

# Air Live<sup>®</sup>

[www.airlive.com](http://www.airlive.com)

## WIAS-1200G

*802.11G Internet Access Server*

### User's Manual



## **Federal Communication Commission Interference Statement**

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio technician for help.

## **FCC Caution**

This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Any changes or modifications not expressly approved by the party responsible for compliance could void the authority to operate equipment.

## **Federal Communication Commission (FCC) Radiation Exposure Statement**

This equipment complies with FCC radiation exposure set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20cm (8 inches) during normal operation.

The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

## **R&TTE Compliance Statement**

This equipment complies with all the requirements of DIRECTIVE 1999/5/EC OF THE EUROPEAN PARLIAMENT AND THE COUNCIL of March 9, 1999 on radio equipment and telecommunication terminal Equipment and the mutual recognition of their conformity (R&TTE)

The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) As of April 8, 2000.

## **Safety**

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

## **EU Countries Intended for Use**

The ETSI version of this device is intended for home and office use in Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, the Netherlands, Portugal, Spain, Sweden, and the United Kingdom. The ETSI version of this device is also authorized for use in EFTA member states: Iceland, Liechtenstein, Norway, and Switzerland.

## **COPYRIGHT**

Copyright ©2007/2008 by this company. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise, without the prior written permission of this company

This company makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability or fitness for any particular purpose. Any software described in this manual is sold or licensed "as is". Should the programs prove defective following their purchase, the buyer (and not this company, its distributor, or its dealer) assumes the entire cost of all necessary servicing, repair, and any incidental or consequential damages resulting from any defect in the software. Further, this company reserves the right to revise this publication and to make changes from time to time in the contents thereof without obligation to notify any person of such revision or changes.

# Declaration of Conformity

We, Manufacturer/Importer

**OvisLink Corp.**

**5F., NO.6, Lane 130, Min-Chuan Rd.,  
Hsin-Tien City, Taipei County, Taiwan**

Declare that the product

**802.11G Internet Access Server**

**WIAS-1200G**

**is in conformity with**

In accordance with 89/336 EEC-EMC Directive and 1999/5 EC-R & TTE Directive

## Clause

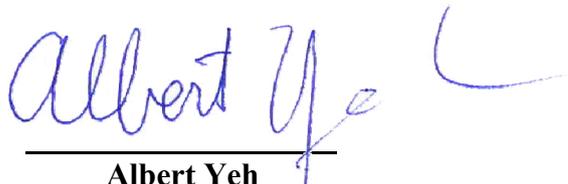
## Description

- **EN 300 328 V1.6.1**  
(2004-11) Electromagnetic compatibility and Radio spectrum Matters (ERM);  
Wideband transmission equipment operating in the 2.4GHz ISM band  
And using spread spectrum modulation techniques; Part 1 : technical  
Characteristics and test conditions Part2 : Harmonized EN covering  
Essential requirements under article 3.2 of the R&TTE Directive
- **EN 301 489-1 V1.6.1** Electromagnetic compatibility and Radio spectrum Matters (ERM);  
(2005-09) Electromagnetic compatibility(EMC) standard for radio equipment and
- **EN 301 489-17 V1.6.1** Services; Part 17 : Specific conditions for wideband data and  
(2005-09) HIPERLAN equipment
- **EN 60950-1:2006** Safety for information technology equipment including electrical  
business equipment

■ **CE marking**



## Manufacturer/Importer

---

**Albert Yeh**  

---

**Vice President**

Signature :  
Name :  
Position/ Title :

Date : **2007/6/7**

(Stamp)

## WIAS-1200G CE Declaration Statement

Country	Declaration	Country	Declaration
<b>cs</b> Česky [Czech]	OvisLink Corp. tímto prohlašuje, že tento WIAS-1200G je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.	<b>lt</b> Lietuvių [Lithuanian]	Šiuo OvisLink Corp. deklaruoja, kad šis WIAS-1200G atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
<b>da</b> Dansk [Danish]	Undertegnede OvisLink Corp. erklærer herved, at følgende udstyr WIAS-1200G overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.	<b>nl</b> Nederlands [Dutch]	Hierbij verklaart OvisLink Corp. dat het toestel WIAS-1200G in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
<b>de</b> Deutsch [German]	Hiermit erkläre OvisLink Corp., dass sich das Gerät WIAS-1200G in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.	<b>mt</b> Malti [Maltese]	Hawnhekk, OvisLink Corp, jiddikjara li dan WIAS-1200G jikkonforma mal-htigijiet essenzjali u ma provvedimenti oħrajn rilevanti li hemm fid-Dirrettiva 1999/5/EC.
<b>et</b> Eesti [Estonian]	Käesolevaga kinnitab OvisLink Corp. seadme WIAS-1200G vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.	<b>hu</b> Magyar [Hungarian]	Alulírott, OvisLink Corp nyilatkozom, hogy a WIAS-1200G megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EC irányelv egyéb előírásainak.
<b>en</b> English	Hereby, OvisLink Corp., declares that this WIAS-1200G is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.	<b>pl</b> Polski [Polish]	Niniejszym OvisLink Corp oświadcza, że WIAS-1200G jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
<b>es</b> Español [Spanish]	Por medio de la presente OvisLink Corp. declara que el WIAS-1200G cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.	<b>pt</b> Português [Portuguese]	OvisLink Corp declara que este WIAS-1200G está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
<b>el</b> Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ OvisLink Corp. ΔΗΛΩΝΕΙ ΟΤΙ WIAS-1200G ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/EK.	<b>sl</b> Slovensko [Slovenian]	OvisLink Corp izjavlja, da je ta WIAS-1200G v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
<b>fr</b> Français [French]	Par la présente OvisLink Corp. déclare que l'appareil WIAS-1200G est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE	<b>sk</b> Slovensky [Slovak]	OvisLink Corp týmto vyhlasuje, že WIAS-1200G spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
<b>it</b> Italiano [Italian]	Con la presente OvisLink Corp. dichiara che questo WIAS-1200G è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.	<b>fi</b> Suomi [Finnish]	OvisLink Corp vakuuttaa täten että WIAS-1200G tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen
<b>lv</b> Latviski [Latvian]	Ar šo OvisLink Corp. deklarē, ka WIAS-1200G atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.	<b>is</b> Íslenska [Icelandic]	Hér með lýsir OvisLink Corp yfir því að WIAS-1200G er í samræmi við grunnkröfur og aðrar kröfur, sem gerðar eru í tilskipun 1999/5/EC.
<b>sv</b> Svenska [Swedish]	Härmed intygar OvisLink Corp. att denna WIAS-1200G står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.	<b>no</b> Norsk [Norwegian]	OvisLink Corp erklærer herved at utstyret WIAS-1200G er i samsvar med de grunnleggende krav og øvrige relevante krav i direktiv 1999/5/EF.

A copy of the full CE report can be obtained from the following address:

**OvisLink Corp.**  
**5F, No.6 Lane 130,**  
**Min-Chuan Rd, Hsin-Tien City,**  
**Taipei, Taiwan, R.O.C.**

This equipment may be used in AT, BE, CY, CZ, DK, EE, FI, FR, DE, GR, HU, IE, IT, LV, LT, LU, MT, NL, PL, PT, SK, SI, ES, SE, GB, IS, LI, NO, CH, BG, RO, TR

This device uses software which is partly or completely licensed under the terms of the GNU General Public License. The author of the software does not provide any warranty. This does not affect the warranty for the product itself.

To get source codes please contact: OvisLink Corp., 5F, No. 96, Min-Chuan Rd, Hsin-Tien City, Taipei, Taiwan, R.O.C. A fee will be charged for production and shipment for each copy of the source code.

## GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.  
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.  
Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software—to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.  
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each license is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

- You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
- You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
- If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

- Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

## NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.  
END OF TERMS AND CONDITIONS  
How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

one line to give the program's name and an idea of what it does.

Copyright (C) yyyy name of author

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'. This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items—whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program `Gnomovision' (which makes passes at compilers) written by James Hacker.

signature of Ty Coon, 1 April 1989  
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License.

# Table of Contents

<b>1. Before You Start .....</b>	<b>1</b>
1.1 Audience .....	1
1.2 Document Conventions.....	1
<b>2. System Overview .....</b>	<b>2</b>
2.1 Introduction of AirLive WIAS-1200G.....	2
2.2 System Concept .....	3
2.3 Specification .....	4
2.3.1 Hardware Specification.....	4
2.3.2 Technical Specification .....	5
<b>3. Base Installation .....</b>	<b>7</b>
3.1 Hardware Installation.....	7
3.1.1 System Requirements.....	7
3.1.2 Package Contents .....	7
3.1.3 Panel Function Descriptions .....	8
3.1.4 Installation Steps.....	9
3.2 Quick Software Configuration.....	10
3.2.1 Instant Account .....	10
3.2.2 Configuration Wizard.....	14
<b>4. Web Interface Configuration.....</b>	<b>21</b>
4.1 System Configuration .....	22
4.1.1 Configuration Wizard.....	22
4.1.2 System Information.....	23
4.1.3 WAN Configuration .....	25
4.1.4 LAN1 & LAN2 Configuration.....	27
4.1.5 LAN3 & LAN4 Configuration.....	29
4.1.6 Wireless Configuration .....	31
4.2 User Authentication .....	36
4.2.1 Authentication Configuration .....	36
4.2.2 Black List Configuration.....	61
4.2.3 Policy Configuration .....	62
4.2.4 Guest User Configuration .....	64
4.2.5 Additional Configuration .....	65
4.3 Network Configuration .....	81
4.3.1 Network Address Translation.....	82
4.3.2 Privilege List.....	84
4.3.3 Monitor IP List.....	86

4.3.4	Walled Garden List .....	87
4.3.5	Proxy Server Properties .....	88
4.3.6	Dynamic DNS .....	89
4.4	Utilities.....	90
4.4.1	Network Utilities.....	91
4.4.2	Change Password .....	92
4.4.3	Backup/Restore Setting.....	95
4.4.4	Firmware Upgrade .....	96
4.4.5	Restart .....	96
4.5	Status.....	97
4.5.1	System Status .....	98
4.5.2	Interface Status.....	100
4.5.3	Current Users .....	102
4.5.4	Traffic History.....	103
4.5.5	Notify Configuration.....	104
4.6	Help.....	105
	<b>Appendix A – Console Interface .....</b>	<b>106</b>
	<b>Appendix B – Accepting Payments via Authorize.Net .....</b>	<b>109</b>
	<b>Appendix C – Accepting Payments via PayPal .....</b>	<b>115</b>
	<b>Appendix D – Examples of Making Payments for End Users .....</b>	<b>122</b>
	<b>Appendix E – Proxy Setting for Hotspot .....</b>	<b>128</b>
	<b>Appendix F – Proxy Setting for Enterprise.....</b>	<b>131</b>
	<b>Appendix G – Disclaimer for On-Demand Users .....</b>	<b>136</b>
	<b>Appendix H – Network Configuration &amp; External Network Access .....</b>	<b>145</b>
	<b>Appendix I – Common Settings .....</b>	<b>161</b>



# 1. Before You Start

## 1.1 Audience

This manual is for Hotspot owners or administrators in enterprises to set up network environment using AirLive WIAS-1200G. It contains step by step procedures and graphic examples to guide MIS staff or individuals with slight network system knowledge to complete the installation.

## 1.2 Document Conventions

- For any caution or warning that requires special attention of readers, a highlight box with the eye-catching italic font is used as below:

**Note:** *For security purposes, you should immediately change the Administrator's password.*



indicates that clicking this button will return to the homepage of this section.



indicates that clicking this button will return to the previous page.



indicates that clicking this button will apply all of your settings.



indicates that clicking this button will clear what you set before these settings are applied.

## 2. System Overview

### 2.1 Introduction of AirLive WIAS-1200G

AirLive WIAS-1200G is an all-in-one product specially designed for small wireless network environment. It integrates “**Access Control**” and “**Wireless Network Access**” into one system to fulfill the needs in Hotspot environment. AirLive WIAS-1200G supports 802.11b and 802.11g dual wireless transmission modes and at the same time incorporates “**convenience**”, “**efficiency**”, “**friendly**” and other useful characteristics for services.

- **Quick Installation Get Online Immediately**

The installation and setup of AirLive WIAS-1200G can be easily done without changing the existing network architecture. The system can be installed and logged within a short amount of time to establish the security mechanism. With the protection by AirLive WIAS-1200G, users must be authenticated before logging in to the network, and the administrator can assign a fine-grained priority to each user stratifying the scope and right of using network resources.

- **Friendly Management and Application Interfaces**

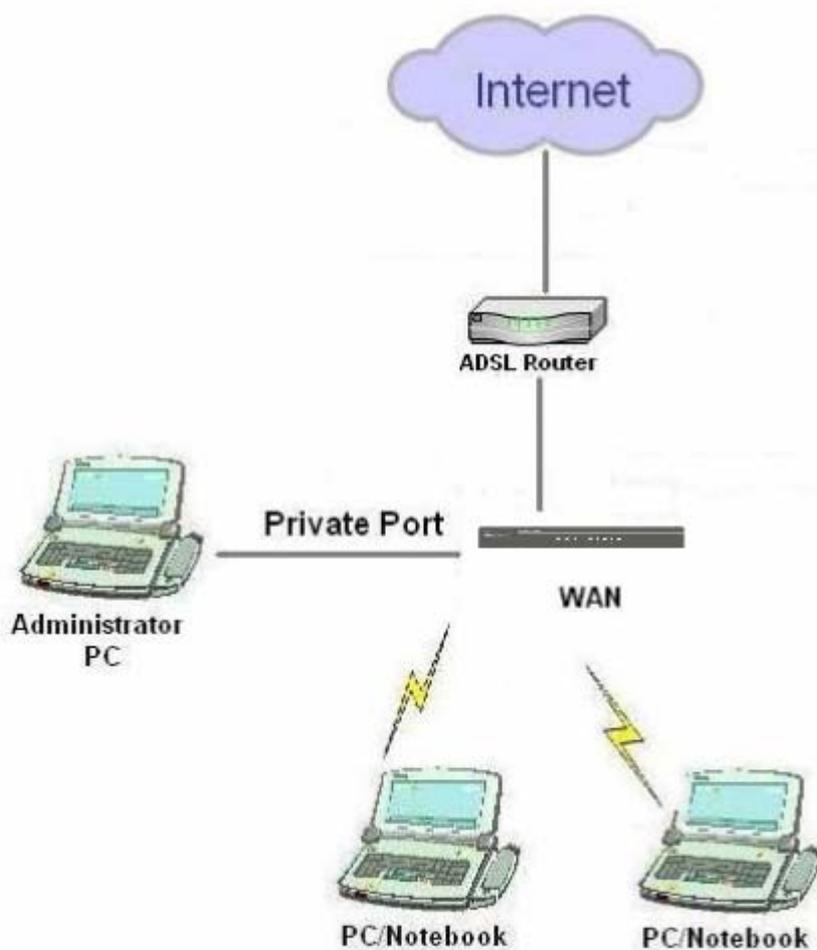
AirLive WIAS-1200G is easy to install. All of the functions of the system can be performed with a simple few clicks. The full web-based management interface allows users to operate and manage the system online via browsers. Users can easily log on to the system via browsers without any additional software installation.

- **Integrating the Existing User Password Database**

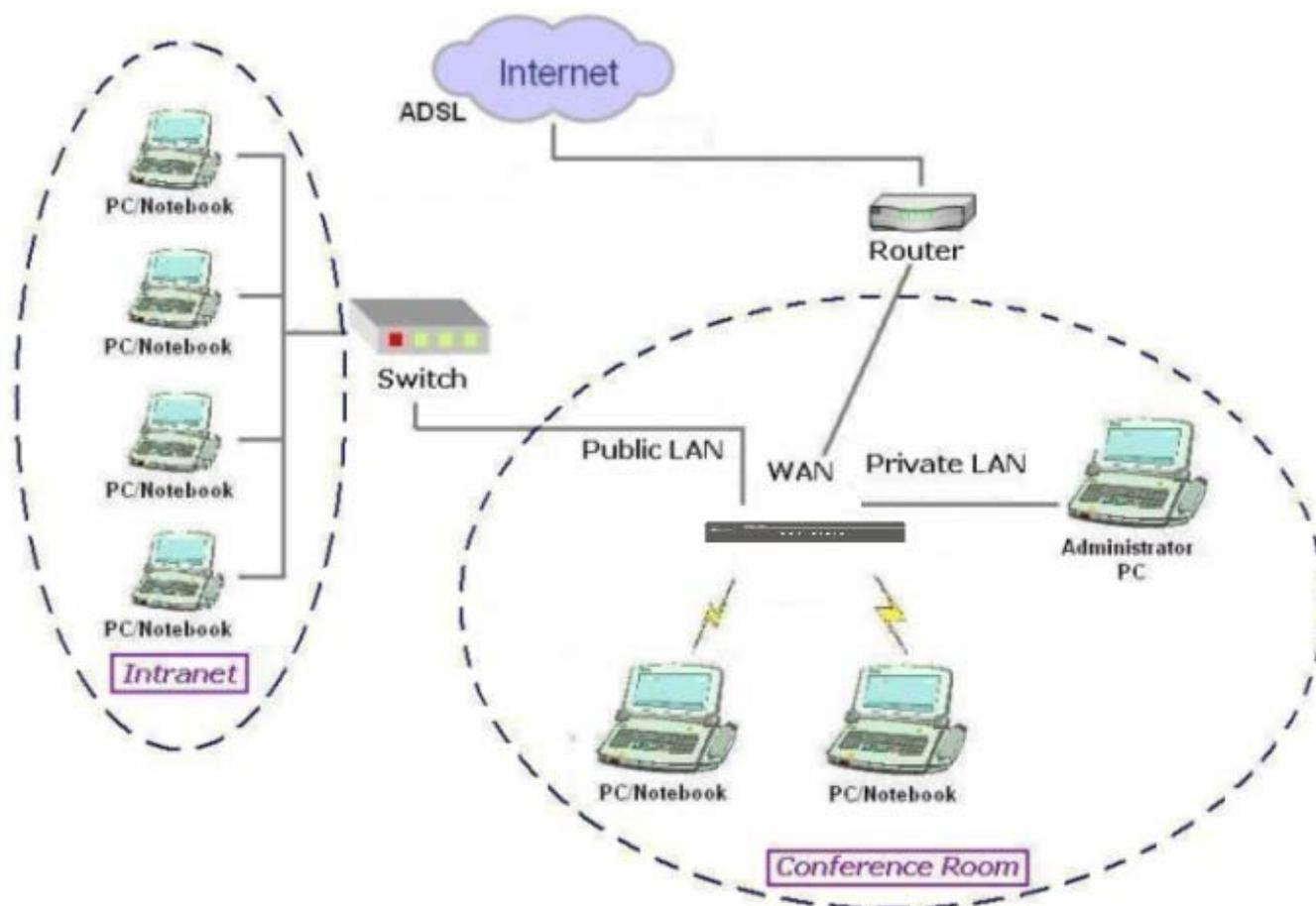
In general, most organizations use specific database system to centrally manage user passwords. AirLive WIAS-1200G supports POP3 (+SSL), RADIUS, LDAP and NT Domain external authentication methods, and allows integration of the current user password database. This system also provides a built-in local user database.

## 2.2 System Concept

AirLive WIAS-1200G is responsible for user authentication, authorization and management. The user account information is stored in the local database or a specified external databases server. The user authentication is processed via the SSL encrypted web interface. This interface is compatible to most desktop devices and palm computers. The following figure is an example of AirLive WIAS-1200G set to control a part of the company's intranet. The whole managed network includes the cable network users and the wireless network users.



The users located at the managed network will be unable to access the network resource without permission. When the browser of a user attempts to connect to a website, the AirLive WIAS-1200G will force the browser to redirect to the user login webpage. The user must enter the username and password for authentication. After the identity is authenticated successfully, the user will gain proper access right defined on the AirLive WIAS-1200G.



## 2.3 Specification

### 2.3.1 Hardware Specification

- Dimensions: 300mm(W) x156mm(D) x 43mm(H)
- Weight: 1.4Kg
- Power: DC12V/2A
- 5 Fast Ethernet
- 1 RS-232 DB9 Console Port
- Built-in 802.11b/g Access Point

## 2.3.2 Technical Specification

- **Standards**

This system supports IEEE 802.1x, 802.11b and 802.11g

- **Networking**

WAN interface supports Static IP, DHCP client, PPPoE client, and PPTP client

Supports NAT mode and Router mode

Built-in DHCP server

Built-in NTP client

Supports Redirect of network data

Supports IPSec (ESP), PPTP and H.323 pass through (under NAT)

Customizable static routing table

Supports Virtual Server

Supports DMZ Server

Supports machine operation status monitoring and reporting system

- **Firewall**

Supports DoS

Customizable packet filtering rules

Customizable walled garden (free surfing area)

- **User Management**

Supports at least 500 on-line users concurrently

Supports Local, POP3 (+SSL), RADIUS, LDAP, and NT Domain authentication mechanisms

Can choose MAC address locking for built-in user database

Can set the time for the user to log in to the system

Can set the user's idle time

Can specify the MAC addresses to enter the managed network without authentication

Can specify the IP addresses to enter the managed network without authentication

Supports the setting to pass or block all the connections when the WAN interface failed

Supports web-based login

Supports several friendly logout methods

Supports RADIUS accounting protocol to generate the billing record on RADIUS server

- **Administration**

Provides online status monitoring and history traffic

Supports SSL encrypted web administration interface and user login interface

Customizable user login & logout web interface

Customizable redirect after users are successfully authenticated during login & logout

Supports Console management interface

Supports SSH remote administration interface

Supports web-based administration interface

Supports SNMP v2

Supports user's bandwidth restriction

Supports remote firmware upgrade

- **Accounting**

Supports built-in user database and RADIUS accounting

## 3. Base Installation

### 3.1 Hardware Installation

#### 3.1.1 System Requirements

- Standard 10/100BaseT including five network cables with RJ-45 connectors
- All PCs need to install the TCP/IP network protocol

#### 3.1.2 Package Contents

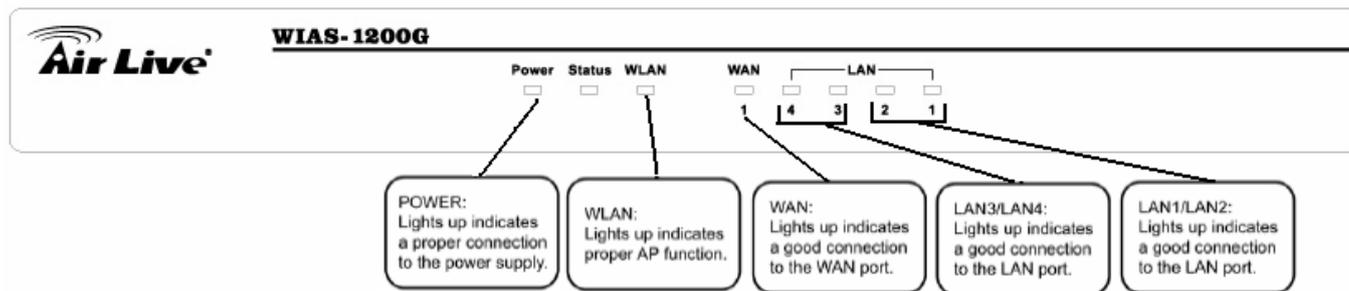
The standard package of AirLive WIAS-1200G includes:

- AirLive WIAS-1200G x 1
- Quick Installation Guide x 1
- CD-ROM x 1
- Console Cable x 1
- Straight-through Ethernet Cable x 1
- Power Adaptor x 1
- Power Cord x 1
- 5dBi Omni-antenna x 2

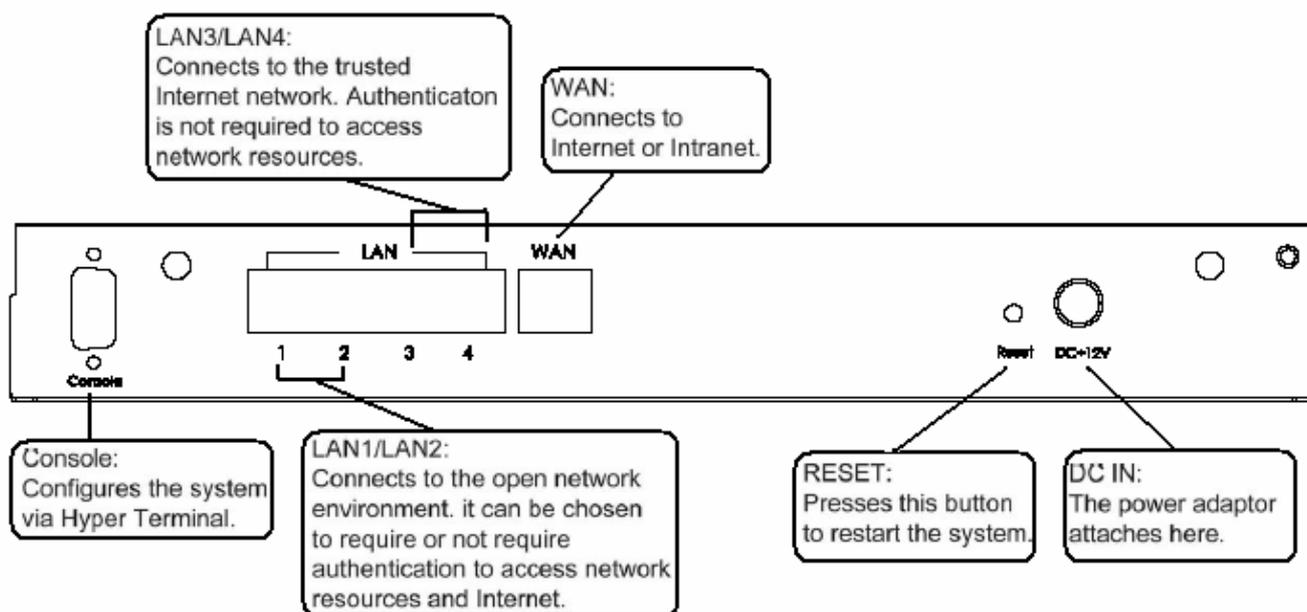
**Note:** Using a power supply with different voltage rating will damage this product.

### 3.1.3 Panel Function Descriptions

#### Front Panel



#### Rear Panel

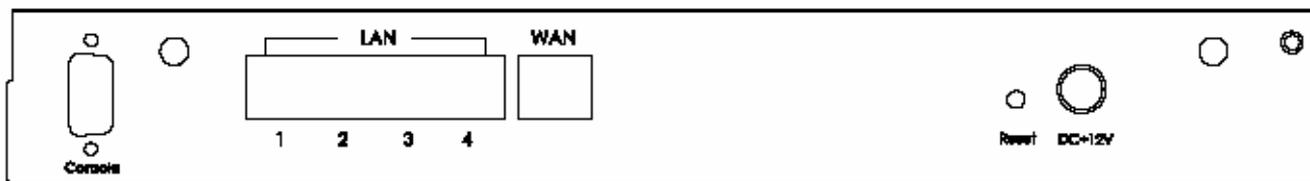


- **DC IN:** The power adaptor attaches here.
- **RESET:** Press this button to restart the system.
- **WAN:** The WAN port is used to connect to a network which is not managed by the AirLive WIAS-1200G, and this port can be used to connect the ATU-Router of ADSL, the port of Cable Modem, or the Switch or Hub on the LAN of a company.
- **LAN1/LAN2:** The two LAN ports are connected to the managed network or WLAN. They can be selected to require or not require authentication to access network resources and Internet.
- **LAN3/LAN4:** The two LAN ports are connected to a trustful network where the users can always use the network resources without authentication. This port can be connected to a server such as File Server or a Database Server, etc.
- **Console:** The system can be configured via HyperTerminal. For example, if you need to set the Administrator's Password, you can connect a PC to this port as a Console Serial Port via a terminal connection program (such as the super terminal with the parameters of 9600, 8, N, 1, None flow control) to change the Administrator's Password. Meanwhile, it also can connect to TP-1000 ticket printer for printing On-demand User ticket.



### 3.1.4 Installation Steps

Please follow the following steps to install AirLive WIAS-1200G:



2,3,4 Ethernet Cable



1 - DC Power Adaptor

1. Connect the power adapter to the power socket on the rear panel. If the power supply and connection is normal, the Power LED on the front panel will light up.
2. Connect an Ethernet cable to the WAN Port on the rear panel. Connect the other end of the Ethernet cable to an ADSL modem, a cable modem or a switch/hub of the internal network. The LED of the WAN on the front panel should be on to indicate a proper connection.
3. Connect an Ethernet cable to the LAN1/LAN2 Port on the rear panel. Connect the other end of the Ethernet cable to an AP or a switch. The LED of LAN1/LAN2 should be on to indicate a proper connection. (Note: Authentication is required for the clients to access the network via the LAN1/LAN2 Port. The LAN port with authentication required is referred to as **Public LAN**.)
4. Connect an Ethernet cable to the LAN3/LAN4 Port on the rear panel. Connect the other end of the Ethernet cable to a networking device such as the administrator's PC. The LED of LAN3/LAN4 should be on to indicate a proper connection. (Note: Authentication is NOT required for the clients to access the network via the LAN3/LAN4 Port. The LAN port without authentication required is referred to as **Private LAN**.)

After the hardware of AirLive WIAS-1200G is installed completely, the system is ready to be configured in the following sections. The manual will guide you step by step to set up the system using a single AirLive WIAS-1200G to manage the network.

## 3.2 Quick Software Configuration

There are two simple ways to configure the system: **Instant Account** and **Configuration Wizard**.

### 3.2.1 Instant Account

WIAS-1200G provides three different level account; **admin**, **manager** and **operator**. The default username and password as follows:

**Admin:** The administrator can access all area of the AirLive WIAS-1200G.

User Name: **admin**

Password: **airlive**

**Manager:** The manager only can access the area under **User Authentication** to manager the user account, but no permission to change the settings of the profiles of Firewall, Specific Route and Schedule.

User Name: **manager**

Password: **airlive**

**Operator:** The operator only can access the area of **Create On-demand User** to create and print out the new on-demand user accounts.

User Name: **operator**

Password: **airlive**

Each account owns the specific access right:

The network constructor can deploy the default system by **admin** account;

The system manager can change or create further authentication rule by **manager** account;

The operator just needs to create new account and print out the ticket for customer by **operator** account.

Following is the example to configure the system per different user account:

For admin account:

1. Select the Connection Type for WAN Port
2. Choose System's Time Zone
3. Configure Policy setting based on customer's request

For manager account:

1. Set up Authentication Configuration for on-demand User Server Configuration
2. Change Billing Configuration
3. Select the Policy, Total bandwidth, Individual Maximum Bandwidth, and Individual Request Bandwidth.

For operator account:

1. Create new account
2. Print out the ticket

Please check the following steps to complete the quick configuration

**Login with admin account:**

1. Select **System Configuration** → **WAN Configuration**, and set up the WAN type and enter the necessary data. For more detail information please check chapter 4.1.3 WAN configuration.

The screenshot shows the 'WAN Configuration' interface. Under the 'WAN Port' section, the 'Static IP Address' option is selected. The fields are filled with: IP Address: 60.250.158.65, Subnet Mask: 255.255.255.0, Default Gateway: 60.250.158.254, Preferred DNS Server: 168.95.1.1, and Alternate DNS Server: (empty). Below these are radio buttons for 'Dynamic IP Address', 'PPPoE Client', and 'PPTP Client'. At the bottom are 'Apply' and 'Clear' buttons.

2. Select **System Configuration** → **System Information**, configure the correct Time Zone and select to enable NTP server or set up time by manually.

The screenshot shows the 'System Information' interface. The 'Device Time' is 2007/06/04 20:17:26. The 'Time Zone' is set to '(GMT+08:00)Taipei'. Under the 'Time' section, the 'NTP Enable' option is selected. Five NTP servers are listed: 1: tock.usno.navy.mil, 2: ntp1.fau.de, 3: clock.cuhk.edu.hk, 4: ntps1.pads.ufrj.br, and 5: ntp1.cs.mu.OZ.AU. There is also an option for 'Set Device Date and Time'.

3. Select **User Authentication** → **Policy Configuration**, to define Policy A with configuring specific Firewall Profile, Route Profile, and Schedule Profile.

The screenshot shows the 'Policy Configuration' interface. 'Select Policy:' is set to 'Policy A'. The settings are: Firewall Profile: [Setting](#), Specific Route Profile: [Setting](#), Schedule Profile: [Setting](#), Total Bandwidth: 1 Mbps, Individual Maximum Bandwidth: 256 Kbps, and Individual Request Bandwidth: 128 Kbps. At the bottom are 'Apply' and 'Clear' buttons, and social media icons for Facebook and Twitter.

**Login with manager account:**

1. Select **User Authentication** → **Authentication Configuration** → **On-demand User**; in this item you can define the Postfix name, Monetary Unit, WALN ESSID and the other information if needed.

2. Select **User Authentication** → **Authentication Configuration** → **On-demand User** → **Billing Configuration**, define the related information based on your policy. The contents include Pay for data or Pay for time, account expiration time, account valid time, policy name and price.

3. Select **User Authentication** → **Policy Configuration**, and define the **Total Bandwidth**, **Individual Maximum Bandwidth**, and **Individual Request Bandwidth**.

Login with operator account:

1. Click Create to create a new account.

Create On-demand User			
Plan	Type	Status	Function
1	2 hrs 0 mins	Enabled	Create
2	N/A	Disabled	Create
3	N/A	Disabled	Create
4	N/A	Disabled	Create
5	N/A	Disabled	Create
6	N/A	Disabled	Create
7	N/A	Disabled	Create
8	N/A	Disabled	Create
9	N/A	Disabled	Create
0	N/A	Disabled	Create

2. Click Printout to print ticket.

Welcome!	
Username	U483@airlive
Password	V84K3NCS
Price	20
Usage	2 hrs 0 mins
ESSID : airlive	
Wireless Key :	
You first time login must be done before 2007/06/07 20:57:05	
The account is valid within 5 days after your first login.	

**Pls wait for login page.**

Printout      Close

Following is the list to display the access right of WIAS-1200G feature per each account:

		admin	manager	operator
<b>System Configuration</b>		Y	--	--
<b>User Authentication</b>	Authentication Configuration	Y	Y	--
	Black List Configuration	Y	Y	--
	Policy Configuration	Y	--	--
	Guest User Configuration	Y	Y	--
	Additional Configuration	Y	Y	--
<b>Network Configuration</b>		Y	--	--
<b>Utility</b>		Y	--	--
<b>Status</b>		Y	--	--

## 3.2.2 Configuration Wizard

The Configuration Wizard has 7 steps providing a simple and easy way to guide you through the setup of AirLive WIAS-1200G. You just need to follow the procedures and instructions given by the Wizard to enter the required information step by step. After saving and restarting AirLive WIAS-1200G, it is ready to use. There will be 7 steps as listed below:

1. Change Admin's Password
2. Choose System's Time Zone
3. Set System Information
4. Select the Connection Type for WAN Port
5. Set Authentication Methods
6. Set Wireless – Access Point Connection
7. Save and Restart AirLive WIAS-1200G

Please follow the following steps to complete the quick configuration

1. Use the network cable of the 10/100BaseT to connect PC to the LAN3/LAN4 port, and then start a browser (such as Microsoft IE). Next, enter the gateway address for that port, the default is <https://192.168.2.254>. Next, the Administrator Login Page will appear on the browser. Enter "**admin**", the default username, and "**airlive**", the default password, in the User Name and Password fields. Click **Enter** to log in.



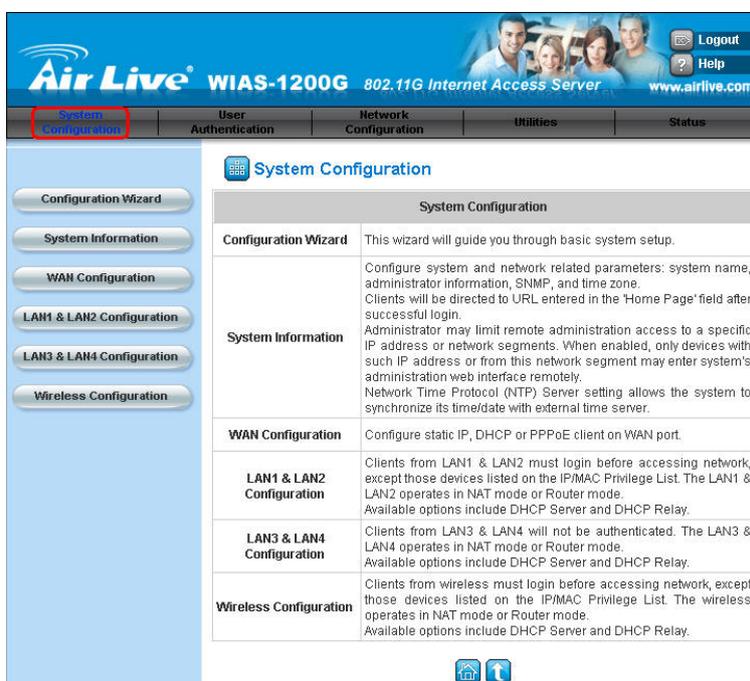
**Note:**

*If you can't get the login screen, you may have incorrectly set your PC to obtain an IP address automatically from authentication LAN port or the IP address used does not have the same subnet as the URL. Please use default IP address such as 192.168.2.xx in your network and then try it again.*

- After successfully logging into AirLive WIAS-1200G, a web management interface with a welcome message will appear. To logout, simply click the **Logout** on the upper right corner of the interface to return.



- Then, run the configuration wizard to complete the configuration. Click **System Configuration** to the **System Configuration** homepage.



- Click the **System Configuration** from the top menu and the homepage of **System Configuration** will appear. Then, click on **Configuration Wizard** and click the **Run Wizard** button to start the wizard.



## 5. Configuration Wizard

A welcome screen that briefly introduces the 7 steps will appear. Click **Next** to begin.

- **Step 1. Change Admin's Password**

Enter a new password for the admin account and retype it in the Verify Password field (maximum characters are twenty and no spaces are allowed). Click **Next** to continue.

- **Step 2. Choose System's Time Zone**

Select a proper time zone via the drop-down menu. Click **Next** to continue.

- **Step 3. Set System Information**

**Home Page:** Enter the URL that clients should be initially redirected to after successfully authenticated to the network.

**NTP Server:** Enter the URL of the external time server for AirLive WIAS-1200G time synchronization or use the default.

**DNS Server:** Enter a DNS Server provided by your ISP (Internet Service Provider). Contact your ISP if you are not sure of DNS IP Address.

Click **Next** to continue.

### Configuration Wizard

Welcome to the Setup Wizard. The wizard will guide you through these 7 quick steps. Begin by clicking on Next.

Step 1. Change Admin's Password

Step 2. Choose System's Time Zone

Step 3. Set System Information

Step 4. Select the Connection Type for WAN Port

Step 5. Set Authentication Methods

Step 6. Set Wireless-Access Point Connection

Step 7. Save and Restart WIAS-1200G

Next

Exit

### Step 1. Change Admin's Password

You may change the Admin's account password by entering in a new password. Click Next to continue.

New Password:

Verify Password:

Back

Next

Exit

### Step 2. Choose System's Time Zone

Select the appropriate time zone for the system. Click Next to continue.

(GMT+08:00)Taipei

Back

Next

Exit

### Step 3. Set System Information

Enter System Information. Click Next to continue.

Home Page:

(e.g. http://www.airlive.com/)

NTP Server:

(e.g. tock.usno.navy.mil)

DNS Server:



- **Step 4. Select the Connection Type for WAN Port**  
There are three types of WAN port to select: **Static IP Address**, **Dynamic IP Address** and **PPPoE Client**.  
Select a proper Internet connection type and click **Next** to continue.

➤ **Dynamic IP Address**

If this option is selected, an appropriate IP address and related information will automatically be assigned.

Click **Next** to continue.

➤ **Static IP Address: Set WAN Port's Static IP Address**

Enter the "IP Address", "Subnet Mask" and "Default Gateway" provided by the ISP.

Click **Next** to continue.

➤ **PPPoE Client: Set PPPoE Client's Information**

Enter the "Username" and "Password" provided by the ISP.

Click **Next** to continue.

- **Step 5. Set Authentication Methods**

Please specify the postfix name for this authentication method. The **Postfix** field (e.g. Local) will be used as the postfix name (e.g. username@Local). A policy can be chosen to apply to this authentication method.

An authentication method has to be selected from one of the five options appeared in this window (Local User is selected for this example). Local User is an authentication method that uses the built-in user database supported by AirLive WIAS-1200G.

Click **Next** to continue.

Step 4. Select the Connection Type for WAN Port

Select the connection type for WAN port. Click Next to continue.

- Static IP Address Choose it to set static IP address.
- Dynamic IP Address Choose it to obtain an IP address automatically. (For most cable modem users.)
- PPPoE Client Choose it to set the PPPoE Client's Username and Password. (For most DSL users.)

Back Next Exit

Step 4 (Cont). Set WAN Port's Static IP Address

Click Next to continue.

IP Address:

Subnet Mask:

Default Gateway:

Back Next Exit

Step 4 (Cont). Set PPPoE Client's Information

Choose it to set the PPPoE Client's Username and Password. (For most DSL users.)

Username:

Password:

Step 5. Set Authentication Methods

Select a default User Authentication Method. Click Next to continue.

Postfix:  (Its postfix name.)

Policy:

Local User  LDAP

POP3  NT Domain

RADIUS

Back Next Exit

➤ **Local User: Add User**

A new user can be added to the local user data base. To add a user here, enter the **Username** (e.g. test), **Password** (e.g. test), and **MAC** (optional). Assign a policy to add this particular local user (or use the default). Upon completing a user adding, more users can be added to this authentication method by clicking the **ADD** bottom.

Click **Next** to continue.

➤ **POP3 User: POP3**

Enter IP/Domain Name and server port of the POP3 server provided by your ISP, and then choose enable SSL or not.

Click **Next** to continue.

➤ **RADIUS User: RADIUS**

Enter RADIUS server IP/Domain Name, authentication port, accounting port and secret key. Then choose to enable accounting service or not, and choose the desired authentication method.

Click **Next** to continue.

➤ **LDAP User: LDAP**

You can add a new user to the LDAP user data base. Enter the “**LDAP Server**”, “**Server Port**”, and “**Base DN**”.

Click **Next** to continue.

**Step 5 (Cont). Add User**

Click "ADD" button to add Local User. Click Next to continue.

Username:

Password:

MAC:  (XXXXXXXXXXXX)

Policy: None ▾

**Step 5 (Cont). POP3**

Configure POP3 Server information. Click Next to continue.

POP3 Server:  \*(Domain Name/IP)

Server Port:  \*(Default: 110)

Enable SSL

**Step 5 (Cont). RADIUS**

Configure RADIUS Server information. Click Next to continue.

RADIUS Server:  \*(Domain Name/IP)

Authentication Port:  \*(Default: 1812)

Accounting Port:  \*(Default: 1813)

Secret Key:  \*

Accounting Service: Disable ▾ \*

Authentication Method: PAP ▾ \*

**Step 5 (Cont). LDAP**

Configure LDAP Server information. Click Next to continue.

LDAP Server:  \*(Domain Name/IP)

Server Port:  \*(Default: 389)

Base DN:  \*(CN=,dc=,dc=)

Account Attribute:  \*(Default: uid)

➤ **NT Domain User: NT Domain**

When NT Domain User is selected, enter the information for “**Server IP Address**”, and choose to enable/disable “**Transparent Login**”.

If “Transparent Login” is enabled, users are logged in AirLive WIAS-1200G’s NT Domain active directory and authenticated automatically when they log into their Windows OS domain.

Click **Next** to continue.

Step 5 (Cont). NT Domain

Configure NT Domain Server information. Click **Next** to continue.

Server IP Address:  \*

Transparent Login

**Back** **Next** **Exit**

• **Step 6. Set Wireless – Access Point Connection**

**SSID:** Enter a SSID (up to 32 characters) for system. The default is **AirLive SSID (Service Set Identifier)** is a unique identifier used for the wireless client’s devices to associate with the built in AP of AirLive WIAS-1200G.

**Transmission Mode:** AirLive WIAS-1200G supports two transmission modes, **802.11b** and **802.11 (b+g)**. Select the appropriate transmission mode to work with the wireless clients in the network.

**Channel:** Select a channel from the “**Channel**” field for AirLive WIAS-1200G to function properly.

Step 6. Set Wireless Access-Point Connection

Enter the SSID name and channel number to be used for the Wireless Access-Point. Click **Next** to continue.

SSID:  \*

Transmission Mode:  ▼

Channel:  ▼

**Back** **Next** **Exit**

**Note:** The available channels depend upon the region. For instance, Channel 1~11 are available in Taiwan, and Channel 1-13 are available in Europe.

• **Step 7. Save and Restart AirLive WIAS-1200G**

Click **Restart** to save the current settings and restart AirLive WIAS-1200G. The Setup Wizard is now completed.

Step 7. Save and Restart WIAS-1200G

The Setup Wizard has completed. Click on **Back** to modify changes or mistakes. Click **Restart** to save the current settings and reboot.

**Back** **Restart** **Exit**

- **Setup Wizard.** During AirLive WIAS-1200G restart, a “Restarting now. Please wait for a while.” message will appear on the screen. Please do not interrupt AirLive WIAS-1200G until the message has disappeared. This indicates that a complete and successful restart process has finished.



Restarting now. Please wait for a moment...

**Note:** During every step of the wizard, click the **Back** button to go back to the previous step if you wish to go back to modify the settings. For more details about Network Configuration, please refer to Appendix H.

## 4. Web Interface Configuration

This chapter will guide you through further detailed settings. The following table shows all the functions of AirLive WIAS-1200G.

System Configuration	User Authentication	Network Configuration	Utilities	Status
----------------------	---------------------	-----------------------	-----------	--------

Welcome to System Administration

This Administrative Web Interface allows you to set various networking parameters, to customize network services, to manage user accounts and to monitor user status.

Functions are separated into 5 main categories:

[System Configuration](#) , [User Authentication](#) , [Network Configuration](#) , [Utilities](#) and [Status](#).

OPTION	System Configuration	User Authentication	Network Configuration	Utilities	Status
FUNCTION	Configuration Wizard	Authentication Configuration	Network Address Translation	Network Utilities	System Status
	System Information	Black List Configuration	Privilege List	Change Password	Interface Status
	WAN Configuration	Policy Configuration	Monitor IP List	Backup/Restore Settings	Current Users
	LAN1 & LAN2 Configuration	Guest User Configuration	Walled Garden List	Firmware Upgrade	Traffic History
	LAN3 & LAN4 Configuration	Additional Configuration	Proxy Server Properties	Restart	Notify Configuration
	Wireless Configuration		Dynamic DNS		

**Note:** After finishing the configuration of the settings, please click **Apply** and pay attention to see if a restart message appears on the screen. If such message appears, system must be restarted to allow the settings to take effect. All on-line users will be disconnected during restart.

## 4.1 System Configuration

This section includes the following functions: **Configuration Wizard**, **System Information**, **WAN Configuration**, **LAN1 & LAN2 Configuration**, **LAN3 & LAN4 Configuration** and **Wireless Configuration**.

System Configuration	
<b>Configuration Wizard</b>	This wizard will guide you through basic system setup.
<b>System Information</b>	Configure system and network related parameters: system name, administrator information, SNMP, and time zone. Clients will be directed to URL entered in the 'Home Page' field after successful login. Administrator may limit remote administration access to a specific IP address or network segments. When enabled, only devices with such IP address or from this network segment may enter system's administration web interface remotely. Network Time Protocol (NTP) Server setting allows the system to synchronize its time/date with external time server.
<b>WAN Configuration</b>	Configure static IP, DHCP or PPPoE client on WAN port.
<b>LAN1 &amp; LAN2 Configuration</b>	Clients from LAN1 & LAN2 must login before accessing network, except those devices listed on the IP/MAC Privilege List. The LAN1 & LAN2 operates in NAT mode or Router mode. Available options include DHCP Server and DHCP Relay.
<b>LAN3 &amp; LAN4 Configuration</b>	Clients from LAN3 & LAN4 will not be authenticated. The LAN3 & LAN4 operates in NAT mode or Router mode. Available options include DHCP Server and DHCP Relay.
<b>Wireless Configuration</b>	Clients from wireless must login before accessing network, except those devices listed on the IP/MAC Privilege List. The wireless operates in NAT mode or Router mode. Available options include DHCP Server and DHCP Relay.

### 4.1.1 Configuration Wizard

There are two ways to configure the system: using **Configuration Wizard** or change the setting by demands manually. The Configuration Wizard has 7 steps providing a simple and easy way to go through the basic setups of AirLive WIAS-1200G and is served as **Quick Configuration**. Please refer to **3.2.2 Quick Configuration** for the introduction and description of **Configuration Wizard**.

**Configuration Wizard**

**WIAS-1200G is an Ethernet Broadband Router with access control features ideal for hotspot, small business and enterprise networking. The wizard will guide you through the process of creating a baseline strategy. Please follow the wizard step by step to configure WIAS-1200G.**

**Run Wizard**

## 4.1.2 System Information

These are some main information about AirLive WIAS-1200G. Please refer to the following description for these blanks:

System Information	
System Name	AirLive WIAS-1200G
Administrator Info	Sorry! The service is temporarily unavailable. <small>(It'll appear when Internet connection fails.)</small>
Device Name	<input type="text"/> <small>(FQDN for this device)</small>
Home Page	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <input type="text" value="http://www.airlive.com/"/> * <small>(e.g. http://www.airlive.com/)</small>
Access History IP	<input type="text"/> <small>(e.g. 192.168.2.1)</small>
Remote Management IP	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
SNMP	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
User Logon SSL	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Time	Device Time : 2007/06/08 06:34:05 Time Zone: <input type="text" value="(GMT+08:00)Taipei"/> <input type="button" value="v"/> <input checked="" type="radio"/> NTP Enable NTP Server 1: <input type="text" value="tock.usno.navy.mil"/> * <small>(e.g. tock.usno.navy.mil)</small> NTP Server 2: <input type="text" value="ntp1.fau.de"/> NTP Server 3: <input type="text" value="clock.cuhk.edu.hk"/> NTP Server 4: <input type="text" value="ntp1.pads.ufrj.br"/> NTP Server 5: <input type="text" value="ntp1.cs.mu.OZ.AU"/> <input type="radio"/> Set Device Date and Time

- **System Name:** Set the system's name or use the default.
- **Administrator Info:** Enter the Administrator's information here, such as administrator's name, telephone number, e-mail address, etc. If users encountered problems in the connection of the WAN port to the system, this information will appear on the user's login screen.
- **Home Page:** Enter the website of a Web Server to be the homepage. When users log in successfully, they will be directed to the homepage set. Usually, the homepage is the company's website, such as <http://www.airlive.com>. Regardless of the original webpage set in the users' computer, they will be redirect to this page after login.
- **Access History IP:** Specify an IP address of the administrator's computer or a billing system to get billing history information of AirLive WIAS-1200G.

Traffic History : <https://10.2.3.213/status/history/2005-02-17>

#Date	TYPE	Name	IP	MAC	Packets In	Bytes In	Packets Out	Bytes Out
2005-02-17 18:09:03 +0800	LOGIN			aaa@w1300.tw	192.168.30.189	00:0C:F1:28:BF:D8	0	0

On-demand History : [https://10.2.3.213/status/ondemand\\_history/2005-02-17](https://10.2.3.213/status/ondemand_history/2005-02-17)

#Date	System Name	Type	Name	IP	MAC	Packets In	Bytes In	Packets Out	Bytes Out	Expiretime	Valid
2005-02-17 16:44:19 +0800	QA-W1300-Casper-213	Create_OD_User	N7E9	0.0.0.0	00:00:00:00:00:00	0	0	0	0	0	0
2005-02-17 16:44:57 +0800	QA-W1300-Casper-213	OD_User_Login	N7E9	192.168.30.189	00:0C:F1:28:BF:D8	0	0	0	0	0	0
2005-02-17 16:45:22 +0800	QA-W1300-Casper-213	OD_User_Logout	N7E9	192.168.30.189	00:0C:F1:28:BF:D8	32	14499	30			

- **Remote Management IP:** Set the IP block with a system which is able to connect to the web management interface via the authenticated port. For example, 10.2.3.0/24 means that as long as you are within the IP address range of 10.2.3.0/24, you can reach the administration page of AirLive WIAS-1200G. Another example is 10.0.0.3, if you are using the IP address 10.0.0.3, you can reach the administration page of AirLive WIAS-1200G. If you would like to allow any IP address to access the remote management, enter the address range with 0.0.0.0/0.0.0.0. The default setting is to disable remote managed function.
- **SNMP:** AirLive WIAS-1200G supports SNMPv2. If the function is enabled, you can assign the Manager IP address and the SNMP community name used to access the management information base (MIB) of the system.
- **User logon SSL:** Enable to activate https (encryption) or disable to activate http (non encryption) login page.
- **Time:** AirLive WIAS-1200G supports NTP communication protocol to synchronize the network time. Please specify the IP address of a server in the system configuration interface for adjusting the time automatically. (Universal Time is Greenwich Mean Time, GMT). You can also set the time manually when you select “**Set Device Date and Time**”. Please enter the date and time for these field.

<b>Time</b>	Device Time : 2005/03/03 10:43:08
	<input type="radio"/> NTP Enable
	<input checked="" type="radio"/> Set Device Date and Time
	Year: <input type="text" value="--"/> Month: <input type="text" value="--"/> Day: <input type="text" value="--"/>
	Hour: <input type="text" value="--"/> Minute: <input type="text" value="--"/> Second: <input type="text" value="--"/>



## 4.1.3 WAN Configuration

There are 4 methods of obtaining IP address for the WAN Port: **Static IP Address**, **Dynamic IP Address**, **PPPoE** and **PPTP Client**.

The screenshot shows the 'WAN Configuration' window. On the left, 'WAN Port' is listed. The main area has four radio buttons: 'Static IP Address' (selected), 'Dynamic IP Address', 'PPPoE Client', and 'PPTP Client'. Below the radio buttons are five input fields: 'IP Address', 'Subnet Mask', 'Default Gateway', 'Preferred DNS Server' (with the value '168.95.1.1'), and 'Alternate DNS Server'. Each of these five input fields has a red asterisk to its right, indicating they are required.

- **Static IP Address:** Manually specifying the IP address of the WAN Port is applicable for the network environment where the DHCP service is unavailable. The fields with red asterisks are required to be filled in.

**IP address:** the IP address of the WAN port.

**Subnet mask:** the subnet mask of the WAN port.

**Default gateway:** the gateway of the WAN port.

**Preferred DNS Server:** The primary DNS Server of the WAN port.

**Alternate DNS Server:** The substitute DNS Server of the WAN port. This is not required.

- **Dynamic IP address:** It is only applicable for the network environment where the DHCP Server is available in the network. Click the **Renew** button to get an IP address.

The screenshot shows the 'WAN Configuration' window. On the left, 'WAN Port' is listed. The main area has four radio buttons: 'Static IP Address', 'Dynamic IP Address' (selected), 'PPPoE Client', and 'PPTP Client'. To the right of the 'Dynamic IP Address' radio button is a 'Renew' button.

- **PPPoE Client:** When selecting PPPoE to connect to the network, please set the “**User Name**”, “**Password**”, “**MTU**” and “**CLAMP MSS**”. There is a **Dial on Demand** function under PPPoE. If this function is enabled, you can set a **Maximum Idle Time**. When the idle time is reached, the system will automatically disconnect itself.

The screenshot shows the 'WAN Configuration' window. On the left, 'WAN Port' is listed. The main area has four radio buttons: 'Static IP Address', 'Dynamic IP Address', 'PPPoE Client' (selected), and 'PPTP Client'. Below the radio buttons are five input fields: 'Username', 'Password', 'MTU' (with the value '1492' and 'bytes (Range:1000~1492)\*'), 'CLAMP MSS' (with the value '1400' and 'bytes (Range:980~1400)\*'), and 'Dial on Demand' (with radio buttons for 'Enable' and 'Disable', where 'Disable' is selected).

- PPTP Client:** Select **STATIC** to specify the IP address of the PPTP Client manually or select **DHCP** to get the IP address automatically. The fields with red asterisks are required to be filled in. There is a **Dial on Demand** function under PPPoE. If this function is enabled, a **Maximum Idle Time** can be set. When the idle time is reached, the system will automatically disconnect itself.

WAN Configuration	
WAN Port	<input type="radio"/> Static IP Address <input type="radio"/> Dynamic IP Address <input type="radio"/> PPPoE Client <input checked="" type="radio"/> PPTP Client
	Type <input checked="" type="radio"/> Static <input type="radio"/> DHCP
	IP Address: <input type="text"/> *
	Subnet Mask: <input type="text"/> *
	Default Gateway: <input type="text"/> *
	Preferred DNS Server: <input type="text"/> *
	Alternate DNS Server: <input type="text"/>
	PPTP Server IP: <input type="text"/> *
	Username: <input type="text"/> *
	Password: <input type="text"/> *
PPTP Connection ID/Name: <input type="text"/>	
Dial on Demand: <input type="radio"/> Enable <input checked="" type="radio"/> Disable	

WAN Configuration	
WAN Port	<input type="radio"/> Static IP Address <input type="radio"/> Dynamic IP Address <input type="radio"/> PPPoE Client <input checked="" type="radio"/> PPTP Client
	Type <input type="radio"/> Static <input checked="" type="radio"/> DHCP
	PPTP Server IP: <input type="text"/> *
	Username: <input type="text"/> *
	Password: <input type="text"/> *
	PPTP Connection ID/Name: <input type="text"/>
	Dial on Demand: <input type="radio"/> Enable <input checked="" type="radio"/> Disable

## 4.1.4 LAN1 & LAN2 Configuration

User authentication for the two LAN ports can be enabled or disabled.

LAN1 & LAN2 Configuration	
LAN1 & LAN2	IP PNP <input type="radio"/> Enable <input checked="" type="radio"/> Disable
	User Authentication <input checked="" type="radio"/> Enable <input type="radio"/> Disable
	Operation Mode <input type="text" value="NAT"/>
	IP Address: <input type="text" value="192.168.1.254"/> *
	Subnet Mask: <input type="text" value="255.255.255.0"/> *
DHCP Server Configuration	<input checked="" type="radio"/> Disable DHCP Server <input type="radio"/> Enable DHCP Server <input type="radio"/> Enable DHCP Relay

- **LAN1 & LAN2 Port**

LAN1 & LAN2 Port	IP PNP <input type="radio"/> Enable <input checked="" type="radio"/> Disable
	User Authentication <input checked="" type="radio"/> Enable <input type="radio"/> Disable
	Operation Mode <input type="text" value="NAT"/>
	IP Address <input type="text" value="192.168.1.254"/> *
	Subnet Mask <input type="text" value="255.255.255.0"/> *

**IP PNP:** Users can use any IP address to connect to the system. Regardless of what the IP address at the user end is, users can still be authenticated through AirLive WIAS-1200G and access the network.

**User Authentication:** Choose to enable or disable this function. If “**User Authentication**” is disabled, users can access Internet without being authenticated.

**Operation Mode:** Choose one of the two modes, **NAT** mode and **Router** mode, by the requirements.

**IP Address:** Enter the desired IP address for the LAN1 & LAN2 port.

**Subnet Mask:** Enter the desired subnet mask for the LAN1 & LAN2 port.

- **DHCP Server Configuration**

There are three methods to set the DHCP server: **Disable DHCP Server**, **Enable DHCP Server** and **Enable DHCP Relay**.

1. **Disable DHCP Server:** Disable DHCP Server function.

DHCP Server Configuration	<input checked="" type="radio"/> Disable DHCP Server <input type="radio"/> Enable DHCP Server <input type="radio"/> Enable DHCP Relay
---------------------------	---

2. **Enable DHCP Server:** Choose “**Enable DHCP Server**” function and set the appropriate configuration for the DHCP server. The fields with red asterisks are required to be filled in.

<b>DHCP Server Configuration</b>	<input type="radio"/> Disable DHCP Server
	<input checked="" type="radio"/> Enable DHCP Server
	DHCP Scope
	Start IP Address: <input type="text" value="192.168.1.1"/> *
	End IP Address: <input type="text" value="192.168.1.100"/> *
	Preferred DNS Server: <input type="text" value="192.168.1.254"/> *
	Alternate DNS Server: <input type="text"/>
	Domain Name: <input type="text" value="airlive.com"/> *
	WINS Server IP: <input type="text"/>
	Lease Time: <input type="text" value="1 Day"/> ▼
<a href="#">Reserved IP Address List</a>	
<input type="radio"/> Enable DHCP Relay	

**DHCP Scope:** Enter the “**Start IP Address**” and the “**End IP Address**” of this DHCP block. These fields define the IP address range that will be assigned to the Public LAN clients.

**Preferred DNS Server:** The primary DNS server for the DHCP.

**Alternate DNS Server:** The substitute DNS server for the DHCP.

**Domain Name:** Enter the domain name.

**WINS IP Address:** Enter the IP address of WINS

**Lease Time:** Choose the time to change the DHCP.

**Reserved IP Address List:** For reserved IP address settings in detail, please click the hyperlink of **Reserved IP Address**. If using the **Reserved IP Address List** function for IP address outside the DHCP range is desired, click on the **Reserved IP Address List** on the management interface. Then, the setup of the Reserved IP Address List as shown in the following figure will appear. Enter the related Reserved IP Address, MAC, and some description (not mandatory). Click **Apply** to complete the setup.

Reserved IP Address List - LAN1 & LAN2			
Item	Reserved IP Address	MAC	Description
1	<input type="text"/>	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>	<input type="text"/>
(Total:40) <a href="#">First</a> <a href="#">Prev</a> <a href="#">Next</a> <a href="#">Last</a>			

3. **Enable DHCP Relay:** If enabling this function is desired, other DHCP Server IP address must be specified. See the following figure.

<b>DHCP Server Configuration</b>	<input type="radio"/> Disable DHCP Server
	<input type="radio"/> Enable DHCP Server
	<input checked="" type="radio"/> Enable DHCP Relay
	DHCP Server IP: <input type="text"/> *

## 4.1.5 LAN3 & LAN4 Configuration

In this section, set the related configuration for LAN3/LAN4 port and DHCP server.

LAN3 & LAN4 Configuration	
LAN3 & LAN4	Operation Mode: <input type="button" value="NAT"/> ▼
	IP Address: <input type="text" value="192.168.2.254"/> *
	Subnet Mask: <input type="text" value="255.255.255.0"/> *
DHCP Server Configuration	<input checked="" type="radio"/> Disable DHCP Server <input type="radio"/> Enable DHCP Server <input type="radio"/> Enable DHCP Relay

- **LAN3 & LAN4 Port**

LAN3 & LAN4 Configuration	
LAN3 & LAN4	Operation Mode: <input type="button" value="NAT"/> ▼
	IP Address: <input type="text" value="192.168.2.254"/> *
	Subnet Mask: <input type="text" value="255.255.255.0"/> *

**Operation Mode:** Choose one of the two modes, **NAT** mode and **Router** mode, by the requirements.

**IP Address:** Enter the desired IP address for the LAN3 & LAN4 port.

**Subnet Mask:** Enter the desired subnet mask for the LAN3 & LAN4 port.

- **DHCP Server Configuration**

There are three methods to set the DHCP server: **Disable DHCP Server**, **Enable DHCP Server** and **Enable DHCP Relay**.

1. **Disable DHCP Server:** Disable DHCP Server function.

DHCP Server Configuration	<input checked="" type="radio"/> Disable DHCP Server <input type="radio"/> Enable DHCP Server <input type="radio"/> Enable DHCP Relay
---------------------------	---

2. **Enable DHCP Server:** Choose “**Enable DHCP Server**” function and set the appropriate configuration for the DHCP server. The fields with red asterisks are required to be filled in.

DHCP Server Configuration	<input type="radio"/> Disable DHCP Server <input checked="" type="radio"/> Enable DHCP Server
	DHCP Scope
	Start IP Address: <input type="text" value="192.168.2.1"/> *
	End IP Address: <input type="text" value="192.168.2.100"/> *
	Preferred DNS Server: <input type="text" value="192.168.2.254"/> *
	Alternate DNS Server: <input type="text"/>
	Domain Name: <input type="text" value="airlive.com"/> *
	WINS Server IP: <input type="text"/>
	Lease Time: <input type="button" value="1 Day"/> ▼
	<a href="#">Reserved IP Address List</a> <input type="radio"/> Enable DHCP Relay

**DHCP Scope:** Enter the “**Start IP Address**” and the “**End IP Address**” of this DHCP block. These fields define the IP address range that will be assigned to the Private LAN clients.

**Preferred DNS Server:** The primary DNS server for the DHCP.

**Alternate DNS Server:** The substitute DNS server for the DHCP.

**Domain Name:** Enter the domain name.

**WINS IP Address:** Enter the IP address of WINS.

**Lease Time:** Choose the time to update the DHCP.

**Reserved IP Address List:** For reserved IP address settings in detail, please click the hyperlink of **Reserved IP Address**. If using the **Reserved IP Address List** function for IP address outside the DHCP range is desired, click the **Reserved IP Address List** on the management interface. The setup of the Reserved IP Address List as shown in the following figure will appear. Enter the related Reserved IP Address, MAC, and some description (not mandatory). Click **Apply** to complete the setup.

Reserved IP Address List - LAN3 & LAN4			
Item	Reserved IP Address	MAC	Description
1	<input type="text"/>	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>	<input type="text"/>
(Total:40) <a href="#">First</a> <a href="#">Prev</a> <a href="#">Next</a> <a href="#">Last</a>			

- Enable DHCP Relay:** If enabling this function is desired, other DHCP Server IP address must be specified. See the following figure.

<b>DHCP Server Configuration</b>	<input type="radio"/> Disable DHCP Server <input type="radio"/> Enable DHCP Server <input checked="" type="radio"/> Enable DHCP Relay DHCP Server IP <input type="text"/> *
----------------------------------	--

## 4.1.6 Wireless Configuration

This section is for setting related configurations for the wireless port.

Wireless Configuration	
<b>Basic Configuration</b>	SSID: <input type="text" value="airlive"/> *
	<input checked="" type="checkbox"/> Sync To Ticket
	Transmission Mode: <input type="text" value="802.11(b+g)"/> ▼
	Channel: <input type="text" value="1"/> ▼
	SSID Broadcast: <input checked="" type="checkbox"/>
	Layer2 Client Isolation: <input checked="" type="checkbox"/>
<a href="#">Security Advance</a>	
<b>Wireless Port</b>	IP PNP: <input type="radio"/> Enable <input checked="" type="radio"/> Disable
	User Authentication: <input checked="" type="radio"/> Enable <input type="radio"/> Disable
	Operation Mode: <input type="text" value="NAT"/> ▼
	IP Address: <input type="text" value="192.168.3.254"/> *
	Subnet Mask: <input type="text" value="255.255.255.0"/> *
<b>DHCP Server Configuration</b>	<input type="radio"/> Disable DHCP Server
	<input checked="" type="radio"/> Enable DHCP Server
	DHCP Scope
	Start IP Address: <input type="text" value="192.168.3.1"/> *
	End IP Address: <input type="text" value="192.168.3.100"/> *
	Preferred DNS Server: <input type="text" value="192.168.3.254"/> *
	Alternate DNS Server: <input type="text"/>
	Domain Name: <input type="text" value="airlive.com"/> *
	WINS Server IP: <input type="text"/>
	Lease Time: <input type="text" value="1 Day"/> ▼
<a href="#">Reserved IP Address List</a>	
<b>WDS Configuration</b>	<input type="radio"/> Enable DHCP Relay
	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

• **Wireless Configuration**

Wireless Configuration		
<b>Basic Configuration</b>	SSID	airlive *
		<input checked="" type="checkbox"/> Sync To Ticket
	Transmission Mode	802.11 (b+g) ▼
	Channel	1 ▼
	SSID Broadcast	<input checked="" type="checkbox"/>
	Layer2 Client Isolation	<input checked="" type="checkbox"/>
	<a href="#">Security Advance</a>	

**SSID:** The SSID is the unique name shared among all devices in a wireless network. The SSID must be the same for all devices in the wireless network. It is case sensitive, must not exceed 32 characters and may be any character on the keyboard.

**Sync to Ticket:** Synchronize the SSID of ticket with this system.

**Channel:** Select the appropriate channel from the list to correspond with your network settings; for example, 1 to 11 channels are suitable for the North America area. All points in the wireless network must use the same channel in order to make sure correct connection.

**Transmission Mode:** There are 2 modes to select from, **802.11b** (2.4G, 1~11Mbps) and **802.11 (b+g)** (2.4G, 1~11Mbps and 2.4G, 54Mbps).

**SSID Broadcast:** Select to enable the SSID broadcast in the network. When configuring the network, this function may be enabled but should be disabled when configuration is finished. Since when SSID Broadcast is enabled, someone could easily obtain the SSID information with the site survey software and get unauthorized access to the network.

**Layer2 Client Isolation:** This function can be enabled to isolate any client from each other.

**Security:** For security settings in detail, please click the hyperlink **Security** to go into the **Security** page. Choose **“Enable”** to configure the setting.

Security	
WEP Key	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
WEP Key Encryption	<input checked="" type="radio"/> 64bits <input type="radio"/> 128bits
Mode	HEX ▼ HEX ASCII
	<input type="radio"/> 2. <input type="text"/>
	<input type="radio"/> 3. <input type="text"/>
	<input type="radio"/> 4. <input type="text"/>

1. **WEP Key: Wired Equivalent Privacy.** If using this function is desired, please choose **“Enable”**.
2. **WEP Key Encryption:** This is a data privacy mechanism based on a 64-bit or 128-bits shared key algorithm.
3. **Mode:** There are two types of encryption, **HEX** and **ASCII**. After selecting one of them, please enter the related information in the blanks below.



**Advance:** For advance settings in detail, please click the hyperlink **Advance** to go into the **Advance** page.

Advanced	
Authentication Type	Auto (Default: Auto)
Transmission Rates	Auto (Default: Auto)
CTS Protection Mode	Disable (Default: Disable)
Basic Rates	Set1 (Default: Set1)
Beacon Interval	100 milliseconds *(Range: 20-1000; Default: 100)
RTS Threshold	OFF *(Range: 256-2346; Default: OFF)
Fragmentation Threshold	2346 *(Range: 256-2346; Default: 2346)
DTIM Interval	20 *(Range: 1-255; Default: 20)
ACK Timeout	48 microseconds *(Range: 0-372; Default: 48)

1. **Authentication Type:** The default value is **Auto**. When “**Auto**” is selected, it will auto-detect to authenticate by **Shared Key** type or **Open System** type. **Shared Key** is used such that both the sender and the recipient share a WEP key for authentication. **Open Key** is that the sender and the recipient do not share a WEP key for authentication. All points on the network must use the same authentication type.
2. **Transmission Rates:** The default value is **Auto**. The range is from 1 to 54Mbps. The rate of data transmission should be set depending on the speed of this particular wireless network. Select from a range of transmission speeds or keep the default setting, **Auto**, to make the Access Point use the fastest possible data rate automatically.
3. **CTS Protection Mode:** The default value is **Disable**. When enabled, a protection mechanism will ensure that the 802.11b devices can connect to Access Point and not be affected by many other 802.11g devices existing at the same time. However, the performance of this 802.11g devices may decrease.
4. **Basic Rate:** The basic rate offers three options, **All**, **Set1** and **Set2** and the default value is **Set1**. Depending on the wireless mode selected, AirLive WIAS-1200G will deliver a pre-defined data rate. Select “**All**” to activate all transmission rates to be compatible with the majority of the devices.
5. **Beacon Interval:** Enter a value between 20 and 1000 msec, default value is 100 milliseconds. The entered time means how often the signal transmission occurs between the access point and the wireless network.
6. **RTS Threshold:** Ready To Send threshold. The range is from 256 to 2346 and the default is **OFF**. The administrator could set the value which is the time to wait before sending another packet. It is recommended that the value remains in the range of 256 to 2346.
7. **Fragmentation Threshold:** The range is from 256 to 2346 and the default is **OFF**. The value specifies the maximum size of packet allowed before data is fragmented into multiple packets. It should be remained in the range of 256 to 2346. A smaller value results smaller packets but with a larger numbers of packets in transmission.
8. **DTIM Interval:** This function indicates the interval of the **Delivery Traffic Indication Message** (DTIM). DTIM is a countdown function to inform clients to listen to broadcast and multicast messages. When an Access Point has buffered broadcast or multicast message from an associated client, it sends the next DTIM at this interval rate (from 1~255), the client will hear the beacons.
9. **ACK Timeout:** This function is to define ACK timeout parameter of Atheros wireless LAN chipset. Generally, the higher the ACK timeout is, the lower the throughput is. Thus, ACK timeout should be the optimization of distance over throughput.

- **Wireless Configuration**

<b>Wireless Port</b>	IP PNP	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
	User Authentication	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
	Operation Mode	NAT <input type="button" value="v"/>
	IP Address:	192.168.3.254 *
	Subnet Mask:	255.255.255.0 *

**IP PNP:** Use any IP address to connect to the system. Regardless of what the IP address at the users end is, they can still be authenticated through AirLive WIAS-1200G and access the network.

**User Authentication:** If “User Authentication” is disabled, “Specific Route Profile” needs to be specified for the users to access Internet.

**Operation Mode:** Choose one of the two modes, NAT mode and Router mode, by the requirements.

**IP Address:** Enter desired IP address for the wireless port.

**Subnet Mask:** Enter desired subnet mask for the wireless port.

- **DHCP Server Configuration**

There are three methods to set the DHCP server: **Disable DHCP Server**, **Enable DHCP Server** and **Enable DHCP Relay**.

1. **Disable DHCP Server:** Disable the DHCP Server function.

<b>DHCP Server Configuration</b>	<input checked="" type="radio"/> Disable DHCP Server
	<input type="radio"/> Enable DHCP Server
	<input type="radio"/> Enable DHCP Relay

2. **Enable DHCP Server:** Choose “Enable DHCP Server” function and set the appropriate configuration for the DHCP server. The fields with red asterisks are required to be filled in.

<b>DHCP Server Configuration</b>	<input type="radio"/> Disable DHCP Server	
	<input checked="" type="radio"/> Enable DHCP Server	
	DHCP Scope	
	Start IP Address:	192.168.3.1 *
	End IP Address:	192.168.3.100 *
	Preferred DNS Server:	192.168.3.254 *
	Alternate DNS Server:	
	Domain Name:	airlive.com *
	WINS Server IP:	
	Lease Time	1 Day <input type="button" value="v"/>
	<a href="#">Reserved IP Address List</a>	
	<input type="radio"/> Enable DHCP Relay	

**DHCP Scope:** Enter the “Start IP Address” and the “End IP Address” of this DHCP block. These fields define the IP address range that will be assigned to the Wireless LAN clients.

**Preferred DNS Server:** The primary DNS server for the DHCP.

**Alternate DNS Server:** The substitute DNS server for the DHCP.

**Domain Name:** Enter the domain name.

**WINS IP Address:** Enter the IP address of WINS.

**Lease Time:** Choose the time to change the DHCP.

**Reserved IP Address List:** For reserved IP address settings in detail, please click the hyperlink of **Reserved IP Address**. If using the **Reserved IP Address List** function for IP address outside the DHCP range is desired, click on the **Reserved IP Address List** on the management interface. The setup of the Reserved IP Address List as shown in the following figure will appear. Enter the related Reserved IP Address, MAC, and some description (not mandatory). Click **Apply** to complete the setup.

Reserved IP Address List - Wireless			
Item	Reserved IP Address	MAC	Description
1	<input type="text"/>	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>

3. **Enable DHCP Relay:** If enabling this function is desired, other DHCP Server IP address must be specified. See the following figure.

DHCP Server Configuration	<input type="radio"/> Disable DHCP Server
	<input type="radio"/> Enable DHCP Server
	<input checked="" type="radio"/> Enable DHCP Relay
	DHCP Server IP <input type="text"/> *

- **WDS configuration**

This function can extend the range of accessing the network. It has to work with a repeater. A repeater is a peripheral device supporting AirLive WIAS-1200G to extend the wireless access by receiving requests from APs or clients and passing the requests to AirLive WIAS-1200G to obtain authentication.

WDS Configuration	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
-------------------	---

When "Enable" is clicked, there will be a warning box showing up.



If this function is enabled, please enter the MAC address of repeater in the blanks. A maximum of three repeaters are supported.

WDS Configuration	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
	Item	WDS Client MAC Address
	1	<input type="text"/>
	2	<input type="text"/>
	3	<input type="text"/>

## 4.2 User Authentication

This section includes the following functions: **Authentication Configuration, Black List Configuration, Policy Configuration, Guest User Configuration and Additional Configuration.**

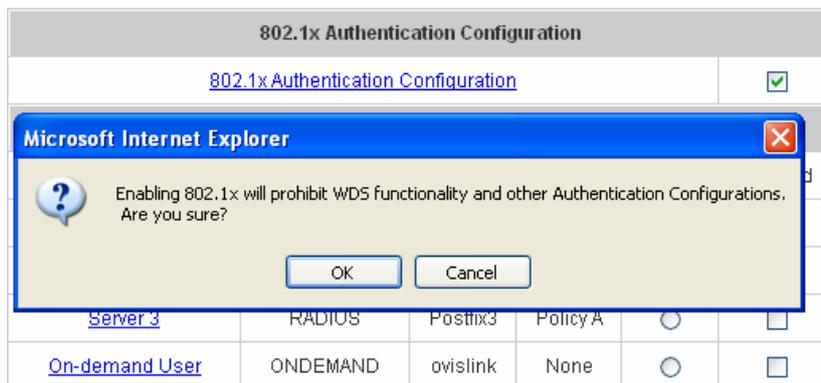
System Configuration	User Authentication	Network Configuration	Utilities	Status
<b>User Authentication</b>				
<b>Authentication Configuration</b>	System provides 3 authentication servers. Each server allows only one type of authentication method and one Black List Profile. An authentication policy may be assigned to any policy. System supports the following external authentication servers: POP3(S), RADIUS, LDAP and NT Domain. System also has embedded user database storing 2500 user accounts for local user group (500) and On-demand user group (2000). System may print out On-demand user accounts information using an external printer. By default, the On-demand user database is empty.			
<b>Black List Configuration</b>	System supports 5 Black List profiles for used within the authentication server. On-demand users are NOT bounded by the Black List.			
<b>Policy Configuration</b>	System provides 3 policies, each policy can apply independent firewall profile, specific route profile, login schedule profile and bandwidth controls.			
<b>Guest User Configuration</b>	System provides up to 10 guest accounts.			
<b>Additional Configuration</b>	Users will be logged out automatically after being idle for a specified period of time. Multiple login of the same user account could be enabled or disabled (not available to On-demand users). System provides Friendly Logout options, Login Page and Logout Page customization, and login notification email to client. When MAC Access Control is enabled, system will only provide login page to those devices listed. SMTP Redirect can be enabled to redirect outgoing emails to the selected SMTP server.			

### 4.2.1 Authentication Configuration

This function is to configure the settings for 802.1x authentication, authentication server, and on-demand user authentication.

System Configuration	User Authentication	Network Configuration	Utilities	Status	
<b>Authentication Configuration</b>					
<b>802.1x Authentication Configuration</b>					
<a href="#">802.1x Authentication Configuration</a>				<input type="checkbox"/>	
<b>Authentication Server Configuration</b>					
Server Name	Auth Method	Postfix	Policy	Default	Enabled
<a href="#">Server 1</a>	LOCAL	Postfix1	Policy A	<input type="radio"/>	<input type="checkbox"/>
<a href="#">Server 2</a>	POP3	Postfix2	Policy A	<input type="radio"/>	<input type="checkbox"/>
<a href="#">Server 3</a>	RADIUS	Postfix3	Policy A	<input type="radio"/>	<input type="checkbox"/>
<a href="#">On-demand User</a>	ONDEMAND	ovislink	None	<input checked="" type="radio"/>	<input checked="" type="checkbox"/>

• **802.1x Authentication Configuration**



There are two kinds of 802.1x authentication methods and one encryption mechanism: **802.1x, WPA w/802.1x** and **WPA-PSK**. Click the hyperlink **802.1x Authentication Configuration** to set the related configurations. After completing and clicking **Apply** to save the settings, go back to the previous page to check the item box next to **802.1x Authentication Configuration** to enable this function. When using 802.1 x authentications, the RADIUS attributes such as idle timeout or session timeout have no effect.

1. **802.1x:** Enable the 802.1x authentication method. The fields with red asterisks are required to be filled in.

802.1x Authentication Configuration

802.1x 
  WPA w/ 802.1x 
  WPA-PSK

Authentication Server IP:  \*

Authentication Port:  \*(Default: 1812)

Secret Key:  \*

Accounting Server IP:  \*

Accounting Port:  \*(Default: 1813)

Secret Key:  \*

Accounting Service:

Policy:

**Authentication Server IP:** The IP address or domain name of the Authentication server.

**Authentication Port:** The port of the authentication server. The default value is 1812.

**Secret Key:** The secret key of the authentication sever for encryption and decryption.

**Accounting Server IP:** The IP address or domain name of the accounting server.

**Account Port:** The port of the accounting server. The default value is 1813.

**Secret Key:** The secret key of the accounting sever for encryption and decryption.

**Accounting Service:** Enable or disable accounting service.

**Policy:** There are three policies to select from.

2. **WPA w/802.1x:** Enable the supported WPA-Enterprise, Wireless Protection Access with 802.1x.

**Authentication Server IP:** The IP address or domain name of the Authentication server.

**Authentication Port:** The port of the authentication server. The default value is 1812.

**Secret Key:** The secret key of the authentication sever for encryption and decryption.

**Accounting Server IP:** The IP address or domain name of the accounting server.

**Account Port:** The port of the accounting server. The default value is 1813.

**Secret Key:** The secret key of the accounting sever for encryption and decryption.

**Accounting Service:** Enable or disable accounting service.

**Policy:** There are three policies to select from.

**Group Re-key Time:** Time interval for re-keying broadcast/multicast keys in seconds. The maximum is 6000 sec.

3. **WPA-PSK:** **Wireless Protection Access-PreShared Key**, when using **WPA-PSK**, there is no user authentication required.

**Group Re-key Time:** Time interval for re-keying broadcast/multicast keys in seconds. The maximum is 6000 sec.

**PSK:** The **Pre-Shared Key** uses 64 hexadecimal.

**Passphrase:** A kind of password using 8 to 63 ASCII characters.

**Note:** After clicking **Apply**, there will be a restart message. You must click **Restart** to apply the settings.

- **Authentication Server Configuration**

The system provides 3 servers and one on-demand server that the administrator can apply with different policy. Click on the server name to set the related configurations for that particular server. After completing and clicking **Apply** to save the settings, go back to the previous page to choose a server to be the default server and enable or disable any server on the list. Users can log into the default server without the postfix to allow faster login process.

Authentication Server Configuration					
Server Name	Auth Method	Postfix	Policy	Default	Enabled
<a href="#">Server 1</a>	LOCAL	Postfix1	Policy A	<input type="radio"/>	<input type="checkbox"/>
<a href="#">Server 2</a>	POP3	Postfix2	Policy A	<input type="radio"/>	<input type="checkbox"/>
<a href="#">Server 3</a>	RADIUS	Postfix3	Policy A	<input type="radio"/>	<input type="checkbox"/>
<a href="#">On-demand User</a>	ONDEMAND	ovislink	None	<input checked="" type="radio"/>	<input checked="" type="checkbox"/>

1. **Server 1~3:** There are 5 kinds of authentication methods, Local User, POP3, RADIUS, LDAP and NTDomain to setup from.

Authentication Server - Server 1	
Server Name	<input type="text" value="Server 1"/> <small>*(Its server name)</small>
Server Status	Disabled
Postfix	<input type="text" value="Postfix1"/> <small>*(Its postfix name)</small>
Black List	None <input type="button" value="v"/>
Authentication Method	Local User <input type="button" value="v"/> <a href="#">Local User Setting</a>
Policy	Policy A <input type="button" value="v"/>
Allow username without postfix	<input type="checkbox"/>

**Server Name:** Set a name for the server using numbers (0~9), alphabets (a~z or A~Z), dash (-), underline (\_) and dot (.) with a maximum of 40 characters, all other letters are not allowed.

**Sever Status:** The status shows that the server is enabled or disabled.

**Postfix:** Set a postfix that is easy to distinguish (e.g. Local) for the server using numbers (0~9), alphabets (a~z or A~Z), dash (-), underline (\_) and dot (.) with a maximum of 40 characters, all other letters are not allowed.

**Note:** The Policy Name cannot contain these words: MAC and IP.

**Black List:** There are 5 sets of the black lists. Select one of them or choose “None”. Please refer to **3.2.2**

### Black List Configuration

**Authentication Methods:** There are 5 authentication methods, **Local**, **POP3**, **RADUUS**, **LDAP** and **NT Domain** to configure from. Select the desired method and click the link besides the pull-down menu for more advanced configuration. For more details, please refer to **4.2.1.1~5 Authentication Method**.

**Note:** Enabling two or more servers of the same authentication method is not allowed.

**Policy:** There are 3 policies to choose from to apply to this particular server.

**Allow username without postfix:** To enable the function, the user name could be set up without postfix.

2. **On-demand User:** This is for the customer’s need in a store environment. When customers need to get wireless access to the Internet in the store, they have to get a printed receipt with username and password

from the store to log in the system for wireless access. There are 2000 On-demand User accounts available.

On-demand User Server Configuration	
Server Status	Enabled
Postfix	<input type="text" value="airlive"/> *(e.g. airlive. Max: 40 char)
Receipt Header 1	<input type="text" value="Welcome!"/> (e.g. Welcome!)
Receipt Header 2	<input type="text"/>
Receipt Footer	<input type="text" value="Pls wait for login page!"/> (e.g. Thank You!)
Printer Baud Rate	9600
Monetary Unit	<input checked="" type="radio"/> none <input type="radio"/> \$ USD <input type="radio"/> £ GBP <input type="radio"/> € EUR <input type="radio"/> <input type="text"/> (Input other desired monetary unit, e.g. AU)
WLAN ESSID	<input type="text" value="airlive"/> (e.g. airlive)
Wireless Key	<input type="text"/>
Remark	<input type="text"/> (for customer)
Billing Notice Interval	<input checked="" type="radio"/> 10mins <input type="radio"/> 15mins <input type="radio"/> 20mins
Twin Ticket	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
<a href="#">Users List</a> <a href="#">Billing Configuration</a> <a href="#">Create On-demand User</a> <a href="#">Billing Report</a> <a href="#">Payment</a>	

For detailed information about configuration, please see 4.2.1.6 Authentication Method – On-demand User

#### 4.2.1.1 Authentication Method – Local User Setting

Choose “Local User” in the **Authentication Method** field, the hyperlink besides the pull-down menu will become “Local User Setting”.

Authentication Server - Server 1	
Server Name	<input type="text" value="Server 1"/> *(its server name)
Server Status	Disabled
Postfix	<input type="text" value="Postfix1"/> *(its postfix name)
Black List	None
Authentication Method	<input type="text" value="Local User"/> <a href="#">Local User Setting</a>
Policy	Policy A
Allow username without postfix	<input type="checkbox"/>

Click the hyperlink for further configuration.

Local User Setting
<a href="#">Edit Local User List</a>

- **Edit Local User List:** Click this to enter the “Local User List” screen.

Users List				
Username	Password	MAC	Policy	Remark

(Total:0) [First](#) [Previous](#) [Next](#) [Last](#)



**Add User:** Click *this* to enter the **Add User** interface. Fill in the necessary information such as “**Username**”, “**Password**”, “**MAC**” and “**Remark**” (optional). Then, select a desired **Policy** and click **Apply** to complete adding the user or users.

Add User			
Item	Username	MAC (xxxxxxxxxxxxxx)	Policy
	Password	Expiration Time	Remark
1	<input type="text"/>	<input type="text"/>	None <input type="button" value="v"/>
	<input type="text"/>	<input type="text"/> <a href="#">Select</a>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>	None <input type="button" value="v"/>
	<input type="text"/>	<input type="text"/> <a href="#">Select</a>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>	None <input type="button" value="v"/>
	<input type="text"/>	<input type="text"/> <a href="#">Select</a>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>	None <input type="button" value="v"/>
	<input type="text"/>	<input type="text"/> <a href="#">Select</a>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>	None <input type="button" value="v"/>
	<input type="text"/>	<input type="text"/> <a href="#">Select</a>	<input type="text"/>

Add User			
Item	Username	MAC (xxxxxxxxxxxxxx)	Policy
	Password	Expiration Time	Remark
1	Tony	<input type="text"/>	Policy A <input type="button" value="v"/>
	tony	02/01/2007 <a href="#">Select</a>	<input type="text"/>
2	Larry	00:01:23:3F:6D:7E	Policy A <input type="button" value="v"/>
	larry	01/31/2007 <a href="#">Select</a>	<input type="text"/>
3	Judy	<input type="text"/>	None <input type="button" value="v"/>
	judy	02/25/2007 <a href="#">Select</a>	<input type="text"/>
4	Oksana	<input type="text"/>	Policy B <input type="button" value="v"/>
	oksana	<input type="text"/> <a href="#">Select</a>	Long Term
5	<input type="text"/>	<input type="text"/>	None <input type="button" value="v"/>
	<input type="text"/>	<input type="text"/> <a href="#">Select</a>	<input type="text"/>

User 'Tony' has been added!  
User 'Larry' has been added!  
User 'Judy' has been added!  
User 'Oksana' has been added!

Add User			
Item	Username	MAC (xxxxxxxxxxxxxx)	Policy
	Password	Expiration Time	Remark
1	<input type="text"/>	<input type="text"/>	None <input type="button" value="v"/>
	<input type="text"/>	<input type="text"/> <a href="#">Select</a>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>	None <input type="button" value="v"/>
	<input type="text"/>	<input type="text"/> <a href="#">Select</a>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>	None <input type="button" value="v"/>
	<input type="text"/>	<input type="text"/> <a href="#">Select</a>	<input type="text"/>

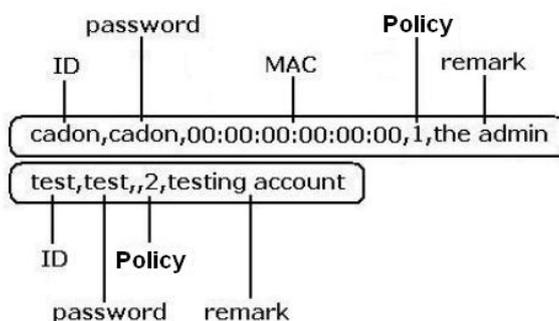
**Upload User:** Click this to enter the **Upload User** interface. Click the **Browse** button to select the text file for the user account upload. Then click **Submit** to complete the upload process.

Note: The format of each line is "ID, Password, MAC, Policy, Expiration Time(MM DD YYYY), Remark" without the quotes. There must be no space between the fields and commas. The MAC and expiration-time fields could be omitted but the trailing commas corresponding to them must be retained. When adding user accounts by uploading a file, existing accounts in the embedded database that are also defined in the data file will not be replaced by the new ones.

Upload User Account

File Name

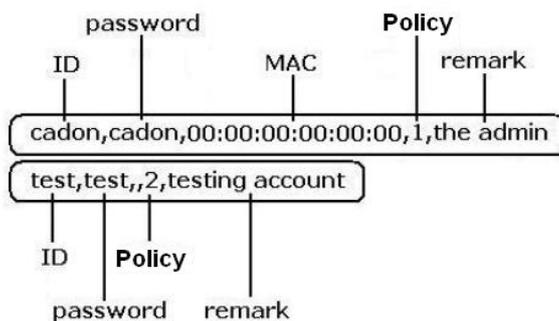
The uploading file should be a text file and the format of each line is "**ID, Password, MAC, Policy, Remark**" without the quotes. There must be no spaces between the fields and commas. The MAC field could be omitted but the trailing comma must be retained. When adding user accounts by uploading a file, the existing accounts in the embedded database will not be replaced by new ones.



**Download User:** Click this to enter the **Users List** page and the system will directly show a list of all created user accounts. Click **Download** to create a .txt file and then save it on disk.

Users List			
Username	Password	MAC	Policy
		Expiration Time	Remark
Tony	tony		1
		02 01 2007	
Larry	larry		1
		00:01:23:3F:6D:7E 01 31 2007	
Judy	judy		0
		02 25 2007	
Oksana	oksana		2
			Long Term

[Download](#)



**Refresh:** Click this to renew the user list.

Users List				
Username	Password	MAC	Policy	Del All
		Expiration Time	Remark	
<a href="#">Tony</a>	tony		Policy A	<a href="#">Delete</a>
		02 01 2007		
<a href="#">Larry</a>	larry	00:01:23:3F:6D:7E	Policy A	<a href="#">Delete</a>
		01 31 2007		
<a href="#">Judy</a>	judy		None	<a href="#">Delete</a>
		02 25 2007		
<a href="#">Oksana</a>	oksana		Policy B	<a href="#">Delete</a>
			Long Term	

(Total:4) [First](#) [Previous](#) [Next](#) [Last](#)

**Search:** Enter a keyword of a username to be searched in the text field and click this button to perform the search. All usernames matching the keyword will be listed.

Users List				
Username	Password	MAC	Policy	Del All
		Expiration Time	Remark	
<a href="#">Oksana</a>	oksana		Policy B	<a href="#">Delete</a>
			Long Term	

(Total:1) [First](#) [Previous](#) [Next](#) [Last](#)

**Del All:** This will delete all the users at once.

**Delete:** This will delete the users individually.

**Edit User:** If editing the content of individual user account is desired, click the username of the desired user account to enter the **Edit User** Interface for that particular user, and then modify or add any desired information such as **“Username”**, **“Password”**, **“MAC”** and **“Remark”** (optional). Then, click **Apply** to complete the modification.

Edit User	
Username	<input type="text" value="Oksana"/> *
Password	<input type="text" value="oksana"/> *
MAC	<input type="text" value="00:01:33:7C:2D:1F"/>
Policy	Policy C ▾
Remark	<input type="text" value="Permanent"/>
Expiration Time	// <input type="text"/> <a href="#">Select</a>

#### 4.2.1.2 Authentication Method – POP3

Choose “**POP3**” in the **Authentication Method** field, the hyperlink beside the pull-down menu will become “**POP3 Setting**”.

Authentication Server - Server 1	
Server Name	Server 1 <small>*(Its server name)</small>
Server Status	Disabled
Postfix	Postfix1 <small>*(Its postfix name)</small>
Black List	None
Authentication Method	POP3 <a href="#">POP3 Setting</a>
Policy	Policy A

Click the hyperlink for further configuration. Enter the related information for the primary server and/or the secondary server (the secondary server is not required). The blanks with red star are necessary information. These settings will become effective immediately after clicking the **Apply** button.

Primary POP3 Server	
Server IP	<input type="text"/> <small>*(Domain Name/IP)</small>
Port	<input type="text"/> <small>*(Default: 110)</small>
SSL Setting	<input type="checkbox"/> Enable SSL Connection
Secondary POP3 Server	
Server IP	<input type="text"/>
Port	<input type="text"/>
SSL Setting	<input type="checkbox"/> Enable SSL Connection

- **Server IP:** Enter the IP address/domain name given by your ISP.
- **Port:** Enter the Port given by the ISP. The default value is 100.
- **Enable SSL Connection:** If this option is enabled, the POP3 protocol will perform the authentication.

#### 4.2.1.3 Authentication Method – Radius

Choose “**Radius**” in the **Authentication Method** field, the hyperlink beside the pull-down menu will become “**Radius Setting**”.

Authentication Server - Server 1	
Server Name	Server 1 <small>*(Its server name)</small>
Server Status	Disabled
Postfix	Postfix1 <small>*(Its postfix name)</small>
Black List	None
Authentication Method	Radius <a href="#">Radius Setting</a>
Policy	Policy A

Click the hyperlink for further configuration. The Radius server sets the external authentication for user accounts. Enter the related information for the primary server and/or the secondary server (the secondary server is not required). The blanks with red star are necessary information. These settings will become effective immediately after clicking the **Apply** button.

Radius Setting	
802.1x Authentication	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <a href="#">Radius Client List</a>
Trans Full Name	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
NASID	<input type="text"/>
Primary RADIUS Server	
Server IP	<input type="text"/> *
Authentication Port	<input type="text"/> *(Default: 1812)
Accounting Port	<input type="text"/> *(Default: 1813)
Secret Key	<input type="text"/> *
Accounting Service	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Authentication Protocol	PAP <input type="button" value="v"/>
Secondary RADIUS Server	
Server IP	<input type="text"/>
Authentication Port	<input type="text"/>
Accounting Port	<input type="text"/>
Secret Key	<input type="text"/>
Accounting Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Authentication Protocol	CHAP <input type="button" value="v"/>

- **802.1X Authentication:** Enable this function and the hyperlink of **Radius Client List** will appear. Click the hyperlink to get into the Radius Client Configuration list for further configuration. In the **Radius Client Configuration** table, the clients, which are using 802.1X as the authentication method, shall be put into this table. AirLive WIAS-1200G will forward the authentication request from these clients to the configured Radius Servers.

Radius Client Configuration				
No.	Type	IP Address	Segment	Secret
1	802.1x <input type="button" value="v"/>	192.168.1.0	255.255.255.255 (/32) <input type="button" value="v"/>	12345678
2	Disable <input type="button" value="v"/>	<input type="text"/>	255.255.255.255 (/32) <input type="button" value="v"/>	<input type="text"/>
3	Disable <input type="button" value="v"/>	<input type="text"/>	255.255.255.255 (/32) <input type="button" value="v"/>	<input type="text"/>
4	Disable <input type="button" value="v"/>	<input type="text"/>	255.255.255.255 (/32) <input type="button" value="v"/>	<input type="text"/>
5	Disable <input type="button" value="v"/>	<input type="text"/>	255.255.255.255 (/32) <input type="button" value="v"/>	<input type="text"/>

- **Trans Full Name:** When enabled, the ID and postfix will be transferred to the RADIUS server for authentication. When disabled, only the ID will be transferred to RADIUS server for authentication.
- **NASID:** Enter a line of characters, for example “meeting room”, for identify the server using numbers (0~9), alphabets (a~z or A~Z), dash (-), underline (\_) and dot (.), all other letters are not allowed.
- **Server IP:** Enter the IP address/domain name of the RADIUS server.
- **Authentication Port:** Enter the authentication port of the RADIUS server and the default value is 1812.
- **Accounting Port:** Enter the accounting port of the RADIUS server and the default value is 1813.
- **Secret Key:** Enter the key for encryption and decryption.
- **Accounting Service:** Select this to enable or disable the “**Accounting Service**” for accounting capabilities.
- **Authentication Protocol:** There are two methods, CHAP and PAP for selection.

#### 4.2.1.4 Authentication Method – LDAP

Choose “LDAP” in the **Authentication Method** field, the hyperlink beside the pull-down menu will become “LDAP Setting”.

Authentication Server - Server 1	
Server Name	Server 1 <small>*(Its server name)</small>
Server Status	Disabled
Postfix	Postfix1 <small>*(Its postfix name)</small>
Black List	None <input type="button" value="v"/>
Authentication Method	LDAP <input type="button" value="v"/> <a href="#">LDAP Setting</a>
Policy	Policy A <input type="button" value="v"/>

Click the hyperlink for further configuration. Enter the related information for the primary server and/or the secondary server (the secondary server is not required). The blanks with red asterisks are necessary information. These settings will become effective immediately after clicking the **Apply** button.

Primary LDAP Server	
Server IP	<input type="text"/> <small>*(Domain Name/IP)</small>
Port	<input type="text"/> <small>*(Default: 389)</small>
Base DN	<input type="text"/> <small>*(CN=,dc=,dc=)</small>
Account Attribute	<input type="text"/> <small>(Default: uid)</small>
Secondary LDAP Server	
Server IP	<input type="text"/>
Port	<input type="text"/>
Base DN	<input type="text"/>
Account Attribute	<input type="text"/>

- **Server IP:** Enter the IP address or domain name of the LDAP server.
- **Port:** Enter the Port of the LDAP server, and the default value is 389.
- **Base DN:** Enter the distinguished name of the LDAP server.
- **Account Attribute:** Enter the account attribute of the LDAP server.

#### 4.2.1.5 Authentication Method – NTDomain

Choose “**NTDomain**” in the **Authentication Method** field, the hyperlink beside the pull-down menu will become “**NTDomain Setting**”.

Authentication Server - Server 1	
Server Name	Server 1 <small>*(Its server name)</small>
Server Status	Disabled
Postfix	Postfix1 <small>*(Its postfix name)</small>
Black List	None <input type="button" value="v"/>
Authentication Method	NTDomain <input type="button" value="v"/> <a href="#">NT Domain Setting</a>
Policy	Policy A <input type="button" value="v"/>

Click the hyperlink for further configuration. Enter the server IP address and enable/disable the transparent login function. These settings will become effective immediately after clicking the **Apply** button.

Domain Controller	
Server IP address	<input type="text"/> *
Transparent Login	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

- **Server IP address:** Enter the server IP address of the domain controller.
- **Transparent Login:** If the function is enabled, users will log into AirLive WIAS-1200G automatically when they log into the Windows domain.

#### 4.2.1.6 Authentication Method – On-demand User

On-demand User Server Configuration: Administrators can enable and configure this authentication method to provide wireless access in a Hotspot environment. Major functions include accounts creation, users monitoring list, billing plan, billing report statistics, and external payment gateway support.

On-demand User Server Configuration	
Server Status	Enabled
Postfix	airlive <small>*(e.g. airtlive. Max: 40 char)</small>
Receipt Header 1	Welcome! <small>(e.g. Welcome!)</small>
Receipt Header 2	
Receipt Footer	Pls wait for login page <small>(e.g. Thank You!)</small>
Printer Baud Rate	9600 <input type="button" value="v"/>
Monetary Unit	<input checked="" type="radio"/> none <input type="radio"/> \$ USD <input type="radio"/> £ GBP <input type="radio"/> € EUR <input type="radio"/> <input type="text"/> <small>(Input other desired monetary unit, e.g. AU)</small>
WLAN ESSID	airlive <small>(e.g. airtlive)</small>
Wireless Key	<input type="text"/>
Remark	<input type="text"/> <small>(for customer)</small>
Billing Notice Interval	<input checked="" type="radio"/> 10mins <input type="radio"/> 15mins <input type="radio"/> 20mins
Twin Ticket	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
<a href="#">Users List</a> <a href="#">Billing Configuration</a> <a href="#">Create On-demand User</a> <a href="#">Billing Report</a> <a href="#">Payment</a>	

**Server Status:** The status shows that the server is enabled or disabled.

**Postfix:** Set a postfix that is easy to distinguish (e.g. Local) for the server using numbers (0~9), alphabets (a~z or A~Z), dash (-), underline (\_) and dot (.) with a maximum of 40 characters, all other letters are not allowed.

**Receipt Header:** There are two fields, **Receipt Header 1** and **Receipt Header 2**, for the receipt's header. Enter receipt header message or use the default.

**Receipt Footer:** Enter receipt footer message here or use the default.

**Printer Baud Rate:** Select the desired transmission baud rate. The default value is 9600.

**Monetary Unit:** Select the desired monetary unit.

**WLAN ESSID:** Enter the ESSID of the AP. Administrators can supply a new name or use the default name.

**Wireless Key:** Enter the Wireless key of the AP such as WEP or WPA.

**Remark:** Enter any additional information that will appear at the bottom of the receipt.

**Billing Notice Interval:** While the on-demand user is still logged in, the system will update the billing notice of the login successful page by the time interval (.) defined here.

**Twin Ticket:** Enable this function to print duplicate receipts.



**Users List:** Click to enter the **On-demand Users List** page. In the **On-demand Users List**, detailed information will be documented here. By default, the On-demand user database is empty.

On-demand Users List					
Username	Password	Remaining Time/Volume	Status	Expiration Time	Delete All
<a href="#">Q2FX</a>	93NH7WYK	Out of Qouta	Not available	2006/05/04-10:22:59	<a href="#">Delete</a>
<a href="#">64MM</a>	V8UF3967	2 hour	Normal	2006/05/05-10:12:15	<a href="#">Delete</a>
<a href="#">N77X</a>	86N99T4E	Out of Qouta	Not available	2006/05/03-10:35:44	<a href="#">Delete</a>
<a href="#">8Y89</a>	5352P766	Redeemed before	Not available	2006/05/03-11:02:02	<a href="#">Delete</a>
<a href="#">8N6X</a>	788VZ9B8	10 min	Expire	2006/05/02-11:15:16	<a href="#">Delete</a>
<a href="#">2797</a>	NW4679S4	10 min	Normal	2006/05/02-11:56:09	<a href="#">Delete</a>
<a href="#">2XD4</a>	7R9S2RR2	2 hour	Normal	2006/05/05-10:56:16	<a href="#">Delete</a>
<a href="#">4HC4</a>	R888S37X	1 hour 59 min 42 sec	Normal	2006/05/07-11:10:16	<a href="#">Delete</a>
<a href="#">2TP4</a>	ZUF7XE5A	10 min	Normal	2006/05/02-12:06:51	<a href="#">Delete</a>

(Total:9) [First](#) [Previous](#) [Next](#) [Last](#)

- **Search:** Enter a keyword of a username that needs to be searched in the text field and click this button to perform the search. All usernames matching the keyword will be listed.
- **Username:** The login name of the on-demand user.
- **Password:** The login password of the on-demand user.
- **Remaining Time/Volume:** The total time/Volume that the user can use currently.
- **Status:** The status of the account. Normal indicates that the account is not in-use and not overdue. Online indicates that the account is in-use and not overdue. Expire indicates that the account is overdue and cannot be used.
- **Expiration Time:** The expiration time of the account.
- **Del All:** This will delete all the users at once.
- **Delete:** This will delete the users individually.
- **Upload User:** Click this to enter the **Upload User** interface. Click the **Browse** button to select the text file for the user account upload. Then click **Submit** to complete the upload process.

Note1:The format of each line is "ID (Username), Password, Type, Status, Available Data transfer or Session length, Activation deadline (Date), Expired Date, Validity duration, Plan, Price, Total Data transfer or Session length when bought, Generated Date, First Login Date, Last Logout Date, Logout Cause" without the quotes. The separator between two columns in a line is a comma. When uploading a file, any format error or duplicated username will terminate the uploading process. No account will be uploaded. Please correct the format in the uploading file or delete the duplicated user account in the database, then try again.  
Note2:The unit of data transfer is byte. The unit of session length is second. ID (Username) and Password must be given in upper case.

Upload On-demand User Account

File Name	<input style="width: 90%;" type="text"/> <input style="width: 5%; padding: 2px 5px;" type="button" value="Browse..."/>
-----------	--

The uploading file should be a text file and the format of each line is "**ID (Username), Password, Type, Status, Available Data transfer or Session length, Activation deadline (Date), Expired Date, Validity duration, Plan, Price, Total Data transfer or Session length when bought, Generated Date, First Login Date, Last Logout Date, Logout Cause**" without the quotes. The separator between two columns in a line is a comma. When uploading a file, any format error or duplicated username will terminate the uploading process and no account will be uploaded. Please correct the

format in the uploading file or delete the duplicated user account in the database, then try again. The unit of data transfer is byte. The unit of session length is second. ID (Username) and Password must be given in upper case.

Example1: For Session Length type

The **Type** must be written as **TIME**, Set Status must be set as **0**. Set **Session Length** in seconds. **Activation Deadline** must be in the format of yyyy/mm/dd hh:mm:ss. Set **Validity Duration** as **1**, and give a **Plan** that's already been generated and enabled from **Billing Configuration** page. Provide a price in any monetary unit defined in **On-demand User Server Configuration** page. Finally, set **Session Length when bought** the same as **Session Length**. Leave other fields blank.

User Name	Password	Type	Status	Session Length	Activation Deadline	Validity Duration	Plan	Price	Session Length when bought
USER1	PASSWORD1	TIME	0	120	2006/09/13 11:35:43	1	3	22	120
USER2	PASSWORD2	TIME	0	120	2006/09/13 11:35:43	1	3	22	120

Example2: For Total Data Transfer type

The **Type** must be written as **DATA**, Set Status must be set as **0**. Set **Total Data Transfer** in bytes. **Activation Deadline** must be in the format of yyyy/mm/dd hh:mm:ss. Set **Validity Duration** as **1**, and give a **Plan** that's already been generated and enabled from **Billing Configuration** page. Provide a price in any monetary unit defined in **On-demand User Server Configuration** page. Finally, set **Total Data Transfer when bought** the same as **Session Length**. Leave other fields blank.

User Name	Password	Type	Status	Total Data Transfer	Activation Deadline	Validity Duration	Plan	Price	Total Data Transfer when bought
USER1	PASSWORD1	DATA	0	2097152	2006/09/13 11:35:43	1	2	11	2097152
USER2	PASSWORD2	DATA	0	2097152	2006/09/13 11:35:43	1	2	11	2097152

- **Download User:** Click this to create a .txt file and then save it on disk.



**Billing Configuration:** Administrators can configure up to 10 billing plans.

Billing Configuration						
Plan	Status	Type	Expiration Time	Valid Duration	Policy Name	Price
1	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	<input type="radio"/> Data <input checked="" type="radio"/> Time	[ ] Mbyte 2 hrs 0 mins	3 days 0 hours	5 days	Policy A 20
2	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	<input checked="" type="radio"/> Data <input type="radio"/> Time	100 Mbyte [ ] hrs [ ] mins	5 days 12 hours	7 days	Policy B 10
3	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	<input type="radio"/> Data <input checked="" type="radio"/> Time	[ ] Mbyte 4 hrs 0 mins	10 days 0 hours	10 days	None 20
4	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	<input checked="" type="radio"/> Data <input type="radio"/> Time	5000 Mbyte [ ] hrs [ ] mins	20 days 0 hours	30 days	Policy A 50
5	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	<input type="radio"/> Data <input type="radio"/> Time	[ ] Mbyte [ ] hrs [ ] mins	[ ] days [ ] hours	[ ] days	None [ ]

- **Status:** Select to enable or disable this billing plan.
- **Type:** Set the billing plan by **“Data”** (the maximum volume allowed is 9,999,999 Mbyte) or **“Time”** (the maximum days allowed is 999 days).
- **Expiration time:** This is the duration of time that the account has to be activated after generation of the account. If the account is not activated during this duration the account will self-expire.
- **Valid Duration:** This is the duration of time that the user can use the Internet after activation of the account. After this duration, the account will self-expires.
- **Price:** The price charged for this billing plan.

**Create On-demand User:** Administrators can create on-demand user accounts.

Create On-demand User				
Plan	Type	Price	Status	Function
1	1 hrs 0 mins	4	Enabled	<b>Create</b>
2	4 hrs 0 mins	6	Enabled	<b>Create</b>
3	500 Mbyte	5	Enabled	<b>Create</b>
4	2000 Mbyte	8	Disabled	<b>Create</b>

Press **Create** button for the desired plan; an On-demand user account will be created, then click **Printout** to print a receipt which will contain this on-demand user's information.

 **Welcome!**

<b>Username</b>	<b>PMBN@airlive</b>
<b>Password</b>	A4X8TE9K
<b>Price</b>	€ 4
<b>Usage</b>	1 hrs 0 mins
<b>ESSID : airtlive</b>	
<b>Wireless Key :</b>	
You first time login must be done before 2007/06/11 06:49:32	
The account is valid within 5 days after your first login.	

Pls wait for login page.

**Billing Report:** Administrators can get a complete report or a report of a particular period.

 **On-demand Users Report Summary**

**From:** -- Year -- Month -- Day  
**To:** -- Year -- Month -- Day

- **Report All:** Click this to get a complete report including all the on-demand records. This report shows the total expenses and individual accounting of each plan for all plans available.

Report All	
Accounts sold in total	4
Plan1	4
Plan2	0
Plan3	0
Plan4	0
Plan5	0
Plan6	0
Plan7	0
Plan8	0
Plan9	0
Plan10	0
Total income	80
Income from tickets sold for time users	80
Income from tickets sold for volume users	0

- **Search:** Select a time period to get a period report. The report tells the total expenses and individual accounting of each plan for all plans available for that period of time.

Report from 2007/03/01 ~ 2007/03/31	
Accounts sold in total	4
Plan1	4
Plan2	0
Plan3	0
Plan4	0
Plan5	0
Plan6	0
Plan7	0
Plan8	0
Plan9	0
Plan10	0
Total income	80
Income from tickets sold for time users	80
Income from tickets sold for volume users	0

**Payment:** This section is for merchants to set up an external payment gateway to accept payments in order to provide wireless access service to end customers who wish to pay for the service on-line.

On-demand User Server Configuration	
Server Status	Enabled
Postfix	<input type="text" value="airlive"/> *(e.g. airlive. Max: 40 char)
Receipt Header 1	<input type="text" value="Welcome!"/> (e.g. Welcome!)
Receipt Header 2	<input type="text"/>
Receipt Footer	<input type="text" value="Pls wait for login page"/> (e.g. Thank You!)
Printer Baud Rate	9600 <input type="button" value="v"/>
Monetary Unit	<input checked="" type="radio"/> none <input type="radio"/> \$ USD <input type="radio"/> £ GBP <input type="radio"/> € EUR <input type="radio"/> <input type="text"/> (Input other desired monetary unit, e.g. AU)
WLAN ESSID	<input type="text" value="airlive"/> (e.g. airlive)
Wireless Key	<input type="text"/>
Remark	<input type="text"/> (for customer)
Billing Notice Interval	<input checked="" type="radio"/> 10mins <input type="radio"/> 15mins <input type="radio"/> 20mins
Twin Ticket	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
<a href="#">Users List</a> <a href="#">Billing Configuration</a> <a href="#">Create On-demand User</a> <a href="#">Billing Report</a> <a href="#">Payment</a>	

Three payment selections include **Authorize.Net**, **PayPal** and **Disable**.

 **Payment Configuration**

External Payment Gateway		
<input type="radio"/> Authorize.Net	<input checked="" type="radio"/> PayPal	<input type="radio"/> Disable

■ **Authorize.Net**

Before setting up “Authorize.Net”, it is required that the merchant owners have a valid Authorize.Net account. Please see **Appendix B – Accepting Payments via Authorize.Net, Appendix E – Examples of Making Payments for End Users** for more information about opening an Authorize.Net account and related maintenance functions.

**External Payment Gateway/ Authorize.Net Payment Page Configuration**

External Payment Gateway	
<input checked="" type="radio"/> Authorize.Net	<input type="radio"/> PayPal <input type="radio"/> Disable

Authorize.Net Payment Page Configuration	
Merchant Login ID	<input type="text" value="cnpdev1421"/> *
Merchant Transaction Key	<input type="text" value="34M49E7Ek5t2R8sX"/> *
Payment Gateway URL	<input type="text" value="https://test.authorize.net/gateway/transact.dll"/> *
Verify SSL Certificate	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Test Mode	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <input type="button" value="Try Test"/> *
MD5 Hash	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

Service Disclaimer Content	
<input type="text" value="We may collect and store the following personal information:"/>	

➤ **Authorize.Net Payment Page Configuration**

**Merchant ID:** This is the “Login ID” that comes with the Authorize.Net account

**Merchant Transaction Key:** The merchant transaction key is similar to a password and is used by Authorize.Net to authenticate transactions.

**Payment Gateway URL:** This is the default website address to post all transaction data.

**Verify SSL Certificate:** This is to help protect the system from accessing a website other than Authorize.Net

**MD5 Hash:** If transaction responses need to be encrypted by the Payment Gateway, enter and confirm a MD5 Hash Value and select a reactive mode. The MD5 Hash security feature enables merchants to verify that the results of a transaction, or transaction response, received by their server were actually sent from the Authorize.Net.

**Test Mode:** In this mode, merchants can post **test** transactions **for free** to check if the payment function works properly.

## Service Disclaimer Content/ Credit Card Payment Page/Client's Purchasing Record

**Service Disclaimer Content**

We may collect and store the following personal information:  
email address, physical contact information, credit card numbers and transactional information based on your activities on the Internet service provided by us.

**Credit Card Payment Page Billing Configuration**

Plan	Enable/Disable	Quota	Price
1	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	2 hrs 0 mins	5.00
2	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	6 hrs 0 mins	8.00
3	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	12 hrs 0 mins	12.00
4	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	600 Mbyte	5.00
5	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	1000 Mbyte	8.00
6	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	2000 Mbyte	12.00
7	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
8	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
9	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
10	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		

**Client's Purchasing Record**

Invoice Number	YK-Cafe- <input style="width: 80px;" type="text" value="00000049"/> * <input type="checkbox"/> Reset
Description	Wireless Internet Acces *
E-mail Header	Thank you very much fo *

➤ **Service Disclaimer Content**

View service agreements and fees for the standard payment gateway services here as well as adding new or editing services disclaimer.

➤ **Credit Card Payment Page Billing Configuration**

These 10 plans are the plans in **Billing Configuration**, and desired plan can be enabled.

➤ **Client's Purchasing Record**

**Invoice Number:** An invoice number may be provided as additional information against a transaction. This is a reference field that may contain any format of information.

**Description:** This is the item information to describe the product (wireless access service).

**Email Header:** Enter the information that should appear in the header of the invoice.

## Credit Card Payment Page Fields Configuration/ Credit Card Page Remark Content

Credit Card Payment Page Fields Configuration		
Item	Displayed Text	Required
<input checked="" type="checkbox"/> Credit Card Number	Credit Card Number *	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Credit Card Expiration Date	Credit Card Expiration Date *	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Card Type	Card Type * <input checked="" type="checkbox"/> Visa <input checked="" type="checkbox"/> American Express <input checked="" type="checkbox"/> Master Card <input checked="" type="checkbox"/> Discover	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Card Code	Card Code *	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> E-mail	E-mail *	<input checked="" type="checkbox"/>
<input type="checkbox"/> Customer ID	Room Number *	<input type="checkbox"/>
<input checked="" type="checkbox"/> First Name	First Name *	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Last Name	Last Name *	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Company	Company *	<input type="checkbox"/>
<input checked="" type="checkbox"/> Address	Address *	<input type="checkbox"/>
<input checked="" type="checkbox"/> City	City *	<input type="checkbox"/>
<input checked="" type="checkbox"/> State	State *	<input type="checkbox"/>
<input checked="" type="checkbox"/> Zip	Zip *	<input type="checkbox"/>
<input checked="" type="checkbox"/> Country	Country *	<input type="checkbox"/>
<input checked="" type="checkbox"/> Phone	Phone *	<input type="checkbox"/>
<input checked="" type="checkbox"/> Fax	Fax *	<input type="checkbox"/>

\*Displayed text fields must be filled.

Credit Card Payment Page Remark Content	
You must fill in the correct credit card number and expiration date. Card code is the last 3 digits of the security code located on the back of your credit card. If	<input type="text"/> <input type="text"/> <input type="text"/>

### ➤ Credit Card Payment Page Fields Configuration

**Item:** Check the box to show this item on the customer's payment interface.

**Displayed Text:** Enter what needs to be shown for this field.

**Required:** Check the box to indicate this item as a required field.

**Credit Card Number:** Credit card number of the customer. The Payment Gateway will only accept card numbers that correspond to the listed card types.

**Credit Card Expiration Date:** Month and year expiration date of the credit card. This should be entered in the format of MMY. For example, an expiration date of July 2005 should be entered as 0705.

**Card Type:** This value indicates the level of match between the Card Code entered on a transaction and the value that is on file with a customer's credit card company. A code and narrative description are provided indicating the results returned by the processor.

**Card Code:** The three- or four-digit code assigned to a customer's credit card number (found either on the front of the card at the end of the credit card number or on the back of the card).

**E-mail:** An email address may be provided along with the billing information of a transaction. This is the customer's email address and should contain an @ symbol.

**Customer ID:** This is an internal identifier for a customer that may be associated with the billing



information of a transaction. This field may contain any format of information.

**First Name:** The first name of a customer associated with the billing or shipping address of a transaction. In the case when John Doe places an order, enter John in the First Name field indicating this customer's name.

**Last Name:** The last name of a customer associated with the billing or shipping address of a transaction. In the case when John Doe places an order, enter Doe in the Last Name field indicating this customer's name.

**Company:** The name of the company associated with the billing or shipping information entered on a given transaction.

**Address:** The address entered either in the billing or shipping information of a given transaction.

**City:** The city is associated with either the billing address or shipping address of a transaction.

**State:** A state is associated with both the billing and shipping address of a transaction. This may be entered as either a two-character abbreviation or the full text name of the state.

**Zip:** The ZIP code represents the five or nine digit postal code associated with the billing or shipping address of a transaction. This may be entered as five digits, nine digits, or five digits and four digits.

**Country:** The country is associated with both the billing and shipping address of a transaction. This may be entered as either an abbreviation or full value.

**Phone:** A phone number is associated with both a billing and shipping address of a transaction. Phone number information may be entered as all number or it may include parentheses or dashes to separate the area code and number.

**Fax:** A fax number may be associated with the billing information of a transaction. This number may be entered as all number or contain parentheses and dashes to separate the area code and number.

➤ **Credit Card Payment Page Remark Content**

Enter additional details for the transaction such as Tax, Freight and Duty Amounts, Tax Exempt status, and a Purchase Order Number, if applicable.

■ **PayPal**

Before setting up “PayPal”, it is required that the merchant owners have a valid PayPal “Business Account”. Please see **Appendix D – Accepting Payments via PayPal, Appendix E – Examples of Making Payments for End Users** for more information about setting up a PayPal Business Account, relevant maintenance functions, and example for end users.

After opening a PayPal Business Account, the merchant should **find the “Identity Token” of this PayPal account to continue “PayPal Payment Page Configuration”**. For more details, please see the steps in **Appendix D / 1. Setting Up**.

**External Payment Gateway/ PayPal Payment Page Configuration**

External Payment Gateway	
<input type="radio"/> Authorize.Net	<input checked="" type="radio"/> PayPal
<input type="radio"/> Disable	

PayPal Payment Page Configuration	
Business Account	<input type="text"/> -
Payment Gateway URL	<input type="text" value="https://www.paypal.com/cgi-bin/webscr"/> -
Identity Token	<input type="text"/> -
Verify SSL Certificate	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Currency	<input type="text" value="USD (U.S. Dollar)"/> ▾ -

Service Disclaimer Content	
We may collect and store the following personal information: <span style="float: right;">▲ ▼</span>	

➤ **PayPal Payment Page Configuration**

**Business Account:** This is the “Login ID” (email address) that is associated with the PayPal Business Account.

**Payment Gateway URL:** This is the default website address to post all transaction data.

**Identity Token:** This is the key used by PayPal to validate all the transactions.

**Verify SSL Certificate:** This is to help protect the system from accessing a website other than PayPal

**Currency:** It is the currency to be used for the payment transactions.

## Service Disclaimer Content /Billing Configuration for Payment Page

**Service Disclaimer Content**

We may collect and store the following personal information:  
 email address, physical contact information, credit card numbers and transactional information based on your activities on the Internet service provided by us.  
 If the information you provide cannot be verified, we may

Billing Configuration for Payment Page				
Plan	Enable/Disable		Quota	Price
1	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable	2 hrs 0 mins	0.01
2	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable	2 Mbyte	0.02
3	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable	3 Mbyte	0.03
4	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable		
5	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable		
6	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable		
7	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable		
8	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable		
9	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable		
10	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable		

➤ **Service Disclaimer Content**

View service agreements and fees for the standard payment gateway services here as well as adding new or editing services disclaimer.

➤ **Billing Configuration for Payment Page**

These 10 plans are the plans in **Billing Configuration**, and desired plan can be enabled.

**Enable/Disable:** Choose to enable or cancel the plan.

**Quota:** The usage time or condition of each plan.

**Price:** The price charged for this plan.

## Client's Purchasing Record/ PayPal Payment Page Remark Content

Client's Purchasing Record	
Invoice Number	Hotspot - 00000001 <input type="checkbox"/> Reset
Description (Item Name)	Internet access .
Title for Message to Seller	Special Note to Seller .

PayPal Payment Page Remark Content	
( A ) Payment is accepted via PayPal. PayPal enables you to send payments securely online using PayPal account, a credit card or bank account. Clicking on "Buy Now" button,	

### ➤ Client's Purchasing Record

**Invoice Number:** An invoice number may be provided as additional information against a transaction. This is a reference field that may contain any format of information.

**Description:** This is the item information to describe the product (wireless access service).

**Title for Message to Seller:** Administrators can edit the header "title" of the message note, used in the PayPal payment page.

### ➤ PayPal Payment Page Remark Content

The message content will be displayed as a special notice to end customers in the page of "Rate Plan". For example, it can describe the cautions for making a payment via PayPal.

## 4.2.2 Black List Configuration

The administrator can add, delete, or edit the black list for user access control. Each black list can include 40 users at most. If a user in the black list wants to log into the system, the user's access will be denied. The administrator can use the pull-down menu to select the desired black list.

Black List Configuration		
Select Black List:	1:Blacklist1	
Name	Blacklist1	
User	Remark	Delete

(Total:0) [First](#) [Prev](#) [Next](#) [Last](#)

[Add User to List](#)

- **Select Black List:** There are 5 lists to select from for the desired black list.
- **Name:** Set the black list name and it will show on the pull-down menu above.
- **Add User to List:** Click the hyperlink to add users to the selected black list.

Add Users to Blacklist Blacklist1		
Item	Username	Remark
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>

After entering the usernames in the “**Username**” blanks and the related information in the “**Remark**” blank (not required), click **Apply** to add the users.

User '12345' has been added!

 **Add Users to Blacklist**

Add Users to Blacklist Blacklist1		
Item	Username	Remark
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>

If removing a user from the black list is desired, select the user's “**Delete**” check box and then click the **Delete** button to remove that user from the black list.

Black List Configuration		
Select Black List:	1:Blacklist1	
Name	Blacklist1	
User	Remark	Delete
12345		<input checked="" type="checkbox"/>

(Total:1) [First](#) [Prev](#) [Next](#) [Last](#)

[Add User to List](#)

## 4.2.3 Policy Configuration

Every Policy has three profiles, **Firewall Profile**, **Specific Route Profile**, and **Schedule Profile** as well as **Bandwidth** setting for that policy and for individual clients.

Policy Configuration	
Select Policy:	Policy A ▼
Firewall Profile	<a href="#">Setting</a>
Specific Route Profile	<a href="#">Setting</a>
Schedule Profile	<a href="#">Setting</a>
Total Bandwidth	Unlimited ▼
Individual Maximum Bandwidth	Unlimited ▼
Individual Request Bandwidth	None ▼

- Firewall Profile**

Click the hyperlink of **Setting** for **Firewall Profile**, the Firewall Profiles list will appear. Click the numbers of **Filter Rule Item** to edit individual rules and click **Apply** to save the settings. The rule status will show on the list. Check “**Active**” to enable that rule.

Profile Name:

Firewall Profile						
Filter Rule Item	Active	Action	Name	Source Destination	Protocol	MAC
1	<input type="checkbox"/>	Block		ANY ANY	ALL	
2	<input type="checkbox"/>	Block		ANY ANY	ALL	

Edit Filter Rule					
Rule Item: 1					
Rule Name: <input type="text"/>			<input type="checkbox"/> Enable this Rule		
Action: <input type="text" value="Block"/>			Protocol: <input type="text" value="ALL"/>		
Source MAC Address: <input type="text"/> (For Specific MAC Address Filter)					
	Interface	IP	Subnet Mask	Start Port	End Port
Source	<input type="text" value="ALL"/>	<input type="text"/>	<input type="text" value="255.255.255.255 (/32)"/>	<input type="text"/>	<input type="text"/>
Destination	<input type="text" value="ALL"/>	<input type="text"/>	<input type="text" value="255.255.255.255 (/32)"/>	<input type="text"/>	<input type="text"/>

**Rule Item:** This is the rule that you have selected.

**Rule Name:** The rule name can be changed here.

**Enable this Rule:** After checking this function, the rule will be enabled.

**Action:** There are two options, **Block** and **Pass**. **Block** is to prevent packets from passing and **Pass** is to permit packets passing.

**Protocol:** There are three protocols to select, **TCP**, **UDP** and **ICMP**, or choose **ALL** to use all three protocols.

**Source MAC Address:** The MAC address of the source IP address. This is for specific MAC address filter.

**Source/Destination Interface:** There are four interfaces to choose, **WAN**, **Wireless**, **Public LAN (LAN1/LAN2)** and **Private LAN (LAN3/LAN4)**.

**Source/Destination IP:** Enter the source and destination IP addresses.

**Source/Destination Subnet Mask:** Enter the source and destination subnet masks.

**Source/Destination Start/End Port:** Enter the range of source and destination ports.

- Specific Route Profile**

Click the hyperlink of **Setting** for **Specific Route Profile**, the Specific Route Profile list will appear.

Profile Name:

Specific Route Profile				
Route Item	Destination		Gateway	Default
	IP Address	Subnet Netmask	IP Address	
1	<input type="text"/>	255.255.255.255 (/32) ▼	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	255.255.255.255 (/32) ▼	<input type="text"/>	<input type="checkbox"/>

**Profile Name:** The profile name can be changed here.

**IP Address:** The destination IP address of the host or the network.

**Subnet Netmask:** Select a destination subnet netmask of the host or the network.

**IP Address:** The IP address of the next router to the destination.

**Default:** Check this option to apply the default value.

- Schedule Profile**

Click the hyperlink of **Setting** for **Schedule Profile** to enter the Schedule Profile list. Select **“Enable”** to show the list. This function is used to restrict the time the users can log in. Please enable/disable the desired time slot and click **Apply** to save the settings. These settings will become effective immediately after clicking the **Apply** button.

Profile Name:   Enable  Disable

Profile Name:   Enable  Disable

Login Schedule Profile							
HOURL	SUN	MON	TUE	WED	THU	FRI	SAT
0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
10	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

- **Bandwidth**

Choose one bandwidth limit for that particular policy.

The screenshot shows the 'Policy Configuration' window. At the top, 'Select Policy' is set to 'Policy A'. Below are several rows with 'Setting' links: Firewall Profile, Specific Route Profile, and Schedule Profile. The 'Total Bandwidth' is set to 'Unlimited'. The 'Individual Maximum Bandwidth' dropdown is open, showing a list of options: Unlimited, 16 Kbps, 32 Kbps, 64 Kbps, 128 Kbps, 256 Kbps, 512 Kbps, 1 Mbps, 2 Mbps, 3 Mbps, 5 Mbps, 8 Mbps, 11 Mbps, 22 Mbps, and 54 Mbps. The 'Apply' button is highlighted with a checkmark, and a 'Clear' button is also visible.

#### 4.2.4 Guest User Configuration

This function can permit guests to log into the system. Select “**Enable Guest User**” and click **Apply** to save the settings.

The screenshot shows the 'Guest User Configuration' window. It has two radio buttons: 'Enable Guest User' (selected) and 'Disable Guest User'. Below them is a link for 'Guest User List'. There are three configuration fields: 'Policy' set to 'None', 'Session Length' set to '6 hours', and 'Idle Timer' set to '10 minutes' with a red note indicating a range of 1-1440 minutes.

- **Guest User List:** AirLive WIAS-1200G offers 10 guest users for log in. To activate a guest user, just enter the password in the corresponding “**Password**” text field for that guest account. Guest accounts with blank password will not be activated.

Guest Users List		
Item	Username	Password
1	guest1	12345
2	guest2	

- **Policy:** Select one policy to apply to.
- **Session Length:** This restricts the connection time of the guest users. The default session length is 6 hours and the available session time ranges from 1 to 12 hours or unlimited.
- **Idle Time:** If a user has been idled with no network activities, the system will automatically kick out the user. The logout timer can be set in the range of 1~1440 minutes, and the default logout time is 10 minutes.



## 4.2.5 Additional Configuration

Additional Configuration	
<b>User Control</b>	Idle Timer: <input type="text" value="10"/> minutes <small>*(Range: 1-1440)</small>
	Multiple Login <input type="checkbox"/> <small>(On-demand and RADIUS authentication do NOT support multiple login.)</small>
	Friendly Logout <input checked="" type="checkbox"/>
<b>Internet Connection Detection</b>	http:// <input type="text"/>
<b>Upload File</b>	<a href="#">Certificate</a> <a href="#">Login Page</a> <a href="#">Logout Page</a> <a href="#">Login Success Page</a> <a href="#">Login Success Page for On-Demand</a> <a href="#">Logout Success Page</a>
<b>Credit Reminder</b>	Volume <input type="radio"/> Enabled <input checked="" type="radio"/> Disable
	Time <input type="radio"/> Enabled <input checked="" type="radio"/> Disable
<b>POP3 Message</b>	<a href="#">Edit Mail Message</a>
<b>Enhance User Authenticate</b>	<a href="#">Permit MAC Address List</a>
<b>SMTP Redirect</b>	<input type="radio"/> Enabled <input checked="" type="radio"/> Disable

- User Control:** Functions under this section applies for all general users.
 

**Idle Timer:** If a user has been idled with no network activities, the system will automatically kick out the user. The logout timer can be set in the range of 1~1440 minutes, and the default logout time is 10 minutes.

**Multiple Login:** When enabled, a user can log in from different computers with the same account. (This function doesn't support On-demand users and RADIUS accounting.)

**Friendly Logout:** When a user logs into the network with wireless connection, a small window will appear to show the user's information and there is a logout button for the logout. If enabled. When the users try to close the small window, there will be a new popup window to confirm the logout in case the users click the logout button by accident.
- Internet Connection Detection:** Enter a specific URL or IP address and AirLive WIAS-1200G will try to detect the network connection by sending packets directly to that specific URL or IP address. If there is a problem in the connection of the WAN port of the system such that the URL or IP address specified cannot be reached, there will be a connection failed message showing on the users' login screen.
- Upload File**
  - Certification:** The administrator can upload new private key and customer certification. Click the **Browse** button to select the file for the certificate upload. Then click **Submit** to complete the upload process.

Upload Private Key	
File Name	<input type="text"/> <input type="button" value="Browse..."/>

Upload Customer Certificate	
File Name	<input type="text"/> <input type="button" value="Browse..."/>

Click **Use Default Certificate** to use the default certificate and key.

You just overwrite with default KEY & default CA file

2. **Login Page:** The administrator can use the default login page or get the customized login page by setting the template page, uploading the page or downloading from the specific website. After finishing the setting, click **Preview** to see the login page.

a. Choose **Default Page** to use the default login page.

**Upload Login Page**

**Login Page Selection for Users**

Default Page       Template Page

Uploaded Page       External Page

**Default Page Setting**

This is default login page for users.  
You could click preview link to preview the default login page.  
Thanks.

[Preview](#)

b. Choose **Template Page** to make a customized login page here. Click **Select** to pick up a color and then fill in all of the blanks. Click **Preview** to see the result first.

 Upload Login Page

Login Page Selection for Users	
<input type="radio"/> Default Page	<input checked="" type="radio"/> Template Page
<input type="radio"/> Uploaded Page	<input type="radio"/> External Page

Template Page Setting	
Color for Title Background	<input type="text"/> <a href="#">Select</a> (RGB values in hex mode)
Color for Title Text	<input type="text"/> <a href="#">Select</a> (RGB values in hex mode)
Color for Page Background	<input type="text"/> <a href="#">Select</a> (RGB values in hex mode)
Color for Page Text	<input type="text"/> <a href="#">Select</a> (RGB values in hex mode)
Title	<input type="text" value="User Login Page"/>
Welcome	<input type="text" value="Welcome To User Login Page"/>
Information	<input type="text" value="Please Enter Your Name and Password to Sign In"/>
Username	<input type="text" value="Username"/>
Password	<input type="text" value="Password"/>
Submit	<input type="text" value="Submit"/>
Clear	<input type="text" value="Clear"/>
Remaining	<input type="text" value="Remaining"/>
Copyright	<input type="text" value="Copyright (c)"/>
<input type="button" value="Preview"/>	

- c. Choose **Uploaded Page** and you can get the login page by uploading. Click the **Browse** button to select the file for the login page upload. Then click **Submit** to complete the upload process.

 Upload Login Page

Login Page Selection for Users	
<input type="radio"/> Default Page	<input type="radio"/> Template Page
<input checked="" type="radio"/> Uploaded Page	<input type="radio"/> External Page

Uploaded Page Setting	
File Name	<input type="text"/> <input type="button" value="Browse..."/>
<input type="button" value="Submit"/>	

**Existing Image Files:**

<b>Total Capacity:</b> 512 K	
<b>Now Used:</b> 0 K	
Upload Image Files	
Upload Images	<input type="text"/> <input type="button" value="Browse..."/>
<input type="button" value="Submit"/>	
<a href="#">Preview</a>	

After the upload process is completed, the new login page can be previewed by clicking **Preview** button at the bottom.



[Click here to purchase by Credit Card Online.](#)

The user-defined login page must include the following HTML codes to provide the necessary fields for username and password.

```
<form action="us erlogin.shtml" method="post" name="Enter">
<input type="text" name="myus ername">
<input type="password" name="mypassword">
<input type="submit" name="submit" value="Enter">
<input type="reset" name="clear" value="Clear">
</form>
```

If the user-defined login page includes an image file, the image file path in the HTML code must be the image file you will upload.

```

```

Then, enter or browse the filename of the images to upload in the **Upload Images** field on the **Upload Images Files** page and then click **Submit**. The system will show the used space and the maximum size of the image file of 512K. If the administrator wishes to restore the factory default of the login page, click the **Use Default Page** button to restore it to default.

<b>Total Capacity:</b> 512 K	
<b>Now Used:</b> 0 K	
Upload Image Files	
Upload Images	<input type="text"/> <input type="button" value="Browse..."/>
<input type="button" value="Submit"/>	

After the image file is uploaded, the file name will show on the **"Existing Image Files"** field. Check the file and click **Delete** to delete the file.

<b>Existing Image Files :</b>
1102474548_732cn.gif <input type="checkbox"/>
<input type="button" value="Delete"/>

In AirLive WIAS-1200G, the end user first gets a login page when she/he opens its web browser right after

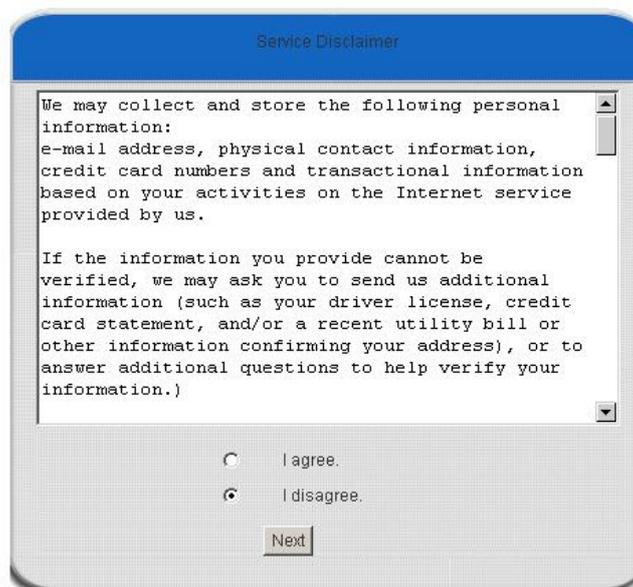
associating with an access point. However, in some situations, the hotspot owners or MIS staff may want to display “terms of use” or announcement information before the login page. Hotspot owners or MIS staff can design a new disclaimer/announcement page and save the page in their local server. After the agreement shown on the page is read, users are asked whether they agree or disagree with the disclaimer. By clicking I agree, users are able to log in. If users choose to decline, they will get a popup window saying they are unable to log in. The basic design is to have the disclaimer and login function in the same page but with the login function hidden until users agree with the disclaimer.

**For more details about the codes of the disclaimer, please refer to Appendix E.**

If the page is successfully loaded, an **upload success** page will show up.



“Preview” can be clicked to see the uploaded page.



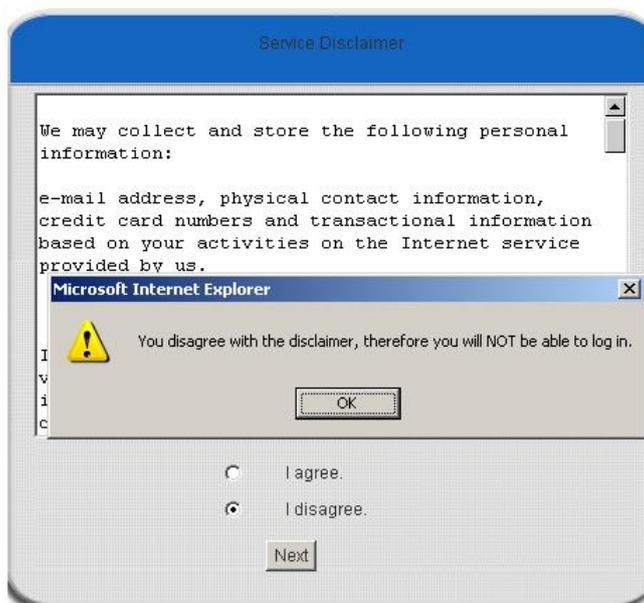
[Click here to purchase by Credit Card Online.](#)

If user checks “I agree” and clicks **Next**, then he/she is prompted to fill in the login name and password.



[Click here to purchase by Credit Card Online.](#)

If user checks “I disagree” and clicks **Next**, a window will pop up to tell user that he/she cannot log in



- d. Choose the **External Page** selection and you can get the login page from the specific website. Enter the website address in the “**External Page Setting**” field and then click **Apply**.

Login Page Selection for Users	
<input type="radio"/> Default Page	<input type="radio"/> Template Page
<input type="radio"/> Uploaded Page	<input checked="" type="radio"/> External Page

External Page Setting	
External URL :	<input type="text" value="http://"/>
<input type="button" value="Preview"/>	

The **External Page** prepared to be loaded here needs to have the following code as well to let the system work properly

```
<form action="userlogin.shtml" method="post" name="Enter">
<input type="text" name="myusername">
<input type="password" name="mypassword">
<input type="submit" name="submit" value="Enter">
<input type="reset" name="clear" value="Clear">
</form>
```

After applying the setting, the new login page can be previewed by clicking **Preview** button at the bottom of this page.



3. **Logout Page:** The users can apply their own logout page here. The process is similar to that of Logout Page.

Upload Logout Page

File Name		<input type="button" value="Browse..."/>
<input type="button" value="Submit"/>		<input type="button" value="Use Default Page"/>

**Existing Image Files:**

<b>Total Capacity:</b> 512 K		
<b>Now Used:</b> 0 K		
Upload Image Files		
Upload Images		<input type="button" value="Browse..."/>
<input type="button" value="Submit"/>		

The different part is the HTML code of the user-defined logout interface must include the following HTML code that the user can enter the username and password. After the upload is completed, the user-defined login user interface can be previewed by clicking **Preview** at the bottom of this page. If want to restore the factory default setting of the logout interface, click the “**Use Default Page**” button.

4. **Login Success Page:** The administrator can use the default login success page or get the customized login success page by setting the template page, uploading the page or downloading from the specific website. After finishing the setting, you can click **Preview** to see the login success page.
  - a. Choose **Default Page** to use the default login success page.

Upload Login Success Page

Login Success Page Selection for Users	
<input checked="" type="radio"/> Default Page	<input type="radio"/> Template Page
<input type="radio"/> Uploaded Page	<input type="radio"/> External Page

Default Page Setting	
This is default success login page for users. You could click preview link to preview the default success login page. Thanks.	
<a href="#" style="color: #0000FF; text-decoration: underline;">Preview</a>	



- b. Choose **Template Page** to make a customized login success page here. Click **Select** to pick up a color and then fill in all of the blanks. You can click **Preview** to see the result first.

 **Upload Login Success Page**

Login Success Page Selection for Users	
<input type="radio"/> Default Page	<input checked="" type="radio"/> Template Page
<input type="radio"/> Uploaded Page	<input type="radio"/> External Page

Template Page Setting	
Color for Title Background	<input type="text"/> <a href="#">Select</a> (RGB values in hex mode)
Color for Title Text	<input type="text"/> <a href="#">Select</a> (RGB values in hex mode)
Color for Page Background	<input type="text"/> <a href="#">Select</a> (RGB values in hex mode)
Color for Page Text	<input type="text"/> <a href="#">Select</a> (RGB values in hex mode)
Title	<input type="text" value="Login Succeed Page"/>
Welcome	<input type="text" value="Hello"/>
Information	<input type="text" value="Please click this button to"/>
Logout	<input type="text" value="Logout"/>
Information2	<input type="text" value="Thank you"/>
Login Time	<input type="text" value="Login Time"/>
<input type="button" value="Preview"/>	

- c. Choose **Uploaded Page** and you can get the login success page by uploading. Click the **Browse** button to select the file for the login success page upload. Then click **Submit** to complete the upload process.

 **Upload Login Success Page**

Login Success Page Selection for Users	
<input type="radio"/> Default Page	<input type="radio"/> Template Page
<input checked="" type="radio"/> Uploaded Page	<input type="radio"/> External Page

Uploaded Page Setting	
File Name	<input type="text"/> <input type="button" value="Browse..."/>
<input type="button" value="Submit"/>	

**Existing Image Files:**

<b>Total Capacity:</b> 512 K
<b>Now Used:</b> 0 K
Upload Image Files
Upload Images <input type="text"/> <input type="button" value="Browse..."/>
<input type="button" value="Submit"/>
<a href="#">Preview</a>

After the upload process is completed, the new login success page can be previewed by clicking **Preview** button at the bottom.

Enter or browse the filename of the images to upload in the **Upload Images** field on the **Upload Images Files** page and then click **Submit**. The system will show the used space and the maximum size of the image file of 512K. If the administrator wishes to restore the factory default of the login success page, click the **Use Default Page** button to restore it to default.

After the image file is uploaded, the file name will show on the “**Existing Image Files**” field. Check the file and click **Delete** to delete the file.

- d. Choose the **External Page** selection and get the login success page from the specific website. Enter the website address in the “**External Page Setting**” field and then click **Apply**. After applying the setting, the new login success page can be previewed by clicking **Preview** button at the bottom of this page.

 **Upload Login Success Page**

5. **Login Success Page for On-Demand:** The administrator can use the default login success page for On-Demand or get the customized login success page for On-Demand by setting the template page, uploading the page or downloading from the specific website. After finishing the setting, you can click **Preview** to see the login success page for On-Demand.

- a. Choose **Default Page** to use the default login success page for On-Demand.

 **Upload Login Success Page for on-demand**

- b. Choose **Template Page** to make a customized login success page for On-Demand here. Click **Select** to pick up a color and then fill in all of the blanks. You can click **Preview** to see the result first.

 **Upload Login Success Page for on-demand**

Login Success Page Selection for on-demand Users	
<input type="radio"/> Default Page	<input checked="" type="radio"/> Template Page
<input type="radio"/> Uploaded Page	<input type="radio"/> External Page

Template Page Setting	
Color for Title Background	<input type="text"/> <a href="#">Select</a> (RGB values in hex mode)
Color for Title Text	<input type="text"/> <a href="#">Select</a> (RGB values in hex mode)
Color for Page Background	<input type="text"/> <a href="#">Select</a> (RGB values in hex mode)
Color for Page Text	<input type="text"/> <a href="#">Select</a> (RGB values in hex mode)
Title	<input type="text" value="Login Succeed Page for on-demand"/>
Welcome	<input type="text" value="Welcome"/>
Information	<input type="text" value="Please click this button to"/>
Logout	<input type="text" value="Logout"/>
Information2	<input type="text" value="Thank you"/>
Remaining Usage	<input type="text" value="Remaining Usage"/>
Day	<input type="text" value="Day"/>
Hour	<input type="text" value="Hour"/>
Min	<input type="text" value="Min"/>
Sec	<input type="text" value="Sec"/>
Login Time	<input type="text" value="Login Time"/>
Redeem	<input type="text" value="Redeem"/>
<input type="button" value="Preview"/>	

- c. Choose **Uploaded Page** and click the **Browse** button to select the file for the login success page for On-Demand upload. Then click **Submit** to complete the upload process.

 **Upload Login Success Page for on-demand**

Login Success Page Selection for on-demand Users	
<input type="radio"/> Default Page	<input type="radio"/> Template Page
<input checked="" type="radio"/> Uploaded Page	<input type="radio"/> External Page

Upload Login Success Page for on-demand	
File Name	<input type="text"/> <input type="button" value="Browse..."/>
<input type="button" value="Submit"/>	

**Existing Image Files:**

---

**Total Capacity:** 512 K  
**Now Used:** 0 K

Upload Image Files	
Upload Images	<input type="text"/> <input type="button" value="Browse..."/>
<input type="button" value="Submit"/>	
<a href="#">Preview</a>	

After the upload process is completed, the new login success page for On-Demand can be previewed by clicking **Preview** button at the bottom.

If the user-defined login success page for On-Demand includes an image file, the image file path in the HTML code must be the image file you will upload.

****

Enter or browse the filename of the images to upload in the **Upload Images** field on the **Upload Images Files** page and then click **Submit**. The system will show the used space and the maximum size of the image file of 512K. If the administrator wishes to restore the factory default of the login success page for On-Demand, click the **Use Default Page** button to restore it to default.

<b>Total Capacity:</b> 512 K <b>Now Used:</b> 0 K
Upload Image Files
Upload Images <input type="text"/> <input type="button" value="Browse..."/>
<input type="button" value="Submit"/>

After the image file is uploaded, the file name will show on the **Existing Image Files** field. Check the file and click **Delete** to delete the file.

<b>Existing Image Files :</b>
1102474548_732cn.gif <input type="checkbox"/>
<input type="button" value="Delete"/>

- d. Choose the **External Page** selection and you can get the login success page for On-Demand e from the specific website. Enter the website address in the “**External Page Setting**” field and then click **Apply**. After applying the setting, the new login success page for On-Demand can be previewed by clicking **Preview** button at the bottom of this page.

 **Upload Login Success Page for on-demand**

Login Success Page Selection for on-demand Users	
<input type="radio"/> Default Page	<input type="radio"/> Template Page
<input type="radio"/> Uploaded Page	<input checked="" type="radio"/> External Page

External Page Setting	
External URL:	<input type="text" value="http://"/>
<input type="button" value="Preview"/>	

6. **Logout Success Page:** The administrator can use the default logout success page or get the customized login success page by setting the template page, uploading the page or downloading from the specific website. After finishing the setting, you can click **Preview** to see the logout success page.
  - a. Choose **Default Page** to use the default logout success page.

 **Upload Logout Success Page**

Logout Success Page Selection for Users	
<input checked="" type="radio"/> Default Page	<input type="radio"/> Template Page
<input type="radio"/> Uploaded Page	<input type="radio"/> External Page

Default Page Setting
<p><b>This is default logout success page for users.</b>  <b>You could click preview link to preview the default logout success page.</b>  <b>Thanks.</b></p> <p style="text-align: center;"><a href="#">Preview</a></p>

- b. Choose **Template Page** to make a customized logout success page here. Click **Select** to pick up a color and then fill in all of the blanks. Click **Preview** to see the result first.

 **Upload Logout Success Page**

Logout Success Page Selection for Users	
<input type="radio"/> Default Page	<input checked="" type="radio"/> Template Page
<input type="radio"/> Uploaded Page	<input type="radio"/> External Page

Template Page Setting	
Color for Title Background	<input type="text"/> <a href="#">Select</a> (RGB values in hex mode)
Color for Title Text	<input type="text"/> <a href="#">Select</a> (RGB values in hex mode)
Color for Page Background	<input type="text"/> <a href="#">Select</a> (RGB values in hex mode)
Color for Page Text	<input type="text"/> <a href="#">Select</a> (RGB values in hex mode)
Title	<input type="text" value="Logout Succeed Page"/>
Information	<input type="text" value="Logout successfully"/>
<input type="button" value="Preview"/>	

- c. Choose **Uploaded Page** and click the **Browse** button to select the file for the logout success page upload. Then click **Submit** to complete the upload process.

 **Upload Logout Success Page**

Logout Success Page Selection for Users	
<input type="radio"/> Default Page	<input type="radio"/> Template Page
<input checked="" type="radio"/> Uploaded Page	<input type="radio"/> External Page

Upload Logout Success Page	
File Name	<input type="text"/> <input type="button" value="Browse..."/>
<input type="button" value="Submit"/>	

**Existing Image Files:**

<b>Total Capacity:</b> 512 K
<b>Now Used:</b> 0 K

Upload Image Files	
Upload Images	<input type="text"/> <input type="button" value="Browse..."/>
<input type="button" value="Submit"/>	
<a href="#">Preview</a>	

After the upload process is completed, the new logout success page can be previewed by clicking **Preview** button at the bottom.

If the user-defined logout success page includes an image file, the image file path in the HTML code must be the image file you will upload.

``

Enter or browse the filename of the images to upload in the **Upload Images** field on the **Upload Images Files** page and then click **Submit**. The system will show the used space and the maximum size of the image file of 512K. If the administrator wishes to restore the factory default of the login success page, click the **Use Default Page** button to restore it to default.

After the image file is uploaded, the file name will show on the “**Existing Image Files**” field. Check the file and click **Delete** to delete the file.

- d. Choose the **External Page** selection and you can get the logout success page from the specific website. Enter the website address in the “**External Page Setting**” field and then click **Apply**. After applying the setting, the new logout success page can be previewed by clicking **Preview** button at the bottom of this page.

- **Credit Reminder:** The administrator can enable this function to remind the on-demand users before their credit run out. There are two kinds of reminder, **Volume** and **Time**. The default reminding trigger level for **Volume** is 1Mbyte and the level for **Time** is 5 minutes.

- **POP3 Message:** Before the users log into the network with their usernames and passwords, the users will receive a welcome mail from AirLive WIAS-1200G. The administrator can edit the contents.

**Edit Mail Message**

Text	<pre>&lt;!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN"&gt; &lt;HTML&gt;&lt;HEAD&gt; &lt;META HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=us-ascii"&gt; &lt;/HEAD&gt; &lt;BODY&gt; &lt;DIV&gt; &lt;DIV&gt; &lt;FONT face="Times New Roman" size=6&gt; &lt;STRONG&gt;Welcome!&lt;/STRONG&gt; &lt;/FONT&gt; &lt;/DIV&gt; &lt;DIV&gt; &lt;FONT size=4&gt;&lt;STRONG&gt;&lt;/STRONG&gt; &lt;/FONT&gt;</pre>
------	---

- **Enhance User Authentication:** With this function, only the users with their MAC addresses in this list can log into AirLive WIAS-1200G. However, user authentication is still required for these users. Please enter the **Permit MAC Address List** to fill in these MAC addresses, select **Enable**, and then click **Apply**.

**MAC Address Control**

Enable
  Disable

Item	MAC Address	Item	MAC Address
1	<input style="width: 100%;" type="text"/>	2	<input style="width: 100%;" type="text"/>
3	<input style="width: 100%;" type="text"/>	4	<input style="width: 100%;" type="text"/>

**Note:** The format of the MAC address is: xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx.

- **SMTP Redirect:** Redirection of the IP address of the SMTP server

Enabled
  Disable

SMTP Server:  Port:



## 4.3 Network Configuration

This section includes the following functions: **Network Address Translation**, **Privilege List**, **Monitor IP List**, **Walled Garden List**, **Proxy Server Properties** and **Dynamic DNS**.

Network Configuration	
<b>Network Address Translation</b>	WIAS-1200G provides 3 types of network address translation: Static Assignments, Public Accessible Server and IP/Port Redirect.
<b>Privilege List</b>	System provides Privilege IP Address List and Privilege MAC Address List. System will NOT control the network access of those listed devices.
<b>Monitor IP List</b>	System can monitor up to 40 network devices with the defined probe interval and retrying.
<b>Walled Garden List</b>	Up to 20 hosts' URL could be defined in Walled Garden List. Clients may access these URL without authentication.
<b>Proxy Server Properties</b>	WIAS-1000GV2 supports up to 10 external proxy servers. System can redirect traffic to external proxy server into built-in proxy server.
<b>Dynamic DNS</b>	WIAS-1200G supports dynamic DNS (DDNS) feature.

### 4.3.1 Network Address Translation

There are three parts, **Static Assignments**, **Public Accessible Server** and **Port and Redirect**, need to be set.

Network Address Translation
<a href="#">Static Assignments</a>
<a href="#">Public Accessible Server</a>
<a href="#">Port and IP Redirect</a>

- Static Assignments**

A computer within the Static Assignments is unprotected by firewall and typically all port accesses are routed through to that computer. A router will forward all traffic to the computer specified in the Static Assignments if it does not otherwise have a rule for how to forward traffic on a given port. There are 40 sets of static **Internal IP Address** and **External IP Address** available. These static IP addresses can be set to the any host which itself needs a static IP address to access the network through WAN port. These settings will become effective immediately after clicking the **Apply** button.

Static Assignments		
Item	Internal IP Address	External IP Address
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>

(Total:40) [First](#) [Prev](#) [Next](#) [Last](#)

- Public Accessible Server**

This function allows the administrator to set 40 virtual servers at most, so that the computers not belonging to the managed network can access the servers in the managed network. Please enter the “**External Service Port**”, “**Local Server IP Address**” and “**Local Server Port**”. According to the different services provided, the network service can use the **TCP** protocol or the **UDP** protocol. In the **Enable** column, check the desired server to enable. These settings will become effective immediately after clicking the **Apply** button.

Public Accessible Server					
Item	External Service Port	Local Server IP Address	Local Server Port	Type	Enable
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
6	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
7	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
8	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
9	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
10	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>

(Total:40) [First](#) [Prev](#) [Next](#) [Last](#)

- **Port and IP Redirect**

This function allows the administrator to set 40 sets of the IP addresses at most for redirection purpose. When the user attempts to connect to a destination IP address listed here, the connection packet will be converted and redirected to the corresponding destination. Please enter the **“IP Address”** and **“Port”** of **Destination**, and the **“IP Address”** and **“Port”** of **Translated to Destination**. According to the different services provided, choose the **“TCP”** protocol or the **“UDP”** protocol. These settings will become effective immediately after clicking **Apply**.

Item	Destination		Translated to Destination		Type
	IP Address	Port	IP Address	Port	
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP
2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP
3	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP
4	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP
5	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP
6	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP
7	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP
8	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP
9	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP
10	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP

(Total:40) [First](#) [Prev](#) [Next](#) [Last](#)

## 4.3.2 Privilege List

There are two parts, **Privilege IP Address List** and **Privilege MAC Address List**, can be set.

Privilege List
<a href="#">Privilege IP Address List</a>
<a href="#">Privilege MAC Address List</a>

- **Privilege IP Address List**

If there are some workstations belonging to the managed server that need to access the network without authentication, enter the IP addresses of these workstations in this list. The “**Remark**” blank is not necessary but is useful to keep track. AirLive WIAS-1200G allows 100 privilege IP addresses at most. These settings will become effective immediately after clicking **Apply**.

Privilege IP Address List		
Item	Privilege IP Address	Remark
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>

(Total:100) [First](#) [Prev](#) [Next](#) [Last](#)

**Note:** *Permitting specific IP addresses to have network access rights without going through standard authentication process at the Public LAN (LAN1/LAN2) may cause security problems.*

- **Privilege MAC Address List**

In addition to the IP address, the MAC address of the workstations that need to access the network without authentication can also be set in this list. AirLive WIAS-1200G allows 100 privilege MAC addresses at most. When manually creating the list, enter the MAC address (the format is xx:xx:xx:xx:xx:xx) as well as the remark (not necessary). These settings will become effective immediately after clicking **Apply**.

Privilege MAC Address List		
Item	MAC Address	Remark
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>

(Total:100) [First](#) [Prev](#) [Next](#) [Last](#)

**Note:** *Permitting specific MAC addresses to have network access rights without going through standard authentication process at the Public LAN (LAN1/LAN2) may cause security problems.*

### 4.3.3 Monitor IP List

AirLive WIAS-1200G will send out a packet periodically to monitor the connection status of the IP addresses on the list. If the monitored IP address does not respond, the system will send an e-mail to notify the administrator that such destination is not reachable. After entering the related information, click **Apply** and these settings will become effective immediately. Click **Monitor** to check the current status of all the monitored IP. The system provides 40 IP addresses for the “**Monitor IP List**”.

Admin Email	
Send To	<input type="text"/> *separate email addresses with a comma
Subject	Monitor Result *The host name and detection time will be appended to subject automatically.
Email Body	<input type="text"/> *The host name, remark, and detection time information will be appended to email body automatically.
Send From	<input type="text"/>
SMTP Server	<input type="text"/> Port: <input type="text"/>
Auth Method	NONE <input type="button" value="v"/>
Send Test Email	<input type="button" value="Send"/>

Settings	
Enable Monitor IP List	<input checked="" type="checkbox"/>
Interval	1 Minute <input type="button" value="v"/>
Probe Retry	Retry if no response: <input type="text" value="3"/> (Range: 1 ~ 10)

Monitor IP List		
Item	IP/Host Name	Remark
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>

- **Send From:** The e-mail address of the administrator in charge of the monitoring. This will show up as the sender's e-mail.
- **Send To:** The e-mail address of the person whom the monitoring result is for. This will be the receiver's e-mail.
- **Interval:** The time interval to send the e-mail report.
- **SMTP Server:** The IP address of the SMTP server.
- **Auth Method:** The system provides four authentication methods, **Plain**, **Login**, **CRAM-MD5** and **NTLMv1**, or “None” to use none of the above. Depending on which authentication method selected, enter the **Account Name**, **Password** and **Domain**.
- **Send Test Email:** To test the settings correct or not.
- **Monitor IP Address:** The IP addresses under monitoring.

Monitor IP result		
No	IP Address	Result
1	192.168.1.200	
2	192.168.1.100	

### 4.3.4 Walled Garden List

This function provides some free services to the users to access websites listed here before login and authentication. Up to 20 addresses or domain names of the websites can be defined in this list. Users without the network access right can still have a chance to experience the actual network service free of charge. Please enter the website **IP Address** or **Domain Name** in the list and these settings will become effective immediately after clicking **Apply**.

Walled Garden List			
Item	IP/Host Name	Item	IP/Host Name
1	<input type="text"/>	2	<input type="text"/>
3	<input type="text"/>	4	<input type="text"/>
5	<input type="text"/>	6	<input type="text"/>
7	<input type="text"/>	8	<input type="text"/>
9	<input type="text"/>	10	<input type="text"/>
11	<input type="text"/>	12	<input type="text"/>
13	<input type="text"/>	14	<input type="text"/>
15	<input type="text"/>	16	<input type="text"/>
17	<input type="text"/>	18	<input type="text"/>
19	<input type="text"/>	20	<input type="text"/>

 **Apply**

 **Clear**

### 4.3.5 Proxy Server Properties

AirLive WIAS-1200G supports Internal Proxy Server and External Proxy Server functions. Please select an **Access Gateway** and then perform the necessary configurations.

External Proxy Server		
Item	Server IP	Port
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>

Internal Proxy Server	
Built-in Proxy Server	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

- External Proxy Server:** Under the AirLive WIAS-1200G security management, the system will match the External Proxy Server list to the end-users' proxy setting. If there isn't a match, then the end-users will not be able to reach the login page and thus unable to access the network. If there is a match, the end-users will be directed to the system first for authentication. After a successful authentication, the end-users will be redirected back to the desired proxy servers depending on various situations.
- Internal Proxy Server:** AirLive WIAS-1200G has a built-in proxy server. If this function is enabled, the end users will be forced to treat AirLive WIAS-1200G as the proxy server regardless of the end-users' original proxy settings.

**Note:** For more details about how to set up the proxy servers, please refer to Appendix E and Appendix F.



## 4.3.6 Dynamic DNS

AirLive WIAS-1200G provides a convenient DNS function to translate the IP address of WAN port to a domain name that helps the administrator memorize and connect to WAN port. If the DHCP is activated at WAN port, this function will also update the newest IP address regularly to the DNS server. These settings will become effective immediately after clicking **Apply**.

Dynamic DNS	
DDNS	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Provider	<input type="text" value="DynDNS.org(Dynamic)"/>
Host name	<input type="text" value="DynDNS.org(Dynamic)"/>
Username/E-mail	<input type="text" value="dhs.org"/>
Password/Key	<input type="text" value="no-ip.com"/>

- **DDNS:** Enabling or disabling of this function.
- **Provider:** Select the DNS provider.
- **Host name:** The IP address/domain name of the WAN port.
- **Username/E-mail:** The register ID (username or e-mail) for the DNS provider.
- **Password/Key:** The register password for the DNS provider.

## 4.4 Utilities

This section provides four utilities to customize and maintain the system including **Change Password**, **Backup/Restore Setting**, **Firmware Upgrade** and **Restart**.

Utilities	
<b>Network Utilities</b>	System provides network diagnostic tools like PING, Trace Route, and Show ARP Table.
<b>Change Password</b>	Change the administration passwords for accounts of admin, manager and operator.
<b>Backup/Restore Settings</b>	Backup and restore system settings. Administrator may also reset system settings to factory default.
<b>Firmware Upgrade</b>	Update WIAS-1200G firmware.
<b>Restart</b>	Restart the system.

## 4.4.1 Network Utilities

The system provides three network diagnostic tools like **PING**, **Trace Route**, and **ARP Table**, for the administrator to diagnose the network status.

Network Utilities	
PING	<input type="text"/> <input type="button" value="PING"/>
Trace Route	<input type="text"/> <input type="button" value="Start"/> <input type="button" value="Stop"/>
ARP Table	<input type="button" value="Show"/>
Status	

- **PING:** Enter the desired IP address such as “10.30.1.254” and click **PING** button to execute PING. The ping result will be shown on the screen. Click **Back** button to go back to the Network Utilities page.

```
PING 10.30.1.254 (10.30.1.254): 56 octets data
64 octets from 10.30.1.254: icmp_seq=0 ttl=64 time=1.8 ms
64 octets from 10.30.1.254: icmp_seq=1 ttl=64 time=1.2 ms
64 octets from 10.30.1.254: icmp_seq=2 ttl=64 time=1.4 ms
64 octets from 10.30.1.254: icmp_seq=3 ttl=64 time=1.3 ms

--- 10.30.1.254 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 1.2/1.4/1.8 ms
```

- **Trace Route:** Enter the desired IP address such as “10.30.1.254” and click **Start** button. The Trace Route result will be shown on the screen. Click **Back** button to go back to the Network Utilities page.

```
traceroute to 10.30.1.254 (10.30.1.254), 20 hops max, 40 byte packets
 1 gw.private (10.30.1.254)  2.125 ms  1.925 ms
```

- **ART Table:** Click **Show** button to get the ART table of the system. The ART Table result will be shown on the screen. Click **Back** button to go back to the Network Utilities page.

Address	HWtype	HWaddress	Flags	Mask	Iface
10.30.1.254	ether	00:11:A3:02:69:42	C		eth2

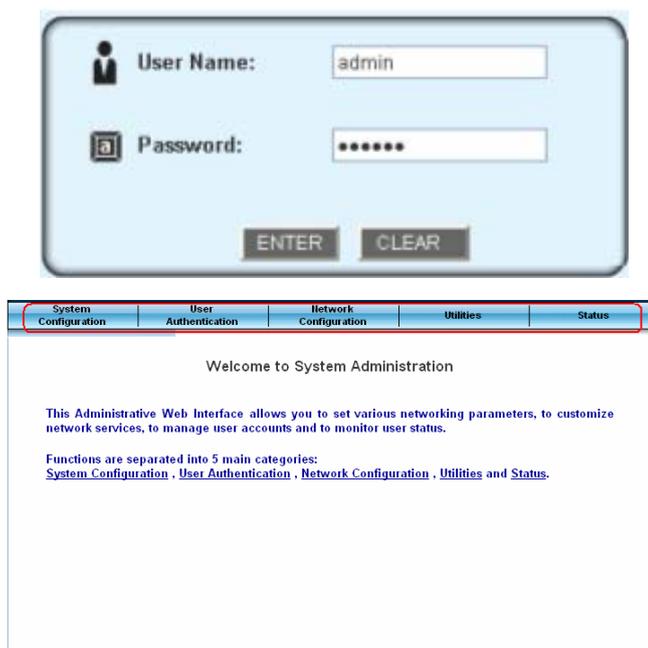
## 4.4.2 Change Password

There are three levels of authorities to use: **admin**, **manager** or **operator**. The default usernames and passwords are as follow:

**Admin:** The administrator can access all configuration pages of the AirLive WIAS-1200G.

User Name: **admin**

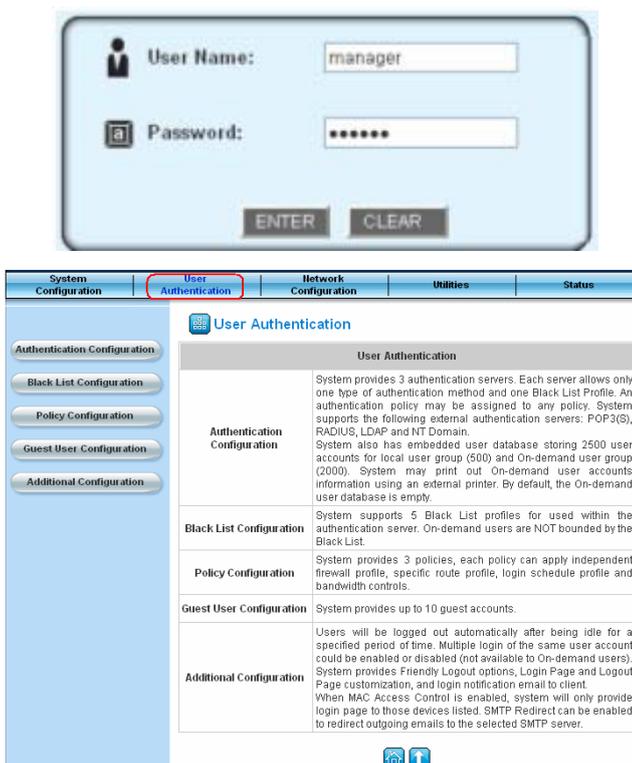
Password: **airlive**



**Manager:** The manager can only access the configuration pages under **User Authentication** to manage the user accounts, but has no permission to change the settings of the profiles for Firewall, Specific Route and Schedule.

User Name: **manager**

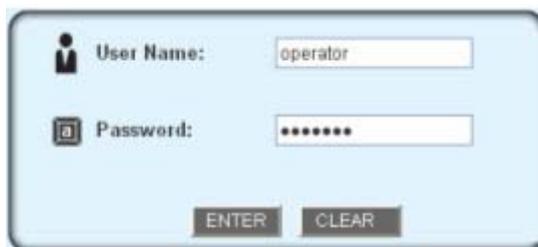
Password: **airlive**



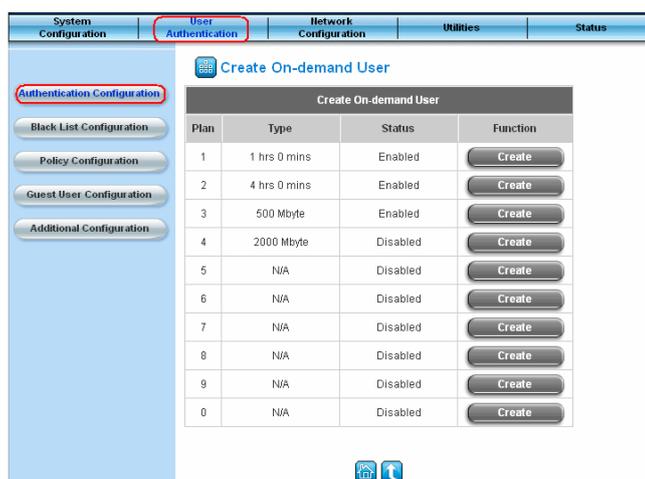
**Operator:** The operator can only access the configuration page of **Create On-demand User** to create and print out the new on-demand user accounts.

User Name: **operator**

Password: **airlive**



A light blue rounded rectangular form containing two input fields. The first field is labeled 'User Name:' and contains the text 'operator'. The second field is labeled 'Password:' and contains seven asterisks. Below the fields are two buttons: 'ENTER' and 'CLEAR'.



The screenshot shows a web interface with a top navigation bar containing 'System Configuration', 'User Authentication', 'Network Configuration', 'Utilities', and 'Status'. The 'User Authentication' tab is selected. On the left, there is a sidebar with 'Authentication Configuration' selected, and other options like 'Black List Configuration', 'Policy Configuration', 'Guest User Configuration', and 'Additional Configuration'. The main content area is titled 'Create On-demand User' and contains a table with columns 'Plan', 'Type', 'Status', and 'Function'. Each row in the table has a 'Create' button in the 'Function' column.

Plan	Type	Status	Function
1	1 hrs 0 mins	Enabled	Create
2	4 hrs 0 mins	Enabled	Create
3	500 Mbyte	Enabled	Create
4	2000 Mbyte	Disabled	Create
5	N/A	Disabled	Create
6	N/A	Disabled	Create
7	N/A	Disabled	Create
8	N/A	Disabled	Create
9	N/A	Disabled	Create
0	N/A	Disabled	Create

The administrator can change the passwords here. Please enter the current password and then enter the new password twice to verify. Click **Apply** to activate this new password.

Change Admin Password	
Old Password	<input type="text"/>
New Password	<input type="text"/>
Verify Password	<input type="text"/>

Change Manager Password	
New Password	<input type="text"/>
Verify Password	<input type="text"/>

Change Operator Password	
New Password	<input type="text"/>
Verify Password	<input type="text"/>

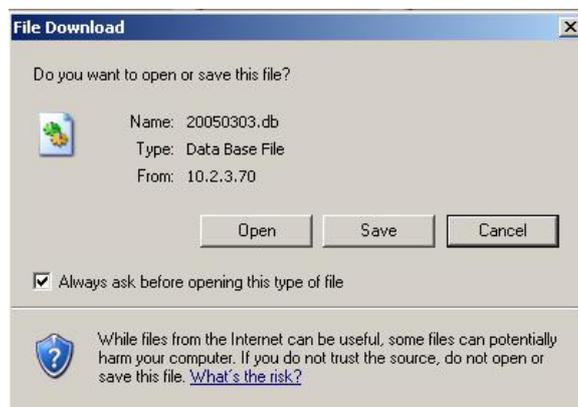
**Note:** If the administrator's password is lost, the administrator's password still can be changed through the text mode management interface on the serial console port.

### 4.4.3 Backup/Restore Setting

This function is used to backup/restore the AirLive WIAS-1200G settings. Also, AirLive WIAS-1200G can be restored to the factory default settings here.

[Backup current system settings]	
<b>Backup</b>	
[Restore system settings]	
File Name	<input type="text"/> <input type="button" value="Browse..."/>
<input type="button" value="Restore"/>	
[Reset to the factory-default settings]	
<b>Reset</b>	

- **Backup Current System Setting:** Click **Backup** to create a .db database backup file and save it on disk.



- **Restore System Setting:** Click **Browse** to search for a .db database backup file created by AirLive WIAS-1200G and click **Restore** to restore to the same settings at the time the backup file was created.
- **Resetting to the Factory-Default configuration:** Click **Reset** to load the factory default settings of AirLive WIAS-1200G.

## 4.4.4 Firmware Upgrade

The administrator can download the latest firmware from website and upgrade the system here. Click **Browse** to search for the firmware file and click **Apply** to go on with the firmware upgrade process. It might be a few minutes before the upgrade process completes and the system needs to be restarted afterwards to make the new firmware effective.

**Note:** For maintenance issues, we strongly recommend you backup system settings before upgrading firmware.

Firmware Upgrade	
Current Version	1.10.00-EN-E
File Name	<input type="text"/> <input type="button" value="Browse..."/>

**Note:**

1. Firmware upgrade may cause the loss of some of the data. Please refer to the release notes for the limitation before upgrading the firmware.
2. Please restart the system after upgrading the firmware. Do not power on/off the system during the upgrade or the restart process. It may damage the system and cause it to malfunction.

## 4.4.5 Restart

This function allows the administrator to safely restart AirLive WIAS-1200G and the process should take about three minutes. Click **YES** to restart AirLive WIAS-1200G; click **NO** to go back to the previous screen. If the power needs to be turned off, restarting AirLive WIAS-1200G first and then turning off the power after completing the restart process is highly recommended.

Do you want to **Restart** WIAS-1200G?

**Note:** The connection of all online users of the system will be disconnected when system is in the process of restarting.



## 4.5 Status

This section includes **System Status**, **Interface Status**, **Current Users**, **Traffic History**, and **Notification Configuration** to provide system status information and online user status.

Status	
<b>System Status</b>	Display current system settings.
<b>Interface Status</b>	Display WAN, LAN1 & LAN2, LAN3 & LAN4 and Wireless LAN configurations and status.
<b>Current Users</b>	Display online user information including: Username, IP, MAC, packet count, byte count and idle time. Administrator may also kick out any online user from here.
<b>Traffic History</b>	Display detail usage information by day. A minimum of 3 days of history can be logged in the system volatile memory.
<b>Notify Configuration</b>	Historical usage log can be sent automatically to a specific e-mail address defined here. <a href="#">External syslog server can be configured here.</a>

## 4.5.1 System Status

This section provides an overview of the system for the administrator.

System Status		
Current Firmware Version	1.00.00-EN-E	
Build	00600	
System Name	AirLive WIAS-1200G	
Admin info	Sorry! The service is temporarily unavailable.	
Home Page	<a href="http://www.airlive.com/">http://www.airlive.com/</a>	
Syslog server-Traffic History	N/A:N/A	
Syslog server-On demand User log	N/A:N/A	
Proxy Server	Disabled	
Friendly Logout	Enabled	
Internet Connection Detection	Disabled	
Management	Remote Management IP	Disabled
	SNMP	Disabled
History	Retained Days	3 days
	Traffic log Email To	N/A
	On-demand log Email To	N/A
Time	NTP Server	(tock.usno.navy.mil)
	Date Time	2007/06/08 06:57:33 +0800
User	Idle Timer	10 Min(s)
	Multiple Login	Disabled
	Guest Account	Disabled
DNS	Preferred DNS Server	168.95.1.1
	Alternate DNS Server	N/A

The description of the table is as follows:

<b><u>Item</u></b>	<b><u>Description</u></b>
<b>Current Firmware Version</b>	The present firmware version of AirLive WIAS-1200G
<b>System Name</b>	The system name. The default is AirLive WIAS-1200G
<b>Admin Info</b>	The information to be shown on the login screen when a user has a connection problem.
<b>Home Page</b>	The page the users are directed to after initial login success.
<b>Syslog server-Traffic History</b>	The IP address and port number of the external Syslog Server. <b>N/A</b> means that it is not configured.

<b>Syslog server-On demand User log</b>		The IP address and port number of the external Syslog Server. <b>N/A</b> means that it is not configured.
<b>Proxy Server</b>		Enabled/disabled stands for that the system is currently using the proxy server or not.
<b>Friendly Logout</b>		Enabled/disabled stands for the setting of hiding/displaying an extra confirmation window when users click the logout button.
<b>Internet Connection Detection</b>		Enabled/Disabled stands for the connection at WAN is normal or abnormal ( <b>Internet Connection Detection</b> ) and all online users are allowed/disallowed to log in the network.
<b>Management</b>	<b>Remote Management IP</b>	The IP or IPs that is allowed for accessing the management interface.
	<b>SNMP</b>	Enabled/disabled stands for the current status of the SNMP management function.
<b>History</b>	<b>Retained Days</b>	The maximum number of days for the system to retain the users' information.
	<b>Traffic log Email To</b>	The email address that the traffic history information will be sent to.
	<b>On-demand log Email To</b>	The email address the history information about on-demand users is sent to.
<b>Time</b>	<b>NTP Server</b>	The network time server that the system is set to align.
	<b>Date Time(GMT+0:00)</b>	The system time is shown as the local time.
<b>User</b>	<b>Idle Timer</b>	The number of minutes allowed for the users to be inactive.
	<b>Multiple Login</b>	Enabled/disabled stands for the current setting to allow/disallow multiple logins form the same account.
	<b>Guest Account</b>	Enabled/disabled stands for the current status of allowing Guest Accounts to log in.
<b>DNS</b>	<b>Preferred DNS Server</b>	IP address of the preferred DNS Server.
	<b>Alternate DNS Server</b>	IP address of the alternate DNS Server.

## 4.5.2 Interface Status

This section provides an overview of the interface for the administrator including **WAN**, **LAN1 & LAN2**, **LAN3 & LAN4**, and **Wireless Port**.

Interface Status		
WAN	MAC Address	00:12:00:00:01:01
	IP Address	169.254.1.1
	Subnet Mask	255.255.255.255
Wireless	Operation Mode	NAT
	MAC Address	00:1A:4D:26:E3:00
	IP Address	192.168.3.254
	Subnet Mask	255.255.255.0
	SSID	airlive
	Channel	1
	Encryption Function	Disabled
Wireless DHCP Server	Status	Enabled
	WINS IP Address	N/A
	Start IP Address	192.168.3.1
	End IP Address	192.168.3.100
	Lease Time	1440 Min(s)
LAN1 & LAN2	Mode	NAT
	MAC Address	00:12:00:00:01:02
	IP Address	192.168.1.254
	Subnet Mask	255.255.255.0
LAN1 & LAN2 DHCP Server	Status	Enabled
	WINS IP Address	N/A
	Start IP Address	192.168.1.1
	End IP Address	192.168.1.100
	Lease Time	1440 Min(s)
LAN3 & LAN4	Mode	NAT
	MAC Address	00:12:00:00:01:02
	IP Address	192.168.2.254
	Subnet Mask	255.255.255.0
LAN3 & LAN4 DHCP Server	Status	Enabled
	WINS IP Address	N/A
	Start IP Address	192.168.2.1
	End IP Address	192.168.2.100
	Lease Time	1440 Min(s)

The description of the table is as follows.

<b><u>Item</u></b>		<b><u>Description</u></b>
<b>WAN</b>	<b>MAC Address</b>	The MAC address of the WAN port.
	<b>IP Address</b>	The IP address of the WAN port.
	<b>Subnet Mask</b>	The Subnet Mask of the WAN port.
<b>Wireless</b>	<b>Operation Mode</b>	The mode of the wireless port.
	<b>MAC Address</b>	The MAC address of the wireless port.
	<b>IP Address</b>	The IP address of the wireless port.
	<b>Subnet Mask</b>	The Subnet Mask of the wireless port.
	<b>SSID</b>	The ESSID of the wireless port, such as AirLive WIAS-1200G.
	<b>Channel</b>	The assigned Channel of the Wireless port.
<b>Wireless DHCP Server</b>	<b>Encryption Function</b>	Enabled/disabled stands for the status of the encryption function of the wireless port.
	<b>Status</b>	Enable/disable stands for status of the DHCP server on the Wireless port.
	<b>WINS IP Address</b>	The WINS server IP on DHCP server. <b>N/A</b> means that it is not configured.
	<b>Start IP Address</b>	The start IP address of the DHCP IP range.
	<b>End IP address</b>	The end IP address of the DHCP IP range.
<b>LAN1 &amp; LAN2</b>	<b>Lease Time</b>	Minutes of the lease time of the IP address.
	<b>Mode</b>	The mode of the LAN1 & LAN2 port.
	<b>MAC Address</b>	The MAC address of the LAN1 & LAN2.
	<b>IP Address</b>	The IP address of the LAN1 & LAN2.
<b>LAN1 &amp; LAN2 DHCP Server</b>	<b>Subnet Mask</b>	The Subnet Mask of the LAN1 & LAN2.
	<b>Status</b>	Enable/disable stands for status of the DHCP server on the LAN1 & LAN2.
	<b>WINS IP Address</b>	The WINS server IP on DHCP server. <b>N/A</b> means that it is not configured.
	<b>Start IP Address</b>	The start IP address of the DHCP IP range.
	<b>End IP address</b>	The end IP address of the DHCP IP range.
<b>LAN3 &amp; LAN4</b>	<b>Lease Time</b>	Minutes of the lease time of the IP address.
	<b>Mode</b>	The mode of the LAN3 & LAN4.
<b>LAN3 &amp; LAN4</b>	<b>MAC Address</b>	The MAC address of the LAN3 & LAN4.

	<b>IP Address</b>	The IP address of the LAN3 & LAN4.
	<b>Subnet Mask</b>	The Subnet Mask of the LAN3 & LAN4.
<b>LAN3 &amp; LAN4 DHCP Server</b>	<b>Status</b>	Enable/disable stands for status of the DHCP server on the LAN3 & LAN4 port
	<b>WINS IP Address</b>	The WINS server IP on DHCP server. <b>N/A</b> means that it is not configured.
	<b>Start IP Address</b>	The start IP address of the DHCP IP range.
	<b>End IP address</b>	The end IP Address of the DHCP IP range.
	<b>Lease Time</b>	Minutes of the lease time of the IP address.

### 4.5.3 Current Users

In this function, each online user's information including **Username, IP Address, MAC Address, Packets In, Bytes In, Packets Out, Bytes Out, Idle Time** and **Logout** can be obtained. Administrator can use this function to force a specific online user to log out. Click the hyperlink of **Logout** next to the online user's name to logout that particular user. Click **Refresh** to renew the current users list.

Current Users List						
Item	Username		Pkts In	Bytes In	Idle	Kick Out
	IP	MAC	Pkts Out	Bytes Out		
1		guest4	12	10C8	454	<a href="#">Logout</a>
	192.168.1.107	00:D0:C9:60:01:04	12	10C8		
2		guest5	15	12E0	454	<a href="#">Logout</a>
	192.168.1.100	00:D0:C9:60:01:05	15	12E0		
3		guest6	25	21C0	64	<a href="#">Logout</a>
	192.168.1.131	00:D0:C9:60:01:06	25	21C0		
4		guest7	25	21C0	64	<a href="#">Logout</a>
	192.168.1.165	00:D0:C9:60:01:07	25	21C0		



## 4.5.4 Traffic History

This function is used to check the history of AirLive WIAS-1200G. The history of each day will be saved separately in the DRAM for at least 3 days.

Traffic History	
Date	Size (Byte)
<a href="#">2007-03-27</a>	65
<a href="#">2007-03-28</a>	65

On-demand User Log	
Date	Size (Byte)
<a href="#">2007-03-27</a>	105
<a href="#">2007-03-28</a>	504

**Note:** Since the history is saved in the SDRAM, if you need to restart the system and also keep the history, then please manually copy and save the information before restarting.

If the **History Email** has been entered under the **Notify Configuration** page, then the system will automatically send out the history information to that email address.

- **Traffic History**

As shown in the following figure, each line is a traffic history record consisting of 9 fields, **Date**, **Type**, **Name**, **IP**, **MAC**, **Pkts In**, **Bytes In**, **Pkts Out**, and **Bytes Out**, of user activities.

Traffic History 2005-03-22									
Date	Type	Name	IP	MAC	Pkts In	Bytes In	Pkts Out	Bytes Out	
2005-03-22 19:12:21 +0800	LOGIN	user1@local.tw	192.168.1.143	00:D0:C9:42:37:20	0	0	0	0	
2005-03-22 19:12:24 +0800	LOGOUT	user1@local.tw	192.168.1.143	00:D0:C9:42:37:20	3	252	3	252	
2005-03-22 19:12:29 +0800	LOGIN	user2@local.tw	192.168.1.143	00:D0:C9:42:37:20	0	0	0	0	
2005-03-22 19:12:32 +0800	LOGOUT	user2@local.tw	192.168.1.143	00:D0:C9:42:37:20	3	252	3	252	
2005-03-22 19:13:51 +0800	LOGIN	user1@local.tw	192.168.1.1	00:D0:C9:60:01:01	0	0	0	0	

- **On-demand User Log**

As shown in the following figure, each line is an on-demand user log record consisting of 13 fields, **Date**, **System Name**, **Type**, **Name**, **IP**, **MAC**, **Pkts In**, **Bytes In**, **Pkts Out**, **Bytes Out**, **Expiretime**, **Validtime** and **Remark**, of user activities.

On-demand User Log 2005-03-22												
Date	System Name	Type	Name	IP	MAC	Pkts In	Bytes In	Pkts Out	Bytes Out	Expiretime	Validtime	Remark
2005-03-22 17:55:58 +0800	My Service	Create_OD_User	P4SP	0.0.0.0	00:00:00:00:00:00	0	0	0	0	2005-03-25 17:55:58	None	2 hrs 0 mins
2005-03-22 17:56:03 +0800	My Service	Create_OD_User	62H6	0.0.0.0	00:00:00:00:00:00	0	0	0	0	2005-03-25 17:56:03	None	2 hrs 0 mins
2005-03-22 17:56:07 +0800	My Service	Create_OD_User	886D	0.0.0.0	00:00:00:00:00:00	0	0	0	0	2005-03-25 17:56:07	None	2 hrs 0 mins

## 4.5.5 Notify Configuration

The AirLive WIAS-1200G will save the traffic history into the internal DRAM. If the administrator wants the system to automatically send out the history to a particular email address, please enter the related information in these fields.

Notify Configuration	
Traffic History Email	Send From: <input type="text"/>
	Send To: <input type="text"/>
	Interval: <input type="text" value="1 Hour"/> <input type="button" value="v"/>
	SMTP Server: <input type="text"/>
	SMTP Server Port: <input type="text" value="25"/>
	Auth Method: <input type="text" value="NONE"/> <input type="button" value="v"/>
	Send Test Email <input type="button" value="Send"/>
Syslog Server	IP: <input type="text"/> Port: <input type="text"/>
	Facility: <input type="text" value="local0"/> <input type="button" value="v"/> Severity: <input type="text" value="Emergency"/> <input type="button" value="v"/>
	Tag: <input type="text"/>
Notify Configuration	
On-demand User Log History Email	Send From: <input type="text"/>
	Send To: <input type="text"/>
	Interval: <input type="text" value="1 Hour"/> <input type="button" value="v"/>
	SMTP Server: <input type="text"/>
	SMTP Server Port: <input type="text" value="25"/>
	Auth Method: <input type="text" value="NONE"/> <input type="button" value="v"/>
	Send Test Email <input type="button" value="Send"/>
Syslog Server	IP: <input type="text"/> Port: <input type="text"/>
	Facility: <input type="text" value="local0"/> <input type="button" value="v"/> Severity: <input type="text" value="Emergency"/> <input type="button" value="v"/>
	Tag: <input type="text"/>

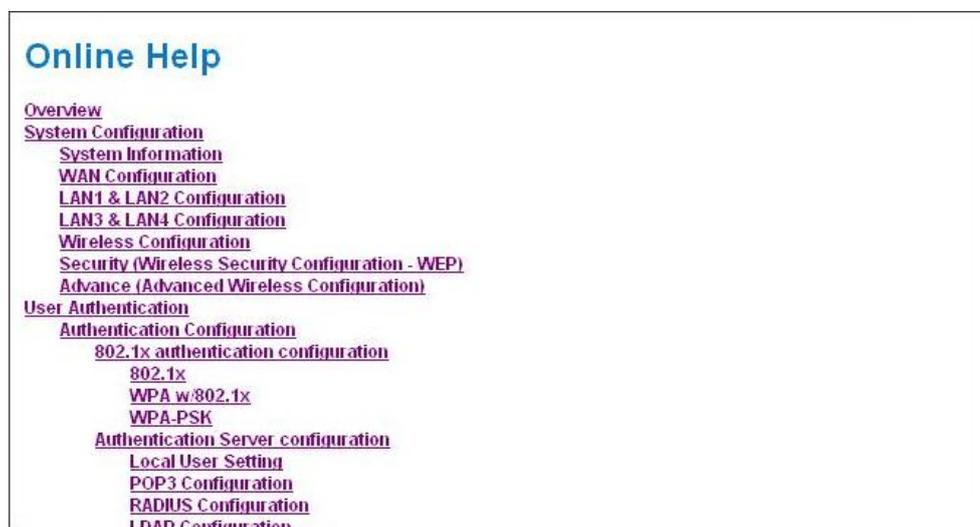
- **Send From:** The e-mail address of the administrator in charge of the monitoring. This will show up as the sender's e-mail.
- **Send To:** The e-mail address of the person whom the history email is for. This will be the receiver's e-mail.
- **Interval:** The time interval to send the e-mail report.
- **SMTP Server:** The IP address of the SMTP server.
- **Auth Method:** The system provides four authentication methods, **Plain**, **Login**, **CRAM-MD5** and **NTLMv1**, or "None" to use none of the above. Depending on which authentication method you select, you have to enter the **Account Name**, **Password** and **Domain**.  
**NTLMv1** is not currently available for general use.  
**Plain** and **CRAM-MD5** are standardized authentication mechanisms while **Login** and **NTLMv1** are Microsoft proprietary mechanisms. Only **Plain** and **Login** can use the UNIX login password. Netscape uses **Plain**. Outlook and Outlook express uses **Login** as default, although they can be set to use **NTLMv1**. Pegasus uses **CRAM-MD5** or **Login** but you are not able to configure which method to use.
- **Send Test Email:** To test the settings correct or not.
- **Syslog Server:** It specifies the IP and Port of the Syslog server.



## 4.6 Help

On the screen, the **Help** button is on the upper right corner.

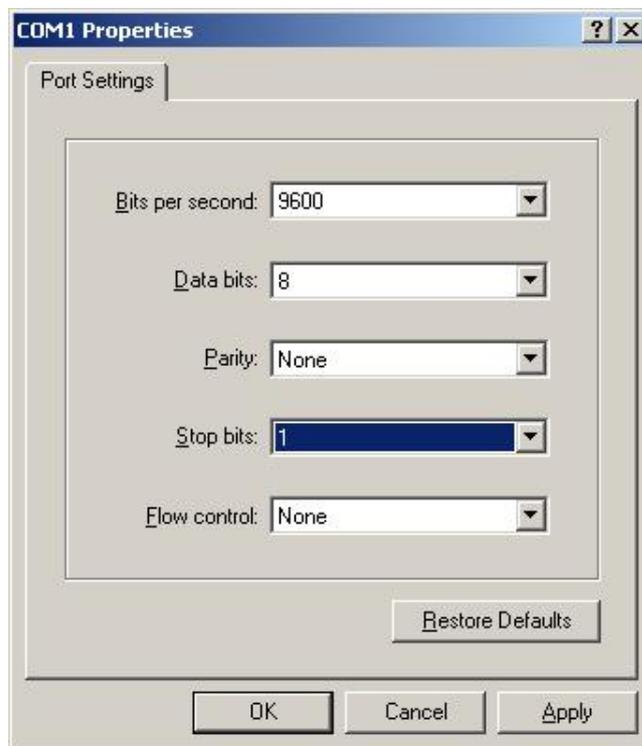
Click **Help** to the **Online Help** window and then click the hyperlink of the items to get the information.



## Appendix A – Console Interface

Via this port to enter the console interface for the administrator to handle the problems and situations occurred during operation.

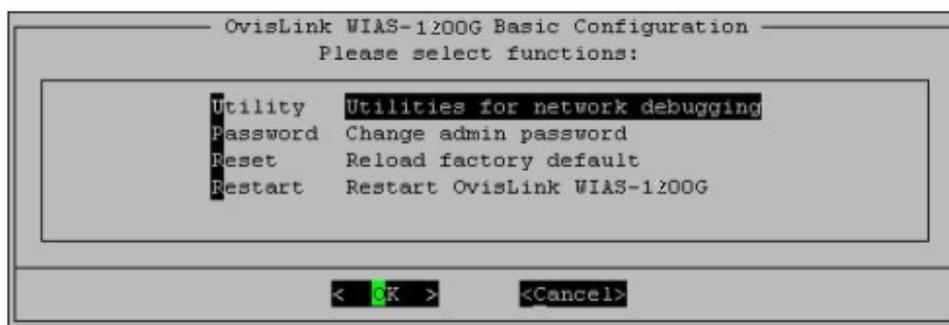
1. In order to connect to the console port of AirLive WIAS-1200G, a console, modem cable and a terminal simulation program, such as the Hyper Terminal are needed.
2. If a Hyper Terminal is used, please set the parameters as **9600,8,n,1**.



**Note:**

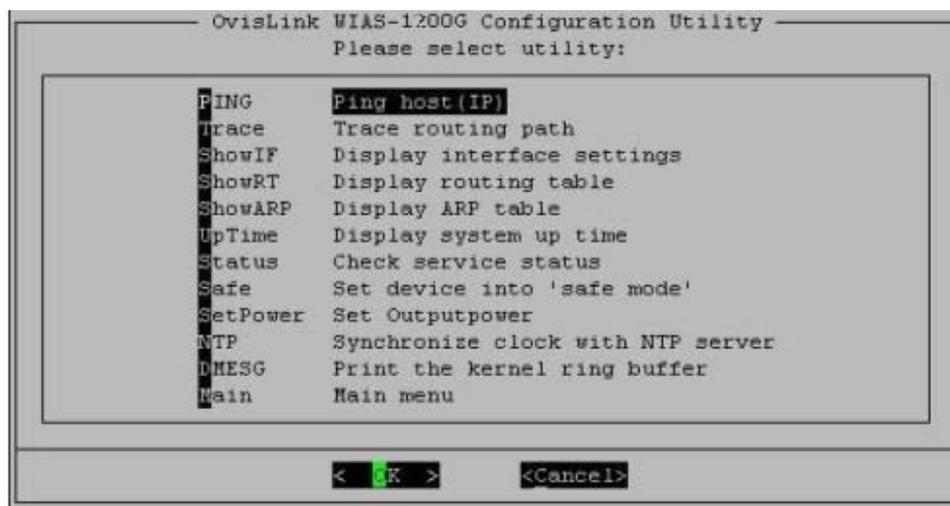
The main console is a menu-driven text interface with dialog boxes. Please use arrow keys on the keyboard to browse the menu and press the **Enter** key to make selection or confirm what you enter.

3. Once the console port of AirLive WIAS-1200G is connected properly, the console main screen will appear automatically. If the screen does not appear in the terminal simulation program automatically, please try to press the arrow keys, so that the terminal simulation program will send some messages to the system and the welcome screen or the main menu should appear. If you are still unable to see the welcome screen or the main menu of the console, please check the connection of the cables and the settings of the terminal simulation program.



- **Utilities for network debugging**

The console interface provides several utilities to assist the Administrator to check the system conditions and to debug any problems. The utilities are described as follow:



- Ping host (IP): By sending ICMP echo request to a specified host and wait for the response to test the network status.
- Trace routing path: Trace and inquire the routing path to a specific target.
- Display interface settings: It displays the information of each network interface setting including the MAC address, IP address, and netmask.
- Display the routing table: The internal routing table of the system is displayed, which may help to confirm the Static Route settings.
- Display ARP table: The internal ARP table of the system is displayed.
- Display system up time: The system live time (time for system being turn on) is displayed.
- Check service status: Check and display the status of the system.
- Set device into “safe mode”: If administrator is unable to use Web Management Interface via the browser for the system failed inexplicitly. Administrator can choose this utility and set IT into safe mode, then administrator can management this device with browser again.
- Synchronize clock with NTP server: Immediately synchronize the clock through the NTP protocol and the specified network time server. Since this interface does not support manual setup for its internal clock, therefore we must reset the internal clock through the NTP.
- Print the kernel ring buffer: It is used to examine or control the kernel ring buffer. The program helps users to print out their boot-up messages instead of copying the messages by hand.
- Main menu: Go back to the main menu.

- **Change admin password**

Besides supporting the use of console management interface through the connection of null modem, the system also supports the SSH online connection for the setup. When using a null modem to connect to the system console, we do not need to enter administrator's password to enter the console management interface. But connecting the system by SSH, we have to enter the username and password.

The username is "admin" and the default password is also "admin", which is the same as for the web management interface. You can use this option to change the administrator's password. Even if you forgot the password and are unable to log in the management interface from the web or the remote end of the SSH, you can still use the null modem to connect the console management interface and set the administrator's password again.

**Note:**

*Although it does not require a username and password for the connection via the serial port, the same management interface can be accessed via SSH. Therefore, we recommend you to immediately change the AirLive WIAS-1200G Admin username and password after logging in the system for the first time.*

- **Reload factory default**

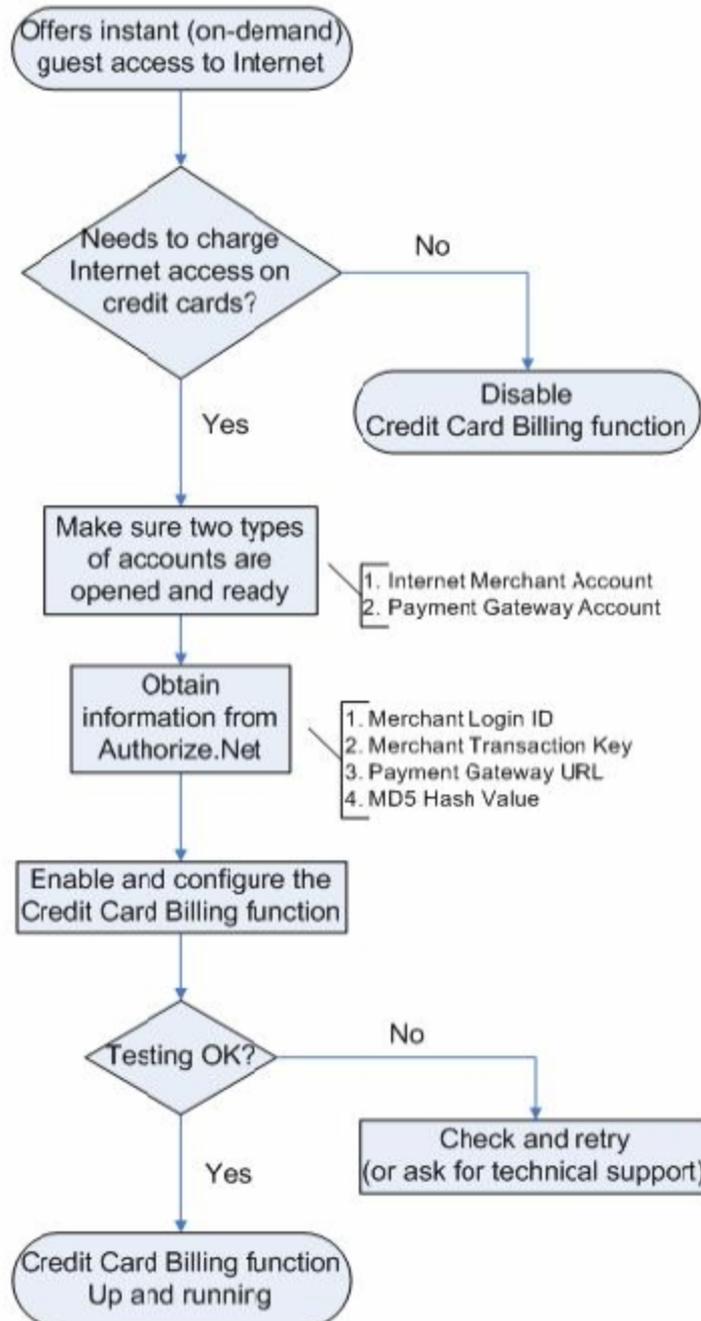
Choosing this option will reset the system configuration to the factory defaults.

- **Restart AirLive WIAS-1200G**

Choosing this option will restart AirLive WIAS-1200G.

## Appendix B – Accepting Payments via Authorize.Net

This section is to show independent Hotspot owners how to configure related settings in order to accept credit card payments via Authorize.Net, making the Hotspot an e-commerce environment for end users to pay for and obtain Internet access using their credit cards.



## 1. Setting Up

### 1.1 Open Accounts

To set up AirLive WIAS-1200G to process credit card billing, the merchant owner will need two accounts (Internet Merchant account and Authorize.Net account).

If you are looking for a merchant account or Internet payment gateway to process transactions, you can fill out the Inquiry Form on <http://www.authorize.net/solutions/merchantsolutions/merchantinquiryform/>.

### 1.2 Configure AirLive WIAS-1200G using an Authorize.Net account

Please log in AirLive WIAS-1200G. **User Authentication** → **Authentication Configuration** → Click the server **On-demand User** → **On-demand User Server Configuration** → Click **Payment** → **Payment Configuration** → **External Payment Gateway** → Select **Authorize.Net**

Some major fields are required:

Setting	Description
<b>Merchant Login ID</b>	This is the "Login ID" that comes with the Authorize.Net account.
<b>Merchant Transaction Key</b>	To get a new key, please log in Authorize.Net → Click <b>Settings and Profile</b> → Go to the " <b>Security</b> " section → Click <b>Obtain Transaction Key</b> → Enter " <b>Secret Answer</b> " → Click <b>Submit</b> .
<b>Payment Gateway URL</b>	<a href="https://secure.authorize.net/gateway/transact.dll">https://secure.authorize.net/gateway/transact.dll</a> (default payment gateway)
<b>MD5 Hash</b>	To enhance the transaction security, merchant owner can choose to enable this function and enter a value in the text box: " <b>MD5 Hash Value</b> ".

**Note:**

**For detailed description, please see 4.2.1.6 Authentication Method – On-demand User → Payment**

### 1.3 Configure the Authorize.Net Merchant Account to Match the Configuration of AirLive WIAS-1200G

Settings of the merchant account on Authorize.Net should be matched with the configuration of AirLive WIAS-1200G:

Setting	Description
<b>MD5 Hash</b>	To configure " <b>MD5 Hash Value</b> ", please log in Authorize.Net → Click <b>Settings and Profile</b> → Go to the " <b>Security</b> " section → click <b>MD5 Hash</b> → Enter " <b>New Hash Value</b> " & " <b>Confirm Hash Value</b> " → Click <b>Submit</b> .
<b>Required Card Code</b>	If the " <b>Card Code</b> " is set up as a required field, please log in Authorize.Net → Click <b>Settings and Profile</b> → Go to the " <b>Security</b> " section → click <b>Card Code Verification</b> → Check the <b>Does NOT Match (N)</b> box → Click <b>Submit</b> .
<b>Required Address Fields</b>	After setting up the required address fields on the " <b>Credit Card Payment Page Billing Configuration</b> " section of AirLive WIAS-1200G, the same requirements must be set on Authorize.Net. To do so, please log in Authorize.Net → Click <b>Settings and Profile</b> → Go to the " <b>Security</b> " section → click <b>Address Verification System (AVS)</b> → Check the boxes accordingly → Click <b>Submit</b> .

### 1.4 Test The Credit Card Payment via Authorize.Net

To test the connection between AirLive WIAS-1200G and Authorize.Net, please log in AirLive WIAS-1200G. **User Authentication** → **Authentication Configuration** → Click the server **On-demand User** → **On-demand User Server Configuration** → **Payment** → **Payment Configuration** → Select **Authorize.Net** → Go to "**Authorize.Net Payment Page Configuration**" section → Enable the "**Test Mode**" → Click **Try Test** and follow the instructions

 **Payment Configuration**

**External Payment Gateway**

Authorize.Net     PayPal     Disable

**Authorize.Net Payment Page Configuration**

Merchant Login ID	<input type="text" value="yourloginid"/>	-
Merchant Transaction Key	<input type="text" value="yourtransactionkey"/>	-
Payment Gateway URL	<input type="text" value="https://secure.authorize.net/gateway/transact.dll"/>	-
Verify SSL Certificate	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Test Mode	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <input type="button" value="Try Test"/>	-
MD5 Hash	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	

## 2. Basic Maintenance

In order to maintain the operation, merchant owners will have to manage the accounts and transactions via Authorize.Net as well as AirLive WIAS-1200G.

### 2.1 Void A Transaction and Remove the On-demand Account Generate on AirLive WIAS-1200G

Sometimes, a transaction (as well as the related user account on AirLive WIAS-1200G) may have to be canceled before it has been settled with the bank.

- To void an unsettled transaction, please log in Authorize.Net. Click **Unsettled Transactions** → Locate the specific transaction record on the “**List of Unsettled Transactions**” → Click the **Trans ID** number → Confirm and click **Void**.

**Note:**

To find the on-demand account name, click **Show Itemized Order Information** in the “**Order Information**” section → Username can be found in the “**Item Description**”

- To remove the specific account from AirLive WIAS-1200G, please log in AirLive WIAS-1200G. **User Authentication** → **Authentication Configuration** → Click the server **On-demand User** → **On-demand User Server Configuration** → **Users List** → Click **Delete** on the record with the account name.
- Click **Delete All** to delete all users at once.

On-demand Users List					
Username	Password	Remaining Time/Volume	Status	Expiration Time	Delete All
<a href="#">V34Q</a>	KP23E64C	2 hour	Normal	2007/02/01-13:35:41	<input type="button" value="Delete"/>



## 2.2 Refund A Settled Transaction and Remove the On-demand Account Generated on AirLive WIAS-1200G

- a. To refund a credit card, please log in Authorize.Net. Click **Virtual Terminal** → Select a Payment Method → Click **Refund a Credit Card** → **Payment/Authorization Information** → Type information in at least three fields: **Card Number**, **Expiration Date**, and **Amount** → Confirm and click **Submit**.
- b. To remove the specific account from AirLive WIAS-1200G, please log in AirLive WIAS-1200G. **User Authentication** → **Authentication Configuration** → Click the server **On-demand User** → **On-demand User Server Configuration** → **Users List** → Click **Delete** on the record with the account name

## 2.3 Find the Username and Password for A Specific Customer

Please log in Authorize.Net. Click **Unsettled Transactions** → Try to locate the specific transaction record on the “**List of Unsettled Transactions**” → Click the **Trans ID** number → Click **Show Itemized Order Information** in the “**Order Information**” section → Username and Password can be found in the “**Item Description**”.

## 2.4 Send An Email Receipt to A Customer

If a valid email address is provided, AirLive WIAS-1200G will automatically send the customer an email receipt for each successful transaction via Authorize.Net. To change the information on the receipt for customer, please log in AirLive WIAS-1200G. **User Authentication** → **Authentication Configuration** → Click the server **On-demand User** → **On-demand User Server Configuration** → **Payment** → **Payment Configuration** → **External Payment Gateway** → Select **Authorize.NET** → Scroll down to **Client's Purchasing Record** section of the page → Type in information in the text boxes: “**Description and E-mail Header**” → Confirm and click **Apply**.

Client's Purchasing Record	
Invoice Number	Hotspot - 00000001 * <input type="checkbox"/> Reset
Description	Internet access *
E-mail Header	Enjoy Online! *

## 2.5 Send An Email Receipt for Each Transaction to the Merchant Owner

A copy of email receipt with payment details for each successful transaction will also be automatically sent to the merchant owner/administrator via Authorize.Net.

To configure the contact person who will receive a receipt for each transaction, please log in Authorize.Net. Click **Settings and Profile** → Go to the “**General**” section → click **Manage Contacts** → click **Add New Contact** to → Enter necessary contact information on this page → Check the “**Transaction Receipt**” box → Click **Submit**.

### 3. Reporting

During normal operation, the following steps will be necessary to generate transaction reports.

#### 3.1 Transaction Statistics by Credit Card Type during the Period

Please log in Authorize.Net. → Click **Reports** → Check “**Statistics by Settlement Date**” radio button → Select “**Transaction Type**”, “**Start Date**”, and “**End Date**” as the criteria → Click **Run Report**

#### 3.2 Transaction Statistics by Different Location

- a. To deploy more than one AirLive WIAS-1200G, the way to distinguish transactions from different locations is to make the invoice numbers different. To change the invoice setting, please log in AirLive WIAS-1200G. **User Authentication** → **Authentication Configuration** → Click the server **On-demand User** → **On-demand User Server Configuration** → **Payment** → **Payment Configuration** → **External Payment Gateway** → Scroll down to “**Client's Purchasing Record**” section of the page → Check the “**Reset**” box → A location-specific ID (for example, Hotspot-A) can be used as the first part of “**Invoice Number**” → Confirm and click **Apply**.

Client's Purchasing Record	
Invoice Number	Hotspot - 00000001 * <input type="checkbox"/> Reset
Description	Internet access *
E-mail Header	Enjoy Online! *

- b. Please log in Authorize.Net → Click **Search and Download** → Specify the transaction period (or ALL Settled, Unsettled) in “**Settlement Date**” section → Go to “**Transaction**” section → Enter the first part of invoice number plus an asterisk character (for example, Hotspot-A\*) in the “**Invoice #**” text box → Click **Search** → If transaction records can be found, the number of accounts sold is the number of search results → Or, click **Download To File** to download records and then use MS Excel to generate more detailed reports.

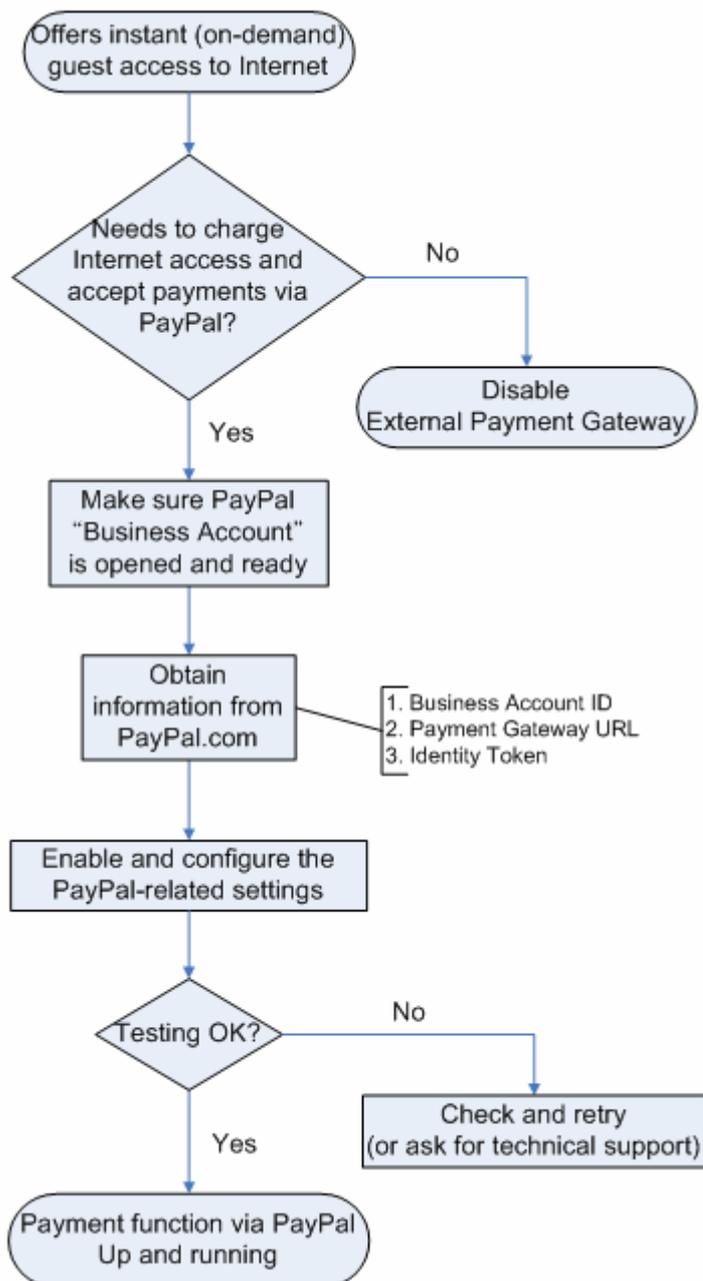
#### 3.3 Search for The Transaction Details for A Specific Customer

Please log in Authorize.Net. Click **Search and Download** → Enter the information for a specific customer as criteria → Click **Search** → Click the **Trans ID** number to view the transaction details.

**For more information about Authorize.Net, please see <http://www.authorize.net>.**

## Appendix C – Accepting Payments via PayPal

This section is to show independent Hotspot owners how to configure related settings in order to accept payments via PayPal, making the Hotspot an e-commerce environment for end users to pay for and obtain Internet access using their PayPal accounts or credit cards.



## 1. Setting Up

As follows are the basic steps to open and configure a **“Business Account”** on **PayPal**.

### 1.1 Open An Account

#### Step 1: Sign up for a PayPal Business Account and login.

Here is a link: <https://www.paypal.com/cgi-bin/webscr?cmd=registration-run>

Choose Account Type → Enter Information → Confirm → Done

---

### Sign Up for a PayPal Account

Anyone with an email address can use PayPal to send and receive money online. [What is PayPal?](#)

**Already have a PayPal Account?**  
[Upgrade your account](#)

- Personal Account**  
Ideal for shopping online. It's a free, secure, and fast way to send payments. You can also accept bank account or PayPal balance-funded payments for free and a limited number of credit or debit card payments per year for a [low fee](#). [Learn more](#)
- Premier Account**  
Perfect for buying and selling on eBay or merchant websites. Accept all payment types for [low fees](#). Do business under your own name.
- Business Account**  
The right choice for your online business. Accept all payment types for [low fees](#). Do business under a company or group name. [Learn more](#)

**Member Log-In** [Forgot your email address?](#)  
[Forgot your password?](#)

Email Address

Password

#### Step 2: Edit necessary settings in “Website Payment Preferences”

Click **Profile** → Click **Website Payment Preferences** in the **Selling Preferences** section

**PayPal** [Log Out](#) | [Help](#) | [Security Center](#)

My Account
Send Money
Request Money
Merchant Tools
Auction Tools

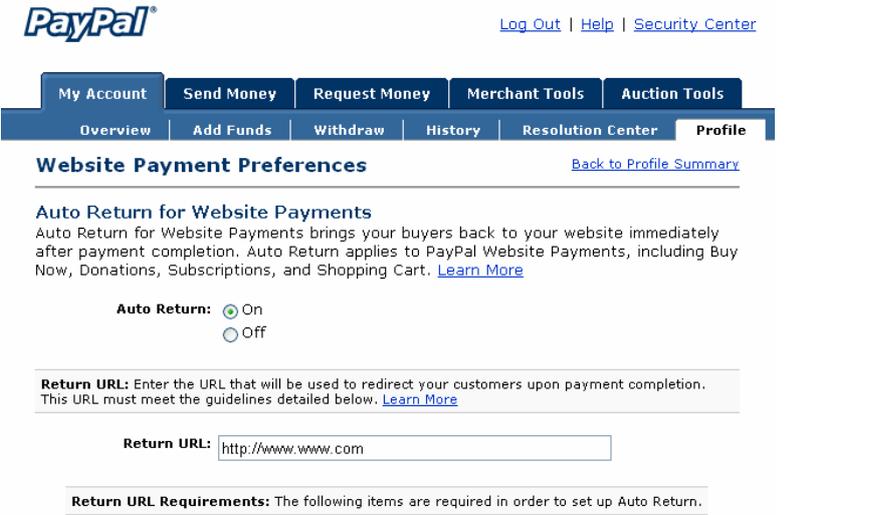
Overview
Add Funds
Withdraw
History
Resolution Center
Profile

### Profile Summary

To edit your Profile information, please click on a link below.

<p><b>Account Information</b></p> <ul style="list-style-type: none"> <li><a href="#">Email</a></li> <li><a href="#">Street Address</a></li> <li><a href="#">Phone</a></li> <li><a href="#">Password</a></li> <li><a href="#">Notifications</a></li> <li><a href="#">Multi-User Access</a></li> <li><a href="#">API Access</a></li> <li><a href="#">Business Information</a></li> <li><a href="#">Close Account</a></li> </ul>	<p><b>Financial Information</b></p> <ul style="list-style-type: none"> <li><a href="#">Credit Cards</a></li> <li><a href="#">Bank Accounts</a></li> <li><a href="#">Currency Balances</a></li> <li><a href="#">Gift Certificates</a></li> <li><a href="#">Monthly Account Statements</a></li> <li><a href="#">Preapproved Payments</a></li> </ul>	<p><b>Selling Preferences</b></p> <ul style="list-style-type: none"> <li><a href="#">Auctions</a></li> <li><a href="#">Regional Tax</a></li> <li><a href="#">Shipping Calculations</a></li> <li><a href="#">Payment Receiving Preferences</a></li> <li><a href="#">Instant Payment Notification Preferences</a></li> <li><a href="#">Reputation</a></li> <li><a href="#">Customer Service Message</a></li> <li><a href="#">Seller Eligibility for PayPal Buyer Protection</a></li> <li style="border: 2px solid red; padding: 2px;"><a href="#">Website Payment Preferences</a></li> <li><a href="#">Encrypted Payment Settings</a></li> <li><a href="#">Custom Payment Pages</a></li> <li><a href="#">Invoice Templates</a></li> <li><a href="#">Language Encoding</a></li> </ul>
---	---	--

Administrators should scroll down to edit each setting as shown in the table below. To activate all the changes, please click **Save** at the end of the page.

Settings	Screenshots
<p><b>Auto Return (On)</b></p> <p><b>Return URL (Redirect Webpage)</b></p> <p>Type <a href="http://www.www.com">http://www.www.com</a> or other URL.</p>	 <p>The screenshot shows the PayPal 'Profile' page under 'Website Payment Preferences'. The 'Auto Return for Website Payments' section is active, with the 'Auto Return' radio button set to 'On'. Below it, the 'Return URL' is set to 'http://www.www.com'. A note states that the Return URL must meet specific guidelines. At the bottom, there are 'Return URL Requirements'.</p>
<p><b>Payment Data Transfer (On)</b></p>	<p><b>Payment Data Transfer (optional)</b></p> <p>Payment Data Transfer allows you to receive notification of successful payments as they are made. The use of Payment Data Transfer depends on your <a href="#">system configuration</a> and your Return URL. Please note that in order to use Payment Data Transfer, you <b>must</b> turn on Auto Return.</p> <p><b>Payment Data Transfer:</b> <input checked="" type="radio"/> On <input type="radio"/> Off</p>
<p><b>Block Non-encrypted Website Payment (Off)</b></p>	<p><b>Encrypted Website Payments</b></p> <p>Using encryption enhances the security of website payments by decreasing the possibility that a 3rd party could manipulate the data in your button code. If you plan on only using encrypted buttons you can block payments from non-encrypted ones.</p> <p><a href="#">Learn more about Encrypted Website Payments</a></p> <p><b>Note:</b> If you enable Encrypted Website Payments, all of your Buy Now, Donations, and Subscriptions buttons <b>must</b> be encrypted via one of the following methods:</p> <ul style="list-style-type: none"> <li>Using the <a href="#">Button Factory</a> with the security settings enabled.</li> <li>Using your own code, you encrypt all website payments before sending them to PayPal.</li> </ul> <p>By enabling this feature, any Buy Now, Donation, or Subscription button that is not encrypted will be rejected by PayPal.</p> <p><b>Block Non-encrypted Website Payment:</b> <input type="radio"/> On <input checked="" type="radio"/> Off</p>
<p><b>PayPal Account Optional (Off)</b></p>	<p><b>PayPal Account Optional</b></p> <p>When this feature is turned on, your customers will go through an optimized checkout experience. This feature is available for Buy Now, Donations, and Shopping Cart buttons, but not for Subscription buttons. <a href="#">Learn More</a></p> <p><b>PayPal Account Optional:</b> <input type="radio"/> On <input checked="" type="radio"/> Off</p>
<p><b>Contact Telephone Number (Off)</b></p> <p><b>Click Save.</b></p>	<p><b>Contact Telephone Number</b></p> <p>When you activate this option, your customers will be asked to include a Contact Telephone Number with their payment information. <a href="#">Learn More</a></p> <p><b>Note:</b> Selecting <b>On (Required Field)</b> could have a negative effect on buyer conversion.</p> <p><b>Contact Telephone:</b> <input type="radio"/> On (Optional Field) <input type="radio"/> On (Required Field) <input checked="" type="radio"/> Off (PayPal recommends this option)</p> <p style="text-align: right;"> <input type="button" value="Save"/> <input type="button" value="Cancel"/> </p>

## 1.2 Configure AirLive WIAS-1200G with a PayPal Business Account

Please log in AirLive WIAS-1200G:

**User Authentication** → **Authentication Configuration** → Click the server **On-demand User** → **On-demand User Server Configuration** → Click **Payment** → **Payment Configuration** → **External Payment Gateway** → Select **PayPal**

The screenshot shows the configuration interface for the AirLive WIAS-1200G. The 'User Authentication' tab is active, and the 'Payment Configuration' page is displayed. In the 'External Payment Gateway' section, the 'PayPal' radio button is selected. The 'PayPal Payment Page Configuration' section contains the following fields:

- Business Account:** [Empty text box]
- Payment Gateway URL:** `https://www.paypal.com/cgi-bin/webscr`
- Identity Token:** [Empty text box]
- Verify SSL Certificate:**  Enable  Disable
- Currency:** USD (U.S. Dollar)

Three fields are required:

Setting	Description
<b>Business Account ID</b>	This is the "Login ID" (email address) that is associated with the PayPal Business Account.
<b>Payment Gateway URL</b>	<code>https://www.paypal.com/cgi-bin/webscr</code> (default URL for PayPal)
<b>Identity Token</b>	<p>Please log in PayPal after saving the above settings → Click <b>Profile</b> → Click <b>Website Payment Preferences</b> in the <b>Selling Preferences</b> section → Scroll down to the section, <b>Payment Data Transfer (optional)</b>.</p> <hr/> <p><b>Payment Data Transfer (optional)</b> Payment Data Transfer allows you to receive notification of successful payments as they are made. The use of Payment Data Transfer depends on your <a href="#">system configuration</a> and your Return URL. Please note that in order to use Payment Data Transfer, you <b>must</b> turn on Auto Return.</p> <p><b>Payment Data Transfer:</b> <input checked="" type="radio"/> On <input type="radio"/> Off</p> <p><b>Identity Token:</b> <code>FIY4OqLV-EMdUbg8D_3y7kLG1C8iGdxpF-z6f6kCo-KBd0fSSQokZkCBQru</code></p> <hr/> <p>Copy the <b>Identity Token</b> in the above page to the section "<b>PayPal Payment Page Configuration</b>" of AirLive WIAS-1200G.</p> <p>The screenshot shows the 'PayPal Payment Page Configuration' section with the following fields:</p> <ul style="list-style-type: none"> <li><b>Business Account:</b> <code>test_business_account@hotmail.com</code></li> <li><b>Payment Gateway URL:</b> <code>https://www.paypal.com/cgi-bin/webscr</code></li> <li><b>Identity Token:</b> <code>FIY4OqLV-EMdUbg8D_3y7kLG1C8iGdxpF-z6f6kCo-</code> (highlighted with a red box)</li> <li><b>Verify SSL Certificate:</b> <input type="radio"/> Enable <input checked="" type="radio"/> Disable</li> <li><b>Currency:</b> USD (U.S. Dollar)</li> </ul>

### 1.3 Requirements for Building a Secure PayPal-based E-Commerce Site

To deploy the PayPal function properly, it is required that the merchant register an **Internet domain name** (for example, www.StoreName.com) for this subscriber gateway device.

System Information	
System Name	OvisLink WIAS-1200G
Administrator Info	Sorry! The service is temporarily unavailable. <small>(It'll appear when Internet connection fails.)</small>
Device Name	www.YourStoreName.com <small>(FQDN for this device)</small>
Home Page	<input checked="" type="radio"/> Enable <input type="radio"/> Disable http://www.ovislink.com/ <small>(e.g. http://www.ovislink.com/)</small>

In addition, it is necessary to sign up for a **SSL certificate**, licensed from a “**Certificate Authority**” (for example, **VerSign**), for this registered Internet domain name.

Thus, by meeting these two requirements, it will allow end customers or subscribers to pay for the Internet access in a securer and convenient way.

## 2. Basic Maintenance

In order to maintain the operation, the merchant owner will have to manage the accounts and payment transactions on PayPal website as well as AirLive WIAS-1200G.

### 2.1 Refund a completed payment and remove the on-demand account generated on AirLive WIAS-1200G

(1) To refund a payment, please log in PayPal → Click **History** → Locate the specific payment listing in the activity history log → Click **Details** of the payment listing → Click **Refund Payment** at the end of the details page → Type in information: **Gross Refund Amount** and/or **Optional Note to Buyer** → Click **Submit** → Confirm the details and click **Process Refund**

(2) To remove the specific account from AirLive WIAS-1200G, please log in AirLive WIAS-1200G:

**User Authentication** → **Authentication Configuration** → Click the server **On-demand User** → **On-demand User Server Configuration** → **Users List** → Click **Delete** on the record with the account ID. Click **Delete All** to delete all users at once.

On-demand Users List					
Username	Password	Remaining Time/Volume	Status	Expiration Time	Delete All
V34Q	KP23E64C	2 hour	Normal	2007/02/01-13:35:41	Delete

## 2.2 Find the username and password for a specific customer

(1) To find the username, please log in PayPal → Click **History** → Locate the specific payment listing in the activity history log → Click **Details** of the payment listing → Username can be found in the **"Item Title"** field

(2) To find the password associated with a specific username, please log in AirLive WIAS-1200G:

**User Authentication** → **Authentication Configuration** → Click the server **On-demand User** → **On-demand User Server Configuration** → **Users List**. Search for the specific username. Password can be found in the same record

On-demand Users List					
Username	Password	Remaining Time/Volume	Status	Expiration Time	Delete All
V34Q	KP23E64C	2 hour	Normal	2007/02/01-13:35:41	Delete

### Note:

As stated by PayPal, you can issue a full or partial refund for any reason and for **60 days** after the original payment was sent. To find the on-demand account name for a specific payment, click **Details** of the payment listing in the activity history log → **Username** can be found in the **"Item Title"** field

## 2.3 Send an email receipt to a customer

If a valid email address is provided, an email receipt with payment details for each successful transaction will be automatically sent to the customer via PayPal. To change the information on the receipt for customer, please log in AirLive WIAS-1200G:

**User Authentication** → **Authentication Configuration** → Click the server **On-demand User** → **On-demand User Server Configuration** → **Payment** → **Payment Configuration** → **External Payment Gateway** → Select **PayPal** → Go to **"Client's Purchasing Record"** section → Type in information in the text boxes: **Invoice Number** and **Description (Item Name)** → Confirm and click **Apply**

Client's Purchasing Record	
Invoice Number	Hotspot - 00000001 * <input type="checkbox"/> Reset
Description(Item Name)	Wireless Internet Access *
Title for Message to Seller	Special Note to Seller *



## 2.4 Send an email receipt for each transaction to the merchant

A copy of email receipt with payment details (including available message note from buyer) for each successful transaction will also be automatically sent to the merchant owner/administrator via PayPal.

## 3. Reporting

During normal operation, the following steps will be necessary to generate transaction reports.

### 3.1 Transaction activity during a period

(1) Please log in PayPal → Click **History** → Choose activity type from the **Show** field as the search criteria → Specify the dates (**From** and **To** fields) for the period → Click **Search**

The screenshot shows the PayPal 'History' page. At the top, there is a navigation bar with tabs: Overview, Add Funds, Withdraw, History (highlighted), Resolution Center, and Profile. Below the navigation bar, the 'History' section is displayed. It includes a link to 'View up to three months of monthly account statements' and a 'View this' button. The 'Search' section contains a 'Show:' dropdown menu set to 'All Activity - Simple View'. There are radio buttons for 'Within:' (The Past Day) and 'From:' (selected). The 'From:' date is set to 12 / 31 / 2006. The 'To:' date is set to 1 / 30 / 2007. A 'Search' button is highlighted with a red box. Below the search fields, a summary line reads 'All Activity - Simple View from Dec. 31, 2006 to Jan. 30, 2007'. A table header is visible with columns: Date, Type, To/From, Name/Email, Status, Details, Action, Gross, Fee, and Net Amount.

### 3.2 Search for the transaction details for a specific customer

Please log in PayPal → Click **History** → Click **Advanced Search** → Enter the name for a specific customer as criteria in the **Search For** field and Choose Last Name or Last Name, First Name in the **In** field → Specify the time period → Click **Submit** → Click **Details** to view the transaction details

The screenshot shows the PayPal 'History' page with the 'Advanced Search' option selected in the left sidebar. The 'Search For:' field contains 'HotSpot00000001'. The 'In:' dropdown menu is set to 'Invoice ID'. The 'Within:' radio button is selected for 'The Past Day'. The 'From:' date is set to 12 / 31 / 2006. The 'To:' date is set to 1 / 30 / 2007. A 'Submit' button is visible at the bottom right of the search section.

For more information about PayPal, please see <http://www.paypal.com>

## Appendix D – Examples of Making Payments for End Users

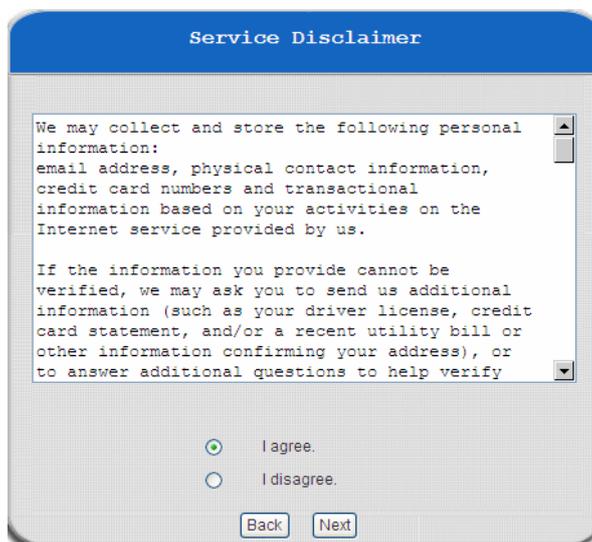
### 1. Making Payments via Authorize.Net

**Step 1:** Click the link below the login window to pay for the service by credit card via Authorize.Net.



The screenshot shows a 'User Login Page' with a blue header. Below the header, it says 'Welcome To User Login Page.' and 'Please Enter Your User Name and Password To Sign In .'. There are two input fields: 'User Name:' with a person icon and 'Password:' with a key icon. At the bottom, there are three buttons: 'Submit', 'Clear', and 'Remaining', each with a checkmark icon. Below the login form, there is a red-bordered box containing a blue link: 'Click here to purchase by Credit Card Online.'

**Step 2:** Choose *I agree* to accept the terms of use and click *Next*.



The screenshot shows a 'Service Disclaimer' window with a blue header. The main content is a scrollable text area containing the following text: 'We may collect and store the following personal information: email address, physical contact information, credit card numbers and transactional information based on your activities on the Internet service provided by us. If the information you provide cannot be verified, we may ask you to send us additional information (such as your driver license, credit card statement, and/or a recent utility bill or other information confirming your address), or to answer additional questions to help verify'. Below the text area, there are two radio buttons: 'I agree.' (which is selected) and 'I disagree.'. At the bottom, there are two buttons: 'Back' and 'Next'.

**Step 3:** Please fill out the form and Click **Submit** to send out this transaction. There will be a confirm dialog box.

Wireless Internet Access

Rate Plan	Price
<input checked="" type="radio"/> 2 hrs 0 mins	\$ 4
<input type="radio"/> 12 hrs 0 mins	\$ 8
<input type="radio"/> 600 Mbyte	\$ 4
<input type="radio"/> 2000 Mbyte	\$ 8

Credit Card & Contact Information

Credit Card Number	<input type="text" value="45631234567890"/> *
Credit Card Expiration Date	<input type="text" value="1208"/> *(MMYY)
Card Type	<input type="text" value="Visa"/> *
Card Code	<input type="text" value="527"/> *
E-mail	<input type="text" value="1223@yahoo.com"/>
First Name	<input type="text" value="Tom"/> *
Last Name	<input type="text" value="Lee"/> *
Company	<input type="text"/>
Address	<input type="text"/>
City	<input type="text"/>
State	<input type="text"/>
Zip	<input type="text"/>
Country	<input type="text"/>
Phone	<input type="text"/>
Fax	<input type="text"/>

Fields denoted by an asterisk(\*) are required.

**Note:**  
You must fill in the correct credit card number and expiration date. Card code is the last 3 digits of the security code located on the back of your credit card. If you choose to enter your e-mail address, you will receive a confirmation letter for your own reference.

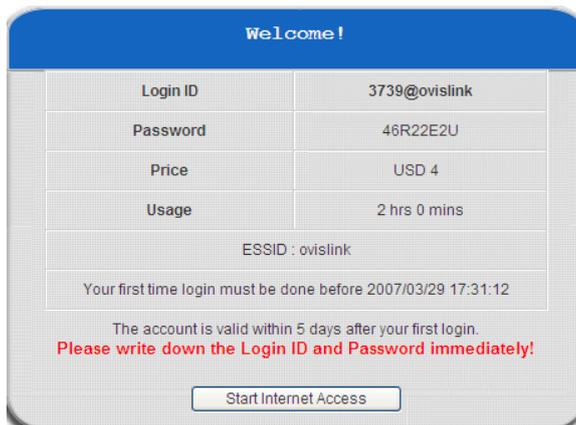
**Step 4:** Please confirm the data and the click **OK** to go on the transaction or click **Cancel** to revise the data or cancel this transaction. After clicking OK, there will be another dialog box showing up to confirm this transaction again.



**Step 5:** Click **OK** to complete the process or click **Cancel** to revise the data or cancel this transaction.



**Step 6:** Click **Start Internet Access** to use the Internet access service.



**Note:** The clients must fill in the correct credit card number and expiration date. Card code is the last 3 digits of the security code located on the back of your credit card. If clients choose to enter the e-mail addresses, clients will receive confirmation letters for reference.

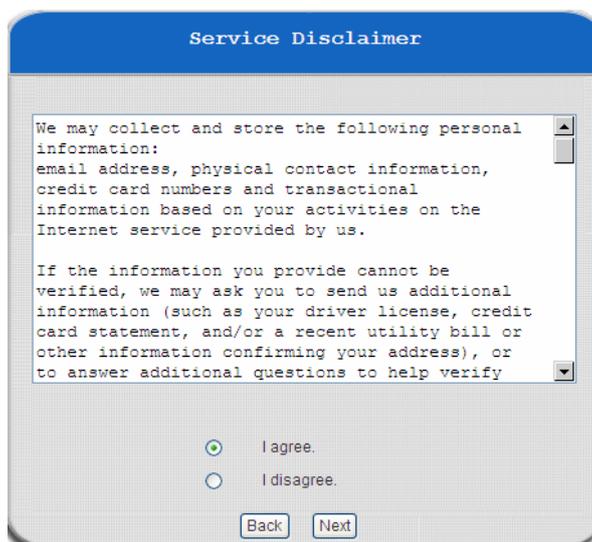
## 2. Making Payments via PayPal

**Step 1:** Click the link below the login window to pay for the service via PayPal.



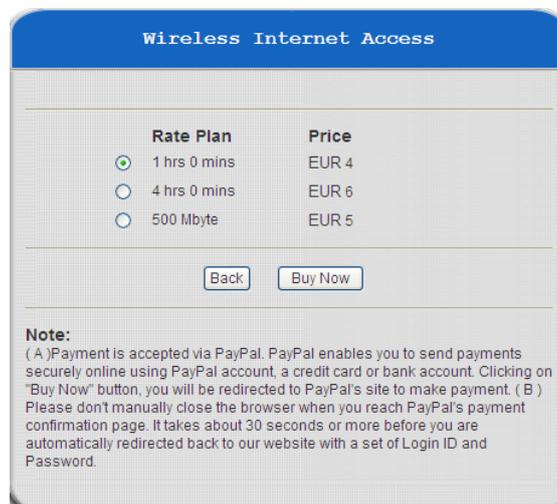
The screenshot shows a 'User Login Page' with a blue header. Below the header, it says 'Welcome To User Login Page.' and 'Please Enter Your User Name and Password To Sign In .'. There are two input fields: 'User Name:' and 'Password:'. Below the input fields are three buttons: 'Submit', 'Clear', and 'Remaining'. A red box highlights a link below the buttons: 'Click here to purchase by PayPal or Credit Card Online.'

**Step 2:** Choose **I agree** to accept the terms of use and click **Next**.



The screenshot shows a 'Service Disclaimer' page with a blue header. The main content is a scrollable text area containing the following text: 'We may collect and store the following personal information: email address, physical contact information, credit card numbers and transactional information based on your activities on the Internet service provided by us. If the information you provide cannot be verified, we may ask you to send us additional information (such as your driver license, credit card statement, and/or a recent utility bill or other information confirming your address), or to answer additional questions to help verify'. Below the text area are two radio buttons: 'I agree.' (selected) and 'I disagree.'. At the bottom are 'Back' and 'Next' buttons.

**Step 3:** Please fill out the form and Click **Submit** to send out this transaction. There will be a confirm dialog box.



The screenshot shows a 'Wireless Internet Access' page with a blue header. Below the header is a table with two columns: 'Rate Plan' and 'Price'. The table has three rows: '1 hrs 0 mins' (selected) for 'EUR 4', '4 hrs 0 mins' for 'EUR 6', and '500 Mbyte' for 'EUR 5'. Below the table are 'Back' and 'Buy Now' buttons. At the bottom is a 'Note:' section with the following text: '( A ) Payment is accepted via PayPal. PayPal enables you to send payments securely online using PayPal account, a credit card or bank account. Clicking on "Buy Now" button, you will be redirected to PayPal's site to make payment. ( B ) Please don't manually close the browser when you reach PayPal's payment confirmation page. It takes about 30 seconds or more before you are automatically redirected back to our website with a set of Login ID and Password.'



**Step 4:** You will be redirected to PayPal website to complete the payment process.

### YK Cafe

Wireless Internet Access (1 hrs 0 mins)	Total: €4.00 EUR
---	------------------

#### Pay Fast With PayPal



PayPal securely processes payments for YK Cafe. You can finish paying in a few clicks.

#### Why use PayPal?

- It's free to send money and shop online.
- You can shop without sharing your financial information with merchants.
- Over 50,000 online merchants accept PayPal.

Don't have a PayPal account?  
No problem. [continue checkout](#)

**LOG IN TO PAYPAL**

Email:

Password:

[Forgotten email address or password?](#)

### YK Cafe

JL, Review Your Payment	
-------------------------	--

Review the payment details below and click **Pay** to complete your secure payment. [Find out](#) how this payment is made.

Item	Unit Price	Qty	Total
Wireless Internet Access (1 hrs 0 mins)	€4.00	1	€4.00
<small>Username: QD2U, Your first time login must be done before 2007/03/29 17:59:45. The account is worth 1 hrs 0 mins of usage and is valid within 5 days after your first login.</small>			
<a href="#">Add special instructions for the Merchant</a>			Total: €4.00
			<b>Total: €4.00 EUR</b>

Payment Method: PayPal Funds £2.84 GBP  
PayPal Conversion Rate as of 26 Mar. 2007: 1 Pound Sterling = 1.41305 Euros  
[Change](#)

### YK Cafe

You Made A Payment	
--------------------	--

Your payment for €4.00 EUR has been completed.  
You are now being redirected to **YK Cafe**  
If you are not redirected within 10 seconds [click here](#).

**Step 5:** Click **Start Internet Access** to use the Internet access service.

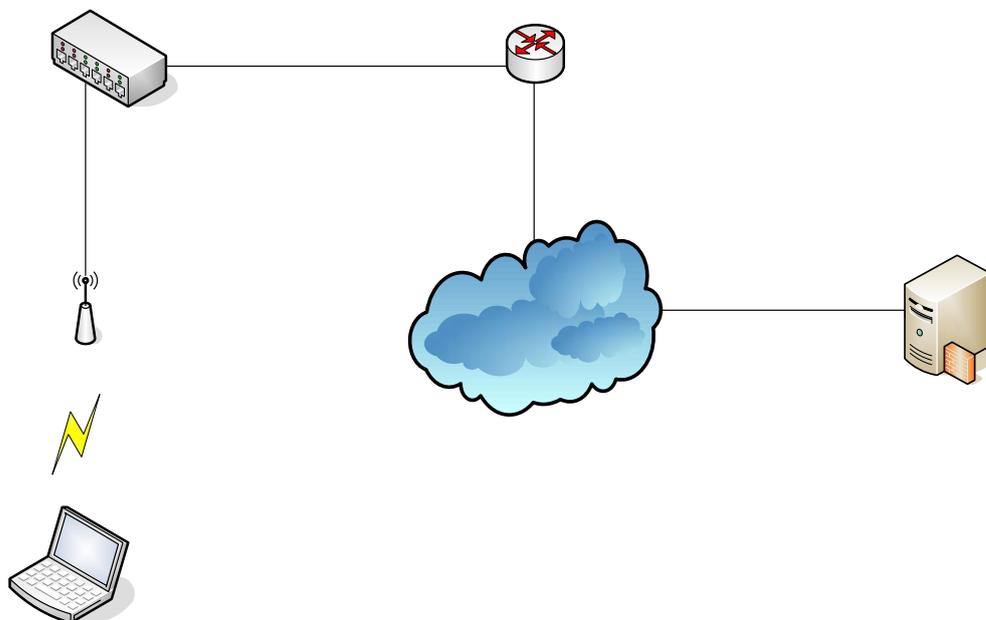
Welcome!	
Login ID	QD2U@AirLive
Password	H5776CB4
Price	EUR 4.00 ( Tax EUR 0.00 )
Usage	1 hrs 0 mins
ESSID : AirLive	
Your first time login must be done before 2007/03/29 17:59:45	
The account is valid within 5 days after your first login. <b>Please write down the Login ID and Password immediately!</b>	
<input type="button" value="Start Internet Access"/>	

**Note:**

1. Payment is accepted via PayPal. PayPal enables you to send payments securely online using PayPal account, a credit card or bank account. Clicking on **Buy Now** button, you will be redirected to PayPal's site to make payment.
2. Please **do not manually close the browser** when you reach PayPal's payment confirmation page. It takes about 30 seconds or more before you are **automatically redirected back to our website with a set of Login ID and Password**.

## Appendix E – Proxy Setting for Hotspot

HotSpot is a place such as a coffee shop, hotel, or a public area where provides Wi-Fi service for mobile and temporary users. HotSpot is usually implemented without complicated network architecture and using some proxy servers provided by Internet Service Providers.



In Hotspots, users usually enable their proxy setting of the browsers such as IE and Firefox. Therefore, so we need to set some proxy configuration in the Gateway need to be set. Please follow the steps to complete the proxy configuration :

1. Login Gateway by using "**admin**".
2. Click the **Network Configuration from top menu** and the homepage of the **Network Configuration** will appear.

Network Configuration	
<b>Network Address Translation</b>	WIAS-1200G provides 3 types of network address translation: Static Assignments, Public Accessible Server and IP/Port Redirect.
<b>Privilege List</b>	System provides Privilege IP Address List and Privilege MAC Address List. System will NOT control the network access of those listed devices.
<b>Monitor IP List</b>	System can monitor up to 40 network devices with the defined probe interval and retrying.
<b>Walled Garden List</b>	Up to 20 hosts' URL could be defined in Walled Garden List. Clients may access these URL without authentication.
<b>Proxy Server Properties</b>	WIAS-1000GV2 supports up to 10 external proxy servers. System can redirect traffic to external proxy server into built-in proxy server.
<b>Dynamic DNS</b>	WIAS-1200G supports dynamic DNS (DDNS) feature.



- Click the **Proxy Server Properties** from left menu and the homepage of the **Proxy Server Properties** will appear.

Proxy Server Properties	
Internal Proxy Server	
<input type="radio"/> Enable <input checked="" type="radio"/> Disable	

External Proxy Server		
Item	Server IP	Port
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>
11	<input type="text"/>	<input type="text"/>

- Add the ISP's proxy Server IP and Port into **External Proxy Server** Setting.

Proxy Server Properties	
Internal Proxy Server	
<input type="radio"/> Enable <input checked="" type="radio"/> Disable	

External Proxy Server		
Item	Server IP	Port
1	<input type="text" value="10.2.3.203"/>	<input type="text" value="6588"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>
11	<input type="text"/>	<input type="text"/>

5. **Enable Built-in Proxy Server** in **Internal Proxy Server** Setting.

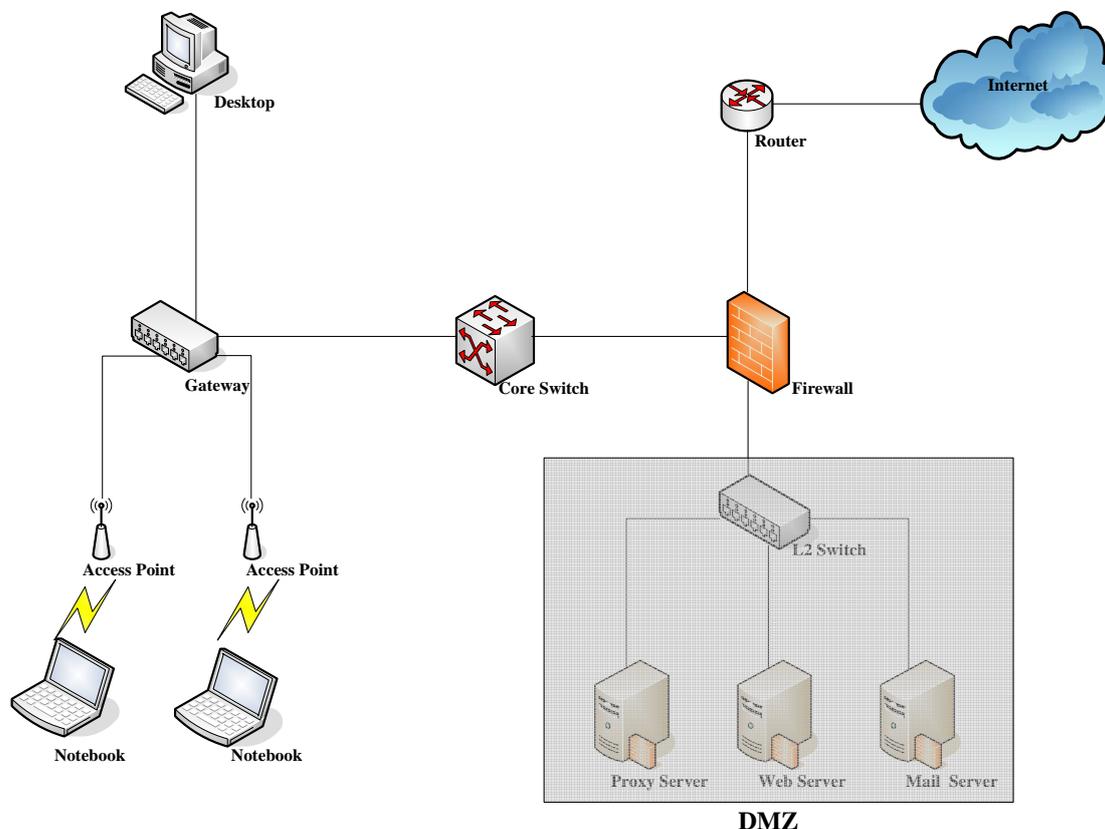
Proxy Server Properties	
Internal Proxy Server	
<input checked="" type="radio"/> Enable <input type="radio"/> Disable	

External Proxy Server		
Item	Server IP	Port
1	<input type="text" value="10.2.3.203"/>	<input type="text" value="6588"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>
11	<input type="text"/>	<input type="text"/>

6. Click **Apply** to save the settings.

## Appendix F – Proxy Setting for Enterprise

Enterprises usually isolate their intranet and internet by using more elaborated network architecture. Many enterprises have their own proxy server which is usually at intranet or DMZ under the firewall protection.



In enterprises, network managers or MIS staff may often ask their users to enable their proxy setting of the browsers such as IE and Firefox to reduce the internet access loading. Therefore some proxy configurations in the Gateway need to be set.

**Note:**

*Some enterprises will automatically redirect packets to proxy server by using core switch or Layer 7 devices. By the way, the clients don't need to enable their browsers' proxy settings, and administrators don't need to set any proxy configuration in the Gateway.*

Please follow the steps to complete the proxy configuration :

## ■ Gateway setting

1. Login Gateway by using “**admin**”.
2. Click the **Network Configuration from top menu** and the homepage of the **Network Configuration** will appear.

Network Configuration	
<b>Network Address Translation</b>	WIAS-1200G provides 3 types of network address translation: Static Assignments, Public Accessible Server and IP/Port Redirect.
<b>Privilege List</b>	System provides Privilege IP Address List and Privilege MAC Address List. System will NOT control the network access of those listed devices.
<b>Monitor IP List</b>	System can monitor up to 40 network devices with the defined probe interval and retrying.
<b>Walled Garden List</b>	Up to 20 hosts' URL could be defined in Walled Garden List. Clients may access these URL without authentication.
<b>Proxy Server Properties</b>	WIAS-1000GV2 supports up to 10 external proxy servers. System can redirect traffic to external proxy server into built-in proxy server.
<b>Dynamic DNS</b>	WIAS-1200G supports dynamic DNS (DDNS) feature.

3. Click the **Proxy Server Properties** from left menu and the homepage of the **Proxy Server Properties** will appear.

Proxy Server Properties	
Internal Proxy Server	
<input type="radio"/> Enable <input checked="" type="radio"/> Disable	

External Proxy Server		
Item	Server IP	Port
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>
11	<input type="text"/>	<input type="text"/>

4. Add your proxy Server IP and Port into **External Proxy Server** Setting.

Proxy Server Properties

Internal Proxy Server

Enable  Disable

External Proxy Server

Item	Server IP	Port
1	10.2.3.203	6588
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		

5. **Disable Built-in Proxy Server** in **Internal Proxy Server** Setting.

Proxy Server Properties

Internal Proxy Server

Enable  Disable

External Proxy Server

Item	Server IP	Port
1	10.2.3.203	6588
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		

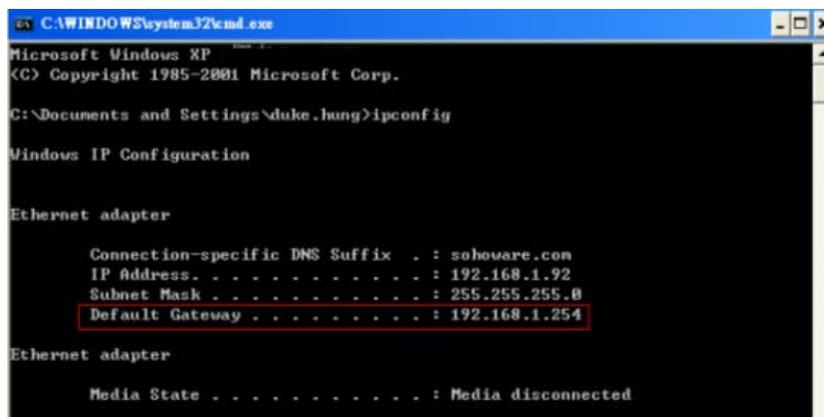
6. Click **Apply** to save the settings.

**Note:** If your proxy server is disabled, it will make the user authentication operation abnormal. When users open the browser, the login page won't appear because the proxy server is down. Please make sure your proxy server is always available.

## ■ Client setting

It is necessary for clients to add default gateway IP address into proxy exception information so the user login successful page can show up normally.

1. Use command “*ipconfig*” to get Default Gateway IP Address.



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\duke.hung>ipconfig

Windows IP Configuration

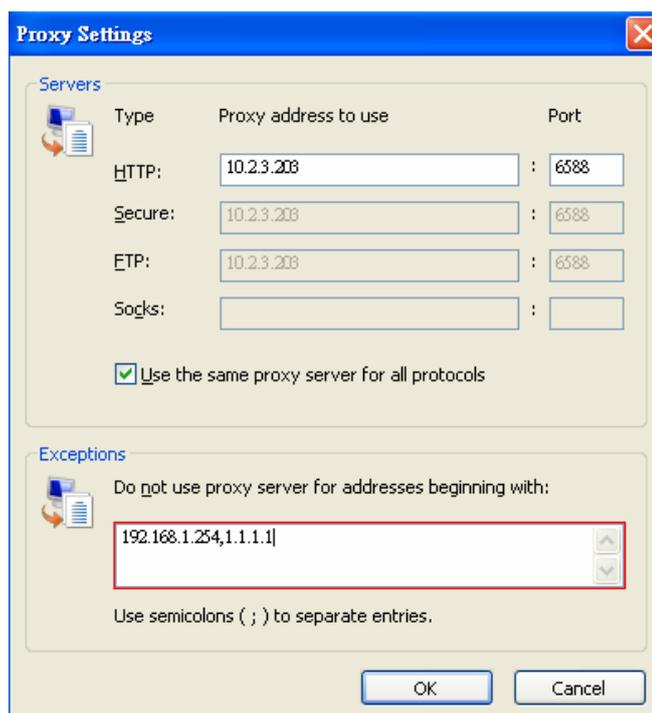
Ethernet adapter

Connection-specific DNS Suffix . : sohware.com
IP Address . . . . . : 192.168.1.92
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.254

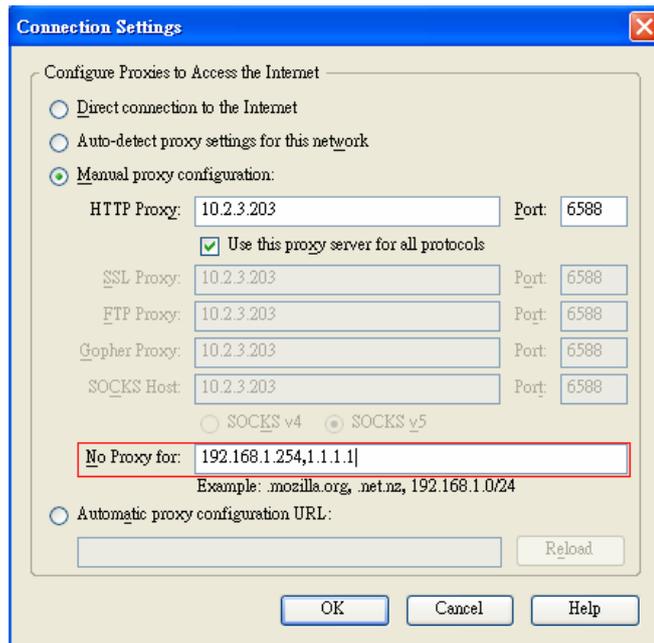
Ethernet adapter

Media State . . . . . : Media disconnected
```

2. Open browser to add **default gateway IP address (e.g. 192.168.1.254)** and **logout page IP address “1.1.1.1”** into proxy exception information.
  - For IE



- For Firefox



## Appendix G – Disclaimer for On-Demand Users

In AirLive WIAS-1200G, the end user first gets a login page when she/he opens its web browser right after associating with an access point. However, in some situations, the hotspot owners or MIS staff may want to display “terms of use” or announcement information before the login page. Hotspot owners or MIS staff can design a new disclaimer/announcement page and save the page in their local server. After the agreement shown on the page is read, users are asked whether they agree or disagree with the disclaimer. By clicking “I agree,” users are able to log in. If users choose to decline, they will get a popup window saying they are unable to log in. The basic design is to have the disclaimer and login function in the same page but with the login function hidden until users agree with the disclaimer.

Here the codes are supplied. Please note that the blue part is for the login feature, the red part is the disclaimer, and the green part can be modified freely by administrators to suit the situation better. Now the default is set to “I disagree” with the disclaimer. Administrators can change the purple part to set “agree” as the default or set no default. These codes should be saved in local storage with a name followed by .html, such as login\_with\_disclaimer.html.

```
<html>
<head>
<META HTTP-EQUIV="Pragma" CONTENT="no-cache">
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<META HTTP-EQUIV="Cache-Control" CONTENT="no-cache">
<link href="../../include/style.css" rel="stylesheet" type="text/css">
<title>Login</title>

<script language="javascript1.2">
    var pham = document.cookie;
    var disableButton=false;

    function getCookie(name)
    {
        name += "="; // append '=' to name string
        var i = 0; // index of first name=value pair
        while (i < pham.length) {
            var offset = i + name.length; // end of section to compare name string
            if (pham.substring(i, offset) == name) { // if string matches
                var endstr = pham.indexOf(";", offset); //end of name=value pair
                if (endstr == -1) endstr = pham.length;
                return unescape(pham.substring(offset, endstr));
            }
            i += name.length + 1;
        }
    }
</script>
```



```

// return cookie value section
    }
    i = pham.indexOf(" ", i) + 1; // move i to next name=value pair
    if (i == 0) break; // no more values in cookie string
    }
    return null; // cookie not found
}

```

```

function CodeCookie(str)
{
var strRtn="";

for (var i=str.length-1;j>=0;i--)
{
    strRtn+=str.charCodeAt(i);
    if (i) strRtn+="a";
}
return strRtn;
}

function DecodeCookie(str)
{
var strArr;
var strRtn="";

strArr=str.split("a");

for(var i=strArr.length-1;j>=0;i--)
strRtn+=String.fromCharCode(eval(strArr[j]));

return strRtn;

}

```

```

function MM_swapImgRestore() { //v3.0
var i,x,a=document.MM_sr; for(i=0;a&&i<a.length&&(x=a[i])&&x.oSrc;i++) x.src=x.oSrc;
}

```

```

function MM_preloadImages() { //v3.0
var d=document; if(d.images){ if(!d.MM_p) d.MM_p=new Array();
var i,j=d.MM_p.length,a=MM_preloadImages.arguments; for(i=0; i<a.length; i++)

```

```
if (a[i].indexOf("#")!=0){ d.MM_p[j]=new Image; d.MM_p[j++].src=a[i];}
}
```

```
function MM_findObj(n, d) { //v4.01
var p,i,x;  if(!d) d=document; if((p=n.indexOf("?"))>0&&parent.frames.length) {
d=parent.frames[n.substring(p+1)].document; n=n.substring(0,p);}
if(!(x=d[n])&&d.all) x=d.all[n]; for (i=0;!x&&i<d.forms.length;i++) x=d.forms[i][n];
for(i=0;!x&&d.layers&&i<d.layers.length;i++) x=MM_findObj(n,d.layers[i].document);
if(!x && d.getElementById) x=d.getElementById(n); return x;
}
```

```
function MM_swapImage() { //v3.0
var i,j=0,x,a=MM_swapImage.arguments; document.MM_sr=new Array; for(i=0;i<(a.length-2);i+=3)
if ((x=MM_findObj(a[i]))!=null){document.MM_sr[j++]=x; if(!x.oSrc) x.oSrc=x.src; x.src=a[i+2];}
}
```

```
function init(form)
{
    id = getCookie("username");
    if(id!="" && id!=null)
    {
        form.myusername.value = id;
    }

    disclaimer.style.display="";
    login.style.display='none';
}
```

```
function Before_Submit(form)
{
    if(form.myusername.value == "")
    {
        alert("Please enter username.");
        form.myusername.focus();
        form.myusername.select();
        disableButton=false;

        return false;
    }
    if(form.mypassword.value == "")
```

```
{
    alert("Please enter password.");
    form.mypassword.focus();
    form.mypassword.select();
    disableButton=false;

    return false;
}

if(disableButton==true)
{
    alert("The system is now logging you in, please wait a moment.");
    return false;
}
else
{
    disableButton=true;
    return true;
}
return true;
}
function reminder_onclick(form)
{
    Reminder.myusername.value = form.myusername.value;
    Reminder.mypassword.value = form.mypassword.value;
    Reminder.submit();
}
function cancel_onclick(form)
{
    form.reset();
}

function check_agree(form)
{
if(form.selection[1].checked == true)
{
    alert("You disagree with the disclaimer, therefore you will NOT be able to log in.");
    return false;
}
}
```

```

disclaimer.style.display='none';
login.style.display="";

```

```

        return true;
    }

```

```

</script>

```

```

</head>

```

```

<body style="font-family: Arial" bgcolor="#FFFFFF"

```

```

onload="init(Enter);MM_preloadImages('../images/submit0.gif','../images/clear0.gif','../images/remaining0.gif')">

```

```

    <ilayer width={marquee_width}; height={marquee_height}; name="cmarquee01">

```

```

    <layer name="cmarquee02" width={marquee_width}; height={marquee_height};></layer>

```

```

</ilayer>

```

```

<form action="userlogin.shtml" method="post" name="Enter">

```

```

<table name="disclaimer" id="disclaimer" width="460" height="430" border="0" align="center"

```

```

background="../images/agreement.gif">

```

```

    <tr>

```

```

        <td height="50" align="center" valign="middle"><div align="center" class="style5">Service

```

```

Disclaimer</div></td>

```

```

    </tr>

```

```

    <tr>

```

```

        <td height="260" align="center" valign="middle"><table width="370" height="260" border="0" align="center">

```

```

            <tr>

```

```

                <td>

```

```

                    <textarea name="textarea" cols="50" rows="15" align="center" readonly>

```

We may collect and store the following personal information:

e-mail address, physical contact information, credit card numbers and transactional information based on your activities on the Internet service provided by us.

If the information you provide cannot be verified, we may ask you to send us additional information (such as your driver license, credit card statement, and/or a recent utility bill or other information confirming your address), or to answer additional questions to help verify your information.)

Our primary purpose in collecting personal information is to provide you with a safe, smooth, efficient, and customized experience. You agree that we may use your personal information to: provide the services and customer support you request; resolve disputes, collect fees, and troubleshoot problems; prevent potentially prohibited or illegal activities; customize, measure, and improve our services and the site's content and layout; compare

information for accuracy, and verify it with third parties.

We may disclose personal information to respond to legal requirements, enforce our policies, respond to claims that an activity violates the rights of others, or protect anyone's rights, property, or safety.

We may also share your personal information with:

members of our corporate family to help detect and prevent potentially illegal acts; service providers under contract who help with our business operations; (such as fraud investigations and bill collection) other third parties to whom you explicitly ask us to send your information; (or about whom you are otherwise explicitly notified and consent to when using a specific service) law enforcement or other governmental officials, in response to a verified request relating to a criminal investigation or alleged illegal activity; (In such events we will disclose name, city, state, telephone number, email address, User ID history, and fraud complaints)

xxxxx participants under confidentiality agreement, as we in our sole discretion believe necessary or appropriate in connection with an investigation of fraud, intellectual property infringement, piracy, or other unlawful activity; (In such events we will disclose name, street address, city, state, zip code, country, phone number, email, and company name.) and other business entities, should we plan to merge with, or be acquired by that business entity. (Should such a combination occur, we will require that the new combined entity follow this privacy policy with respect to your personal information. If your personal information will be used contrary to this policy, you will receive prior notice.)

Without limiting the above, in an effort to respect your privacy and our ability to keep the community free from bad actors, we will not otherwise disclose your personal information to law enforcement, other government officials, or other third parties without a subpoena, court order or substantially similar legal procedure, except when we believe in good faith that the disclosure of information is necessary to prevent imminent physical harm or financial loss or to report suspected illegal activity.

Your password is the key to your account. Do not disclose your password to anyone. Your information is stored on our servers. We treat data as an asset that must be protected and use lots of tools (encryption, passwords, physical security, etc.) to protect your personal information against unauthorized access and disclosure. However, as you probably know, third parties may unlawfully intercept or access transmissions or private communications, and other users may abuse or misuse your personal information that they collect from the site. Therefore, although we work very hard to protect your privacy, we do not promise, and you should not expect, that your personal information or private communications will always remain private.

By agreeing above, I hereby authorize xxxxx to process my service charge(s) by way of my credit card.

```
</textarea>
</td>
</tr>
</table></td>
</tr>
```

```
<tr>
  <td height="40"><table width="170" height="20" border="0" align="center" cellpadding="2">
    <tr>
      <td align="left"><input name="selection" value="1" type="radio"></td>
      <td><span class="style4">I agree.</span></td>
    </tr>
    <tr>
      <td align="left"><input name="selection" value="2" checked type="radio"></td>
      <td><span class="style4">I disagree.</span></td>
    </tr>
  </table></td>
</tr>
<tr>
  <td height="30"><table width="110" height="20" border="0" align="center" cellpadding="2">
    <tr>
      <td width="45" align="center" valign="middle"><input name="next_button" type="button" value="Next"
onclick="javascript:check_agree(Enter)"></td>
    </tr>
  </table></td>
</tr>
<tr>
  <td height="20">&nbsp;</td>
</tr>
</table>

<div align="center">
<table name="login" id="login" width="497" height="328" border="0" align="center" cellpadding="2" cellspacing="0"
background="../images/userlogin.gif">
  <tr>
    <td height="146" colspan="2">&nbsp;</td>
  </tr>
  <tr>
    <td width="43%" height="53">&nbsp;</td>
    <td><input type="text" name="myusername" size="20"></td>
  </tr>
  <tr>
    <td height="42">&nbsp;</td>
    <td><input type="password" name="mypassword" size="20"></td>
  </tr>
```

```
<tr>
  <td colspan="2">
    <div align="center">
      <a onclick="javascript:if(Before_Submit(Enter)){Enter.submit();}" onmouseout="MM_swapImgRestore()"
onmouseover="MM_swapImage('Image3','../images/submit0.gif',1)">
        
      </a>
      <a onclick="cancel_onclick(Enter)" onmouseout="MM_swapImgRestore()"
onmouseover="MM_swapImage('Image5','../images/clear0.gif',1)">
        
      </a>
      <a onclick="javascript:if(Before_Submit(Enter)){reminder_onclick(Enter);}"
onmouseout="MM_swapImgRestore()" onmouseover="MM_swapImage('Image4','../images/remaining0.gif',1)">
        
      </a>
    </div>
  </td>
</tr>
</table>
```

```
<table>
<tr>
  <td width="100%">
    <font color="#808080" size="2"><script language="JavaScript">if( creditcardenable == "Enabled" )
document.write("<a href='../loginpages/credit_agree.shtml'">Click here to purchase by Credit Card
Online.<a>");</script></font>
  </td>
</tr>
</table>
```

```
</div>
</form>
<form action="reminder.shtml" method="post" name="Reminder">
<input type="hidden" name="myusername" value="">
<input type="hidden" name="mypassword" value="">
</form>
<br>
<div align="center">
<table>
<tr>
```

```
<td width="100%">  
<font color="#808080" size="2"><script language="JavaScript">document.write(copyright);</script></font></td>  
</tr>  
</table>  
</div>  
</body>  
  
</html>
```



## Appendix H – Network Configuration & External Network

### Access

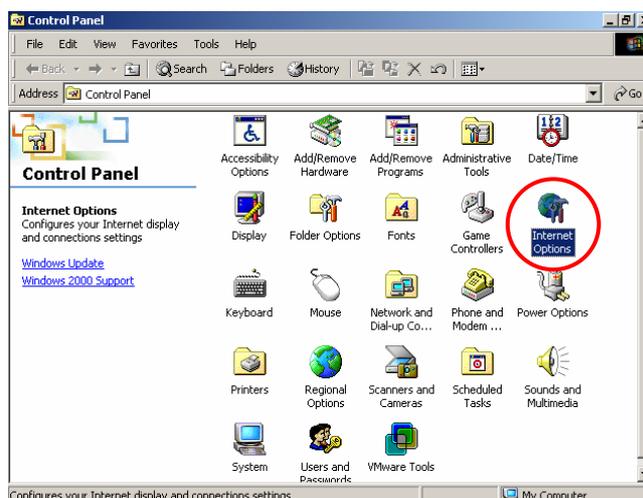
#### 1. Network Configuration on PC

After AirLive WIAS-1200G is installed, the following configurations must be set up on the PC: **Internet Connection Setup** and **TCP/IP Network Setup**.

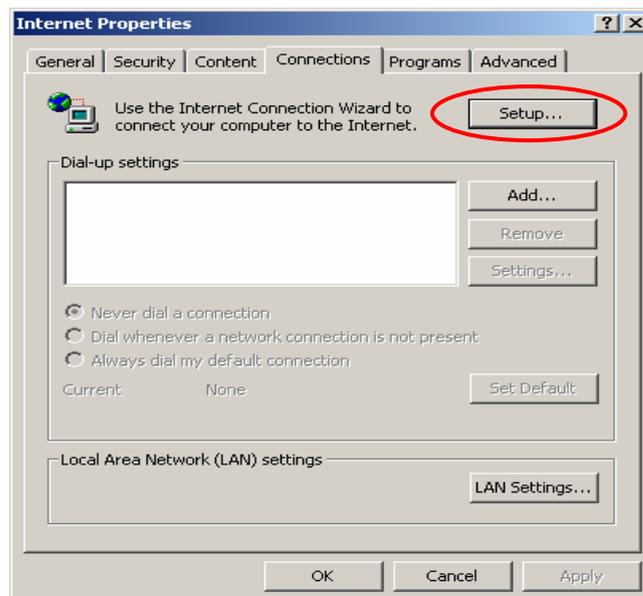
- **Internet Connection Setup**

- ◆ **Windows 9x/2000**

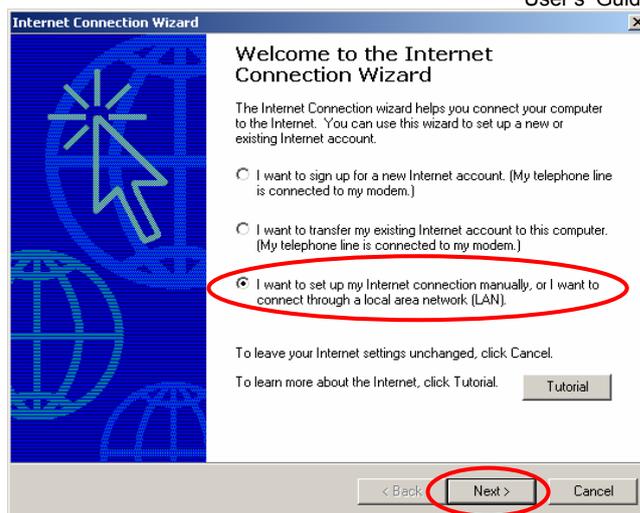
- 1) Choose **Start > Control Panel > Internet Options**.



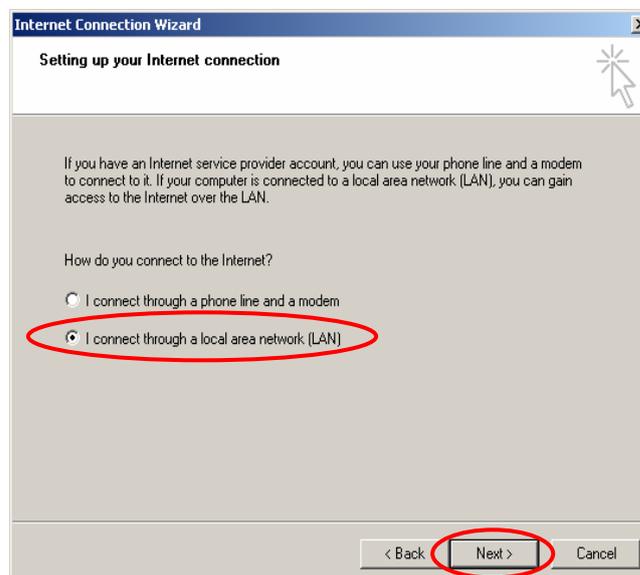
- 2) Choose the **"Connections"** label, and then click **Setup**.



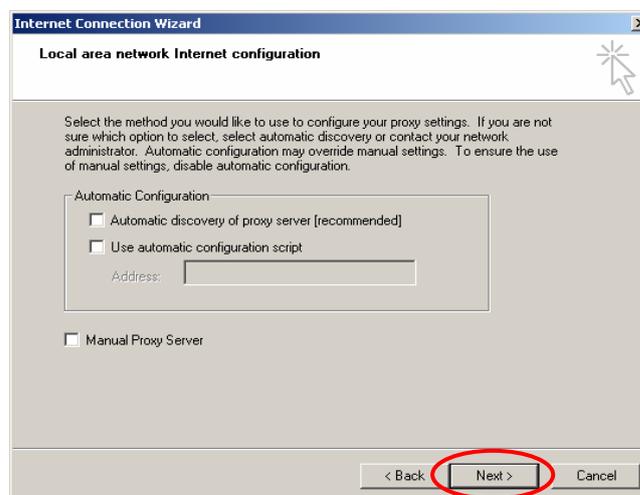
- 3) Choose “I want to set up my Internet connection manually, or I want to connect through a local Area network (LAN)”, and then click **Next**.



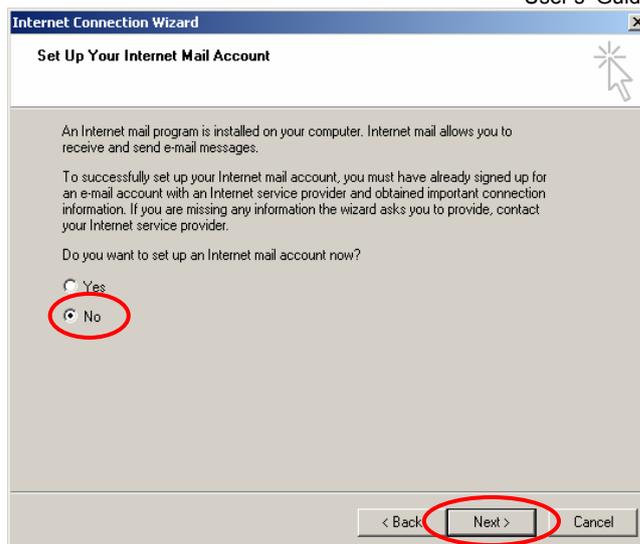
- 4) Choose “I connect through a local area network (LAN)” and click **Next**.



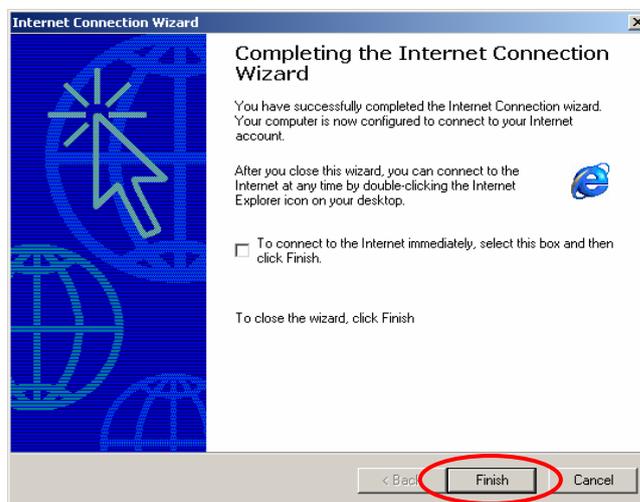
- 5) **DO NOT** choose any option in the following LAN window for Internet configuration, and just click **Next**.



6) Choose “**No**”, and click **Next**.

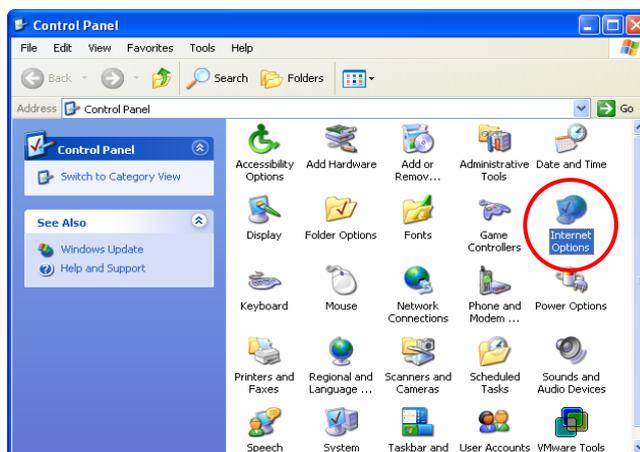


7) Finally, click **Finish** to exit the **Internet Connection Wizard**. Now, the set up has been completed.

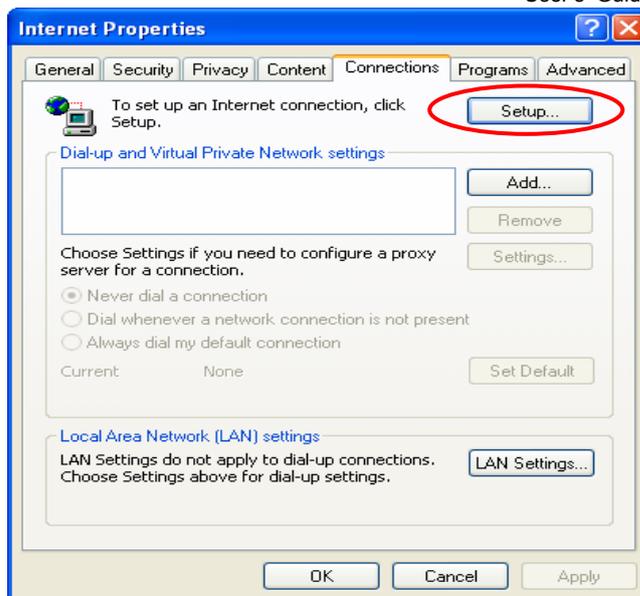


◆ **Windows XP**

1) Choose **Start > Control Panel > Internet Option**.



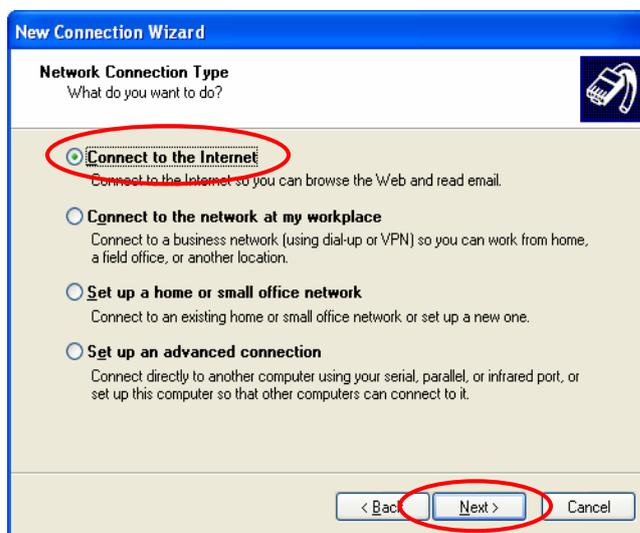
- 2) Choose the “**Connections**” label, and then click **Setup**.



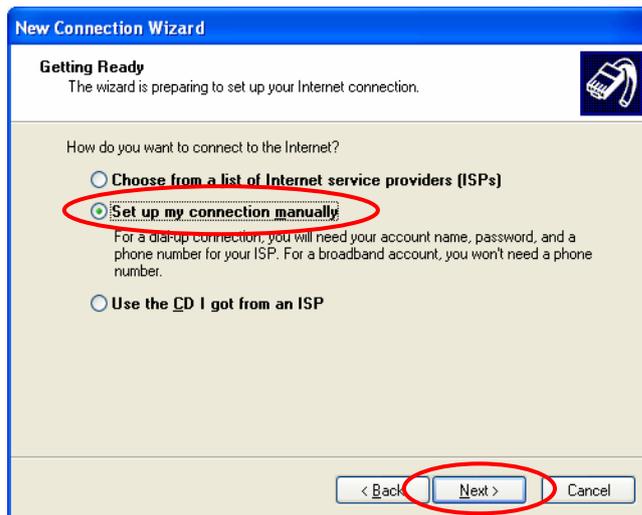
- 3) Click **Next** when **Welcome to the New Connection Wizard** screen appears.



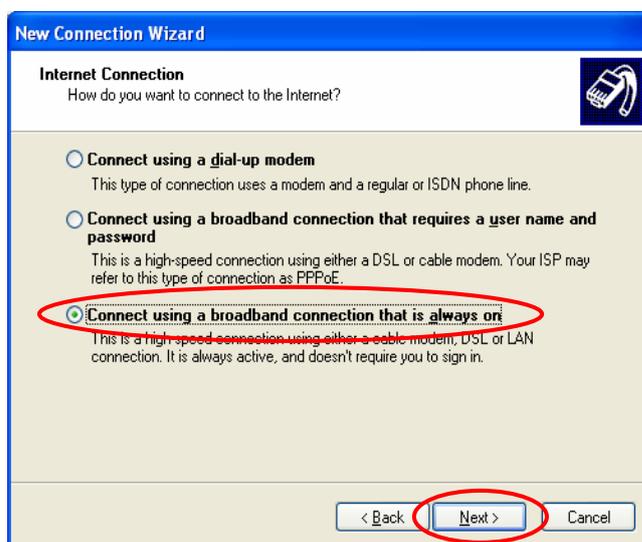
- 4) Choose “**Connect to the Internet**” and then click **Next**.



- 5) Choose “**Set up my connection manually**” and then click **Next**.



- 6) Choose “**Connect using a broadband connection that is always on**” and then click **Next**.



- 7) Finally, click **Finish** to exit the **Connection Wizard**. Now, you have completed the setup.

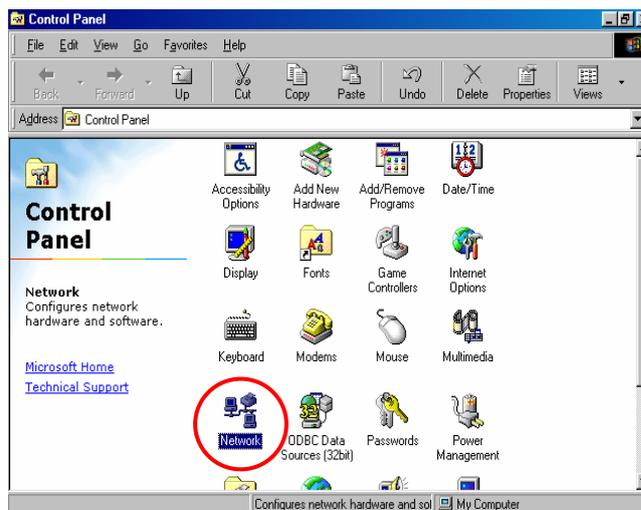


• **TCP/IP Network Setup**

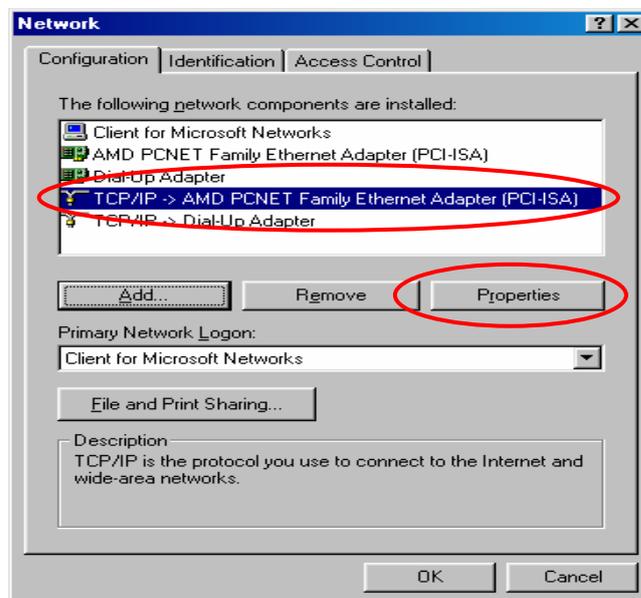
If the operating system of your PC is Windows 95/98/ME/2000/XP, keep the default settings without any change to directly start/restart the system. With the factory default settings, during the process of starting the system, AirLive WIAS-1200G with DHCP function will automatically assign an appropriate IP address and related information for each PC. If the Windows operating system is not a server version, the default settings of the TCP/IP will regard the PC as a DHCP client, and this function is called “**Obtain an IP address automatically**”. If you want to check the TCP/IP setup or use the static IP in the LAN1/LAN2 or LAN3/LAN4 section, please follow the following steps:

◆ **Check the TCP/IP Setup of Window 9x/ME**

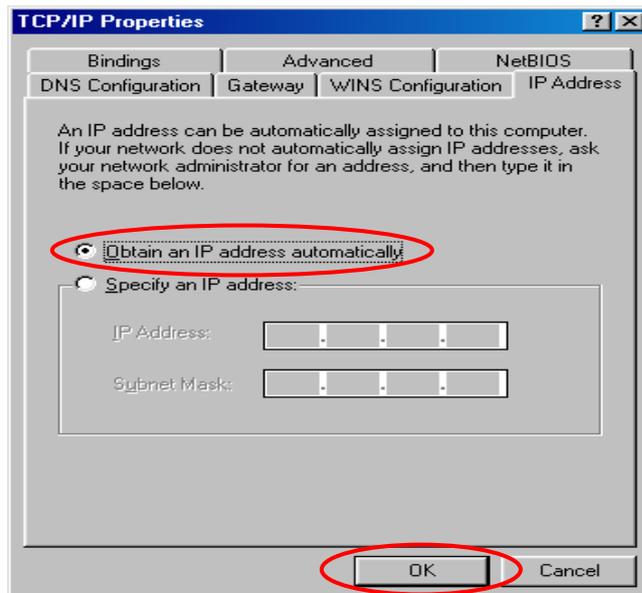
1) Choose **Start > Control Panel > Network**.



2) Choose “**Configuration**” label and select “**TCP/IP > AMD PCNET Family Ethernet Adapter (PCI-ISA)**”, and then click **Properties**.  
Now, you can choose to use **DHCP** or **specific IP address**.



- 3) **Using DHCP:** If you want to use DHCP, please choose “**Obtain an IP address automatically**” on the “**IP Address**” label and click **OK**. This is also the default setting of Windows. Then, reboot the PC to make sure an IP address is obtained from AirLive WIAS-1200G.

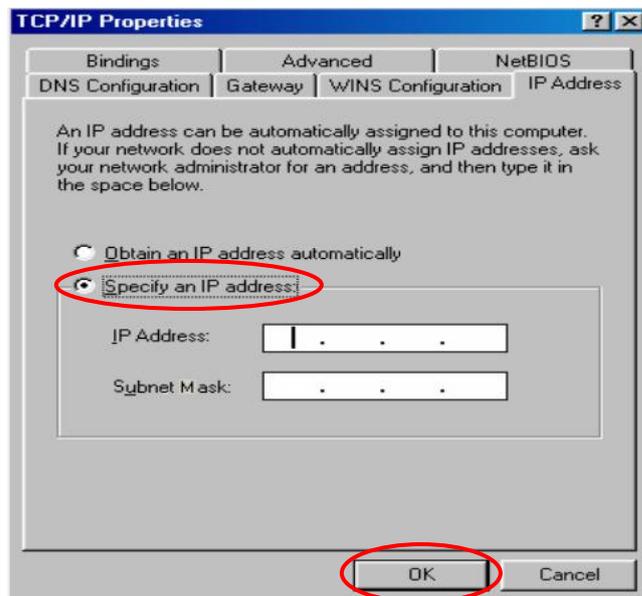


- 4) **Using Specific IP Address:** If you want to use specific IP address, you have to ask the network administrator for the information of AirLive WIAS-1200G: **IP address**, **Subnet Mask**, **New gateway** and **DNS server address**.

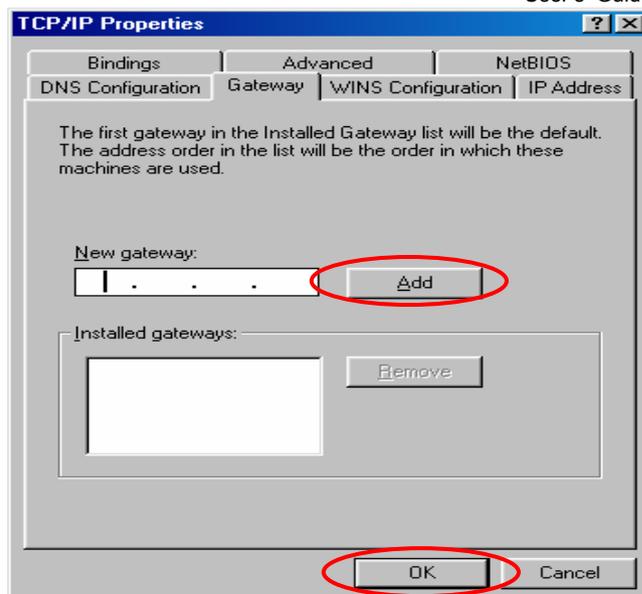
**Note:**

*If your PC has been set up completed, please inform the network administrator before proceeding to the following steps.*

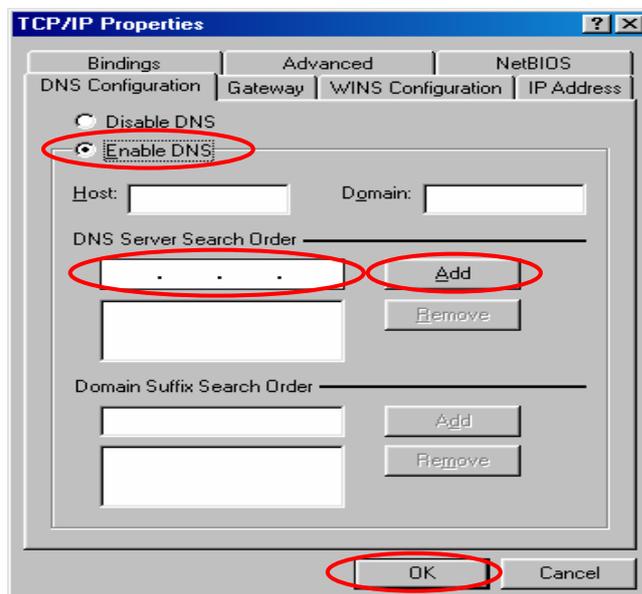
- Please choose “**Specify an IP address**” and enter the information given by the network administrator in “**IP Address**” and “**Subnet Mask**” on the “**IP Address**” label and then click **OK**.



- Choose “**Gateway**” label and enter the gateway address of AirLive WIAS-1200G in the “**New gateway:**” and then click **Add** and **OK**.

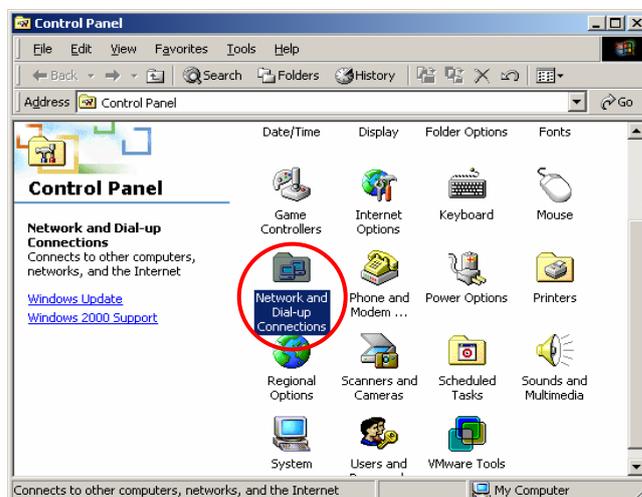


- Choose “**DNS Configuration**” label. If the DNS Server column is blank, please click **Enable DNS** and then enter the DNS address or the DNS address provided by ISP. Then, click **Add** and click **OK**.



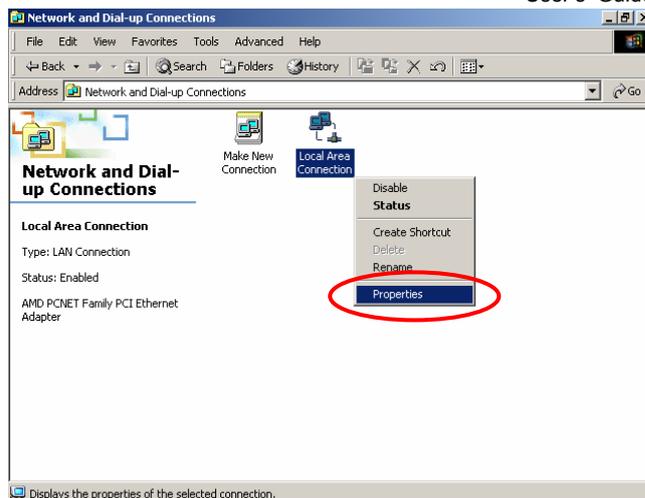
◆ **Check the TCP/IP Setup of Window 2000**

- 1) Select **Start > Control Panel > Network and Dial-up Connections**.

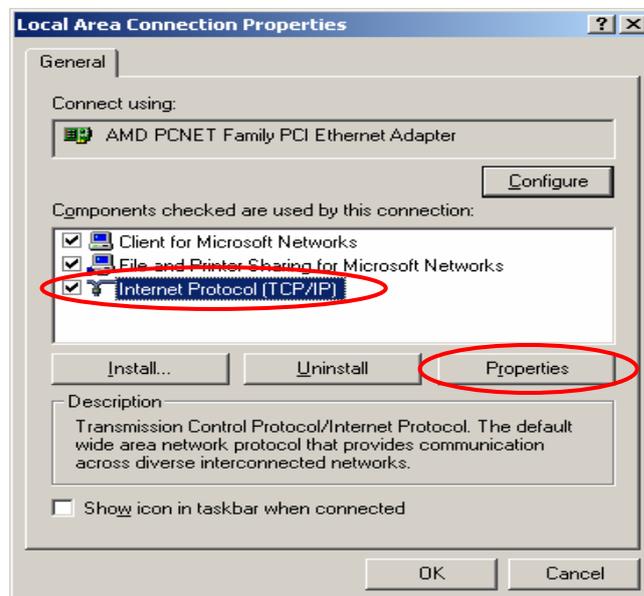




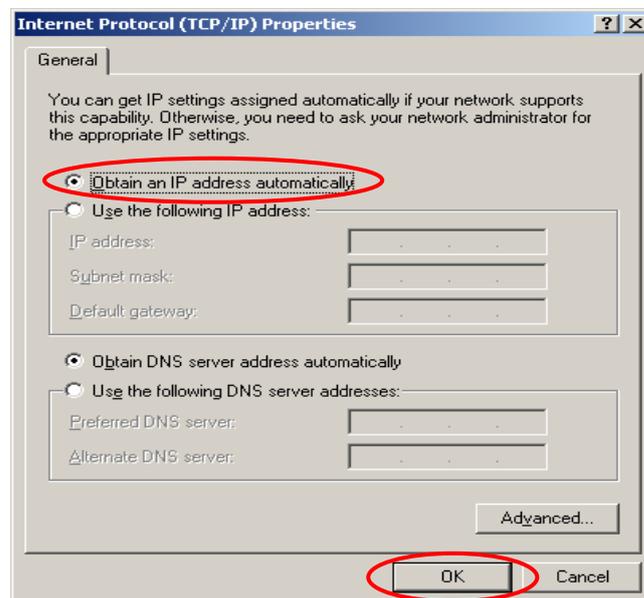
- 2) Click the right button of the mouse on “**Local Area Connection**” icon and then select “**Properties**”.



- 3) Select “**Internet Protocol (TCP/IP)**” and then click **Properties**. Now, you can choose to use **DHCP** or **specific IP address**, please proceed to the following steps.



- 4) **Using DHCP:** If want to use DHCP, please choose “**Obtain an IP address automatically**” and click **OK**. This is also the default setting of Windows. Then, reboot the PC to make sure an IP address is obtained from AirLive WIAS-1200G.

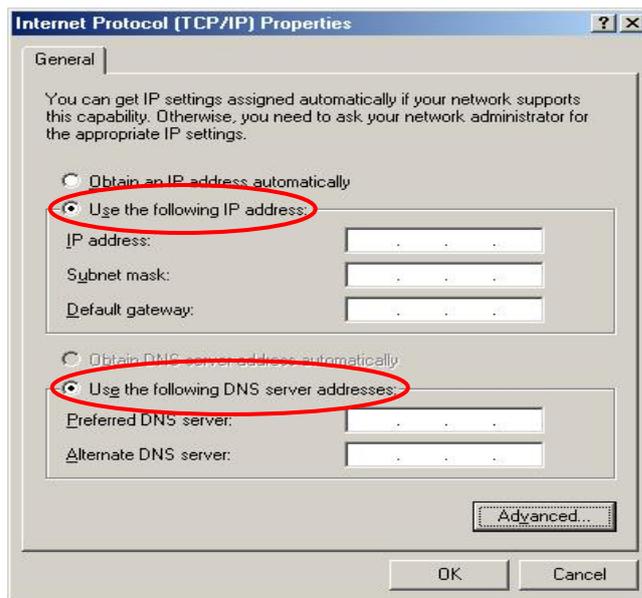


- 5) **Using Specific IP Address:** If you want to use specific IP address, you have to ask the network administrator for the information of the AirLive WIAS-1200G: **IP address**, **Subnet Mask**, **New gateway** and **DNS server address**.

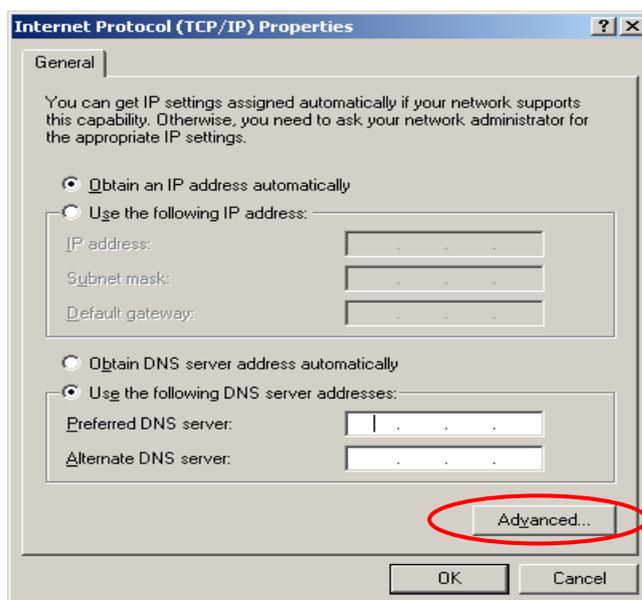
**Note:**

If your PC has been set up completed, please inform the network administrator before proceeding to the following steps.

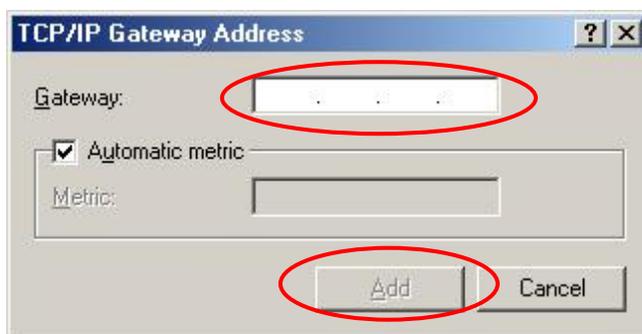
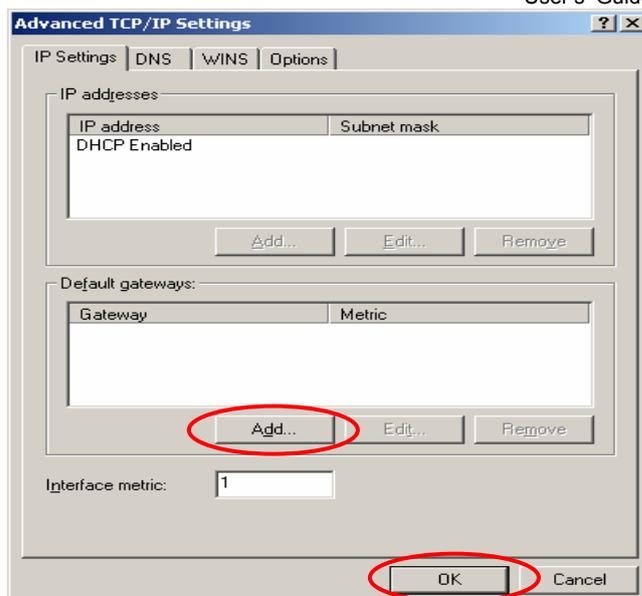
- Please choose “**Use the following IP address**” and enter the information given from the network administrator in “**IP address**” and “**Subnet mask**” If the DNS Server column is blank, please choose “**Using the following DNS server addresses**” and then enter the DNS address or the DNS address provided by ISP and then click **OK**.



- Then, click **Advanced** in the window of “**Internet Protocol (TCP/IP)**”.

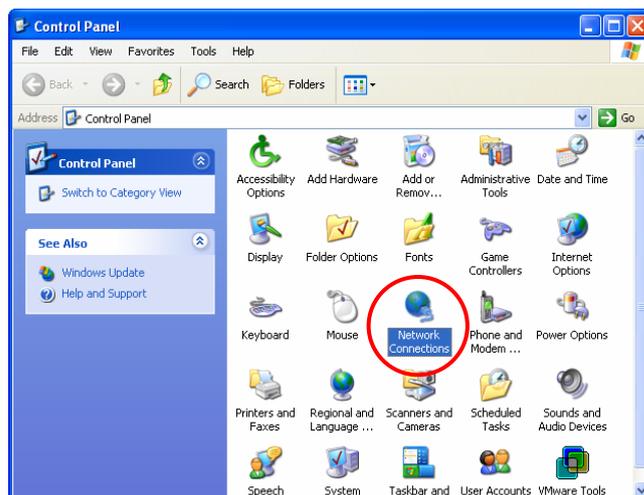


- Choose the “**IP Settings**” label and click **Add** below the “**Default Gateways**” column and the “**TCP/IP Gateway Address**” window will appear. Enter the gateway address of AirLive WIAS-1200G in the “**Gateway**” of “**TCP/IP Gateway Address**” window, and then click **Add**. After back to the “**IP Settings**” label, click **OK** to finish.

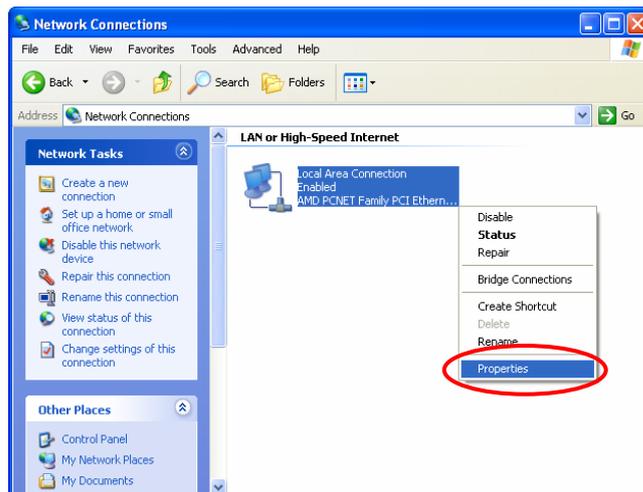


◆ **Check the TCP/IP Setup of Window XP**

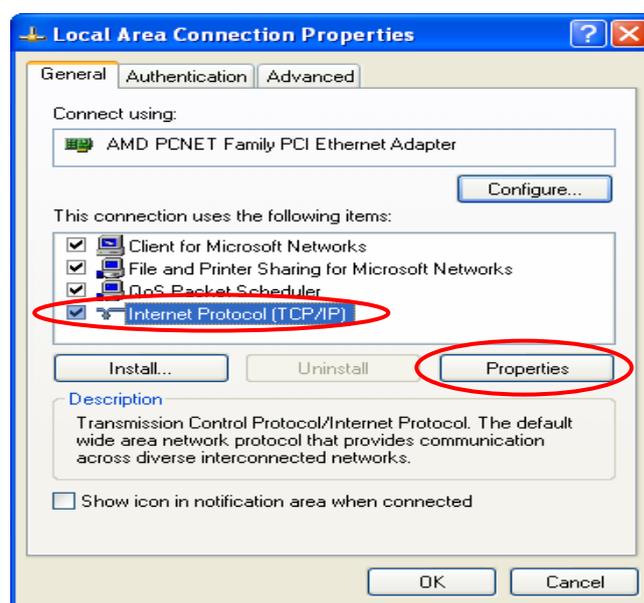
- 1) Select **Start > Control Panel > Network Connection**.



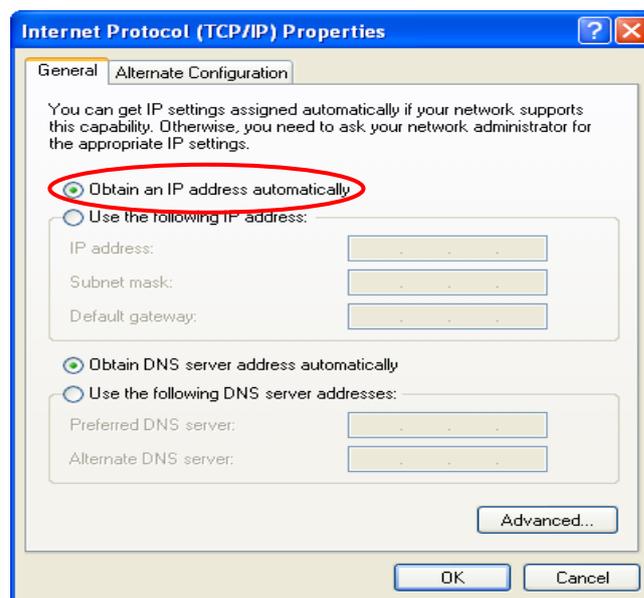
- 2) Click the right button of the mouse on the “**Local Area Connection**” icon and select “**Properties**”



- 3) Select “**General**” label and choose “**Internet Protocol (TCP/IP)**” and then click *Properties*.  
Now, you can choose to use **DHCP** or **specific IP address**, please proceed to the following steps.



- 4) **Using DHCP:** If want to use DHCP, please choose “**Obtain an IP address automatically**” and click *OK*. This is also the default setting of Windows. Then, reboot the PC to make sure an IP address is obtained from AirLive WIAS-1200G.

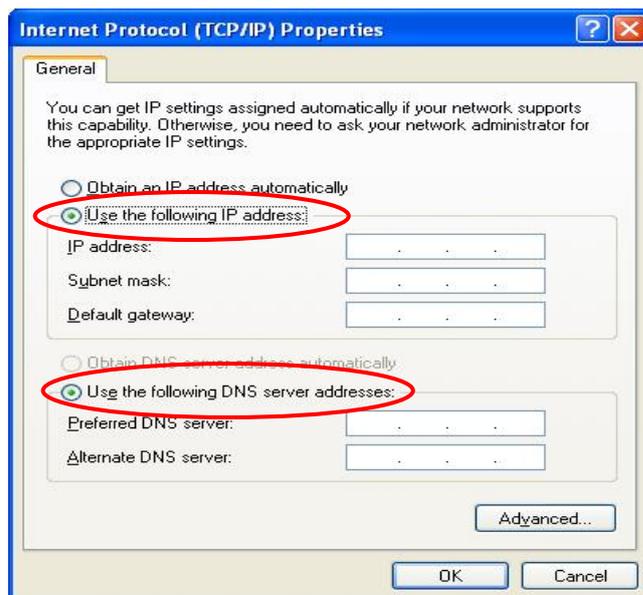


- 5) **Using Specific IP Address:** If want to use specific IP address, you have to ask the network administrator for the information of the AirLive WIAS-1200G: **IP address, Subnet Mask, New gateway and DNS server address.**

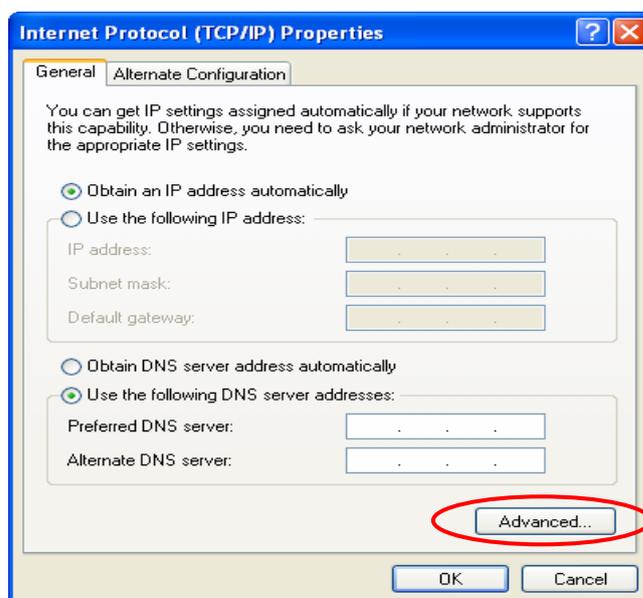
**Note:**

If your PC has been set up completed, please inform the network administrator before proceeding to the following steps.

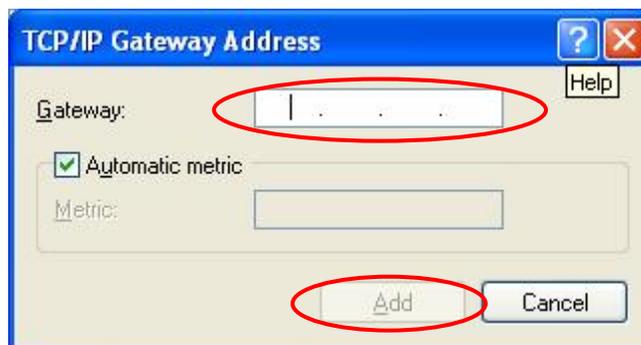
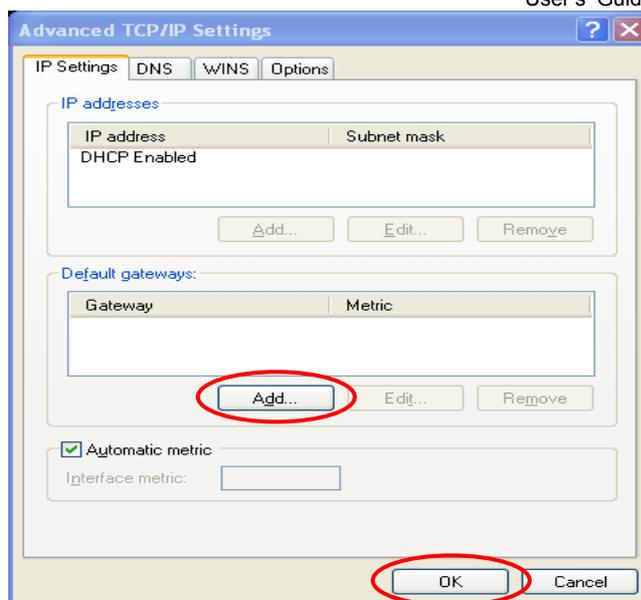
- Please choose “**Use the following IP address**” and enter the information given from the network administrator in “**IP address**” and “**Subnet mask**” If the DNS Server column is blank, please choose “**Using the following DNS server addresses**” and then enter the DNS address or the DNS address provided by ISP and then click **OK**.



- Then, click **Advanced** in the window of “**Internet Protocol (TCP/IP)**”.



- Choose the “**IP Settings**” label and click “**Add**” below the “**Default Gateways**” column and the “**TCP/IP Gateway Address**” window will appear. Enter the gateway address of AirLive WIAS-1200G in the “**Gateway**” of “**TCP/IP Gateway Address**” window, and then click **Add**. After back to the “**IP Settings**” label, click **OK** to finish.



## 2. External Network Access

If all the steps are set properly, AirLive WIAS-1200G can be further connected to the managed network to experience the controlled network access environment. Firstly, connect an end-user device to the network at AirLive WIAS-1200G’s LAN1/LAN2 and set to obtain an IP address automatically. After the network address is obtained at the user end, open an Internet browser and link to any website. Then, the default logon webpage will appear in the Internet browser.

- 1) First, connect a user-end device to LAN3/LAN4 port of the AirLive WIAS-1200G, and set the dynamical access network. After the user end obtains the network address, please open an Internet browser and the default login webpage will appear on the Internet browser. Key in the username and password created in the local user account or the on-demand user account in the interface and then click **Submit** button. Here, we key in



the local user account (e.g. **test@Local** for the username and **test** for the password) to connect the network.

- 2) Login page appearing means AirLive WIAS-1200G has been installed and configured successfully. Now, you can browse the network or surf the Internet!



- 3) If the screen shows “**Sorry, this feature is available for on-demand user only**”, the “**Remaining**” button has been clicked. This button is only for on-demand users. For users other than on-demand users, please click the **Submit** button.



- 4) An on-demand user can enter the username and password in the “**User Login Page**” and click the **Remaining** button to view the remaining time the account.



- 5) When an on-demand user logs in successfully, the following **Login Successfully** screen will appear. There is an extra line showing “**Remaining usage**” and a “**Redeem**” button.



- **Remaining usage:** Show the rest of use time that the on-demand user can surf Internet.
- **Redeem:** When the remaining time or data size is insufficient, the user has to pay for adding credit at the counter, and then, the user will get a new username and password. After clicking the **Redeem** button, you will see the following screen. Please enter the new username and password you got and click **Redeem** button to merge the two accounts and add up the available use time and data size by the system, and then, you will see the total available use time and data size after adding credit.



**Note:** The maximum session time/data transfer is 24305 days/9,999,999 Mbyte. If the redeem amount exceeds this number, the system will automatically reject the redeem process.

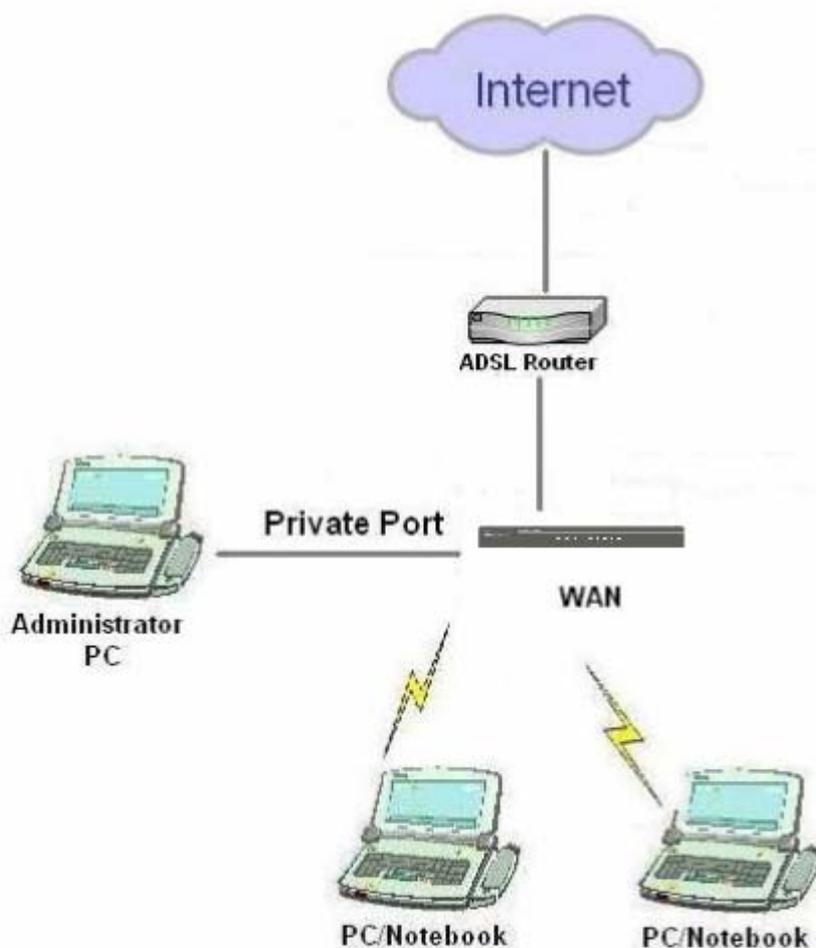


## Appendix I – Common Settings

AirLive WIAS-1200G is an all-in-one product specially designed for small wireless network environment. It integrates “**Access Control**” and “**Wireless Network Access**” into one system to fulfill the needs in Hotspot and SMB. In the Quick Installation Guide, two common scenarios are described below that allows you to use the **Configuration Wizard** utility to speed up the configuration process of AirLive WIAS-1200G. Please refer to section **1. Hotspot** for hotspot environment and section **2. SMB** for small & medium size business environment.

### 1. Hotspot

AirLive WIAS-1200G used in the hotspot environment is usually connected to the Internet through ADSL. Please refer to the following diagram on connecting AirLive WIAS-1200G with an ADSL modem.

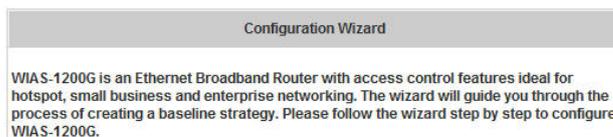


After completing the hardware installation and successfully logging into the web management interface, AirLive WIAS-1200G can then be configured from the web browser. In the hotspot environment, it is convenient to use the built-in authentication server to quickly setup the services. One example is to set **Local User** authentication method in the **Configuration Wizard** for employees and for visitors.

Click the **System Configuration** from the top menu and the **System Configuration** page will appear. Then, click **Configuration Wizard**.

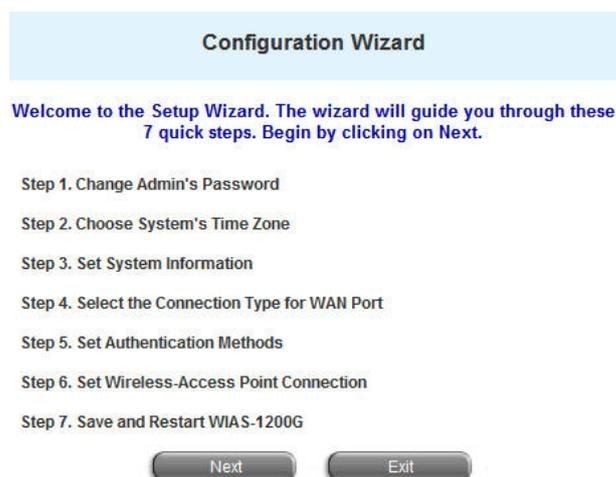


Click **Run Wizard** to begin the **Configuration Wizard**.



The **Configuration Wizard** will appear in a separated window.

Click **Next** to begin.



### Step 1. Change Admin's Password

Enter a new password for the admin account and retype it in the Verify Password field (maximum characters are twenty and no spaces are allowed).

Click **Next** to continue.

### Step 2. Choose System's Time Zone

Select a proper time zone via the drop-down menu.

Click **Next** to continue.

### Step 3. Set System Information

- **Home Page:** Enter the URL that clients should be initially redirected to after successfully authenticated to the network.
- **NTP Server:** Enter the URL of the external time server for AirLive WIAS-1200G time synchronization or use the default.
- **DNS Server:** Enter a DNS Server provided by your ISP (Internet Service Provider). Contact your ISP if you are not sure of the DNS IP Address.

Click **Next** to continue.

### Step 1. Change Admin's Password

You may change the Admin's account password by entering in a new password. Click Next to continue.

New Password:  \*  
Verify Password:  \*

### Step 2. Choose System's Time Zone

Select the appropriate time zone for the system. Click Next to continue.

(GMT+08:00)Taipei

### Step 3. Set System Information

Enter System Information. Click Next to continue.

Home Page:  \*  
(e.g. http://www.airlive.com/)

NTP Server:  \*  
(e.g. tock.usno.navy.mil)

DNS Server:  \*

#### Step 4. Select the Connection Type for WAN Port

There are three types of WAN connection types: **Static IP Address**, **Dynamic IP Address** and **PPPoE Client**. Select a proper Internet connection type.

PPPoE connection type is chosen as an example, so select **PPPoE Client**. Then, click **Next** to continue.

#### Step 4 (Cont). Set PPPoE Client's Information

Enter the **Username** and **Password** provided by your ISP. Click **Next** to continue.

#### Step 5. Select Authentication Methods

Please specify the postfix name for this authentication method. The **Postfix** field (e.g. Local) will be used as the postfix name (e.g. username@Local). A policy can be chosen to apply to this authentication method. An authentication method has to be selected from one of the five options appeared in this window (Local User is selected for this example). Local User is an authentication method that uses the built-in user database supported by AirLive WIAS-1200G.

Click **Next** to continue.

#### Step 4. Select the Connection Type for WAN Port

Select the connection type for WAN port. Click Next to continue.

- Static IP Address Choose it to set static IP address.
- Dynamic IP Address Choose it to obtain an IP address automatically. (For most cable modem users.)
- PPPoE Client Choose it to set the PPPoE Client's Username and Password. (For most DSL users.)

Back Next Exit

#### Step 4 (Cont). Set PPPoE Client's Information

Choose it to set the PPPoE Client's Username and Password. (For most DSL users.)

Username:

Password:

Back Next Exit

#### Step 5. Set Authentication Methods

Select a default User Authentication Method. Click Next to continue.

Postfix:   
(its postfix name.)

Policy:

- Local User  LDAP
- POP3  NT Domain
- RADIUS

Back Next Exit

### Step 5 (Cont). Add User

A new user can be added to the local user database. To add a user here, enter the **Username** (e.g. test), **Password** (e.g. test), **and MAC** (optional). Assign a policy to add this particular local user (or use the default). Upon completing to add a user, more users can be added to this authentication method by clicking the **ADD** button.

Click **Next** to continue.

**Step 5 (Cont). Add User**

Click "ADD" button to add Local User. Click Next to continue.

Username:

Password:

MAC:  (XX:XX:XX:XX:XX:XX)

Policy: None

### Step 6. Set Wireless – Access Point Connection

- **SSID:** Enter a SSID (up to 32 characters) for the system. The default is **airlive**. **SSID (Service Set Identifier)** is a unique identifier used for the wireless client's devices to associate with the built in AP of AirLive WIAS-1200G.
- **Transmission Mode:** AirLive WIAS-1200G supports two transmission modes, **802.11b** and **802.11 (b+g)**. Select the appropriate transmission mode to work with the wireless clients in the network.
- **Channel:** If the default channel is occupied by many other APs, it is necessary to select another channel from the **Channel** field for a better performance.

Click **Next** to continue.

**Step 6. Set Wireless Access-Point Connection**

Enter the SSID name and channel number to be used for the Wireless Access-Point. Click Next to continue.

SSID:

Transmission Mode: 802.11(b+g)

Channel: 1

### Step 7. Save and Restart AirLive WIAS-1200G

Click **Restart** to save the current settings and restart AirLive WIAS-1200G. The Setup Wizard is now completed.

**Step 7. Save and Restart WIAS-1200G**

The Setup Wizard has completed. Click on Back to modify changes or mistakes. Click Restart to save the current settings and reboot.

During AirLive WIAS-1200G restarting, a **“Restarting now. Please wait for a moment...”** Message will appear on the screen. Please do not interrupt AirLive WIAS-1200G until the **Configuration Wizard** window has disappeared. Then the Administrator Login page will appear. This indicates that the restart process has completed.

**Now, the basic configuration for Hotspot environment has been finished!**

If all the steps are done properly, AirLive WIAS-1200G can be further connected to the managed network to experience the controlled network access environment. Firstly, connect a client's networking device to Public Port or Wireless interface of WIAS-1200G to obtain an IP address automatically. After the IP address is obtained, launch an Internet browser and link to any website. The User Login Page will appear.

Key in the username and password created previously by Setup Wizard in the local user database (e.g. **test@Local** for the username and **test** for the password) or from on-demand user account, click **Submit** to connect to the network.

**Congratulation!**

Login success page appearing means AirLive WIAS-1200G has been installed and configured successfully. Now, you can browse the network or surf on the Internet!

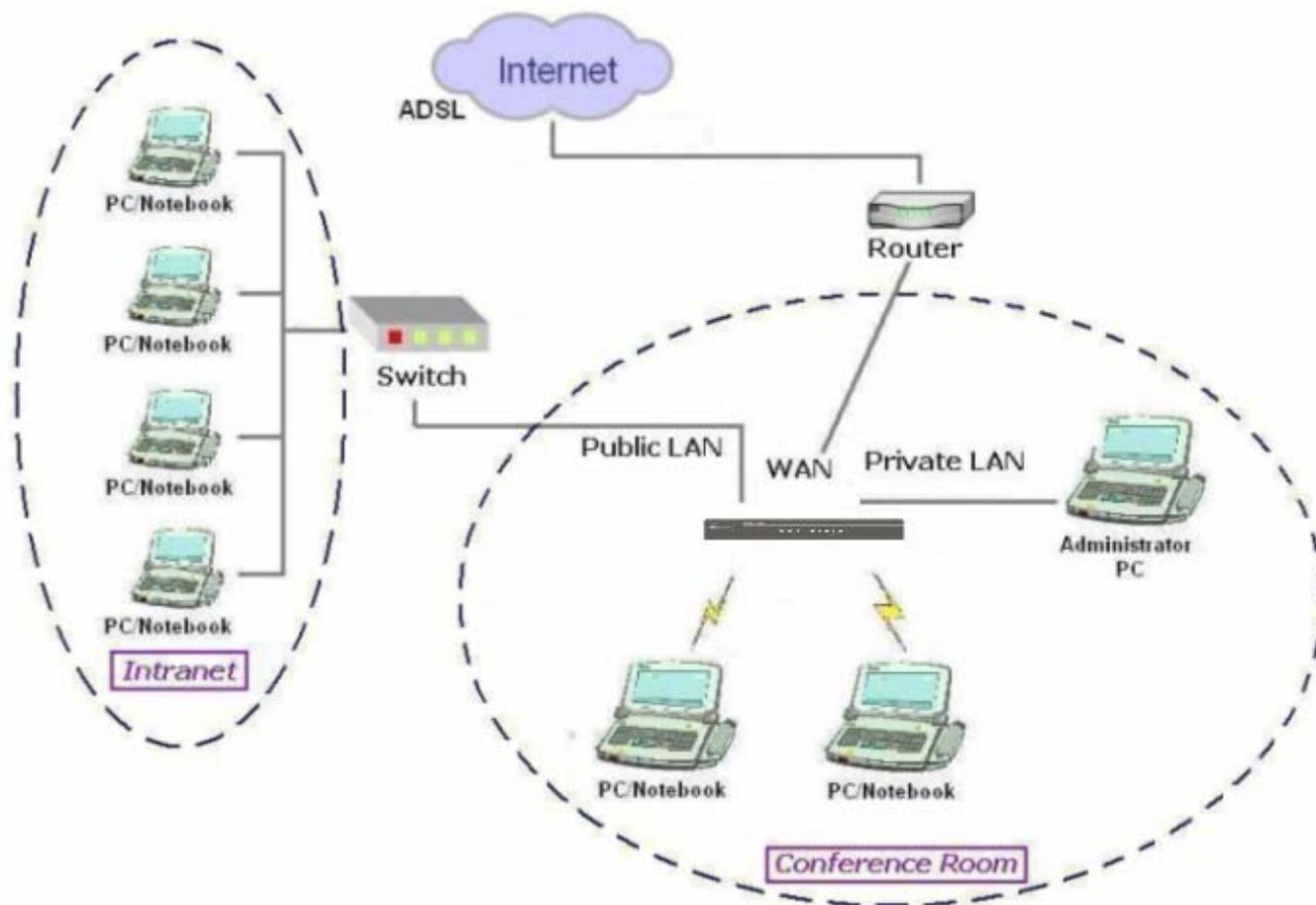


Restarting now. Please wait for a moment...



## 2. SMB (Small & Medium Size Business)

AirLive WIAS-1200G used in the enterprise environment (mostly small and medium size business) is usually connected Internet through ADSL. Please refer to the following figure on connecting AirLive WIAS-1200G with ADSL modem.

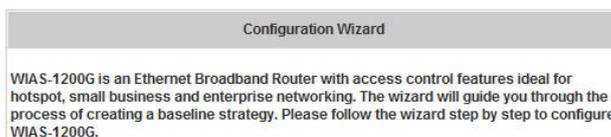


After completing the hardware installation and successfully logging into the web management interface, AirLive WIAS-1200G can then be configured from the web browser. Please refer to the following steps.

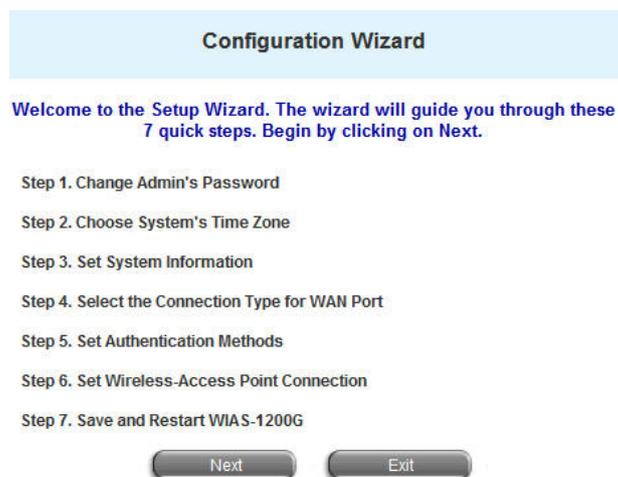
Click the **System Configuration** from the top menu and the **System Configuration** page will appear. Then, click on **Configuration Wizard**.



Click **Run Wizard** to begin the **Configuration Wizard**.



The **Setup Wizard** will appear in a separated window.  
Click **Next** to begin.





### Step 1: Change Admin's Password

Enter a new password for the admin account and retype it in the Verify Password field (maximum characters are twenty and no spaces are allowed).

Click **Next** to continue.

### Step 2: Choose System's Time Zone

Select a proper time zone via the drop-down menu.

Click **Next** to continue.

### Step 3: Set System Information

- **Home Page:** Enter the URL that clients should be initially redirected to after successfully authenticated.
- **NTP Server:** Enter the URL of the external time server for AirLive WIAS-1200G time synchronization or use the default.
- **DNS Server:** Enter a DNS Server provided by your ISP (Internet Service Provider). Contact your ISP if you are not sure of the DNS IP Address.

Click **Next** to continue.

### Step 1. Change Admin's Password

You may change the Admin's account password by entering in a new password. Click Next to continue.

New Password:  \*  
Verify Password:  \*

### Step 2. Choose System's Time Zone

Select the appropriate time zone for the system. Click Next to continue.

(GMT+08:00)Taipei ▾

### Step 3. Set System Information

Enter System Information. Click Next to continue.

Home Page:  \*  
(e.g. http://www.airlive.com/)

NTP Server:  \*  
(e.g. tock.usno.navy.mil)

DNS Server:  \*

#### Step 4: Select the Connection Type for WAN Port

Select a proper Internet connection. **Static IP Address** is chosen as the example for SMB scenario. Static IP Address is an assigned IP address from the ISP used to connect to the Internet. Click **Next** to continue.

#### Step 4 (Cont). Set WAN Port's Static IP Address

Enter the IP Address, Subnet Mask and Default Gateway provided by your ISP.  
Click **Next** to continue.

#### Step 5: Set Authentication Methods

Please specify the postfix name for this authentication method. The **Postfix** field (e.g. NT Domain) will be used as the postfix name (e.g. username@NTDomain). An authentication method has to be selected from one of the five options appeared in this window (NT Domain is selected for this setup example). NT Domain is an authentication method that uses the external NT server for authentication.  
Click **Next** to continue.

#### Step 4. Select the Connection Type for WAN Port

Select the connection type for WAN port. Click **Next** to continue.

- Static IP Address** Choose it to set static IP address.
- Dynamic IP Address** Choose it to obtain an IP address automatically. (For most cable modem users.)
- PPPoE Client** Choose it to set the PPPoE Client's Username and Password. (For most DSL users.)

Back Next Exit

#### Step 4 (Cont). Set WAN Port's Static IP Address

Click **Next** to continue.

IP Address:  \*

Subnet Mask:  \*

Default Gateway:  \*

Back Next Exit

#### Step 5. Set Authentication Methods

Select a default User Authentication Method. Click **Next** to continue.

Postfix:  \*  
(Its postfix name.)

Policy:

Local User  LDAP

POP3  **NT Domain**

RADIUS

Back Next Exit

### Step 5 (Cont). NT Domain

When NT Domain User is selected, please enter the NT Domain Server information for **Server IP Address**, and enable/disable **Transparent Login**. Click **Next** to continue.

### Step 6: Set Wireless – Access Point Connection

- **SSID:** Enter a SSID (up to 32 characters) for the system. The default is **airLive. SSID (Service Set Identifier)** is a unique identifier used for the wireless client's device to associate with the built in AP of AirLive WIAS-1200G.
  - **Transmission Mode:** AirLive WIAS-1200G supports two transmission modes, **802.11b** and **802.11 (b+g)**. Select the appropriate transmission mode to work with the wireless clients in the network.
  - **Channel:** If the default channel is occupied by many other APs, it is necessary to select another channel from the **Channel** field for a better performance.
- Click **Next** to continue.

### Step 7: Save and Restart AirLive WIAS-1200G

Click **Restart** to save the current settings and restart AirLive WIAS-1200G. The Setup Wizard is now completed.

### Step 5 (Cont). NT Domain

Configure NT Domain Server information. Click Next to continue.

Server IP Address:  \*

Transparent Login

Back

Next

Exit

### Step 6. Set Wireless Access-Point Connection

Enter the SSID name and channel number to be used for the Wireless Access-Point. Click Next to continue.

SSID:  \*

Transmission Mode

Channel

Back

Next

Exit

### Step 7. Save and Restart WIAS-1200G

The Setup Wizard has completed. Click on Back to modify changes or mistakes. Click Restart to save the current settings and reboot.

Back

Restart

Exit

During AirLive WIAS-1200G restarting, a **“Restarting now. Please wait for a moment....”** message will appear on the screen. Please do not interrupt AirLive WIAS-1200G until the **Configuration Wizard** window has disappeared. Then the Administrator Login page will appear. This indicates that the restart process has completed.

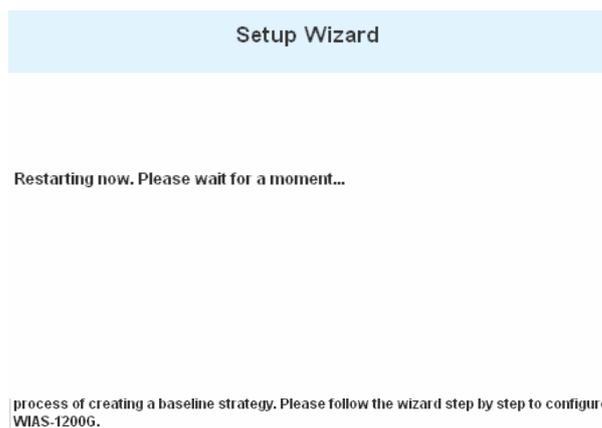
**Now, the basic configuration for SMB environment has been finished!**

If all the steps are done properly, AirLive WIAS-1200G can be further connected to the managed network to experience the controlled network access environment. Firstly, connect a client's networking device to Public Port or Wireless Interface of WIAS-1200G to obtain an IP address automatically. After the IP address is obtained, launch an Internet browser and link to any website. The User Login Page will appear.

Key in the username and password (e.g. **test@NTDomain** for the username and **test** for the password) created in the NT Domain server user account in the interface and then click **Submit** to connect the network.

### **Congratulation!**

Login success page appearing means AirLive WIAS-1200G has been installed and configured successfully. Now, you can browse the network or surf on the Internet!



Run Wizard

