CHECK POINT™

macmon
smartly simple

MACMON NAC WHITE PAPER

Integration of macmon NAC with Check Point Identity Awareness

Contents

Version: 1.0_en

Introduction

Check Point Software Technologies Ltd. is a leading provider of cyber security solutions to governments and corporate enterprises globally. Its solutions protect customers from cyber-attacks with an industry leading catch rate of malware, ransomware and other types of attacks. Check Point offers a multilevel security architecture that defends enterprises' cloud, network and mobile device held information, plus the most comprehensive and intuitive one point of control security management system. Check Point protects over 100,000 organizations of all sizes.

Use Cases

In the integration of Check Point Identity Awareness and macmon, macmon provides a lot of endpoint-specific information that complements the database of Identity Awareness. This makes it much easier for network administrators to implement group-based policies for access possibilities of endpoints within the corporate network. In so-called sessions, Check Point Identity Awareness manages information about each endpoint in the corporate network, from which an assignment to different configured policies in Identity Awareness results. Thus, for example, access privileges for an endpoint are derived.

New endpoint is passed on to Check Point Identity Awareness

If the IT department of a company procures a new endpoint and puts it into operation, or if an endpoint is switched on in the morning, macmon detects this immediately. To ensure that the session for this endpoint can also be started in Check Point Identity Awareness, macmon passes on detailed information about this endpoint, starts the session, and thus relieves the network administrator of double data management.

Disconnecting an endpoint from the corporate network ends the session in Check Point Identity Awareness

At the end of the day, endpoints are switched off or, in the case of notebooks, even disconnected from the corporate network for a longer period of time. macmon passes on the disconnection of an endpoint from the corporate network to Check Point Identity Awareness, thus stopping the previously started session. The session information is thus effectively tracked by Identity Awareness even in this case.

Changing endpoint information modifies the session in Check Point Identity Awareness

A move within the company building or a change of department often involves changing the IP address of an endpoint. To ensure that the firewall rules and the associated firewall decisions continue to apply correctly and the correct IP addresses are taken into account, macmon immediately passes on such a change to Identity Awareness to update both the running session and its information.

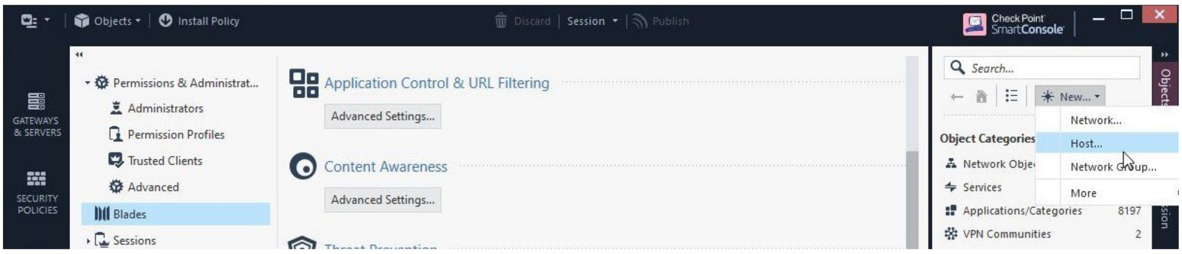
Renewal of Check Point Identity Awareness sessions

Endpoints such as telephones are always switched on and active in the corporate network for their operation. macmon always ensures that the session in Check Point Identity Awareness is up to date and continues to run to ensure optimal protection and overview.

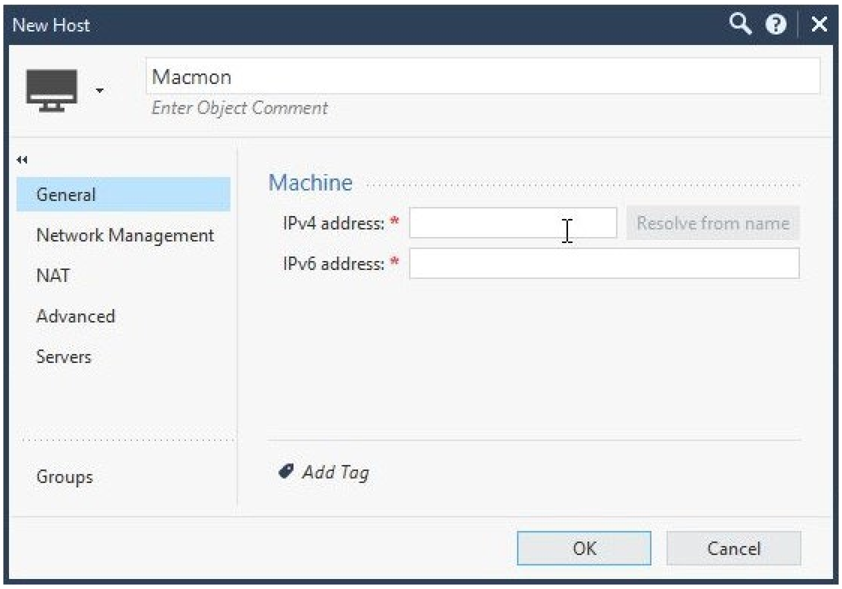
Configuration of Check Point Identity Awareness

The following steps guide you through the configuration of Check Point Identity Awareness. It is necessary to create the client secret that is needed for configuring the integration in the macmon GUI.

1. If you haven't already created a host for your macmon installation, select New and Host in the section on the right side of the *Check Point SmartConsole*.

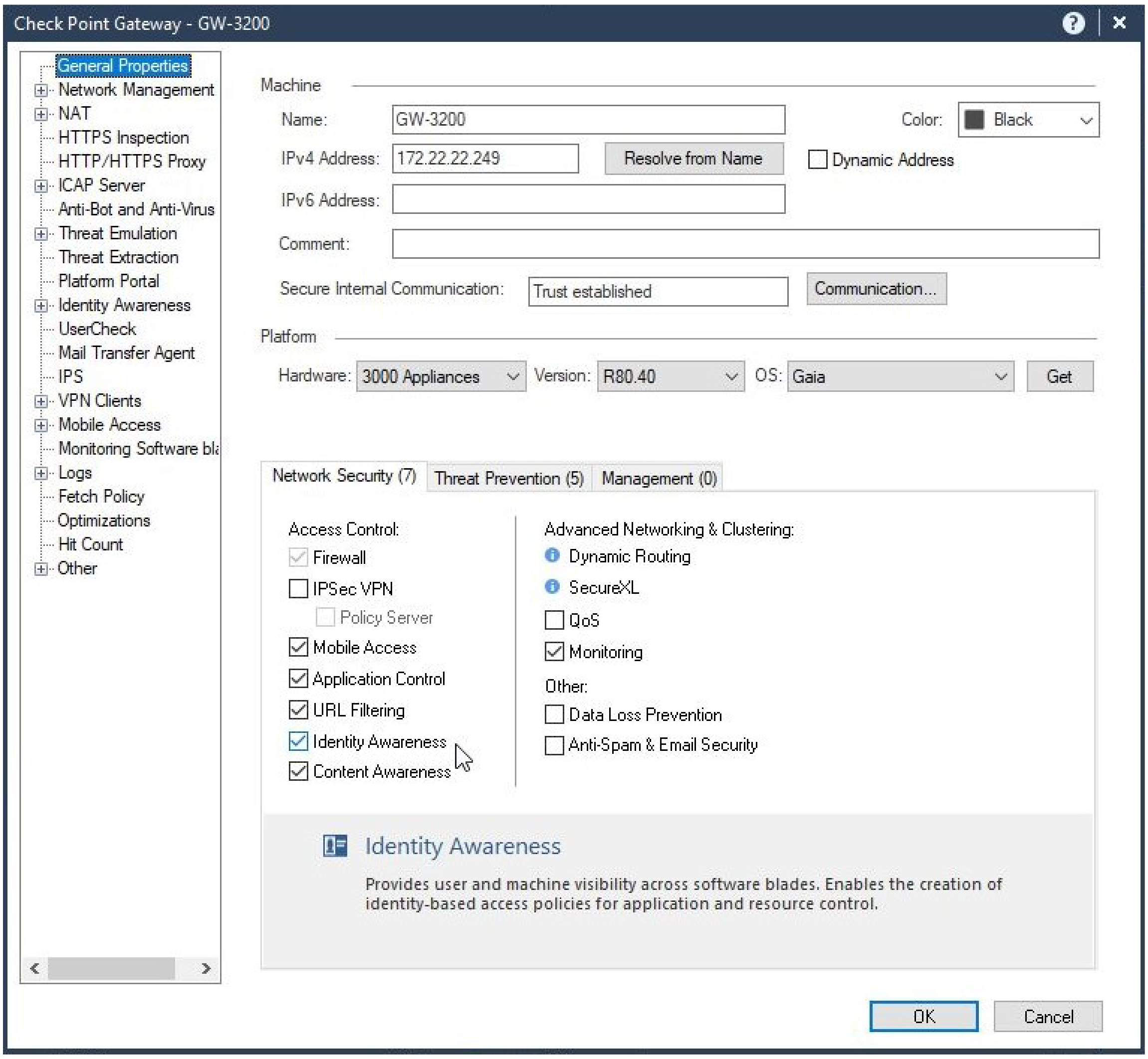


2. Choose a name, e. g. *macmon*. Enter either the *IPv4* or *IPv6 address* or both addresses of your macmon installation.


New Host

Macmon

3. From this step on, the configuration of the *Check Point Gateway* is done. In the *General Properties* section on the tab Network Security activate the *Identity Awareness* blade by checking the corresponding box. Cancel the wizard that might appear.



Machine

Name: GW-3200

Color: Black

IPv4 Address: 172.22.22.249

□ Dynamic Address

IPv6 Address:

Comment:

Secure Internal Communication: Trust established

Platform

Hardware: 3000 Appliances Version: R80.40 OS: Gaia

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:

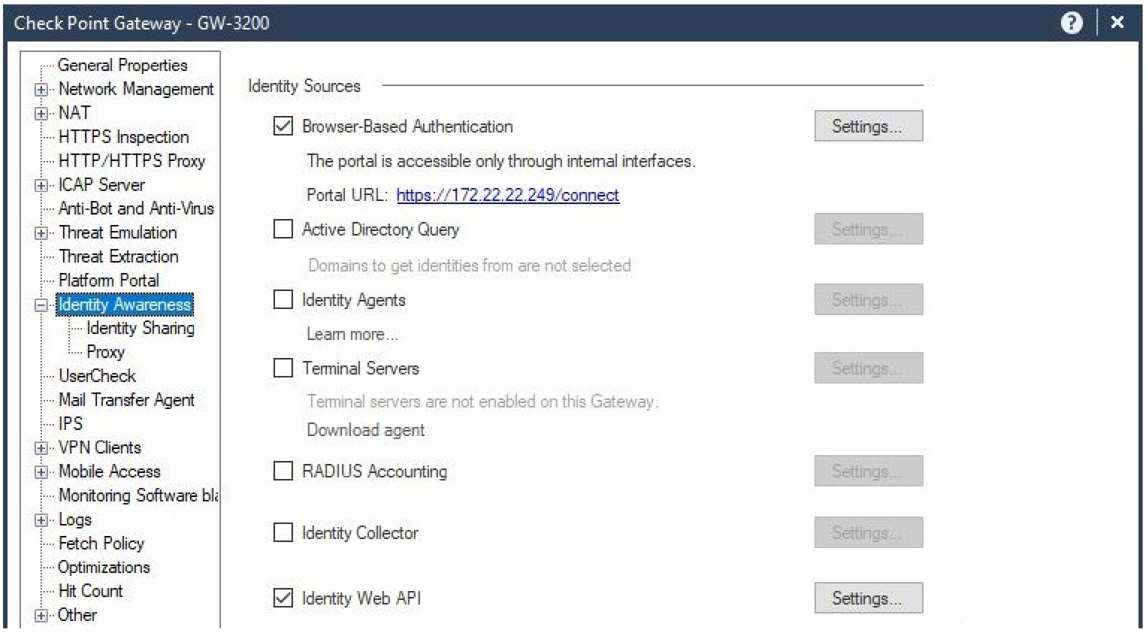
□ Data Loss Prevention

□ 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.

4. Select the *Identity Awareness* section and check *Identity Web API* in the *Identity Sources* section There, click on the *Settings* button.



Identity Sources

☑ Browser-Based Authentication

The portal is accessible only through internal interfaces.

Portal URL: https://172.22.22.249/connect

☐ Active Directory Query

Domains to get identities from are not selected

☐ Identity Agents

Learn more...

☐ Terminal Servers

Terminal servers are not enabled on this Gateway.

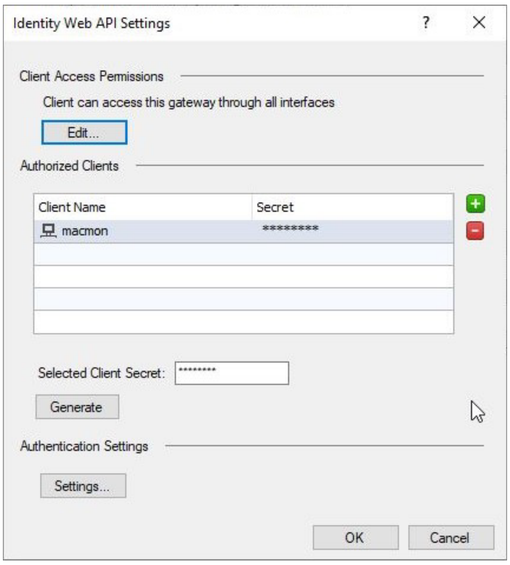
Download agent

☐ RADIUS Accounting

☐ Identity Collector

☑ Identity Web API

5. Click on the Edit button in the *Client Access Permissions* section of the new dialog window. There, select the interfaces through which *Check Point Identity Awareness* should be accessible. Add the host you created in step 1 as an *authorized client* by clicking the green plus sign. Remember the *Client Secret*, which is required in the configuration of the integration in the macmon GUI. Complete the configuration by clicking *OK*.



Client Access Permissions

Client can access this gateway through all interfaces

Authorized Clients

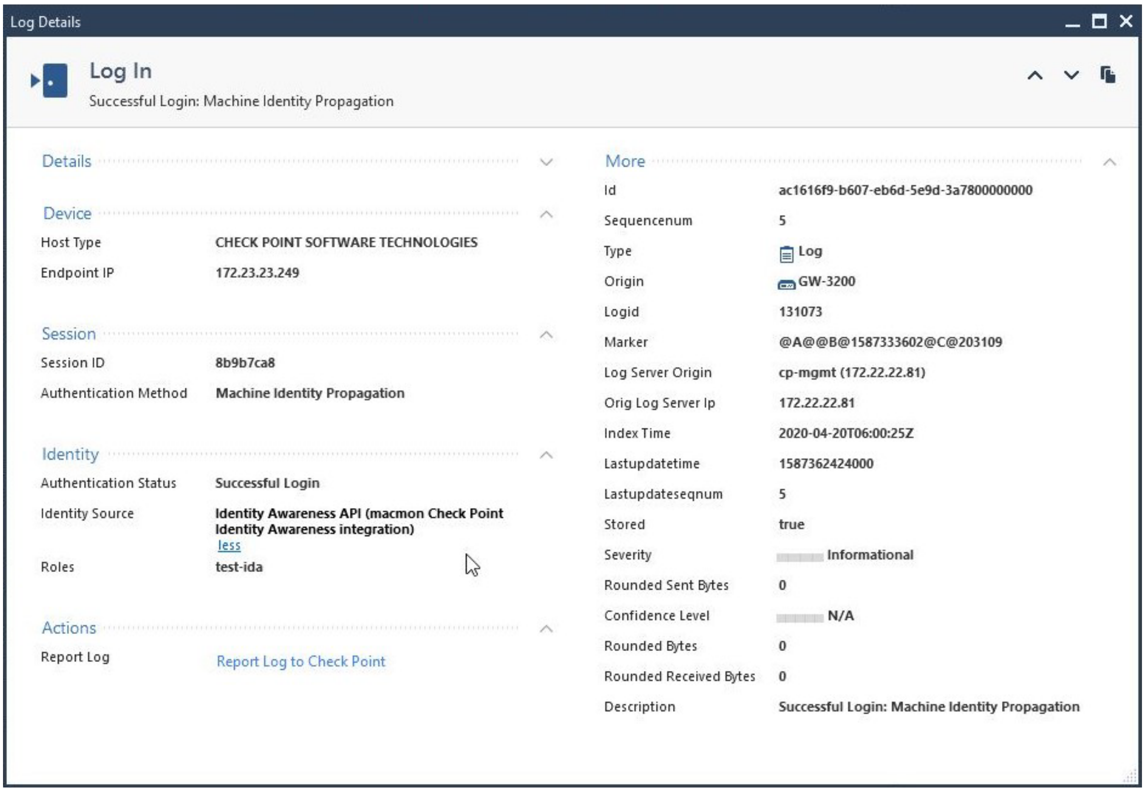
Client Name	Secret
macmon	********

Selected Client Secret: ********

Authentication Settings

6. Activate the changed configuration by tapping on *Publish*.

In the *Logs & Monitor* section you will find various login events. Select the *Identity Awareness* blade to find these entries.



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) less
Roles	test-ida

Actions

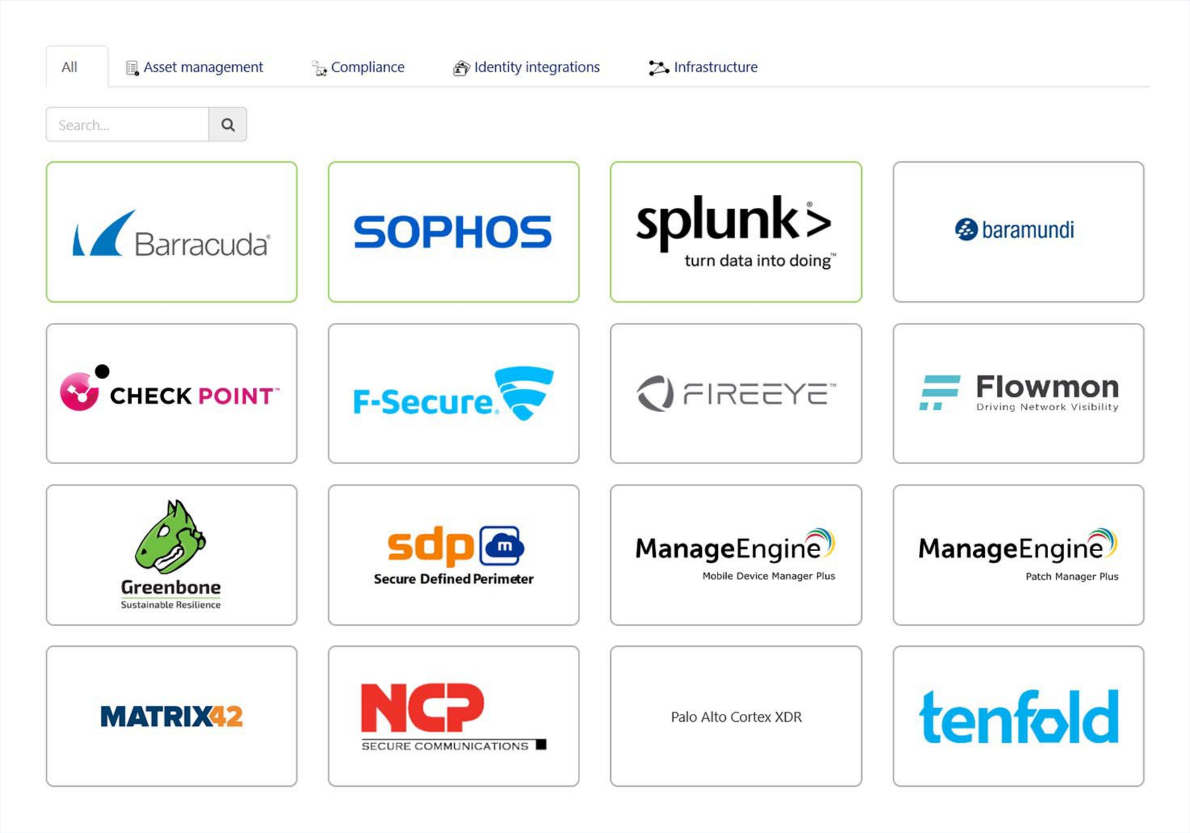
Report Log	Report Log to Check Point

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
Lastupdatetime	1587362424000
Lastupdateseqnum	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

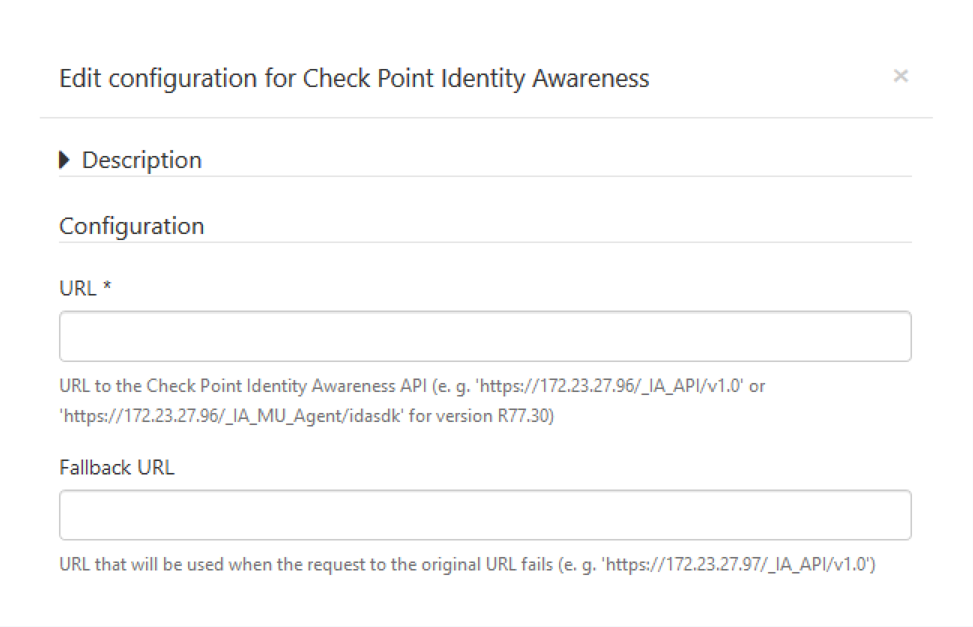
Configuration of macmon NAC

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


All
Asset management
Compliance
Identity integrations
Infrastructure
Search...
Barracuda
SOPHOS
splunk> turn data into doing
baramundi
CHECK POINT
F-Secure
FIREEYE
Flowmon Driving Network Visibility
Greenbone Sustainable Resilience
sdp Secure Defined Perimeter
ManageEngine Mobile Device Manager Plus
ManageEngine Patch Manager Plus
MATRIX42
NCP SECURE COMMUNICATIONS
Palo Alto Cortex XDR
tenfold

If the border of the *Check Point Identity Awareness* 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 needed to access the API of the Check Point Identity Awareness. Make sure to also enter the *Fallback URL* that is needed when the API of *URL* fails to respond.



Edit configuration for Check Point Identity Awareness ×

▶ Description

Configuration

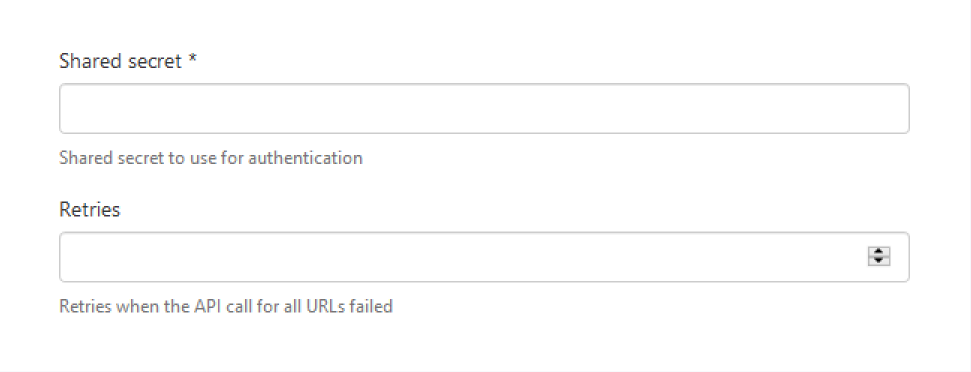
URL *

URL to the Check Point Identity Awareness API (e. g. 'https://172.23.27.96/_IA_API/v1.0' or 'https://172.23.27.96/_IA_MU_Agent/idasdk' for version R77.30)

Fallback URL

URL that will be used when the request to the original URL fails (e. g. 'https://172.23.27.97/_IA_API/v1.0')

2. Enter the *Shared secret* needed for authenticating with the system and in the field *Retries* enter the amount of times that macmon is supposed to retry connecting to the API when previous connection attempts failed.



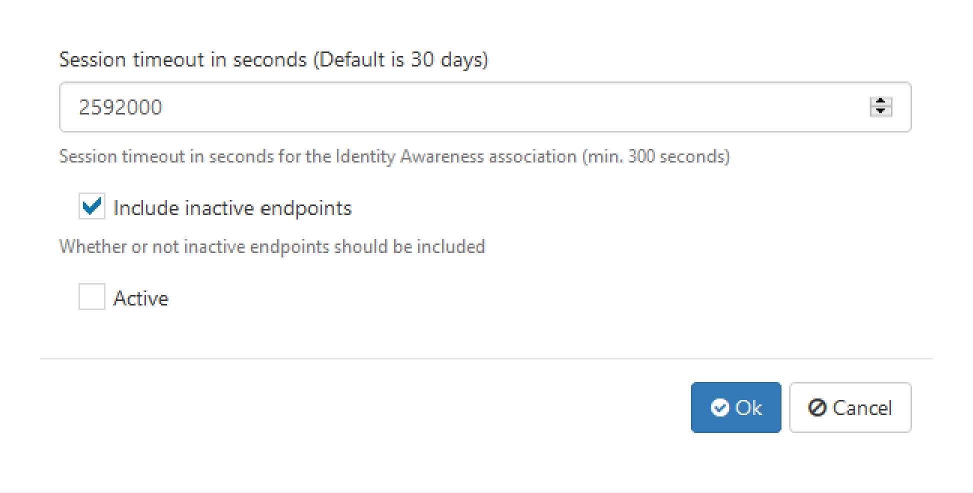
Shared secret *

Shared secret to use for authentication

Retries

Retries when the API call for all URLs failed

3. Enter the *Session timeout in seconds* that indicates when macmon is supposed to consider the association with *Check Point Identity Awareness* to be expired. Please note that this value is given in seconds. Check the box *Include inactive endpoints* if you want inactive endpoints to be included. Finally, make sure to check the box *Active* to activate the integration.



Session timeout in seconds (Default is 30 days)

2592000

Session timeout in seconds for the Identity Awareness association (min. 300 seconds)

☑ Include inactive endpoints

Whether or not inactive endpoints should be included

□ Active

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

Contact Check Point

Please find the Identity Awareness Administration Guide here:
https://sc1.checkpoint.com/documents/R80.30/WebAdminGuides/EN/CP_R80.30_IdentityAwareness_AdminGuide/html_frameset.htm

Check Point Software Technologies GmbH
Zeppelinstraße 1
85399 Hallbergmoos

Email: contact-germany@checkpoint.com
Web: www.checkpoint.com/de

Contact

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