Autonet Mobile customer support line:

1-800-977-2107

© 2014 Autonet Mobile, Inc.

P/N: 186-1100-001 Rev. 06

Important Product Information Guide

Autonet mobile

Important Product Information Guide

Welcome	2
Quickstart Guide	4
Configuring the In-Car Router	5
Configuring Wireless Settings	6
Configuring Wireless Security Settings	9
Configuring Login Screen	10
Changing the Password on Your In-Car Router	11
Checking the Connection Status of the In-Car Router	12
Troubleshooting Guide	13
Safety Policy	14
Acceptable Use Policy	20
Autonet Mobile Software License	24
Autonet Mobile Limited Warranty and Liability	26
Legal Disclosure	27

Autonet™ mobile

Welcome to Autonet Mobile

To activate your account with Autonet Mobile, please submit a completed service agreement online or by fax.

Online

Go to https://signup.autonetmobile.com

Fax

Download the service agreement from: https://signup autonetmobile.com and fax the completed agreement to 415-840-1725.

If you have any questions please call 1-800-977-2107.

For technical support call the Autonet Mobile customer service center: 1-800-977-2107.

Autonet Mobile assumes no responsibility for the configurations, security, or data files on your wireless device resulting from connection to Autonet Mobile's network. Anti-virus, privacy and security protection is the responsibility of the user.

Do not operate the In-Car Router while driving or perform any function that takes your attention away from safely driving your vehicle. Any function that requires prolonged attention should be performed after coming to a complete stop. Always stop the vehicle in a safe location before performing these functions. Failure to do so may result in an accident.

If the In-Car Router is found, please call: 1-800-977-2107. The router is automatically disabled if lost.

Quickstart Guide

Step 1

Turn your car to power up Autonet Mobile. Shortly “autonet” will appear in your wireless network list.

Step 2

In your wireless network list connect to the wireless network that contains the name “autonet”.

Step 3

Open your web browser. Click on the login button.

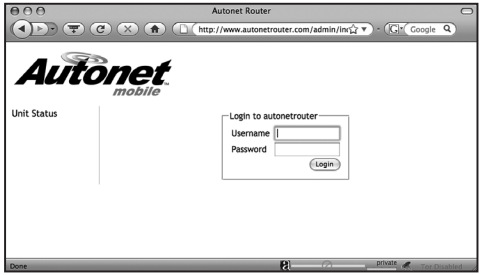
Step 4

Happy surfing!

Configuring the In-Car Router

It is highly recommended that the user enable WEP security and change the default password on the Autonet Mobile In-Car Router.

Configuring the WiFi interface on your In-Car Router



The unit’s serial number is is a ten digit hexadecimal number located in 2 places. It is located:

1. On the back of the In-Car Router
2. On the front of the quickstart guide.

If you have trouble locating the serial number of the router please call our customer support line at 1-800-977-2107 for assistance.

or

Open a web browser and go to the URL: http://www. autonetrouter.com/admin login as username “autonet” and use the unit’s serial number as the password. (e.g. 0024C76258) and click on the “login” button.

Configuring Wireless Settings

Click on “Wireless Settings”

ESSID

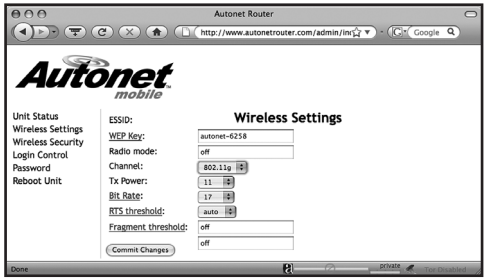
Extended Service Set ID. The ESSID is the identifying name of a wireless network - strictly it is the identifying name of a wireless access point. It allows one wireless network to be clearly distinguishable from another. The default ESSID is autonet-XXXX, where XXXX is the last 4 digits of the In-Car Router’s serial number. It is recommended that you keep this ESSID in order to distinguish your router from other routers that may be in the area.

WEP key

The WEP key is not shown if it is set. You do not have to set it, if you want it to remain the same. To set the current encryption key, just enter the key in hex digits as XXXXXXXXXX. The key must be 10 hex digits, (e.G. 1234567890) You can also enter the key as an ASCII string by using the s: prefix. The ASCII string must be five characters, (e.g. s:smile). To disable WEP, enter “off” as the WEP key.

Radio Mode

This allows you to select whether the radio is in 802.11b, 802.11g and 802.11a mode. Not all routers support all modes, so only the supported modes for your In-Car Router are shown.



Channel

Direct communication between an 802.11 Radio card and an access point occurs over a common channel frequency. The FCC allows channels 1 through 11 within the U.S. An important concept to note regarding channel assignments is that the channel actually represents the center frequency that the transceiver within the radio and access point uses (e.g., 2.412 GHz for channel 1 and 2.417 GHz for channel 2). There is only 5 MHz separation between the center frequencies, and an 802.11b signal occupies approximately 30 MHz of the frequency spectrum. The signal falls within about 15 MHz of each side of the center frequency. As a result, an 802.11b signal overlaps with several adjacent channel frequencies. This leaves you with only three channels (channels 1, 6, and 11 for the U.S.) That you can use without causing interference between access points.

Bit rate

This allows you to set the bit rate in Mbs. The bit rate is the speed at which bits are transmitted over the medium. The user speed of the link is lower due to medium sharing and various overhead. Select a value to lock the card to a particular bit rate. If you specify auto, the driver will use all bit rates to find an optimum rate.

RTS threshold

RTS/CTS adds a handshake before each packet transmission to make sure that the channel is clear. This adds overhead, but Increases performance in case of hidden nodes or a large number of active nodes. This parameter sets the size of the smallest packet for which the node sends rts; a value equal to the maximum packet size disables the mechanism. You may also set this parameter to off.

Fragmentation threshold

Fragmentation allows to split an IP packet in a burst of smaller fragments transmitted on the medium. In most cases this adds overhead, but in a very noisy environment this reduces the error penalty and allow packets to get through interference bursts. This parameter sets the maximum fragment size. You may also set this to off to disable the mechanism.

TxPower

This allows you to set the transmit power of the radio. Setting a lower value limits the range of the radio and reduces Interference with other access points.

Configuring Wireless Security Settings

Click on “Wireless Security”

The Wireless Security Settings allow you to control which wireless-equipped devices may communicate with the router depending on their MAC addresses. By default these MAC filters are disabled. If you turn MAC filters on, you should be sure and include the MAC address of the device that you are using to communicate with. Otherwise, the machine that you’re using will lose its connection to the In-Car Router.

This page will show you all of the wireless devices currently attached to the In-Car Router..

To enable MAC filters, change the MAC filters option to “on” and then check the “Allowed” box next to the MAC addresses that you wish to allow to join the network.

If you would like to have devices connect that are not currently attached to the In-Car Router you may add them in the box. You can add multiple devices by separating them with a space.

Select “commit changes” when you are finished.

Configuring Login Screen

Click on “login control”

Normally a device that connects to the Autonet Mobile network must first click through the login screen that comes up on your web browser. However, there are some devices that do not have a web browser (cameras, music players, etc.) So we’ve created a method for disabling the login page for those devices.

This page will show you all of the wireless devices currently attached to the In-Car Router.

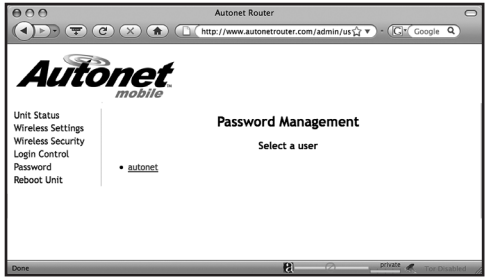
To bypass the login screen for a device, check the box under “no login required” next to the MAC address of that device.

If you would like to add devices that are not currently attached to the In-Car Router, then you may add them in the box. You can add multiple devices by separating them with a space.

Select “Commit Changes” when you are finished.

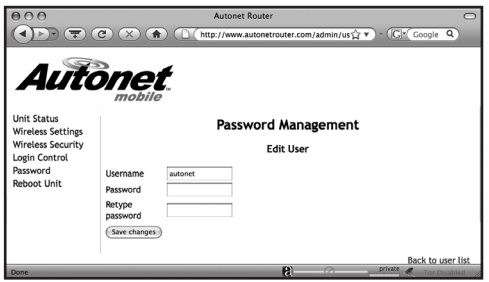
Changing the password on your In-Car Router

Click on “Password”



Click on the user name “autonet”

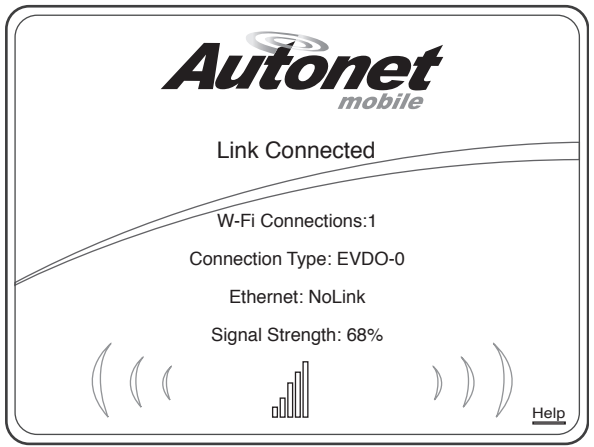
Enter a new password and click on “Save Changes”



If you ever forget your password, please contact the Autonet Mobile customer service center to have it reset.

Checking the Connection Status of the In-Car Router

In your web browser open the URL http://www.autonetrouter.com to see the current connect status of your In-Car Router.



Copyright © 2009 www.autonetmobile.com All rights reserved.

Troubleshooting Guide

The solid blue light on top of the In-Car Router indicates the internet connection is currently connected. If there are no WiFi users currently connected to the In-Car Router, the connection will be dropped and the blue light will start blinking to indicate that it is in idle mode. When a WiFi user attempts to connect to the internet, the In-Car Router will automatically set up the connection and the blue light will go solid when the internet connection is ready.

A flashing blue light on top of the In-Car Router indicates the unit is attempting to connect to the internet or is in idle mode. If the light doesn't stop flashing after three minutes, try the following steps:

1. Ensure the antennas on the In-Car Router are screwed on tightly.

2. Unplug/plug in the In-Car Router.

If the light continues to flash, it is likely that you are in an area that has no coverage.

If you receive the "limited or no connectivity" status after connecting wirelessly to the In-Car Router:

1. Click the disconnect button.

2. Click the connect button to reconnect.

If Autonet does not appear in the list of wireless networks window, try the following steps:

1. Refresh your available wireless networks window.

2. Disable and then Enable your wireless interface.

3. If autonet still does not appear in this list, consult the configuration instructions provided by your WiFi device manufacturer, or call the Autonet Mobile customer service center. Please have your serial number available when you call.

Safety Policy

Please read this Safety Policy concerning the use of a wireless router suitable for use in motorized vehicles ("Autonet Mobile") before operating the In-Car Router. Retain this Safety Policy for your future reference.

Accessories

Use only accessories manufactured by Autonet Mobile, Inc. with the In-Car Router. The use of any accessories not manufactured by Autonet Mobile, Inc. for use with the In-Car Router may be dangerous.

Driving

Do not use the In-Car Router when driving a motor vehicle because driving safely is your first responsibility and requires your full attention. If you find it necessary to use the In-Car Router while driving a motor vehicle, please pull off the road and park in a safe place before using the In-Car Router.

For vehicles equipped with air bags

An air bag inflates with great force. **Do not** place objects, including the In-Car Router, in the area adjacent to any air bag or in any air bag deployment area. If the In-Car Router is improperly installed and an air bag inflates, serious injury could result.

Electronic Devices

Most modern electronic equipment is shielded from radio frequency (RF) signals. However, certain electronic equipment may not be shielded against the RF signals from the In-Car Router. It is your responsibility to determine any effects that your use of the In-Car Router may have on other electronic equipment. In particular, consult the manufacturer of any motor vehicle in which you intend to use the In-Car Router to determine if the electronic equipment in that vehicle is adequately shielded from the RF energy emitted by your In-Car Router. You should also consult the manufacturer of any electronic equipment that you have added to that vehicle to ensure that it is adequately shielded from the RF energy emitted by the In-Car Router. You are responsible for any affects that your use of the In-Car Router may have on the electronic equipment in any vehicle in which it is operated.

Warning

Pacemakers

If you have a pacemaker, you should consult a physician or the manufacturer of your pacemaker if you have questions regarding the effect of RF signals on your pacemaker. If you have a pacemaker, ensure that you are using the In-Car Router in accordance with the safety requirements for that particular pacemaker, which may Include the following:

1. Always keep the In-Car Router more than 20 cm (7 Inches) from the pacemaker when the In-Car Router is turned on;
2. Do not carry the In-Car Router in any breast pocket; and if you have any reason to believe that the In-Car Router is Interfering with the proper functioning of your pacemaker, turn the In-Car Router off immediately.

Hearing Aids

Some digital wireless devices may interfere with the normal operations of some hearing aids. In case of such interference, consult your service provider or contact the manufacturer of your hearing aid to determine alternatives.

Other Medical Devices

If you use any other personal medical devices, consult the manufacturer of that device to determine if it is adequately shielded from external RF energy. Your physician may be able to assist you in obtaining this information.

Medical Facilities

Turn the In-Car Router off in hospitals and other health care facilities when any regulations posted in these facilities tell you to do so. Hospitals and other health care facilities may be using equipment that could be sensitive to external RF energy.

Posted Facilities

Turn the In-Car Router off in any facility where posted notices so require.

Blasting Areas

To avoid interfering with any blasting operations, turn the In-Car Router off when in any "blasting area" or in any area posted: "turn off two-way radio." Obey all signs and instructions.

Potentially Explosive Atmospheres

Turn the In-Car Router off when in any area with a potentially explosive atmosphere and obey all signs and instructions. Sparks in such areas could cause an explosion or fire and result in bodily injury or death.

Areas with a potentially explosive atmosphere are often, but not always, clearly marked. They Include fueling areas, like a gasoline/petrol station, fuel or chemical transfer or storage facilities; vehicles using liquefied petroleum gas (such as propane and butane); areas where the air contains chemicals or particles, such as grain, dust, or metal powders; and any other area where you would normally be advised to turn off your vehicle engine.

Power Cord

Protect any power cord from being walked on or plnched, and such protection especially should be afforded at any plugs, receptacles, and the point where they exit from the In-Car Router;

1. Unplug the power cord during lightning storms to avoid electrical shock or fire;

2. Unplug the power cord prior to cleaning the In-Car Router;

3. Keep the minimum required amount of space between the power cord and any heat sources;

4. Clean the power plug when it is dirty;

5. Do not bend, twist, pull, or heat the power cord because such actions may damage the power cord;

6. Do not use the power plug if it is loose as it may cause a fire or electric shock;

7. Wash hands after handling the power cord;

8. To reduce the risk of damage to the cord or the plug, pull the plug instead of the cord when disconnecting from a receptacle.

Foreign Objects and Liquids

Never push objects of any kind into the In-Car Router or any accessories because such insertion may cause parts to short out and result in a fire or electric shock. Do not use the In-Car Router or any accessories near or in water or if wet. Never spill liquid of any kind on the In-Car Router or any accessories. Disconnect the In-Car Router and any accessories before cleaning them.

Stability

Do not place the In-Car Router or any accessories on any unstable suRFaces. They may fall, thereby potentially causing serious injury to a person or animal, and/or serious damage to the In-Car Router or any accessories.

Care

Do not use liquid or aerosol cleaners or solvents on or near your In-Car Router, or any accessories. Clean your In-Car Router, or any accessories only with a dry cloth. If you use harsh chemicals, like alcohol, benzene, or thinners, to clean the In-Car Router, there is a risk of causing a fire.

Magnetic Items

Do not place items with magnetic components, like credit cards, phone cards, bank books, or subway tickets, near your In-Car Router.

Extreme Temperatures

Never expose your In-Car Router to excessively hot or cold temperatures because the In-Car Router may malfunction or be damaged. The In-Car Router and any accessories should be located away from any heat sources.

Storage

Store your In-Car Router in a clean, dust-free environment when not in use. Store your In-Car Router out of reach of small children and animals.

Service

Disconnect your In-Car Router, any charging unit, or any accessory and, if necessary, refer them to qualified service personnel if:

1. The power supply, plug, or connector to your In-Car Router is damaged;

2. Liquid has been spilled or objects have fallen into your In-Car Router, any charging unit, or any accessory;

3. Your In-Car Router, any charging unit, or any accessory has been exposed to rain or water;

4. Your In-Car Router or any accessory becomes very hot to the touch;

5. Your In-Car Router, any charging unit, or any accessory has been dropped or damaged in any way;

6. Your In-Car Router or any accessory does not operate normally in accordance with the instructions contained in any guide Provided by Autonet Mobile, Inc.;

7. Your In-Car Router or any accessory exhibits a distInct change in performance.

All servicing of the In-Car Router or any accessory should be undertaken only by qualified service personnel. Do not attempt to disassemble, modify, or repair the In-Car Router or any accessory yourself.

Adjustments

Adjust only those controls for the In-Car Router that are discussed in the instructions contained in any guide provided by Autonet Mobile, Inc. An improper adjustment of other controls for the In-Car Router may result in damages and may require extensive work by a qualified technician to restore the In-Car Router or any accessory, as the case may be.

Rough Treatment

Do not drop, strike, or shake severely the In-Car Router. Such actions may damage its internal circuit boards.

Antenna Care

Only use any supplied integral antenna with the In-Car Router. Unauthorized antenna modifications, or attachments could damage the In-Car Router and may violate U.S. Federal communications commission (FCC) regulations. No one should hold the antenna or let it come into contact with his or her body when the In-Car Router is in use. Do not use the In-Car Router if the antenna is damaged. If a damaged antenna touches skin, it may cause a slight burn.

Local Laws

Drivers and their passengers are responsible for determining and complying with any local laws affecting the use of the In-Car Router. Accordingly, you should familiarize yourself with any applicable laws in jurisdictions where you use the In-Car Router. Always obey those laws.

Exposure to Radio Frequency Signals

The In-Car Router is a low power radio transmitter and receiver. When it is turned on, it sends out and receives RF signals. The In-Car Router complies with FCC guidelines respecting safe levels of RF exposure for handled wireless devices, which in turn are consistent with the following safety standards previously set by certain standards bodies:

1. ANSI/IEEE C95.1-1999, IEEE standard for safety levels with respect to Human Exposure To Radio Frequency Electromagnetic Fields, 3 Khz to 300 GHz;

2. National Counsel On Radiation Protection And Measurements (NCRP) report 86, - 1986, Biological Effects and Exposure Criterion for Radio Frequency Electromagnetic Fields; and

3. International Commission on Non-Ionising Radiation Protection (ICNIRP) 1988, guidelines for limiting exposure to time-varying Electric, magnetic, and electromagnetic fields (up to 300 GHz).

To maintain compliance with FCC exposure guidelines, use only accessories supplied or approved by Autonet Mobile, Inc.

Specific Absorption Rate Data

The In-Car Router meets U.S. Government requirements for exposure to radio waves. The In-Car Router is a radio transmitter and receiver. It is designed and manufactured not to exceed the emission limits for exposure to RF energy set by the FCC. These limits are part of comprehensive guidelines and establish permitted levels of exposure to RF energy for the general population. These guidelines are based on standards that were developed by independent scientific organizations through periodic and thorough evaluation of scientific studies. The standards Include a substantial safety margin designed to assure the safety of all persons, regardless of age and health.

FCC Compliance Statement

This equipment has been tested and found to comply with the limits for a class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense. Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment. The antenna used for this transmitter must be installed to provide a separation distance of at least 20cm from all persons and must not be located or operating in conjunction with any other antenna or transmitter.

Acceptable Use Policy

1. Introduction

Autonet Mobile, Inc's Acceptable Use Policy ("AUP") is intended to help enhance the use of the internet by preventing unacceptable use. All users of Autonet Mobile, Inc's internet services (the "services") those who access some of our services but do not have accounts ("visitors"), as well as those who pay a monthly service fee to subscribe to the services ("members") must comply with this AUP. We support the free flow of information and ideas over the internet and do not actively monitor use of the services under normal circumstances. Similarly, we do not exercise editorial control over the content of any web site, electronic mail transmission, newsgroup, or other material created or accessible over or through the services, except for

certain proprietary websites. However, in accordance with our internet Service Agreement, we may remove any materials that, in our sole discretion, may be illegal, may subject us to liability, or which may violate this AUP. Autonet Mobile, Inc may cooperate with legal authorities and/or third parties in the investigation of any suspected or alleged crime or civil wrong. Your violation of this AUP may result in the suspension or termination of either your access to the services and/or your Autonet Mobile, Inc account or other actions as detailed in section 3. This AUP should be read in conjunction with our internet Service Agreement and other policies.

2. Violations of Autonet Mobile's Acceptable Use Policy

A. Illegal use. Using the services to transmit any material (by e-mail, uploading, posting, or otherwise) that, intentionally or unintentionally, violates any applicable local, state, national or international law, or any rules or regulations promulgated there under.

B. Harm to minors. Using the services to harm, or attempt to harm, minors in any way.

C. Threats. Using the services to transmit any material (by e-mail, uploading, posting, or otherwise) that threatens or encourages bodily harm or destruction of property.

D. Harassment. Using the services to transmit any material (by e-mail, uploading, posting, or otherwise) that harasses another.

E. Fraudulent activity. Using the services to make fraudulent offers to sell or buy products, items, or services or to advance any type of financial scam such as "pyramid schemes," "ponzi schemes," and "chain letters."

F. Forgery or impersonation. Adding, removing, or modifying identifying network header information in an effort to deceive or mislead is prohibited. Attempting to impersonate any person by using forged headers or other identifying information is prohibited. The use of anonymous remailers or nicknames does not constitute impersonation. Using deliberately misleading headers ("munging" headers) in news postings in order to avoid spam e-mail address collectors is allowed.

G. Unsolicited commercial e-mail/unsolicited bulk e-mail. Using the services to transmit any unsolicited commercial e-mail or unsolicited bulk e-mail. Activities that have the effect of facilitating unsolicited commercial e-mail or unsolicited bulk e-mail whether or not that email is commercial in nature, are prohibited.

H. Unauthorized access. Using the services to access, or to attempt to access, the accounts of others, or to penetrate, or attempt to penetrate, security measures of Autonet Mobile, Inc's or another entity's computer software or hardware, electronic communications system, or telecommunications system, whether or not the intrusion results in the corruption or loss of data.

I. Copyright or trademark infringement. Using the services to transmit any material (by e-mail, uploading, posting, or otherwise) that Infringes any copyright, trademark, patent, trade secret, or other proprietary rights of any third party, Including, but not limited to, the unauthorized copying of copyrighted material, the digitization and distribution of photographs from magazines, books, or other copyrighted sources, and the unauthorized transmittal of copyrighted software. Autonet Mobile, Inc. is registered under the digital millennium copyright act of 1998.

J. Collection of personal data. Using the services to collect, or attempt to collect, personal information about third parties without their knowledge or consent.

K. Reselling the services. Reselling the services without Autonet Mobile's authorization.

L. Network disruptions and unfriendly activity. Using the services for any activity which adversely affects the ability of other people or systems to use Autonet Mobile, Inc services or the internet. This Includes "denial of service" (dos) attacks against another network host or individual user. Interference with or disruption of other network users, network services or network equipment is prohibited. It is the user's responsibility to ensure that their network is configured in a secure manner. A user may not, through action or inaction, allow others to use their network for illegal or inappropriate actions. A user may not permit their network, through action or inaction, to be configured in such a way that gives a third party the capability to use their network in an illegal or inappropriate manner.

M. News. Autonet Mobile users should use their best judgment when posting to any newsgroup. Many groups have charters, published guidelines, faqs, or "community standards" describing what is and is not considered appropriate. Usenet can be a valuable resource if used properly. The continued posting of off-topic articles is prohibited. Commercial advertisements are off- topic in most newsgroups, especially regional groups not specifically named for such. The presence of such articles in a group is not indicative of the group's "intended" use. Please familiarize yourself with basic usenet netiquette before posting to a newsgroup.

Autonet Mobile considers "multiposting" to 10 or more groups within a two week sliding window to be excessive. Autonet Mobile servers currently limit the number of allowable "cross-posts" to 9.

Autonet Mobile users may not cancel messages other than their own messages. A user may cancel posts forged in that user's name. We may cancel any postings which violate this AUP.

N. Long connections and multiple logins. Using a personal account for high volume or commercial use is prohibited. The services are intended for periodic, active use of e-mail, newsgroups, file transfers, internet chat, games, and browsing the world wide web. Users may stay connected so long as they are actively using that connection for the above purposes. Users may not use the services on a standby or inactive basis in order to maintain a connection. Pinging is expressly prohibited. Accordingly, Autonet Mobile, Inc maintains the right to terminate any member's connection following any extended period of inactivity as determined by Autonet Mobile, Inc.

3. Reporting Violations of Autonet's AUP

Autonet Mobile, Inc requests that anyone who believes that there is a violation of this AUP direct the information to director abuse department, at: abuse@ autonetmobile.com. If available, please provide the following information:

1. The IP address used to commit the alleged violation

2. The date and time of the alleged violation, Including the time zone or offset from GMT

3. Evidence of the alleged violation

   E-mail with full header information provides all of the above, as do syslog files. Other situations will require different methods of providing the above information.

Autonet Mobile, Inc may take any one or more of the following actions in response to complaints:

1. Issue warnings: written or verbal

2. Suspend the member's newsgroup posting privileges

3. Suspend the member's account

4. Terminate the member's account

5. Bill the member for administrative costs and/or reactivation charges

6. Bring legal action to enjoin violations and/or to collect damages, if any, caused by violations.

Autonet Mobile Software License

Important – read carefully. By removing the tamper label or otherwise using the software in your Autonet Mobile In-Car Router, you agree to be bound by the license terms and conditions below. If you do not agree to these terms and conditions you must immediately return your Autonet Mobile In-Car Router in its original condition and packaging to the point of purchase for a refund of your purchase price (after inspection).

Subject to these terms and conditions, Autonet Mobile, Inc. grants you a non-exclusive license, with no right to sublicense, to execute the software included with the Autonet Mobile In-Car Router or subsequently provided to you by Autonet Mobile (together, the "software") on your Autonet Mobile In-Car Router solely for your personal use on the intended features and functions of the Autonet Mobile In-Car Router. The license may be transferred only with the transfer of the Autonet Mobile In-Car Router on which Autonet Mobile, Inc. has installed the software; any transferee will be subject to the terms and conditions of this license.

This license will terminate automatically, without notice, if you fail to comply with the terms and conditions, including the restrictions, of this license.

Autonet Mobile, Inc. and its licensors own and retain all proprietary rights, including all patents, copyright, trade secret, trademark, and other intellectual property rights in and to the Autonet Mobile In-Car Router software. You acknowledge that the license granted above does not provide you with title to or ownership of the software, but only a right of limited use under these terms and conditions. The software embodies Autonet Mobile, Inc.'s trade secrets and other proprietary information and materials. Any attempt to modify, enhance, disassemble, decompile, reverse engineer or otherwise gain access to the source code of the software, to remove or unbundle the software from the Autonet Mobile In-Car Router, or to sublicense or distribute the software is strictly prohibited, except as expressly set for in the paragraph titled "GPLand lGPL software" and "other open source software" below or except as may be otherwise agreed by Autonet Mobile, Inc. in writing. Certain components of the software included with the Autonet Mobile In-Car Router are subject to the GNU general public license ("GPL"), the lesser GNU general public license ("lGPL"), or other "open source" or "free software" licenses ("open source software"). Some of the open source software is owned by third parties. The open source software is not subject to the terms and conditions of the section titled "Autonet Mobile, Inc. software license" above. Instead,each item of open source software is licensed under the terms of the end-user license that accompanies such open source software. Nothing in this document limits your rights under, or grants you rights that supersede, the terms and conditions of any applicable end user license for the open source software. In particular, nothing in this document restricts your right to copy, modify, and distribute that open source software subject to the terms of the GPL and lGPL. As required by the terms of the GPL and lGPL, Autonet Mobile, Inc. makes the open source software provided under the GPL and lGPL available to the public in source code form on a CD. To receive a CD, please send $9.00 To Autonet Mobile, Inc.

for the cost of preparing and mailing the CD to you. Requests can be mailed to Source Code CD Request, Autonet Mobile Inc.., 1700 Montgomery Ste. 111, San francisco, CA 94111.

The following open source software is included with the Autonet Mobile In-Car Router. GPL and lGPL software. The Autonet Mobile In-Car Router is provided with the following software licensed under the GPL and lGPL. A copy of the GNU GPL license is available from the free software foundation (http://www.GNU.Org).

1. BusyBox from http://www.busybox.net
2. Card Services for Linux from http://pcmcia-cs.sourceforge.net
3. Host AP driver from http://hostap.epitest.
4. fiiptables from http://www.netfilter.org
5. Linux operating system version 2.4.29
6. Openswan (http://www.openswan.org
7. PPP from http://www.samba.org/ftp/unpacked/ppp/
8. dnsmasq from http://www.thekelleys.org.uk/dnsmasq/
9. nocat from http://nocat.net
10. wifiadmin from http://wifiadmin.sourceforge.net/
11. gpsd from http://gpsd.berlios.de/
12. squid from http://www.squid-cache.org/
13. radius from http://www.freeradius.org/

4. Revisions to this Acceptable Use Policy

Autonet Mobile, Inc. reserves the right to revise, amend, or modify this AUP, our internet Service Agreement and our other policies and agreements at any time and in any manner. Notice of any revision, amendment, or modification will be posted in accordance with the Internet Service.

Other Open Source Software.

Autonet Mobile In-Car Router is provided with the following software licensed under bsd licenses or other open source software licenses. The software and license details are available from the referenced web-sites.

1. net-snmp from the net-snmp project (http://www.net-snmp.org)

2. openssh from the openbsd project (http://www.openssh.com)

3. thttpd from jef poskanzer (http://www.acme.com)

Autonet Mobile Limited Warranty and Liability

No warranties of any kind are provided by Autonet Mobile, Inc. With respect to this product, except as stated in Autonet Mobile Limited Warranty below.

Autonet Mobile, Inc. warrants to the original end user purchaser ("you") that the product shall be free of defects in materials and workmanship under normal use for one (1) year from the original date of purchase (the "warranty period"). These warranties are expressly in lieu of all other warranties, express or implied, including, without limitation, all implied warranties of merchantability and fitness for a particular purpose and any warranties arising from course of performance, course of dealing or trade usage.

Autonet Mobile, Inc.'s exclusive liability and your exclusive remedy hereunder is expressly limited to, at Autonet Mobile Inc.'s sole option and discretion, (a) exchange, repair or replacement of defective or nonconforming materials, parts or components; or (b) refund of all amounts paid directly to Autonet Mobile, Inc. For any defective product. Replacement products may be new or remanufactured.

The above shall apply whether Autonet Mobile, Inc.'s liability arises from any breach of its express warranty, breach of any obligation or otherwise with respect to the manufacture and sale of any units of the product, whether liability is asserted in contract or tort, including negligence and strict product liability. In no event shall Autonet Mobile, Inc. Be liable for special, indirect, incidental or consequential damages of any kind or nature due to any cause, regardless of whether Autonet Mobile, Inc. Has been advised of the potential for such damages or if such damages are foreseeable, or for claims by any third party. Autonet Mobile Inc.'s maximum aggregate liability to purchaser shall not exceed the amount paid by purchaser for the product.

The foregoing warranties do not extend to: (i) nonconformities, defects, or errors in the product due to accident, abuse, misuse, or negligent use of the product or use in other than a normal and customary manner, environmental conditions not conforming to Autonet Mobile, Inc.'s specification, improper installation, or failure to follow prescribed operating and maintenance procedures;

(ii) defects, errors or non conformities in the product due to modifications, alterations, additions, or changes to the product not authorized by Autonet Mobile, Inc., In writing in advance; (iii) normal wear and tear; (iv) damage caused by force of nature or act of any third person, including shipping damage; (v) service or repair of product by the purchaser without prior written consent from Autonet Mobile, Inc.; (Viii) products designated by Autonet Mobile, Inc. As beta site test samples, experimental, developmental, reproduction, sample, incomplete or out-of-specification products; (viii) returned products if the original identification marks or tamper seals have been removed from the product or altered; (ix) condensation, water, or liquid damage; (x) damage caused to the user's computer; (xi) loss of data; or (xii) damage caused by viruses. The foregoing limitations will apply even if any warranty or remedy provided hereunder fails of its essential purpose. This warranty gives you specific legal rights, and you may also have other rights that vary by jurisdiction. Some jurisdictions do not allow limitations on how long an implied warranty lasts or the exclusion or limitation of incidental or consequential damages, so the above warranty limitations may not apply to you.

Legal Disclosure

Copyright © 2014 by Autonet Mobile, Inc.

All rights reserved. No part of this publication may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from Autonet Mobile, Inc.

Autonet Mobile, Inc. Reserves the right to revise this publication and to make changes in content from time to time without obligation to provide notification of such revision or change. Autonet Mobile, Inc. Provides this guide without warranty of any kind, either implied or expressed, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Autonet Mobile, Inc. may make improvements or changes in the product(s) and product specifications described in this user guide at any time.

Product may contain repackaged and/or reconditioned parts. By using this product, you agree to the terms and conditions of the Autonet Mobile, Inc. Service Agreement.

All trademarks, trade names, product names, service names, and service marks listed in this user guide or with the software are the exclusive property of their respective owners. Neither Autonet Mobile, Inc. Nor the Autonet Mobile In-Car Router are endorsed by or affiliated with the respective companies listed above and no such endorsement is implied.

Autonet Mobile, Inc. Autonet mobile In-Car Router, the Autonet Mobile logo, and TRU technology are all trademarks of Autonet Mobile, Inc. All other trademarks, product names or service names, are the property of their respective owners.

If you have any questions or problems, please call the Autonet Mobile customer service center at 1-800-977-2107