



# MACMON NAC WHITEPAPER

## Integration von macmon NAC mit Greenbone Security Manager

## Inhaltsverzeichnis

Einleitung .....	3
Anwendungsfälle .....	3
macmon NAC erkennt ein neues Endgerät und lässt es von GSM scannen .....	3
macmon NAC erkennt ein wiederkehrendes Endgerät und lässt es von GSM scannen .....	3
macmon NAC überprüft regelmäßig die Integrität aller Endgeräte .....	3
Konfiguration in macmon NAC .....	4
Konfiguration der <i>Greenbone Security Manager</i> -Integration .....	4
Konfiguration in Greenbone Security Manager .....	7
Konfiguration des GMP-Service .....	7
Unterstützte Versionen .....	10
Kontakt bei Greenbone .....	10

## Einleitung

Der Greenbone Security Manager (GSM) von Greenbone Networks identifiziert Sicherheitslücken in der Unternehmens-IT und bewertet deren Risikopotenzial. Zudem empfiehlt der GSM Maßnahmen zur Behebung gefundener Schwachstellen. Ziel ist, Angriffspunkte vor den Cyberkriminellen zu erkennen und Angriffe zu verhindern. Denn die Praxis zeigt: 999 von 1000 ausgenutzten Schwachstellen waren bereits über 12 Monate bekannt. Zur Lösung gehört ein tägliches Security-Update mit über 56.000 Netzwerk-Schwachstellen-Tests. Die schlüsselfertige Appliance-Lösung basiert auf Open Source Software und lässt sich innerhalb von 10 Minuten in Betrieb nehmen. Das private Unternehmen mit Sitz in Osnabrück wurde 2008 von führenden Experten aus den Bereichen Netzwerksicherheit und Open Source gegründet.

## Anwendungsfälle

### macmon NAC erkennt ein neues Endgerät und lässt es von GSM scannen

In einem Unternehmensnetzwerk gibt es ständig neue Geräte. Gewöhnlich stellt ein Netzwerkadministrator sicher, dass ein solches Endgerät nicht mit Schadcode infiziert und damit eine Gefahr für die Datenintegrität und die Netzwerksicherheit ist. macmon NAC erkennt ein neues Endgerät, wenn es mit dem Netzwerk verbunden wird und beauftragt GSM mit einem Scan. Das Ergebnis dieses Scans wird von GSM bereitgestellt: Wenn das Gerät im Einklang mit den Unternehmensrichtlinien steht, wird der Netzwerkzugang weiterhin gewährt. Ist dies nicht der Fall, kann macmon NAC mit einer konfigurierten Reaktion das Endgerät isolieren und den Administrator benachrichtigen.

### macmon NAC erkennt ein wiederkehrendes Endgerät und lässt es von GSM scannen

Einige Endgeräte können nicht regelmäßig gescannt werden, weil sie nicht dauerhaft ans Unternehmensnetzwerk angeschlossen sind. Beispielsweise kann eine Mitarbeiterin im Außendienst für Tage oder Wochen außer Haus sein. Kommt diese zurück ins Büro und verbindet ihr Endgerät erneut mit dem Unternehmensnetzwerk, erkennt macmon dies und beauftragt GSM mit einem Scan. Das Ergebnis dieses Scans wird von GSM bereitgestellt: Wenn das Gerät im Einklang mit den Unternehmensrichtlinien steht, wird der Netzwerkzugang weiterhin gewährt. Ist dies nicht der Fall, kann macmon NAC mit einer konfigurierten Reaktion das Endgerät isolieren und den Administrator benachrichtigen.

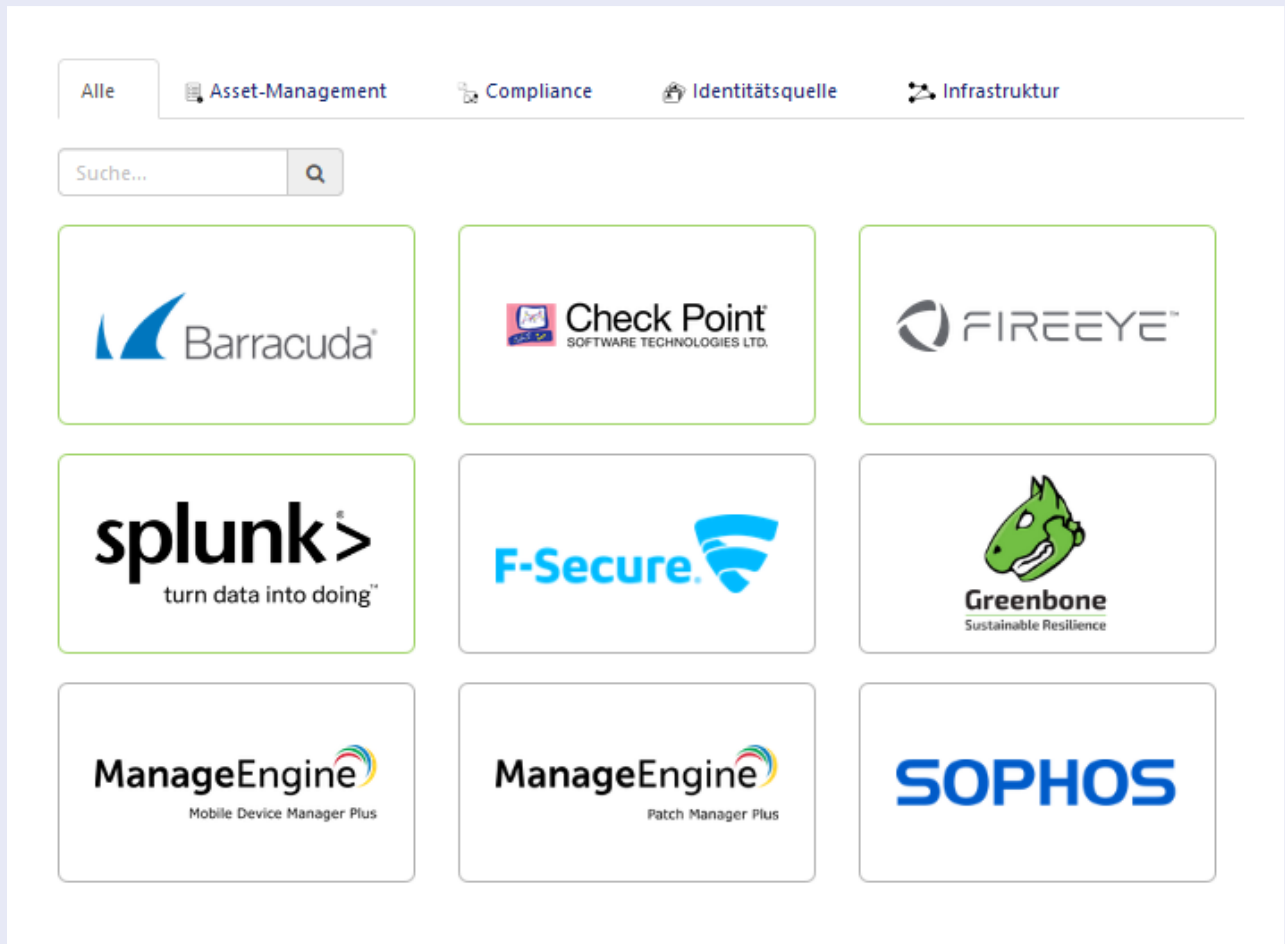
### macmon NAC überprüft regelmäßig die Integrität aller Endgeräte

Es ist wichtig, das Unternehmensnetzwerk regelmäßig zu scannen. Das Ergebnis dieses Scans wird von GSM bereitgestellt und in regelmäßigen Abständen von macmon NAC ausgewertet. Wenn das Gerät im Einklang mit den Unternehmensrichtlinien steht, wird der Netzwerkzugang weiterhin gewährt. Ist dies nicht der Fall, kann macmon NAC mit einer konfigurierten Reaktion das Endgerät isolieren oder gar vom Netzwerk trennen und den Administrator benachrichtigen.

## Konfiguration in macmon NAC

### Konfiguration der *Greenbone Security Manager*-Integration

Die Konfiguration wird über die Web-GUI vorgenommen. Wählen Sie dazu bitte *Einstellungen* und *Drittanbieter-Integrationen*, danach den Tab *Compliance*.



Wenn der Rahmen der *Greenbone Security Manager*-Kachel grau ist, ist die Integration noch nicht aktiviert. Bitte tippen Sie auf die Kachel, um den Konfigurationsdialog aufzurufen.

1. Geben Sie zunächst den *Hostnamen* oder die *IP-Adresse* und den *SSH-Port* ein, unter der Ihre Installation von *Greenbone Security Manager* erreichbar ist.

### Konfiguration für Greenbone Security Manager bearbeiten ×

---

► Beschreibung

---

#### Konfiguration

---

Hostname/IP-Adresse \*

Hostname/IP-Adresse von Greenbone Security Manager

Port \*

SSH-Port von Greenbone Security Manager

2. Im nächsten Abschnitt geben Sie den *Benutzernamen* und das *Passwort* ein, das nötig ist, um sich via SSH mit Greenbone Security Manager zu verbinden. Diese Verbindung ist zunächst nötig, um überhaupt im nächsten Schritt eine Verbindung zur API herzustellen. Die Zugangsdaten für den SSH- und API-Zugang können verschieden sein.
3. Danach geben Sie den *API-Benutzernamen* und das *API-Passwort* ein, womit die API-Verbindung über das Protokoll GMP hergestellt werden kann. Damit der Compliance-Status festgelegt wird, setzen Sie den Haken bei *Compliance-Status setzen*.

Benutzername \*

SSH-Benutzername für Greenbone Security Manager

Passwort \*

SSH-Passwort für Greenbone Security Manager

API-Benutzername \*

API-Benutzername für Greenbone Security Manager

API-Passwort \*

API-Passwort für Greenbone Security Manager

Compliance-Status setzen

Definiert, ob der Compliance-Status eines Endgeräts gesetzt werden soll

4. In *Grenzwert für Schweregrad* bestimmen Sie auf einer Skala von 0.0 bis 10.0, ab wann ein Endgerät in der Datenbank von Greenbone Security Manager als *noncompliant* erachtet werden soll, nachdem es auf Schwachstellen untersucht wurde. Setzen Sie den Haken bei *Neue*

*Unternehmensgeräte scannen*, wenn neue oder wiederkehrende Endgeräte im Netzwerk gescannt werden sollen. Der Wert in *Maximaler Zeitraum seit dem letzten Scanzeitpunkt* bestimmt, nach welcher Zeit das besagte Endgerät erneut gescannt werden soll.

Grenzwert für Schweregrad \*

Wenn der konfigurierte Grenzwert (Bereich: 0,0-10,0) überschritten wird, wird der Compliance-Status des Endgeräts auf noncompliant gesetzt.

Neue Unternehmensgeräte scannen

Wenn aktiv, wird ein neues Unternehmensgerät gescannt, sobald es ans Unternehmensnetzwerk angeschlossen wird.

Maximaler Zeitraum seit dem letzten Scanzeitpunkt. \*

Wenn der konfigurierte Zeitraum in Tagen (Bereich: 1-31) überschritten wird, wird das Unternehmensgerät erneut gescannt.

5. In *Intervall* geben Sie ein, wie oft (in Minuten) Daten von *Greenbone Security Manager* abgefragt werden sollen.

Intervall \*

Intervall in Minuten (Bereich: 1-59), in dem Daten von Greenbone Security Manager abgefragt werden.

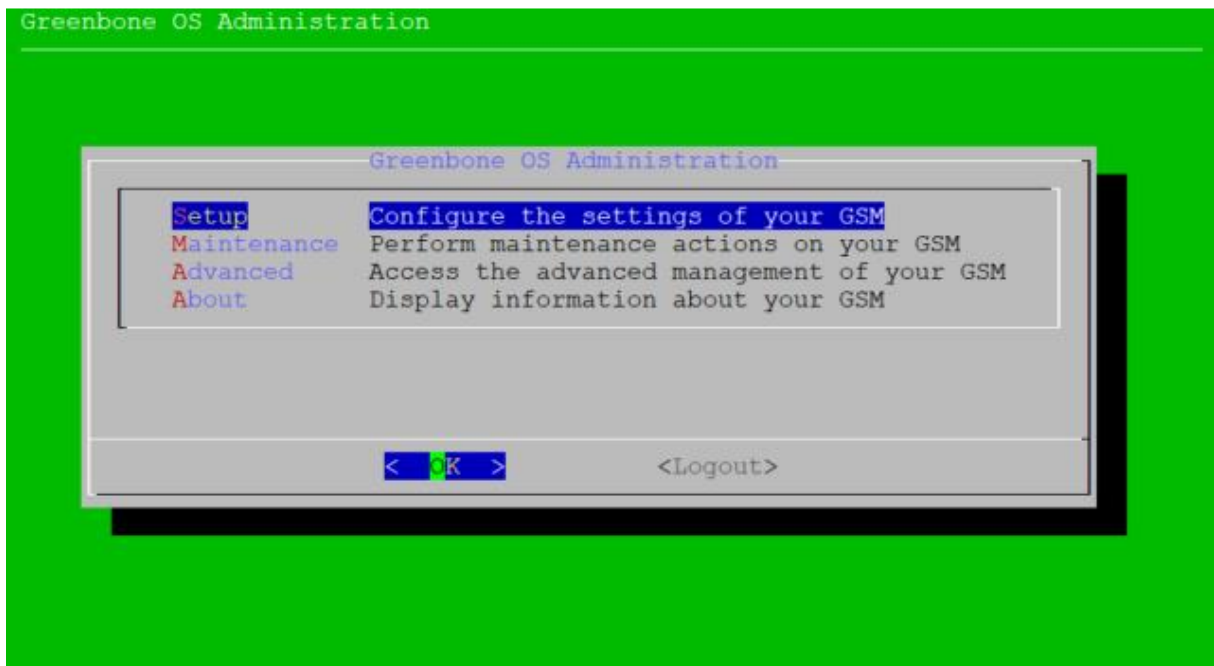
Aktiv

6. Aktivieren Sie die Integration durch Setzen des Hakens der Checkbox *Aktiv* und schließen Sie die Konfiguration durch Drücken von *Ok* ab.

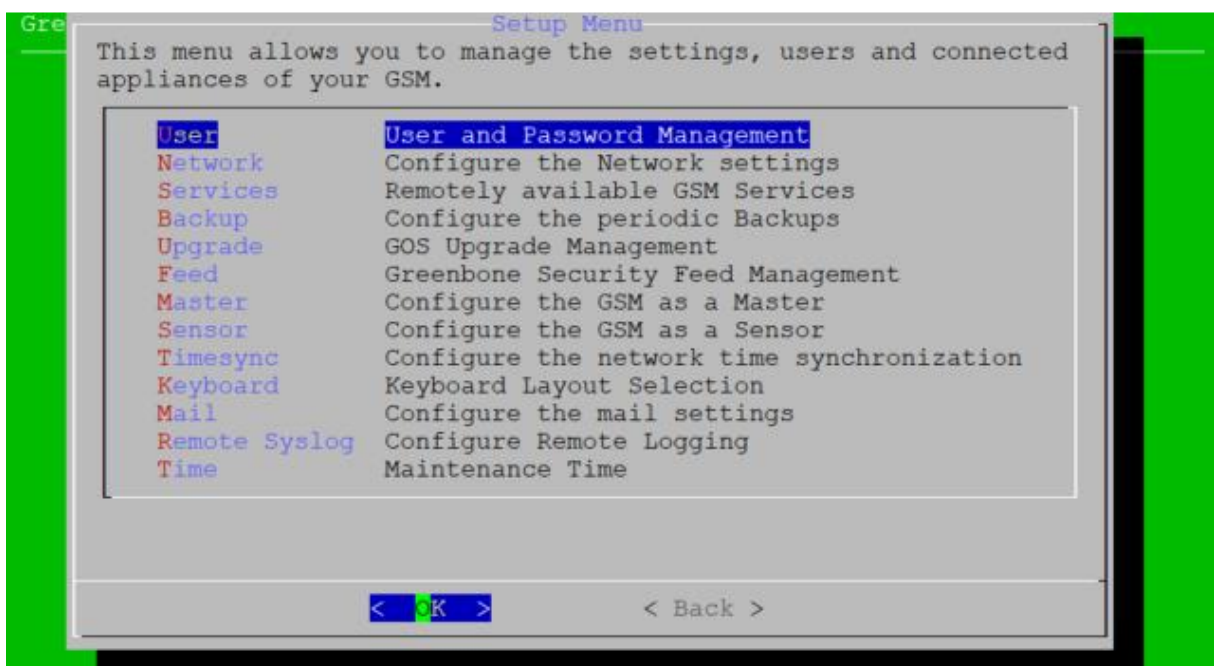
## Konfiguration in Greenbone Security Manager

### Konfiguration des GMP-Service

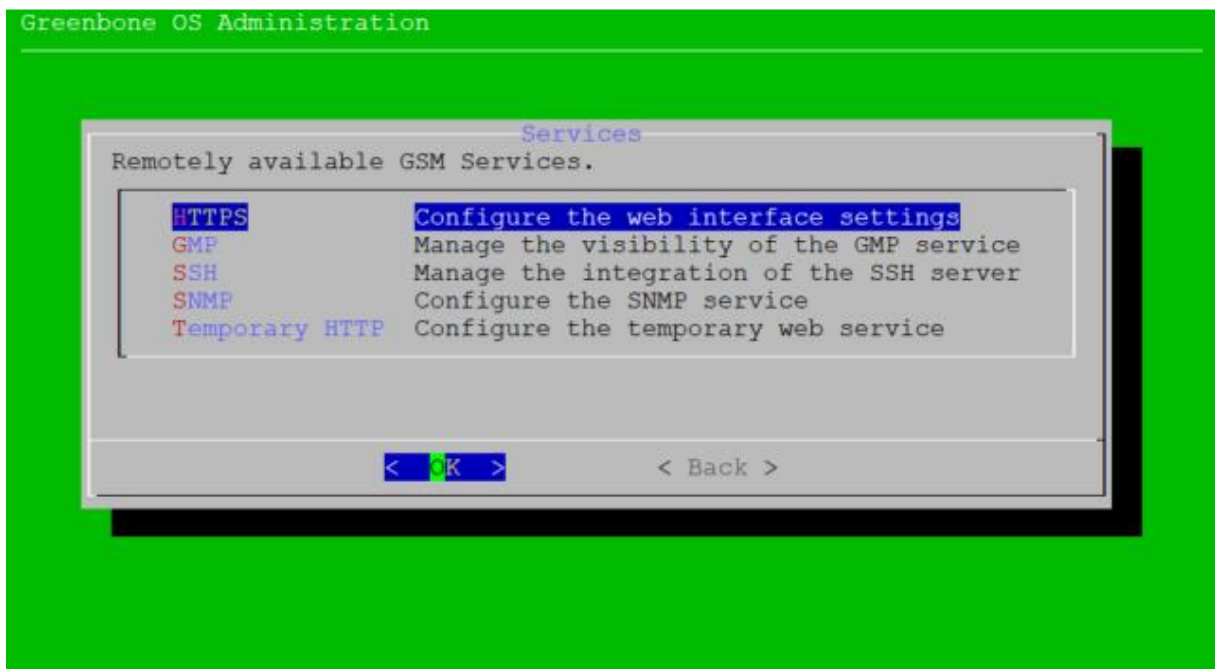
1. Loggen Sie sich in die Oberfläche von Greenbone OS Administration ein, indem Sie die gewöhnlichen SSH-Anmeldedaten verwenden. Nach einer erfolgreichen Anmeldung erscheint der Willkommensbildschirm.



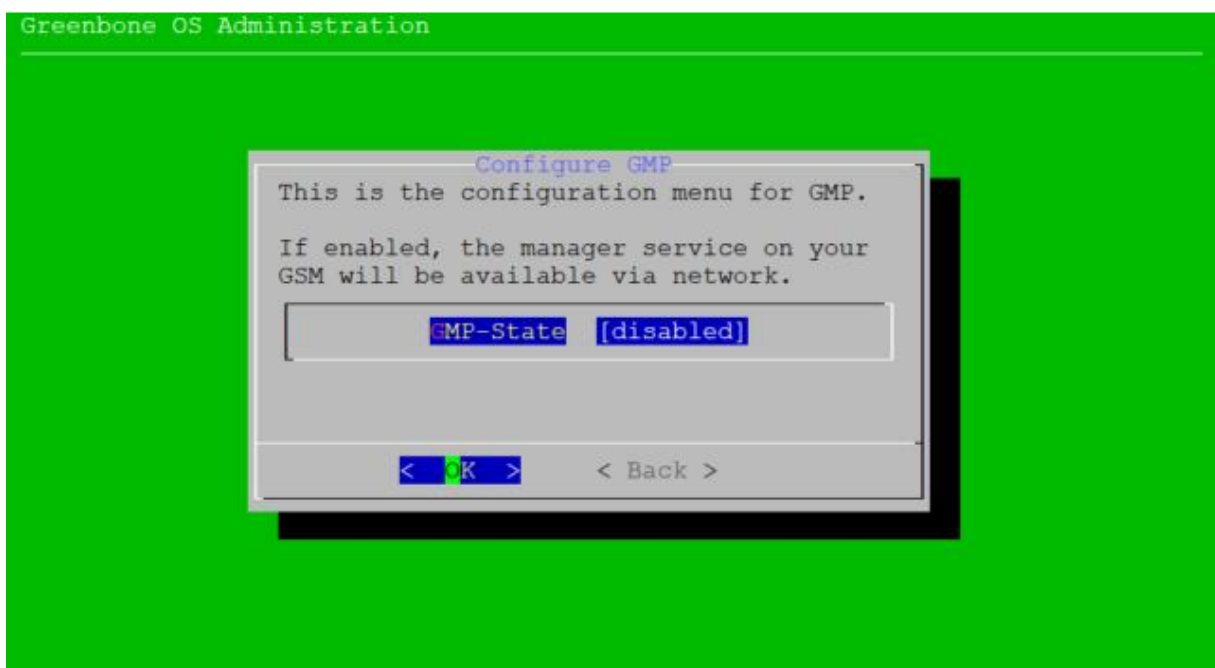
2. Im Willkommensbildschirm wählen Sie *Setup*.



3. Danach wählen Sie *User*.



4. Wählen Sie als Nächstes *GMP*.



5. Um den GMP-Dienst anzuschalten, betätigen Sie die Leertaste.

Greenbone OS Administration

Configure GMP

This is the configuration menu for GMP.

If enabled, the manager service on your GSM will be available via network.

GMP-State	[enabled]
-----------	-----------

Save Save the pending modifications

< OK >      < Back >

6. Danach wählen Sie *Save* und betätigen Sie die Enter-Taste.

Greenbone OS Administration

Configure GMP

This is the configuration menu for GMP.

If enabled, the manager service on your GSM will be available via network.

GMP-State	[enabled]
-----------	-----------

< OK >      < Back >

7. Um die Konfiguration abzuschließen, wählen Sie *Back*.

## Unterstützte Versionen

macmon, ab Version 5.25.0 mit der Lizenz *Premium Bundle*

Greenbone Security Manager, ab Version 6.0.12

## Kontakt bei Greenbone

Wenn Sie Fragen haben, kontaktieren Sie Greenbone bitte unter [support@greenbone.net](mailto:support@greenbone.net)

### Kontakt

macmon secure GmbH

Alte Jakobstraße 79-80 | 10179 Berlin

Tel.: +49 30 2325777-0 | [nac@macmon.eu](mailto:nac@macmon.eu) | [www.macmon.eu](http://www.macmon.eu)