

Air Live[®]

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 must be installed and operated in accordance with provided instructions and the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter. End-users and installers must be provided with antenna exposure compliance.

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

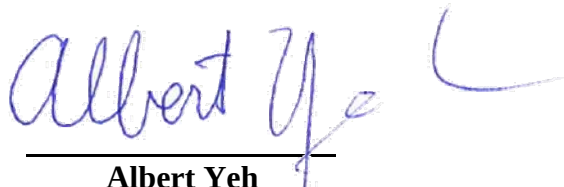
In accordance with 89/336 EEC-EMC Directive and 1999/5 EC-R & TTE Directive

<u>Clause</u>	<u>Description</u>
■ 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 (2005-09)	Electromagnetic compatibility and Radio spectrum Matters (ERM); Electromagnetic compatibility(EMC) standard for radio equipment and
■ EN 301 489-17 V1.6.1 (2005-09)	Services; Part 17 : Specific conditions for wideband data and 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
cs Česky [Czech]	OvisLink Corp. tímto prohlašuje, že tento WIAS-1200G je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.	lt Lietuvių [Lithuanian]	Šiuo OvisLink Corp. deklaruoja, kad šis WIAS-1200G atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
da 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.	nl 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.
de 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.	mt 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.
et Eesti [Estonian]	Käesolevaga kinnitab OvisLink Corp. seadme WIAS-1200G vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.	hu Magyar [Hungarian]	Alulírott, OvisLink Corp nyilatkozom, hogy a WIAS-1200G megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EC irányelv egyéb előírásainak.
en 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.	pl Polski [Polish]	Niniejszym OvisLink Corp oświadcza, że WIAS-1200G jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
es 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.	pt Português [Portuguese]	OvisLink Corp declara que este WIAS-1200G está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
el 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/ΕΚ.	sl Slovensko [Slovenian]	OvisLink Corp izjavlja, da je ta WIAS-1200G v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
fr 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	sk Slovensky [Slovak]	OvisLink Corp týmto vyhlasuje, že WIAS-1200G spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
it 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.	fi 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
lv Latviski [Latvian]	Ar šo OvisLink Corp. deklarē, ka WIAS-1200G atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.	is 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.
sv 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.	no 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 licensee 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:
a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
b) 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 to no charge to all third parties under the terms of this License.
c) 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:
a) 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
b) 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,
c) 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

1.	<i>Before You Start</i>	1
1.1	Audience	1
1.2	Document Conventions	1
2.	<i>System Overview</i>	2
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
3.	<i>Base Installation</i>	7
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
4.	<i>Web Interface Configuration</i>	21
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
Appendix A – Console Interface		106
Appendix B – Accepting Payments via Authorize.Net		109
Appendix C – Accepting Payments via PayPal		115
Appendix D – Examples of Making Payments for End Users		122
Appendix E – Proxy Setting for Hotspot		128
Appendix F – Proxy Setting for Enterprise.....		131
Appendix G – Disclaimer for On-Demand Users		136
Appendix H – Network Configuration & External Network Access		145
Appendix I – Common Settings.....		161

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**

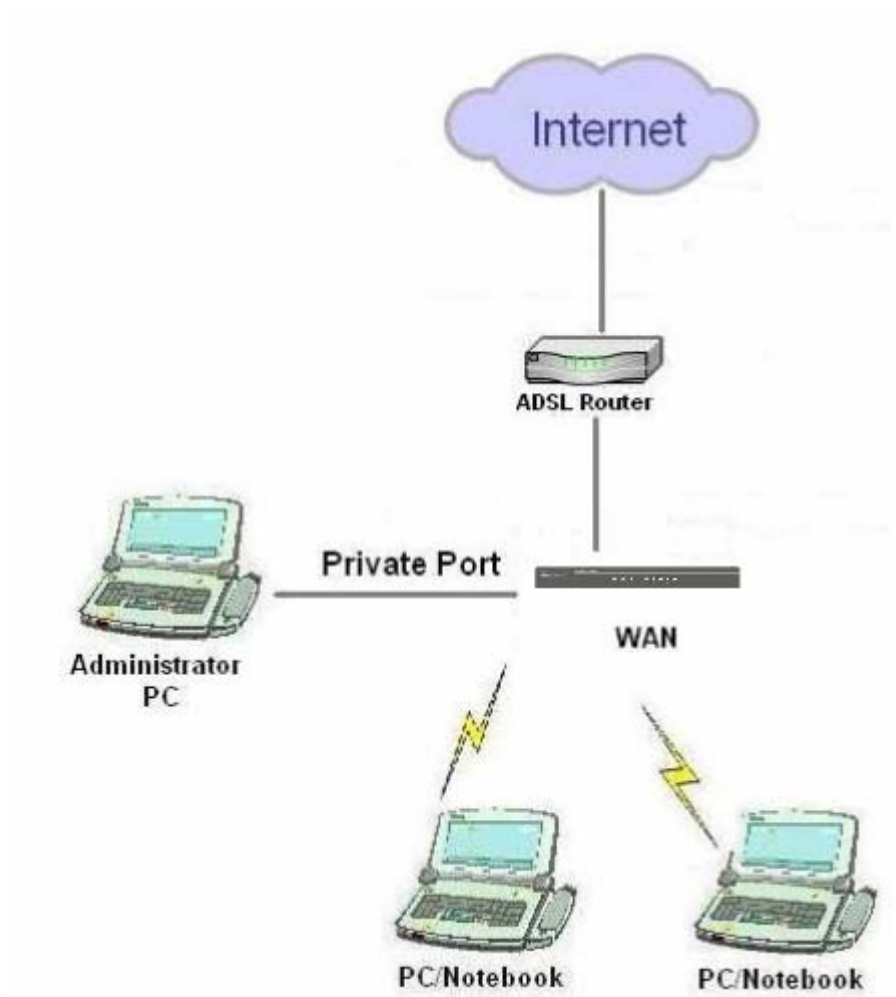
AirLive WIAS-1200G is easy to install. All of the functions of the system can be performed with a simple few clicks. The full web-based management interface allows users to operate and manage the system online via browsers. Users can easily log on to the system via browsers without any additional software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

- **Integrating the Existing User Password Database**

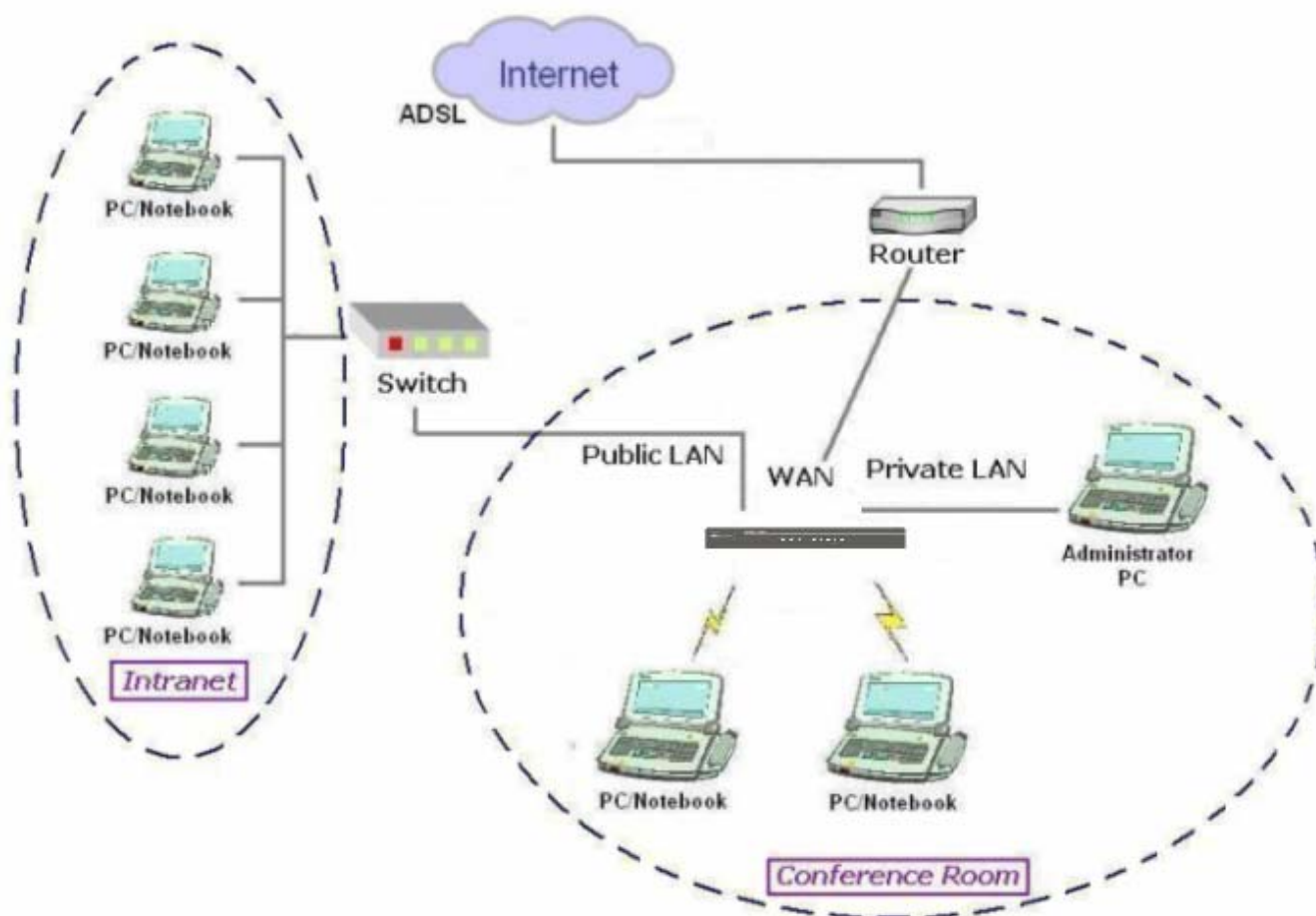
In general, most organizations use specific database system to centrally manage user passwords. AirLive WIAS-1200G supports POP3 (+SSL), RADIUS, LDAP and NT Domain external authentication methods, and allows integration of the current user password database. This system also provides a built-in local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

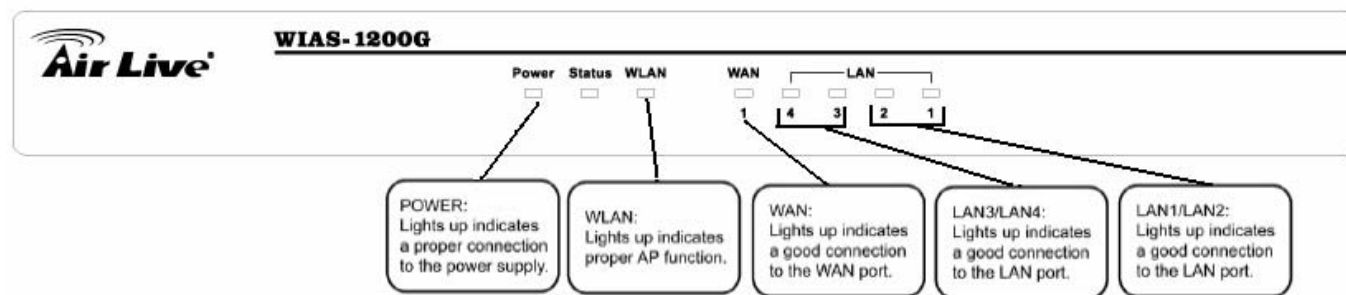
The standard package of AirLive WIAS-1200G includes:

- 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

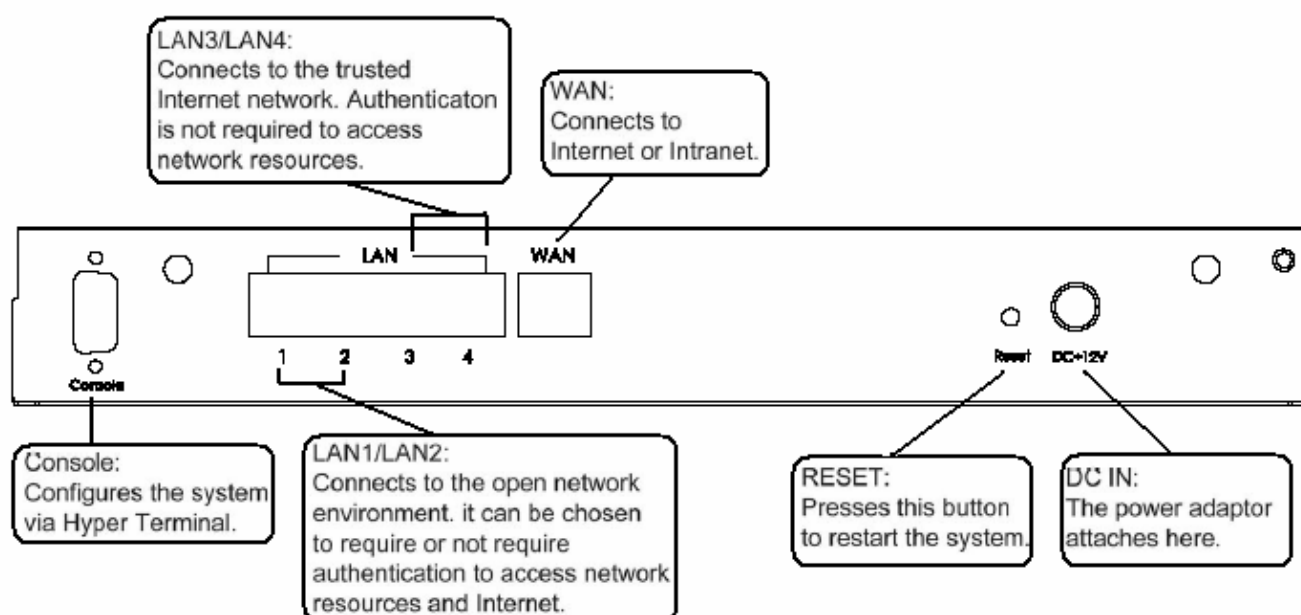
Note: *Using a power supply with different voltage rating will damage this product.*

3.1.3 Panel Function Descriptions

Front Panel



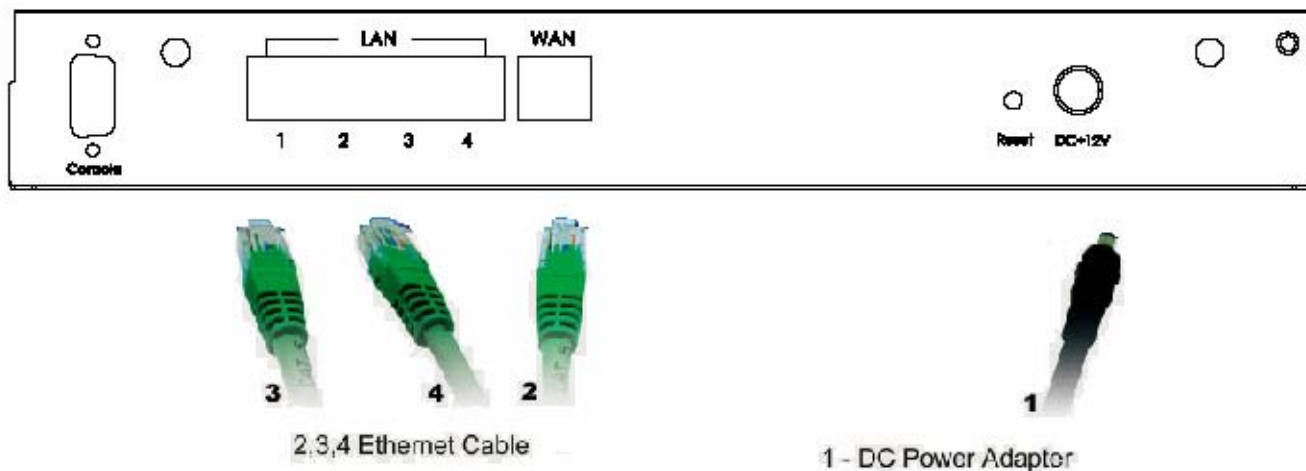
Rear Panel



- **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:



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.

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

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

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.

On-demand User Server Configuration

On-demand User Server Configuration	
Server Status	Enabled
Postfix	AirLive *(e.g. airlive, Max: 40 char)
Receipt Header 1	Welcome! (e.g. Welcome!)
Receipt Header 2	
Receipt Footer	Pis wait for login page (e.g. Thank You!)
Printer Baud Rate	9600
Monetary Unit	☐ none ☐ \$ USD ☐ £ GBP ☒ € EUR ☐ (Input other desired monetary unit, e.g. AU)
WLAN ESSID	airlive (e.g. airlive)
Wireless Key	
Remark	(for customer)
Billing Notice Interval	☒ 10mins ☐ 15mins ☐ 20mins
Twin Ticket	☐ Enable ☒ Disable

[Users List](#)
[Billing Configuration](#)
[Create On-demand User](#)
[Billing Report](#)
[Payment](#)

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.

Billing Configuration

Plan	Status	Type	Expiration Time	Valid Duration	Policy Name	Price
1	☒ Enable ☐ Disable	☐ Data ☒ Time	Mbyte 3 days hrs 2 mins 0	5 days	Policy A	20
2	☐ Enable ☒ Disable	☐ Data ☐ Time	Mbyte hrs mins	days	None	
3	☐ Enable ☒ Disable	☐ Data ☐ Time	Mbyte hrs mins	days	None	
4	☐ Enable ☒ Disable	☐ Data ☐ Time	Mbyte hrs mins	days	None	

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

Policy Configuration

Select Policy: Policy A

Firewall Profile	Setting
Specific Route Profile	Setting
Schedule Profile	Setting
Total Bandwidth	8 Mbps
Individual Maximum Bandwidth	256 Kbps
Individual Request Bandwidth	128 Kbps

Login with operator account:

1. Click Create to create a new account.

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
10	N/A	Disabled	Create

2. Click Printout to print ticket.

Username	U483@airlive
Password	V84K3NCS
Price	20
Usage	2 hrs 0 mins
ESSID : airtlive	
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
System Configuration		Y	--	--
User Authentication	Authentication Configuration	Y	Y	--
	Black List Configuration	Y	Y	--
	Policy Configuration	Y	--	--
	Guest User Configuration	Y	Y	--
	Additional Configuration	Y	Y	--
Network Configuration		Y	--	--
Utility		Y	--	--
Status		Y	--	--

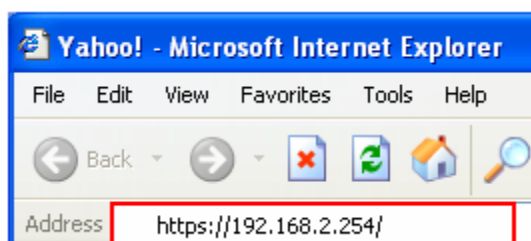
3.2.2 Configuration Wizard

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

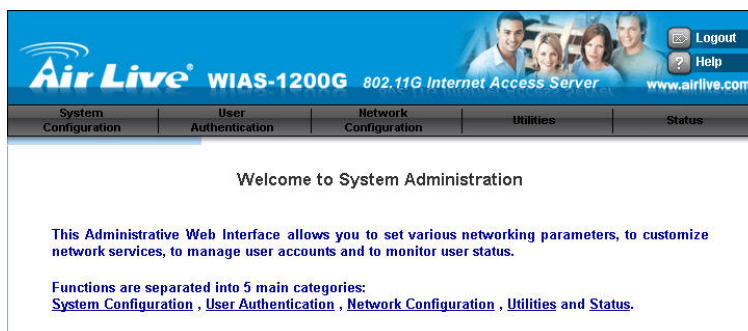
1. Use the network cable of the 10/100BaseT to connect PC to the LAN3/LAN4 port, and then start a browser (such as Microsoft IE). Next, enter the gateway address for that port, the default is <https://192.168.2.254/>. Next, the Administrator Login Page will appear on the browser. Enter “**admin**”, the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



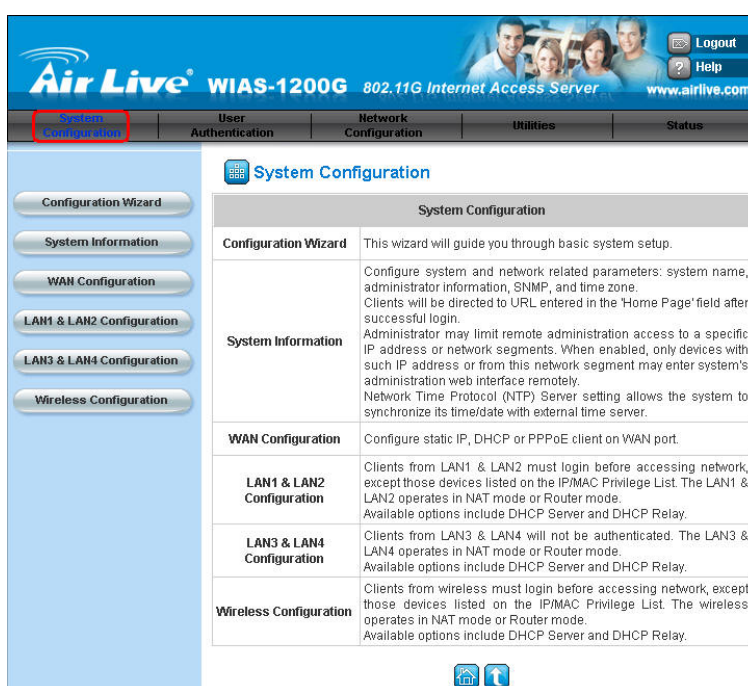
Note:

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: (XXXXXXXXXX)

Policy: None ▼

Back

Next

Exit

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 ▼ *

Back

Next

Exit

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)

Back

Next

Exit

➤ **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

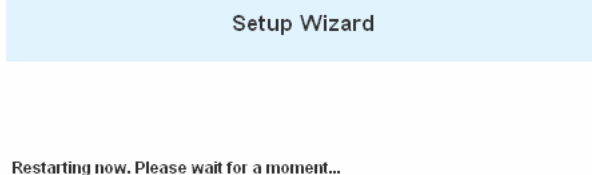
The Setup Wizard has completed. Click on **Back** to modify changes or mistakes. Click **Restart** to save the current settings and reboot.

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.



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**.

The screenshot displays the web interface of the AirLive WIAS-1200G. At the top, there is a navigation bar with five tabs: **System Configuration** (highlighted with a red box), **User Authentication**, **Network Configuration**, **Utilities**, and **Status**. Below the navigation bar, on the left side, is a vertical menu with buttons for **Configuration Wizard**, **System Information**, **WAN Configuration**, **LAN1 & LAN2 Configuration**, **LAN3 & LAN4 Configuration**, and **Wireless Configuration**. The main content area is titled **System Configuration** and contains a table with the following data:

System Configuration	
Configuration Wizard	This wizard will guide you through basic system setup.
System Information	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.
WAN Configuration	Configure static IP, DHCP or PPPoE client on WAN port.
LAN1 & LAN2 Configuration	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.
LAN3 & LAN4 Configuration	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.
Wireless Configuration	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.

At the bottom of the main content area, there are two icons: a home icon and a refresh icon.

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**.

The screenshot shows the introduction screen of the Configuration Wizard. It has a title bar that says **Configuration Wizard**. The main text reads: "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. (It'll appear when Internet connection fails.)
Device Name	(FQDN for this device)
Home Page	☒ Enable ☐ Disable http://www.airlive.com/ (e.g. http://www.airlive.com/)
Access History IP	(e.g. 192.168.2.1)
Remote Management IP	☐ Enable ☒ Disable
SNMP	☐ Enable ☒ Disable
User Logon SSL	☒ Enable ☐ Disable
Time	Device Time : 2007/06/08 06:34:05 Time Zone: (GMT+08:00)Taipei ☒ NTP Enable NTP Server 1: tock.usno.navy.mil *(e.g. tock.usno.navy.mil) NTP Server 2: ntp1.fau.de NTP Server 3: clock.cuhk.edu.hk NTP Server 4: ntps1.pads.ufrj.br NTP Server 5: ntp1.cs.mu.OZ.AU ☐ 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	0	0

On-demand History : 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.

Time	Device Time : 2005/03/03 10:43:08	
	☐ NTP Enable	
	☒ Set Device Date and Time	
	Year:	Month: Day:
	Hour:	Minute: Second:

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**.

WAN Configuration	
WAN Port	☒ Static IP Address IP Address: * Subnet Mask: * Default Gateway: * Preferred DNS Server: 168.95.1.1 * Alternate DNS Server: ☐ Dynamic IP Address ☐ PPPoE Client ☐ PPTP Client

- **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.

WAN Configuration	
WAN Port	☐ Static IP Address ☒ Dynamic IP Address Renew ☐ PPPoE Client ☐ PPTP Client

- **PPPoE Client:** When selecting PPPoE to connect to the network, please set the “**User Name**”, “**Password**”, “**MTU**” and “**CLAMPMSS**”. 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.

WAN Configuration	
WAN Port	☐ Static IP Address ☐ Dynamic IP Address ☒ PPPoE Client Username: * Password: * MTU: 1492 bytes (Range:1000~1492)* CLAMPMSS: 1400 bytes (Range:980~1400)* Dial on Demand: ☐ Enable ☒ Disable ☐ PPTP Client

- **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	☐ Static IP Address ☐ Dynamic IP Address ☐ PPPoE Client ☒ PPTP Client Type ☒ Static ☐ DHCP
	IP Address: *
	Subnet Mask: *
	Default Gateway: *
	Preferred DNS Server: *
	Alternate DNS Server:
	PPTP Server IP: *
	Username: *
	Password: *
	PPTP Connection ID/Name:
	Dial on Demand: ☐ Enable ☒ Disable

WAN Configuration	
WAN Port	☐ Static IP Address ☐ Dynamic IP Address ☐ PPPoE Client ☒ PPTP Client Type ☐ Static ☒ DHCP
	PPTP Server IP: *
	Username: *
	Password: *
	PPTP Connection ID/Name:
	Dial on Demand: ☐ Enable ☒ 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 ☐ Enable ☒ Disable
	User Authentication ☒ Enable ☐ Disable
	Operation Mode NAT
	IP Address: 192.168.1.254 *
	Subnet Mask: 255.255.255.0 *
DHCP Server Configuration	☒ Disable DHCP Server ☐ Enable DHCP Server ☐ Enable DHCP Relay

• LAN1 & LAN2 Port

LAN1 & LAN2 Port	IP PNP ☐ Enable ☒ Disable
	User Authentication ☒ Enable ☐ Disable
	Operation Mode NAT
	IP Address 192.168.1.254 *
	Subnet Mask 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	☒ Disable DHCP Server
	☐ Enable DHCP Server
	☐ 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	☐ Disable DHCP Server
	☒ Enable DHCP Server
	DHCP Scope
	Start IP Address: 192.168.1.1 *
	End IP Address: 192.168.1.100 *
	Preferred DNS Server: 192.168.1.254 *
	Alternate DNS Server:
	Domain Name: airlive.com *
	WINS Server IP:
	Lease Time: 1 Day ▼
Reserved IP Address List	
☐ 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			
2			
3			
4			
5			
6			
7			
8			
9			
10			
(Total:40) First Prev Next Last			

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

DHCP Server Configuration	☐ Disable DHCP Server
	☐ Enable DHCP Server
	☒ Enable DHCP Relay
	DHCP Server IP: *

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: NAT
	IP Address: 192.168.2.254 *
	Subnet Mask: 255.255.255.0 *
DHCP Server Configuration	☒ Disable DHCP Server ☐ Enable DHCP Server ☐ Enable DHCP Relay

• LAN3 & LAN4 Port

LAN3 & LAN4 Configuration	
LAN3 & LAN4	Operation Mode: NAT
	IP Address: 192.168.2.254 *
	Subnet Mask: 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	☒ Disable DHCP Server ☐ Enable DHCP Server ☐ 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	☐ Disable DHCP Server ☒ Enable DHCP Server
	DHCP Scope
	Start IP Address: 192.168.2.1 *
	End IP Address: 192.168.2.100 *
	Preferred DNS Server: 192.168.2.254 *
	Alternate DNS Server:
	Domain Name: airlive.com *
	WINS Server IP:
	Lease Time: 1 Day
	Reserved IP Address List ☐ 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			
2			
3			
4			
5			
6			
7			
8			
9			
10			
(Total:40) First Prev Next Last			

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	☐ Disable DHCP Server ☐ Enable DHCP Server ☒ Enable DHCP Relay
	DHCP Server IP *

4.1.6 Wireless Configuration

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

Wireless Configuration		
Basic Configuration	SSID	airlive *
		☒ Sync To Ticket
	Transmission Mode	802.11(b+g) ▼
	Channel	1 ▼
	SSID Broadcast	☒
	Layer2 Client Isolation	☒
		Security Advance
Wireless Port	IP PNP	☐ Enable ☒ Disable
	User Authentication	☒ Enable ☐ Disable
	Operation Mode	NAT ▼
	IP Address:	192.168.3.254 *
	Subnet Mask:	255.255.255.0 *
DHCP Server Configuration	☐ Disable DHCP Server ☒ 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 ▼
		Reserved IP Address List
WDS Configuration	☐ Enable DHCP Relay ☐ Enable ☒ Disable	

- **Wireless Configuration**

Wireless Configuration		
Basic Configuration	SSID	airlive *
		☒ Sync To Ticket
	Transmission Mode	802.11 (b+g) ▼
	Channel	1 ▼
	SSID Broadcast	☒
	Layer2 Client Isolation	☒
Security Advance		

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	☒ Enable ☐ Disable
WEP Key Encryption	☒ 64bits ☐ 128bits
Mode	HEX ▼ HEX ASCII
	☐ 2.
	☐ 3.
	☐ 4.

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

Wireless Port	IP PNP	☐ Enable ☒ Disable
	User Authentication	☒ Enable ☐ Disable
	Operation Mode	NAT 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.

DHCP Server Configuration	☒ Disable DHCP Server ☐ Enable DHCP Server ☐ 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	☐ Disable DHCP Server ☒ 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 v
	Reserved IP Address List ☐ 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			
2			
3			

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	☐ Disable DHCP Server ☐ Enable DHCP Server ☒ Enable DHCP Relay
	DHCP Server IP *

• 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	☐ Enable ☒ 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	☒ Enable ☐ Disable	
	Item	WDS Client MAC Address
	1	
	2	
	3	

4.2 User Authentication

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

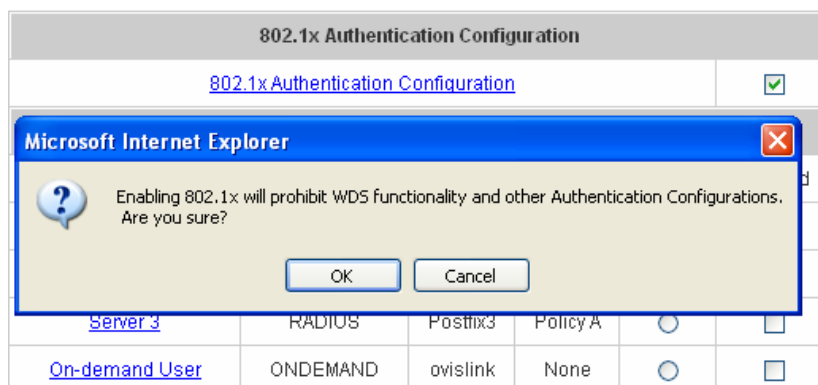
System Configuration	User Authentication	Network Configuration	Utilities	Status
User Authentication				
Authentication Configuration				
System provides 3 authentication servers. Each server allows only one type of authentication method and one Black List Profile. An authentication policy may be assigned 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.				
Black List Configuration				
System supports 5 Black List profiles for used within the authentication server. On-demand users are NOT bounded by the Black List.				
Policy Configuration				
System provides 3 policies, each policy can apply independent firewall profile, specific route profile, login schedule profile and bandwidth controls.				
Guest User Configuration				
System provides up to 10 guest accounts.				
Additional Configuration				
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	
Authentication Configuration					
802.1x Authentication Configuration					
802.1x Authentication Configuration				☐	
Authentication Server Configuration					
Server Name	Auth Method	Postfix	Policy	Default	Enabled
Server 1	LOCAL	Postfix1	Policy A	☐	☐
Server 2	POP3	Postfix2	Policy A	☐	☐
Server 3	RADIUS	Postfix3	Policy A	☐	☐
On-demand User	ONDEMAND	ovislink	None	☒	☒

- 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.

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:

Group Re-key Time: seconds *(Range: 0-6000)

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.

802.1x Authentication Configuration

☐ 802.1x
 ☐ WPA w/ 802.1x
 ☒ WPA-PSK

Group Re-key Time: seconds *(Range: 0-6000)

☐ PSK:

☒ Passphrase:

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
Server 1	LOCAL	Postfix1	Policy A	☐	☐
Server 2	POP3	Postfix2	Policy A	☐	☐
Server 3	RADIUS	Postfix3	Policy A	☐	☐
On-demand User	ONDEMAND	ovislink	None	☒	☒

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	Server 1 *(Its server name)
Server Status	Disabled
Postfix	Postfix1 *(Its postfix name)
Black List	None
Authentication Method	Local User Local User Setting
Policy	Policy A
Allow username without postfix	☐

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	airlive *(e.g. airtlive. Max: 40 char)
Receipt Header 1	Welcome! (e.g. Welcome!)
Receipt Header 2	
Receipt Footer	Pls wait for login page (e.g. Thank You!)
Printer Baud Rate	9600 v
Monetary Unit	☒ none ☐ \$ USD ☐ £ GBP ☐ € EUR (Input other desired monetary unit, e.g. AU)
WLAN ESSID	airlive (e.g. airtlive)
Wireless Key	
Remark	(for customer)
Billing Notice Interval	☒ 10mins ☐ 15mins ☐ 20mins
Twin Ticket	☐ Enable ☒ Disable
Users List Billing Configuration Create On-demand User Billing Report Payment	

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	Server 1 *(its server name)
Server Status	Disabled
Postfix	Postfix1 *(its postfix name)
Black List	None v
Authentication Method	☒ Local User v Local User Setting
Policy	Policy A v
Allow username without postfix	☐

Click the hyperlink for further configuration.

Local User Setting
Edit Local User List

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

Add User	Upload User	Download User	Refresh	
		Search		
Users List				
Username	Password	MAC	Policy	Del All
			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 (xxxxxxxxxxxx)	Policy
	Password	Expiration Time	Remark
1			None v
		Select	
2			None v
		Select	
3			None v
		Select	
4			None v
		Select	
5			None v
		Select	

Add User			
Item	Username	MAC (xxxxxxxxxxxx)	Policy
	Password	Expiration Time	Remark
1	Tony		Policy A v
	tony	02/01/2007 Select	
2	Larry	00:01:23:3F:6D:7E	Policy A v
	larry	01/31/2007 Select	
3	Judy		None v
	judy	02/25/2007 Select	
4	Oksana		Policy B v
	oksana	Select	Long Term
5			None v
		Select	

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 (xxxxxxxxxxxx)	Policy
	Password	Expiration Time	Remark
1			None v
		Select	
2			None v
		Select	
3			None v
		Select	

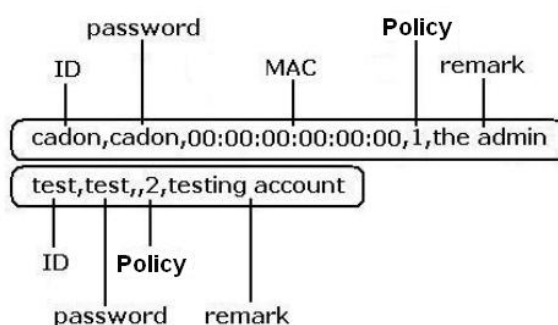
Upload User: Click this to enter the **Upload User** interface. Click the **Browse** button to select the text file for the user account upload. Then click **Submit** to complete the upload process.

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

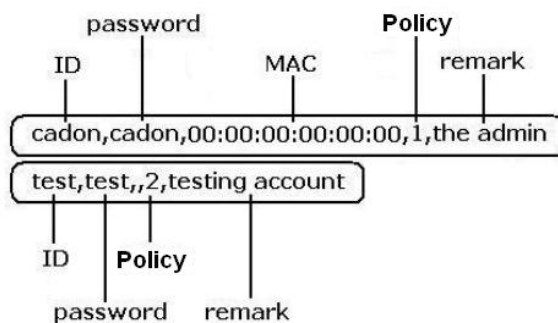
The uploading file should be a text file and the format of each line is "**ID, Password, MAC, Policy, Remark**" without the quotes. There must be no spaces between the fields and commas. The MAC field could be omitted but the trailing comma must be retained. When adding user accounts by uploading a file, 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	00:01:23:3F:6D:7E	1
		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	
Tony	tony	02 01 2007	Policy A	Delete
Larry	larry	00:01:23:3F:6D:7E 01 31 2007	Policy A	Delete
Judy	judy	02 25 2007	None	Delete
Oksana	oksana		Policy B	Delete
			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	
Oksana	oksana		Policy B	Delete
			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	Oksana *
Password	oksana *
MAC	00:01:33:7C:2D:1F
Policy	Policy C ▾
Remark	Permanent
Expiration Time	// Select

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 *(its server name)
Server Status	Disabled
Postfix	Postfix1 *(its postfix name)
Black List	None ▼
Authentication Method	POP3 ▼ POP3 Setting
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	*(Domain Name/IP)
Port	*(Default: 110)
SSL Setting	☐ Enable SSL Connection
Secondary POP3 Server	
Server IP	
Port	
SSL Setting	☐ 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 *(its server name)
Server Status	Disabled
Postfix	Postfix1 *(its postfix name)
Black List	None ▼
Authentication Method	Radius ▼ Radius Setting
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	☒ Enable ☐ Disable Radius Client List
Trans Full Name	☒ Enable ☐ Disable
NASID	
Primary RADIUS Server	
Server IP	*
Authentication Port	*(Default: 1812)
Accounting Port	*(Default: 1813)
Secret Key	*
Accounting Service	☐ Enable ☒ Disable
Authentication Protocol	PAP v
Secondary RADIUS Server	
Server IP	
Authentication Port	
Accounting Port	
Secret Key	
Accounting Service	☒ Enable ☐ Disable
Authentication Protocol	CHAP 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 v	192.168.1.0	255.255.255.255 (/32) v	12345678
2	Disable v		255.255.255.255 (/32) v	
3	Disable v		255.255.255.255 (/32) v	
4	Disable v		255.255.255.255 (/32) v	
5	Disable v		255.255.255.255 (/32) v	

- **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 *(Its server name)
Server Status	Disabled
Postfix	Postfix1 *(Its postfix name)
Black List	None 
Authentication Method	LDAP  LDAP Setting
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 asterisks are necessary information. These settings will become effective immediately after clicking the **Apply** button.

Primary LDAP Server	
Server IP	*(Domain Name/IP)
Port	*(Default: 389)
Base DN	*(CN=,dc=,dc=)
Account Attribute	(Default: uid)
Secondary LDAP Server	
Server IP	
Port	
Base DN	
Account Attribute	

- **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 *(Its server name)
Server Status	Disabled
Postfix	Postfix1 *(Its postfix name)
Black List	None ▼
Authentication Method	NTDomain ▼ NT Domain Setting
Policy	Policy A ▼

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	*
Transparent Login	☐ Enable ☒ 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 *(e.g. airtlive. Max: 40 char)
Receipt Header 1	Welcome! (e.g. Welcome!)
Receipt Header 2	
Receipt Footer	Pls wait for login page (e.g. Thank You!)
Printer Baud Rate	9600 v
Monetary Unit	☒ none ☐ \$ USD ☐ £ GBP ☐ € EUR ☐ (Input other desired monetary unit, e.g. AU)
WLAN ESSID	airlive (e.g. airtlive)
Wireless Key	
Remark	(for customer)
Billing Notice Interval	☒ 10mins ☐ 15mins ☐ 20mins
Twin Ticket	☐ Enable ☒ Disable
Users List Billing Configuration Create On-demand User Billing Report Payment	

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
Q2FX	93NH7WYK	Out of Qouta	Not available	2006/05/04-10:22:59	Delete
64MM	V8UF3967	2 hour	Normal	2006/05/05-10:12:15	Delete
N77X	86N99T4E	Out of Qouta	Not available	2006/05/03-10:35:44	Delete
8Y89	5352P766	Redeemed before	Not available	2006/05/03-11:02:02	Delete
8N6X	788VZ9B8	10 min	Expire	2006/05/02-11:15:16	Delete
2797	NW4679S4	10 min	Normal	2006/05/02-11:56:09	Delete
2XD4	7R9S2RR2	2 hour	Normal	2006/05/05-10:56:16	Delete
4HC4	R888S37X	1 hour 59 min 42 sec	Normal	2006/05/07-11:10:16	Delete
2TP4	ZUF7XE5A	10 min	Normal	2006/05/02-12:06:51	Delete

(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	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	☒ Enable ☐ Disable	☐ Data ☒ Time	Mbyte hrs mins	days hours	days	Policy A	20		
2	☒ Enable ☐ Disable	☒ Data ☐ Time	100 Mbyte hrs mins	5 days 12 hours	7 days	Policy B	10		
3	☒ Enable ☐ Disable	☐ Data ☒ Time	Mbyte 4 hrs 0 mins	10 days 0 hours	10 days	None	20		
4	☒ Enable ☐ Disable	☒ Data ☐ Time	5000 Mbyte hrs mins	20 days 0 hours	30 days	Policy A	50		
5	☐ Enable ☒ Disable	☐ Data ☐ 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	<button>Create</button>
2	4 hrs 0 mins	6	Enabled	<button>Create</button>
3	500 Mbyte	5	Enabled	<button>Create</button>
4	2000 Mbyte	8	Disabled	<button>Create</button>

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.



Username	PMBN@airlive
Password	A4X8TE9K
Price	€ 4
Usage	1 hrs 0 mins
ESSID : airtlive	
Wireless Key :	
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.



Report All

From: -- Year -- Month -- Day

To: -- Year -- Month -- Day Search

- **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	airlive *(e.g. airtlive. Max: 40 char)
Receipt Header 1	Welcome! (e.g. Welcome!)
Receipt Header 2	
Receipt Footer	Pls wait for login page (e.g. Thank You!)
Printer Baud Rate	9600 v
Monetary Unit	☒ none ☐ \$ USD ☐ £ GBP ☐ € EUR (Input other desired monetary unit, e.g. AU)
WLAN ESSID	airlive (e.g. airtlive)
Wireless Key	
Remark	(for customer)
Billing Notice Interval	☒ 10mins ☐ 15mins ☐ 20mins
Twin Ticket	☐ Enable ☒ Disable
Users List Billing Configuration Create On-demand User Billing Report Payment	

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

Payment Configuration

External Payment Gateway		
☐ Authorize.Net	☒ PayPal	☐ 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	
☒ Authorize.Net	☐ PayPal ☐ Disable

Authorize.Net Payment Page Configuration	
Merchant Login ID	cnpdev1421 *
Merchant Transaction Key	34M49E7Ek5t2R8sX *
Payment Gateway URL	https://test.authorize.net/gateway/transact.dll *
Verify SSL Certificate	☒ Enable ☐ Disable
Test Mode	☒ Enable ☐ Disable Try Test *
MD5 Hash	☐ Enable ☒ Disable

Service Disclaimer Content	
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	☒ Enable ☐ Disable	2 hrs 0 mins	5.00
2	☒ Enable ☐ Disable	6 hrs 0 mins	8.00
3	☒ Enable ☐ Disable	12 hrs 0 mins	12.00
4	☒ Enable ☐ Disable	600 Mbyte	5.00
5	☒ Enable ☐ Disable	1000 Mbyte	8.00
6	☒ Enable ☐ Disable	2000 Mbyte	12.00
7	☐ Enable ☒ Disable		
8	☐ Enable ☒ Disable		
9	☐ Enable ☒ Disable		
10	☐ Enable ☒ Disable		

Client's Purchasing Record	
Invoice Number	YK-Cafe- 00000049 * ☐ 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
☒ Credit Card Number	Credit Card Number *	☒
☒ Credit Card Expiration Date	Credit Card Expiration Date *	☒
☒ Card Type	Card Type * ☒ Visa ☒ American Express ☒ Master Card ☒ Discover	☒
☒ Card Code	Card Code *	☒
☒ E-mail	E-mail *	☒
☐ Customer ID	Room Number *	☐
☒ First Name	First Name *	☒
☒ Last Name	Last Name *	☒
☒ Company	Company *	☐
☒ Address	Address *	☐
☒ City	City *	☐
☒ State	State *	☐
☒ Zip	Zip *	☐
☒ Country	Country *	☐
☒ Phone	Phone *	☐
☒ Fax	Fax *	☐

*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	

➤ 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	
☐ Authorize.Net	☒ PayPal
☐ Disable	

PayPal Payment Page Configuration	
Business Account	
Payment Gateway URL	https://www.paypal.com/cgi-bin/webscr
Identity Token	
Verify SSL Certificate	☒ Enable ☐ Disable
Currency	USD (U.S. Dollar) ▼

Service Disclaimer Content	
We may collect and store the following personal information:	

➤ 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	☒ Enable ☐ Disable	2 hrs 0 mins	0.01	
2	☒ Enable ☐ Disable	2 Mbyte	0.02	
3	☒ Enable ☐ Disable	3 Mbyte	0.03	
4	☐ Enable ☒ Disable			
5	☐ Enable ☒ Disable			
6	☐ Enable ☒ Disable			
7	☐ Enable ☒ Disable			
8	☐ Enable ☒ Disable			
9	☐ Enable ☒ Disable			
10	☐ Enable ☒ 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 ☐ 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		
2		
3		

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		
2		

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		☒
(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	Setting
Specific Route Profile	Setting
Schedule Profile	Setting
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 1

Firewall Profile						
Filter Rule Item	Active	Action	Name	Source Destination	Protocol	MAC
1	☐	Block		ANY	ALL	
				ANY		
2	☐	Block		ANY	ALL	
				ANY		

Edit Filter Rule						
Rule Item: 1						
Rule Name:				☐ Enable this Rule		
Action : Block ▼				Protocol ALL ▼		
Source MAC Address: (For Specific MAC Address Filter)						
	Interface	IP	Subnet Mask	Start Port	End Port	
Source	ALL ▼		255.255.255.255 (/32) ▼			
Destination	ALL ▼		255.255.255.255 (/32) ▼			

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		255.255.255.255 (/32) ▼		☐
2		255.255.255.255 (/32) ▼		☐

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							
Hour	SUN	MON	TUE	WED	THU	FRI	SAT
0	☒	☒	☒	☒	☒	☒	☒
1	☒	☒	☒	☒	☒	☒	☒
2	☒	☒	☒	☒	☒	☒	☒
3	☒	☒	☒	☒	☒	☒	☒
4	☒	☒	☒	☒	☒	☒	☒
5	☒	☒	☒	☒	☒	☒	☒
6	☒	☒	☒	☒	☒	☒	☒
7	☒	☒	☒	☒	☒	☒	☒
8	☒	☒	☒	☒	☒	☒	☒
9	☒	☒	☒	☒	☒	☒	☒
10	☒	☒	☒	☒	☒	☒	☒

- **Bandwidth**

Choose one bandwidth limit for that particular policy.

Policy Configuration	
Select Policy:	Policy A ▼
Firewall Profile	Setting
Specific Route Profile	Setting
Schedule Profile	Setting
Total Bandwidth	Unlimited ▼
Individual Maximum Bandwidth	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 54 Mbps
Individual Request Bandwidth	Unlimited

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.

Guest User Configuration	
Guest User Configuration	☒ Enable Guest User ☐ Disable Guest User
	Guest User List
	Policy: None ▼
	Session Length: 6 ▼ hours
	Idle Timer: 10 minutes *(Range: 1-1440)

- **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	
User Control	Idle Timer: 10 minutes *(Range: 1-1440)
	Multiple Login ☐ (On-demand and RADIUS authentication do NOT support multiple login.)
	Friendly Logout ☒
Internet Connection Detection	http://
Upload File	Certificate Login Page Logout Page Login Success Page Login Success Page for On-Demand Logout Success Page
Credit Reminder	Volume ☐ Enabled ☒ Disable
	Time ☐ Enabled ☒ Disable
POP3 Message	Edit Mail Message
Enhance User Authenticate	Permit MAC Address List
SMTP Redirect	☐ Enabled ☒ 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	Browse...

Upload Customer Certificate	
File Name	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	
☐ Default Page	☒ Template Page
☐ Uploaded Page	☐ External Page

Template Page Setting	
Color for Title Background	Select (RGB values in hex mode)
Color for Title Text	Select (RGB values in hex mode)
Color for Page Background	Select (RGB values in hex mode)
Color for Page Text	Select (RGB values in hex mode)
Title	User Login Page
Welcome	Welcome To User Login Page
Information	Please Enter Your Name and Password to Sign In
Username	Username
Password	Password
Submit	Submit
Clear	Clear
Remaining	Remaining
Copyright	Copyright (c)
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	
☐ Default Page	☐ Template Page
☒ Uploaded Page	☐ External Page

Uploaded Page Setting	
File Name	Browse...
Submit	

Existing Image Files:

Total Capacity: 512 K	
Now Used: 0 K	
Upload Image Files	
Upload Images	Browse...
Submit	
Preview	

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

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

```
<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>
```

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.

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.

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.

A screenshot of a web page titled 'Service Disclaimer' in a blue header. The main content area has a light gray background and contains two paragraphs of text. The first paragraph states that personal information (e-mail address, physical contact information, credit card numbers, and transactional information) may be collected and stored based on internet service activities. The second paragraph states that if the provided information cannot be verified, additional information (such as driver license, credit card statement, or utility bill) or answers to questions may be required for verification. At the bottom, there are two radio buttons: 'I agree.' (which is selected) and 'I disagree.'. Below the radio buttons is a 'Next' button.

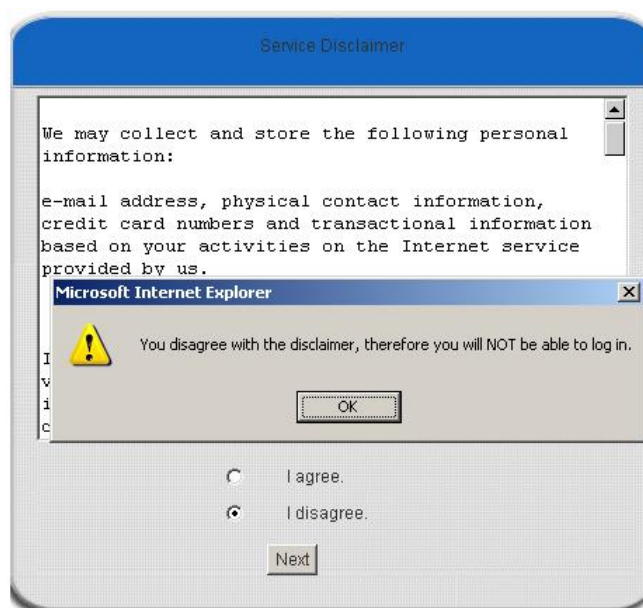
[Click here to purchase by Credit Card Online.](#)

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

A screenshot of a web page titled 'User Login Page' in a blue header. The page has a light gray background. 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.

[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	
☐ Default Page	☐ Template Page
☐ Uploaded Page	☒ External Page

External Page Setting	
External URL :	http://
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

Upload Logout Page	
File Name	Browse...
Submit Use Default Page	

Existing Image Files:

Total Capacity: 512 K Now Used: 0 K	
Upload Image Files	
Upload Images	Browse...
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	
☒ Default Page	☐ Template Page
☐ Uploaded Page	☐ 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.
Preview

- 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	
☐ Default Page	☒ Template Page
☐ Uploaded Page	☐ External Page

Template Page Setting	
Color for Title Background	Select (RGB values in hex mode)
Color for Title Text	Select (RGB values in hex mode)
Color for Page Background	Select (RGB values in hex mode)
Color for Page Text	Select (RGB values in hex mode)
Title	Login Succeed Page
Welcome	Hello
Information	Please click this button to
Logout	Logout
Information2	Thank you
Login Time	Login Time
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	
☐ Default Page	☐ Template Page
☒ Uploaded Page	☐ External Page

Uploaded Page Setting	
File Name	Browse...
Submit	

Existing Image Files:

Total Capacity: 512 K Now Used: 0 K	
Upload Image Files	
Upload Images	Browse...
Submit	
Preview	

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.

Total Capacity: 512 K	
Now Used: 0 K	
Upload Image Files	
Upload Images	Browse...
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.

Existing Image Files :
1102474548_732cn.gif ☐
Delete

- 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

Login Success Page Selection for Users	
☐ Default Page	☐ Template Page
☐ Uploaded Page	☒ External Page

External Page Setting	
External URL :	http://
Preview	

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

Login Success Page Selection for on-demand Users	
☒ Default Page	☐ Template Page
☐ Uploaded Page	☐ External Page

Default Page Setting
This is default success login page for on-demand users. You could click preview link to preview the default login success page. Thanks. Preview

- 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	
☐ Default Page	☒ Template Page
☐ Uploaded Page	☐ External Page

Template Page Setting	
Color for Title Background	Select (RGB values in hex mode)
Color for Title Text	Select (RGB values in hex mode)
Color for Page Background	Select (RGB values in hex mode)
Color for Page Text	Select (RGB values in hex mode)
Title	Login Succeed Page for on-demand
Welcome	Welcome
Information	Please click this button to
Logout	Logout
Information2	Thank you
Remaining Usage	Remaining Usage
Day	Day
Hour	Hour
Min	Min
Sec	Sec
Login Time	Login Time
Redeem	Redeem
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	
☐ Default Page	☐ Template Page
☒ Uploaded Page	☐ External Page

Upload Login Success Page for on-demand	
File Name	Browse...
Submit	

Existing Image Files:

Total Capacity: 512 K
Now Used: 0 K

Upload Image Files	
Upload Images	Browse...
Submit	

[Preview](#)

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.

Total Capacity: 512 K Now Used: 0 K	
Upload Image Files	
Upload Images	Browse...
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.

Existing Image Files :	
1102474548_732cn.gif ☐	
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	
☐ Default Page	☐ Template Page
☐ Uploaded Page	☒ External Page

External Page Setting	
External URL:	http://
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	
☒ Default Page	☐ Template Page
☐ Uploaded Page	☐ External Page

Default Page Setting
This is default logout success page for users. You could click preview link to preview the default logout success page. Thanks. Preview

- 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	
☐ Default Page	☒ Template Page
☐ Uploaded Page	☐ External Page

Template Page Setting	
Color for Title Background	Select (RGB values in hex mode)
Color for Title Text	Select (RGB values in hex mode)
Color for Page Background	Select (RGB values in hex mode)
Color for Page Text	Select (RGB values in hex mode)
Title	Logout Succeed Page
Information	Logout successfully
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	
☐ Default Page	☐ Template Page
☒ Uploaded Page	☐ External Page

Upload Logout Success Page	
File Name	Browse...
Submit	

Existing Image Files:

Total Capacity: 512 K Now Used: 0 K	
Upload Image Files	
Upload Images	Browse...
Submit	
Preview	

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.

Upload Logout Success 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><!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN"> <HTML><HEAD> <META HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=us-ascii"> </HEAD> <BODY> <DIV> <DIV> Welcome! </DIV> <DIV> </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		2	
3		4	

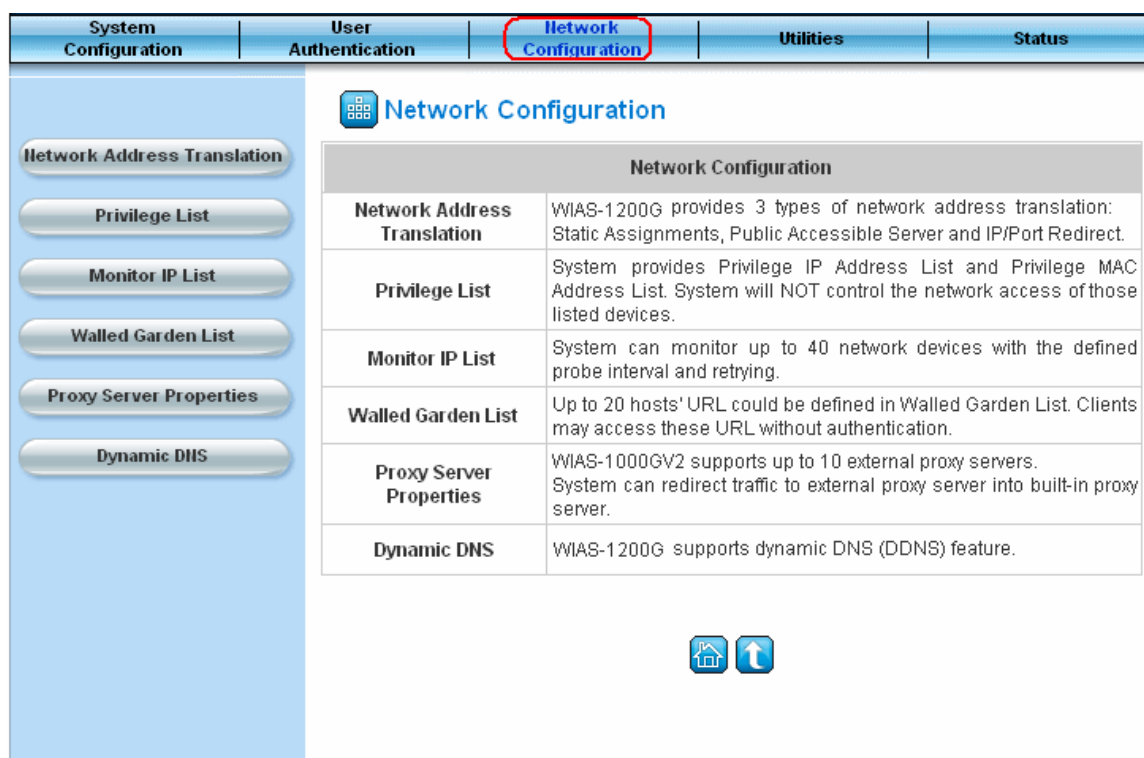
Note: The format of the MAC address is: xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx.

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

SMTP Redirect	☒ 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**.



The screenshot displays the 'Network Configuration' page. The top navigation bar includes 'System Configuration', 'User Authentication', 'Network Configuration' (highlighted with a red box), 'Utilities', and 'Status'. The left sidebar contains buttons for 'Network Address Translation', 'Privilege List', 'Monitor IP List', 'Walled Garden List', 'Proxy Server Properties', and 'Dynamic DNS'. The main content area is titled 'Network Configuration' and contains a table with the following information:

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

At the bottom of the main content area, there are two icons: a home icon and an up arrow icon.

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
Static Assignments
Public Accessible Server
Port and IP Redirect

- 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		
2		
3		
4		
5		
6		
7		
8		
9		
10		

(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.