

DOCUMENTACIÓN TÉCNICA DE MACMON NAC

Integración de macmon NAC con Sophos Central

Índice

| | |
|--|---|
| Introducción | 3 |
| Casos prácticos..... | 3 |
| macmon reestablece el estado de salud de los terminales desde Sophos Central | 3 |
| Configuración de Sophos Central..... | 4 |
| Configuración de macmon NAC | 6 |

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 de 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.

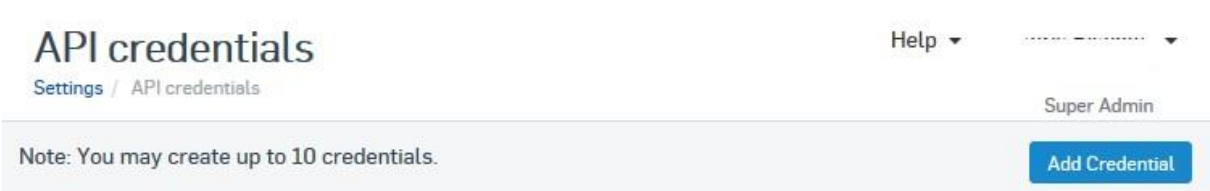
Configuración de Sophos Central

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



The screenshot shows the Sophos Central Admin interface. On the left is a dark sidebar with the 'SOPHOS CENTRAL Admin' logo at the top. Below the logo is an 'Overview' section with a list of menu items: Dashboard, Alerts, Threat Analysis Center, Logs & Reports, People, Devices, Global Settings (highlighted in blue), and Protect Devices. The main content area is titled 'Global Settings' with the subtitle 'Manage your settings'. Underneath, there is a section for 'Administration' with a gear icon. This section lists several options: 'AD Sync Settings/Status' (Manage Active Directory settings and view status), 'Role Management' (Manage Administration Roles), 'API Token Management' (Manage API tokens used for secure access to Sophos Central APIs), 'API credentials' (Create and manage API credentials), 'Federated Sign-in' (Federated Sign-in enables users to sign in with Microsoft credentials), and 'Registered Firewall Appliances' (Register firewalls to enable security heartbeat).

Haga click sobre «Add Credential».



The screenshot shows the 'API credentials' page. At the top left is the title 'API credentials' and below it the breadcrumb 'Settings / API credentials'. At the top right are 'Help' and a user profile dropdown showing 'Super Admin'. A light grey banner contains the text 'Note: You may create up to 10 credentials.' and a blue 'Add Credential' button.

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

Add credential ×

Credential name*

macmon API

Description

Notes:

- Upon clicking the Add button, a Client ID and Client Secret will be generated.
- Credentials will expire in 36 months

Cancel

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.

macmon API

API credentials / macmon API

Help ▾

macmon API ▾

Super Admin

Delete

API credential summary

Name macmon API

Created on Feb 12, 2020

Expires on Feb 11, 2023

Description

Client ID

5ac32fe6-██████████-bc23b651e8ed

Copy

Client Secret

[Show Client Secret](#)

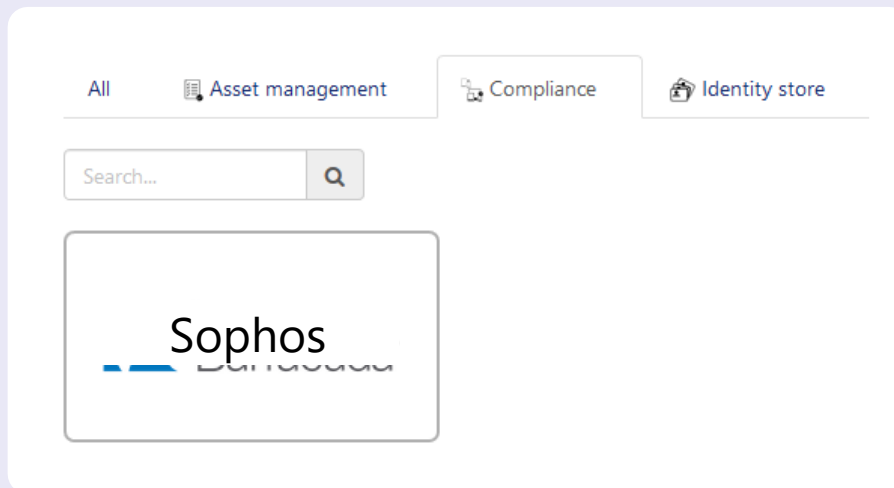
Note: For security reasons, the Client Secret will only be shown one time. Click the Show Client Secret link only when you are ready to implement it.

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.

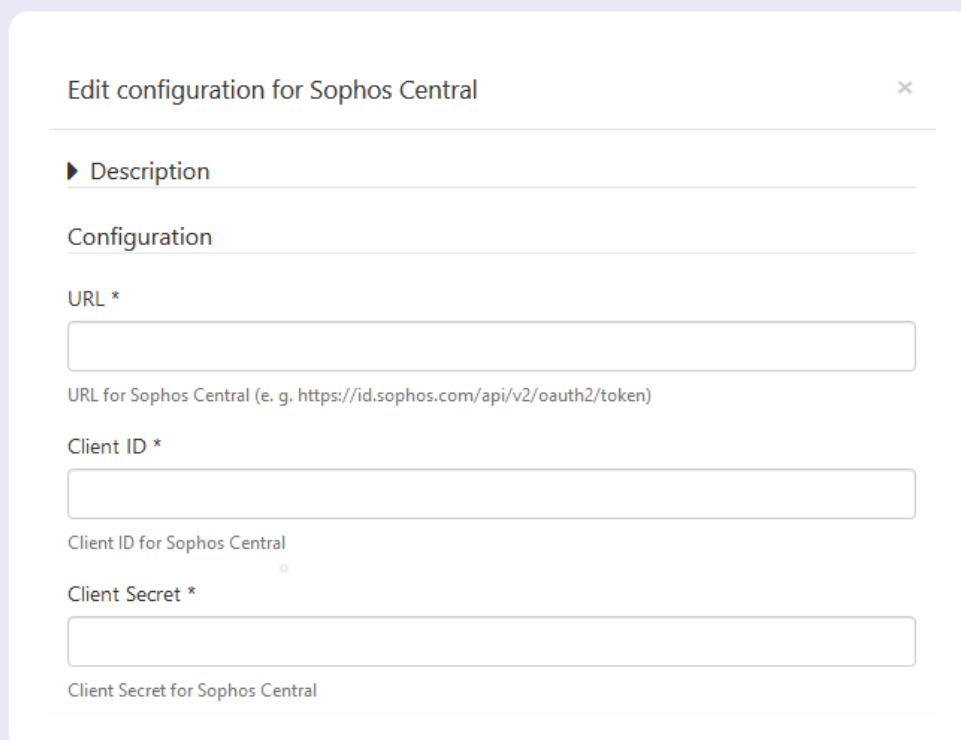
Se puede ver un resumen de todos los terminales consultados en *Reports* → *Endpoints* → *Client Compliance*. Ahí puede filtrarlos por fuente *Sophos Central*.

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*.

The image shows a screenshot of a dialog box titled 'Edit configuration for Sophos Central'. The dialog has a close button (X) in the top right corner. Below the title, there is a section labeled 'Description' with a right-pointing triangle icon. Underneath, there is a section labeled 'Configuration'. This section contains three input fields, each with a label and a description below it: 1. 'URL *' with a text input field and the description 'URL for Sophos Central (e. g. https://id.sophos.com/api/v2/oauth2/token)'. 2. 'Client ID *' with a text input field and the description 'Client ID for Sophos Central'. 3. 'Client Secret *' with a text input field and the description 'Client Secret for Sophos Central'.

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.

Set compliance status
This defines if the compliance status is going to be set on an endpoint.

Health status: Good *

compliant

This maps the health status "good" to the configured macmon compliance status.

Health status: Suspicious *

almost_noncompliant

This maps the health status "suspicious" to the configured macmon compliance status.

Health status: Bad *

noncompliant

This maps the health status "bad" to the configured macmon compliance status.

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

Interval *

Interval in minutes (range: 1-59) at which data is being retrieved from Sophos Central.

Active

Ok Cancel

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