Greenbone
Sustainable Resilience

macmon
nac smartly simple

MACMON NAC WHITEPAPER

Integration of macmon NAC with Greenbone Security Manager

Contents

Version: 1.2_en

Introduction

The Greenbone Security Manager (GSM) developed by Greenbone Networks identifies security vulnerabilities in enterprise IT and evaluates the risk potential. Furthermore, the GSM recommends measures to resolve detected vulnerabilities. The goal is to find weaknesses before cyber criminals do and to prevent attacks. 999 out of 1000 exploited vulnerabilities had already been known more than 12 months prior to the attack. A daily security update with over 56,000 network vulnerability tests is part of the solution. The turnkey appliance solution is based on open source software and can be implemented within 10 minutes. The privately owned company was founded in 2008 by leading network security and open source experts. It is located in Osnabrück, Germany.

Use Cases

macmon NAC detects a new endpoint and have GSM scan it

There are always new corporate devices, a so-called endpoint, on the corporate network. A network administrator usually wants to make sure that a new endpoint is not infected by malicious code and thus not a threat to the data integrity and overall security. macmon NAC detects a new endpoint when it is connected to the network and requests GSM to scan it right away. GSM in turn will pass the information about its findings on to macmon NAC. If the endpoint was found to be in perfect condition, network access will be granted. If not, macmon NAC will respond with a predefined configured reaction that could either isolate the endpoint in order to remediate the situation or disconnect it from the network.

macmon NAC detects a recurring endpoint and have GSM scan it

Some endpoints cannot be scanned periodically because they are not always connected to the network. A road warrior, for example, might be out of office for some days or even weeks. Once they get back to the office they connect their corporate device to the network. macmon NAC detects a recurring endpoint when it is connected to the network and requests GSM to scan it right away. GSM in turn will pass the information about its findings on to macmon NAC. If the endpoint was found to be in perfect condition, network access will be granted. If not, macmon NAC will respond with a predefined configured reaction that could either isolate the endpoint in order to remediate the situation or disconnect it from the network.

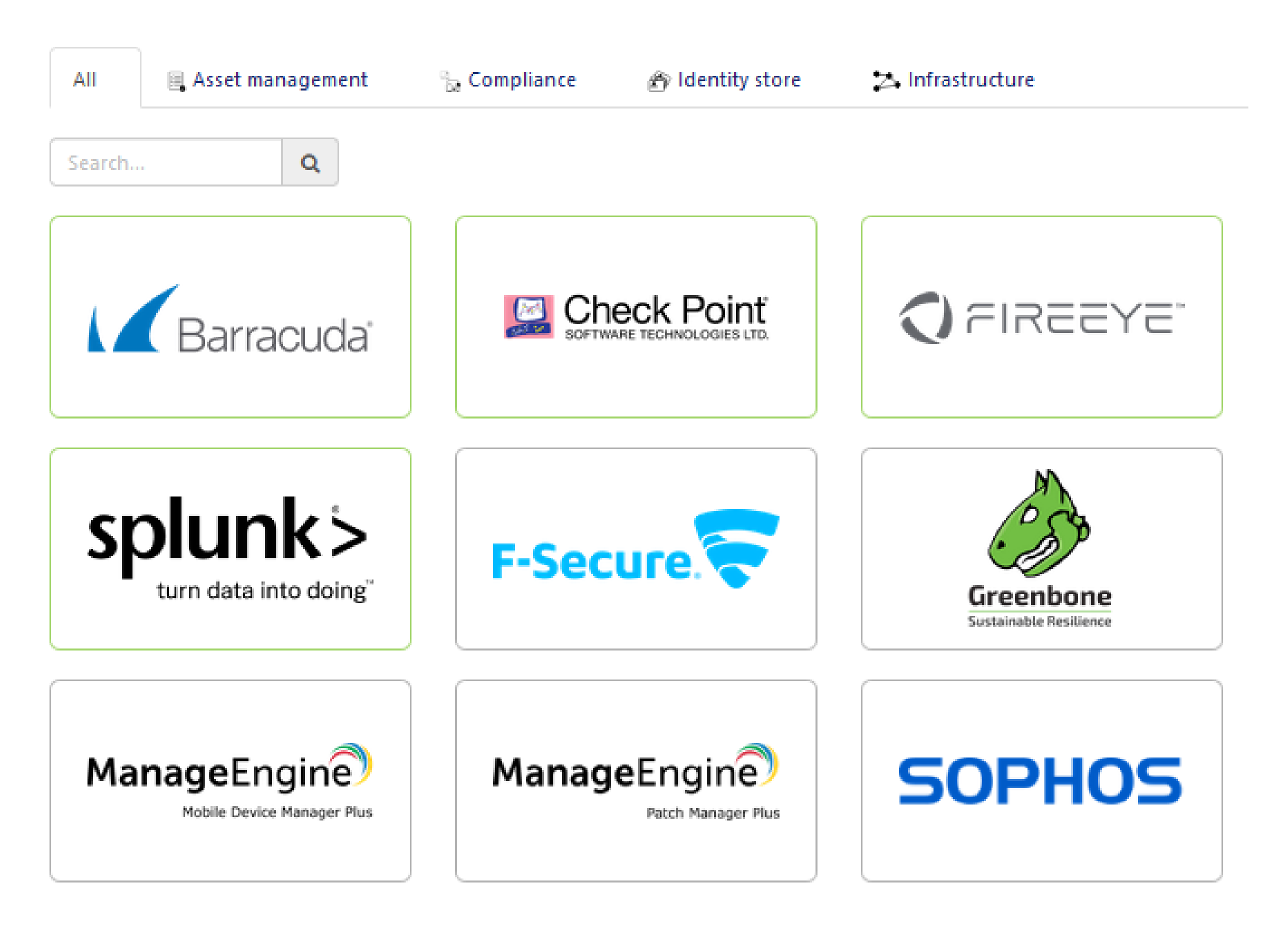
macmon NAC checks the endpoints’ integrity periodically

Having the corporate network scanned periodically is key. The results of these scans are provided by GSM and analyzed regularly by macmon NAC. Whenever macmon NAC finds an endpoint that is infected or does not meet the corporate compliance policy, it will respond with a predefined configured reaction that could either isolate the endpoint in order to remediate the situation or disconnect it from the network.

Configuration in macmon NAC

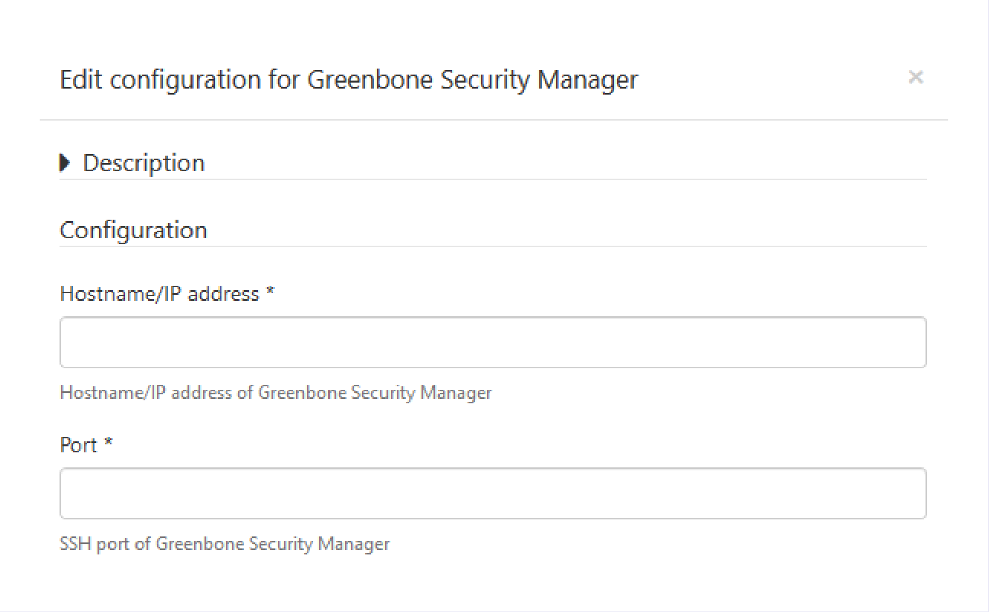
Configuration of the Greenbone Security Manager integration

The configuration is done via the web GUI. Please tap on *Settings* and *Third party integrations*, then on *Compliance*.


All
Asset management
Compliance
Identity store
Infrastructure
Search...
Barracuda
Check Point SOFTWARE TECHNOLOGIES LTD.
FIREEYE
splunk> turn data into doing
F-Secure
Greenbone Sustainable Resilience
ManageEngine Mobile Device Manager Plus
ManageEngine Patch Manager Plus
SOPHOS

If the border of the *Greenbone Security Manager (GSM)* tile appears gray the integration is not yet activated. Please tap on the tile for the configuration dialog to be shown.

1. Enter the *hostname* or *IP address* and *SSH port* that is needed to access *Greenbone Security Manager*.



Edit configuration for Greenbone Security Manager

Configuration

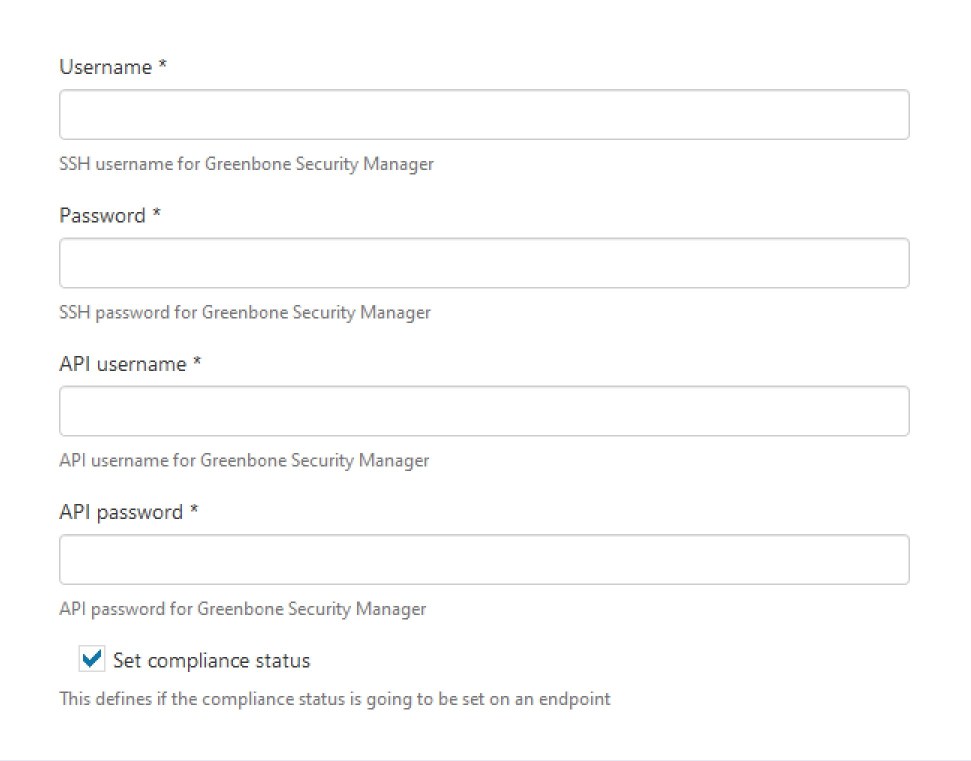
Hostname/IP address *

Hostname/IP address of Greenbone Security Manager

Port *

SSH port of Greenbone Security Manager

2. In the next section, enter the *username* and *password* that is needed to connect to *Greenbone Security Manager* via SSH. This connection is required in order to connect to the API in the following step. The access credentials for SSH and API do not necessarily be the same.
3. Afterwards, enter the *API username* and *API password* to connect the API via the GMP protocol. In order to have the compliance status set, tick the box of *Set compliance status*.



Username *

SSH username for Greenbone Security Manager

Password *

SSH password for Greenbone Security Manager

API username *

API username for Greenbone Security Manager

API password *

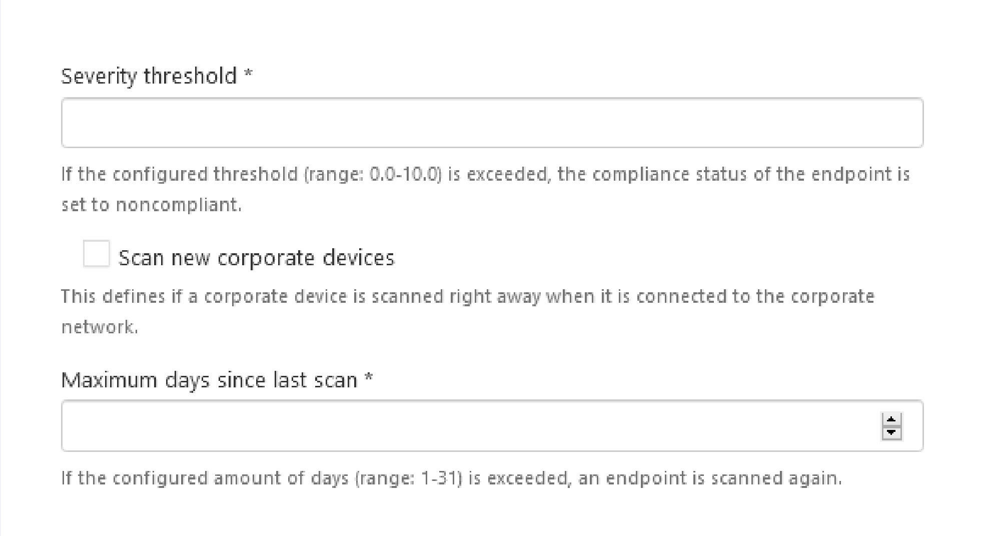
API password for Greenbone Security Manager

☑ Set compliance status

This defines if the compliance status is going to be set on an endpoint

4. In *Severity threshold* you enter the threshold on a scale from 0.0 and 10.0 at which an endpoint in the *Greenbone Security Manager* database is being considered noncompliant after it was scanned for vulnerabilities by the GSM scanner. Tick the box *Scan new corporate devices* if you want new or recurring endpoints to be scanned when they are connected to the network. The value in *Maximum*

days since last scan defines the amount of time that is supposed to have passed since the last scan of said new or recurring endpoint to avoid having it scanned too often.



Severity threshold *

If the configured threshold (range: 0.0-10.0) is exceeded, the compliance status of the endpoint is set to noncompliant.

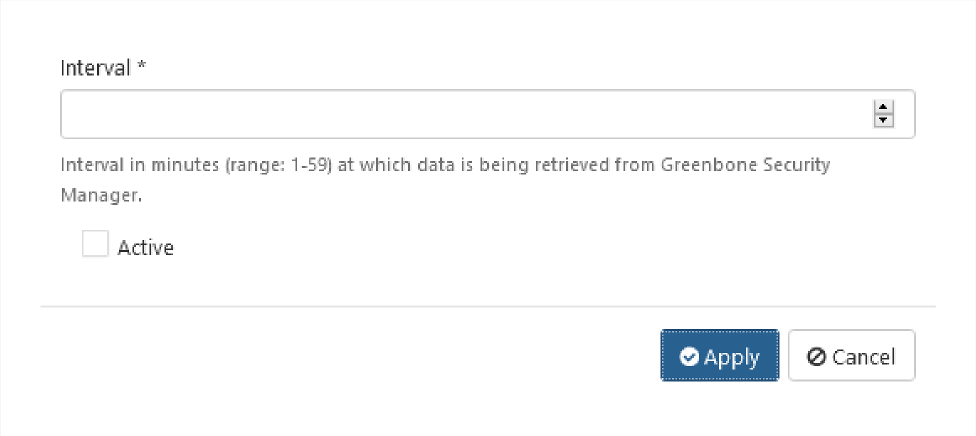
□ Scan new corporate devices

This defines if a corporate device is scanned right away when it is connected to the corporate network.

Maximum days since last scan *

If the configured amount of days (range: 1-31) is exceeded, an endpoint is scanned again.

5. In *Interval* you enter the interval in minutes at which data is being retrieved from *Greenbone Security Manager*.



Interval *

Interval in minutes (range: 1-59) at which data is being retrieved from Greenbone Security Manager.

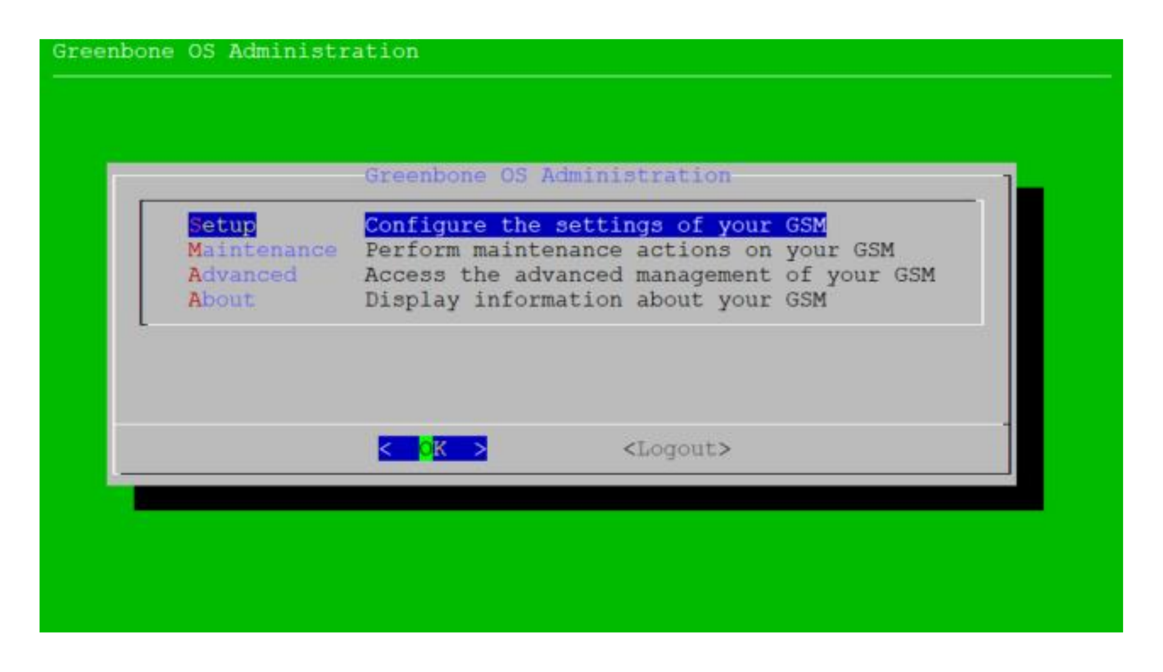
□ Active

6. Activate the integration by ticking the box *Active* and confirm by tapping *Ok*.

Configuration in Greenbone Security Manager

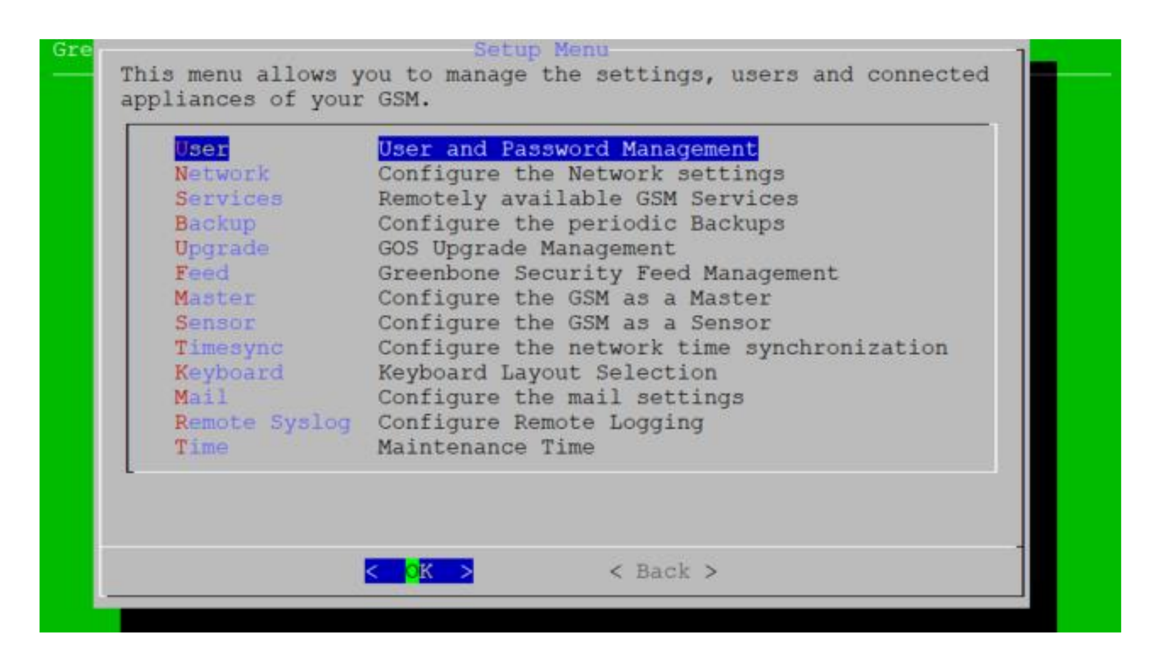
Configuration of the GMP service

1. Login into the Greenbone OS Administation shell via SSH using your SSH credentials. After having successfully logged in the welcome screen is shown.



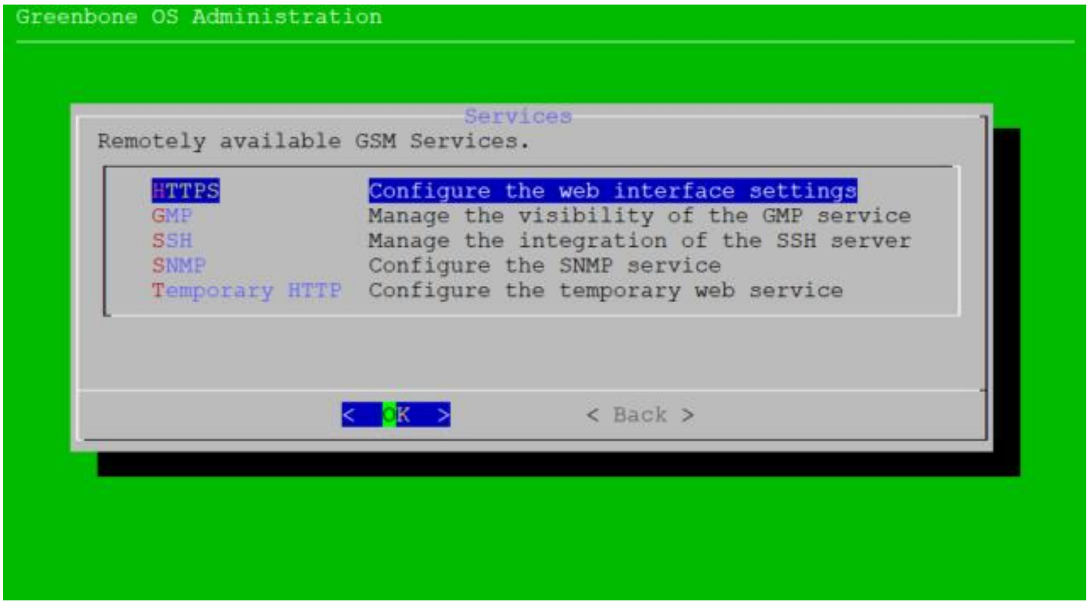
```
Greenbone OS Administration

                 Greenbone OS Administration

      Setup          Configure the settings of your GSM
      Maintenance    Perform maintenance actions on your GSM
      Advanced       Access the advanced management of your GSM
      About          Display information about your GSM

                  <  OK  >           <Logout>
```

2. In the welcome screen, select *Setup*.



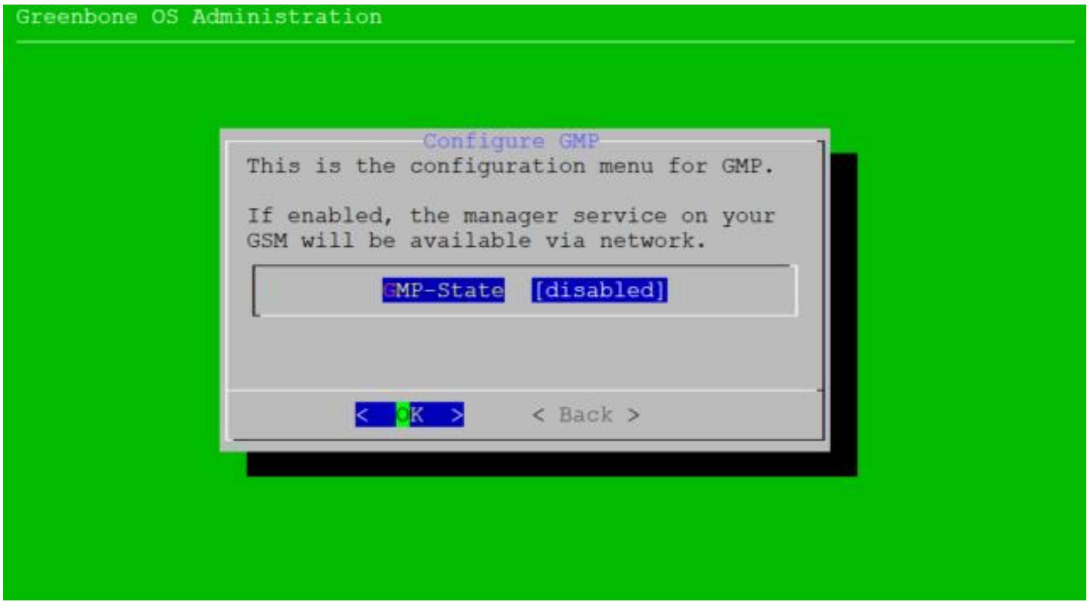
```
Gre                     Setup Menu
   This menu allows you to manage the settings, users and connected
   appliances of your GSM.

     User             User and Password Management
     Network          Configure the Network settings
     Services         Remotely available GSM Services
     Backup           Configure the periodic Backups
     Upgrade          GOS Upgrade Management
     Feed             Greenbone Security Feed Management
     Master           Configure the GSM as a Master
     Sensor           Configure the GSM as a Sensor
     Timesync         Configure the network time synchronization
     Keyboard         Keyboard Layout Selection
     Mail             Configure the mail settings
     Remote Syslog    Configure Remote Logging
     Time             Maintenance Time

                  <  OK  >          < Back >
```

3. Afterwards, select *User*.



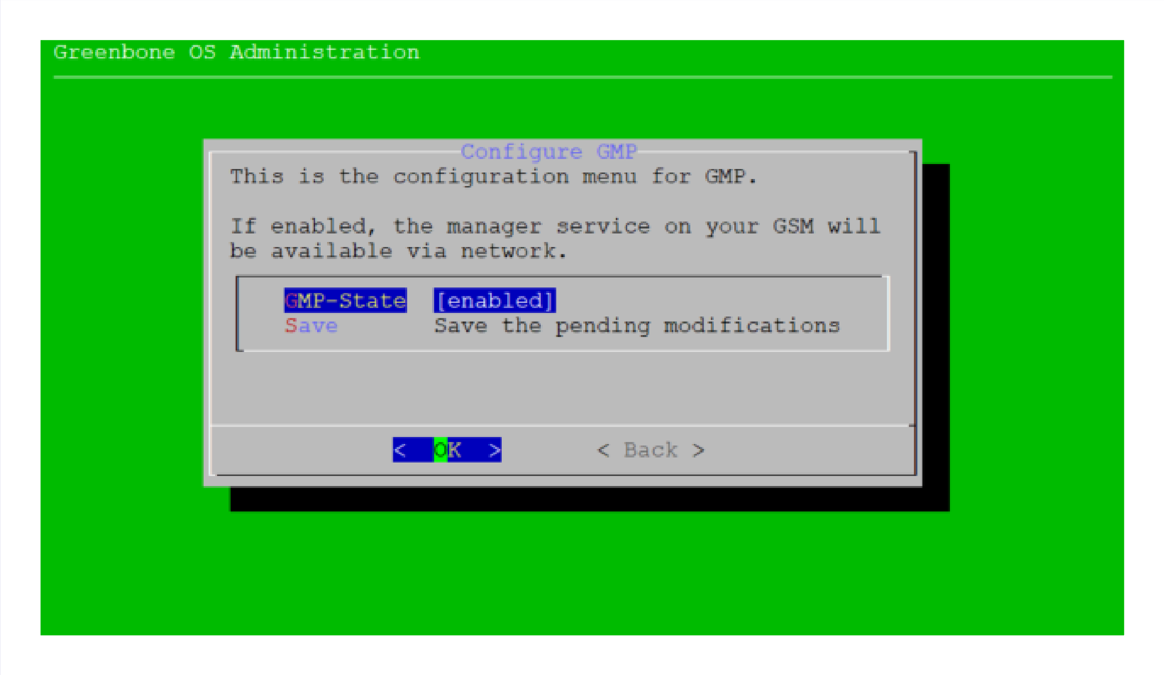
```
Greenbone OS Administration

                                Services
  Remotely available GSM Services.

      HTTPS            Configure the web interface settings
      GMP              Manage the visibility of the GMP service
      SSH              Manage the integration of the SSH server
      SNMP             Configure the SNMP service
      Temporary HTTP   Configure the temporary web service

                  <  OK  >            < Back >
```

4. Next, select *GMP*.



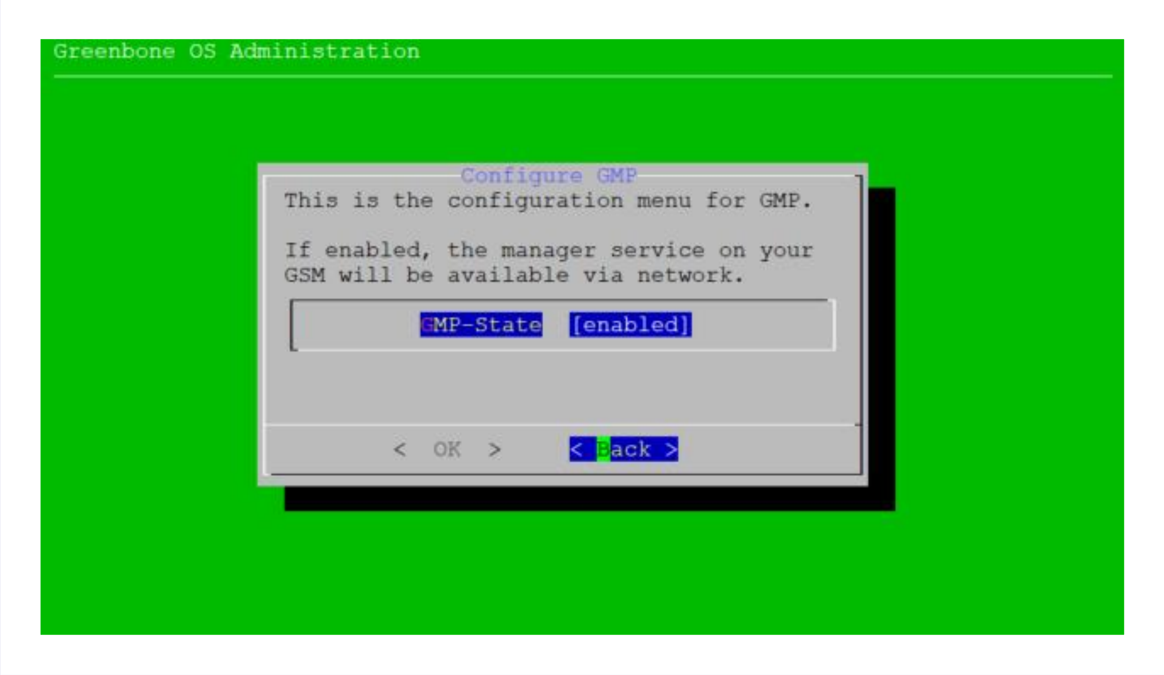
```
Greenbone OS Administration

                   Configure GMP
  This is the configuration menu for GMP.

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

          GMP-State  [disabled]

          <  OK  >        < Back >
```

5. In order to enable the GMP service, hit the space bar.



```
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. Select *Save* and hit the return key.



```
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. Select *Back* to finish the configuration.

Supported versions

macmon, version 5.25.0 or later with the *Premium Bundle* license
Greenbone Security Manager, version 6.0.12 or later

Contact Greenbone

Please contact Greenbone via email: support@greenbone.net

Contact

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