SOPHOS

macmon
nac intelligent einfach

MACMON NAC WHITEPAPER

Integration von macmon NAC mit Sophos Central

Inhaltsverzeichnis

Version: 1.1_de

Einleitung

Sophos schützt über 400.000 Organisationen in mehr als 150 Ländern vor modernen Cyberbedrohungen. Unterstützt durch das Expertenwissen der SophosLabs sind die cloud-nativen und KI-optimierten Lösungen von Sophos in der Lage, sich jederzeit an die Änderungen der Bedrohungslandschaft anzupassen. So können sie Endpoints und Netzwerke selbst vor noch komplett unbekannten Taktiken und Techniken von Cyberkriminellen schützen.

Anwendungsfälle

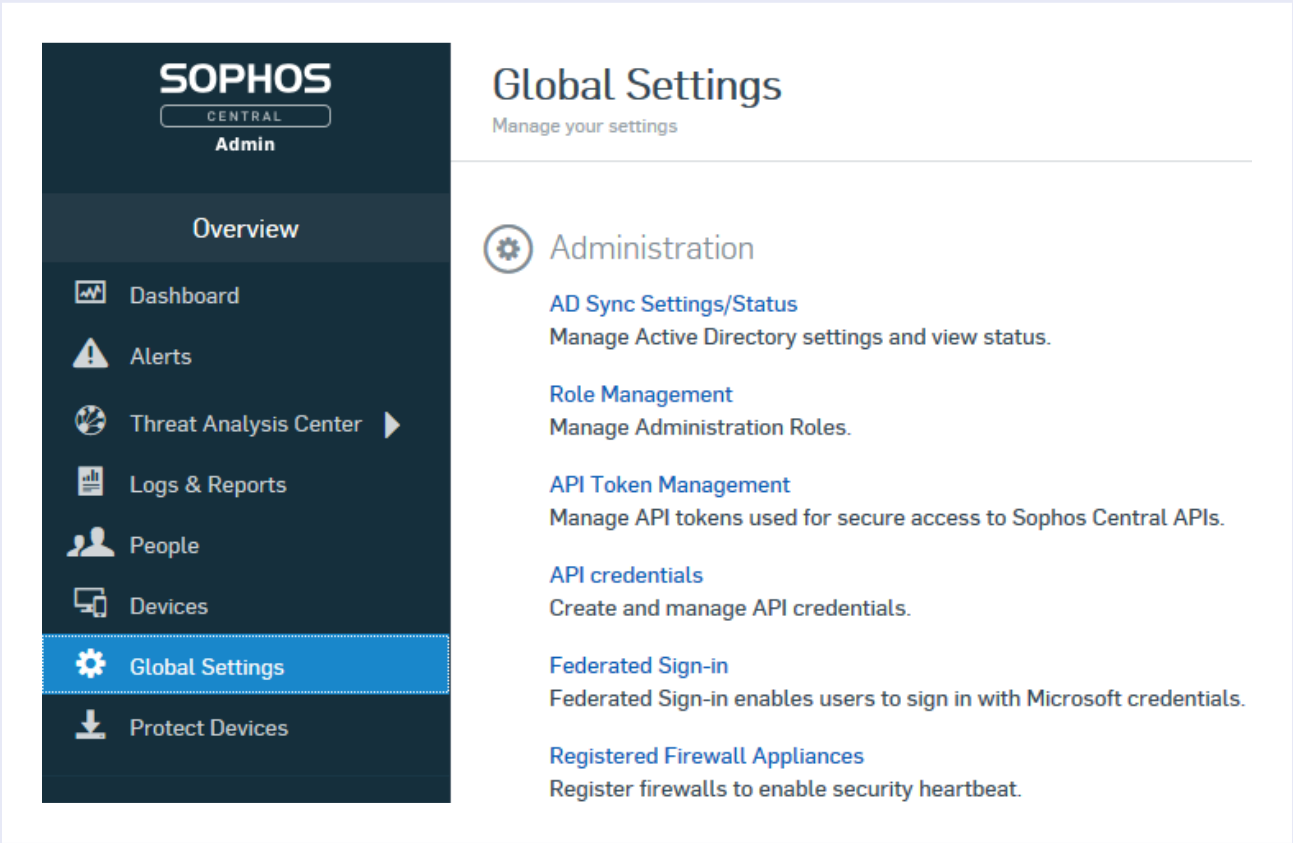
macmon ruft bei Sophos Central die Systemzustände von Endgeräten ab

Viren und Schadsoftware können das Leben eines Administrators hart machen. Wenn eine solche schädliche Software trotz aller Vorsichtsmaßnahmen ein Endgerät infiziert, muss die Isolierung dieses Endgeräts aus dem Netzwerksegment so schnell wie möglich erfolgen. Dadurch wird verhindert, dass sich eine Schadsoftware über das Netzwerk verbreitet und andere im Netzwerk befindlichen Ressourcen infiziert. Sophos Intercept X ist in der Lage, eine solche Bedrohung schnell zu erkennen. In Sophos Central wird der Systemzustand eines jeden Endgeräts im Unternehmensnetzwerk festgehalten und für macmon NAC bereitgestellt. Die Kombination aus Sophos Central und macmon NAC ist eine leistungsstarke Kombination aus Erkennung von Bedrohungen und Isolation von betroffenen Endgeräten.

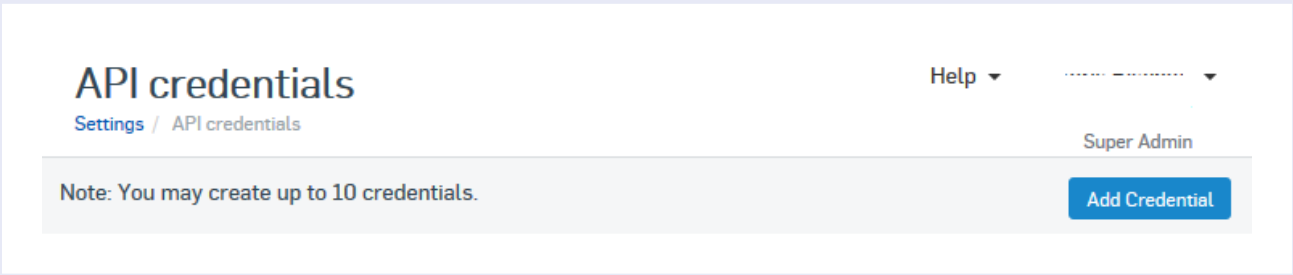
Durch die bereitgestellten Informationen kann macmon NAC den Compliance-Status eines Endgeräts basierend auf dem von Sophos Intercept X festgestellten Systemstatus erzwingen. Dies gilt für Netzwerke jeglicher Größe, denn in jedem Netzwerk finden Sie Geräte, die möglicherweise Bedrohungen ausgesetzt sind. Wenn Sophos Intercept X eine solche in Ihrem Netzwerk erkennt, klassifiziert sie die Bedrohungslage in die drei Zustände „gut", „verdächtig" und „schlecht" und übermittelt diese an Sophos Central. Diese werden von macmon NAC regelmäßig ausgewertet und konfigurierbar verschiedenen Compliance-Status zugeordnet. Wird der Systemzustand „schlecht" beispielsweise dem Compliance-Status „noncompliant" zugeordnet, so sorgt eine voreingestellte Regel für die Isolation eines Endgeräts, indem es ins Remediation-VLAN verschoben oder der Netzwerkanschluss am Switch abgeschaltet wird.

Konfiguration von Sophos Central

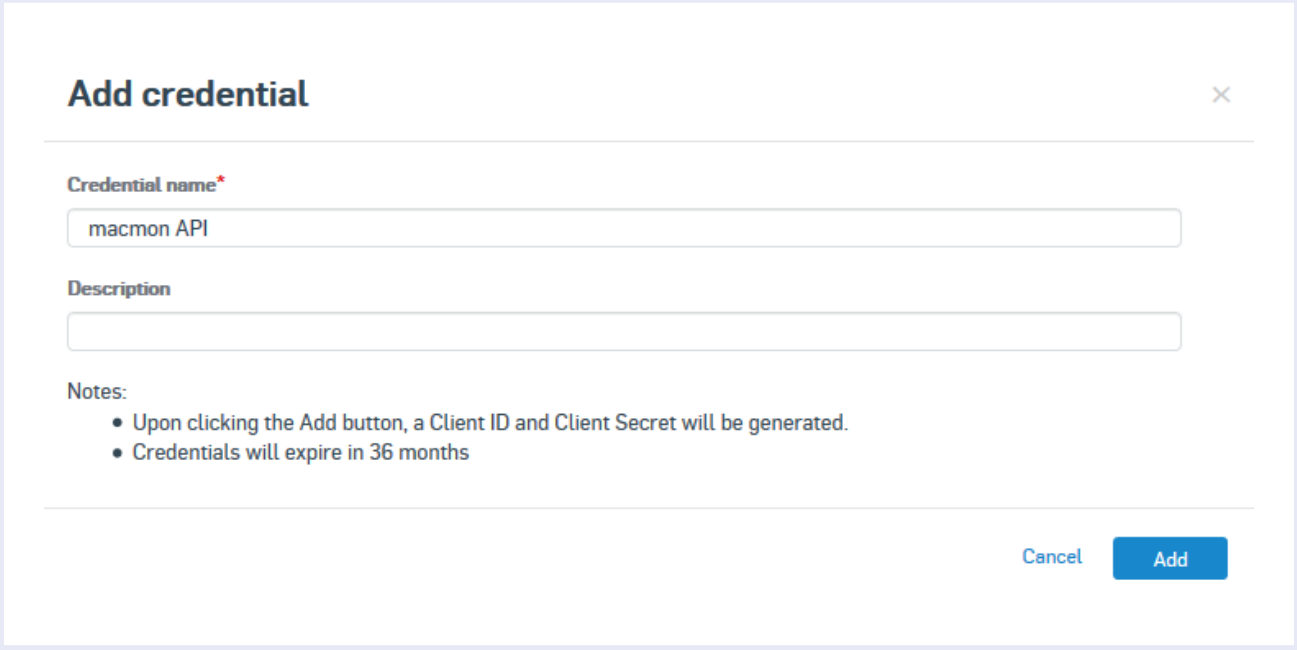
Zur Vorbereitung müssen lediglich API-Credentials angelegt werden. Klicken Sie auf „API credentials“.



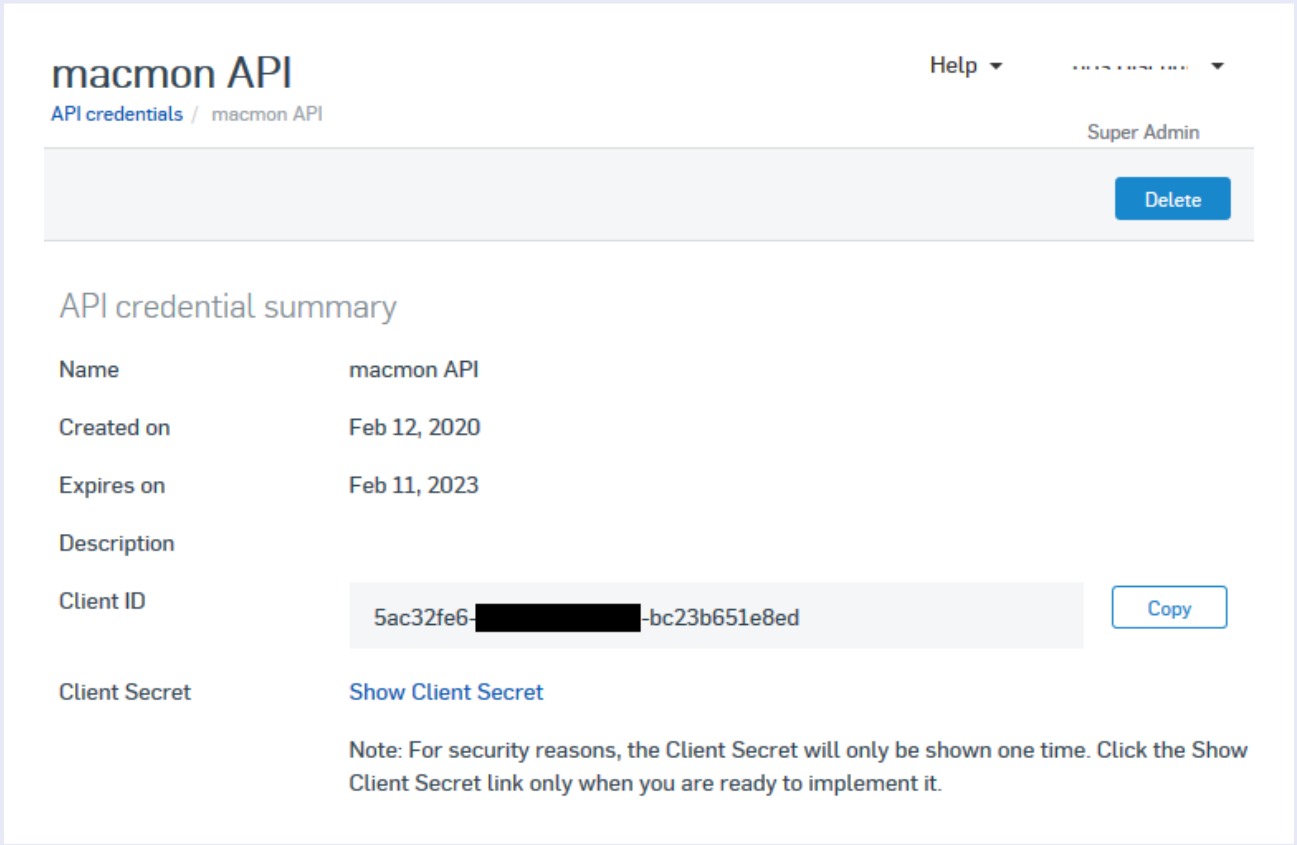
Klicken Sie auf „Add Credential“.



Vergeben Sie einen beliebigen Namen im Feld „Credential name“ und bestätigen Sie mit „Add“.



Im „API credential summary“ kopieren Sie die „Client ID“ und nach Betätigen des Links „Show Client Secret“ das „Client Secret“ in Ihre Unterlagen. Diese beiden Informationen werden zur Einrichtung in der macmon-GUI benötigt.

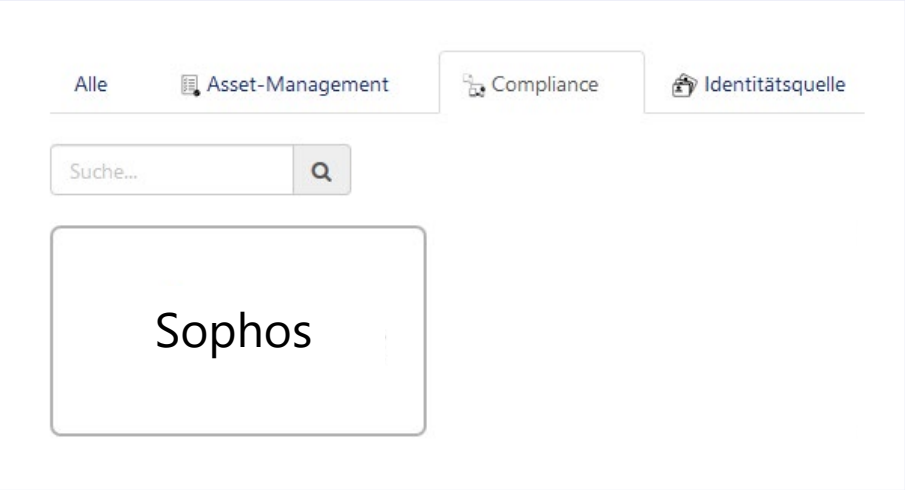


Konfiguration von macmon NAC

Im Folgenden wird beschrieben, wie die vorliegende Integration konfiguriert und aktiviert wird. Mit der Aktivierung wird ein Task in *Einstellungen → Geplante Tasks* angelegt, der im konfigurierten Intervall ausgeführt wird.

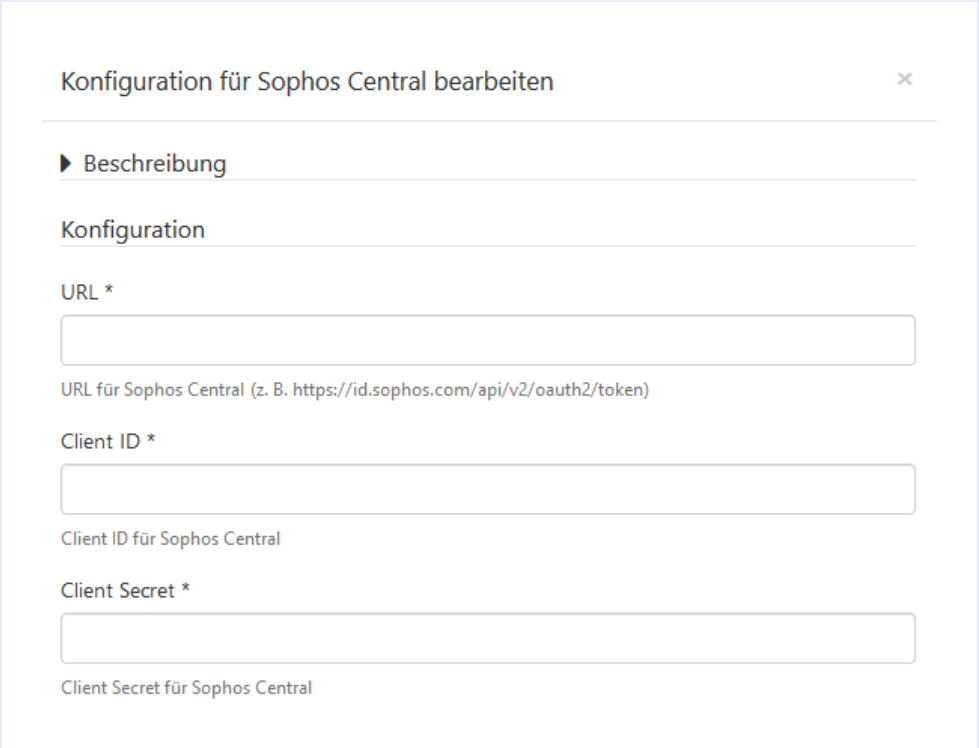
Eine Übersicht über alle abgefragten Endgeräte können Sie unter *Berichte → Endgeräte → Client Compliance* einsehen. Sie können dort nach der Quelle *Sophos Central* filtern.

Die Konfiguration wird über die Web-GUI vorgenommen. Wählen Sie dazu bitte *Einstellungen* und *Drittanbieter-Integrationen*, danach den Tab *Compliance*.



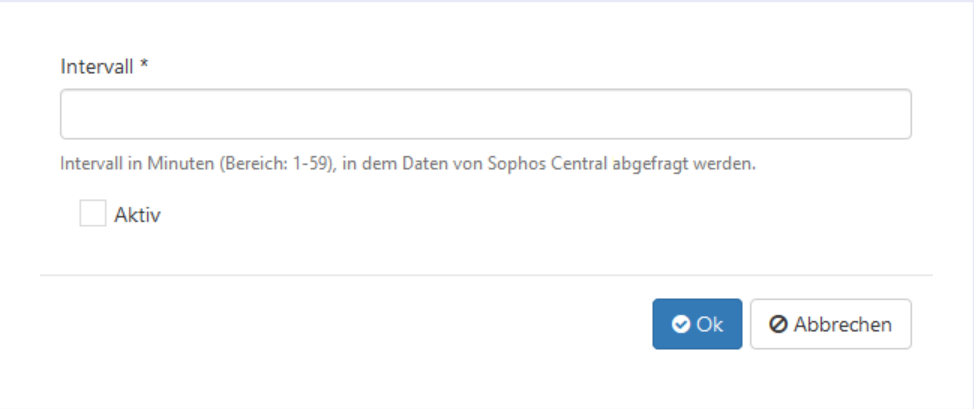
Wenn der Rahmen der *Sophos Central*-Kachel grau erscheint, ist die Integration noch nicht aktiviert. Bitte drücken Sie auf die Kachel, um den Konfigurationsdialog aufzurufen.

1. Geben Sie die *URL* ein, die notwendig ist, um die API von *Sophos Central* aufzurufen. Geben Sie außerdem die *Client ID* und das *Client Secret* ein.



2. Setzen Sie den Haken bei Compliance, wenn der Compliance-Status gesetzt werden soll. Konfigurieren Sie, die wie die verschiedenen Systemzustände in macmon abgebildet werden sollen. Dies hat Auswirkungen auf das Setzen des Compliance-Status in macmon.

3. Geben Sie das Intervall ein, in dem Daten abgerufen werden sollen.



4. Schließen Sie die Aktivierung ab, indem Sie den Knopf *Ok* betätigen.

Kontakt

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