



MACMON NAC WHITEPAPER

Nutzung des macmon Compliance Moduls
in Verbindung mit dem McAfee ePO in 5 Schritten

Inhalt

Einleitung

1. Vorbereitungen
2. Das Script
3. Parameter & Beispiele
4. Konfiguration ePO
5. Konfiguration macmon

Einleitung

Das macmon compliance Modul erlaubt die Kopplung beliebiger Compliance-Quellen zur automatisierten Durchsetzung der Sicherheitsregeln mit macmon. In diesem Whitepaper wird in kurzen und einfachen Schritten erläutert, wie das zentrale Management der McAfee Security Lösungen (der ePO) mit macmon – Network Access Control gekoppelt wird. Die Konfiguration und die Nutzung sind auf beliebige weitere Quellen – modifiziert – anwendbar.

1. Vorbereitung

- Die macmon compliance Schnittstelle (macutil) erfordert eine Authentifizierung via https, dafür kann jeder bei macmon angelegte und aktive Benutzer verwendet werden (Administrator Rolle auf macmon erforderlich).
- Für den Aufruf von https-Kommandos via Script wird ein Drittanbieter-Tool (in unserem Beispiel Wget) auf dem ausführenden System (ePO-Server) benötigt.
<http://gnuwin32.sourceforge.net/packages/wget.htm>
- Der Pfad zum installierten Wget muss später im Script entsprechend angepasst werden!

2. Das Script

Das folgende Beispiel Script ruft im ersten Step Wget auf und nutzt die vom ePO übergebenen Variablen, um eine Client-IP-Adresse in die entsprechende MAC-Adresse aufzulösen. Das Ergebnis wird in einer Text-Datei gespeichert (wird im Pfad des Scripts abgelegt). Im zweiten Step wird diese MAC-Adresse wieder ausgelesen und ein weiterer Wget Aufruf ändert jetzt den Compliance-Status des Zielsystems mit den vom ePO übergebenen Variablen. In unserem Beispiel haben wir das Script Compliance.bat genannt:

- `%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`

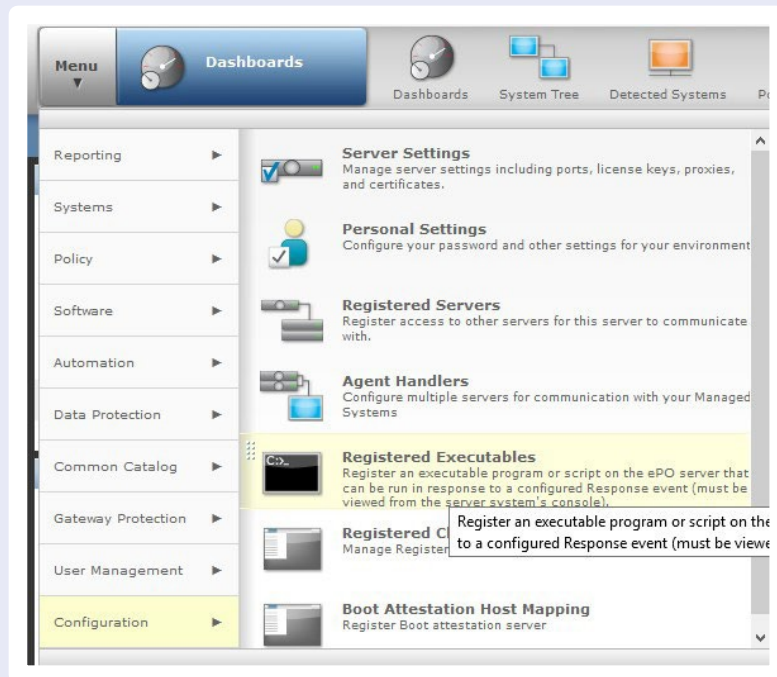
3. Parameter & Beispiele:

compliance.bat macmonuser password macmonip targetclientip4 source reason
status(noncompliant|compliant|te sting|almost_noncompliant|outdated)

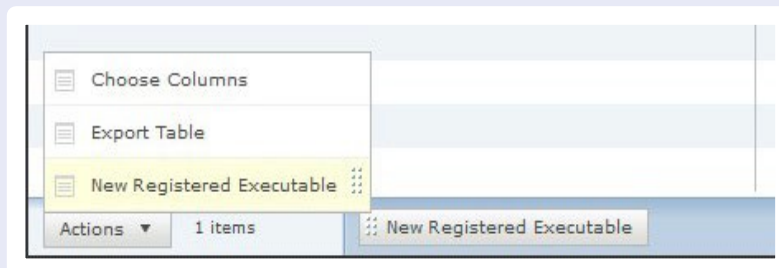
- `compliance.bat admin macmon 192.168.1.190 %targetIPV4%
McAfee Virenfund noncompliant`
- `compliance.bat admin macmon 192.168.1.190 %targetIPV4%
Kaspersky Unerlaubtes-USB-Device noncompliant`
- `compliance.bat admin macmon 192.168.1.190 %targetIPV4%
WSUS Fehlende-Systemupdates noncompliant`
- `compliance.bat admin macmon 192.168.1.190 %targetIPV4%
Astaro Firewall-Deny-Regel noncompliant`

4. Konfiguration ePO:

Hinzufügen einer registrierten ausführbaren Datei.



Unten Links unter Aktionen kann eine neue Datei angelegt werden.



Edit Registered Executable

Type the name and path of the registered executable.

Name:

Macmon Script

Path:

Old Path: E:\Install\Compliance.bat
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: user@domain.com
Password:
Confirm Password:

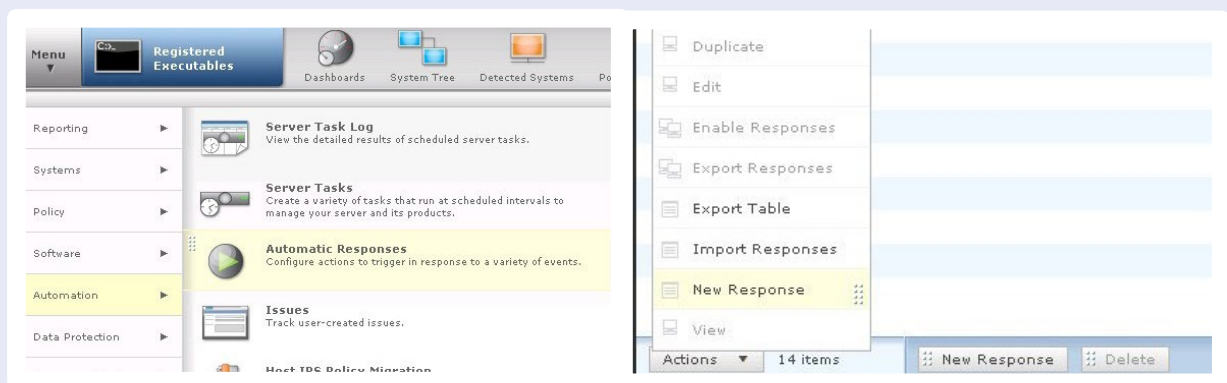
Test Executable:

To perform test run of this Registered Executable, enter any test parameters and click Run button.
Arguments:
Timeout (milliseconds): 60000
Run

Zur Ausführung des angegebenen Scripts wird ein lokaler Administrator auf dem ePO-Server benötigt! Dieser muss wie angegeben mit Benutzer@domäne.de eingetragen werden. Bei Bedarf kann die Ausführung auch getestet werden. Ob das alles nach Wunsch funktioniert, lässt sich unter „Menü – Benutzerverwaltung – Audit Protokoll“ überprüfen.

Diese ausführbare Datei lässt sich nun als Reaktion auf ein eintreffendes Ereignis ausführen. In folgendem Beispiel wird es bei jeder gefundenen Malware, die nicht gelöscht werden konnte, ausgeführt. Dabei müssen Variablen an das Script übergeben werden, damit macmon das richtige System in z.B. Quarantäne versetzt.

Es muss eine automatische Antwort angelegt werden:



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	My Organization
	Threat		
	Threat Category	Belongs to	Malware
	and Threat Handled	Equals	False

Der Trigger soll bei jedem neuen Event die Prüfung durchführen.

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:

Wenn das Event den Kriterien entspricht, soll das macmon Script ausgeführt werden.

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

Übersicht der erstellten Konfiguration:

Dies kann für alle Bedrohungs-Ereignisse, die vom Client an den ePO-Server gesendet werden, durchgeführt werden.

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. Konfiguration macmon

Sollte der eine oder andere Endpunkt nicht der erkannten Unternehmensrichtlinie entsprechen, reagiert macmon auf den Sicherheitsvorfall und ändert den Compliance-Status des Unternehmensgeräts.

Hierdurch greift bereits das Standardregelwerk, welches automatisch den Port sperrt, oder das unter „Einstellungen“ → „Scan Engine“ hinterlegte VLAN schaltet.

The screenshot displays the macmon web interface for managing NAC policies. The sidebar on the left contains a menu with items such as 'Endgeräte', 'Benutzer', 'Netzwerk', 'Richtlinien', 'Compliance', 'Berichte', 'Past Viewer', 'Skalierbarkeit', 'Statistiken', 'Status', 'Einstellungen', and 'Hilfe'. The main area is titled 'NAC-Richtlinien verwalten (vertriebsdemo50)' and features tabs for 'Authentifizierung', 'Regeln', and 'Berechtigungen'. Below the tabs, there is a 'Regel hinzufügen' button and a table of existing rules. The table has columns for 'Aktionen', 'Status', 'Name', 'Beschreibung', and 'Ergebnis'. One rule is highlighted with a green border: 'Standardregel für die Enforcement-Konfigurationen von Compliance. Endgeräte und Endgerätegruppen'.

Aktionen	Status	Name	Beschreibung	Ergebnis
	aktiv	Use guest vlan in meeting rooms	Meeting rooms only use the guest VLAN	1 Berechtigung(en)
	aktiv	No NAC for the CEO	The CEO should never be handled via NAC. Standard authorization.	1 Berechtigung(en)
Interne Regeln verstecken				
	aktiv	Standardregel für die Enforcement-Konfigurationen von Compliance. Endgeräte und Endgerätegruppen		
	aktiv	Verschiebe unbekannte oder deaktivierte Endgeräte ins VLAN für unautorisierte Endgeräte.		
	aktiv	Zugang verweigern		

Weitere Reaktionen von macmon auf die Änderung des Compliance-Status können mithilfe der automatisch generierten Ereignisse "now_noncompliant" und "now_compliant" definiert werden. Das Ereignis "now_noncompliant" wird ausgelöst, wenn ein Unternehmensgerät von einer Quelle als nicht richtlinienkonform eingestuft wird, und "now_compliant", wenn ein solches Gerät den Unternehmensrichtlinien wieder entspricht.

Um differenziert auf bestimmte Compliance-Stati (z.B. wegen anderer „Quelle“) zu reagieren, nutzt man zusätzlich zur internen Standardregel eine oder mehrere Ereignis-Regeln analog der hier dargestellten Regel, setzt jedoch keinen Wert für das Feld „remediation_vlans“ in den Einstellungen. Hiermit wird ein VLAN direkt an der MAC hinterlegt, welche eine höhere Priorität hat, als das MAC-Gruppen-VLAN.

macmon nac intelligent einfach Richtlinien für Ereignisse verwalten (vertriebsdemo50) 2020-05-19 10:10:51 CEST Version 5.20.0-39185

- Endgeräte
- Benutzer
- Netzwerk
- Richtlinien**
 - Ereignisse
 - Benutzeroberfläche
 - NAC
 - RADIUS (ohne NAC)
 - Gästeportal
- Compliance
- Berichte
- Past Viewer
- Skalierbarkeit
- Statistiken
- Status
- Einstellungen
- Hilfe

Regeln

◀ Zur Regelliste Aktion ▶

Regel erstellen

Name

Beschreibung

Aktiv ☒

Ereignis

Bedingungen

UND Ausdruck hinzufügen Bedingung hinzufügen

Logging

Reaktionen

Benötigte Parameter sind mit einem Stern markiert (*)

macmon nac intelligent einfach Richtlinien für Ereignisse verwalten (vertriebsdemo50) 2020-05-19 10:10:51 CEST Version 5.20.0-39185

- Endgeräte
- Benutzer
- Netzwerk
- Richtlinien**
 - Ereignisse
 - Benutzeroberfläche
 - NAC
 - RADIUS (ohne NAC)
 - Gästeportal
- Compliance
- Berichte
- Past Viewer
- Skalierbarkeit
- Statistiken
- Status
- Einstellungen
- Hilfe

Reaktionen

Benötigte Parameter sind mit einem Stern markiert (*)

Reaktion	Parameter
Endgerät ändern	MAC-Adresse *
Ändern eines Endgerätes	MAC-Adresse
	Endgerätegruppe
	Inaktiv
	Gültigkeit
	Inventar Text
	Variable hinzufügen
	Kommentar
	Variable hinzufügen
	Aufweckzeit
	Autorisierte VLANs
	noncompliant_vlan

Reaktion hinzufügen

Mit der unten gezeigten Regel wird anhand des „now_compliant“ Ereignisses das VLAN, welches direkt an der MAC konfiguriert wurde wieder entfernt und das MAC-Gruppen-VLAN wird wieder aktiv.

macmon
nac intelligent einfach

Richtlinien für Ereignisse verwalten (vertriebsdemo50) 2020-05-19 10:32:14 CEST
Version 5.20.0-39585

Endgeräte
Benutzer
Netzwerk
Richtlinien
Ereignisse
Benutzeroberfläche
NAC
RADIUS (ohne NAC)
Gästportal
Compliance
Berichte
Past Viewer
Skalierbarkeit
Statistiken
Status
Einstellungen
Hilfe

Regeln

Zur Regelliste Aktion

Regel erstellen

Name

Beschreibung

Aktiv ☒

Ereignis now_compliant

Bedingungen

UND

Ausdruck hinzufügen Bedingung hinzufügen

Logging

Reaktionen

Benötigte Parameter sind mit einem Stern markiert (*)

macmon
nac intelligent einfach

Richtlinien für Ereignisse verwalten (vertriebsdemo50) 2020-05-19 10:32:14 CEST
Version 5.20.0-39585

Endgeräte
Benutzer
Netzwerk
Richtlinien
Ereignisse
Benutzeroberfläche
NAC
RADIUS (ohne NAC)
Gästportal
Compliance
Berichte
Past Viewer
Skalierbarkeit
Statistiken
Status
Einstellungen
Hilfe

Reaktionen

Benötigte Parameter sind mit einem Stern markiert (*)

Reaktion	Parameter
Endgerät ändern	MAC-Adresse *
Ändern eines Endgerätes	MAC-Adresse
	Endgerätegruppe
	Inaktiv
	Gültigkeit
	Inventar Text
	Variable hinzufügen
	Kommentar
	Variable hinzufügen
	Aufweckzeit
	Autorisierte VLANs

Reaktion hinzufügen

Selbstverständlich sind die macmon-Konfigurationen auch für die Anbindung mit anderen Sicherheits- / Compliance-Lösungen leicht übertragbar. Wenn mehrere Systeme verbunden sind, kann eine zusätzliche differenzierte Reaktion auch über die Variable „Quelle“ unter „Bedingungen“ erreicht werden, während eine neue Ereignisregel erstellt wird.

Fertig ... McAfee und macmon können auf diese einfache Weise miteinander kommunizieren.

Gern unterstützen wir Sie auch bei der Planung bzw. der direkten Integration Ihrer bestehenden Lösungen mit unserem kompetenten Support Team. Kommen Sie einfach auf uns zu.

Ihr macmon-Team

Kontakt

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