



MACMON NAC WHITEPAPER

Integration von macmon NAC mit Check Point Identity Awareness

Inhaltsverzeichnis

Einleitung	3
Anwendungsfälle	3
Neues Endgerät wird an Check Point Identity Awareness übertragen.....	3
Trennung eines Endgeräts vom Unternehmensnetzwerk beendet die Sitzung in Check Point Identity Awareness.....	3
Änderung von Endgeräteinformationen modifiziert die Sitzung in Check Point Identity Awareness.....	3
Verlängerung von Sitzungen in Check Point Identity Awareness	3
Konfiguration von Check Point Identity Awareness	4
Konfiguration von macmon NAC	8
Kontakt bei Check Point.....	11

Einleitung

Check Point Software Technologies GmbH ist ein führender Anbieter von Cybersicherheits-Lösungen für öffentliche Verwaltungen und Unternehmen weltweit. Die Lösungen schützen Kunden vor Cyberattacken mit einer branchenführenden Erkennungsrate von Malware, Ransomware und anderen Arten von Attacken. Check Point bietet eine mehrstufige Sicherheitsarchitektur, die Unternehmensinformationen in CloudUmgebungen, Netzwerken und auf mobilen Geräten schützt sowie das umfassendste und intuitivste „One Point of Control“-Sicherheits-Managementsystem. Check Point schützt über 100.000 Unternehmen aller Größen.

Anwendungsfälle

In der Integration von Check Point Identity Awareness und macmon stellt macmon viele endgerätespezifische Informationen zur Verfügung, die den Datenbestand von Identity Awareness ergänzen. Dies erleichtert es Netzwerkadministratoren enorm, gruppenbasierte Richtlinien für Zugriffsmöglichkeiten von Endgeräten innerhalb des Unternehmensnetzwerks umzusetzen. In sogenannten Sitzungen verwaltet Check Point Identity Awareness Informationen zu jedem Endgerät im Unternehmensnetzwerk, aus denen sich eine Zuordnung in verschiedene konfigurierte Policies in Identity Awareness ergeben. So leiten sich dann beispielsweise Zugriffsrechte für ein Endgerät ab.

Neues Endgerät wird an Check Point Identity Awareness übertragen

Wenn die IT-Abteilung eines Unternehmens ein neues Endgerät beschafft und dieses in Betrieb genommen wird oder wenn ein Endgerät morgens eingeschaltet wird, erkennt macmon das umgehend. Damit die Sitzung für dieses Endgerät auch in Check Point Identity Awareness gestartet werden kann, überträgt macmon detaillierte Informationen zu diesem Endgerät, startet die Sitzung und nimmt dem Netzwerkadministrator damit eine doppelte Datenführung ab.

Trennung eines Endgeräts vom Unternehmensnetzwerk beendet die Sitzung in Check Point Identity Awareness

Am Ende eines Tages werden Endgeräte abgeschaltet oder im Falle von Notebooks sogar für längere Zeit vom Unternehmensnetzwerk getrennt. macmon überträgt die Trennung eines Endgeräts vom Unternehmensnetzwerk an Check Point Identity Awareness und stoppt so die zuvor gestartete Sitzung. Die Sitzungsinformationen werden somit auch in diesem Fall von Identity Awareness effektiv nachgeführt.

Änderung von Endgeräteinformationen modifiziert die Sitzung in Check Point Identity Awareness

Ein Umzug innerhalb des Unternehmensgebäudes oder ein Abteilungswechsel zieht oft auch die Änderung der IP-Adresse eines Endgeräts mit sich. Damit die Firewall-Regeln und die damit verbundenen Firewall-Entscheidungen dennoch weiterhin richtig greifen und die korrekten IP-Adressen berücksichtigt werden, überträgt macmon eine solche Änderung umgehend an Identity Awareness, um die dort laufende Sitzung und deren Informationen zu aktualisieren.

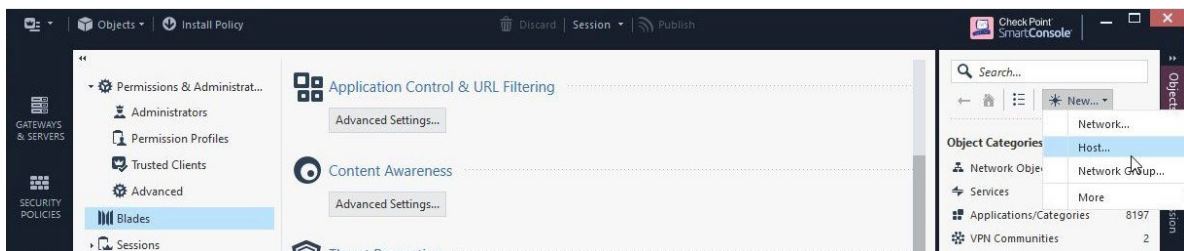
Verlängerung von Sitzungen in Check Point Identity Awareness

Endgeräte wie Telefone sind für deren Betrieb immer eingeschaltet und im Unternehmensnetzwerk aktiv. macmon stellt dabei stets sicher, dass die Sitzung in Check Point Identity Awareness auf dem aktuellen Stand ist und weiterläuft, um einen optimalen Schutz und Überblick zu gewährleisten.

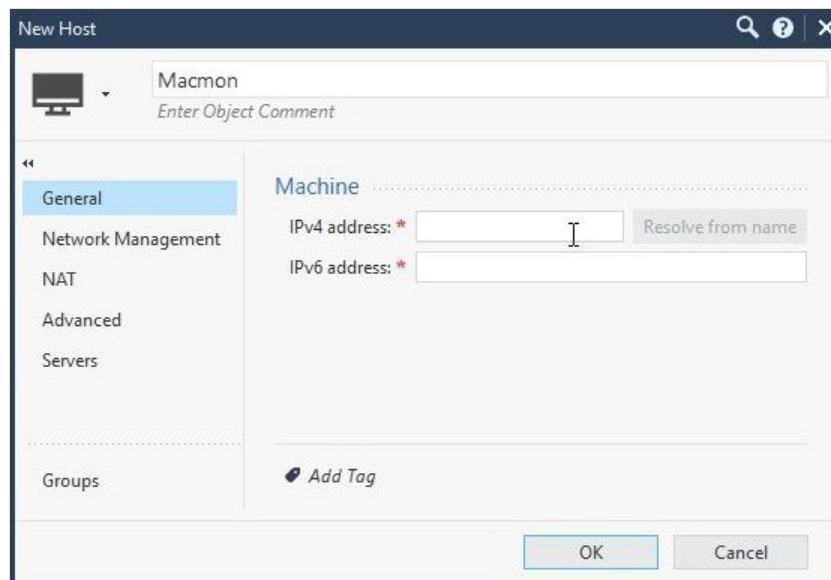
Konfiguration von Check Point Identity Awareness

Die nachfolgenden Schritte führen durch die Konfiguration von Check Point Identity Awareness. Sie ist nötig, um das Client Secret zu erzeugen, das Sie für die Konfiguration der Integration in der GUI von macmon benötigen werden.

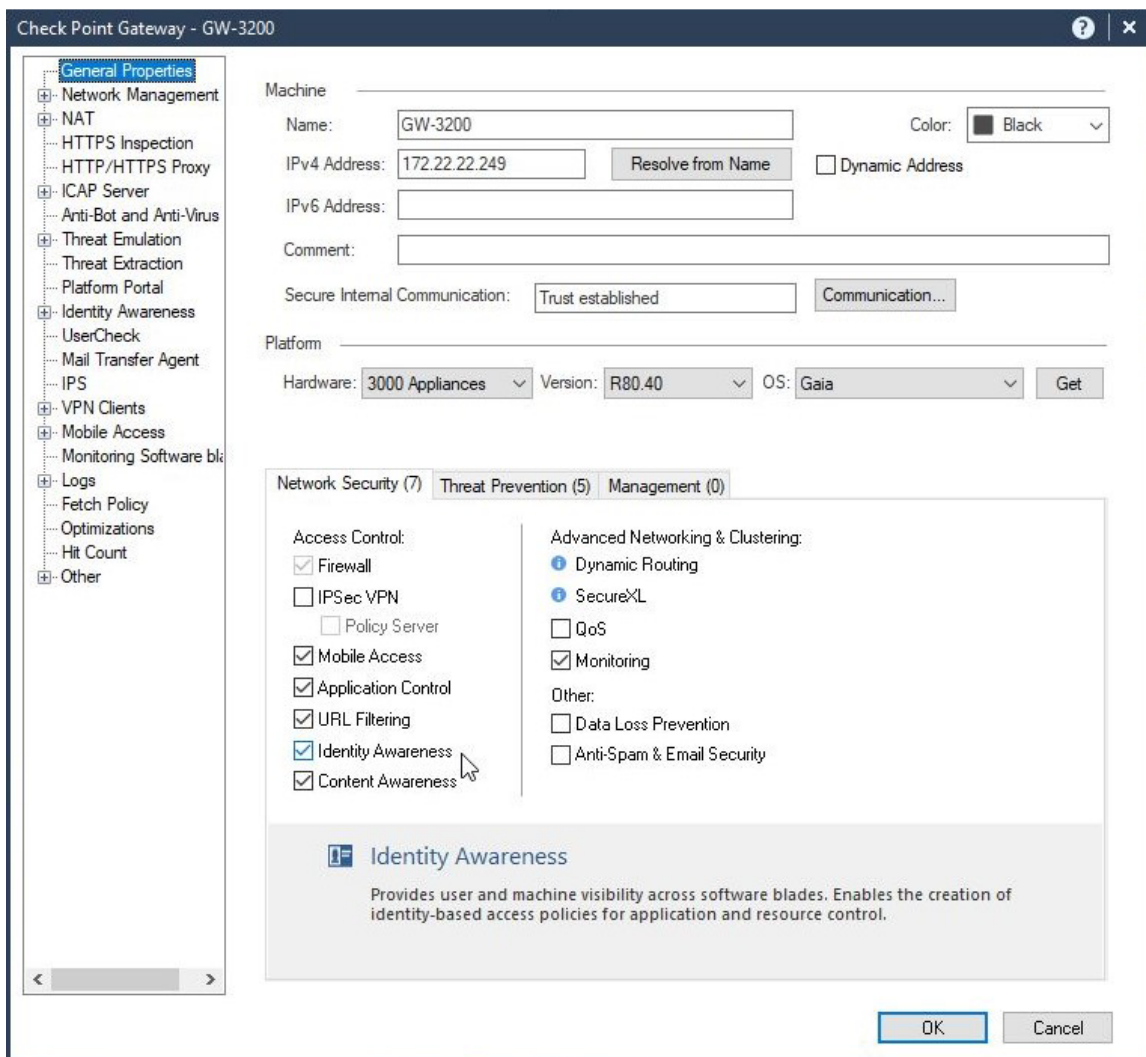
1. Wenn Sie noch keinen Host für Ihre macmon-Installation angelegt haben, wählen Sie in der *Check Point SmartConsole* im rechten Bereich der Console *New* und *Host*.



2. Wählen Sie einen Namen wie beispielsweise *macmon* und geben Sie sowohl die *IPv4*- und/oder die *IPv6*-Adresse Ihrer macmon-Installation an.



3. Ab diesem Schritt erfolgt die Konfiguration des *Check Point Gateway*. Im Bereich *General Properties* und dort im Tab *Network Security* aktivieren Sie das *Identity Awareness*-Blade durch Setzen des Hakens. Den erscheinenden Wizard können Sie gerne an dieser Stelle abbrechen.



Check Point Gateway - GW-3200

General Properties

- Network Management
- NAT
- HTTPS Inspection
- HTTP/HTTPS Proxy
- ICAP Server
- Anti-Bot and Anti-Virus
- Threat Emulation
- Threat Extraction
- Platform Portal
- Identity Awareness
- UserCheck
- Mail Transfer Agent
- IPS
- VPN Clients
- Mobile Access
- Monitoring Software blades
- Logs
- Fetch Policy
- Optimizations
- Hit Count
- Other

Machine

Name: Color:

IPv4 Address: ☐ Dynamic Address

IPv6 Address:

Comment:

Secure Internal Communication:

Platform

Hardware: Version: OS:

Network Security (7) Threat Prevention (5) Management (0)

Access Control:

- ☒ Firewall
- ☐ IPSec VPN
 - ☐ Policy Server
- ☒ Mobile Access
- ☒ Application Control
- ☒ URL Filtering
- ☒ Identity Awareness
- ☒ Content Awareness

Advanced Networking & Clustering:

- ☒ Dynamic Routing
- ☒ SecureXL
- ☐ QoS
- ☒ Monitoring

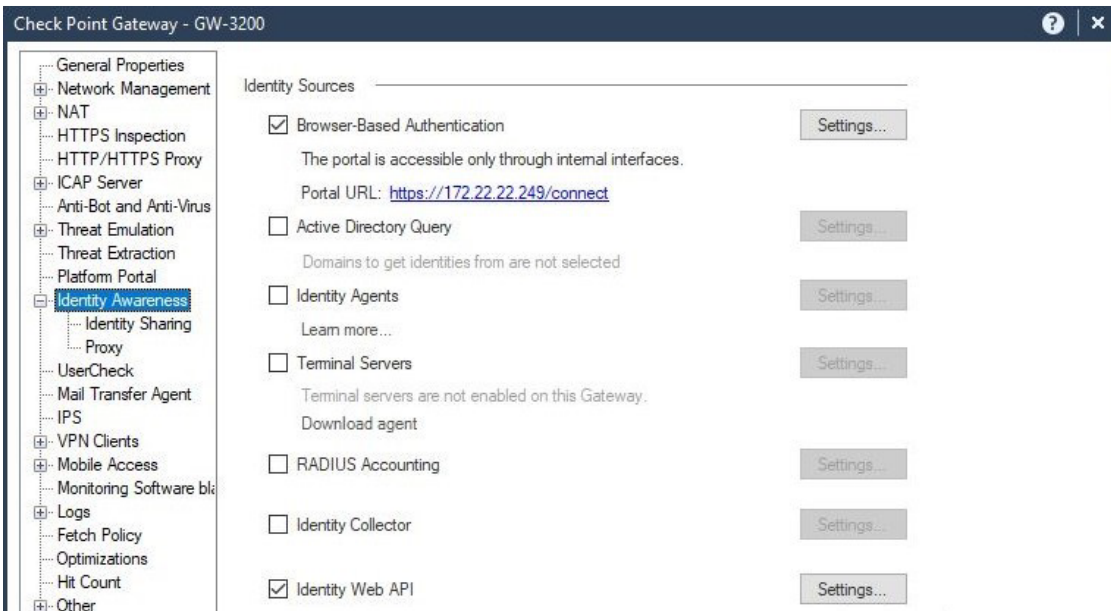
Other:

- ☐ Data Loss Prevention
- ☐ Anti-Spam & Email Security

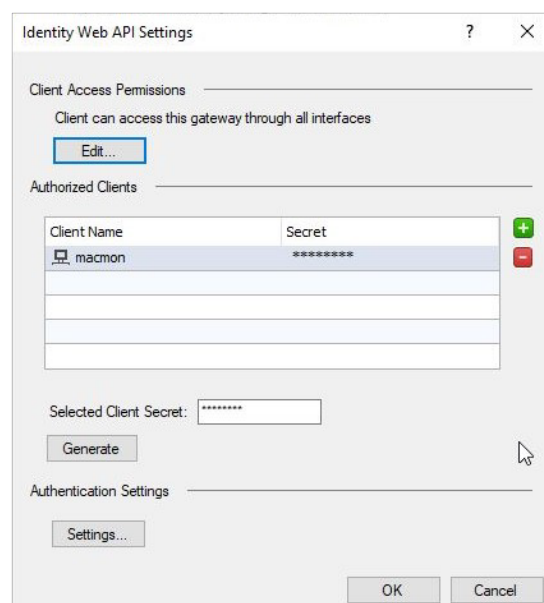
Identity Awareness

Provides user and machine visibility across software blades. Enables the creation of identity-based access policies for application and resource control.

- Wählen Sie den Bereich *Identity Awareness* und setzen Sie dort im Bereich *Identity Sources* den Haken bei *Identity Web API*. Klicken Sie dort auf die Schaltfläche *Settings*.



- Klicken Sie im neuen Dialogfenster im Bereich Client Access Permissions auf die Schaltfläche *Edit*. Wählen Sie dort die Interfaces, über die Check Point Identity Awareness erreichbar sein soll. Fügen Sie durch Klick auf das grüne Plus-Zeichen den in Schritt 1 angelegten Host als *authorized client* hinzu. Notieren Sie sich das Client Secret. Dieses wird in der Konfiguration der Integration in der macmon-GUI benötigt. Schließen Sie die Konfiguration mit Klick auf *OK* ab.



6. Aktivieren Sie die veränderte Konfiguration durch einen Klick auf *Publish*.

Im Bereich *Logs & Monitor* finden Sie verschiedene Login-Ereignisse. Wählen Sie dazu das Blade *Identity Awareness* aus.

Log Details

Log In

Successful Login: Machine Identity Propagation

Details

Device

Host Type

CHECK POINT SOFTWARE TECHNOLOGIES

Endpoint IP

172.23.23.249

Session

Session ID

8b9b7ca8

Authentication Method

Machine Identity Propagation

Identity

Authentication Status

Successful Login

Identity Source

Identity Awareness API (macmon Check Point Identity Awareness integration)

Roles

test-ida

Actions

Report Log

Report Log to Check Point

More

Id

ac1616f9-b607-eb6d-5e9d-3a7800000000

Sequencenum

5

Type

Log

Origin

GW-3200

Logid

131073

Marker

@A@@B@1587333602@C@203109

Log Server Origin

cp-mgmt (172.22.22.81)

Orig Log Server Ip

172.22.22.81

Index Time

2020-04-20T06:00:25Z

Lastupdateatime

1587362424000

Lastupdateatime

5

Stored

true

Severity

Informational

Rounded Sent Bytes

0

Confidence Level

N/A

Rounded Bytes

0

Rounded Received Bytes

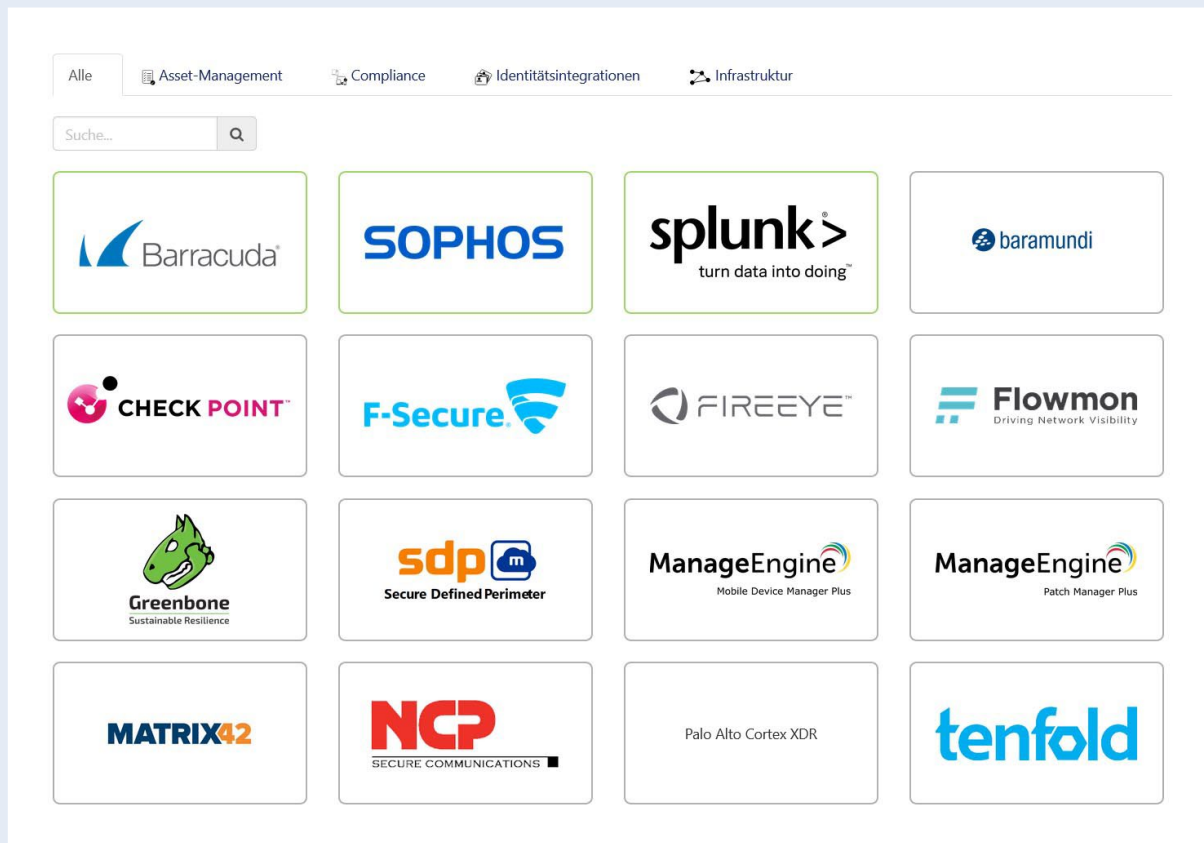
0

Description

Successful Login: Machine Identity Propagation

Konfiguration von macmon NAC

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



Wenn der Rahmen der *Check Point Identity Awareness*-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 *Check Point Identity Awareness* aufzurufen. Geben Sie ebenfalls die *Fallback-URL* an, die verwendet wird, wenn die API, die im Feld *URL* angegeben wurde, nicht antwortet.

Konfiguration für Check Point Identity Awareness bearbeiten

Beschreibung

Konfiguration

URL *

URL zur Check Point identity Awareness API (z. B. 'https://172.23.27.96/_IA_API/v1.0' oder 'https://172.23.27.96/_IA_MU_Agent/idasdk' für Version R77.30)

Fallback-URL

URL welche verwendet wird, wenn die Anfrage zur Original-URL fehlschlägt (z. B. 'https://172.23.27.97/_IA_API/v1.0')

2. Geben Sie das *Shared secret* ein, das zur Authentifizierung mit dem System verwendet wird. Im Feld *Wiederholungen* geben Sie an, wie oft macmon erneute Verbindungsversuche unternehmen soll, wenn vorhergehende Versuche gescheitert sind.

Shared secret *

Shared secret, welches für die Authentifizierung verwendet wird

Wiederholungen

Wiederholungen, wenn die API-Anfrage für alle URLs fehlgeschlägt

3. Geben Sie das *Session-Timeout* ein, das angibt, nach welchem Zeitraum macmon die Verbindung mit Check Point Identity Awareness als abgelaufen erachten soll. Bitte beachten Sie, dass dieser Wert in Sekunden angegeben wird. Setzen Sie einen Haken bei *Inaktive Endgeräte berücksichtigen*, wenn inaktive Endgeräte beachtet werden sollen. Setzen Sie zum Schluss den Haken bei *Aktiv*, um die Integration zu aktivieren.

Session-Timeout in Sekunden (Standard ist 30 Tage)

2592000

Timeout der Sessions in Sekunden für die Identity Awareness-Zuweisung (min. 300 Sekunden)

☒ Inaktive Endgeräte berücksichtigen

Gibt an, ob inaktive Endgeräte mit einbezogen werden sollen oder nicht

☐ Aktiv

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

Kontakt bei Check Point

Hier finden Sie den Identity Awareness Administration Guide:

https://sc1.checkpoint.com/documents/R80.30/WebAdminGuides/EN/CP_R80.30_IdentityAwareness_Admin_Guide/html_frameset.htm

Check Point Software Technologies GmbH
Zeppelinstraße 1
85399 Hallbergmoos

E-Mail: contact-germany@checkpoint.com

Web: www.checkpoint.com/de

Kontakt

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