the user is not compliant, only limited access is granted.



### Configurations

Use this section in order to configure the ASA and the ISE.

### ASA

Here is the basic ASA configuration for Cisco AnyConnect access:

```
<#root>
ip local pool
POOL 10.10.10.10-10.10.10.100
mask 255.255.255.0
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address xxxx 255.255.25.0
I
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 162.168.111.10 255.255.255.0
aaa-server ISE protocol radius
aaa-server ISE (inside) host 10.48.66.74
key cisco
webvpn
enable outside
anyconnect image disk0:/anyconnect-win-arm64-4.10.06079-webdeploy-k9.pkg 1
 anyconnect enable
tunnel-group-list enable
group-policy GP-SSL internal
group-policy GP-SSL attributes
vpn-tunnel-protocol ikev1 ikev2 ssl-client ssl-clientless
tunnel-group RA type remote-access
tunnel-group RA general-attributes
address-pool POOL
 authentication-server-group ISE
 default-group-policy GP-SSL
tunnel-group RA webvpn-attributes
 group-alias RA enable
```

For ASA integration with the ISE posture, ensure that you:

- Configure the Authentication, Authorization, and Accounting (AAA) server for dynamic authorization in order to accept CoA.
- Configure the accounting as a tunnel-group in order to send VPN session details towards the ISE.
- Configure the interim accounting which sends IP address assigned to the user and periodically update the session status on ISE
- Configure the redirect ACL, which decides if the DNS and the ISE traffic are allowed. All other HTTP traffic is redirected to the ISE for posture.



Note: Only registered Cisco users can access internal Cisco tools and information.

Here is the configuration example:

<#root>

access-list

#### redirect

extended deny udp any any eq domain access-list

#### redirect

extended deny ip any host 10.48.66.74 access-list

redirect

extended deny icmp any any access-list

redirect

extended permit tcp any any eq www

aaa-server ISE protocol radius

authorize-only

interim-accounting-update periodic 1

dynamic-authorization

aaa-server ISE (inside) host 10.48.66.74
key cisco

tunnel-group RA general-attributes
address-pool POOL
authentication-server-group ISE

accounting-server-group ISE

default-group-policy GP-SSL

ASA accounting mode:

The accounting mode on ASA needs to be single (default) otherwise ASA is not able to correctly process ISE sessions; that is, ASA rejects the CoA request with "Action not supported".

#### ISE

Complete these steps in order to configure the ISE:

1. Navigate to **Administration > Network Resources > Network Devices** and add the ASA as a network device:

cisco Identity Services Engine	Home Operations      Policy      Administration
🔆 System 🛛 🖉 Identity Management 🛛 📷 N	letwork Resources 🛃 Web Portal Management 👸 Feed Service
Network Devices Network Device Groups Exte	ernal RADIUS Servers RADIUS Server Sequences SGA AAA Servers NAC Managers
Network Devices	Network Devices List > New Network Device Network Devices
<u>р</u>	* Name ASA
@ •	Description
Network Devices     Default Device	* IP Address: 192.168.111.10 / 32 Model Name Software Version * Network Device Group Location All Locations
	Device Type All Device Types 📀 Set To Default
	✓ Authentication Settings
	Enable Authentication Settings
	Protocol RADIUS
	- Snared Secret Show

2. Navigate to **Policy > Results > Authorization > Downloadable ACL** and configure the DACL so that it permits full access. The default ACL configuration permits all IP traffic on the ISE:

cisco Identity Services Engine	Administration   ▼
Authentication Authorization Dictionaries Conditions Results	Profiling Posture Client Provisioning Security Group Access Downloadable ACL List > PERMIT_ALL_TRAFFIC
	Downloadable ACL  *Name PERMIT_ALL_TRAFFIC  Description Allow all Traffic  *DACL Content  permit ip any any  3 4 5 6 7 8 9 10
	Check DACL Syntax

- 3. Configure a similar ACL that provides limited access (for non-compliant users).
- 4. Navigate to Policy > Results > Authorization > Authorization Profiles and configure the Authorization Profile named ASA92-posture, which redirects users for posture. Check the Web Redirection check box, select Client Provisioning from the drop-down list, and ensure that redirect appears in the ACL field (that ACL is defined locally on the ASA):

cisco Identity Services Engine	
Authentication Authorization Pro Dictionaries Conditions Results Results	Mome Operations  Policy   Administration   rofiling   Posture   Client Provisioning   Security Group Access Authorization Profiles   Authorization Profile  *Name   ASA92-posture Description   *Access Type   ACCESS_ACCEPT   Service Template   Voice Domain Permission
	Web Redirection (CWA, DRW, MDM, NSP, CPP) Client Provisioning (Posture)  ACL redirect Static IP/Host name

5. Configure the Authorization Profile named **ASA92-compliant**, which must only return the DACL named **PERMIT\_ALL\_TRAFFIC** that provides full access for the compliant users:

altalu	
cisco Identity Services Engine	Administration   ▼
🔟 Authentication 🛛 🧕 Authorization	🔀 Profiling 👩 Posture 🕞 Client Provisioning 📑 Security Group Access
Dictionaries Conditions Results	
Results         Image: Security Group Access	Authorization Profiles > ASA92-compliant Authorization Profile * Name ASA92-compliant Description * Access Type ACCESS_ACCEPT Service Template Common Tasks DACL Name PERMIT_ALL_TRAFFIC

- 6. Configure a similar Authorization Profile named **ASA916-noncompliant**, which must return the DACL with limited access (for non compliant users).
- 7. Navigate to **Policy > Authorization** and configure the Authorization Rules:

- Create a rule that allows full access if the posture results are compliant. The result is the authorization policy **ASA916-compliant**.
- Create a rule that allows limited access if the posture results are non-compliant. The result is the authorization policy **ASA916-noncompliant**.
- Ensure that if neither of the previous two rules are hit, then the default rule returns the **ASA916**-**posture**, which forces a redirection on the ASA.

2	ASA92 complaint	if	Session:PostureStatus EQUALS Compliant	then	ASA92-compliant
	ASA92 non complaint	if	Session:PostureStatus EQUALS NonCompliant	then	ASA92-noncompliant
<b>~</b>	ASA92 redirect	if	Radius:NAS-IP-Address EQUALS 192.168.111.10	then	ASA92-posture

8. The default authentication rules check the user name in the internal identity store. If this must be changed (checked in the Active Directory (AD), for example), then navigate to **Policy** > **Authentication** and make the change:

cisco	Identity Services Engine		Policy   V Administration   V
🔔 Au	uthentication 🧕 🧕 Authorizati	on 🔀 Profiling 👩 Posture 📷 Clie	ent Provisioning 📑 Security Group Access 🔒 Po
Auther	ntication Policy		
Define the Policy Typ	e Authentication Policy by selecti pe O Simple	ng the protocols that ISE should use to communicat d	te with the network devices, and the identity sources that it sh
	MAB	: If Wired_MAB OR Wireless_MAB	Allow Protocols : Default Network Access
	Dot1X	: If Wired_802.1X OR Wireless_802.1X	Allow Protocols : Default Network Access
	🗹 Default	use Internal Users	
6	Default Rule (If no match)	: Allow Protocols : Default Network Access	and use : Internal Users

9. Navigate to **Policy > Client Provisioning** and configure the provisioning rules. These are the rules that decide the type of Agent that must be provisioned. In this example, only one simple rule exists, and the ISE selects the NAC Agent for all Microsoft Windows systems:

cisco Identity Services Engine	🙆 Home (	Operations   • Policy   • Ad	Iministration   •	
🛓 Authentication 🛛 🧕 Authorization	🛃 Profiling 🛛 👩 Posture	Client Provisioning	🚞 Security Group Access	🐥 Policy Elements
Client Provisioning Policy Define the Client Provisioning Policy to determine For Agent Configuration: version of agent, agent pr For Native Supplicant Configuration: wizard profile	what users will receive upon I ofile, agent compliance modu and/or wizard. Drag and drop	login and user session initiation: Jle, and/or agent customization pa rules to change the order.	ickage.	
<ul> <li>Rule Name</li> </ul>	Identity Groups	Operating Systems	Other Conditions	Results
ASA92-posture	If Any and	Windows All and	Condition(s)	then NACAgent 4.9.0.1013

When the Agents are not on the ISE, it is possible to download them:

\CAgent 4.9 🗢 🔄		Done
Agent Configuration		
Agent:	NACAgent 4.9.0.1013	📀 🗹 Is Upgrade Mandatory
Profile:	Choose a Profile	Agents
Compliance Module:	Choose a Compliance Module	
Agent Customization Package:	Choose a Customization Package	(-)
Native Supplicant Co Config Wizard: Choose a Wizard Profile: Choose a	nfiguration Config Wizard O Wizard Profile O	<ul> <li>Cled So Download Resource</li> <li>NAC Upload Resource</li> <li>NACAgent 4.9.0.52</li> <li>NACAgent 4.9.0.1009</li> <li>NACAgent 4.9.0.1013</li> <li>WebAgent 4.9.0.24</li> <li>WebAgent 4.9.0.28</li> <li>WebAgent 4.9.0.31</li> <li>WebAgent 4.9.0.1005</li> </ul>

- 10. If necessary, you can navigate to **Administration > System > Settings > Proxy** and configure the proxy for the ISE (to access the Internet).
- 11. Configure the posture rules, which verify the client configuration. You can configure rules that check:
  - files existence, version, date
  - registry key, value, existence
  - application process name, running, not running
  - service service name, running, not running
  - antivirus more than 100 vendors supported, version, when definitions are updated
  - antispyware more than 100 vendors supported, version, when definitions are updated
  - compound condition mixture of all
  - custom dictionary conditions usage of most of the ISE dictionaries
- 12. In this example, only a simple file existence check is performed. If the c:\test.txt file is present on the client machine, it is compliant and allowed full access. Navigate to Policy > Conditions > File Conditions and configure the file condition:

cisco Identity Services Engine	Administration   ▼
🛃 Authentication 🛛 🧔 Authorization 🔀	Profiling 👩 Posture 👩 Client Provisioning 📄 Security Group Access 🔒 Policy Elements
Dictionaries Conditions Results	
Posture	File Conditions List > file_condition * Name file_condition Description + File Path ABSOLUTE_PATH * [::\test.txt () + File Type FileExistence * + File Operator Exists * * Operating System Windows All () Save Reset

13. Navigate to Policy > Results > Posture > Requirements and create a requirement. This requirement must be met when the previous condition is satisfied. If it is not, then remediation action is executed. There can be many types of remediation actions available, but in this example, the simplest one is used: a specific message is displayed.

cisco Identity Services Engine			Administration   *			
Authentication  Authorization Dictionaries Conditions Results	🛃 Profiling	🖉 Posture 🕞 Client Provisio	ning 📃 Security Group Acc	888 🦷	Policy Elements	
Results	Re	quirements				
	ρ	Name	Operating Systems		Conditions	Remediation Actions
↓ ± *	@					
<ul> <li>Authentication</li> <li>Authentication</li> </ul>		file_requirement	for Windows All		file_condition	else Message Text Only
Profiling		Any_AV_Installation_Win	for Windows All	met if	ANY_av_win_inst	else Message Text Only
<ul> <li>Posture</li> <li>Remediation Actions</li> </ul>		Any_Av_Definition_Win	for Windows All	met if	ANY_av_win_def	else AnyAVDefRemediationWi n
Requirements     Gilent Provisioning		Any_AS_Installation_Win	for Windows All	met if	ANY_as_win_inst	else Message Text Only
<ul> <li>Security Group Access</li> </ul>		Any_AS_Definition_Win	for Windows All	metif	ANY_as_win_def	else AnyASDefRemediationWi n
		Any_AV_Installation_Mac	for Mac OSK	met if	ANY_av_mac_inst	else Message Text Only
	4	Any_AV_Definition_Nac	for Mac OSX	metif	ANY_av_mac_def	else AnyAvDetRemediationMa ¢
		Any_AS_Installation_Mac	for MacOSX	met if	ANY_as_mac_inst	eise Message Text Only
		Any_AS_Definition_Mac	for Mac OSX	metif	ANY_as_mac_def	else Message Text Only

Note: In a normal scenario, the File Remediation action can be used (the ISE provides the downloadable file).

14. Navigate to Policy > Posture and use the requirement that you created in the previous step (named file\_requirement) in the posture rules. The only posture rule requires that all Microsoft Windows systems meet the file\_requirement. If this requirement is met, then the station is compliant; if it is not met, then the station is non-compliant.

cisco Identity Services Engine	🟠 Home Opera	tions   • Policy   • Administra	iion   🔻	
🛃 Authentication 🛛 🧕 Authorization	Refine Posture	📷 Client Provisioning 🛛 🚊 Sec	urity Group Access 👘 🤱 Poli	cy Elements
Posture Policy Define the Posture Policy by configuring rules ba	sed on operating system and/or othe	r conditions.		
-				
Status Rule Name	Identity Groups	Operating Systems	Other Conditions	Requirements
posture	If Any	and Windows All		then file_requirement

#### **Periodic Reassessment**

By default, posture is a one-time event. However, there is sometimes a need to periodically check the user compliance and adjust the access to the resources based on the results. This information is pushed via SWISS protocol (NAC Agent) or encoded within the application (Web Agent).

Complete these steps in order to check the user compliance:

1. Navigate to **Administration > Settings > Posture > Reassessments** and enable reassessment globally (per identity group configuration):



2. Create a posture condition that matches all reassessments:

cisco Identity Services Engine	Home Operations   ▼ Policy   ▼ Administration   ▼
🛃 Authentication 🧕 Authorization	🧹 Profiling 👩 Posture 👦 Client Provisioning 🚊 Security Group Access 🛛 🦺 Policy Elements
Dictionaries Conditions Results	
Posture	Dictionary Conditions           Dictionary Simple Condition           * Name reassesment           Description
File Condition	
Registry Condition	
Application Condition	* Attribute * Operator * Value
Service Condition	Session:Agent-Request-Type 😳   Equals 👻 Periodic Reassessment
Compound Condition	Submit Cancel
E AV Compound Condition	
AS Compound Condition	
Dictionary Simple Condition	

3. Create a similar condition that matches only the initial assessments:

cisco Identity Services Engine	Home Operations        Policy        Administration
🚨 Authentication 🛛 🧔 Authorization	Profiling 🔗 Posture 👩 Client Provisioning 📄 Security Group Access 🔒 Policy Elements
Dictionaries Conditions Results	
Posture	Dictionary Conditions List > New Dictionary Condition Dictionary Simple Condition
↓ ■ .	Description
E File Condition	
Registry Condition	
E Application Condition	* Attribute * Operator * Value
Service Condition	Session:Agent-Request-Type 😳 🛛 Equals 🔹 🚽 Initial 🔹
E Compound Condition	Submit Cancel
AV Compound Condition	
AS Compound Condition	
Dictionary Simple Condition	
E Dictionary Compound Condition	

Both of these conditions can be used in the posture rules. The first rule matches only the initial assessments and the second one matches all of the subsequent assessments:

cise cise	ili. co Idei	ntity Services Engine		🏠 Home Ope	rations   •	Policy   👻 Admi	nistration   👻		
4	Authentic	ation 🧕 Authorization	🔀 Profiling	Posture	🐹 Clier	nt Provisioning	Security Group Access	🐴 Policy Elements	
Post Define	ure Pol the Postu	icy re Policy by configuring rules ba	ased on operatio	ng system and/or o	ther conditio	ons.			
	Status	Rule Name		Identity Groups		Operating Systems	Other Conditions		Requirements
		posture_initial	r	Any	and	Windows All	initial	ther	file_requirement
	×	posture_reassessment	lf	Any	and	Windows All	reassessment	ther	file_requirement

## Verify

In order to confirm that your configuration works correctly, ensure that these steps are completed as described:

- 1. The VPN user connects to the ASA.
- 2. The ASA sends a RADIUS-Request and receives a response with the **url-redirect** and the **url-redirect-acl** attributes:

• • 🖌 🔳 🔬 🗁 (	🗎 🗶 😂 🔍 🔶 🌳		[ 💽   Q, Q, Q, 💟   📓 🕅 🚼 😹	8
Filter:		<ul> <li>Expression.</li> </ul>	Clear Apply Save	
No. Source	Destination	Protocol Leng	th Info	
1 192.168.111.10	10.48.66.74	RADIUS	12 Access-Request(1) (id=46, l=270)	
2 10.48.66.74	192.168.111.10	RADIUS	11 Access-Accept(2) (id=46, 1=269)	
1				
Frame 2: 311 bytes on	wire (2488 bits), 3	11 bytes capt	red (2488 bits)	
Ethernet II, Src: Vmw	are_c0:00:03 (00:50:	56:c0:00:03),	Dst: Vmware_e8:ef:25 (00:0c:29:e8:c	ef:25)
Internet Protocol Ver	sion 4, Src: 10.48.6	6.74 (10.48.6	.74), Dst: 192.168.111.10 (192.168.	.111.10)
User Datagram Protoco	l, Src Port: sightli	ne (1645), Ds	Port: 54459 (54459)	
Radius Protocol				
Code: Access-Accept Packet identifier: Length: 269 Authenticator: bef2 [This is a response [Time from request:	(2) 0x2e (46) 2fb479a10c1e2dea5093 to a request in fra 0.059399000 seconds	7882e0d4 10 11		
* Attribute Value Pai	rs			
▷ AVP: l=7 t=User-M	lame(1): cisco			
▷ AVP: l=40 t=State	(24): 52656175746853	65737369616e3	63306138373030613030	
> AVP: l=50 t=Class	(25): 434143533a6330	6138373030613	30303064303030353262	
* AVP: 1=33 t=Vende	or-Specific(26) vmcis	coSystems(9)		
▷ VSA: l=27 t=Cisc	o-AVPair(1): url-red	irect-acl=red	rect	
✓ AVP: l=119 t=Vend	for-Specific(26) v=ci	scoSystems(9)		
▷ VSA: l=113 t=Cis	co-AVPair(1): url-re	direct=https:	/ise2.test-cisco.com:8443/guestport	ial/gateway?sessionId=c0a8700a0000d00052b1b1bc&action=cpp

3. The ISE logs indicate that the authorization matches the posture profile (the first log entry):

×	à	#ACSACL#-IP-P		ASA9-2		Compliant	ise2
×	-Q		192.168.10.67	ASA9-2	ASA92-compliant	Compliant	ise2
0	0	0 cisco	192.168.10.67			Compliant	ise2
×	0	cisco	192.168.10.67	ASA9-2	ASA92-posture	User Identity Gro Pending	ise2

4. The ASA adds a redirect to the VPN session:

<#root>

aaa\_url\_redirect

```
: Added url redirect:https://ise2.test-cisco.com:8443/
guestportal/gateway?sessionId=c0a8700a0000900052b840e6&action=cpp
acl:redirect for
```

10.10.10.10

5. The status of the VPN session on the ASA shows that the posture is required and redirects the HTTP traffic:

<#root>

ASA#

show vpn-sessiondb detail anyconnect

: 9 Index Username : cisco Assigned IP : 10.10.10.10 Public IP : 10.147.24.61 Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel License : AnyConnect Essentials Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)RC4 DTLS-Tunnel: (1)AES128 : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1 Hashing Bytes Rx : 16497 Bytes Tx : 16077 Pkts Rx Pkts Tx : 43 : 225 Pkts Tx Drop : 0 Pkts Rx Drop : 0 Group Policy : GP-SSL Tunnel Group : RA Login Time : 14:55:50 CET Mon Dec 23 2013 Duration : 0h:01m:34s Inactivity : 0h:00m:00s VLAN Mapping : N/A VLAN : none Audt Sess ID : c0a8700a000900052b840e6 Security Grp : 0 AnyConnect-Parent Tunnels: 1 SSL-Tunnel Tunnels: 1 DTLS-Tunnel Tunnels: 1 AnyConnect-Parent: Tunnel ID : 9.1 Public IP : Public IP : 10.147.24.61 Encryption : none Hashing : none TCP Src Port : 50025 TCP Dst Port : 443 Auth Mode : userPassword Idle Time Out: 30 Minutes Idle TO Left : 28 Minutes Client OS : win Client Type : AnyConnect Client Ver : Cisco AnyConnect VPN Agent for Windows 3.1.02040 Bytes Tx : 5204 Bytes Rx : 779 Pkts Tx : 4 Pkts Rx : 1 Pkts Tx Drop : 0 Pkts Rx Drop : 0 SSL-Tunnel: : 9.2 Tunnel ID Assigned IP : 10.10.10.10 Public IP : 10.147.24.61 Encryption : RC4 Hashing : SHA1 Encapsulation: TLSv1.0 TCP Src Port : 50044 TCP Dst Port : 443 Auth Mode : userPassword Idle Time Out: 30 Minutes Idle TO Left : 28 Minutes Client OS : Windows

Client Type : SSL VPN Client Client Ver : Cisco AnyConnect VPN Agent for Windows 3.1.02040 Bytes Tx : 5204 Bytes Rx : 172 Pkts Rx : 2 Pkts Tx : 4 Pkts Tx Drop : 0 Pkts Rx Drop : 0 DTLS-Tunnel: Tunnel ID : 9.3 Assigned IP : 10.10.10.10 Public IP : 10.147.24.61 Encryption : AES128 Hashing : SHA1 Encapsulation: DTLSv1.0 UDP Src Port : 63296 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 3.1.02040 : 5669 Bytes Rx : 18546 Bytes Tx Pkts Tx : 35 : 222 Pkts Rx Pkts Tx Drop : 0 Pkts Rx Drop : 0 ISE Posture: Redirect URL : https://ise2.test-cisco.com:8443/guestportal/gateway? sessionId=c0a8700a0000900052b840e6&action=cpp

6. The client that initiates the HTTP traffic that matches the redirect ACL is redirected to the ISE:

<#root>
aaa\_url\_redirect: Created proxy for 10.10.10.10
aaa\_url\_redirect:
Sending url redirect
:https://ise2.test-cisco.com:8443/
guestportal/gateway?sessionId=c0a8700a0000900052b840e6&action=cpp
for
10.10.10.10

7. The client is redirected to the ISE for posture:

Redirect ACL : redirect

	https://ise2.test-cisco.com:0443/au	ch/CppSetup.action?session=c0a0700a00052b0056c&cs=Windows T (A) 🏠 🔻 🤁 🚺 🜉 - AVC Secure Search 🛛 🔎 🐥 🏫	<b>•</b>
	cisco Client Pr	ovisioning Portal	
ľ	Cisco Identity Se Engine Network	Ervices Determining prior Cisco Agent Installation on device28 second(s). Security Warning	
	Notice	Do you want to Continue? The connection to this website is untrusted. Website: https://ise2.test-cisco.com:8443	
l		Note: The certificate is not valid and cannot be used to verify the identity of this website. This application will be blocked in a future Jave security update because the JAR file manifest does not contain the Permissions attribute. Please contact the Publisher for more information. More information	
ļ		This application will be blocked in a future Java security update because the JAR file manifest does not contain the Permissions attribute. Please contact the Publisher for more information. Nore information	

8. The NAC Agent is installed. After the NAC Agent is installed, it downloads the posture rules via SWISS protocol and performs checks in order to determine compliance. The posture report is then sent to the ISE.

🧭 Cisco NAC Agent	
cisco NAC Agent	About
Full Network Access	
Your device conforms with all the security policies for this protected network	

9. The ISE receives the posture report, reevaluates the authorization rules, and (if needed) changes the authorization status and sends a CoA. This can be verified in the **ise-psc.log**:

```
<#root>
cisco.cpm.posture.runtime.PostureHandlerImpl -:cisco:c0a8700a0000900052b840e6
:::-
Decrypting report
cisco.cpm.posture.runtime.PostureManager -:cisco:c0a8700a0000900052b840e6
:::- U
ser cisco belongs to groups NAC Group:NAC:IdentityGroups:User Identity
Groups:Employee
```

```
,NAC Group:NAC:IdentityGroups:An
cisco.cpm.posture.runtime.PostureManager -:cisco:c0a8700a0000900052b840e6
:::-
Posture report token for endpoint mac 08-00-27-CD-E8-A2 is Healthy
cisco.cpm.posture.runtime.PostureManager -:cisco:c0a8700a0000900052b840e6
:::-
Posture state is compliant for endpoint with mac 08-00-27-CD-E8-A2
cisco.cpm.posture.runtime.PostureCoA -:cisco:c0a8700a0000900052b840e6
:::-
Posture CoA is triggered for
endpoint [null] with session
[c0a8700a0000900052b840e6]
```

10. The ISE sends a RADIUS CoA that includes the **session\_id** and the DACL name that permits full access:

No.	Source	Destination	Protocol	Length	Info	
	7 10.48.66.74	192.168.111.10	RADIUS	231	CoA-Request(43) (id=	11, l=189)
;	8 192.168.111.10	10.48.66.74	RADIUS	62	CoA-ACK(44) (id=11,	l=20)
4						
▶ Fi	rame 7: 231 bytes on w	/ire (1848 bits), 23	1 bytes	capture	d (1848 bits)	
▶ E1	thernet II, Src: Vmwar	re_c0:00:03 (00:50:5	6:c0:00:	03), Ds	t: Vmware_e8:ef:25 (	00:0c:29:e8:ef:25)
⊳ Ir	nternet Protocol Versi	ion 4, Src: 10.48.66	.74 (10.	48.66.7	4), Dst: 192.168.111	.10 (192.168.111.10)
≥ Us	ser Datagram Protocol,	Src Port: 44354 (4	4354), D	st Port	: mps-raft (1700)	
⇒ Ré	adius Protocol					
	Code: CoA-Request (43	)				
	Packet identifier: 0x	b (11)				
	Length: 189					
	Authenticator: d20817	c6ca828ce7db4ee54f1	5177b8d			
	[The response to this	request is in frame	81			
~	Attribute Value Pairs					
	> AVP: l=6 t=NAS-IP-/	Address(4): 10.147.2	4.61			
	> AVP: l=15 t=Calling	g-Station-Id(31): 19	2.168.10	.67		
	> AVP: l=6 t=Event-T:	imestamp(55): Dec 18	, 2013 1	5:32:10	.000000000 CET	
	AVP: l=18 t=Message	e-Authenticator(80):	lee29f1	d83e5f3	aa4934d60aa617ebeb	
	▼ AVP: l=75 t=Vendor	-Specific(26) v=cisc	oSystems	(9)		
	▹ VSA: l=69 t=Cisco-	AVPair(1): ACS:Cisco	Secure -	Defined	·ACL=#ACSACL#-IP-PERM	AIT_ALL_TRAFFIC-51ef7db1
	▼ AVP: l=49 t=Vendor	-Specific(26) v=cisc	oSystems	(9)		
	▹ VSA: l=43 t=Cisco-	AVPair(1): audit-se	ssion-id	=c0a870	0a0000d00052b1b1bc	

This is reflected in the ISE logs:

- The first log entry is for the initial authentication that returns the posture profile (with redirection).
- The second log entry is populated after the compliant SWISS report is received.
- The third log entry is populated when the CoA is sent, along with the confirmation (described as Dynamic Authorization Succeeded).
- The final log entry is created when the ASA downloads the DACL.

1	<u>o</u>	#ACSACL#-IP	e.	ASA9-2		Co	mpliant is	ie2
×	à		192.168.10.67	ASA9-2	ASA92-compliant	Co	mpliant is	ie2
 0	à	0 cisco	192.168.10.67			Co	mpliant is	e2
×	à	cisco	192.168.10.67	ASA9-2	ASA92-posture	User Identity Gro Pe	nding is	e2

11. Debugs on the ASA show that the CoA is received and the redirect is removed. The ASA downloads the DACLs if needed:

<#root>

ASA#

Received RAD\_COA\_REQUEST

RADIUS packet decode (CoA-Request)

 Radius: Value (String) =

 41 43 53 3a 43 69 73 63 6f 53 65 63 75 72 65 2d
 | ACS:CiscoSecure 

 44 65 66 69 6e 65 64 2d 41 43 4c 3d 23 41 43 53
 | Defined-ACL=#ACS

 41 43 4c 23 2d 49 50 2d 50 45 52 4d 49 54 5f 41
 | ACL#-IP-PERMIT\_A

 4c 4c 5f 54 52 41 46 46 49 43 2d 35 31 65 66 37
 | LL\_TRAFFIC-51ef7

 64 62 31
 | db1

Got AV-Pair with value audit-session-id=c0a8700a0000900052b840e6 Got AV-Pair with value ACS:CiscoSecure-Defined-ACL=

```
#ACSACL#-IP-PERMIT_ALL_TRAFFIC-51ef7db1
```

aaa\_url\_redirect:
 Deleted url redirect
 for
10.10.10.10

12. After the VPN session, Cisco has the DACL applied (full access) for the user:

```
Protocol
            : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License
            : AnyConnect Essentials
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)RC4 DTLS-Tunnel: (1)AES128
            : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Hashing
Bytes Tx
            : 94042
                                    Bytes Rx : 37079
Pkts Tx
            : 169
                                    Pkts Rx
                                                : 382
Pkts Tx Drop : 0
                                    Pkts Rx Drop : 0
Group Policy : GP-SSL
                                    Tunnel Group : RA
Login Time : 14:55:50 CET Mon Dec 23 2013
Duration
            : 0h:05m:30s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A
                                    VLAN
                                                : none
Audt Sess ID : c0a8700a000900052b840e6
Security Grp : 0
AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1
AnyConnect-Parent:
 Tunnel ID : 9.1
 Public IP
              :
10.147.24.61
 Encryption : none
                                      Hashing : none
 TCP Src Port : 50025
                                      TCP Dst Port : 443
 Auth Mode : userPassword
 Idle Time Out: 30 Minutes
                                      Idle TO Left : 24 Minutes
 Client OS : win
 Client Type : AnyConnect
 Client Ver : Cisco AnyConnect VPN Agent for Windows 3.1.02040
 Bytes Tx
                                      Bytes Rx : 779
              : 5204
 Pkts Tx
              : 4
                                      Pkts Rx
                                                   : 1
 Pkts Tx Drop : 0
                                      Pkts Rx Drop : 0
SSL-Tunnel:
 Tunnel ID
              : 9.2
 Assigned IP :
 10.10.10.10
          Public IP
                    :
10.147.24.61
                                              : SHA1
 Encryption : RC4
                                      Hashing
 Encapsulation: TLSv1.0
                                      TCP Src Port : 50044
 TCP Dst Port : 443
                                      Auth Mode : userPassword
 Idle Time Out: 30 Minutes
                                      Idle TO Left : 24 Minutes
 Client OS : Windows
 Client Type : SSL VPN Client
 Client Ver : Cisco AnyConnect VPN Agent for Windows 3.1.02040
 Bytes Tx
              : 5204
                                      Bytes Rx : 172
 Pkts Tx
                                      Pkts Rx
                                                   : 2
              : 4
 Pkts Tx Drop : 0
                                      Pkts Rx Drop : 0
  Filter Name :
```

#ACSACL#-IP-PERMIT\_ALL\_TRAFFIC-51ef7db1

```
DTLS-Tunnel:
 Tunnel ID
              : 9.3
 Assigned IP :
10.10.10.10
         Public IP
                    :
10.147.24.61
 Encryption : AES128
                                      Hashing : SHA1
 Encapsulation: DTLSv1.0
                                      UDP Src Port : 63296
 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 3.1.02040
 Bytes Tx : 83634
Pkts Tx : 161
                                       Bytes Rx : 36128
                                       Pkts Rx
                                                  : 379
                                      Pkts Rx Drop : 0
 Pkts Tx Drop : 0
  Filter Name :
#ACSACL#-IP-PERMIT_ALL_TRAFFIC-51ef7db1
```

**Note**: The ASA always removes the redirect rules, even when the CoA does not have any DACL attached.

## Troubleshoot

This section provides information you can use in order to troubleshoot your configuration.

### **Debugs on the ISE**

Navigate to **Administration > Logging > Debug Log Configuration** in order to enable debugs. Cisco recommends that you enable temporary debugs for:

- SWISS
- Nonstop Forwarding (NSF)
- NSF-Session
- Provision
- Posture

Enter this command in the CLI in order to view the debugs:

<#root> ise2/admin# show logging application ise-psc.log tail count 100

Navigate to Operations > Reports > ISE Reports > Endpoints and Users > Posture Details Assessment

### in order to view the posture reports:

alah									242   abox	Legent   Feelbeck D	
CIDED Identity Services Engine	🚖 Home Oper	ntiens   🔻	Policy	💌 Admini	stration   +					84	up.A
🔮 Authentications 📑 Reports 📷 End	point Protection Genice	Tota	letih port								
Report Selector	Posture Detail Asses	sment								🔶 Favoita 🛛 🍙 Export	
Favorites										Generated at 201	13-12-
ISE Reports	From 12/23/2013 12:08:0	0 AM to 12	15255812	07:56:58 PM						Page << 1 >> Parents 1 to	τ
<ul> <li>Auth Dervices Status</li> </ul>	Logged At	51st us	Detail	PRA	Identity	Endpoint ID	P Address	Drépoint DS	Agent	Message	
6 reports	2013-12-23 15:21:34.9	-	.0	continue	cisco	08:01:27:CD:68:A	10.147.24.92	Windows 7 Enterprise 64-bit	CISCO RAE A	Received a posture report from an end	point
Ouployment Status     T1 reports	2013-12-23 15:08:58.3		.o	continue	cisco	08/08/27/CD/EB/A	10.147.24.92	Windows 7 Enterprise 64-bit	Cisco NAC A	Received a posture report from an end	point
+ Endpoint's and Users	2013-12-23 14:59:34.3		.0	continue	cisco	08:01:27:CD:68:A	10.147.24.92	Windows 7 Enterprise 64-bit	CISCO RAC A	Received a posture report from an end	poirs
Client Provisioning	2013-12-23 14:55:28.6	٠	.0	NA	cisco	08/08/27/CD/E8/A	10.147.24.92	Windows 7 Enterprise 64-bit	Cisco NAC A	Received a posture report from an end	poirt
Current Active Sessions	2013-12-23 14:44:45.0	۰	.0	NA	cisco	08:01:27:CD:68:A	10.147.24.92	Windows 7 Enterprise 64-bit	CISCO NAC A	Received a posture report from an end	ipoirs
Guest Activity	2013-12-23 13:34:30.3	۰	.o	NA	cisco	08/08/27/7F/SF/6	10.147.24.92	Windows 7 Utimate 64-bit	Cisco NAC A	Received a posture report from an end	poirt
direct Annual and	2013-12-23 13:27:10.3	٠	.0	NA	cisco	08:08:27:77:57:6	10.147.24.92	Windows 7 Utimate 64-bit	CISCO NAC A	Received a posture report from an end	ipoirs
Quest Accounting											
Guest Spotsor Happing											
Guest Spotsor Summary											
Endpoint Protection Service Audit											
Mobile Device Hanagement											
Posture Detail Assessment Pitters • Time Range Today •											

On the Posture More Detail Assessment page, there is policy name with a requirement name that is displayed, along with the results:

#### **Posture More Detail Assessment**

Time Range:	From 12/23/2013 12:00:00 AM to 12/23/2013 03:57:31 PM
Generated At:	2013-12-23 15:57:31.248

Client Details						
Username:	cisco					
Mac Address:	08:00:	27:CD:E8:A2				
IP address:	10.147	.24.92				
Session ID:	c0a870	00a0000b00052b	846c0			
Client Operating System	n: Window	vs 7 Enterprise 64	l-bit			
Client NAC Agent:	Cisc o N	IAC Agent for Win	dows 4.9.	0.1013		
PRA Enforcement:	1					
CoA:	Receive	ed a posture repor	t from an	endpoint		
PRA Grace Time:						
PRA Interval:	240					
PRA Action:	continu	16				
User Agreement Statu:	s: NotEna	abled				
System Name:	MGARC	ARZ-WS01				
System Domain:	cisco.c	om				
System User:	mgarca	arz				
User Domain:	CISCO					
AV Installed:	McAfee	VirusScan Enterp	orise;8.8.0	0.975;7227;10/	13/2013;McAfeeAV	Cisco Security Agent;6.0.2.130;;;CiscoAV
AS Installed:	Window	vs Defender; 6.1.7	600.1638	35;1.95.191.0;1	1/19/2010;Microso	ftAS
Posture Report						
Posture Status:	Compli	ant				
Logged At:	2013-1	2-23 15:21:34.90	)2			
Posture Policy Details						
Belles		E.C.	0	Deres d	Collect.	
Policy	Name	Enforcement	Statu	Passed	Failed	Skipped Conditions
posture_initial	file_require	Mandatory	10.000	file_condition	1	

## **Debugs on the ASA**

You can enable these debugs on the ASA:

- debug aaa url-redirect
- debug aaa authorization
- debug radius dynamic-authorization
- debug radius decode
- debug radius user cisco

### **Debugs for the Agent**

For the NAC Agent, it is possible to gather the debugs with the Cisco Log Packager, which is initiated from the GUI or with the CLI; use CCAAgentLogPackager.app.

🛨 Cisco Log Pa	ackager v1.7.0.11	- • •	
cisco.	Cisco Log Packager		
	Cisco Log Packager collects information for product support requests. The information is stored in a ZIP archive that can be protected by a password.		
	Click the <collect data=""> button to start the information collection.</collect>		
Protect dat	ta with following password:		
Collect Da	ata Show Log Locate Report File Cancel	Exit	

 $\mathcal{P}$  Tip: You can decode the results with the Technical Assistance Center (TAC) tool.

In order to retrieve the logs for the Web Agent, navigate to these locations:

- C: > Document and Settings > <*user*> > Local Settings > Temp > webagent.log (decoded with the TAC tool)
- C: > Document and Settings > <user> > Local Settings > Temp > webagentsetup.log

**Note**: If the logs are not in these locations, then verify the **TEMP Environment** variable.

### NAC Agent Posture failure

If the posture fails, the user is presented with the reason:



The user is then allowed remediation actions if they are configured:

cisco Client F	Provisioning Portal	
Information	Cisco NAC Agent Cisco Cisco NAC Agent Cisco Cisco NAC Agent Temporary Network Access There is at least one mandatory requirement failing. You are required to up before you can access the network. Repair Show Details Continue System Check Complete	Cancel About OO:O3:58 left

## **Related Information**

- <u>Cisco ASA 5500 Series Configuration Guide with the CLI, 8.4 and 8.6</u>
- <u>CLI Book 3: Cisco ASA Series VPN CLI Configuration Guide, 9.1</u>
- <u>Cisco Technical Support & Downloads</u>