Configure ASA VPN Posture with ISE

Contents

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.

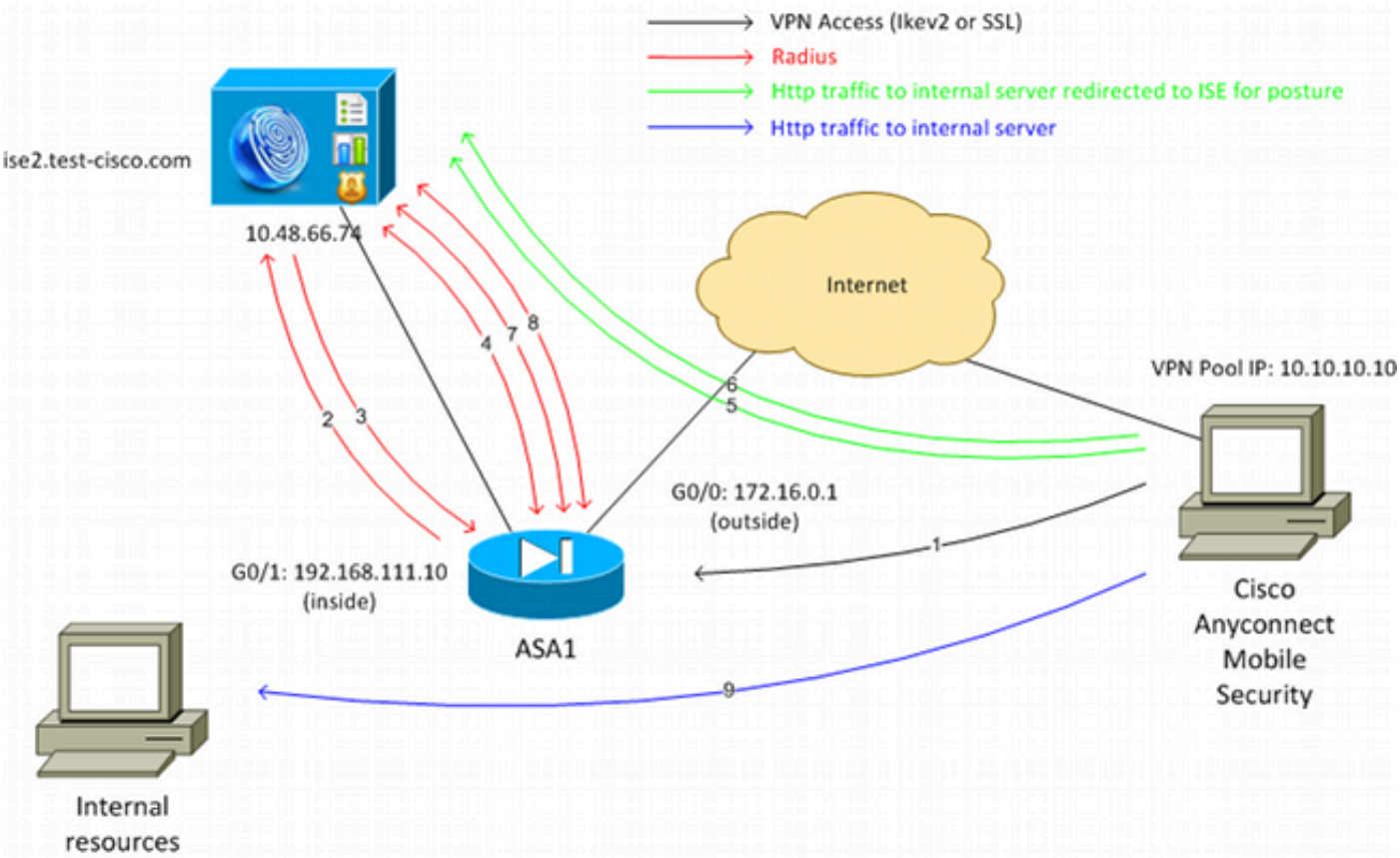
Background Information

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.

Note: This flow model differs from most scenarios that use RADIUS CoA. For wired/wireless 802.1x authentications, RADIUS CoA does not include any attributes. It only triggers the second authentication in which all attributes, such as DACL, are attached. For the ASA VPN posture, there is no second authentication. All of the the attributes are returned in the RADIUS CoA. The VPN session is active and it is not possible to change most of the VPN user settings.

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 255.255.255.0


!
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
```

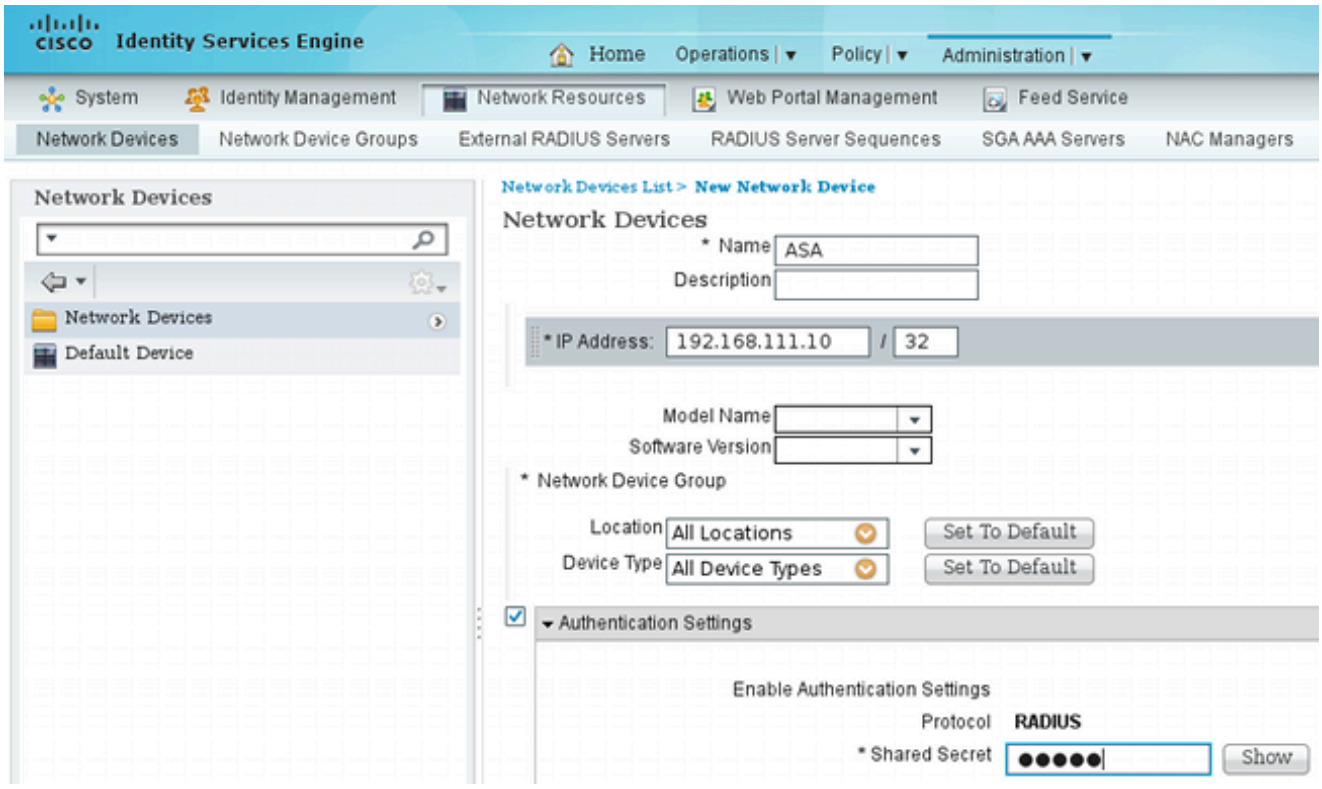
ASA accounting mode:

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”.

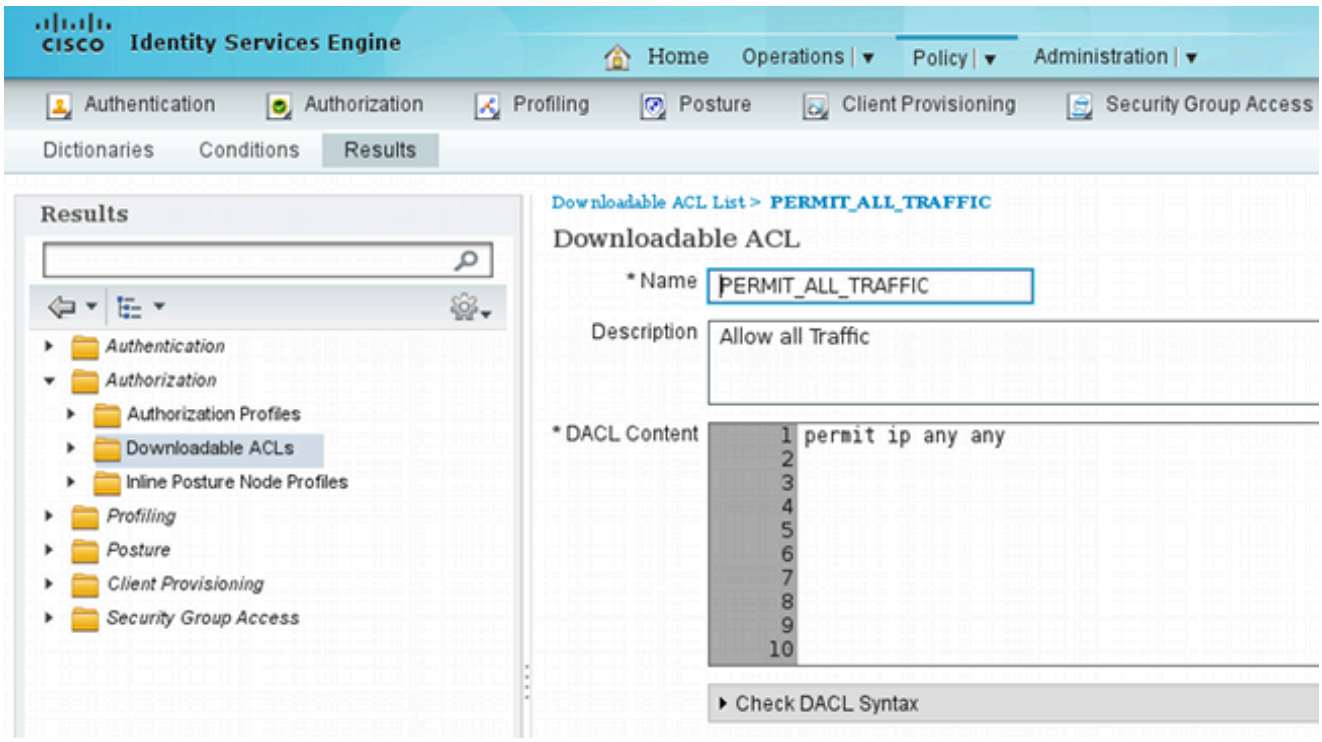
ISE

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:

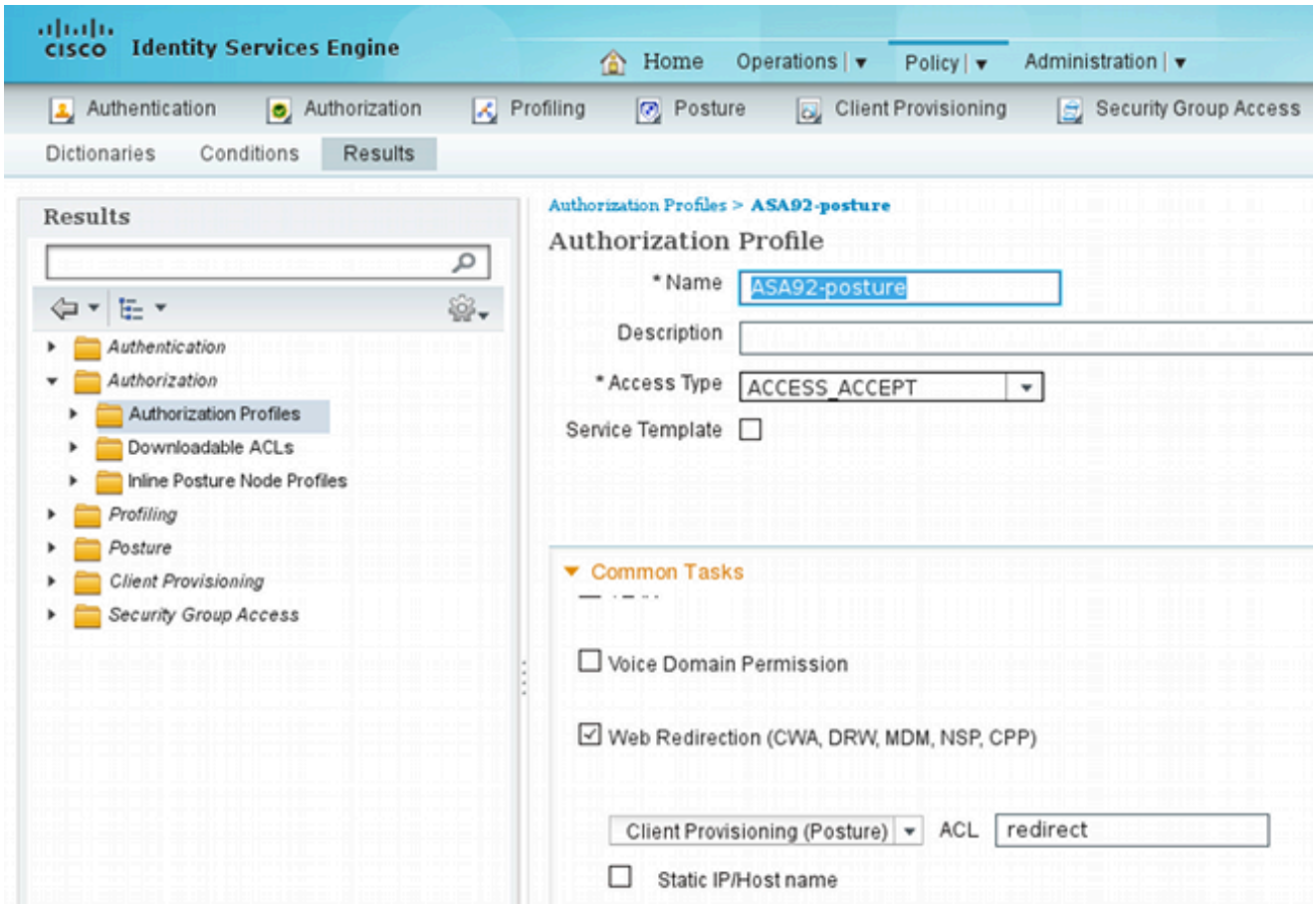


2. Navigate to **Policy > Results > Authorization > Downloadable ACL** and configure the DACL so that it permits full access. The default ACL configuration permits all IP traffic on the ISE:

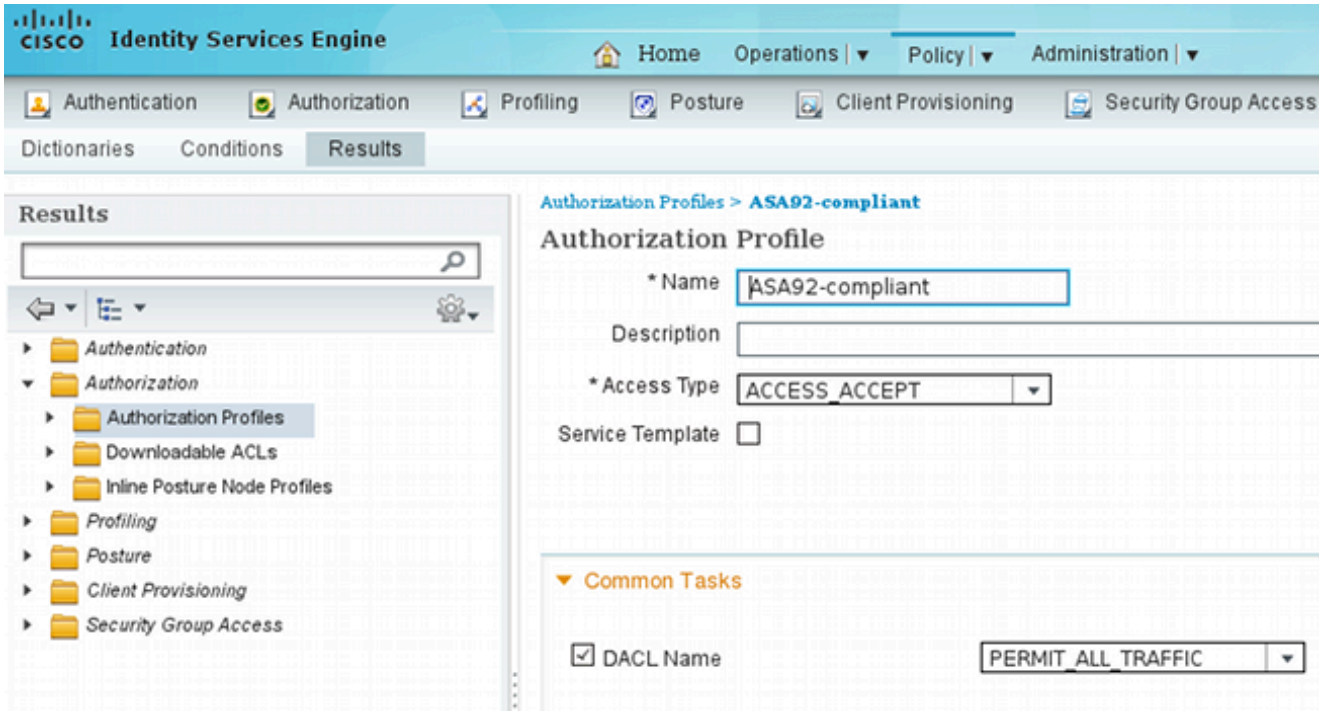


3. Configure a similar ACL that provides limited access (for non-compliant users).

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):



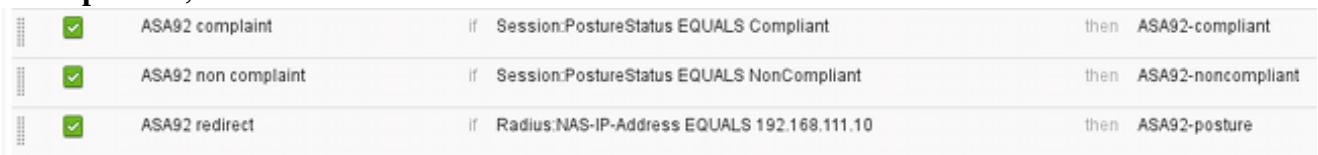
5. Configure the Authorization Profile named **ASA92-compliant**, which must only return the DACL named **PERMIT_ALL_TRAFFIC** that provides full access for the compliant users:



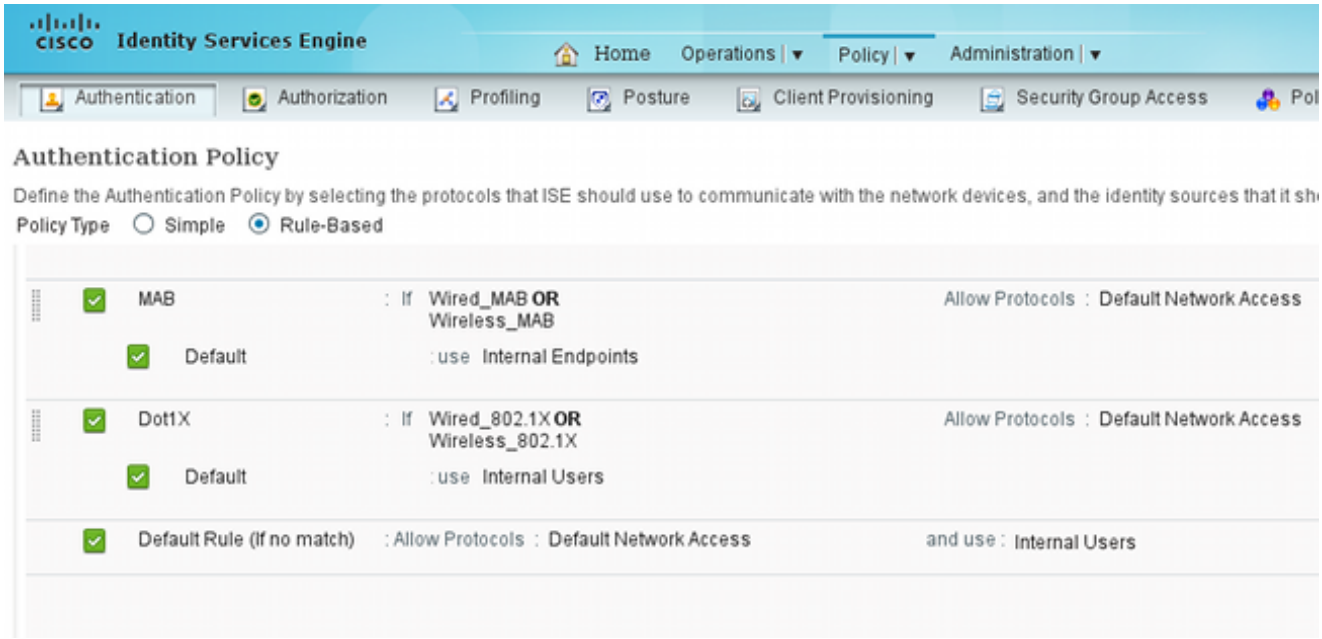
6. Configure a similar Authorization Profile named **ASA916-noncompliant**, which must return the DACL with limited access (for non compliant users).

7. Navigate to **Policy > Authorization** and configure the Authorization Rules:

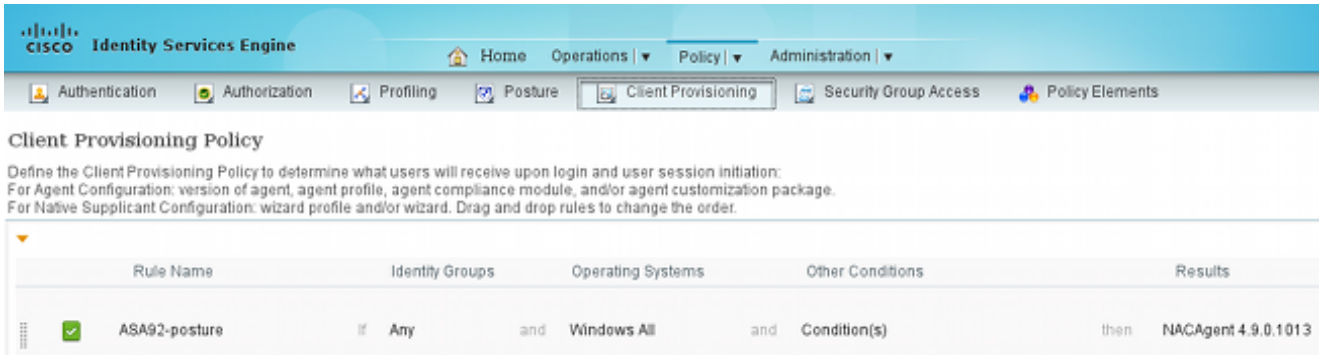
- Create a rule that allows full access if the posture results are compliant. The result is the authorization policy **ASA916-compliant**.
- Create a rule that allows limited access if the posture results are non-compliant. The result is the authorization policy **ASA916-noncompliant**.
- Ensure that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



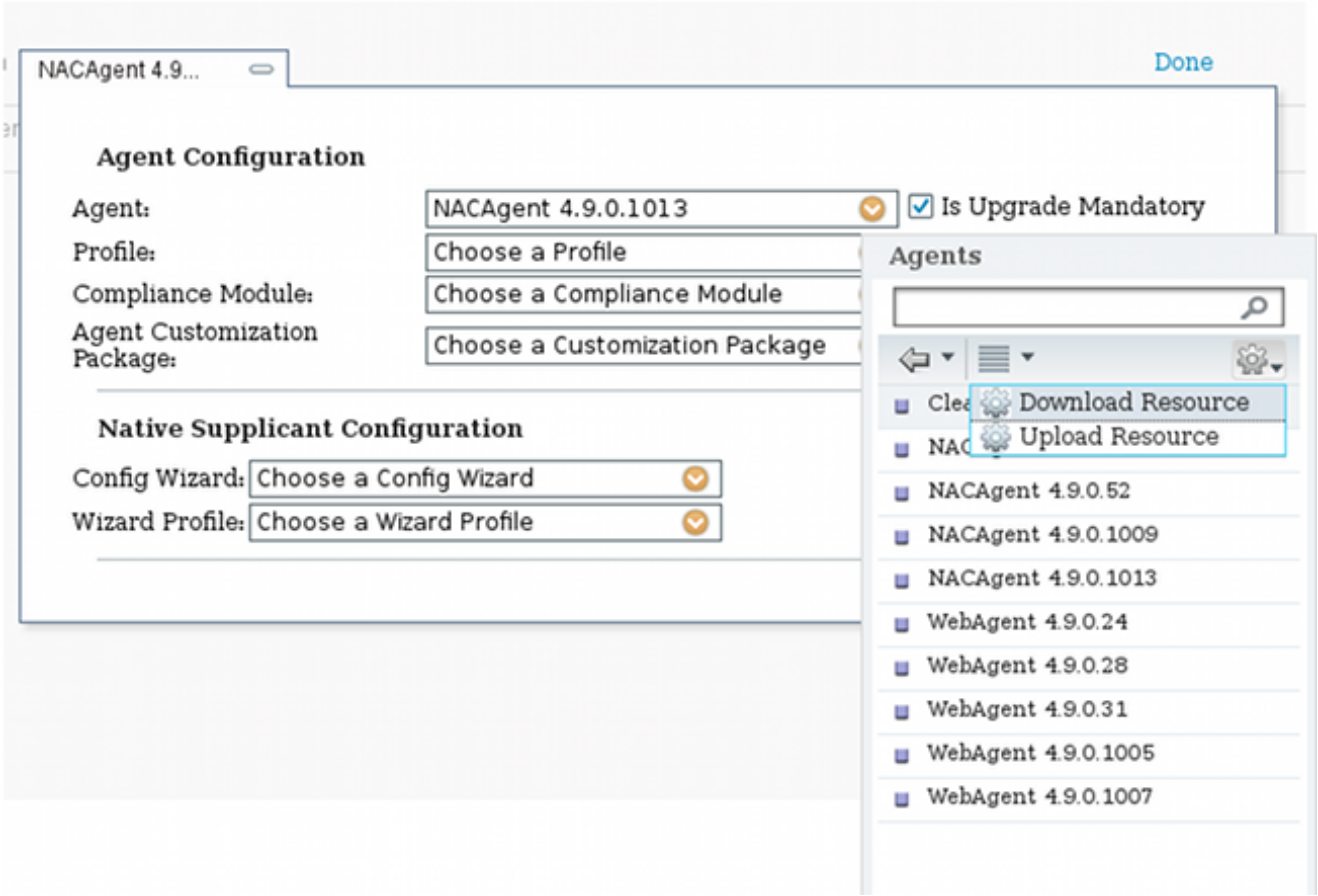
8. The default authentication rules check the user name in the internal identity store. If this must be changed (checked in the Active Directory (AD), for example), then navigate to **Policy > Authentication** and make the change:



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:



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

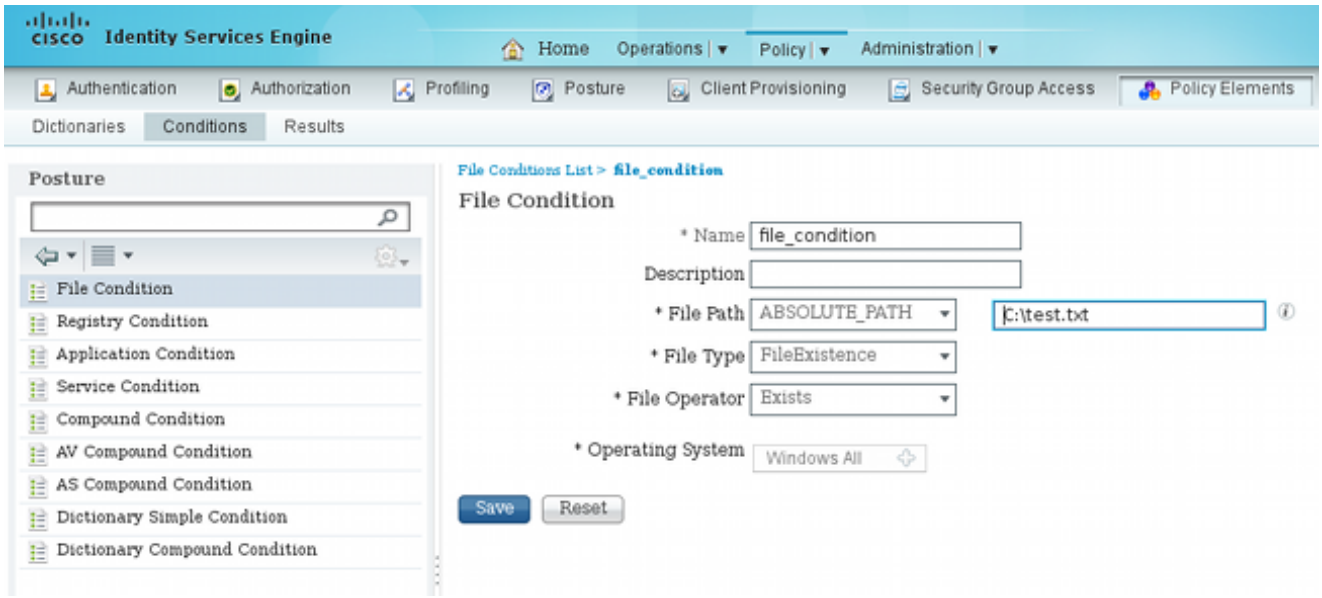


10. If necessary, you can navigate to **Administration** > **System** > **Settings** > **Proxy** and configure the proxy for the ISE (to access the Internet).

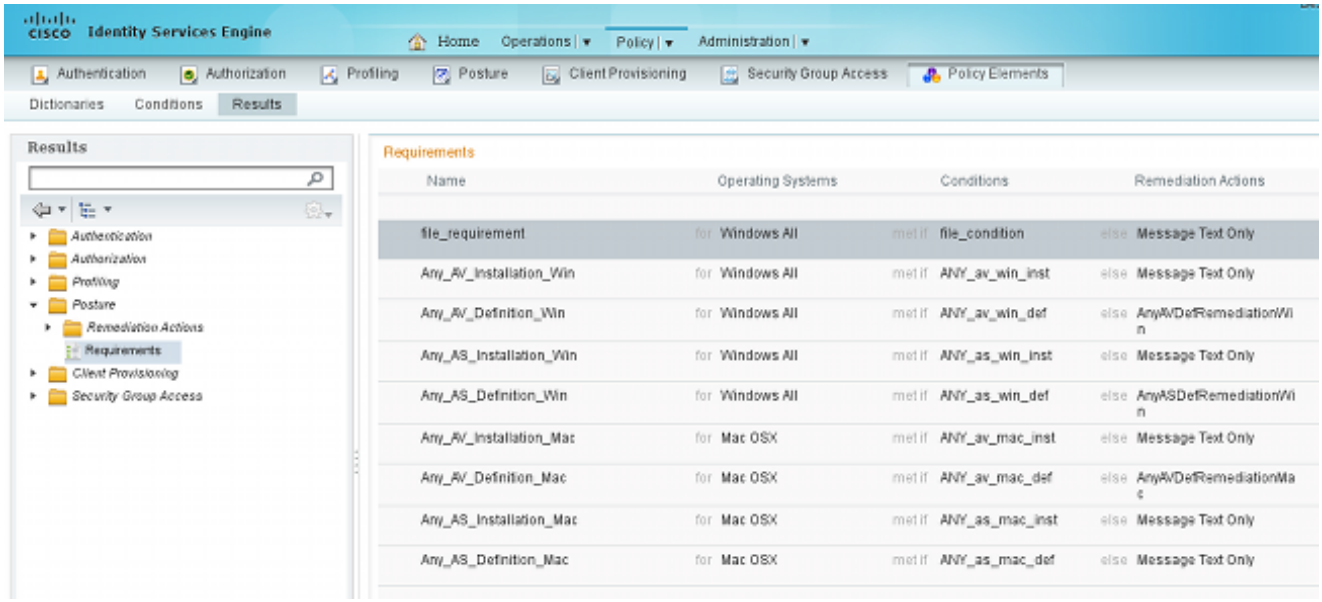
11. Configure the posture rules, which verify the client configuration. You can configure rules that check:

    - **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:

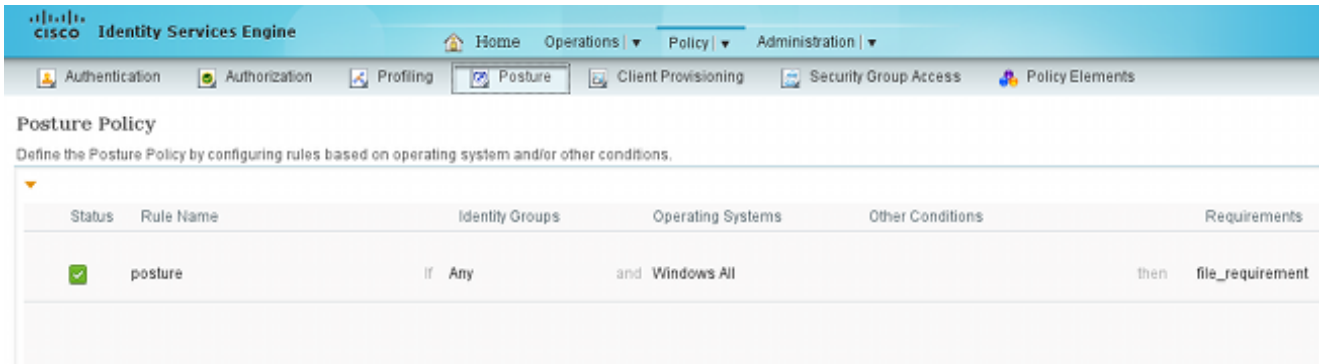


13. Navigate to **Policy > Results > Posture > Requirements** and create a requirement. This requirement must be met when the previous condition is satisfied. If it is not, then remediation action is executed. There can be many types of remediation actions available, but in this example, the simplest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



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.

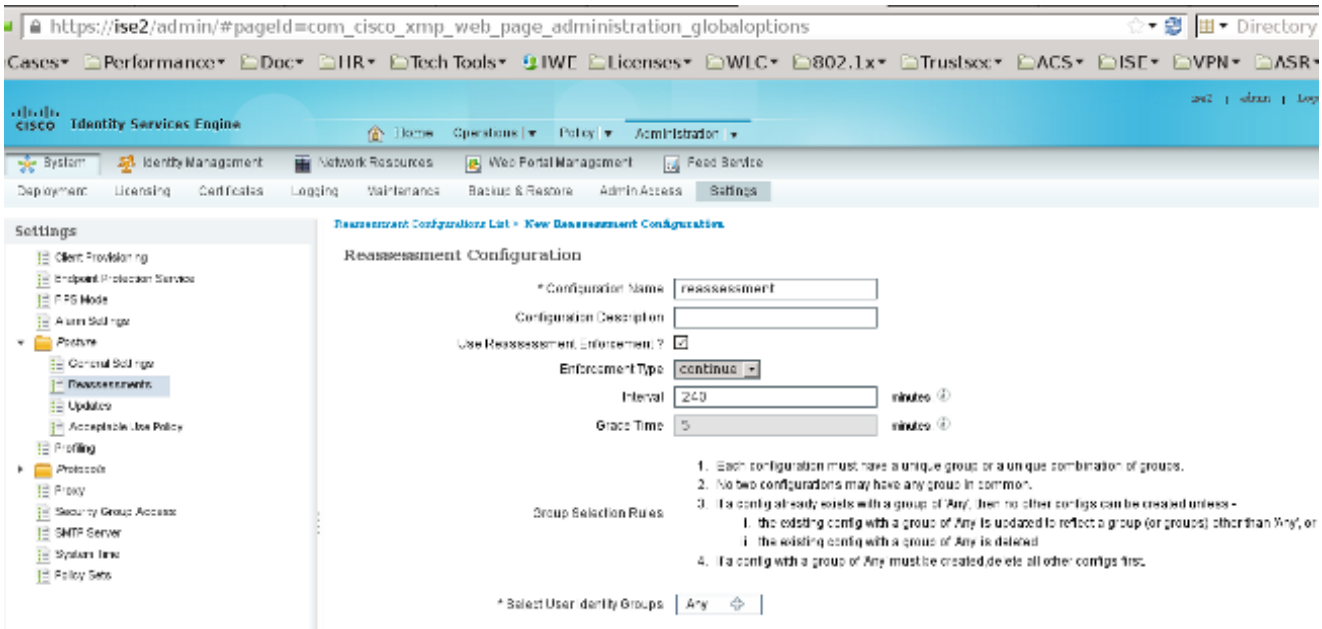


Periodic Reassessment

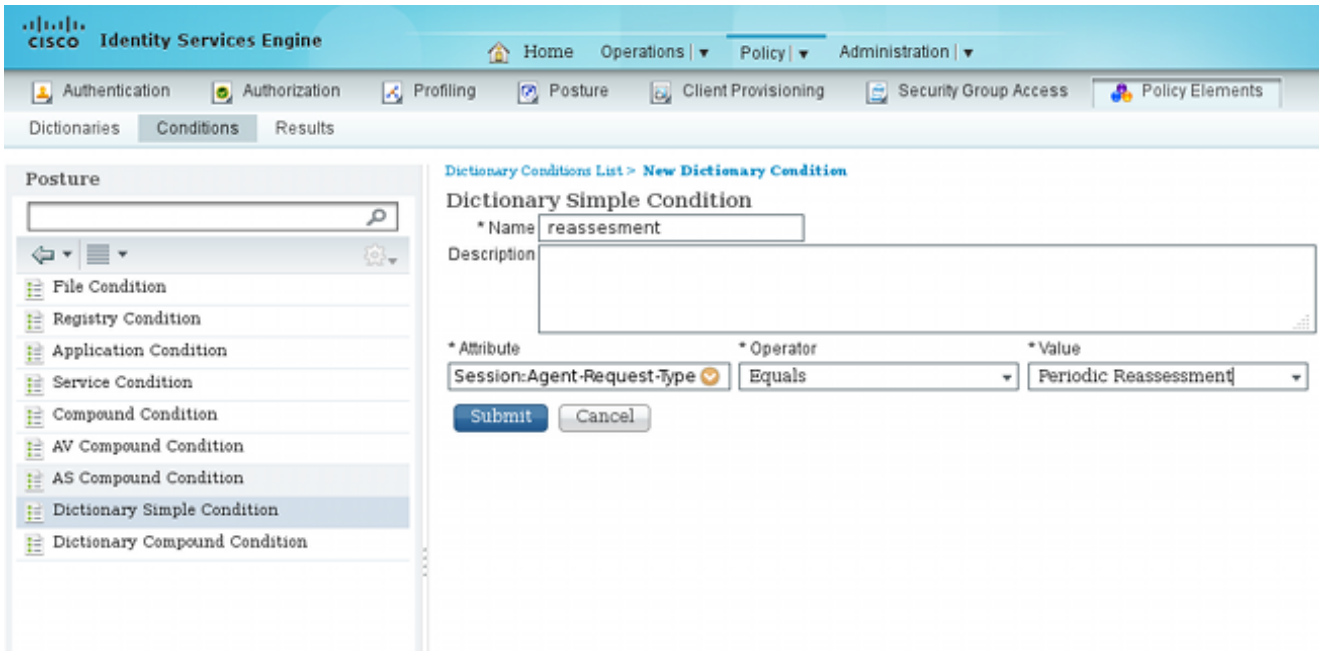
By default, posture is a one-time event. However, there is sometimes a need to periodically check the user compliance and adjust the access to the resources based on the results. This information is pushed via SWISS protocol (NAC Agent) or encoded within the application (Web Agent).

Complete these steps in order to check the user compliance:

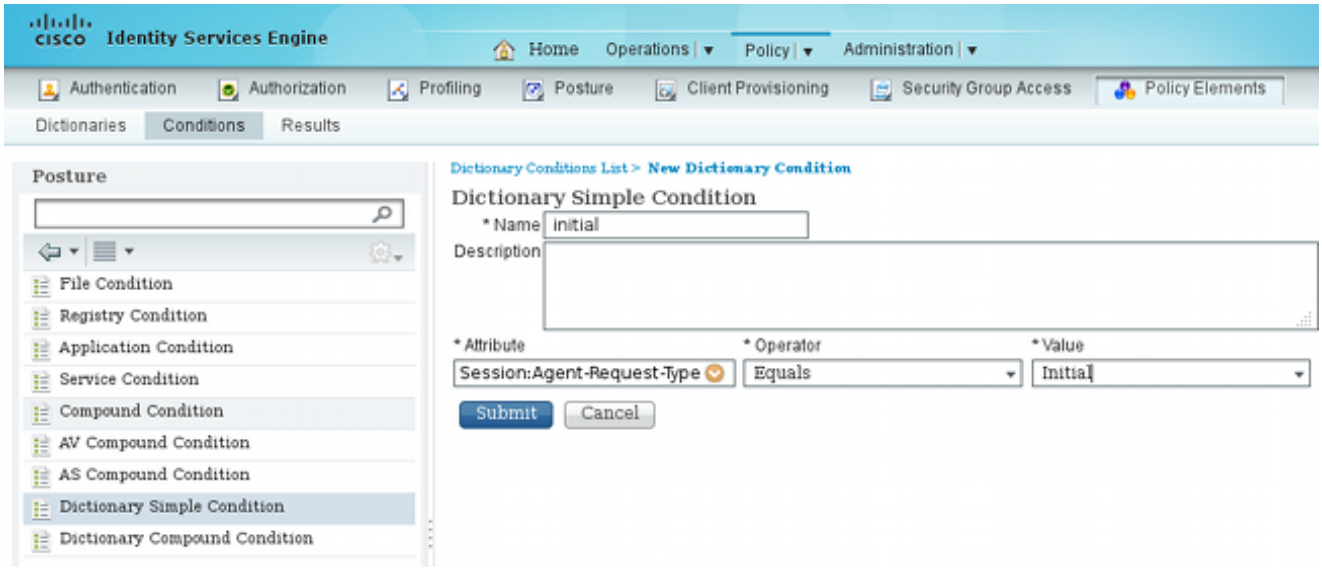
1. Navigate to **Administration** > **Settings** > **Posture** > **Reassessments** and enable reassessment globally (per identity group configuration):



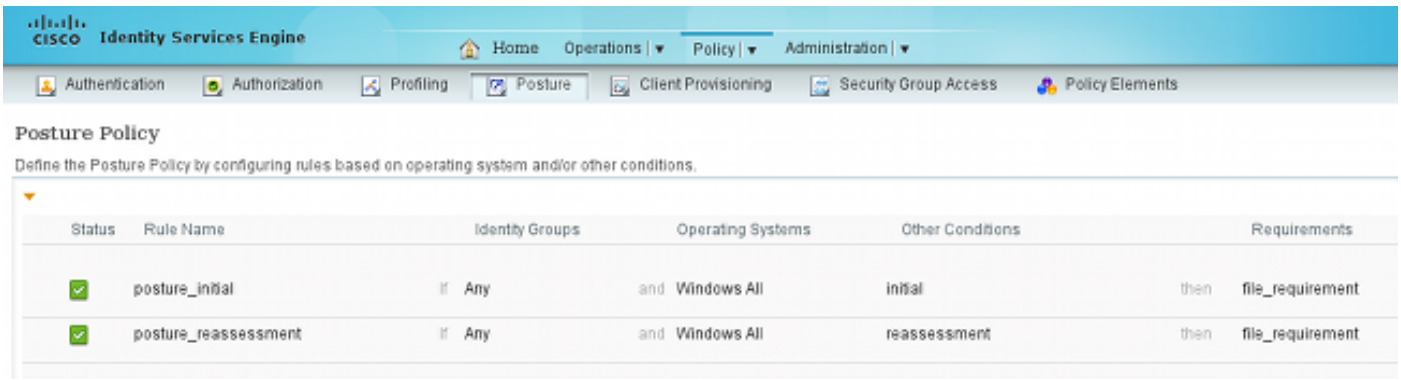
2. Create a posture condition that matches all reassessments:



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



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:

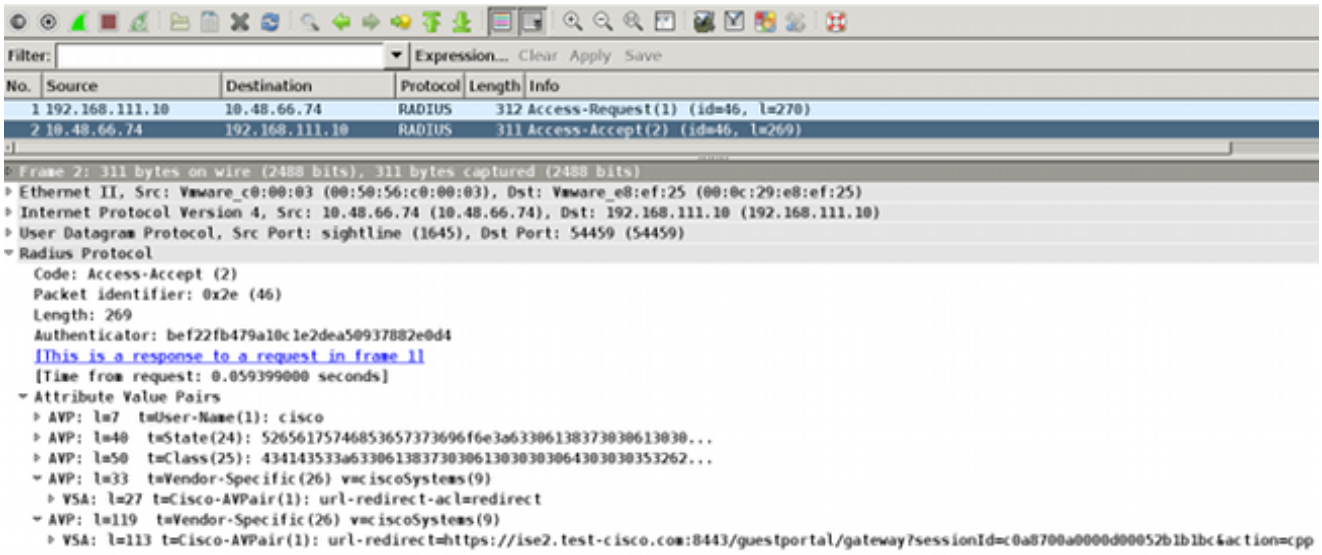


Verify

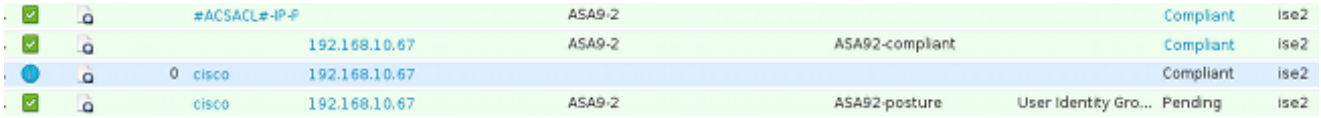
In order to confirm that your configuration works correctly, ensure that these steps are completed as described:

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:



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



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
```

```
Session Type: AnyConnect Detailed
```

```
Username     : cisco                  Index        : 9
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
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA1  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 16077                  Bytes Rx     : 16497
Pkts Tx      : 43                     Pkts Rx      : 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 : c0a8700a0000900052b840e6
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 : 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:
  Tunnel ID    : 9.2
  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 Tx      : 4                     Pkts Rx      : 2
  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
  Bytes Tx     : 5669                  Bytes Rx     : 18546
  Pkts Tx      : 35                    Pkts Rx      : 222
  Pkts Tx Drop : 0                     Pkts Rx Drop : 0
```

ISE Posture:

Redirect URL : https://ise2.test-cisco.com:8443/guestportal/gateway?sessionId=c0a8700a0000900052b840e6&action=cpp

Redirect ACL : redirect

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

<#root>

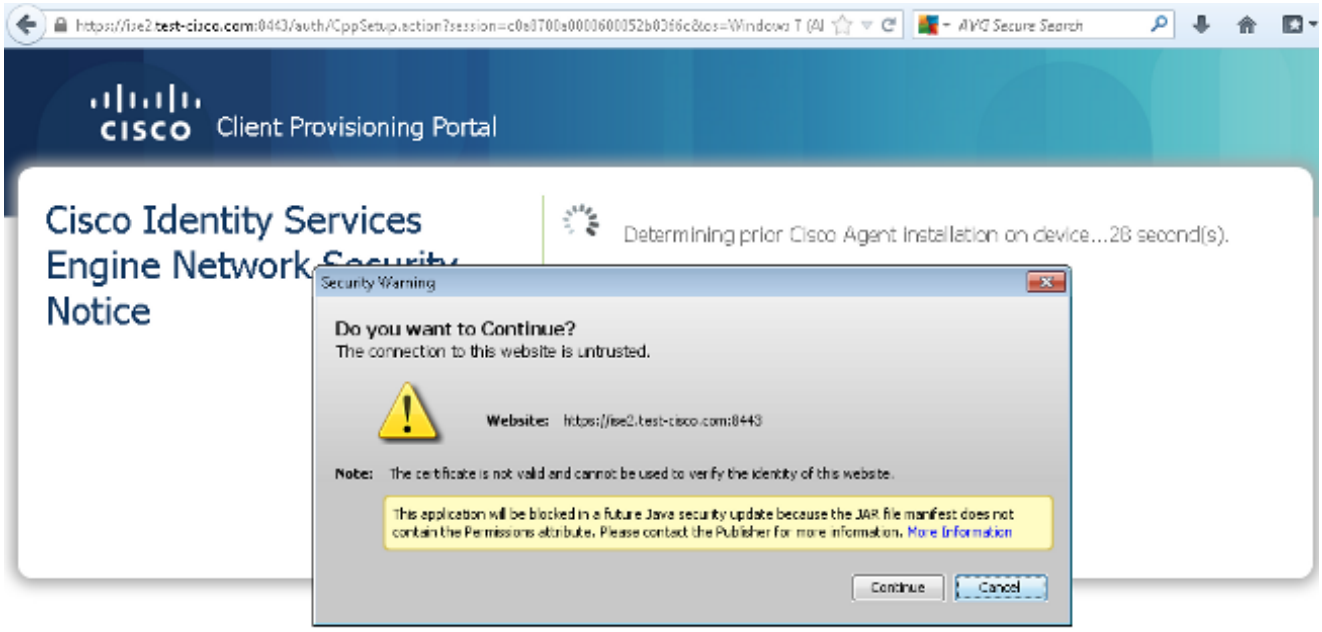
```
aaa_url_redirect: Created proxy for 10.10.10.10
aaa_url_redirect:
```

Sending url redirect

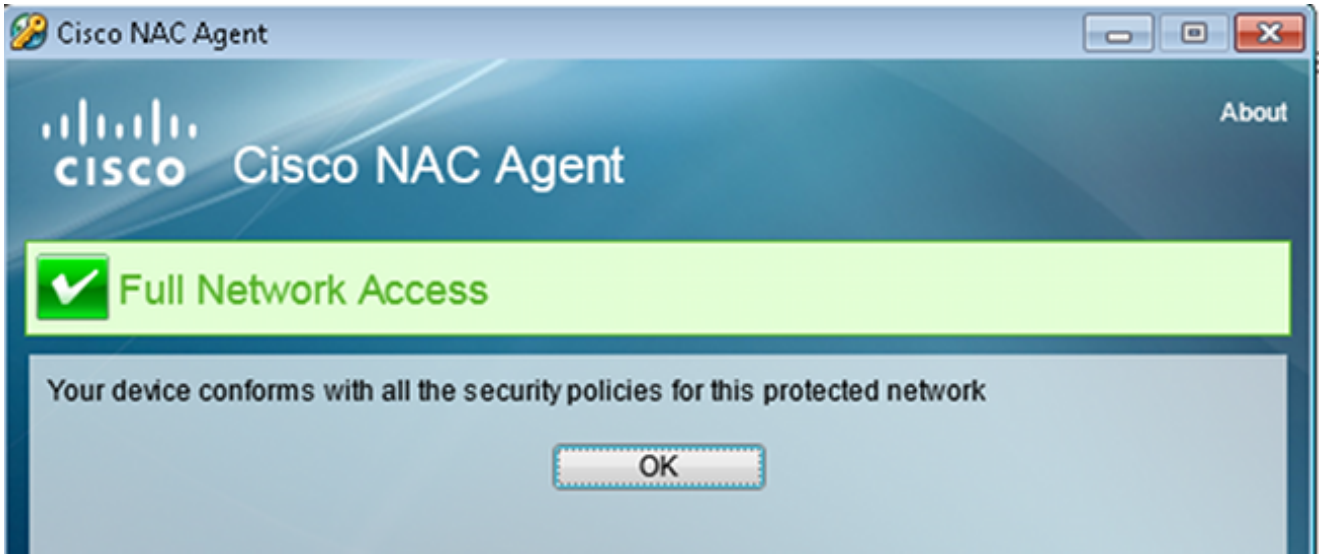
```
:https://ise2.test-cisco.com:8443/
 guestportal/gateway?sessionId=c0a8700a0000900052b840e6&action=cpp
 for
```

10.10.10.10

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



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.



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
 :::-
```

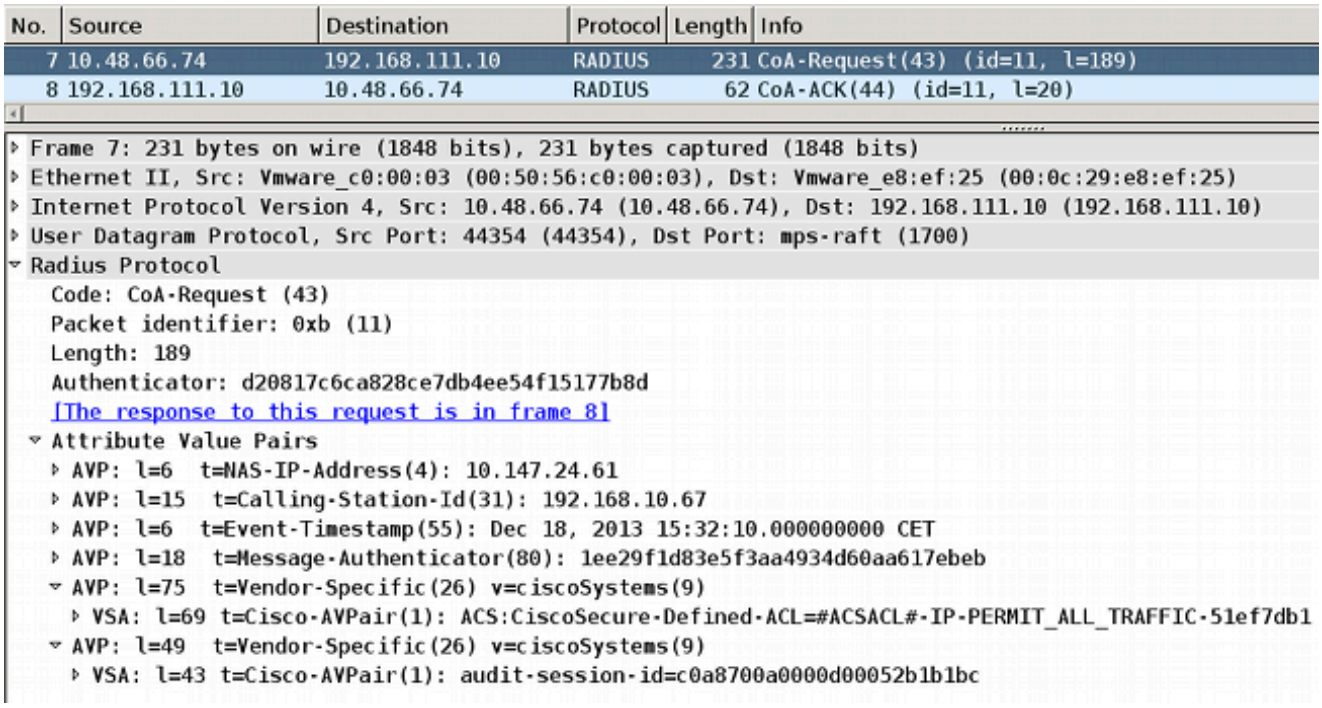
Posture state is compliant for endpoint with mac 08-00-27-CD-E8-A2

```
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:



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.

			#ACSACL#-IP-F		ASA9-2			Compliant	ise2
				192.168.10.67	ASA9-2	ASA92-compliant		Compliant	ise2
		0	cisco	192.168.10.67				Compliant	ise2
			cisco	192.168.10.67	ASA9-2	ASA92-posture	User Identity Gro...	Pending	ise2

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:

<#root>

```
ASA#
show vpn-sessiondb detail anyconnect


Session Type: AnyConnect Detailed

Username     : cisco                  Index        : 9
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
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA1  DTLS-Tunnel: (1)SHA1
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 : c0a8700a0000900052b840e6
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     : 5204                   Bytes Rx     : 779
  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

```
  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 : 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      : 4                      Pkts Rx      : 2
  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                  Bytes Rx     : 36128
  Pkts Tx      : 161                    Pkts Rx      : 379
  Pkts Tx Drop : 0                      Pkts Rx 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

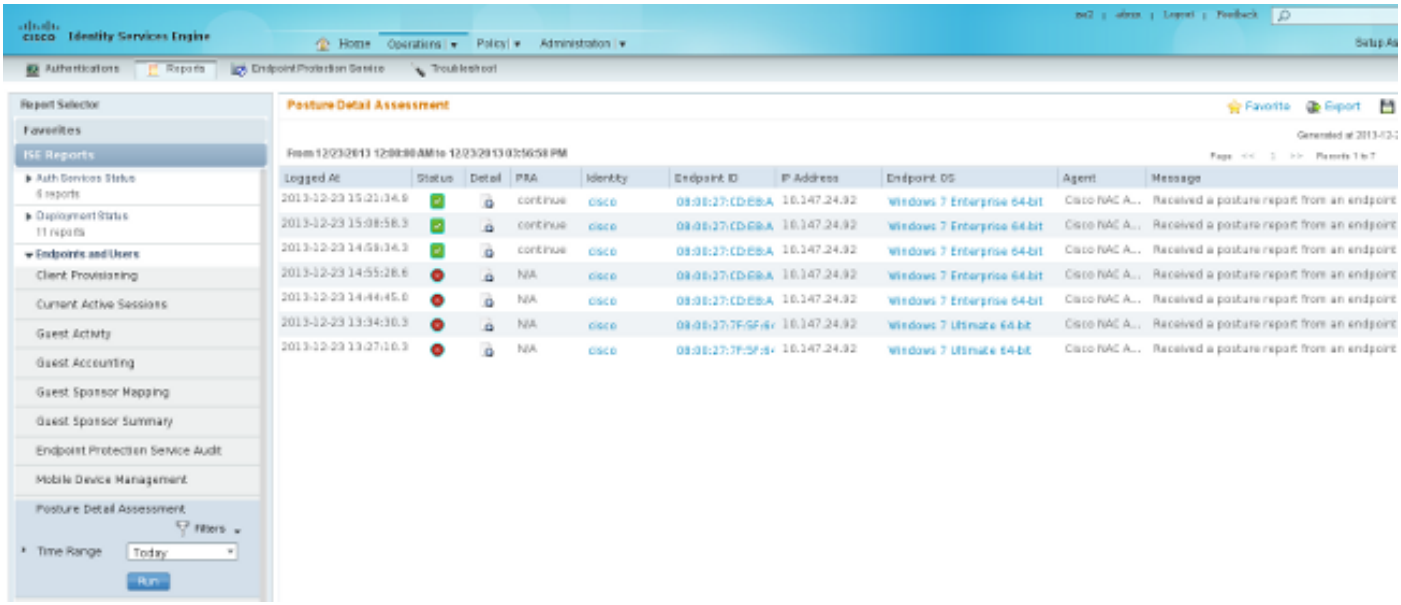
Enter this command in the CLI in order to view the debugs:

<#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:



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:	c0a8700a0000b00052b846c0
Client Operating System:	Windows 7 Enterprise 64-bit
Client NAC Agent:	Cisco NAC Agent for Windows 4.9.0.1013
PRA Enforcement:	1
CoA:	Received a posture report from an endpoint
PRA Grace Time:	
PRA Interval:	240
PRA Action:	continue
User Agreement Status:	NotEnabled
System Name:	MGARCARZ-WS01
System Domain:	cisco.com
System User:	mgarcarz
User Domain:	CISCO
AV Installed:	McAfee VirusScan Enterprise;8.8.0.975;7227;10/13/2013;McAfeeAV,Cisco Security Agent;6.0.2.130;;;CiscoAV
AS Installed:	Windows Defender;6.1.7600.16385;1.95.191.0;11/19/2010;MicrosoftAS

Posture Report

Posture Status:	Compliant
Logged At:	2013-12-23 15:21:34.902

Posture Policy Details

Policy	Name	Enforcement	Statu	Passed	Failed	Skipped Conditions
posture_initial	file_require...	Mandatory		file_condition		

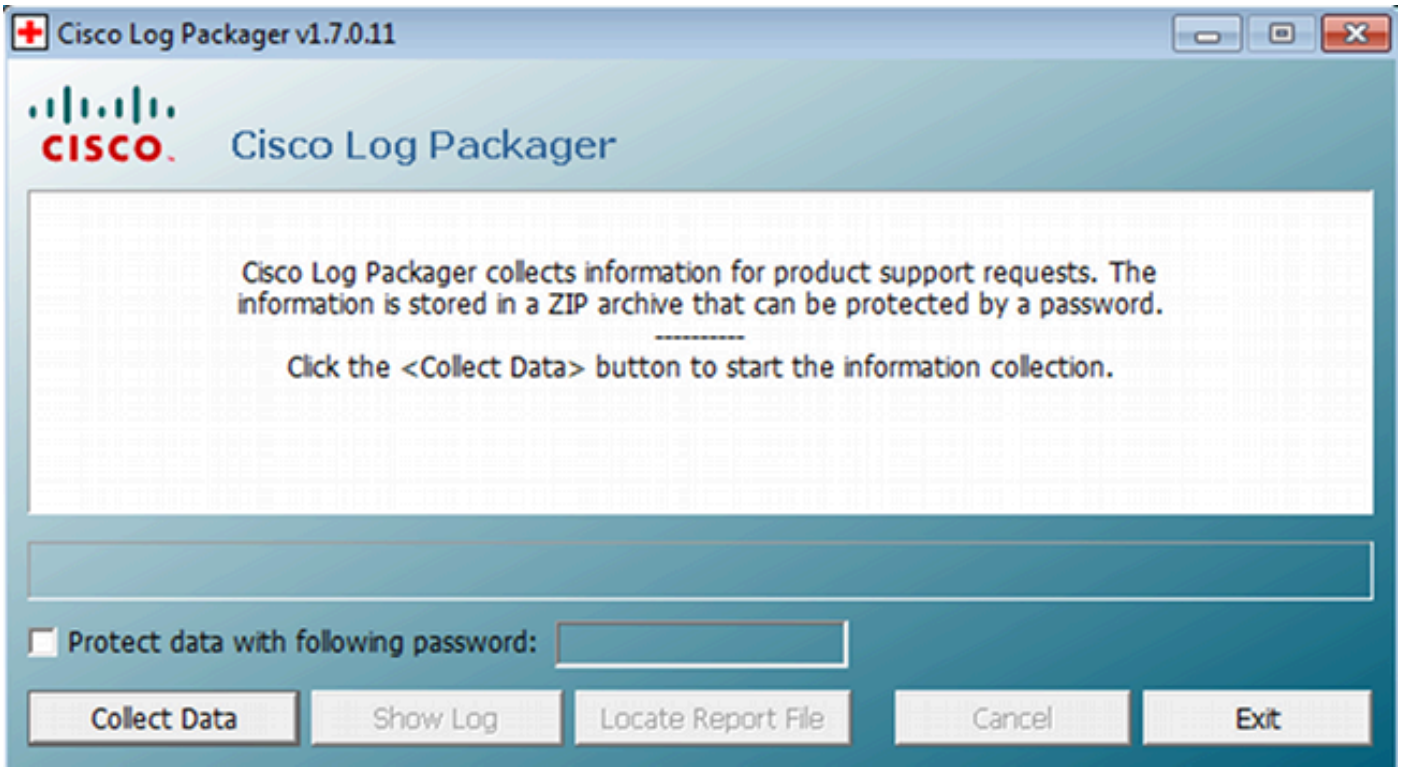
Debugs on the ASA

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.



Tip: You can decode the results with the Technical Assistance Center (TAC) tool.

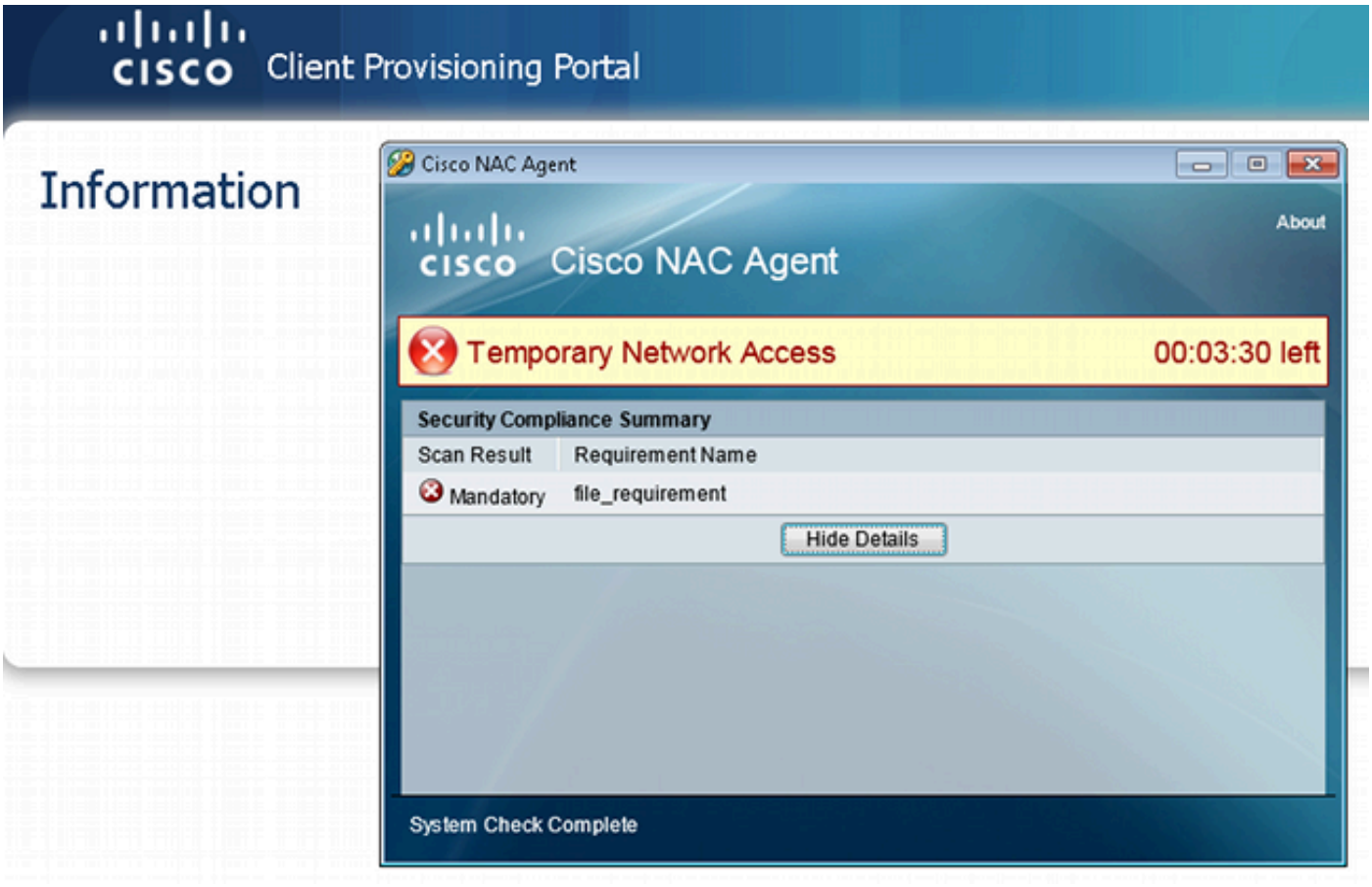
In order to retrieve the logs for the Web Agent, navigate to these locations:

- **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**

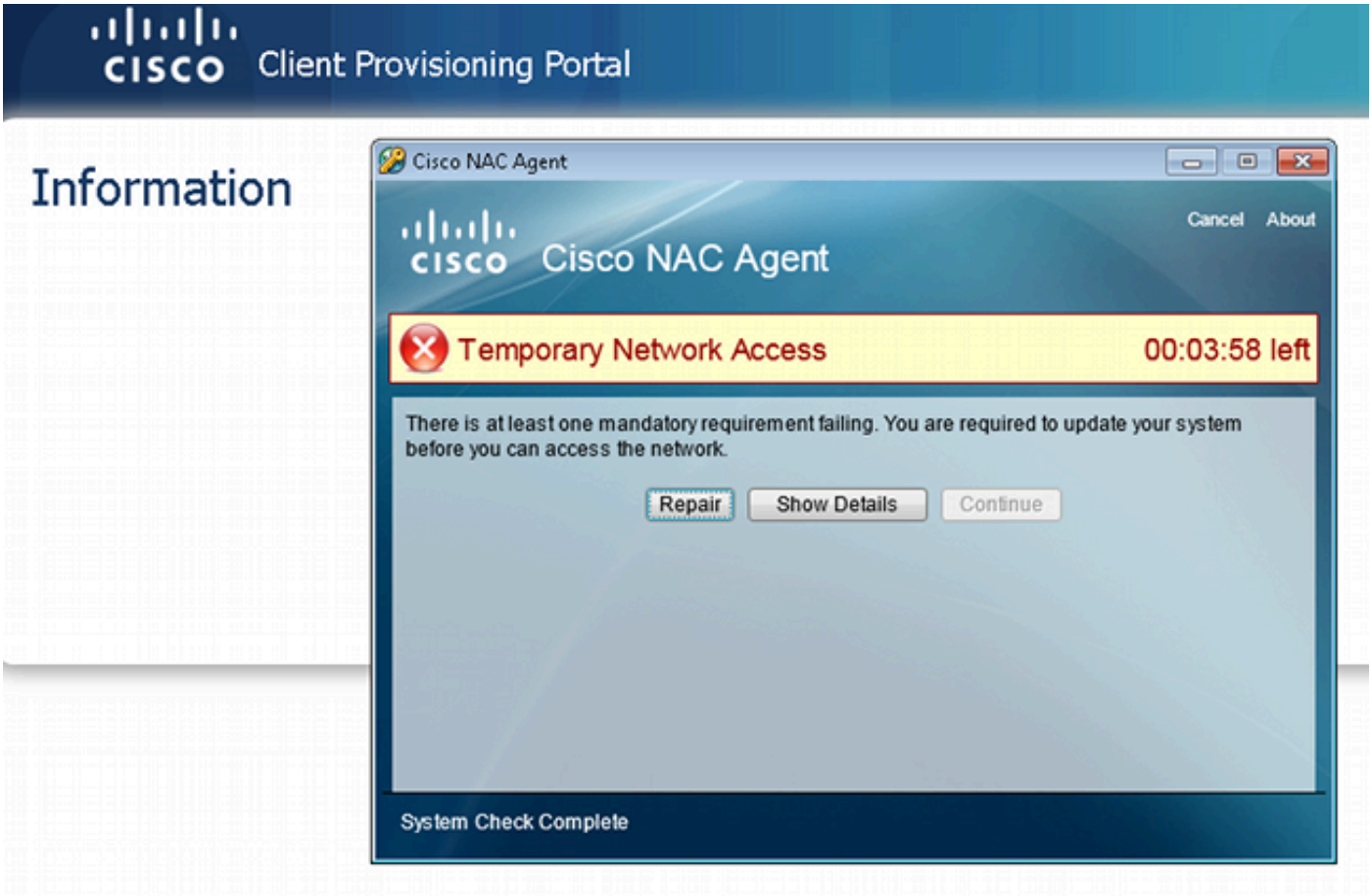
Note: If the logs are not in these locations, then verify the **TEMP Environment** variable.

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:



Related Information

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