



MACMON NAC WHITE PAPER

Integration of macmon NAC with Sophos Central

Contents

Introduction 3

Use Cases 3

 macmon retrieves endpoint health status from Sophos Central..... 3

Configuration of Sophos Central..... 4

Configuration of macmon NAC 6

Introduction

Sophos evolves to meet every new challenge, protecting more than 400,000 organizations of all sizes in more than 150 countries from today's most advanced cyber threats. Powered by SophosLabs, cloud-native and AI-enhanced solutions from Sophos are able to adapt and evolve to secure endpoints and networks against never-before-seen cybercriminal tactics and techniques.

Use Cases

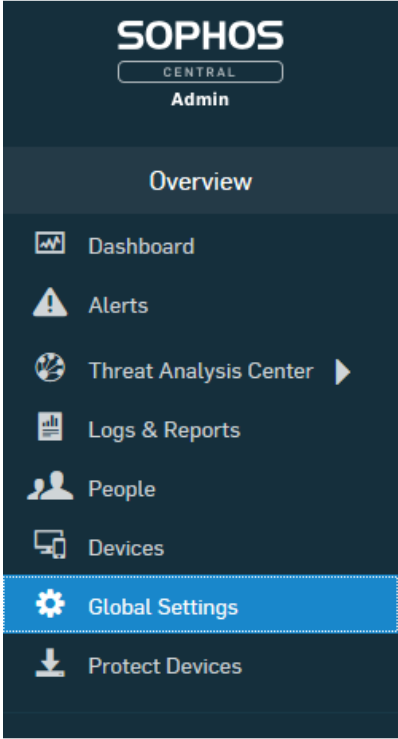
macmon retrieves endpoint health status from Sophos Central

Ransomware can make an administrator's life hard. If a ransomware managed to infect an endpoint despite all security precautions, it's important to isolate this exact device from the network segment quickly. This prevents the malicious software from spreading over and infecting other resources available on the network. Sophos Intercept X is capable of detecting a malicious threat in the corporate network. The combination of Sophos Central and macmon NAC is a powerful combination of threat detection and network enforcement.

macmon NAC enables Sophos Central to enforce the compliance status of an endpoint based on its health status determined by Sophos Intercept X. This applies to virtually any network you can imagine. In any network you can find devices that potentially are subject to malicious threats. When Sophos Intercept X detects such in your network it classifies the threat level into the three states "good", "suspicious" and "bad" which is then passed on to Sophos Central. These are periodically analyzed by macmon NAC and they can be freely configured to different compliance states. For example, if the health status "bad" is assigned to the compliance status "noncompliant", a pre-set rule then would either isolate the infected device by moving it into remediation VLAN or by physically shutting down the network switch port.

Configuration of Sophos Central

For preparation, you only need to create API credentials. Click on "API credentials".



The screenshot shows the Sophos Central Admin interface. On the left is a dark sidebar with the 'SOPHOS CENTRAL Admin' header and a menu including Overview, Dashboard, Alerts, Threat Analysis Center, Logs & Reports, People, Devices, Global Settings (highlighted), and Protect Devices. The main content area is titled 'Global Settings' with the subtitle 'Manage your settings'. Under the 'Administration' section, there are links for AD Sync Settings/Status, Role Management, API Token Management, API credentials, Federated Sign-in, and Registered Firewall Appliances, each with a brief description of its function.


SOPHOS CENTRAL Admin

Global Settings
Manage your settings

Administration

- [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.
- [Registered Firewall Appliances](#)
Register firewalls to enable security heartbeat.

Click on „Add Credential“.



The screenshot shows the 'API credentials' page in the Sophos Central Admin interface. It includes a breadcrumb trail 'Settings / API credentials', a 'Help' dropdown, and a 'Super Admin' user indicator. A note states 'You may create up to 10 credentials.' and there is a prominent blue 'Add Credential' button.

API credentials

Settings / API credentials

Help ▾ Super Admin

Note: You may create up to 10 credentials.

[Add Credential](#)

Assign any name in the "Credential name" field and confirm with "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

In the "API credential summary" copy the "Client ID" and after clicking the link "Show Client Secret" copy the "Client Secret" into your documents. These access credentials are needed for the setup in the macmon GUI.

macmon API

Help ▾

macmon API ▾

API credentials / 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-[REDACTED]-bc23b651e8ed

Copy

Client Secret

[Show Client Secret](#)

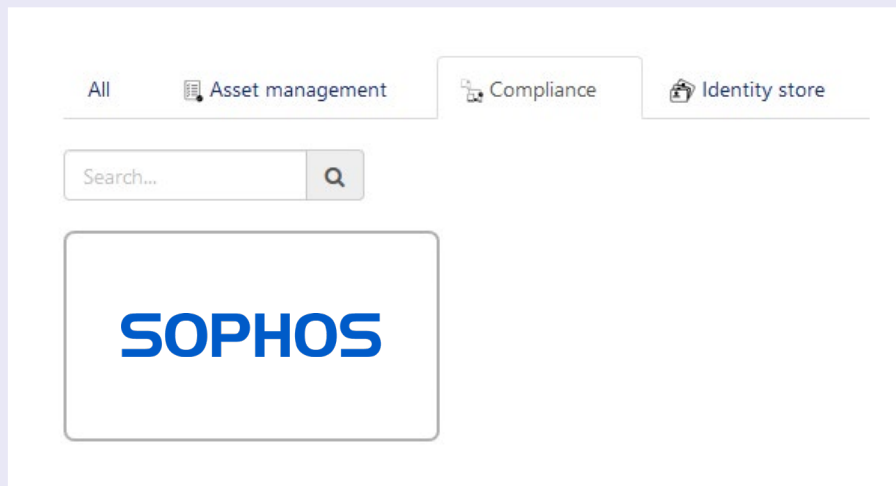
Note: For security reasons, the Client Secret will only be shown one time. Click the Show Client Secret link only when you are ready to implement it.

Configuration of macmon NAC

The following describes how to configure and activate this integration. Activation creates a task in *Settings* → *Scheduled Tasks* that is executed at the configured interval.

An overview of all queried endpoints can be viewed under *Reports* → *Endpoints* → *Client Compliance*. You can filter by source *Sophos Central* there.

The configuration is done via the web GUI. Please tap on *Settings* and *Third party integrations*, then on *Asset management*.



If the border of the *Sophos Central* tile appears gray the integration is not yet activated. Please tap on the tile for the configuration dialog to be shown.

1. Enter the *URL* that is required to access the Sophos Central API Also enter the *Client ID* and *Client Secret*.

A screenshot of a configuration dialog box titled 'Edit configuration for Sophos Central' with a close button (X) in the top right corner. The dialog has a section header 'Description' followed by a 'Configuration' section. Under 'Configuration', there are three input fields: 'URL *', 'Client ID *', and 'Client Secret *'. Below each input field is a small text label: 'URL for Sophos Central (e. g. https://id.sophos.com/api/v2/oauth2/token)' under the URL field, 'Client ID for Sophos Central' under the Client ID field, and 'Client Secret for Sophos Central' under the Client Secret field.

2. Check the Compliance box if you want to set the compliance status. Configure which of the different system states should be mapped in macmon like. This affects the setting of the compliance status in 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. Enter the interval at which data should be retrieved.

Interval *

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

☐ Active

4. Please finish the activation by tapping on the *Ok* button.

Contact

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