Servicios de la postura en la guía de configuración de Cisco ISE

Contenido

Introducción

Este documento describe los servicios de la postura, el aprovisionamiento del cliente, la creación de la directiva de la postura, y la configuración de la política de acceso para el Cisco Identity Services Engine (ISE). Los resultados de la evaluación del punto final para ambos clientes atados con alambre (conectados con los switches Cisco) y los clientes de red inalámbrica (conectados con los reguladores de la tecnología inalámbrica de Cisco) se discuten.

Prerequisites

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Identity Services Engine (ISE)
- Configuración del switch del software del ® del Cisco IOS
- Configuración del controlador LAN de la tecnología inalámbrica de Cisco (WLC)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Versión 1.1.3 de Cisco ISE
- Versión 15.0(2) SE2 del Cisco Catalyst 3560 Series Switch
- Versión 7.4.100.0 del WLC de las Cisco 2504 Series

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Antecedentes

Servicios de la postura ISE

El flujo de trabajo de los servicios de la postura se comprende de tres secciones de configuración principal:

- Aprovisionamiento del cliente
- Directiva de la postura
- Directiva de la autorización

Aprovisionamiento del cliente

Para realizar la evaluación de la postura y determinar el estado de la conformidad de un punto final, es necesario provision el punto final con un agente. El agente del Network Admission Control (NAC) puede ser persistente, por el que el agente esté instalado y automáticamente cargado cada vez un usuario abra una sesión. Alternativamente, el agente del NAC puede ser temporal, por el que un agente basado en web se descargue dinámicamente al punto final para cada nueva sesión y después se quite después del proceso de la evaluación de la postura. Los agentes del NAC también facilitan la corrección y proporcionan un Acceptable Use Policy opcional (AUP) al usuario final.

Por lo tanto, uno de los primeros pasos en el flujo de trabajo es extraer los archivos del agente del sitio Web de Cisco y crear las directivas que determinan qué agente y archivos de configuración se descargan a los puntos finales, sobre la base de los atributos tales como tipo de la Identificación del usuario y del OS cliente.

Directiva de la postura

La directiva de la postura define el conjunto de los requisitos para que un punto final sea obediente juzgado basado sobre la presencia del archivo, clave de registro, proceso, aplicación, Windows, y los controles y las reglas del contra virus (AV) /anti-spyware (COMO). La directiva de la postura se aplica a los puntos finales basados sobre un conjunto de condiciones definido tal como tipo de la Identificación del usuario y del OS cliente. El estatus de la conformidad (postura) de un punto final puede ser:

- Desconocido: No se recogió ningunos datos para determinar el estado de la postura.
- Noncompliant: Una evaluación de la postura fue realizada, y uno o más requisitos fallaron.
- Obediente: El punto final es obediente con todos los requisitos obligatorios.

Los requisitos de la postura se basan en un conjunto configurable de una o más condiciones. Las condiciones simples incluyen un solo control de la evaluación. Las condiciones compuestas son un grupo lógico de una o más condiciones simples. Cada requisito se asocia a una acción de la corrección que ayude a los puntos finales para satisfacer el requisito, tal como actualización de firma AV.

Directiva de la autorización

La directiva de la autorización define los niveles de acceso a la red y de servicios opcionales que se entregarán a un punto final basado en el estatus de la postura. Los puntos finales que se juzgan no obedientes con la directiva de la postura pueden quarantined opcionalmente hasta que el punto final llegue a ser obediente; por ejemplo, una directiva típica de la autorización puede limitar el acceso a la red de un usuario para posture y los recursos de la corrección solamente. Si la corrección del agente o del usuario final es acertada, después la directiva de la autorización puede conceder el acceso a la red privilegiado al usuario. La directiva se aplica a menudo con las listas de control de acceso transferibles (dACLs) o la asignación del VLAN dinámico. En este ejemplo de configuración, los dACLs se utilizan para la aplicación del acceso del punto final.

Flujo de trabajo del ejemplo de la postura

En estos archivos persistentes (agente del NAC) y temporales del ejemplo de configuración, (de la red del agente) del agente se descargan al ISE, y se definen las directivas de aprovisionamiento del cliente que requieren a los Domain User descargar el agente y a los

Usuarios invitados del NAC para descargar el agente de la red.

Antes de la evaluación de la postura se configuran las directivas y los requisitos, la directiva de la autorización se pone al día para aplicar los perfiles de la autorización a los Domain User y a los invitados que se señalan por medio de una bandera como noncompliant. El nuevo perfil de la autorización definido en este acceso de los límites de configuración para posture y los recursos de la corrección. No prohiben los empleados y los Usuarios invitados señalados por medio de una bandera como obediente el acceso de red común. Una vez que han verificado a los servicios del aprovisionamiento del cliente, los requisitos de la postura se configuran para marcar para saber si hay instalación del contra virus, actualizaciones de la definición de virus, y actualizaciones críticas de Windows.

> **Note**: Verifique todos los elementos en estos punto final y las listas de verificación ISE antes de que usted intente configurar la postura.

Lista de verificación del punto final

1. El nombre de dominio completo (FQDN) ISE debe ser resolvable por el dispositivo de punto final.
2. Verifique que configuren al navegador del punto final como se muestra aquí:

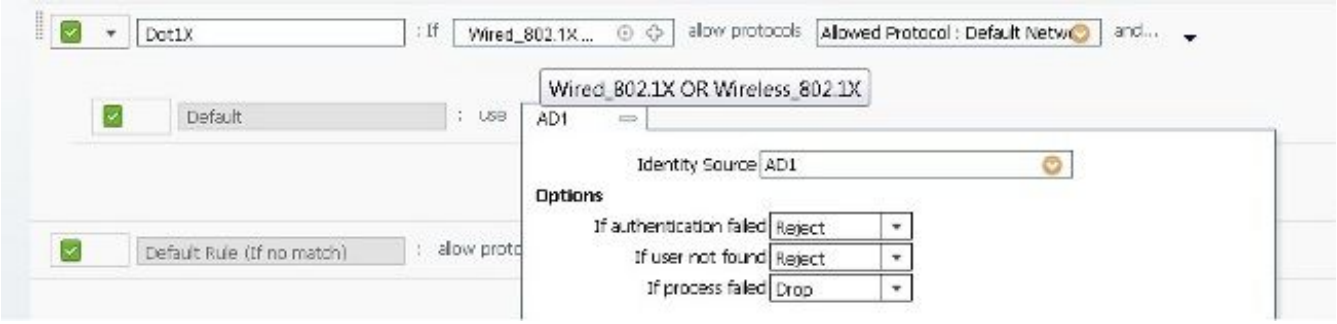
   Firefox o Chrome: Plug-in de Javas se debe habilitar en los navegadores.**Internet Explorer**: ActiveX se debe habilitar en las configuraciones del buscador.**Internet Explorer 10**:**Importación del certificado autofirmado**: Si usted está utilizando un certificado autofirmado para el ISE, funcione con al Internet Explorer 10 en el modo administrador para instalar estos Certificados.**Modo de compatibilidad**: El modo de compatibilidad debe ser cambiado en las configuraciones del Internet Explorer 10 para permitir la descarga del agente del NAC. Para cambiar esta configuración, haga clic con el botón derecho del ratón la barra azul en la cima de la pantalla del Internet Explorer 10, y elija la **barra de comandos**. Navegue a las **herramientas** > a las configuraciones de la **opinión de la compatibilidad**, y agregue el IP o el FQDN ISE a la lista de sitios.
   Habilitar el control ActiveX: Cisco ISE instala el agente del NAC de Cisco y el agente de la red con el control ActiveX. En el Internet Explorer 10, la opción a indicar para los controles ActiveX se inhabilita por abandono. Tome estas medidas para habilitar esta opción: Navegue a las **herramientas > a las opciones de Internet**.Navegue a la **ficha de seguridad**, y haga clic el **nivel de Internet** y de la **aduana**.En los controles ActiveX y los plug-in seccione, habilite **indicar automático para los controles ActiveX**.
3. Si un Firewall existe localmente en el cliente o a lo largo del trayecto de red al ISE, usted debe abrir estos puertos para la comunicación del NAC ISE:

   UDP/TCP 8905: Utilizado para la comunicación de la postura entre el agente y ISE (puerto del NAC del suizo).UDP/TCP 8909: Utilizado para el aprovisionamiento del cliente.TCP 8443: Utilizado para el invitado y la detección de la postura.**Note**: El ISE utiliza no más el puerto TCP 8906 de la herencia.
4. Si el cliente hace un servidor proxy configurar, modifique las configuraciones de representación para excluir la dirección IP del ISE. El error hacer rompe tan las comunicaciones requeridas para el aprovisionamiento central de la autenticación Web (CWA) y del cliente.

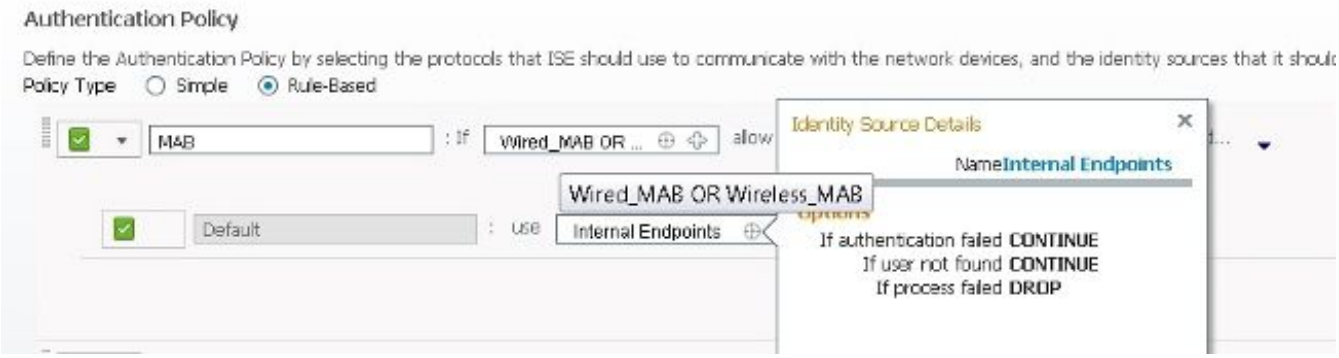
Lista de verificación ISE

- Navegue a la **administración > las fuentes > Active Directory externos de la identidad**, y verifique que el ISE está unido a al dominio del Active Directory (AD).
- Haga clic la lengueta de los **grupos**, y verifiquela que agregan al grupo de Domain User a la configuración AD.
- Navegue a la **administración > a los recursos de red > a los dispositivos de red**, y verifique que el Switch y el WLC están definidos como dispositivos de acceso a la red (NAD).
- Bajo la **directiva > autenticación**, asegúrese que el dot1x y las reglas de puente de la autenticación de MAC (MAB) estén configurados según lo descrito aquí:

  Las autenticaciones del dot1x para atado con alambre y los clientes de red inalámbrica se envían al almacén de la identidad AD.



  Las autenticaciones MAB para atado con alambre y los dispositivos de red inalámbrica se envían a los puntos finales internos; esté seguro de marcar la opción **si el usuario no encontrado CONTINÚA**.



Configure el ISE

Información general sobre la configuración ISE

Esta configuración del ejemplo ISE se comprende de estos pasos:

1. Configure y despliegue los servicios del aprovisionamiento del cliente.
2. Configure las directivas de la autorización.
3. Configure las directivas de la postura.
4. Configure la corrección del servicio de la actualización del Servidor Windows (WSUS).

Configure y despliegue los servicios del aprovisionamiento del cliente

1. Verifique la configuración de representación ISE.

   Navegue a la **administración > al sistema > a las configuraciones > al proxy**. Si un proxy se requiere para el acceso a internet, complete el servidor y a los portes detailes.
2. Descargue las comprobaciones para PRE-construidas de la postura AV/AS y el Microsoft Windows.

   Navegue a la **administración > al sistema > a las configuraciones > a la postura > a las actualizaciones**. La información de actualización en el panel derecho inferior debe estar vacía puesto que no se ha descargado ningunas actualizaciones todavía. Configure estos valores:

   Ahora haga clic la **actualización**, y reconozca la advertencia que las actualizaciones pueden tardar un cierto tiempo para completar.

   Note: Si el ISE no tiene acceso a internet, las actualizaciones offline de la postura están disponibles para la descarga en el cisco.com.
3. (Opcional) configure las opciones generales para el comportamiento del agente.

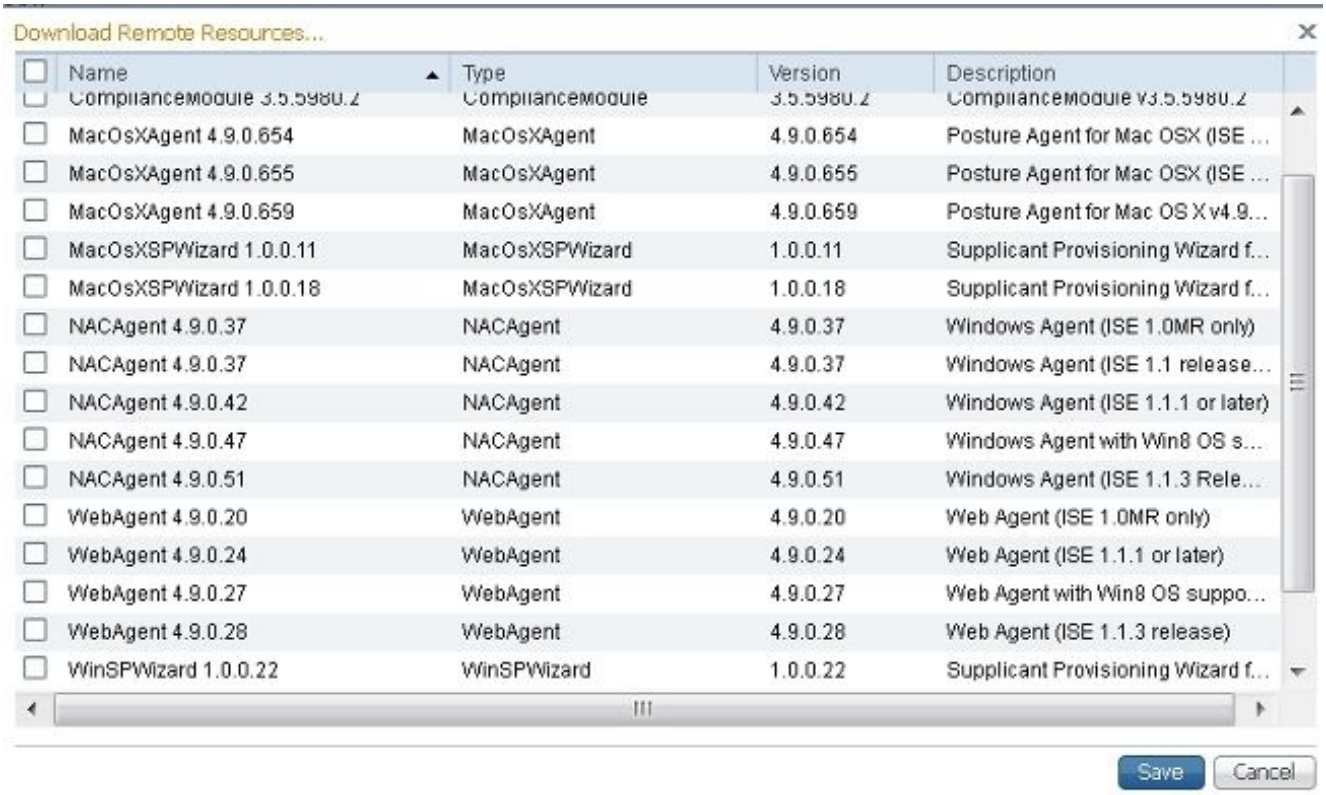
   Seleccione la **administración > el sistema > las configuraciones > la postura > las opciones generales**, y revise los valores predeterminados para el temporizador de la corrección, el retardo de la transición de la red, y el estatus predeterminado de la postura. Fije el temporizador de la corrección a 8 minutos.Marque (permiso) la **pantalla automáticamente cercana del éxito del login después del** checkbox, y fije la hora a 5 segundos como se muestra aquí:

   Click **Save**.
   Note: Valores asignados a través de la invalidación del perfil del agente estas configuraciones globales. El estatus predeterminado de la postura define el estatus para los clientes que no hacen un agente del NAC instalar. Si el aprovisionamiento del cliente no se está utilizando, este valor se puede fijar a noncompliant.
4. Fije la ubicación y la directiva para descargar las actualizaciones del aprovisionamiento del cliente.

   Haga clic la **administración > el sistema > las configuraciones > el aprovisionamiento del cliente del** panel de la izquierda, y verifiquelos que estos valores predeterminados están fijados:

5. Descargue los archivos del agente.

   Navegue a la **directiva > a los elementos > a los resultados de la directiva**, amplíe la carpeta del **aprovisionamiento del cliente**, y seleccione los **recursos**.Del panel derecho, el tecleo **agrega** > los **recursos del agente del sitio de Cisco de la** lista desplegable. Una ventana emergente visualiza a los recursos remotos:



Al mínimo, seleccione el agente actual del NAC, el agente de la red, y el módulo de la conformidad (módulo del soporte AV/AS) de la lista, y de la **salvaguardia del** tecleo. Los tipos de archivo del aprovisionamiento del cliente son:

Agente del NAC: Agente persistente de la postura para el cliente de Windows PC.**Agente de Mac OS X**: Agente persistente de la postura para el cliente PC de Mac OS X.**Agente de la red**: Agente temporal de la postura para Windows solamente PC.**Módulo de la conformidad**: Módulo OPSWAT que proporciona las actualizaciones al soporte de vendedor actual AV/AS para el agente del NAC y el agente de Mac OS X. No corresponde al agente de la red.**Perfiles**: Archivos de configuración del agente para el agente del NAC y el agente de Mac OS X. Las actualizaciones localmente instalaron los archivos XML en el cliente PC. No corresponde al agente de la red.Espere hasta que los archivos se descarguen al dispositivo ISE.

6. (Opcional) cree un perfil de la Configuración del agente del NAC para sus clientes.

   Del panel derecho, el tecleo **agrega**, después selecciona el **perfil del agente de la postura ISE de la** lista desplegable. Modifique el perfil para satisfacer los requisitos del despliegue.

   La opción de la fusión pone al día el parámetro actual del perfil del agente solamente si no se define ningún otro valor.La opción del sobregrabar pone al día el Valor de parámetro si está definida explícitamente o no.Para una lista completa de parámetros configurables del agente del NAC, refiera al guía del usuario del Cisco Identity Services Engine, la versión 1.1.x.
7. Defina la directiva de aprovisionamiento del cliente para los Domain User y los Usuarios invitados.

   Navegue a la **directiva > al aprovisionamiento del cliente**. Agregue dos nuevas reglas del aprovisionamiento del cliente de acuerdo con esta tabla. Haga clic las **ACCIONES** abotonan

a la derecha de cualquier entrada de la regla para insertar o duplicar las reglas.

Note: Si las versiones múltiples del mismo tipo de archivo (módulo de la conformidad del agente de la red del agente del NAC) fueron descargadas al repositorio del aprovisionamiento del cliente, seleccione la mayoría de la versión actual disponible cuando usted configura la regla.**Salvaguardia del** tecleo cuando está acabado**.**

8. Configure el portal de la autenticación Web para descargar el agente de la postura según lo definido por la directiva de aprovisionamiento del cliente.

   Navegue a la **administración > a la Administración > a las configuraciones del portal web**, amplíe la carpeta del **invitado**, las **configuraciones Multi-porta** selectas, y seleccione **DefaultGuestPortal**.Bajo lengueta de la **operación**, permita a la opción para permitir que los Usuarios invitados descarguen los agentes y al uno mismo regístrese.

   Defina un perfil del tiempo del registro del rol de invitado y del uno mismo del registro del uno mismo como se muestra aquí. El servicio del uno mismo del invitado es una configuración optativa que deja a los usuarios crear las cuentas sin la intervención del patrocinador. Este ejemplo permite al servicio del uno mismo para simplificar el proceso de inscripción del invitado.

   (Opcional) fije el AUP para los Usuarios invitados como se muestra aquí:

   Salvaguardia del tecleo cuando está acabado.

Directiva de la autorización de la configuración para el aprovisionamiento y la postura del cliente

La directiva de la autorización fija los tipos de acceso y de servicios que se concederán a los puntos finales basados sobre sus atributos tales como identidad, método de acceso, y conformidad con las directivas de la postura. Las directivas de la autorización en este ejemplo se aseguran de que los puntos finales que no son postura obediente quarantined; es decir, los puntos finales se conceden el acceso limitado suficiente provision el software agente y a los requisitos fallados remediate. Solamente los puntos finales obedientes de la postura se conceden el acceso a la red privilegiado.

1. (Opcional). Defina un dACL que restrinja el acceso a la red para los puntos finales que no son postura obediente.

   Navegue a la **directiva > a los elementos > a los resultados de la directiva**, amplíe la carpeta de la **autorización**, y seleccione los **ACL transferibles**.El tecleo **agrega del** panel derecho bajo Administración DACL, y ingresa estos valores para el nuevo dACL.

Esto es un dACL de la postura de la muestra. Revise las entradas del dACL para la exactitud, porque el ISE 1.1.x no soporta actualmente la validación de la sintaxis ACL.

El tecleo **somete** cuando está completado.

2. Defina un nuevo perfil de la autorización para los usuarios agentes 802.1X-authenticated/NAC nombrados **Posture_Remediation**. El perfil leverages el nuevo dACL para el control de acceso del puerto y el URL reorienta el ACL para el cambio de dirección del tráfico.

   Navegue a la **directiva > a los elementos > a los resultados > a la autorización de la directiva**, y seleccione los **perfiles de la autorización**.El tecleo **agrega del** panel derecho, y ingresa estos valores para el perfil de la autorización:

   Estos detalles resultantes del atributo deben aparecer en la parte inferior de la página:

   Tipo de acceso = ACCESS_ACCEPT
   DACL = POSTURE_REMEDIATION
   Cisco: la POSTURA del cisco-av-pair=url-redirect-acl=ACL- REORIENTA
   Cisco: cisco-av-pair=url-redirect = https://
   ip:8443/guestportal/gateway?sessionId=SessionIdValue@action=cppEl tecleo **somete** para aplicar sus cambios.

   Note: El ACL-POSTURE-REDIRECT ACL se debe configurar localmente en el Switch o el WLC. El ACL se refiere por nombre a la directiva de la autorización ISE. Para el Switch reoriente el ACL, las entradas del permiso determinan qué tráfico se debe reorientar al ISE mientras que, en un WLC, las entradas del permiso definen qué tráfico no debe ser reorientado.

3. Defina un nuevo perfil de la autorización para los usuarios agentes red-autenticada/de la red nombrados **CWA_Posture_Remediation**. El perfil leverages el nuevo dACL para el control de acceso del puerto y el URL reorienta el ACL para el cambio de dirección del tráfico.

   Navegue a la **directiva > a los elementos > a los resultados > a la autorización de la directiva**, y seleccione los **perfiles de la autorización**.El tecleo **agrega del** panel derecho, y ingresa estos valores para el perfil de la autorización:

   Estos detalles resultantes del atributo deben aparecer en la parte inferior de la página:

   Tipo de acceso = ACCESS_ACCEPT
   DACL = POSTURE_REMEDIATION
   Cisco: la POSTURA del cisco-av-pair=url-redirect-acl=ACL- REORIENTA
   Cisco: cisco-av-pair=url-redirect
   =https://ip:8443/guestportal/gateway?sessionId=SessionIdValue@action=cwaEl tecleo **somete** para aplicar sus cambios.

   Note: La diferencia entre los dos perfiles es el URL reorienta el atributo del Cisco-av-pair.

Reorientan a los usuarios que necesitan ser autenticados al portal del invitado para CWA. Una vez que están autenticados, reorientan a los usuarios automáticamente a CPP según las necesidades. Reorientan a los usuarios autenticados con el 802.1x directamente a CPP.

4. Ponga al día la directiva de la autorización para soportar la conformidad de la postura.

   Navegue a la **directiva > a la autorización**. Ponga al día la directiva existente de la autorización con estos valores. Utilice el selector en el extremo de una entrada de la regla para insertar o duplicar las reglas:

   Salvaguardia del tecleo para aplicar sus cambios.

   Note: Este perfil de la autorización se aplica al acceso atada con alambre y de usuario de red inalámbrica. El WLC no toma en la consideración el dACL. La característica del dACL se soporta solamente en el Switches. Para la Tecnología inalámbrica, la reorientación ACL es bastante para negar todo el tráfico a excepción del servidor de la corrección y de la postura ISE.

Directiva de la postura de la configuración AV

Este ejemplo muestra cómo definir una directiva AV con estas condiciones de la postura:

- Posture la directiva para que los Domain User hagan ClamWin AV instalar y corriente.
- Posture la directiva para que los Usuarios invitados instalen ClamWin AV si no se instala ningún contra virus.

1. Defina una condición de la postura AV que valide la instalación de ClamWin AV en un punto final. Este control será utilizado en los requisitos de la postura aplicados a los empleados.

   Navegue a la **directiva > a los elementos > a las condiciones de la directiva**, amplíe la carpeta de la **postura**, y seleccione la **condición de compuesto AV**.El tecleo **agrega del** menú del panel derecho. Si ningunos Productos AV aparecen bajo campo del **vendedor**, las actualizaciones de la postura todavía no se han descargado o la descarga todavía no ha completado. Ingrese estos valores:

   El tecleo **somete** en la parte inferior de la página.
2. Defina una condición de la postura AV que valide la versión de firma de ClamWin AV en un punto final. Este control será utilizado en los requisitos de la postura aplicados a los empleados.

   Seleccione la **condición de compuesto AV del** panel de la izquierda, y el tecleo **agrega del** menú del panel derecho. Ingrese estos valores:

   El tecleo **somete** en la parte inferior de la página.
3. Defina una condición de la postura AV que valide la instalación de cualquier AV soportado en un punto final. Este control será utilizado para los requisitos de la postura aplicados a los Usuarios invitados.

   Seleccione la **condición de compuesto AV del** panel de la izquierda, y el tecleo **agrega del**

menú del panel derecho. Ingrese estos valores:

El tecleo **somete** en la parte inferior de la página.

4. Defina una acción de la corrección de la postura que instale ClamWin AV en un punto final.

   Navegue a la **directiva > a los elementos > a los resultados de la directiva**, y amplíe la carpeta de la **postura**.Amplíe el contenido de las **acciones de la corrección**.Seleccione la **corrección del link**, y el tecleo **agrega del** menú del panel derecho. Ingrese estos valores:

   Haga clic en Submit (Enviar).

   Note: *El REM IP DEL SERVIDOR* representa la dirección IP de su servidor de la corrección donde existe la instalación de ClamWin. El archivo ejecutable en este ejemplo fue preposicionado en el servidor de la corrección. Para que la corrección trabaje, asegúrese de que el IP del servidor de actualización de ClamWin está incluido en el dACL previamente configurado y reoriente el ACL.
5. Defina una acción de la corrección de la postura esa las actualizaciones ClamWin AV en un punto final.

   Seleccione la **corrección AV/AS del** panel de la izquierda, y el tecleo **agrega del** menú del panel derecho. Ingrese estos valores:

   Haga clic en Submit (Enviar).
6. Defina los requisitos de la postura que serán aplicados a los empleados y a los Usuarios invitados.

   Seleccione los **requisitos de la directiva > de los elementos > de los resultados > de la postura de la directiva**. Ingrese estas entradas en la tabla. Utilice el selector en el extremo de una entrada de la regla para insertar o duplicar las reglas:

   Haga clic la **salvaguardia** cuando está acabado.

   Note: Si una condición preconfigurada no visualiza conforme a la lista de condiciones, verifique que el OS apropiado se haya seleccionado para la condición así como la regla del requisito. Solamente condiciones que son lo mismo o son un subconjunto del OS seleccionado para la visualización de la regla en la lista de la selección de las condiciones.
7. Configure la directiva de la postura para asegurarse de que ClamWin AV está instalado y la corriente en los ordenadores del empleado con Windows 7 y de que cualquier AV soportado está instalado y corriente en los ordenadores del Usuario invitado.

   Navegue a la **directiva > a la postura**, y cree las nuevas reglas de la directiva con los valores proporcionados en esta tabla. Para especificar un requisito de la postura como obligatorio, opcional, o la auditoría, haga clic el icono a la derecha del nombre del requisito, y elija una opción de la lista desplegable.

   Salvaguardia del tecleo para aplicar sus cambios.

Corrección de la configuración WSUS

Este ejemplo muestra cómo asegurarse de que todos los ordenadores del empleado con Windows 7 tienen las últimas correcciones críticas instaladas. Manejan a los servicios de la actualización del Servidor Windows (WSUS) internamente.

1. Defina una acción de la corrección de la postura que marque para y instale las últimas correcciones de Windows 7.

   Navegue a la **directiva > a los elementos > a los resultados de la directiva**, y amplíe la carpeta de la **postura**.Amplíe el contenido de las **acciones de la corrección**.Seleccione la **corrección de la actualización del Servidor Windows**, y el tecleo **agrega del** menú del panel derecho. Ingrese estos valores, y el tecleo **somete**:

   Note: Si usted quiere utilizar las reglas de Cisco para validar la actualización de Windows, cree sus condiciones de la postura, y defina sus condiciones en el paso 2.
2. Defina los requisitos de la postura que serán aplicados a los empleados.

   Navegue a la **directiva > a los elementos > a los resultados > a la postura de la directiva**, y seleccione los **requisitos**. Ingrese estas entradas en la tabla. Utilice el selector en el extremo de una entrada de la regla para insertar o duplicar las reglas:

   Note: Usted puede encontrar que **pr_WSUSRule de la** condición bajo **Cisco definió la condición > condición compuesta regular**. (Esto es una regla simulada elegida porque Step1 fijó las actualizaciones de Windows que se validarán por el nivel de gravedad.)
3. Configure la directiva de la postura para asegurarse de que los ordenadores del empleado con Windows 7 tienen las últimas correcciones críticas de Windows 7.

   Navegue a la **directiva > a la postura**, y cree las nuevas reglas de la directiva con los valores en esta tabla:

   Salvaguardia del tecleo para aplicar sus cambios.

Configuración del switch de la muestra

Esta sección proporciona un extracto de la configuración del switch. Se piensa para la referencia solamente y no debe ser copiado o ser pegado en un switch de producción.

Configuración global del radio y del dot1x

```
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
dot1x system-auth-control
ip radius source-interface Vlan (x)
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-acce ss-req
radius-server attribute 25 access-request include
```

```
radius-server host <ISE IP> key <pre shared key>
radius-server vsa send accounting
radius-server vsa send authentication
```

ACL predeterminado que se aplicará en el puerto

```
ip access-list extended permitany
permit ip any any
```

Cambio del radio del permiso de la autorización

```
aaa server radius dynamic-author
client <ISE IP> server-key <pre share d key>
```

Cambio de dirección y registro URL del permiso

```
Ip device tracking
Epm logging
Ip http server
Ip http secure server
```

Cambio de dirección ACL

```
ip access-list extended ACL-POSTURE-REDIRECT
deny udp any eq bootpc any eq bootps
deny udp any any eq domain
deny udp any host <ISE IP> eq 8905
deny tcp any host <ISE IP> eq 8905
deny tcp any host <ISE IP> eq 8909
deny udp any host <ISE IP> eq 8909
deny tcp any host <ISE IP> eq 8443
deny ip any host <REM SERVER IP>
deny ip any host 192.230.240.8          (one of the ip of CLAMwin database virus Definitions)
permit ip any any
```

> **Note**: La dirección IP del dispositivo de punto final debe ser accesible de la interfaz virtual del Switch (SVI) para que el cambio de dirección trabaje.

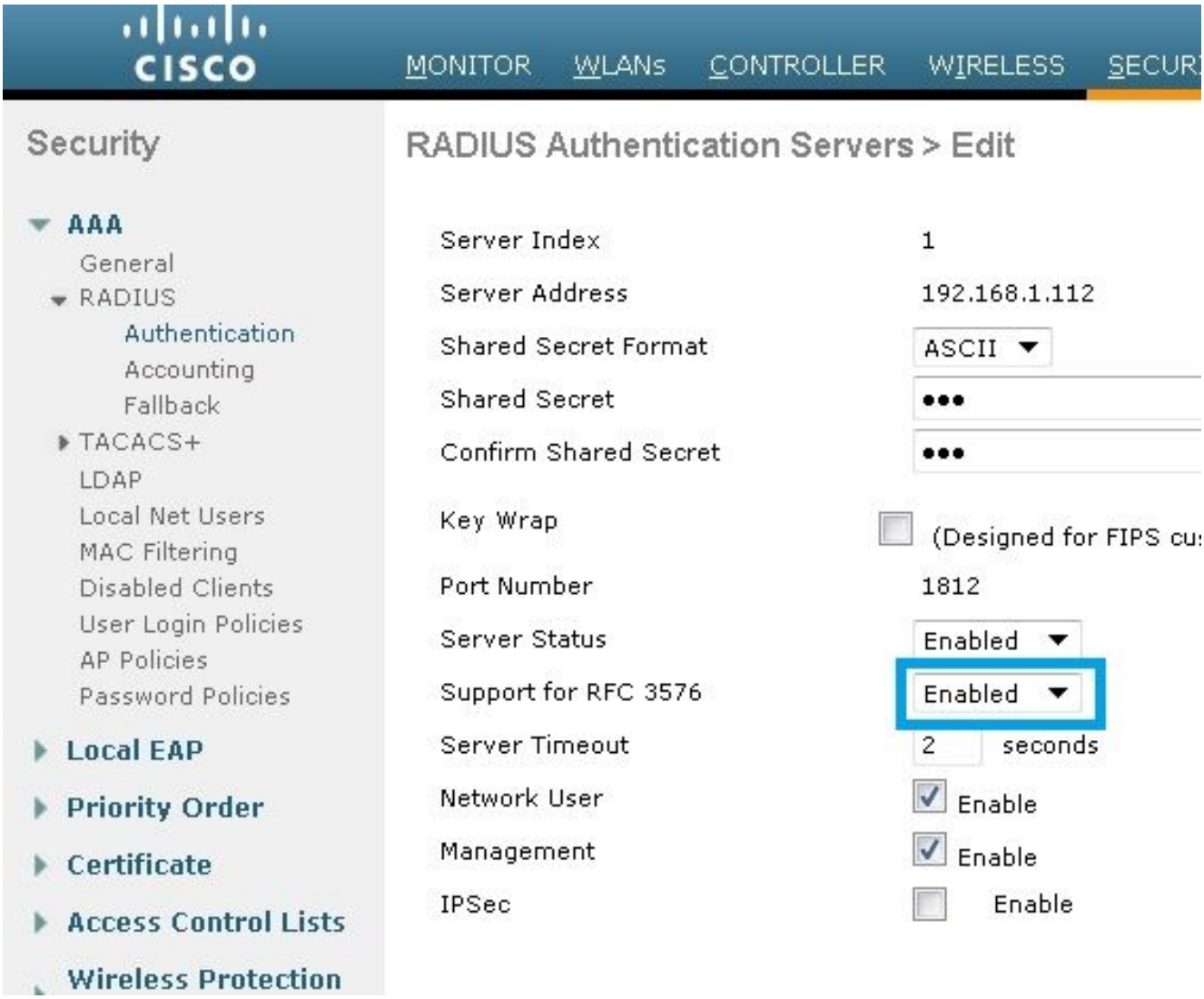
Configuración de puerto de switch

```
switchport access Vlan xx
switchport voice Vlan yy
switchport mode access
dot1x pae authenticator
authentication port-control auto
authentication host-mode multi-domain
authentication violation restrict
ip access-group permitany in (Note: This is mandatory for dACL for versions of Cisco IOS earlier
than Release 12.2(55)SE.)
dot1x timeout tx-period 7
authentication order dot1x mab
authentication priority dot1x mab
mab
```

Configuración del WLC de la muestra

Configuración global

1. Asegúrese de que el servidor de RADIUS haga el RFC3576 (CoA) habilitar; se habilita por abandono.



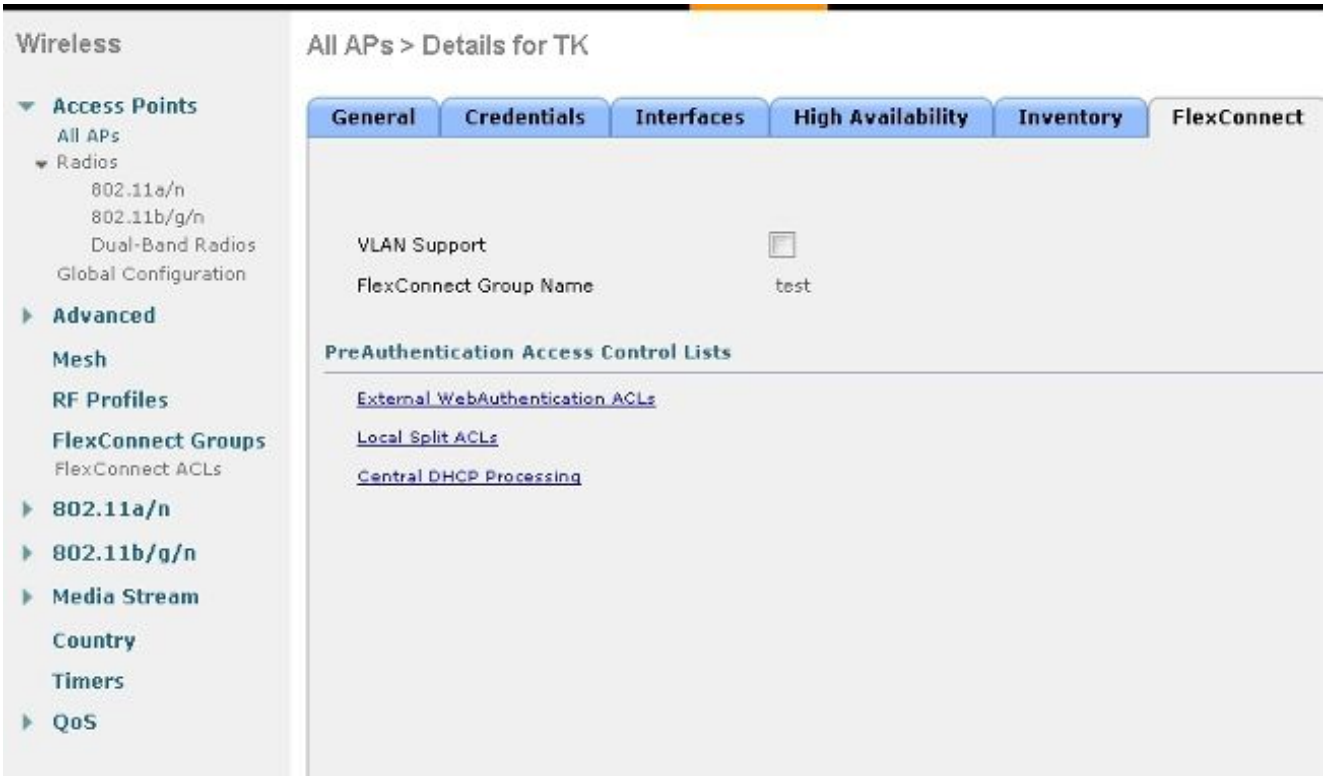
2. Navegue a la **Seguridad > a las listas de control de acceso**, cree un ACL en el WLC y llámelo “ACL-POSTURE-REDIRECT.”

15 y 16 se utilizan en este ejemplo para la actualización de ClamWin AV donde 192.230.240.8 contiene el archivo de definición de la base de datos.

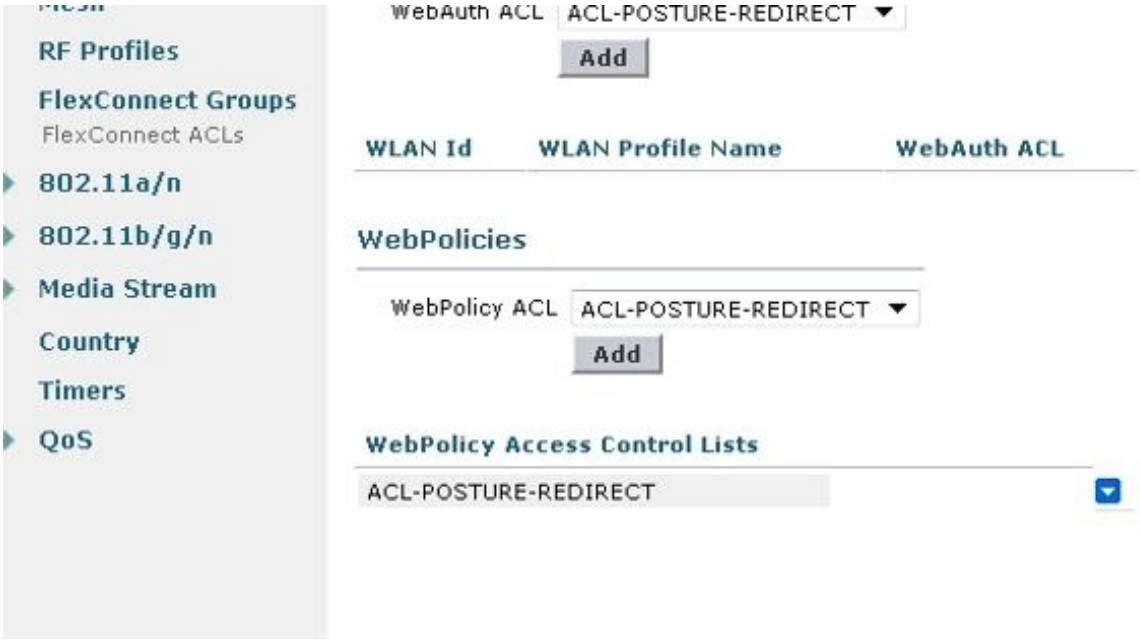
Para FlexConnect con el Local Switching, usted debe crear un FlexConnect ACL, y lo aplica al WebPolicy ACL. El ACL tiene el mismo nombre que el ACL en el WLC y tiene los mismos atributos.

1. Tecleo **FlexConnect ACL**.

2. Tecleo **WebAuthentication externo ACL**.



3. Agregue el WebPolicy ACL.



4. Haga clic en Apply (Aplicar).

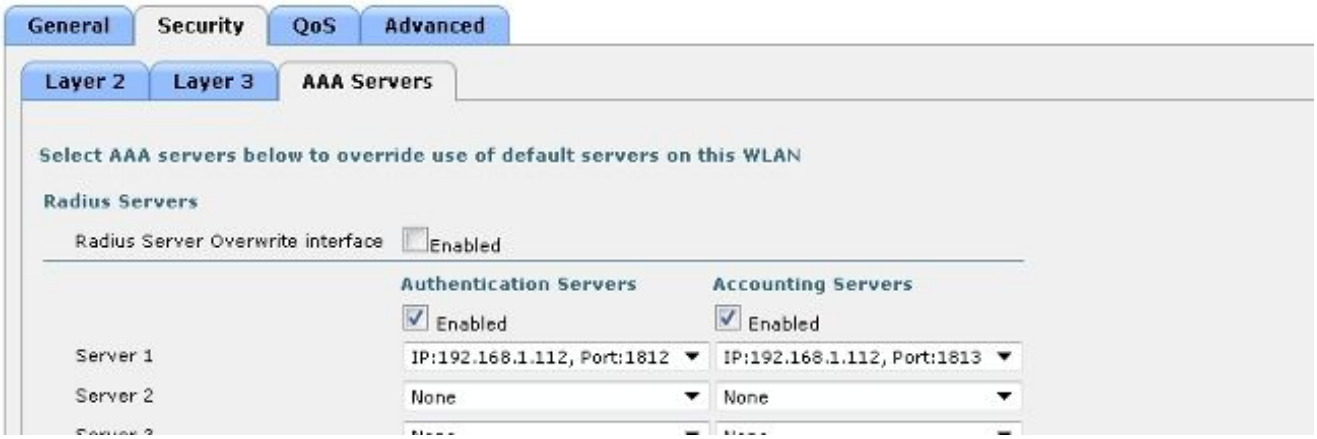
Configuración del empleado SSID

Cree un nuevo Service Set Identifier (SSID) del empleado o modifique el actual.

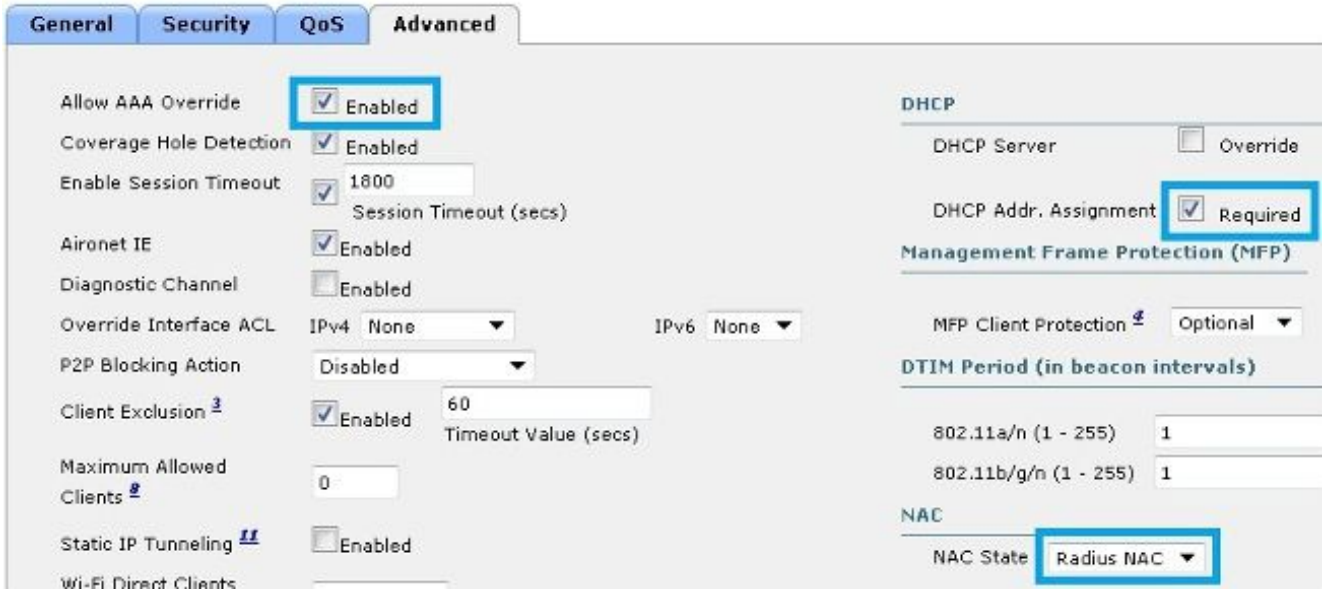
1. En la lengueta de la **red inalámbrica (WLAN)**, el tecleo **crea nuevo** o hace clic una red inalámbrica (WLAN) existente.

2. Haga clic la **ficha de seguridad**, haga clic la lengueta de la **capa 2**, después fije la Seguridad apropiada. Aquí está una configuración del WPA con el dot1x.

3. Haga clic la lengueta de los **servidores de AAA**, y marque (permiso) el ISE como el servidor de RADIUS para la autenticación y las estadísticas.



4. Haga clic la **ficha Avanzadas**, marque (permiso) la **invalidación de la permit AAA** y el **addr del DHCP.** El checkboxes de la **asignación**, y fijó el **estado del NAC al** NAC del radio.



Configuración del invitado SSID

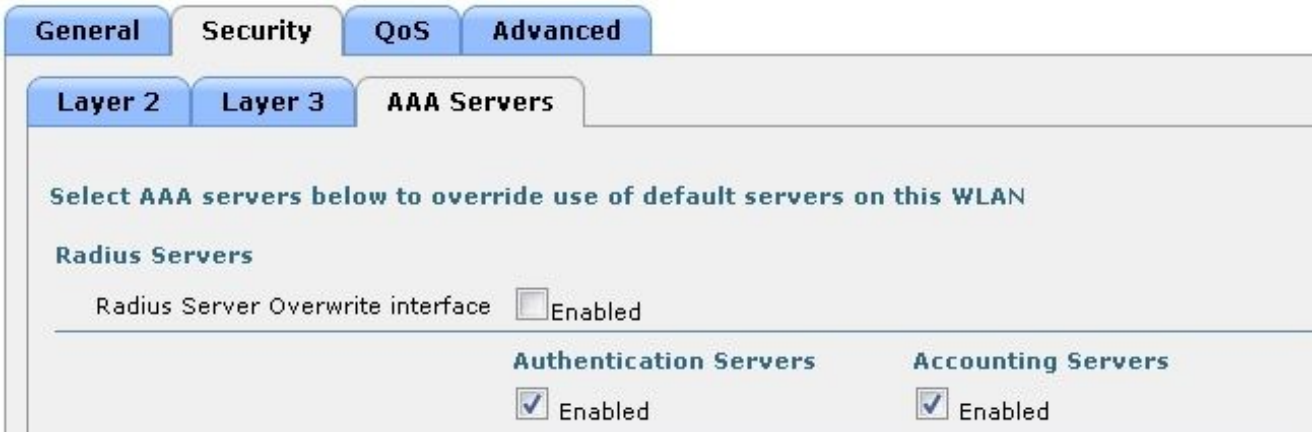
Cree una nueva red inalámbrica (WLAN) con el invitado SSID o modifique actual.

1. En la lengueta de la **red inalámbrica (WLAN)**, el tecleo **crea nuevo** o hace clic una red inalámbrica (WLAN) existente.

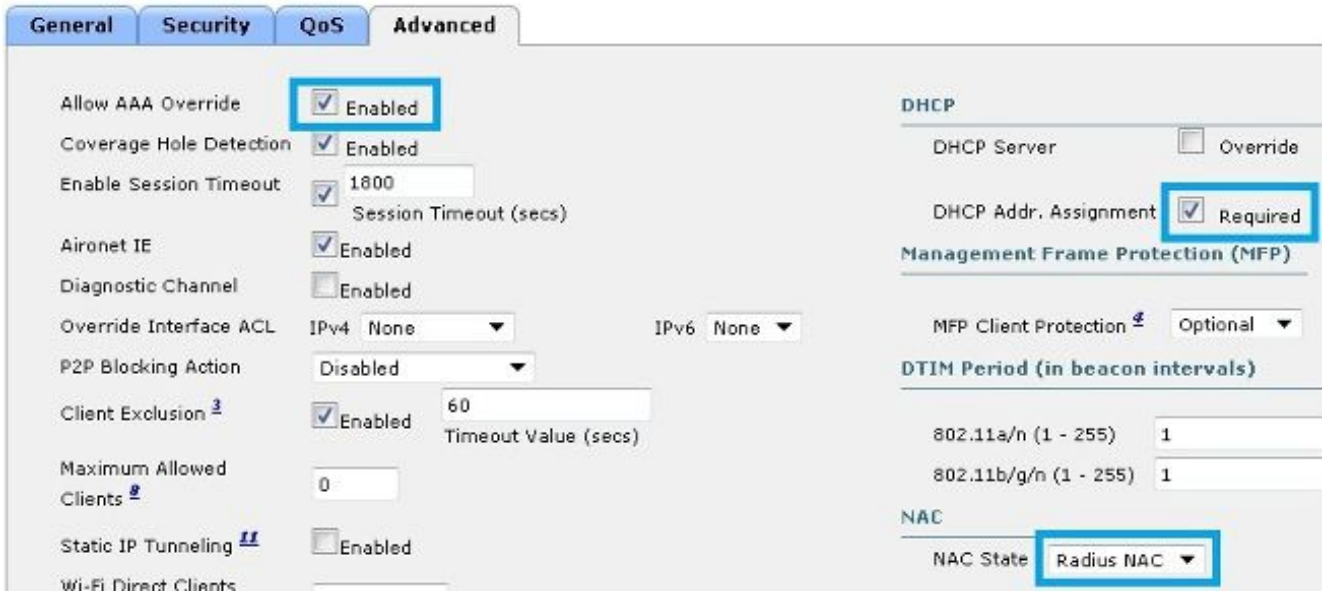
2. Haga clic la **ficha de seguridad**, haga clic la lengueta de la **capa 2**, después marque (permiso) el checkbox de **filtración MAC**.

3. Haga clic la lengueta de la **capa 3**, y asegúrese que todas las opciones están inhabilitadas.

4. Haga clic la lengueta de los **servidores de AAA**, y marque (permiso) el ISE como un servidor de autenticación y servidor de contabilidad.



5. Haga clic la **ficha Avanzadas**, marque (permiso) la **invalidación de la permit AAA** y el **addr del DHCP.** El checkboxes de la **asignación**, y fijó el **estado del NAC al** NAC del radio.



Postura del dot1x del empleado (agente del NAC)

Éste es el procedimiento de la postura sí mismo de una perspectiva del cliente, una vez que el cliente conecta con los WLAN configurados previamente.

1. Configure su Tecnología inalámbrica SSID (empleado) o la red alámbrica para PEAP MSCHAP V2, y conecte con un usuario AD en el grupo de Domain User.
2. Abra a un navegador, e intente navegar a un sitio. Se visualiza un prompt de la reorientación.
3. **Tecleo del** tecleo **para instalar el agente**.

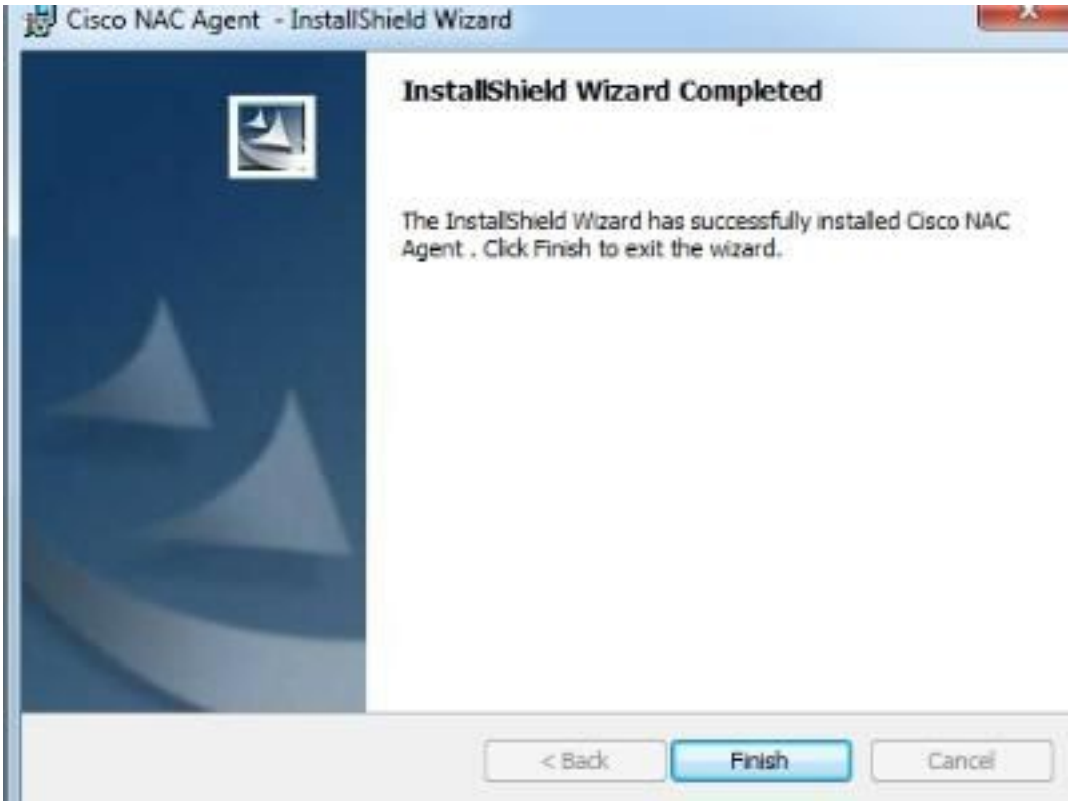
4. Haga clic en Next (Siguiente).

5. El tecleo **l valida los términos del acuerdo de licencia**, y hace clic **después**.

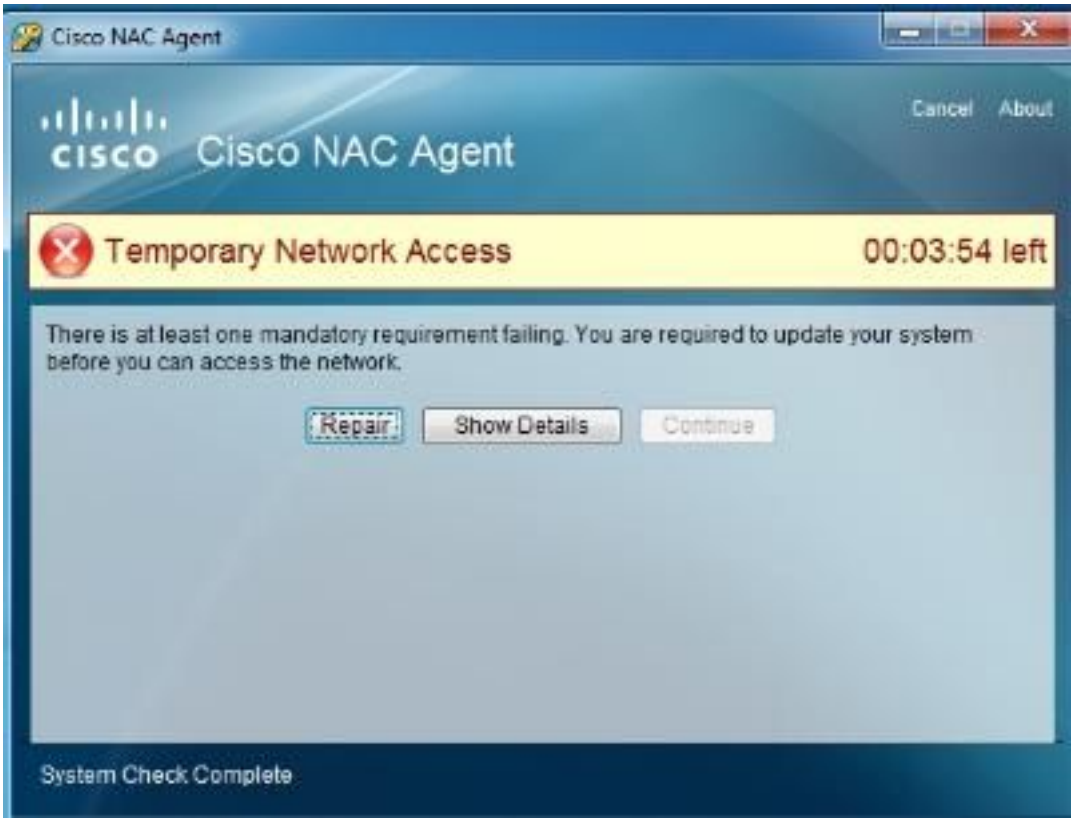
6. Tecleo **completo**, y tecleo **después**.

7. El tecleo **instala**.

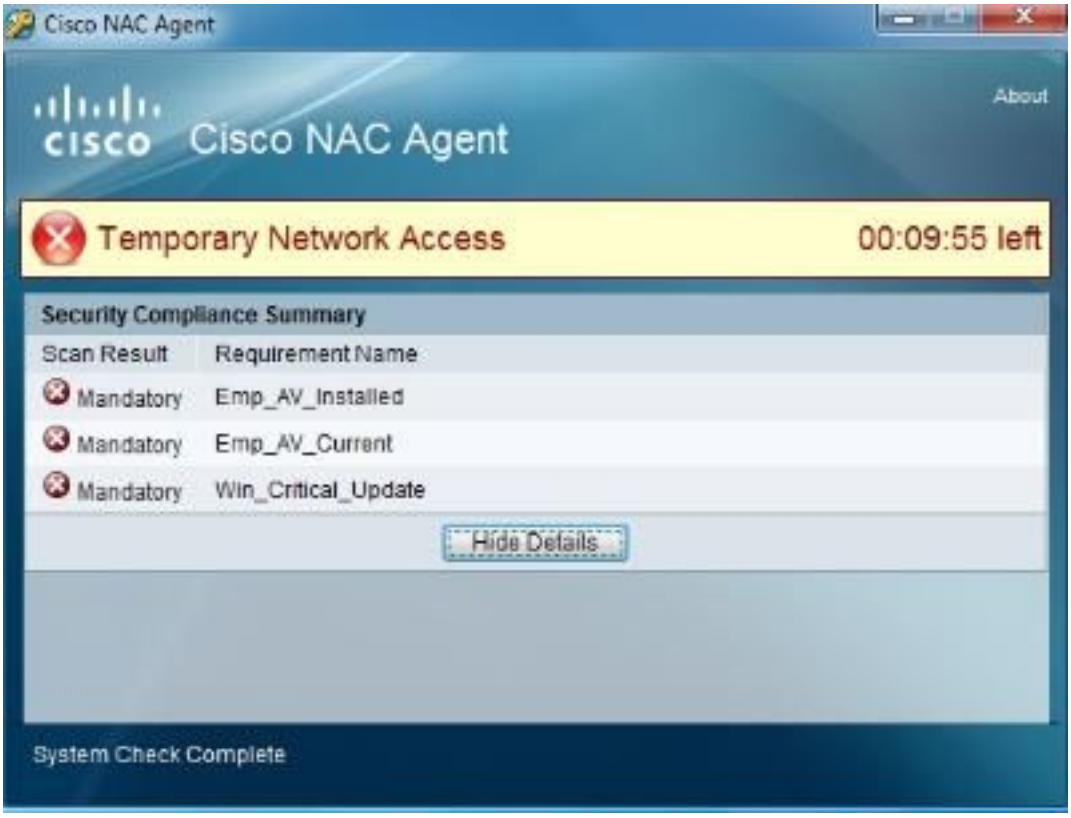
8. Seleccione el **final**.



9. Una vez que la instalación es completa, el agente del NAC surge. **Detalles de la demostración del** tecleo.



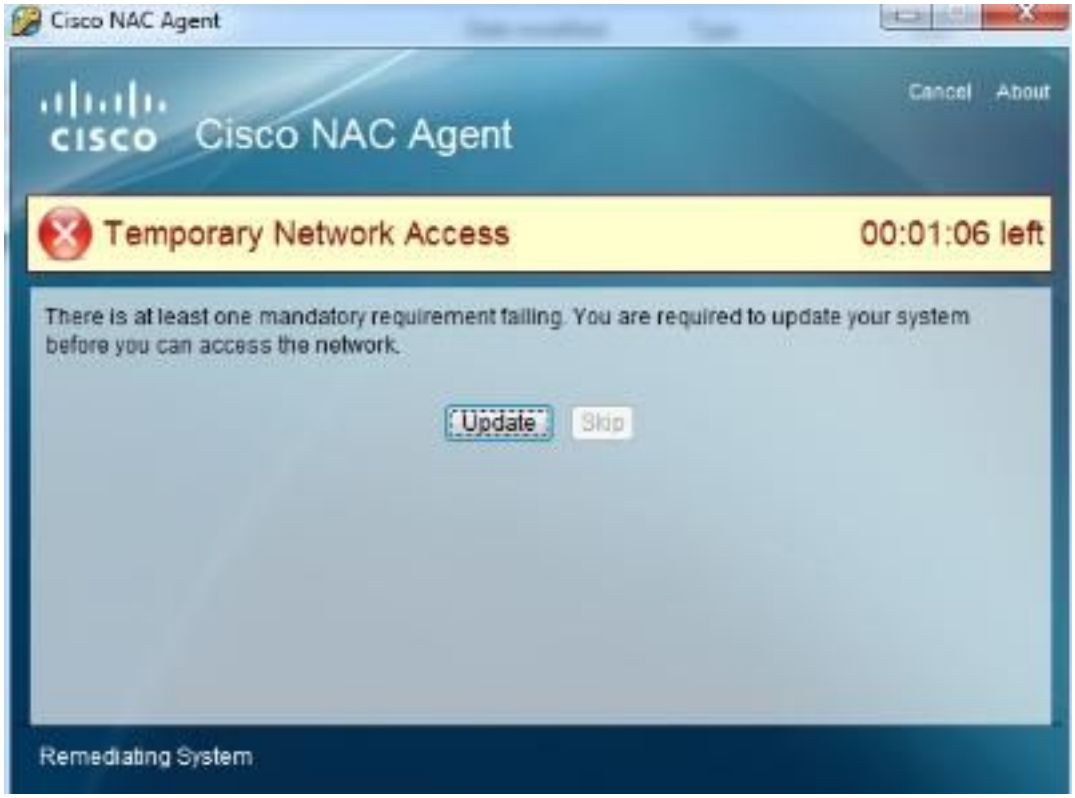
La salida muestra que ClamWin no está instalado y no es actualizada. Algunas actualizaciones críticas de Windows no están instaladas.



10. El tecleo **va al link** para instalar el contra virus del servidor de la corrección.

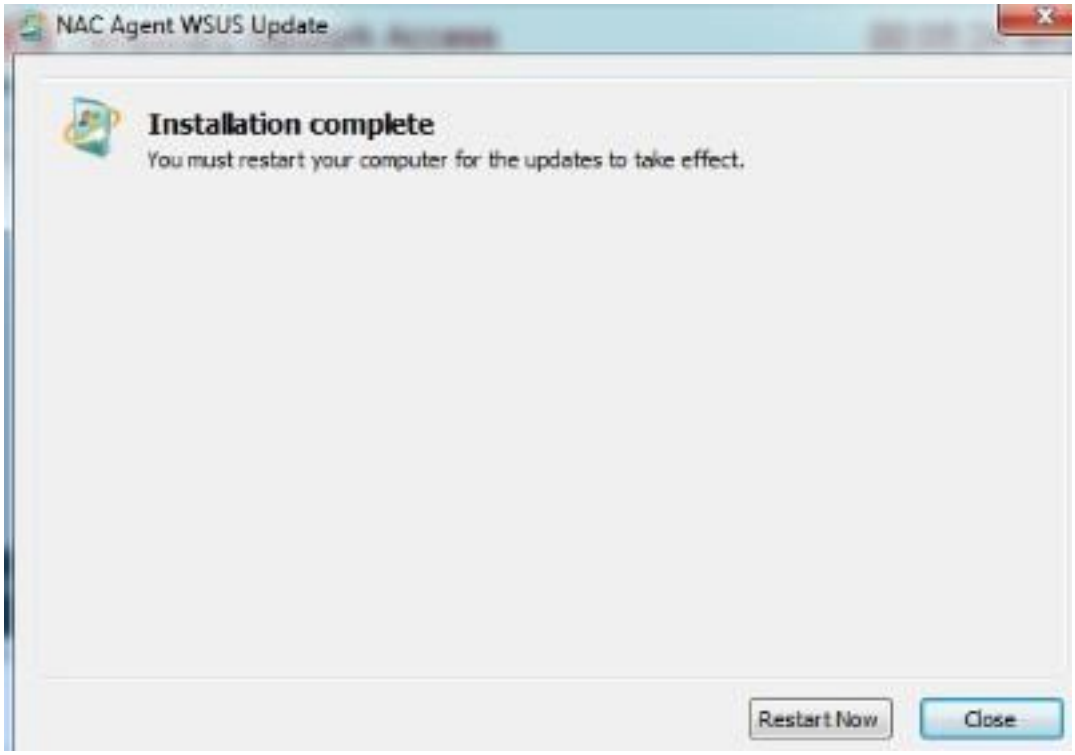
11. Haga clic el **funcionamiento**, y proceda con la instalación de ClamWin AV.

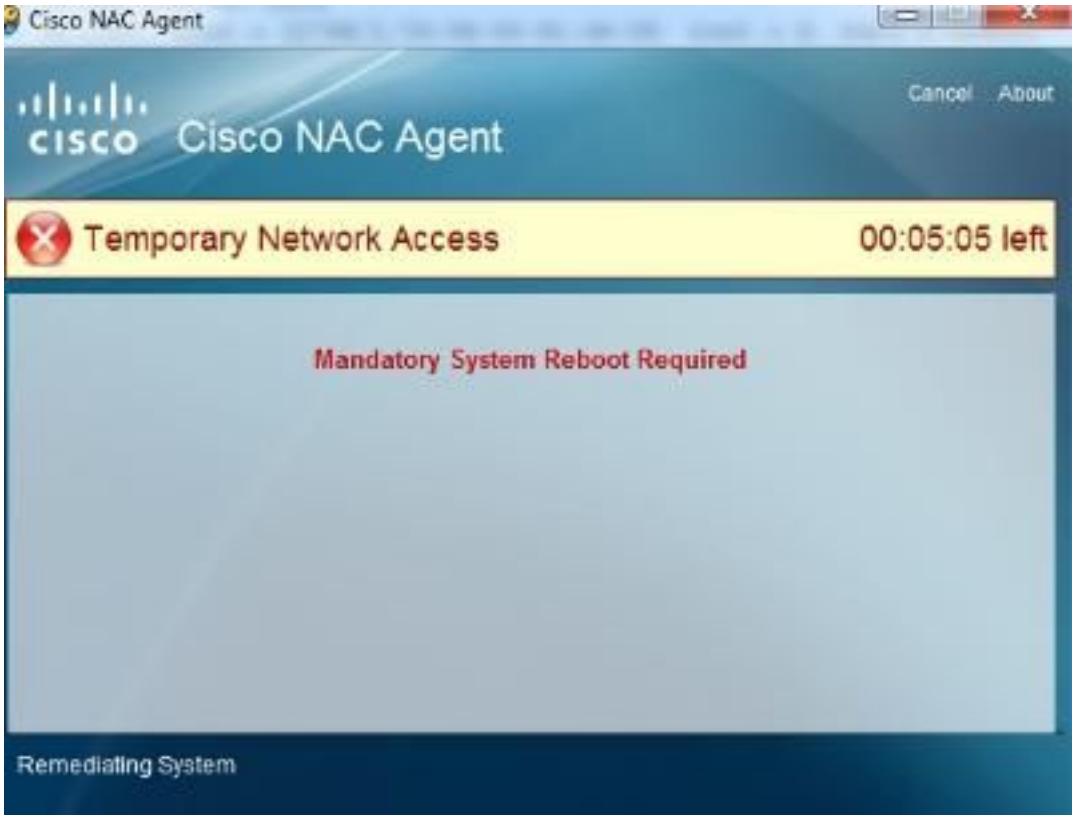
12. Después de que el contra virus esté instalado, el agente del NAC indica para las actualizaciones. **Actualización del** tecleo para conseguir el último archivo de definición de virus. Cuando la misma pantalla se presenta un por segunda vez, haga clic la **actualización** otra vez para instalar las actualizaciones de Windows.



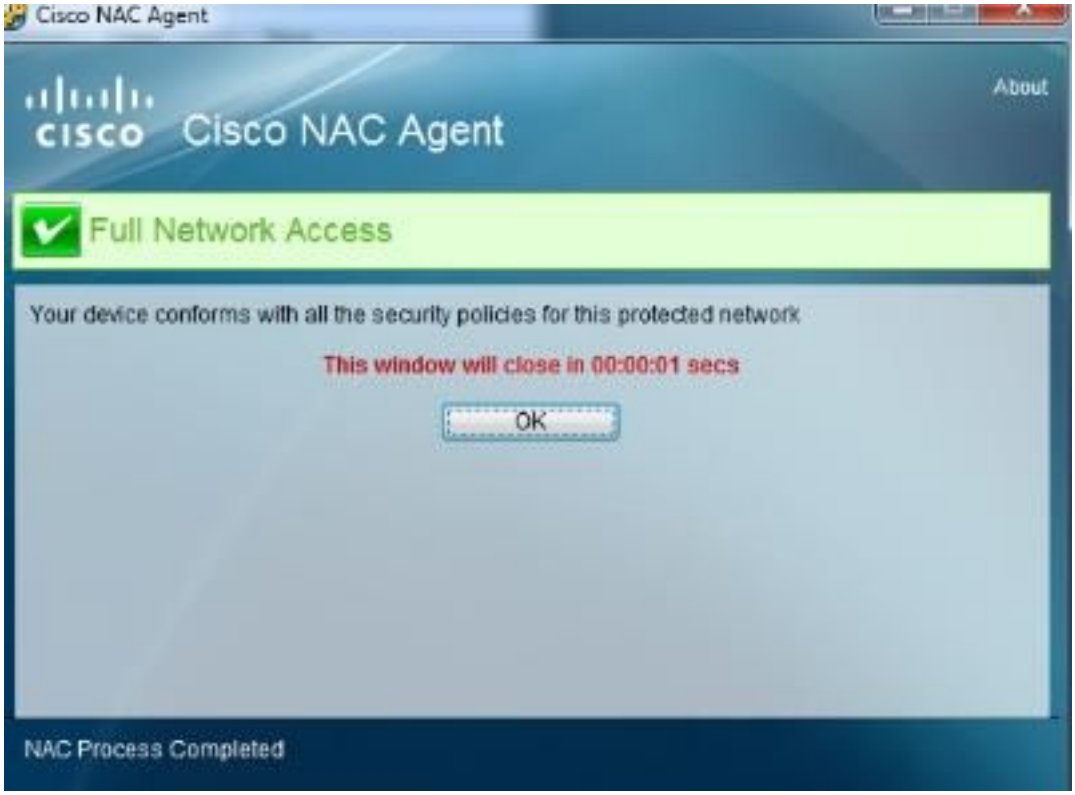
El agente del NAC entra en contacto su WSUS para marcar para y instalar las últimas actualizaciones críticas.

13. **Reinicio del** tecleo **ahora** para completar la actualización.





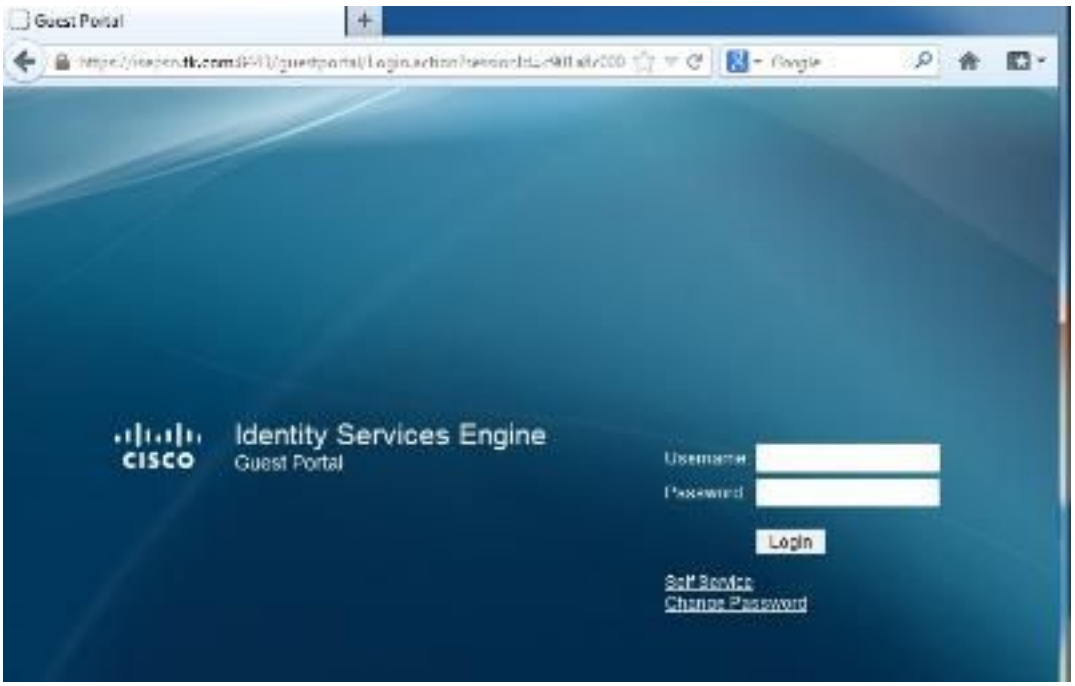
14. Después de que el reinicio, el sistema sea obediente.



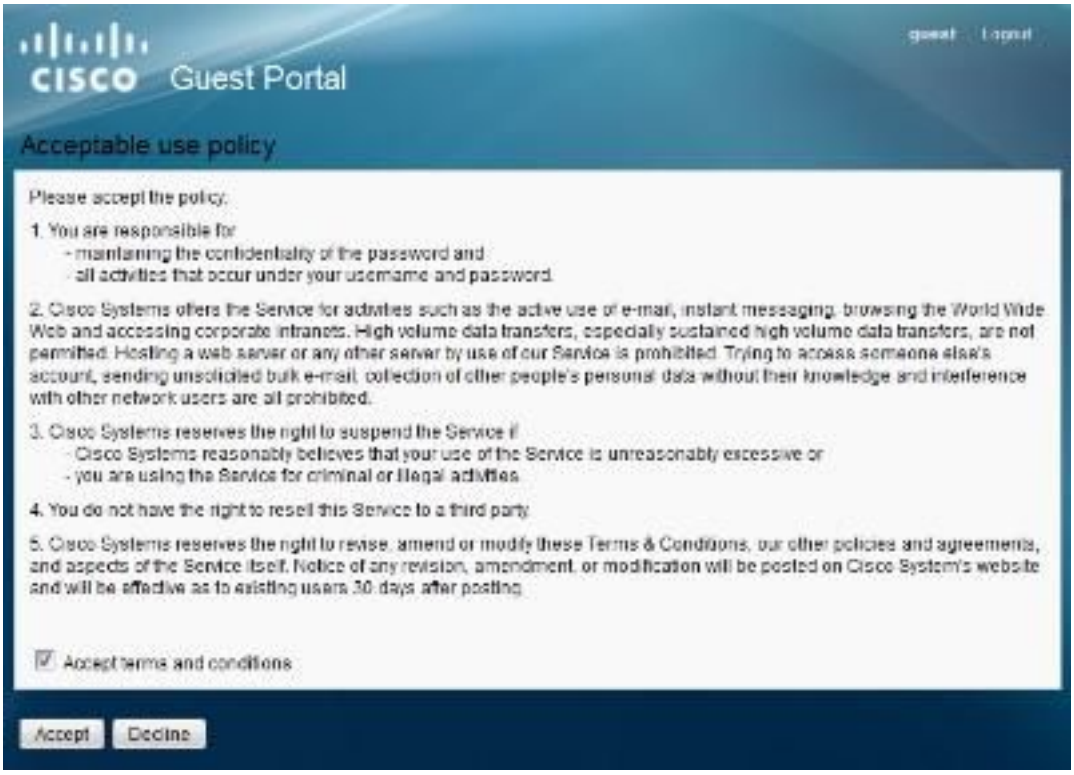
Postura del invitado CWA (agente de la red del NAC)

Éste es el procedimiento que los usuarios realizan, una vez que conectan con el invitado SSID con la postura habilitada.

1. Conecte con su invitado SSID, o no configure el dot1x en su red alámbrica.
2. Abra a un navegador, e intente navegar a un sitio.
3. Reorientan al navegador al portal del invitado.
4. Haga clic el **registro del uno mismo**, y proceda con la autenticación.



5. El tecleo **valida** para validar el AUP.

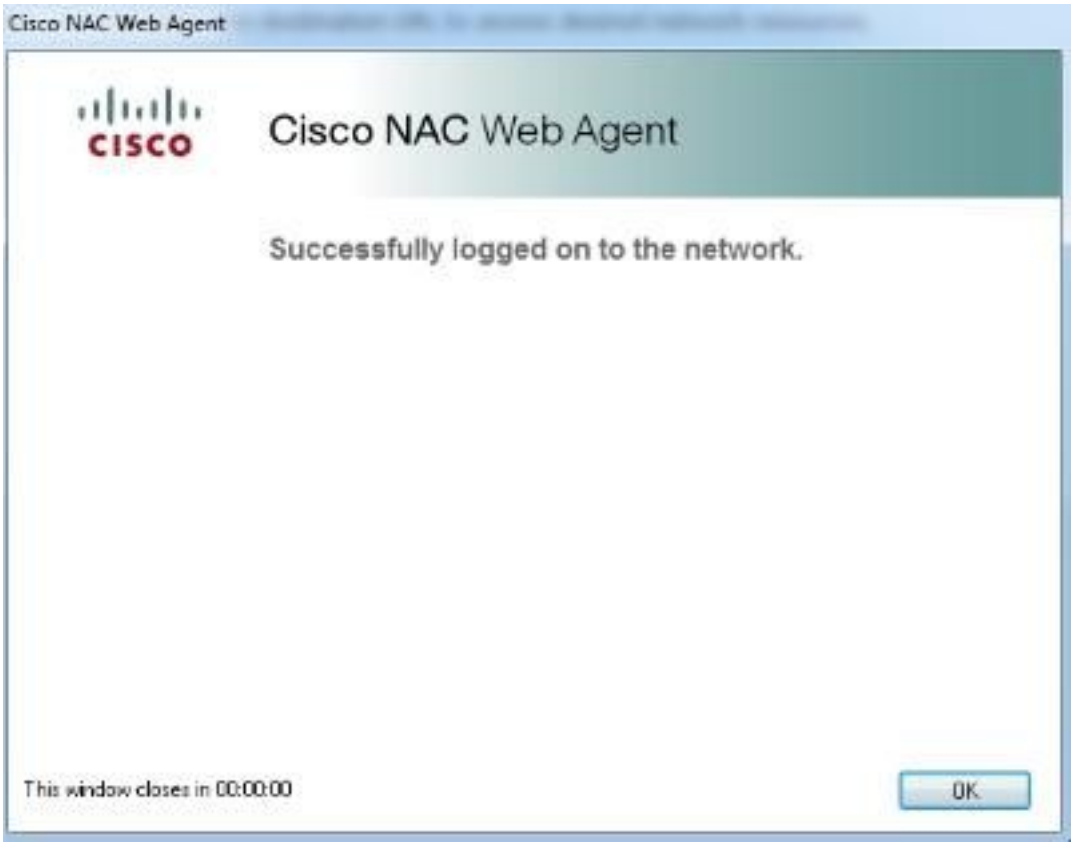


6. Seleccione el **tecleo para instalar el agente**.

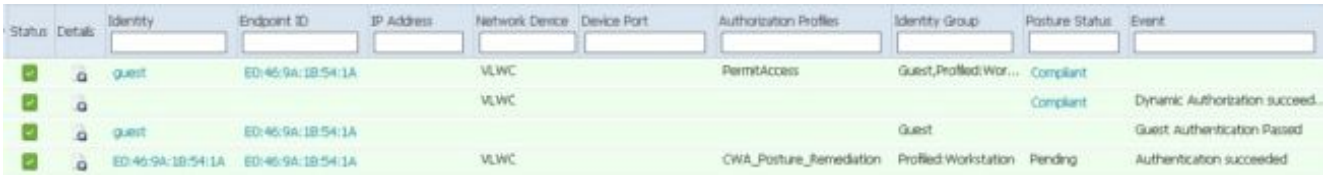
7. Haga clic **hacen clic aquí al remediate**.

8. Haga clic el **funcionamiento**, y proceda con la instalación del contra virus.

El PC ahora se encuentra para ser obediente.



9. Marque la autenticación ISE abre una sesión la orden para verificar que la autorización dinámica tuvo éxito y que usted está correspondiendo con el perfil de la autorización se relacionó con el estatus obediente.



Preguntas Frecuentes

Opciones de instrumentación con excepción del aprovisionamiento del cliente

Refiera al guía del usuario del Cisco Identity Services Engine, la versión 1.1x: Máquinas del cliente de disposición con el Instalador MSI del agente del NAC de Cisco.

Host de la detección para el agente del NAC

El agente del NAC alcanza el punto de decisión de políticas correcto ISE (PDP) en las maneras diferentes, dependiendo de si el host de la detección está definido:

1. Si no se define ningún host de la detección: El agente del NAC envía el pedido de HTTP en el puerto 80 al gateway; este tráfico se debe reorientar al link de la detección de la postura (CPP) para que la detección trabaje correctamente.
2. Si se define un host de la detección: El agente del NAC envía el pedido de HTTP en el puerto 80 al host; este tráfico se debe reorientar al link de la detección de la postura (CPP) para que la detección trabaje correctamente. Si hay un problema con el cambio de dirección, los intentos del agente del NAC para entrar en contacto directamente el host de la detección definieron en el puerto 8905; la validación de la postura no se garantiza, porque la información de la sesión puede no estar disponible en ésa PDP a menos que definan a los grupos del nodo, y el PDP está dentro del mismo grupo.
3. Si el host de la detección no se puede alcanzar en absoluto, el agente del NAC recurre al método 1, intenta tan entrar en contacto con el default gateway.

Eligiendo el host de la detección, uno debe tomar en la consideración, que el tráfico inicial del agente del NAC hacia el host de la detección debe ser visible al PDP. Así pues, las buenas opciones podían ser: Direccionamiento sí mismo PDP, host inexistente en la misma subred como Nodos PDP.

Configuran a los navegadores del empleado con el proxy

1. Si usted no está utilizando el aprovisionamiento del cliente y configuran al empleado PC con el proxy, no hay necesidad de los cambios puesto que los paquetes de detección de la postura se envían en el puerto 80 y desvían las configuraciones de representación.
2. Si usted está utilizando el servicio del aprovisionamiento del cliente, realice estos cambios a la configuración del switch y al WLC para interceptar el tráfico HTTP en el puerto definido del proxy (aquí 8080 en este ejemplo) si el proxy no está en el puerto 80.

   - Configuración de representación en el puerto 8080 en el Switch:

```
switchport access Vlan xx
switchport voice Vlan yy
```

```
switchport mode access
dot1x pae authenticator
authentication port-control auto
authentication host-mode multi-domain
authentication violation restrict
ip access-group permitany in (Note: This is mandatory for dACL for versions of Cisco IOS
earlier than Release 12.2(55)SE.)
dot1x timeout tx-period 7
authentication order dot1x mab
authentication priority dot1x mab
mab
```

```
switchport access Vlan xx
switchport voice Vlan yy
switchport mode access
dot1x pae authenticator
authentication port-control auto
authentication host-mode multi-domain
authentication violation restrict
ip access-group permitany in (Note: This is mandatory for dACL for versions of Cisco IOS
earlier than Release 12.2(55)SE.)
dot1x timeout tx-period 7
authentication order dot1x mab
authentication priority dot1x mab
mab
```

- WLC de la configuración de representación. Por abandono, los pedidos de HTTP de las interceptaciones del WLC con el puerto 80 del TCP de destino solamente. Este comando se debe configurar a través del comando line interface(cli) si usted quiere interceptar el otro tráfico HTTP en el puerto 8080:

```
switchport access Vlan xx
switchport voice Vlan yy
switchport mode access
dot1x pae authenticator
authentication port-control auto
authentication host-mode multi-domain
authentication violation restrict
ip access-group permitany in (Note: This is mandatory for dACL for versions of Cisco IOS
earlier than Release 12.2(55)SE.)
dot1x timeout tx-period 7
authentication order dot1x mab
authentication priority dot1x mab
mab
```

Note: El Switches permite el cambio de dirección en un puerto. Por lo tanto, si usted especifica otro puerto para el cambio de dirección del Switch, la detección de la postura falla, y el tráfico de la postura se envía al host de la detección definido en el NACAgentCFG.xml (el perfil del agente del NAC).

dACL y cambio de dirección ACL

El cambio de dirección ACL es obligatorio para el aprovisionamiento del cliente, la autenticación Web central, y la detección de la postura. Sin embargo, el dACL se utiliza para limitar el acceso a la red y se aplica solamente al tráfico NON-reorientado.

Para resolver esta situación, usted puede:

1. Defina solamente un cambio de dirección ACL, y reoriente todo el tráfico que usted quiere ser caído (según lo hecho en el ejemplo).
2. Defina un cambio de dirección ACL que sea menos restrictivo, y aplique un dACL que filtre el tráfico que no se reorienta.
3. Defina un cambio de dirección ACL, y aplique un VLA N que restrinja el acceso a la red. Éste es el mejor acercamiento porque el tráfico VLAN se puede filtrar por un Firewall que reconoce la aplicación.

El agente del NAC no surge

1. Marque la autenticación viva ISE, y verifiquela que la autenticación hace juego su perfil de la autorización de la postura.
2. Del PC del cliente, abra el cmd. Teclee el **nslookup**, y verifiquele puede resolver el nombre de host ISE PDP.
3. De su buscador del cliente, teclee el ISE-*nombre de host de* **https://: 8905/auth/discovery**, y se aseeguran le recibir ISE FQDN como respuesta.

Si todos estos pasos son acertados y si su Switch o configuración del WLC cumple con este documento, sus siguientes pasos deben ser:

- Utilice Wireshark para comenzar una captura en el PC.
- Recomience el servicio del agente del NAC.
- Recoja al embalador del registro de Cisco.
- Localice NACAgentCFG.xml en el Directorio del agente del NAC.

Entre en contacto el TAC de Cisco una vez que usted ha recolectado la captura de paquetes, los registros del agente del NAC, el archivo de configuración de NACAgentCFG, y los registros del visor de eventos de Windows.

Incapaz de acceder WSUS para la corrección

Si usted está utilizando el 3.0 SP2 WSUS y el agente del NAC no puede acceder las actualizaciones WSUS Windows, verifique que usted tenga la última corrección de WSUS instalado. Esta corrección es obligatoria para los clientes de Windows para hojear las actualizaciones de WSUS.

Verifique que usted pueda acceder este archivo: *wsus* **/selfupdate/iuident.cab del** *IP de* **http://**.

Refiera al guía paso a paso del 3.0 SP2 de los servicios de la actualización del Servidor Windows para la información adicional.

No tenga un WSUS manejado interno

Usted puede todavía utilizar los servidores de Windows Update mientras que usted configura su regla de la corrección de la postura.

El cliente debe ser permitido acceder estos sitios, así que estos URL no deben ser reorientados:

- http://windowsupdate.microsoft.com
- http://*.windowsupdate.microsoft.com
- https://*.windowsupdate.microsoft.com

- http://*.update.microsoft.com
- https://*.update.microsoft.com
- http://*.windowsupdate.com
- http://download.windowsupdate.com
- http://*.download.windowsupdate.com
- http://wustat.windows.com
- http://ntservicepack.microsoft.com
- http://stats.microsoft.com
- https://stats.microsoft.com

Ninguna autenticación fallida vista en los registros vivos ISE

Usted puede ser que sea tentado para crear una regla de la directiva de la autorización que acciona en la condición de un cliente noncompliant para restringir el acceso. Sin embargo, usted no verá que el intento de autenticación falla hasta que expire el temporizador de la corrección, especialmente cuando usted está utilizando el agente de la red. De hecho, el agente nota el incumplimiento y comienza el temporizador de la corrección.

Se notifica El ISE que la postura era un error solamente cuando expira el temporizador de la corrección o la **cancelación de los** tecleos del usuario. Por lo tanto, es una práctica adecuada dar un acceso predeterminado a todos los clientes que permita la corrección pero bloquea cualquier otra forma de acceso.

Verificación

Algunos procedimientos de verificación se incluyen en las secciones precedentes.

Troubleshooting

Algunos procedimientos deTroubleshooting se incluyen en las secciones precedentes.