Ejemplo de Configuración de la Postura VPN de ASA Versión 9.2.1 con ISE

Contenido

Introducción

Este documento describe cómo configurar Cisco Adaptive Security Appliance (ASA) versión 9.2.1 para exponer a los usuarios de VPN frente a Cisco Identity Services Engine (ISE) sin necesidad de un nodo de estado en línea (IPN).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimientos básicos sobre la configuración de ASA CLI y la configuración de VPN con Secure Socket Layer (SSL)
- Conocimiento básico de la configuración de VPN de acceso remoto en ASA

- Conocimientos básicos de ISE y servicios de estado

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- Software Cisco ASA versión 9.2.1 y posteriores
- Microsoft Windows versión 7 con Cisco AnyConnect Secure Mobility Client versión 3.1
- Cisco ISE versión 1.2 con parche 5 o posterior

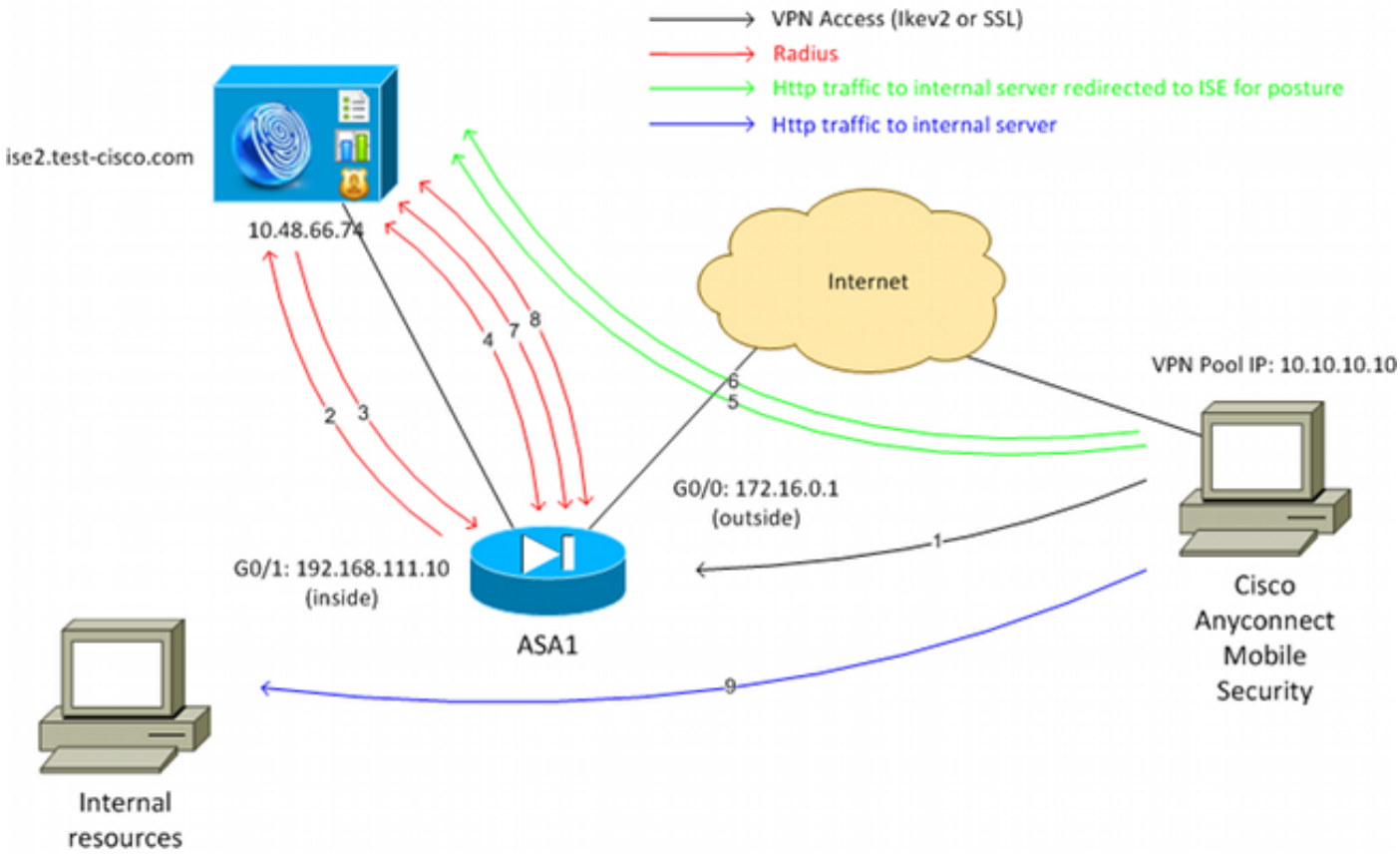
Antecedentes

La versión 9.2.1 de Cisco ASA admite el cambio de autorización (CoA) de RADIUS (RFC 5176). Esto permite el estado de los usuarios de VPN frente a Cisco ISE sin la necesidad de un IPN. Después de que un usuario de VPN inicia sesión, ASA redirige el tráfico web a ISE, donde el usuario se aprovisiona con un agente de control de admisión a la red (NAC) o un agente web. El agente realiza comprobaciones específicas en el equipo del usuario para determinar su conformidad con un conjunto configurado de reglas de estado, como sistema operativo (SO), parches, antivirus, servicio, aplicación o reglas del Registro.

Los resultados de la validación de estado se envían a ISE. Si se considera que la máquina presenta una queja, ISE puede enviar una CoA RADIUS al ASA con el nuevo conjunto de políticas de autorización. Después de la validación de estado y CoA correctas, el usuario puede acceder a los recursos internos.

Configurar

Diagrama de red y flujo de tráfico



Este es el flujo de tráfico, como se ilustra en el diagrama de red:

1. El usuario remoto utiliza Cisco Anyconnect para el acceso VPN al ASA.

2. ASA envía una solicitud de acceso RADIUS para ese usuario a ISE.

3. Esta solicitud afecta a la política denominada **condición de ASA92** en ISE. Como resultado, se devuelve el perfil de autorización **de estado ASA92**. ISE envía una aceptación de acceso RADIUS con dos pares atributo-valor de Cisco:

   url-redirect-acl=redirect: se trata del nombre de la lista de control de acceso (ACL) que se define localmente en el ASA, que decide el tráfico que se debe redirigir.

   url-redirect=https://ise2.test-cisco.com:8443/guestportal/gateway?sessionId=xx&action=cpp: URL a la que se debe redirigir al usuario remoto.**Sugerencia**: los servidores del sistema de nombres de dominio (DNS) asignados a los clientes VPN deben poder resolver el nombre de dominio completo (FQDN) que se devuelve en la URL de redirección. Si los filtros VPN se configuran para restringir el acceso en el nivel de grupo de túnel, asegúrese de que el grupo de clientes pueda acceder al servidor ISE en el puerto configurado (**TCP 8443** en este ejemplo).
4. El ASA envía un paquete de inicio de solicitud de contabilización de RADIUS y recibe una respuesta. Esto es necesario para enviar todos los detalles relativos a la sesión a ISE. Estos detalles incluyen session_id, la dirección IP externa del cliente VPN y la dirección IP del ASA. ISE utiliza session_id para identificar esa sesión. El ASA también envía información de cuenta temporaria periódica, donde el atributo más importante es Framed-IP-Address con la IP que el ASA asigna al cliente (**10.10.10.10** en este ejemplo).

5. Cuando el tráfico del usuario VPN coincide con la ACL definida localmente (redirección), se redirige a **https://ise2.test-cisco.com:8443**. En función de la configuración, ISE aprovisiona al agente NAC o al agente web.

6. Una vez instalado el agente en el equipo cliente, realiza automáticamente comprobaciones específicas. En este ejemplo, busca el archivo **c:\test.txt**. También envía un informe de estado a ISE, que puede incluir varios intercambios con el uso del protocolo SWISS y los puertos TCP/UDP 8905 para acceder a ISE.

7. Cuando ISE recibe el informe de estado del agente, vuelve a procesar las reglas de autorización. Esta vez, se conoce el resultado de la postura y se aplica otra regla. Envía un paquete CoA RADIUS:

   Si el usuario cumple con la normativa, se envía un nombre de ACL descargable (DACL) que permite el acceso completo (conforme a la regla ASA92 de AuthZ).

   Si el usuario no cumple con la normativa, se envía un nombre de DACL que permite el acceso limitado (regla ASA92 de AuthZ no conforme).**Nota**: RADIUS CoA siempre se confirma; es decir, el ASA envía una respuesta al ISE para confirmar.
8. ASA elimina la redirección. Si no tiene las DACL almacenadas en caché, debe enviar una solicitud de acceso para descargarlas de ISE. La DACL específica se asocia a la sesión VPN.

9. La próxima vez que el usuario de VPN intente acceder a la página web, podrá acceder a todos los recursos permitidos por la DACL que está instalada en el ASA.
   Si el usuario no cumple las normas, solo se concede acceso limitado.
   Nota: Este modelo de flujo difiere de la mayoría de los escenarios que utilizan RADIUS CoA. Para las autenticaciones 802.1x por cable/inalámbricas, RADIUS CoA no incluye ningún atributo. Sólo activa la segunda autenticación en la que se adjuntan todos los atributos, como DACL. Para el estado de VPN ASA, no hay una segunda autenticación. Todos los atributos se devuelven en RADIUS CoA. La sesión VPN está activa y no es posible cambiar la mayoría de los parámetros de usuario de VPN.

Configuraciones

Utilice esta sección para configurar ASA e ISE.

ASA

Esta es la configuración básica de ASA para el acceso de Cisco AnyConnect:

```
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 192.168.111.10 255.255.255.0

aaa-server ISE protocol radius
aaa-server ISE (inside) host 10.48.66.74
 key cisco

webvpn
 enable outside
 anyconnect-essentials
 anyconnect image disk0:/anyconnect-win-3.1.02040-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
```

Para la integración de ASA con el estado de ISE, asegúrese de que:

- Configure el servidor de Autenticación, Autorización y Contabilización (AAA) para la autorización dinámica para aceptar CoA.
- Configure la contabilización como un grupo de túnel para enviar los detalles de la sesión VPN hacia ISE.
- Configure la contabilidad provisional que enviará la dirección IP asignada al usuario y actualice periódicamente el estado de la sesión en ISE
- Configure la ACL de redirección, que decide si se permite el tráfico DNS e ISE. El resto del tráfico HTTP se redirige al ISE para su estado.

Este es el ejemplo de configuración:

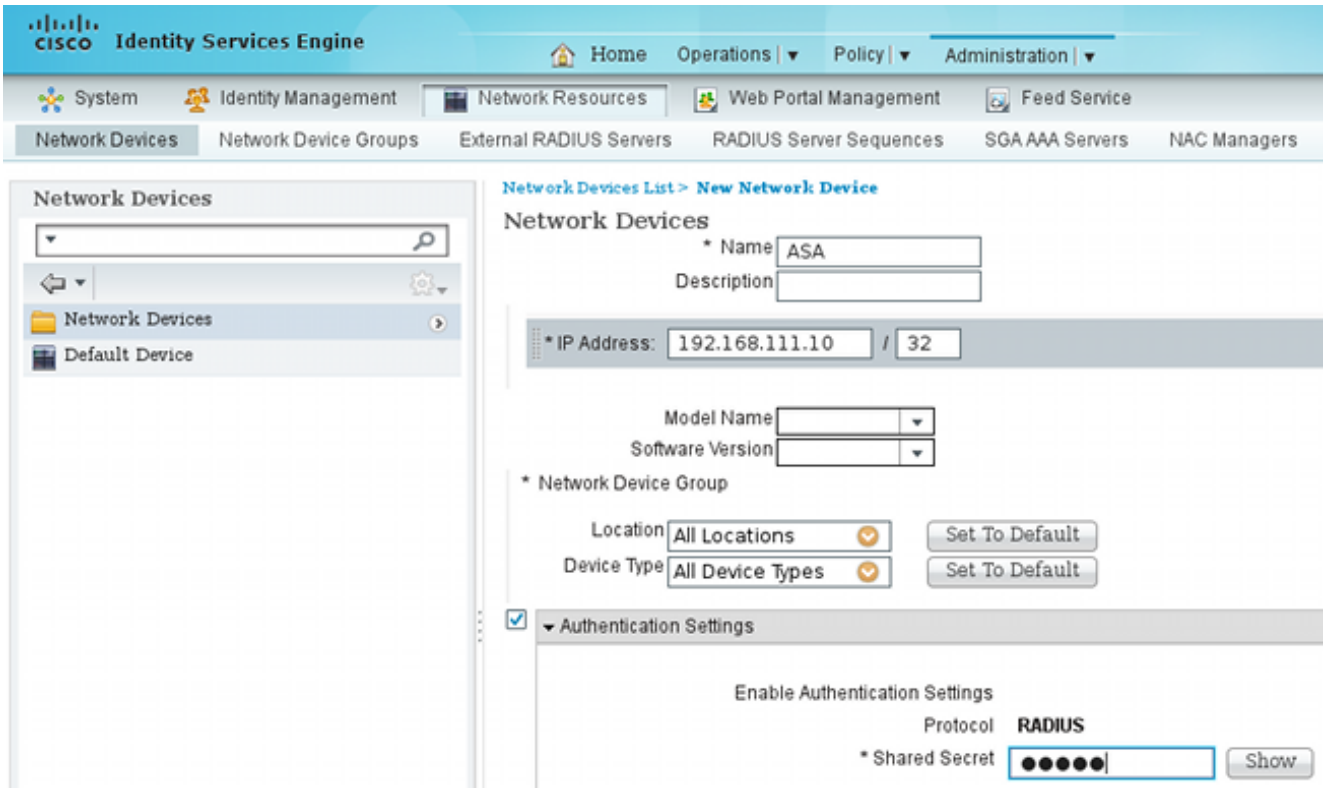
```
access-list redirect extended deny udp any any eq domain
access-list redirect extended deny ip any host 10.48.66.74
access-list redirect extended deny icmp any any
access-list redirect extended permit tcp any any eq www

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
```

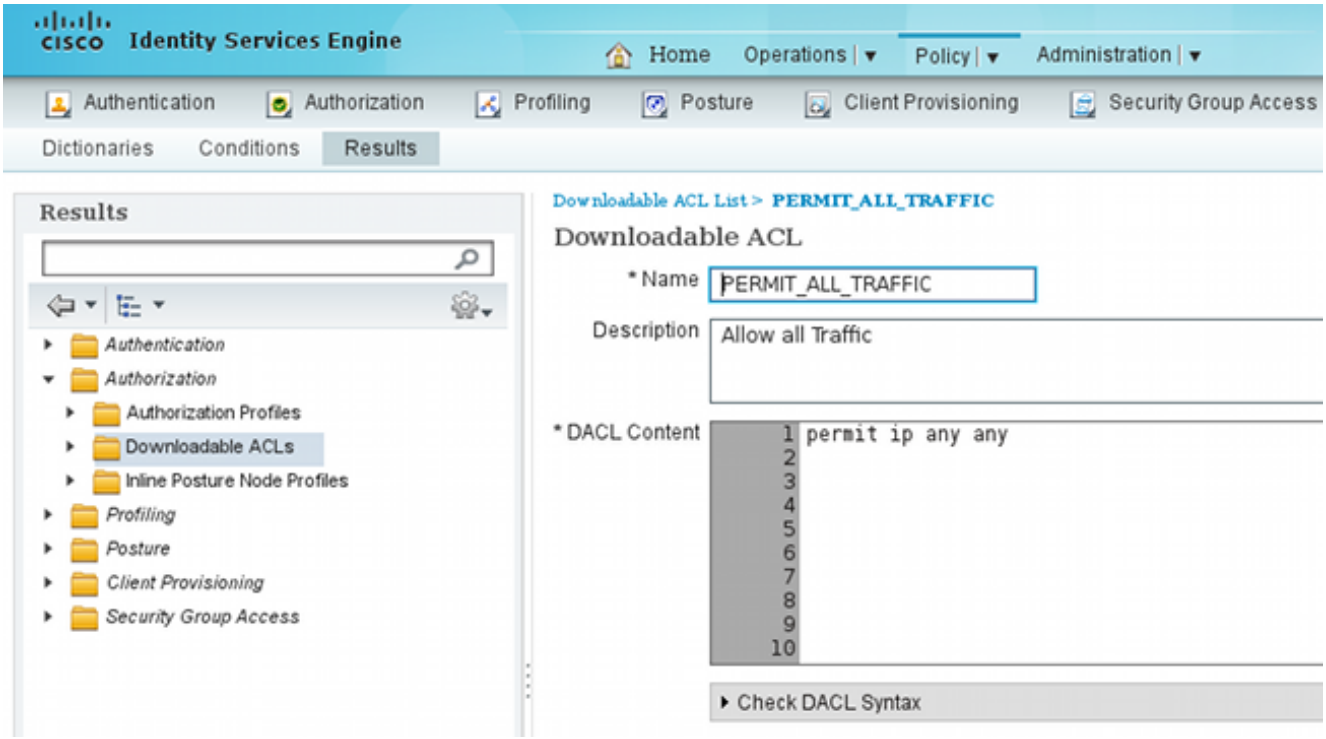
ISE

Complete estos pasos para configurar el ISE:

1. Vaya a **Administration > Network Resources > Network Devices** y agregue el ASA como un dispositivo de red:

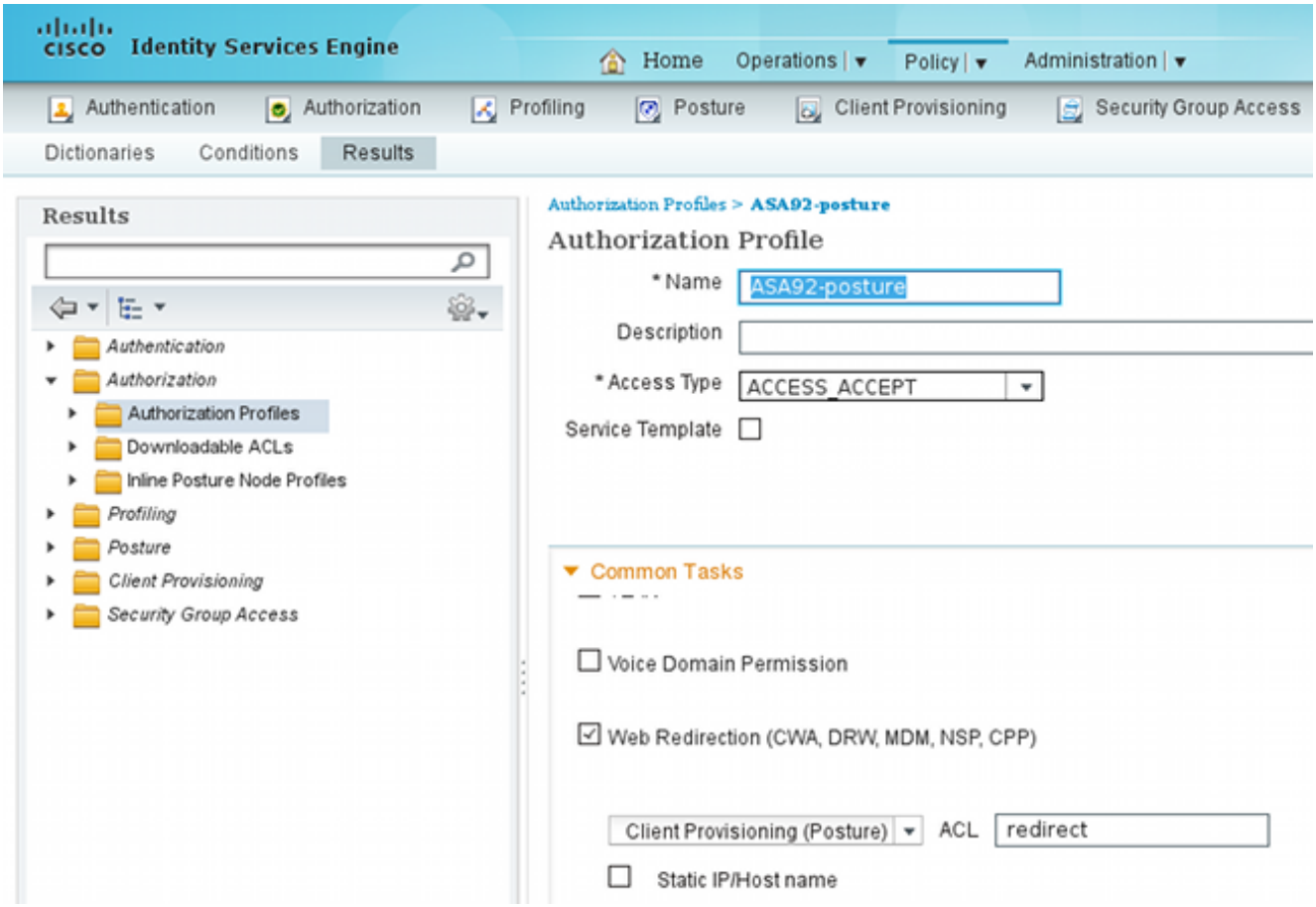


2. Vaya a **Policy > Results > Authorization > Downloadable ACL** y configure la DACL de modo que permita el acceso completo. La configuración de ACL predeterminada permite todo el tráfico IP en ISE:

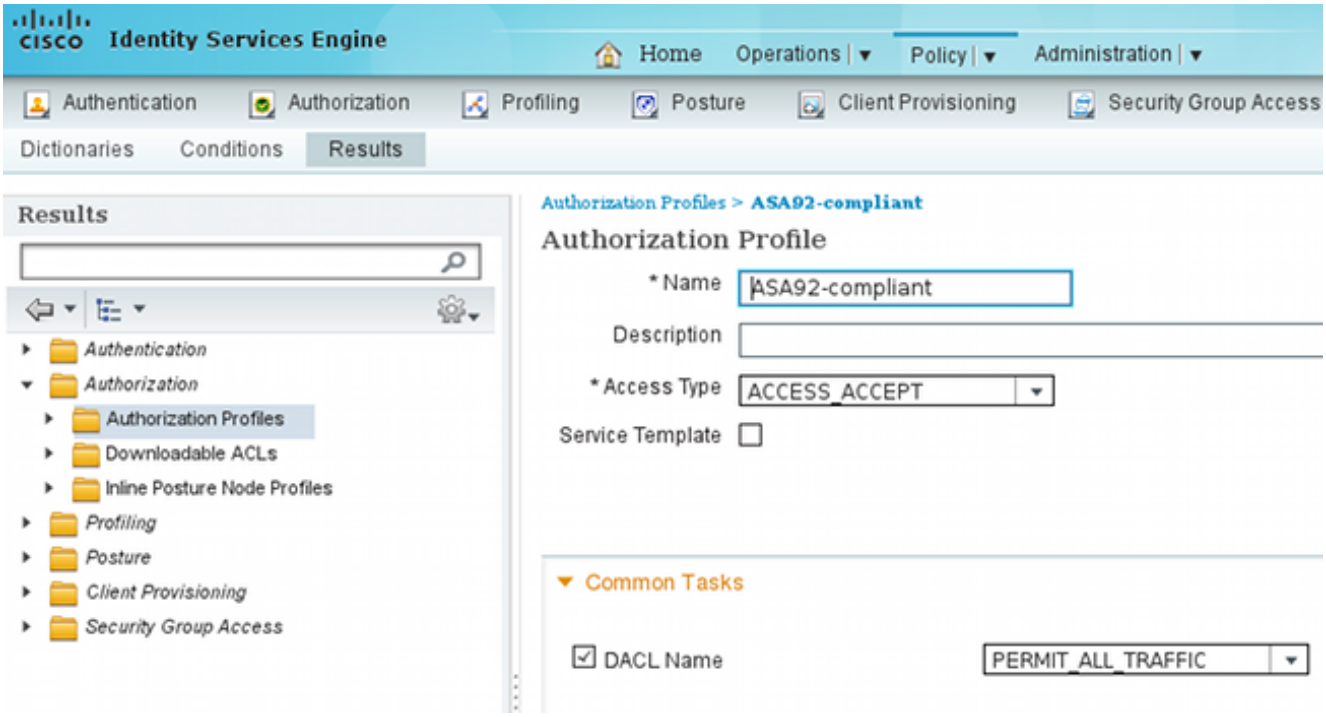


3. Configure una ACL similar que proporcione acceso limitado (para usuarios no conformes).

4. Navegue hasta **Policy > Results > Authorization > Authorization Profiles** y configure el perfil de autorización llamado **ASA92-posture**, que redirige a los usuarios para el estado. Marque la casilla de verificación **Web Redirection**, seleccione **Client Provisioning** en la lista desplegable y asegúrese de que **redirect** aparezca en el campo ACL (esa ACL se define localmente en ASA):



5. Configure el perfil de autorización denominado **compatible con ASA92**, que solo debe devolver la DACL denominada **PERMIT_ALL_TRAFFIC** que proporciona acceso completo a los usuarios compatibles:



6. Configure un perfil de autorización similar denominado **ASA92-noncompliance**, que debería devolver la DACL con acceso limitado (para usuarios no conformes).

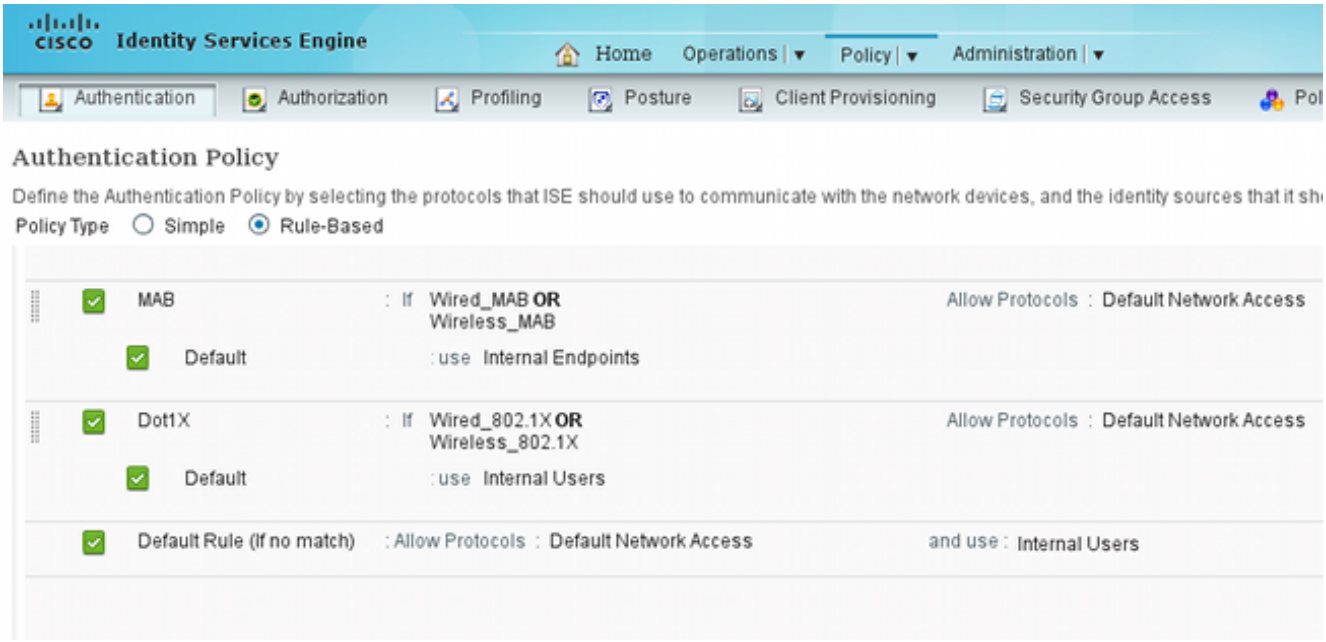
7. Navegue hasta **Policy > Authorization** y configure las reglas de autorización:

   Cree una regla que permita el acceso completo si los resultados del estado son compatibles. El resultado es que la política de autorización **cumple con ASA92**.

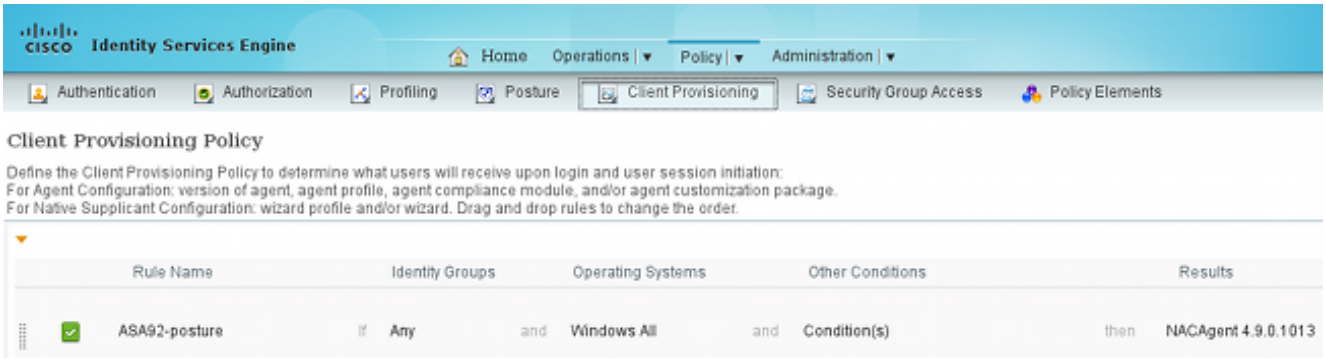
   Cree una regla que permita un acceso limitado si los resultados del estado no son conformes. El resultado es que la política de autorización **ASA92 no es conforme**.

   Asegúrese de que si ninguna de las dos reglas anteriores es alcanzada, la regla predeterminada devuelve la **postura ASA92**, que fuerza una redirección en el ASA.

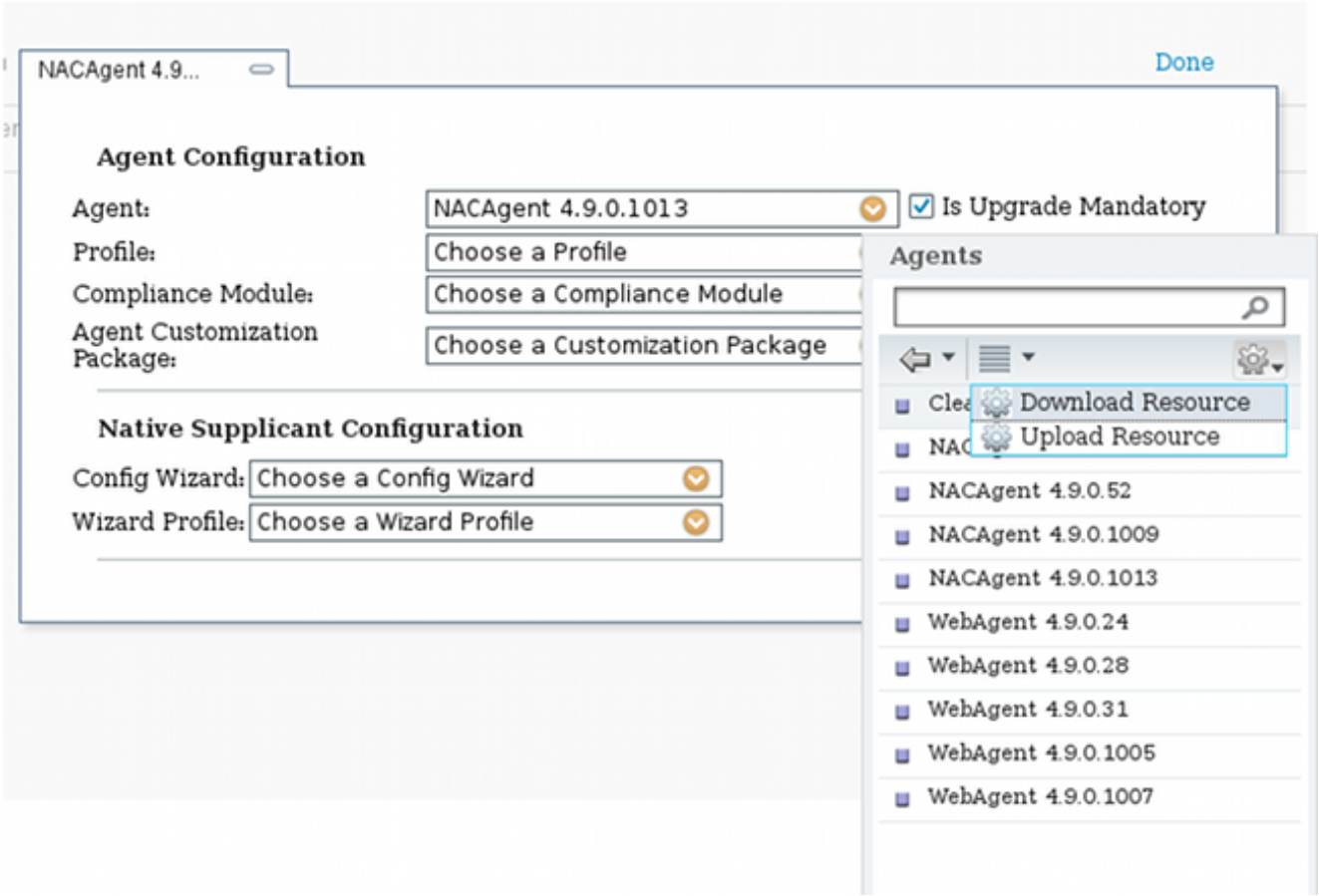
8. Las reglas de autenticación predeterminadas comprueban el nombre de usuario en el almacén de identidad interno. Si debe cambiarse (por ejemplo, si está activado en Active Directory (AD)), vaya a **Directiva > Autenticación** y realice el cambio:



9. Vaya a **Policy > Client Provisioning** y configure las reglas de aprovisionamiento. Estas son las reglas que deciden el tipo de agente que se debe aprovisionar. En este ejemplo, solo existe una regla simple, e ISE selecciona el agente NAC para todos los sistemas de Microsoft Windows:



Cuando los agentes no están en el ISE, es posible descargarlos:



10. Si es necesario, puede navegar hasta **Administration > System > Settings > Proxy** y configurar el proxy para ISE (para acceder a Internet).

11. Configure las reglas de estado, que comprueban la configuración del cliente. Puede configurar reglas que comprueben:

    archivos: existencia, versión, fecha

    registro: clave, valor, existencia

    aplicación: nombre de proceso, en ejecución, no en ejecución

    servicio: nombre de servicio, en ejecución, no en ejecución

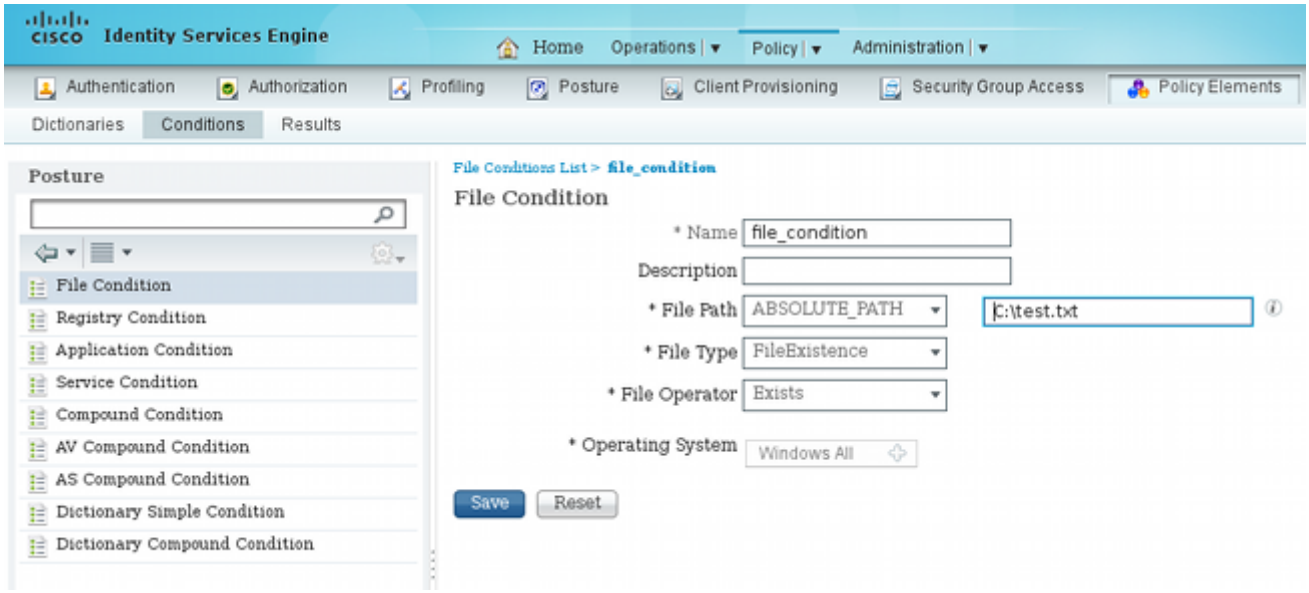
    antivirus: más de 100 proveedores admitidos, versión, cuando se actualizan las definiciones

    antispyware: más de 100 proveedores admitidos, versión, cuando se actualizan las definiciones

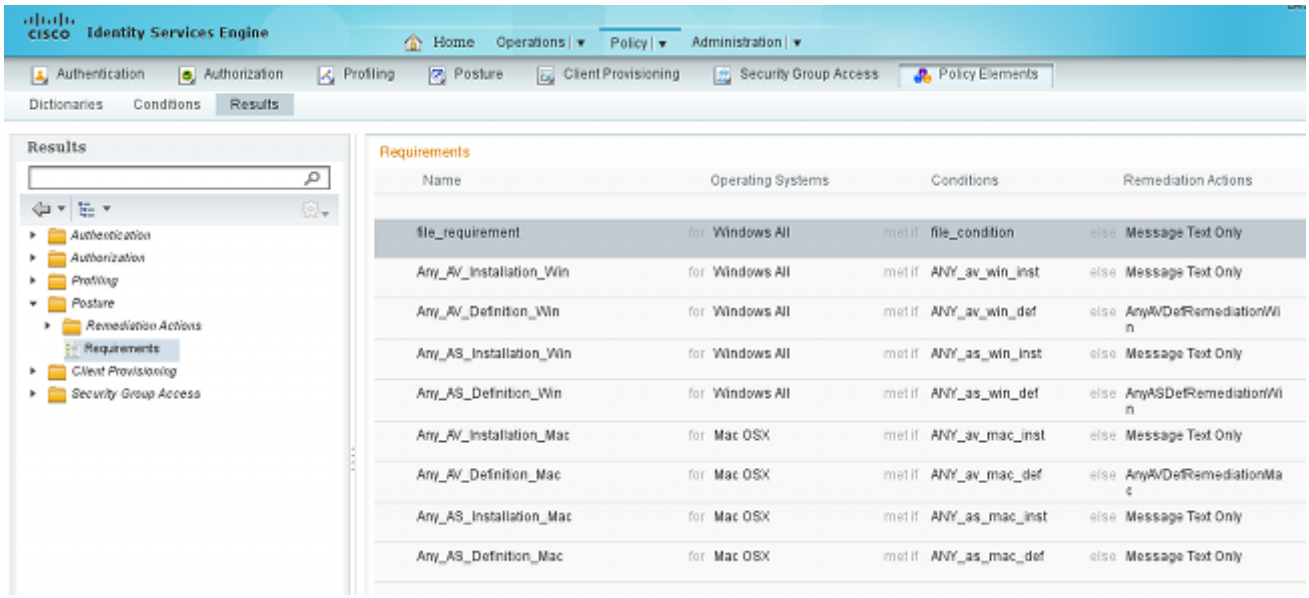
    condición compuesta - mezcla de todos

    condiciones de diccionario personalizadas - uso de la mayoría de los diccionarios ISE

12. En este ejemplo, sólo se realiza una simple comprobación de la existencia de un archivo. Si el archivo **c:\test.txt** está presente en el equipo cliente, es compatible y tiene acceso completo. Vaya a **Policy > Conditions > File Conditions** y configure la condición del archivo:

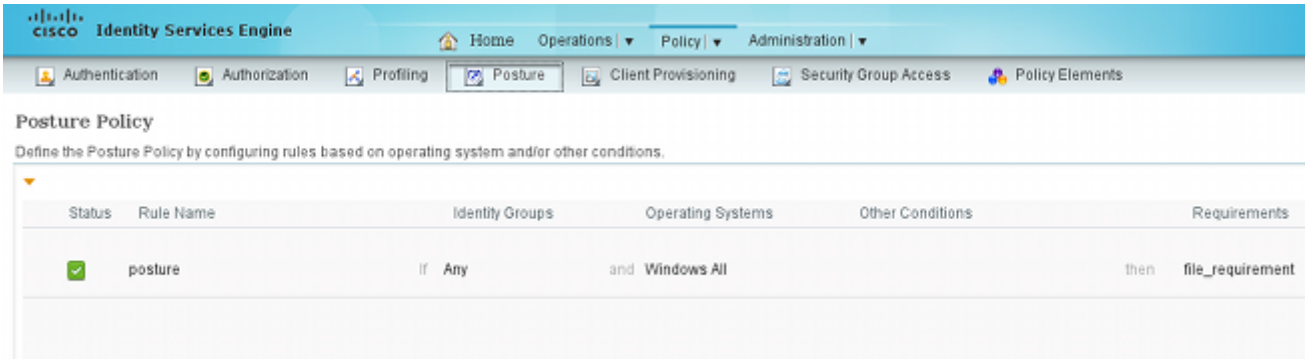


13. Navegue hasta **Política > Resultados > Postura > Requisitos** y cree un requisito. Este requisito debe cumplirse cuando se cumpla la condición anterior. Si no es así, se ejecuta la acción de remediación. Puede haber muchos tipos de acciones de remediación disponibles, pero en este ejemplo se utiliza la más sencilla: se muestra un mensaje específico.



Nota: en una situación normal, se puede utilizar la acción de remediación de archivos (ISE proporciona el archivo descargable).

14. Navegue hasta **Policy > Posture** y utilice el requisito que creó en el paso anterior (llamado **file_required**) en las reglas de postura. La única regla de estado requiere que todos los sistemas de Microsoft Windows cumplan el **file_required**. Si se cumple este requisito, la estación cumple los requisitos; si no se cumple, la estación no cumple los requisitos.

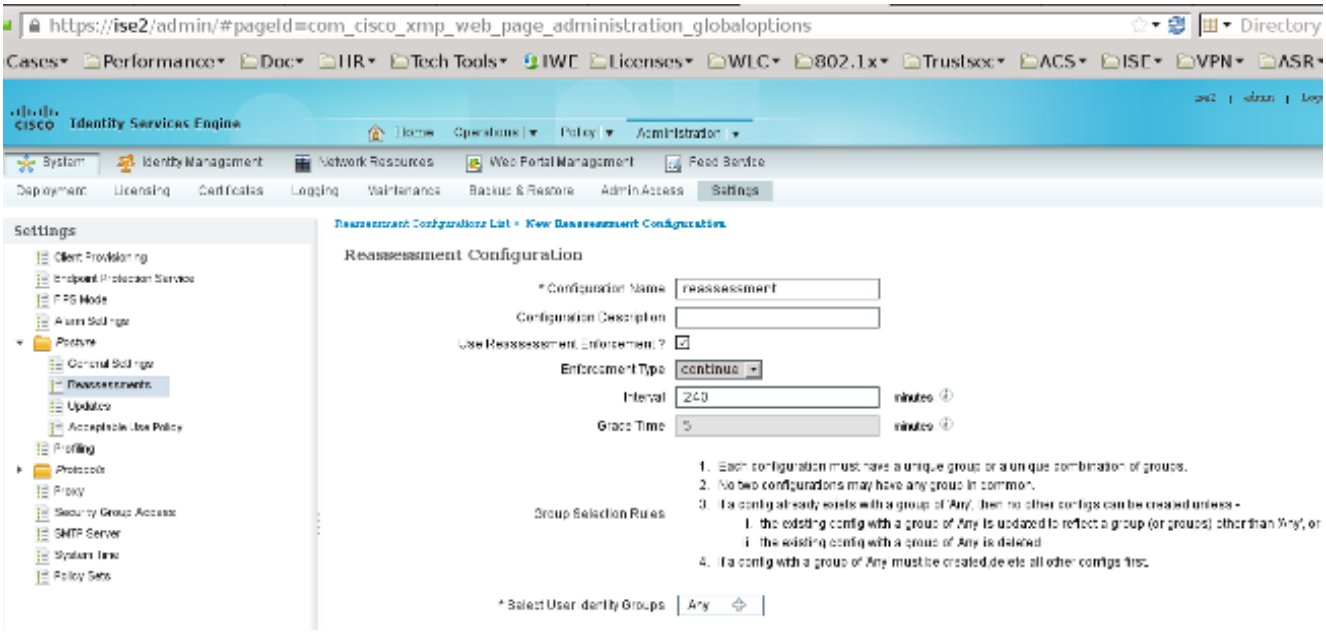


Reevaluación periódica

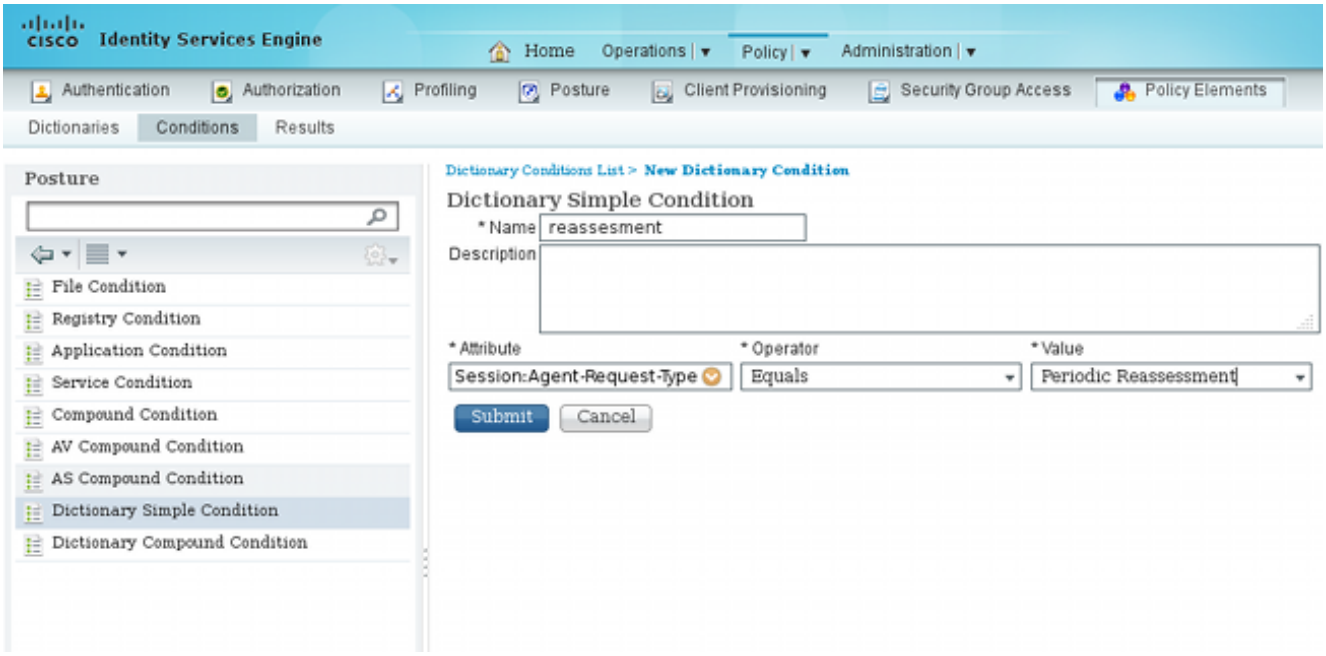
De forma predeterminada, el estado es un evento que se produce una sola vez. Sin embargo, a veces es necesario comprobar periódicamente la conformidad del usuario y ajustar el acceso a los recursos en función de los resultados. Esta información se envía a través del protocolo SWISS (agente NAC) o se codifica dentro de la aplicación (agente web).

Complete estos pasos para verificar la conformidad del usuario:

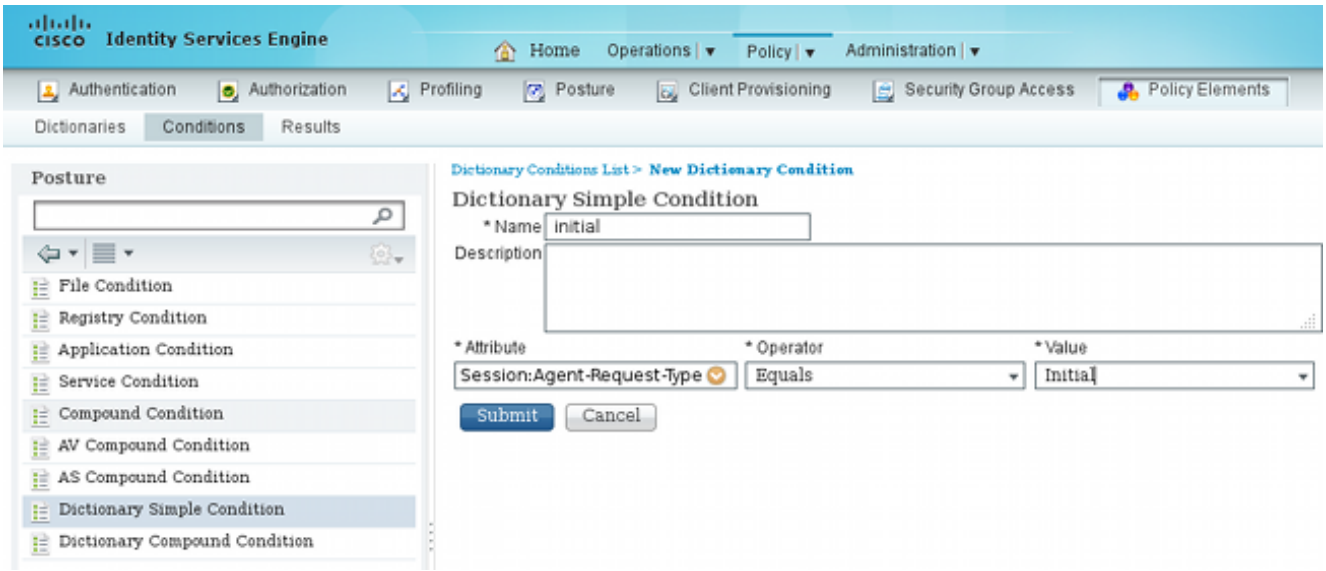
1. Vaya a **Administration > Settings > Posture > Reassessment** y habilite la reevaluación globalmente (por configuración de grupo de identidad):



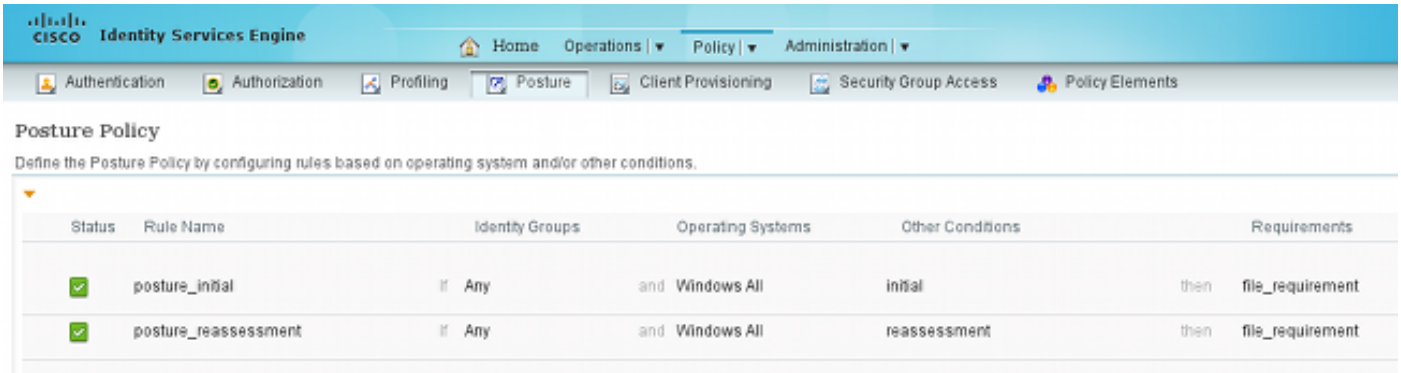
2. Cree una condición de estado que coincida con todas las reevaluaciones:



3. Cree una condición similar que coincida sólo con las evaluaciones iniciales:



Ambas condiciones se pueden utilizar en las reglas de postura. La primera regla coincide sólo con las evaluaciones iniciales y la segunda coincide con todas las evaluaciones subsiguientes:



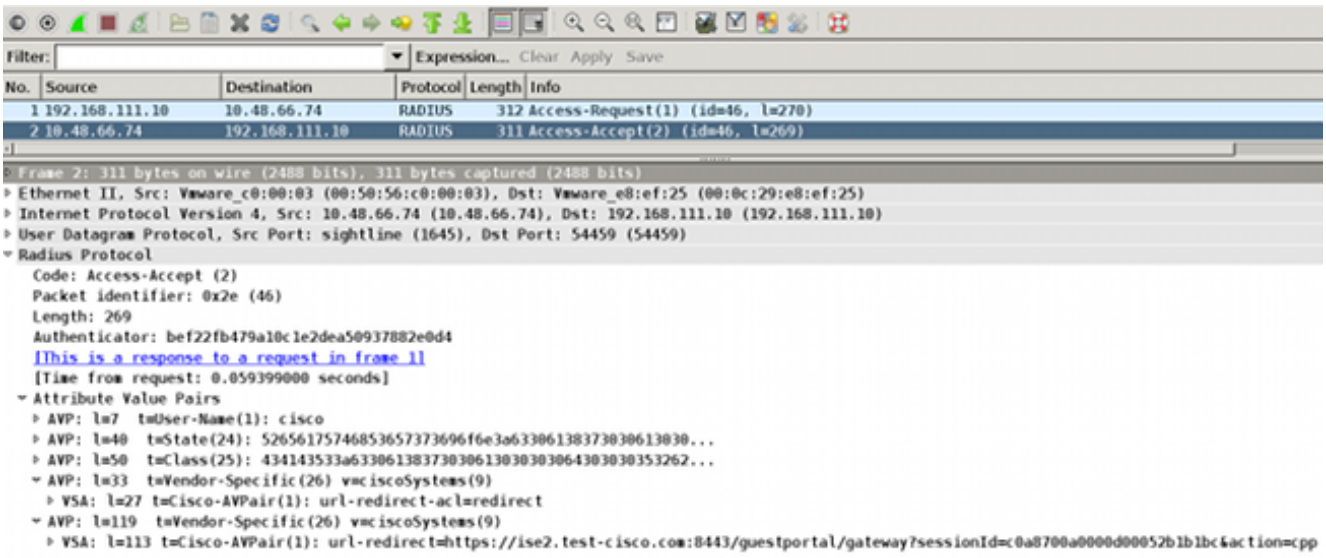
Verificación

Para confirmar que su configuración funciona correctamente, asegúrese de que estos pasos se

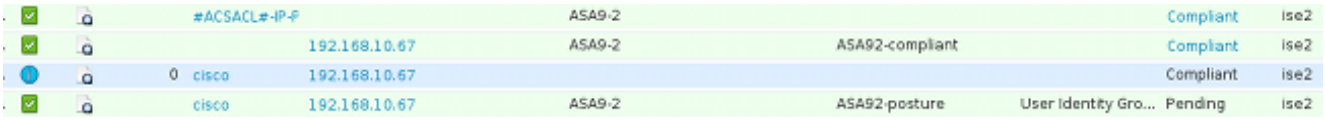
completan como se describe a continuación:

1. El usuario VPN se conecta al ASA.

2. ASA envía una solicitud RADIUS y recibe una respuesta con los atributos **url-redirect** y **url-redirect-acl**:



3. Los registros de ISE indican que la autorización coincide con el perfil de estado (la primera entrada de registro):



4. ASA agrega un redireccionamiento a la sesión VPN:

```
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. El estado de la sesión VPN en el ASA muestra que el estado es obligatorio y redirige el tráfico HTTP:

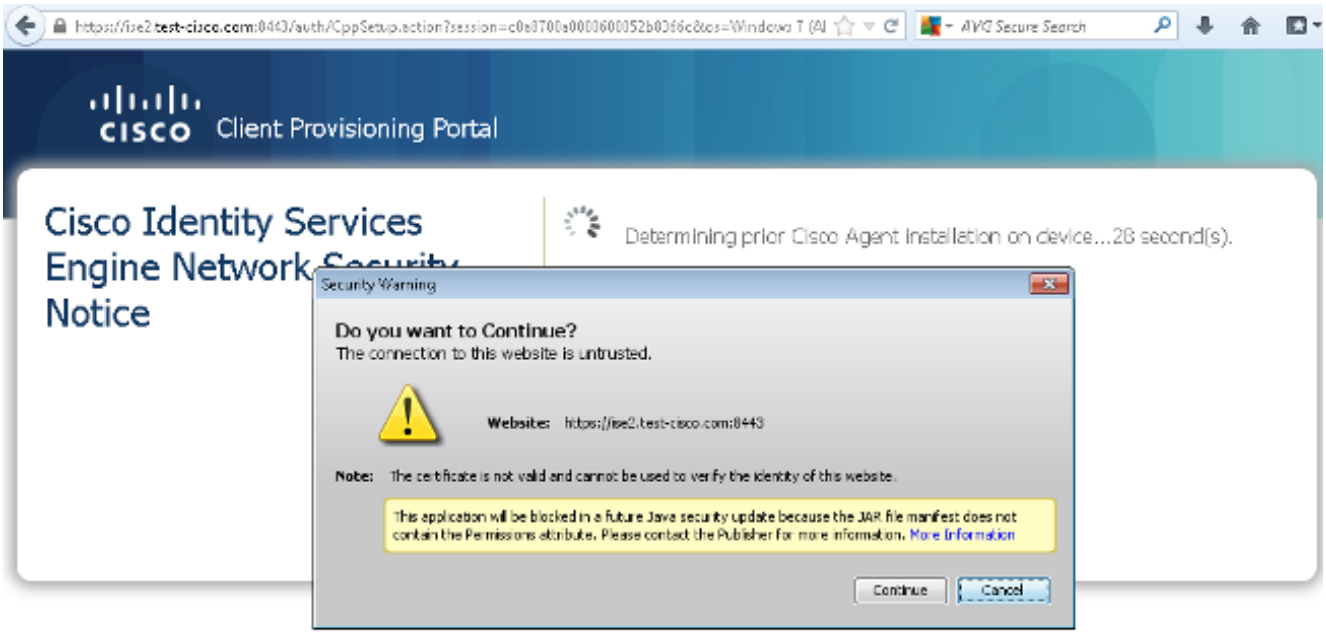
```
ASA# show vpn-sessiondb detail anyconnect

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     : 19497
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
```

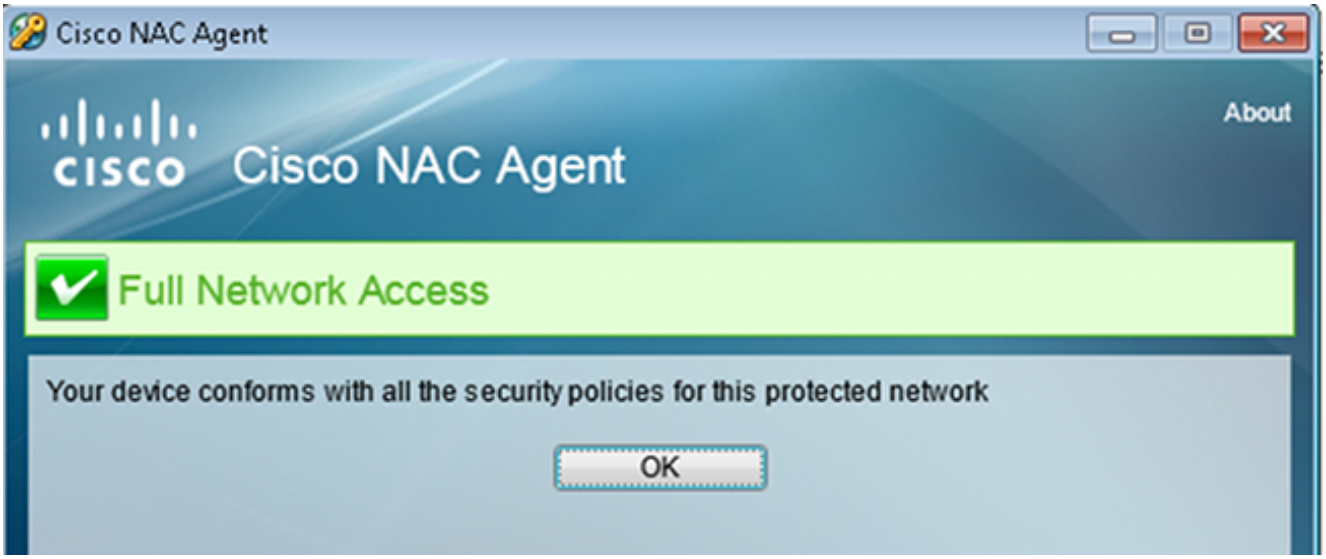
6. El cliente que inicia el tráfico HTTP que coincide con la ACL de redirección se redirige a ISE:

```
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. El cliente se redirige a ISE para conocer el estado:



8. El agente NAC está instalado. Una vez instalado el agente NAC, descarga las reglas de estado a través del protocolo SWISS y realiza comprobaciones para determinar el cumplimiento. A continuación, el informe de estado se envía al ISE.

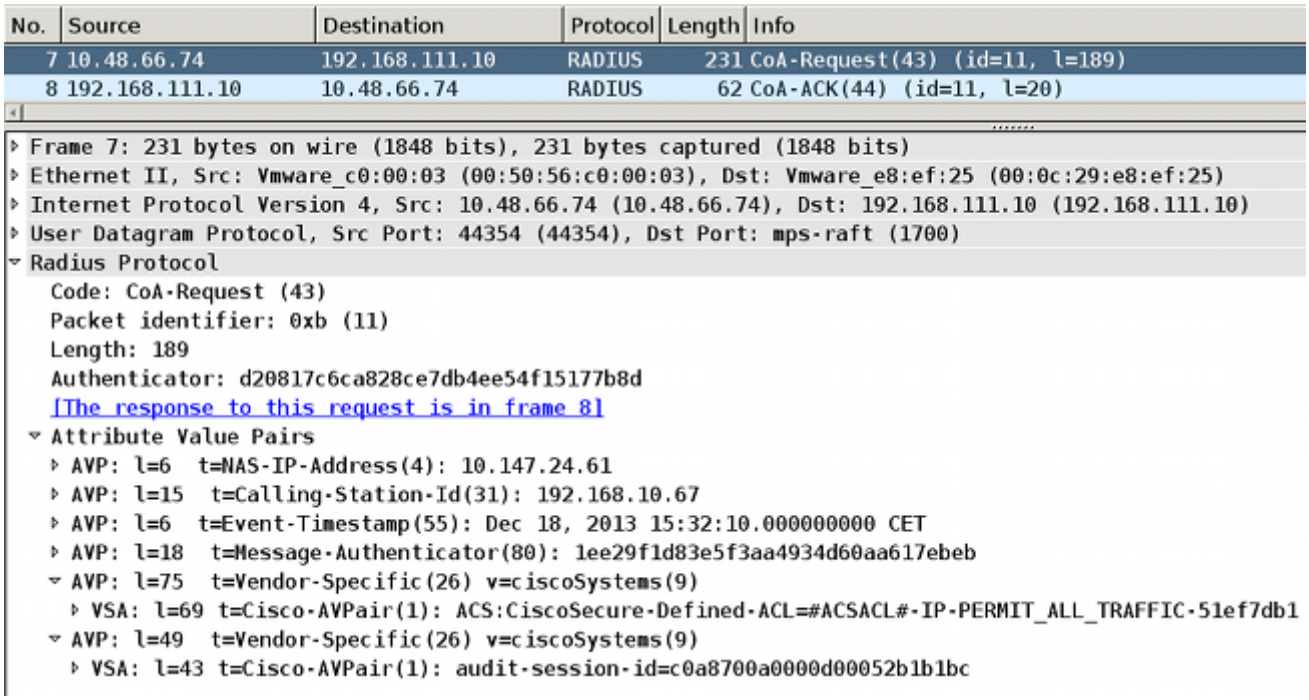


9. ISE recibe el informe de estado, vuelve a evaluar las reglas de autorización y (si es necesario) cambia el estado de autorización y envía una CoA. Esto se puede verificar en **ise-psc.log**:

```
cisco.cpm.posture.runtime.PostureHandlerImpl -:cisco:c0a8700a0000900052b840e6
 :::- Decrypting report
cisco.cpm.posture.runtime.PostureManager -:cisco:c0a8700a0000900052b840e6
 :::- User 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. ISE envía una CoA de RADIUS que incluye el **session_id** y el nombre de DACL que permite

el acceso completo:



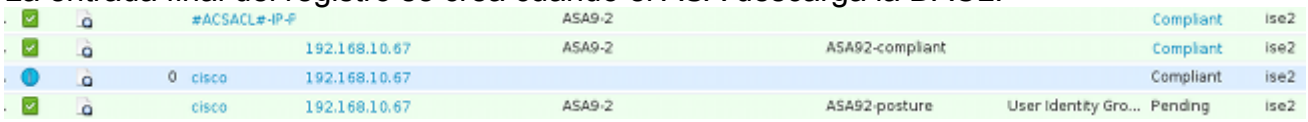
Esto se refleja en los registros de ISE:

La primera entrada del registro es para la autenticación inicial que devuelve el perfil de estado (con redirección).

La segunda entrada de registro se rellena después de recibir el informe SWISS conforme.

La tercera entrada del registro se rellena cuando se envía el CoA, junto con la confirmación (descrita como Autorización dinámica correcta).

La entrada final del registro se crea cuando el ASA descarga la DACL.



11. Las depuraciones en el ASA muestran que se recibe el CoA y se elimina el redireccionamiento. ASA descarga las DACL si es necesario:

```
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. Después de la sesión VPN, Cisco aplica la DACL (acceso completo) para el usuario:

```
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
```

Nota: ASA siempre elimina las reglas de redirección, incluso cuando el CoA no tiene ninguna DACL conectada.

Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

Depuraciones en ISE

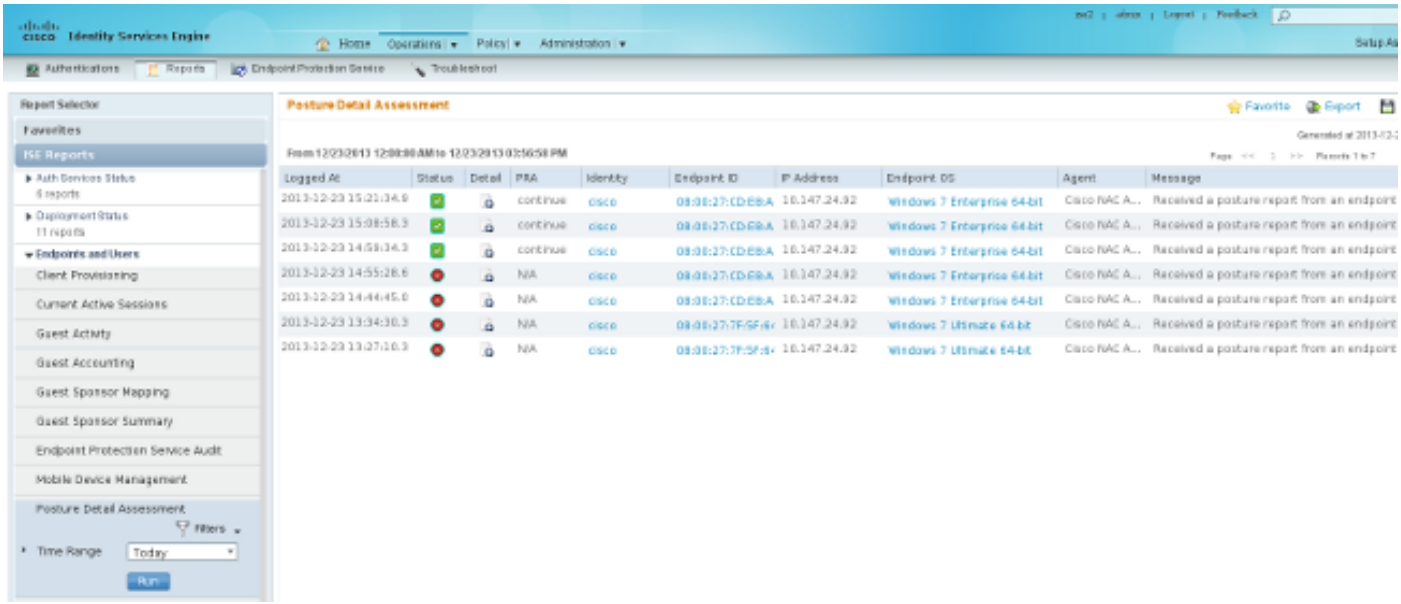
Navegue hasta **Administration > Logging > Debug Log Configuration** para habilitar los debugs. Cisco recomienda habilitar las depuraciones temporales para:

- SUIZO
- Reenvío ininterrumpido (NSF)
- NSF-Session
- Aprovisionamiento
- Condición

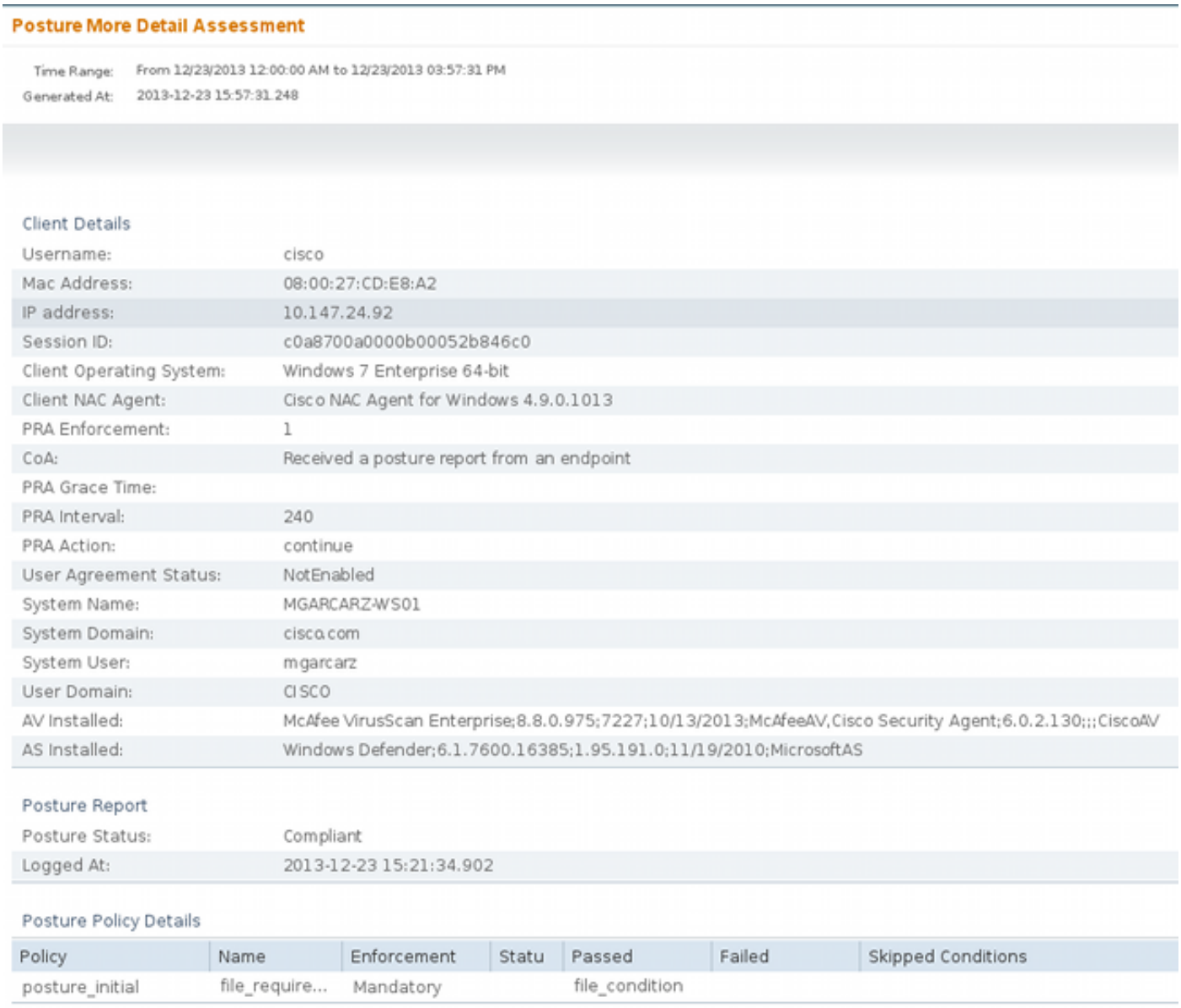
Ingrese este comando en la CLI para ver las depuraciones:

```
ise2/admin# show logging application ise-psc.log tail count 100
```

Navegue hasta **Operaciones > Informes > Informes de ISE > Terminales y usuarios > Evaluación de detalles de estado** para ver los informes de estado:



En la página Evaluación más detallada de la posición, se muestra un nombre de directiva con un nombre de requisito, junto con los resultados:



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		

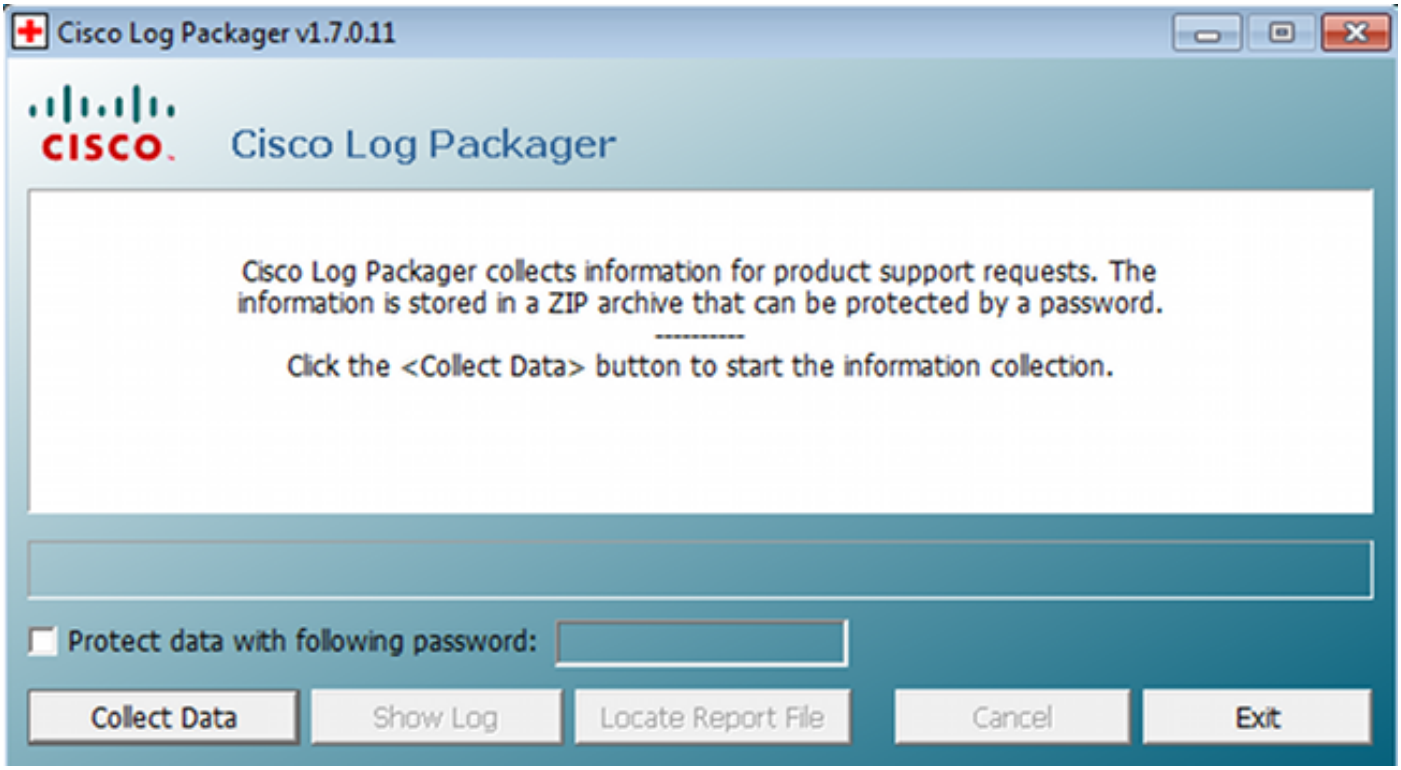
Depuraciones en ASA

Puede habilitar estos debugs en el ASA:

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

Depuraciones para el agente

Para el agente NAC, es posible recopilar las depuraciones con Cisco Log Packager, que se inicia desde la GUI o con la CLI: **CCAgentLogPackager.app**.



Sugerencia: puede descodificar los resultados con la herramienta Technical Assistance Center (TAC).

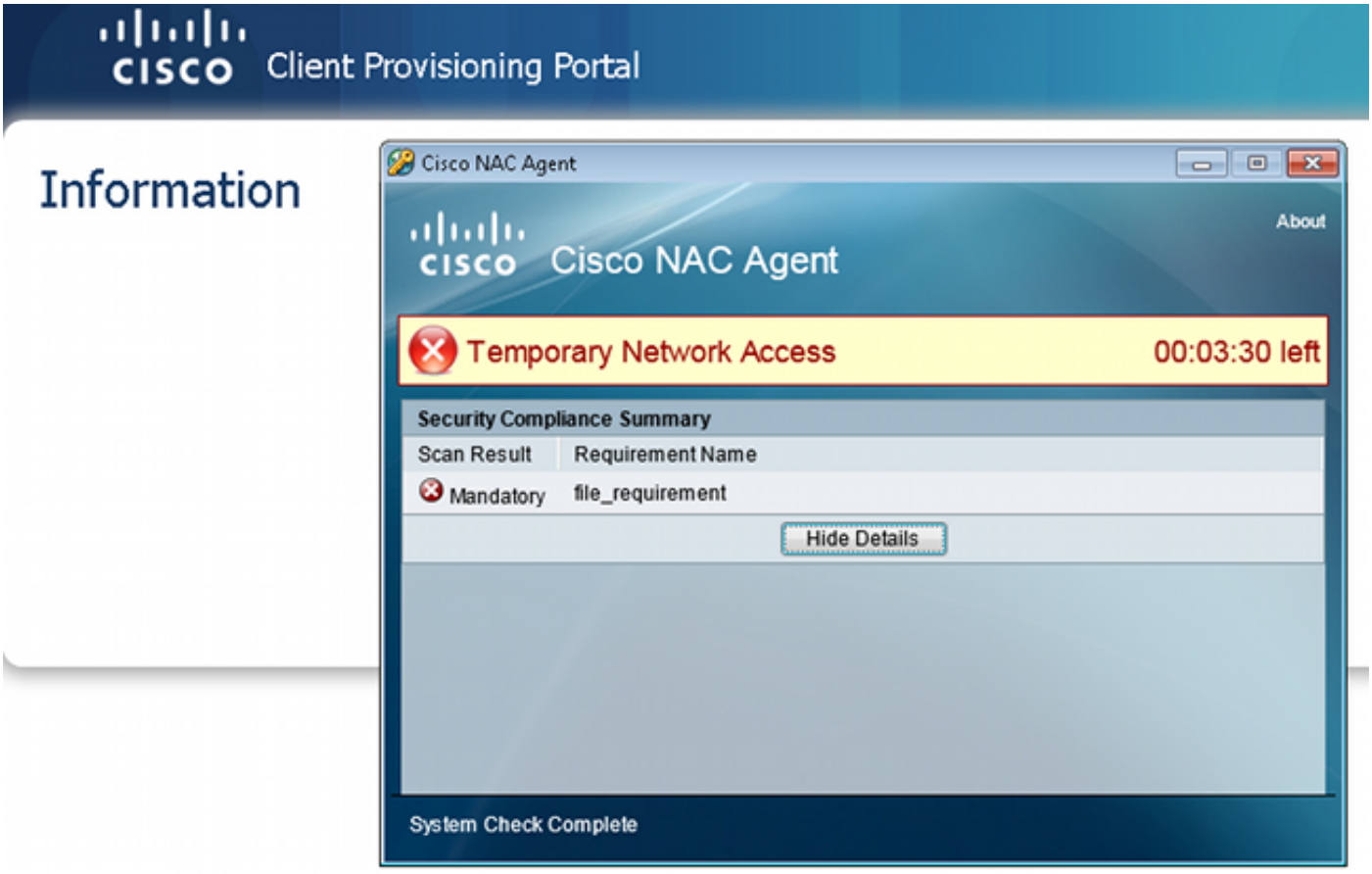
Para recuperar los registros para el Agente Web, navegue hasta estas ubicaciones:

- **C: > Documento y configuración > *<user>* > Configuración local > Temperatura > webagent.log** (descodificado con la herramienta TAC)
- **C: > Documento y configuración > *<user>* > Configuración local > Temperatura > webagentsetup.log**

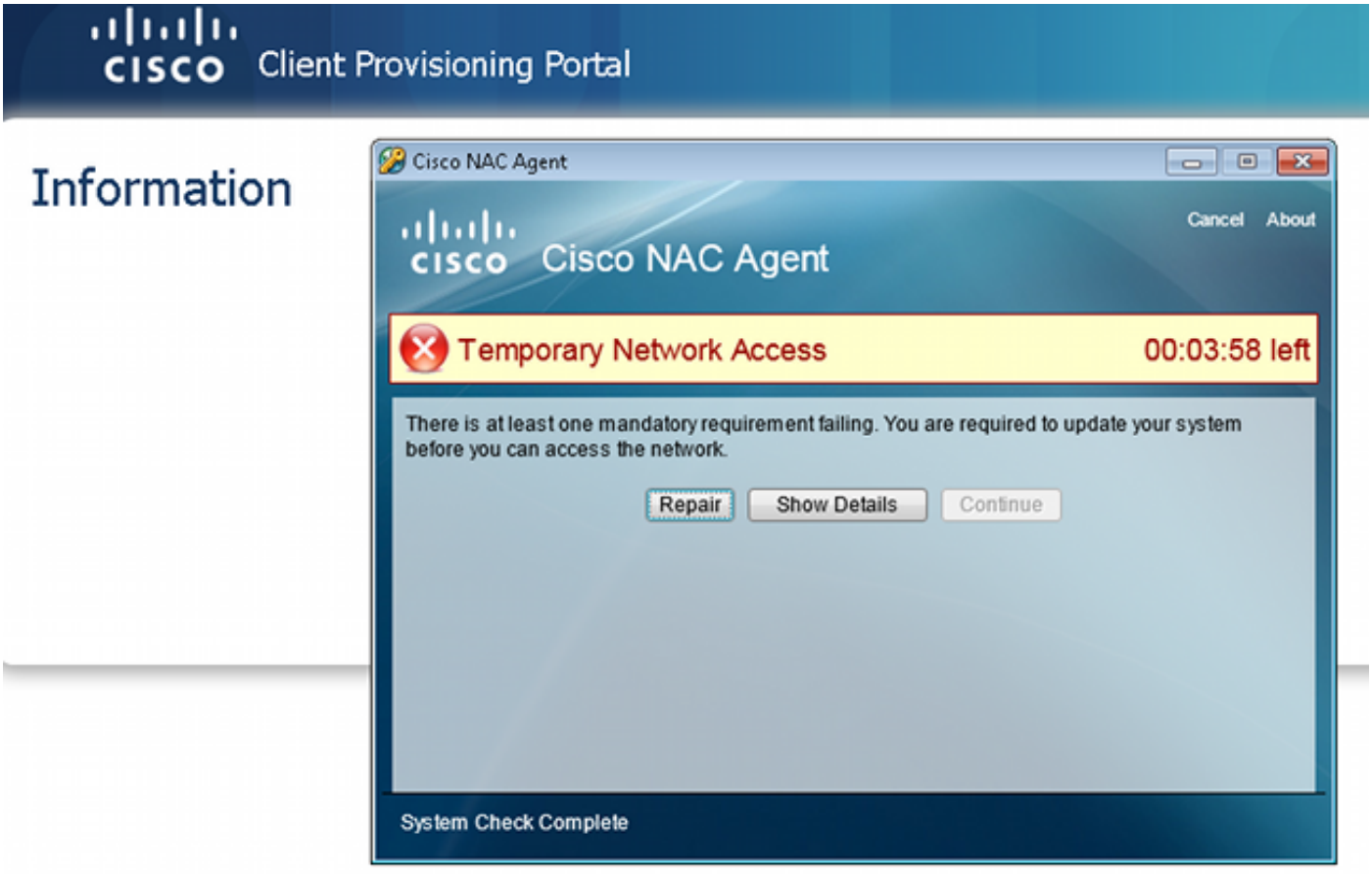
Nota: Si los registros no se encuentran en estas ubicaciones, verifique la variable **Entorno TEMP**.

Falla de estado del agente NAC

Si la postura falla, se presenta al usuario la razón:



El usuario podrá entonces tomar medidas correctivas si se configuran:



Información Relacionada

- Configuración de un servidor externo para la autorización de usuario de dispositivo de seguridad
- Guía de configuración CLI VPN Cisco Serie ASA, 9.1
- Guía de usuario de Cisco Identity Services Engine, versión 1.2
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).