

# **HOTSPOT Manual**

**NetModule Router How To** 



Hotspot Router Software Version 1.11 Manual Version 1.11

NetModule AG, Switzerland

November 19, 2018

# Legal Notice

The specifications and information regarding the products in this manual are subject to change without notice. We would like to point out that NetModule makes no representation or warranties with respect to the contents herein and shall not be responsible for any loss or damage caused to the user by the direct or indirect use of this information This document may contain information about third party products or processes. Such third party information is generally out of influence of NetModule and therefore NetModule shall not be responsible for the correctness or legitimacy of this information. Users must take full responsibility for their application of any products.

#### Copyright ©2018 NetModule AG, Switzerland All rights reserved

This document contains proprietary information of NetModule. No parts of the work described herein may be reproduced. Reverse engineering of the hardware or software is prohibited and protected by patent law. This material or any portion of it may not be copied in any form or by any means, stored in a retrieval system, adopted or transmitted in any form or by any means (electronic, mechanical, photographic, graphic, optic or otherwise), or translated in any language or computer language without the prior written permission of NetModule. A large amount of the source code to this product is available under licenses which are both free and open

source. Most of it is covered by the GNU General Public License which can be obtained from www.gnu.org. The remainder of the open source software which is not under the GPL, is usually available under one of a variety of more permissive licenses. A detailed license information for a particular software package can be provided on request.

*NetModule* is a trademark and the logo is a service mark of NetModule AG, Switzerland.

All other products or company names mentioned herein are used for identification purposes only and may be trademarks or registered trademarks of their respective owners. The following description of software, hardware or process of NetModule or other third party provider may be included with your product and will be subject to the software, hardware or other license agreements.

#### Contact www.netmodule.com/support

NetModule AG	Tel +41 31 985 25 10
Meriedweg 11	Fax +41 31 985 25 11
CH-3172 Niederwangen	info@netmodule.com
Switzerland	http://www.netmodule.com

# Contents

1		Conformity
	1.1	Safety Instructions
	1.2	Declaration of Conformity
	1.3	Waste Disposal
	1.4	National Restrictions
	1.5	Open Source Software
2		About this Manual
3		Overview
	3.1	Supported NetModule Routers
	3.2	Feature List    9
4		Detailed Feature Explanation
	4.1	Administration
	4.2	Advanced Settings
		4.2.1 ToS
		4.2.2 RADIUS
	4.3	UAM
	4.4	Walled Garden
5		Example
	5.1	Scenario
	5.2	Prerequisites
	5.3	Configuration
		5.3.1 WLAN Administration
		5.3.2 WLAN Configuration
		5.3.3 Hotspot Interface
	5.4	Results
6		Technical Support

U

# List of Figures

4.1	Hotspot Feature Administration
4.2	ToS
4.3	RADIUS
4.4	UAM
4.5	HotSpot Feature Walled Garden    15
5.1	Mobile WWAN configuration
5.2	WLAN administration
5.3	WLAN configuration
5.4	WLAN Access Point configuration 20
5.5	HotSpot Configuration
5.6	Client redirect
5.7	Client ToS

U

# 1 Conformity

This chapter provides general information for putting the router into operation.

# **1.1 Safety Instructions**

NetModule routers must be used in compliance with any and all applicable national and international laws and with any special restrictions regulating the utilization of the communication module in prescribed applications and environments.

We would like to point out that only the original accessories, shipping with the router, must be used in order to prevent possible injury to health or damage to appliances and to ensure that all the relevant provisions have been complied with. Unauthorized modifications or utilization of unapproved accessories may void the warranty. The routers must not be opened. However, it is possible to replace any pluggable SIM cards even during operation.

All circuits connected to the interfaces of the router must comply with the requirements of Safety Extra Low Voltage (SELV) circuits and have to be designed for indoor use only. Interconnections must not leave the building nor penetrate the body shell of a vehicle. Possible antenna circuits must be limited to over-voltage transient levels below 1 500 V<sub>DC</sub> (according to IEC 62368-1, TNV-1 circuit levels) by using safety approved components.

HotSpot routers shall only be used with a certified (CE or equivalent) power supply which must have a power limited and SELV circuit<sup>1</sup> output.

They are basically designed for indoor use. Do not expose the communication module to extreme ambient conditions and protect the communication module against dust, moisture and high temperature.

We remind the user of the duty to observe the restrictions concerning the utilization of radio devices at petrol stations, in chemical facilities or in the course of blasting works in which explosives are used. Switch off the communication module when traveling by plane.

You need to pay increased attention when using the communication module close to personal medical devices, such as cardiac pacemakers or hearing aids. NetModule routers may also cause interference in the nearer distance of TV sets, radio receivers and personal computers.

Avoid any installation of the antenna during a lightning. Always keep a distance of more than 40 cm from the antenna in order to reduce exposure to electromagnetic fields below the legal limits. This distance applies to  $\frac{\lambda}{4}$ - and  $\frac{\lambda}{2}$ -antennas. Larger distances may apply to antennas with higher gain.

Any Ethernet cabling must be shielded, the Ethernet section of this manual provides more information.

Devices with a WLAN interface may be operated only with applicable Regulatory Domain configured. Special attention must be paid to country, number of antennas and the antenna gain. A misconfiguration will lead to loss of the approval.

Cellular antennas attached to the router must have an antenna gain of equal or less than 2.5 dBi. If an extension cable is used to attach the antenna, the antenna gain may be higher by

<sup>&</sup>lt;sup>1</sup>**Note:** Power supplies for routers with the Pb option (72-110 V<sub>DC</sub>) cannot be a SELV circuit, since the voltage is greater than 60 V<sub>DC</sub>.

the amount of cable attenuation. The user is responsible for the compliance with the legal regulations.

We highly recommended creating a copy of a working system configuration. It can be downloaded using the Web Manager and easily applied to a newer software release afterwards as we generally guarantee backward compatibility.

## **1.2 Declaration of Conformity**



NetModule hereby declares that under our own responsibility that the routers comply with the relevant standards following the provisions of the *RED Directive 2014/53/EU*. The signed version of the *Declarations of Conformity* can be found on the NetModule web page.

#### **1.3 Waste Disposal**



In accordance with the requirements of the *Council Directive 2002/96/EC* regarding Waste Electrical and Electronic Equipment (WEEE), you are urged to ensure that this product will be segregated from other waste at end-of-life and delivered to the WEEE collection system in your country for proper recycling.

## **1.4 National Restrictions**

This product may be generally used in all EU countries (and other countries following the *RED Directive 2014/53/EU*) without any limitation. Please refer to our WLAN Regulatory Database for getting further national radio interface regulations and requirements for a particular country.

#### **1.5 Open Source Software**

We inform you that NetModule products may contain in part open-source software. We are distributing such open-source software to you under the terms of GNU General Public License (GPL)<sup>2</sup>, GNU Lesser General Public License (LGPL)<sup>3</sup> or other open-source licenses<sup>4</sup>. These licenses allow you to run, copy, distribute, study, change and improve any software covered by GPL, Lesser GPL, or other open-source licenses without any restrictions from us or our end user license agreement on what you may do with that software. Unless required by applicable law or agreed to in writing, software distributed under open-source licenses is distributed on an "AS IS" basis, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.

To obtain the corresponding open source codes covered by these licenses, please contact our technical support at router@support.netmodule.com.

#### Acknowledgements

This product includes:

- PHP, freely available from http://www.php.net
- Software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org)
- Cryptographic software written by Eric Young (eay@cryptsoft.com)
- Software written by Tim Hudson (tjh@cryptsoft.com)
- Software written Jean-loup Gailly and Mark Adler
- MD5 Message-Digest Algorithm by RSA Data Security, Inc.
- An implementation of the AES encryption algorithm based on code released by Dr Brian Gladman
- Multiple-precision arithmetic code originally written by David Ireland
- Software from The FreeBSD Project (http://www.freebsd.org)
- CoovaChilli, freely available from https://coova.github.io/

<sup>&</sup>lt;sup>2</sup>Please find the GPL text under http://www.gnu.org/licenses/gpl-2.0.txt

<sup>&</sup>lt;sup>3</sup>Please find the LGPL text under http://www.gnu.org/licenses/lgpl.txt

<sup>&</sup>lt;sup>4</sup>Please find the license texts of OSI licenses (ISC License, MIT License, PHP License v3.0, zlib License) under http://opensource.org/licenses

# 2 About this Manual

This manual describes the features of the NetModule Hotspot Standalone Solution and gives at the end of the document a short configuration example.

# **3 Overview**

#### **3.1 Supported NetModule Routers**

- NB800
- NB1600
- NB2700
- NB2710
- NB2800
- NB3700
- NB3701
- NB3710
- NB3711
- NB3720
- NB3800

#### 3.2 Feature List

- 1. Up to four different Hotspot interfaces
- 2. Administration
  - a) Network configuration
  - b) Captive portal name
  - c) Logging
  - d) Upload landing pages
  - e) Pre-installed landing pages
- 3. Advanced
  - a) Terms only service
    - i. Bandwidth limitations
    - ii. Traffic limitations
    - iii. Inactivity timeout
    - iv. Session timeout
  - b) Radius
    - i. Radius configuration
    - ii. Accounting configuration
- 4. Walled Garden

# 4 Detailed Feature Explanation

# 4.1 Administration

net S	HOME INTERFACES ROUTING FIREWALL VPN SERVICES SYSTEM LOGOUT
SDK Administration Job Management Testing	Administration     Advanced     UAM     Walled Garden       Administrative status: <ul> <li>enabled</li> <li>disabled</li> </ul>
DNS Server NTP Server	Interface: WLAN1 V
Dynamic DNS E-mail	Network.         192.168.200.0           Netmask:         255.255.255.0
Events SSH/Telnet Server	Local address:     192.168.200.1       Portal name:     Hotspot
SINMP Agent Web Server	Logging. I disabled enabled
Redundancy Hotspot	Status: not installed
	Durchsuchen Keine Datei ausgewahit. Default landing page: download
	Apply Continue

Figure 4.1: Hotspot Feature Administration

Parameter	Administration
Administrative status	Enable or disable the Hotspot instance
Interface	The interface which should be controlled by the Hotspot in- stance
Network	The network address
Netmask	The netmask
Local address	The local IP address
Portal name	The captive portal name
Logging	If enabled the Hotspot instance will show more logging
Status	Indication if the landing page is installed or not
Upload landing page	Upload customized landing pages
Default landing page	Download a landing page example

## 4.2 Advanced Settings

Two operational modes are available. The terms-only service (ToS) mode shows a Terms of Service page and the user has to accept these terms before getting access to the Internet. The second mode is for using an RADIUS configuration, which requires an external RADIUS server. In this mode the user is getting an captive portal web page with user login and password field before he can reach the Internet.

#### 4.2.1 ToS

Module 🔨	HOME INTERFACES	ROUTING FIREWALL VF	N SERVICES	SYSTEM LOGOU
SDK	Administration Administration	vanced UAM	Walled Garden	
Administration Job Management Testing	Operational mode:	O Terms-only service		
DHCP Server		RADIUS configuration		
DNS Server	Bandwidth Limitation Down:	Linitia		
NTP Server		KDIVS		
Dynamic DNS	Bandwidth Limitation Up:	0 kbit/s		
E-mail	Traffic Limitation:	0 MByte		
Events	Inactivity Timeout			
SMS	matany micou.	0 seconds		
SSH/Telnet Server	Session Timeout	0 seconds		
SNMP Agent				
Web Server	Access local interfaces:			
Discovery				
Redundancy	Apply Continue			

Figure 4.2: ToS

Parameter	
Bandwidth Limitation	This option limits the bandwidth (up and download) of each user/device which is connected and authenticated to the Hotspot interface. This option is available with ToS only.
Traffic Limitation	With this option it is possible to limit the data consumption per user/client. After reaching the given traffic limitation the user/client will be redirected to the login page again. This op- tion is available. with ToS only.

Parameter	
Inactivity Timeout	If a station does not send anything within this timeout the user will be automatically logged out. This option is available with ToS only.
Session Timeout	With this option it is possible to set the maximum session time in seconds. The client will be logout after the session timeout was reached. The default value 0 means unlimited time.
Access local interfaces	If selected, the user can reach services which are connected on a local interface of the router

# 4.2.2 RADIUS

SDK Administration Job Management	Operational mode:	
Testing DHCP Server		<ul> <li>Terms-only service</li> <li>RADIUS configuration</li> </ul>
DNS Server	Primary RADIUS server:	1021601254
NTP Server	Secondary PADIUS server	
Dynamic DNS	Shared Secret	192.168.1.253
E-mail	Authentisation Part	
Events	Addrendication Port.	1812
SSH/Telnet Server	Accounting Port:	1813
SNMP Agent	Accounting Interval:	0 seconds
Web Server	Account external traffic only:	
Discovery	Account SSID:	
Redundancy Hotspot	Access local interfaces:	0
	Apply Continue	

Figure 4.3: RADIUS

Parameter	
RADIUS Server	The IP address of the radius server. This option is available with RADIUS configuration only
Shared Secret	This option defines the shared secret of the radius server (RA- DIUS configuration only)

Parameter	
Authentication Port	The authentication port of the radius server. This option is available with radius only.
Accounting Port	The authentication port of the radius server. This option is available with radius only.
Accounting Interval	This interval specifies in which seconds the Hotspot process will report accounting information to the radius server. This option is available with radius only.
Account external traffic only	If enabled the Hotspot process will report external traffic only. This means the internal traffic like Walled Garden traffic will be ignored. This option is available with radius only.
Account SSID	If enabled the Hotspot process will append the MAC of the RADIUS Called Station ID with the SSID of the current WLAN interface separeted by a colon. This option is available with radius only.
Access local interfaces	If selected, the user can reach services which are connected on a local interface of the router

#### 4.3 UAM

With the Universal Access Method (UAM) settings it is possible to configure external services for hotspot e.g. external custom landing page.

SDK       Administration         Administration       Advanced         Job Management       External UAM Server:         DHCP Server       UAM Port:         DHCP Server       UAM Port:         DHS Server       External UAM Homepage:         NTP Server       UAM Secret         Dynamic DNS       UAM Secret	HOME INTERFACES ROUTING FIREWALL VPN SERVICES SYSTEM LOGOUT         Administration       Advanced       UAM       Walled Garden         External UAM Server:	Interfaces routing frewall VPN services system logout   SDK   Administration   Sbk administration   Shk administration   Shk administration   Shk administration   Administration   Administration   Sbk administration   Shk administration   Administration </th <th></th> <th></th>		
SDK     Administration       Administration     Job Management       Job Management     External UAM Server:       DHCP Server     UAM Port:       DHS Server     External UAM Homepage:       NTP Server     UAM Sercet.       Dynamic DNS     Image: Image	Administration     Advanced     UAM     Walled Garden       External UAM Server:	SDK Administration   Administration Advanced UAM   Valied Garden   Dob Management   Testing   DHCP Server   UAM Port:   3990   DNS Server   External UAM Homepage:   DNS Server   UAM Secret:   Dynamic DNS   E-mail   Events   SNMP Agent   Web Server   Discovery   Redundancy	net S	HOME INTERFACES ROUTING FIREWALL VPN SERVICES SYSTEM LOGOUT
DHCP Server UAM Port. 3990 DNS Server External UAM Homepage: NTP Server UAM Secret. Dynamic DNS	VAM Port: 3990 External VAM Homepage: VAM Secret Apply Continue	DHCP Server UAM Port:   DHS Server External UAM Homepage:   NTP Server UAM Secret:   Dynamic DHS   E-mail   Events   SSH/Tentet Server   SNMP Agent   Web Server   Discovery   Redundancy	SDK Administration Job Management Testing	Administration Advanced UAM Walled Garden
DNS Server External UAM Homepage: DMTP Server UAM Secret Dynamic DNS	External UAM Homepage: UAM Secret Apply Continue	DNS Server External UAM Homepage:   NTP Server UAM Secret:   Dynamic DNS   E-mail   Events   SSH/Teinet Server   SINIP Agent   Web Server   Discovery   Redundancy	DHCP Server	UAM Port: 3990
NTP Server UAM Secret:	UAM Secret Apply Continue	NTP Server   Dynamic DNS   E-mail   Events   SSH/Telnet Server   SNMP Agent   Web Server   Discovery   Redundancy	DNS Server	External UAM Homepage:
Dynamic DNS	Apply Continue	Dynamic DNS E-mail Apply Continue Events SSH/Telnet Server SNMP Agent Web Server Discovery Redundancy	NTP Server	UAM Secret
	Apply Continue	E-mail Apply Continue Events SSH/Telnet Server SNMP Agent Web Server Discovery Redundancy	Dynamic DNS	
E-mail Apply Continue		Events SSH/Telnet Server SNMP Agent Web Server Discovery Redundancy	E-mail	Apply Continue
Events		SSH/Telnet Server SNMP Agent Web Server Discovery Redundancy	Events	
SSH/Telnet Server		SNMP Agent Web Server Discovery Redundancy	SSH/Telnet Server	
SNMP Agent		Web Server Discovery Redundancy	SNMP Agent	
Web Server		Discovery Redundancy	Web Server	
Discovery		Redundancy	Discovery	
Redundancy			Redundancy	
		Hotspot	Hotspot	
Hotspot				
Hotspot				
SI/MP Agent		Web Server Discovery Redundancy	SNMP Agent	
Web Server		Discovery Redundancy	Web Server	
Discovery		Redundancy	Discovery	
Redundancy			Redundancy	-
i contrario i c		listenst	Hetmot	

Figure 4.4: UAM

Parameter	
External UAM Server	The URL of the web server for client authentication
UAM Port	If an unauthenticated client tries to access the internet the client will be redirected to this port of the local IP address of the router
External UAM Homepage	The URL of the homepage where unauthenticated clients were redirected
UAM Secret	The shared secret between external UAM server and hotspot process.

**Note:** If not using an external UAM server or UAM hompage, leave the configuration parameter empty to use the default values.

# 4.4 Walled Garden

SDK Administration   Job Maragement Testing   DHCP Server NetModule   DNS Server NetModule   Dynamic DNS   E-mail   Events   SSH/Telnet Server   SNMP Agent   Web Server   Discovery   Redundancy   Hetspot	Module SS	нс	OME INTERFAC	CES ROUTING	5 FIREWALL	VPN SERVICES	SYSTEM	LOGOUT
Job Management   Testing   DHCP Server   DNS Server   DNS Server   Oynamic DNS   E-mail   Events   SSH/Telnet Server   SNMP Agent   Web Server   Discovery   Redundancy	SDK Administration	Ad	ministration	Advanced	UAM	Walled Garde	'n	
DHCP Server     Image: MetModule     Image: metmodule.com     Image: MetModule       DNS Server     Apply     Continue       Dynamic DNS     E-mail       Events     SSH/Teinet Server       SNMP Agent       Web Server       Discovery       Redundancy       Hospot	Job Management Testing		Description	U	RL			
DNS Server   NTP Server   Dynamic DNS   E-mail   Events   SSH/Teinet Server   SNMP Agent   Web Server   Discovery   Redundancy   Hotspot	DHCP Server	•	NetModule	r	etmodule.com			V X
NTP Server     Apply     Continue       Dynamic DNS       E-mail       Events       SSH/Teinet Server       SNMP Agent       Web Server       Discovery       Redundancy       Hotspot	DNS Server		h. Contin	1				
Dynamic DNS E-mail Events SSH/Telnet Server SNMP Agent Web Server Discovery Redundancy Hotspot	NTP Server	App	iy Continue	J				
E-mail Events SSH/Telnet Server SNMP Agent Web Server Discovery Redundancy Hotspot	Dynamic DNS							
Events SSH/Telnet Server SNMP Agent Web Server Discovery Redundancy Hotspot	E-mail							
SSH/Teinet Server SNMP Agent Web Server Discovery Redundancy Hotspot	Events							
SNMP Agent Web Server Discovery Redundancy Hotspot	SSH/Telnet Server							
Web Server Discovery Redundancy Hotspot	SNMP Agent							
Discovery Redundancy Hotspot	Web Server							
Redundancy Hotspot	Discovery							
Hotspot	Redundancy							
	Hotspot							

Figure 4.5: HotSpot Feature Walled Garden

With the Walled Garden settings it is possible to offer free services like web pages to the customer/user without having an account or without accepting the ToS agreements. The services which are configured via an URL and a description will be ignored by the captive portal and the user will reach the services directly.

# 5 Example

This chapter describes how to configure the NetModule standalone hHotspot solution with a small example.

## 5.1 Scenario

- WAN uplink via mobile interface
- WLAN
  - 2.4 GHz operation mode
  - Channel 1
  - SSID name "Hotspot"
  - public wlan with no security option
- Hotspot
  - Captive portal name: "Hotspot"
  - Network: 192.168.200.0/24
  - Operational mode: "terms-only service"

#### **5.2 Prerequisites**

- NetModule router with WLAN interface and supporting hotspots.
- Official NetModule router with installed hotspot patch image. Download here

The following configurations steps are made with the GUI of the NetModule router. Therefore access the IP-address of the router with an internet browser. The manual uses software version 4.0.0.106 with hotspot version 1.7 on a NetModule NB2800 router (screenshots might look different).

# 5.3 Configuration

(Mobile->Interfaces->Connection)

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~			
Module 💦	HOME INTERFACES	ROUTING FIREWALL VPN SEF	VICES SYSTEM LOGOUT
WAN			
Link Management Supervision Settings	Mobile Connection	Advanced	
Ethernet Port Setup	Connection settings:	<ul> <li>load from database</li> <li>specify</li> </ul>	
IP Settings	Select country:	Switzerland	
Mobile			
Interfaces	Provider	APN	Username
WLAN	M-Budget	gprs.swisscom.ch	
Administration Configuration	Orange	click	
IP Settings	Orange	intranetaccess	
USB	Orange	mobileoffice3g	
Serial	O Salt	click	
GNSS	<ul> <li>Salt</li> </ul>	internet	
	O Sunrise	internet	internet
	Swisscom	corporate.swisscom.ch	testprofil
	Swisscom	event.swisscom.ch	

Figure 5.1: Mobile WWAN configuration

Configure mobile WWAN interface. For further information how to configure a WWAN uplink please refer to the router user manual.

#### 5.3.1 WLAN Administration

(Interfaces->WLAN->Administration)

net 💸	
Module 🐼	HOME INTERFACES ROUTING FIREWALL VPN SERVICES SYSTEM LOGOUT
WAN Link Management Supervision	− WLAN Management Administrative status:
Settings Ethernet Port Setup VLAN Management IP Settings	Operational mode:
Mobile Silvis Interfaces	Regulatory domain: Switzerland 🔻
WLAN Administration Configuration IP Settings	Number of antennas:     2 v       Antenna gain:     0 dB
USB	Operation type: 802.11n V
Serial	Radio band: 2.4 GHz 🔻
GNSS	Bandwidth: 20 MHz v
	Channel: 1 (2412 MHz) V Channel utilisation
	Apply Continue

Figure 5.2: WLAN administration

Enable administration status and configure WLAN interface as follows:

Parameter	Setting
Regulatory domain	The country where the access point is used
Operation type	To have optimal compatibility use 802.11n or 802.11ac if avail- able
Radio band	2.4 GHz operation
Bandwidth	20Mhz
Channel	1 (2412 MHz)

## 5.3.2 WLAN Configuration

(Interfaces->WLAN->Configuration)

Module SS	HOME	INTERFACES	ROUTING	FIREWALL	VPN	SERVICES	SYSTEM	LOGOUT
	- WLAN Acces	s-Point Configurat	ion					
WAN Link Management	Interface	SSID		Security	Mode	WPA / Ciph	er	
Supervision Settings	WLAN1	NB2800		Off				e e
Ethernet Port Setup VLAN Management IP Settings	Apply							U I
Mobile SIMs Interfaces								
WLAN Administration Configuration IP Settings								
USB								
Serial								
GNSS								
	_							

Figure 5.3: WLAN configuration

Press continue and follow up with access point configuration page. Add WLAN interface by clicking the "edit"-button.

net S	HOME INTERFACES ROUTING FIREWALL VPN SERVICES SYSTEM LOGOUT
WAN Link Management Supervision	WLAN Access-Point Configuration SSID: Hotspot Security mode: None T
Ethernet Port Setup VLAN Management IP Settings	Security features:
Mobile Silvis Interfaces	Accounting:
WLAN Administration Configuration IP Settings	Apply Continue
USB	_
GNSS	-
	_

Figure 5.4: WLAN Access Point configuration

Parameter	Setting
SSID	Hotspot
Security mode	none

Apply configuration via "Apply"-button.

## 5.3.3 Hotspot Interface

#### (Services->Hotspot)

Add hotspot interface by clicking the "+"-button

Enable administrative status and continue with following configuration:

net SS	HOME INTERFACES ROUTING FIREWALL	VPN SERVICES SYSTEM LOGOUT
SDK Administration Job Management Testing DHCP Server	Administration Advanced UAM Administrative status: © enabled ◯ disabled	Walled Garden
DNS Server NTP Server	nterface: ₩LAN1 ▼ Network: 192.168.200.0	
Dynamic DNS E-mail Events	vetmask: 255.255.0 .ocal address: 192.168.200.1	
SSH/Telnet Server SNMP Agent Web Server	Portal name: Hotspot .ogging: © disabled enabled	
Discovery Redundancy	anding Page Status: not installed	
Hotspot	Jpload landing page: Durchsuchen Ke Default landing page: download	ine Datei ausgewählt.
	Apply Continue	

# Figure 5.5: HotSpot Configuration

Parameter	Setting
Interface	Choose "WLAN1" as interface
Portal name	type "Hotspot" as portal name

Apply configuration: press "Apply"-Button

## 5.4 Results

Now the client will be redirected to the captive portal site first.



Figure 5.6: Client redirect



Figure 5.7: Client ToS

# 6 Technical Support

NetModule's mission statement includes a professional and friendly team of support engineers which will be pleased to offer consultancy, provide assistance and deliver solutions in case of technical issues. With their broad-based experience they will be able to narrow down your problem and thus prevent you from getting too much gray hair.

In case of support requests please use the form at our support page and submit a detailed description of your problem together with a tech-support file which contains all the necessary information to speed up the process of analyzing and resolving your problem.

The latest software and documentation material can be found in the technical support area via the NetModule website.