

SOPHOS

Sophos Compliance Agent Guía de configuración

Versión: 3.3

Edición: septiembre de 2009



Contenido

- 1 Acerca de esta guía.....3
- 2 Agente de cuarentena.....4
- 3 Agente soluble.....10
- 4 Idiomas del agente.....14
- 5 Soporte técnico.....15
- 6 Copyright.....16

1 Acerca de esta guía

En esta guía se describe la configuración del agente de cumplimiento para el software de Sophos Endpoint Security and Control.

En concreto, ofrece información sobre:

- El diseño, configuración y registro del agente de cumplimiento y el agente soluble de cumplimiento.
- Los componentes de la interfaz de cada agente, como los cuadros de diálogo.
- Los idiomas disponibles del agente.

Esta guía le será útil si:

- Utiliza Enterprise Console.
- Utiliza Sophos NAC para Endpoint Security and Control.
- Desea información sobre el diseño del agente de cumplimiento y del agente soluble de cumplimiento.
- Desea saber qué componentes de la interfaz aparecen en las estaciones.

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 Introducción

El agente de cumplimiento de Sophos es una aplicación de estaciones configurable que evalúa e impone el cumplimiento con las políticas NAC. El agente toma la política NAC, evalúa el cumplimiento de la estación, remedia aplicaciones de forma automática y proporciona mensajes al usuario, y envía información de informes.

Sophos NAC es compatible con dos configuraciones del agente. El agente de cuarentena se instala en estaciones con Microsoft Windows®. El agente soluble se utiliza para ordenadores invitados con Microsoft Windows.

- **Agente de cuarentena:** El agente de cuarentena evalúa estaciones para determinar si cumplen la política NAC. Las evaluaciones se realizan antes y de forma periódica después de permitir el acceso a la red. El agente no necesita demasiada interacción del usuario. El agente de cuarentena tiene una función de imposición y limita las estaciones a áreas específicas de la red si no cumplen la política NAC.
- **Agente soluble:** El agente soluble evalúa estaciones para determinar si cumplen la política NAC antes de permitir el acceso a la red. El agente soluble debe ejecutarse desde un navegador. El agente soluble está diseñado para usuarios que no tienen un agente instalado pero que necesitan acceder a determinados recursos de red. El agente soluble no cuenta con funciones de imposición, pero puede utilizarse con imposición DHCP.

Para más información, consulte la *Guía de configuración de DHCP de Sophos NAC*.

2 Agente de cuarentena

En esta sección se describe el diseño y la configuración del agente de cuarentena.

2.1 Diseño

El agente de cuarentena es una aplicación de la bandeja del sistema que se instala en las estaciones y realiza procesos de forma periódica según la política NAC definida en NAC Manager. Para la instalación se requieren derechos de administrador local.

Configuración del agente

El agente de cuarentena aparece como un icono en la bandeja del sistema que muestra el estado actual del agente. El icono del agente de cuarentena cambia cuando la estación está en cuarentena, cuando tiene acceso total a la red, o cuando hay resultados pendientes. La configuración del agente se realiza mediante plantillas desde NAC Manager y puede utilizarse para controlar las opciones que se muestran y las funciones de la interfaz. Al añadir una plantilla de configuración del agente a una política, los agentes pueden obtenerla e implementar la configuración en las estaciones.

Procesos

El agente de cuarentena realiza una evaluación inicial del cumplimiento y evaluaciones periódicas para asegurar que la estación sigue cumpliendo la política NAC. El agente de cuarentena intentará completar todas las operaciones: obtención de políticas, verificación, control, remediación y notificación. Si se produce un error en alguna operación, se vuelve a intentar la próxima vez que esté programada.

Acceso a la red

El usuario podrá acceder a los recursos de la red según el estado de cumplimiento del sistema y la plantilla de acceso asociada. Por ejemplo, si la estación no cumple las políticas, el agente puede ponerla en cuarentena y restringir el acceso a la red según esté definido en las plantillas de acceso asociadas en caso de infracción. Si se restringe el acceso, el agente debe permitir que los usuarios lo recuperen y habilitar el acceso a un servidor proxy para la remediación, si es necesario.

Acceso al servidor proxy

Si es necesaria la autenticación del usuario mediante un servidor proxy para que el agente se comunique con el servidor NAC, aparece el cuadro de diálogo de solicitud de credenciales en la estación para que el usuario introduzca el nombre de usuario y la contraseña antes de recuperar la política. Si el nombre de usuario y la contraseña del proxy se guardaron como configuración del agente en NAC Manager, el agente administra de forma automática las solicitudes de autenticación de la estación sin solicitar la intervención del usuario.

Evaluaciones de cumplimiento y cuarentena

Las estaciones permanecen en la cuarentena hasta que cumplen las políticas. Sin embargo, los usuarios pueden anularla durante una sesión del agente si la política NAC lo permite. La cuarentena se restablece cuando el usuario desactiva la anulación de la misma o cuando cierra la sesión en el equipo. Además de las comprobaciones periódicas, el usuario también puede solicitar una comprobación de su estado de cumplimiento en cualquier momento, desde el

icono del agente de cuarentena de la bandeja del sistema o desde el cuadro de diálogo de resultados.

Informes y mensajes

El agente también realiza funciones de notificación, incluyendo detalles sobre el software en el sistema, el estado de cumplimiento según la política NAC, las acciones llevadas a cabo y los mensajes mostrados. Durante el proceso, el agente de cuarentena muestra mensajes al usuario, definidos en NAC Manager, y errores.

2.2 Configuración

Para configurar el agente de cuarentena, siga estos pasos:

1. **En NAC Manager, cree recursos de red y aplíquelos a las plantillas de acceso de Agent Enforcer utilizadas en la política para estaciones infractoras.**

Los recursos de red son aplicaciones o dispositivos necesarios para la remediación de estaciones o aquellos a los que se les niega el acceso a las estaciones en cuarentena. Las plantillas de acceso de Agent Enforcer se utilizan junto con las políticas para identificar los recursos de red que las estaciones pueden acceder o no al imponer cuarentenas. Es necesario incluir recursos de red para la remediación de estaciones que no cumplen con las políticas establecidas, además de permitir el acceso a un servidor proxy para la remediación, si corresponde.

2. **Distribuir el agente de cumplimiento de Sophos a las estaciones desde Sophos Enterprise Console.**

En Sophos Enterprise Console, utilice el asistente para proteger ordenadores para distribuir el agente de cuarentena a las estaciones. El agente se encargará de obtener e implementar la política correspondiente. El agente obtiene la política asociada con el grupo de la estación en Sophos Enterprise Console y la utiliza para la evaluación del cumplimiento de la estación.

Para más información sobre recursos de red, plantillas de acceso de Agent Enforcer y políticas, consulte la ayuda de NAC Manager.

2.3 Registro

El agente de cuarentena dispone de diferentes archivos de registro para facilitar la resolución de cualquier problema.

Durante la instalación del agente de cumplimiento de Sophos, se crean registros de forma automática. Si tiene problemas con la instalación, el registro le ayudará a identificar la causa. El registro de instalación del agente se encuentra en el directorio **%tmp%**. Si no ha modificado la ubicación predeterminada del directorio temporal, podrá abrirlo desde Windows Explorer escribiendo la dirección **%tmp%**.

El registro también se puede utilizar para solucionar problemas del agente en las estaciones. El registro afecta al rendimiento del agente; por eso, se recomienda activarlo sólo para solucionar problemas y desactivarlo una vez solucionados. En los registros no se incluye información privada del usuario. El registro se activa desde la interfaz del agente y se pueden configurar diferentes niveles.

Existen tres archivos de registro:

- **Session Log:** Ofrece información sobre errores de alto nivel.
- **Trace Log:** Ofrece información detallada sobre errores.
- **Agent Log:** Ofrece información sobre errores del agente.

1. En NAC Manager, abra la página de **creación de plantillas de configuración del agente**.
2. Añada la función **Logging** en la plantilla del agente con las opciones correspondientes.
Para más información sobre la configuración del agente, consulte la ayuda de NAC Manager.
3. En el ordenador donde desee activar el registro, abra el cuadro de diálogo **Acerca de** y seleccione **Activar registro**.

Los archivos de registro se encuentran en la carpeta <unidad>:\Documents and Settings\All Users\Datos de programa\Sophos\Sophos NAC\Logs, en Vista será <unidad>:\ProgramData\Sophos\Sophos NAC\Logs.

4. Una vez solucionado el problema, en la estación, abra el cuadro de diálogo **Acerca de** del agente y desactive la opción **Activar registro**.

2.4 Iconos, menús, mensajes y cuadros de diálogo

A continuación se describen los iconos, menús, mensajes y cuadros de diálogo del agente de cuarentena.

2.4.1 Iconos de la bandeja del sistema e información emergente

El icono en la bandeja del sistema ofrece información sobre el estado del agente mediante:

- El color del icono para los diferentes estados.
- Los mensajes que aparecen al situar el puntero del ratón sobre el icono.



Figura 1: Ejemplo de icono de la bandeja del sistema e información emergente

En la siguiente tabla se describen los diferentes iconos.

| Icono | Información emergente | Descripción |
|-------|---|---|
| | Haga doble clic para ver los resultados pendientes. Haga doble clic para ver los resultados. | Aparece cuando existen acciones pendientes que se mostrarán en el cuadro de resultados. |
| | Sophos agente de cumplimiento: inactivo. Equipo en cuarentena. | Icono que aparece cuando la estación está en cuarentena. |
| | Sophos agente de cumplimiento: inactivo. | Aparece cuando el agente está inactivo. |

2.4.2 Menú

Al menú se accede haciendo clic con el botón derecho del ratón sobre el icono en la bandeja del sistema. Si hace doble clic en el icono se ejecuta la acción predeterminada (se muestra en **negrita**).

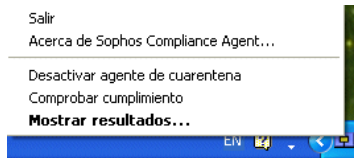


Figura 2: Menú

A continuación se describen las diferentes acciones disponibles en el menú.

| Opción del menú | Descripción |
|--|--|
| Salir | Se cierra el agente, se elimina el icono de la bandeja del sistema y se pone el ordenador en cuarentena, si procede. Nota: Esta opción del menú está visible si Show Exit Agent está configurado como Show. Esta opción del menú no está visible si Show Exit Agent está configurado como Hide (valor predeterminado). Para más información sobre la configuración del agente, consulte la ayuda de NAC Manager. |
| Acerca de Sophos agente de cumplimiento... | Muestra el cuadro de diálogo Acerca de. |
| Desactivar agente de cuarentena | Anula la cuarentena de la estación. Cuando se desactiva la cuarentena, se mostrará una marca indicativa junto al texto. Cuando la cuarentena está activada, no hay ninguna marca junto al texto. Nota: Si la opción Quarantine Override de la política está configurada como False (es decir, si la estación no puede anular la cuarentena), esta opción no aparece en el menú. |
| Comprobar cumplimiento | Inicia el proceso de comprobación del cumplimiento: obtención y revisión de políticas, imposición, acciones de remediación y notificación. |
| Mostrar resultados... | Muestra el cuadro de diálogo con los resultados más recientes. |

2.4.3 Mensajes

Los mensajes que aparecen junto al icono en la bandeja del sistema informan al usuario de cambios en el estado del agente. Los mensajes aparecen si es necesaria la intervención del usuario porque hay resultados pendientes o si el estado del agente cambia.

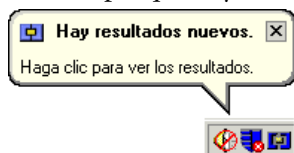


Figura 3: Ejemplo de mensaje

A continuación se describen los diferentes mensajes disponibles.

| Icono | Texto del mensaje | Descripción |
|-------|---|---|
| | Título: Hay resultados nuevos. Texto: Haga clic para ver los resultados. | Aparece cuando existen acciones pendientes que se mostrarán en el cuadro de resultados. |
| | Título: El equipo se ha puesto en cuarentena. Texto variable. | Aparece cuando la estación está en cuarentena. |
| | Título: El equipo ya no está en cuarentena. Texto variable. | Aparece cuando la estación se elimina de la cuarentena. |

2.4.4 Cuadro de diálogo de solicitud de credenciales

El cuadro de diálogo de solicitud de credenciales aparece si se requiere autenticación a través de un proxy para que el servidor se comunice con el servidor NAC.

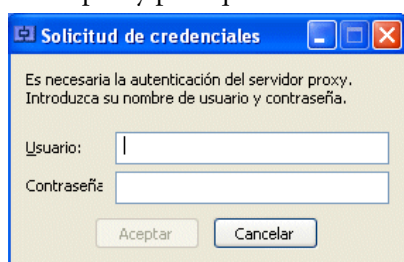


Figura 4: Cuadro de diálogo de solicitud de credenciales

2.4.5 Cuadro de diálogo de resultados

El cuadro de diálogo de resultados muestra los mensajes dirigidos al usuario según la política y mensajes de error. Se puede acceder a este cuadro de diálogo desde la opción Mostrar resultados en el menú del icono.



Figura 5: Cuadro de diálogo de resultados

2.4.6 Cuadro de diálogo Acerca de

El cuadro de diálogo Acerca de muestra información sobre el agente, copyright y la opción Activar registro. Se puede acceder a este cuadro de diálogo desde la opción Acerca de en el menú del icono.



Figura 6: Cuadro de diálogo Acerca de

3 Agente soluble

En esta sección se describe el diseño y la configuración del agente soluble.

3.1 Diseño

El agente soluble puede instalarse en cualquier servidor web de Windows, incluido el servidor NAC, y ofrece una página web desde la que los usuarios pueden ejecutarlo. Este agente es una aplicación independiente y se ejecuta en las estaciones sin necesidad de permisos de administrador. Si es necesaria la autenticación del usuario mediante un servidor proxy para que el agente soluble se comunique con el servidor NAC, el navegador web pide las credenciales al usuario.

Procesos

Una vez iniciado, el agente soluble muestra una serie de cuadros de diálogo que indican el progreso y las acciones correspondientes. El agente soluble lleva a cabo los procesos (obtener políticas, evaluar políticas, imponer políticas, remediar y crear informes) según se establezca en la política NAC definida en NAC Manager. Una vez finalizados los procesos, el agente soluble se elimina de la estación. El agente soluble no cuenta con funciones de imposición, pero puede utilizarse con imposición DHCP.

Informes y mensajes

El agente también realiza funciones de notificación, incluyendo detalles sobre el software en el sistema, el estado de cumplimiento según la política NAC, las acciones llevadas a cabo y los mensajes mostrados. Durante el proceso, el agente de cuarentena muestra mensajes al usuario, definidos en NAC Manager, y errores.

3.2 Configuración

Para poder utilizar el agente soluble en la red, es necesario instalarlo en un servidor web Windows al que tengan acceso los ordenadores invitados. Puede utilizar el mismo servidor con Sophos NAC.

1. Instale el agente soluble de cumplimiento de Sophos en un servidor web Windows.

El agente soluble está disponible en el sitio web de Sophos. También puede instalar el agente soluble desde el CD-ROM Sophos Install. La instalación del agente soluble de cumplimiento de Sophos instala todos los archivos compatibles con el agente soluble. Para más información, consulte la *Guía avanzada de inicio de Sophos Endpoint Security and Control*.

2. Distribuya la dirección web del agente soluble de cumplimiento de Sophos a los usuarios invitados, según sea necesario.

Las estaciones obtienen la política asignada y evalúan su cumplimiento. Si instala el agente soluble en el directorio predeterminado, las estaciones pueden acceder al agente soluble desde la dirección web: `http://<dirección IP/nombre DNS>/dissolvableagent`. La dirección IP o nombre DNS corresponde al servidor donde instaló el agente.

3.3 Registro

El registro del agente soluble no se configura desde NAC Manager. El registro se define en las estaciones.

El agente dispone de diferentes archivos de registro para facilitar la resolución de cualquier problema. El registro afecta al rendimiento del agente; por eso, se recomienda activarlo sólo para solucionar problemas y desactivarlo una vez solucionados. En los registros no se incluye información privada del usuario.

Existen tres archivos de registro:

- **Session Log:** Ofrece información sobre errores de alto nivel.
- **Trace Log:** Ofrece información detallada sobre errores.
- **Agent Log:** Ofrece información sobre errores del agente.

1. Inicie el agente soluble.
2. Haga clic en el icono de Sophos NAC en el cuadro de diálogo de **resultados** y seleccione **Acerca de Sophos agente de cumplimiento**.
3. En el cuadro de diálogo **Acerca de**, active la casilla **Activar registro**.
4. Utilice el agente soluble.
5. Busque los archivos del registro, que se encuentran en el directorio `<unidad>:\Sophos\SDA<número aleatorio>\Logs`.
6. Una vez solucionado el problema, vuelva ejecutar el agente soluble, vaya al cuadro de diálogo **Acerca de** del agente y desactive la opción **Activar registro**.

3.4 Cuadros de diálogo

A continuación se describen los diferentes cuadros de diálogo del agente soluble.

3.4.1 Cuadro de diálogo de solicitud de credenciales

El cuadro de diálogo de solicitud de credenciales aparece si se requiere autenticación a través de un proxy para que el agente soluble se comuniquen con el servidor NAC.

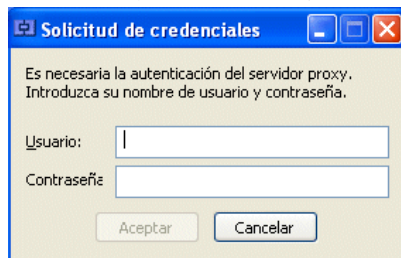


Figura 7: Cuadro de diálogo de solicitud de credenciales

3.4.2 Cuadro de diálogo de evolución

Este cuadro de diálogo se muestra mientras el agente está realizando alguna operación: obtener políticas, evaluar políticas, imponer políticas, remediar o crear informes. El cuadro de diálogo

de evolución muestra el estado, el progreso de las operaciones paso a paso y el progreso general de las operaciones.

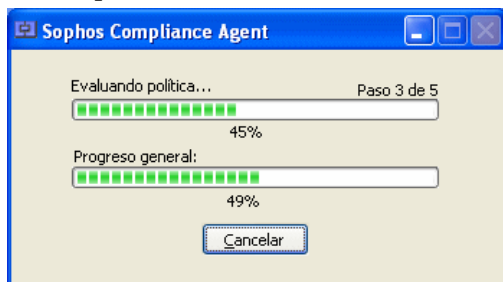


Figura 8: Cuadro de diálogo de evolución

3.4.3 Cuadro de diálogo de resultados

El cuadro de diálogo de resultados muestra los mensajes dirigidos al usuario según la política y mensajes de error.



Figura 9: Cuadro de diálogo de resultados

3.4.4 Cuadro de diálogo Acerca de

El cuadro de diálogo Acerca de muestra información sobre el agente, copyright y la opción Activar registro. El cuadro de diálogo Acerca de aparece al hacer clic en el icono de Sophos en el cuadro de diálogo de resultados.



Figura 10: Cuadro de diálogo Acerca de

4 Idiomas del agente

El agente está disponible inicialmente en los siguientes idiomas: inglés, francés, español, alemán, italiano, japonés, chino simplificado y chino tradicional.

Los mensajes del usuario se definen en los perfiles de NAC Manager. El agente muestra los mensajes del usuario en un idioma determinado sólo si están definidos.

Sophos recomienda crear un mensaje para un perfil en inglés (idioma predeterminado) para que, si no se puede mostrar en otro idioma, el usuario vea de todas formas un mensaje.

Para más información sobre la creación de mensajes de usuario, consulte la ayuda de NAC Manager.

5 Soporte técnico

Para soporte técnico, visite <http://esp.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

6 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.