

IAS-2000 v2

Internet Access Gateway

User's Manual

www.airlive.com

1

	Declaration of Conformity We, Manufacturer/Importer OvisLink Corp. 5F., NO.6, Lane 130, Min-Chuan Rd., Hsin-Tien City, Taipei County, Taiwan		
I	Declare that the product Internet Access Gateway AirLive IAS-2000 v2 is in conformity with n accordance with 2004/108 EC Directive and 1999/5 EC-R & TTE Directive		
<u>Clause</u>	Description		
■ EN 55022:1998	Limits and methods of measurement of radio disturbance characteristics of information technology equipmen		
EN 61000-3-2:2000 Disturbances in supply systems caused by household appliances and similar electrical equipment "Harmonics			
EN 61000-3-3:1995/ A1:2001	Disturbances in supply systems caused by household appliances and similar electrical equipment "Voltage fluctuations		
■ EN 55024:1998/A1 :2001/A2:2003	Information Technology equipment-Immunity characteristics-Limit And methods of measurement		

■ CE marking

CE

Manufacturer/Importer

Albert

Albert Yeh

Vice President

Signature : _____ Name : _____ Position/ Title : _____

Date : 2008/10/9

AirLive IAS-2000 v2 CE Declaration Statement

Country	Declaration	Country	Declaration
cs	OvisLink Corp. tímto prohlašuje, že tento AirLive	lt	Šiuo OvisLink Corp. deklaruoja, kad šis AirLive
Česky [Czech]	IAS-2000 v2 je ve shodě se základními	Lietuvių	IAS-2000 v2 atitinka esminius reikalavimus ir kitas
	požadavky a dalšími příslušnými ustanoveními	[Lithuanian]	1999/5/EB Direktyvos nuostatas.
	směrnice 1999/5/ES.		
da	Undertegnede OvisLink Corp. erklærer herved, at	nl	Hierbij verklaart OvisLink Corp. dat het toestel AirLive
Dansk [Danish]	følgende udstyr AirLive IAS-2000 v2 overholder	Nederlands [Dutch	IAS-2000 v2 in overeenstemming is met de
	de væsentlige krav og øvrige relevante krav i	-	essentiële eisen en de andere relevante bepalingen
	direktiv 1999/5/EF.		van richtlijn 1999/5/EG.
de	Hiermit erklärt OvisLink Corp., dass sich das	mt	Hawnhekk, OvisLink Corp, jiddikjara li dan AirLive
Deutsch	Gerät AirLive IAS-2000 v2 in Übereinstimmung	Malti [Maltese]	IAS-2000 v2 jikkonforma mal-ħtigijiet essenzjali u ma
[German]	mit den grundlegenden Anforderungen und den		provvedimenti oħrajn relevanti li hemm fid-Dirrettiva
	übrigen einschlägigen Bestimmungen der		1999/5/EC.
	Richtlinie 1999/5/EG befindet.		
et	Käesolevaga kinnitab OvisLink Corp. seadme	hu	Az OvisLink Corporation kijelenti, hogy az AirLive
Eesti [Estonian]	AirLive IAS-2000 v2 vastavust direktiivi	Maqyar	IAS-2000 v2 megfelel az 1999/05/CE irányelv
	1999/5/EÜ põhinõuetele ja nimetatud direktiivist	[Hungarian]	alapvető követelményeinek és egyéb vonatkozó
	tulenevatele teistele asiakohastele sätetele.		rendelkezéseinek.
en	Hereby, OvisLink Corp., declares that this AirLive	pl	Ninieiszym OvisLink Corp oświadcza, że AirLive
English	IAS-2000 v2 is in compliance with the essential	Polski [Polish]	IAS-2000 v2 jest zgodny z zasadniczymi wymogami
5	requirements and other relevant provisions of		oraz pozostałymi stosownymi postanowieniami
	Directive 1999/5/EC.		Dvrektvwv 1999/5/EC.
es	Por medio de la presente OvisLink Corp. declara	pt	OvisLink Corp declara que este AirLive IAS-2000 v2
Español	que el AirLive IAS-2000 v2 cumple con los	Português	está conforme com os requisitos essenciais e outras
[Spanish]	requisitos esenciales y cualesquiera otras	[Portuguese]	disposições da Directiva 1999/5/CE.
	disposiciones aplicables o exigibles de la	[
	Directiva 1999/5/CE.		
el	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ OvisLink Corp. ΔΗΛΩΝΕΙ	sl	OvisLink Corp izjavlja, da je ta AirLive IAS-2000 v2 v
Ελληνική [Greek]	OTI AirLive IAS-2000 v2 ΣΥΜΜΟΡΦΩΝΕΤΑΙ	Slovensko	skladu z bistvenimi zahtevami in ostalimi relevantnimi
	ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ	[Slovenian]	določili direktive 1999/5/ES.
	ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ	. ,	
	1999/5/EK.		
fr	Par la présente OvisLink Corp. déclare que	sk	OvisLink Corp týmto vyhlasuje, že AirLive IAS-2000
Francais [French]	l'appareil AirLive IAS-2000 v2 est conforme aux	Slovensky [Slovak]	v2 spĺňa základné požiadavky a všetky príslušné
	exigences essentielles et aux autres dispositions	, , , , ,	ustanovenia Smernice 1999/5/ES.
	pertinentes de la directive 1999/5/CE		
it	Con la presente OvisLink Corp. dichiara che	fi	OvisLink Corp vakuuttaa täten että AirLive IAS-2000
Italiano [Italian]	questo AirLive IAS-2000 v2 è conforme ai	Suomi [Finnish]	v2 tyyppinen laite on direktiivin 1999/5/EY oleellisten
	requisiti essenziali ed alle altre disposizioni		vaatimusten ja sitä koskevien direktiivin muiden
	pertinenti stabilite dalla direttiva 1999/5/CE.		ehtojen mukainen
lv	Ar šo OvisLink Corp. deklarē, ka AirLive		Hér með lýsir OvisLink Corp yfir því að AirLive
Latviski [Latvian]	IAS-2000 v2 atbilst Direktīvas 1999/5/EK	Íslenska [Icelandic]	IAS-2000 v2 er í samræmi við grunnkröfur og aðrar
	būtiskajām prasībām un citiem ar to saistītajiem		kröfur, sem gerðar eru í tilskipun 1999/5/EC.
	noteikumiem.		
sv	Härmed intygar OvisLink Corp. att denna AirLive	no	OvisLink Corp erklærer herved at utstyret AirLive
Svenska	IAS-2000 v2 står I överensstämmelse med de	Norsk [Norwegian]	IAS-2000 v2 er i samsvar med de grunnleggende
[Swedish]	väsentliga egenskapskrav och övriga relevanta		krav og øvrige relevante krav i direktiv 1999/5/EF.
[bestämmelser som framgår av direktiv		
	1999/5/EG.		

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' reputation

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 des.

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 a section 1 above.

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 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 at 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 for 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 base the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this Licens

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, 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 The source code for a work means the preferred form of the work for making induitications 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 you do not 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 7. In, as a consequence or a court judgment or allegation to paterin infiningement or nor any outer reason (not infinited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradic the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satify 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 Porgram by all those who receive cocies 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 warranty of MERCHANT 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.

Copyright

The contents of this publication may not be reproduced in any part or as a whole, stored, transcribed in an information retrieval system, translated into any language, or transmitted in any form or by any means, mechanical, magnetic, electronic, optical, photocopying, manual, or otherwise, without the prior written permission.

Trademarks

All products, company, brand names are trademarks or registered trademarks of their respective companies. They are used for identification purpose only. Specifications are subject to be changed without prior notice.

FCC Interference Statement

The **IAS-2000 v2** has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against radio interference in a commercial environment. This equipment can generate, use and radiate radio frequency energy and, if not installed and used in accordance with the instructions in this manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause interference, in which case the user, at his own expense, will be required to take whatever measures are necessary to correct the interference.

CE Declaration of Conformity

This equipment complies with the requirements relating to electromagnetic compatibility, EN 55022:1998, EN 61000-3-2, EN 61000-3-3/A1, EN 55024/A1/A2, Class A.

.

Contents

Chapter 1	. Bef	fore You Start	1
1.1	Auc	Audience	
1.2	Doc	Document Conventions	
Chapter 2	. Ove	erview	2
2.1	Intr	roduction of IAS-2000 v2	2
2.2	Sys	tem Concept	2
Chapter 3	. Ha	rdware Installation	5
3.1	Pan	el Function Descriptions	5
3.2	Pac	kage Contents	6
3.3	Sys	tem Requirement	6
3.4	Inst	tallation Steps	7
Chapter 4	. Net	twork Configuration on PC	9
4.1.	Inte	ernet Connection Setup for Windows XP	9
4.2.	TC	P/IP Network Setup	12
Chapter 5	. Wei	b Interface Configuration	16
5.1	Sys	tem Configuration	18
	5.1.1	Configuration Wizard (Also served as Quick Installation)	19
	5.1.2	System Information	
	5.1.3	WAN1 Configuration	
	5.1.4	WAN2 & Failover	
	5.1.5	LAN1 Configuration	36
	5.1.6	LAN2 Configuration	43
5.2	Net	work Configuration	49
	5.2.1	Network Address Translation	50
	5.2.2	Privilege List	53
	5.2.3	Monitor IP List	56
	5.2.4	Walled Garden List	58
	5.2.5	Proxy Server Properties	59
	5.2.6	Dynamic DNS	60
	5.2.7	IP Mobility	61
5.3	Use	er Authentication	62
	5.3.1	Authentication Configuration	63

.

			User s Mariuar
	5.3.2	Policy Configuration	
	5.3.3	Black List Configuration	
	5.3.4	Guest User Configuration	
	5.3.5	Additional Configuration	
5.4	Ut	ilities	
	5.4.1	Change Password	119
	5.4.2	Backup/Restore Setting	
	5.4.3	Firmware Upgrade	
	5.4.4	Restart	
5.5	Sta	atus	
	5.5.1	System Status	
	5.5.2	Interface Status	
	5.5.3	Current Users	
	5.5.4	Traffic History	
	5.5.5	Notification Configuration	
	5.5.6	Online Report	
5.6	He	elp	140
Appendix	<i>A</i> .	External Network Access	141
Appendix	<i>B</i> .	Console Interface Configuration	
Appendix	С.	Specifications	146
a.	Hard	ware Specification	146
b.	Tech	nical Specification	146
Appendix	D.	Proxy Setting for Hotspot	148
Appendix	<i>E</i> .	Proxy Setting for Enterprise	

Chapter 1. Before You Start

1.1 Audience

Clear

This manual is for Hotspot owners or administrators in enterprises to set up network environment using IAS-2000 v2. 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:

Warning: 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.

Apply 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.

Chapter 2. Overview

2.1 Introduction of IAS-2000 v2

IAS-2000 v2 is a Network Access Control System specially designed for middle-scaled or large network environments while retaining network efficiency. IAS-2000 v2 delivers "manageability", "efficiency" and "friendly interface" and suits perfectly for campuses, libraries, gymnasiums, small and middle enterprises, factories, Hotspots and community hospitals.

2.2 System Concept

IAS-2000 v2 is dedicatedly designed for controlling all network data passing through the system. The users under the managed network must be authenticated to access the network beyond the managed area. The authentication mechanism at the user's end is provided by the IAS-2000 v2 server, and the SSL encryption is used to protect the webpage. In the system, IAS-2000 v2 is responsible for authentication, authorization, and management functions. The user account information is stored in the IAS-2000 v2 database, or other specified external authentication databases.



The process of authenticating the user's identity is executed via the SSL encrypted webpage. Using the web interface, it can be ensured that the system is compatible to most desktop systems and palm computers. When a user authentication is requested, the IAS-2000 v2 server software will check the authentication database at the rear end to confirm the user's access right. The authentication database can be the local database of IAS-2000 v2 or any external database that IAS-2000 v2 supports. If the user is not an authorized user, IAS-2000 v2 will refuse the user's

request for the access. In the meantime, IAS-2000 v2 will also continue blocking the user from accessing the network. If the user is an authorized user, then IAS-2000 v2 will authorize the user with an appropriate access right, so that the user can use the network. If the online user remains idle without using the network for a time exceeding a predetermined idle time on IAS-2000 v2 or the online user logs out of the system, IAS-2000 v2 will exit the working stage of such user and terminate the user's access right of the network.

The following figure provides a simple example of setting up a small enterprise network. IAS-2000 v2 is set to control a part of the company's intranet. The whole managed network includes cable network users and wireless network users. In the beginning, any user located at the managed network is unable to access the network resource without permission. If the access right to the network beyond the managed area is required, an Internet browser such as the Internet Explorer must be opened and a connection to any website must be performed. When the browser attempts to connect to a website, IAS-2000 v2 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 IAS-2000 v2.

Attention: Public LAN is referred to as the LAN port with the authentication function enabled from where the Authentication is required for the users to get access of the network; And, **Private LAN** is referred to as the LAN port with the authentication function disabled.



Another setup example is shown in the following figure. The WAN1 and WAN2 of IAS-2000 v2 simultaneously supports the Switch of 802.3ad (Support Port Trunk), and the bandwidth of the Switch will be the sum of the WAN1 and WAN2 bandwidths, which aims at eliminating the bottleneck caused by the narrow bandwidth between IAS-2000 v2 and the 802.3ad Switch.





Chapter 3. Hardware Installation

3.1 Panel Function Descriptions

Front Panel



LED	Color	Status	Description
POWER	Green	On	Power on the device
	Green	Off	BIOS running
Status LED		Blink	OS running
		On	System ready
WAN1, LAN1,			
WAN2, LAN2	Orange	Blink	Sending / Receiving
(L)			
WAN1, LAN1,	Croop	Off	10 Mbps
WAN2, LAN2	Green	On	100 Mbps
(R)	Orange	On	1000 Mbps

Port	Description
WAN1 / WAN2	Connect to Internet or Intranet
LAN1 / LAN2	Connect to the open environment. It can be chosen to require authentication to access network resources and Internet.
Console Port	9-pin serial port connector to resume the factory defaults or reconfigures the system.
Panel Button	LCD Panel to display system info and network interface info

LED: There are four kinds of LED, power, status, port speed and link/act, to indicate different status of the system. **Console Port:** 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. **LAN1/LAN2:** The two LAN ports can be independently configured such that users cannot access Internet before authentication. Thus, administrators can choose to force the authentication for users connected to these ports.

WAN1/WAN2: The two WAN ports are connected to a network which is not managed by the IAS-2000 v2 system, 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.

Rear Panel



attaches here

System Fan: Keep the machine cool.

Power Fan: Keep the power cool.

Power Socket: The power cord attaches here.

Power Switch: Turn on and off the machine.

3.2 Package Contents

The standard package of IAS-2000 v2 includes:

- IAS-2000 v2 x 1
- CD-ROM x 1
- Power Cord x 1
- Ethernet Cable (Crossover) x 1
- Ethernet Cable (Straight) x1
- Console Cable x 1
- Accessory Packing x 1

3.3 System Requirement

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

3.4 Installation Steps



Please follow the following steps to install IAS-2000 v2:

- 1. Connect the power cord to the power socket on the rear panel.
- 2. Turn on the power switch on the rear panel. The Power LED will light up.



3. Connect an Ethernet cable to one LAN port with the user authentication function enabled on the front panel. The default port is LAN1 port. (Note: Authentication is required for the users to access the network via this LAN port. The LAN port with authentication function is referred to as *Public LAN*.) Connect the other end of the Ethernet cable to an AP or switch. The LED of this LAN port should be on to indicate a proper connection.

- 4. Connect an Ethernet cable to one LAN port with the user authentication function disabled on the front panel. The default port is LAN2 port. (Note: No authentication is required for the users to access the network via this LAN port. The LAN port without authentication function is referred to as *Private LAN* and the administrator can enter the administrative user interface to perform configurations via *Private LAN*.) Connect the other end of the Ethernet cable to a client's PC. The LED of this LAN port should be on to indicate a proper connection.
- 5. Connect an Ethernet cable to one of the WAN ports on the front panel. Connect the other end of the Ethernet cable to ADSL modem, cable modem or a switch/hub of the internal network. The LED of this WAN should be on to indicate a proper connection.

Attention: Usually a straight RJ-45 could be applied if IAS-2000 v2 is connected to a hub/computer which supports automatic crossover, such as the Access Point. However, after the Access Point hardware reset, IAS-2000 v2 should not be able to connect to Access Point while connecting with a straight cable unless the cable was pulled out and plug-in again. This scenario does NOT occur while using a crossover cable.

After the hardware of IAS-2000 v2 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 IAS-2000 v2 to manage the network.

Chapter 4. Network Configuration on PC

After IAS-2000 v2 is installed, the following configurations must be set up on the PC: **Internet Connection Setup** for Windows XP and TCP/IP Network Setup.

4.1. Internet Connection Setup for Windows XP

1. Choose Start > Control Panel > Internet Options.



2. Choose the "Connections" label, and then click Setup.

	rity Privacy Cor	ntent Connection	8 Programs Advance
To sel	t up an Internet co	onnection, click	Setup
Dial-up and \	Virtual Private Netv	vork settings	
			Add
			Remove
Choose Sett server for a	ings if you need to connection.	configure a proxy	Settings
Never da	al a connection		
 Dial when Always d 	never a network ci ial my default conr	onnection is not pre lection	esent
O Dial when Always d Current	never a network c ial my default conn None	onnection is not pre lection	esent Set Default
Current Local Area N LAN Settings Choose Sett	never a network con ial my default conr None letwork (LAN) setti s do not apply to d ings above for dia	onnection is not pre lection ngs lal-up connections l-up settings.	Set Default

 Click *Next* when Welcome to the New Connection Wizard screen appears.

New Connection Wizard	
Ś	Welcome to the New Connection Wizard
	This wizard helps you:
	Connect to the Internet.
	 Connect to a private network, such as your workplace network.
	 Set up a home or small office network.
Kai	To continue, click Next.
	< Back Next > Cancel
	To continue, click Next.

4. Choose "Connect to the Internet" and then click *Next*.

New Connection Wizard
Network Connection Type What do you want to do?
 Connect to the Internet Connect to the latemet so you can browse the Web and read email. Connect to the network at my workplace Connect to a business network (using dial-up or VPN) so you can work from home, a field office, or another location.
 Set up a home or small office network Connect to an existing home or small office network or set up a new one. Set up an advanced connection Connect directly to another computer using your serial, parallel, or infrared port, or set up this computer so there computers can connect to it.

5. Choose "Set up my connection manually" and then click *Next*.

New Connection Wizard
Getting Ready The wizard is preparing to set up your Internet connection.
How do you want to connect to the Internet? Choose from a list of Internet service providers (ISPs) Set up my connection manually For a dialoge connection, you will need your account name, password, and a phone number for your ISP. For a broadband account, you won't need a phone number. Use the <u>CD I got from an ISP</u>
< <u>B</u> ack <u>N</u> ext > Cancel

 Choose "Connect using a broadband connection that is always on" and then click *Next*.

New Connection Wizard
Internet Connection How do you want to connect to the Internet?
O Connect using a <u>d</u> ial-up modem
This type of connection uses a modem and a regular or ISDN phone line.
Connect using a broadband connection that requires a user name and password
This is a high-speed connection using either a DSL or cable modem. Your ISP may refer to this type of connection as PPPoE.
Connect using a broadband connection that is always on This is a high-speed connection using either a cable modern, DSL or LAN connection. It is always active, and doesn't require you to sign in.
< Back Next > Cancel

7. Finally, click *Finish* to exit the **Connection Wizard**. New Connection Wizard Now, the setup has been completed



4.2. TCP/IP Network Setup

If the operating system of the PC in use is Windows 95/98/ME/2000/XP, keep the default settings without any change to directly start/restart the system. With the factory default settings, during the process of starting the system, IAS-2000 v2 with DHCP function will automatically assign an appropriate IP address and related information for each PC. If the Windows operating system is not a server version, the default settings of the TCP/IP will regard the PC as a DHCP client, and this function is called "**Obtain an IP address automatically**".

If checking the TCP/IP setup or use the static IP in the LAN1 or LAN2 section is needed, please follow the steps below

Check the TCP/IP Setup of Window XP

 Select Start > Control Panel > Network Connections.



 Click the right button of the mouse on the "Local Area Connection" icon and select "Properties"



 Select "General" label and choose "Internet Protocol (TCP/IP)" and then click *Properties*. Now, choose to use DHCP or specific IP address.

🗕 Local Area Connection Properties 🛛 🔹 💽
General Authentication Advanced
Connect using:
AMD PCNET Family PCI Ethernet Adapter
Configure
This connection uses the following items:
Client for Microsoft Networks Sector A strain for Microsoft Networks Sector A strain for Microsoft Networks
Internet Protocol (TCP/IP)
Install Uninstall Properties
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
Show icon in notification area when connected
OK Cancel

- 4-1. Using DHCP: If using DHCP is desired, please choose
 "Obtain an IP address automatically" and click OK.
 This is also the default setting of Windows. Then, reboot the PC to make sure an IP address is obtained from IAS-2000 v2.
- 4-2. Using Specific IP Address: If using specific IP address is desired, ask the network administrator for the information of the IAS-2000 v2: *IP address*, *Subnet Mask*, *New gateway* and *DNS server address*.

nternet	Protocol (TCP/IP) Proper	ties 🤶 🔀				
General	Alternate Configuration					
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.						
	Obtain an IP address automatically					
IP ad	Idress:					
Subr	net mask:					
Defa	ult gateway:					
📀 OE	Obtain DNS server address automatically					
OUs	se the following DNS server addr	esses:				
Prefe	erred DNS server:	and the second				
Alterr	nate DNS server:					
		Advanced				
		OK Cancel				

Caution: If your PC has been set up completed, please inform the network administrator before modifying the following setup.

Please choose "Use the following IP address:" and enter the information given from the network administrator in "IP address:" and "Subnet mask:" as well as "Default gateway" If the DNS Server column is blank, please choose "Use the following DNS server addresses:" and then enter a known DNS address or the DNS address provided by ISP and then click OK.

ou can get IP settings assigned a s capability. Otherwise, you nee e appropriate IP settings.	automatically if your network supports d to ask your network administrator for
Obtain an IP address automa	itically
Use the following IP address:	
<u>I</u> P address:	
S <u>u</u> bnet mask:	20 81 63
<u>D</u> efault gateway:	
Obtain DNS server address of Use the following DNS serve Preferred DNS server: Alternate DNS server:	
<u>A</u> lternate DNS server:	

• Then, click *Advanced* in the window of "Internet Protocol (TCP/IP) Properties".

nternet	Protocol (TCP/IP) Properties
General	Alternate Configuration
You car this cap the app	n get IP settings assigned automatically if your network supports ability. Otherwise, you need to ask your network administrator for ropriate IP settings.
📀 OE	tain an IP address automatically
-O Us	e the following IP address:
IP ad	dress:
Subr	et mask:
Defa	ult gateway:
O OĐ	tain DNS server address automatically
_⊙ Us	e the following DNS server addresses:
Prefe	rred DNS server:
Alterr	hate DNS server:
	Advanced
	OK Cancel

 Choose the "IP Settings" label and click "Add" below the "Default gateways" column and the "TCP/IP Gateway Address" window will appear. Enter the gateway address of IAS-2000 v2 in the "Gateway:" of "TCP/IP Gateway Address" window, and then click Add. After returning to the "IP Settings" label, click OK to finish.

Advanced TCP/IP Settings	? ×
IP Settings DNS WINS Options	
_ IP add <u>r</u> esses	
IP address Subnet mask	
DHCP Enabled	
<u>A</u> dd <u>E</u> dit Remo <u>v</u> e	
Default gateways:	
Gateway Metric	
A <u>d</u> d Edi <u>t</u> Re <u>m</u> ove	
✓ Automatic metric	
Interface metric:	
ОКСА	ancel

TCP/IP Gateway	Address	? 🛛
<u>G</u> ateway: ┌── Automatic me	etric	
Metric:		Coursel
	Add	Cancel

Chapter 5. Web Interface Configuration

This chapter will present further detailed settings. The following table shows all the functions of IAS-2000 v2.

OPTION	System Configuration	Network Configuration	User Authentication	Utilities	Status
FUNCTION	Configuration Wizard	Network Address Translation	Authentication Configuration	Change Password	System Status
	System Information	Privilege List	Policy Configuration	Backup/Restore Setting	Interface Status
	WAN1 Configuration	Monitor IP List	Black List Configuration	Firmware Upgrade	Current Users
	WAN2 & Failover	Walled Garden List	Guest User Configuration	Restart	Traffic History
	LAN1	Proxy Server	Additional		Notification
	Configuration	Properties	Configuration		Configuration
	LAN2 Configuration	Dynamic DNS			Online Report
		IP Mobility			

Caution: 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.

After the basic installation shown previously has been completed, IAS-2000 v2 can be further configured with the following steps

 Use the network cable of the 10/100BaseT to connect a PC to the *Private Port*, and then start a browser (such as Microsoft IE). Next, enter the gateway address for that port, the default is <u>https://192.168.2.254</u>. In the opened webpage, an administrative login page will appear. Enter *"admin"* as the default username and password *"airlive"*. Click *Enter* to log in.

Air Live	www.airlive.com IAS-2000 v2 Internet Access Gateway
	Welcome To Administrator Login Page! Please Enter Your User Name and Password To Sign In.

Caution: If you can't get the login page, 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 IAS-2000 v2, enter the web management interface and see the welcome page. There is a *Logout* button on the upper right corner to log out the system.

Air Live	IAS-2000 v2	(www.airlive.com) Internet Access Gateway	Des Logout
System Network Configuration Configuration	User Authentication	Utilities	Status
Welc	ome to Administration	System	
In this web administration inter customize network services, as we Administration functions are separ <u>System Configuration</u> , <u>Network Co</u>	face, you may configure Il as manage and monitor a ated into several categories onfiguration , <u>User Authentic</u>	networking parameters, en all users. s: <u>cation</u> , <u>Utilities</u> , and <u>Status</u> .	able and

5.1 System Configuration

This section includes the following functions: **Configuration Wizard**, **System Information**, **WAN1 Configuration**, **WAN2 & Failover**, **LAN1 Configuration** and **LAN2 Configuration**.

Air Live	° ias	(www.airlive.com) ■ Logout -2000 v2 Internet Access Gateway		
System Configuration	Network Configuration Au	User Utilities Status		
	Bystem Cont	figuration		
Configuration Wizard	nfiguration Wizard System Configuration			
System Information	Configuration Wizard	This wizard will guide you through the basic system setup.		
WAN1 Configuration		Configure system and network related parameters: system name, administrator information, SNMP, and time zone. Clients will be redirected to the URL entered in the "Home Page"		
WAN2 & Failover	System Information	field after successful login. Administrator may limit remote administration access to a specific IP address or network segments. When Remote Management IP is configured, only the devices with the IP addresses or from this		
LAN1 Configuration				
LAN2 Configuration	network segment may enter system administration web removed Network Time Protocol(NTP)Server allows system to synchroniz time/date with the configured external time server.			
	WAN1 Configuration	Configure static IP, DHCP, or PPPoE client on WAN1 port.		
	WAN2 & Failover WAN2 & Failover WAN2 will be combined with WAN1 inte WAN1 port setting. Both WAN1 and WAN2 ports a The "Internet Connection Detection" and "WAN configured here.			
LAN Configurations LAN Configurations Clients from LAN must login before access those devices that are listed on the Privilege The LAN interfaces can operate in NAT mod Available options includes DHCP Server, D VLAN.		Clients from LAN must login before accessing network, excluding those devices that are listed on the Privilege IP or MAC List. The LAN interfaces can operate in NAT mode or Router mode. Available options includes DHCP Server, DHCP Relay, and up to 32 VLAN.		
	(b)			

5.1.1 Configuration Wizard (Also served as Quick Installation)

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 set up IAS-2000 v2 and can be served as Quick Installation. There are **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 WAN1 Port
- 5. Configure LAN1
- 6. Select Authentication Method
- 7. Restart

Now, click the System Configuration from the top menu and the System Configuration page will appear.

Air Live	2 [°] 1A5	5-2000 v2	(www.airlive Internet Access Gal	Logout Reway
System Configuration	Network Configuration A	User uthentication	Utilities	Status
	Bystem Con	figuration		
Configuration Wizard		Syste	em Configuration	
System Information	Configuration Wizard	This wizard will	guide you through the basic	c system setup.
WAN1 Configuration		Configure syste administrator in Clients will be	em and network related pa formation, SNMP, and time redirected to the URL ente	rameters: system name, zone. ered in the "Home Page"
WAN2 & Failover		field after successful login. Administrator may limit remote administration access to a specific IP address or network segments. When Remote Management IP is configured, only the devices with the IP addresses or from this network segment may enter system administration web remotely. Network Time Protocol(NTP)Server allows system to synchronize its time/date with the configured external time server.		
LAN1 Configuration				
LAN2 Configuration				
	WAN1 Configuration	Configure statio	IP, DHCP, or PPPoE client	on WAN1 port.
	WAN2 & Failover WAN2 & Failover WAN2 & Failover WAN1 port setting. Both WAN1 and WAN2 ports are still f The "Internet Connection Detection" and "WAN Failover" configured here.		AN2 port. If Bonding is N1 interface and use the ports are still functional. "WAN Failover" are also	
	LAN Configurations	Clients from LAN must login before accessing network, excluding those devices that are listed on the Privilege IP or MAC List. Ins The LAN interfaces can operate in NAT mode or Router mode. Available options includes DHCP Server, DHCP Relay, and up to 32 VLAN.		
6				

Then, click on Configuration Wizard and click the Run Wizard button to start the wizard.



Running the 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 (twenty-character maximum and no spaces).

Click Next to continue.

Air Live		www.airlive.com
Step 1: Change	Admin's Pas	ssword
You may change the password o one. Click Ne	f admin accou ext to continue.	nt by entering a new
New Password:	******	*
Verify Password:		*
Back	lext	Exit

Step 2: Choose System's Time Zone

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

Air Live	(www.airlive.com) IAS-2000 v2		
Step 2: Choose System's Time Zone			
Select the appropriate time zone fictor	or the system. Click Next to		
(GMT+08:00)Taipei	×		
Back Next	Exit		

Step 3: Set System Information

Home Page: Enter the URL to where the clients should be directed when they are properly authenticated.
NTP Server: Enter the URL of external time server for IAS-2000 v2 time synchronization or use the default.
DNS Server: Enter a DNS Server provided by the ISP (Internet Service Provider). Contact the ISP if the DNS IP Address is unknown.

Click Next to continue.

Air Live		(www.airlive.com) IAS-2000 v2
Step 3: Set System Information		
Enter System Infor	mation. Click Next to c	ontinue.
Home Page:	http://www.airlive.com	•
NTP Server:	(e.g. http://www.airlive.com/) tock.usno.navy.mil (e.g. tock.usno.navy.mil)	
DNS Server:	192.168.1.254 •	
Back	Next	Exit

- Step 4: Select the Connection Type for WAN1 Port
 There are three types that WAN1 port supports: 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 be assigned automatically. Click **Next** to continue.
- Air Live
 IAS-2000 v2

 Step 4: Select the Connection Type for WAN1 Port

 Step 4: Select the Connection Type for WAN1 Port

 Select the connection type for WAN1 port. Click Next to continue.

 Static IP Address
 Set WAN1 port with a static IP address.

 Opnamic IP Address
 Set WAN1 port to obtain an IP address automatically. (For most cable modem users.)

 PPPoE Client
 Set the Username and Password for PPPoE dial-up. (For most DSL users.)

(www.airlive.com)

Static IP Address: Set WAN1 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: Configure LAN1's Information

IP Address: Enter the Public LAN port IP Address or use the default.

Subnet Mask: Enter the Public LAN port Subnet Mask or use the default.

Disable DHCP Server: If the DHCP server is disabled, the clients in Public LAN must be configured with an IP address manually.

Enable DHCP Server: When the option is selected, IAS-2000 v2 will automatically provide the necessary IP address to all clients in Public LAN.

Click Next to continue.

Air Live		www.airlive.com
Step 5: Configure LAN1's Information		
Configure LAN1's informati	on. Click Next	to continue.
IP Address:	192.168.1.254	•
Subnet Mask:	255.255.255.0	•
 Disable Enable I 	DHCP Server DHCP Server	
Back Ne	ext	Exit

Step 5: Set LAN1 DHCP Server

If Enable DHCP Server option is selected, fields marked with red asterisk must be filled in.

Start IP Address: The start IP address that will be assigned to the Public LAN clients.

End IP Address: The end IP address that will be assigned to the Public LAN clients.

(Note: Be sure that IP addresses assigned from Start IP address to End IP address are NOT used in other settings by IAS-2000 v2.)

Domain Name: Enter a domain name provided by the ISP (e.g. airlive.com).

Step 5 (cont.): Set	LAN1 DHCP Server	
Configure DHCP settings	. Click Next to continue.	
Start IP Address:	192.168.1.101 -	
End IP Address:	192.168.1.200 -	
Domain Name:	airlive.com .	
WINS Server:		
Preferred DNS Server:	168.95.1.1	
Alternate DNS Server:		
Preferred DNS Server: Alternate DNS Server:	168.95.1.1 -	

WINS Server: Enter the IP address of the WINS Server (Windows Internet Naming Service Server). This field is optional.

Preferred DNS Server: The DNS Server settings are provided by the ISP. Only the Preferred DNS Server field is mandatory. Contact the ISP if the DNS Server settings are unknown.

Alternate DNS Server: The DNS Server settings are provided by the ISP. This field is optional.

Click *Next* to continue.

Step 6: Select Default Authentication Server

Set the user's information in advance. Enter an easy identified name as the postfix name in the *Postfix Name* field (e.g. airlive) and choose an authentication method.

Click *Next* to continue.

Air Li	ve	far Ps	www.airlive.com
Step 6:	Select Defa	ult Authentic	ation Server
Select defau	It authenticat	ion server. Click	Next to continue.
Postfix Name:	airlive	*(Default Authe	ntication Server)
	O Local	I Server	
	O POP3	3 Server	
		US Server	
	O LDAP	Server	
	O NT Do	omain	
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), **MAC** (optional) and assign it a policy (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.

Air Live	(www.airlive.com) IAS-2000 v2
Step 6 (cont.): Ad	dd User
Click the "ADD" button to add a Local U	lser. Click Next to continue.
Username:	
Password:	
MAC:	X-XX-XX)
Policy None	
ADD	
Back Next	Exit

> POP3 User- Authentication Method-POP3

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

Click Next to continue.

Air Liv	<i>r</i> e'	(www.airlive.com) IAS-2000 v2		
Step 6 (cont.): Authentication Method-POP3				
Configure POP:	3 Server information	n. Click Next to continue.		
POP3 Server:	mail.airlive.com	*(Domain Name/IP Address)		
Server Port:	110	*(Default: 110)		
Enable SSL				
Back	Next	Exit		

RADIUS User- Authentication-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.

Air Live	(www.airlive.com) IAS-2000 v2
Step 6 (cont.): A	uthentication Method-RADIUS
Configure RADIUS Serv	ver information. Click Next to continue.
RADIUS Server:	*(Domain Name/IP Address)
Authentication Port:	*(Default: 1812)
Accounting Port:	*(Default: 1813)
Secret Key:	-
Accounting Service	Enable 💙 -
Authentication Method	CHAP 🗸 -
Back	Next Exit

(www.airlive.com)

LDAP User- Authentication Method-LDAP

Add a new user to the LDAP user data base. Enter the "LDAP Server", "Server Port" and "Base DN" and select one kind of Binding Type and Account Attribute to access the LDAP server.

If User Account binding type is selected, the system will use the **Base DN** to be the user account to access the LDAP server.

Air Live IAS-2000 v2 Step 6 (cont.): Authentication Method-LDAP Configure LDAP Server information. Click Next to continue. LDAP Server: *(Domain Name/IP Address) Server Port: *(Default: 389) Base DN: *(CN=,do=,do=) Binding Type User Account 🗸 Account Attribute
OUD
OCN
OsAMAccountName Back Next Exit

If Anonymous binding type is selected, the system will access the LDAP servers without requiring authentication.

Air Live	,°	(www.airlive.com) IAS-2000 v2
Step 6 (cont.): Authentica	ation Method-LDAP
Configure LDAP Se	erver informatio	on. Click Next to continue.
LDAP Server:		*(Domain Name/IP Address)
Server Port:		*(Default: 389)
Base DN:		*(CN=,do=,do=)
Binding Type	Anonymous 💌	
Account Attribute		sAMAccountName
Back	Next	Exit

If Specified DN binding type is selected, username and *password* in the "Bind RDN" and "Bind Password" fields must be entered to access the LDAP server.

www.airlive.com
): Authentication Method-LDAP
erver information. Click Next to continue.
*(Domain Name/IP Address)
*(Default: 389)
*(CN=,do=,do=)
Specified DN 💌
● UID ○ CN ○ sAMAccountName
Next Exit

If **Windows AD** binding type is selected, please enter the domain name of Windows AD to access the LDAP server.

Click Next to continue.

Air Live	e	(www.airflve.com) IAS-2000 v2
Step 6 (cont	t.): Authenti	cation Method-LDAP
Configure LDAP S	Server informat	tion. Click Next to continue.
LDAP Server:		*(Domain Name/IP Address)
Server Port:		*(Default: 389)
Base DN:		*(CN=,dc=,dc=)
Binding Type Domain	Windows AD	
Back	Next	Exit

NT Domain User- Authentication Method-NT Domain

When NT Domain User is selected, enter the information for "Server IP Address", and enable/disable "Transparent Login". After this setup is completed, click *Next* to continue.

Air Live	(www.airlive.com) IAS-2000 v2
Step 6 (cont.): Authentication	n Method-NT Domain
Configure NT Domain Server informat	ion. Click Next to continue.
Server IP Address:	•
Back Next	Exit

Step 7: Restart

•

Click *Restart* to save the current settings and restart IAS-2000 v2. The Setup Wizard is now completed.



During IAS-2000 v2 restart, a "**Restarting now. Wait** for a minute." message will appear on the screen. Please do not interrupt IAS-2000 v2 until the message has disappeared. This indicates that a complete and successful restart process has finished.

•

Air Live	(www.airlive.com) IAS-2000 v2
Wizard Completed.	Rebooting Now.
Restarting now. Please wait for a momen	ıt.

Caution: During every step of the wizard, if you wish to go back to modify the setting. Please click the **Back** button to go back to the previous step.

5.1.2 System Information

System Information	
System Name	Internet Access Ga
Device Name	(FQDN for this device)
Home Page	Enable Disable http://www.airlive.com *(e.g.
Remote Management IP	*(e.g. 192.168.3.1 or 192.168.3.0/24)
SNMP	○ Enable ④ Disable
User Logon SSL	⊙ Enable ○ Disable
System Time	Device Time:2008/09/26 16:41:53 Enable NTP NTP NTP Server Time Zone (GMT+08:00)Taipei Set Device Date and Time (UTC)
History Report Interval	

These are some main information about IAS-2000 v2. Please refer to the following description for these blanks:

- System Name: Set the system's name or use the default.
- Device Name: FQDN (Fully-Qualified Domain Name). This is used as the domain name used in login page. For example, if Device Name=IAS-2000v2.com, the URL of login page will be https://IAS-2000v2.com/loginpages/login.shtml
- 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 here. Usually, the homepage is the company's website or a popular 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.
- **Remote Management IP:** Set a specific IP or the IP range or subnet with a system which is able to connect to the web management interface via the WAN port. For example, 10.2.3.0/24 means that as long as an administrator is within the IP address range of 10.2.3.0/24, user can reach the administration page of IAS-2000.
- **SNMP:** IAS-2000 v2 supports SNMPv2 and SNMPv3. If the function is enabled, assign the Manager IP and the community of SNMPv2 and SNMPv3 to access the management information base (MIB) of the system.
- User Logon SSL: Enable SSL when user login with encryption to have a safer login process.

System Time: IAS-2000 v2 supports NTP communication protocol to synchronize the network time. Please specify the IP address of a NTP server and select the desired time zone in the system configuration interface for adjusting the time automatically. (Universal Time is Greenwich Mean Time, GMT). Time can also be set manually when by selecting "Set Device Date and Time". Please enter the date and time for these fields.

	Device Time:2008/09/26 16:41:53
System Time	Enable NTP NTP tock.usno.navy.mil *(e.g. tock.usno.navy.mil)
	Time Zone (GMT+08:00)Taipei
	O Set Device Date and Time (UTC)

• History Report Interval: Time interval for sending the history notice.
5.1.3 WAN1 Configuration

WAN1 Configuration			
	 Static IP Address 		
	IP Address:	60.250.158.64	-
	Subnet Mask:	255.255.255.0	•
	Default Gateway:	60.250.158.254].
WAN1 Port	Preferred DNS Server:	192.168.0.254]•
	Alternate DNS Server:		
	Enable Bridge Mode		
	 Dynamic IP Address PPPoE Client 		

There are 3 methods that WAN1 Port supports: Static IP Address, Dynamic IP Address, and PPPoE Client.

- Static IP Address: Manually specifying the IP address of the WAN1 Port which is applicable for the network environment where the DHCP service is unavailable. The option of 802.3ad for WAN2 is only available when WAN1 is using a static IP address. The fields with red asterisks are required. Please fill in these fields.
 - > **IP Address:** The IP address of the WAN1 port.
 - > Subnet Mask: The subnet mask of the WAN1 port.
 - > Default Gateway: The gateway of the WAN1 port.
 - > Preferred DNS Server: The primary DNS Server of the WAN1 port.
 - > Alternate DNS Server: The substitute DNS Server of the WAN1 port. This is not required.
 - Enable Bridge Mode: WAN1 is set to use a static IP address and "Enable Bridge Mode" is checked, WAN2 and all LAN ports will share the WAN1 IP address and go into bridge mode as well. See the following figures. The PC connected to LAN1 or LAN 2 must be set to static IP address manually, or it can receive the IP address from upper DHCP server via WAN1. The IP address they received is the same IP subnet with WAN1 IP.

WAN1 Configuration			
	 Static IP Address 		
	IP Address:	60.250.158.64	•
	Subnet Mask:	255.255.255.0	-
	Default Gateway:	60.250.158.254	•
WAN1 Port	Preferred DNS Server:	168.95.1.1]-
	Alternate DNS Server:		
	Enable Bridge Mode		
	O Dynamic IP Address		
	PPPoE Client		

WAN2 & Failover		
WAN2	Bridge Mode	

LAN1 Configuration		
LAN1	Bridge Mode	

LAN2 Configuration		
LAN2	Bridge Mode	

• **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.

WAN1 Configuration	
WAN1 Port	 Static IP Address Dynamic IP Address PPPoE Client

• **PPPoE Client:** When selecting PPPoE to connect to the network, please enter the "Username" and "**Password**". 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.

WAN1 Configuration		
	 Static IP Address Dynamic IP Address PPPoE Client 	255
	User Name:	86128161@hinet.net -
WAN1 Port	Password:	•••••••
	MTU:	1492 bytes (Range :1000~1492)*
	CLAMPMSS:	1400 bytes (Range :980~1400)*
	Dial on Demand:	🔘 Enable 💿 Disable

5.1.4 WAN2 & Failover

There are 3 methods of obtaining an IP address for the WAN2 Port: **None**, **Static IP Address**, and **Dynamic IP Address**.

• **None:** The WAN2 Port is not functional.

WAN2 & Failover		
WAN2 Port	 None Static IP Address Dynamic IP Address 	
Connection Detection & WAN Failover	Probe Target URL1: http:// URL2: http:// URL3: http:// Warning of Internet Disconnection	

> Warning of Internet Disconnection: Enable to detect the WAN1 port connection status.

WAN2 & Failover		
WAN2 Port	 None Static IP Address Dynamic IP Address 	
Connection Detection & WAN Failover	Probe Target URL1: http:// www.google.com URL2: http:// URL3: http:// ✓ Warning of Internet Disconnection When Internet Connection is down, the system will display the warning messages as: Sorry! The service is temporarily unavailable. ★	

- Static IP Address: Specify the IP Address, Subnet Mask, Default Gateway of WAN2 Port and Preferred DNS Server, which should be applicable for the network environment. Up to three URLs can be entered. Check "Warning of Internet Disconnection" to work with the WAN Failover function.
 - > WAN Failover: When WAN1 connection fails, the traffic will be routed to WAN2 automatically.
 - Fallback to WAN1 when possible: When WAN1 connection is recovered, the routed traffic will be back to WAN1.

WAN2 & Failover			
	 ○ None ④ Static IP Address 		
	IP Address:	59.124.2.55	•
	Subnet Mask:	255.255.255.0].
WAN2 Port	Default Gateway:	59.124.2.254].
	Preferred DNS Server:	168.95.1.1	*
	Alternate DNS Server:]
	O Dynamic IP Address		
	Probe Target		
	URL1: http:// www.google.com		
	URL2: http://		
	URL3: http://		
Connection Detection &	WAN Failover		
WAN Failover	Fallback to WAN1 when possible		
	✓ Warning of Internet Disconnection		
	When Internet Connection is down, the system will display the warning messages as:		
	Sorry! The service is temporarily unavailable. *		

• **Dynamic IP Address:** Select this when WAN2 Port can obtain IP address automatically, such as a DHCP Server available from WAN2 Port. Up to three URLs can be entered. Check "**Warning of Internet Disconnection**" to work with the **WAN Failover** function.

WAN2 & Failover		
WAN2 Port	 None Static IP Address Dynamic IP Address 	
Connection Detection & WAN Failover	Probe Target URL1: http:// www.google.com URL2: http:// URL3: http:// ✓ WAN Failover Fallback to WAN1 when possible ✓ Warning of Internet Disconnection When Internet Connection is down, the system will display the warning messages as: Sorry! The service is temporarily unavailable.	

For Dynamic IP Address, **WAN Failover** and **Fallback to WAN1 when possible** also can be enabled like as the function for **Static IP Address**. If **Warning of Internet Disconnection** is enabled, a warning message can be entered to indicate what the system should display when Internet connection is down.

5.1.5 LAN1 Configuration

User authentication can be chosen to enable or disable in LAN1 port. In this part, you can set the related configurations about LAN1 port and DHCP server.

LAN1 Configuration		
LAN1	Enable User AuthenticationOperation ModeNATIP Address:192.168.1Subnet Mask:255.255.2	 ✓ .254 * .55.0 *
DHCP Server Configuration	 Disable DHCP Server Enable DHCP Server DHCP Scope Start IP Address: End IP Address: Preferred DNS Server: Alternate DNS Server: Domain Name: WINS Server: Lease Time Reserved IP Address Ling Enable DHCP Relay 	192.168.1.101 * 192.168.1.200 * 168.95.1.1 * airlive.com * 1 Day ▼ st

• DHCP Server Configuration

> **Disable DHCP Server:** Disable the function of the DHCP Server.

LAN1 Configuration		
LAN1	Enable User Authentication Operation Mode NAT IP Address: 192.168.1.254 * Subnet Mask: 255.255.0 *	
DHCP Server Configuration	 Disable DHCP Server Enable DHCP Server Enable DHCP Relay 	

Enable DHCP Server: Enter proper setting of Start IP Address, End IP Address, Preferred DNS Server, Alternate DNS Server, Domain Name, WINS Server, Lease Time, and Reserved IP Address List. See the following figure. Fields marked with red asterisks must be filled in.

LAN1 Configuration		
LAN1	Enable User AuthenticationOperation ModeNATIP Address:192.168.1Subnet Mask:255.255.2	 ✓ .254 * .55.0 *
DHCP Server Configuration	 Disable DHCP Server Enable DHCP Server DHCP Scope Start IP Address: End IP Address: Preferred DNS Server: Alternate DNS Server: Domain Name: WINS Server: Lease Time Reserved IP Address Lit Enable DHCP Relay 	192.168.1.101 * 192.168.1.200 * 168.95.1.1 * airlive.com * 1 Day ▼ st

Reserved IP Address List: Click on the Reserved IP Address List on the management interface to fill in the reserved IP addresses if desired. 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 Description (not compulsory). When finished, click *Apply* to complete the setup.

Reserved IP Address List LAN 1			
Item	Reserved IP Address	MAC	Description
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
	(Total:40) <u>First Prev Next Last</u>		

Enable DHCP Relay : Specify other DHCP Server IP address if using DHCP Relay is desired. See the following figure.

LAN1 Configuration		
LAN1	Enable User Authentication Operation Mode NAT IP Address: 192.168.1.254 * Subnet Mask: 255.255.25.0 *	
DHCP Server Configuration	 Disable DHCP Server Enable DHCP Server Enable DHCP Relay DHCP Server IP: * 	

Enable VLAN: If you want to split LAN1 to several VLANs, please select the Enable VLAN. After Enable VLAN is selected, the following screen will appear. Choose the desired Item and click Edit for further configuration. See the following figure.

VLAN	Activate VLAN and Edit	VLAN List 🗹	
	VLAN	List	
Item	Тад	Status	
1		Disabled	Edit
2		Disabled	Edit
3		Disabled	Edit
4		Disabled	Edit
5		Disabled	Edit
6		Disabled	Edit
7		Disabled	<u>Edit</u>

The system will need confirmation for enabling individual VLAN segment. Click *Enable* to continue. See the following figure.

After enabling this VLAN segment, the following screen will appear. See the following description and figure for details.

• Enable User Authentication (on this individual VLAN):

VLAN Interface Configuration		
	Enable	
	Enable User Authentication	
	VLAN Tag	* (Range: 2~4094)
VLAN	Mode	NAT 💌
	IP Address	*
	Subnet Mask	*
VLAN DHCP Configuration	 Disable DHCP Server Enable DHCP Server DHCP Relay 	

- > Enable: Enable this VLAN segment.
- Enable User Authentication: Choose to enable or disable user authentication for this individual VLAN segment.
- > VLAN Tag: Enter any integer number within the range of 2~4094 as the Tag for this VLAN segment.
- > **Mode:** Two modes are provided: NAT mode and ROUTER mode.
 - NAT: All IP addresses externally connected through the VLAN port (these IP addresses must belong to the same network of the VLAN port) will be converted into the IP address of the WAN1 port by IAS-2000 v2 and onward to outside the network.
 - Router: All IP addresses externally connected through the VLAN port use its original IP addresses for external connection. Thus, IAS-2000 v2 acts like a Router.
- > IP Address: Enter the desired IP address for this VLAN.
- > Subnet Mask: Enter the desired Subnet Mask for this VLAN.

• VLAN DHCP Configuration

> **Disable DHCP Server:** Disable the function of the DHCP Server of IAS-2000 v2.

VLAN DHCP Configuration	 Disable DHCP Server Enable DHCP Server DHCP Relay
----------------------------	---

Enable DHCP Server: If you want to use the DHCP Server function of IAS-2000 v2, set proper configurations is necessary. Related information needed on setting up the DHCP Server is described as follows: Start IP Address, End IP Address, Preferred DNS Server, Alternate DNS Server, Domain Name, WINS Server, Lease Time, and Reserved IP Address List. See the following figure.

	 Disable DHCP Server Enable DHCP Server DHCP Scope 	
	Start IP Address	*
	End IP Address	*
VLAN DHCP Configuration	Preferred DNS Server	168.95.1.1 *
	Alternate DNS Server	
	Domain Name	ovislink.com *
	WINS Server	
	Lease Time	1 Day 💌
	Reserved IP Address Li	<u>st</u>
	O DHCP Relay	

Reserved IP Address List: If you want to use the reserved IP address function, 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 Description (not compulsory). When finished, click *Apply* to complete the setup.

Reserved IP Address List VLAN Tag:			
Item	Reserved IP Address	MAC	Description
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
(Total:40) <u>First Prev Next Last</u>			

Enable DHCP Relay: If you want to enable this function, you must specify a DHCP Server IP address. See the following figure.

VLAN DHCP Configuration	 Disable DHCP Server Enable DHCP Server DHCP Relay 	
	DHCP Server IP	*

5.1.6 LAN2 Configuration

User authentication can be chosen to enable or disable in LAN2 port. In this part, you can set the related configurations about LAN2 port and DHCP server.

LAN2 Configuration		
LAN2	Enable User AuthenticationOperation ModeNATIP Address:192.168.2Subnet Mask:255.255.2	× .254 * .55.0 *
DHCP Server Configuration	 Disable DHCP Server Enable DHCP Server DHCP Scope Start IP Address: End IP Address: Preferred DNS Server: Alternate DNS Server: Domain Name: WINS Server: Lease Time Reserved IP Address Lit Enable DHCP Relay 	192.168.2.101 * 192.168.2.200 * 192.168.2.254 * domain * 1 Day V

• DHCP Server Configuration

> **Disable DHCP Server:** Disable the function of the DHCP Server.

LAN2 Configuration		
LAN2	Enable User Authentication Operation Mode NAT IP Address: 192.168.2.254 * Subnet Mask: 255.255.25.0 *	
DHCP Server Configuration	 Disable DHCP Server Enable DHCP Server Enable DHCP Relay 	

Enable DHCP Server: Enter proper setting of Start IP Address, End IP Address, Preferred DNS Server, Alternate DNS Server, Domain Name, WINS Server, Lease Time, and Reserved IP Address List. See the following figure. Fields marked with red asterisks must be filled in.

LAN2 Configuration			
LAN2	Enable User AuthenticationOperation ModeNATIP Address:192.168.2Subnet Mask:255.255.2	254 * 55.0 *	
DHCP Server Configuration	 Disable DHCP Server Enable DHCP Server DHCP Scope Start IP Address: End IP Address: Preferred DNS Server: Alternate DNS Server: Domain Name: WINS Server: Lease Time Reserved IP Address Ling Enable DHCP Relay 	192.168.2.101 * 192.168.2.200 * 192.168.2.254 * domain * 1 Day ♥ st	

Reserved IP Address List: Click on the Reserved IP Address List on the management interface to fill in the reserved IP addresses if desired. 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 Description (not compulsory). When finished, click *Apply* to complete the setup.

Reserved IP Address List LAN 2			
Item	Reserved IP Address	MAC	Description
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
(Total:40) <u>First Prev Next Last</u>			

Enable DHCP Relay : Specify other DHCP Server IP address if using DHCP Relay is desired. See the following figure.

LAN2 Configuration			
LAN2	Enable User Auth Operation Mode IP Address: Subnet Mask:	NAT 192.168.2.254 255.255.255.0	*
DHCP Server Configuration	 Disable DHCF Enable DHCP Enable DHCP DHCP Server 	P Server Server Relay r IP:	*

Enable VLAN: If you want to split LAN2 to several VLANs, please select the Enable VLAN. After Enable VLAN is selected, the following screen will appear. Choose the desired Item and click Edit for further configuration. See the following figure.

VLAN	Activate VLAN and Edit V	/LAN List 🔽	
	VLAN	List	
Item	Tag	Status	
1		Disabled	Edit
2		Disabled	Edit
3		Disabled	Edit
4		Disabled	Edit
5		Disabled	Edit
6		Disabled	Edit
7		Disabled	Edit

The system will need confirmation for enabling individual VLAN segment. Click *Enable* to continue. See the following figure.

After enabling this VLAN segment, the following screen will appear. See the following description and figure for details.

• Enable User Authentication (on this individual VLAN):

VLAN Interface Configuration			
	Enable		
	Enable User Authentication	\checkmark	
	VLAN Tag	* (Range: 2~4094)	
VLAN	Mode	NAT 💌	
	IP Address	*	
	Subnet Mask	*	
VLAN DHCP Configuration	 Disable DHCP Server Enable DHCP Server DHCP Relay 		

- > **Enable:** Enable this VLAN segment.
- Enable User Authentication: Choose to enable or disable user authentication for this individual VLAN segment.
- > VLAN Tag: Enter any integer number within the range of 2~4094 as the Tag for this VLAN segment.
- > **Mode:** Two modes are provided: NAT mode and ROUTER mode.
 - NAT: All IP addresses externally connected through the VLAN port (these IP addresses must belong to the same network of the VLAN port) will be converted into the IP address of the WAN1 port by IAS-2000 v2 and onward to outside the network.
 - Router: All IP addresses externally connected through the VLAN port use its original IP addresses for external connection. Thus, IAS-2000 v2 acts like a Router.
- > IP Address: Enter the desired IP address for this VLAN.
- > Subnet Mask: Enter the desired Subnet Mask for this VLAN.
- VLAN DHCP Configuration
 - > **Disable DHCP Server:** Disable the function of the DHCP Server of IAS-2000 v2.

VLAN DHCP Configuration	 Disable DHCP Server Enable DHCP Server DHCP Relay
----------------------------	---

Enable DHCP Server: If you want to use the DHCP Server function of IAS-2000 v2, set proper configurations is necessary. Related information needed on setting up the DHCP Server is described as follows: Start IP Address, End IP Address, Preferred DNS Server, Alternate DNS Server, Domain Name, WINS Server, Lease Time, and Reserved IP Address List. See the following figure.

	 Disable DHCP Server Enable DHCP Server DHCP Scope 	
	Start IP Address	*
	End IP Address	*
VI AN DHCP	Preferred DNS Server	168.95.1.1 *
Configuration	Alternate DNS Server	
	Domain Name	vislink.com *
	WINS Server	
	Lease Time 1 Day 💌	
	Reserved IP Address Li	<u>st</u>
	O DHCP Relay	

Reserved IP Address List: If you want to use the reserved IP address function, 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 Description (not compulsory). When finished, click *Apply* to complete the setup.

Reserved IP Address List VLAN Tag:			
Item	Reserved IP Address	MAC	Description
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
(Total:40) <u>First Prev Next Last</u>			

Enable DHCP Relay: If you want to enable this function, you must specify a DHCP Server IP address. See the following figure.

VLAN DHCP Configuration	 Disable DHCP Server Enable DHCP Server DHCP Relay 			
	DHCP Server IP		*	

5.2 Network Configuration

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

Air Live	IAS	(www.airlive.com) Image: Logout G-2000 v2 Internet Access Gateway	
System Configuration Co	Network onfiguration A	User Utilities Status	
	Network Co	nfiguration	
Network Address Translation	Network Configuration		
Privilege List	Network Address Translation	System provides three types of Network Address Translation: DMZ, Virtual Server and Port/IP Redirection.	
Monitor IP List	Privilege List	System provides Privilege IP Address List and Privilege MAC Address List. Authentication is NOT required for those listed devices. Policies defined in "User Authentication" can be applied to devices in MAC Address List as well.	
Proxy Server Properties	Monitor IP List System can monitor up to 40 network devices using IP packet periodically. Walled Garden List Up to 20 URLs or IP addresses could be defined in Walled Gardet List. Clients may access these sites without authentication.		
Dynamic DNS			
	Proxy Server Properties	System has one built-in Proxy Server and supports up to 20 external Proxy Servers.	
IP Mobility	Dynamic DNS	System supports dynamic DNS (DDNS) to translate WAN IP to a domain name automatically.	
IP Mobility System supports IP PNP and Mobile IP Configuration			
		(b)	

5.2.1 Network Address Translation

There are three parts, DMZ, Virtual Servers and Port and IP Redirect, need to be set.

Network Address Translation		
DMZ		
Virtual Servers		
Port and IP Redirection		

• DMZ

DMZ (**De-M**ilitarized **Z**one) allows administrators to define mandatory external to internal IP mapping; hence a user on WAN side network can access the private machine via the external IP (similar to DMZ usage in firewall product). There are 40 sets of static **Internal IP Address** and **External IP Address** available. If a host needs a static IP address to access the network through WAN port, set a static IP for the host. These settings will become effective immediately after clicking the **Apply** button.

DMZ			
Item	Internal IP Address	External IP Address	
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			

Virtual Servers

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 via WAN port IP of IAS-2000 v2. 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.

		Virtual Se	rvers		
Item	External Service Port	Local Server IP Address	Local Server Port	Туре	Enable
1				O TCP O UDP	
2				O TCP	
3				O TCP O UDP	
4				O TCP O UDP	
5				O TCP O UDP	
6				O TCP O UDP	
7				O TCP O UDP	
8				O TCP O UDP	
9				O TCP O UDP	
10				O TCP O UDP	

• Port and IP Redirection

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

.

Port and IP Redirection					
	Original Destin	ation	Redirect to)	T
Item	IP Address	Port	IP Address	Port	Туре
1					O TCP O UDP
2					O TCP O UDP
3					O TCP O UDP
4					O TCP O UDP
5					O TCP O UDP
6					O TCP O UDP
7					O TCP O UDP
8					O TCP O UDP
9					O TCP O UDP
10					O TCP O UDP

5.2.2 Privilege List

There are two parts, Privilege IP Address List and Privilege MAC Address List, need to be set.

Privilege List
Privilege IP Address List
Privilege MAC Address List

Privilege IP Address List

If there are some workstations belonging to the managed server that need to access the network without authentication, and enter the IP addresses of these workstations in this list. The "**Remark**" blank is not necessary but is useful to keep track. IAS-2000 v2 allows 100 privilege IP addresses at most. These settings will become effective immediately after clicking *Apply*.

	Privilege IP Address List				
Item	Privilege IP Address	Remark			
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					

Warning: Permitting specific IP addresses to have network access rights without going through standard authentication process at the authenticated LAN may cause security problems.

• Privilege MAC Address List

In addition to the IP address, the MAC address of the workstations that need to access the network without authentication can also be set in this list. IAS-2000 v2 allows 100 privilege MAC addresses at most. The list can be created by entering data in the table or by import from a file. The list can be exported as well.

Be sure to enter the MAC address (the format is xx:xx:xx:xx:xx) as well as the remark (not necessary) if manually creating the list is desired, and select a policy for the individual entry. These settings will become effective immediately after clicking *Apply*.

Attention: No matter how you choose to create the list, you must select an Access Gateway first.

	Privilege MAC Address List			
	MAC	Import List Export List		
Item	MAC Address	Policy	Remark	
1		Policy1 🗸		
2		Policy1 🗸		
3		Policy1 🗸		
4		Policy1 🗸		
5		Policy1 🗸		
6		Policy1 🗸		
7		Policy1 🗸		
8		Policy1 🗸		
9		Policy1 🗸		
10		Policy1 🗸		

Warning: Permitting specific MAC addresses to have network access rights without going through standard authentication process at the authenticated LAN may cause security problems.

Import List: Select an Access Gateway and then click Import List to enter the Upload Privilege MAC Address List interface. Click the Browse button to select the text file for the user account upload. Then click Submit to complete the upload.

Import Privilege MAC Address List		
Note: The format of each line is "MAC, Policy, Remark" without the quotes. There must be no space between the fields and commas. The Remark field could be omitted but the leading comma must be retained. While uploading the list, existing MAC address in the Privilege MAC Address List will not be replaced.		
Upload MAC Address		
File Name Browse		

The uploading file should be a text file and the format of each line is "*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.



Export List: Click this to export the Mac List to create a .txt file and then save it on disk.

File Dov	vnload 🛛 🛛 🗙
Do yo	u want to open or save this file?
11 II.	Name: privilege_mac_address.txt Type: Text Document, 2 bytes From: 192.168.0.84
	Open Save Cancel
1	While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. <u>What's the risk?</u>

5.2.3 Monitor IP List

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

		r IP List				
		Admin	Email			
Send Fr	om					
Send	То					
Interv	al	6 Hour	6 Hours 🗸			
SMTP Se	erver					
Auth Me	thod	NONE	~			
Send Test	Email	send				
Item	IP Addres	S	Item	IP Address		
1			2			
3			4			
5			6			
7			8			
9			10			
11			12			
13			14			
15			16			
17			18			
19			20			

- Send From: The e-mail address of the administrator in charge of the monitoring. This will show up as the sender's e-mail.
- Send To: The e-mail address of the person whom the monitoring result is for. This will be the receiver's e-mail.
- **Interval:** The time interval to send the e-mail report.
- **SMTP Server:** The IP address of the SMTP server.

- Auth Method: The system provides four authentication methods, PLAIN, LOGIN, CRAM-MD5 and NTLMv1, or "NONE" to use none of the above. Depending on which authentication method selected, enter the Account Name, Password and Domain.
- Send Test Email: Click "Send" to send out a test e-mail of the IP monitoring report.
- IP Address: The IP addresses under monitoring.

In the **Monitor IP result** page, green light means the IP address is alive and reachable. On the other hand, red light means the IP address is not reachable now. The administrator can understand the some networking devices by this feature.

Monitor IP Result			
Item	IP Address	Result	
1	192.168.0.201	9	
2	192.168.0.145	9	
3	192.168.0.245	6	

5.2.4 Walled Garden List

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

Walled Garden List			
Item	Address	Item	Address
1		2	
3		4	
5		6	
7		8	
9		10	
11		12	
13		14	
15		16	
17		18	
19		20	

5.2.5 Proxy Server Properties

IAS-2000 v2 supports Internal Proxy Server and External Proxy Server functions. Please perform the necessary configurations.



	External Proxy Server			
Item	Server IP	Port		
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				

- Internal Proxy Server: IAS-2000 v2 has a built-in proxy server. If this function is enabled, the end users will be forced to treat IAS-2000 v2 as the proxy server regardless of the end-users' original proxy settings.
- External Proxy Server: Under the IAS-2000 v2 security management, the system will match the External Proxy Server list to the end-users' proxy setting. If there isn't a matching, then the end-users will no be able to reach the login page and thus unable to access the network. If there is a matching, then the end-users will be directed to the system first for authentication. After a successful authentication, the end-users will be redirected back to the desired proxy servers depending on various situations.

Please click *Apply* and these settings will become effective immediately. For more details about how to set proxy servers, please see Appendix D and E.

5.2.6 Dynamic DNS

IAS-2000 v2 provides a convenient DNS function to translate the IP address of WAN port to a domain name that helps the administrator memorize and connect to WAN port. If the DHCP is activated at WAN port, this function will also update the newest IP address regularly to the DNS server. These settings will become effective immediately after clicking *Apply*.

DDNS	◯ Enable ④ Disable	
Provider	DynDNS.org(Dynamic) 🗸	
Host name	•	
Username/E-mail	•	
Password/Key	•	

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

Please click *Apply* and these settings will become effective immediately.

5.2.7 IP Mobility

IP PNP	Enable
Mobile IP	Enable

• IP PNP

Clients can use any IP address to connect to the system. Regardless of what the IP address at the client end is, he or she can still authenticate through IAS-2000 v2 and access the network.

• Mobile IP

If several sets of IAS-2000 v2 are used to construct a network environment, a client can use the same group of IP configurations. When a client roams into different locations, the connection will be kept alive; therefore no disconnection will occur when, for example, downloading data.

5.3 User Authentication

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

Air Live	IAS-:	2000 v2	(www.airlive.	com) 💿 Logout eway 🅄 Help
System Configuration	Network Configuration Auth	User	Utilities	Status
	💼 User Authenti	cation		
Authentication Configuration	User Authentication			
Policy Configuration Black List Configuration	Authontication	System provides 9 external server configurations (POP3, RADIUS, LDAP and NT Domain), one internal user DB (Local User) and two pre-defined mechanisms for paying users (On-Demand User and PMS) to authenticate user access. Each authentication or the pay of the pay o		
Guest User Configuration	Configuration	control. Regarding paying users, On-Demand Server Configuration supports print-out of user account information from an optional ticket printer. As for PMS, PMS Server Configuration supports		
	Policy Configuration	Fidelio Property Manageme rts one Global and 10 pc an define a policy with the gin schedule profile, and ba	elio Property Management System Billing. one Global and 10 policies for traffic control define a policy with the firewall profile, specific schedule profile, and bandwidth	
	Black List Configuration	System supports 5 Black Lists for authentication. On-Demand and PMS Server DOES NOT support Black List configuration.		
	Guest User Configuration	System provides up to 10 guest accounts. Guest permission different from general user accounts. G are stored on embedded-database under Global po		
	Additional Configuration	System suppor Idle/Session t logout, and Per It also suppor certificate file.	ts other authentication setti imeout, Multiple login e mit MAC address list ts uploading customized l	ings, such as: nable/disable, Friendly login/logout pages and
		(

5.3.1 Authentication Configuration

This function is to configure the settings for different authentication servers. The system provides 10 servers (Local, POP3, RADIUS, LDAP and NT Domain), one On-demand User and one PMS User that the administrator can apply with different policies. 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 screen to choose a server to be the default server and enable or disable any server on the list.

Authentication Configuration					
Server Name	Auth Method	Postfix	Policy	Default	Enable
LOCAL	LOCAL	Postfix1	Policy1	۲	~
LDAP	LDAP	Postfix2	Policy1	0	
RADIUS Server	RADIUS	Postfix3	Policy1	0	
LDAP Server	LDAP	Postfix4	Policy1	0	
NT Domain	NTDOMAIN	Postfix5	Policy1	0	
POP3 Server	POP3	Postfix6	Policy1	0	
RADIUS Server	RADIUS	Postfix7	Policy1	0	
LDAP Server	LDAP	Postfix8	Policy1	0	
NT Domain	NTDOMAIN	Postfix9	Policy1	0	
POP3 Server	POP3	Postfix10	Policy1	0	
On Demand User	ONDEMAND	ondemand	Policy1	0	
PMS User	PMS	pms	Policy1	0	

5.3.1.1 Local Server

Authentication Server - LOCAL LOCAL Server Name *(Its server name.) Server Status Enable Postfix Postfix1 **(Its postfix name.) ¥ Blacklist None Local User Account Local User Setting Policy1 🗸 Policy Name Apply Clear

This server is only for "Local User" and the authentication method can not be changed for this server.

- Server Name: Set a name for the server using numbers (0 to 9), alphabets (a to z or A to 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 by using numbers (0 to 9), alphabets (a to z or A to Z), dash (-), underline (_) and dot (.) with a maximum of 40 characters, all other letters are not allowed.
- Blacklist: There are five sets of the black lists. Select one of them or choose "None". Please refer to 5.3.3 Black List Configuration
- Local User Account: Click the Local User Setting hyperlink to set the further configuration.
- **Policy Name:** There are ten policies to choose from to apply to this particular server.

Click the *Local User Setting* hyperlink for further configuration.

Local User Setting			
Edit Local User List			
Radius Roaming Out	○ Enable ⊙ Disable		
802.1x Authentication	○ Enable		

• Edit Local User List: Click this to enter the "Local User List" screen.

Add User Import List Export List Refresh					
Search					
User List					
lleornamo	Decoword	MAC	Policy		
USemanie	Username Password	MAC	Remark	DerAil	
jacky	1111		None	Doloto	
				Delete	

Add User: Click this button to enter the Add User page. Fill in the necessary information such as "Username", "Password", "MAC" (optional) and "Remark" (optional). Select a desired Maximum Bandwidth, Request Bandwidth and Policy.

Add User					
Item	Username	MAC	Maximum Bandwidth	Policy	
	Password	(XX:XX:XX:XX:XX:XX)	Request Bandwidth	Remark	
	jacky		5 Mbps 🖌	Policy1 🗸	
1	1234		2 Mbps 💉	In door	
	josh		10 Mbps 💌	Policy3 🗸	
2	1111	00:4F:63:01:37:EA	None 💌		
_	Ryan		Unlimited 🐱	Policy2 🗸	
3	2222		None 💌		
4			Unlimited 🐱	None 🗸	
			None 🗸		
Click Apply to complete adding the user or users

Successfully added user(s): jacky josh ryan				
		Add User	r	
Itom	Username	MAC	Maximum Bandwidth	Policy
item	Password	(XX:XX:XX:XX:XX:XX)	Request Bandwidth	Remark
4			Unlimited 🐱	None 🗸
1			None 💌	
2			Unlimited 🐱	None 🗸
2			None 💌	
2			Unlimited 🐱	None 🗸
3			None 🗸	

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

🏥 Upload User

Note: The format of each line is "ID, Password, MAC, Policy, Remark" or "ID, Password, MAC, Max bandwidth, Request bandwidth, Policy, Remark" without the quotes. There must be no space 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, 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	Browse		

The uploading file should be a text file and the format of each line is "*ID*, *Password*, *MAC*, *Policy*, *Remark*" or "*ID*, *Password*, *MAC*, *Max bandwidth*, *Request bandwidth*, *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.





> Export List: Click this to create a .txt file and then save it on disk.



Refresh: Click this to refresh the list.

Add User Import List Export List Refresh						
	Search					
		User List				
lleornamo	Deceword	MAC	Policy			
USername	Password	MAC	Remark	DerAil		
jacky	1234		Policy1	Delete		
				Delete		
<u>josh</u>	1111	00.45.62.01.37.54	Policy3	Delete		
		00.41.03.01.37.EA		Delete		
<u>ryan</u>	2222		Policy2	Delete		
				Delete		

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

Add User Import List Export List Refresh					
j Search					
		User List			
lleornamo	Decoword	MAC	Policy		
USername	Passworu	Remark		Der All	
jacky	1234		Policy1	Delete	
				Delete	
<u>josh</u>	1111	00-4E-62-01-37-EA	Policy3	Delete	
		00.41.03.01.37.EA		Delete	

- > **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 needed, 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", "Maximum Bandwidth", "Request Bandwidth", "Policy" and "Remark" (optional). Then, click *Apply* to complete the modification.

Edit User			
Username	josh •		
Password	•		
MAC	00:4F:63:01:37:EA		
Maximum Bandwidth	10 Mbps 💌		
Request Bandwidth	None 💌		
Policy	Policy3 💌		
Remark	long term		

• Radius Roaming Out / 802.1x Authentication: These 2 functions can be enabled or disabled by checking the radio button. Checking either of them makes the hyperlink called *Radius Client List* show up.

Local User Setting			
Edit Local User List			
Radius Roaming Out	● Enable ○ Disable		
802.1x Authentication	● Enable ○ Disable		
	Radius Client List		

Click the hyperlink of *Radius Client List* to enter the **Radius Client Configuration** interface. Choose the desired type, **Disable**, **Roaming Out** or **802.1x** and key in the related data and then click *Apply* to complete the settings.

Radius Client Configuration					
No.	Туре	IP Address	Segment	Secret	
1	Roaming Out 💌	10.0.0.0	255.0.0.0 (/8)	12345678	
2	Disable 🗸		255.255.255.255 (/32) 💌		
3	Disable 🗸		255.255.255.255 (/32) 💌		
4	Disable 🗸 🗸		255.255.255.255 (/32) 💌		
5	Disable 🗸 🗸		255.255.255.255 (/32) 💌		
6	Disable 🗸 🗸		255.255.255.255 (/32) 💙		

- Radius Roaming Out: When "Radius Roaming Out" is selected, local users can login from other domains by using their original accounts.
- 802.1x Authentication: 802.1x is a security standard for wired and wireless LANs. It encapsulates EAP (Extensible Authentication Protocol) processes into Ethernet packets instead of using the protocol's native PPP (Point-to-Point Protocol) environment, thus reducing some network overhead. It also puts the bulk of the processing burden upon the client (called a supplicant in 802.1x parlance) and the authentication server (such as a RADIUS), letting the "authenticator" middleman simply pass the packets back and forth.

5.3.1.2 POP3 Server

POP3, RADIUS, LDAP and NT Domain Server can be chosen to be the authentication method. Choose "**POP3**" in the **Authentication Method** field, the hyperlink beside the pull-down menu will become "**POP3 Setting**".

Authentication Server - POP3 Server				
Server Name	POP3 Server **(Its server name.)			
Server Status	Disable			
Postfix	Postfix6 **(Its postfix name.)			
Blacklist	None 💌			
Authentication Method	POP3 POP3 Setting			
Policy Name Policy1 V				
Apply X Clear				

- Server Name: Set a name for the server using numbers (0 to 9), alphabets (a to z or A to 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 by using numbers (0 to 9), alphabets (a to z or A to Z), dash (-), underline (_) and dot (.) with a maximum of 40 characters, all other letters are not allowed.
- Blacklist: There are five sets of the black lists. Select one of them or choose "None". Please refer to 5.3.3 Black List Configuration
- Authentication Method: There are four authentication methods, POP3, Radius, LDAP and NTDomain to configure from. Select the desired method and then click the link besides the pull-down menu for more advanced configuration.
- **Policy Name:** There are ten policies to choose from to apply to this particular server.

Click the hyperlink of **POP3 Setting** 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 POP3 Server			
Server IP	mail.airlive.com *(Domain Name/IP Address)		
Port	110 *(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 the ISP.
- **Port:** Enter the Port given by the ISP. The default value is 110.
- SSL Setting: If this option is enabled, the POP3 protocol will perform the authentication.

5.3.1.3 Radius Server

Choose "Radius" in the Authentication Method field, the hyperlink beside the pull-down menu will become "RADIUS Setting".

Authentication Server - RADIUS Server				
Server Name	RADIUS Server	**(Its server name.)		
Server Status	Disable			
Postfix	Postfix3	**(Its postfix name.)		
Blacklist	None 🗸			
Authentication Method	Radius 💌	RADIUS Setting		
Policy Name Policy1 V				
Apply X Clear				

- Server Name: Set a name for the server using numbers (0 to 9), alphabets (a to z or A to 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 by using numbers (0 to 9), alphabets (a to z or A to Z), dash (-), underline (_) and dot (.) with a maximum of 40 characters, all other letters are not allowed.
- Blacklist: There are five sets of the black lists. Select one of them or choose "None". Please refer to 5.3.3 Black List Configuration
- Authentication Method: There are four authentication methods, POP3, Radius, LDAP and NTDomain to configure from. Select the desired method and then click the link besides the pull-down menu for more advanced configuration.
- **Policy Name:** There are ten policies to choose from to apply to this particular server.

Click the hyperlink of **RADIUS Setting** 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 asterisks are necessary information. These settings will become effective immediately after clicking the *Apply* button.

	RADIUS Setting			
802.1x Authentication	Enable O Disable <u>Radius Client List</u>			
Trans Full Name	Enable O Disable			
	Primary RADIUS Server			
Server IP	•			
Authentication Port	*(Default: 1812)			
Accounting Port	*(Default: 1813)			
Secret Key	•			
Accounting Service	○ Enable ⊙ Disable			
Authentication Protocol	CHAP 🗸			
Secondary RADIUS Server				
Server IP				
Authentication Port				
Accounting Port				
Secret Key				
Accounting Service	○ Enable ⊙ Disable			
Authentication Protocol	CHAP 🗸			

- 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. Please refer to Radius Roaming Out/802.1x Authentication in 5.3.1.1 Local User.
- **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.
- 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.

Notice: If Radius Server does not assign idle-timeout value, IAS-2000 v2 will use the local idle-timeout instead.

5.3.1.4 LDAP Server

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

Authentication Server - LDAP				
Server Name	LDAP	**(Its server name.)		
Server Status	Disable			
Postfix	Postfix2	**(Its postfix name.)		
Blacklist	None 🗸			
Authentication Method	LDAP 🔽	LDAP Setting		
Policy Name	Policy1 💌			
Apply X Clear				

- Server Name: Set a name for the server using numbers (0 to 9), alphabets (a to z or A to 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 by using numbers (0 to 9), alphabets (a to z or A to Z), dash (-), underline (_) and dot (.) with a maximum of 40 characters, all other letters are not allowed.
- Blacklist: There are five sets of the black lists. Select one of them or choose "None". Please refer to 5.3.3 Black List Configuration
- Authentication Method: There are four authentication methods, POP3, Radius, LDAP and NTDomain to configure from. Select the desired method and then click the link besides the pull-down menu for more advanced configuration.
- **Policy Name:** There are ten policies to choose from to apply to this particular server.

Click the hyperlink of **LDAP Setting** 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 Address)	
Port	*(Default: 389)	
Base DN	*(CN=,dc=,dc=)	
Binding Type	User Account 💌	
Account Attribute	User Account Anonymous	
	Specified DN Windows AD DAP Server	
Server IP		
Port		
Base DN		
Binding Type	User Account 💌	
Account Attribute	⊙ UID ○ CN	

- Server IP: Enter the IP address/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.
- Binding Type: There are four binding types, User Account, Anonymous, Specific DN and Windows AD to select.
 - User Account: Use the user account's login username and password of the system, and then select one Account Attribute (UID, CN or sAMAccountName) to access the LDAP server.

Primary LDAP Server				
Server IP	*(Domain Name/IP Address)			
Port	*(Default: 389)			
Base DN	*(CN=,do=,do=)			
Binding Type	User Account 🗸			
Account Attribute				

Anonymous: Access the LDAP servers without requiring authentication but only select one Account Attribute (UID, CN or sAMAccountName).

Primary LDAP Server		
Server IP	*(Domain Name/IP Address)	
Port	*(Default: 389)	
Base DN	*(CN=,do=,do=)	
Binding Type	Anonymous 🗸	
Account Attribute	⊙ UID ○ CN ○ sAMAccountName	

Specified DN: Enter more information for the specific DN username and password in the "Bind RDN" and "Bind Password" fields, and then select one Account Attribute (UID, CN or sAMAccountName) to access the LDAP server.

Primary LDAP Server				
Server IP	*(Domain Name/IP Address)			
Port	*(Default: 389)			
Base DN	*(CN=,do=,do=)			
Binding Type	Specified DN 💌			
Bind RDN:				
Bind Password:				
Account Attribute	⊙ UID ○ CN ○ sAMAccountName			

> Windows AD: Enter the domain name of Windows AD to access the LDAP server.

Primary LDAP Server		
Server IP	*(Domain Name/IP Address)	
Port	*(Default: 389)	
Base DN	*(CN=,do=,do=)	
Binding Type	Windows AD 💌	
Domain		

5.3.1.5 NT Domain Server

Choose "NTDomain" in the Authentication Method field, the hyperlink beside the pull-down menu will become "NT Domain Setting".

Authentication Server - NT Domain			
Server Name	NT Domain	**(Its server name.)	
Server Status	Disable		
Postfix	Postfix5	**(Its postfix name.)	
Blacklist	None 💌		
Authentication Method	NTDomain 💌	NT Domain Setting	
Policy Name	Policy1 🗸		
Apply X Clear			

- Server Name: Set a name for the server using numbers (0 to 9), alphabets (a to z or A to 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 by using numbers (0 to 9), alphabets (a to z or A to Z), dash (-), underline (_) and dot (.) with a maximum of 40 characters, all other letters are not allowed.
- Blacklist: There are five sets of the black lists. Select one of them or choose "None". Please refer to 5.3.3 Black List Configuration
- Authentication Method: There are four authentication methods, POP3, Radius, LDAP and NTDomain to configure from. Select the desired method and then click the link besides the pull-down menu for more advanced configuration.
- **Policy Name:** There are ten policies to choose from to apply to this particular server.

Click the hyperlink of NT Domain Setting 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 NT domain controller.
- **Transparent Login:** If this function is enabled, when users log into the Windows domain, they will log into IAS-2000 v2 automatically.

5.3.1.6 On Demand User

This is for the customer's need in a store environment. When the customers need to use wireless 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	Disable	
Postfix	ondemand *(e.g. ondemand. Max: 40 char)	
Receipt Header 1	Welcome! (e.g. Welcome!)	
Receipt Header 2	Header2	
Receipt Footer	Thank You! (e.g. Thank You!)	
Monetary Unit	None ○ £ GBP ○ € EUR ○ \$ USD (Input other desired monetary unit, e.g. AU)	
Policy Name	Policy1 🗸	
WLAN ESSID	ondemand (e.g. ondemand)	
Wireless Key		
Remark	(for customer)	
Billing Notice Interval	● 10mins ○ 15mins ○ 20mins	
Users List Billing Configuration Create On-Demand User		
Apply X Clear		

- 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 by using numbers (0 to 9), alphabets (a to z or A to 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.
- Monetary Unit: Select the desired monetary unit for a region or input the needed monetary unit if not listed.
- **Policy Name:** Select a policy for the on-demand user.
- WLAN ESSID: Enter the ESSID of the AP.
- WEP Key: Enter the WEP key of the AP.
- **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.

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

			[Search	
	On-demand User List					
Username	Password	Remain Time/Volume	Status	Expire Time	Delete All	
2BQU	867E6CDY	30 min	Normal	2008/10/04- 17:16:44	Delete	
V699	S3R376NG	100M 0K bytes	Normal	2008/10/04- 17:16:49	<u>Delete</u>	
M8V4	4KFNRF4A	30 min	Normal	2008/10/04- 17:16:53	Delete	
4A2B	3U5443W4	1 hour	Normal	2008/10/04- 17:16:56	Delete	
W3Y8	WEQ7WQ4K	100M 0K bytes	Normal	2008/10/04- 17:16:59	<u>Delete</u>	

- Search: Enter a keyword of a username to be searched in the text filed 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.
- > **Remain 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.
- **Expire Time:** The expiration time of the account.
- > **Delete All:** This will delete all the users at once.
- > **Delete:** This will delete the users individually.

• **Billing Configuration:** Click this to enter the **Billing Configuration** screen. In the **Billing Configuration** page, Administrator may configure up to 10 billing plans.

Billing Configuration							
Plan	Status		Туре		Expired Info	Valid Duration	Price
1	 Enable Disable 	DataTime	0 0 30	Mbyte Hrs Mins	3 Days 0 Hrs	3 Days	20
2	 Enable Disable 	DataTime	0 1 0	Mbyte Hrs Mins	3 Days 0 Hrs	3 Days	30
3	 Enable Disable 	DataTime	100 0 0	Mbyte Hrs Mins	3 Days 0 Hrs	3 Days	30

- Status: Select to enable or disable this billing plan.
- Type: Set the billing plan by "Data" (the maximum volume allowed is 999,999 Mbyte) or "Time" (the maximum days allowed is 999 Hrs).
- Expired Info: This is the duration of time that the user can use the account after the 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 account after the activation of the account. After this duration, the account will self-expire.
- > **Price:** The price charged for this billing plan.

• Create On-demand User: Click this to enter the On-demand User Generate page.

On-Demand User Generation				
Plan	Туре	Status	Function	
1	0 hrs 30 mins	Enabled	Create	
2	1 hrs 0 mins	Enabled	Create	
3	100Mbyte	Enabled	Create	
4	N/A	Disabled	Create	

Pressing the *Create* button for the desired plan, an On-demand user will be created, then click *Printout* to print a receipt which will contain this on-demand user's information. There are 2000 On-demand user accounts available.



5.3.1.7 PMS User

The system integrates a hotel in-door billing system, PMS, developed by Micros Fidelio, and it is usually used in the hotel environment. When the customers need to use wireless Internet in the hotel, they have to get printed receipts with usernames and passwords from the hotel to log in the system for wireless access.

	PMS User Configuration
Server Status	Disable
PMS Server IP	(e.g. 10.0.0.1)
PMS Server Port	9877
Postfix	pms *(e.g. pms. Max: 40 char)
Policy Name	Policy1 💌
Receipt Header 1	Welcome! (e.g. Welcome!)
Receipt Header 2	Enjoy your stay
Receipt Footer	Thank You ! (e.g. Thank You!)
WLAN ESSID	pms (e.g. pms)
Wireless Key	
Remark	Have a nice day! (for customer)
<u>Users List</u>	Billing Configuration Create PMS User

- Server Status: The status shows that the server is enabled or disabled.
- **PMS Server IP:** Enter the IP address of the PMS server.
- **PMS Server Port:** Enter the Port of the PMS server.
- **Postfix:** Set a postfix that is easy to distinguish (e.g. Local) for the server by using numbers (0 to 9), alphabets (a to z or A to Z), dash (-), underline (_) and dot (.) with a maximum of 40 characters, all other letters are not allowed.
- **Policy Name:** There are ten policies to select from.
- **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.
- WLAN ESSID: Enter the ESSID of the AP.
- **WEP Key:** Enter the WEP key of the AP.
- **Remark:** Enter any additional information that will appear at the bottom of the receipt.
- Users List: Click to enter the PMS User List page. In the PMS User List page, detailed information will be documented here. By default, the PMS user database is empty.

						Search	
PMS User List							
Room No.	User Name	Password	Remain Time	Status	Expire/Valid Time	Delete All	
(Total: 0) <u>First Prev Next Last</u>							

- Search: Enter a keyword of a username to be searched in the text filed and click this button to perform the search. All usernames matching the keyword will be listed.
- > Room No.: The room number of the PMS user.
- **User Name:** The login name of the PMS user.
- > **Password:** The login password of the PMS user.
- **Remain Time:** 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.
- Expire/Valid Time: The Valid Time indicates the duration of time that the user can use the Internet service after the account is activated. After this duration, the account will self-expire. The Expire Time indicates the duration of time that the account needs to be activated after the generation. If the account is not activated during this duration, the account will self-expire.
- > Delete All: This will delete all the users at once.
- > Delete: This will delete users individually.
- Billing Configuration: Click this to enter the PMS User Billing Configuration page. In the PMS Billing Configuration page, the administrator may configure up to 5 billing plans.

	PMS User Billing Configuration										
Plan	Status	Hr. Purchased (Hours)	Valid Period (Hours)	Assign to Policy	Price (e.g.: 10.00)						
1	 Enable Disable 	24	48	1: Policy1 💌	10.00						
2	○ Enable⊙ Disable	0	0	0: NONE	0						
3	○ Enable⊙ Disable	0	0	0: NONE	0						
4	 Enable Disable 	0	0	0: NONE	0						
5	 Enable Disable 	0	0	0: NONE	0						

- > Status: Select to enable or disable this billing plan.
- > Hr. Purchased: This is the duration of time that the user purchases. 1-999 hour(s) can be entered.
- Valid Period: This is the duration of time that the user can use the Internet service after the activation of the account. After this duration, the account will self-expire. 1-999 hours can be entered.
- > Assign to Policy: Assign a policy for this billing plan.
- > **Price:** The price charged for this billing plan.

Note: There is an **Auto Expired** mechanism is for preventing that an account is created but never logged in. If the account is created but never been logged in, the account will be invalid after a period.

• **Create PMS User:** Click this to enter the **PMS User Generation** page. There are 5000 PMS user accounts available.

	PMS User Generation								
Plan	Туре	Price	Status	Configuration	Function				
1	24 hrs	10.00	Enabled	Room Number: Maximum User: 1	Create				
2	0 hrs	0	Disabled	Room Number: Maximum User: 1	Create				
3	0 hrs	0	Disabled	Room Number: Maximum User: 1	Create				
4	0 hrs	0	Disabled	Room Number: Maximum User: 1	Create				
5	0 hrs	0	Disabled	Room Number: Maximum User: 1	Create				

By default, the PMS user database is empty. After entering "*Room Number*" and "*Maximum User*" then pressing *Create* button by the desired plan, a PMS user will be created. Click *Printout* to print a receipt which will contain this PMS user's information. See the following figure.

Room Number	12345
Username	822S@Hotel
Passward	6892BN7Q
Ртісе	1.02
Usage	10 hrs
ESSID : airlive	
Shared WEP keys:	
Concurrent user access: 1	
Must login before:2008/10/0	1 17:54:15
Must login before:2008/10/0	1 17:54:15 Creating Time:2008/10/01 09:00
Must login before:2008/10/0 Th	1 17:54:15 Creating Time:2008/10/01 09:00 ank You !
Must login before:2008/10/0 Тh cut heгe	1 17:54:15 Creating Time:2008/10/01 09:00 ank You ! cut here
Must login before:2008/10/0 Th cut here Room Number	1 17:54:15 Creating Time:2008/10/01 09:00 ank You ! cut here 12345
Must login before:2008/10/0 Th cut here Room Number Username	1 17:54:15 Creating Time:2008/10/01 09:00 ank You ! cut here 12345 822S@Hotel
Must login before:2008/10/0 Th cut here Room Number Username Price	1 17:54:15 Creating Time:2008/10/01 09:00 ank You ! cut here 12345 822S@Hotel 1.02
Must login before:2008/10/0 Th cut here Room Number Username Price Usage	1 17:54:15 Creating Time:2008/10/01 09:00 ank You ! cut here 12345 822S@Hotel 1.02 10 hrs
Must login before:2008/10/0 Th cut here Room Number Username Price Usage Concurrent user access: 1	1 17:54:15 Creating Time:2008/10/01 09:00 ank You ! cut here 12345 822S@Hotel 1.02 10 hrs
Must login before:2008/10/0 Th cut here Room Number Username Price Usage Concurrent user access: 1 Must login before:2008/10/0	1 17:54:15 Creating Time:2008/10/01 09:00 ank You ! cut here 12345 822S@Hotel 1.02 10 hrs
Must login before:2008/10/0 Th cut here Room Number Username Price Usage Concurrent user access: 1 Must login before:2008/10/0 Signature:	1 17:54:15 Creating Time:2008/10/01 09:00 ank You ! cut here 12345 822S@Hotel 1.02 10 hrs

5.3.2 Policy Configuration

There are ten policies that IAS-2000 v2 supports and a Global policy. Every Policy has three profiles, **Firewall Profile**, **Specific Route Profile**, and **Schedule Profile** as well as one **Bandwidth** setting for that policy. But **Global** policy only has **Firewall Profile** and **Specific Route Profile** settings.

Global Policy

Policy Configuration			
Select Policy: Global 🗸			
Firewall Profile	Setting		
Specific Route Profile	Setting		
Maximum Concurrent Sessions	500 Sessions per User		

- > Select Policy: Select Global to set the Firewall Profile and Specific Route Profile.
- Firewall Profile: Click the hyperlink of Setting for Firewall Profile, the Firewall Profiles page 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: G	Profile Name: Global								
			all Profile						
Filter Rule	Active	Action	Name	Source IP	Destination IP	Protocol	MAC		
1		Block		Any	Any	ALL			
2		Block		Any	Any	ALL			
<u>3</u>		Block		Any	Any	ALL			
4		Block		Any	Any	ALL			
<u>5</u>		Block		Any	Any	ALL			
<u>6</u>		Block		Any	Any	ALL			
Z		Block		Any	Any	ALL			
<u>8</u>		Block		Any	Any	ALL			
<u>9</u>		Block		Any	Any	ALL			
<u>10</u>		Block		Any	Any	ALL			

Edit Filter Rule						
Rule Item: 1						
Rule Name:			Enable this	Rule		
Action : Block	v		Protocol : ALL			
Source MAC A	ddress:		(For Specific M	AC Address Filter)		
	Interface	Netw	ork/IP Address	Subnet Mask		
Source	ALL 🗸	0.0.	0.0	0.0.0.0 (/0)		
Destination	ALL 🗸	0.0.	0.0	0.0.0.0 (/0)		

- **Rule Item:** This is the rule 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 five interfaces to choose, ALL, WAN1, WAN2, LAN1 and LAN2.
- **Source/Destination IP:** Enter the source and destination IP addresses.
- **Source/Destination Subnet Mask:** Enter the source and destination subnet masks.

Specific Route Profile: Click the hyperlink of Setting for Specific Route Profile, the Specific Route Profile page will appear.

Profile Name: Global Specific Route										
	Global Route Table									
Route No	De	estination	Gateway							
Noute no.	Network/IP Address	Subnet Mask	IP Address							
1		255.255.255.255 (/32) 🗸								
2		255.255.255.255 (/32) 💙								
3		255.255.255.255 (/32) 🗸								
4		255.255.255.255 (/32) 🗸								
5		255.255.255.255 (/32) 💌								
6		255.255.255.255 (/32) 💌								
7		255.255.255.255 (/32) 🗸								
8		255.255.255.255 (/32) 🗸								
9		255.255.255.255 (/32) 🗸								
10		255.255.255.255 (/32) 🗸								

View System Route Table

- **Profile Name:** The profile name can be changed here.
- **Destination IP Address:** The destination IP address of the host or the network.
- Destination Subnet Netmask: Select a destination subnet netmask of the host or the network.
- Gateway IP Address: The IP address of the next router to the destination.

System Route Table							
Network Address	Netmask	Gateway	Interface	Metric			
192.168.2.0	255.255.255.0	0.0.00	LAN2	0			
192.168.1.0	255.255.255.0	0.0.0.0	LAN1	0			
192.168.0.0	255.255.255.0	0.0.0.0	WAN1	0			
127.0.0.0	255.0.0.0	0.0.0.0	lo	0			
0.0.0.0	0.0.00	192.168.0.254	WAN1	0			

View System Route Table: Click the hyperlink of View System Route Table to see the information of the hosts or the networks. Maximum Concurrent Sessions: The concurrent sessions for each user; it can be restricted by administrator. When a user reaches the session limit, this user will be implicitly suspended from any new connection for a fixed time period.

Policy Configuration				
Select Policy: Global 🗸				
Firewall Profile	Setting			
Specific Route Profile	Setting			
Maximum Concurrent Sessions	500 Sessions per User			

• Policy 1~Policy 10

Policy Configuration				
Select Policy: Policy1 🗸				
Policy Name 1 : Policy1				
Firewall Profile	Setting			
Specific Route Profile	<u>Setting</u>			
Schedule Profile	Setting			
Bandwidth	Unlimited 🐱			
Maximum Concurrent Sessions	500 🖌 Sessions per User			

- Select Policy / Policy Name: Select a desired policy and rename it in the Policy Name field if desired.
- Firewall Profile: Click the hyperlink of Setting for Firewall Profile, the Firewall Profiles page 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.

1	Profile Name: IP Filter 1									
				all Profile						
	Filter Rule	Active	Action	Name	Source IP	Destination IP	Protocol	MAC		
	1		Block		Any	Any	ALL			
	2		Block		Any	Any	ALL			
	<u>3</u>		Block		Any	Any	ALL			
	<u>4</u>		Block		Any	Any	ALL			
	<u>5</u>		Block		Any	Any	ALL			
	<u>6</u>		Block		Any	Any	ALL			
	Z		Block		Any	Any	ALL			
	<u>8</u>		Block		Any	Any	ALL			
	<u>9</u>		Block		Any	Any	ALL			
	<u>10</u>		Block		Any	Any	ALL			

Edit Filter Rule					
Rule Item: 1	Rule Item: 1				
Rule Name:	Rule Name: Enable this Rule				
Action : Block	Action : Block V Protocol : ALL V				
Source MAC A	Source MAC Address: (For Specific MAC Address Filter)				
	Interface	Network/IP Addr	ess Subnet Mask		
Source	ALL 💌	0.0.0.0	0.0.0.0 (/0)		
Destination	ALL 🗸	0.0.0.0	0.0.0.0 (/0)		

- **Rule Item:** This is the rule 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 five interfaces to choose, ALL, WAN1, WAN2, LAN1 and LAN2.
- Source/Destination IP: Enter the source and destination IP addresses.

- Source/Destination Subnet Mask: Enter the source and destination subnet masks.
- Specific Route Profile: Click the hyperlink of Setting for Specific Route Profile, the Specific Route \triangleright Profile page will appear.

Profile Name: Specific Route 1				
Specific Route Profile				
Douto No.	Destination		Gateway	Default
Route No.	Network/IP Address	Subnet Mask	IP Address	Delault
1		255.255.255.255 (/32) 🗸		
2		255.255.255.255 (/32) 💌		
3		255.255.255.255 (/32) 💌		
4		255.255.255.255 (/32) 🗸		
5		255.255.255.255 (/32) 🗸		
6		255.255.255.255 (/32) 💌		
7		255.255.255.255 (/32) 💌		
8		255.255.255.255 (/32) 💌		
9		255.255.255.255 (/32) 💌		
10		255.255.255.255 (/32) 🗸		

- Profile Name: The profile name can be changed here.
- Destination IP Address: The destination IP address of the host or the network.
- Destination Subnet Netmask: Select a destination subnet netmask of the host or the network.
- Gateway IP Address: The IP address of the next router to the destination.
- **Default:** Check this option to apply to the default values.
- Schedule Profile: Click the hyperlink of Setting for Schedule Profile to enter the Schedule Profile list. \geq 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: Schedule1 Schedule1 Enable Obisable							
		Log	gin Schedu	le Profile			
HOUR	SUN	MON	TUE	WED	THU	FRI	SAT
0				✓			
1			✓	✓			
2			✓	✓			
3			✓	✓			
4							
5							
6				✓			
7			✓	✓			
8			✓	✓			
9			✓	✓			
10	✓	✓	✓	✓	~	~	✓

ofilo No Schedule1

Coshlo O Disable

Bandwidth: Choose one bandwidth limit for that particular policy. ۶

Policy Configuration			
Select Policy: Policy1 🗸	elect Policy: Policy1 🗸		
Policy Name 1 : Policy1			
Firewall Profile	Setting		
Specific Route Profile	Setting		
Schedule Profile	Setting		
Bandwidth	Unlimited 🐱		
Maximum Concurrent Sessions	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	Sessions per User	
	22 Mbps 54 Mbps		

Maximum Concurrent Sessions: The concurrent sessions for each user; it can be restricted by administrator. When a user reaches the session limit, this user will be implicitly suspended from any new connection for a fixed time period.

Policy Configuration			
Select Policy: Policy1 💌			
Policy Name 1 : Policy1			
Firewall Profile	Setting		
Specific Route Profile	Setting		
Schedule Profile	<u>Setting</u>		
Bandwidth	Unlimited 🐱		
Maximum Concurrent Sessions	500 Sessions per User		

5.3.3 Black List Configuration

The administrator can add, delete, or edit the black list for user access control. Each black list can include 500 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				
Black List Configuration				
Select Black List: 1:Blacklist1 🗸				
Name	Blacklist1			
User	Remark	Delete		

(Total:0) First Prev Next Last

Add User to List Import Black List Export Black 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, click *Apply* to add the users.

Add Users to Blacklist - Blacklist1			
No	Username	Remark	
1	jacky		
2	josh		
3	ryan		
4			
5			
6			
7			
8			
9			
10			

Add Users to Blacklist - Blacklist1			
No	Username	Remark	
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			

Added User(s): jacky, josh, ryan

Black List Configuration				
Select Black List: 1:Blacklist1 🗸				
Name	Blacklist1			
User	Remark	Delete		
jacky				
josh				
ryan				

If the administrator wants to remove a user from the black list, just select the user's "**Delete**" check box and then click the **Delete** button to remove that user from the black list.

Import Black List: Click this to enter the Upload black List Account – (Blacklist1) page. Click the Browse button to select the text file for the user account upload to the black list. Then click Submit to complete the upload process.

Upload Black List Account - (Blacklist1)			
Note 1:The format of each line is "Username, Remark" without the quotes. There must be no space between the fields and commas. When adding user accounts by uploading a file, any existing account in the embedded database that has the same user name as the one defined in the uploaded file will not be replaced by the new one.			
Upload Black List Account			
File Name Browse			

The uploading file should be a text file and the format of each line should be **"ID, Remark"** without the quotes. There must be no spaces between the fields and commas. 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.



Export Black List: Click *Export List* to create a .txt file and then save it on disk.



5.3.4 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			
	Enable Guest User O Disable Guest User Guest User List		
Guest User Configuration	Session Length 12 🖌 hours		

• Guest User List: IAS-2000 v2 offers ten guest user accounts. To activate a guest user, just enter the password in the corresponding "Password" field for that guest account. Guest accounts with blank password will not be activated.

Guest Users List			
Item	Username	Password	
1	Guest1		
2	Guest2		
3	Guest3		
4	Guest4		
5	Guest5		
6	Guest6		
7	Guest7		
8	Guest8		
9	Guest9		
10	Guest10		

• **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.

5.3.5 Additional Configuration

Additional Configuration		
User Control	Idle Timer: 10 minutes *(Range: 1-1440) Multiple Login (On-Demand User and RADIUS accounting do not support multiple login.) Friendly Logout	
Roaming Out Timer	Session Timeout: 5 minutes *(Range: 5-1440) Idle Timeout: 3 minutes *(Range: 1-120) Interim Update: 1 minutes *(Range: 1-120)	
Customize Login Pages	Certificate Login Page Logout Page Login Success Page for On-Demand Login Success Page Logout Success Page	
Credit Reminder	Volume O Enable O Disable	
POP3 Message	Edit Mail Message	
Enhanced User Authentication	◯ Enable ⊙ 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 account can be logged in from different computers at the same time. (This function doesn't support for On-demand users and RADIUS authentication method.)
 - Friendly Logout: When a user logs into the network, a small login successful window will appear to show the user's information. If enabled, when users try to close the small window, a confirming popup window will appear to notify users in case users close the small window by accident.
- Roaming Out Timer

•

- Session Timeout: The time that the user can access the network while roaming. When the time is up, the user will be kicked out automatically.
- Idle Timeout: If a user has been idled with no network activities for more than the idle time, the system will automatically kick out the user.
- Interim Update: The system will update the users' current status and usage according to this time value periodically.

Customize Login Pages

1. **Certificate:** The administrator can upload a new private key and a customer certificate. Click the **Browse** button to select the file for the certificate to upload. Then click **Submit** to complete the upload process.

Upload Certificate		
Upload Private Key		
File Name	Browse	
Upload Customer Certificate		
File Name	Browse	
	Set To Default	

Click Set To Default and then click restart to use the default certificate and key.



- 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 external website. After finishing the setting, Click *Preview* to see the login page.
 - a. Choose *Default Page* to use the default login page.

B Customizing Login Page		
Customizing Login Pag		
Oefault Page	Template Page	
O Uploaded Page	C External Page	

Default Page Setting	
A default dialog box is used for the Login Page. You can preview the page via Preview button.	
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.

B Customizing L	.ogin Page	
-----------------	------------	--

Customizing Login Pag		
O Default Page	 Template Page 	
O Uploaded Page	O 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 upload a login page. Click the *Browse* button to select the file to upload. Then click *Submit* to complete the upload process.

Customizing Login Page		
Customizing Login Pag		
🔘 Default Page	🔿 Template Page	
Oploaded Page	🔘 External Page	
Uploaded Page Setting		
File Name	Browse	

Submit

Existing Image Files:	
Total Capacity: 512 K Capacity Used: 0 K	
	Upload Image Files
File Name	Browse
	Submit
	Preview

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

Air Live	User Login Page
Welcome To Please Enter Your User N	User Login Page! lame and Password To Sign In.
User Name:	
a Password:	
Submit	Clear 🖌 🗸 Remaining

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 to be uploaded.

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.

Total Capacity: 512 K Capacity Used: 0 K		
Upload Image Files		
File Name	Browse	
Submit		
Preview		

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: S4200015.JPG		
	Delete	

d. Choose the *External Page* selection and get the login page from the specific website. Enter the website address in the "*External Page Setting*" field and then click *Apply*.

B Customizing Login Page		
Customizing Login Pag		
O Default Page	◯ Template Page	
O Uploaded Page	 External Page 	

External Page Setting	
External URL :	http://
Preview	

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

about:blank - Microsoft Internet Explorer	
File Edit View Favorites Tools Help	*
🕞 Back - 🐑 - 💌 🖻 🏠 🔎 Search 📌 Favorites 🚱 🙆 - 嫨 🚍 🛄 鑬 🐥 🚸	
Address http://10.2.3.2/loginpages/login.shtml	Links »
	<u> </u>
$\overline{\mathcal{T}}$	
Air Live User Login Page	
Welcome To Heart anis Devel	
Welcome To User Login Page! Please Enter Your User Name and Password To Sign In.	
Pacaward:	
Submit Clear Remaining	
	_
	<u> </u>

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

Customize Logout Page		
 Internal Page 	 External Page 	
Customize Logout Page		
File Name	Browse	
Submit Use Default Page		
Existing Image Files :		
Total Capacity: 512 K Capacity Used: 0 K		
Upload Image Files		
File Name	Browse	
S	ubmit	

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.

<form action="userlogout.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>

- 4. 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, 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.

Customize Login Success Page for On-demand		
Customize Login Success Page for On-demand		
 Default Page 	◯ Template Page	
O Uploaded Page	O External Page	

Default Page Setting
A default dialog box is used for the Login Success Page for On-demand. You can preview the page via Preview button.
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. Click *Preview* to see the result first.

Customize Login Success Page for On-demand

Customize Login Success Page for On-demand		
O Default Page	 Template Page 	
O Uploaded Page	O 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 get the login success page for On-Demand by uploading. 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

Customize Login Success Page for On-demand		
Customize Login Success Page for On-demand		
🔘 Default Page	🔿 Template Page	
💽 Uploaded Page	🔘 External Page	
Uploa	d Login Success Page for on-demand	
File Name	Browse	
Submit		
Existing Image Files:		
Total Capacity: 512 K Capacity Used: 0 K		
Upload Image Files		
File Name	Browse	
Submit		
Preview		

After the upload process is completed, the new I 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 to be uploaded.

Then, enter or browse the filename of the images to upload in the **Upload Images** field on 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 Capacity Used: 0 K		
Upload Image Files		
File Name	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:	
20080423(007).jpg	
	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 for On-Demand can be previewed by clicking *Preview* button at the bottom of this page.

Customize Login Success Page for On-demand

Customize Login Success Page for On-demand		
O Default Page	◯ Template Page	
O Uploaded Page	 External Page 	

External Page Setting	
External URL : http://	
Preview	

- 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, click *Preview* to see the login success page.
 - a. Choose *Default Page* to use the default login success page.

B Customize Login Success Page

Customize Login Success Page		
Oefault Page	C Template Page	
O Uploaded Page	C External Page	

Default Page Setting
A default dialog box is used for the Login Success Page. You can preview the page via Preview button.
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. Click *Preview* to see the result first.

B Customize	Login	Success	Page
-------------	-------	---------	------

Customize Login Success Page		
O Default Page	 Template Page 	
O Uploaded Page	C 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 get the login success page to upload. Click the *Browse* button to select the file for the login success page upload. Then click *Submit* to complete the upload process.

🗰 Customize Login Success Page		
Customize Login Success Page		
🔘 Default Page	🔿 Template Page	
💿 Uploaded Page	🔿 External Page	

Uploaded Page Setting		
File Name	Browse	
	Submit	
Existing Image Files:		
Total Capacity: 512 K Capacity Used: 0 K		
Upload Image Files		
File Name	Browse	
	Submit	
	Preview	

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

If the user-defined login success page includes an image file, the image file path in the HTML code must be the image file to be uploaded.

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 success page, click the **Use Default Page** button to restore it to default.

Total Capacity: 512 K Capacity Used: 0 K	
Upload Image Files	
File Name	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:	
20080424(003).jpg	
	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.

Customize Login Success Page		
Customize Login Success Page		
O Default Page	◯ Template Page	
O Uploaded Page	 External Page 	

External Page Setting	
External URL : http://	
Preview	

Please note that is needed in your HTML code to make sure the page works correctly.

<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>

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

Customize Logout Success Page		
Customize Logout Success Page		
Oefault Page	O Template Page	
OUploaded Page	O External Page	

Default Page Setting	
A default dialog box is used for the Logout Success Page. You can preview the page via Preview button.	
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.

B Customize Logout Success Page

Customize Logout Success Page		
O Default Page	 Template Page 	
OUploaded Page	C 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 get the logout success page to upload. Click the *Browse* button to select the file for the logout success page to be uploaded. Then click *Submit* to complete the upload process.

Customize Logout Success Page		
C	Customize Logout Success Page	
🔘 Default Page	🔿 Template Page	
💽 Uploaded Page	🔘 External Page	
	Upload Logout Success Page	
File Name	Browse	
	Submit	
Existing Image Files:		
Total Capacity: 512 K Capacity Used: 0 K		
Upload Image Files		
File Name	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 to be uploaded.

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 success page, click the **Use Default Page** button to restore it to default.

Total Capacity: 512 K Capacity Used: 0 K		
Upload Image Files		
File Name	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:	
20080424(004).jpg	
	Delete

d. Choose the *External Page* selection and get the logout success page from the specific external 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.



External Page Setting		
External URL : http://		
Preview		

• **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.

	Volume 💿 Enable 🔘 Disable
Credit Reminder	1 Mbyte *(Default: 1; Range: 1-10)
	Time 💿 Enable 🔘 Disable
	5 minutes *(Default: 5; Range: 1-30)

• **POP3 Message:** If a user tries to retrieve mail from POP3 mail server before login, the users will receive a welcome mail from IAS-2000 v2. The administrator can edit the content of this welcome mail.

Edit Mail Message			
Edit Mail Message			
Text	<pre><!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN"> <html><head> <meta content="text/html; charset=utf-8" http-equiv="Content-Type"/> </head> <body> <div> <div> Welcome! </div> <div> </div></div></body></html></pre>		

Enhance User Authentication: With this function, only the users with their MAC addresses in this list can log into IAS-2000 v2. There will only be 40 users allowed in this MAC address list. User authentication is still required for these users. Please click the hyper link of Permitted MAC Address List to enter the MAC Address Control page and fill in the wanted MAC addresses.

MAC Address Control List			
Item	MAC Address	Item	MAC Address
1		2	
3		4	
5		6	
7		8	
9		10	
11		12	
13		14	
15		16	
17		18	
19		20	

B MAC Address Control

(Total :40) First Prev Next Last

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

5.4 Utilities

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

System Configuration	Network Configuration	User Authentication	Utilities	Status
	Utilities			
Change Password			Utilities	
Backup/Restore Setting	Change Password	Change the admin	istration password.	
Firmware Upgrade	Backup/Restore Setting	Backup and resto system settings to	re system settings. Adminis factory default.	trator may also rese
Restart	Firmware Upgrade	Upgrade to the late	est system firmware.	
	Ping Utility	Send ICMP ECHO	_REQUEST to network hosts.	
	Restart	Restart the system		
		(0	

5.4.1 Change Password

The administrator can change passwords here. Please enter the required fields marked with red asterisks. Click *Apply* to activate the new passwords.

Change Password			
Change Admin Password			
Old Password	•		
New Password	•		
Verify Password	•		
Apply	X Clear		
Change Mana	ger Password		
New Password	•		
Verify Password	•		
Apply	X Clear		
Change Operator Password			
New Password	•		
Verify Password	•		
Apply	X Clear		

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

5.4.2 Backup/Restore Setting

This function is used to backup/restore the IAS-2000 v2 settings. Also, IAS-2000 v2 can be restored to the factory default settings here.

Backup/Restore Setting		
Backup Current Setting		
Backup settings		
Restore system settings		
File Name Browse		
Restore system settings		
Reset to the factory-default settings		
Reset		

• Backup Current Setting: Click Backup Settings to create a .db database backup file and save it on disk.

File Dov	vnload 🛛 🔀
Do you	u want to open or save this file?
	Name: 20081003.db
<u>></u>	Type: Data Base File
	From: 192.168.0.84
	Open Save Cancel
🗹 Alwa	ays ask before opening this type of file
While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. <u>What's the risk?</u>	

- **Restore system settings:** Click *Browse* to search for a .db database backup file created by IAS-2000 v2 and click *Restore system settings* to restore to the backup settings saved previously.
- Reset to the factory-default settings: Click *Reset* to load the factory default settings of IAS-2000 v2.

Caution: Resetting to factory default settings will clear/restore all settings such as policies, billing plans, all user databases, and any configuration to the initial states.

5.4.3 Firmware Upgrade

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

Birmware Upgrade

Firmware Upgrade		
Current Version	1.00.00	
File Name	Browse	

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

Warning: 1. Firmware upgrade may cause the loss of some of the data. Please refer to the release notes for the limitation before upgrading the firmware.

2. Please restart the system after upgrading the firmware. Do not power on/off the system during the upgrade or the restart process. It may damage the system and cause it to malfunction.

5.4.4 Restart

This function allows the administrator to safely restart IAS-2000 v2 and the process should take about three minutes. Click **YES** to restart IAS-2000 v2; click **NO** to go back to the previous screen. If turning off the power is necessary, restarting IAS-2000 v2 first and turning off the power after completing the restart process is recommended.

Restart		
	Do you want to Restart IAS-2000v2?	
	YES NO	

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

5.5 Status

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

System Configuration	Network onfiguration A	User uthentication	Utilities	Status
	B Status			
System Status			Status	
Interface Status	System Status	Display the curre	ent system settings.	
Current Users	Interface Status	Display WAN1, V	VAN2, and LANs configurations	and status.
Traffic History	Current Users	Display online packet count, by out any on-line u	user information including: U te count and idle time. Adminis ser from here.	sername, IP, MAG trator may also kio
Notification Configuration	Traffic History	Display detail us history can be lo	sage information by day. A ma gged in the system volatile men	ximum of 3 days on the second se
Online Report	Notification Configuration	Historical usage address defined here.	log can be sent automatically d here. External syslog server	to a specific e-ma can be configure
	Online Report	Display the on interfaces, and n	line status for the system, etwork sessions.	services, netwo
			0	

5.5.1 System Status

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

🏥 System Status System Status 1.00.00 **Current Firmware Version** Build 00400 System Name Internet Access Gateway Home Page http://www.airlive.com Syslog Server - Traffic History N/A:N/A **Proxy Server** Disabled Friendly Logout Disabled Internet Connection Detection Disabled WAN Failover Disabled Remote Management IP 0.0.0/0.0.0.0 Management SNMP Disabled **Retainable Days** 3 Day(s) History Traffic log Email To N/A NTP Server tock.usno.navy.mil Time 2008/10/03 15:11:50 +0800 Date Time Idle Timer 10 Min(s) User Multiple Login Disabled Guest Account Disabled Preferred DNS Server 192.168.0.254 DNS Alternate DNS Server N/A Server Status Disabled PMS IP:Port N/A:9877 Syslog Server Disabled Email To Session Log Disabled FTP Server Disabled

.

The description of the table is as follows:

<u>Item</u>		Description
Curre	ent Firmware Version	The present firmware version of IAS-2000 v2
System Name		The system name. The default is Internet Access Gateway
		The page the users are directed to after initial login is
	Home Page	successful.
Syslog	server- Traffic History	The IP address and port number of the external Syslog
		Server. N/A means that it is not configured.
	Proxv Server	Enabled / Disabled stands for the system is currently using
		the proxy server or not.
		Enabled / Disabled stands for the setting of hiding or
	Friendly Logout	displaying an extra confirmation window when users click
		the logout button.
Interne	t Connection Detection	Show a warning message when Internet connection is
		down.
	WAN Failover	Show WAN1 and WAN2 status when WAN Failover is
	· · · · · · · · · · · · · · · · · · ·	enabled.
	Remote Management IP	The IP or IP range that is allowed for accessing the
Manage		management interface.
J	SNMP	Enabled / Disabled stands for the current status of the
		SNMP management function.
	Retainable Davs	The maximum number of days for the system to retain the
History		users' information.
	Traffic log Email To	The email address that the traffic history information will be
	-	sent to.
Time	NTP Server	The network time server that the system is set to align.
Time	Date Time	The system time is shown as the local time.
	Idle Timer	The number of minutes allowed for the users to be inactive.
	Multiple Login	Enabled / Disabled stands for the current setting to allow or
User	wuitiple Login	disallow multiple logins form the same account.
	Guest Assount	Enabled / Disabled stands for the current status of allowing
		Guest Accounts to log in.
DNG	Preferred DNS Server	IP address of the preferred DNS Server.
DNO	Alternate DNS Server	IP address of the alternate DNS Server.
DMO	Server Status	The current status of the PMS server.
PMS –	IP:Port	The IP and Port information of the PMS server.

.

		Enabled / Disabled stands for the current setting to allow or
	Syslog Server	disallow recording logs at syslog server.
Session	Emeil	Enabled / Disabled stands for the current setting to allow or
Log	Email	disallow mailing out logs to specific recipient.
	FTP Server	Enabled / Disabled stands for the current setting to allow or
		disallow sending out logs at FTP server.

5.5.2 Interface Status

Provide an overview of the interface for the administrator including WAN1, WAN2, LAN1 and LAN2.

Interface Status				
	Interface Status			
	MAC Address	00:90:0B:08:D9:90		
10/0.014	IP Address	192.168.0.84		
WANT	Subnet Mask	255.255.255.0		
	Connection Status	Up		
	MAC Address	00:90:0B:08:D9:92		
MANO	IP Address	N/A		
WANZ	Subnet Mask	N/A		
	Connection Status	Down		
	Mode	NAT		
	MAC Address	00:90:0B:08:D9:91		
LAN1	IP Address	192.168.1.254		
	Subnet Mask	255.255.255.0		
	Connection Status	Down		
	Status	Enabled		
	Preferred DNS Server	168.95.1.1		
	Alternate DNS Server	N/A		
LAN1 DHCP Server	WINS IP Address	N/A		
	Start IP Address	192.168.1.101		
	End IP Address	192.168.1.200		
	Lease Time	1440 Min(s)		
	Mode	NAT		
	MAC Address	00:90:0B:08:D9:93		
LAN2	IP Address	192.168.2.254		
	Subnet Mask	255.255.255.0		
	Connection Status	Down		
	Status	Enabled		
	Preferred DNS Server	192.168.2.254		
	Alternate DNS Server	N/A		
LAN2 DHCP Server	WINS IP Address	N/A		
	Start IP Address	192.168.2.101		
	End IP Address	192.168.2.200		
	Lease Time	1440 Min(s)		

.

The description of the table is as follows:

ltem		Description	
	MAC Address	The MAC address of the WAN1 port.	
WAN1	IP Address	The IP address of the WAN1 port.	
	Subnet Mask	The Subnet Mask of the WAN1 port.	
	Mode	The mode of the WAN2 port.	
	MAC Address	The MAC address of the WAN2 port.	
WAN2	IP Address	The IP address of the WAN2 port.	
	Subnet Mask	The Subnet Mask of the WAN2 port.	
	Mode	The mode of the LAN1 port.	
	MAC Address	The MAC address of the LAN1.	
LAN1	IP Address	The IP address of the LAN1.	
	Subnet Mask	The Subnet Mask of the LAN1.	
	Statuc	Enable / Disable stands for status of the DHCP server on	
	Status	the LAN1.	
	Preferred DNS Server	The primary DNS server of the LAN1.	
LAN1	Alternate DNS Server	The secondary DNS server of the LAN1.	
DHCP Server	WINS IP Address	The WINS server IP. N/A means that it is not configured.	
	Start IP Address	The start IP address of the DHCP IP range of LAN1.	
	End IP Address	The end IP address of the DHCP IP range of LAN1.	
	Lease Time	Minutes of the lease time of the IP address of LAN1.	
	Mode	The mode of the LAN2.	
LAN2	MAC Address	The MAC address of the LAN2.	
	IP Address	The IP address of the LAN2.	
	Subnet Mask	The Subnet Mask of the LAN2.	
	Status	Enable / Disable stands for status of the DHCP server on	
	Status	the LAN2.	
	Preferred DNS Server	The primary DNS server of the LAN2.	
LAN2	Alternate DNS Server	The secondary DNS server of the LAN2.	
DHCP Server	WINS IP Address	The WINS server. N/A means that it is not configured.	
	Start IP Address	The start IP address of the DHCP IP range of LAN2.	
	End IP Address	The end IP address of the DHCP IP range of LAN2.	
	Lease Time	Minutes of the lease time of the IP address of LAN2.	

5.5.3 Current Users

In this function, each online user's information including Username, IP, MAC, Pkts In, Bytes In, Pkts Out, Bytes Out, Idle and Kick Out can be obtained. Administrator can use this function to force a specific online user to log out. Just click the hyperlink of *Kick Out* next to the online user's name to logout that particular user. Click *Refresh* to renew the Current User List.

Current User List

Current User List						
Itom	Username		Pkts In	Bytes In	Idlo	Kick Out
nem	IP	MAC	Pkts Out	Bytes Out	lale	NICK OUL
4		2BQU@ondemand	637	801842	0	Logout
1	192.168.1.150	00:D0:59:59:79:2D	421	42096	0	Loquu

Refresh



5.5.4 Traffic History

This function is used to check the history of IAS-2000 v2. The history of each day will be saved separately in the DRAM for 3 days.

Traffic History

Traffic History					
Date	No. of Items	Download	Delete		
2008-10-03	5	Download	Delete		

On-demand User Log					
Date	No. of Items	Download	Delete		
2008-10-03	6	Download	Delete		

PMS User Log				
Date	No. of Items	Download	Delete	

Roaming Out Traffic History				
Date	No. of Items	Download	Delete	

Roaming In Traffic History				
Date	No. of Items	Download	Delete	

Interface Performance				
Date	No. of Items	Download	Delete	
2008-10-03	4	Download	Delete	

Internal Service					
Date	No. of Items	Download	Delete		
2008-10-03	9	Download	Delete		

System Performance					
Date	No. of Items	Download	Delete		
2008-10-03	1	Download	Delete		

Monthly Report					
Date	No. of Items	Download	Delete		
<u>2008-10</u>	5	Download	Delete		
2008-09	5	Download	Delete		

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

Click *Download* to save every history log in a text file.



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

• Traffic History

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

Traffic History 2008-10-03								
Date	Туре	Name	IP	MAC	Pkts In	Pkts Out	Bytes In	Bytes Out
2008-10-03 18:28:08 +08	0 LOGOUT	jacky@Postfix1	192.168.1.150	00:D0:59:59:79:2D	4332	2563	4605523	305833
2008-10-03 17:22:32 +08	0 LOGIN	jacky@Postfix1	192.168.1.150	00:D0:59:59:79:2D	0 0	0	0	0
2008-10-03 17:18:40 +08	0 LOGOUT	jacky@Postfix1	192.168.1.150	00:D0:59:59:79:2D	3939	2292	4431235	546035
2008-10-03 17:11:47 +08	0 LOGIN	jacky@Postfix1	192.168.1.150	00:D0:59:59:79:2D	0 0	0	0	0
2008-10-03 17:09:39 +08	0 LOGOUT	jacky@Postfix1	192.168.1.150	00:D0:59:59:79:2D	147	142	120692	28918
2008-10-03 17:08:58 +08	0 LOGIN	jacky@Postfix1	192.168.1.150	00:D0:59:59:79:2D	0 0	0	0	0

• On-demand User Log

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

On-demand User Log 2005-03-22

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

PMS User Log

As shown in the following figure, each line is a on-demand user log record consisting of 14 fields, **Date**, **Posting Number**, **Type**, **Name**, **Room ID**, **IP**, **MAC**, **Packets In**, **Packets Out**, **Bytes In**, **Bytes Out**, **Expiretime**, **Validtime** and **Remark**, of user activities.

				PMSUserLogN	lame 2005-08-23						
date	postingNum	type name	roomID	ip	mac	packetsIn	packetsOut bytesh	n bytesOut	expirtime	validtime	remark
2005-08-23 10:50:15 +0800	2724	Create_PMS_UserT744	1234	0.0.0.000:00	0:00:00:00:00	O	0	0 0	O	999 hr.	3596400

• Roaming Out Traffic History

As shown in the following figure, each line is a roaming out traffic history record consisting of 14 fields, **Date**, **Type, Name**, **NSID**, **NASIP**, **NASPort**, **UserMAC**, **SessionID**, **SessionTime**, **Bytes in**, **Bytes Out**, **Pkts In**, **Pkts Out** and **Message**, of user activities.

 Roaming Out Traffic History 2005-03-22

 Date Type Name NASID NASIP NASPort UserMAC sessionID sessionTime Bytes In Bytes Out Pkts In Pkts Out Message

Roaming In Traffic History

•

As shown in the following figure, each line is a roaming in traffic history record consisting of 15 fields, **Date**, **Type, Name**, **NSID**, **NASIP**, **NASPort**, **UserMAC**, **UserIP**, **SessionID**, **SessionTime**, **Bytes in**, **Bytes Out**, **Pkts In**, **Pkts Out** and **Message**, of user activities.

Roaming In Traffic History 2005-03-22

Date Type Name NASID NASIP NASPort UserMAC UserIP SessionID SessionTime Bytes In Bytes Out Pkts In Pkts Out Message

Interface Performance

As shown in the following figure, the history record consists of 5 fields, **Interface**, **Speed-IN (bps)**, **Speed-OUT (bps)**, **Packet-IN (pps)** and **Packet-OUT (pps)** for WAN and LAN status.

Interface Performance (2008-10-03)							
Interface	Speed-In (bps)	Speed-Out (bps)	Packet-In (pps)	Packet-Out (pps)			
		16:20					
WAN2	0.00	0.00	0.00	0.00			
WAN1	8.673828 K	0.398438 K	8.25	0.50			
LAN2	0.00 K	0.00 K	0.00	0.00			
LAN1	0.00 K	0.00 K	0.00	0.00			
	16:15						
WAN2	0.00 K	0.00 K	0.00	0.00			
WAN1	235.307617 K	50.837891 K	53.50	43.00			
LAN2	0.00 K	0.00 K	0.00	0.00			
LAN1	50.347656 K	229.060547 K	42.38	47.88			
16:10							
WAN2	0.00 K	0.00 K	0.00	0.00			
WAN1	8.685547 K	0.523438 K	7.25	0.75			
LAN2	0.00 K	0.00 K	0.00	0.00			
LAN1	0.00 K	0.00 K	0.00	0.00			

Internal Service

As shown in the following figure, the history record consists of 6 fields, DHCP Server, Syslog Server, SNMP Server, HTTP Server, Agent, SSH Server, EMS Server, RADIUS Server, Proxy Server and Redirector Server for network service status.

Internal Service Status (2008-10-03)						
Service	Status					
16:20-	16:20					
DHCP	Running					
Syslog	Stop					
SNMP	Stop					
HTTP	Running					
Agent	Running					
SSH	Running					
RADIUS	Stop					
PROXY	Running					
Redirector	Running					

• System Performance

As shown in the following figure, the history record consists of 5 fields, **CPU Usage %**, **Memory Usage %**, **Total Memory (KB)**, **Memory Used (KB)** and **Memory Free (KB)** of IAS-2000 v2 status.

System Performance (2008-10-03)							
CPU Usage (%)	Memory Usage (%)	Total Memory (KB)	Memory Used (KB)	Memory Free (KB)			
		16:20					
0	81.09	125268	101592	23676			
	16:15						
0	81.09	125268	101592	23676			
	16:10						
0	80.9	125268	101352	23916			
		16:05					
18	79.33	125268	99380	25888			
	16:00						
5	79.63	125268	99752	25516			
	15:55						
1	79.66	125268	99792	25476			

Monthly Report

As shown in the following figure, 5 fields, Local, Roaming in, Roaming out, On Demand Users, PMS Users is provided.

Monthly Report (2008-10)				
	Number of People	Total Time		
Local	0	0 min 0 sec		
Roaming In	0	0 min 0 sec		
Roaming Out	0	0 min 0 sec		
On-Demand Users	0	0 min 0 sec		
PMS Users	0	0 min 0 sec		

5.5.5 Notification Configuration

IAS-2000 v2 will save the traffic history and session logs into the internal DRAM. If the administrator wants the system to automatically send out the history to a particular email address, please enter the related information in these fields.

Notification Configuration						
	Sender's Address					
	Receiver's Address					
	Send Log every	1 Hour 💌				
Tranic history Email	SMTP Server					
	SMTP Auth Method	NONE 💌				
	SMTP Setting Test	Send Test Log				
Syslog Server	IP Address	Port				

Notification Configuration:

- Sender's Address: The e-mail address of the administrator in charge of the monitoring. This will show up as the sender's e-mail.
- **Receiver's Address:** The e-mail address of the person whom the history email is for. This will be the receiver's e-mail.
- Send Log every: The time interval to send the e-mail report.
- SMTP Server: The IP address of the SMTP server.
- SMTP Auth Method: The system provides four authentication methods, PLAIN, LOGIN, CRAM-MD5 and NTLMv1, or "NONE" to use none of the above. Depending on which authentication method selected, enter the Account Name, Password and Domain.
 - > **NTLMv1** is not currently available for general use.
 - Plain and CRAM-MD5 are standardized authentication mechanisms while LOGIN and NTLMv1 are Microsoft proprietary mechanisms. Only PLAIN and LOGIN can use the UNIX login password. Netscape uses PLAIN. Outlook and Outlook express uses LOGIN as default, although they can be set to use NTLMv1.
 - > Pegasus uses **CRAM-MD5** or **LOGIN** but which method to be used can not be decided manually.
- **SMTP Setting Test**: Click "Send Test Log" button to send a test email of the report.
- Syslog Server: Enter the IP and Port of the Syslog server.

	Session Log for the Entir	e System
Suchas Comun	◯ Enable	
Syslog Server	IP Address	Port
Send Log (to Email & FTP) e	every 1 Hour 💌	
	◯ Enable ⓒ Disable	
	Sender's Address	
Email Dov	Receiver's Address	
Email Box	SMTP Server	
	SMTP Auth Method	NONE
	SMTP Setting Test	Send Test Log
	○ Enable	
	IP Address	Port
	Anonymous	◯Yes ⊙No
FTP Server	Username	
	Password	
	FTP Setting Test	Send Test Log

Session Log for the Entire System:

- **Syslog Server:** Enter the IP and Port of the Syslog server.
- Send Log (to Email & FTP) every: The time interval to send the e-mail report, for upload logs to FTP server.
- Email Box:
 - > Enable / Disable: Enable or Disable the feature to export session log via email.
 - Sender's Address: The e-mail address of the administrator in charge of the monitoring. This will show up as the sender's e-mail.
 - Receiver's Address: The e-mail address of the person whom the history email is for. This will be the receiver's e-mail.
 - > SMTP Server: The IP address of the SMTP server.
 - SMTP Auth Method: The system provides four authentication methods, PLAIN, LOGIN, CRAM-MD5 and NTLMv1, or "NONE" to use none of the above. Depending on which authentication method selected, enter the Account Name, Password and Domain.
 - **SMTP Setting Test**: Click "Send Test Log" button to send a test email of the report.
 - FTP Server:
 - **Enable / Disable:** Enable or Disable the feature to export session log to FTP server.
 - > IP Address: Specify FTP server IP address and FTP port number.
 - Anonymous: Allow or Disallow Anonymous account login to FTP server.
 - **Username:** Specify FTP user name.

.

- > **Password:** Specify FTP account password.
- > **FTP Setting Test**: Click "Send Test Log" button to send a test report to FTP server.
5.5.6 Online Report

This function provides real time on-line report of the IAS-2000 v2 system including **System Status**, **Service Status**, **Network Interface Status** and **Network Session Status**.

Online Report
Online Report
System Status
Service Status
Network Interface Status
Network Session Status

• System Status

As shown in the following figure, the online report consists of 5 fields, **CPU Usage**, **Memory Usage**, **Total Memory**, **Memory Used** and **Memory Free** of IAS-2000 v2 status.

System Performance					
CPU Usage (%)	Memory Usage (%)	Total Memory (KB)	Memory Used (KB)	Memory Free (KB)	
0	81.07	125268	101556	23712	

• Service Status

As shown in the following figure, the online report consists of 6 fields, DHCP Server, Syslog Server, SNMP Server, HTTP Server, Agent, SSH Server, RADIUS Server, Proxy Server and Redirector Server for network service status.

Internal Service Status			
Service	Status		
DHCP	Running		
Syslog	Stop		
SNMP	Stop		
HTTP	Running		
Agent	Running		
SSH	Running		
RADIUS	Stop		
PROXY	Running		
Redirector	Running		

• Network Interface Status

As shown in the following figure, the online report consists of 5 fields, Interface, Speed-IN (bps), Speed-OUT (bps), Packet-IN (pps) and Packet-OUT (pps) for WAN and LAN status.

	Interface Performance					
Interface	Speed-In (bps)	Speed-Out (bps)	Packet-In (pps)	Packet-Out (pps)	Status	
WAN1	7.429688 K	0.398438 K	7.62	0.50	UP	
WAN2	0.00	0.00	0.00	0.00	DOWN	
LAN1	0.00	0.00	0.00	0.00	UP	
LAN2	0.00	0.00	0.00	0.00	DOWN	

• Network Session Status

As shown in the following figure, the online report consists of 3 fields, **IP**, **TCP session count** and **UDP session count**. This report tells how many connections each IP address uses now.

Session Information				
IP	TCP Session Counted	UDP Session Counted		
127.0.0.1	5	0		
192.168.0.75	0	1		
192.168.99.220	0	1		
192.168.0.201	3	0		
192.168.99.29	0	1		
192.168.0.128	0	1		
192.168.0.8	0	1		
192.168.0.231	0	1		
192.168.0.66	0	3		
192.168.0.39	0	3		
192.168.0.157	0	2		
192.168.99.25	0	2		
192.168.0.236	0	1		

5.6 Help

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

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

AS-2000 v2 - Microsoft Internet Explorer						(X
File Edit View Favorites Tools Help							1	7
🕞 Back 🔹 🐑 👻 🛃 🏠 🔎 Search 🤺 Favorites 🚱 👔	2.	W	-		12	8	*	
Address http://192.168.2.254/help.shtml					Y E	Go	Link	s »
Online Help								
Overview								
System Configuration								
System Information								
WAN1 Configuration								
WAN2 & Failover								
LAN1 Configuration								
LAN2 Configuration								
Network Configuration								
Network Address Translation								
Privilege List								
Monitor IP List								
Walled Garden List								
Proxy Server Properties								
Dynamic DNS								
IP Mobility								
User Authentication								
Authentication Configuration								
Authentication Server Configuration								•
A Done				🙆 Ir	hernet			

Appendix A. External Network Access

If all the steps are set properly, IAS-2000 v2 can be further connected to the managed network to experience the controlled network access environment. Firstly, connect an end-user device to the network at IAS-2000 v2's LAN1 and set to obtain an IP address automatically. After the network address is obtained at the user end, open an Internet browser and link to any website. Then, the default logon webpage will appear in the Internet browser.

 First, connect a user-end device to LAN1 port of IAS-2000 v2, and set the dynamical access network. After the user end obtains the network address, please open an Internet browser and the default login webpage will appear on the Internet browser.

Key in the username and password created in the local user account or the on-demand user account in the interface and then click **Submit** button. Here, we key in the local user account (e.g. **jacky** for the username and **1234** for the password) to connect the network.

 Login page appearing means IAS-2000 v2 has been installed and configured successfully. Now, a client can browse the network or surf the Internet!





 But if "Sorry, this feature is available for on-demand or PMS user only." appears, it means a wrong button has been clicked. "*Remaining*" is only for on-demand users. Please click the *Submit* button instead.



 An on-demand user can enter the username and password in the "User Login Page" and click *Remaining* button to know the remaining time or data quota of the account.

- 5. When an on-demand user logs in successfully, the following Login Successfully screen will appear and it is a little different from the normal user's login successfully screen. There is an extra line showing "Remaining usage" and a "Redeem" button.
 - **Remaining usage:** Show the rest of use time that the on-demand user can surf Internet.
 - Redeem: When the remaining time or data size is insufficient, the user has to pay for adding credit at the counter, and then, the user will get a new username and password. After clicking the *Redeem* button, the following screen will show up. Please enter the new username and password obtained and click *Redeem* button to merge the two accounts and add up the available use time and data size by the system. Total available use time and data size after adding credit will be shown.



Air L	ive	www.airlive.com
	Hello, 2BQ	J@ondemand
Please rin	se this window or o	lick this button to
riedse cio	J Logout	
	Thank you!!	
	Remaining Usa	ge:
	22 Min 28	Sec
Lo	22 Min 28 gin time: 2008-10]Sec 1-3 17:3:29
Lo	22 Min 28 gin time: 2008-10]Sec I-3 17:3:29

Welco	me To Redeem	Page!
Please Enter Your Us	er Name and Pa	assword To Sign In.
User Nam	e: V699@ond	emand
a Password		

Appendix B. Console Interface Configuration

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

- To connect the console port of IAS-2000 v2, a console, modem cable and a terminal simulation program, such as the Hyper Terminal are required.
- 2. Please set the parameters as **9600,8,n,1** for Hyper Terminal.

<u>B</u> its per second:	9600	•
<u>D</u> ata bits:	8	•
<u>P</u> arity:	None	•
<u>S</u> top bits:	1	•
Elow control:	None	•

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

3. Once the console port of IAS-2000 v2 is connected properly, the console main screen will appear automatically. If the screen does not appear in the terminal simulation program automatically, please try to press the arrow keys, so that the terminal simulation program will send some messages, and the welcome screen or the main menu will appear. If the welcome screen or the main menu of the console still does not appear, please check the connection of the cables and the settings of the terminal simulation program.

OvisLink IAS Pleas	-2000v2 Basic Configuration
Configuration Utility Password Reset Restart	Network Configuration Debugging Utilities Change admin password Restore factory default Restart OvisLink IAS-2000v2
 < 0 	K > < <u><c< u="">ancel></c<></u>

Utilities for network debugging

The console interface provides several utilities to assist the Administrator to check the system conditions and debugging. The utilities are described as following:

OvisLink	IAS-2000v2 Configuration Utility
PING Trace ShowIF ShowRT ShowARP Iptables Top TCPdump UpTime Status NTP DMESG Wain	Ping host (IP) Trace routing path Display interface settings Display routing table Display ARP table Display iptables Display CPU and RAM by topo Display network traffic Display system up time Check service status Synchronize clock with NTP server Print the kernel ring buffer Main menu
	< <mark>C</mark> ancel>

- Ping host (IP): By sending ICMP echo request to a specified host and wait for the response to test the network status.
- > **Trace routing path:** Trace and inquire the routing path to a specific target.
- Display interface settings: It displays the information of each network interface setting including the MAC address, IP address, and netmask.
- Display the routing table: The internal routing table of the system is displayed, which may help to confirm the Static Route settings.
- > **Display ARP table:** The internal ARP table of the system is displayed.
- > **Display iptables:** The internal iptables of the system is displayed.
- Display CPU and RAM by top: The CPU and RAM usage of the system is displayed by Linux utility, Top.
- > **Display network traffic:** The network traffic of the system is displayed.
- > **Display system up time:** The system live time (time for system being turn on) is displayed.
- > Check service status: Check and display the status of the system.
- Set device into "safe mode": If administrator is unable to use Web Management Interface via the browser for the system failed inexplicitly. Administrator can choose this utility and set IAS-2000 V2 into safe mode, then administrator can management this device with browser again.
- Synchronize clock with NTP server: Immediately synchronize the clock through the NTP protocol and the specified network time server. Since this interface does not support manual setup for its internal clock, therefore we must reset the internal clock through the NTP.

Print the kernel ring buffer: It is used to examine or control the kernel ring buffer. The program helps users to print out their boot-up messages instead of copying the messages by hand.

• Change admin password

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

The username is "admin" and the default password is also "airlive", which is the same as for the web management interface. The administrator's password can be changed here. Even if the password is forgotten and the management interface can not be accessed from the web or the remote end of the SSH, use the null modem to connect the console management interface and set the administrator's password again.

Caution: Although it does not require a username and password for the connection via the serial port, the same management interface can be accessed via SSH. Therefore, we recommend you to immediately change the IAS-2000 v2 Admin username and password after logging into the system for the first time.

- **Restore factory default** Choose this option to reset the system configuration to the factory default settings.
- Restart IAS-2000 v2
 Choose this option to restart IAS-2000 v2.

Appendix C. Specifications

a. Hardware Specification

- Dimensions: 42.6cm(W) x 4.4cm(H) x 27cm(D)
- Weight: 6kg
- Power: 90-264 VAC 43~63Hz
- Operating Temperature: 5-40°C
- 19" 1U Rack Mount Design
- 4 Gigabyte Ethernet (10/100/1000)
- RS-232 DB9
- Supports 10/100/1000Mbps Full / Half Duplex Transfer Speed

b. Technical Specification

• Networking

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

Interface supports static IP

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

Supports roaming across networks

• Firewall

Provides Several DoS protection mechanisms

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, and LDAP LAN1/LAN2 mechanisms Supports LAN1& LAN2 mechanisms simultaneously 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 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

Appendix D. Proxy Setting for Hotspot

HotSpot is a place such as a coffee shop, hotel, or a public area where provides Wi-Fi service for mobile and temporary users. HotSpot is usually implemented without complicated network architecture and using some proxy servers provided by Internet Service Providers.



In Hotspots, users usually enable their proxy setting of the browsers such as IE and Firefox. Therefore, so we need to set some proxy configuration in the Gateway need to be set. Please follow the steps to complete the proxy configuration :

- 1. Login Gateway by using "admin".
- 2. Click the *Network Configuration from top menu* and the homepage of the *Network Configuration* will appear.

System Configuration C	Network onfiguration A	User Utilities Status
	B Network Co	nfiguration
Network Address Translation		Network Configuration
Privilege List	Network Address Translation	System provides three types of Network Address Translation: DMZ Virtual Server and Port/IP Redirection.
Monitor IP List	Privilege List	System provides Privilege IP Address List and Privilege MAC Address List. Authentication is NOT required for those listed devices. Policies defined in "User Authentication" can be applied to devices in MAC Address List as well.
Proxy Server Properties	Monitor IP List	System can monitor up to 40 network devices using IP packets periodically.
Dynamic DNS	Walled Garden List	Up to 20 URLs or IP addresses could be defined in Walled Garder List. Clients may access these sites without authentication.
IP Mobility	Proxy Server Properties	System has one built-in Proxy Server and supports up to 20 externa Proxy Servers.
ir mobility	Dynamic DNS	System supports dynamic DNS (DDNS) to translate WAN IP to a domain name automatically.
	IP Mobility	System supports IP PNP and Mobile IP Configuration

3. Click the *Proxy Server Properties* from left menu and the homepage of the **Proxy Server Properties** will appear.



External Proxy Server			
Item	Server IP	Port	
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			

4. Add the ISP's proxy Server IP and Port into *External Proxy Server* Setting.

Proxy Server Properties	
Internal Proxy Server	
🔿 Enable 💿 Disable	

External Proxy Server			
Item	Server IP	Port	
1	10.2.3.203	6588	
2			
3			
4			
5			

5. Enable Built-in Proxy Server in Internal Proxy Server Setting.

Proxy Server Properties	
Internal Proxy Server	
 Enable Disable 	

External Proxy Server			
Item	Server IP	Port	
1	10.2.3.203	6588	
2			
3			
4			
5			

6. Click *Apply* to save the settings.

Appendix E. Proxy Setting for Enterprise

Enterprises usually isolate their intranet and internet by using more elaborated network architecture. Many enterprises have their own proxy server which is usually at intranet or DMZ under the firewall protection.



In enterprises, network managers or MIS staff may often ask their users to enable their proxy setting of the browsers such as IE and Firefox to reduce the internet access loading. Therefore some proxy configurations in the Gateway need to be set.

Caution : Some enterprises will automatically redirect packets to proxy server by using core switch or Layer 7 devices. By the way, the clients don't need to enable their browsers' proxy settings, and administrators don't need to set any proxy configuration in the Gateway.

Please follow the steps to complete the proxy configuration :

■ Gateway setting

- 1. Login Gateway by using "*admin*".
- 2. Click the *Network Configuration from top menu* and the homepage of the *Network Configuration* will appear.

Air Live	IAS	www.airlive.com © Logout 5-2000 v2 Internet Access Gateway [®] Help		
System Configuration	Network onfiguration A	User Utilities Status		
	B Network Co	nfiguration		
Network Address Translation	Network Configuration			
Privilege List	Network Address Translation	System provides three types of Network Address Translation: DMZ, Virtual Server and Port/IP Redirection.		
Monitor IP List	Privilege List	System provides Privilege IP Address List and Privilege MAC Address List. Authentication is NOT required for those listed devices. Policies defined in "User Authentication" can be applied to devices in MAC Address List as well		
Proxy Server Properties	Monitor IP List	System can monitor up to 40 network devices using IP packa periodically.		
Dynamic DNS	Walled Garden List	Up to 20 URLs or IP addresses could be defined in Walled Garden List. Clients may access these sites without authentication.		
IP Mobility	Proxy Server Properties	System has one built-in Proxy Server and supports up to 20 external Proxy Servers.		
	Dynamic DNS	System supports dynamic DNS (DDNS) to translate WAN IP to a domain name automatically.		
	IP Mobility	System supports IP PNP and Mobile IP Configuration		
		6		

3. Click the *Proxy Server Properties* from left menu and the homepage of the *Proxy Server Properties* will appear.



External Proxy Server			
Item	Server IP	Port	
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			

4. Add your proxy Server IP and Port into *External Proxy Server* Setting.

Proxy Server Properties		
Internal Proxy Server		
◯ Enable ⊙ Disable		

	External Proxy Server			
Item	Server IP	Port		
1	10.2.3.203	6588		
2				
3				
4				
5				

5. Disable Built-in Proxy Server in Internal Proxy Server Setting.

Proxy Server Properties			
Internal Proxy Server			
	🔘 Enable 💿 Disable		

External Proxy Server			
Item	Server IP	Port	
1	10.2.3.203	6588	
2			
3			
4			
5			

6. Click Apply to save the settings.

Warning: If your proxy server is disabled, it will make the user authentication operation abnormal. When users open the browser, the login page won't appear because the proxy server is down. Please make sure your proxy server is always available.

■ Client setting

It is necessary for clients to add default gateway IP address into proxy exception information so the user login successful page can show up normally.

1. Use command "*ipconfig*" to get Default Gateway IP Address.

C:\WINDOWS\system32\cmd.exe	- 🗆 🗙
C:\Documents and Settings\jacky>ipconfig	_
Windows IP Configuration	
Ethernet adapter Local Area Connection:	
Connection-specific DNS Suffix .: airlive.com IP Address: 192.168.1.150 Subnet Mask: 255.255.255.0 Default Gateway: 192.168.1.254	
Ethernet adapter Web UPN (SSL UPN):	
Media State Media disconnected	
C:\Documents and Settings\jacky>	
	-
	• //

- 2. Open browser to add *default gateway IP address (e.g. 192.168.1.254)* and *logout page IP address "1.1.1.1"* into proxy exception information.
 - For I.E.

88	6588	:	10.2.3.208	HTTP:	♥					
88	6588	:	10.2.3.203	<u>S</u> ecure:						
88	6588	:	10.2.3.208	ETP:						
	:			So <u>c</u> ks:						
	:h:	s beginning with	roxy server for addresses	Do <u>n</u> ot use p	Exception					
192.168.1.254,1.1.1.1					⊊ <u>∎</u>					
Use the same proxy server for all protocols tions Do not use proxy server for addresses beginning with: 192.168.1.254,1.1.1.1										

.

• For Firefox

onnection Settings								
Configure Proxies to Access the Internet								
 Auto-detect proxy settings for this network 								
Manual proxy configuration:								
HTTP Proxy:	10.2.3.203	Port:	6588					
	Use this proxy server for all protocols							
SSL Proxy:	10.2.3.203	Port:	6588					
ETP Proxy:	10.2.3.203	Port:	6588					
<u>G</u> opher Proxy:	10.2.3.203	Port:	6588					
SO <u>C</u> KS Host:	10.2.3.203	Por <u>t</u> :	6588					
	○ SOCKS v4							
No Proxy for:	192.168.1.254,1.1.1.1							
Example: .mozilla.org, .net.nz, 192.168.1.0/24 Automatic proxy configuration URL: Reload								
OK Cancel Help								