

SOPHOS

Sophos NAC DHCP Guía de configuración

Versión: 3.3

Edición: septiembre de 2009



Contenido

- 1 Acerca de esta guía.....3
- 2 Imposición DHCP.....4
- 3 Lista de comprobación para la imposición DHCP.....5
- 4 Instalar el software de DHCP Enforcer.....6
- 5 Completar tareas de NAC Manager.....7
- 6 Apéndice A: Usar la utilidad de configuración de DHCP Enforcer.....17
- 7 Apéndice B: Actualizar la imposición DHCP.....20
- 8 Soporte técnico.....22
- 9 Copyright.....23

1 Acerca de esta guía

Esta guía le ayudará a configurar la imposición DHCP dentro de Sophos Endpoint Security and Control para poder identificar las estaciones desconocidas que se conectan a su red, verificar el nivel de seguridad y controlar el acceso a los recursos de red. En él se describe cómo configurar DHCP Enforcer de NAC y el servidor NAC. También contiene información sobre la reconfiguración de la imposición DHCP para utilizar la configuración DHCP de Endpoint Security and Control 8.

En concreto, ofrece información sobre:

- La instalación y configuración por primera vez del software de DHCP Enforcer.
- La configuración de DHCP mediante NAC Manager.
- La reconfiguración de la imposición DHCP para que funcione con la implementación anterior si ha utilizado la imposición DHCP en Sophos Endpoint Security and Control 8.

Esta guía le será útil si:

- Utiliza Enterprise Console.
- Utiliza Sophos NAC para Endpoint Security and Control.
- Desea configurar la imposición DHCP.

Antes de leer esta guía, consulte la *Guía rápida de inicio de Sophos Endpoint Security and Control*.

Todos los documentos de Sophos Endpoint Security and Control están disponibles en: http://esp.sophos.com/support/docs/Endpoint_Security_Control-all.html.

1.1 Requisitos de DHCP Enforcer

Para utilizar la imposición DHCP en Sophos NAC, deberá instalar Sophos DHCP Enforcer en todos los servidores DHCP.

Requisitos de DHCP Enforcer	
Sistema operativo	Servidor Windows 2000 ó 2003
Software DHCP	Microsoft [®] Dynamic Host Configuration Protocol (DHCP)

2 Imposición DHCP

Sophos NAC contiene una configuración predeterminada de la imposición DHCP. Dicha configuración es válida para la implementación de DHCP más habitual, de forma que no sea necesario modificarla demasiado al instalar Sophos NAC. Sin embargo, las implementaciones de DHCP son muy variadas, por lo que puede ser necesario ajustarla.

Nota: En la lista de comprobación para la imposición DHCP podrá ver las tareas necesarias para implementar este tipo de control. Para más información, consulte [Lista de comprobación para la imposición DHCP](#) en la página 5.

Configuración predeterminada de la imposición DHCP

Utilice NAC Manager para cambiar la configuración predeterminada según sea necesario.

- Las estaciones desconocidas tienen permiso de acceso a la red. Las estaciones desconocidas no tienen el agente instalado y no están exentas.

Nota: Para poner en cuarentena estaciones desconocidas mediante la imposición DHCP, cambie el valor de la opción Unknown Endpoint por Enforce. Para más información, consulte [Activar la imposición DHCP para estaciones desconocidas](#) en la página 13.

- Las estaciones conocidas, es decir, las estaciones que utilizan el agente, tienen permiso de acceso a la red. Las políticas NAC están configuradas con el modo Report Only. Para activar la imposición DHCP para estaciones conocidas, cambie el modo de las políticas que tenga intención de utilizar por Enforce.

Nota: Cuando la imposición DHCP está activada, las estaciones conformes y parcialmente conformes a las políticas que utilizan el agente tienen permiso de acceso a la red. Las estaciones que no cumplen las políticas y ejecutan el agente tienen prohibido el acceso a la red. Para más información, consulte [Activar la imposición DHCP para estaciones conocidas](#) en la página 14.

Sophos recomienda utilizar la imposición DHCP para las estaciones desconocidas y la imposición del agente para las conocidas. Sin embargo, Sophos NAC permite utilizar la imposición DHCP con estaciones conocidas. Para más información sobre la imposición del agente, consulte la [Guía de configuración del agente de cumplimiento de Sophos](#).

3 Lista de comprobación para la imposición DHCP

En la lista de comprobación para la imposición DHCP podrá ver las tareas necesarias para implementar este tipo de control. Toda la información necesaria para completarlas se incluye en este documento, a menos que se indique lo contrario.

Tarea	Descripción	Completado
Instalación de Sophos NAC y el agente de cumplimiento		
1.	Instalar y configurar Sophos NAC. Para más información, consulte la <i>Guía rápida de inicio de Sophos Endpoint Security and Control</i> .	
2.	Instalar el agente de cumplimiento en las estaciones utilizando Sophos Enterprise Console. Para más información, consulte la <i>Guía rápida de inicio de Sophos Endpoint Security and Control</i> .	
Tareas del servidor DHCP		
3.	Instalar DHCP Enforcer en los servidores DHCP. Nota: Desinstale la versión anterior del software antes de instalar la versión actualizada.	
Tareas de Sophos NAC Manager		
4.	Ejecutar el asistente de configuración DHCP para que los servidores proxy, de remediación, del agente soluble y DHCP utilicen la imposición DHCP de NAC.	
5.	Ejecutar el informe de DHCP Enforcer para: <ul style="list-style-type: none"> ■ Determinar si las estaciones conocidas recibirán el acceso a la red adecuado al activar la imposición DHCP. ■ Localizar estaciones que necesiten excluirse. 	
6.	Crear excepciones para las estaciones que no puedan ejecutar el agente de cumplimiento, como aquellas con sistemas operativos no Windows. Las excepciones también se aplican a estaciones que no necesitan evaluación del cumplimiento, como servidores, routers e impresoras. Nota: Para las estaciones que necesiten protección NAC, utilice Sophos Enterprise Console para instalar el agente de cumplimiento.	
7.	Activar la imposición DHCP.	

4 Instalar el software de DHCP Enforcer

Instale DHCP Enforcer en los servidores Microsoft DHCP. El software de DHCP Enforcer incluye DHCP Enforcer y la utilidad de configuración de DHCP Enforcer. La instalación configura el servidor DHCP. Si necesita cambiar la configuración de DHCP server especificada durante la instalación de DHCP Enforcer, utilice la utilidad de configuración de DHCP Enforcer. Para más información, consulte el [Apéndice A: Usar la utilidad de configuración de DHCP Enforcer](#) en la página 17.

Nota: Desinstale la versión anterior del software antes de instalar la versión actualizada.

1. Vaya al sitio web de Sophos y descargue el programa de instalación de Sophos NAC DHCP Enforcer.
Si lo prefiere, inserte el CD-ROM DHCP Enforcer Install. El CD-ROM se debería iniciar de forma automática.
2. Se abrirá el asistente de instalación. En el cuadro de diálogo de **bienvenida**, haga clic en **Next**.
3. En el cuadro de diálogo **Sophos DHCP Enforcer**, escriba la dirección IP del servidor NAC, la clave compartida del servidor NAC y confírmela. Haga clic en **Next**.
Anote la clave compartida que utilice. Deberá introducir la misma clave compartida al ejecutar el asistente de configuración de DHCP con NAC Manager.
4. En el cuadro de diálogo **Ready to Install the Program**, haga clic en **Install** para instalar DHCP Enforcer.
5. Haga clic en **Finish**.
Una vez instalado DHCP Enforcer en todos los servidores DHCP, utilice NAC Manager para configurar los servidores DHCP para que funcionen con Sophos NAC. Para más información, consulte [Completar tareas de NAC Manager](#) en la página 7.

4.1 Desinstalar el software de DHCP Enforcer

1. En el menú Inicio, seleccione **Panel de Control > Agregar o quitar programas**.
2. Seleccione **Sophos DHCP Enforcer Software** y haga clic en **Eliminar**.
3. Haga clic en **Sí** para confirmar la eliminación del software.

5 Completar tareas de NAC Manager

La configuración necesaria para la imposición DHCP utilizando NAC Manager es mínima. La imposición DHCP se instala por defecto en modo de notificación. Es necesario activar la imposición.

- Las **estaciones desconocidas** no se administran desde Sophos Enterprise Console, no tienen el agente de cumplimiento instalado, no están exentas y no han ejecutado el agente soluble.
- Las **estaciones conocidas** se administran con Sophos Enterprise Console y tienen el agente de cumplimiento instalado y en ejecución.

Nota: Cree excepciones para estaciones que no puedan ejecutar el agente de cumplimiento, como aquellas con sistemas operativos no Windows. Las excepciones también se aplican a estaciones que no necesitan evaluación del cumplimiento, como servidores, routers e impresoras. Sólo es necesario excluir estaciones que reciben una asignación dinámica de la dirección IP mediante DHCP.

Entre las tareas que debe realizar en NAC Manager se incluyen:

1. Ejecutar el asistente de configuración DHCP para que los servidores proxy, de remediación, del agente soluble y DHCP utilicen la imposición DHCP de NAC.
2. Ejecutar el informe DHCP Enforcer de NAC Manager para determinar si las estaciones conocidas tendrán el acceso a la red adecuado cuando la imposición DHCP esté activada. Además de localizar estaciones que necesiten excluirse.
3. Crear excepciones para estaciones que no pueden ejecutar el agente de cumplimiento o no necesitan evaluación del cumplimiento.
4. Activar la imposición DHCP.

5.1 Ejecutar el asistente de configuración DHCP

El asistente de configuración DHCP le ayudará a identificar servidores proxy, de remediación y DHCP a utilizar con Sophos NAC DHCP, y configurar de forma automática las plantillas de acceso predefinidas de DHCP Enforcer.

Procedimiento

1. Inicie sesión en NAC Manager.
2. Seleccione **Configure System > DHCP Configuration Wizard**. Haga clic en **Next**.
3. Escoja una de las siguientes opciones:
 - Si utiliza servidores proxy, haga clic en **Yes** y luego en **Next**. Vaya al siguiente paso.
 - Si **no** utiliza servidores proxy, haga clic en **No** y luego en **Next**. Vaya al paso 5.
4. Defina los servidores proxy de acceso a Internet y haga clic en **Next**.
Siga una de las siguientes opciones:
 - Desactive los servidores que **no** desea incluir como servidor proxy.
 - Haga clic en **Add** para añadir nuevos servidores, introduzca la información del proxy y haga clic en **OK**. Repita este paso según sea necesario para añadir servidores adicionales. Podrá administrar los servidores desde **Enforce > Network Resources**.

Nota: Los servidores seleccionados sustituirán a los servidores existentes en la plantilla de acceso predeterminada DHCP - Internet Access DHCP Enforcer.

- Defina los servidores de remediación, como los controladores de dominio, y haga clic en **Next**.

Siga una de las siguientes opciones:

- Desactive los servidores que **no** desea incluir como servidor de remediación.
- Haga clic en **Add** para añadir nuevos servidores, introduzca la información del servidor de remediación y haga clic en **OK**. Repita este paso según sea necesario para añadir servidores adicionales. Podrá administrar los servidores desde **Enforce > Network Resources**.

Nota: Los servidores seleccionados sustituirán a los servidores existentes en la plantilla de acceso predeterminada DHCP - Remediation Access DHCP Enforcer.

- Escoja una de las siguientes opciones:

- Si ha instalado el agente soluble, haga clic en **Yes** y luego en **Next**. Vaya al siguiente paso.
- Si **no** ha instalado el agente soluble, haga clic en **No** y luego en **Next**. Vaya al paso 8.

Nota: Si ha instalado el agente soluble en el mismo servidor que Sophos NAC, no necesita crear un servidor adicional.

- Defina los servidores que incluyen el agente soluble para que DHCP Enforcer pueda conectarse. Esto es necesario para que estaciones invitadas puedan darse a conocer en la red. Haga clic en **Add** para añadir nuevos servidores, introduzca la información del servidor con el agente soluble y haga clic en **OK**. Haga clic en **Next**. Podrá administrar los servidores desde **Configure System > Server Settings**.
- Defina los servidores que se utilizarán para la imposición DHCP. Haga clic en **Add** para añadir nuevos servidores, introduzca la información del servidor de DHCP Enforcer y haga clic en **OK**. Repita este paso según sea necesario para añadir servidores adicionales. Haga clic en **Next**. Podrá administrar los servidores desde **Configure System > Server Settings**.
- Haga clic en **Finish**.

5.2 Ejecutar el informe de DHCP Enforcer

Ejecute el informe de DHCP Enforcer de Sophos NAC para comprobar el estado de cumplimiento de las estaciones antes de activar la imposición DHCP. Las políticas predefinidas de NAC vienen en modo de sólo informes. Estos informes le permitirán determinar si se aplican las plantillas de acceso correspondientes a cada estado de cumplimiento. Desde el informe de DHCP Enforcer puede omitir dispositivos y acceder a los detalles de la evaluación.

Procedimiento

- Inicie sesión en NAC Manager.
- Haga clic en **Report > Troubleshooting**.
- Haga clic en la lista **Report Type** y seleccione **DHCP Enforcer**.

- Haga clic en el **signo más** junto a **Report Criteria** e indique las opciones de búsqueda que desee. También puede hacer clic en el enlace **Custom Sort** para ver las opciones de orden, que se aplicarán sólo de forma temporal.

Nota: Puede utilizar los caracteres comodín * y % al realizar búsquedas. Por ejemplo, si escribe M% en el campo de la clase de usuario, aparecerán todos los equipos cuyo nombre empiece por M. Del mismo modo, si escribe M sin el símbolo % en el campo de la clase de usuario, aparecerán sólo los equipos cuyo nombre sea M.

- Haga clic en **Run**.

Campos y descripciones

Campo	Descripción
Entrada resumida del informe	
Date/Time	Fecha y hora del intento de acceso a la red. Nota: La fecha y hora se derivan del huso horario en el que se encuentre el navegador que accede a NAC Manager.
MAC Address	Dirección MAC del dispositivo que intenta conectarse a la red. La dirección MAC de la lista se asigna al NIC asociado con la solicitud del cliente de DHCP.
Computer Name	Nombre del dispositivo que intenta conectarse a la red. El nombre del ordenador se deriva de la solicitud del cliente.
Compliance State	Estado de cumplimiento de la estación, asignado durante la evaluación del cumplimiento. Los estados de cumplimiento disponibles son Compliant, Partially Compliant y Non-Compliant. Tres guiones (---) indican que el agente no ha informado del estado de cumplimiento. Las plantillas de acceso de DHCP Enforcer asociadas con el estado de cumplimiento de la política determina el acceso a la red.
Template Name (Version)	Nombre y versión de la plantilla de acceso que determinó la acción que DHCP Enforcer llevó a cabo. La plantilla de acceso utilizada se basa en la razón. A continuación se describe la plantilla de acceso predeterminada: <ul style="list-style-type: none"> ■ DHCP - Full Access: Ofrece acceso a la red sin restricciones. ■ DHCP - Internet Access: Ofrece acceso a Internet pero no a la red interna. ■ DHCP - Remediation Access: Ofrece acceso sólo a los servidor NAC de Sophos y al servidor del agente soluble.
Reason	Razón por la que DHCP Enforcer asigna una plantilla de acceso determinada. Las razones disponibles son: <ul style="list-style-type: none"> ■ Assessment: La evaluación realizada por el agente determinó el estado de cumplimiento. Las plantillas de acceso de DHCP Enforcer asociadas con el estado de cumplimiento de la política determina el acceso a la red. Aparece un enlace que accede a los datos sobre la evaluación del cumplimiento asociado con esta entrada de DHCP Enforcer.

Campo	Descripción
	<ul style="list-style-type: none"> ■ Default Template: La estación puede tener una política asociada o ser una excepción designada, pero no se encontró una plantilla de acceso asociada. Las plantillas de acceso de estación desconocida designadas en el área Configure System > Enforcer Settings determinan el acceso a la red. ■ Enforcer Override: No se comprobó la imposición. Si la casilla de anulación de DHCP Enforcer no está seleccionada en el área Configure System > Enforcer Settings, las plantillas de acceso del modo de mantenimiento y de anulación de Enforcer también designadas en el área determinan el acceso a la red. ■ Exempted: La estación está exenta según los criterios de excepción definidos en el área Enforce > Exemptions. Las plantillas de acceso asociadas con los criterios de excepción determinan el acceso a la red. Las siguientes razones secundarias de excepción aparecen en paréntesis: <ul style="list-style-type: none"> ■ User Class: La clase de usuario se encuentra exenta. ■ Vendor Class: La clase de proveedor se encuentra exenta. ■ MAC: La dirección MAC se encuentra exenta. ■ IP Scope: El ámbito IP se encuentra exenta. ■ Maintenance Mode: El software está en modo de mantenimiento. Las plantillas de acceso de Maintenance Mode/Enforcer Override designadas en el área Configure System > Enforcer Settings se utilizan para determinar el acceso a la red. ■ Policy Retrieval Error: El estado de cumplimiento de la estación no está actualizado según el campo del umbral de actualización de la política de DHCP configurada en el área Configure System > Enforcer Settings. Las plantillas de acceso de DHCP Enforcer asociadas con el estado de obtención de la política determinan el acceso a la red. ■ Remediate: Esta política está en modo de remediación. Las plantillas de acceso de DHCP Enforcer asociadas con el modo de política de remediación determinan el acceso a la red. ■ Report Only: Esta política está en el modo de sólo informes. Las plantillas de acceso de DHCP Enforcer asociadas con el modo de política de sólo informes determinan el acceso a la red. ■ Reserved: La dirección MAC del dispositivo que solicita acceso a la red está reservada como dispositivo especial en el servidor de DHCP. ■ System Error: Enforcer encontró un error que impidió la realización de la operación. La configuración del registro SystemErrors en el servidor NAC deniega por defecto el acceso a la red. ■ Template Error: No se encontró una plantilla de acceso asociada y las plantillas de acceso predeterminadas designadas en el área Configure System > Enforcer Settings no se pudieron utilizar. Si aparece este error, el servidor de DHCP determina el acceso a la red, que no devolverá una clase de usuario y denegará el acceso al usuario.

Campo	Descripción
	<ul style="list-style-type: none"> ■ Unknown Endpoint: No existe un registro del cumplimiento. Las plantillas de acceso de estación desconocida designadas en el área Configure System > Enforcer Settings determinan el acceso a la red.
Returned User Class	Clase de usuario de DHCP devuelta al servidor de DHCP por DHCP Enforcer para la imposición.
DHCP Server	Dirección IP del servidor de DHCP que solicita acceso a la red desde DHCP Enforcer. Este servidor de DHCP es el servidor en el que está instalado el software de DHCP Enforcer.
Entrada detallada del informe	
Agent Enforcement Action	<p>Acción llevada a cabo por el agente en relación a la asignación de la dirección IP. La estación inicia la publicación y renovación de direcciones IP según la acción de imposición del agente especificada en la política. El agente obtiene direcciones IP nuevas cuando se inicia y comienza la evaluación del cumplimiento, cuando el estado de cumplimiento de la estación cambia, cuando el modo de la política cambia y cuando las plantillas de acceso de DHCP Enforcer definidas en la política de la estación cambian. Los valores disponibles incluyen:</p> <ul style="list-style-type: none"> ■ None: No se publican ni renuevan direcciones IP para la estación. ■ Release Renew: Se publican las direcciones IP para la estación y se renuevan utilizando el servidor DHCP. Las direcciones IP actuales se abandonan antes de obtener las nuevas. ■ Tres guiones (---): El agente no informó sobre ninguna acción.
Vendor Class	Clase de proveedor del cliente de DHCP.
DHCP Relay	La dirección IP del transmisor de DHCP (si existe en la solicitud de DHCP original) utilizada por DHCP Enforcer para seleccionar una plantilla de acceso de DHCP Enforcer. Aparece 0.0.0.0 si no se utiliza el transmisor de DHCP.
Transaction ID	Identificador de transacción que devuelve el servidor de DHCP. El ID de transacción asocia los mensajes del cliente de DHCP con las respuestas del servidor.

5.3 Crear excepciones DHCP

Las estaciones exentas no pueden ejecutar el agente de cumplimiento, como aquellas con sistemas operativos no Windows. Las excepciones también se aplican a estaciones que no necesitan evaluación del cumplimiento, como servidores, routers e impresoras. Sólo es necesario excluir estaciones que reciben una asignación dinámica de la dirección IP mediante DHCP. Si no crea excepciones, estos equipos no tendrán acceso a la red.

Desde NAC Manager podrá crear:

- **Excepciones DHCP por criterio:** Mediante direcciones MAC, clases de usuario o fabricantes.
- **Excepciones IP por ámbito:** Mediante segmentos de red.

5.3.1 Crear excepciones DHCP por criterio

Desde NAC Manager podrá crear excepciones por criterio DHCP. Los criterios de excepciones y las plantillas de acceso de DHCP Enforcer se utilizan en conjunto para identificar excepciones y designar acciones. Una vez que se encuentran criterios de excepciones definidos que corresponden, las plantillas de acceso de DHCP Enforcer asociadas determinan la acción de acceso a la red adecuada.

Procedimiento

1. Inicie sesión en NAC Manager.
2. Haga clic en **Enforce > Exemptions**. Después, haga clic en **Create Exemption** en la parte inferior izquierda de la página.
3. Escriba un nombre y una descripción de la excepción.
4. Haga clic en la lista **Exemption Type** y seleccione **DHCP Criteria**.
5. En la sección Exemption Criteria, seleccione las opciones **MAC Address**, **User Class** o **Vendor Class** para especificar los criterios de excepción que quiere definir, escriba la dirección MAC (o prefijo), la clase de usuario o la clase de proveedor adecuados en el campo proporcionado y haga clic en **Add**.

Repita este paso según sea necesario para añadir criterios de excepciones adicionales.

Nota: Puede utilizar el símbolo * para especificar excepciones con comodines, siempre y cuando el símbolo * vaya al final. Por ejemplo, si especifica AA* como dirección de MAC, todas las direcciones de MAC que empiecen por AA se exceptuarán. Si indica la dirección MAC sin el símbolo *, deberá especificar la dirección MAC exacta.

6. Haga clic en **Select** para añadir plantillas de acceso de DHCP Enforcer a la excepción, seleccione la plantilla de acceso **DHCP - Full Access** y haga clic en **OK**.

La plantilla de acceso **DHCP - Full Access** está predefinida en Sophos NAC para permitir el acceso a la red. Las excepciones que utilicen esta plantilla darán acceso a la red sin necesidad de comprobar el estado de cumplimiento con Sophos NAC.

7. Haga clic en **Save**.

5.3.2 Crear excepciones de ámbito IP

Sólo es necesario excluir estaciones que reciben una asignación dinámica de la dirección IP mediante DHCP. Desde NAC Manager podrá crear excepciones de ámbito IP. El ámbito se define mediante segmentos de la red. Las excepciones de ámbito IP son útiles cuando se realizan implementaciones por fases; puede excluir estaciones o redes a las que no quiera imponer las políticas de momento.

Procedimiento

1. Inicie sesión en NAC Manager.

2. Haga clic en **Enforce > Exemptions**. Después, haga clic en **Create Exemption** en la parte inferior izquierda de la página.
3. Escriba un nombre y una descripción de la excepción.
4. Haga clic en la lista **Exemption Type** y seleccione **IP Scope**.
5. En la sección **Exempted IP Scopes**, haga clic en **Select** para añadir un nuevo ámbito IP a la excepción, seleccione el ámbito apropiado y haga clic en **OK**.
Si no encuentra el ámbito IP que necesita, cree uno nuevo. Para ello, es necesario crear una plantilla de acceso nueva de DHCP Enforcer o actualizar una de las predefinidas.
6. Según sea necesario, utilice las flechas para dar prioridad a los ámbitos.
Si una excepción está relacionada con más de un rango IP, se utiliza el primero. Sophos recomienda dar prioridad a los rangos IP más estrictos y específicos primero y a los menos después.
7. Haga clic en **Save**.

Importante: Una vez creadas las excepciones, puede darles mayor o menor prioridad en la página **Exemptions**. Si más de una excepción está relacionada con una estación determinada, se utiliza la primera excepción asociada con la estación. Sophos recomienda dar prioridad a las excepciones más estrictas y específicas primero y a las menos después.

5.4 Activar la imposición DHCP

Si lo desea, puede activar la imposición DHCP tanto para estaciones conocidas como desconocidas, lo que permite utilizar la imposición DHCP para las estaciones desconocidas y la imposición del agente para las conocidas.

5.4.1 Activar la imposición DHCP para estaciones desconocidas

Si lo desea, puede activar la imposición DHCP para estaciones desconocidas en todos los servidores DHCP, lo que permite especificar qué servidores DHCP pondrán en cuarentena estaciones desconocidas. Utilice esta función para realizar distribuciones por fases de la imposición DHCP.

Antes de activar la imposición DHCP para las estaciones desconocidas, es necesario crear excepciones. Sólo es necesario excluir estaciones que reciben una asignación dinámica de la dirección IP mediante DHCP. Para más información, consulte [Crear excepciones DHCP](#) en la página 11.

Procedimiento

1. Haga clic en **Configure System > Server Settings**.
2. Haga clic en el nombre del servidor DHCP para el que quiere activar la imposición DHCP.
3. Haga clic en la lista **Unknown Endpoint Mode** y seleccione **Enforce**.

Nota: Por defecto, la plantilla de acceso **DHCP - Remediation Access** determina el acceso a la red. Dicha plantilla pone la estación en cuarentena y permite el acceso a los servidores de remediación especificados al ejecutar el asistente de configuración DHCP. Puede cambiar la plantilla de acceso en el área **Configure System > Enforcer Settings**.

4. Haga clic en **Save**.

5.4.2 Activar la imposición DHCP para estaciones conocidas

Si tiene intención de utilizar la imposición DHCP en lugar o además de la imposición del agente para estaciones conocidas, cambie el modo de políticas a Enforce en las políticas correspondientes.

Importante: Todas las políticas y cambios tienen efecto de forma inmediata, pero las políticas no se aplican a las estaciones hasta que el agente las recupera.

Procedimiento

1. Inicie sesión en NAC Manager.
2. Haga clic en **Manage > Políticas**. Después, haga clic en el nombre de la política que desee actualizar. Para más información sobre las políticas predefinidas, consulte [Utilizar las políticas predefinidas](#) en la página 15.
3. Haga clic en la lista **Policy Mode** y seleccione **Enforce**.
 - **Enforce:** Modo de control en el que las estaciones se evalúan según las políticas asignadas y se genera un informe en NAC Manager. Se muestran mensajes y se realizan acciones de remediación e imposición según el estado de acceso. El modo de imposición utiliza las plantillas de acceso asignadas en el paso 5.
4. Haga clic en la lista **Agent Enforcement Action** y seleccione **Release Renew**. Debe seleccionar Release Renew al utilizar la imposición DHCP para estaciones conocidas.
5. En el área Network Access, haga clic en **DHCP**. Abra la ficha **Enforce** y verifique las asignaciones de la plantilla de acceso.

Nota: Por defecto, cada política se rellena de forma automática con las plantillas de acceso. Asegúrese de que se aplican las plantillas de acceso apropiadas. No modifique las asignaciones de las plantillas para el modo de sólo informes y el de remediación.

Asignaciones predefinidas de plantillas de DHCP Enforcer

- **Policy Retrieval Error:** El estado de cumplimiento de la estación no está actualizado según el campo del umbral de actualización de la política de DHCP configurada en el área **Configure System > Enforcer Settings**. La plantilla de acceso DHCP - Remediation Access impide el acceso a la red excepto a los servidores de remediación especificados al ejecutar el asistente de configuración DHCP.
- **Compliant:** La estación cumple las políticas. La plantilla de acceso DHCP - Full Access permite el acceso a la red cuando la estación cumple la política.
- **Partially Compliant:** La estación cumple de forma parcial con la política establecida. La plantilla de acceso DHCP - Full Access permite el acceso a la red cuando la estación cumple la política parcialmente.
- **Non-Compliant:** La estación no cumple con la política establecida. La plantilla de acceso DHCP - Remediation Access impide el acceso a la red excepto a los servidores de remediación especificados al ejecutar el asistente de configuración DHCP.

6. Según sea necesario, utilice las flechas para dar mayor o menor prioridad a las plantillas de acceso de DHCP Enforcer.
Si un estado determinado tiene más de una plantilla, se utiliza la primera que cumple el estado. Sophos recomienda dar prioridad a las plantillas de acceso más estrictas y específicas primero, y a las menos después.
7. Haga clic en **Save**.

5.4.2.1 Utilizar las políticas predefinidas

Las políticas predefinidas se pueden utilizar para imponer el cumplimiento de la seguridad en estaciones tanto administradas como no.

- **Default:** Esta política se usa cuando una estación tiene el agente de cumplimiento instalado pero no se ha asignado ninguna otra política. El modo de políticas está configurado por defecto para sólo enviar informes. Esta política realiza acciones de remediación en la estación si el modo de políticas se configura para remediar o imponer.
- **Managed:** Esta política puede utilizarse para estaciones administradas con Sophos Enterprise Console que tengan un agente de cumplimiento instalado. El modo de políticas está configurado por defecto para sólo enviar informes. Esta política realiza acciones de remediación en la estación si el modo de políticas se configura para remediar o imponer.
- **Unmanaged:** Esta política puede utilizarse para equipos que no pertenecen a la empresa. Esta política no realiza acciones de remediación en las estaciones. El agente soluble utiliza la política no administrada.

Nota: Si una estación no tiene un agente de cumplimiento instalado y no utiliza el agente soluble, la configuración de Enforcer determina el acceso a la red.

5.4.3 Consecuencias para el usuario de la imposición DHCP

Las repercusiones de la activación de la imposición DHCP en el usuario varían según el carácter conocido o desconocido de las estaciones. Además, los invitados pueden ejecutar el agente soluble de cumplimiento para obtener acceso a la red.

- Las **estaciones desconocidas** no se administran desde Sophos Enterprise Console, no tienen el agente de cumplimiento instalado, no están exentas y no han ejecutado el agente soluble.
- Las **estaciones invitadas** pueden utilizar agente soluble de cumplimiento para controlar el acceso a la red.
- Las **estaciones conocidas** se administran con Sophos Enterprise Console y tienen el agente de cumplimiento instalado y en ejecución.

Consecuencias de la imposición DHCP para estaciones desconocidas

Cuando la imposición DHCP está activada, las estaciones desconocidas:

1. Las estaciones se inician.
2. Cuando está activada la imposición DHCP para estaciones desconocidas, las estaciones tienen un acceso limitado a la red. Dichas estaciones pueden acceder a Internet y a los servidores de remediación especificados al ejecutar el asistente para la configuración DHCP.

Consecuencias de la imposición DHCP para estaciones invitadas

Cuando la imposición DHCP está activada y las estaciones invitadas deben utilizar el agente soluble de cumplimiento:

1. Las estaciones se inician.
2. El usuario abre Internet Explorer, va a la dirección web del agente soluble de cumplimiento y ejecuta el agente soluble de cumplimiento.
3. El agente soluble de cumplimiento realiza una evaluación y determina si la estación es conforme, parcialmente conforme o infringe la política NAC.
4. Cuando se configura y activa la imposición DHCP:
 - Las estaciones que cumplen las políticas tienen permiso de acceso a la red.
 - Las estaciones que cumplen parcialmente las políticas tienen permiso de acceso a la red. El agente soluble de cumplimiento muestra mensajes a los usuarios para que puedan remediar las estaciones y hacer que cumplan las políticas. Si la política NAC está configurada para ello, las estaciones se remedian de forma automática. Por defecto, la remediación está desactivada. No es habitual que se desee remediar las estaciones invitadas.
 - Las estaciones que no cumplen las políticas tienen prohibido el acceso a la red. Dichas estaciones pueden acceder a Internet y a los servidores de remediación especificados al ejecutar el asistente para la configuración DHCP. El agente soluble de cumplimiento muestra mensajes a los usuarios para que puedan remediar las estaciones y hacer que cumplan las políticas. Si la política NAC está configurada para ello, las estaciones se remedian de forma automática. Por defecto, la remediación está desactivada. No es habitual que se desee remediar las estaciones invitadas.

Consecuencias de la imposición DHCP para estaciones conocidas

Cuando la imposición DHCP está activada:

1. La estación se inicia y se ejecuta el agente de cumplimiento.
2. El agente de cumplimiento realiza una evaluación y determina si la estación es conforme, parcialmente conforme o infringe la política NAC.
3. Cuando se configura y activa la imposición DHCP:
 - Las estaciones que cumplen las políticas tienen permiso de acceso a la red.
 - Las estaciones que cumplen parcialmente las políticas tienen permiso de acceso a la red. El agente de cumplimiento muestra mensajes a los usuarios para que puedan remediar las estaciones y hacer que cumplan las políticas. Si la política NAC está configurada para ello, las estaciones se remedian de forma automática.
 - Las estaciones que no cumplen las políticas tienen prohibido el acceso a la red. Dichas estaciones pueden acceder a Internet y a los servidores de remediación especificados al ejecutar el asistente para la configuración DHCP. El agente de cumplimiento muestra mensajes a los usuarios para que puedan remediar las estaciones y hacer que cumplan las políticas. Si la política NAC está configurada para ello, las estaciones se remedian de forma automática.

6 Apéndice A: Usar la utilidad de configuración de DHCP Enforcer

Si necesita cambiar la configuración de DHCP Enforcer especificada durante la instalación de DHCP Enforcer, utilice la utilidad de configuración de DHCP Enforcer. Al instalar DHCP Enforcer se instala esta utilidad en el servidor DHCP. Si cuenta con más de uno, cambie la configuración de DHCP Enforcer en todos ellos.

6.1 Actualizar la clave compartida

Procedimiento

1. Desde el menú Inicio del servidor DHCP, seleccione **Sophos > NAC > Support Tools > DHCP Enforcer Configuration Utility**.
Aparece el cuadro de diálogo **DHCP Enforcer Configuration Utility** con la ficha **Enforcer** seleccionada.
2. En el cuadro de diálogo **DHCP Enforcer Configuration Utility**, haga clic en el botón **Edit**.
3. En el cuadro de diálogo **DHCP Enforcer RADIUS Enforcer Server Settings**, introduzca y confirme la clave compartida nueva y haga clic en **OK**.

6.2 Actualizar la configuración avanzada

En esta sección se describe cómo actualizar la configuración avanzada de DHCP mediante la utilidad de configuración de DHCP Enforcer. En la mayoría de los casos, no es necesario actualizar esta configuración.

Procedimiento

1. Desde el menú **Inicio** del servidor DHCP, seleccione **Sophos > NAC > Support Tools > DHCP Enforcer Configuration Utility**.
Aparece el cuadro de diálogo **DHCP Enforcer Configuration Utility** con la ficha **Enforcer** seleccionada.
2. En el cuadro de diálogo **DHCP Enforcer Configuration Utility**, abra la ficha **Advanced**.
3. Cambie la configuración de DHCP Enforcer según sea necesario.
4. Haga clic en **OK**.
Repita estos pasos en todos los servidores DHCP que necesite.

6.2.1 Campos y descripciones de la utilidad de configuración de DHCP Enforcer

Campos	Descripciones
Ficha Enforcer	
Access for Multiple Servers	Esta opción no está disponible en Sophos Endpoint Security and Control.
Cuadro de diálogo DHCP Enforcer RADIUS Enforcer Server Settings Haga clic en el botón Edit para acceder a este cuadro de diálogo. Nota: Los campos en este cuadro de diálogo se refieren al servidor NAC.	
Enable	Permite activar/desactivar el uso del servidor NAC. Al estar activado, el servidor NAC se utiliza para el cumplimiento de políticas y para informes.
IP Address	Indica la dirección IP del servidor NAC.
Authentication Port	Designa el puerto de autenticación del servidor NAC.
Accounting Port	Designa el puerto de cuenta del servidor NAC.
Shared Key	Indica la clave compartida del servidor DHCP. La clave compartida es la misma utilizada en la instalación de DHCP Enforcer.
Confirm Shared Key	Sirve para confirmar la clave compartida del servidor DHCP.
Cuadro de diálogo DHCP Enforcer Resolve IP	
Hostname	Cuando no se conoce la dirección IP, permite identificar el nombre del host del servidor NAC. Al introducir el nombre del host, se puede resolver la dirección IP.
Ficha Advanced	
Enable Policy Compliance	Active esta opción para disponer de cumplimiento y notificación en todas las solicitudes DHCP, a excepción de las indicadas con algún código de opción reservado.
Attempts	Indica el número de intentos por cada solicitud DHCP.
Timeout	Indica el tiempo en segundos antes de intentarlo de nuevo.
Default User Class	Especifica la clase de usuario a utilizar si no se puede obtener la especificada en la política.
Error	Al estar seleccionado, los mensajes de error de Microsoft se guardan en el registro de eventos de aplicaciones.

Campos	Descripciones
Warning	Al estar seleccionado, los mensajes de advertencia de Microsoft se guardan en el registro de eventos de aplicaciones.
Information	Al estar seleccionado, los mensajes de información de Microsoft se guardan en el registro de eventos de aplicaciones.
Trace	Al estar seleccionado, el registro de seguimiento de Microsoft se guarda en el registro de eventos de aplicaciones.
Subnet Mask Override	Especifica la máscara de subred disponible para los usuarios que no cumplen las políticas y anula la subred del servidor DHCP para limitar el acceso a la red.
Black Hole IP Address	DHCP Enforcer utiliza esta dirección IP ficticia para anular el tráfico de recursos bloqueado.
Cuadro de diálogo DHCP Enforcer Informs IP Address	
IP Address	Designa la dirección IP asociada con la estación, como un concentrador de acceso remoto (RAC) para el que se desea ignorar el cumplimiento de políticas y los informes de paquetes de informe de DHCP. Por defecto, el cumplimiento de políticas e informes se realizan para los paquetes de informe de DHCP. Cuando no se especifica una dirección IP, no se realiza el cumplimiento de políticas e informes para los paquetes de informe de DHCP de esa estación.
Cuadro de diálogo DHCP Enforcer Resolve IP	
Hostname	Identifica el nombre del host (cuando no se conoce la dirección IP) de la estación para la que se desea ignorar el cumplimiento de políticas e informes. Al introducir el nombre del host, se puede resolver la dirección IP.

7 Apéndice B: Actualizar la imposición DHCP

Al actualizar Endpoint Security and Control con la versión 9, la configuración DHCP dejará de funcionar. Es necesario volver a configurar la imposición DHCP.

La actualización afecta a la configuración DHCP de Endpoint Security and Control 8 de la forma siguiente:

- Elimina las plantillas de acceso anteriores de DHCP Enforcer de todas las políticas y de la página Enforcer Settings de NAC Manager.
- Actualiza todas las plantillas de acceso de DHCP Enforcer creadas con la anulación de subred de DHCP activada para restringir el acceso a la red. Se permite el acceso a Internet.
- Actualiza todas las plantillas de acceso de DHCP Enforcer creadas con la anulación de subred de DHCP desactivada para permitir el acceso a la red.

7.1 Reconfigurar la imposición DHCP

Al actualizar Endpoint Security and Control con la versión 9, es necesario volver a configurar la implementación de DHCP. Utilice las instrucciones siguientes para seguir utilizando la configuración de la imposición DHCP de Endpoint Security and Control 8.

1. Inicie sesión en NAC Manager.
2. Haga clic en **Configure System > Enforcer Settings**.
3. En el área **DHCP Enforce Access Templates**, haga clic en el icono de la **papelera** situado junto a cada plantilla de acceso DHCP.

Con este paso se eliminan las plantillas de acceso DHCP de la configuración de Enforcer para poder añadir las plantillas de acceso DHCP existentes, como se describe a continuación.

4. Haga clic en **Select** en **DHCP Enforcer Access Templates**; active las opciones **Unknown Endpoint (Report Only)**, **Maintenance Mode/Enforcer Override** y **Default - DHCP Permit (NULL User Class)**; y haga clic en **OK**.

Esta combinación de opciones permite el acceso a las estaciones desconocidas, y a todas las estaciones cuando el servidor NAC está en modo de mantenimiento o la opción **Override DHCP Enforcer** está seleccionada.

5. Haga clic en **Select** en **DHCP Enforcer Access Templates**; active las opciones **Unknown Endpoint (Enforce)**, **Default** y **Default - DHCP Deny (NACDeny User Class)**; y haga clic en **OK**.

Esta combinación de opciones impide el acceso a las estaciones desconocidas cuando la imposición DHCP está activada para las estaciones desconocidas. Para más información, consulte [Activar la imposición DHCP para estaciones desconocidas](#) en la página 13. Esta combinación de opciones también impide el acceso a las estaciones desconocidas cuando Sophos NAC no puede determinar la plantilla de acceso asociada.

6. Haga clic en **Manage > Policies**. A continuación, haga clic en el nombre de la política que utiliza para la imposición DHCP.

7. En el área de navegación izquierda **Network Access**, haga clic en **DHCP**, abra la ficha del modo de políticas **Report Only** y haga clic en el icono de la **papelera**.

Repita este paso en las fichas de los modos **Remediate** y **Enforce**.

Con este paso se eliminan las plantillas de acceso DHCP de la política para poder añadir las plantillas existentes en el paso siguiente.

8. Abra la ficha del modo de políticas **Report Only**, haga clic en **Select**, active la opción **Default - DHCP Permit (NULL User Class)** y haga clic en **OK**.

Repita este paso en las fichas de los modos **Remediate** y **Enforce**. Para la remediación, seleccione la plantilla de acceso **Default - DHCP Permit (NULL User Class)**. Para la imposición, seleccione la plantilla de acceso **Default - DHCP Deny (NACDeny User Class)**.

Cuando la política está en modo Report Only o Remediate, las estaciones que tienen el agente de cumplimiento instalado tienen permiso de acceso. Cuando la política está en modo Enforce, las políticas que tienen el agente de cumplimiento instalado y no cumplen las políticas no tienen permiso de acceso.

9. Haga clic en **Save**.

La imposición DHCP se ha configurado para que pueda seguir utilizando la configuración de la imposición DHCP de Endpoint Security and Control 8.

8 Soporte técnico

Para soporte técnico, visite <http://www.sophos.com/support>.

Cuando se ponga en contacto con el servicio de soporte técnico, ofrezca toda la información posible, incluyendo:

- La versión del software de Sophos
- Los sistemas operativos y parches
- El texto exacto de cualquier mensaje de error

9 Copyright

Copyright © 2009 Sophos Group. Reservados todos los derechos. Ninguna parte de esta publicación puede ser reproducida, almacenada o transmitida de ninguna forma, ni por ningún medio, sea éste electrónico, químico, mecánico, electro-óptico, grabación, fotocopia o cualquier otro, a menos que disponga de una licencia válida, en cuyo caso puede reproducirse según los términos del acuerdo de licencia, o con la previa autorización escrita por parte del propietario.

Todos los demás nombres de productos o empresas mencionados son marcas comerciales o registradas de sus respectivos propietarios.