MACMON NAC WHITE PAPER

Integration of macmon NAC with Vectra Cognito

Integration of macmon NAC with Vectra Cognito

macmon smartly simple

Content

Version 1.3

1 Introduction

Vectra is a global leader in AI solutions for real-time detection and defense against cyber attacks in cloud, data center and enterprise infrastructures.

These solutions enable security analysts to effectively investigate security incidents and conduct AI-powered threat hunting. In today's challenging data environments, it is essential to be able to effectively detect and respond to all cyber attacks.

Unlike other companies, Vectra enables you to proactively hunt cyber attackers and reduce risks to your business.

Our core team consists of threat researchers, white hat hackers, data scientists, network security experts and UI designers. We are continually pushing the boundaries of what is possible in order to usher in the next generation of security.

2 Sample use cases

2.1 macmon queries endpoints' risk rating from Vectra Cognito

In addition to viruses and malware, administrators also have to deal with suspicious endpoint behavior. If an endpoint becomes infected with malware despite the precautions taken, that endpoint must be isolated from the network segment as soon as possible. This prevents malware from spreading across the network and infecting other resources in the network. **Vectra Cognito** is able to quickly detect such threats with the use of artificial intelligence.

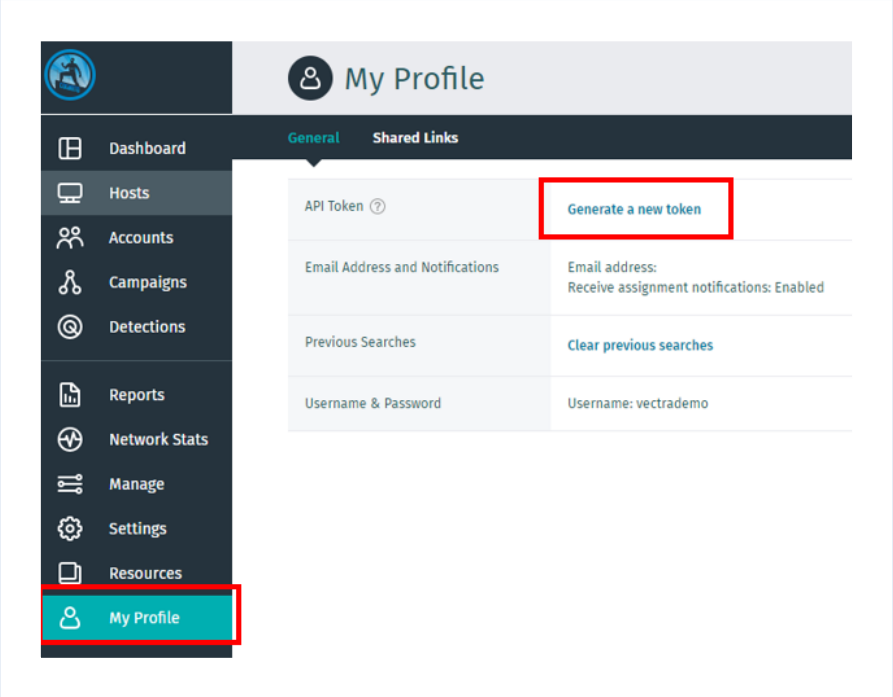
Vectra Cognito records the system status of every endpoint in the corporate network and makes these available to **macmon NAC**. The combination of **Vectra Cognito** and **macmon NAC** provides a powerful combination of threat detection and isolation of affected endpoints.

The information provided allows **macmon NAC** to enforce an endpoint's compliance status based on the risk rating determined by **Vectra Cognito**. And it works on networks of any size – because device threats are a feature of every network. Once **Vectra Cognito** detects such a threat in your network, it classifies the threat into four states: "low," "medium," "high" and "critical." These states are regularly reviewed by **macmon NAC** and assigned to different compliance statuses. For example, if the system state "critical" is assigned to the compliance status "noncompliant," a preset rule ensures that a critical endpoint is isolated by moving it to the remediation VLAN or switching off the network connection at the switch.

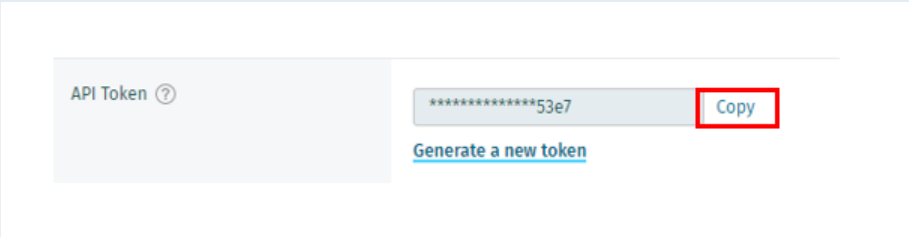
3 Configuring Vectra Cognito

The steps below describe how to create a token for API access by **macmon NAC**.

1. Tap *My Profile* and then the *General* tab. Then tap *Generate a new token*.



On the next page, tap *Copy* next to the *API Token* field. You need this token in step 1 of the procedure for configuring **macmon NAC**.

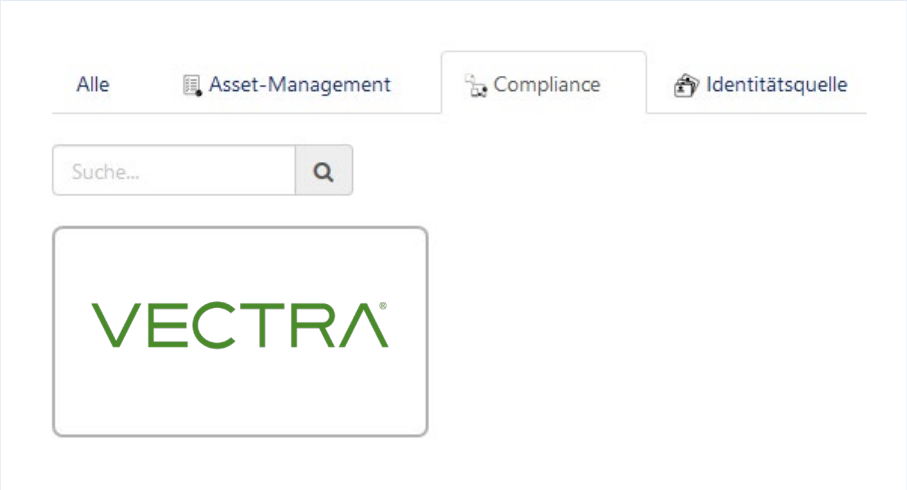


4 Configuring macmon NAC

The steps below describe how to configure and enable the integration. Enabling the integration creates a task in *Settings → Scheduled Tasks*, which is executed at the configured interval.

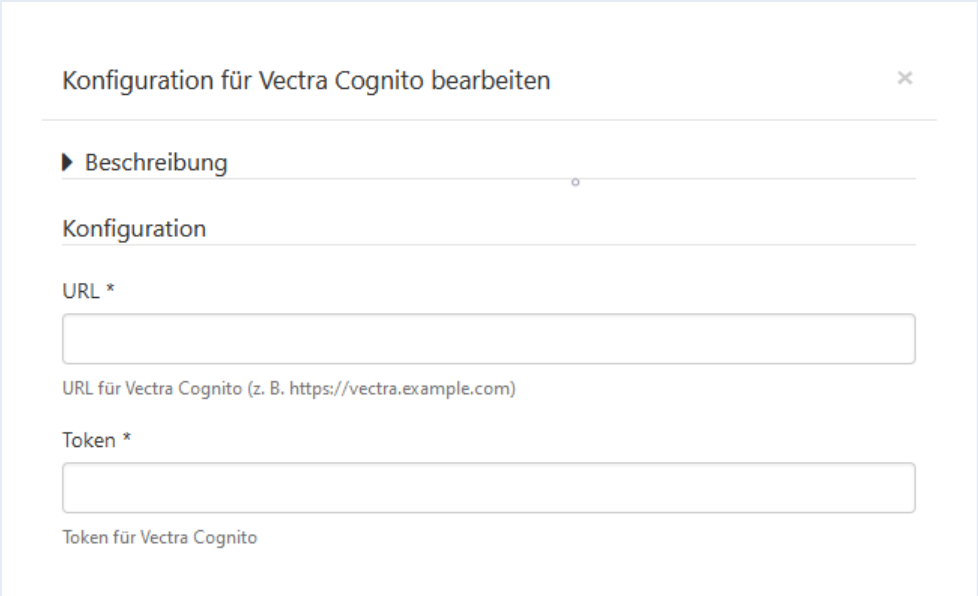
You can see a list of all queried endpoints under *Reports → Endpoints → Client Compliance*. You can filter this list by the source *Vectra TDR-Platform*.

The configuration is carried out in the web GUI. Select *Settings*, *Third-Party Integrations* and then the *Compliance* tab.



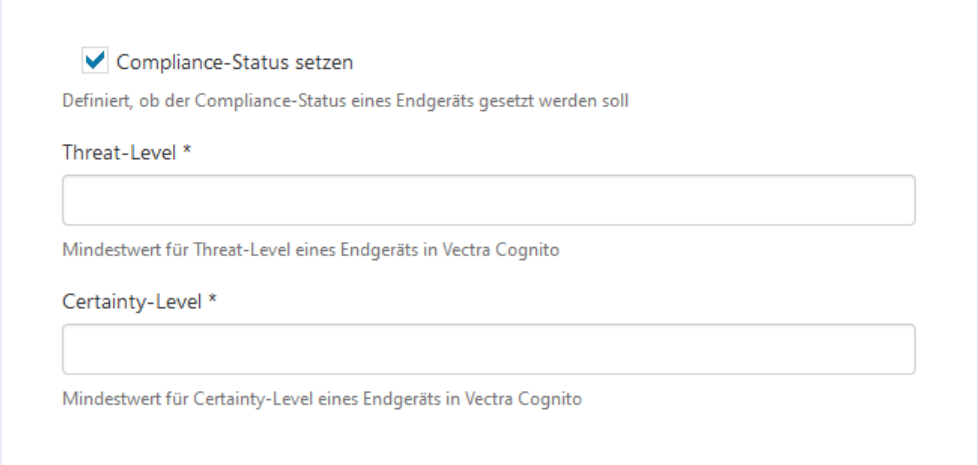
If the frame around the **Vectra Cognito** tile is gray, the integration has not been enabled yet. Please tap the tile to open the configuration dialog box.

1. Enter the URL for calling the **Vectra TDR-Platform** API. Also enter the token.

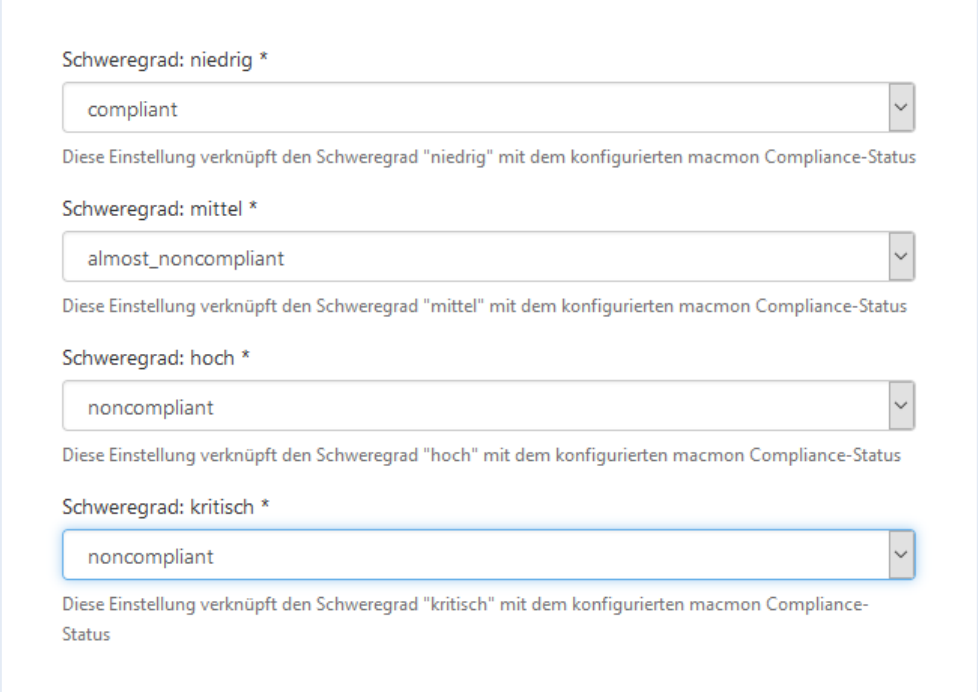


2. Select the Compliance box if you want to set the Compliance Status.
   Select the Threat Level and the Certainty Level by which to filter the endpoints so that you obtain information only on endpoints at or above a certain criticality level.

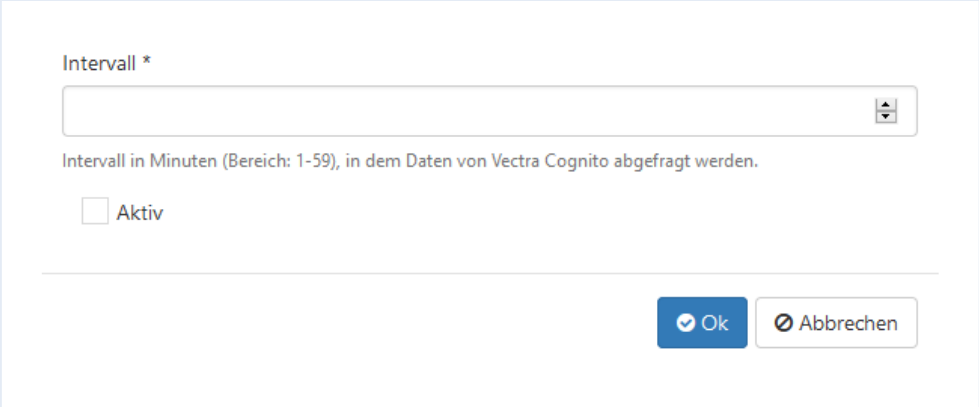
   According to Vectra's terminology, the Threat Level refers to the severity of the threat, and the Certainty Level refers to the likelihood that the threat will be exploited, which is used to calculate the risk.



3. Configure how you want to map the various system statuses to **macmon NAC**. This will determine which compliance status is set in **macmon** as well as the associated response, such as isolation of the particular endpoint.



4. Enter the Interval at which you want to retrieve the data.



5. Click ***OK*** to complete the activation.

5 Versions supported

macmon NAC, version 5.33.1. and later with the **Premium Bundle** License
Vectra Cognito, version 6.1.0 and later

Contact to Vectra

Vectra Networks Germany GmbH
Elsenheimerstrasse 7
80667 Munich, Germany

E-mail: info_dach@vectra.ai
Website: https://www.vectra.ai/products/cognito-platform