



MACMON NAC WHITE PAPER

Integration of macmon Compliance Module with McAfee ePO

Table of contents

Introduction

1. preparations

2. The script

3. Parameters & examples

4. ePO configuration

5. macmon configuration

Introduction

The macmon compliance module allows for the coupling of any compliance sources for the automated implementation of the security rules with macmon. This white paper explains in short and simple steps, how the Central Management of the McAfee security solutions (ePO) can be coupled with macmon Network Access Control. The configuration and usage can be applied to any other sources – with modifications.

1. Preparations

- The macmon compliance interface (macutil) requires an authentication via https. Any user created and active in macmon can be used for it (Administrator role on macmon is required).
- In order to invoke https commands via script, a third party tool (Wget in this example) is necessary on the executing system (ePO server).

<http://gnuwin32.sourceforge.net/packages/wget.htm>

- **The path to the installed Wget has to be later updated accordingly in the script!**

2. The script

The following example script calls Wget in the first step and uses the variables transferred by ePO, in order to resolve a client IP address into the corresponding MAC address. The result is saved to a text file (stored in the path of the script). In the second step, this MAC address is read again and another Wget call now modifies the compliance state of the target system with the variables transferred by ePO. In our example, we have named the script compliance.bat:

- %ProgramFiles(x86)%\GnuWin32\bin\wget.exe" --output-document=- --http-user=%1
--http-password=%2 --no-check-certificate --timeout=10 --tries=2
„https://%3/ macutil/?select=refmacs&C=[LAST_IP]='%4'“ >
macmon_compliance_temp.txt
set /p mac= < macmon_compliance_temp.txt
- „%ProgramFiles(x86)%\GnuWin32\bin\wget.exe" --output-document=- --http-user=%1
--http-password=%2 --no-check-certificate --timeout=10 --tries=2
https://%3/macutil/? compliance&address=%mac%&source=%5&reason=%6&status=%7

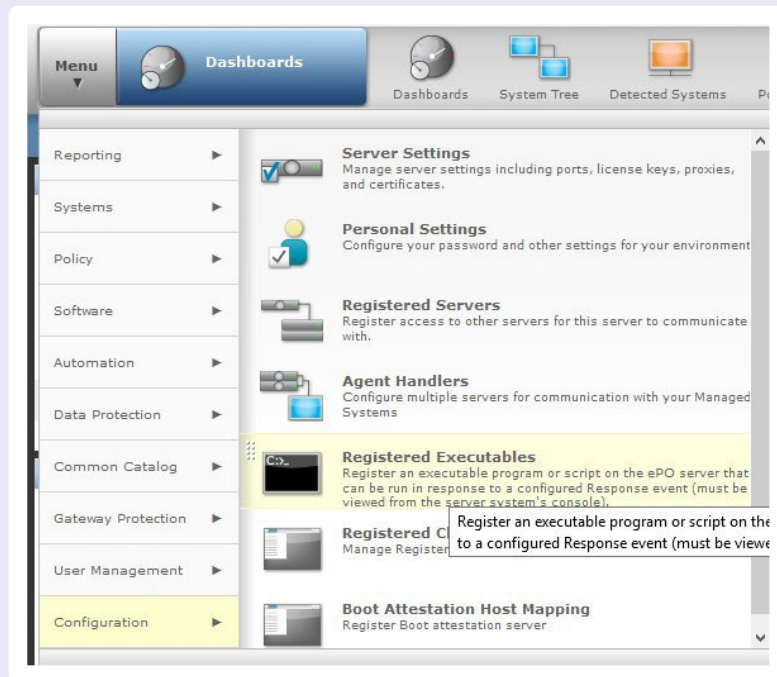
3. Parameters & examples:

compliance.bat macmonuser password macmonip targetclientipv4 source reason
status(noncompliant|compliant|te sting|almost_noncompliant|outdated)

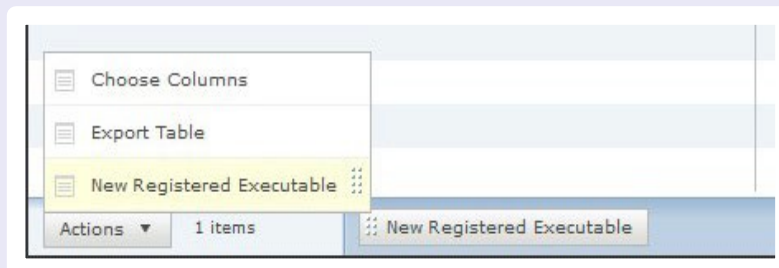
- compliance.bat admin macmon 192.168.1.190 %targetIPV4%
McAfee virus found noncompliant
- compliance.bat admin macmon 192.168.1.190 %targetIPV4%
Kaspersky unauthorised USB device noncompliant
- compliance.bat admin macmon 192.168.1.190 %targetIPV4%
WSUS missing system updates noncompliant
- compliance.bat admin macmon 192.168.1.190 %targetIPV4%
Astaro firewall deny rule noncompliant

4. ePO configuration:

Adding a registered executable file.



In the lower left side, under Actions, a new file can be created.



Edit Registered Executable	
Type the name and path of the registered executable.	
Name:	<input type="text" value="Macmon Script"/>
Path:	Old Path: E:\Install\Compliance.bat <input type="text" value="E:\Install\Compliance.bat"/>
Run As:	If it is necessary to run this Registered Executable as a specific user, provide the credentials here. Use for domain account. The user needs to have "Log on as a batch job" user rights. User Name: <input type="text" value="user@domain.com"/> Password: <input type="password" value="....."/> Confirm Password: <input type="password" value="....."/>
Test Executable:	To perform test run of this Registered Executable, enter any test parameters and click Run button. Arguments: <input type="text"/> Timeout (milliseconds): <input type="text" value="60000"/> <input type="button" value="Run"/>

A local administrator account on the ePO server is required for the execution of the specified script! The user has to be entered as specified, with user@domain.com. If needed, the execution can also be tested. You can check if everything works as desired under "Menu - User Management - Audit Log"

This executable file can now be executed as reaction to an incoming event. In the following example, it will be executed for each malware found which could not be deleted. In this case, variables need to be transferred to the script, so macmon can for instance move the correct system to quarantine.

An automatic answer has to be created:

Response Builder 1 Description 2 Filter 3 Aggregation

What is this response's name, target language, and event type? Is the response enabled?

Name:

Description:

Language:

Event: Event group:
Event type:

Available Properties	Property	Comparison	Value
▼ Threat			
Agent GUID			
Detected			
Detecting Product			
Detecting Product Dat V...			
Detecting Product Detec...			
Detecting Product Engin...			
Detecting Product Host ...			
	Required Criteria		
	Defined at	System is in group or subgroup	<input type="text" value="My Organization"/>
	Threat		
	Threat Category	Belongs to	<input type="text" value="Malware"/>
	and Threat Handled	Equals	<input type="text" value="False"/>

The trigger has to perform the check for each new event

Response Builder 1 Description 2 Filter 3 Aggregation

What kind of aggregation, grouping, and throttling behavior should this response have?

Aggregation: ☒ Trigger this response for every event.
☐ Trigger this response if multiple events occur within:
☐ When the number of distinct values for an event property is at least a certain value.
Property: Number of distinct values:
or
☐ When the number of events is at least:

Grouping: ☒ Do not group aggregated events.
☐ Group aggregated events by:

Throttling: ☐ At most, trigger this response once every:

If the event corresponds to the criteria, the macmon script has to be executed.

Response Builder
1 Description
2 Filter
3 Aggregation

What actions do you want this response to take when triggered?

▼ Run External Command ▼

Select a registered executable, and specify any arguments for it.

Registered executable: Macmon Script ▼

Arguments: macmonuser password Macmon-serverip {targetIPV4} Source(z.B. McAfee-EPO) Reason(e.g. Malware_detected) status(e.g.not_handled) noncompliant|compliant|testing|almost_noncompliant|outdated

Insert variable: Value ▼ Target IPV4 Address ▼ Insert

Timeout (milliseconds): 60000

Overview of the created configuration:

This can be performed for all threat events which are sent by the client to the ePO server.

Response Builder
1 Description
2 Filter
3 Aggregation


Please review the summary of the response below. If it is configured properly, click "Save". Otherwise, click "Back" to continue edit

Name:	Malware detected and not handled
Description:	
Language:	English
Event:	Event group: ePO Notification Events Event type: Threat
Status:	Enabled
Aggregation:	Trigger this response for every event.
Grouping:	Do not group aggregated events.
Throttling:	This response is not throttled.
Actions:	1: Externen Befehl ausführen

5. macmon configuration

Should one or another Endpoint not corresponding to the company's policy being detected, then the macmon responds to the security incident and will respectively changes compliance status of the corporate device.

















Hereby the standard set of rules takes effect, which automatically blocks the port or sets the VLAN stored under "Settings -> Scan Engine -> VLAN Management".



macmon Manage NAC policies (vertriebsdemo50) 2020-05-18 16:08:29 CEST Version 5.20.0-39585

Authentication Rules Permissions

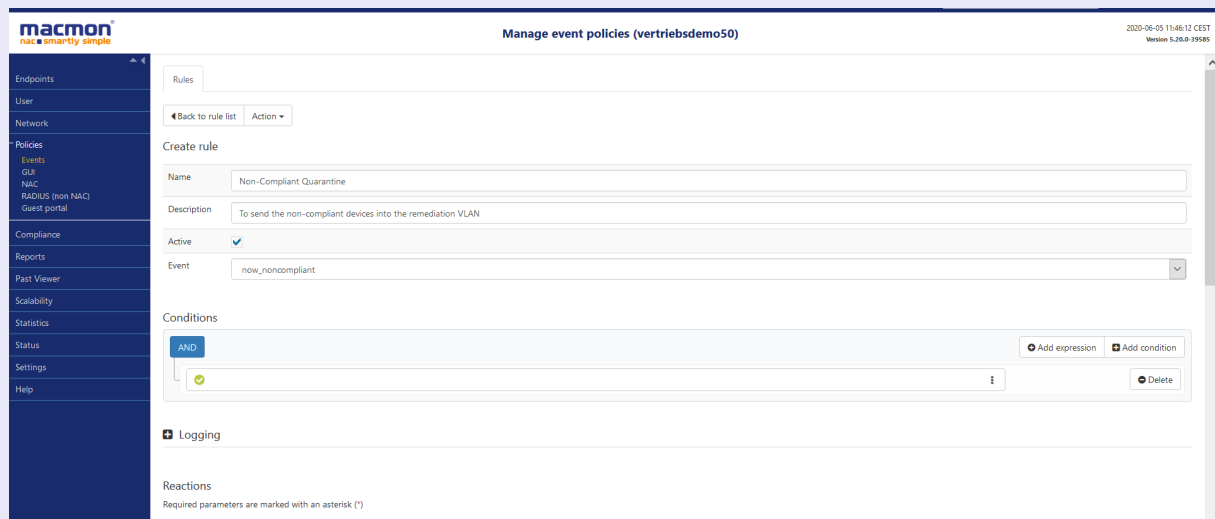
Add rule

Actions	Status	Name	Description	Result
   	active	Use guest vlan in meeting rooms	Meeting rooms only use the guest VLAN	1 Permission(s)
   	active	No NAC for the CEO	The CEO should never be handled via NAC. Standard authorization.	1 Permission(s)
Hide built-in rules				
   	active	Default rule for enforcement configuration of compliance. endpoints and endpoint groups.		
   	active	Move unknown and deactivated endpoints to unauthorized VLAN.		
   	active	Access deny		

The further reactions of macmon to the change of compliance status can be defined by using automatically generated events "now_noncompliant" and "now_compliant". The event "now_noncompliant" is triggered when a corporate device is assessed as non-compliant by a source and "now_compliant" when a non-compliant device becomes compliant again.

It's possible either to set an individual targeted VLAN for different scenarios – e.g. to differentiate between the source of compliance status – or to use the remediation_vlans already listed under menu "Settings -> Scan engine -> VLAN Management -> remediation_vlans".

As shown in the example below, a possible reaction to the event "now_noncompliant" could be the change of Authorized VLAN. This could be configured under "Policies -> Events -> Add rule"



macmon
nac smartly simple

Manage event policies (vertriebsdemo50)

2020-06-05 11:46:12 CEST
Version 5.20.0-39585

Rules

Back to rule list Action

Create rule

Name: Non-Compliant Quarantine

Description: To send the non-compliant devices into the remediation VLAN

Active: ☒

Event: now_noncompliant

Conditions

AND

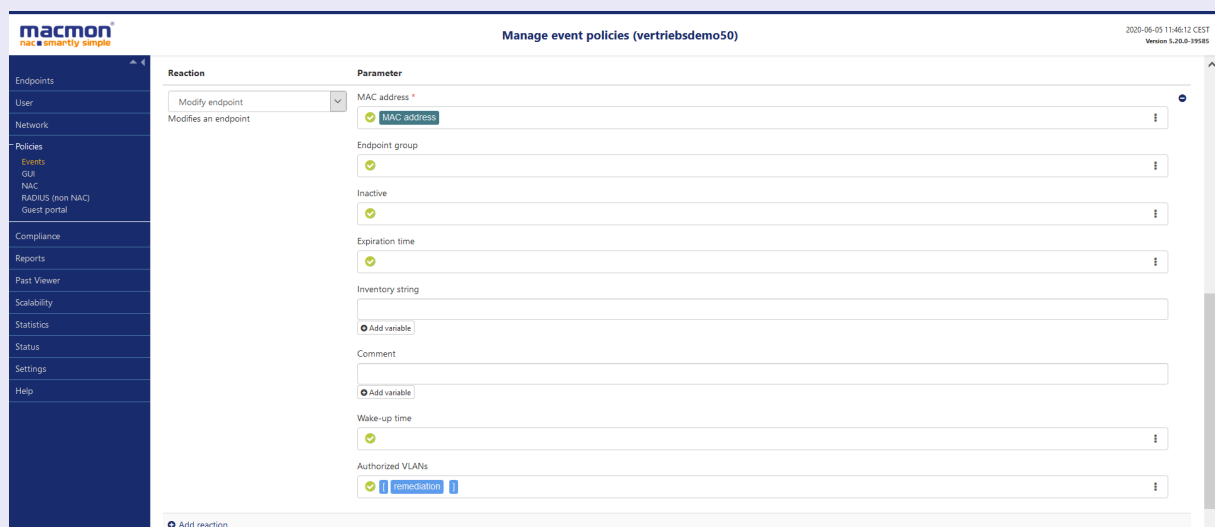
Add expression Add condition

Delete

Logging

Reactions

Required parameters are marked with an asterisk (*)



macmon
nac smartly simple

Manage event policies (vertriebsdemo50)

2020-06-05 11:46:12 CEST
Version 5.20.0-39585

Reaction

Modify endpoint

Modifies an endpoint

Parameter

MAC address *

MAC address

Endpoint group

Inactive

Expiration time

Inventory string

Add variable

Comment

Add variable

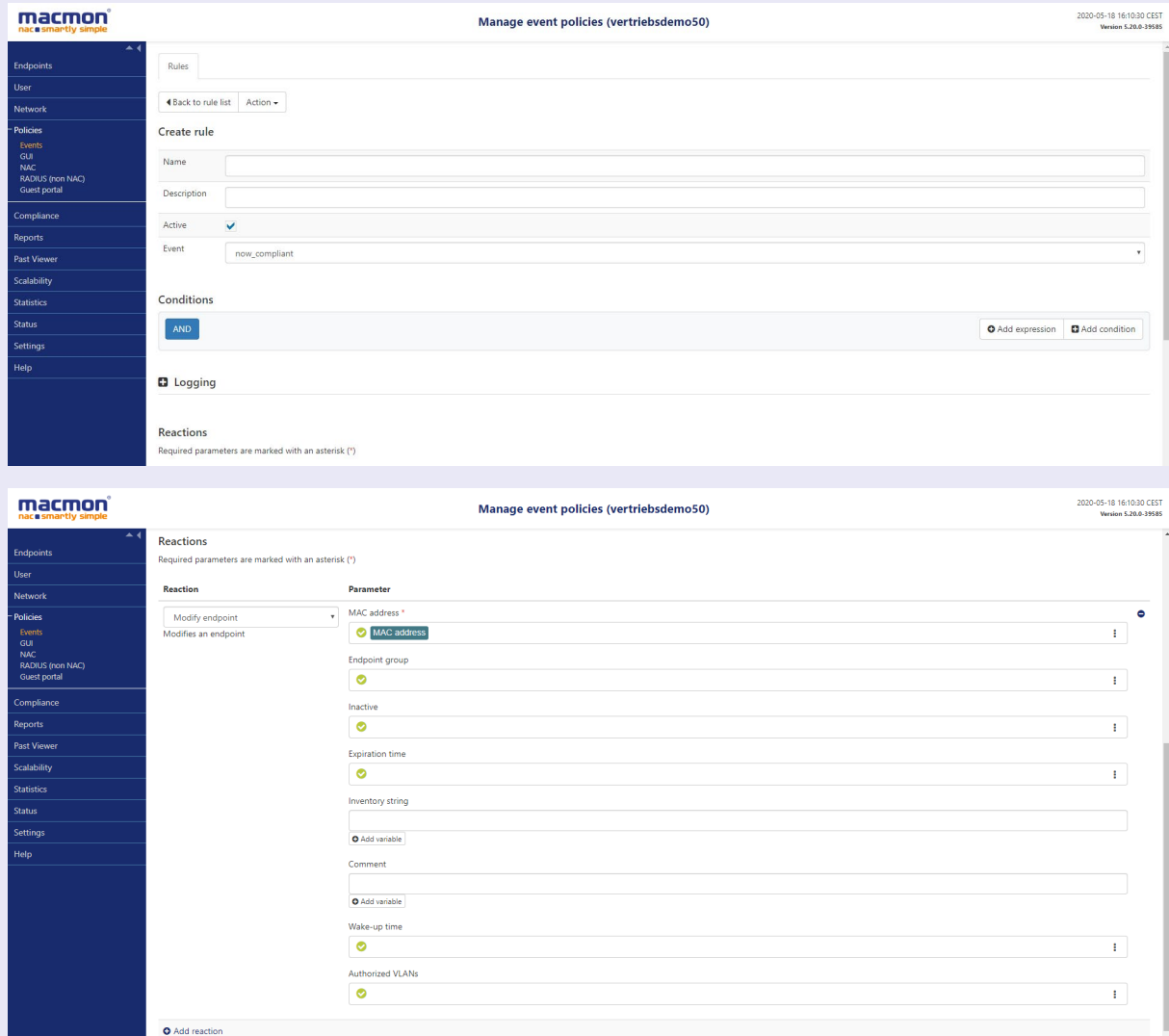
Wake-up time

Authorized VLANs

remediation

Add reaction

A respective configuration can also be done for the event "now_compliant", where the VLAN of affected MAC (previously noncompliant) can be removed, so the usual VLAN of MAC-Group can be active again.



The first screenshot shows the 'Create rule' form in the 'Manage event policies (vertriebsdemo50)' section. The form includes fields for Name, Description, Active status (checked), and Event (set to 'now_compliant'). Below the form are sections for 'Conditions' (with an 'AND' button and 'Add expression'/'Add condition' links) and 'Reactions' (with a 'Logging' button and a note that required parameters are marked with an asterisk). The second screenshot shows the 'Reactions' configuration table. It lists various parameters for the 'Modify endpoint' reaction, including MAC address, Endpoint group, Inactive status, Expiration time, Inventory string, Comment, Wake-up time, and Authorized VLANs. Each parameter has a dropdown menu and a 'MAC address' button. The table is titled 'Reactions' and includes a note that required parameters are marked with an asterisk. The 'Add reaction' button is at the bottom.

As a matter of course, the macmon configurations are also readily transferable for connecting to other security / compliance solutions. If several systems are connected, an additional differentiated reaction can also be attained by means of the "Source," variable under "Conditions" while creating a new event rule.

Done... McAfee and macmon can be coupled together in this easy manner.

We are happy to also support you in planning or in the direct integration of your existing solutions with our competent support team. Simply approach us.

Your macmon team

Contact

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