EGOSECURE
ENJOY DATA PROTECTION

macmon
nac intelligent einfach

MACMON NAC WHITE PAPER

Connection with Matrix42 EgoSecure Data Protection

CONNECTION WITH MATRIX42 EGOSECURE DATA PROTECTION

Contents

Version: 1.2_en

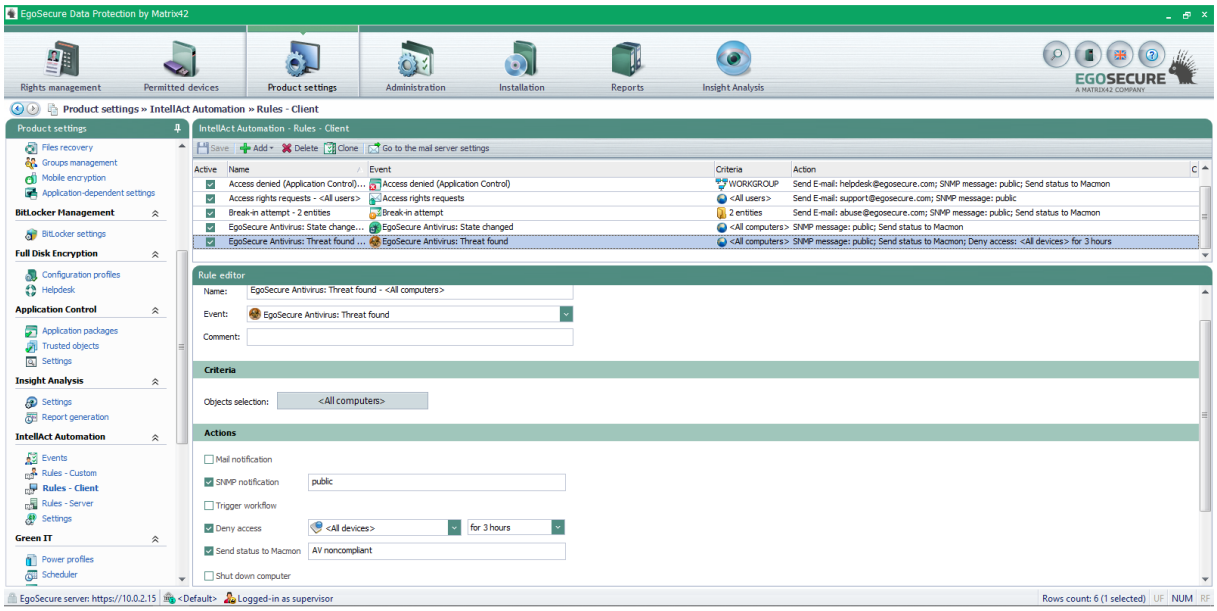
Introduction

EgoSecure Data Protection offers a comprehensive endpoint security solution, which provides endpoints with a central management for security features that range from virus protection to device control and application control to encryption. It provides an excellent source of information on compliance violations for macmon NAC by providing an up-to-date overview of incidents on endpoints and compliance with security policies. Based on any event or policy violation, macmon NAC can be notified about endpoints that do not comply and therefore be moved into a pre-configured isolation VLAN or disconnected from the regular corporate network. The direct connection between both systems and the resulting automated reaction to compliance or policy violations are explained in this white paper.

Use Cases

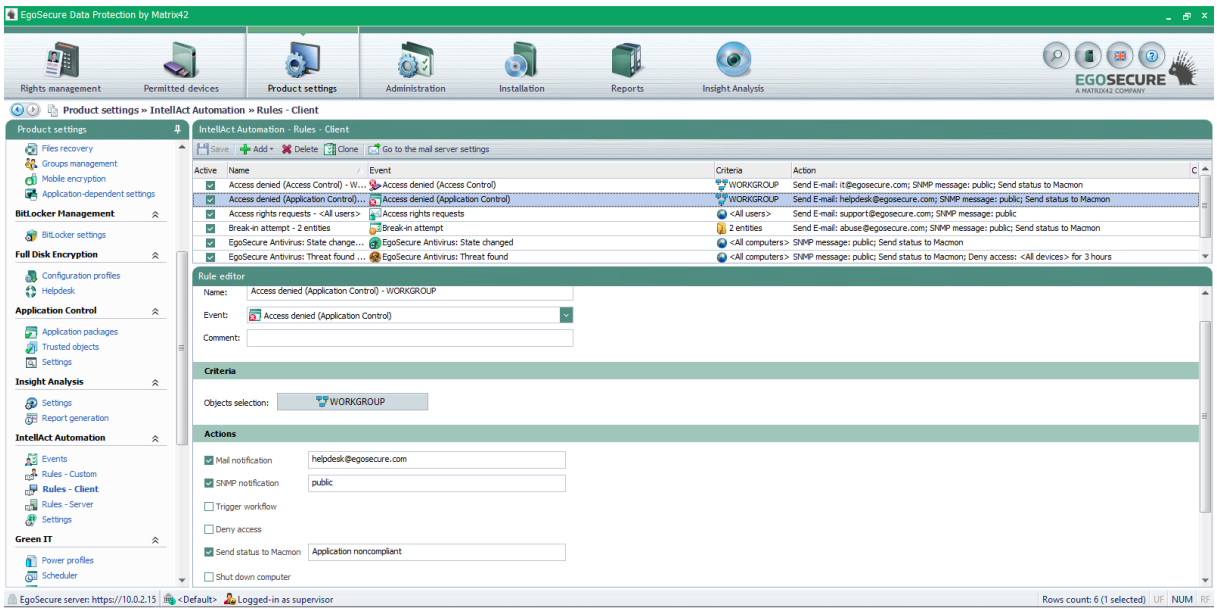
Malware detection

You can create a policy that informs macmon NAC about the detection of viruses, trojans and malicious code under *Product settings* → *IntellAct Automation* → *Rules* → *Client*.



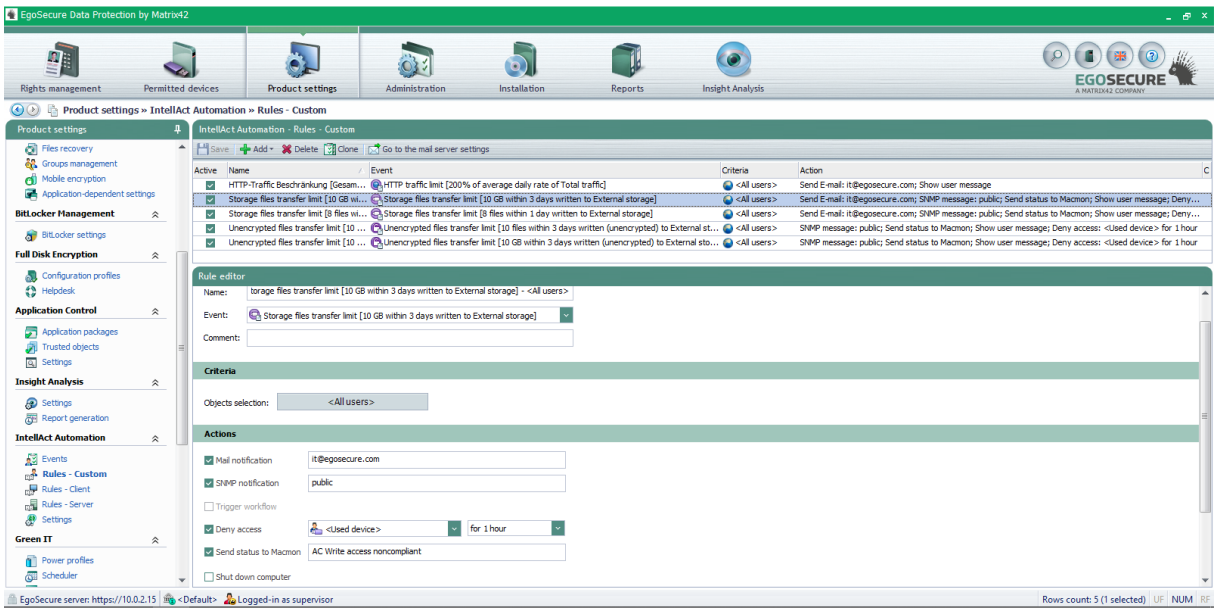
Detection of an unwanted application

If EgoSecure Application Control detects a launched application that is not on the whitelist or blacklist, a *non-compliant* message is sent to macmon NAC.



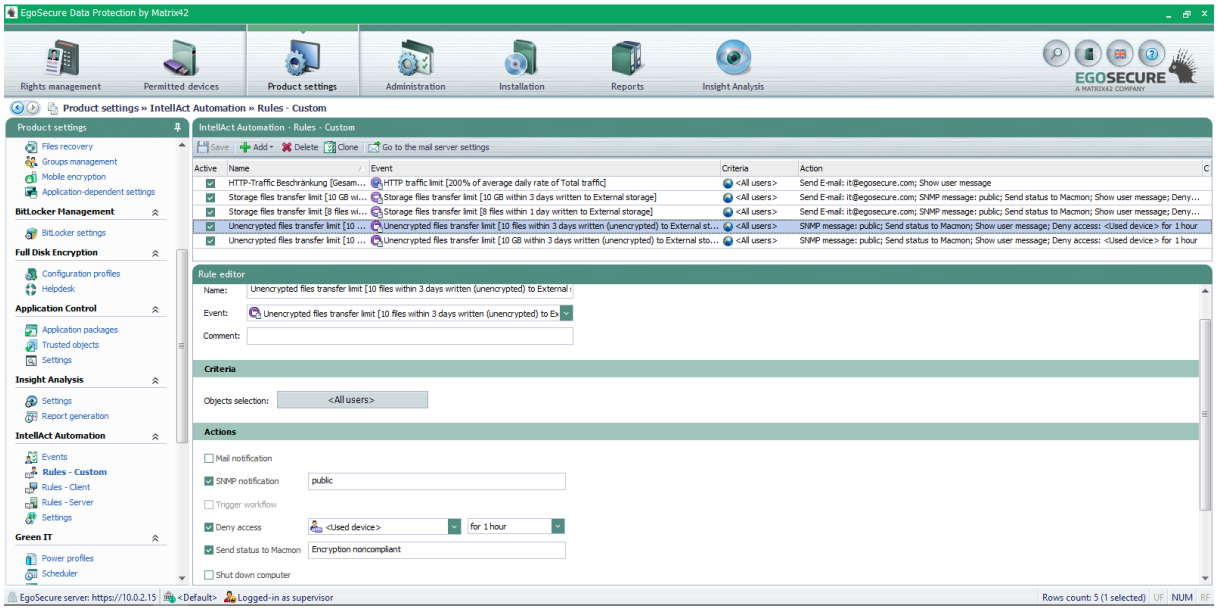
Exceeding data access on external storage media

If a certain limit of data access to external storage media is exceeded, a status message is transferred to macmon NAC.



Exceeding unencrypted write access to external storage media

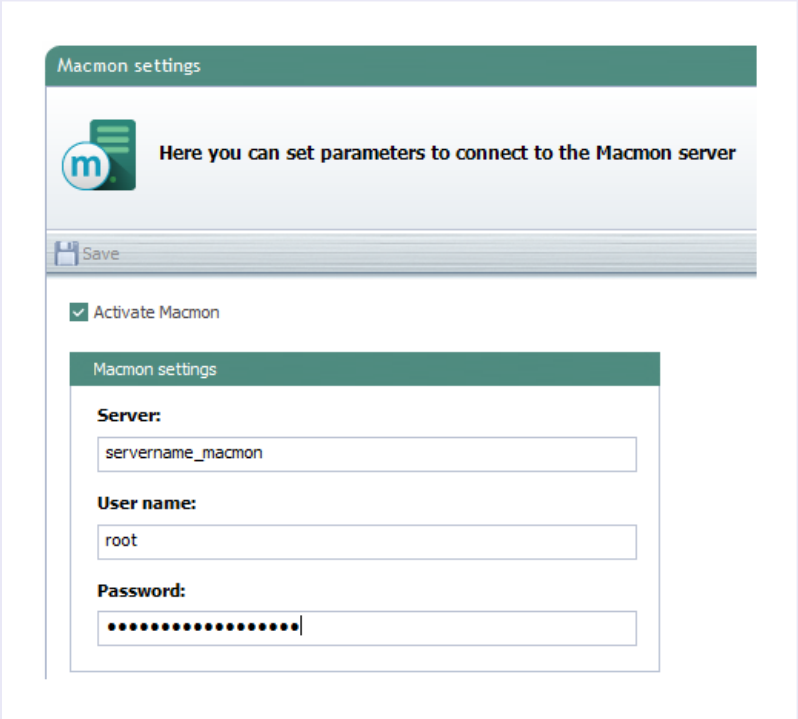
If a number of unencrypted write access to external storage media are exceeded, a status message is sent to macmon NAC.



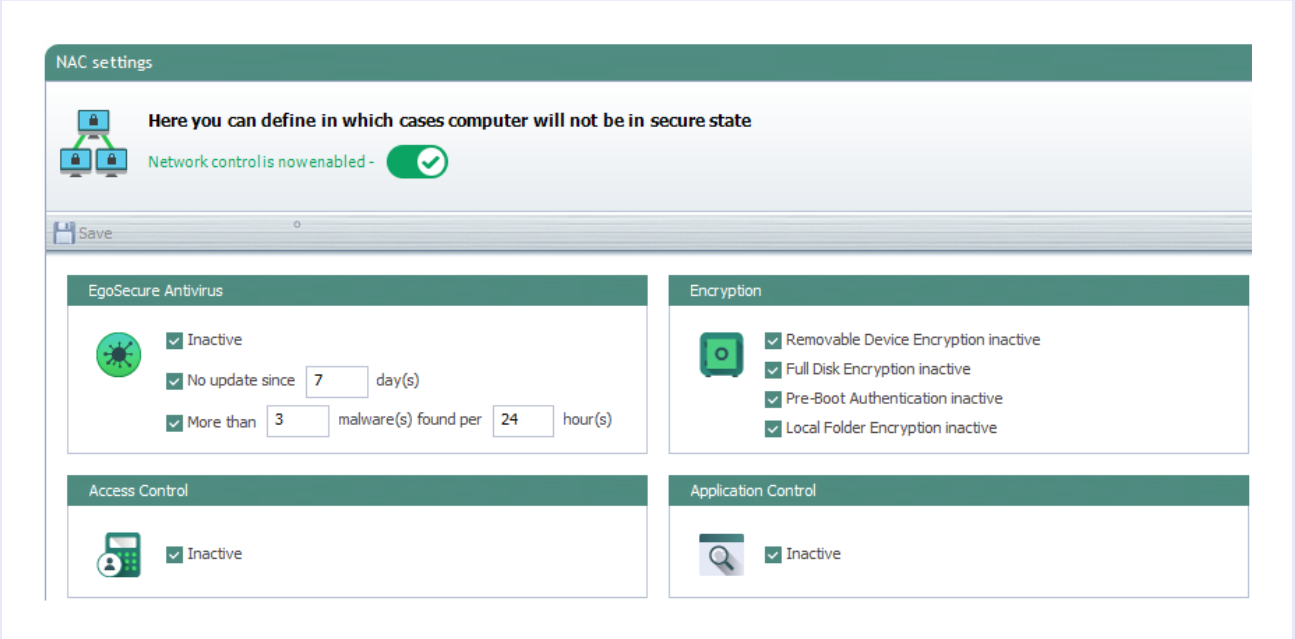
Configuration of EgoSecure Data Protection

Settings for communication with macmon NAC

In *Administration* → *NAC* → *macmon Settings* only the connection to macmon NAC has to be activated. Please enter the server name of your macmon installation in the input field *Server* and enter your macmon access credentials in the input fields *User name* and *Password*.



In *Administration* → *NAC* → *NAC Settings* you can create a global default in which situations an endpoint is considered *non-compliant*.



Configuration of macmon NAC

Policies

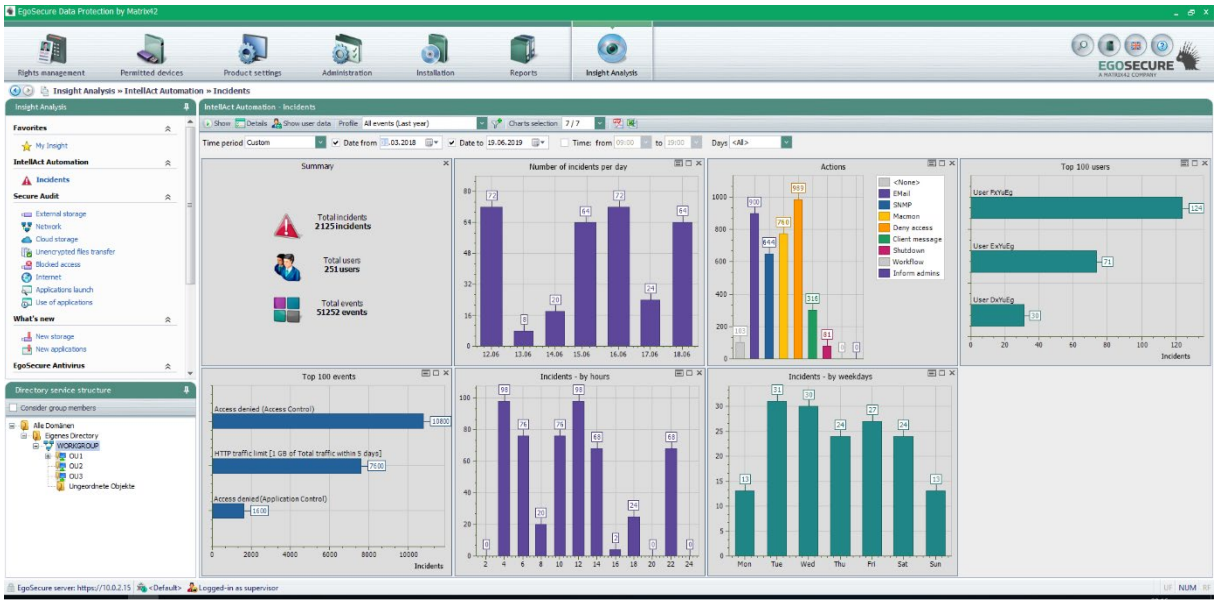
Endpoints are automatically moved to the Remediation VLAN when they are marked as non-compliant by EgoSecure Data Protection. This VLAN is configured in *Settings* → *Scan engine* → *remediation_vlans*. There is no further configuration needed.

In order to react differently to specific reasons for a non-compliant status, various rules can be created in *Policies* → *Events*.

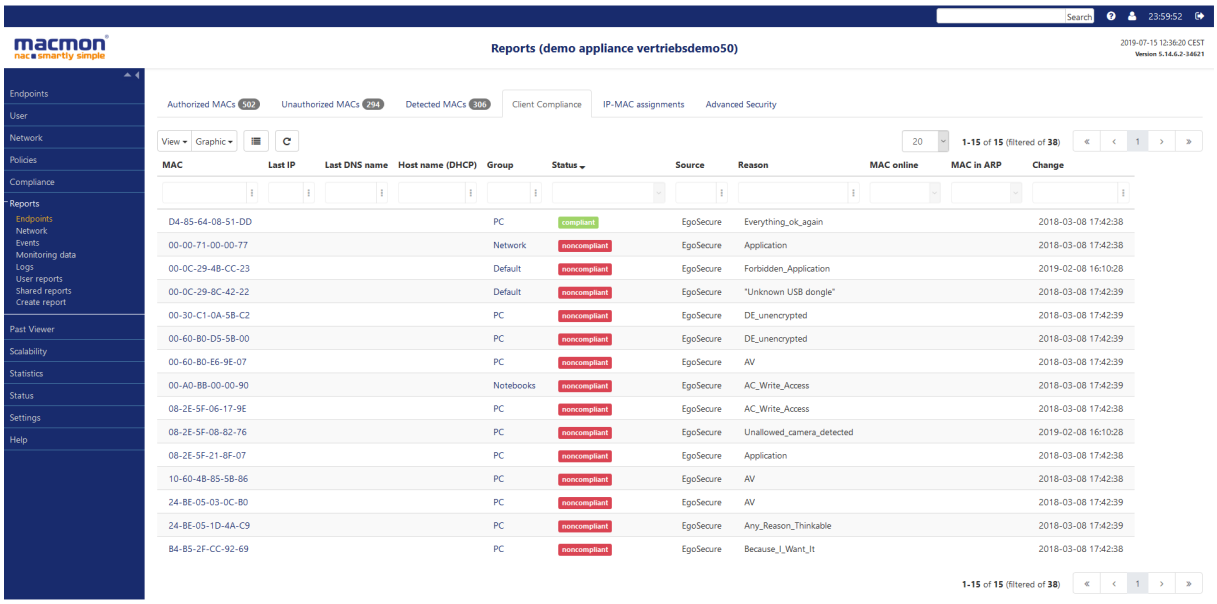
- Click on *Add rule*
- *Name* and *Description* can be freely chosen
- Select *now_noncompliant* as event
- Conditions:
  - Malware detection:
    mac.getEndpoint().getComplianceEntry("EgoSecure").getReason().isEqual("AV noncompliant")
  - Detection of an unwanted application:
    mac.getEndpoint().getComplianceEntry("EgoSecure").getReason().isEqual("Application noncompliant")
  - Exceeding data access on external storage media:
    mac.getEndpoint().getComplianceEntry("EgoSecure").getReason().isEqual("AC Write access noncompliant")
  - Exceeding unencrypted data access on external storage media:
    mac.getEndpoint().getComplianceEntry("EgoSecure").getReason().isEqual("Encryption noncompliant")
- Reaction could be *Send mail*

Overview of compliance violations

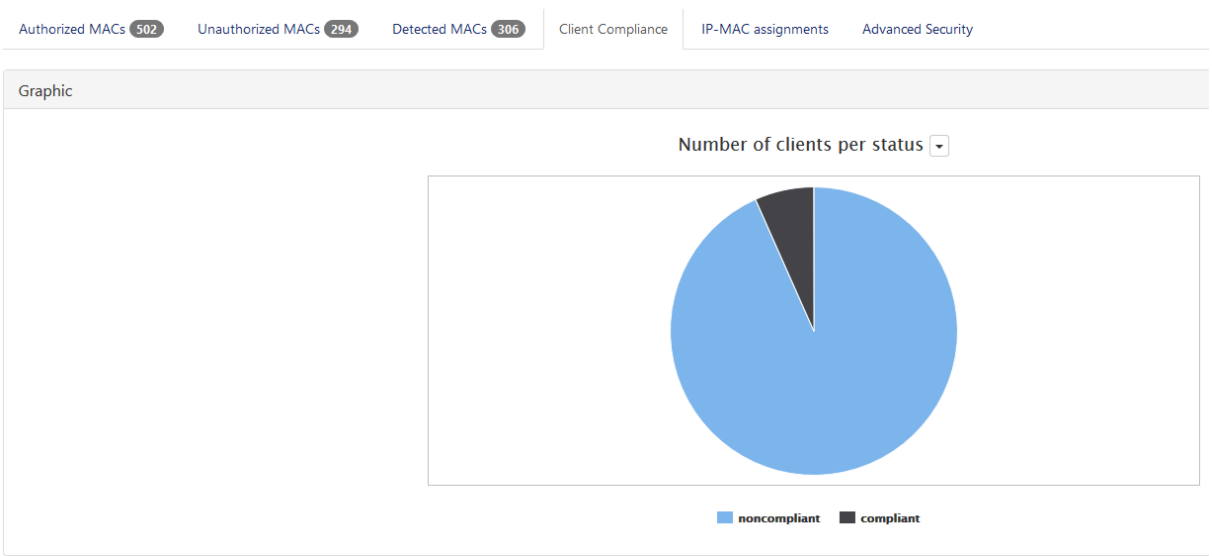
Once the events have occurred and the actions of EgoSecure Data Protection have been performed, these actions are displayed in its reporting as follows:



The status, the source and the reason of an endpoint are displayed in the report *Client Compliance*.



When filtered by the source *EgoSecure* the amount of endpoints can also be analyzed by status:



Contact at EgoSecure – a Matrix42 Company

Daniel Döring, Technical Director, Security and Strategic Alliances
Pforzheimer Str. 128b | 76275 Ettlingen
Tel.: +49 724335495-0 | support@egosecure.com | www.egosecure.com

Contact

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