Cisco ISE and ASA with Change of Authorization for Posture

ISE / ASA CoA integration
How-To Guide:

Table of Contents

Cisco ISE and ASA with CoA

Solution Overview

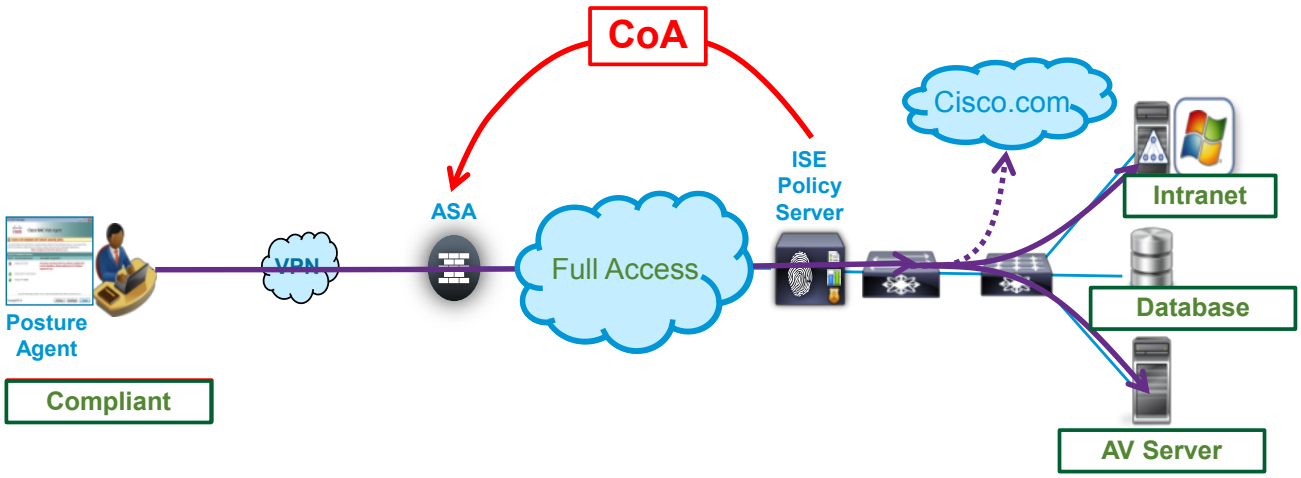
This paper will focus on Identity Services Engine (ISE) ability to determine the endpoint state by doing a posture assessment. Before the release of ASA 9.2.1 VPN users requiring posture functionality required an Inline Posture Node (IPN) between the VPN infrastructure and the LAN protected network. With the release of ASA 9.2.1 we now have the ability to enforce policy the ASA and ISE has the ability to send a "policy push" after a posture assessment has taken place.

This document will walk the administrator through the basic configuration components of the ASA and ISE for Change of Authorization.

Components

- Cisco ISE 1.2 patch 5 or later
- ASA 9.2.1 with ASDM 7.2(1) or later
- AnyConnect 3.1 MR 6 or later
- NAC agent 4.x (update) or later

Network Diagram



Configuring ASA for CoA with ASDM

This section enables the CoA functionality on the ASA. Connect to your ASA by launching your ASDM client.

Note: The CLI configurations that are being performed in this section can be found in the next section commands are available in the **Configuring ASA 9.2.1 for CoA with CLI** section.

Configuring the Tunnel Group and Authentication Method

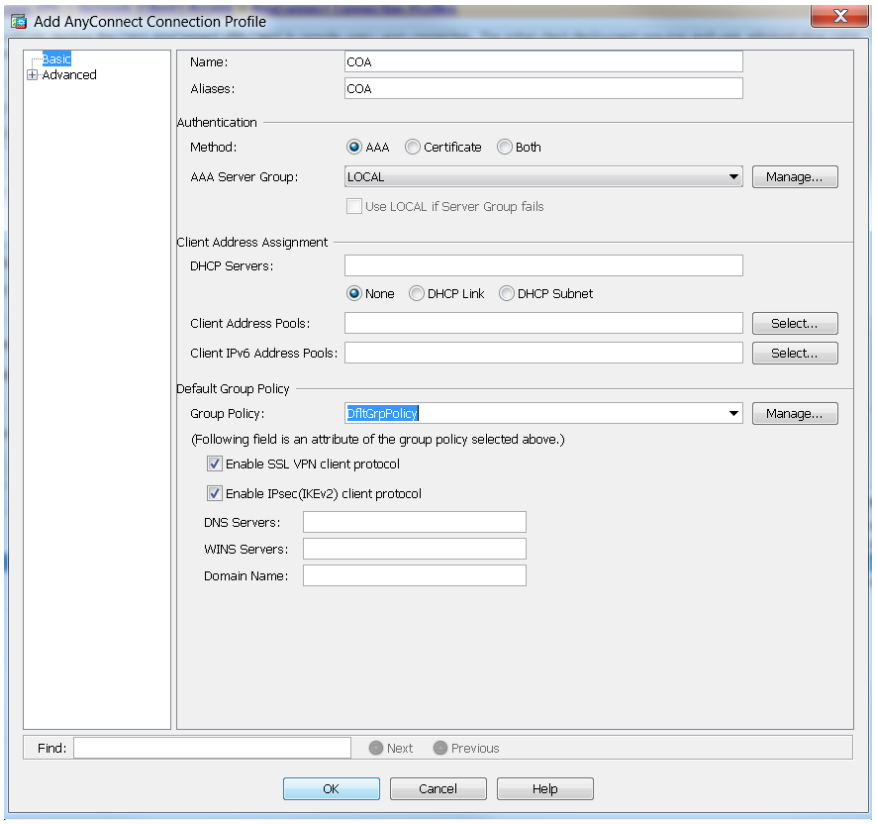
The ASA appliance provides two default tunnel groups one for remote access (DefaultRAGroup) and one for clientless (DefaultWEBVPNGroup). In this document we will create a new Tunnel Group and name it **COA**. We will also need to configure the Authentication method and point it to ISE for RADIUS authentication. When VPN users connect to their corporate headend they will have a Tunnel Group named **COA** in their AnyConnect dropdown selection.

This section you will configure a **Redirect ACL** (Access Control List) ISE will use for the initial VPN connection until the user is placed into a compliant state. Once compliant, ISE will then push a new dACL (dynamic Access Control List) with a new set of access.

Step 1: Navigate to **Configuration→Remote Access VPN→Network(Client)Access→AnyConnect Connection Profiles,** select **Add**

Step 2: In the **AnyConnect Connection Profile:**

- Enter a Name: (Example: **COA)**
- Enter a Aliases: (Example: **COA)**



Step 3: Under Authentication

Depending on your company policy you have the option to choose between **AAA, Certificate, or Both.**

- Method: for simplicity of configuration we choose to use **AAA**

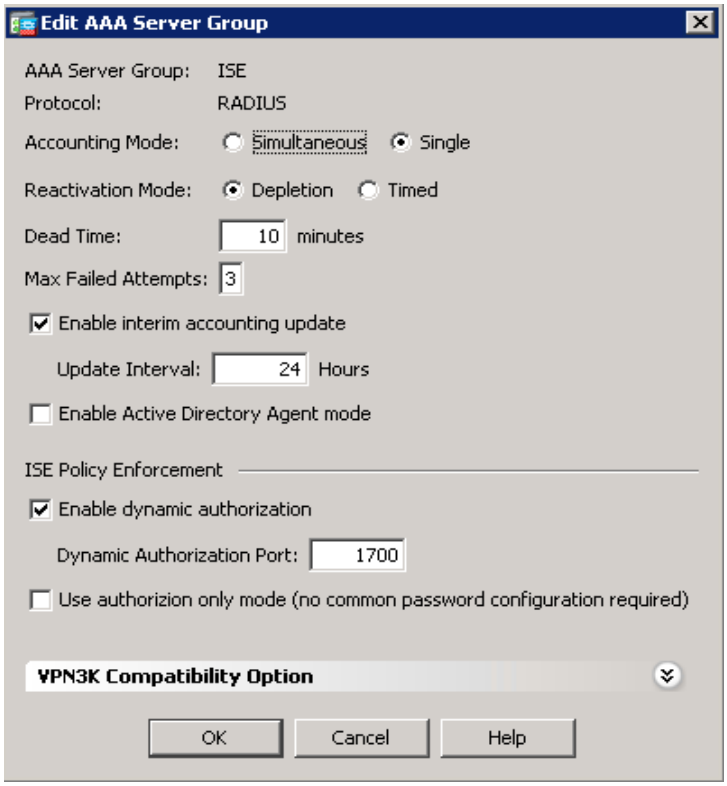
Note: If using certificate authentication you must enable the "Use Authorize only mode" in the below configuration.

- In AAA Server Group: Select **Manage**
    - A new window will pop up, **Configure AAA Server Groups,** Select **Add** under **AAA Server Groups**
        - Enter in name for AAA Server Group: (Example: **ISE)**
        - Protocol: **RADIUS**
        - Accounting mode: Single (Default setting)
        - Reactivation Mode: Depletion (Default setting)
        - Dead Time: 10 Time (Default setting)
        - Max Failed Attempts: 3 (Default setting)
        - Tick the box **"Enable interim accounting update"**
        - Under ISE Policy Enforcement tick the box **"Enable dynamic authorization"**

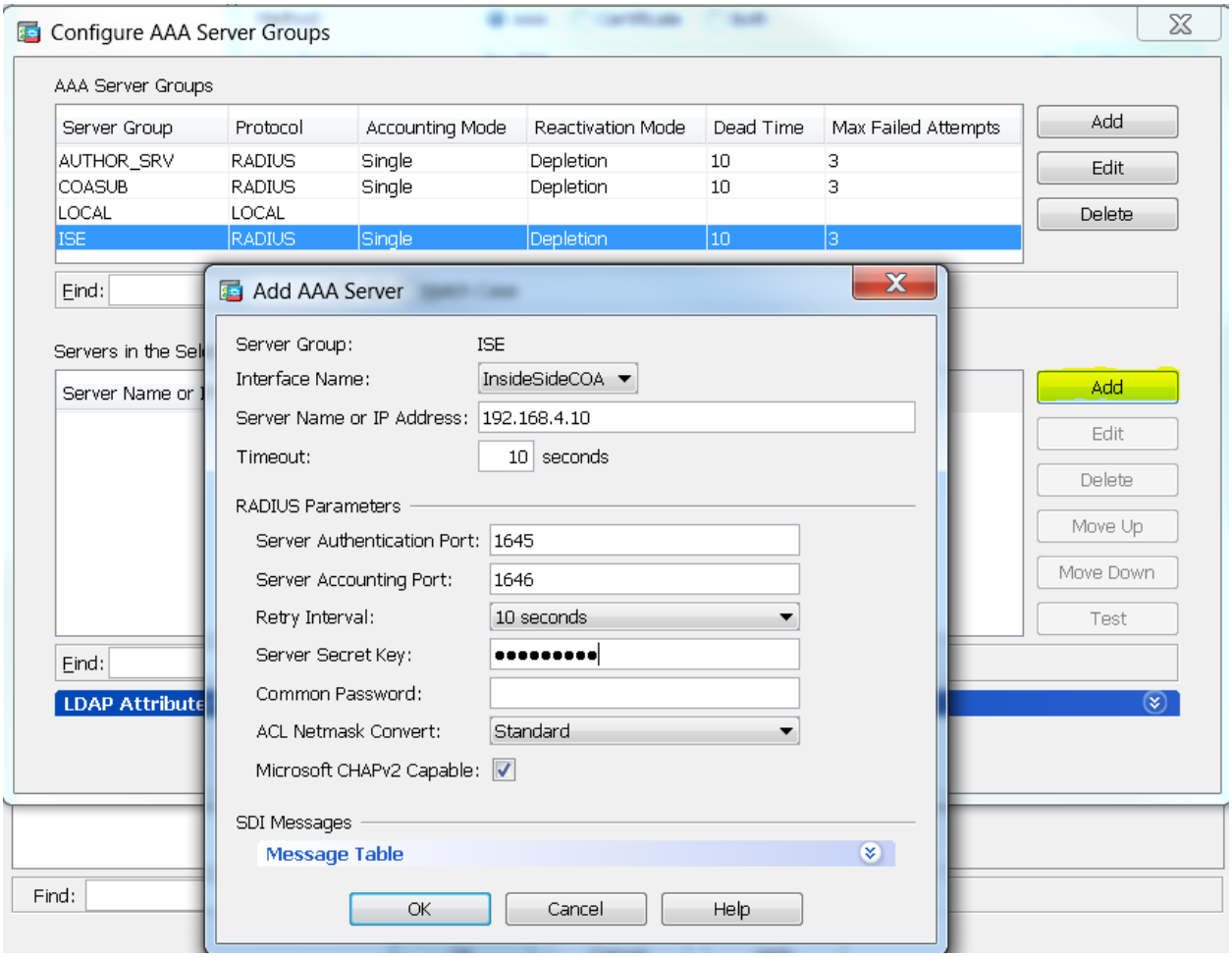
Note: This is what enables ASA Change of Authorization (CoA)

- Leave the default port of 1700, Click **OK**

Screen shot of the configuration below.



- With the newly created **ISE** AAA server Group highlighted select **Add** under **Server in the Selected Group**
    - Interface Name: Select the appropriate interface for which the ISE server can be reached.
    - Server Name or IP Address: This is the IP address of the ISE server
    - Timeout: 10 seconds (Default setting)
    - Server Authentication Port: 1645 (Default setting) Supports 1812
    - Server Accounting Port: 1646 (Default setting) Supports 1813
    - Retry Interval: 10 seconds (Default setting)
    - Server Secret Key: Enter in a phrase which will be used later on in our ISE configuration section.
    - Common Password:
    - ACL Netmask Converter: Standard (Default setting)
    - Microsoft CHAPv2 Capable: Enabled (Default setting)
    - Select **OK** Select **OK** again to accept the **Configure AAA Server Groups** pop out box and will bring you back to **Add AnyConnect Connection Profile** pop out.

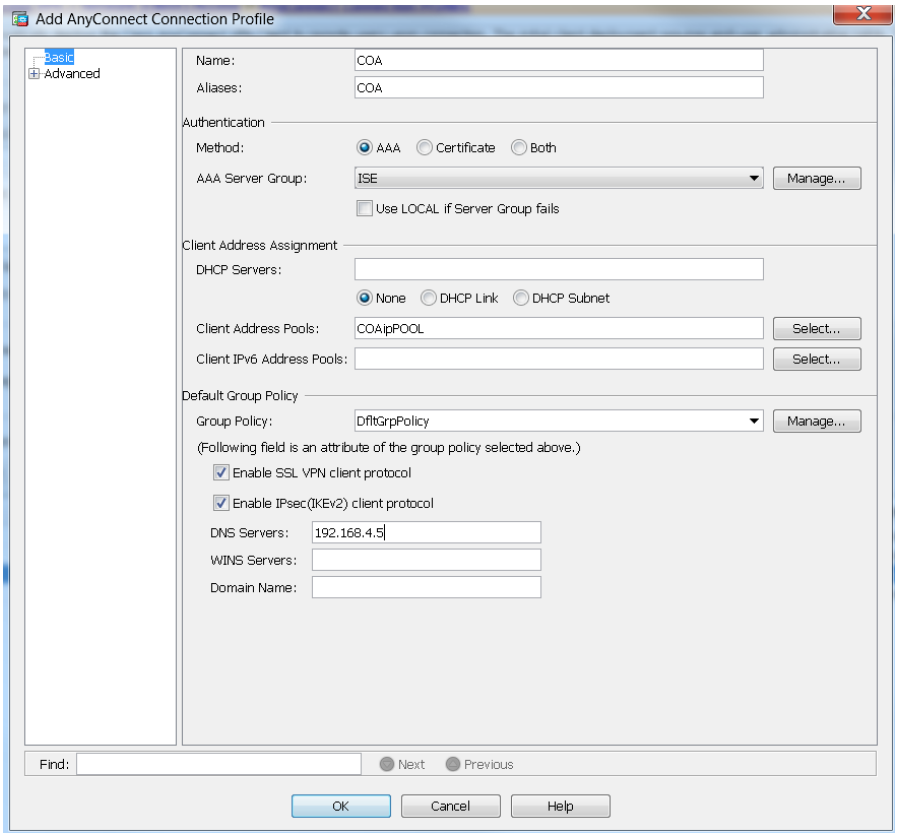


Step 4: Under Client Address Assignment

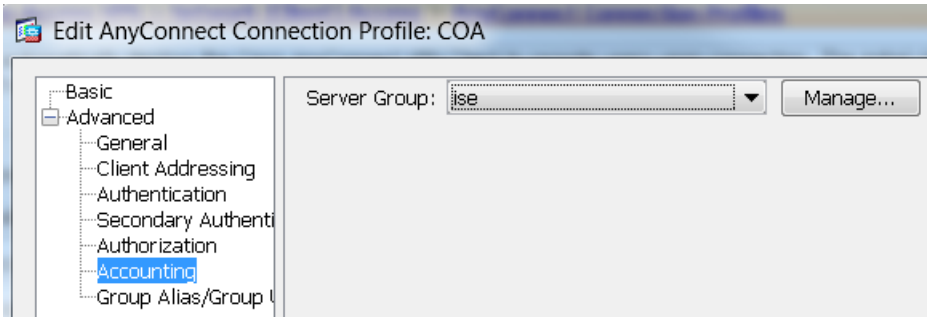
- Client Address Pools: Assign the appropriate VPN IP Pool

Step 5: Under Default Group Policy

- Group Policy: Select the appropriate Group Policy
- Enable SSL or IKEv2 protocol or both
- DNS Servers: These DNS servers will be sent down to the AnyConnect Client. Enter the DNS server in this field which will be used to resolve the ISE server IP address



- In the Connection profile expand the Advance option and configure accounting to point to ISE.



- Select **OK** and **Apply** your configuration.

Configuring the ACL for posture redirection

Step 1: Navigate to **Configuration→Firewall→Advanced→ACL Manager,** select **Add ACL**

Step 2: ACL Name: Enter in ACL access you want to allow you user pre-posture Example name "redirect"

Step 3: Highlight the newly created ACL and add an ACE access rules and allow the client enough access to remediate the untrusted system. In the example rule 1 & 2 allows NAC discovery to our ISE server, rule 3 provide AD/DNS, rule 4 & 5 provides access to our AV and Microsoft Patch server, and rule 6 is a permit http to allow all other traffic to be redirected.

#	Enabled	Source	Destination	Service	Action	Description
redirect						
1	☑	any	192.168.1.10	8905	Deny	swiss
2	☑	any	192.168.1.10	8905	Deny	swiss
3	☑	any	192.168.1.5	domain	Deny	DNS Server
4	☑	any	192.168.1.15	ip	Deny	AV Server
5	☑	any	192.168.1.20	ip	Deny	Microsoft Patch Server
6	☑	any	any	http	Permit	Allow for redirect

Note: ISE also provides the ability to limit certain user group access with dACL sent from ISE.

Configuring ASA for CoA using CLI

This section takes you through the command line interface of the ASA to configure CoA.

Step 1: Create the AAA server Group

- ASA> en
  Password: *********
  ASA# conf t
  ASA(config)# aaa-server ISE protocol radius
  ASA(config-aaa-server-group)# interim-accounting-update
  ASA(config-aaa-server-group)# dynamic-authorization
  ASA(config-aaa-server-group)# aaa-server ISE host 192.168.4.10
  ASA(config-aaa-server-host)# timeout 21
  ASA(config-aaa-server-host)# key **********
  ASA(config-aaa-server-host)# exit
  ASA(config)#

Step 2: Create an Access-list needed for "Unknown or non-compliant" state. This should be limited to anything required for client remediation. In this use case we're limiting traffic to AD for DNS, ISE, AV Server, and Microsoft Patch Management. Once the machine has passed posture this ACL will be replaced with another DACL once the CoA takes place. In this document we name the ACL **redirect** and will call on this ACL later on when configuring ISE.

- ASA(config)# access-list redirect remark exclude ISE server
  ASA(config)# access-list redirect extended deny ip any4 host 192.168.4.10 (hostname/IP of ISE server)
  ASA(config)# access-list redirect remark exclude DNS server
  ASA(config)# access-list redirect extended deny ip any4 host 192.168.4.5 (hostname/IP of DNS server)
  ASA(config)# access-list redirect remark redirect all other traffic
  ASA(config)# access-list redirect permit ip any4 any4

Step 3: Create the tunnel-group and apply VPN IP address-pool, AAA Server group,

- ASA(config)# tunnel-group "CoA" type remote-access
  ASA(config)# tunnel-group "CoA" general-attributes
  ASA(config-tunnel-general)# address-pool **add in your "**IP pool address"
  ASA(config-tunnel-general)# authentication-server-group **add in your** "ISE server group name"
  ASA(config-tunnel-general)# accounting-server-group **add in your** "ISE server group name"
  ASA(config-tunnel-general)# default-group-policy **add in your** "Group Policy"
  ASA(config-tunnel-general)#exit
  ASA(config)# tunnel-group "COA" webvpn-attributes
  ASA(config-tunnel-webvpn)# group-alias "COA" enabled
  ASA(config-tunnel-webvpn)# exit
  ASA(config)# exit
  ASA# write memory

Configuring ISE for CoA

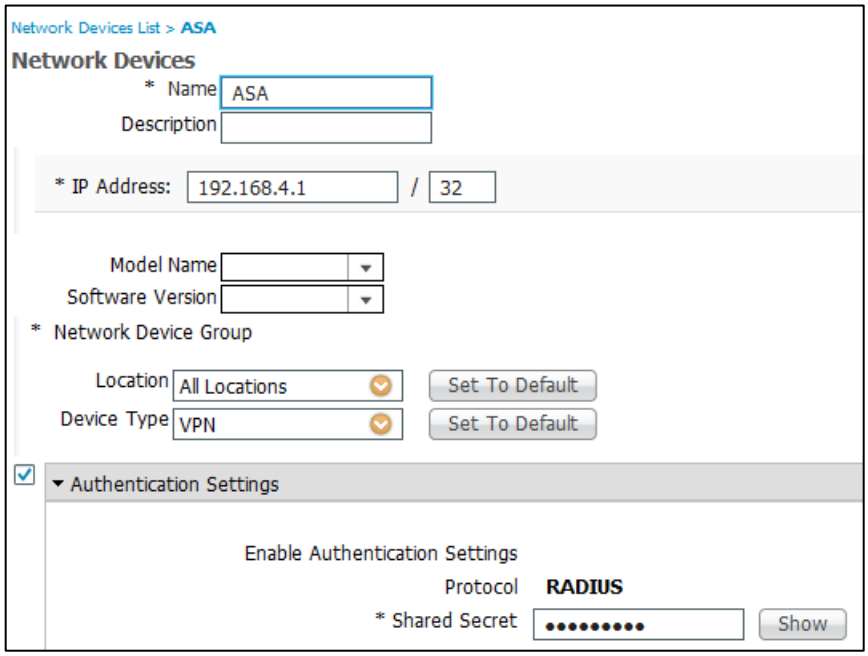
Creating a Network Device entry for the ASA

We need to log into our ISE console and navigate to our Network devices and add our ASA. This configuration allows ISE and the ASA to communicate through RADIUS..

Step 1: Navigate to **Administrator→Network Resources→Network Devices**, select **Add**

- **Name:** Add the name of the ASA
- **Description:** optionally add a description
- **IP Address:** add in the IP address of the ASA
- Click on the **Authentication Settings** drop down
  - **Shared Secret:** Enter in the same shared secret key that was created for the ASA.

Step 2: Select **Submit**



Configuring Policies for ISE Posture

The document takes into account ISE was already joined to an Active Directory domain controller and will focus on the steps required for ISE and the ASA to communicate through RADIUS for authentication.

For this particular use case we will focus on creating a policy to install ISE NAC agent onto a Windows 7 system and do a posture policy check for a file.

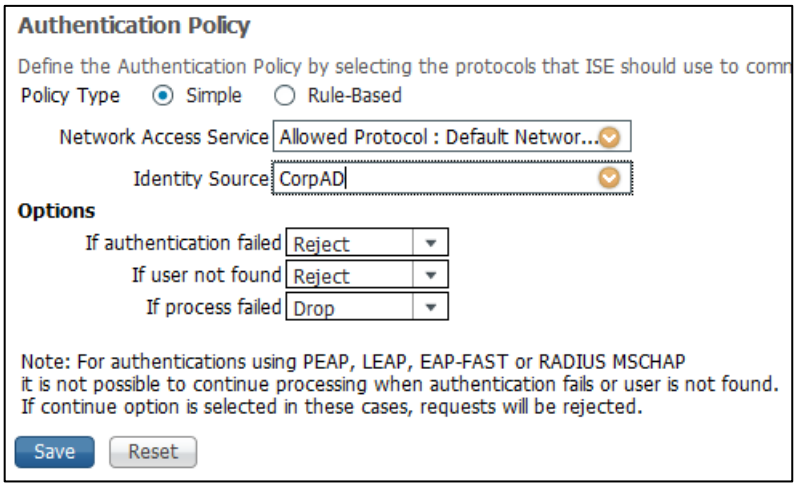
The ASA will send the authentication request to ISE and will leverage this authentication policy to determine what Identity Source the user should be authenticated against. In this case we have selected the COA Identity Source which is our Active Directory.

In this section we need to create an authorization conditions for untrusted and trusted devices, ISE will then push policies based on these results down to the ASA. In this use cases if ISE cannot determine the compliance state of the machine it will be identified as unknown device and we will apply a policy to instruct the user to download our ISE NAC agent. If the user is complaint we will push an ISE policy of full access.

Configuring Authentication

Step 1: Navigate to **Policy→Authentication**

- **Policy Type**: Select Simple **or** Rule Based
- **Network Access Service:** Select the drop down and select **Allowed Protocols→Default Network Access**
- **Identity Source:** Select your Active Directory Domain (Example Corp AD)
- Click **Save**



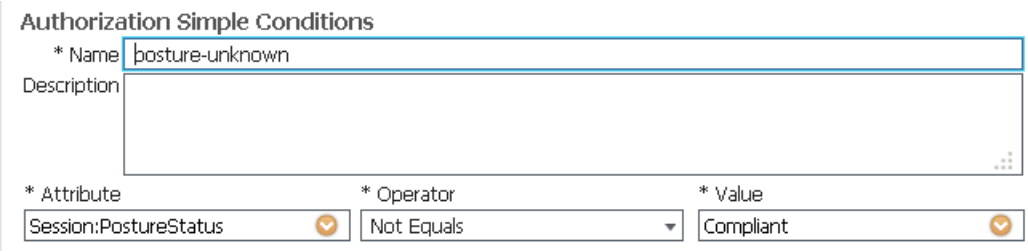
Configuring Authorization

Create the Posture-Uknown condition

Step 1 Navigate to **Policy→Policy Elements→Conditions,**

Step 2 Select **Authorization→Simple Condition,** select **Add**

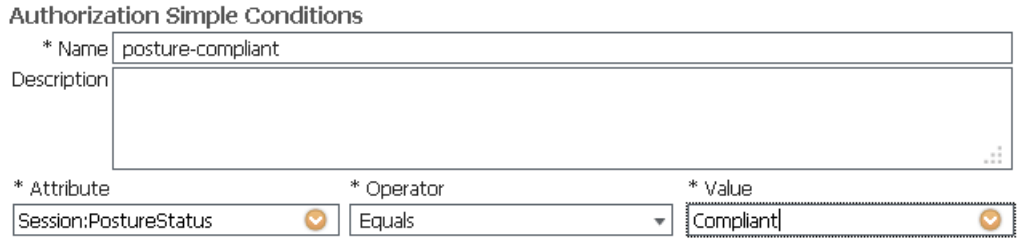
- **Name:** Provide a name (Example: posture-unknown)
- **Description:** Give the Policy a description
- **Attribute: Session→Posture | Operator: Not Equals | Value: Compliant**
- Select **Submit**



Create the Posture-Compliant condition

Step 1 Navigate to **Policy→Policy Elements→Conditions,**

- Select **Authorization→Simple Condition,** select **Add**
  - **Name:** Provide a name (Example: posture-compliant)
  - **Description:** Give the Policy a description
  - **Attribute: Session→Posture | Operator: Equal | Value: Compliant**
  - Select **Submit**



Create the Authorization Profile for VPN redirect

This authorization policy will call our **redirect** ACL created on our ASA and allow users the ability to install the NAC client. The **redirect** ACL could have also been used to provide limited access to an AV server or WSUS.

Procedure: Navigate **Policy→Policy Elements→Results**

- From left select **Authorization→Authorization Profiles** and select **Add**
  - **Name:** Posture-Remediation
  - **Description:** Optional
  - **Access type:** ACCESS_ACCEPT
  - Under Common Tasks, check **Web Redirection** and select **Client Provisioning (Posture)** from the drop down. Fill in **redirect** next to ACL. (The **redirect** was the ACL created on the ASA in the previous section of this document. The text in the ACL box is case sensitive and must match what was created on the ASA ACL)

Note: The following step is only required if DNS provided by the ASA to the endpoint cannot resolve the ISE hostname.

  - Under Advanced Attributes Settings, select **Cisco-VPN3000→CVPN300/ASA/PIX7.x-Primary-DNS.** In the value box provide the IP address of a DNS server that is capable of resolving ISE hostname.

Using the information above with the exception of the DNS IP entry should yield a similar **Attributes Detail** as shown below.

Create a dynamic Access Control List (dACL) for Compliant Users

The dACL is an Access Control list which is called by an authorization policy

Procedure: Navigate **Policy→Policy Elements→Results**

- From left select **Authorization→Downloadable ACLs** and select **Add**
  - Name: Enter in a name (Example: **Posture-Compliant**)
  - Description: **Posture status returned compliant**
  - DACL Content: **permit ip any any**
  - Select **Submit**

Create an Authorization Policy for compliant users

The dACL will be pushed down to VPN users who have successfully passed the ISE NAC agent posture assessment.

Procedure: Navigate **Policy→Policy Elements→Results**

- From left select **Authorization→Authorization Profiles** and select **Add**
  - Name: **Posture-compliant**
  - Description: **User is compliant**
  - Access type: **ACCESS_ACCEPT**
  - Under Common Tasks, enable **DACL Name** and select **Posture-Compliant** from the dropdown.
  - Select **Submit**

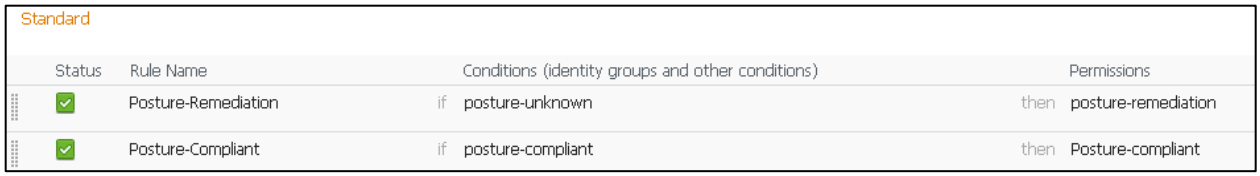
Create an Authorization Policy for unknown /non-compliant posture status

Procedure: Navigate **Policy→Authorization**

- Next to the Edit button on the top most rule, click the arrow **Insert New Rule Above**
- Rule Name: **Posture-Remediation**
- Any: **Any**
- Condition: Select Existing Condition from Library, Select Condition Name, then navigate to **Simple Conditions→ posture-unknown**
- Permissions: **Standard→posture-remediation**
- Hit **Done,** then **Save**

Create an Authorization Policy for Compliant posture status

- Next to the Edit button on the top most rule, click the arrow **Insert New Rule Below**
- Rule Name: **Posture-Compliant**
- Any: **Any**
- Condition: Select Existing Condition from Library, Select Condition Name, then navigate to **Simple Conditions→ posture-compliant**
- Permissions: **Standard→posture-compliant**
- Hit **Done,** then **Save**


Standard
Status
Rule Name
Conditions (identity groups and other conditions)
Permissions
Posture-Remediation
if
posture-unknown
then
posture-remediation
Posture-Compliant
if
posture-compliant
then
Posture-compliant

Configuring Posture Agent for Deployment

ISE has 2 types of agents for Windows, one you download to the machine and the other is a dissolvable Web agent. ISE supports NAC agent for MAC as well.

This section explains how to deploy the ISE NAC agent and configure a basic posture rule. In the first step you have the option to manually configure or have ISE automatically download ISE NAC agent and Compliance modules. The Compliance module contains the latest vendor updates and should be routinely added to your client provisioning policy to ensure proper endpoint assessment.

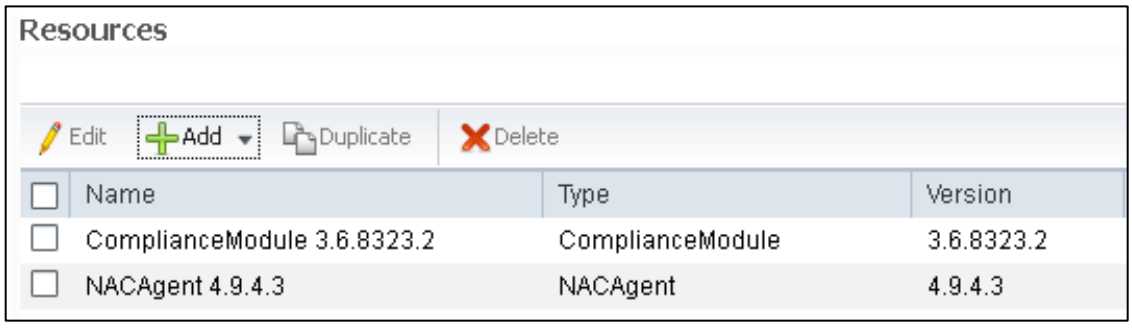
In this case Automatic Download was selected which routinely updates ISE with the latest modules. In this use case policy was created bases on the latest Client based NAC agent and Compliance module for a Windows system made available at the time this document was written.

Configuring Client Provisioning Resources

Procedure: Navigate, **Policy→Results**

- Select, **Client Provisioning→Resources,** Select **Add**

Note: Selecting **add** provides you with a choice between local disk or Cisco site, depending on you ISE environment model choose the appropriate method. If you would like ISE to Automatically Download Navigate, **Administration→Settings→Client Provisioning** and select **Enable** next to Enable Automatic Download from the dropdown.



Configuring Client Provisioning Policy

Procedure: Navigate, **Policy→Client Provisioning**

- Rule Name: Enter in a name (Example: **Windows-nac-download**)
- Identity Groups: **Any**
- Operating System: Select Windows OS (In this example **Windows All** was selected)
- Other Conditions: **N/A**
- Results:
  - Agent: **NACAgent 4.x**
  - Profile: **N/A**
  - Compliance Module: **ComplianceModule 3.x**
  - All other fields left default

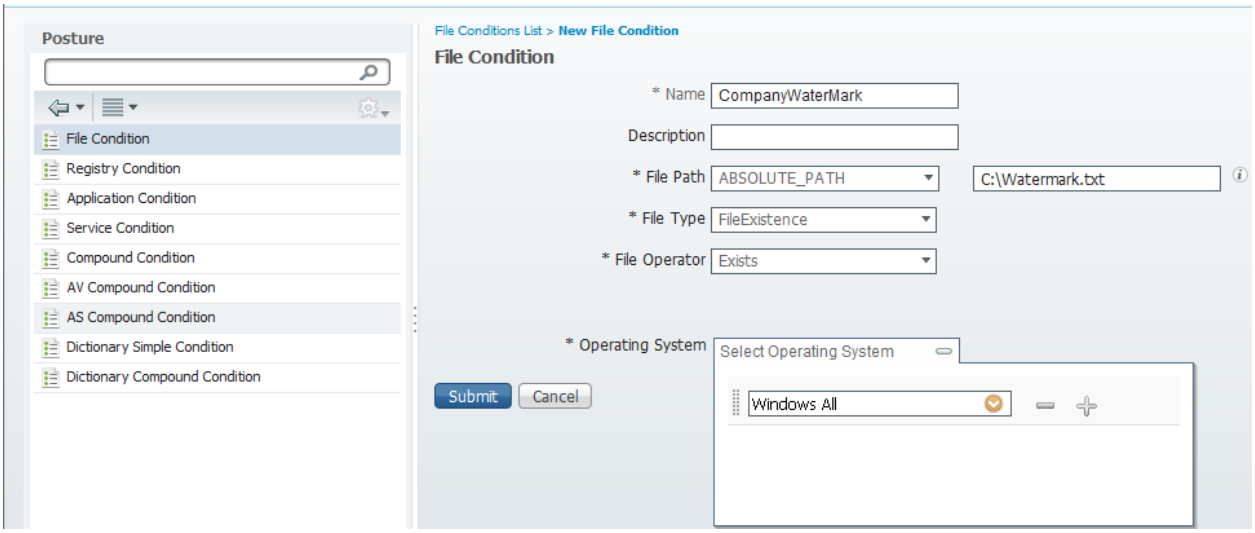
- **Save**

Configuring a Posture Requirement

A Posture Requirement is defined as something you want the machine to be checked for prior to allowing the extended access. In this use case we are checking for a corporate water mark. You also have the option to check endpoints for Anti-Virus and if the latest definitions have been applied.

Procedure: Navigate **Policy→Policy Elements→Conditions**

- Select **Posture→File Condition** from the left hand tree, select **Add**
  - Name: **CompanyWaterMark**
  - File Path: Absolute_Path, C:\Watermark.txt
  - File Type: FileExistence
  - File Operator: Exists
  - Operating System: Windows All



Create a Posture Requirement

Now that a posture condition has been configured we need to assign it to be a required posture check for end-points trying to gain access to the corporate network. In this use case we will inform the user that their machine is noncompliant by sending a message through the NAC agent stating a missing file requirement check has occurred and to add back the file Watermark.txt to the proper directory.

- **Procedure:** Navigate **Policy→Policy Elements→Results**
- Select **Posture→Requirements** from the left hand tree, select the drop down next to edit and **Insert new Requirement**
  - Name: **Findfile**
  - Operating System: **Windows All**

- Condition: **User Defined→File Condition→CompanyWaterMark**
- Remediation Actions: **Message Text Only**
  - Message informing the User: You're missing **C:\Watermark.txt** please add back the file

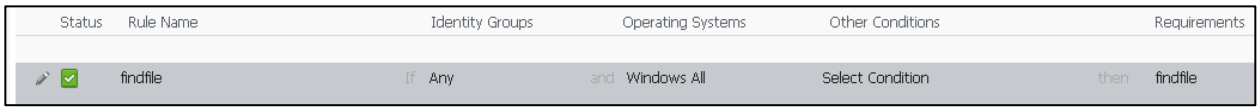
o Hit **Done,** then **Save**

Create a Posture Policy to be applied to all Windows endpoints.

In this section we take the condition and the requirement and build a posture policy that the ISE NAC agent will user to assesses during network connection.

Procedure: Navigate **Policy→Posture**

- Name: **Findfile**
- Identity Groups: **Any**
- Operating System: **Windows All**
- Other Condition: <leave blank>
- Requirements: **findfile**
- Hit **Done,** then **Save**



Connect VPN Client and monitor ASA and ISE logs

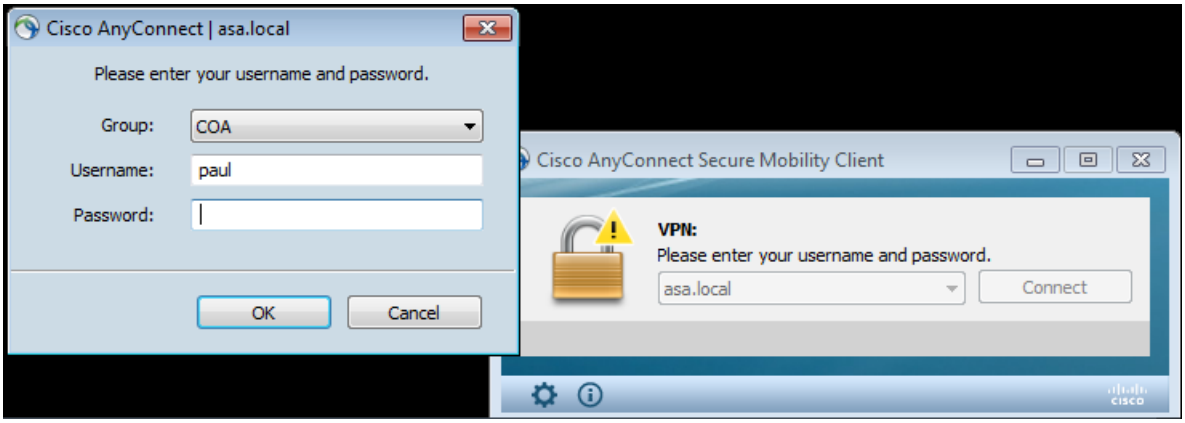
With ISE and ASA configured for CoA and a posture policy has been configured to check for Watermark.txt in the c:\ directory it is time to VPN connect the remote end-point. In this example, the end-point is a Windows 7 machine and does NOT have the Watermark.txt added to the c:\ directory. NAC will report the status of the end-point to ISE and ISE will restrict access and notify the user the end-point is non-compliant. The user will need to add the Watermark.txt to the c:\ directory to become compliant.

We will monitor the status of the end-point before and after a Change of Authorization (CoA) from both the ASA CLI and ISE.

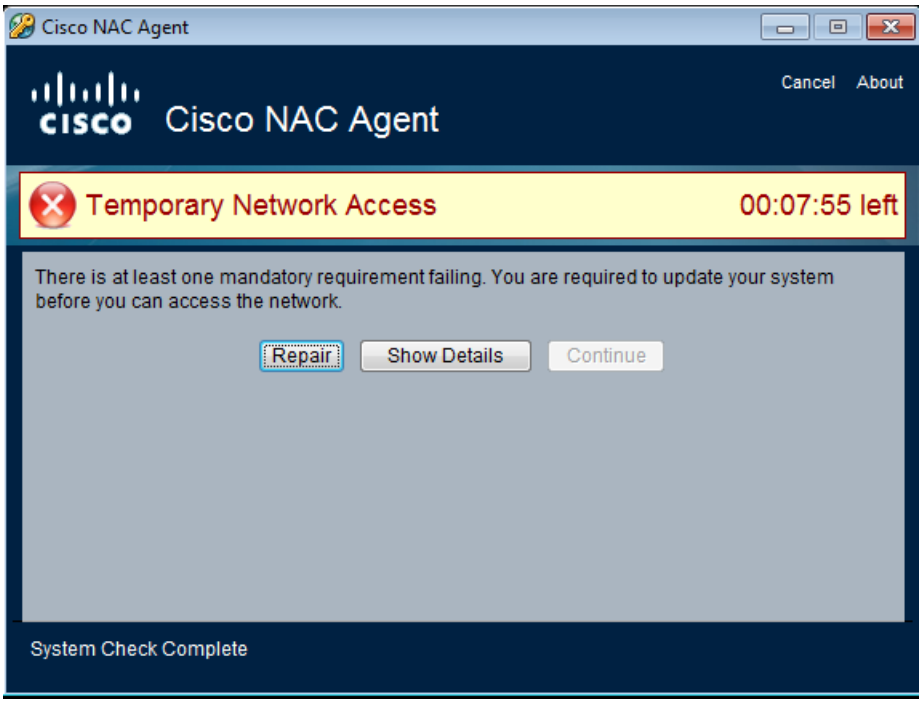
Connecting Non-Compliant end-point to ASA head-end

Step 1 Connect to ASA head-end

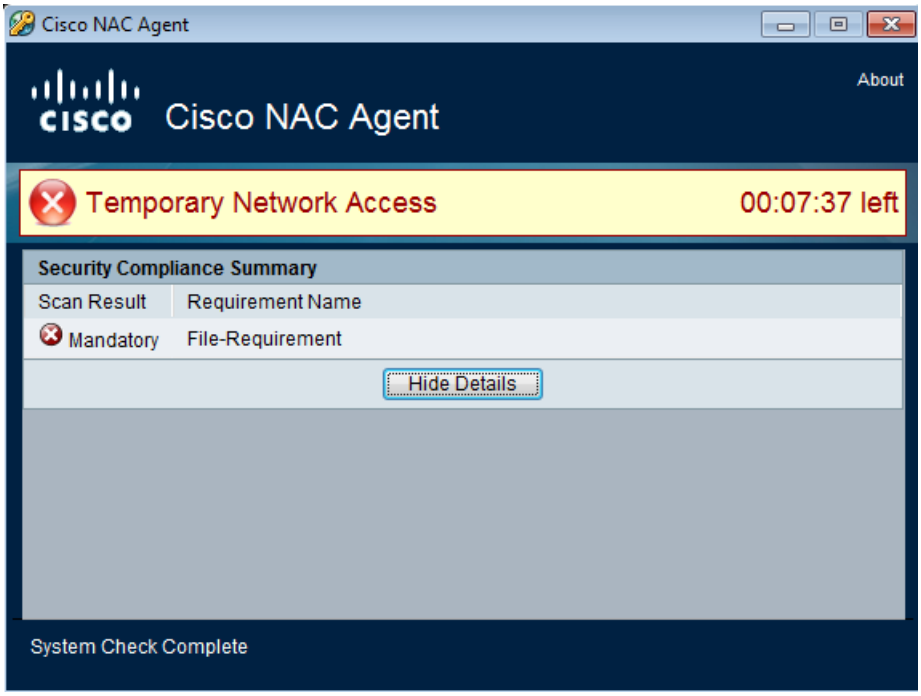
From your client PC launch the AnyConnect VPN agent and connect to your ASA configured for CoA.



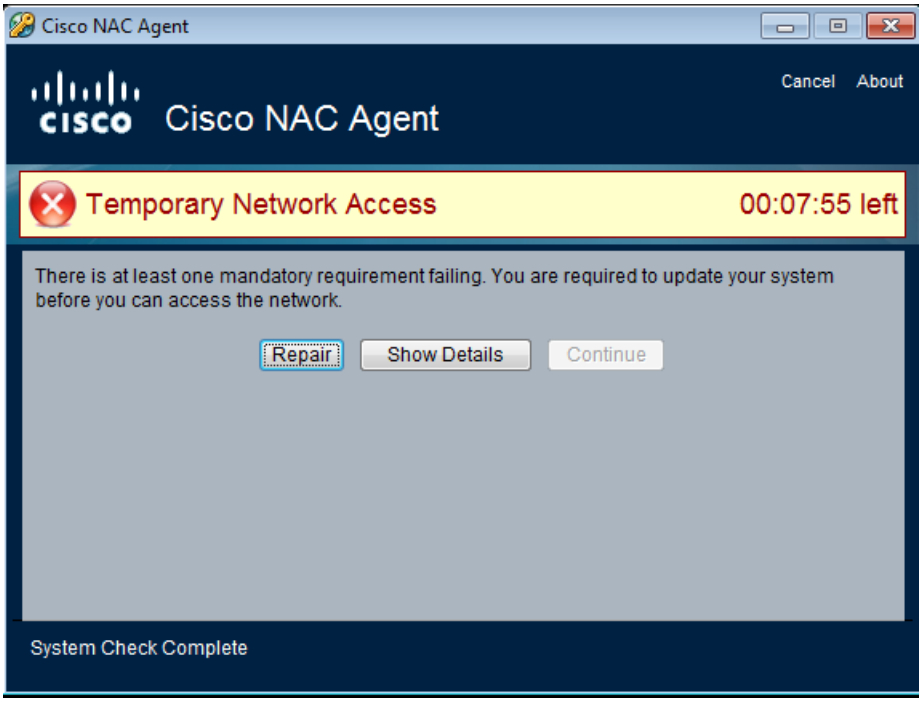
The NAC agent will pop up with a notification showing the device is non-compliant.



Step 2 Clicking on the details will notify the user what is failing and in this case we're missing the Watermark.txt in the c:\ directory (file requirement)



Step 3 Click Hide Details and now click the Repair button. When the posture policy was created a message was defined in the policy to message the user to add a Watermark.txt to the c:\ directory.



Review the ASA CLI

With the end-point in a non-compliant state ISE will call the redirect ACL on the ASA. From the ASA enable prompt of the CLI, run **sh vpn-sessiondb detail anyconnect.** You will notice ISE has assigned a session ID to the end-point shown below

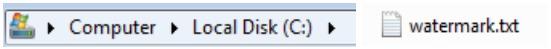
```
COA# sh vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username     : paul                   Index        : 12
Assigned IP  : 192.168.5.100          Public IP    :         .177
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
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     : 1065060                Bytes Rx     : 347025
Pkts Tx      : 2297                   Pkts Rx      : 2277
Pkts Tx Drop : 0                      Pkts Rx Drop : 0
Group Policy : COA_GroupPol           Tunnel Group : COA
Login Time   : 10:37:40 EDT Thu Jun 12 2014
Duration     : 0h:01m:45s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : c0a804010000c0005399bb34
Security Grp : none

AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1
```

ISE has assigned the end-point with the redirect ACL configured earlier in this guide. The end-point will only receive a new dACL once they have added the Watermark.txt to the c:\ directory or placed in quarantine if the NAC agent remediation timer expires.

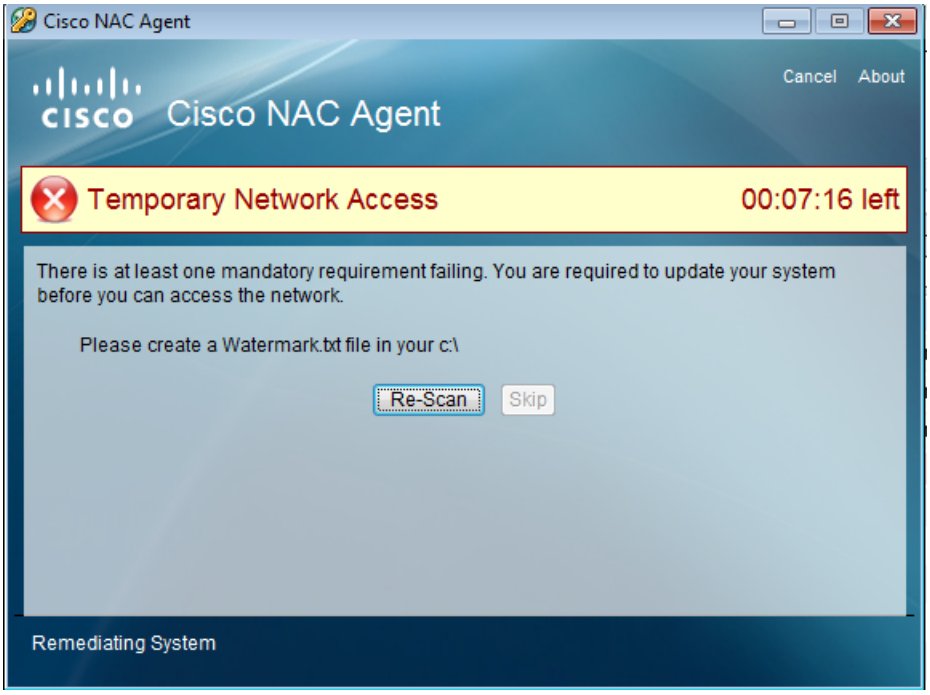
```
ISE Posture:
  Redirect URL : https://FCS-ISE.cert.loco:8443/guestportal/gateway?sessionId=c0a804010000c
0005399bf7a&action=cpp
  Redirect ACL : redirect
```

Add the Watermark.txt to the end-point and rescan

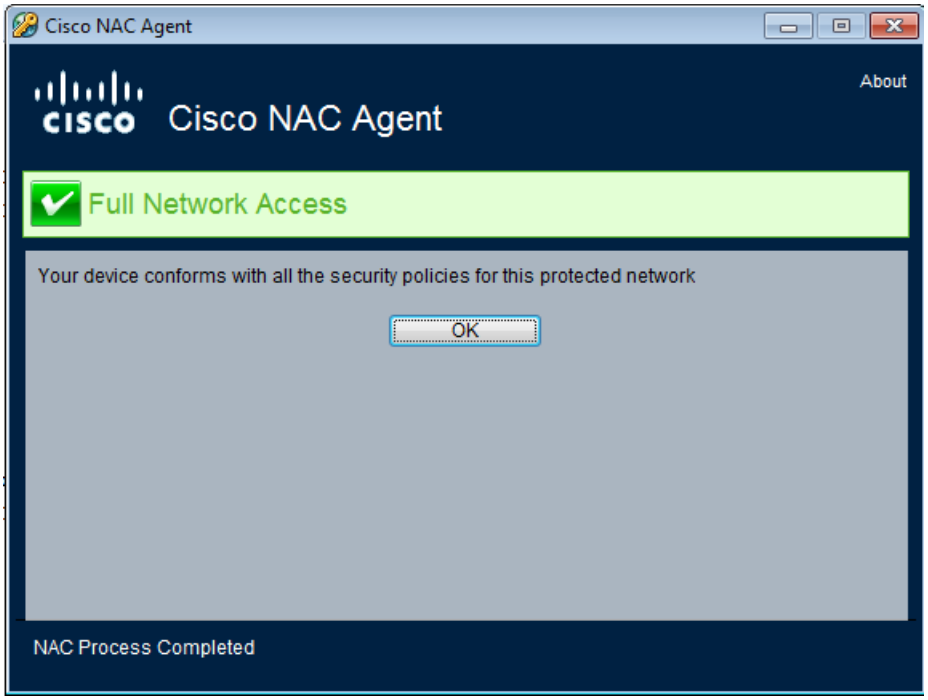
Step 1 Create a file named Watermark.txt and save it your c:\ directory



Step 2 With the watermark.txt added to the c:\ directory, select rescan from the NAC agent.



NAC will scan for the watermark.txt file and provide the user with full network access.



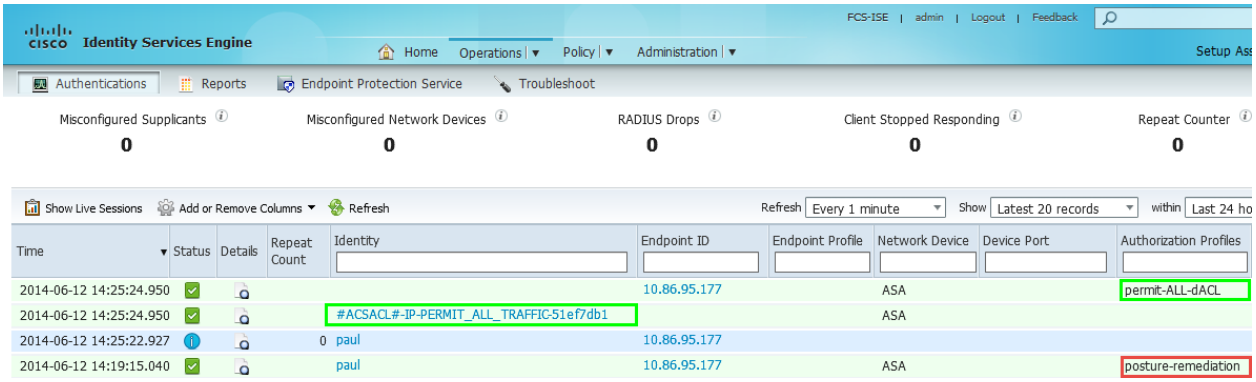
Review the ASA CLI and ISE logs

With the end-point now compliant, ISE will push down a dACL of permit ip any any onto the ASA. From the ASA enable prompt of the CLI, run **sh vpn-sessiondb detail anyconnect.** You will notice ISE has assigned the new dACL for the end-point shown below

```
DTLS-Tunnel:
  Tunnel ID    : 16.3
  Assigned IP  : 192.168.5.100          Public IP    :          .177
  Encryption   : AES128                 Hashing      : SHA1
  Encapsulation: DTLSv1.0               UDP Src Port : 64243
  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 3.1.05152
  Bytes Tx     : 89887                  Bytes Rx     : 64615
  Pkts Tx      : 318                    Pkts Rx      : 473
  Pkts Tx Drop : 0                      Pkts Rx Drop : 0
  Filter Name  : #ACSACL#-IP-PERMIT_ALL_TRAFFIC-51ef7db1
```

Review ISE operation logs

Procedure: Navigate **Operations→Authentications** and you should see the end-point went from noncompliant state (posture-remediation) to posture compliant (permit-ALL-dACL)


Identity Services Engine
FCS-ISE | admin | Logout | Feedback
Home
Operations
Policy
Administration
Setup Ass
Authentications
Reports
Endpoint Protection Service
Troubleshoot
Misconfigured Supplicants
0
Misconfigured Network Devices
0
RADIUS Drops
0
Client Stopped Responding
0
Repeat Counter
0
Show Live Sessions
Add or Remove Columns
Refresh
Refresh Every 1 minute
Show Latest 20 records
within Last 24 ho
Time
Status
Details
Repeat Count
Identity
Endpoint ID
Endpoint Profile
Network Device
Device Port
Authorization Profiles
2014-06-12 14:25:24.950
10.86.95.177
ASA
permit-ALL-dACL
2014-06-12 14:25:24.950
#ACSACL#-IP-PERMIT_ALL_TRAFFIC-51ef7db1
ASA
2014-06-12 14:25:22.927
0
paul
10.86.95.177
2014-06-12 14:19:15.040
paul
10.86.95.177
ASA
posture-remediation

References

http://www.cisco.com/c/en/us/td/docs/security/asa/compatibility/asamatrx.html#pgfId-42231

http://www.cisco.com/c/en/us/td/docs/security/asa/asa92/release/notes/asarn92.html