DOCUMENTACIÓN TÉCNICA DE MACMON NAC

Integración de macmon NAC con Sophos Central

INTEGRACIÓN DE MACMON Y SOPHOS CENTRAL

Índice

Versión: 1.1_en

Introducción

Sophos evoluciona para hacer frente a los nuevos desafíos, protegiendo a más de 400.000 organizaciones de todos los tamaños, en más de 150 países, de las ciberamenazas más avanzadas de la actualidad. Impulsadas por SophosLabs, las soluciones en la nube y mejoradas por IA de Sophos, son capaces de adaptarse y evolucionar para proteger los equipos y las redes frente a las técnicas de cibercrimen nunca vistas anteriormente.

Casos prácticos

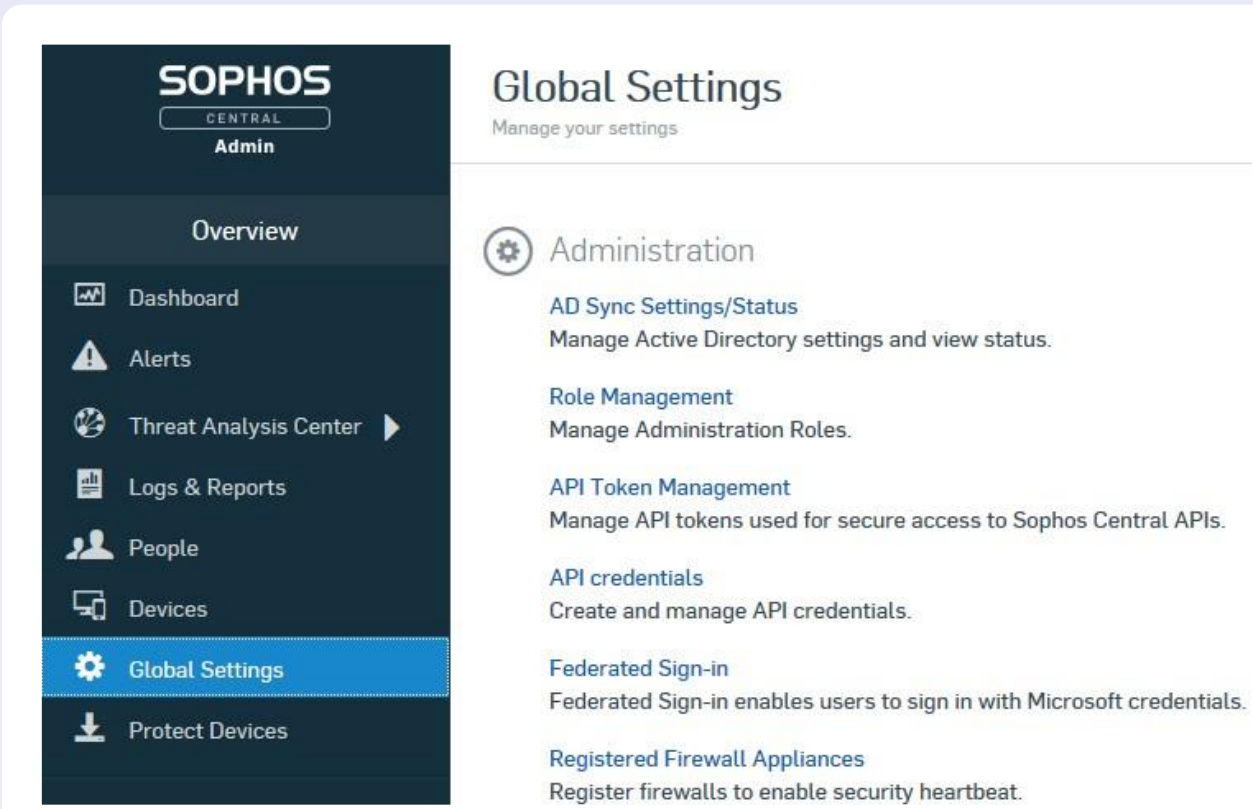
macmon reestablece el estado de salud de los terminales desde Sophos Central

El ransomware puede dificultar la vida de un administrador. Si un ransomware logra infectar algún equipo a pesar de todas las precauciones de seguridad, es importante aislar rápidamente ese dispositivo de la red, lo que evitará que el software malicioso se propague e infecte a otros recursos disponibles en la misma red. Sophos Intercept X es capaz de detectar una amenaza maliciosa en la red corporativa. La unión de Sophos Central y macmon NAC es una poderosa combinación para la detección de amenazas y el cumplimiento de la red.

macmon NAC permite que Sophos Central ejecute el estado de cumplimiento de un terminal en función de su estado de salud determinado por Sophos Intercept X, pudiendo esto aplicarse a casi todos los tipos redes existentes. En cualquier red se pueden encontrar dispositivos potencialmente sujetos a amenazas maliciosas. Cuando Sophos Intercept X detecta alguna anomalía en la red, clasifica el nivel de la amenaza en función de tres estados «bueno», «sospechoso» y «malo», y luego la transmite a Sophos Central. macmon NAC las analiza de manera periódica y pueden ser configuradas libremente en distintos estados de cumplimiento. Por ejemplo, si el estado de salud es «malo» se asigna al estado de cumplimiento «no conforme», y después una norma preestablecida podrá aislar el dispositivo infectado trasladándolo a la VLAN de reparación o apagando el puerto del conmutador de red.

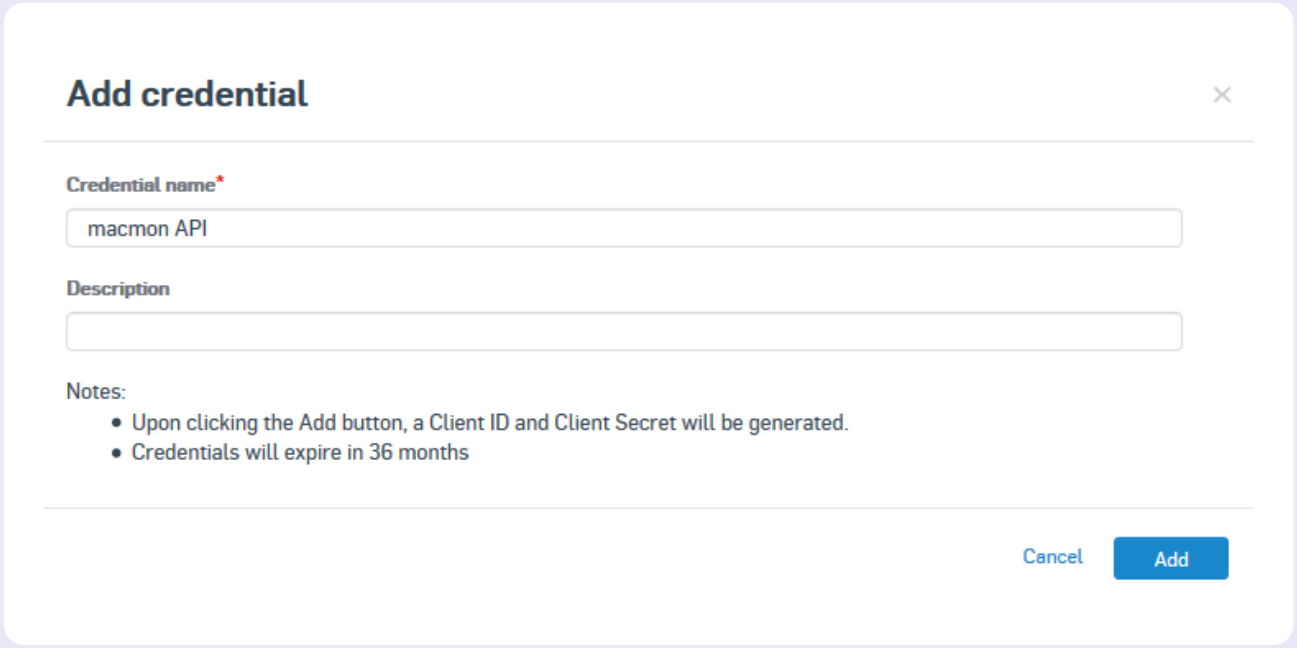
Configuración de Sophos Central

Para prepararlo, solo tendrá que crear credenciales de API. Haga click sobre «API credentials».

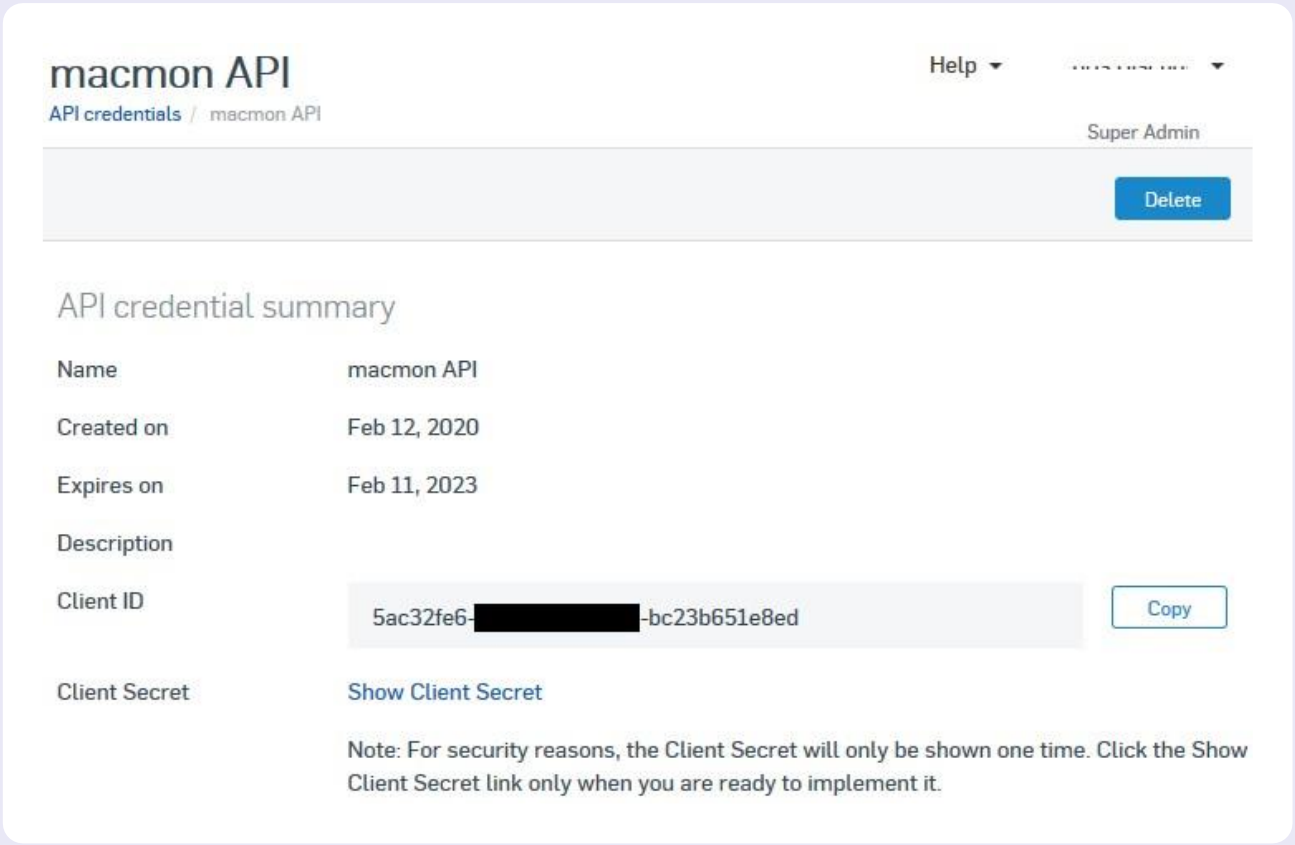


Haga click sobre «Add Credential».

Introduzca un nombre en el campo «Credential name» y confirme con «Add».



En «API credential summary» copie el «Client ID» y después haga click en el enlace «Show Client Secret» copie el «Client Secret» en sus documentos. Estas credenciales de acceso son necesarias para configurar la GUI de macmon.



Configuración de macmon NAC

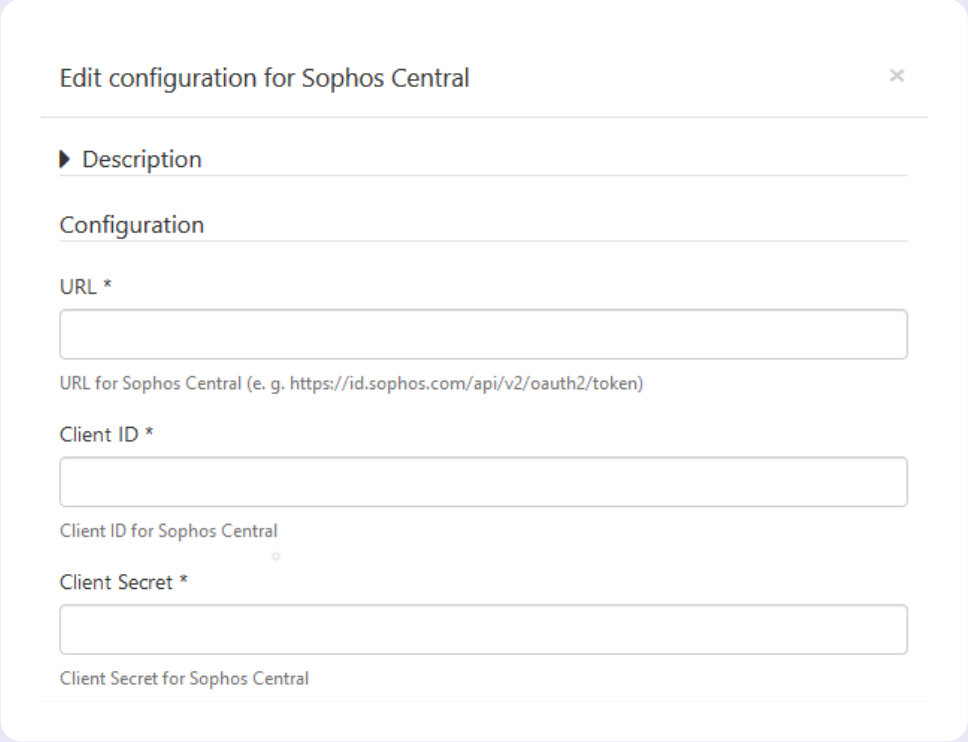
A continuación, se describe cómo configurar y activar esta integración. La activación crea una tarea en *Settings → Scheduled Tasks*, que se ejecutará en el intervalo configurado.

Se puede ver un resumen de todos los terminales consultados en *Reports → Endpoints → Client Compliance*. Ahí puede filtrarlos por fuente *Sophos Central*.

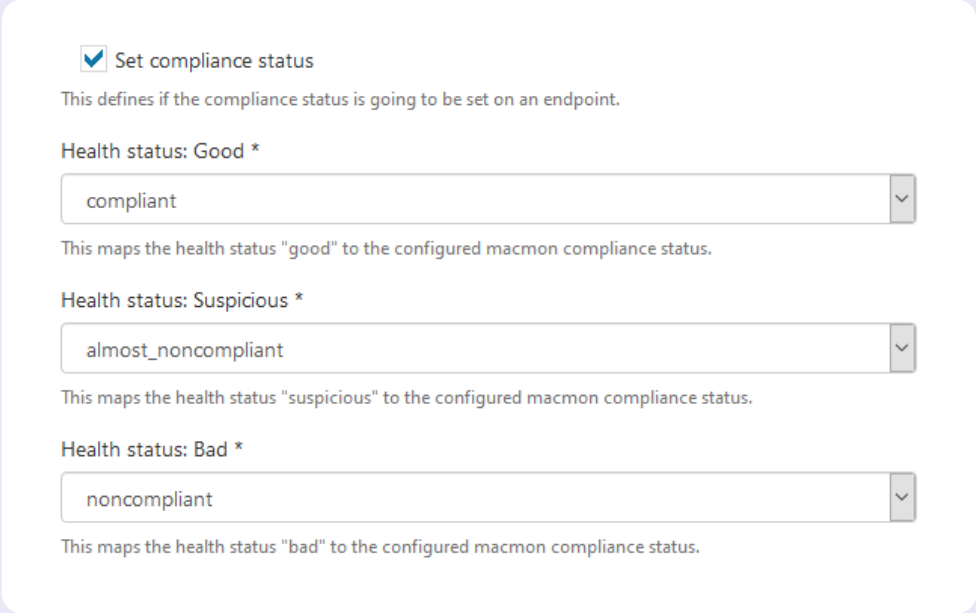
La configuración se realiza a través de la GUI de la web. Pinche sobre *Settings* y *Third party integrations*, y después sobre *Asset management*.

Si el borde del recuadro de *Sophos Central* aparece en gris, la integración aún no está activada. Pinche sobre el recuadro para que aparezca el diálogo de configuración.

1. Introduzca la *URL* necesaria para acceder a la API de Sophos Central e introduzca el *Client ID* y el *Client Secret*.



2. Verifique la casilla de cumplimiento si quiere configurar el estado de cumplimiento. Configure cuál de los diferentes estados del sistema debe asignarse en macmon. Esto afecta a la configuración del estado de cumplimiento en macmon.



3. Introduzca el intervalo en el que deban recuperarse los datos.

4. Finalice la activación pulsando sobre el botón *OK*.

Contacto

macmon secure GmbH
Alte Jakobstrasse 79-80 | 10179 Berlín
Tel.: +49 30 2325777-0 | nac@macmon.eu | www.macmon.eu