

MACMON NAC WHITE PAPER

Connection with Matrix42

EgoSecure Data Protection

Contents

Introduction 3

Use Cases 4

 Malware detection 4

 Detection of an unwanted application 4

 Exceeding data access on external storage media 5

 Exceeding unencrypted write access to external storage media 5

Configuration of EgoSecure Data Protection 6

 Settings for communication with macmon NAC 6

Configuration of macmon NAC 7

 Policies 7

Overview of compliance violations 8

Contact at EgoSecure – a Matrix42 Company 9

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*.

The screenshot shows the EgoSecure Data Protection by Matrix42 interface. The left sidebar contains various management categories: Rights management, Permitted devices, Product settings, Administration, Installation, Reports, and Insight Analysis. The main window is titled 'Product settings > IntellAct Automation > Rules - Client'. It displays a table of rules and a 'Rule editor' for the selected rule.

Active	Name	Event	Criteria	Action
☒	Access denied (Application Control)...	Access denied (Application Control)	WORKGROUP	Send E-mail: helpdesk@egosecure.com; SNMP message: public; Send status to Macmon
☒	Access denied (Application Control)...	Access denied (Application Control)	WORKGROUP	Send E-mail: support@egosecure.com; SNMP message: public; Send status to Macmon
☒	Access rights requests - <All users>	Access rights requests	<All users>	Send E-mail: abuse@egosecure.com; SNMP message: public; Send status to Macmon
☒	Break-in attempt - 2 entities	Break-in attempt	2 entities	Send E-mail: abuse@egosecure.com; SNMP message: public; Send status to Macmon
☒	EgoSecure Antivirus: State change...	EgoSecure Antivirus: State changed	<All computers>	SNMP message: public; Send status to Macmon
☒	EgoSecure Antivirus: Threat found...	EgoSecure Antivirus: Threat found	<All computers>	SNMP message: public; Send status to Macmon; Deny access: <All devices> for 3 hours

The 'Rule editor' for the selected rule 'EgoSecure Antivirus: Threat found - <All computers>' shows the following configuration:

- Name:** EgoSecure Antivirus: Threat found - <All computers>
- Event:** EgoSecure Antivirus: Threat found
- Comments:**
- Criteria:** Objects selection: <All computers>
- Actions:**
 - ☐ Mail notification
 - ☒ SNMP notification: public
 - ☐ Trigger workflow
 - ☒ Deny access: <All devices> for 3 hours
 - ☒ Send status to Macmon: AV noncompliant
 - ☐ Shut down computer

The status bar at the bottom indicates 'EgoSecure server: https://10.0.2.15', '<Default>', 'Logged-in as supervisor', and 'Rows count: 6 (1 selected)'.

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.

The screenshot shows the EgoSecure Data Protection by Matrix42 interface. The left sidebar contains various management categories: Rights management, Permitted devices, Product settings, Administration, Installation, Reports, and Insight Analysis. The main window is titled 'Product settings > IntellAct Automation > Rules - Client'. It displays a table of rules and a 'Rule editor' for the selected rule.

Active	Name	Event	Criteria	Action
☒	Access denied (Access Control) - W...	Access denied (Access Control)	WORKGROUP	Send E-mail: it@egosecure.com; SNMP message: public; Send status to Macmon
☒	Access denied (Application Control)...	Access denied (Application Control)	WORKGROUP	Send E-mail: helpdesk@egosecure.com; SNMP message: public; Send status to Macmon
☒	Access rights requests - <All users>	Access rights requests	<All users>	Send E-mail: support@egosecure.com; SNMP message: public; Send status to Macmon
☒	Break-in attempt - 2 entities	Break-in attempt	2 entities	Send E-mail: abuse@egosecure.com; SNMP message: public; Send status to Macmon
☒	EgoSecure Antivirus: State change...	EgoSecure Antivirus: State changed	<All computers>	SNMP message: public; Send status to Macmon
☒	EgoSecure Antivirus: Threat found...	EgoSecure Antivirus: Threat found	<All computers>	SNMP message: public; Send status to Macmon; Deny access: <All devices> for 3 hours

The 'Rule editor' for the selected rule 'Access denied (Application Control) - WORKGROUP' shows the following configuration:

- Name:** Access denied (Application Control) - WORKGROUP
- Event:** Access denied (Application Control)
- Comments:**
- Criteria:** Objects selection: WORKGROUP
- Actions:**
 - ☒ Mail notification: helpdesk@egosecure.com
 - ☒ SNMP notification: public
 - ☐ Trigger workflow
 - ☐ Deny access
 - ☒ Send status to Macmon: Application noncompliant
 - ☐ Shut down computer

The status bar at the bottom indicates 'EgoSecure server: https://10.0.2.15', '<Default>', 'Logged-in as supervisor', and 'Rows count: 6 (1 selected)'.

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.

The screenshot shows the EgoSecure Data Protection by Matrix42 interface. The left sidebar contains various management categories: Rights management, Permitted devices, Product settings, Administration, Installation, Reports, and Insight Analysis. The main window is titled 'Product settings » IntelAct Automation » Rules - Custom'. It displays a table of rules and a 'Rule editor' for a selected rule.

Active	Name	Event	Criteria	Action
☒	HTTP-Traffic-Beschränkung (Gesam...)	HTTP traffic limit [200% of average daily rate of Total traffic]	<All users>	Send E-mail: it@egosecure.com; Show user message
☒	Storage files transfer limit [10 GB wi...	Storage files transfer limit [10 GB within 3 days written to External storage]	<All users>	Send E-mail: it@egosecure.com; SNMP message: public; Send status to Macmon; Show user message; Deny...
☒	Storage files transfer limit [8 files wi...	Storage files transfer limit [8 files within 1 day written to External storage]	<All users>	Send E-mail: it@egosecure.com; SNMP message: public; Send status to Macmon; Show user message; Deny...
☒	Unencrypted files transfer limit [10 ...]	Unencrypted files transfer limit [10 files within 3 days written (unencrypted) to External st...	<All users>	SNMP message: public; Send status to Macmon; Show user message; Deny access: <Used device> for 1 hour
☒	Unencrypted files transfer limit [10 ...]	Unencrypted files transfer limit [10 GB within 3 days written (unencrypted) to External sto...	<All users>	SNMP message: public; Send status to Macmon; Show user message; Deny access: <Used device> for 1 hour

The 'Rule editor' for the selected rule 'Storage files transfer limit [10 GB within 3 days written to External storage]' shows the following configuration:

- Name:** Storage files transfer limit [10 GB within 3 days written to External storage]
- Event:** Storage files transfer limit [10 GB within 3 days written to External storage]
- Comment:**
- Criteria:** Objects selection: <All users>
- Actions:**
 - ☒ Mail notification: it@egosecure.com
 - ☒ SNMP notification: public
 - ☐ Trigger workflow
 - ☒ Deny access: <Used device> for 1 hour
 - ☒ Send status to Macmon: AC Write access noncompliant
 - ☐ Shut down computer

The status bar at the bottom indicates 'EgoSecure server: https://10.0.2.15', '<Default>', 'Logged-in as supervisor', and 'Rows count: 5 (1 selected)'.

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.

The screenshot shows the EgoSecure Data Protection by Matrix42 interface, similar to the previous one, but with the 'Rule editor' configured for unencrypted file transfer limits.

Active	Name	Event	Criteria	Action
☒	HTTP-Traffic-Beschränkung (Gesam...)	HTTP traffic limit [200% of average daily rate of Total traffic]	<All users>	Send E-mail: it@egosecure.com; Show user message
☒	Storage files transfer limit [10 GB wi...	Storage files transfer limit [10 GB within 3 days written to External storage]	<All users>	Send E-mail: it@egosecure.com; SNMP message: public; Send status to Macmon; Show user message; Deny...
☒	Storage files transfer limit [8 files wi...	Storage files transfer limit [8 files within 1 day written to External storage]	<All users>	Send E-mail: it@egosecure.com; SNMP message: public; Send status to Macmon; Show user message; Deny...
☒	Unencrypted files transfer limit [10 ...]	Unencrypted files transfer limit [10 files within 3 days written (unencrypted) to External st...	<All users>	SNMP message: public; Send status to Macmon; Show user message; Deny access: <Used device> for 1 hour
☒	Unencrypted files transfer limit [10 ...]	Unencrypted files transfer limit [10 GB within 3 days written (unencrypted) to External sto...	<All users>	SNMP message: public; Send status to Macmon; Show user message; Deny access: <Used device> for 1 hour

The 'Rule editor' for the selected rule 'Unencrypted files transfer limit [10 files within 3 days written (unencrypted) to External storage]' shows the following configuration:

- Name:** Unencrypted files transfer limit [10 files within 3 days written (unencrypted) to External storage]
- Event:** Unencrypted files transfer limit [10 files within 3 days written (unencrypted) to External storage]
- Comment:**
- Criteria:** Objects selection: <All users>
- Actions:**
 - ☐ Mail notification
 - ☒ SNMP notification: public
 - ☐ Trigger workflow
 - ☒ Deny access: <Used device> for 1 hour
 - ☒ Send status to Macmon: Encryption noncompliant
 - ☐ Shut down computer

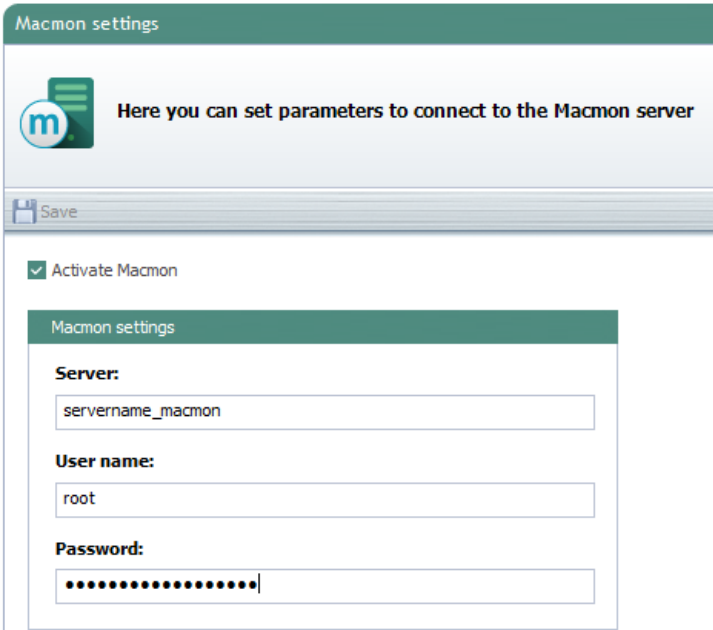
The status bar at the bottom indicates 'EgoSecure server: https://10.0.2.15', '<Default>', 'Logged-in as supervisor', and 'Rows count: 5 (1 selected)'.

Configuration of EgoSecure Data Protection

Settings for communication with macmon NAC

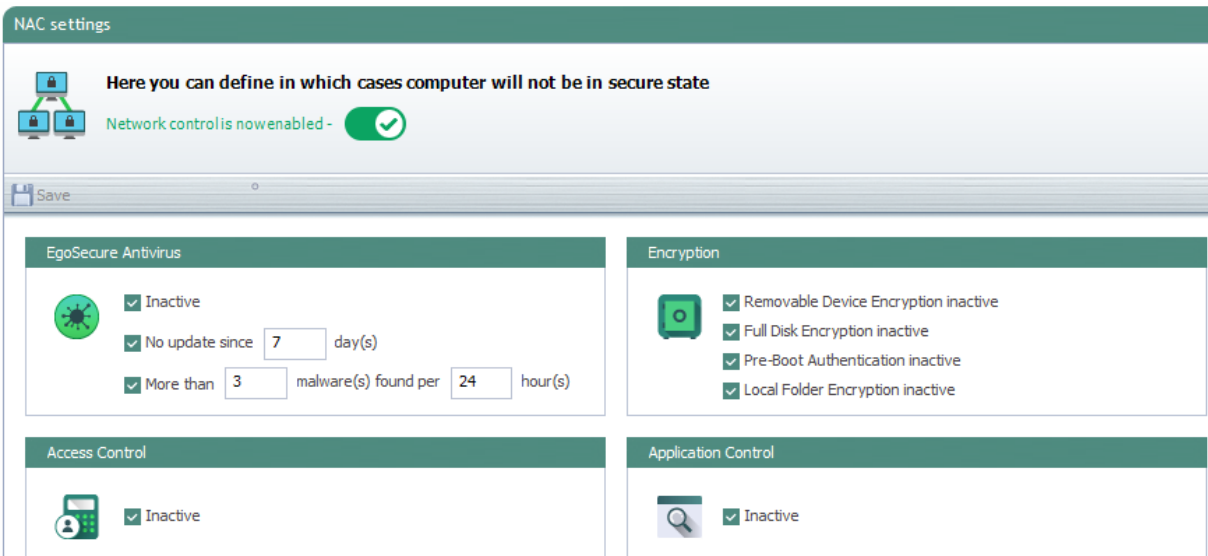
In *Administration* → *NAC* → *macmon Settings* only the connection to macmon NAC has to be activated.

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*.



The screenshot shows the 'Macmon settings' window. At the top, there is a header 'Macmon settings' and a sub-header 'Here you can set parameters to connect to the Macmon server'. Below this is a 'Save' button. A checkbox labeled 'Activate Macmon' is checked. Below the checkbox is a section titled 'Macmon settings' containing three input fields: 'Server:' with the value 'servername_macmon', 'User name:' with the value 'root', and 'Password:' with a masked password represented by dots.

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



The screenshot shows the 'NAC settings' window. At the top, there is a header 'NAC settings' and a sub-header 'Here you can define in which cases computer will not be in secure state'. Below this is a 'Save' button. A status bar indicates 'Network control is now enabled -' with a green checkmark icon. Below the status bar are four sections: 'EgoSecure Antivirus' with checkboxes for 'Inactive', 'No update since 7 day(s)', and 'More than 3 malware(s) found per 24 hour(s)'; 'Encryption' with checkboxes for 'Removable Device Encryption inactive', 'Full Disk Encryption inactive', 'Pre-Boot Authentication inactive', and 'Local Folder Encryption inactive'; 'Access Control' with a checkbox for 'Inactive'; and 'Application Control' with a checkbox for 'Inactive'.

Configuration of macmon NAC

Policies

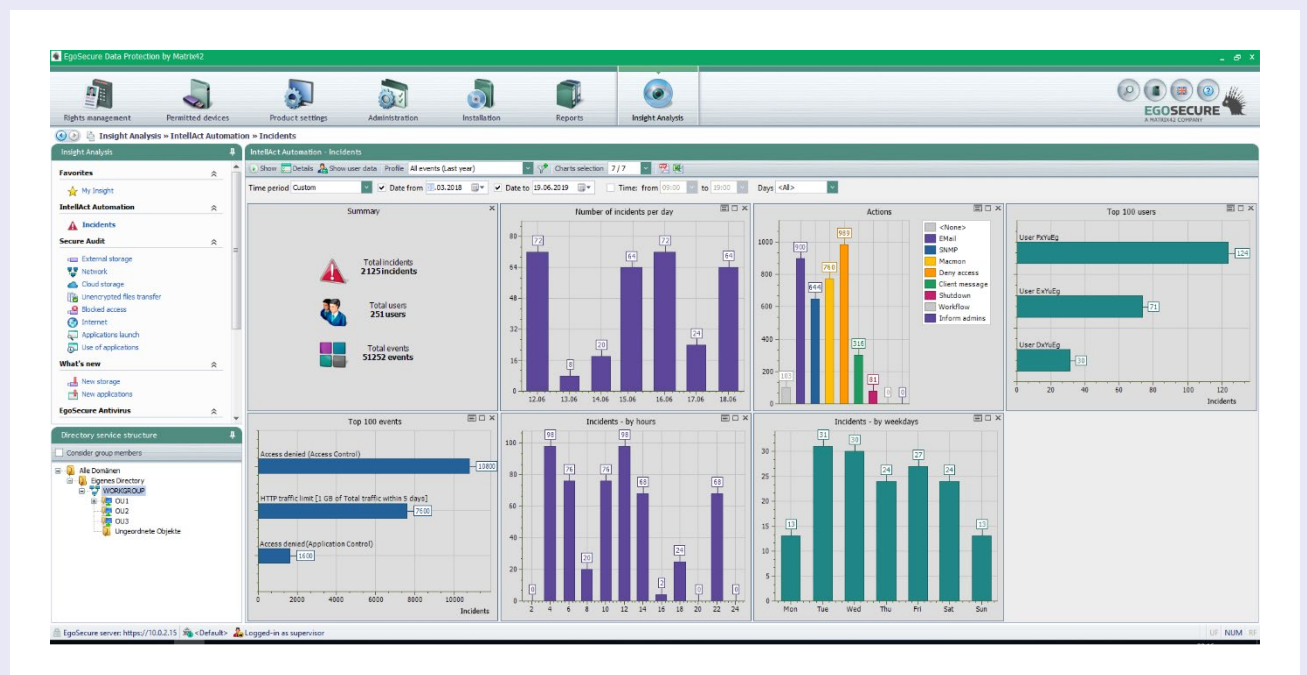
Endpoints are automatically moved to the Remediation VLAN when they are marked as non-compliant by EgoSecure Data Protection. This VLAN is configured in *Settings* → *Scan engine* → *remediation_vlans*. There is no further configuration needed.

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

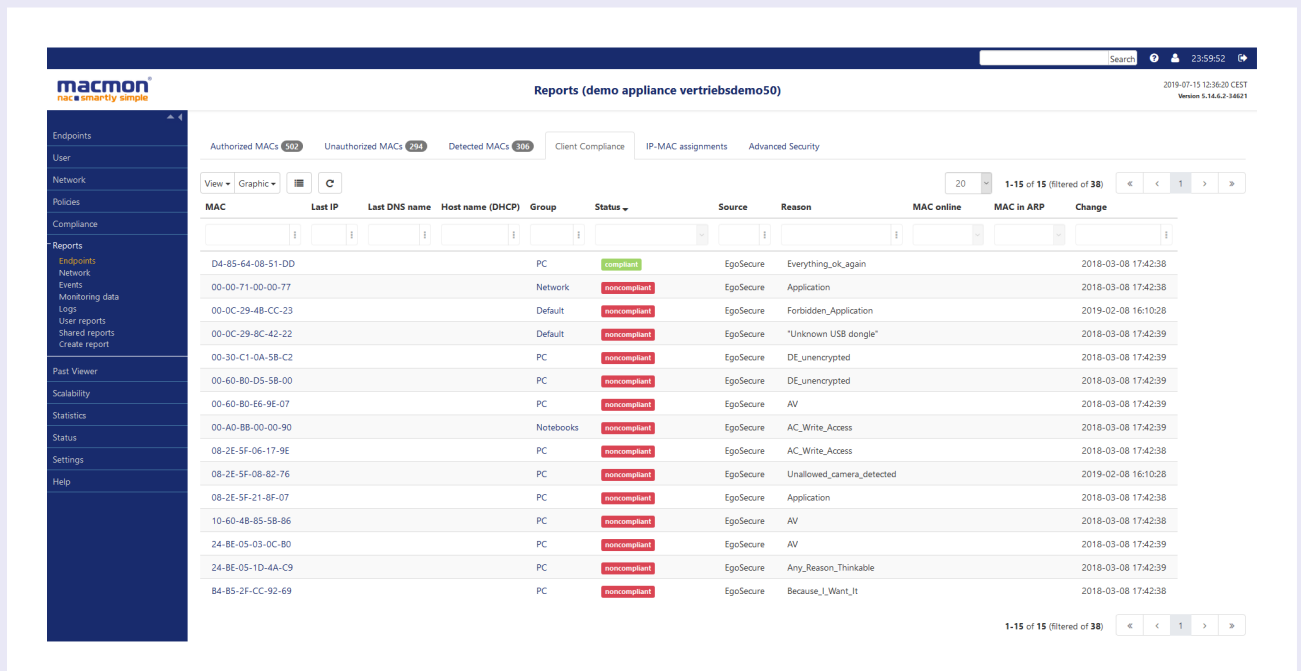
- Click on *Add rule*
- *Name* and *Description* can be freely chosen
- Select *now_noncompliant* as event
- Conditions:
 - Malware detection:
`mac.getEndpoint().getComplianceEntry("EgoSecure").getReason().isEqual("AV noncompliant")`
 - Detection of an unwanted application:
`mac.getEndpoint().getComplianceEntry("EgoSecure").getReason().isEqual("Application 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:

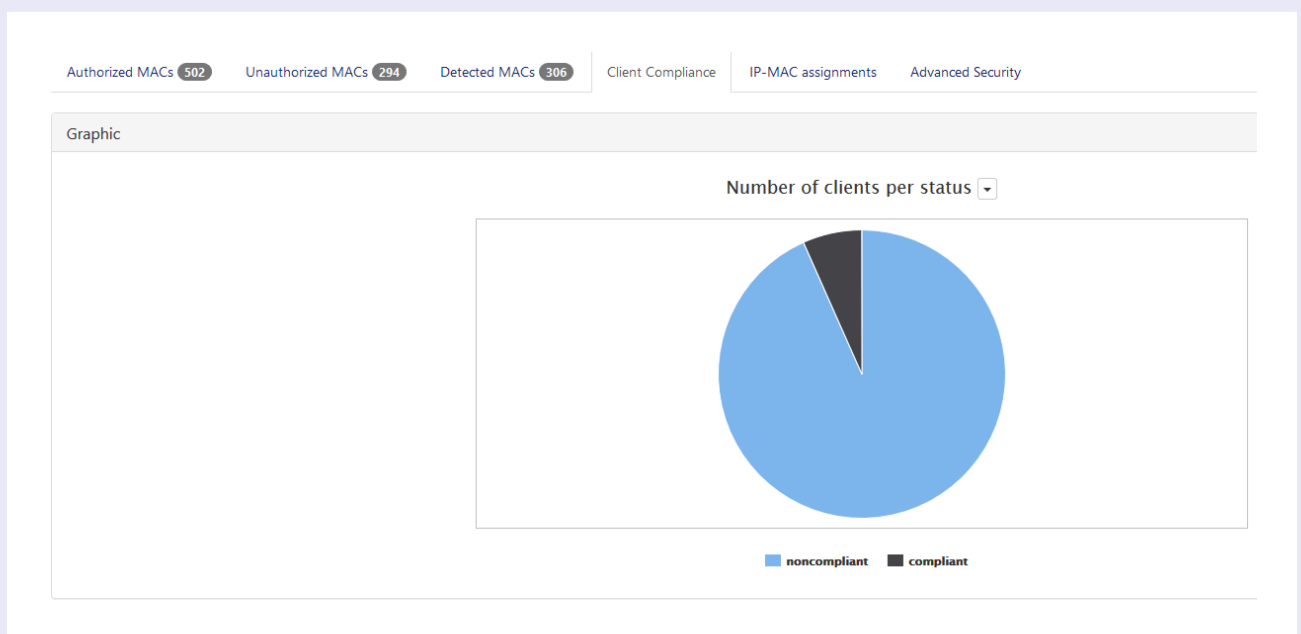


The status, the source and the reason of an endpoint are displayed in the report *Client Compliance*.



MAC	Last IP	Last DNS name	Host name (DHCP)	Group	Status	Source	Reason	MAC online	MAC in ARP	Change
D4-85-64-08-51-DD				PC	compliant	EgoSecure	Everything_ok_again			2018-03-08 17:42:38
00-00-71-00-00-77				Network	noncompliant	EgoSecure	Application			2018-03-08 17:42:38
00-0C-29-48-CC-23				Default	noncompliant	EgoSecure	Forbidden_Application			2019-02-08 16:10:28
00-0C-29-8C-42-22				Default	noncompliant	EgoSecure	"Unknown USB dongle"			2018-03-08 17:42:39
00-30-C1-0A-5B-C2				PC	noncompliant	EgoSecure	DE_unencrypted			2018-03-08 17:42:39
00-60-80-D5-58-00				PC	noncompliant	EgoSecure	DE_unencrypted			2018-03-08 17:42:39
00-60-80-E6-9E-07				PC	noncompliant	EgoSecure	AV			2018-03-08 17:42:39
00-A0-B8-00-00-90				Notebooks	noncompliant	EgoSecure	AC_Write_Access			2018-03-08 17:42:39
08-2E-5F-06-17-9E				PC	noncompliant	EgoSecure	AC_Write_Access			2018-03-08 17:42:38
08-2E-5F-08-82-76				PC	noncompliant	EgoSecure	Unallowed_camera_detected			2019-02-08 16:10:28
08-2E-5F-21-8F-07				PC	noncompliant	EgoSecure	Application			2018-03-08 17:42:38
10-60-48-85-58-86				PC	noncompliant	EgoSecure	AV			2018-03-08 17:42:38
24-BE-05-03-0C-B0				PC	noncompliant	EgoSecure	AV			2018-03-08 17:42:39
24-BE-05-1D-4A-C9				PC	noncompliant	EgoSecure	Any_Reason_Thinkable			2018-03-08 17:42:39
B4-85-2F-CC-92-69				PC	noncompliant	EgoSecure	Because_I_Want_It			2018-03-08 17:42:38

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