

# Unified Office Gateway

UMG-2000  
UMG-2100  
UMG-2200



---

## User's Manual

---

Version 1.0.0

## **Copyright**

Copyright (C) 2010 PLANET Technology Corp. All rights reserved.

The products and programs described in this User's Manual are licensed products of PLANET Technology, This User's Manual contains proprietary information protected by copyright, and this User's Manual and all accompanying hardware, software, and documentation are copyrighted.

No part of this User's Manual may be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form by any means by electronic or mechanical. Including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's personal use, and without the prior express written permission of PLANET Technology.

## **Disclaimer**

PLANET Technology does not warrant that the hardware will work properly in all environments and applications, and makes no warranty and representation, either implied or expressed, with respect to the quality, performance, merchantability, or fitness for a particular purpose.

PLANET has made every effort to ensure that this User's Manual is accurate; PLANET disclaims liability for any inaccuracies or omissions that may have occurred.

Information in this User's Manual is subject to change without notice and does not represent a commitment on the part of PLANET. PLANET assumes no responsibility for any inaccuracies that may be contained in this User's Manual. PLANET makes no commitment to update or keep current the information in this User's Manual, and reserves the right to make improvements to this User's Manual and/or to the products described in this User's Manual, at any time without notice.

If you find information in this manual that is incorrect, misleading, or incomplete, we would appreciate your comments and suggestions.

## **FCC Warning**

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the Instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

## **FCC Caution**

To assure continued compliance (example-use only shielded interface cables when connecting to computer or peripheral devices). Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

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

## **CE mark Warning**

The is a class A device, In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

## **Energy Saving Note of the Device**

This power required device does not support Stand by mode operation.

For energy saving, please remove the DC-plug or push the hardware Power Switch to OFF position to disconnect the device from the power circuit.

Without remove the DC-plug or switch off the device, the device will still consuming power from the power circuit. In the view of Saving the Energy and reduce the unnecessary power consuming, it is strongly suggested to switch off or remove the DC-plug for the device if this device is not intended to be active.

### **Trademarks**

The PLANET logo is a trademark of PLANET Technology. This documentation may refer to numerous hardware and software products by their trade names. In most, if not all cases, these designations are claimed as trademarks or registered trademarks by their respective companies.

### **WEEE Warning**



To avoid the potential effects on the environment and human health as a result of the presence of hazardous substances in electrical and electronic equipment, end users of electrical and electronic equipment should understand the meaning of the crossed-out wheeled bin symbol. Do not dispose of WEEE as unsorted municipal waste and have to collect such WEEE separately.

### **Safety**

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

### **Revision**

User's Manual for PLANET Unified Office Gateway  
Model: UMG-2000 / UMG-2100 / UMG-2200  
Rev: 1.0 (December. 2010)  
Part No.: EM-UMG2000 Series\_v1.0

# Table of Contents

<b>1. Introduction</b> .....	<b>7</b>
<b>1.1 Product Features</b> .....	<b>8</b>
<b>1.2 Package Contents</b> .....	<b>10</b>
<b>1.3 Application</b> .....	<b>11</b>
<b>1.4 Outlook</b> .....	<b>13</b>
1.4.1 Front Panel.....	13
1.4.2 Rear Panel.....	14
<b>1.5 Technical Specifications</b> .....	<b>15</b>
<b>2. Installation</b> .....	<b>17</b>
<b>2.1 Hardware Installaion</b> .....	<b>17</b>
2.1.1 Unpack the UMG-2000 Series.....	17
2.1.2 Choosing a Setup Location.....	17
2.1.3 Preparing for Setup.....	18
2.1.4 Precautions.....	18
2.1.5 Installation Consideration.....	18
2.1.6 The Desktop Brackets Installation.....	19
2.1.7 The Rack Mount Installation.....	19
2.1.8 The Hard Disk Installation.....	21
<b>2.2 Physical Connection</b> .....	<b>22</b>
2.2.1 WAN Connection.....	22
2.2.2 LAN Port Connection.....	22
2.2.3 PSTN FXO Port Connection.....	23
2.2.4 ISDN T1/E1 Port Connection.....	23
<b>2.3 Quick Setup Wizard</b> .....	<b>24</b>
2.3.1 First Time Login.....	24
2.3.2 Welcom to Quick Start.....	25
<b>3. Web Management - Home</b> .....	<b>33</b>
<b>3.1 Overview</b> .....	<b>33</b>
<b>3.2 Spanning Tree Protocol</b> .....	<b>34</b>
<b>3.3 Alert Log</b> .....	<b>35</b>
<b>4. Web Management - User</b> .....	<b>36</b>
<b>4.1 User Overview</b> .....	<b>36</b>
<b>4.2 Deleting a User Account</b> .....	<b>37</b>
<b>4.3 Updating the User Setting</b> .....	<b>37</b>
<b>4.4 Creating a User Account</b> .....	<b>38</b>
<b>4.5 Departments and Groups</b> .....	<b>39</b>
<b>4.6 Deleting a Group</b> .....	<b>39</b>
<b>5. Web Management - Network</b> .....	<b>40</b>
<b>5.1 Overview</b> .....	<b>40</b>
<b>5.2 Internet</b> .....	<b>42</b>
<b>5.3 Local Network</b> .....	<b>42</b>
<b>5.4 Service</b> .....	<b>43</b>
<b>5.5 The VPN Log</b> .....	<b>43</b>
<b>6. Web Management - Wireless</b> .....	<b>44</b>
<b>6.1 Overview</b> .....	<b>44</b>
<b>6.2 Wireless Setting</b> .....	<b>45</b>
<b>6.3 Wireless Clients</b> .....	<b>46</b>
<b>6.4 Blocking the Connected Wireless Client</b> .....	<b>46</b>
<b>6.5 Wireless MAC Block List</b> .....	<b>47</b>
<b>7. Web Management - Storage</b> .....	<b>48</b>
<b>7.1 Storage Overview</b> .....	<b>49</b>

7.2 View a Volume by SMB .....	50
7.3 Updating a Volume .....	50
7.4 Deleting a Volume .....	51
7.5 Creating a Storage Volume.....	51
7.6 Storage Setting.....	53
7.7 Storage Backup and Restore .....	54
7.8 The Storage Log.....	55
8. Web Management - PBX.....	56
8.1 IP PBX Overview .....	56
8.2 IP PBX Call Setting.....	58
8.3 Voice.....	60
8.4 IP PBX Call Rules .....	61
8.5 IP PBX Channel Setting .....	62
8.6 SIP Trunk Setting .....	63
8.7 IP PBX Call Reference .....	64
8.8 IP PBX Call Log .....	65
9. Web Management - Email.....	66
9.1 Email Overview.....	67
9.2 Email Basic Setting.....	68
9.3 Email Blacklist.....	69
9.4 Email Alias .....	70
9.5 Email Forward .....	71
9.6 Email Log.....	72
10. Web Management - FTP .....	73
10.1 FTP Overview .....	73
10.2 FTP Setting .....	73
10.3 FTP Account .....	73
10.4 FTP Log.....	74
11. Web Server .....	75
11.1 Web Server Overview.....	75
11.2 Web Server Settings .....	75
12. Web Management - Security .....	76
12.1 Security Overview .....	76
12.2 Security Setting.....	77
12.3 Content Filter.....	79
12.4 Access Control.....	80
12.5 Port Forwarding .....	81
12.6 Security Log .....	82
13. Web Management - System.....	83
13.1 System Overview .....	83
13.2 System Setting .....	84
13.3 System Event Log.....	85
14. Web Management - Branch-to-Branch.....	86
14.1 Branch-to-Branch Setup.....	86
14.2 Security Channel.....	86
14.3 Remote Calls .....	86
14.4 Remote Data Synchronization .....	87
14.5 Shared Services .....	87
14.6 Global user Profile .....	88
14.7 Centralized Configuration management .....	88
14.8 Branch-to-Branch Overview.....	88
14.9 Delete a Branch .....	90

14.10 Branch-to-Branch Setting .....	91
14.11 Branch Users .....	92
14.12 Branch-to-Branch Log .....	92
15. Web Management - Maintenance.....	93
15.1 System .....	93
15.2 Software Update .....	94
15.3 Diagnose .....	94
15.4 Remote Service .....	95
16. Personal Account Web Administration.....	96
16.1 User Login .....	96
16.2 User Home Page.....	97
16.3 Access to Administrator .....	98
16.4 Personal Setting.....	98
16.5 Contract List.....	99
16.6 Personal Call Records .....	99
16.7 Call Reference .....	100
16.8 Logout.....	100
Appendix A - Fast Recovery .....	101
Welcome to Fast Recovery .....	101
Fast Recovery .....	101
Appendix B - Hard Disk Hot Plug .....	103
Before Unplug .....	103
Unplug Disk .....	103
Insert a New Disk (Hot-Plug) .....	103
Appendix C - Remote Access .....	104
Appendix D – Scenario Example .....	105
Case 1_ X-Lite how to register on the UMG-2000 Series.....	105
Case 2_ VIP-880 VoIP Gateway how to register on the UMG-2000 Series.....	111
Case 3_ VIP-281GS GSM Gateway how to register on the UMG-2000.....	116
Case 4_ VIP-254 and VIP-360PT how to register on the UMG-2000.....	125
Case 5_ How do you setup a VPN with UMG-2000 Series.....	132
Case 6_ How to use LCR function on UMG-2000 Series .....	141

# 1. Introduction

The PLANET UMG-2000 Series is a new model in PLANET Unified Office Gateway series to provide total IT solution for the small and medium business (SMB). It integrates commonly used office appliance features and provides Internet Access, IP PBX, Fax / E-mail server, data storage and print server services in one device. With built-in 24-Port Fast Ethernet plus 2-Port Gigabit Ethernet Switch, Wireless Access Point, 4 / 8-Port FXO, and 1-Port T1/E1 application. The UMG-2000 Series allows you to connect to various Internet and telephone carriers.

Via the 4 / 8-Port FXO and the 1-Port T1/E1 interface, the UMG-2000 Series provides a feature-rich IP PBX system that supports seamless communications between existing PSTN/ISDN calls, analog, IP phones and SIP-based endpoints. Branch-to-Branch secured network and call features bring your remote offices together. The UMG-2000 Series facilitates sharing files safely between multiple office locations through secure channels. For VoIP functions, the users can call any extension from any remote location without paying local or long distance charge. Smart Wizard automatically adjusts your configuration and guides you through initial setup. The administrator can easily manage user accounts with privilege and access control.

In the storage feature, the storage volumes can be created for individual users and groups within the corporate. The UMG-2000 Series is also as the Web and E-mail servers that are able to be set up with one mouse click. It provides schedule automated snapshot and backup tasks to prevent data loss. Besides the above functions, the extensive features include DMZ support, VoIP call control, Call Detail Record (CDR), Least Cost Routing (LCR), and Busy Lamp Field (BLF), configuration backup and restore, secure remote management capabilities and many more.

## 1.1 Product Features

---

### IP PBX / VoIP Service

- SIP 2.0 (RFC3261)
- PSTN/ISDN Support
- Call-Parking, Echo Cancellation
- FXO/ISDN Disconnection Tone Detection
- QoS Support
- Music on Hold and Upload Music Files for MoH
- Telephone Conference, 3-Way Calling
- Voicemail to E-mail
- Forwards to Voicemail on No-Answer
- Supports Call Hold, Call Waiting
- Blacklist of Number Patterns
- Call Privilege Control, Call Log
- 450 Minutes Recording Time
- Unconditional, Unavailable, Busy Call Forward
- Fax Server Support
- Multiple SIP Trunk Support
- Upload Sound Files for IVR
- Least Cost Routing (LCR)
- Busy Lamp Field (BLF)

### E-mail Service

- Supports POP3, SMTP, IMAP
- Secured Socket Layer (SSL)
- Junk Mail Filtering
- E-mail Storage Quota
- E-mail Alias Group Assignment
- Mail Attachment Size Restriction
- User E-mail Storage Quota
- E-mail Log Record Management
- Anti-Virus and Anti-Spam
- Auto Backup, Auto Reply
- E-mail White and Black list Based on Domain Name, User Name, and E-mail Address
- Supports Web Mail
- Supports Mail Service via DDNS

### Internet Security Service

- Static IP, PPPoE, DHCP, PPTP, L2TP
- Web Content Filter by Domain and Keyword
- Access Control List (ACL)
- URL / IM / P2P Blocking
- Firewall / NAT
- IPSec / PPTP / L2TP Pass-through
- DoS Attack Protection (TCP SYN Flood, UDP Flood, ICMP Flood, Ping of Death)
- UPnP and DMZ
- Site-to-Site SSL VPN
- PPTP VPN Remote Access
- RIP / Static Route
- IP-MAC Binding

### **Network Storage Service**

- RAID 0, 5, 10, and JBOD
- Up to 4TB Hot-swap Disk Array
- Supports User Network Storage Quota
- Compatible Windows 2000 / XP / Vista, Mac, Linux
- Scheduled Auto Backup, Auto Snapshot
- Support User / Group Privilege ACL

### **System Management**

- Single Point of Management
- System Logging with E-mail Alert
- Fast Recovery with Remote Service
- Environment Monitoring
- Dynamic Domain Name Services (DDNS)
- Multiple Domain Name Support
- Multiple Hostname Support

### **WiFi Service**

- 1 x 802.11b/g/n Wireless Access Point
- 2 x RP-SMA Detachable Antenna
- Security: WEP / WPA / WPA2
- SSID
- Wireless 802.1x Authentication

### **24+2G Switch Service**

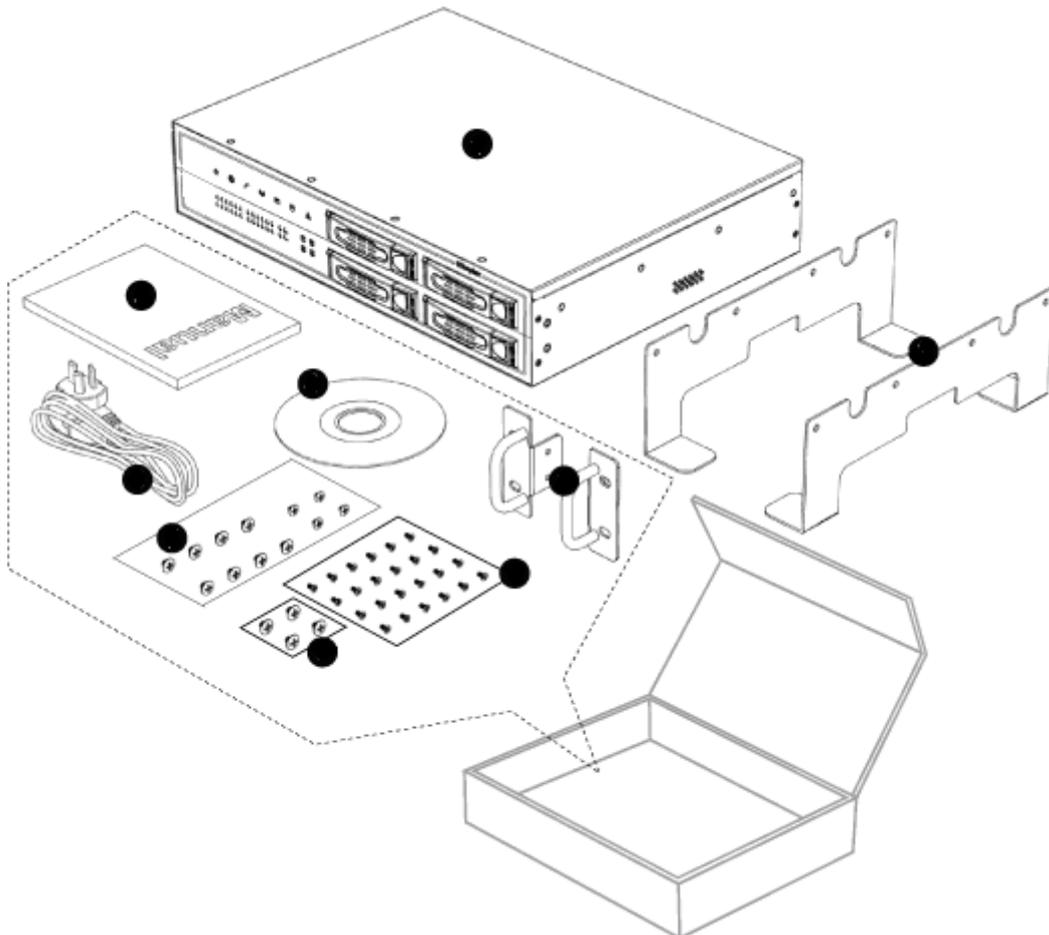
- IEEE 802.1d Spanning Tree
- IGMP Snooping

## 1.2 Package Contents

---

- UMG-2000 / UMG-2100 / UMG-2200 Unit x 1
- AC Power Cord x 1
- CD x 1
- Quick Installation Guide x 1
- Ear Brackets x 2
- Desk Brackets x 2
- Brackets Fixing Screws x 12
- Plug Screws x 4
- Disk Carrier Screws x 25

If any of above items are damaged or missing, please contact your dealer immediately.

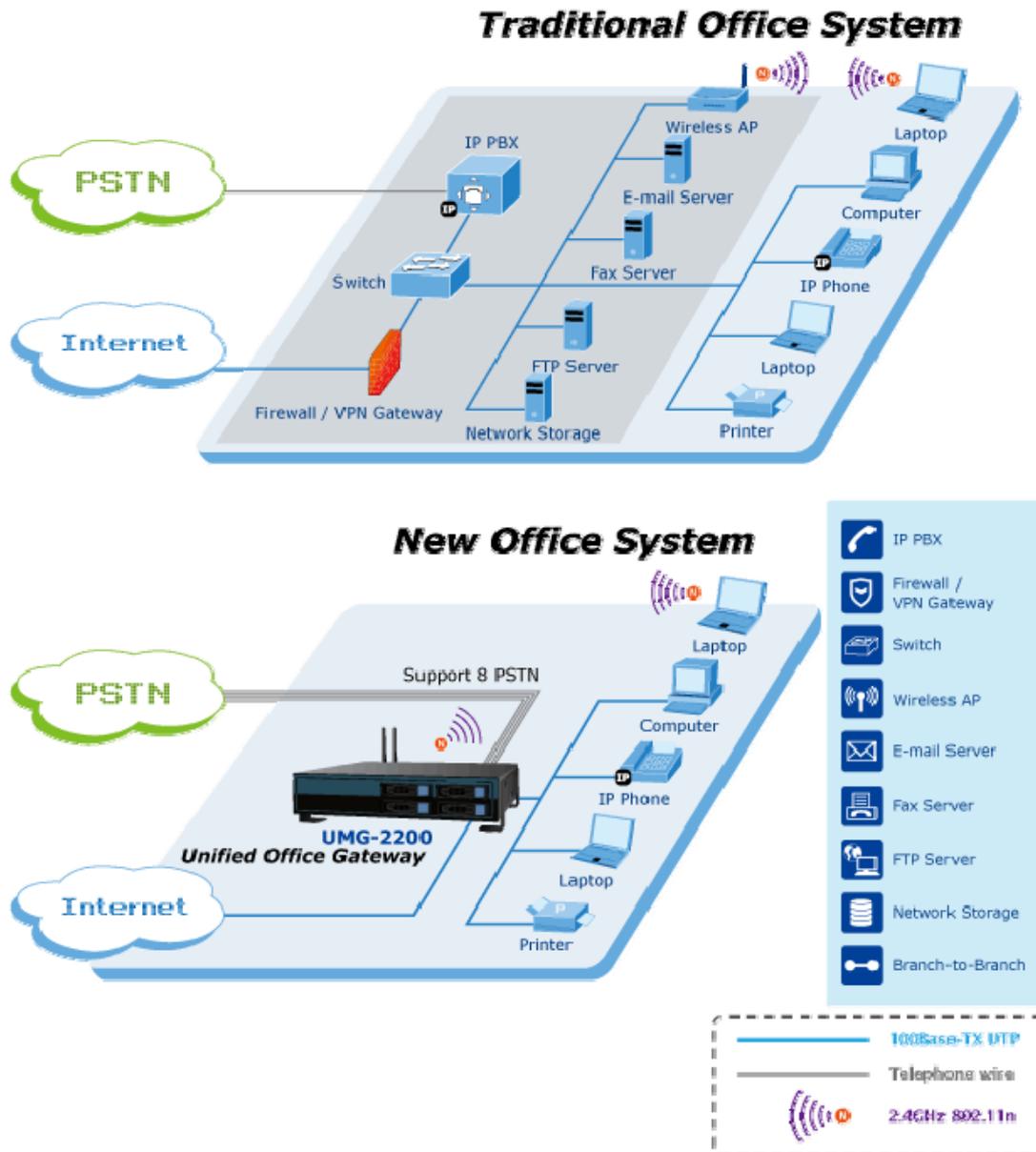


### 1.3 Application

#### Highly Integrated IT Services

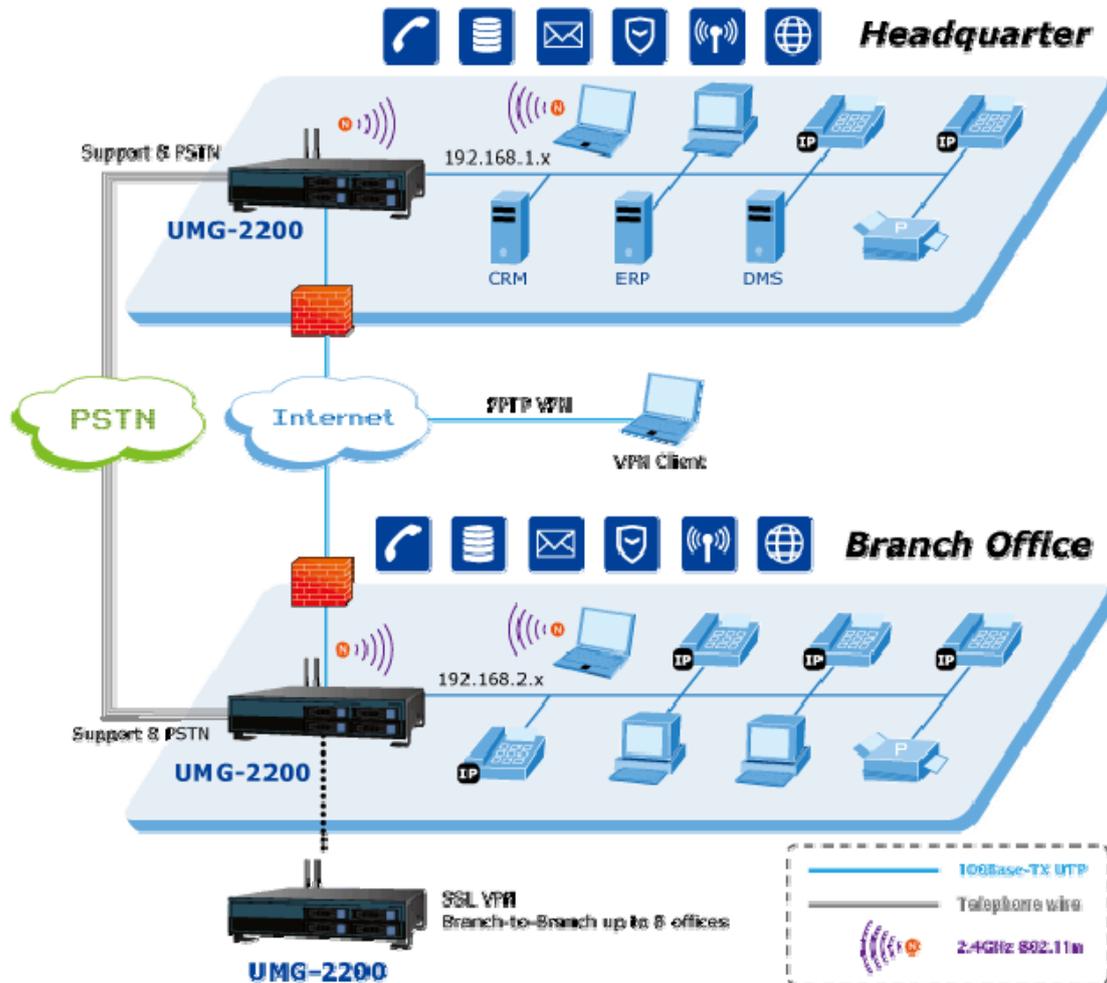
Providing IP PBX / VoIP, Internet Security, E-mail / FAX Server, Switch, Wireless AP, and Network Storage service, the UMG-2000 / UMG-2100 Series (Use “**UMG Series**” to represent UMG-2000 / UMG-2100 Series at the following descriptions) features single point of management to improve IT service ability.

The UMG Series benefits the SMBs lower cost of ownership, quick and easy deployment, low noise, space saving and energy conservation for better business environment.



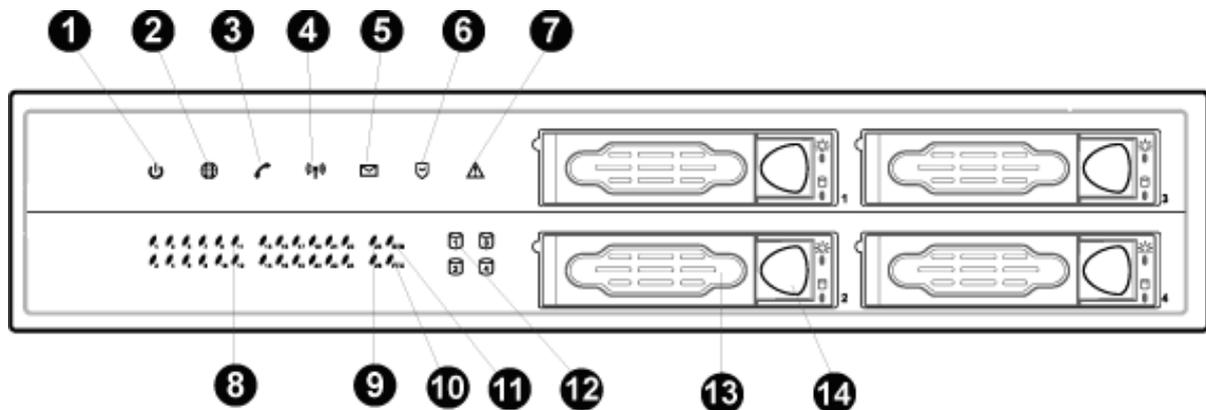
## Office Voice and Data Communication

The exchange of business data and voice with high security and superior performance is in great demand. A secure channel based on SSL VPN is built for data synchronization. A private voice switching system helps to avoid local or long distance charges by exchanging voice via a secure Internet tunnel. Additionally, web based remote management makes it possible to manage all IT resources in your branches without leaving your own office. The UMG Series supports Branch-to-Branch up to 8 offices.



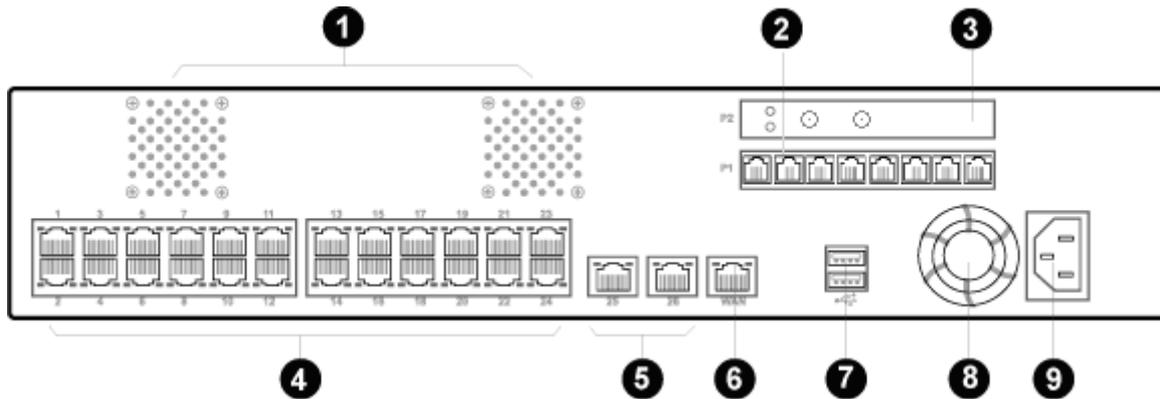
## 1.4 Outlook

### 1.4.1 Front Panel



1	PWR LED	On	Power On
		Off	Power Off
2	Internet LED	On	Connect to Internet
		Off	Disconnect to Internet
3	PBX LED	On	PBX function turn on
		Off	PBX function turn off
4	WLAN LED	On	Wireless function turn on
		Off	Wireless function turn off
5	E-mail LED	On	E-mail function turn on
		Off	E-mail function turn off
6	Firewall LED	On	Firewall/Security function turn on
		Off	Firewall/Security function turn off
7	Alert LED	On	Don't insert or pull put hard disk
		Off	Normal status
8	1~24 LED	On	Connect to 1~24 10/100Mbps LAN ports
		Off	Disconnect to 1~24 10/100Mbps LAN ports
9	25~26 LED	On	Connect to 25~26 10/100/1000Mbps LAN ports
		Off	Disconnect to 25~26 10/100/1000Mbps LAN ports
10	FTX LED	On	Fault redundant unit is connected and activated (future feature)
		Off	Fault redundant unit is not available (future feature)
11	BTB LED	On	Branch to Branch SSL VPN secure link is established
		Off	Branch to Branch SSL VPN secure link is not enabled or disconnected
12	Storage 1~4 LED	On	Read/Write data in the hard disk
		Off	Don't Read/Write data in the hard disk
13	Disk Carrier Handler	Push the handler to lock the carrier. Unlock and pull the handler to get the carrier out	
14	Disk Carrier switch	Press the button to pop out the SATA carrier	

## 1.4.2 Rear Panel



1	Cooling Fans	System cooling fans on rear panel
2	Voice (P1)	<b>UMG-2000</b> : 4 x RJ-11 (4 x FXO) <b>UMG-2100</b> : 1 x RJ-45 (1 x T1/E1) <b>UMG-2200</b> : 8 x RJ-11 (8 x FXO)
3	Wireless (P2)	1 x 802.11b/g/n Wireless Access Point, 2 x Antenna Detachable
4, 5	LAN	1~24 ports: 24 x RJ-45 (10/100Base-TX, Auto-Negotiation, Auto MDI/MDI-X) 25~26 ports: 2 x RJ-45 (10/100/1000Base-T, Auto-Negotiation, Auto MDI/MDI-X)
6	WAN	1 x RJ-45 (10/100Base-TX, Auto-Negotiation, Auto MDI/MDI-X)
7	USB	2 x USB2.0 (future feature)
8	Cooling Fan	Power supply cooling fan
9	AC PWR	100~127V AC 6.3A, 200~240V AC 3.0A, 50/60 Hz, 200 Watts

## 1.5 Technical Specifications

Hardware Specification	
Case	2U high Rack or Desk
WAN	1 x RJ-45 (10/100Base-TX, Auto-Negotiation, Auto MDI/MDI-X)
LAN	2 x RJ-45 (10/100/1000Base-T, Auto-Negotiation, Auto MDI/MDI-X) 24 x RJ-45 (10/100Base-TX, Auto-Negotiation, Auto MDI/MDI-X)
SATA support	4-Port SATA Controller (SATA I, SATA II Hard Disk)
Hard Disk	Hot-Swappable SATA Disk (4 x 80GB/160GB/250GB/500GB/1TB)
Voice	<b>UMG-2000: 4 x RJ-11 (4 x FXO)</b> <b>UMG-2100: 1 x RJ-45 (1 x T1/E1)</b> <b>UMG-2200: 8 x RJ-11 (8 x FXO)</b>
Wireless	1 x 802.11b/g/n Wireless Access Point, 2 x RP-SMA Detachable Antenna
USB	2 x USB2.0 (future feature)
LED Indicators	1 x PWR LED 1 x Internet LED 1 x PBX LED 1 x WLAN LED 1 x E-mail LED 1 x Firewall LED 1 x Alert LED 4 x Storage LEDs 1 x BTB LED 1 x FTX LED 26 x LAN LEDs
Software Specification	
VoIP	SIP protocol - SIP 2.0 (RFC3261,RFC2833) Registration - Factory Default: 50 nodes, Max. 250 nodes Calls - Max. 50 concurrent calls Voice Compression Code Technology - G.711, G.726, G.723.1 (5.3, 6.3kbps), G.729A (8kbps), GSM Echo Cancellation - G.165/G.168 Gain Control - In/Out +/-6db Voice Processing - Voice Activated Detection - DTMF Detection/Generation - G.165/G.168 Echo Cancellation (ECN) - Comfort Noise Generation (CNG) - Gain Control
IP PBX	- Support call hold, call waiting, 3-way call conference with feature phones - Built-in in-line call transfer - Unconditional, unavailable, busy call forward, custom time of no answer - Per-calling-number forward and rejection - Group-based call pick-up - Call-parking - Inter-PBX SIP trunking - Multi-room meet-me conference - Auto-attendant - Voice mail system

	<ul style="list-style-type: none"> <li>- Call privilege grouping</li> <li>- FXO/ISDN interface for PSTN/ISDN Inbound/outbound</li> <li>- FXO/ISDN disconnection tone detection</li> <li>- Caller ID detection</li> <li>- In-band/RFC2833/SIP-INFO DTMF translation</li> <li>- Music on hold (MoH), user upload MoH</li> <li>- Direct line Outbound</li> <li>- User upload IVR</li> <li>- Least Cost Routing (LCR)</li> <li>- Busy Lamp Field (BLF)</li> </ul>
Voicemail	<ul style="list-style-type: none"> <li>- User PIN</li> <li>- 450 minutes for personal record</li> <li>- E-mail notification</li> <li>- Personal reception on unavailability</li> <li>- Reply call or new call in voicemail menu</li> </ul>
E-mail	<p>Protocol</p> <ul style="list-style-type: none"> <li>- POP3,IMAP,SMTP, Web mail</li> </ul> <p>Support accounts</p> <ul style="list-style-type: none"> <li>- 250 users</li> </ul> <p>Email Security</p> <ul style="list-style-type: none"> <li>- Secured Socket Layer (SSL)</li> </ul> <p>Anti-Virus</p> <ul style="list-style-type: none"> <li>- ClamAV</li> </ul> <p>Anti-Spam</p> <p>Junk mail block</p> <p>Mailbox size Limit</p> <ul style="list-style-type: none"> <li>- 200M/500M/1G/2G/No Limit</li> </ul> <p>Attachment</p> <ul style="list-style-type: none"> <li>- 2M/5M/10M/20M/50M/No Limit</li> </ul> <p>Block List</p> <ul style="list-style-type: none"> <li>- Share/User/Domain security modes</li> </ul> <p>Email Backup</p> <ul style="list-style-type: none"> <li>- Auto-Backup</li> </ul>
Network Storage	<p>RAID</p> <ul style="list-style-type: none"> <li>- RAID 0, RAID 0/1, RAID 5, JBOD</li> </ul> <p>Date Sharing</p> <ul style="list-style-type: none"> <li>- Windows Network Sharing, NFSv3</li> </ul>
Security	<p>Network Security</p> <ul style="list-style-type: none"> <li>- DoS attack Prevention</li> </ul> <p>VPN Max. connection</p> <ul style="list-style-type: none"> <li>- 100 PPTP VPN tunnels</li> <li>- 8 Site-to-Site SSL VPN tunnels</li> </ul> <p>VPN pass-through</p> <ul style="list-style-type: none"> <li>- IPSec, PPTP, L2TP pass-through</li> </ul> <p>Internet Security</p> <ul style="list-style-type: none"> <li>- Domain/Keyword Content Filter, Access Control</li> <li>- IP-MAC Binding</li> </ul>
Other Protocol / Function	<p>Protocol</p> <ul style="list-style-type: none"> <li>- TCP/IP, NAT, DHCP, HTTP, DNS, NTP, HTTPS, CIFS/SMB, NFSv3</li> </ul> <p>LAN</p> <ul style="list-style-type: none"> <li>- IEEE 802.1d Spanning Tree</li> </ul> <p>Internet Access</p> <ul style="list-style-type: none"> <li>- Static IP, PPPoE, DHCP, PPTP, L2TP</li> </ul> <p>DMZ, UPnP, QoS, DDNS</p> <p>Multiple host name</p>
Management	<ul style="list-style-type: none"> <li>- Web based GUI management</li> <li>- Firmware upgradeable via local</li> </ul>

## 2. Installation

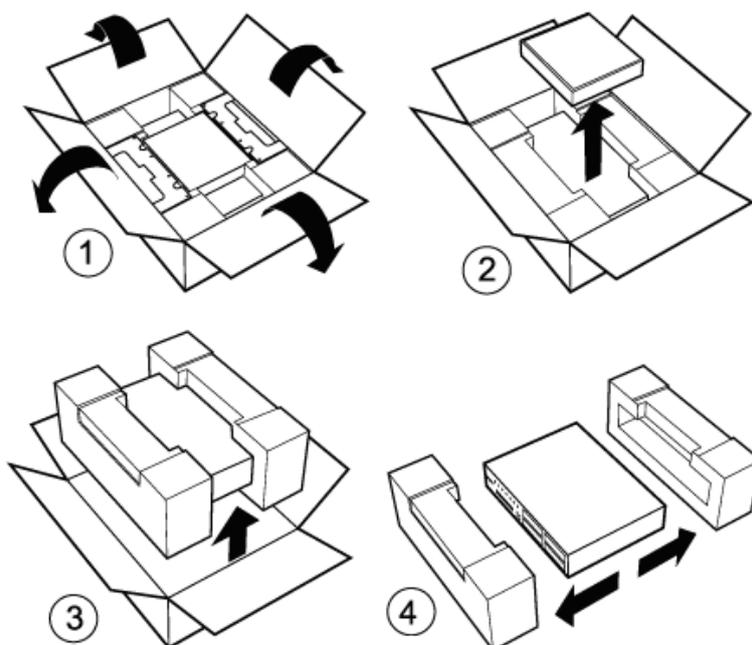
The followings are instructions for setting up the UMG-2000 Series. Refer to the illustration and follow the steps install your unified office gateway.

### 2.1 Hardware Installaion

#### 2.1.1 Unpack the UMG-2000 Series

**Note:**

You should inspect the box which the system was shipped in and note if it was damaged in any way before the unpacking. If the UMG-2000 Series itself shows damage you should file a damage claim with the carrier to who delivered it. Unpack the UMG-2000 Series as listed below.



#### 2.1.2 Choosing a Setup Location

Decide on a suitable location for the UMG-2000 Series which should be situated in a clean, dust-free, and well ventilated area. Avoid areas where heat, electrical noise and electromagnetic fields are generated. Place the UMG-2000 Series near a grounded power outlet and pay attention to the following requirements.

- Leave approximately 40cm (16inche) of clearance in front of the UMG-2000 Series to ensure the disk carriers can be unplugged.
- Leave approximately 30cm (12 inch) of clearance in the back of the UMG-2000 Series to allow for sufficient airflow and ease in servicing.

### 2.1.3 Preparing for Setup

The UMG-2000 Series system was shipped with desk brackets, ear brackets, and mounting screws, so it is possible to install the UMG-2000 Series into the mounted rack or on the desk brackets. Please read following sections in its entirety before you begin the installation and follow the steps in the order given to complete the installation process correctly.

### 2.1.4 Precautions

- ✓ Review the electrical and general safety precautions.
- ✓ Install the heaviest server components on the bottom of the rack first, and then work up if you want to mount the UMG-2000 Series to a rack.
- ✓ Use a power supply regulating uninterruptible (UPS) to protect the server from failure.
- ✓ Allow the hot plug SATA drives and power supply units to cool before touching them.
- ✓ Always keep the rack's front door and all panels and components on the servers closed when not servicing to maintain proper cooling.

### 2.1.5 Installation Consideration

#### **Ambient Operating Temperature**

If installed in a closed or multi-unit rack assembly, the ambient operating temperature of the rack environment may be greater than the ambient temperature of the room. Therefore, consideration should be given to installing the equipment in an environment compatible with the manufacturer's maximum rated ambient temperature.

#### **REDUCED AIRFLOW**

Consideration should be given to the amount of airflow required for safe operation maybe not compromised for the rack mounting.

#### **Circuit Overloading**

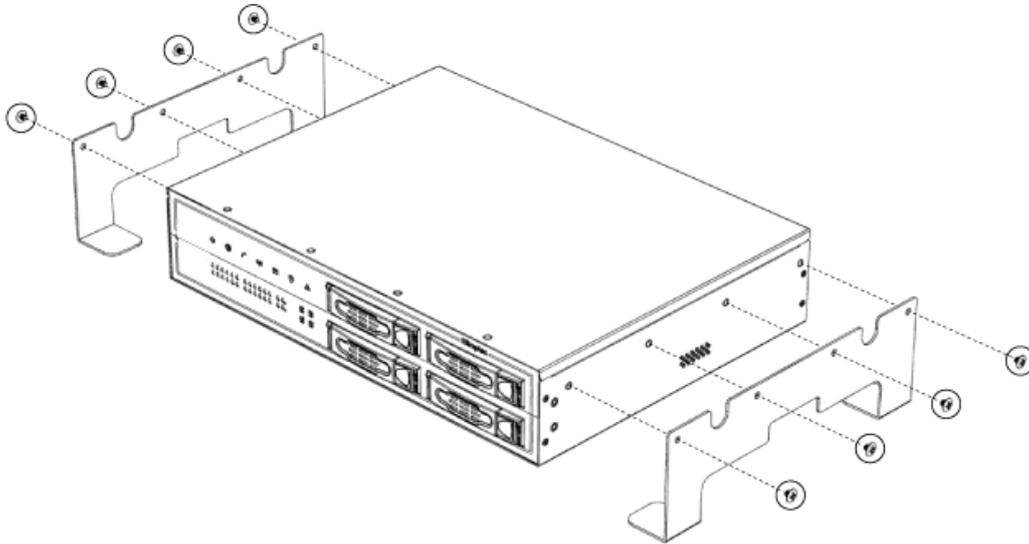
Consideration should be given to the connection of the equipment to the power supply circuitry and the effect that any possible overloading of circuits might have on over-current protection and power supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.

#### **Reliable Ground**

A reliable ground must be maintained at all times. To ensure this, the rack itself should be grounded. Particular attention should be given to power supply connections other than the direct connections to the branch circuit (i.e. the use of power strips, etc.).

## 2.1.6 The Desktop Brackets Installation

- Unpack the UMG-2000 Series.
- The desk brackets have been fixed to the device before packing.
- Place the system to appropriate site.

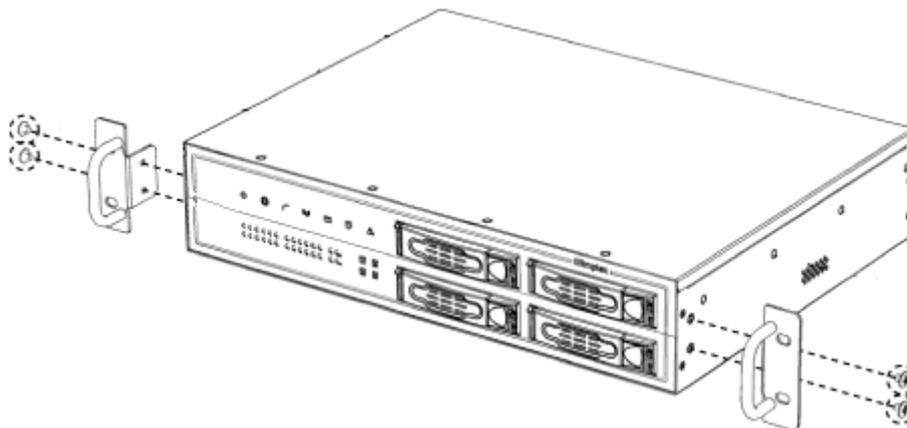


## 2.1.7 The Rack Mount Installation

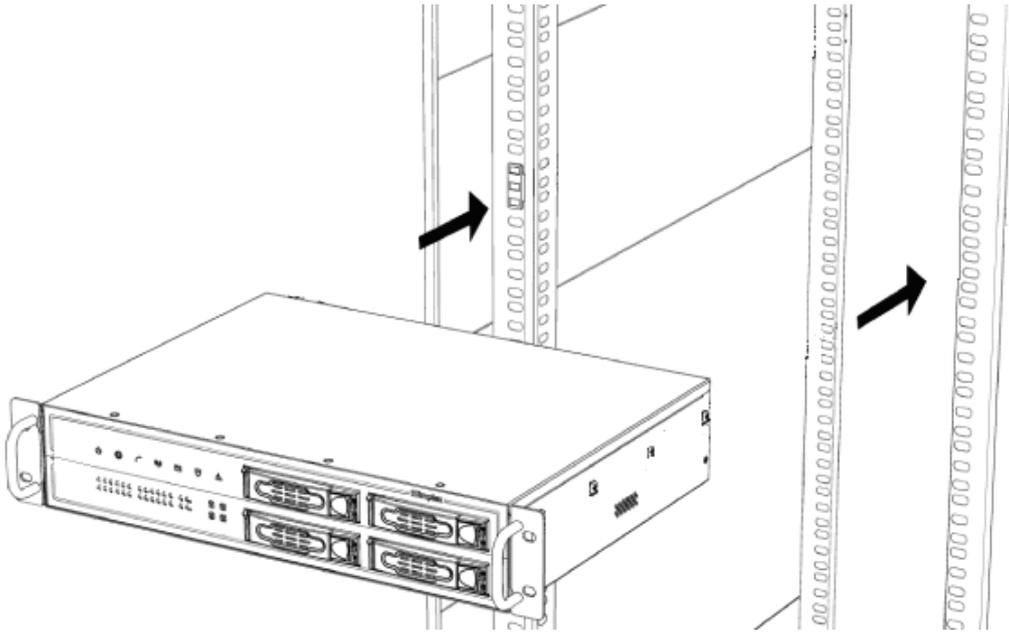
It is strongly recommended to securely fasten the mounting rack to the floor or wall to eliminate any possibility of tipping over the rack. This is especially important if you decide to install several UMG-2000 Series chassis in the top of the rack.

A brief overview of the UMG-2000 Series installation is as follows:

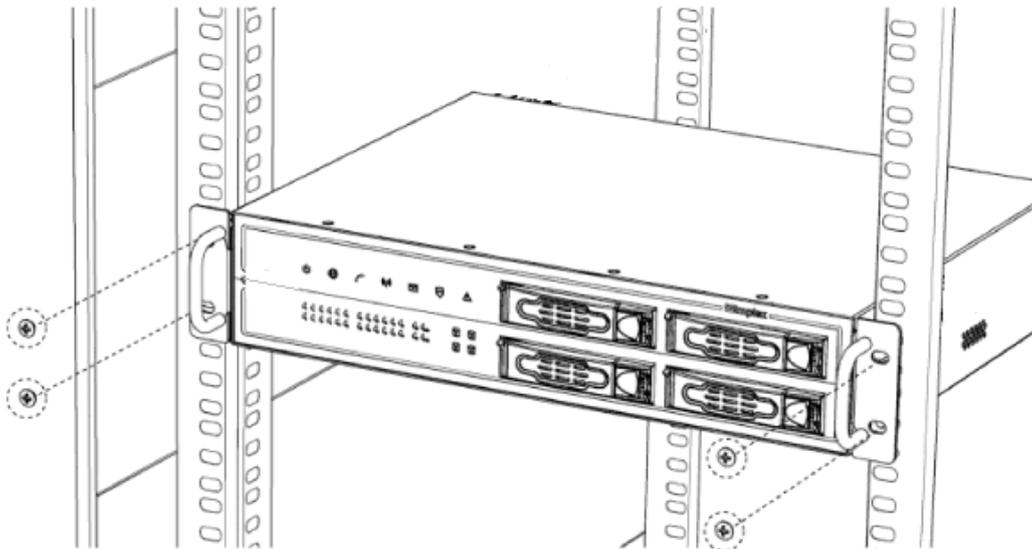
- Select an appropriate site in the rack.
- Unload 4 the plug screws from each side of the server.
- Mount the ear brackets to the server from the each side.



- Mount the server into the rack.



- Lock the server to the rack by mounting the ear brackets to the rack.



## 2.1.8 The Hard Disk Installation

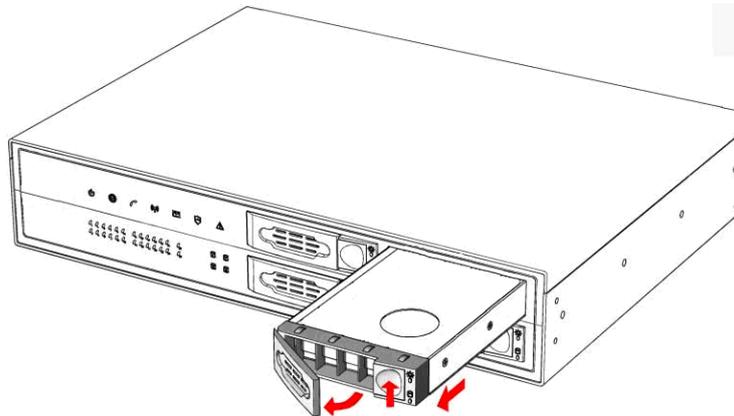
The SATA subsystem supports four hot-swappable hard drives. The SATA drives are inserted to the SATA backplane that provides power and bus termination.

---

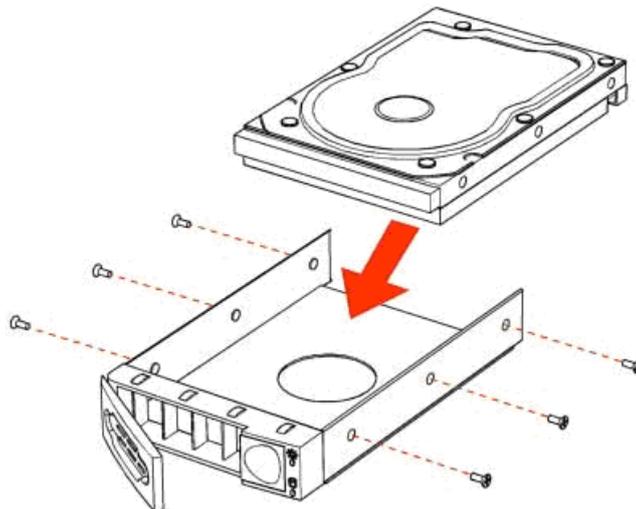
**Note:**

1. Please install at least one 80G HDD to the No.1 disk carrier before system configurations.
  2. If with single HDD, please select RAID level to JBOD.
- 

- Locate the storage subassembly.
- Press the disk carrier switch to unlock the carrier.
- Unplug the disk carrier by pulling the carrier handler.



- Mount the disk into the carrier and load the fixing screws.

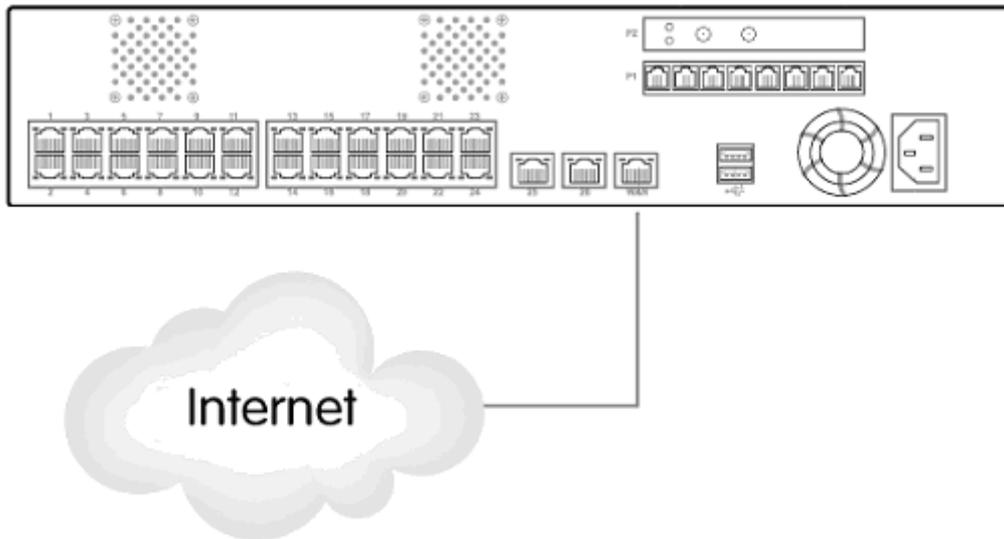


- Press the disk carrier switch to insert the carrier to the disk slot.
- Close the disk carrier lock/switch to lock the carrier.

## 2.2 Physical Connection

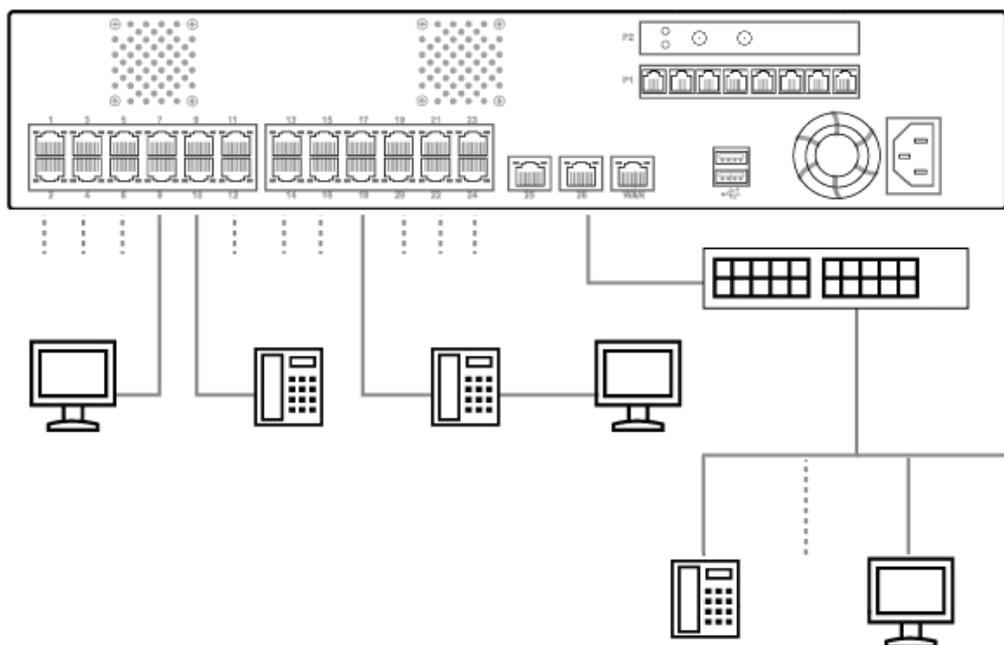
### 2.2.1 WAN Connection

- Locate the WAN port on the rear panel.
- Connect the WAN port with the Ethernet cable.



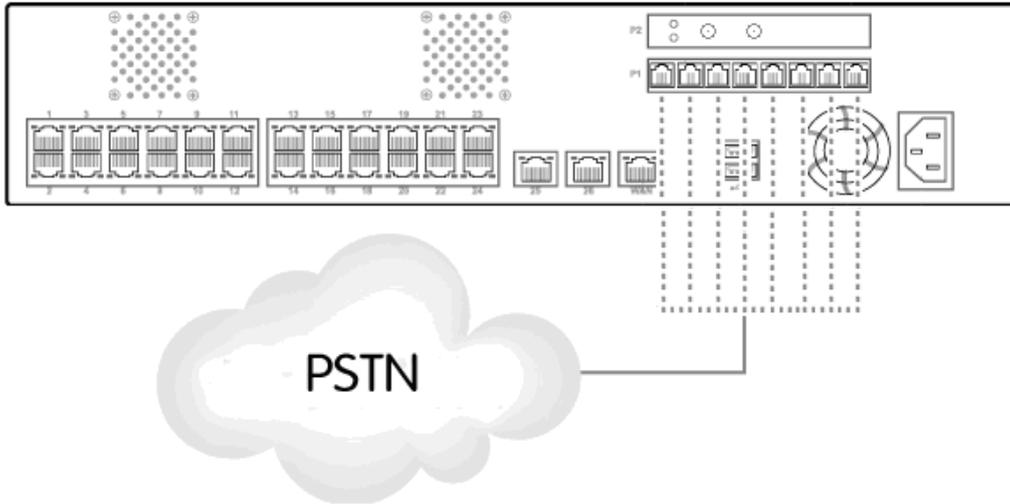
### 2.2.2 LAN Port Connection

- There are 26 Ethernet ports on the rear panel. The port 1 to 24 are 10/100 Mbps Ethernet ports and the port 25 and port 26 are 10/100/1000 Ethernet ports.
- It is recommended to connect the third party switches to the port 25, 26 to expand the LAN ports.



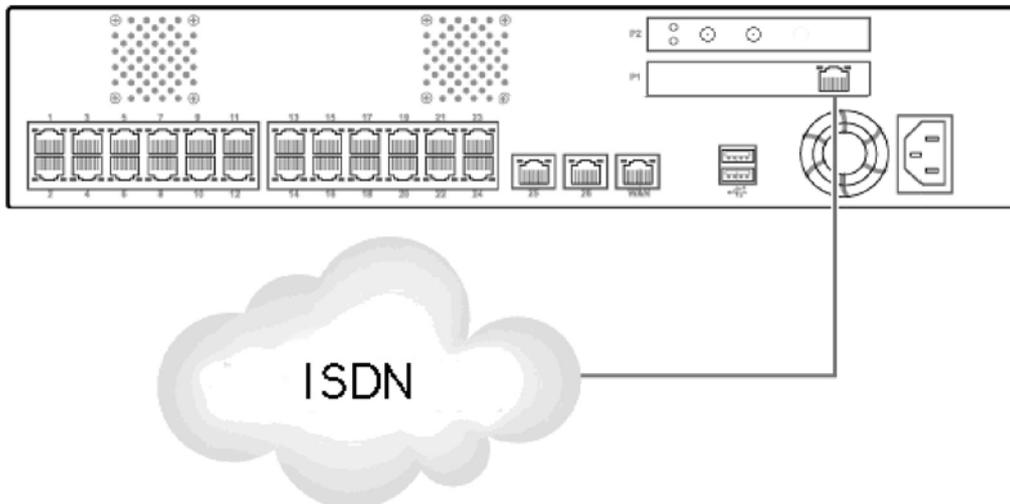
### 2.2.3 PSTN FXO Port Connection

- Locate the voice port of the PSTN adapter on the rear panel.
- The Analog PSTN port may vary from 4 / 8 FXO ports.
- Connect one or more telephone cables to one of the selected FXO port.



### 2.2.4 ISDN T1/E1 Port Connection

- Locate the digital voice port of the T1/E1 adapter on the rear panel.
- Connect the ISDN network with the T1/E1 port.



## 2.3 Quick Setup Wizard

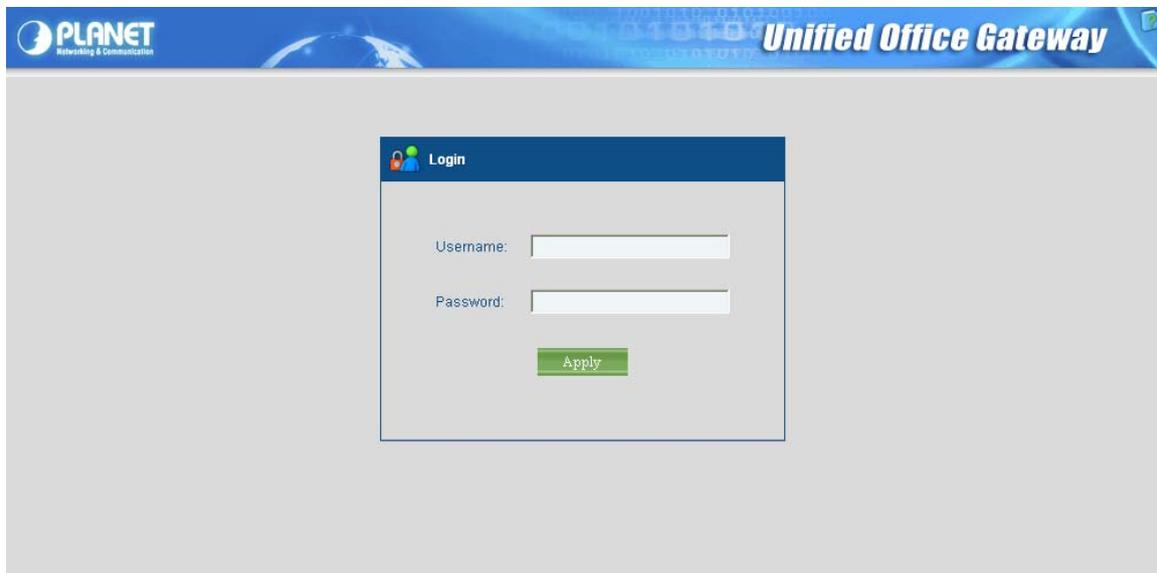
---

### 2.3.1 First Time Login

Now that the network connection between your PC and UMG-2000 Series has been established, you must login in order to access PLANET View.

Launch a web browser (for example: IE, Firefox etc.) and type the UMG-2000 Series IP address in the address bar. The default address is "<http://192.168.1.1>".

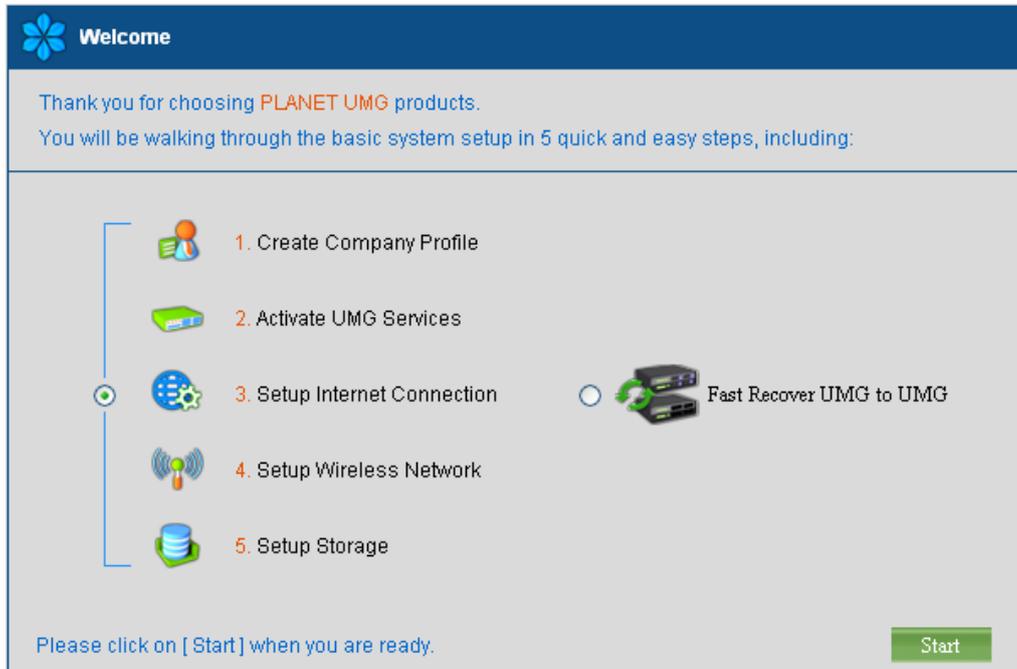
If you can not see the following login page, recheck your physical LAN connection and repeat Section 4.2 LAN Connection. To avoid web-based management abused by unauthorized users, the login sessions will logout automatically if the session is inactive for more than 5 minutes. Type in an authorized username and password and then click the button "Apply". The default username is "**admin**", and its password is "**admin**" all in lower case.



The screenshot shows the login interface for the PLANET Unified Office Gateway. At the top, there is a blue banner with the PLANET logo on the left and the text "Unified Office Gateway" on the right. Below the banner, the main content area is light gray. In the center, there is a "Login" box with a blue header containing a user icon and the word "Login". Inside the box, there are two input fields: "Username:" and "Password:". Below the password field is a green "Apply" button.

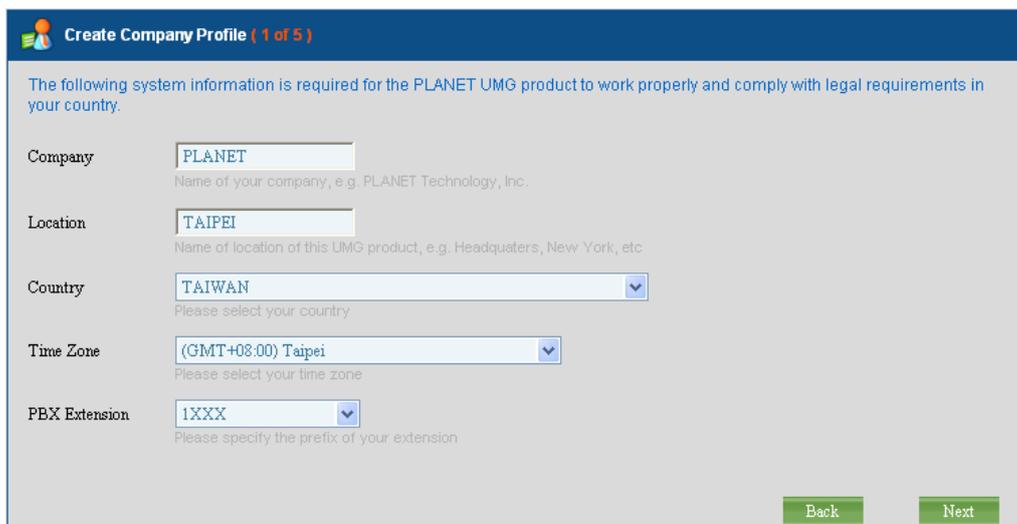
### 2.3.2 Welcom to Quick Start

After the first login, an easy and short quick start up should be completed to make the UMG-2000 Series service normally. There is an alternative selection in the page “Welcome”. One selection is for “Quick Start” and the other is for “Faster Recovery UMG to UMG” which will be explained in the user’s manual. The quick start includes five steps which will lead administrator to setup the UMG-2000 Series. Check the first radio box and then click the button “Start” to continue.



### Step 1: Create the Company Profile

This page allows an administrator to build a company profile. Specify the profile and then click the button “Next” to go to step 2.



Item	Description
Company	Specify your company name.
Location	Specify your city name.
Country	Specify your country name.
Time Zone	Specify the time zone.
PBX Extension	Specify the prefix of the extensions. All PBX extensions will be prefixed with this number. (X=0~9).

## Step 2: Activating UMG-2000 Series services

The UMG-2000 Series allows the administrator to activate the service on demand. By default, all services are inactive. The administrator can activate the service in this page by checking the radio box of the corresponding service. The activated services will start up by using the default configuration after the quick start. Click the button “Next” to go to step 3.

Item	Description
PBX	Enable or disable the IP PBX service.
PPTP VPN	Enable or disable the PPTP VPN service.
Email	Enable or disable the Email service.
Network Storage	Enable or disable the network storage service.
Internet Domain Name	Specify a valid Internet domain for the email server if the email service is enabled.

### Step 3: Setting up the Internet Connection

This page allows the administrator to quickly setup the WAN connection. To setup the Internet connection, you should be awarded of what method you are using to connect to the Internet. All technical information should be provided by your Internet Service Provider (ISP). The ISP type should be one of the followings: static, DHCP, PPPoE or PPTP. Select your ISP type in the drop down menu. Specify the Internet connection configuration and then click the button “Next” to go to step 4 or click the button “Skip” to skip this step.

#### AUTO DETECT ISP TYPE

By clicking the button “Detect”, you can make the UMG-2000 Series to recognize the ISP type automatically.

Setup Internet Connection (3 of 5)

ISP Type: Static [Detect]

IP Address: [ ][ ][ ][ ]

Subnet Mask Address: [ ][ ][ ][ ]

Default Gateway Address: [ ][ ][ ][ ]

DNS Server Address: [ ][ ][ ][ ]

MAC Address: 00:30:4F:71:23:17

[Back] [Next] [Skip]

It may take a while to detect your ISP type. Please wait.

Setup Internet Configuration

System is detecting your type of internet service provider (ISP)...

Detecting :32%

32%

Operation is in process, please wait...

The ISP type will be detected and the result will be presented as follows. If “Network Cable Disconnected” is detected, please recheck the physical connection and repeat the action as shown in Section “WAN Connection”. There could be more than one ISP type recognized, so choose the most suitable type from the list and then click the button “Next” to continue.

The screenshot shows a window titled "Setup Internet Configuration". Below the title bar, it says "Internet service provider(ISP) type detect result :". There is a list of radio buttons with the following options: "Network Cable Disconnected", "ADSL PPOE Detected", "PPTP Detected", "DHCP Detected" (which is selected), and "Static Detected". Below the list, it says "Please select one to config as your ISP type." and there is a green "Next" button in the bottom right corner.

**MANUAL SETUP INTERNET CONFIURATION: STATIC**

If your ISP type is “Static”, choose it as your ISP type and setup the configuration.

The screenshot shows a window titled "Setup Internet Connection (3 of 5)". It contains several input fields: "ISP Type" with a dropdown menu set to "Static" and a "Detect" button; "IP Address", "Subnet Mask Address", and "Default Gateway Address" each with four input boxes; "DNS Server Address" with a dropdown arrow and two input boxes; and "MAC Address" with the value "00:30:4F:71:23:17". At the bottom right, there are three buttons: "Back", "Next", and "Skip".

Item	Description
IP Address	Specify the static IP address.
Subnet Mask Address	Specify the subnet mask address.
Default Gateway Address	Specify the IP address of the default gateway.
DNS Server Address	Specify the IP address of the primary and secondary Domain Name System.
MAC Address	Show MAC address information.

**MANUAL SETUP INTERNET CONFIURATION: DHCP**

If your ISP type is “DHCP”, choose it as your ISP type and setup the configuration.

Item	Description
DNS Server Address	Automatically obtain the DNS address or specify the IP address of the primary and secondary DNS server.
MAC Address	Show MAC address information.

**MANUAL SETUP INTERNET CONFIURATION: PPPOE**

If your ISP type is “PPPoE”, choose it as your ISP type and setup the configuration.

Item	Description
Login Name	Specify the login username to the PPPoE server.
Password	Specify the login password to the PPPoE server.
Confirm Password	Retype the password.
Static IP Address	Specify whether you have a static IP address.
IP address	Specify your static WAN IP address if you have enabled the “Static IP Address”.
Subnet Mask Address	Specify the subnet mask address if you have enabled the “Static IP Address”.
DNS Server Address	Automatically obtain the DNS address or specify the IP address of the primary and secondary DNS server.
MAC Address	Show MAC address information.

**MANUAL SETUP INTERNET CONFIURATION: PPTP**

If your ISP type is “PPTP”, choose it as your ISP type and setup the configuration.

Item	Description
PPTP Server	Specify the PPTP server IP address.
Login Name	Specify the username to login to the PPTP server.
Password	Specify the corresponding password to login to the PPTP server.
Confirm Password	Retype the password.
Static IP Address	Specify whether you have a static WAN IP address.
IP address	Specify whether you have a static IP address.
Subnet Mask Address	Specify your static WAN IP address if you have enabled the “Static IP Address”.
DNS Server Address	Specify the subnet mask address if you have enabled the “Static IP Address”.
MAC Address	Show MAC address information

## Step 4: Setting the Wireless Network

This page allows the administrator to quickly setup the wireless Access Point (AP). Specify the wireless configuration and then click the button “Next” to go to step 5.

Item	Description
Access Point (AP)	Enable or disable the wireless AP service.
Hide SSID	Decide whether or not to make the wireless AP SSID visible.
Network Name (SSID)	Specify the preferred SSID name string.
Wireless Region	Select the area of location yours.
Wireless Mode	Select the preferred wireless AP mode: 802.11b / 802.11g / 802.11n.
Channel	Select the preferred wireless channel number.
Authentication Type	Specify the authentication type: Open system / Shared Key / WPA / WPA2.
Data Encryption	Select the Data Encrypt type.
Encrypt Strength	Select the encrypt strength.
Security Key	Specify the key for the clients to access this AP.

## Step 5: Creating the Network Storage

This page allows the administrator to quickly setup the storage. Specify the Redundant Array of Independent Disks (RAID) level and then click the button “Next” to go to step 6.

🗄️
**Create Network Storage ( 5 of 5 )**

Please select the raid level

**Hard Drives**

SATA1:	Hitachi HDT721010SLA360 976.76 GB	SATA3:	Hitachi HDT721010SLA360 976.76 GB
SATA2:	Hitachi HDT721010SLA360 976.76 GB	SATA4:	Hitachi HDT721010SLA360 976.76 GB

Total Capacity: 976.76 GB

Please select the raid level

JBOD
  RAID 0
  RAID 0+1
  RAID 5

Warning: ALL DATA ON THESE HARD DRIVES WILL BE ERASED!

Back
Next

## Step 6: Confirmation

Please recheck your input data to ensure the accurate. Click the button “Back” to make changes. Then confirm your data and wait for the accomplishment of the wizard. It will take a couple of minutes. Please “**do not**” close the browser. The browser will show the RAID building progress. After finishing the wizard successfully, the page of “Personal Account Web Administration” will automatically appear.

🌸
**Confirm**

You have just completed the quick start setup. Here is a summary of your settings:

<p><b>Profile</b></p> <table style="width: 100%; border-collapse: collapse;"> <tr><td style="width: 30%;">Company</td><td>PLANET</td></tr> <tr><td>Location</td><td>TAIPEI</td></tr> <tr><td>Country</td><td>TAIWAN</td></tr> <tr><td>Extension</td><td>1XXX</td></tr> </table>	Company	PLANET	Location	TAIPEI	Country	TAIWAN	Extension	1XXX	<p><b>Service</b></p> <table style="width: 100%; border-collapse: collapse;"> <tr><td style="width: 30%;">PBX</td><td>Disabled</td></tr> <tr><td>Email</td><td>Disabled</td></tr> <tr><td>PPTP VPN</td><td>Disabled</td></tr> <tr><td>Storage</td><td>Disabled</td></tr> <tr><td>Internet Domain Name</td><td>N/A</td></tr> </table>	PBX	Disabled	Email	Disabled	PPTP VPN	Disabled	Storage	Disabled	Internet Domain Name	N/A																
Company	PLANET																																		
Location	TAIPEI																																		
Country	TAIWAN																																		
Extension	1XXX																																		
PBX	Disabled																																		
Email	Disabled																																		
PPTP VPN	Disabled																																		
Storage	Disabled																																		
Internet Domain Name	N/A																																		
<p><b>Storage</b></p> <table style="width: 100%; border-collapse: collapse;"> <tr><td style="width: 30%;">RAID Level</td><td>JBOD</td></tr> </table>	RAID Level	JBOD																																	
RAID Level	JBOD																																		
<p><b>Wireless</b></p> <table style="width: 100%; border-collapse: collapse;"> <tr><td style="width: 30%;">Access Point(AP)</td><td>Disabled</td></tr> <tr><td>Hide SSID</td><td>Disabled</td></tr> <tr><td>Network Name(SSID)</td><td>UMG_WIFI</td></tr> <tr><td>Wireless Region</td><td>USA</td></tr> <tr><td>Channel</td><td>1</td></tr> <tr><td>Wireless Mode</td><td>802.11b</td></tr> <tr><td>Authentication Type</td><td>open</td></tr> <tr><td>Data Encryption</td><td>none</td></tr> <tr><td>Security Key</td><td>N/A</td></tr> </table>	Access Point(AP)	Disabled	Hide SSID	Disabled	Network Name(SSID)	UMG_WIFI	Wireless Region	USA	Channel	1	Wireless Mode	802.11b	Authentication Type	open	Data Encryption	none	Security Key	N/A	<p><b>Internet</b></p> <table style="width: 100%; border-collapse: collapse;"> <tr><td style="width: 30%;">ISP Type</td><td>static</td></tr> <tr><td>IP Address</td><td>210.66.155.75</td></tr> <tr><td>Subnet Mask Address</td><td>255.255.255.224</td></tr> <tr><td>Default Gateway Address</td><td>210.66.155.94</td></tr> <tr><td>Primary DNS Address</td><td>168.95.1.1</td></tr> <tr><td>Secondary DNS Address</td><td>168.95.192.1</td></tr> <tr><td>MAC</td><td>00:30:4F:71:23:17</td></tr> <tr><td>MTU</td><td>1400</td></tr> </table>	ISP Type	static	IP Address	210.66.155.75	Subnet Mask Address	255.255.255.224	Default Gateway Address	210.66.155.94	Primary DNS Address	168.95.1.1	Secondary DNS Address	168.95.192.1	MAC	00:30:4F:71:23:17	MTU	1400
Access Point(AP)	Disabled																																		
Hide SSID	Disabled																																		
Network Name(SSID)	UMG_WIFI																																		
Wireless Region	USA																																		
Channel	1																																		
Wireless Mode	802.11b																																		
Authentication Type	open																																		
Data Encryption	none																																		
Security Key	N/A																																		
ISP Type	static																																		
IP Address	210.66.155.75																																		
Subnet Mask Address	255.255.255.224																																		
Default Gateway Address	210.66.155.94																																		
Primary DNS Address	168.95.1.1																																		
Secondary DNS Address	168.95.192.1																																		
MAC	00:30:4F:71:23:17																																		
MTU	1400																																		

Now the UMG is ready to serve your office once you have added user accounts.

Back
Confirm

## 3. Web Management - Home

UMG-2000 Series provides a basic chassis as the hardware platform, back-end service control software and front-end web-based GUI management tool PLANET View. This chapter gives a general description of UMG-2000 Series.

### 3.1 Overview

The “Overview” screen presents the UMG-2000 Series system service status summary in one convenient location. You can quickly and efficiently view the important details of the system status, service state, and environment condition.

The screenshot displays the PLANET Unified Office Gateway web management interface. The header includes the PLANET logo, a welcome message for user 'gamin', and the company name 'PLANET' and location 'TAIPEI'. The main content area is divided into three sections: System Status, Smart IT Service, and Network Port Status. The System Status section lists various system parameters such as Software Version (v3.7.0), Hardware Version (v2.0.0), Current Date (12/06/2010 17:04:15), Internet Domain Name (planet.com.tw), Internet IP Address (210.66.155.82), Local Server Address (192.168.1.75), PBX Call Prefix (5XXX), Storage Workgroup Name (workgroup), Deploy Mode (Standalone), System Uptime (0:49:06), Last Reboot Date (12/06/2010 16:14:33), Last Software Update Date (12/01/2010 09:47:13), Temperature (106.70Fah/41.50°C), and CPU Usage (1%). The Smart IT Service section shows the status of various services: PBX VoIP (Enabled, Up), Wireless-AP (Enabled, Up), Email Server (Enabled, Up), Firewall (Enabled, Up), Network Storage (Enabled, Up), PPTP VPN (Enabled, Up), DDNS(DynDns) (Disabled, Down), Fax Server (Enabled, Up), WEB Server (Disabled, Down), FTP/S Server (Disabled, Down), and Alert (Enabled, Normal). The Network Port Status section shows a grid of 28 network ports, with ports 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, and 26 marked as 'WAN'.

#### HEADER

**Welcome:** Displays the effective user ID.

**Company:** Displays the company name.

**Location:** Displays the location.

#### SYSTEM STATUS

This section lists the system status of UMG-2000 Series, including the current system information and the software, hardware versions.

**Software Version:** Displays the software running version number.

**Hardware Version:** Displays the hardware version.

**Internet domain Name:** Displays the Internet Domain Name configuration.

**Storage Workgroup Name:** Displays the Workgroup name of the Network Storage.

**Deploy Mode:** Displays the deployment mode: Standalone, Headquarter, or Branch mode.

**System Uptime:** Displays the total uptime since the last reboot.

**Last Reboot Time:** Displays the last system reboot time.

**Current Date:** Displays the current date.

**Temperature:** Display the current system internal temperature.

**CPU Usage:** Displays the current CPU utilization rate.

## UMG SERVICE

This section lists the state and status of all the IT services.

**PBX:** Displays the state (enable or disable) and status (up or down) of VoIP service.

**Wireless:** Display the state (enabled or disabled) and status (up or down) of WiFi service.

**Email:** Displays the Email service state (enabled or disabled) and its status (up or down).

**Firewall:** Displays the Firewall service state (enabled or disabled) and its status (up or down).

**Storage:** Displays the storage service state (enabled or disabled) and its status (up or down).

**PPTP VPN:** Displays the VPN service state (enabled or disabled) and its status (up or down).

**Alert:** Displays the current system alert state, enabled or normal.

## NETWORK CONNECTION

This section shows the current status of all the physical network links.

**Port 1-24:** Displays the physical link state of the 10/100 Mbps ports, connected or disconnected.

**Port 25:** Displays the physical link state of the 10/100/1000 Mbps network port, connected or disconnected.

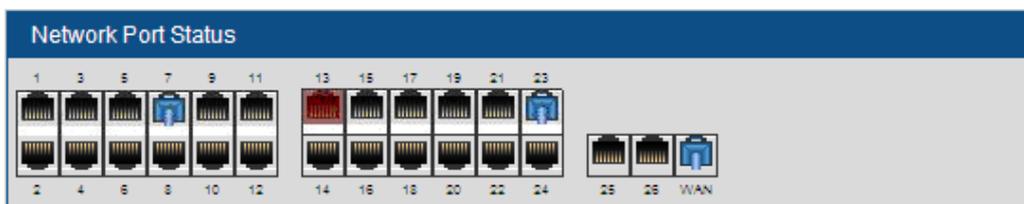
**Port 26:** Displays the physical link state of the 10/100/1000 Mbps network port, connected or disconnected.

**WAN:** Displays the physical link state of the 10/100 Mbps WAN port state, connected or disconnected.

## 3.2 Spanning Tree Protocol

---

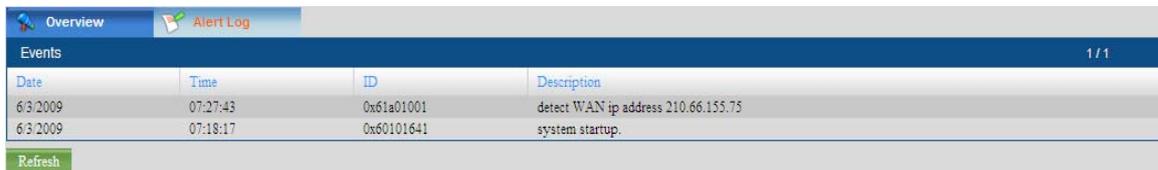
Spanning Tree Protocol (STP) is a link management protocol that provides path redundancy while preventing undesirable loops in the network. For an Ethernet network to function properly, only one active path can exist between two stations. The UMG-2000 Series uses STP on the switch (Port 1 to Port 26) to detect the loop link. If the loop occurs, the information will be presented in the “Overview” page. Then, unplug the indicated cable and check your physical Ethernet link.



### 3.3 Alert Log

---

The screen displays the UMG-2000 Series alert log list. If the administrator has assigned the alert email address, the messages will be sent to the added email address.



Overview		Alert Log		
Events				1 / 1
Date	Time	ID	Description	
6/3/2009	07:27:43	0x61a01001	detect WAN ip address 210.66.155.75	
6/3/2009	07:18:17	0x60101641	system startup.	

Refresh

**Date:** Displays the date of the alert log.

**Time:** Displays the time of the alert log.

**ID:** Displays the alert log ID.

**Description:** Displays the detail description of the alert Log.

## 4. Web Management - User

The UMG-2000 Series provides a user based service provisioning with secured access control based on the given privilege.

### GROUP MANAGEMENT

Group management allows the administrator to organize groups and departments similar to the organization of your company and assign different privileges to different groups. It creates a more efficient way of managing and controlling large numbers of users.

### USER MANAGEMENT

User management allows the administrator to manage the user profile. Based on the profile, the data and services of this user can be created, updated or deleted. An user provisioning services include email, voice, remote access VPN, and network storage.

## 4.1 User Overview

The administrator can get the overview of all the available users' profile including a brief introduction in the "Overview" page. To get more detailed information on a specific user, click the corresponding user name. (Refer to Section - Updating the User Setting.) The administrator can also delete or temporarily suspend the user's access by checking the radio box and clicking the "delete" button. (Refer to Section - Delete a User Account.)



Username ▲	Department ▲	Email ▲	PPTP VPN ▲	Extension ▲	Call Privilege ▲	Quota ▲	Delete
alex	ENM	Enabled	Enabled	7001	Local	1 GB	<input type="radio"/>
allen	ENM	Enabled	Enabled	7000	Local	1 GB	<input type="radio"/>
james	ENM	Enabled	Enabled	7002	Local	1 GB	<input type="radio"/>

### USER LIST

This section lists all the available user information:

**Username:** Displays a user name.

**Department:** Displays the department which the specific user belongs to.

**Email:** Displays the email service status of the user.

**PPTP VPN:** Displays the PPTP VPN status of the user.

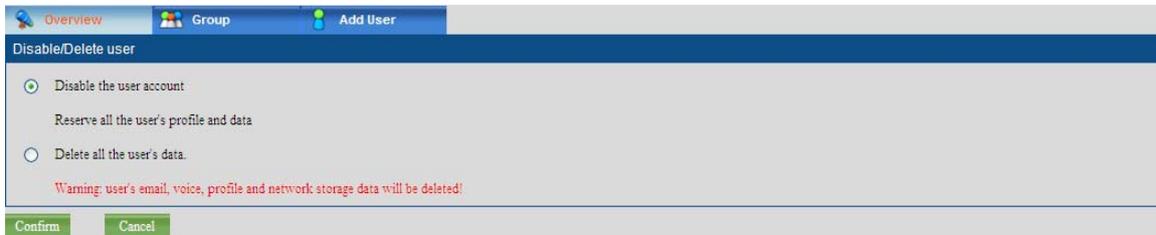
**Extension:** Displays the VoIP phone number of the specific user.

**Call Privilege:** Displays the call privilege of the specific user.

**Quota:** Displays the maximum quota of the specific user.

## 4.2 Deleting a User Account

Check the radio box and click the “delete” button. You can delete or disable the specific user account. Disabling the user account will freeze all user services without damaging the profile and data of the user. Deleting the user account will clear the entire data and profile of the user. If you want to freeze this account for a period of time, check the “Disable the user account” check box and confirm. If you want to delete the user, check the “Delete all the user’s data” check box and confirm.



Overview Group Add User

Disable/Delete user

Disable the user account  
Reserve all the user's profile and data

Delete all the user's data

Warning: user's email, voice, profile and network storage data will be deleted!

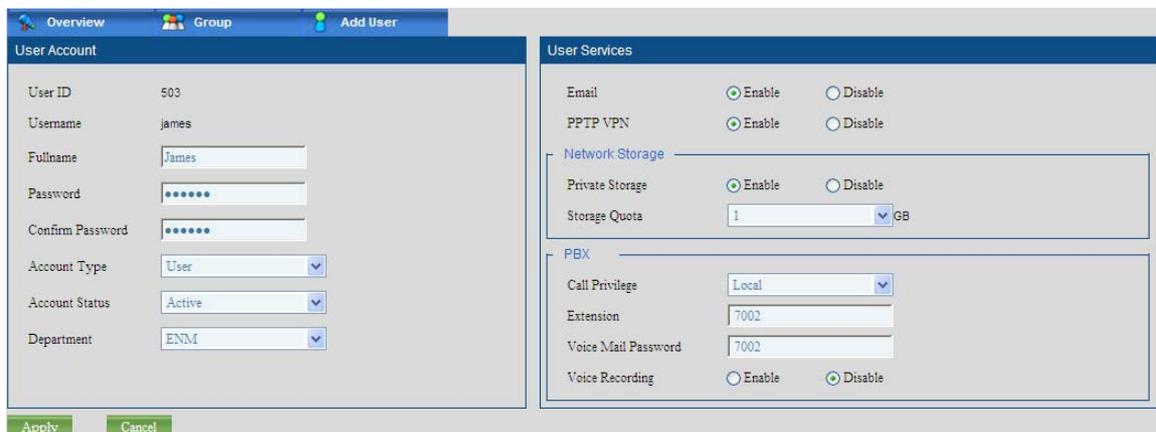
Confirm Cancel

### Note:

Delete all user account data, the user’s email, voice, private data and profile will be deleted. Please backup the data first.

## 4.3 Updating the User Setting

Click the username that you want to update in the “Overview” page, and the detailed user profile will appear. Change the user profile and then click the “Apply” button to update the user setting.



Overview Group Add User

User Account

User ID 503

Username james

Fullname James

Password

Confirm Password

Account Type User

Account Status Active

Department ENM

User Services

Email  Enable  Disable

PPTP VPN  Enable  Disable

Network Storage

Private Storage  Enable  Disable

Storage Quota 1 GB

PBX

Call Privilege Local

Extension 7002

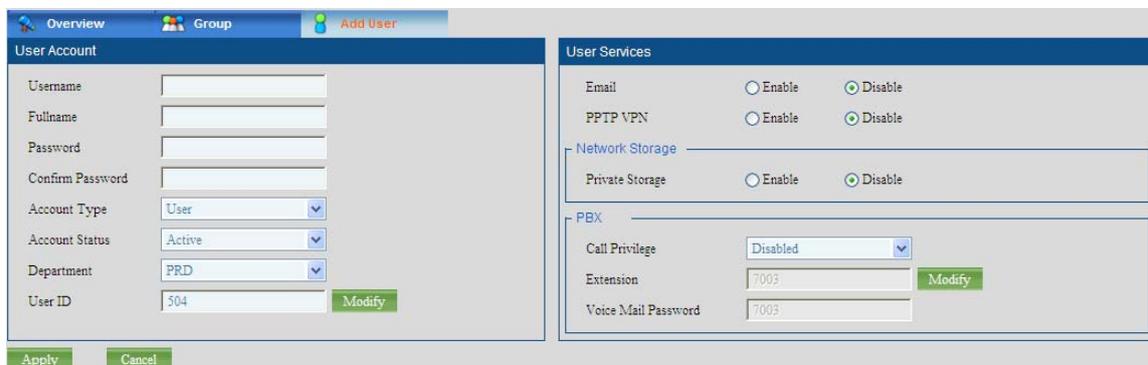
Voice Mail Password 7002

Voice Recording  Enable  Disable

Apply Cancel

## 4.4 Creating a User Account

To create a new user account, click the “User” tab in the “User” screen. This screen allows the administrator to create a new user profile with specified service privileges.



### USER ACCOUNT:

This section lists all the available settings of the user profile:

**User name:** Specifies a user name. All user related IT services will be created based on this name. It cannot be changed once set.

**Full Name:** Specifies the user’s full name.

**Password:** Specifies the user’s access password. This password will be applied to all the user related services, too.

**Confirm password:** Confirms and verifies the entered user password.

**Account Type:** Specifies either a common user or admin user privilege. The user with the admin privilege can access the GUI management pages to manage the UMG-2000 Series except the storage service.

**Account Status:** Indicates whether the user account is in an active or suspended state. Active: all user subscribed IT services can be optionally enabled. Suspended: all user subscribed IT services are disabled.

**Department:** Indicates a proper group or department for the user. You can create a new group or department by clicking the “Group” tab from the “User” screen.

**User ID:** Specifies a unique user identifier for the user. The default value is recommended.

### USER SERVICES:

This section lists all the available settings of the user services:

**Email:** Allows or denies user Email services.

**PPTP VPN:** Allows or denies a user’s VPN remote access privileges.

**Private Storage:** Allows or denies a user’s local storage access.

**Storage Quota:** Specifies the maximum user quota.

**IP PBX phone privilege:** Allows or denies a user’s VoIP phone access.

**Disable:** Denies a user’s VoIP phone access.

**Local:** Allows the user to dial a local external phone.

**National:** Allows the user to dial a national external phone.

**International:** Allows the user to dial an international external phone.

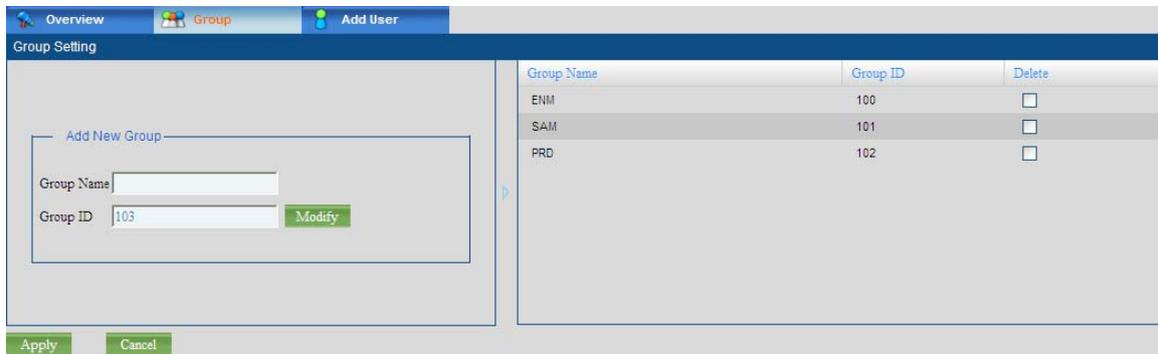
**Extension:** Specifies the VoIP phone number of the specific user which starts with the local dial prefix. It must be specified if the IP PBX phone privilege is not disabled and it cannot be changed once applied.

**Voice Mail Password:** Specifies the password that is used to access the voice mail. It must be specified if the IP PBX service is enabled.

## 4.5 Departments and Groups

---

You may assemble your defined users into different groups based on different criteria. To add a new group, click the “Group” tab. The “Group Settings” screen will then appear.



The screenshot shows the 'Group Setting' interface. On the left, there is a form titled 'Add New Group' with two input fields: 'Group Name' and 'Group ID' (containing '103'), and a 'Modify' button. On the right, there is a table with three columns: 'Group Name', 'Group ID', and 'Delete'. The table contains three rows: ENM (ID 100), SAM (ID 101), and PRD (ID 102). Each row has a checkbox in the 'Delete' column. At the bottom of the form, there are 'Apply' and 'Cancel' buttons.

Group Name	Group ID	Delete
ENM	100	<input type="checkbox"/>
SAM	101	<input type="checkbox"/>
PRD	102	<input type="checkbox"/>

### GROUP SETTING

This section lists all the available settings of the group:

**Group ID:** Specifies the group unique identifier. The default group ID is recommended.

**Group Name:** Specifies a name for the group i.e. sales, marketing, or operation.

### GROUP LIST

This section lists available group information:

**Group ID:** Displays the group ID.

**Group Name:** Displays the group name.

## 4.6 Deleting a Group

---

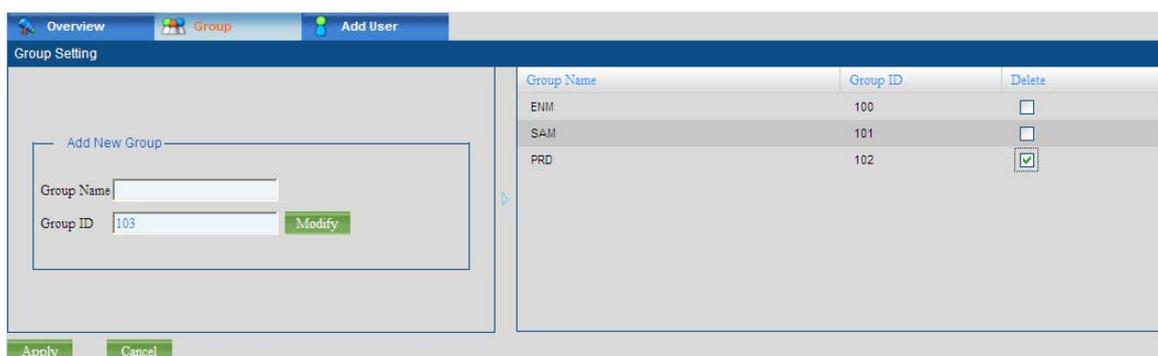
Check the check box “delete” and click the “Apply” button to delete a group.

---

### Note:

You must delete all the members within the group before you delete the group.

---



This screenshot is identical to the previous one, but the checkbox in the 'Delete' column for the 'PRD' group (ID 102) is now checked, indicating it is selected for deletion.

Group Name	Group ID	Delete
ENM	100	<input type="checkbox"/>
SAM	101	<input type="checkbox"/>
PRD	102	<input checked="" type="checkbox"/>

## 5. Web Management - Network

The UMG-2000 Series network management suite provides the administrator the ability to configure Internet service, Local Area Network services, FTP control services, NTP service and network storage security services.

### INTERNET Configuration

The UMG-2000 Series provides 10/100Mbps WAN ports as the internet interface and supports static IP, DHCP, PPTP and PPPoE as the ISP type. Internet management provides the ability for the administrator to manage the configuration of the Internet interface. The UMG-2000 Series can also work as the gateway which connects the Internet and the LAN and determines where to direct the package of data that arrive at the UMG-2000 Series.

### LAN Configuration

A Local Area Network (LAN) is a high-speed communications system designed to link computers and other data processing devices to share vital computing resources, such as printers, files etc. The UMG-2000 Series provides 24x4 10/100 Mbps and 2x10/100/1000 Mbps ports for LAN switching. The UMG-2000 Series also provides the Spanning Tree Protocol (STP) to prevent undesirable loops in the network.

### NETWORK SERVICES Configuration

The UMG-2000 Series provides many network services, including FTP, DNS, SAMBA, NTP, DHCP etc. Network services management allows for the ability to manage the configuration of these services.

## 5.1 Overview

The administrator can get the overview of the network settings and the status of the network services.

Internet Setting		Local Network Setting	
ISP Type	Static	Connected Users	Loading...
IP Address	210.66.155.75	Local Server Address	192.168.1.1
Subnet Mask Address	255.255.255.224	Subnet Mask Address	255.255.255.0
Default Gateway Address	210.66.155.94	DHCP Server	Enabled
Primary DNS Address	168.95.1.1	DHCP Range Start Address	192.168.1.10
Secondary DNS Address	168.95.192.1	DHCP Range End Address	192.168.1.250
Internet Link Speed	Loading...	Local Network Link Speed	Loading...

Internet Service		Local Network Service	
Internet Domain Name	yang92.cn	Network Storage	Enabled
DNS Server	Enabled	PPTP VPN Server	Enabled
Domain/Workgroup	workgroup	NTP Server	Enabled

## **INTERNET SETTING:**

This section lists the current settings of the Internet:

**ISP Type:** Displays the ISP type.

**IP Address:** Displays the IP address of the WAN port of UMG-2000 Series.

**Subnet Mask Address:** Displays the subnet mask address.

**Default Gateway Address:** Displays the IP address of the default gateway.

**Primary DNS Address:** Displays the primary DNS address.

**Secondary DNS Address:** Displays the secondary DNS address.

**Internet Link Speed:** Displays the maximum speed of the Internet link.

## **LOCAL NETWORK SETTING**

This section lists all the current settings of LAN:

**Connected Users:** Displays the number of users that have been connected to the UMG-2000 Series.

**Local Server Address:** Displays the LAN IP address of the UMG-2000 Series.

**Subnet Mask Address:** Displays the LAN subnet mask address.

**DHCP Server:** Displays the state of the DHCP server, enabled or disabled.

**DHCP Range Start Address:** Displays the start address of the DHCP IP range.

**DHCP Range End Address:** Displays the end address of the DHCP IP range.

**Local Network Link Speed:** Displays the maximum speed of the LAN link.

## **INTERNET SERVICES**

This section lists the service state of the WAN services:

**Internet Domain Name:** Displays the Internet domain name.

**DNS Server:** Displays the state of the DNS service, enabled or disabled.

**Email Server:** Displays the state of the email service, enabled, or disabled.

**PPTP VPN Server:** Displays the state of the PPTP VPN server, enabled or disabled.

**Network Storage:** Displays the state of the network storage service (SAMBA), enabled or disabled.

## **LOCAL NETWORK SERVICES**

This section lists the service state of the LAN services:

**Domain Controller:** Displays whether the UMG-2000 Series is the domain controller.

**Domain Work Group:** Displays the Windows workgroup that UMG-2000 Series belongs to.

**NTP Server:** Displays the state of the NTP server, enabled or disabled.

## 5.2 Internet

The “Internet” screen allows the administrator to change the Internet settings.

The screenshot shows the 'Internet Setting' configuration page. At the top, there are navigation tabs: Overview, Internet (selected), Local Network, Service, and VPN Log. The main content area is titled 'Internet Setting' and contains the following fields:

- ISP Type: Static (dropdown menu) with a Detect button.
- IP Address: 210, 66, 155, 75
- Subnet Mask Address: 255, 255, 255, 224
- Default Gateway Address: 210, 66, 155, 94
- DNS Server Address: 168, 95, 1, 1 (radio button selected)
- MAC Address: 168, 95, 192, 1

At the bottom, there are 'Apply' and 'Cancel' buttons.

## 5.3 Local Network

The “Local Network” screen allows the administrator to change the Internet settings.

The screenshot shows the 'Local Network Setting' configuration page. At the top, there are navigation tabs: Overview, Internet, Local Network (selected), Service, and VPN Log. The main content area is titled 'Local Network Setting' and contains the following fields:

- Local Server Address: 192, 168, 1, 1
- Subnet Mask Address: 255, 255, 255, 0
- Local DHCP Server: Enable (radio button selected), Disable
- DHCP Range Start Address: 192, 168, 1, 10
- DHCP Range End Address: 192, 168, 1, 250

Below the settings is a table titled 'Attached Device' with 1/1 devices listed:

IP	MAC	Hostname
00:11:D8:19:09:49	192.168.1.250	unknown

At the bottom, there are 'Apply' and 'Cancel' buttons.

### LOCAL NETWORK SETTING

This section lists all the available settings of the LAN:

**Local Server Address:** Specifies the LAN IP address of the UMG-2000 Series

**Subnet Mask Address:** Specifies the LAN subnet mask address.

**DHCP Server:** Specifies the state of the DHCP server, enabled or disabled.

**DHCP Range Start Address:** Specifies the start address of the DHCP IP range.

**DHCP Range End Address:** Specifies the end address of the DHCP IP range.

## 5.4 Service

The “Service” screen allows the administrator to change the setting of the network services.

The screenshot shows the 'Service' configuration page with the following settings:

- Network Service:**
  - Domain/Workgroup:
  - Network Storage:  Enable  Disable
  - PPTP VPN Server:  Enable  Disable
  - NTP Server:  Enable  Disable
  - RIP:  Enable  Disable
- Dynamic DNS Service:**
  - DDNS(DynDns):  Enable  Disable
  - Domain Name:
  - MX Record:  (Your email server FQDN)
  - Username:
  - Password:
- Multi-Domain Setting:**
  - Primary Domain Name:
  - Secondary Domain Name:
  - Third Domain Name:
  - Fourth Domain Name:
  - Fifth Domain Name:

Buttons:

### INTERNET SERVICES

This section lists all the available settings of the WAN services:

- Domain Work Group:** Specifies the UMG-2000 Series Windows workgroup.
- Network Storage:** Enables or disables the network storage server (SAMBA) service.
- PPTP VPN Server:** Enables or disables the PPTP VPN service.
- NTP Server:** Enables or disables the NTP service.

### DYNAMIC DNS SERVICES

This section lists all the available settings of the LAN services:

- Internet Domain Name:** Specifies the Internet domain name.

## 5.5 The VPN Log

The “VPN Log” screen allows the administrator to trace the VPN logging history. The administrator can also search by using the login ID to find the user’s VPN history.

Date	Time	Source IP	Assign IP	Login ID	Event
06/04/2009	08:05:23	210.66.155.73	10.8.1.3	james	Login

Search by login ID

### VPN Log

This section lists the VPN logging history:

- Date:** Displays the date of the log.
- Time:** Displays the time of the log.
- Source IP:** Displays the client WAN IP
- Assign IP:** Displays the IP address that the server has assigned to the client.
- Login:** Displays the effective login ID of the client.
- Event:** Displays the detail description of the Log.

## 6. Web Management - Wireless

The UMG-2000 Series wireless suite integrates the following services: standard access point (AP), multiple layers of wireless security and client blocking.

### STANDARD WIRELESS ACCESS POINT

The UMG-2000 Series supports three task groups in 802.11 standard working groups: 802.11b/g/n. 802.11b supports data rates up to 11 Mbps, 802.11g supports data rates of at least 20 Mbps and 802.11n supports up to 300Mbps / 2T2R.

### ENCRYPTION and Security

A wireless client will connect and join the network if no encryption is enabled. However, the encryption greatly enhances the security of the connection and data transmission between the access point and the wireless client. This includes the IEEE 802.1x port-based authentication protocol, Wireless Protected Access (WPA), Wireless Protected Access –version 2 (WPA2,) Wireless Encryption Protocol (WEP). If WEP is chosen as the encrypt method, each packet is composed of the 24 bits Initialization vector and 40/104 bits encryption. Therefore, WEP encrypt length will be 64bits or 128 bits. WEP uses the RC4 stream encryption (a fresh key stream for each package). WEP, with minimal flaws, is enough to prevent most hacking. At the same time, WEP will cause often a 20-50% reduction of the wireless speed. WPA is an interim solution until the 802.11i comes out. It also uses the RC4 with the key changed to TKIP. TKIP works by generating a sequence of WEP keys based on a master key and re-keying periodically.

### CLIENT BLOCKING

The wireless is the opening network system for the wireless clients and any authenticated clients can access the Wireless LAN (WLAN). However, the wireless AP can monitor the status of the connected clients and set access limitation to the clients. To temporarily block client access, the administrator can add the client MAC to the block list. The client cannot connect to the AP unless the administrator releases the blocking.

## 6.1 Overview

The wireless “Overview” screen presents the current wireless services status summary. The administrator can quickly view important details of your wireless Access Point services (AP) status.



Wireless Network	
Access Point(AP) .....	Enabled
Hide SSID .....	Disabled
Network Name(SSID) .....	UMG_WIFI
Wireless Mode .....	802.11b/g
Wireless Region .....	USA
Channel .....	6
Authentication Type .....	Open System
Link Speed .....	11/54 Mbps
Data Encryption .....	None

## WIRELESS NETWORK

This section lists all the current settings of the wireless Access Point (AP).

**Access Point:** Displays the wireless AP service state, enabled or disabled.

**Hide SSID:** Displays the visibility of the wireless AP SSID.

**Network Name (SSID):** Displays the SSID of this wireless network.

**Wireless Mode:** Displays the wireless AP supporting mode.

**Wireless Region:** Displays the region that the wireless AP belongs to.

**Channel:** Displays the current channel configuration mode: auto or channel number

**Authentication type:** Displays the current wireless AP security access type.

**Link speed:** Displays the wireless AP link speed.

**Data Encryption Type:** Displays the type of data encryption.

**Encrypt Strength:** Displays the encrypt strength if WEP is the data encryption type.

**Security Key:** Displays the key for the clients to access this AP if WEP is the data encryption type.

## 6.2 Wireless Setting

The wireless “Setting” screen enables the administrator to manage the wireless AP.

The image shows two screenshots of a network configuration interface. The top screenshot is titled "Wireless Network Settings" and contains the following fields: "Access Point (AP)" with radio buttons for "Enable" (selected) and "Disable"; "Hide SSID" with radio buttons for "Enable" and "Disable" (selected); "Network Name (SSID)" with a text input field containing "UMG-2200"; "Wireless Region" with a dropdown menu set to "Asia"; "Channel" with a dropdown menu set to "1"; "Wireless Mode" with a dropdown menu set to "802.11b/g"; "Authentication Type" with a dropdown menu set to "Open System"; and "Data Encryption" with a dropdown menu set to "None". The bottom screenshot is titled "Wireless 802.1X Settings" and contains: "Authentication" with radio buttons for "Enable" and "Disable" (selected); "Username" with an empty text input field; and "Password" with an empty text input field. At the bottom of the interface are "Apply" and "Cancel" buttons.

## WIRELESS NETWORK

This section lists all the available settings to the wireless Access Point (AP). Service is only accessible when enabled. SSID is visible and can be scanned only when “Hide SSID” is disabled.

**Access Point:** Enables or disables the wireless AP service.

**Hide SSID:** Specifies whether the wireless AP SSID is visible or not.

**Network Name (SSID):** An SSID is the name of a wireless local area network (WLAN). Specifies the preferred SSID name string.

**Wireless Region:** Specifies the region that the wireless AP belongs to. The region will affect the channels and the working frequency of your AP.

**Wireless Mode:** Specifies the preferred wireless AP mode.

**Channel:** Specifies a preferred wireless channel number or an auto channel.

**Authentication Type:** Specifies the authentication type.

**Data Encryption:** Specifies the type of Data Encrypt.

**Encrypt Strength:** Specifies the encrypt strength if WEP is the data encryption type.

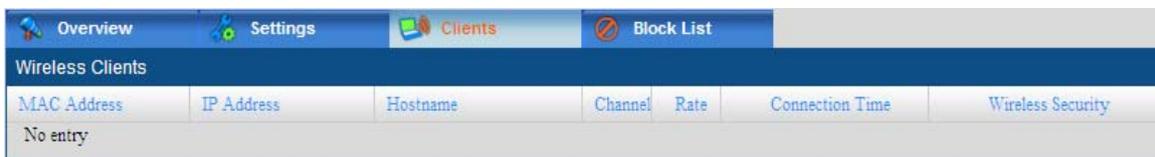
**Security Key:** Specifies the key for the clients to access this AP if WEP is the data encryption type.

**Note:**

You cannot detect the AP if “Hide SSID” is enabled.

### 6.3 Wireless Clients

The wireless “Clients” screen shows the wireless clients current connection to the UMG-2000 Series wireless Access Point (AP). Each connected wireless clients information is listed in a tabulated form. The following are the wireless client connection information.



MAC Address	IP Address	Hostname	Channel	Rate	Connection Time	Wireless Security
No entry						

#### WIRELESS CLIENT

This section lists the current information on the connected wireless clients.

**MAC Client:** Displays the MAC Address of the wireless client.

**IP Address:** Displays the IP Address of the wireless client.

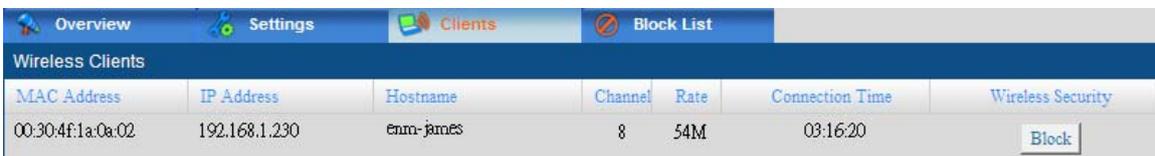
**Hostname:** Displays the host name of the wireless client.

**Channel:** Displays the connected channel number.

**Rate:** Displays the data transfer rate.

### 6.4 Blocking the Connected Wireless Client

The administrator can block any connected wireless client by clicking the “block” button. The selected wireless client will be blocked and access will be denied.

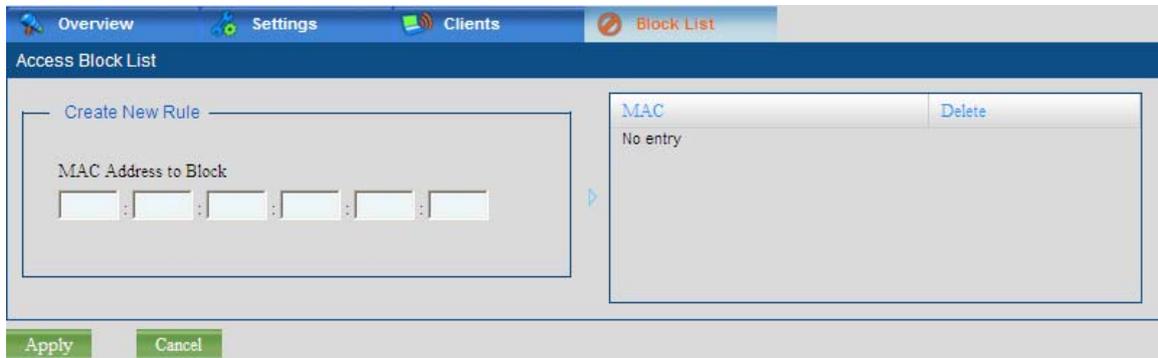


MAC Address	IP Address	Hostname	Channel	Rate	Connection Time	Wireless Security
00:30:4f:1a:0a:02	192.168.1.230	emm-james	8	54M	03:16:20	Block

## 6.5 Wireless MAC Block List

---

The wireless “Block List” screen displays the current block list. The administrator can unblock any or all of the computers currently prohibited to access the shared resources through the wireless AP.



### CREATE NEW RULE

This section lists the settings to block a wireless client to access the wireless AP.

**MAC Address to Block:** Specifies the MAC address to block.

### ACCESS BLOCK LIST

This section lists all the currently blocked wireless clients to the wireless AP.

**MAC:** Displays the MAC address in the block list.

### ADD TO THE BLOCK LIST

The administrator can add a new MAC address to the block list by filling in the client MAC address and clicking the “Apply” button. The client with the newly added MAC address cannot access this AP any more.

### REMOVE FROM THE BLOCK LIST

The administrator can remove a selected MAC address from the block list by checking the corresponding checkbox and clicking the “Apply” button. The unblocked client with the MAC address can then access the wireless AP again.

## 7. Web Management - Storage

The UMG-2000 Series storage suite includes the following services: Redundant Array of Independent Disks (RAID), Network Storage Server, backup/restore, and remote data synchronizing.

### RAID AND JBOD

The UMG-2000 Series supports RAID on storage devices. A RAID device is a logical device that has physical devices underlying it. These physical devices are disk partitions. The supported RAID levels are:

**Level 0:**

**Provides data striping, or the spreading out of blocks of each file across multiple disk drives but without redundancy. This improves performance but does not deliver fault tolerance. If one drive fails then all data in the array is lost.**

**Level 0+1:**

**RAID 0+1 is a mirrored configuration of two striped sets. This is a technique in which data is written to two duplicate disks simultaneously, providing data redundancy.**

**Level 5:**

**Provides data striping and utilizes one disk for backup information, which enables it to restore any other disk in the array.**

On top of the RAID, the UMG-2000 Series supports Logical Volume Management (LVM2) that provides a higher-level view of the disk storage on a computer system than the traditional view of disks and partitions. This gives the system administrator much more flexibility in allocating storage to applications and users. Storage volumes created under the control of the LVM can be resized and relocated. The LVM also allows management of storage volumes in user defined groups, allowing the system administrator to deal with sensibly named volume groups.

Another choice other than RAID is the technology of “Just a Bunch Of Disks” (JBOD). The RAID system stores the same data redundantly on multiple disks that nevertheless appear to the operating system as a single disk. Although, JBOD also makes the disks appear to be a single one, it accomplishes that by combining the drives into one larger logical disk. JBOD doesn’t deliver any advantages over using separate disks independently and doesn’t provide any of the fault tolerance or performance benefits of RAID.

### NETWORK STORAGE SERVER

The UMG-2000 Series supports Server Message Block (SMB), also known as Common Internet File System (CIFS) to share files on the private network which can be used for WINDOWS, Linux/Unix and other operating systems and Network File System (NFS) clients/servers.

### BACKUP AND RESTORE

The UMG-2000 Series will automatically backup storage according to the scheduled time. The administrator can also backup the current storage manually. The UMG-2000 Series supports two solutions for backup. One is snapshot and the other is full data copy. Snapshot is an effectual and space-saving method. It is a picture in time of how the data

was organized rather than a copy of the data. It provides a consistent view of the device, but it can build a snapshot of the device on and only on the local UMG-2000 Series. Another way is building a full data copy. It is a safer method to build all your data into a ZIP file; however, it takes much more storage space because of redundancy. Backup to the remote SAMBA or NFS server is supported and it is a good choice if you already have a storage server. It is strongly recommended to enable the feature of auto backup because the administrator can restore the data to a previous backup when data corruption occurs.

## REMOTE DATA SYNCHRONIZATION

Please refer to Section - Remote Data Synchronization.

## 7.1 Storage Overview

The Storage “Overview” screen presents the current network storage services status summary. The system administrator can quickly view important details of the network storage condition and services.

The screenshot shows the 'Overview' page of a storage management interface. It is divided into three main sections: Network Storage Status, Disk Status, and Volume List.

**Network Storage Status:**

- Service Status: Normal
- Disk Array: JBOD
- Array Status: Operational
- Total Capacity: 275G
- Total Free Capacity: 248G
- NFS Server: Down

**Disk Status:**

- Disk1: Operational
- Disk2: Operational
- Disk3: N/A
- Disk4: N/A

**Volume List:**

Name	Capacity	Free Capacity	Auto Backup	Auto Snapshot	Mount Type	Status	Delete
system_log	1G	925M	No	No	cifs	Ready	
umg_mirror	N/A	N/A	No	No	cifs	reserved	
home	5G	4.6G	Yes	Yes	cifs	Ready	
email	5G	4.6G	No	No	cifs	Ready	
ptbx	5G	4.6G	No	No	cifs	Ready	<input type="radio"/>
ftp	5G	4.6G	No	No	cifs	Ready	<input type="radio"/>
web	1G	925M	No	No	cifs	Ready	<input type="radio"/>

At the bottom left of the interface is a 'Refresh' button.

## NETWORK STORAGE STATUS

This section lists the current status of the storage.

**Service Status:** Displays the current RAID state of operation: active, rebuilding, sync, or removed. Once the RAID is in “removed” state, check the disk status to determine which disk is fault. Please refer to Appendix A - FAST RECOVERY.

**DISK Array:** Displays the current storage RAID level: RAID 0, RAID 0+1, or RAID 5.

**Array Status:** Displays the status of the 4 disks, good or bad.

**Total Capacity:** Displays the total storage size in Gigabyte.

**Total Free Capacity:** Displays the available storage size in Gigabyte.

**NFS Server:** Displays the status of the NFS service, up or down.

## DISK STATUS

This section lists the current status of the four disks, good or bad. If any disk is in bad state,

please replace the faulty one as soon as possible to avoid the loss of data.

- Disk1: Displays the status of the first disk,**
- Disk2: Displays the status of the second disk.**
- Disk3: Displays the status of the third disk.**
- Disk4: Displays the status of the fourth disk.**

## VOLUME LIST

This section lists all the existing volumes with the brief information of their configuration and status.

- Name: Displays the volume name.**
- Capacity: Displays the specific volume capacity in Gigabyte.**
- Free Capacity: Displays the available size of the specific volume in Gigabyte.**
- Auto Backup: Displays the auto backup status of the specific volume, Yes or No.**
- Auto Snapshot: Displays the auto snapshot status of the specific volume, Yes or No.**
- Mount Type: Displays the file system that can be used in NAS of the specific volume.**

## 7.2 View a Volume by SMB

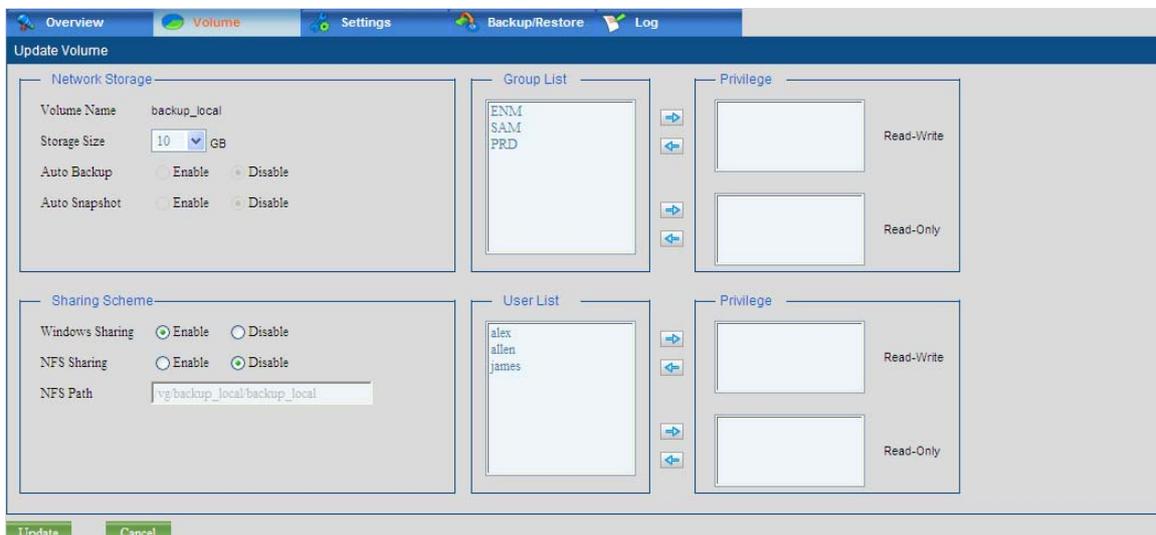
Check the radio box “view” of the specific volume or browse to <file://ip/dir> (where “ip” stands for the LAN IP address of UMG-2000 Series and “dir” stands for the volume you want to access) to view the volume by the SAMBA.

### Note:

It is recommended to add a user with the same name and password of the PC Window account to access the Network Shared Storage.

## 7.3 Updating a Volume

Click the volume name that you want to update, and you can get the detailed information. Change the setting and click the “update” button to update the volume.



## NETWORK STORAGE

Refer to Section - Creating a Storage Volume.

### 7.4 Deleting a Volume

Select the radio button “delete” then click the “Delete” button to delete a volume.

The screenshot shows the 'Volume' tab in the management console. It displays the 'Network Storage Status' and a 'Volume List' table.

Name	Capacity	Free Capacity	Auto Backup	Auto Snapshot	Mount Type	Status	Delete
home	20G	19G	Yes	Yes	cifs	Ready	
system_log	10G	9.3G	No	No	cifs	Ready	
umg_mirror	N/A	N/A	No	No	cifs	reserved	
ptx	10G	9.3G	No	No	cifs	Ready	
email	10G	9.3G	No	No	cifs	Ready	
ftp	3G	2.8G	No	No	cifs	Ready	
backup_local	10G	9.3G	No	No	cifs	Ready	<input type="radio"/>

#### Note:

All data in this volume will be deleted if the volume is deleted.

### 7.5 Creating a Storage Volume

The Storage “Volume” screen allows the administrator to create a network shared storage volume.

The screenshot shows the 'Create Volume' configuration screen. It is divided into several sections for configuring network storage, sharing schemes, and user/group permissions.

- Network Storage:** Includes fields for Volume Name, Storage Size (0 GB), and radio buttons for Auto Backup and Auto Snapshot (both set to Disable).
- Sharing Scheme:** Includes radio buttons for Windows Sharing (Enable) and NFS Sharing (Disable).
- Group List:** A list of groups (ENM, SAM, PRD) with arrows to assign Read-Write or Read-Only privileges.
- User List:** A list of users (alex, allen, james) with arrows to assign Read-Write or Read-Only privileges.

## **NETWORK STORAGE**

This section lists all the available settings for network storage. The system will backup the volume automatically only if “Auto Backup” or “Auto Snapshot” is enabled.

**Volume Name:** Specifies the preferred Volume name.

**Storage Size:** Specifies the capacity of this volume.

**Auto Backup:** Allows or denies this volume to backup automatically.

**Auto Snapshot:** Allows or denies this volume to build the snapshot automatically.

## **SHARING SCHEME**

This section lists all the available sharing schemes.

**Windows Sharing:** Specifies whether to share this volume to Windows clients by SAMBA (CIFS).

**NFS Sharing:** Allows or denies this volume to be shared as a Network File System. It is mainly used among UNIX/LINUX operation system..

## **USER GROUP**

The user group displays all groups that can be set to access the volume. All the users in the group can also access the volume.

## **PRIVILEGE**

**Privilege:** Read-Write/Read Only.

**[Right] button:** Selects a group in the User Group drop down menu and click the [right] button to set a privilege to the group. All users in the group will have the same privilege.

**[Left] button:** Selects a group name in the Privilege drop down menu and click the [left] button to withdraw a privilege from the group. All users' privileges will then be called back.

## **USER LIST**

The user list displays all users that can be set to access the volume. Only the user specified or in the specified group can access this volume via network.

**Privilege:** Read-Write/Read Only.

**[Right] button:** Selects a group in the User Group drop down menu and click the [right] button to set a privilege to the group.

**[Left] button:** Selects a user name in the Privilege drop down menu and click the [left] button to withdraw a privilege from the user.

## 7.6 Storage Setting

The Storage “Setting” screen enables the administrator to manage the storage backup policy.

The screenshot displays the 'Settings' tab of a storage management interface. It is divided into three main sections:

- Snapshot Schedule:** Features a 'Daily Snapshot' section with radio buttons for 'Enable' and 'Disable' (currently 'Disable' is selected). Below it is a 'Time' dropdown menu set to '8:00'.
- Backup Schedule:** Features a 'Weekly Full Backup' section with radio buttons for 'Enable' and 'Disable' (currently 'Enable' is selected). Below this are three fields: 'Weekday' (dropdown set to 'Friday'), 'Time' (dropdown set to '20:00'), and 'Keep Copies' (dropdown set to '3'). Below these is a 'Daily Incremental Backup' section with radio buttons for 'Enable' and 'Disable' (currently 'Enable' is selected) and a 'Time' dropdown set to '20:00'.
- Backup Volume Path Setting:** Features radio buttons for 'Local' and 'NFS'. The 'NFS' option is selected. Below are two text input fields: 'Remote Host IP' (containing '192.168.1.2') and 'Exported Path' (containing '/mnt/backupvolume/').

At the bottom of the form are two buttons: 'Apply' and 'Cancel'.

### SNAPSHOT SCHEDULE

This section lists all the available settings of the daily snapshot policy.

**Daily Snapshot:** Specifies whether to allow the system to create a storage snapshot automatically or manually.

**Time:** Specifies the time to create the snapshot automatically.

### BACKUP SCHEDULE

This section lists all the available settings of the backup policy.

**Weekly full backup:** Specifies whether to allow the system to create weekly full backup automatically or manually.

**Weekday:** Specifies the day to create the full backup files automatically.

**Time:** Specifies the specific time to create the full backup files.

**Keep Copies:** Specifies the maximum number of the full backup copies.

**Daily Incremental backup:** Specifies whether to allow the system to create daily incremental backup automatically or not.

**Time:** Specifies the specific time to create the incremental backup files.

### VOLUME BACKUP PATH SETTING

This section lists all the available settings of the backup policy.

**Local:** Backs up volumes to local storage.

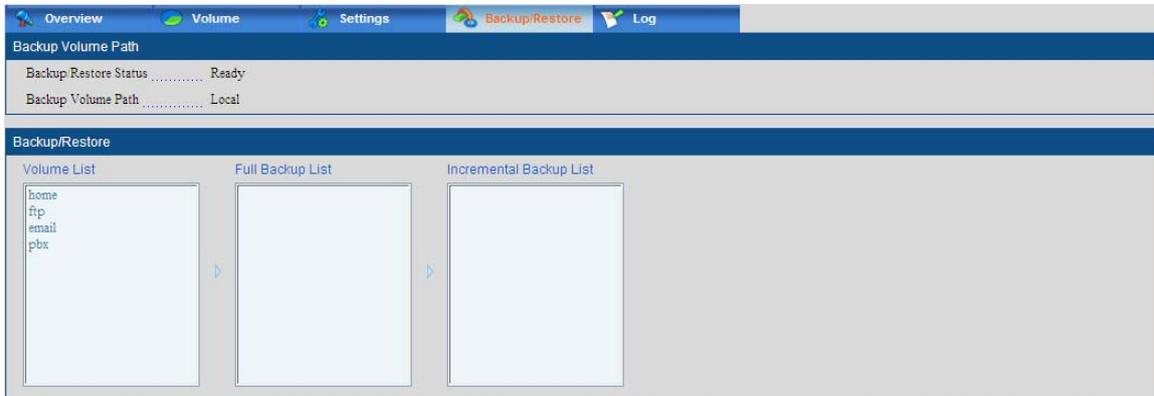
**NFS:** Backs up volumes to the specified NFS server.

**Host:** Specifies the NFS server host.

**Path:** Specifies the available path of the NFS server.

## 7.7 Storage Backup and Restore

The Storage “Backup” screen allows the administrator to backup a volume manually, view an existing backup, delete an existing backup, and restore a volume to an existing backup.



### BACKUP/RESTORE

This section lists all the volumes and the available backup.

**Volume List:** Displays all the existing volumes in the UMG-2000 Series.

**Backup List:** Displays the date of the available backup point of a volume which is in the format of MM/DD/YYYY HH:MM:SS

**Backup:** Specifies a volume in the volume list and backs up the volume manually.

**Restore:** Specifies a backup file in the backup list and clicks the button to restore the selected volume to the specific backup file.

**Delete:** Deletes a backup file manually.

### BACKUP VOLUME PATH

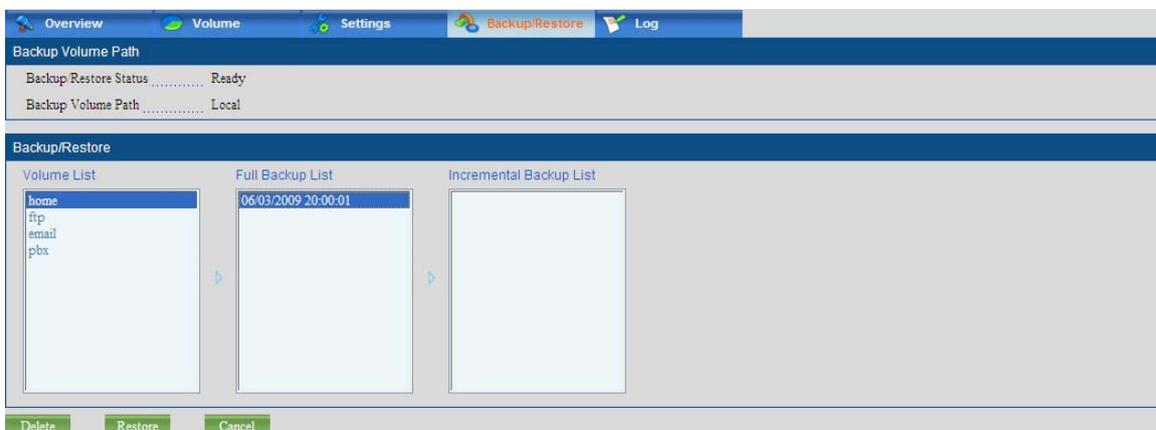
This section lists settings of the backup path.

**Back/Restore Status:** Displays the backup/restore operation status.

**Backup Volume Path:** Displays all the volumes' backup path.

### BACKUP A VOLUME

Select a volume and then click the “backup” button to backup the volume.



## Delete and restore Backup files

Select a backup file of a volume in the full backup list and then click the “Restore” button to restore the volume to the file. Click the “Delete” button to delete the backup files.

---

### Note:

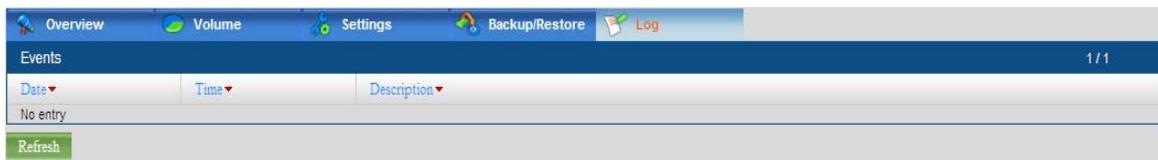
It is strongly recommended that the administrator to perform manually backs up to the current volume, and then restores the volume.

---

## 7.8 The Storage Log

---

The storage log shows the network storage history.



### EVENTS

**Date:** Displays the date of the event.

**Time:** Displays the time of the event.

**Description:** Display the detailed description of the event.

## 8. Web Management - PBX

The UMG-2000 Series's Private Branch Exchange (PBX) solution provides a private telephone switching system that allows the telephone extensions to connect internally and domestically, as well as externally and internationally. In most cases, a PBX is an independent piece of equipment residing in an enterprise and is responsible for switching calls between enterprise users. It allows these end users to place calls using a network instead of the standard telephone infrastructure. The UMG-2000 Series supports the PBX, enabling users to share a specific number of external phone lines, saving the added cost of having an external phone line for each user. The UMG-2000 Series's PBX allows end users to place calls using a network instead of the standard telephone infrastructure. UMG-2000 Series's PBX manages both the Plain Old Telephone Service (POTS) and Voice over IP (VoIP) devices, utilizing VoIP accounts to connect them to telephone proxies. Devices within the UMG-2000 Series's PBX allow users to freely communicate with each other, thus creating a cost-effective telephone environment.

### 8.1 IP PBX Overview

The UMG-2000 Series IP PBX overview displays the current IP PBX services status.

Extension	Username	R/W Privilege	Calling State	Registration State	IP Address	Voice Recording
1000	jonas	Operator	Free	Unregistered	N/A	Enabled
1001	brian	International	Free	Unregistered	N/A	Enabled
1002	evan	National	Free	Unregistered	N/A	Enabled
1003	jasper	Local	Free	Unregistered	N/A	Enabled

#### CALL FEATURE

This section indicates the status of the following PBX features.

**VoIP Service:** Displays the state of the IP PBX service, enabled or disabled.

**Call Forwarding:** Displays the state of the feature “Call Forwarding”, enabled or disabled.

**Call Pickup:** Displays the state of the feature “Call Pickup”, enabled or disabled.

**Call Parking:** Displays the state of the feature “Call Parking”, enabled or disabled.

**Do Not Disturb:** Displays the state of the feature “Do Not Disturb”, enabled or disabled.

**LCR:** Display the state of the feature “LCR”, enabled or disabled.

**Fax to Email Address:** Displays the fax receiver’s email address

**Conference Call:** Displays the state of the feature “Conference Call”, enabled or disabled.

**Voice Recording:** Displays the state of the feature “Record Voice”, enabled or disabled.

**BLF Support:** Display the state of the feature “BLF”, enabled or disabled.

**Video Calling:** Display the state of the feature “Video Calling”, enabled or disabled.

**Stun Server:** Display the state of the feature “Stun Server”, enabled or disabled.

**Password Protect Outside Call:** Display the state of the feature, enabled or disabled.

**PBX Call Prefix:** Displays the call prefix.

## **EXTENSION LIST**

This section lists all the extensions with the owner’s information in the UMG-2000 Series.

**Extension:** Displays an extension number.

**Username:** Displays the full name of the specific extension.

**R/W Privilege:** Display the state of the specific extension.

**Calling State:** Displays the call state of the specific extension, free or busy.

**Registration State:** Displays the status of the phone with the specific extension, registered or unregistered.

**IP Address:** Displays the current IP Address of the phone with the specific extension.

**Voice Recording:** Displays if open the voice recording feature with the specific extension.

## 8.2 IP PBX Call Setting

Click the “Setting” tab in the “VoIP” screen. The VoIP “Setting” screen appears, allowing the administrator to manage the IP PBX services and features. The IP PBX service and call features can be globally or individually enabled or disabled.

The screenshot shows the 'Call Setting' tab in a VoIP management interface. The 'Call Features' section contains two columns of settings. The first column includes: PBX Service (radio buttons for Enable/Disable), Call Forwarding (radio buttons for Enable/Disable), Call Pickup (radio buttons for Enable/Disable), Call Parking (radio buttons for Enable/Disable), Do Not Disturb (radio buttons for Enable/Disable), LCR (radio buttons for Enable/Disable), and Stun Server (radio buttons for Enable/Disable). The second column includes: Conference Recording (radio buttons for Enable/Disable), Voice Recording (radio buttons for Enable/Disable), BLF Support (radio buttons for Enable/Disable), Video Calling (radio buttons for Enable/Disable), Password Protect Outside Call (radio buttons for Enable/Disable), PBX Call Prefix (dropdown menu with '1XXX'), and Extension Digits (dropdown menu with '4'). Below this is the 'Audio Quality Tuning Options' section with 'Receive Gain' set to 5 db and 'Transmit Gain' set to 3 db. The 'Codec' section shows 'Audio Codec' with checked boxes for G.711 u-law, G.711 A-law, and G.726 RFC3551, and 'Video Codec' with checked boxes for H.264 Video, H.263+ Video, H.263 Video, and H.261 Video. The 'Fax Server' section has a 'Fax To Email Address' field. The 'Group Pickup' section has three lists: 'User List' (jonas, brian, evan, jasper), 'Group Pickup List' (empty), and 'Group List' (ENM). At the bottom are 'Apply' and 'Cancel' buttons.

### CALL FEATURE SETTING

This section lists all the available setting of IP PBX. The IP PBX service is accessible only when the VoIP service is enabled.

**PBX Service:** Enables or disables the IP PBX service

**Call Forwarding:** Enables or disables the feature “Call Forwarding”. Enabling this feature will allow the user in the UMG-2000 Series to forward the incoming calls to another telephone. The call forwarding extension number can only be set by the individual user in the personal account web administration.(Refer to Section - Personal Account Web Administration )

**Call Pickup:** Enables or disables the feature “Call Pickup”. Enabling this feature will allow answering an incoming call to the specific extension from another phone within the same call pick up group.

**Call Parking:** Enables or disables the feature “Call Parking”. Enabling this feature will allow parking an incoming call and pick up it at another location.

**Do Not Disturb:** Enables or disables the feature “Do Not Disturb”. Enabling this feature will prevent ringing of the incoming call.

**LCR:** When enable this option, the LCR function just could be used.

**Stun Server:** This function can help the IP PBX could working properly behind NAT. To change these settings please following your ISP information.

**Conference Record:** Enables or disable the feature “Conference Record”.  
Enabling this feature will allow record conference.

**Voice Recording:** Enables or disables the feature “Record Voice”.

**BLF Support:** If the subscriber device (IP Phone ) also support the BLF function, the subscriber could monitor the current usage status for other subscribers.

**Video Calling:** The subscriber could use Video Phone to achieve the video communication.

**Password Protect Outside Call:** When the subscriber want to make external PSTN call, the subscriber will be prompted to input the password if enable this option.

**PBX Call Prefix:** Specifies the call prefix. All the extensions in the group will be prefixed with the number.

**Extension Digits:** It could define the extension number length.

## **AUDIO QUALITY TUNING OPTIONS**

This section lists all the tunings of audio quality.

**Receive Gain:** Specifies the receive gain.

**Transmit Gain:** Specifies the transmit gain.

## **Codec**

This section set the audio and ideo codec types.

**Audio Codec:** Specifies the audio codec for voice communication.

**Video Codec:** Specifies the video codec for video communication.

## **FAX Server**

This section set the email address of fax receiver.

**Fax to Email Address:** the email address of fax receiver.

## **Group Pickup**

Each user could define the group at “Group Pickup List”, so this user could carry out the pickup service for specific group.

**User List:** To list all of users.

**Group Pickup List:** Move the specific group from “Group List” to here, so that the user could carry out the call pickup service for the members of group.

**Group List:** To list all of groups.

## 8.3 Voice

Click the “Voice” tab in the “VoIP” screen. This page could setup the Conference, Upload Music on Hold Music and IVR Voice Prompts.

The screenshot displays the 'Voice' configuration page with three main sections:

- Conference Room:** Includes an 'Add Conference Room' form with fields for 'Conference Room' (value: 1111) and 'Conference Password'. To the right is a table with columns 'Conference Room', 'Conference Password', and 'Delete', currently showing 'No entry'.
- Music On Hold:** Features an 'MP3 Gallery' (empty), an 'MP3 Play List' containing 'fpm-calm-river.mp3', and an 'Upload New Music File' section with a 'Browser...' button.
- IVR Voice Prompt Editor:** Has dropdowns for 'Language' (EN) and 'Sound Module' (Autoattend). Below is a table of prompts:

Voice Prompt	Voice Speech Description	Upload	Restore
greeting	Welcome, please dial the extension you try to reach or 0 for operator	<input type="radio"/>	<input type="checkbox"/>
wish to call	Please enter the number you wish to call	<input type="radio"/>	<input type="checkbox"/>
extension	Please enter your extension	<input type="radio"/>	<input type="checkbox"/>
busy	The person at extension is on the phone; please press 0 for operator or press 1 to leave a message	<input type="radio"/>	<input type="checkbox"/>
unavailable	the extension is unavaible please dial the extension the person you try to reach or 0 for operator	<input type="radio"/>	<input type="checkbox"/>

At the bottom, there is an 'Upload Sound File' section with a 'Browser...' button and 'Apply' and 'Cancel' buttons.

### Conference Room

This section need to select the conference room number and set room password.

### Music On Hold

This section could upload the MP3 file for on hold music.

**MP3 Gallery:** Here will list all of MP3 music.

**MP3 Play List:** To choose the current using on hold music from MP3 Gallery to here.

### IVR Voice Prompt Editor

The user could record the personal IVR prompts and upload to UMG system via this section.

**Upload:** Select which voice sound want to upload.

**Restore:** The IVR will reture to default voice.

## 8.4 IP PBX Call Rules

Additional call rules (call restrictions) can be specified according to each country's specific rules in the screen "Call Rule". The blocking call rule setting is to restrict unexpected user calls which may result in additional costs for the business. Another call rule is to add the prefix to the external calls automatically which may help reduce the call charges.

The screenshot displays the 'Call Rule' configuration page. At the top, there is a navigation bar with tabs for Overview, Call Setting, Voice, Call Rule (active), Channels, SIP Trunk, LCR, and Call Log. Below the navigation bar is the 'Call Rule List' section, which contains a table with columns: Rule, R/W Privilege, Prefix, Number Pattern, and Delete. The table currently shows 'No entry'. Below this is the 'Call Rule Setting' section. It features two radio buttons: 'Block Rule' (selected) and 'Add Prefix Rule'. Under 'Block Rule', there is a dropdown for 'R/W Privilege' set to 'Local' and a text input for 'Number Pattern'. Under 'Add Prefix Rule', there is a dropdown for 'R/W Privilege' set to 'Local', a text input for 'Prefix', and a text input for 'Number Pattern'. Both sections include a note: '(Example: 1234 or 1234\*;\*\* matches one or more characters.)'. At the bottom, there are 'Apply' and 'Cancel' buttons.

### Call Rule List

This section lists all the existing call rules.

**Rule:** Displays the type of the call rule.

**Privilege:** Displays the call privilege that the call rule has been applied on.

**Prefix:** Displays the prefix of the call rule if it is a prefix rule.

**Number Pattern:** Displays the number pattern.

**Delete:** Deletes the call rule.

### Call Rule Setting

This section lists all the call rule settings.

**Block Rule:** Specifies whether or not the rule is a block rule.

**Privilege:** Specifies the privileges of the call rule.

**Number Pattern:** Specifies the number pattern to be blocked.

**Add Prefix Rule:** Specifies whether or not the rule is a prefix rule.

**Privilege:** Specifies the call privilege that is applied to the call rule. Use "\*" for serial unknown numbers and "?" for a signal number.

**Prefix:** Specifies the prefix that will be added to the number.

**Number Patten:** Specifies the number pattern applied to the rule. Use "\*" for serial unknown numbers and "?" for a signal number.

## 8.5 IP PBX Channel Setting

The PBX “Channels” allows the administrator to see the list of the PSTN card.

The screenshot shows the 'Channels' configuration page for a PSTN Card. The top navigation bar includes Overview, Call Setting, Voice, Call Rule, Channels (selected), SIP Trunk, LCR, and Call Log. The main content area is divided into three sections:

- Hardware Type:** A table listing 8 channels, all set to 'FXO'.

Channel	Type
Channel 1	FXO
Channel 2	FXO
Channel 3	FXO
Channel 4	FXO
Channel 5	FXO
Channel 6	FXO
Channel 7	FXO
Channel 8	FXO
- Channels Forward:** A table with columns for Channels, Call Id, Extension, and Delete. It currently shows 'No entry'.
- Channels Setting:** A form with a 'Channels' dropdown set to 'channel1', a 'Call Id' text input, and an 'Extension' dropdown set to '5000'. There are 'Apply' and 'Cancel' buttons at the bottom.

### Hardware Type

This section lists the channels of PSTN Card. The UMG-2000 will show from Channel 1 ~ Channel 4, the UMG-2100 will show from Channel 1 ~ Channel 8.

### Channels Forward

This section lists the settings of the caller ID.

**Name:** Specifies the call name that will be shown to the call receiver.

**Number:** Specifies the call number that will be shown to the call receiver.

The administrator can choose a channel as a voice or a data channel by clicking the corresponding “right” button or removing a channel from the existing list by clicking the corresponding “left” button.

### Channels setting

This section set the channel, call ID and related extension. This means that the related channel will just response the related call number and extension.

The PBX “Channels” allows the administrator to see the list of the T1/E1 card.

The screenshot shows the 'Channels' configuration page for a T1/E1 Card. The top navigation bar is the same as the previous screenshot. The main content area is divided into three sections:

- Hardware Type:** A section for a T1/E1 Card. It includes a 'Channel List' with a scrollable list of channels from 'channel1' to 'channel11'. There are 'right' and 'left' arrow buttons between the list and two empty boxes labeled 'Voice Channel' and 'Data Channel'.
- Assign Caller ID:** A form with 'Name' and 'Number' text input fields.
- Connect to Internet Using T1/E1 Port:** A checkbox that is currently checked (radio button selected).

At the bottom, there are 'Apply' and 'Cancel' buttons.

## Hardware Type

This section lists the channels of T1/E1 Card. The T1 card will show from Channel 1 ~ Channel 24, the E1 card will show from Channel 1 ~ Channel 31.

**Channel List:** To list all of channels.

**Voice Channel:** According to the practical ISDN line to assign the voice channel here.

**Data Channel:** According to the practical ISDN line to assign the data channel here.

**Assign Caller ID:** If this ISDN line could define the Caller ID, you could fill it in here. Please contact with your ISP for detail information.

**Connect to Internet Using T1/E1 Port:** Always choose “Enable” for this option.

## 8.6 SIP Trunk Setting

**SIP Trunk Setting** allows UMG system register to different SIP systems and ITSP Services (SIP Trunk).

The screenshot displays the SIP Trunk configuration interface. At the top, there is a navigation menu with tabs for Overview, Call Setting, Voice, Call Rule, Channels, SIP Trunk, LCR, and Call Log. Below the menu, there are two tables: 'IAX2 Trunk Outbound Call Rule List (Autoconfig Between Branches)' and 'SIP Trunk List'. The 'SIP Trunk List' table is currently empty. Below the tables is the 'SIP Trunk Setting' form, which includes fields for Outbound Prefix (set to \*1), Trunk/User ID, Incoming Number, Trunk/User Password, Available Time Period (0:00 to 24:00), SIP Register Domain, Registration Required (set to Enabled), SIP Proxy Domain, SIP Proxy Port, and DTMF Mode (set to rfc2833). There are 'Apply' and 'Cancel' buttons at the bottom of the form.

### SIP Trunk List

This section lists the SIP Trunk records.

### SIP Trunk Setting

This section to fill the relation registration information to create SIP Trunk.

**Outbound Prefix:** To assign the prefix number for this record. When the subscriber want to make external call via this SIP Trunk, the dialing number need start by the prefix number.

**Trunk/User ID:** Specifics the account ID for registering.

**Incoming Number:** Specifics the number for registering.

**Trunk/User Password:** Specifics the password for registering.

**Available Time Period:** Specifics what time can use this SIP Trunk for calling.

**SIP Register Domain:** Specifics the register server address.

**Registration Required:** Specifics if need send registration require with server.

**SIP Proxy Domain:** Specifics the proxy server address.

**SIP Proxy Port: Specifics the SIP port.**  
**DTMF Mode: Specifics the DTMF mode.**

## 8.7 IP PBX Call Reference

The system could define the prefix number for FXO or SIP Trunk, or integrate the external gateway for prefix number at this page. Please remember to enable the “LCR” function at **Call Setting** page at first.

Gateway Trunk Setting		
IP Address	Port (1~65535)	Group Name
<input type="text"/>	5060	<input type="text"/>
No entry		
<input type="button" value="Add"/>		

FXO Trunk Setting	
Group Name	Channels
<input type="text"/>	<input type="text"/> (eg:1,3,5)
No entry	
<input type="button" value="Add"/>	

LCR Trunk Group Setting (LCR Feature must be enabled in call setting)		
Group Name	Prefix Number	Path (FXO Gateway/SIP Trunk)
<input type="text"/>	<input type="text"/>	<input type="text"/>
No entry		
<input type="button" value="Add"/>		

LCR Dialing Rules Setting (LCR Feature must be enabled in call setting)				
Prefix Number	Delete Length (0~16)	Add Prefix Number	Path (FXO Gateway/SIP Trunk)	Secondary Path
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	N/A
No entry				
<input type="button" value="Add"/>				

### Gateway Trunk Setting

UMG-2000 Series can make the off-net call either via the external voice gateway. Before you can make the successful call, you have to fill in gateway’s IP address and SIP port.

### FXO Trunk Setting

You also could determine use which FXO port for outgoing call via LCR function.

### LCR Trunk Group Setting

When want to make VoIP calls through the above Gateway Trunk, FXO channel or SIP Trunk, the user can use this function to accomplish the 2\_Stage dialing method.

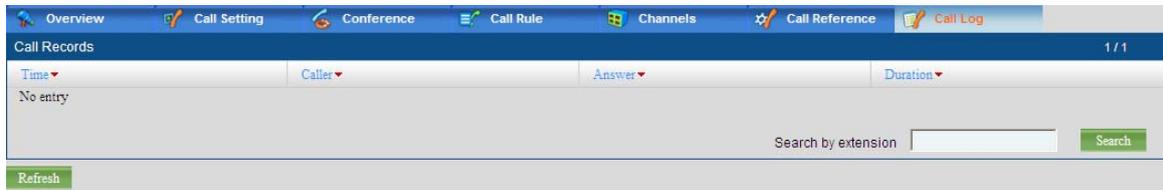
### LCR Dialing Rules Setting

This is another way to make VoIP calls through the above Gateway Trunk, FXO channel or SIP Trunk, the user can use this function to accomplish the 1\_Stage dialing method.

## 8.8 IP PBX Call Log

---

The “Call Log” screen enables the administrator to check all the call history.



### CALL RECORDS

This section lists all the information of the history call records.

**Time:** Displays the time the call occurs.

**From:** Displays the calling number.

**To:** Displays the called number.

**Duration:** Displays the call duration.

## 9. Web Management - Email

The UMG-2000 Series Email suite includes the following service: commonly used Email server, Email filtering, Email message management and email blacklist. These services provide users a basic, secure and easy-managing email service.

### **EMAIL SERVER**

The UMG-2000 Series supports common Email servers that support Post Office Protocol version 3 (POP3), Internet Message Access Protocol (IMAP) and Simple Mail Transfer Protocol (SMTP). POP3 is a standard mail protocol used to receive emails from a remote server to local clients. It also allows clients to download email messages to local computers and read them offline. IAMP is used for accessing the email on the remote web server from a local client. It allows the mail box to be managed by multiple users. SMTP is the standard protocol for sending emails.

### **EMAIL FILTER**

Email Filtering is the Anti-Spam and Anti-Virus of email. Every email sent to or received from the UMG-2000 Series email server will be verified and filtered according to the standard rules and virus database. This will greatly reduce the potential harm to your private network. The email server uses the common filter standard and builds the virus database which can be updated from the virus server automatically.

### **EMAIL MESSAGE MANAGEMENT**

The UMG-2000 Series supports the email message management including auto backup and auto replay. The email server can backup every sent and received email and reply to the mail sender with the user pre-selected email if the corresponding feature is enabled.

### **EMAIL BLACK LIST**

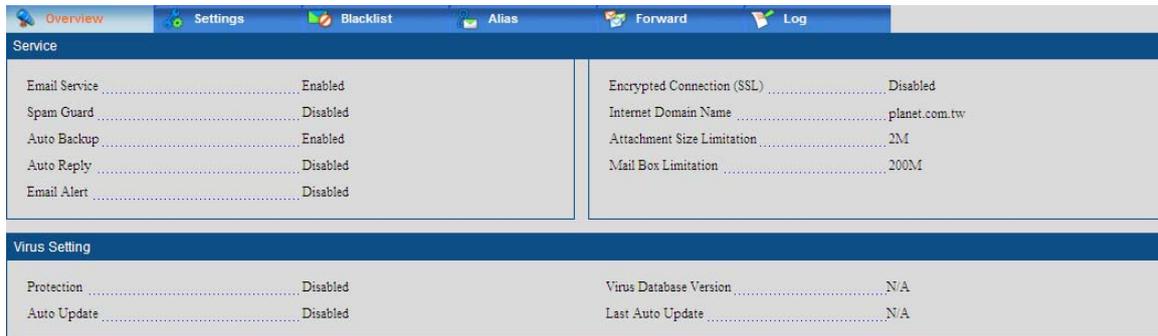
An email server always gathers the reports about the spam and threaten coming from certain addresses. The administrator can add these addresses to the email blacklist so that the email server will filter, reject and drop mails from these addresses.

### **EMAIL forward**

The UMG-2000 Series supports the email forward function. The email either received or sent will be forwarded from monitored user to monitor user

## 9.1 Email Overview

The email overview shows the current setting of the Email service.



Service	
Email Service .....	Enabled
Spam Guard .....	Disabled
Auto Backup .....	Enabled
Auto Reply .....	Disabled
Email Alert .....	Disabled
Encrypted Connection (SSL) .....	Disabled
Internet Domain Name .....	planet.com.tw
Attachment Size Limitation .....	2M
Mail Box Limitation .....	200M

Virus Setting	
Protection .....	Disabled
Auto Update .....	Disabled
Virus Database Version .....	N/A
Last Auto Update .....	N/A

### SERVICE

The section lists the current settings of the email service.

**Email Service:** Displays the state of Email services, enabled or disabled

**Spam Guard:** Displays the state of the feature “Spam Guard”, enabled or disabled.

**Auto Backup:** Displays the state of the feature “Auto Backup” feature, enabled or disabled.

**Auto Reply:** Displays the state of the feature “Auto Reply”, enabled or disabled

**Email Alert:** Displays the state of the feature “Email Alert”, enabled or disabled

**Encrypted Connection:** Displays the state of the feature “Encrypted Connection”, enabled or disabled.

**Encrypted Connection (SSL):** Displays the state of the feature “Encrypted Connection”, enabled or disabled.

**Internet Domain Name:** Displays the domain name of the server.

**Attachment Size Limitation:** Displays the attachment size limitation.

**Mail Box Limitation:** Displays the mail box limitation of each user.

### VIRUS SETTING

The section lists the current setting of the virus database.

**Protection:** Displays the antivirus state.

**Auto Update:** Displays the state of the feature “auto update Email virus database”, enable or disable.

**Virus Database Version:** Displays the current version of the virus data base.

**Last Update:** Displays the last upgraded date in format of “MM DD HH:MM:SS YY”.

## 9.2 Email Basic Setting

The “Email Setting” page allows the administrator to manage the setting of the Email service.

### SERVICE

This section lists all the available settings of the email service. The email service is accessible only when Email service is enabled.

**Email Service:** Enables or disables the Email services.

**Spam Guard:** Enables or disables the feature “Spam Guard”. Enabling this feature will allow filtering all the junk mail and it will protect the mail box from invasion of spammers.

**Auto Backup:** Enables or disables “Auto Backup” feature. Enable this feature to make the UMG-2000 Series backup all your incoming and outgoing email.

**Auto Reply:** Enables or disables “Auto Reply” feature. Enabling this feature will allow the mail server to reply to the receiver automatically.

**Encrypted Connection:** Enables or disables “Encrypted Connection”. Enable this feature if you would like to build a secure channel between your Email clients and the UMG-2000 Series Email when you send or receive Email.

**Email Alert:** Enables or disables the “Email Alert” feature. Enabling this feature will allow the UMG-2000 Series to send an email to the pre-assigned address with a detailed event report when the system encounters critical error.

**Internet Domain Name:** Specifies the Internet domain name.

**Attachment Size Limitation:** Specifies the limitation size of the mail attachment.

**Mail Box Limitation:** Specifies the limitation size of the users’ mail box.

### VIRUS SETTING

This section lists all the settings of the email antivirus database.

**Protection:** Enables or disables antivirus protection. Enable this feature if you would like to scan mail for antivirus.

**Auto Update:** Enables or disables the feature “Auto Update Email Virus Database”. Enable this feature if you want to make the UMG-2000 Series update the email virus database automatically.

### ALERT EMAIL ADDRESS

This section lists all the email alert mail addresses that the UMG-2000 Series will send

email to when the system encounters critical error.

**Alert Mail Receiver: Displays the alert email receiver.**

**Add new email alert address: Specifies the alert email receiver.**

### ADD MAIL ADDRESS TO ALERT EMAIL LIST

Specify a full Email address and click the “Apply” button to add the email address to the alert list.

### DELETE MAIL ADDRESS FROM ALERT EMAIL LIST

Check the “delete” check box and click the “Apply” button to delete the selected email address from the alert list.

## 9.3 Email Blacklist

---

All the email from the email addresses, email accounts, domain names in the email blacklist will be reject by the email server. The administrator can manage the email black list in the “Blacklist” page.

Blacklist	Type	Delete
No entry		

### EMAIL BLACK LIST SETTING

This section allows for the adding of new entities to the email black list

**Username: Specifies the username that you want to add to the black list.**

**Email Address: Specifies the email address that you want to add to the black list.**

**Domain Name: Specifies the domain name that you want to add to the black list.**

**All the emails sent to this domain will be blocked.**

### EMAIL BLACK LIST

This section shows all the entities in the email black list

**Username: Displays the name of the black entity.**

**Email Address: Display the type of the black entity, username, email address, or domain name.**

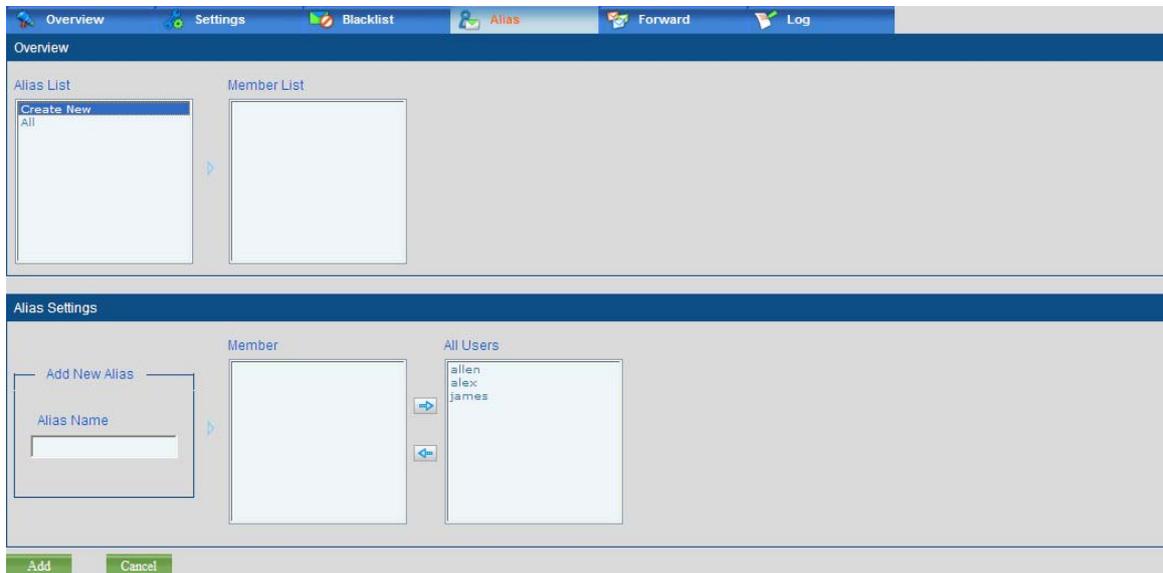
### DELETE ENTITIES FROM THE BLACK LIST

Check the “Delete” check box and click the “Apply” button to delete an entity from the black list.

## 9.4 Email Alias

---

Administrators can manage the Email alias here. Email alias is not a real email account. Instead, it is an address that forwards all emails that it has received to its email accounts.



### OVERVIEW

This section lists all the existing email alias accounts and their numbers. Select an alias name and its numbers will be shown in the number menu.

**Alias List: Displays all alias names.**

**Number List: Displays the numbers of an alias.**

### SETTINGS

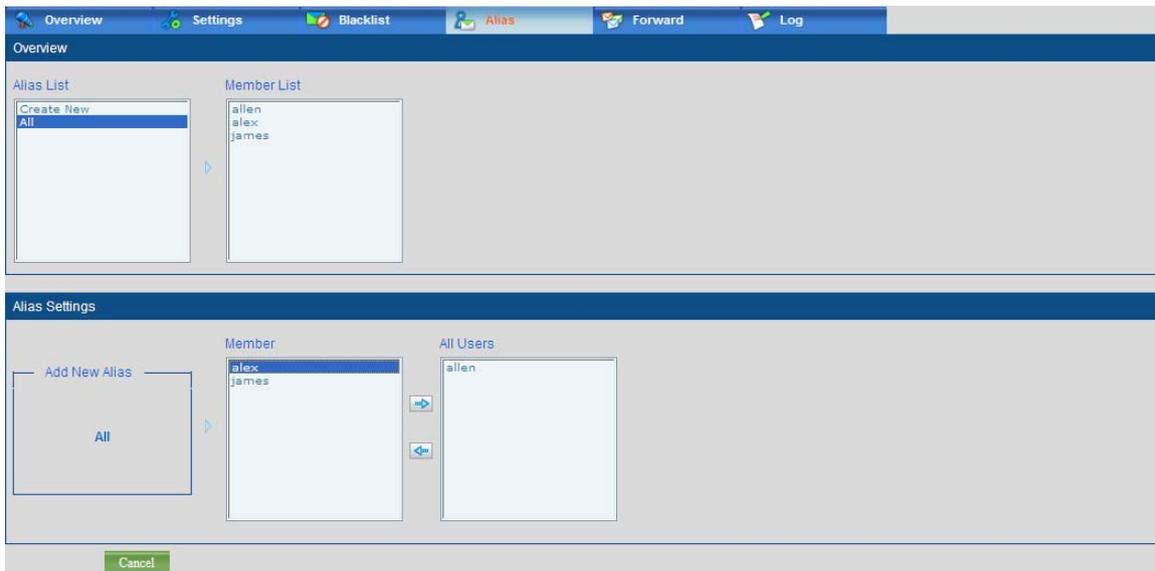
**Alias Name: Specifies a preferred alias name.**

**Number: Specifies the number of the alias from the user list.**

**All number: Displays all available users.**

### CREATING AN EMAIL ALIAS

Type an alias name and use the “Left” and “Right” button to add or delete numbers. Then click the “Add” button to create an Email alias.



### DELETING AN EMAIL ALIAS

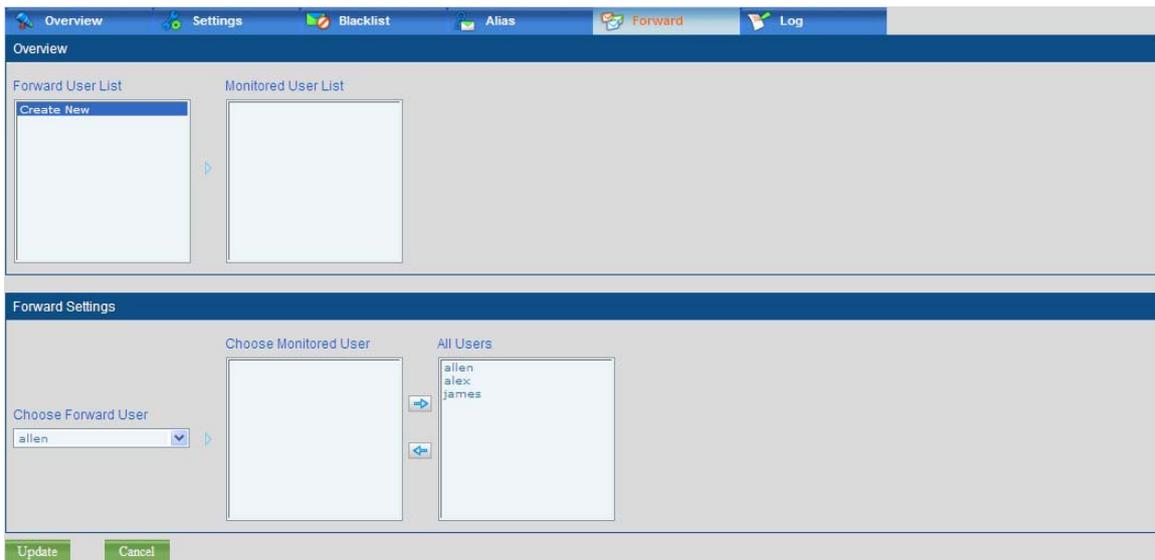
Select an alias from the alias list, and then click the “Delete” button to delete the email alias.

### UPGRADING AN EMAIL ALIAS

Select an alias from the alias list. Use the “Left” and “Right” buttons to add or remove its numbers, and then click the “Upgrade” button to upgrade an alias.

## 9.5 Email Forward

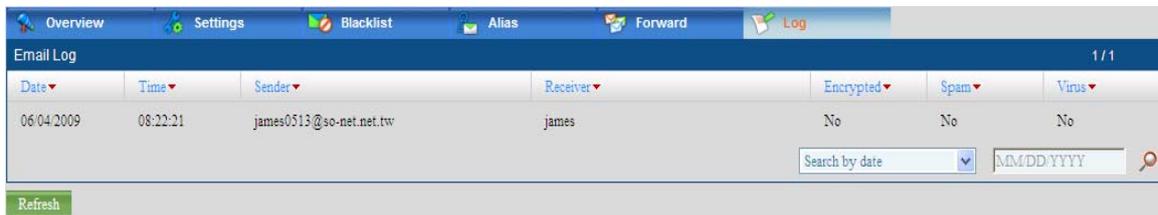
The page “Email Forward” allows the administrator to set forward user and monitored user. Select one forward user and multi monitored user. Both received email and sent email will forward one copy to monitored user.



## 9.6 Email Log

---

The page “Email Log” allows the administrator to scan and query the Email log. The log will show the mail history, spam and virus mail history, and user connection history.



Date	Time	Sender	Receiver	Encrypted	Spam	Virus
06/04/2009	08:22:21	james0513@so-net.net.tw	james	No	No	No

### EMAIL LOG

This section lists all the email logs.

**Date:** Displays the date of an incoming or outgoing mail.

**Time:** Displays the time of an incoming or outgoing mail.

**From:** Displays the full address of the email sender.

**To:** Displays the full address of the email receiver.

**Encrypted:** Display whether it is an encrypted connection between the email client and the UMG-2000 Series Email server.

**Spam:** Displays whether it is a junk mail.

**Virus:** Displays whether a virus is existing in the mail.

### EMAIL LOG SORTING

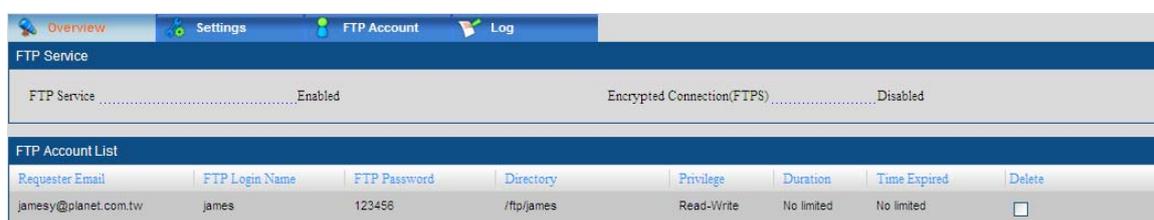
Select “Search by name” or “Search by date” in the drop down menu and specify the key word in the text fill. Then click the “Search” button, and the results will appear.

## 10. Web Management - FTP

The “FTP Server” screen allows the administrator to manage the FTP server. When adding an account to the FTP authorized list, the UMG-2000 Series will send the email with the suitable account and password information to the specified requested email and the account will expire automatically after the expiration time.

### 10.1 FTP Overview

The page “FTP Overview” shows the current FTP settings.



The screenshot shows the 'FTP Overview' page with a navigation bar containing 'Overview', 'Settings', 'FTP Account', and 'Log'. The main content area is divided into two sections: 'FTP Service' and 'FTP Account List'.

Requester Email	FTP Login Name	FTP Password	Directory	Privilege	Duration	Time Expired	Delete
jamesy@planet.com.tw	james	123456	/ftp/james	Read-Write	No limited	No limited	<input type="checkbox"/>

### 10.2 FTP Setting

The “FTP Setting” page allows the administrator to manage the FTP service.



The screenshot shows the 'FTP Setting' page with a navigation bar containing 'Overview', 'Settings', 'FTP Account', and 'Log'. The main content area is titled 'Service' and contains two rows of settings:

- FTP Service:  Enable  Disable
- Encrypted Connection(FTPS):  Enable  Disable

At the bottom of the form are 'Apply' and 'Cancel' buttons.

#### FTP SETTING

This section lists all the available settings of the FTP service:

**FTP Server:** Enables or disables the FTP server.

**Encrypted Connection (FTPS):** Enables or disables the encrypted connection.

### 10.3 FTP Account

The “FTP Account” page allows the administrator to manage the FTP User.



The screenshot shows the 'FTP Account' page with a navigation bar containing 'Overview', 'Settings', 'FTP Account', and 'Log'. The main content area is titled 'FTP Account' and contains several input fields and dropdown menus:

- Requester Email:
- FTP Login Name:
- FTP Password:
- Privilege:  (dropdown menu)
- Duration:  (dropdown menu)

At the bottom of the form are 'Apply' and 'Cancel' buttons.

## FTP USER

This section lists all the available settings of FTP configuration management:

**Requested Email:** Specifies the email address of the one who requested the FTP service.

**Login Name:** Specifies the account that is used to login to the FTP service.

**Password:** Specifies the corresponding password.

**Directory:** Specifies the authorized directory of this account.

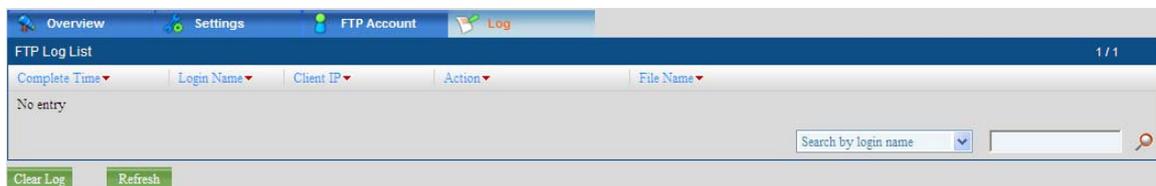
**Privileges:** Specifies the privileges of this account.

**Duration:** Displays the valid duration of the account. After the specified period, the account will expire automatically.

## 10.4 FTP Log

---

The “FTP Log” page show FTP Log.



### FTP LOG LIST

This section lists the service state of the LAN services:

**Requested Email:** Displays the email address of the one who requested the FTP service.

**Login Name:** Displays the login account.

**Client IP:** Displays the current client IP address.

**File Name:** Displays the downloading or uploading file name.

**Action:** Displays the action of the account: download, upload, or idle.

**Complete Status:** Displays the status of the account.

**Complete Time:** Displays the completed time of the account.

# 11. Web Server

The UMG-2000 Series has support the Web Server feature, it let administrator could put the web pages into system for web services.

## 11.1 Web Server Overview

The page “Web Server Overview” shows the current Web Server settings.

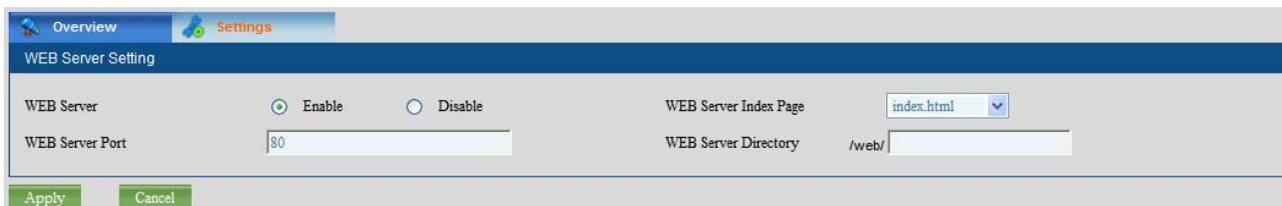


The screenshot shows the 'Web Server Overview' page with two tabs: 'Overview' and 'Settings'. The 'Service' section displays the following settings:

WEB Server	Disabled	WEB Server Index Page	index.html
WEB Server Port	80	WEB Server Directory	/web/
WEB Server Access Address	N/A		

## 11.2 Web Server Settings

The page “Web Server Overview” shows the current Web Server settings.



The screenshot shows the 'Web Server Setting' page with two tabs: 'Overview' and 'Settings'. The 'WEB Server Setting' section displays the following configuration options:

WEB Server	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	WEB Server Index Page	index.html
WEB Server Port	80	WEB Server Directory	/web/

Buttons: Apply, Cancel

### Web Server Setting

The “Web Server Setting” page allows the administrator to setup the Web Server parameters.

**WEB Server:** TO enable or disable the Web Server function.

**Web Server Port:** Specifies the web server service port.

**Web Server Index Page:** Specific the index page format type.

**Web Server Directory:** Specific the file located path.

## 12. Web Management - Security

The UMG-2000 Series security suite includes the comprehensive services: package inspection Firewall, Point-to-Point Tunneling Protocol (PPTP) based Virtual Private Network (VPN). These services will allow connection to the Internet and protection from any Internet threats.

### Firewall Security

The UMG-2000 Series provides an easy-understanding and professional network security management. By default, firewall enables all prevention schemes and exclusively drops all packages to protect the user's private network except the ones matching the predefined rules by the safety applications in LAN. The administrator can also set the access control rules to achieve a better network environment by denying some services of the clients in LAN. The administrators can also assign authorized users in LAN to a trusted IP list. The users in the trusted IP list will not be shielded or blocked by all the firewall rules.

### PPTP VPN Security

PPTP VPN is a secure tunnel for transporting IP traffic using PPP. It is supported by Microsoft dial-up Networking. The UMG-2000 Series provides the PPTP VPN server to build a secure link to the UMG-2000 Series from the outside of the office. It is a good choice especially for mobile and remote users who can connect to the Internet and want to securely access the office network.

## 12.1 Security Overview

The page "Security Overview" shows the current security settings.

The screenshot displays the 'Security Overview' page with a navigation bar at the top containing 'Overview', 'Settings', 'Content Filter', 'Access Control', 'Port Forwarding', and 'Log'. The main content is divided into two sections: 'Firewall Security' and 'PPTP VPN Security'.

Firewall Security	
DMZ Server Address	N/A
Response to Ping	Enabled
Passthrough	
IPSec Passthrough	Enabled
PPTP Passthrough	Enabled
L2TP Passthrough	Enabled
DoS Prevention	
TCP SYN Flood	Enabled
UDP Flood	Enabled
ICMP Flood	Enabled
Ping of Death	Enabled
UPnP Support	Enabled

PPTP VPN Security	
PPTP VPN Service	Enabled
VPN Server Address	N/A
VPN Client Address Range	10.8.1.2-254
Authentication Type	mschap-v2
Encryption Type	mppe-128
Compression	N/A

### FIREWALL SECURITY

This section lists all the current firewall settings.

**DMZ Server Address:** Displays the DMZ host IP address.

**Response to Ping:** Displays the state of the feature "Response to Ping", enabled or disabled.

**UPnP Support:** Displays the state of the feature "UPnP Support", enabled or disabled.

## PASSTHROUGH

This section lists all the current firewall pass-through rules.

**IPSec Passthrough:** Displays whether the “IPSec Passthrough” feature is enabled or disabled.

**PPTP Passthrough:** Displays whether the “PPTP Passthrough” feature is enabled or disabled.

**L2TP Passthrough:** Displays whether the “LTP Passthrough” feature is enabled or disabled.

## DOS PREVENTION

This section lists all the current settings for the DOS prevention.

**TCP SYN Flood:** Displays the state of the “TCP SYN Flood” feature, enabled or disabled.

**UDP Flood:** Displays the state of the “UDP Flood” feature, enabled or disabled.

**ICMP Flood:** Displays the state of the “ICMP Flood” feature, enabled or disabled

**Ping of Death:** Displays the state of the “Ping of Death” feature, enabled or disabled.

## PPTP VPN SECURITY

This section lists all the current PPTP VPN settings.

**PPTP VPN Service:** Displays the state of the PPTP VPN service, enabled or disabled.

**VPN Server Address:** Displays the IP address PPTP VPN server.

**VPN Client Address Range:** Displays the IP address range which will be granted to PPTP clients by the server.

**Authentication Type:** Displays the authentication method in which the PPTP server authenticates its clients.

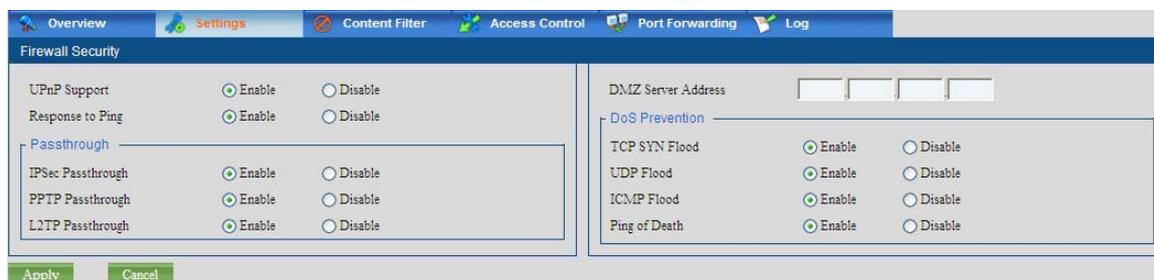
**Encryption Type:** Display the encryption type in which the PPTP server encrypts the data.

**Compression:** Displays the state of the data compression, enabled or disabled.

## 12.2 Security Setting

---

The “Security Setting” page allows the administrator to manage the firewall.



## FIREWALL SECURITY

This section lists all the available security settings.

**UPnP Support:** Enables or disables the “UPnP Support” feature. Enable this feature if you would like to support the Universal Plug and Play (UPnP) protocol.

**Response to Ping:** Enables or disables the “Response to Ping” feature. Enable

this feature to make the UMG-2000 Series respond to the ping request from the Internet.

**DMZ Server Address:** Specifies the DMZ host IP address. The clients on the outside network cannot connect to the servers in the private network which are protected by the firewall. To solve this problem, a DMZ (demilitarized zone) host is inserted between the company's private network and the public network. The DMZ host will be exposed to the Internet without protection. Specify it only if you need a special Internet service or expose one computer with no restriction.

## **PASSTHROUGH**

This section lists all the settings of the firewall pass-through rules.

**IPSec Passthrough:** Enables or disables the "IPSEC Passthrough" feature. Enable this feature to allow Internet Protocol Security (IPSEC) pass-through.

**PPTP Passthrough:** Enables or disables the "PPTP Passthrough" feature. Enable this feature to allow PPTP VPN pass-through.

**L2TP Passthrough:** Enables or disables the "L2TP Passthrough" feature.

## **DOS PREVENTION**

This section lists all the settings of the firewall DoS prevention rules.

**TCP SYN Flood:** Enables or disables the "TCP SYN Flood" feature. Enable this feature for protection from the TCP SYN flood attack.

**UDP Flood:** Enables or disables the "UDP Flood" feature. Enable this feature for protection from the UDP SYN flood attack.

**ICMP Flood:** Enables or disables the "ICMP Flood" feature. Enable this feature for protection from the ICMP SYN flood attack.

**Ping of Death:** Enables or disables the "Ping of Death" feature. Enable this feature for protection from a "Ping to Death" attack.

---

### **Note:**

A DMZ host will be exposed on the web without protection by a firewall. Assigning a DMZ host may make other computers in the network vulnerable. When assigning a DMZ host, you must take security into account and protect it if possible.

---

## 12.3 Content Filter

The “Content Filter” page allows the administrator to set the HTTP content filter rules and assign the trusted IP.

The screenshot shows the 'URL Content Filtering Setting' page. It features a top navigation bar with 'Overview', 'Settings', 'Content Filter', 'Access Control', 'Port Forwarding', and 'Log'. The main content area is titled 'URL Content Filtering Setting' and is divided into two columns. The left column contains two sections: 'Add Site/Keyword to Block' and 'Add Trusted IP'. The 'Add Site/Keyword to Block' section has two radio buttons: 'Block Site' (with an example 'sex.com') and 'Keyword' (with an example 'sex'). The 'Add Trusted IP' section has a 'Trusted IP' field with an example '192.168.21.1'. The right column contains two tables: 'Site/Keyword' and 'Trusted IP', both showing 'No entry' and a 'Delete' button. At the bottom are 'Apply' and 'Cancel' buttons.

### URL SITE/KEYWORD TO BLOCK RULES

This section allows for the setting of the HTTP content filter rules.

**Block Site:** Specifies the URL site if you want to block all the content of this site.

**Keyword:** Specifies the keyword that you wish to block. All sites containing this keyword will be blocked.

### DELETING THE URL SITE/KEYWORD TO BLOCK RULES

Check the check box of the corresponding site/keyword and click the “Apply” button. The site/keyword will be deleted from the block list, and the site/keyword will can be accepted again.

### ADDING TRUSTED IP

This section allows setting the trusted IP.

**Trusted IP:** Specifies the trusted IP address.

### DELETING FROM THE TRUSTED IP LIST

Check the check box of the corresponding IP address and click the “Apply” button. The trusted IP address will be deleted from the trusted list. The IP will be treated as the normal again.

## 12.4 Access Control

To control access to Internet of some services in LAN, the administrator can set the access control rules in the page “Access Control”. The specific services of the PC in LAN cannot be accessed through the Internet any more.

Service Name	Protocol	Start Port	End Port	Mac Address	Local Network	Delete
No entry						

**Access Control**

Service Name:

Service Type:

Protocol:

Start Port:  (Range:1~65534)

End Port:  (Range:1~65534)

**Access Control Local Network**

Mac Address

IP Address

All

**Application Control**

QQ	<input type="radio"/> Block <input checked="" type="radio"/> Allow	MSN	<input type="radio"/> Block <input checked="" type="radio"/> Allow
BT	<input type="radio"/> Block <input checked="" type="radio"/> Allow	Thunder	<input type="radio"/> Block <input checked="" type="radio"/> Allow
eDonkey	<input type="radio"/> Block <input checked="" type="radio"/> Allow		

### SERVICE ACCESS CONTROL

This section allows for the setting of access rules on the LAN PC.

**Service Name:** Specifies the service to block.

**Service Type:** Specifies the service type. It can be the system defined or user defined.

**Protocol:** Specifies the network protocol that the rule will apply to if you select “user defined” as the service type.

**Start Port:** Specifies the start port that the rule will apply to if you select “user defined” as the service type.

**End Port:** Specifies the end port that the rule will apply to if you select “user defined” as the service type.

**MAC Address:** Specifies the MAC address of the PC client in LAN on which you want to apply the rule.

**IP Address:** If you want to apply the rule on a special IP address, check this option.

**Single IP Address:** Specifies one single IP address in LAN on which you want to apply the rule.

**IP Address Range:** Specifies the IP address range in LAN on which you want to apply the rule.

**All:** Specifies whether or not you want to apply the rules on all PC clients in LAN.

### DELETING SERVICES FROM THE ACCESS CONTROL LIST

Check the “Delete” check box of the corresponding service and click the “Delete” button to delete the service from the access control list. The firewall will not block this service any more.

## 12.5 Port Forwarding

To control forward some special internet request from WAN to LAN, the administrator can set the port forwarding rules in the page “Port Forwarding”. The specific internet request can forward from WAN to LAN.

The screenshot displays the 'Port Forwarding' configuration page. At the top, there is a navigation bar with tabs for Overview, Settings, Content Filter, Access Control, Port Forwarding (selected), and Log. Below the navigation bar is a 'Service List' table with columns: Service Name, Protocol, Exterior Start Port, Exterior End Port, Server Ip Address, and Delete. The table currently shows 'No entry'. Below the table is the 'Port Forwarding' configuration form. The form includes the following fields: Service Name (text input), Service Type (dropdown menu set to 'All'), Protocol (dropdown menu set to 'TCP/UDP'), Exterior Start Port (text input set to '1', with a range of 1~65534), Exterior End Port (text input set to '65534', with a range of 1~65534), and a 'Port Forwarding Local Network' section containing a 'Server Ip Address' field (set to '192.168.1'). At the bottom of the form are 'Apply' and 'Cancel' buttons.

### SERVICE PORT forward

This section allows for the setting of port forward rules.

**Service Name:** Specifies the service to forward.

**Service Type:** Specifies the service type. It can be the system defined or user defined.

**Protocol:** Specifies the network protocol that the rule will apply to if you select “user defined” as the service type.

**Extension Start Port:** Specifies the start port that the rule will apply to if you select “user defined” as the service type.

**Extension End Port:** Specifies the end port that the rule will apply to if you select “user defined” as the service type.

**Server IP Address:** If you want to apply the rule to a special IP address, check this option.

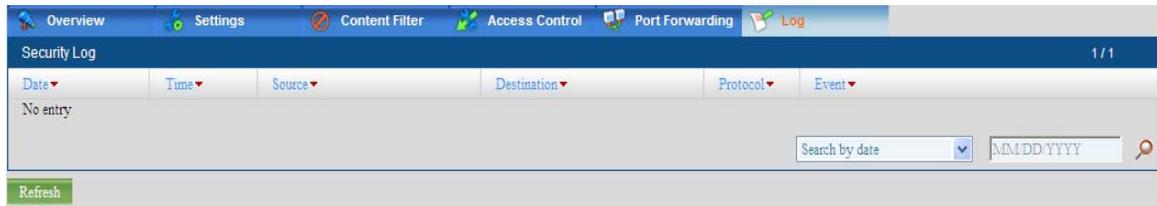
### DELETING SERVICES FROM THE port forward LIST

Check the “Delete” check box of the corresponding service and click the “Delete” button to delete the service from the port forward list. The firewall will not forward this service any more.

## 12.6 Security Log

---

The “Security Log” page shows the firewall logs.



### SECURITY LOG

This section lists all the firewall logs.

**Date:** Displays the date of the log.

**Time:** Displays the time of the log.

**Source:** Displays the source IP address of the package.

**Destination:** Displays the destination of the package.

**Protocol:** Displays the protocol of the package.

**Event:** Displays the action that the firewall has taken to deal with the package.

### SECURITY LOG SORTING

Select “Search by addresses” or “Search by date” in the drop down menu. Specify the key word in the text fill, and then click “Search” button. The results will then appear.

# 13. Web Management - System

The UMG-2000 Series provides system management mechanisms to understand and manage our system. It mainly provides: hardware overview, company profile setup, and system event management.

## HARDWARE OVERVIEW

The UMG-2000 Series will display all hardware information, including: hardware version, the technical parameter of CPU, Memory, Flash, RTC, Disk etc.

## COMPANY PROFILE SETUP

The UMG-2000 Series provides the ability to build and update the profile of the customer's company.

## SYSTEM EVENT MANAGEMET

The UMG-2000 Series provides the event reporting system that strives for the continued improvement product safety and reliability through the systematic collection and analysis. It gives the administrator the ability to determine what should be done when events occur.

### 13.1 System Overview

The system "Overview" screen presents a summary of the UMG-2000 Series system status.

Version				
Software Version	v342.0.0	Hardware Version	v2.0.0	

Hardware Information				
CPU	PPC440GX 800 MHz	Local Network Ethernet Port	24*10/100Mbps	
Memory	DDR ECC 1024 MBytes	Internet Port	10/100Mbps	
Flash	64 MBytes	Extention Port	2*10/100/1000Mbps	
Real Time Clock	DS1324	PBX Card	WCTDM0	
Wireless Card	N/A			

Disk Information				
Disk	Model Number	Serial Number	Firmware Revision	Capacity
Disk 1	Hitachi HDT721010SLA360	STF604MH0\$IMJB	ST60A31B	976.76 GB
Disk 2	N/A	N/A	N/A	0.00 GB
Disk 3	N/A	N/A	N/A	0.00 GB
Disk 4	N/A	N/A	N/A	0.00 GB

## VERSION

**Software Version:** Displays the current software version of the UMG-2000 Series.

**Hardware Version:** Displays the current hardware version of the UMG-2000 Series.

## HARDWARE INFORMATION

**CPU:** Displays the CPU information.

**Memory:** Displays the memory information.

**Flash:** Displays the flash information.

**Real Time Clock (RTC):** Displays the RTC information.

**Wireless:** Displays the information of the wireless adapter.

**Local Network Ethernet Port:** Displays the information of the switch.

**Internet Port:** Displays the information of the WAN interface.

**Extension Port:** Displays the information of the extension ports.

**PBX Card:** Displays the information of VoIP card.

## DISK INFORMATION

**Disk:** Displays the disk name.

**Model Number:** Displays the model number of the disk.

**Serial Number:** Displays the serial number of the disk.

**Firmware Revision:** Displays the firmware version of the disk.

**Capacity:** Displays the raw capacity of the disk.

## 13.2 System Setting

---

The page “System Setting” allows the administrator to update the company profile.

The screenshot shows the 'System Setting' page in a web browser. At the top, there are tabs for 'Overview', 'Settings', and 'Events'. The 'System Setting' page has a header bar with the same tabs. Below the header, there are several input fields: 'Company' (text box with 'PLANET'), 'Location' (text box with 'TAIPEI'), 'Country' (dropdown menu with 'TAIWAN'), and 'Time Zone' (dropdown menu with '(GMT+08:00) Taipei'). Below these fields is a section titled 'Date & Time'. It contains two radio buttons: 'Set Local Time' (selected) and 'Synchronize system clock with a time server over the Internet'. Under 'Set Local Time', there are fields for 'Date' (06/05/2009) and 'Time' (01:33:13). Under 'Synchronize system clock...', there is a 'Time Server' dropdown menu (time-nw.nist.gov) and a 'Next Synchronization' date (Sat Jun 6 00:00:00 2009). At the bottom of the form are 'Apply' and 'Cancel' buttons.

## SYSTEM SETTING

This section lists all the settings of company profile.

**Company:** Specifies your company name.

**Location:** Specifies your company location.

**Country:** Specifies the country of your company.

**Time Zone:** Specifies the time zone of your city.

## DATE & TIME

This section allows the administrator to set the local time.

**Set Local Time:** Manually set the local date and time

**Date:** Specifies the local date in format of MM/DD/YYYY.

**Time:** Specifies the local time in format of hh:mm:ss.

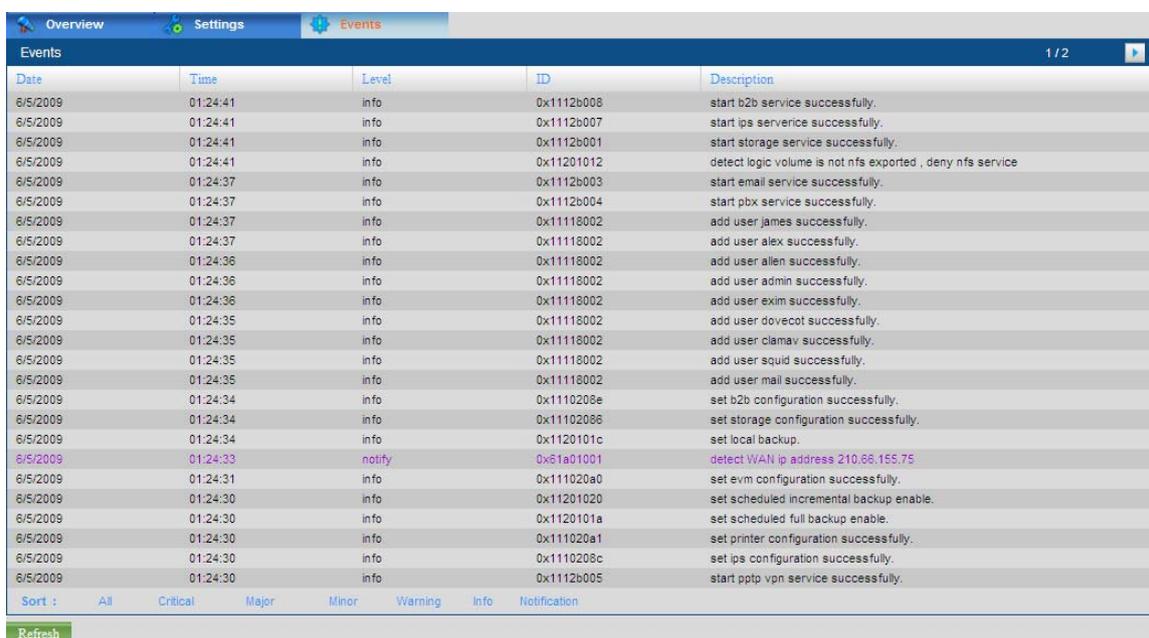
**Synchronize clock with server over the internet:** Automatically updates the local date and time from the specified time server.

**Time Server:** Specifies the time server you would like to synchronize time with.

## 13.3 System Event Log

The UMG-2000 Series system events are classified by its severity which includes Critical, Major, Minor, Notification, Warning, and Informational.

- The Critical event shows that the UMG-2000 Series is in critical, unrecoverable condition and cannot service any more.
- The major event shows that the UMG-2000 Series encountered major error and some services cannot be used any more.
- The minor event shows that some error occurred because an action or an operation has failed, however, the UMG-2000 Series is still in good state.
- The notification event shows that actions should be taken to prevent loss of data and to avoid further losses.
- The warning event shows that a wrong operation has been taken.
- The info event shows that an action has been taken but no damages have occurred.



Date	Time	Level	ID	Description
6/5/2009	01:24:41	info	0x1112b008	start b2b service successfully.
6/5/2009	01:24:41	info	0x1112b007	start ips service successfully.
6/5/2009	01:24:41	info	0x1112b001	start storage service successfully.
6/5/2009	01:24:41	info	0x11201012	detect logic volume is not nfs exported , deny nfs service
6/5/2009	01:24:37	info	0x1112b003	start email service successfully.
6/5/2009	01:24:37	info	0x1112b004	start pbx service successfully.
6/5/2009	01:24:37	info	0x11118002	add user james successfully.
6/5/2009	01:24:37	info	0x11118002	add user alex successfully.
6/5/2009	01:24:36	info	0x11118002	add user allen successfully.
6/5/2009	01:24:36	info	0x11118002	add user admin successfully.
6/5/2009	01:24:36	info	0x11118002	add user exim successfully.
6/5/2009	01:24:35	info	0x11118002	add user dovecot successfully.
6/5/2009	01:24:35	info	0x11118002	add user clamav successfully.
6/5/2009	01:24:35	info	0x11118002	add user squid successfully.
6/5/2009	01:24:35	info	0x11118002	add user mail successfully.
6/5/2009	01:24:34	info	0x1110208e	set b2b configuration successfully.
6/5/2009	01:24:34	info	0x11102086	set storage configuration successfully.
6/5/2009	01:24:34	info	0x1120101c	set local backup.
6/5/2009	01:24:33	notify	0x51a01001	detect WAN ip address 210.66.155.75
6/5/2009	01:24:31	info	0x111020a0	set evm configuration successfully.
6/5/2009	01:24:30	info	0x11201020	set scheduled incremental backup enable.
6/5/2009	01:24:30	info	0x1120101a	set scheduled full backup enable.
6/5/2009	01:24:30	info	0x111020a1	set printer configuration successfully.
6/5/2009	01:24:30	info	0x1110208c	set ips configuration successfully.
6/5/2009	01:24:30	info	0x1112b005	start pptp vpn service successfully.

### EVENTS

This section lists all the system events information.

**Date:** Displays the date of the events.

**Time:** Displays the time of the events.

**Level:** Displays the event severities.

**ID:** Displays the event IDs.

**Description:** Displays the detailed descriptions of the events.

### Alert Event Classification

This section lists the event sorting information by a user's selected criterion.

**All:** Displays all events.

**Critical:** Displays the critical events only.

**Major:** Displays the major events only.

**Minor:** Displays the minor events only.

**Warning:** Displays the warning events only.

**Info:** Displays the information events only.

## 14. Web Management - Branch-to-Branch

The Branch-to-Branch is a solution for building a company intranet which provides the ability to build a secure intranet, share data, setup voice link, and manage remote IT resources between all your branches by using the Internet. First, a reliable, secure, and auto recoverable connection is built between the different branches via the Internet or your private network. Second, an intranet which can only be accessed by authorized users, especially for the numbers or employees of the organization will be built based on this connection. Third, the VoIP switching and data synchronization systems are automatically setup for inter-branch communication. Finally, a centralized configuration management platform for the administrator to organize and manage all data and resources within the whole intranet is implemented. When the enabling the Branch-to-Branch feature, the UMG-2000 Series can be in only one of the following modes.

### **STANDALONE**

Standalone is a standby mode when the Branch-to-Branch feature is disabled.

### **HEADQUARTER**

Headquarter is a server or master mode. The UMG-2000 Series in this mode will be the master node in this group.

### **DIVISION**

Division is a client or slave mode. The UMG-2000 Series in this mode will be a slave node in the group and can be managed by its headquarter.

## 14.1 Branch-to-Branch Setup

---

If you want to setup up Branch-to-Branch, you must connect the UMG-2000 Series to the Internet or your private network. Choose one system as the headquarter (server) of this group and others as divisions (clients). Refer to Section - Branch-to-Branch Setting to setup the configuration.

## 14.2 Security Channel

---

Once Branch-to-Branch is setup, the secure Intranet will be built automatically. To setup the connection, both the headquarter and divisions will negotiate and SSL will be used for the authentication to protect from any Internet threats. Then a VPN channel is built for the encryption data transmission and this secure channel will be maintained until the physical network link is down or disconnected manually.

## 14.3 Remote Calls

---

Once the connection is settled, the database of all the branches and the voice link will be setup automatically. This means that users can call the extensions in the UMG-2000 Series

group once the connection is settled. For example, a user of the headquarter named user\_hq with the extension “1456” can call the user named user\_div1 with the extension “5678” by dialing “5678” directly. If another UMG-2000 Series joins the UMG-2000 Series group as a new division and the user named user\_div2 with extension 7890 is in it, the three users can call each other directly. Any call features in the call group e.g., call transfer, conference, and call forwarding is available between connected branches. All calls between extensions in different branches are visa VoIP without paying any long distance charges.

---

**Note:**

The call prefix of the divisions is determined by the headquarter.

---

## 14.4 Remote Data Synchronization

---

When a new division is added to the profile of the headquarter, two directories named “FromBran-<location>-<prefix>” and “ToBran-<location>-<prefix>” (where <location> stands for the location of the branch and <prefix> stands for the extension prefix of the branch) are created, too. The former is used for receiving data from the specific branch and the latter is used for sending data to the specific branch. When a headquarter is add to the division’s profile, two directories named “FromHQ” and “ToHQ” are also created. The former one is used to receive the data from the headquarter and the latter one is for sending data to the headquarter. All these directories will be shown in the page “Overview” of storage. The following is the detailed mapping of the four directories:

Headquarter		Divisions
ToBran-<location>-<prefix>	→	FromHQ
FromBran-<location>-<prefix>	←	ToHQ

The data will be synchronized every few minutes.

---

**Note:**

Data can only be synchronized automatically between the Headquarter and it associated divisions when the link status is “connected”.

---

## 14.5 Shared Services

---

Some specific services can be shared among different UMG-2000 Series systems. Email is now supported. This means that if divisions do not have valid domain names but headquarter does, all users in divisions can use the email service in the headquarter. For example, if the headquarter has a valid Internet domain name “PLANET.com.tw” and its division does not, the user named “demo” with its enabled email service will have an email box whose address is demo@PLANET.com.tw. However, its email address will be changed as the division gets a valid Internet domain name. If the division gets a domain name “sh.PLANET.com.tw”, the user’s email address will be changed to demo@PLANET.com.tw. All this information will be shown on a contract list.

## 14.6 Global user Profile

---

After connection, the profile of the headquarter and its divisions will be synchronized. So far, the contact list synchronization is supported. Anyone who can access the UMG-2000 Series can get the fully detailed contract list which includes all users in the UMG-2000 Series group in user private web administration.

## 14.7 Centralized Configuration management

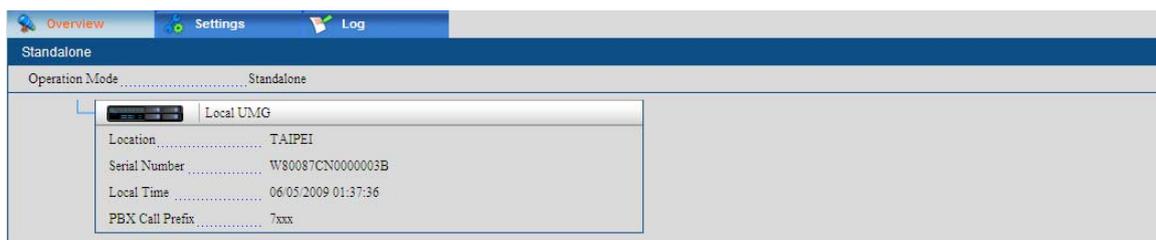
---

Another facility is the centralized configuration platform. It provides the ability for the administrator of the headquarters to manage all the divisions IT resources in his own office. Click the “Web Management on the “Branch-to-Branch Overview” page to access the division administration GUI (Refer to Section - Branch-to-Branch Overview).

## 14.8 Branch-to-Branch Overview

---

The “Branch-to-Branch Overview” page presents the current Branch-to-Branch settings.



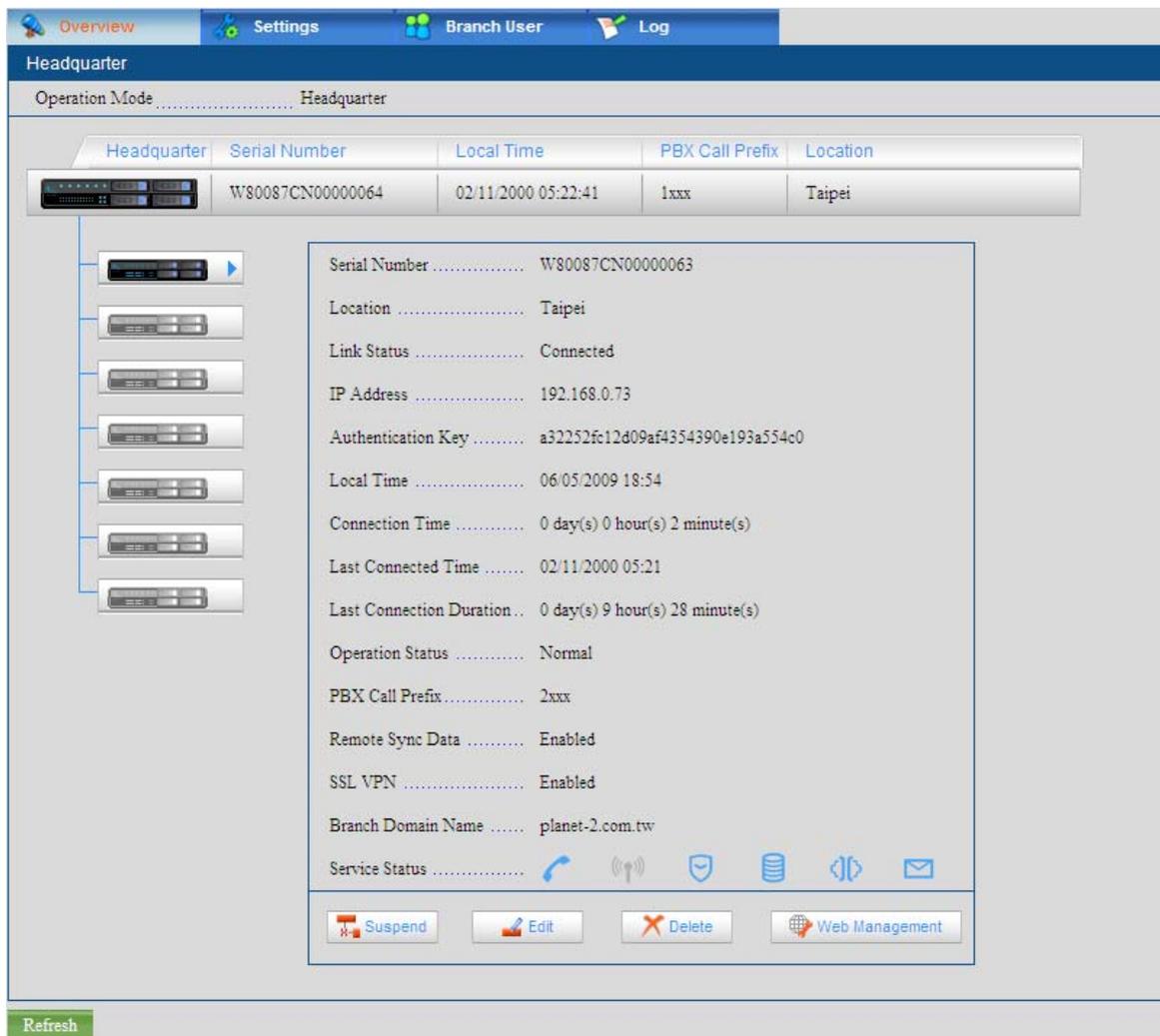
### STANDALONE

**Operation mode:** Displays the current operation mode.

**Serial Number:** Displays the BTB serial number.

**Local Time:** Displays the local time.

**Call Prefix:** Displays the local call prefix.



## HEADQUARTER

**Operation mode:** Displays the current operation mode

**Headquarter Location:** Displays the location of the UMG-2000 Series.

**Headquarter Serial Number:** Displays the BTB serial number.

**Headquarter Local Time:** Displays the local time of the UMG-2000 Series.

**Headquarter Call Prefix:** Displays the call prefix of the UMG-2000 Series.

**Location:** Displays the location of the specific Branch.

**Serial Number:** Displays the BTB serial number of the specific Branch.

**Link Status:** Displays the link status of the specific Branch.

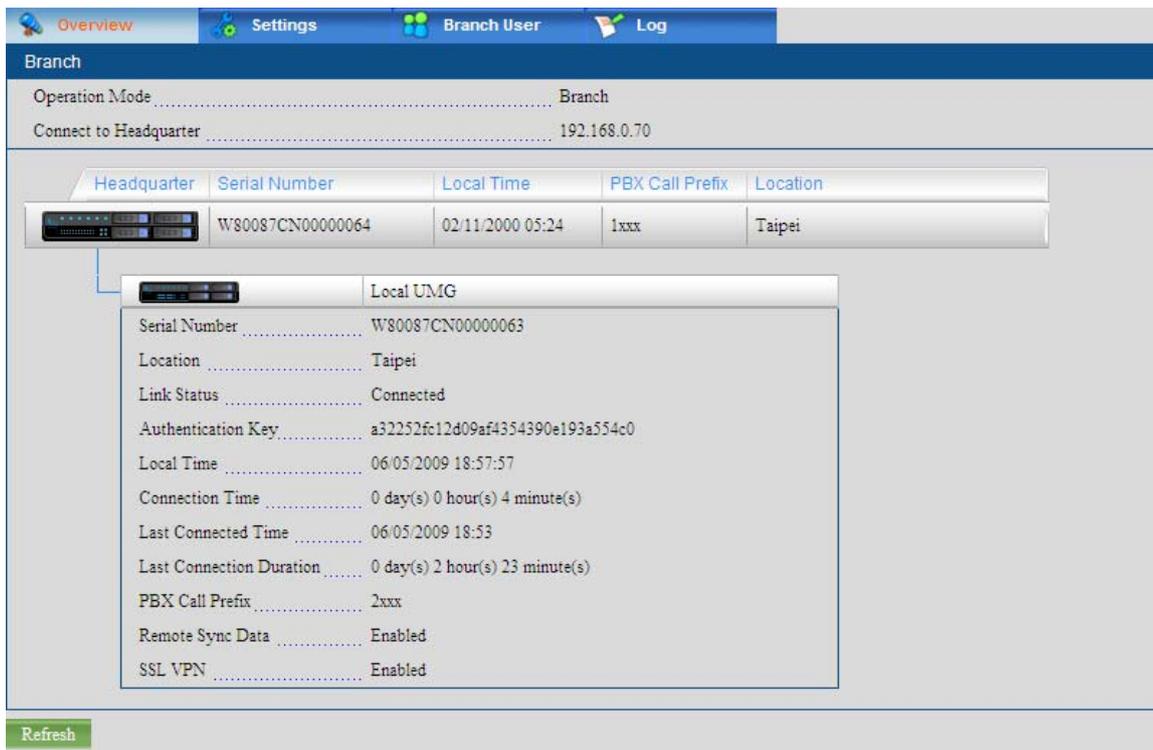
**Key:** Displays the key used to authenticate the specific Branch.

**Local Time:** Displays the local time of the specific Branch.

**Connection Time:** Displays the total connection live time of the specific Branch.

**Call Prefix:** Displays the call prefix of the specific Branch.

**Admin:** Click this button to go to the branch web administration to manage the IT resource of the branch UMG-2000 Series when and only when connected.



## BRANCH

**Operation mode:** Displays the current operation mode

**Connect to Headquarter:** Displays the host/IP address of headquarter UMG-2000 Series.

**Headquarter Location:** Displays the location of the headquarter UMG-2000 Series.

**Headquarter Serial Number:** Displays the BTB serial number of the headquarter.

**Headquarter Local Time:** Displays the local time of the headquarter UMG-2000 Series.

**Headquarter Call Prefix:** Displays the call prefix of the headquarter UMG-2000 Series.

**Location:** Displays the location of the UMG-2000 Series.

**Serial Number:** Displays the BTB serial number.

**Link Status:** Displays the link status of the UMG-2000 Series.

**Key:** Displays the key used to connect to the headquarter UMG-2000 Series.

**Local Time:** Displays the local time of the UMG-2000 Series.

**Connection Time:** Displays the total connection live time of the headquarter UMG-2000 Series.

**Call Prefix:** Displays the call prefix of the UMG-2000 Series.

## 14.9 Delete a Branch

If the mode of your UMG-2000 Series is Headquarter, check the “Delete” check box in the page “Overview” and then click the “Delete” button. The selected branch will then be deleted.

### Note:

Delete a branch will delete the entire branch configuration profile.

## 14.10 Branch-to-Branch Setting

The “Branch-to-Branch Setting” page allows administrator to manage branch to branch. There are three modes of Branch-to-Branch, Headquarter, Division, and Standalone.



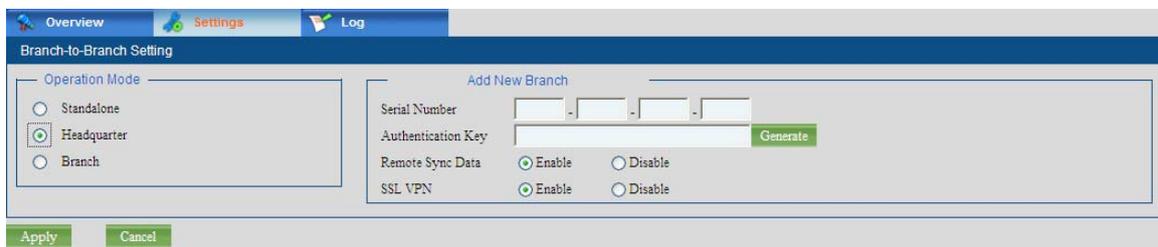
The screenshot shows the 'Branch-to-Branch Setting' page. At the top, there are tabs for 'Overview', 'Settings', and 'Log'. Below the tabs, the page title is 'Branch-to-Branch Setting'. Underneath, there is a section titled 'Operation Mode' with three radio button options: 'Standalone' (which is selected), 'Headquarter', and 'Branch'. At the bottom of the page, there are two buttons: 'Apply' and 'Cancel'.

### OPERATION MODE

**Standalone:** Disables the Branch-to-Branch feature.

**Headquarter:** Specifies the operation mode to Headquarter.

**Division:** Specifies the operation mode to Branch.



The screenshot shows the 'Branch-to-Branch Setting' page with the 'Operation Mode' section on the left and the 'Add New Branch' section on the right. The 'Operation Mode' section has three radio button options: 'Standalone', 'Headquarter' (which is selected), and 'Branch'. The 'Add New Branch' section contains a 'Serial Number' field with a format of '\_\_\_\_-\_\_\_\_-\_\_\_\_-\_\_\_\_', an 'Authentication Key' field with a 'Generate' button, and two sets of radio buttons for 'Remote Sync Data' and 'SSL VPN', each with 'Enable' and 'Disable' options. At the bottom, there are 'Apply' and 'Cancel' buttons.

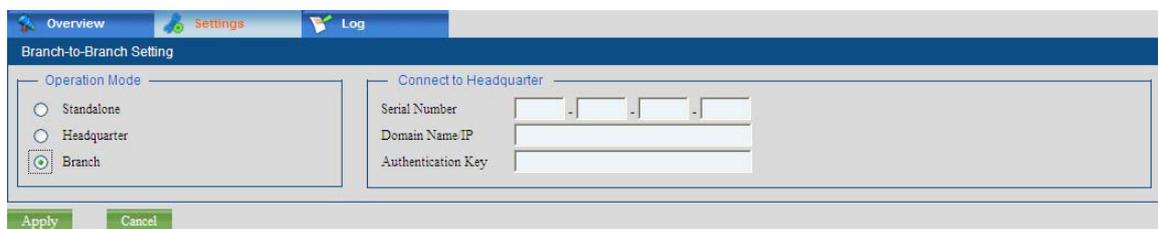
### ADD NEW BRANCH

**Serial Number:** Specifies the BTB serial number of the allowable branch.

**Key:** Generates the key that will be used as the authentication password when building the connection between the UMG-2000 Series and the branch.

**Call Prefix:** Specifies the call prefix of the branch.

**Remote Sync Data:** Enables or disables the feature “Synchronize data” between the UMG-2000 Series and the branch.



The screenshot shows the 'Branch-to-Branch Setting' page with the 'Operation Mode' section on the left and the 'Connect to Headquarter' section on the right. The 'Operation Mode' section has three radio button options: 'Standalone', 'Headquarter', and 'Branch' (which is selected). The 'Connect to Headquarter' section contains a 'Serial Number' field with a format of '\_\_\_\_-\_\_\_\_-\_\_\_\_-\_\_\_\_', a 'Domain Name IP' field, and an 'Authentication Key' field. At the bottom, there are 'Apply' and 'Cancel' buttons.

### CONNECT TO HEADQUARTER

**Serial Number:** Specifies the BTB serial number of the headquarter you want to connect.

**Domain Name/IP:** Specifies the host or IP address of the headquarter you want to access.

**Key:** Specifies the key that the headquarter has provided as the authentication password for the branch.

## 14.11 Branch Users

This section shows all the user contact information in different branches.



The screenshot shows a web interface with a navigation bar containing 'Overview', 'Settings', 'Branch User', and 'Log'. The 'Branch User' tab is active. Below the navigation bar is a 'Contact List' table with 7 columns: Username, Fullname, Extension, Call Privilege, Department, Location, and Email Address. The table contains 15 rows of user data. A 'Refresh' button is located at the bottom left of the table area.

Username	Fullname	Extension	Call Privilege	Department	Location	Email Address
alex	Alex Tien	1101	Local	ENM	Taipei	alex@planet-1.com.tw
allen	Allen Huang	1100	National	ENM	Taipei	allen@planet-1.com.tw
allenh	Allen	2001	International	administrator	Taipei	allenh@planet-2.com.tw
amy	Amy Lee	1701	Local	RMA	Taipei	amy@planet-1.com.tw
chloe	Chloe Hsu	1500	National	MKT	Taipei	chloe@planet-1.com.tw
dennis	Dennis Huang	1200	National	RDM	Taipei	dennis@planet-1.com.tw
higgins	James Higgins	1111	Operator	President	Taipei	higgins@planet-1.com.tw
james	James Yan G	1102	Local	ENM	Taipei	james@planet-1.com.tw
jesmine	Jesmine Chang	1400	National	ADM	Taipei	jesmine@planet-1.com.tw
justin	Justin Liu	1202	Local	RDM	Taipei	justin@planet-1.com.tw
karen	Karen Tsai	1601	Local	PRD	Taipei	karen@planet-1.com.tw
kim	Kim Huang	1401	Local	ADM	Taipei	kim@planet-1.com.tw
lana	Lana Chen	1700	National	RMA	Taipei	lana@planet-1.com.tw
lidia	Lidia Sung	1300	National	SAM	Taipei	lidia@planet-1.com.tw
lory	Lory Lee	1501	Local	MKT	Taipei	lory@planet-1.com.tw

## 14.12 Branch-to-Branch Log

The branch-to-branch log shows the branch-to-branch history.



The screenshot shows a web interface with a navigation bar containing 'Overview', 'Settings', and 'Log'. The 'Log' tab is active. Below the navigation bar is an 'Events' table with 3 columns: Date, Time, and Description. The table is currently empty, showing 'No entry'. A 'Refresh' button is located at the bottom left of the table area.

Date	Time	Description
No entry		

### EVENTS

**Date:** Displays the date of the event.

**Time:** Displays the time of the event.

**Description:** Displays the detailed description of the event.

## 15. Web Management - Maintenance

The UMG-2000 Series maintenance suit includes the following services: configure backup/restore, software update, diagnose, and remote support request.

### BACKUP/RESTORE CONFIGURE

The UMG-2000 Series provides the ability to backup the configuration in case of losing the configuration when abnormal events occur. Users can backup the current configuration to their own PC, file server etc., and avoid monotonous reconfiguration. It is possible for the administrator to restore the configuration to an older one if some mishandling has occurred.

### UPDATE

The UMG-2000 Series provides to update to the latest software. The administrator should download the latest software image from <http://www.PLANET.com.tw> and start the update process manually.

### DIAGNOSE

The UMG-2000 Series provides the mechanism of self diagnostic. The diagnostic includes: memory test, Wireless test, PBX test, flash memory test, USB port test, storage RAID testing, Real-time clock test, network test, and LED test. If one or more test fail, please replace the faulty product or contact your product provider.

### REMOTE SERVICE

If your UMG-2000 Series does not work normally, please contact your product provider. However, you can also choose the remote service. Request the remote service and provide a temporary login ID and password from an PLANET support engineer by sending an email with the description of the problem and the authorized access permission.

## 15.1 System

The "System" page allows the administrator to backup or restore the configuration.



### CONFIGURATION

**Backup Configuration:** Backs up the current configuration to your PC.

**Restore Configuration From Selected File:** Restores the configuration to the user's specified file.

**Restore To Default:** Restores the configuration to default.

**System Reboot:** Reboots the UMG-2000 Series.

**Shut Down:** Shuts down the UMG-2000 Series.

**Restore To Manufacture Default:** Restores the UMG-2000 Series to manufacture default. This will restore all configurations to default and clear all data in the disks. You must backup the configuration and important data first.

## 15.2 Software Update

---

The “Software Update” page allows the administrator to update the software to the latest version.



### SOFTWARE UPDATE

**Select Software Image:** Selects the update image file on your PC or file server.

**Uploaded Version Number:** Displays the uploaded software version.

Download the latest image file to your PC. Select the software image that you want to update on your PC and then click “Apply” to update.

## 15.3 Diagnose

---

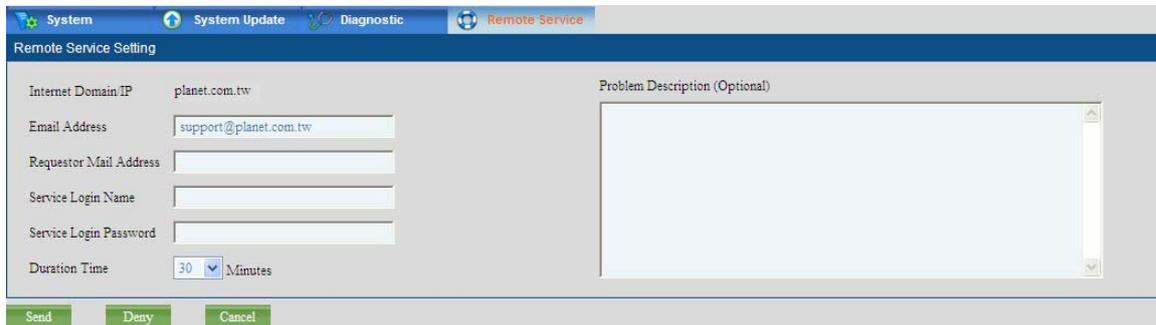
The page “Diagnose” allows the administrator to test hardware. The diagnostic report will be shown after the testing.



## 15.4 Remote Service

---

The page “Remote Service” allows the administrator to report problems and get online help.



The screenshot shows a web interface titled "Remote Service Setting" with a navigation bar at the top containing "System", "System Update", "Diagnostic", and "Remote Service". The main content area includes several input fields: "Internet Domain/IP" (pre-filled with "planet.com.tw"), "Email Address" (pre-filled with "support@planet.com.tw"), "Requestor Mail Address", "Service Login Name", "Service Login Password", and "Duration Time" (a dropdown menu set to "30" with "Minutes" next to it). To the right of these fields is a large text area labeled "Problem Description (Optional)". At the bottom of the form are three buttons: "Send", "Deny", and "Cancel".

**Internet Domain/IP:** Displays the Host/IP of the UMG-2000 Series.

**Email Address:** Specifies the address that the email will be sent to. By default, the email will be sent to support@planet.com.tw. You can also send the email to your own product provider.

**Requestor Mail Address:** Specifies requester’s email address.

**Service Login Name:** Specifies the username to login to your GUI and access your UMG-2000 Series via PPTP VPN. The username and password will be sent to the former email address.

**Service Login Password:** Specifies the password corresponding to the user account.

**Duration Time:** Specifies the MAX duration time of connection. PLANET support engineers cannot access the UMG-2000 Series if this time expires.

**Problem Description (Optional):** A brief description to the problem. It will help the email receiver locate and solve the problem more quickly.

## 16. Personal Account Web Administration

The personal account web administration is a very important concept of the user-based and centralized service for the UMG-2000 Series and allows every user to be his own administrator. Once an active user account is added to UMG-2000 Series, the user can login to the personal account web administration. After login, the user can update his or her profile, view the contact list and the UMG-2000 Series tutorial, etc

### UPDATE THE USER PROFILE

The UMG-2000 Series provides every user a simple platform to manage his or her personal profile and private information. Some are invisible to the administrator. It is convenient for users to update the profile in their own way. However, for the sake of security, the service privilege can only be assigned by the administrator.

### CONTRACT LIST

Based on all the user's profiles, a detailed contact list will be presented, including the user's email address and extension. All branch users will be presented here if the feature "Branch to Branch" is enabled. Refer to Section - Profile in One to get further information.

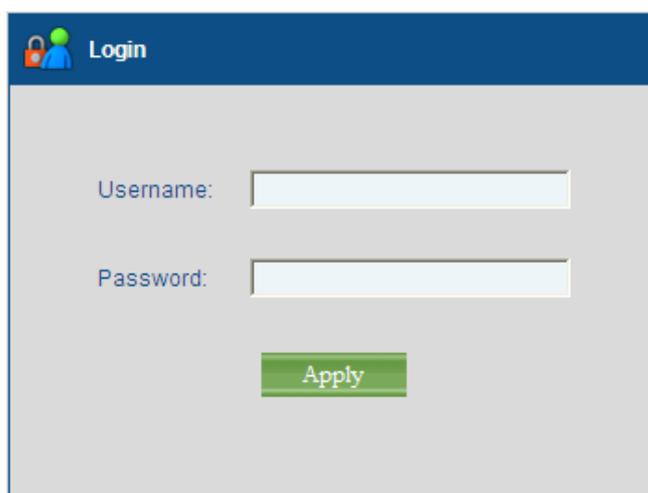
### UMG-2000 Series TUTORIAL

The UMG-2000 Series provides some basic tutorials to help users learn how to use the features. The call reference is presented to give instructions to the call features. We will also put other tutorials on the web administration gradually.

## 16.1 User Login

---

Any user who wants to access the UMG-2000 Series web management must login here. Type an authorized username and password and then login.



The image shows a web login interface. At the top, there is a blue header bar containing a lock icon and the text "Login". Below this, the main content area is light gray. It features two text input fields: the first is labeled "Username:" and the second is labeled "Password:". Below the password field is a green rectangular button with the text "Apply" in white.

---

### Note:

The user login session will be automatically terminated for security reason, If no action is taken in 5 minutes.

---

## 16.2 User Home Page

The page “My Account” shows the user profile.

The screenshot displays the PLANET Unified Office Gateway user profile page. The page is titled "My Account" and shows the user profile for "admin". The page is divided into several sections:

- Account Information:** Username: admin, Fullname: admin, Department: admin, Account Status: Active.
- Service Privilege:** Email: Disabled, PPTP VPN: Disabled, Email Address: N/A.
- Network Storage:** Private Capacity: Enabled, Storage Quota: 0 GB, Storage Used: N/A.
- PBX:** Call Privilege: Disabled, Extension Number: N/A, Voice Mail Password: N/A, Forward Calls On Busy to: N/A, Forward Calls no answer to: N/A, Do Not Disturb: Disabled, Forward All Calls to: N/A, Personal Greeting: Disabled, Send Voicemail to Email: Disabled, Registration State: N/A.
- Wireless:** Access Point(AP): Disabled, Hide SSID: Disabled, Network Name(SSID): UMG\_WIFI, Wireless Mode: 802.11b/g, Wireless Region: USA, Channel: 1, Authentication Type: Open System, Link Speed: 11/54Mbps, Data Encryption: None.

### ACCOUNT INFORMATION

This section lists the current user account settings.

**Username:** Displays the username.

**Fullname:** Displays the full name.

**Department:** Displays the department/group that the user belongs to.

**Account Status:** Displays the state of this account, active or suspend.

### SERVICE PRIVILEGE

This section lists the current service privileges of this user.

**Email:** Displays the state of the email service, enabled or disabled.

**PPTP VPN:** Displays the state of the PPTP VPN service, enabled or disabled.

### NETWORK STORAGE

This section lists the current network storage usage and status of the user.

**Private Capacity:** Displays the private capacity.

**Storage Quota:** Displays the storage quota.

**Storage Used:** Displays the storage size that has been used.

### VOIP

This section lists the VoIP settings of this user.

**Call Privilege:** Displays the call privilege of the user.

**Extension Number:** Displays the VoIP phone number.

**Voice Mail Password:** Displays the password to access voice mail.

**Do Not Disturb:** Displays the state of the feature “Do Not Disturb”, enable or disable.

**Forward All Calls to:** Displays the unconditional forward extension.

**Forward Calls on Busy to:** Displays the extension which your call will be forwarded to when your line is busy.

## 16.3 Access to Administrator

---

If your account is the administrator, there will be an “Admin” button on the left. Click that button to access the UMG-2000 Series web management.

---

### Note:

Only one system administrator login session is allowed at any time.

---

## 16.4 Personal Setting

---

Users can update the profile in their own way on the “Personal Setting” page.

The screenshot shows the 'Basic Setting' page with the following details:

- User Account:** Username: admin, Fullname: admin, New Password: [masked], Confirm Password: [masked].
- Call Setting:** Voice Mail Password: [text box], Forward All Calls to: [text box], Forward Calls On Busy to: [text box], Forward Calls no answer to: [text box], Do Not Disturb:  Enable,  Disable, Send Voicemail to Email:  Enable,  Disable, Personal Greeting:  Enable,  Disable.
- Email Setting:** Auto Reply:  Enable,  Disable. Auto Reply Message:  Maximum:512 Characters.

### USER ACCOUNT

**Username:** Displays your account username.

**Full Name:** Specifies your full name.

**New Password:** Specifies your new password.

**Confirm Password:** Confirms and verifies the typed password.

### CALL SETTING

**Voice Mail Password:** Specifies your voice mail password.

**Forward All Call to:** Specifies the unconditional forward extension. Fill the text fill only if you would like to forward all your calls to the extension.

**Forward Calls on Busy to:** Specifies the forward extension. Fill the text fill if you would like to forward your calls to the extension when your line is busy.

**Do Not Disturb:** Enable or disable the “Do Not Disturb” feature. Enable this feature only if you would like to prevent ringing of incoming calls.

## EMAIL SETTING

**Auto Reply:** Enable or disable the feature “Email Auto Reply”. Enable it if you would like to make the email server automatically reply to the emails that you receive.

**Auto Reply Message:** Specifies the auto reply message.

## 16.5 Contract List

---

All users with their extensions and email addresses in the UMG-2000 Series will be listed in the page “Contact List”.

Contact List							1 / 1
Username ▲	Fullname ▲	Extension ▲	Call Privilege ▲	Department ▲	Location ▲	Email Address ▲	
alex	Alex	7001	Local	ENM	TAIPEI	alex@yang92.cn	
allen	Allen	7000	Local	ENM	TAIPEI	allen@yang92.cn	
james	James	7002	Local	ENM	TAIPEI	james@yang92.cn	

Refresh

## CONTACT LIST

**Username:** Displays a username.

**Full Name:** Displays the full name of the user.

**Extension:** Displays the extension of the user.

**Department:** Displays the department/group the user belongs to.

**Location:** Displays the location of this user.

**Email Address:** Displays the Email address of the user.

## 16.6 Personal Call Records

---

The “Call Records” page shows the call records of the user.

Call Records				1 / 1
Time ▼	Caller ▼	Answer ▼	Duration ▼	
No entry				

Please refer to Section - IP PBX Call Records.

## 16.7 Call Reference

Users can get the call reference from the page “Call Reference”.

Call Reference			
Dial External	9	Call Transfer	#
Dial Operator	0	Attendant Transfer	* - 2 - Flash
Retrieve Voice Mail	* - 9 - 8	Call Pickup	* - 8 - Ext.
Conference	* - 1 - 2 - 3 - 4	Group Pickup	* - 8 - #
Record Personal Greeting	* - 9 - 7	Enable No Answer Forwarding	* - 9 - 2 - Ext.
Personal Greeting Menu	* - 9 - 6	Disable No Answer Forwarding	* - 9 - 3
Enable Busy Forwarding	* - 9 - 0 - Ext.	Enable Do Not Disturb	* - 7 - 8
Disable Busy Forwarding	* - 9 - 1	Disable Do Not Disturb	* - 7 - 9
Call Parking	7 - 0 - 0	Enable Unconditional Forwarding	* - 7 - 2 - Ext.
Retrieve Parked Call	7 - 0 - 1 ~ 7 - 0 - 5	Disable Unconditional Forwarding	* - 7 - 3

IAX2 Trunk Outbound Call Rule List (Autoconfig Between Branches)			
Branch Location	Remote Outbound Dialing Prefix	Branch Location	Remote Outbound Dialing Prefix

Please refer to Section - IP PBX Call Reference.

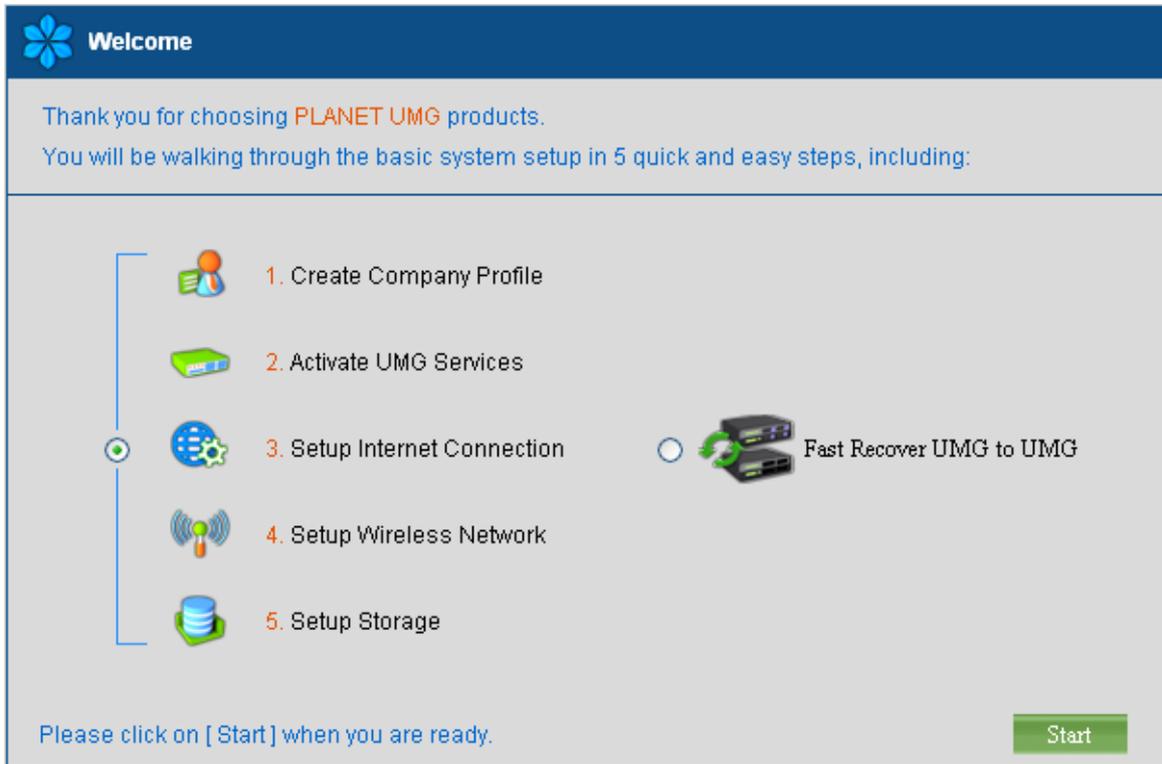
## 16.8 Logout

Click the button “sign out” in the right top corner or close the browser to logout the current session. If no action has been taken in 5 minutes, the session will be logout automatically.

# Appendix A - Fast Recovery

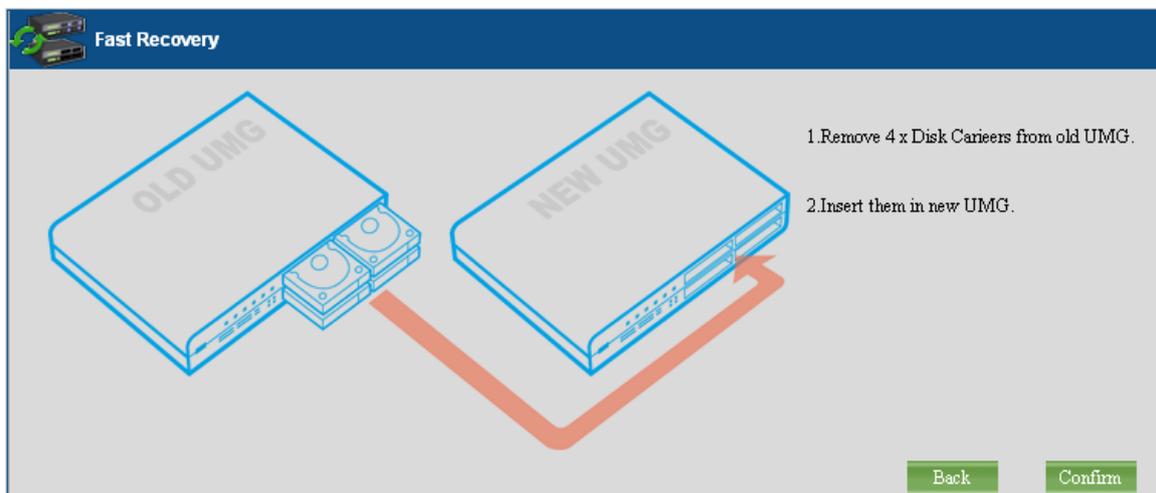
## Welcome to Fast Recovery

After logging in, the welcome page appears again. Please select the “Fast Recovery UMG to UMG” and click the “Start” button to continue.

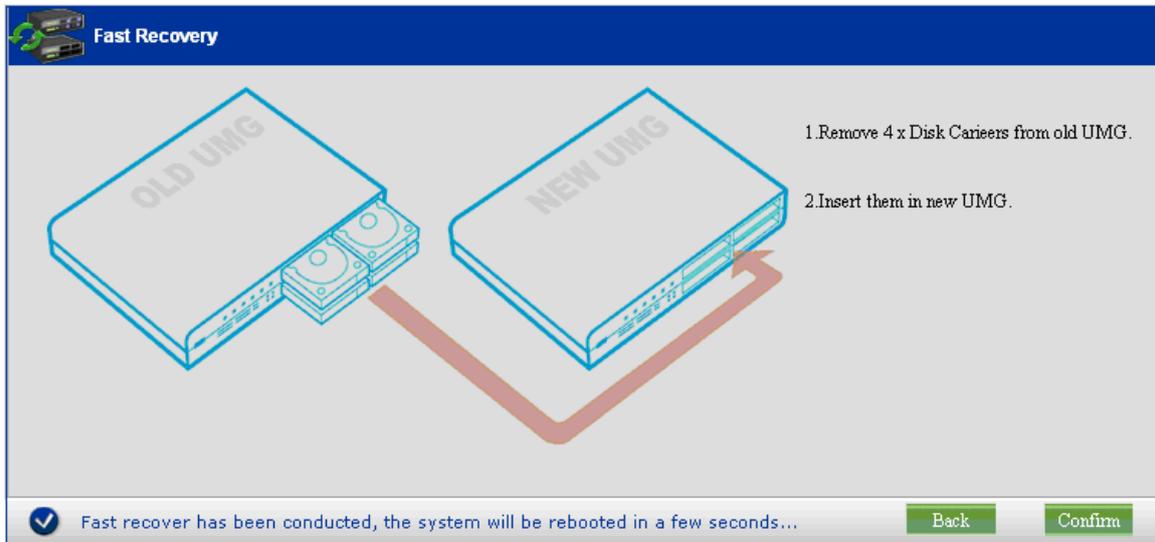


## Fast Recovery

Insert the four disks that you removed from the faulty UMG-2000 Series into the new system. Click the “Confirm” button and the rebuilding will be implemented. Please do not close the browser and wait patiently for the results.



If the following screen appears, it means the fast recovery has completed successfully. Otherwise, check the devices. After the rebuilding, the UMG-2000 Series will reboot automatically. Then the new UMG can serve normally.



## Appendix B - Hard Disk Hot Plug

The UMG-2000 Series supports the SATA hot plug. The hot plug allows the administrator to replace the faulty device with a new one with the same model at the running time rather than rebooting the system.

### Before Unplug

---

If one of the SATA devices is faulty, the panel will show the faulty device by alerting the administrator with a corresponding SATA LED red. The next figure shows the mapping of the four devices and their LED. The administrator can also get the exact indication in the page "System Overview". Before unplugging the faulty device, make sure of the model and the raw capacity of the device. We strongly recommend that the device with the same model should be chosen to replace the faulty one. If it is impossible, get the device which has a larger raw capacity.



---

**Note:**

Make sure the storage RAID configuration is RAID5 or RAID 0/1.

---

### Unplug Disk

---

When unplugging the faulty device, do NOT unplug/plug any disks when rebooting. The alert LED will flash if any one disk is unplugged and do NOT take any actions while the alert LED is flashing. After a short period of time, the alert LED will be turned off and you can take the next step. If the alert LED does not flash, plug in the new one and reboot.

---

**Note:**

Make sure you unplug the correct damaged-hard disk. The damaged hard disk can be found by observing the UMG front panel disk LED. A Flushing RED led indicates the faulty disk.

---

### Insert a New Disk (Hot-Plug)

---

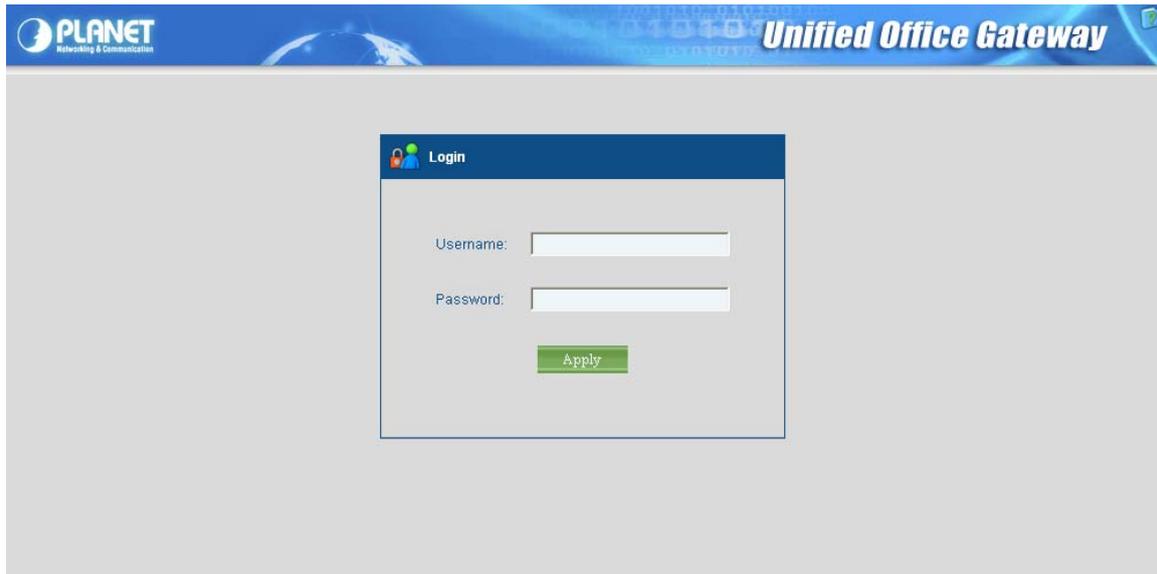
After the alert LED is turned off, you can plug in the new hard disk. Then the alert LED will flash again. Please do not insert or remove any disks while the LED is flashing. After plugging the new devices into the disk bay, the RAID will rebuilt corrupted data automatically. The data repair duration may be vary depend upon the size of the storage disk. For example, the hard disk capacity of 160GBytes may take 45 minutes to repair; while the hard disk capacity of 1TBytes will take approximately 8 hours to repair the damaged data.

## Appendix C - Remote Access

The UMG-2000 Series supports remote access. Administrator can access the web management remotely via secure HTTPS.

From remote PC, launch a web browser (for example: IE, Firefox etc.) and type "<https://ipaddress>" in the address bar of browser.

Type in an authorized username and password and then click the button "Apply". The default username is "[admin](#)", and its password is "[admin](#)" all in small case.



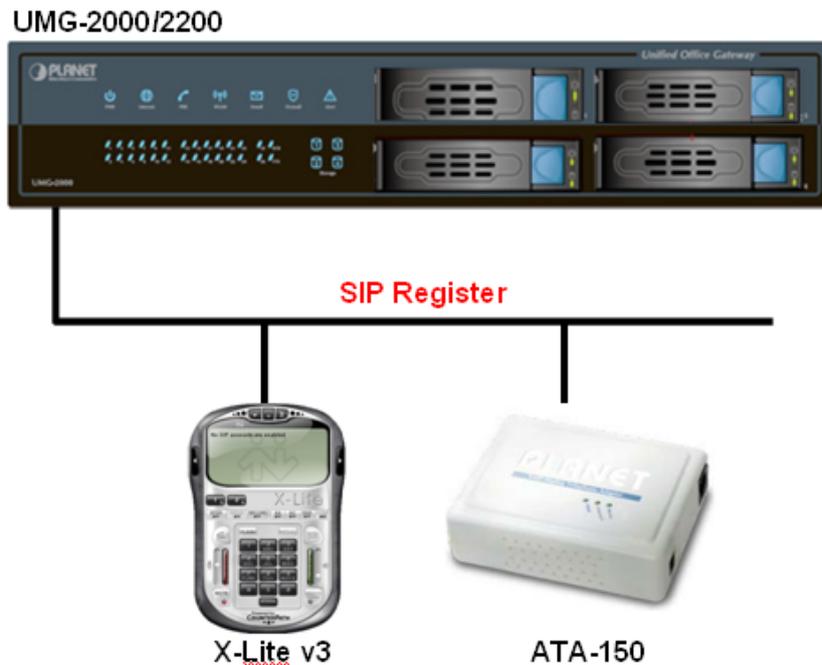
The screenshot shows the login interface for the Planet Unified Office Gateway. At the top, there is a blue header with the Planet logo on the left and the text "Unified Office Gateway" on the right. Below the header, the main content area is light gray. In the center, there is a white login box with a blue header that says "Login" next to a user icon. Inside the box, there are two input fields: "Username:" and "Password:". Below these fields is a green button labeled "Apply".

## Appendix D – Scenario Example

The chapter shows you the concept and command to help you configure your UMG-2000 Series through sample configuration. And provide several ways to make calls to desired destination in UMG-2000 Series. In this section, we'll lead you step by step to establish your first voice communication via web browsers operations.

### Case 1\_X-Lite how to register on the UMG-2000 Series.

---



#### \*\*\* FW & Utility version List:

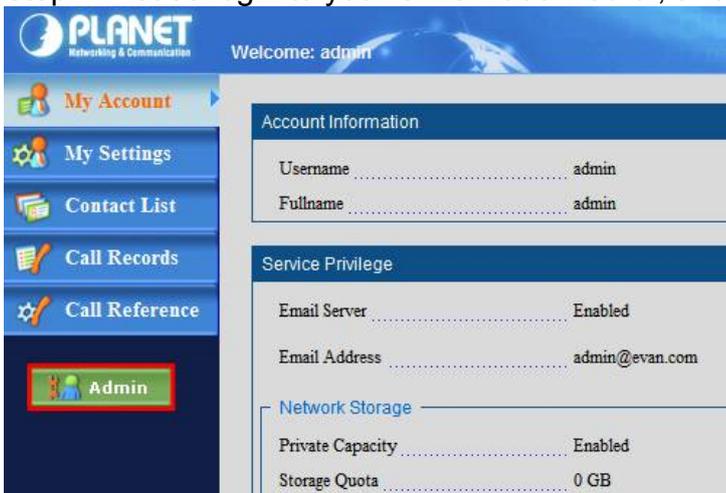
UMG-2000:v.3.6.4

ATA-150:v1.1

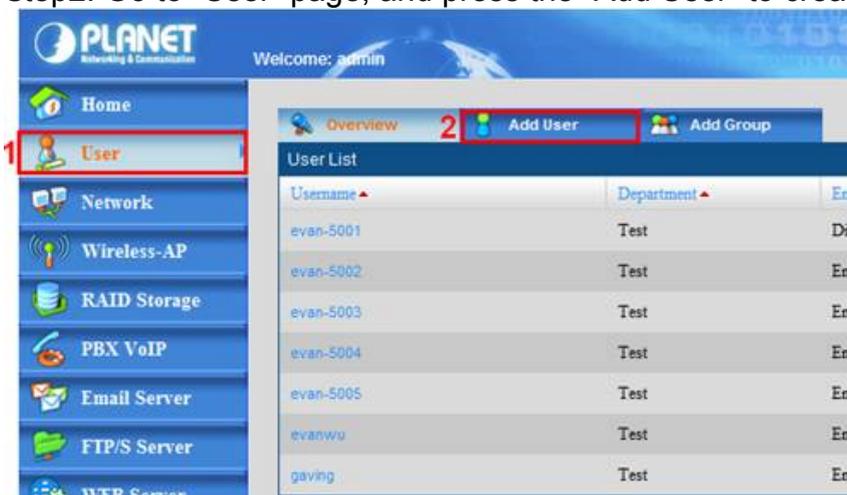
X-Lite:v3.0 build 56125

### \*\*\* Create your UMG-2000 user account:

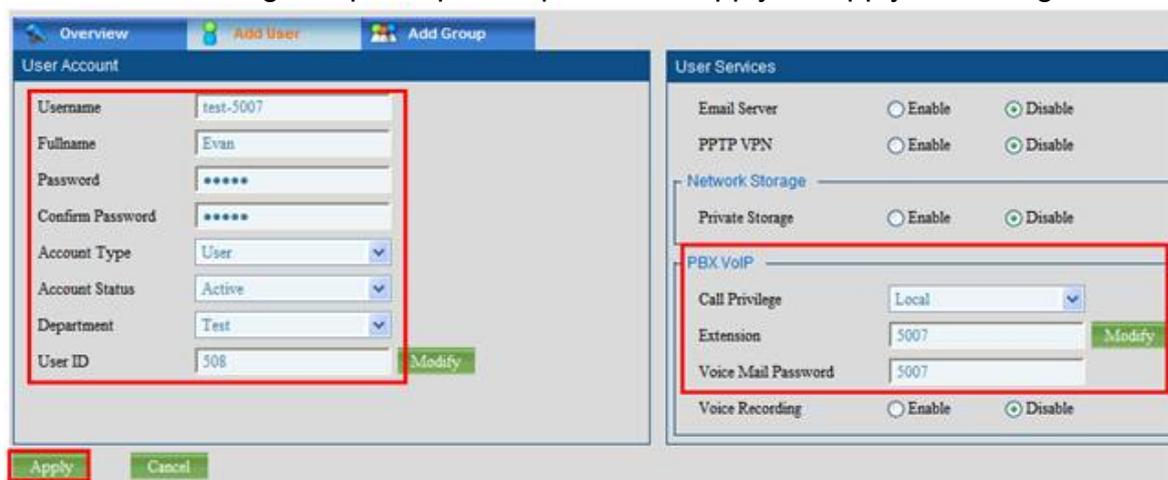
Step1. Please login to your UMG-2000 web-ui, and press the “Admin” button.



Step2. Go to “User” page, and press the “Add User” to create the user account.



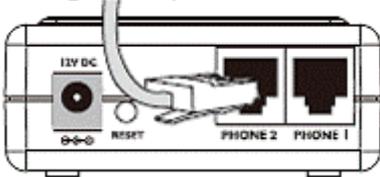
Step3. Input the Username, password..., and modify the “Extension” number you want.  
After setting complete, please press the “Apply” to apply the configure.



### \*\*\* Use ATA-150 to register to UMG-2000 :

#### Step1. Connecting Telephone:

Using a telephone cable, connect your telephone to the Phone port of the Phone Adapter.

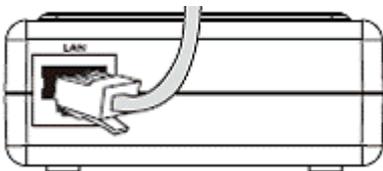


#### Step2. Connecting Network and Power AC Power:

Connect the included Ethernet network cable to the LAN port of the Phone Adapter.

Connect the included power adapter to the POWER port of the Phone Adapter.

The PWR, LNK/ACT, and RING LEDs will be solidly lit when the Phone Adapter is ready for use.



#### Step3. Basic Configuration & Administration Interface:

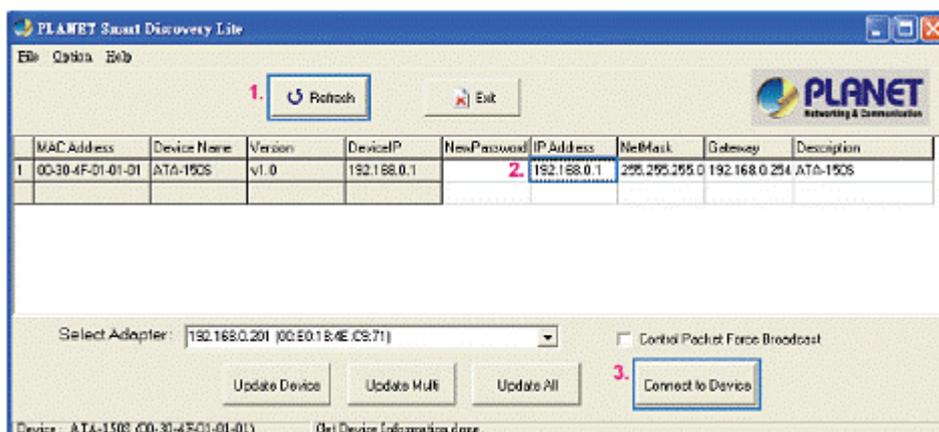
Using for soft utility to search SIP ATA from current network.

The utility not only easy-to-use and provides user more convenience for configuration access.

At the some time if you forget this IP address can also found that via the utility.

Please download the “SmartDiscoveryLite\_v10.rar” at our FTP Server:

[ftp://surve\\_quest:7194@ftp.planet.com.tw/SmartDiscoveryLite\\_v10.rar](ftp://surve_quest:7194@ftp.planet.com.tw/SmartDiscoveryLite_v10.rar)

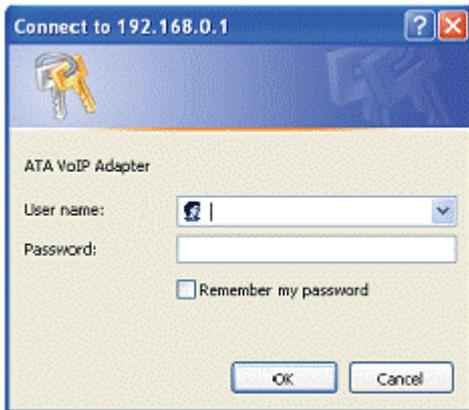


To press “**Refresh**” the button to show out the SIP ATA, then click IP Address item and press the “**Connect to Device**” button.

#### Step4. Login to your ATA-150 Web-UI :

You will connect to SIP ATA via your web browser automatically.

ATA will prompt for logon **username/ password**, please enter: **admin / 123** to continue machine administration.



\*The default IP address of ATA is 192.168.0.1.

You also could open your web browser, and insert http://192.168.0.1 in the address bar on your web browser to logon ATA web configuration page.

### Step5. Configure the ATA-150 to register on UMG-2000 :

- (1) Press the “SIP Setting”.
- (2) Press the “General” to open VoIP General Settings page.
- (3) Press the “Service Domain” button.
- (4) Display Name : Input the name you want.  
 .Line Number : Input the UMG-2000 Extension number, Ex. 5007  
 .Register Name : Same as the UMG-2000 Extension number, Ex. 5007  
 .Register Password : Same as the UMG-2000 Extension number, Ex. 5007  
 .Proxy : Tick the Enable  
 .Proxy Server : Input your UMG-2000 IP Address.
- (5) Press the “Apply All” to apply the setting, then if success to register on UMG-2000. The “Register Status” will show the “Registered”.



Also, you can see the UMG-2000 Web-UI “PBX VoIP” page, there is show the 5007 Extension is work and Registered.

Company: PLA

Call Features

PBX Service	Enabled	Conference Recording	Enabled
Call Forwarding	Enabled	Voice Recording	Enabled
Call Pickup	Enabled	Call Parking	Enabled
Do Not Disturb	Disabled	PBX Call Prefix	SXXX
Fax To Email Address	evanwu@210.66.155.75		

User PBX Extension List

Extension	Username	P.W Privilege	Calling State	Registration State	IP Address	Voice Res
5000	evanwu	Local	Free	Unregistered	N/A	Enabled
5001	evan-5001	Local	Free	Registered	192.168.0.183	Enabled
5002	evan-5002	Local	Free	Registered	192.168.0.168	Enabled
5003	evan-5003	Local	Free	Unregistered	N/A	Enabled
5004	evan-5004	Local	Free	Unregistered	N/A	Enabled
5005	evan-5005	Local	Free	Unregistered	N/A	Enabled
5006	gaving	Local	Free	Unregistered	N/A	Disabled
5007	test-5007	Local	Free	Registered	192.168.0.3	Enabled

**\*\*\* Use X-Lite to register to UMG-2000 :**

**Step1.** Please download the X-Lite at X-Lite office web-page :  
<http://www.counterpath.com/x-lite.html>

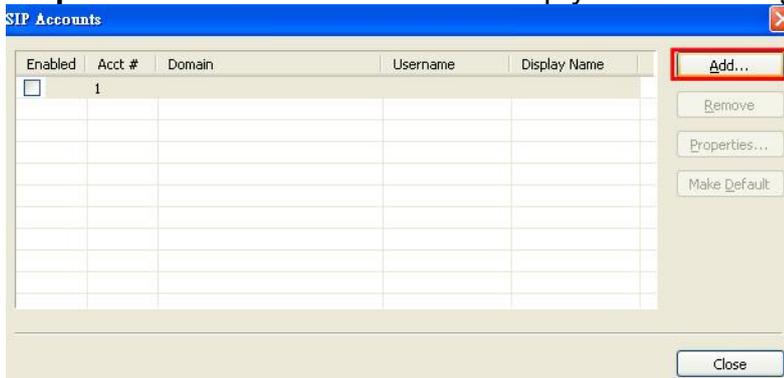
**Step2.** After download and install complete, please open the X-Lite software.



**Step3.** Click the “Show Menu” button, and select the “SIP Account Settings” to setup your SIP Account.

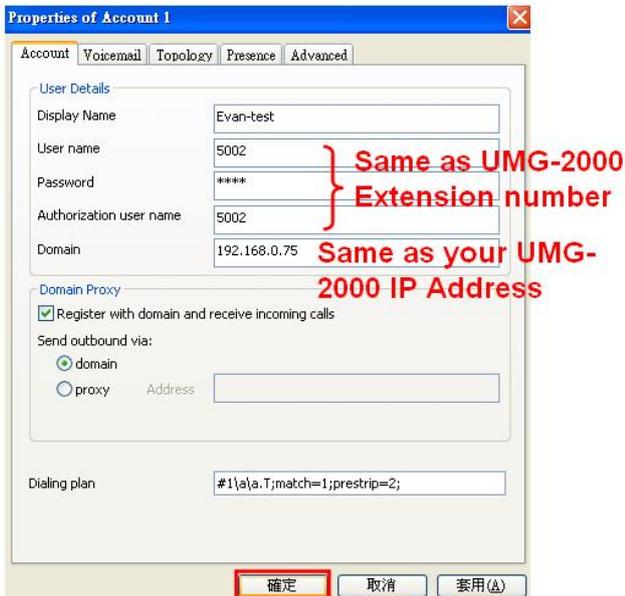


**Step4.** Press the “Add” button to setup your SIP setting.



**Step5.** Input the setting and press the “OK” button to apply the setting.

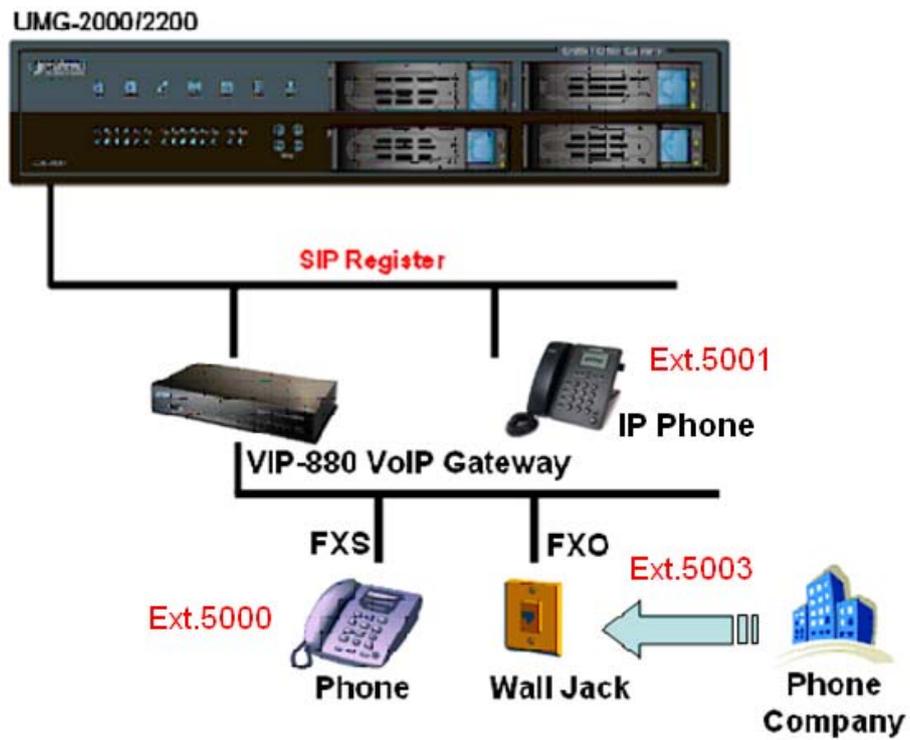
\*The Username and Password same as the UMG-2000 Extension number. Ex.5002



**Step6.** After setting complete, you will see the “Ready” on the X-Lite Screen. And you can use it now.



## Case 2\_ VIP-880 VoIP Gateway how to register on the UMG-2000 Series.



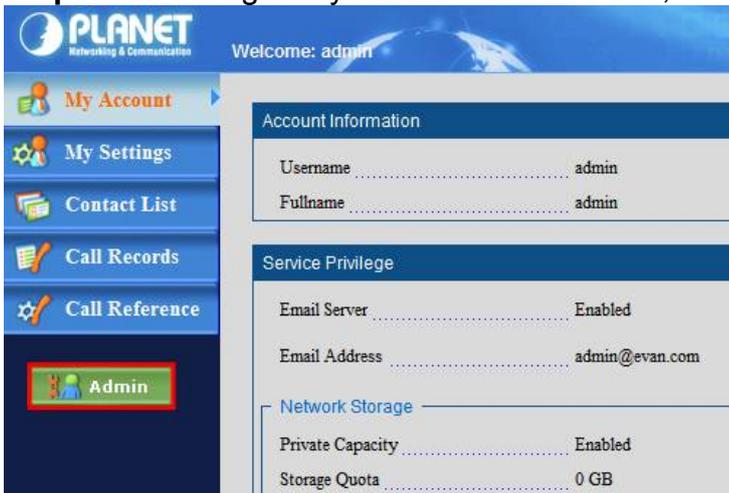
### \*\*\* FW & Utility version List:

UMG-2000:v.3.6.5

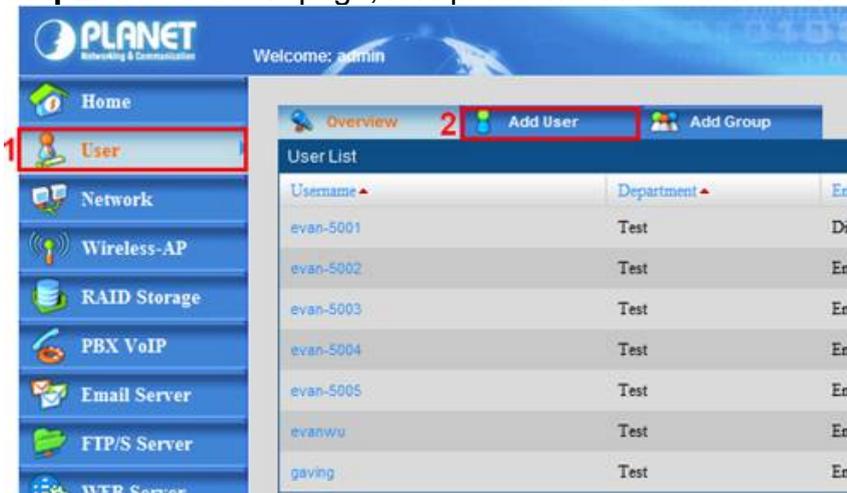
VIP-880 : 2.9.9

### \*\*\* Create your UMG-2000 user account :

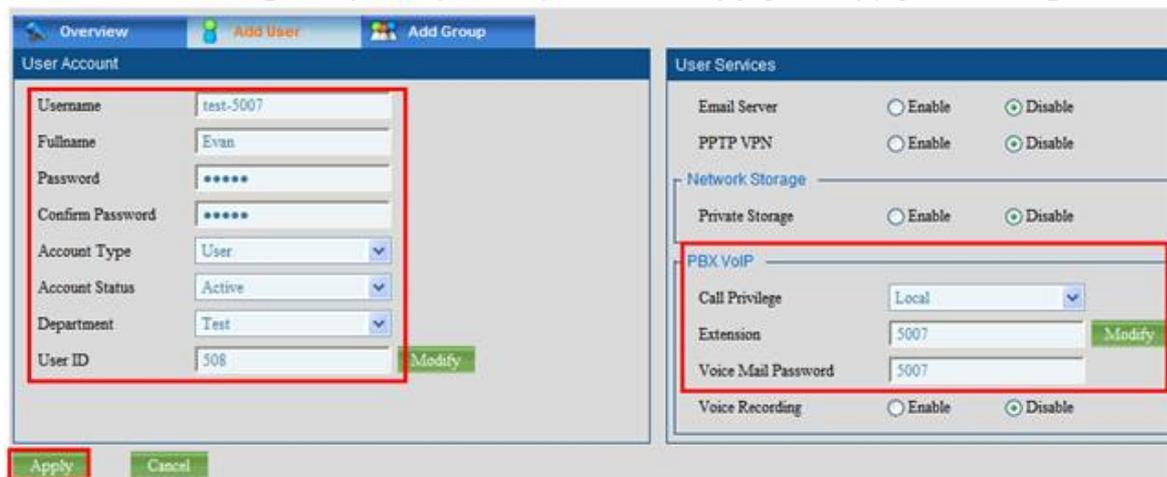
**Step1.** Please login to your UMG-2000 web-ui, and press the “Admin” button.



**Step2.** Go to “User” page, and press the “Add User” to create the user account.



**Step3.** Input the Username, password..., and modify the “Extension” number you want. After setting complete, please press the “Apply” to apply the configure.



**\*\*\* Use VIP-880 to register to UMG-2000 :**

**Step1. Configuration VoIP Setting register to UMG-2000 :**

- (1) Go to “**VoIP Basic**” page, and “**VoIP Protocol Setting**” select “**SIP**”.
- (2) Choose the FXS/FXO Port you want to register to UMG-2000.  
Key-in the UMG-2000 extension number and password.  
(the default extension password same as extension number)

Example. We used the **FXS/Port 5** to register to UMG-2000 “**5000**” extension number.  
We used the **FXO/Port 6** to register to UMG-2000 “**5003**” extension number.



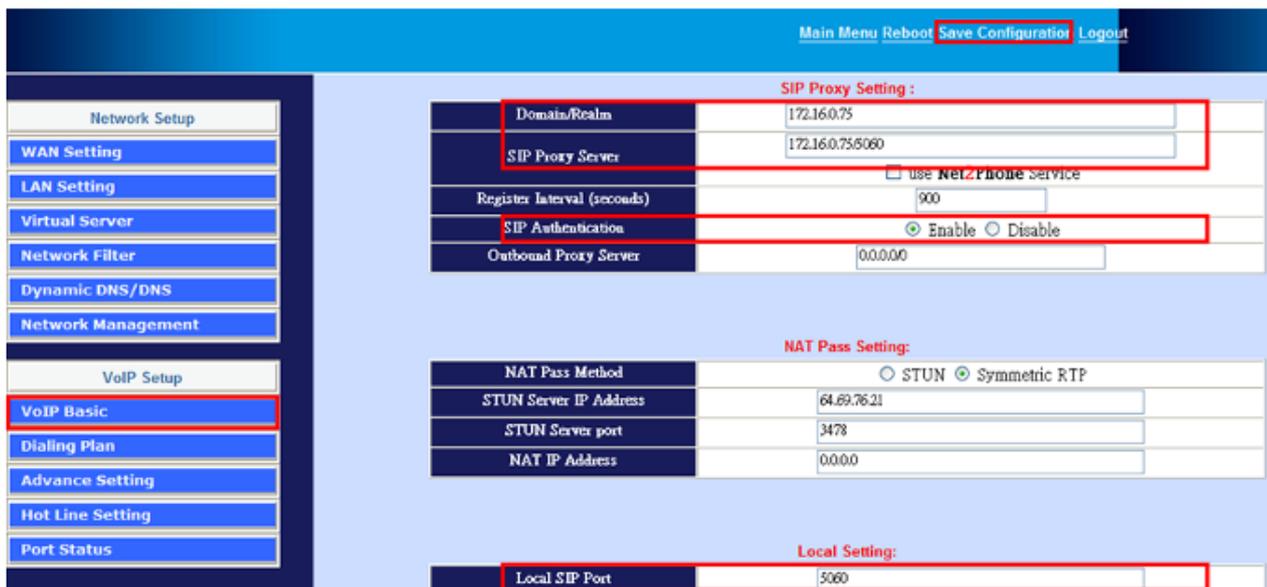
(3)Go to the below of page, please key-in your UMG-2000 IP-Address for connect to SIP Server.

Domain/Realm : UMG-2000 IP-Address or Domain name.

Sip Proxy Server : UMG-2000 IP-Address

SIP Authentication : Select “Enable”

Local SIP Port : 5060



When setting is complete, please press the “**Apply**” button on the below of page, then click the “**Save Configuration**” on the above of page to save setting.

If your setting is correct, you will see the “Register” information at UMG-2000.

The screenshot shows the PBX VoIP configuration interface. The 'Overview' tab is selected. The 'Call Features' section includes settings for PBX Service, Call Forwarding, Call Pickup, Call Parking, Do Not Disturb, and Fax To Email Address. The 'User PBX Extension List' table shows the following data:

Extension	Username	R/W Privilege	Calling State	Registration State	IP Address	Voice Port
5000	evan-5000	Local	Free	Registered	172.16.8.1	Disabled
5001	evan-5001	Local	Free	Unregistered	N/A	Disabled
5002	evan-5002	Local	Free	Unregistered	N/A	Enabled
5003	evan-5003	Local	Free	Registered	172.16.8.1	Enabled
5004	evan-5004	Local	Free	Unregistered	N/A	Enabled
5005	evan-5005	Local	Free	Unregistered	N/A	Enabled
5006	evan-5006	Local	Free	Unregistered	N/A	Enabled

**Step2. Configuration Hotline for when outside call in to forward extension number :**

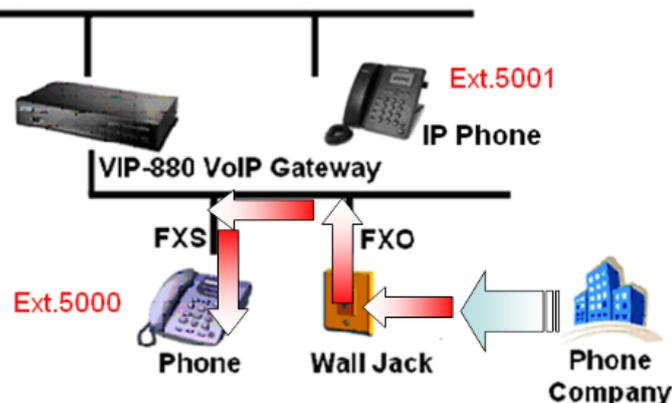
- (1)Go to “Hot Line Setting” page.
- (2)Set you want to forward to extension number which port you plug the PSTN Line.

The screenshot shows the 'Hot Line Setting' configuration page. The 'Hotline Delay' section has 'Disable' selected. The 'Hotline Delay Time' is set to 3 seconds. The 'Port' settings are as follows:

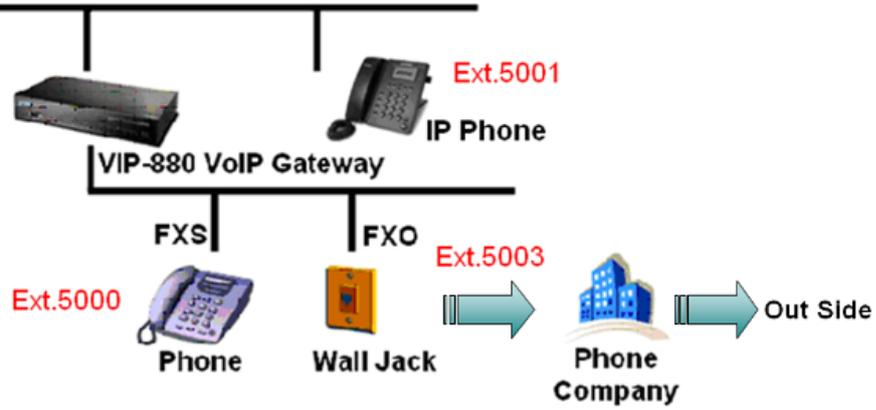
Port	Number
Port 1 number	None
Port 2 number	None
Port 3 number	None
Port 4 number	None
Port 5 number	None
Port 6 number	5000
Port 7 number	None
Port 8 number	None

After setting complete :

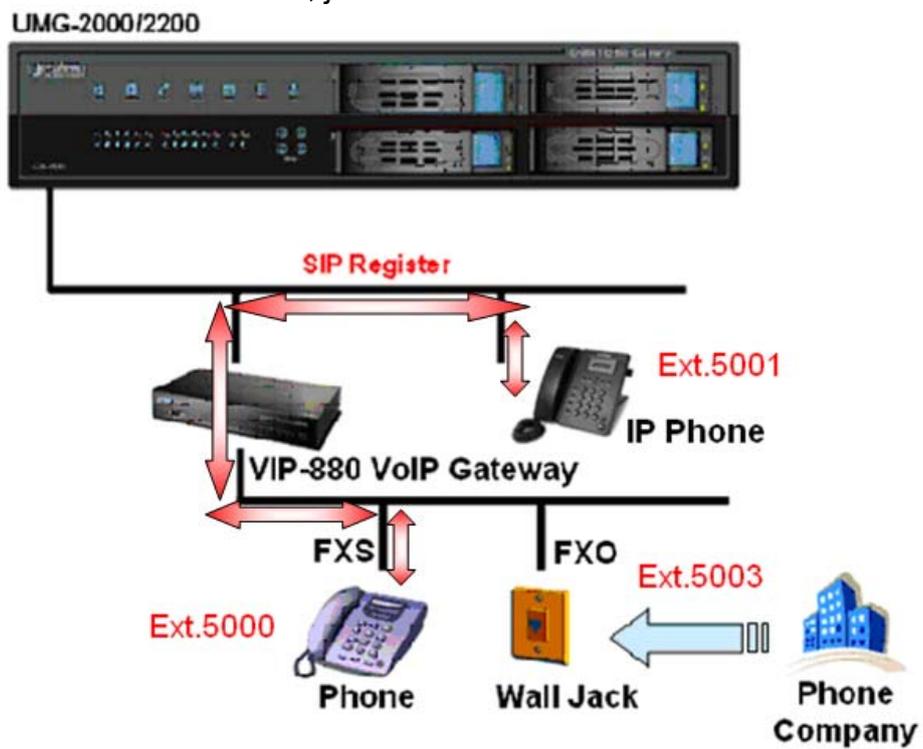
- (1)when call form outside, that will forward to your extension number 5000.



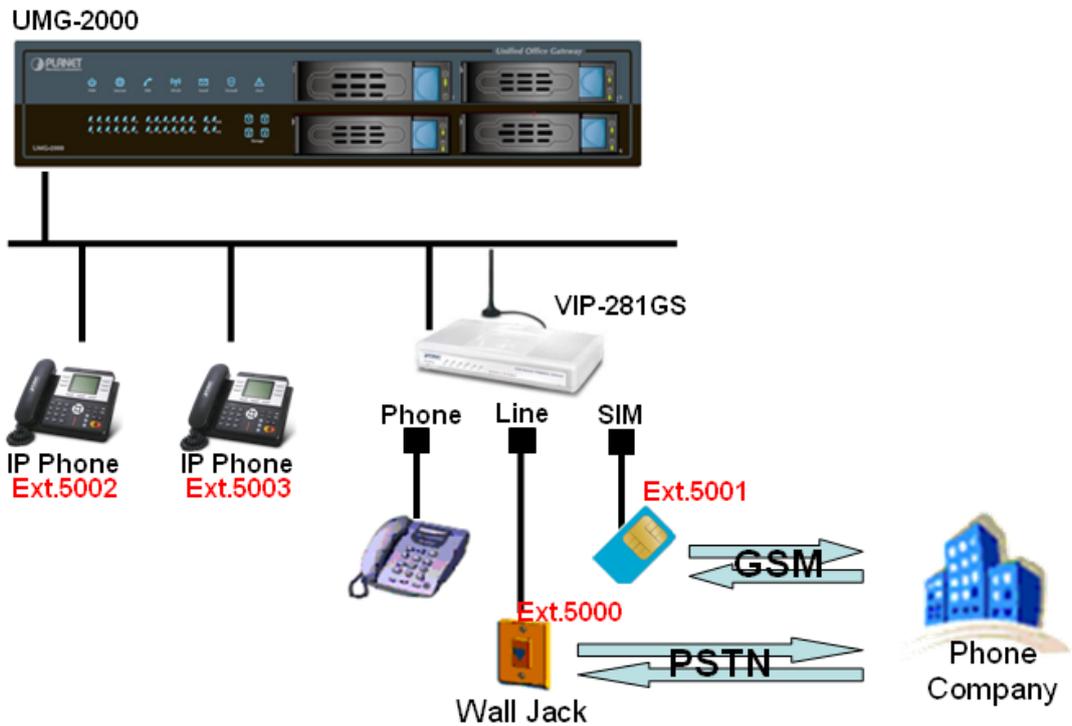
(2) When you want make a outside call, just dial the 5003 number to has outside call.



(3) If want call to another IP-Phone, just dial the extension number.



### Case 3\_ VIP-281GS GSM Gateway how to register on the UMG-2000.

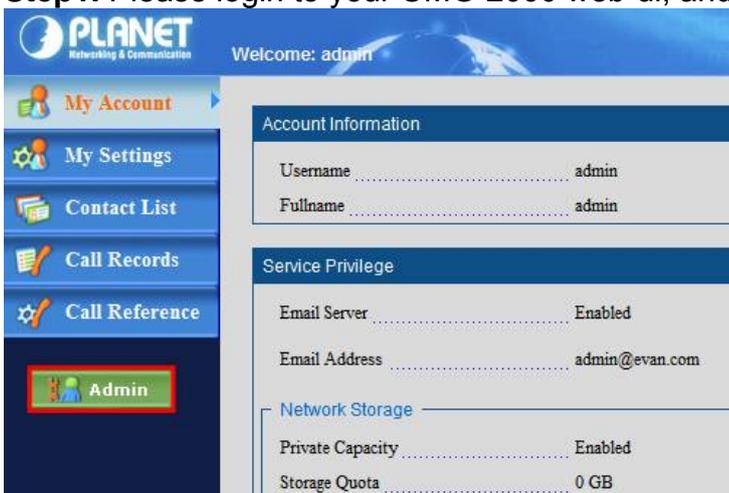


#### \*\*\* FW & Utility version List:

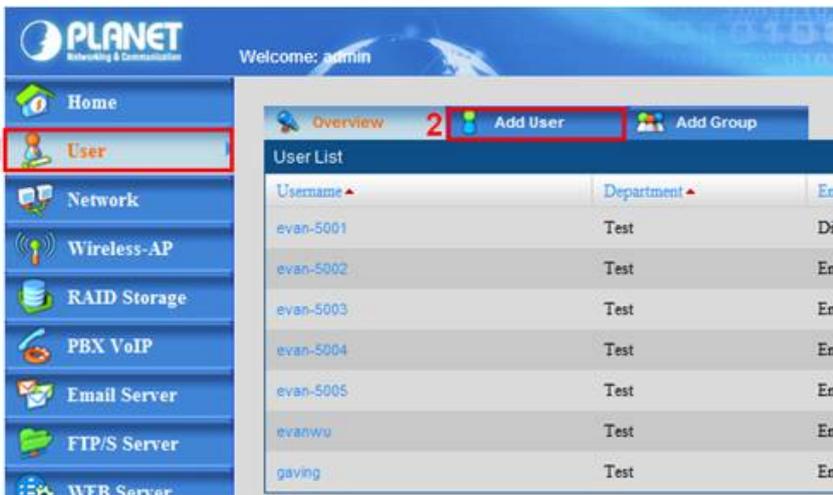
UMG-2000:v.3.6.5  
VIP-281GS : 3.2.4L

#### \*\*\* Create your UMG-2000 user account :

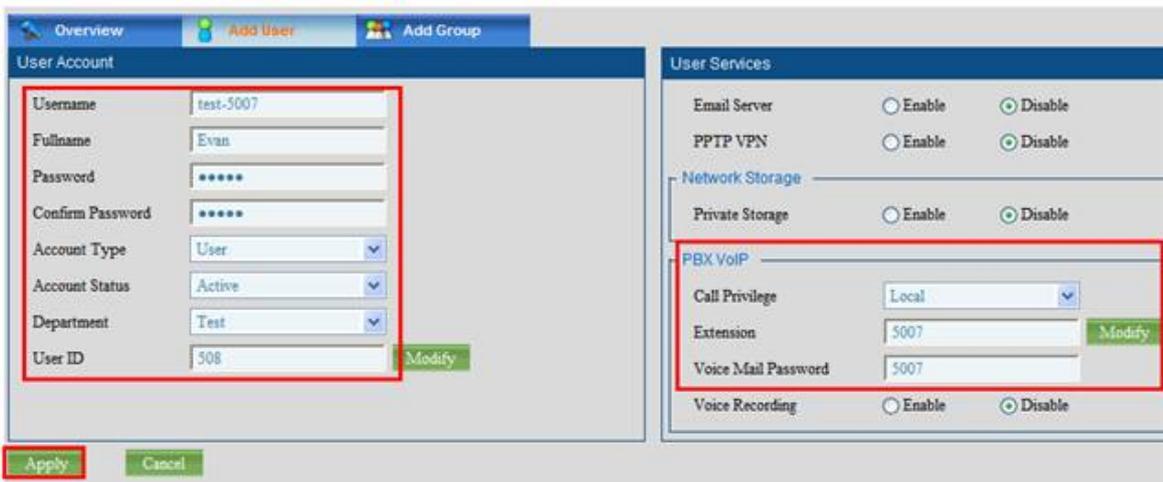
**Step1.** Please login to your UMG-2000 web-ui, and press the “Admin” button.



**Step2.** Go to “User” page, and press the “Add User” to create the user account.



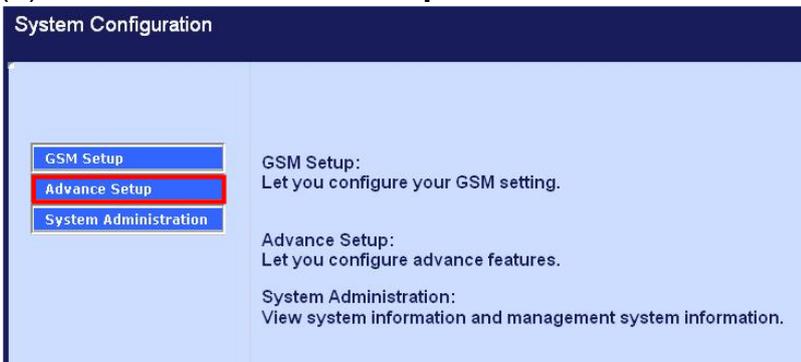
**Step3.** Input the Username, password..., and modify the “**Extension**” number you want. After setting complete, please press the “**Apply**” to apply the configure.



**\*\*\* Use VIP-281GS to register to UMG-2000 :**

**Step1.Configuration VoIP Setting register to UMG-2000 :**

(3) Select the “**Advance Setup**”.



(4) Go to “**VoIP Basic**” page, and “**VoIP Protocol Setting**” select “**SIP**”.

(5) Register FXS and GSM on the UMG-2000.

Key-in the UMG-2000 extension number and password.

(the default extension password same as extension number)

Example. We used the **FXS** to register to UMG-2000 “**5000**” extension number.  
 We used the **GSM** to register to UMG-2000 “**5001**” extension number.

VoIP Basic Configuration

VoIP Protocol Setting: SIP

Port Number / Password Setting(MAX 20 digit):

No.	Number	Reg	Account	Password	Register Status	Reason
1(FXS)	5000	<input checked="" type="checkbox"/>	5000	●●●●	Success	OK
2(GSM)	5001	<input checked="" type="checkbox"/>	5001	●●●●	Success	OK

Use Public Account (PORT 1):  Enable  Disable

SIP Hunting Table:

No.	Hunting Member
1	<input checked="" type="checkbox"/> Port 1 <input type="checkbox"/> Port 2
2	<input type="checkbox"/> Port 1 <input checked="" type="checkbox"/> Port 2

(3)Go to the below of page, please key-in your UMG-2000 IP-Address for connect to SIP Server.

Domain/Realm : UMG-2000 IP-Address or Domain name.

Sip Proxy Server : UMG-2000 IP-Address

SIP Authentication : Select “Enable”

Local SIP Port : 5060

SIP Proxy Setting:

Domain/Realm	192.168.0.75
SIP Proxy Server	192.168.0.75/5060
SIP User Agent	
Register Interval (seconds)	10
SIP Authentication	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Outbound Proxy Server	0.0.0.0

NAT Transversal Setting:

NAT Transversal Method	<input type="radio"/> STUN <input checked="" type="radio"/> Symmetric RTP
STUN Server IP Address	64.69.76.21
STUN Server port	3478

When setting is complete, please press the “**Apply**” button on the below of page, then click the “**Save Configuration**” on the above of page to save setting.

If your setting is correct, you will see the “**Register**” information at UMG-2000.

PLANET Unified Office Gateway

Welcome: admin

Company: PLANET

Call Features

PBX Service	Enabled	Conference Recording	Disabled
Call Forwarding	Enabled	Voice Recording	Enabled
Call Pickup	Enabled	BLF Support	Enabled
Call Parking	Enabled	Video Calling	Enabled
Do Not Disturb	Disabled	Stun Server	Disabled
Fax To Email Address	N/A	PBX Call Prefix	.5XXX

Extension	Username	R/W Privilege	Calling State	Registration State	IP Address	Voice Re
5000	evan-5000	Local	Free	Registered	192.168.0.50	Disabled
5001	evan-5001	Local	Free	Registered	192.168.0.50	Disabled
5002	evan-5002	Local	Free	Registered	192.168.0.10	Enabled
5003	evan-5003	Local	Free	Unregistered	N/A	Enabled
5004	evan-5004	Local	Free	Unregistered	N/A	Enabled
5005	evan-5005	Local	Free	Registered	192.168.0.25	Enabled
5006	evan-5006	Local	Free	Registered	192.168.0.10	Enabled

## Step2.Configuration the GSM Setting :

(1) Select the “GSM Setup”.

System Configuration

**GSM Setup**  
Let you configure your GSM setting.

Advance Setup:  
Let you configure advance features.

System Administration:  
View system information and management system information.

(2)Go to “GSM Parameter” page.

(3)If your PIN Card had set password, please “PIN Code Protection” select “Enable” and key-in your password.

(4)Choose your “GSM Frequency”.

(5)After setting complete, press the “Apply” button and click the “Save Configuration”.

PLANET **GSM Setup** Main Menu Reboot Save Configuration Logout

GSM Setup

- GSM Parameter**
- PSTN Dialplan
- GSM Dialplan
- Send SMS
- Receive SMS
- Terminate Phonebook
- Originate Phonebook

GSM Parameter Table	
GSM Parameter table	
PIN Code Protection	<input checked="" type="radio"/> Enable <input type="radio"/> Disable PIN: 3456
Failsafe Mechanism (FXS rely on PSTN)	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Baby Call	<input type="radio"/> Enable <input checked="" type="radio"/> Disable Delay Time: 0 Calling Number:
FXS Battery Reverse	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Talking Time Limit	0 mins
GSM Frequency	<input checked="" type="radio"/> 900/1800 <input type="radio"/> 850/1900
CLI Presentation	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
CLI Detection	<input checked="" type="radio"/> Disable <input type="radio"/> Enable <input type="radio"/> Asterisk 1.3 <input type="radio"/> IDT
Answer Supervision	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
GSM Receive Gain	<input type="radio"/> -18db <input checked="" type="radio"/> -10db <input type="radio"/> -8db <input type="radio"/> -6db <input type="radio"/> -4db <input type="radio"/> -2db <input type="radio"/> 0db <input type="radio"/> +2db <input type="radio"/> +4db <input type="radio"/> +6db
GSM Transmit Gain	<input type="radio"/> +30db <input checked="" type="radio"/> +33db <input type="radio"/> +36db <input type="radio"/> +39db <input type="radio"/> +42db
GSM Answer Mode	<input checked="" type="radio"/> Auto Answer <input type="radio"/> Connecting Answer
VoIP TO GSM	<input type="radio"/> Enable <input checked="" type="radio"/> Disable Calling Number:

(6)Go to “System Administration” page.

**System Configuration**

- GSM Setup: GSM Setup: Let you configure your GSM setting.
- Advance Setup: Advance Setup: Let you configure advance features.
- System Administration: System Administration: View system information and management system information.**

(7)Go to “System Information” for check your GSM is success connect.

**System Administration** Main Menu Reboot Logout

System Information:

Software Version	3.2.4L
WAN Type	Fixed IP
WAN MAC Address	00-0f-fd-48-00-0c
VoIP Status	SIP Proxy Mode Register Successful
VoIP Codec	G723.1
GSM Signal Level	-89 dBm
GSM Operator	Chunghwa Telecom
PIN Code	Verify Successful
Model	GSM+VoIP Gateway
Current system time	0/0/0 00:00:00

**Step3. Configuration the prefix number for auto select PSTN Line or GSM Line when had outside call :**

(1)Go to “PSTN Dialplan” page.

(2)Set the prefix number for choose PSTN Line outside call.

Example. We use prefix number “2” for choose PSTN Line outside call.

(3)After setting complete, press the “Apply” button and click the “Save Configuration”.

**GSM Setup** Main Menu Reboot Save Configuration Logout

Routing Configuration:

**PSTN Routing Table**

Call Service route by PSTN network . According to the prefix of dialed number on FXS interface you can Route the calls to PSTN Network

Item	Phone Number
1	2x
2	
3	
4	
5	
6	
7	
8	
9	
10	

Apply

- (4)Go to “GSM Dialplan” page.
  - (5)Select “GSM Dial Termination Key”.
  - (6)Set the prefix number for choose GSM Line outside call.
- Example. We use prefix number “09” for choose GSM Line outside call.
- (7)After setting complete, press the “Apply” button and click the “Save Configuration”.

**GSM Setup**

Main Menu Reboot **Save Configuration** Logout

**GSM Routing Table**  
Call Service route by GSM network : According to the prefix of dialed number on FXS interface you can Route the calls to GSM Network.

GSM Dial Termination Key: 09x

Item	Phone Number	Length
1	09x	10
2		0
3		0
4		0
5		0
6		0
7		0
8		0
9		0
10		0

**Step4.Configuration Hotline for when outside call in to forward extension number :**

- (1)Go to “Hot Line Setting” page.
- (2)Set you want to forward to extension number for PSTN Line and GSM Line.

**Advance Setup**

Main Menu Reboot Logout

Hot Line Number Setting (Hotline Setting)

Hotline Delay:  Disable  Enable

Hotline Delay Time(Max. 20 sec): 3 sec

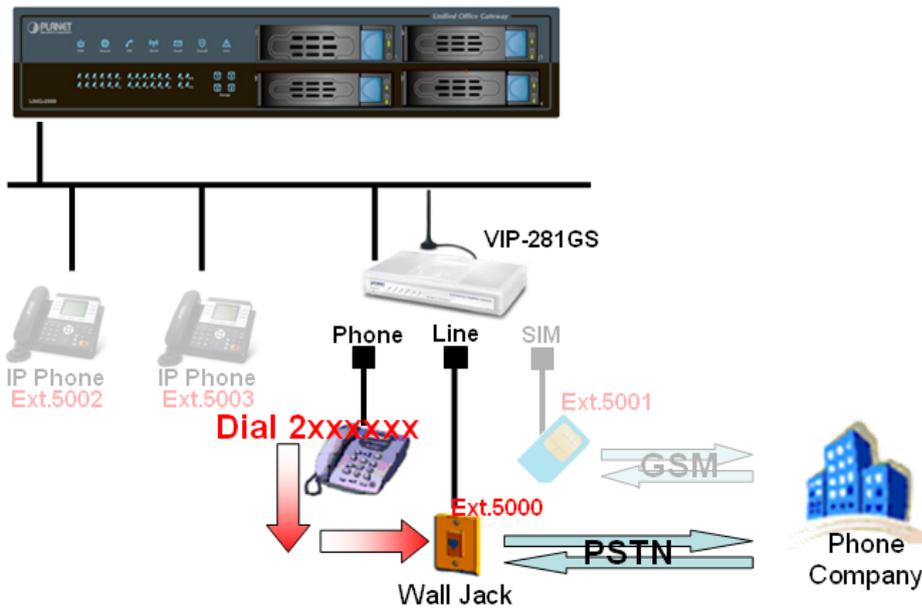
**PSTN** Port 1 number: 5002

**GSM** Port 2 number: 5003

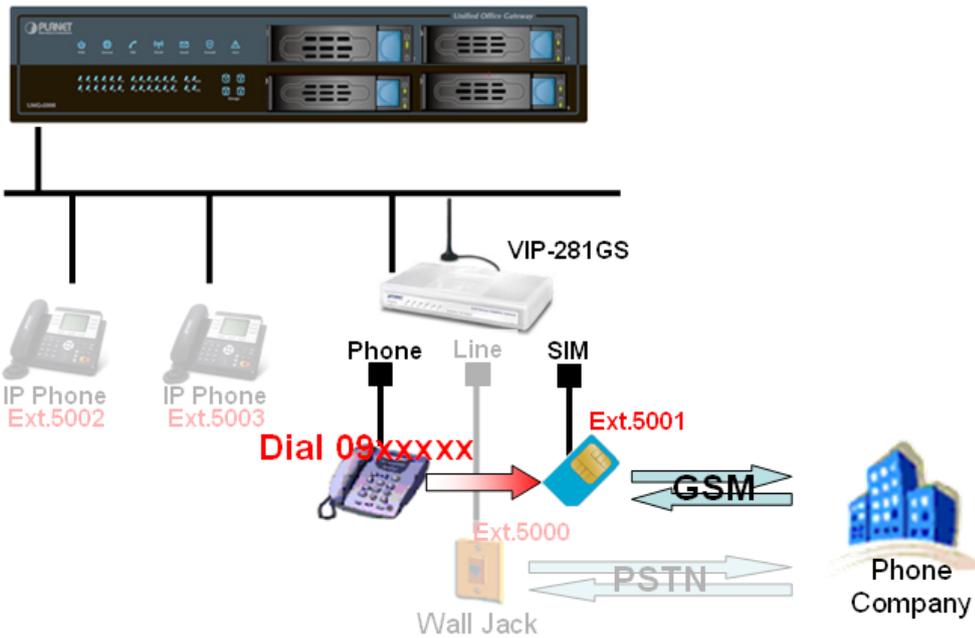
Apply

After setting complete :

(1)When use phone call “2xxxxxx”, then will auto choose PSTN Line to outside.  
UMG-2000

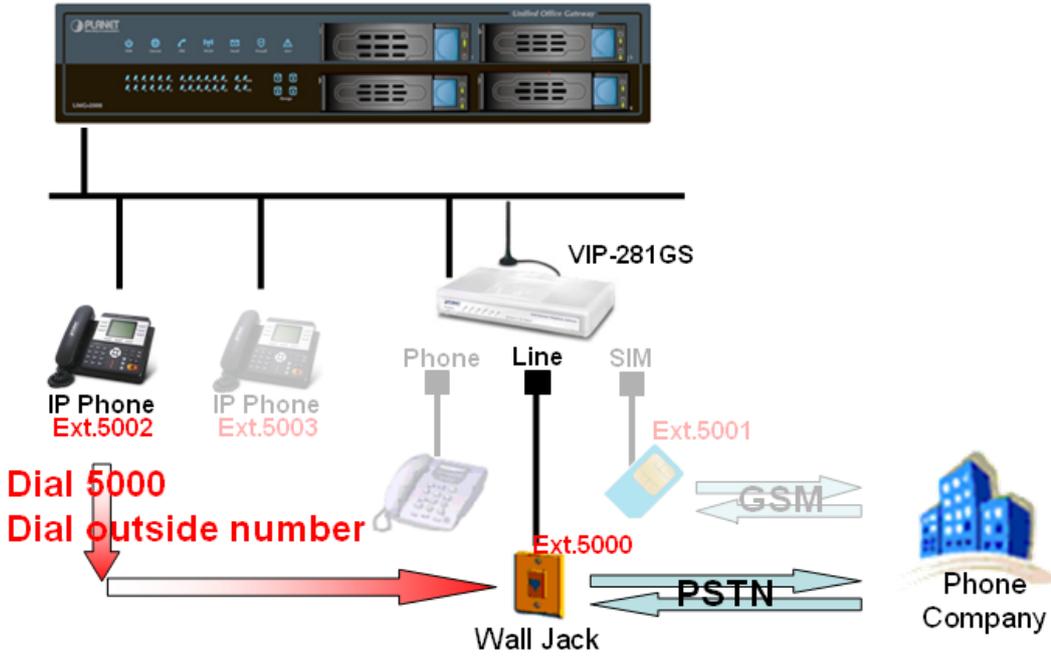


(2)When use phone call “09xxxxxx”, then will auto choose GSM Line to outside.  
UMG-2000



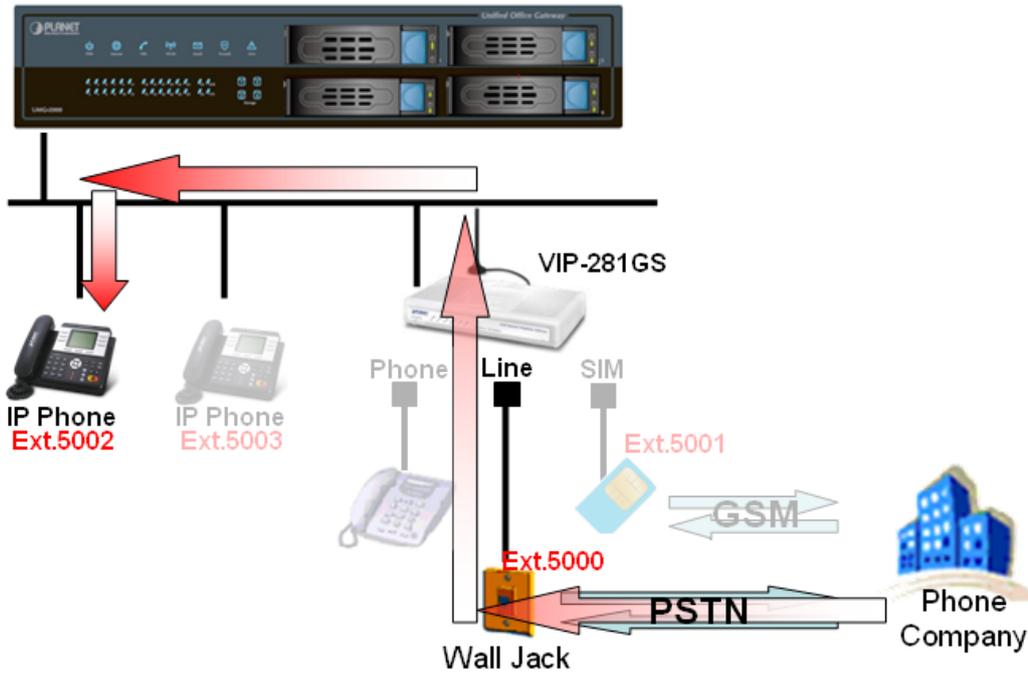
(3) Use IP Phone to call outside by PSTN Line.

UMG-2000



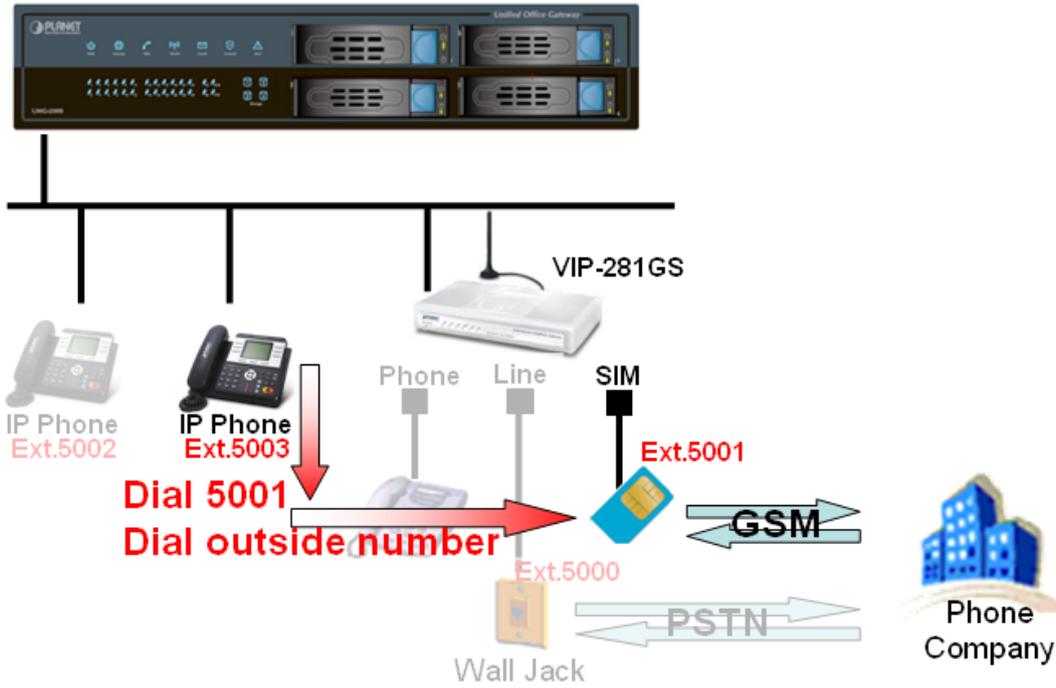
(4) When call form outside to PSTN Line, that will forward to your extension number 5002.

UMG-2000



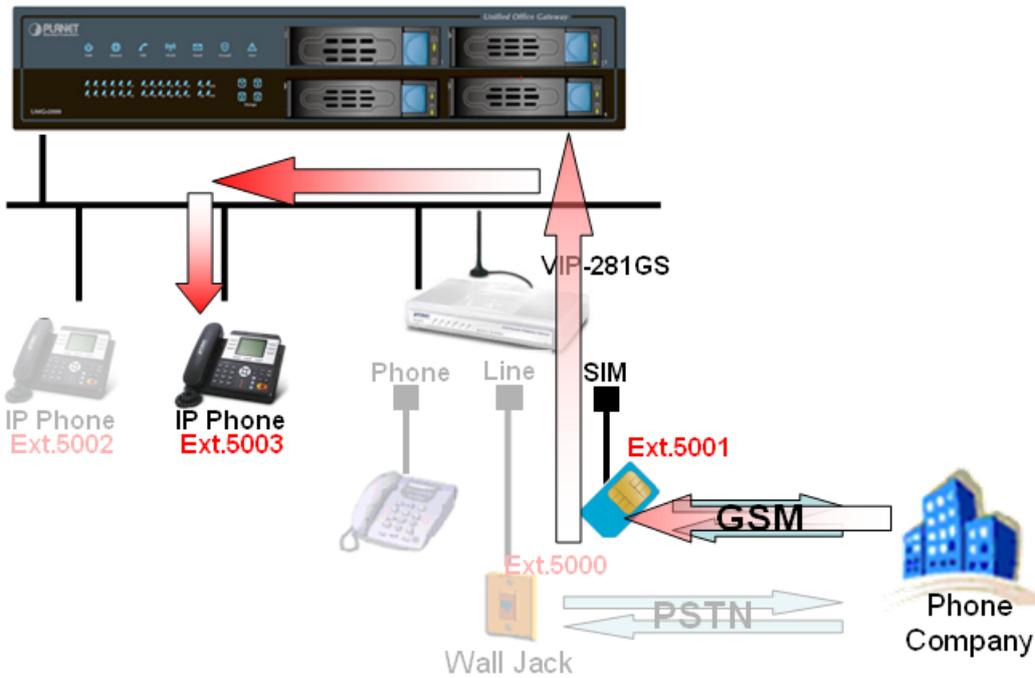
(5) Use IP Phone to call outside by GSM Line.

UMG-2000



(6) When call form outside to GSM Line, that will forward to your extension number 5003.

UMG-2000



## Case 4\_ VIP-254 and VIP-360PT how to register on the UMG-2000.

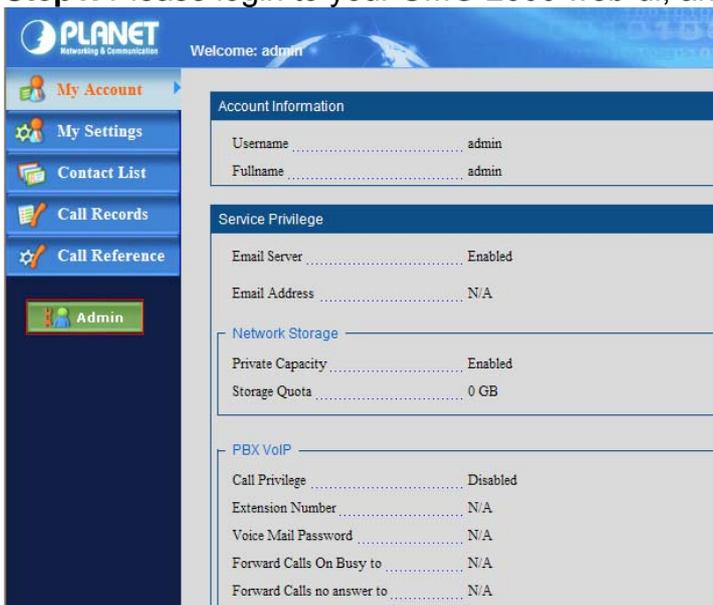


### \*\*\* FW & Utility version List:

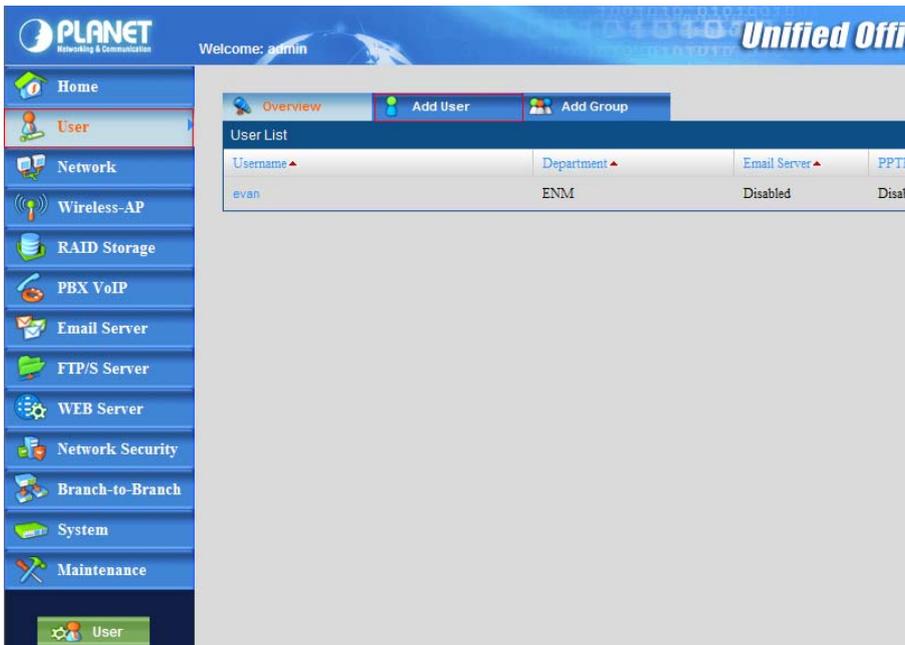
UMG-2000:v.3.6.6  
VIP-254T/PT:V1.0.2  
VIP-360PT: 2.0002

### \*\*\* Create your UMG-2000 user account :

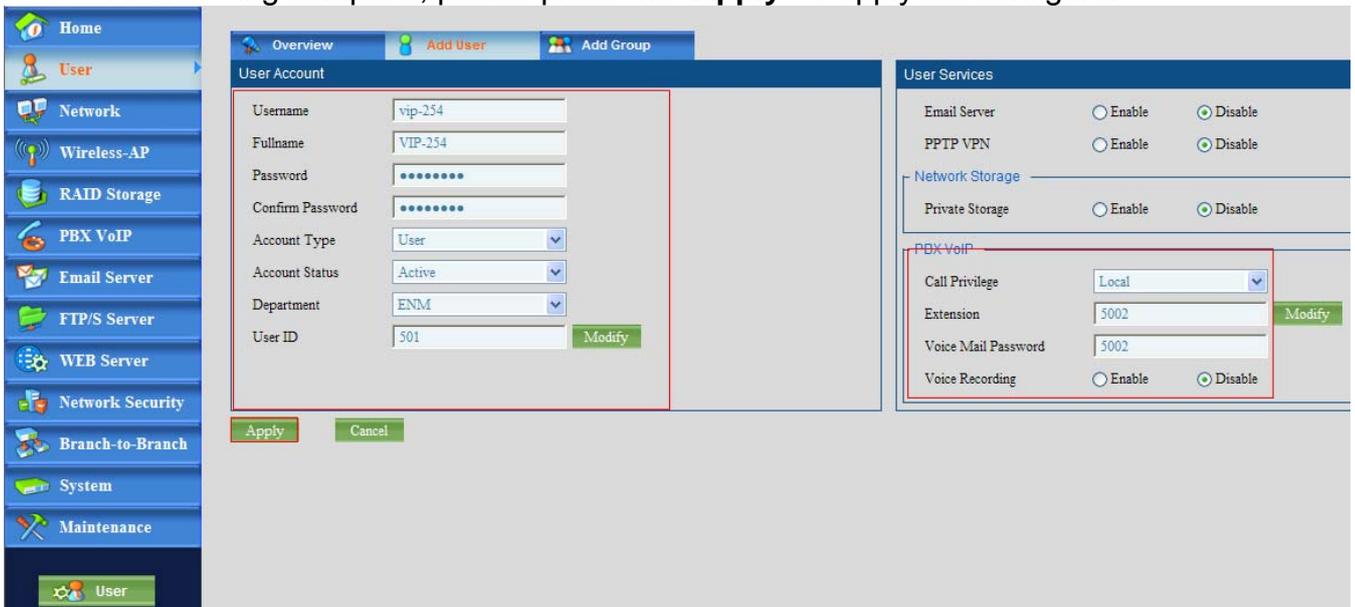
**Step1.** Please login to your UMG-2000 web-ui, and press the “Admin” button.



**Step2.** Go to “User” page, and press the “Add User” to create the user account.



**Step3.** Input the Username, password..., and modify the “**Extension**” number you want. After setting complete, please press the “**Apply**” to apply the configure.



Overview Add User Add Group

User Account

Username vip-360pt  
 Fullname VIP-360PT  
 Password .....  
 Confirm Password .....  
 Account Type User  
 Account Status Active  
 Department ENM  
 User ID 502

Apply

User Services

Email Server  Enable  Disable  
 PPTP VPN  Enable  Disable

Network Storage

Private Storage  Enable  Disable

PBX VoIP

Call Privilege Local  
 Extension 5003   
 Voice Mail Password 5003  
 Voice Recording  Enable  Disable

Overview Add User Add Group

User List

Username	Department	Email Server	PPTP VPN	Extension	Call Privilege
evan	ENM	Disabled	Disabled	5000	Operator
vip-254	ENM	Disabled	Disabled	5002	Local
vip-360pt	ENM	Disabled	Disabled	5003	Local

**\*\*\* Use VIP-254 to register to UMG-2000 :**

Step1. VIP-254 will prompt for logon **username/ password, please enter: root / No password** to continue machine administration.

Enter Network Password

Enter your username and password to login  
 PLANET IP Phone Configuration

Username root  
 Password

\*The default IP address of ATA is 192.168.0.1.  
 You also could open your web browser, and insert http://192.168.0.1 in the address bar on your web browser to logon VIP-254 web configuration page.

## Step2: Insert IP information

Go to Network -> LAN Setting , You will login LAN Setting page. Please insert IP information and press "Submit". After check "DHCP Client"



### LAN Settings

You could configure the LAN settings in this page.

LAN Mode:  Bridge  NAT

**LAN Setting**

IP Type:  Fixed IP  DHCP Client  PPPoE

IP:

Mask:

Gateway:

DNS Type:  Fixed  Auto

DNS Server1:

DNS Server2:

MAC:

Host Name:

**PPPoE Setting**

User Name:

Password:

Service Name:



### LAN Settings

You could configure the LAN settings in this page.

LAN Mode:  Bridge  NAT

**LAN Setting**

IP Type:  Fixed IP  DHCP Client  PPPoE

IP:

Mask:

Gateway:

DNS Type:  Fixed  Auto

DNS Server1:

DNS Server2:

MAC:

Host Name:

**PPPoE Setting**

User Name:

Password:

Service Name:

## Step3. Set SIP

(1) Press the "SIP Settings".

(2) Check the "Realm#1" in Realm No.

(3) Display Name : Input the name you want. EX. 5002

.User Name : Input the name you want, Ex. 5002

.Register Name : Same as the UMG-2000 Extension number, Ex. 5002

.Register Password : Same as the UMG-2000 Extension number, Ex. 5002

.Proxy Server : Input your UMG-2000 IP Address.

(4) Press the "Apply All" to apply the setting, then if success to register on UMG-2000.

**PLANET**  
Networking & Communication

SIP Phone  
Configuration Menu

- Phone Book >
- Phone Setting >
- Network >
- SIP Settings >
- NAT Trans. >
- Others >
- System Auth. >
- Save & Reboot >
- System Settings >
- Reboot without Saving

## Service Domain Settings

You could set information of service domains in this page.

Realm No.: Realm # 1

Realm	
Active:	<input checked="" type="radio"/> On <input type="radio"/> Off
Display Name:	<input type="text" value="5002"/>
User Name:	<input type="text" value="5002"/>
Register Name:	<input type="text" value="5002"/>
Register Password:	<input type="password" value="••••••••••"/>
Domain Server:	<input type="text"/>
Proxy Server:	<input type="text" value="172.16.0.75"/>
Outbound Proxy:	<input type="text"/>
Status:	Registered

Also, you can see the UMG-2000 Web-UI “PBX VoIP” page, there is show the 5002 Extension is work and Registered.

Company: PLANET

Overview | Call Setting | Feature Setting | Call Rule | Channels | SIP Trunk | LCR | Call Log

Call Features

PBX Service	Enabled	Conference Recording	Disabled
Call Forwarding	Enabled	Voice Recording	Enabled
Call Pickup	Enabled	BLF Support	Enabled
Call Parking	Enabled	Video Calling	Enabled
Do Not Disturb	Disabled	Stun Server	Disabled
Fax To Email Address	N/A	PBX Call Prefix	5XXX

User PBX Extension List

Extension	Username	R/W Privilege	Calling State	Registration State	IP Address	Voice Recording
5000	evan	Operator	Free	Unregistered	N/A	Enabled
5002	jasper	Local	Free	Registered	172.16.0.249	Disabled
5003	jasper1	Local	Free	Registered	172.16.0.248	Disabled

**\*\*\* Use VIP-360PT to register to UMG-2000 :**

**Step1.**

VIP-360PT will prompt for logon **username/ password**, please enter: **admin / 123** to continue machine administration.



\*The default IP address of ATA is 192.168.0.1.

You also could open your web browser, and insert <http://192.168.0.1> in the address bar on your web browser to logon VIP-360PT web configuration page.

**Step2.** Insert IP information

Go to Network -> LAN Setting , You will login LAN Setting page. Please insert IP information and press "Submit".



**Step3.** Set SIP Settings

(1) Press the "VOIP".

(2) Server Name : Input the name you want. EX.5003

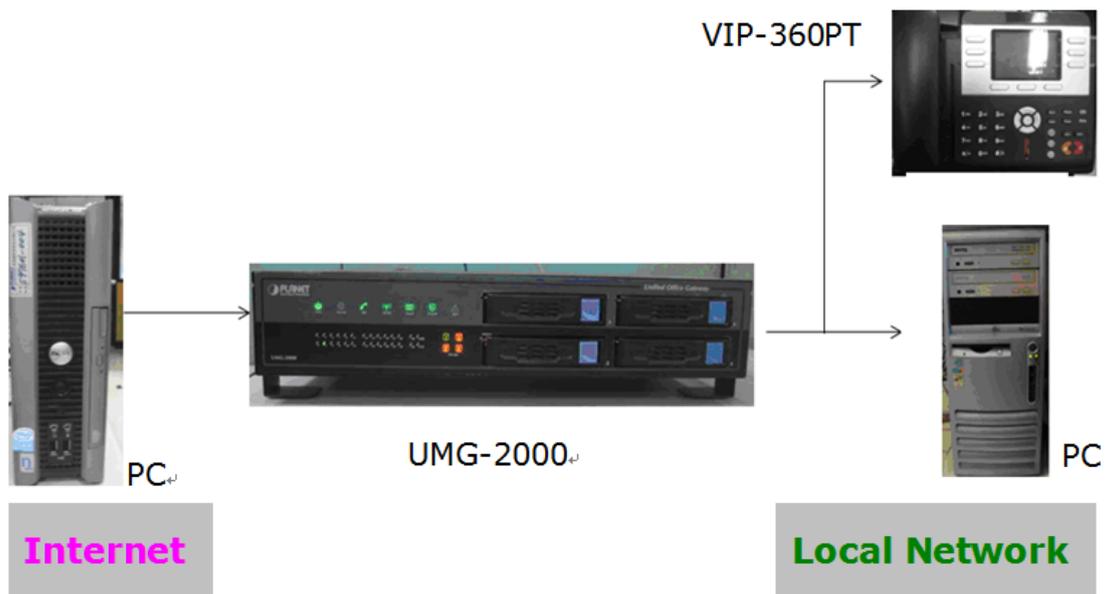
- .Server Address : Input the UMG-2000 IP Address, EX.172.16.0.75
- .Password : Same as the UMG-2000 Extension number, Ex. 5003
- .Phone number : Input the UMG-2000 Extension number, Ex. 5003

(3) Press the “**Apply**” to apply the setting, then if success to register on UMG-2000. The “**Register Status**” will show the “Registered”.

Also, you can see the UMG-2000 Web-UI “**PBX VoIP**” page, there is show the 5003 Extension is work and Registered.

Extension	Username	R/W Privilege	Calling State	Registration State	IP Address
5000	evan	Operator	Free	Unregistered	N/A
5002	vip-254	Local	Free	Registered	172.16.0.249
5003	vip-360pt	Local	Free	Registered	172.16.0.247

## Case 5\_ How do you setup a VPN with UMG-2000 Series.



### \*\*\* FW & Utility version List:

UMG-2000:v.3.6.6

### \*\*\* Create your UMG-2000 internet :

**Step1.** Please login to your UMG-2000 web-UI, and press the “Admin” button.

The screenshot shows the UMG-2000 web-UI. The header includes the PLANET logo and the text "Welcome: admin" and "Unified Office Gateway". The left sidebar contains navigation buttons: My Account, My Settings, Contact List, Call Records, Call Reference, and Admin. The main content area displays account information and service privileges.

Account Information	
Username .....	admin
Department .....	admin
Fullname .....	admin
Account Status .....	Active

Service Privilege	
Email Server .....	Enabled
PPTP VPN .....	Disabled
Email Address .....	N/A

Network Storage	
Private Capacity .....	Enabled
Storage Used .....	N/A
Storage Quota .....	0 GB

## Step2. Insert your "Internet"

The screenshot shows the PLANET Unified Office Gateway web interface. The left sidebar contains navigation options: Home, User, Network (highlighted), Wireless-AP, RAID Storage, PBX VoIP, Email Server, FTP/S Server, WEB Server, Network Security, Branch-to-Branch, System, and Maintenance. The main content area is titled "Internet Setting" and includes tabs for Overview, Internet (selected), Local Network, Service, and Route. The configuration fields are as follows:

ISP Type	STATIC-IP	Detect		
IP Address	210	66	155	75
Subnet Mask Address	255	255	255	224
Default Gateway Address	210	66	155	94
DNS Server Address	8	8	8	8
MAC Address	00-30-4E-7D-5E-61			

Buttons for "Apply" and "Cancel" are located at the bottom of the configuration area.

## Step3. Insert your "Local Network"

The screenshot shows the PLANET Unified Office Gateway web interface with the "Local Network" tab selected. The left sidebar is the same as in Step 2. The main content area is titled "Local Network Setting" and includes tabs for Overview, Internet, Local Network (selected), Service, and Route. The configuration fields are as follows:

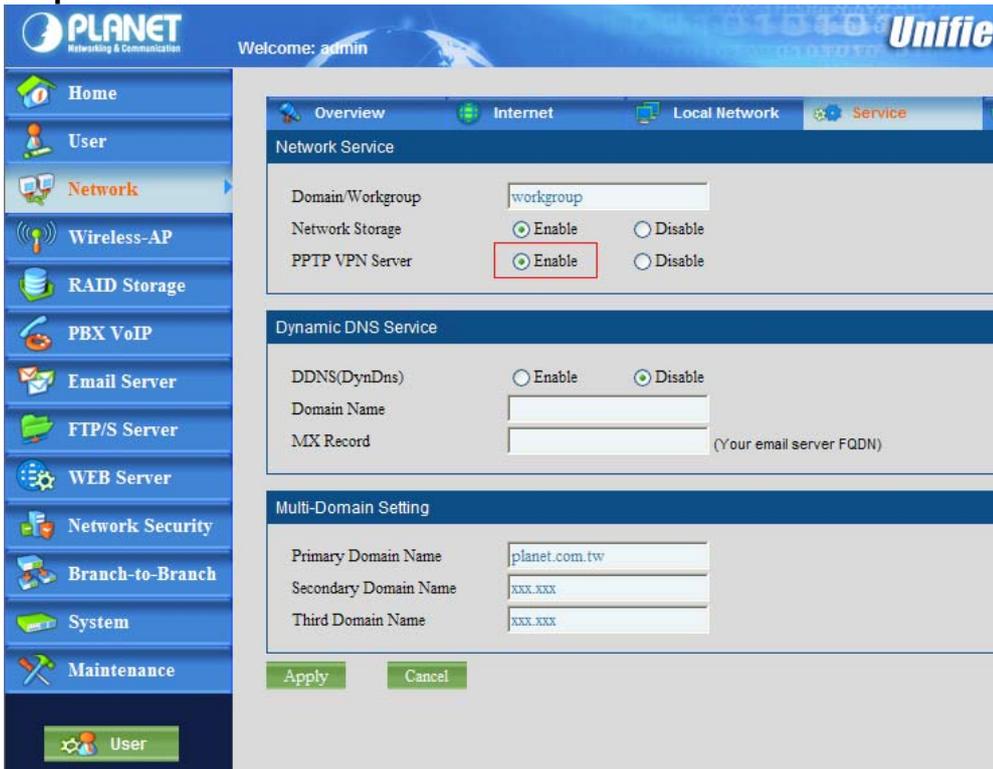
Local Server Address	172	16	0	75
Subnet Mask Address	255	255	255	0

Below the configuration fields is a "Hostname List" section with a table containing one entry:

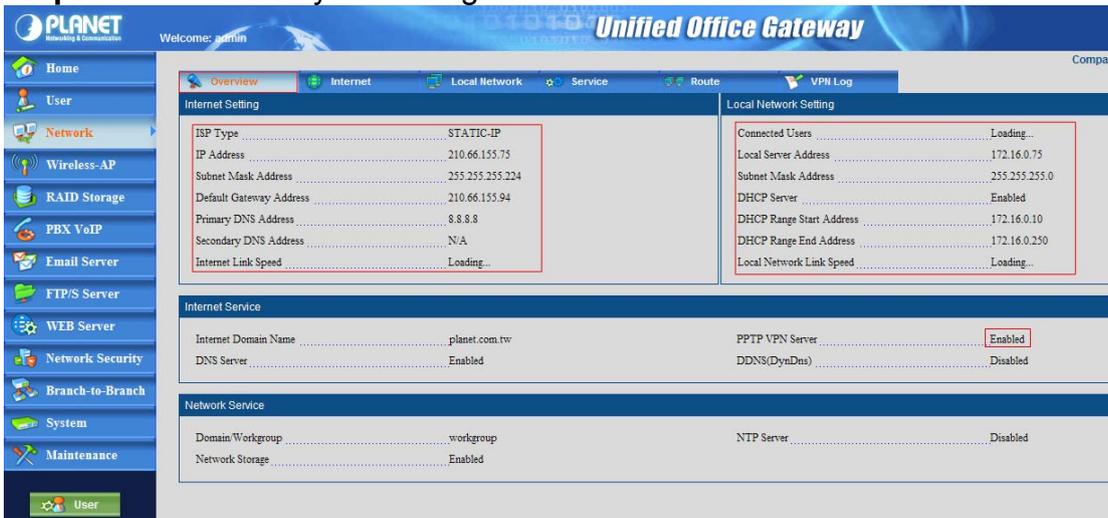
Hostname
umg

There is an "Add Hostname" input field below the list. Buttons for "Apply" and "Cancel" are located at the bottom of the configuration area.

**Step4. Check enable in the “PPTP VPN Server”**



**Step5. Double check your setting**



### \*\*\* Create your UMG-2000 user account :

**Step1.** Go to “User” page, and press the “Add User” to create the user account.

Planet Unified Office Gateway  
Welcome: admin  
Company: Planet

Overview Add User Add Group

User Account

Username: jasper  
Fullname: jasper  
Password: \*\*\*\*\*  
Confirm Password: \*\*\*\*\*  
Account Type: User  
Account Status: Active  
Department: ENM  
User ID: 301  
Modify

Apply Cancel

User Services

Email Server:  Enable  Disable  
PPTP VPN:  Enable  Disable  
Private Storage:  Enable  Disable

PBX VoIP

Call Privilege: Disabled  
Extension: 3000  
Voice Mail Password: 3000  
Modify

**Step2.** Double check your setting and make sure “Enable” PPTPVPN

Planet Unified Office Gateway  
Welcome: admin  
Company: Planet

Overview Add User Add Group

User List

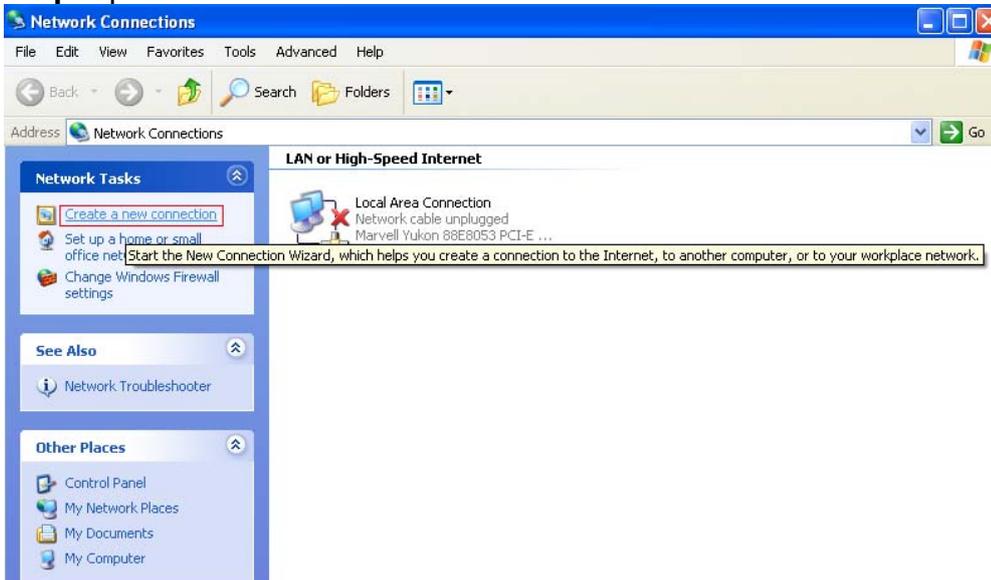
Username	Department	Email Server	PPTP VPN	Extension	Call Privilege	Quota
jasper	ENM	Disabled	Enabled	3000	Disabled	0 GB

### \*\*\* Create your PCs a new connect :

**Step1.** Go to start→setting→Network Connections



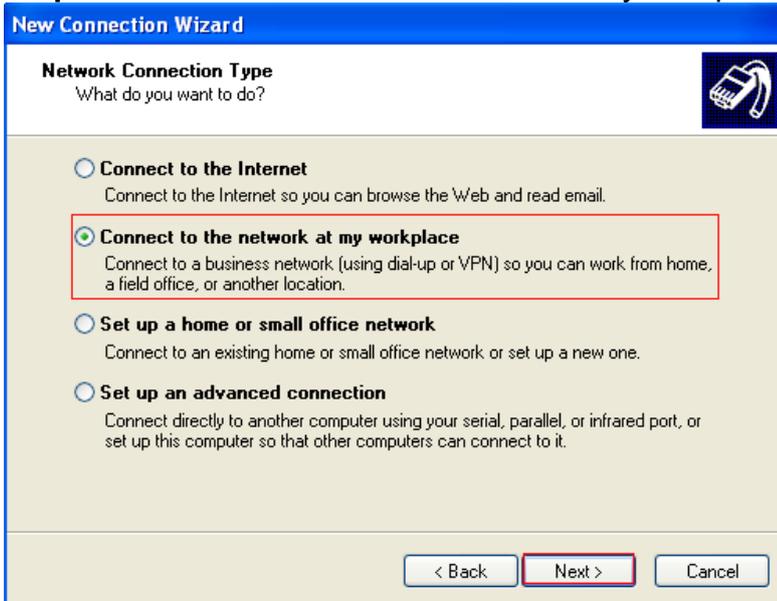
**Step2.** press “Create a new connection”



**Step3.** Press “Next”



**Step4.** Check “Connect to the network at my workplace ” and press “Next”



**Step5.** Check “Virtual Private Network connect” and press “Next”



## Step6. Insert your company name

**New Connection Wizard**

**Connection Name**  
Specify a name for this connection to your workplace.



Type a name for this connection in the following box.

Company Name

For example, you could type the name of your workplace or the name of a server you will connect to.

< Back   Next >   Cancel

## Step7. Insert your UMG-2000 internet IP address(Static-IP)

**New Connection Wizard**

**VPN Server Selection**  
What is the name or address of the VPN server?



Type the host name or Internet Protocol (IP) address of the computer to which you are connecting.

Host name or IP address (for example, microsoft.com or 157.54.0.1 ):

< Back   Next >   Cancel

**Step8.** Check “Add a shortcut to this connect to my desktop” and press “Finish”



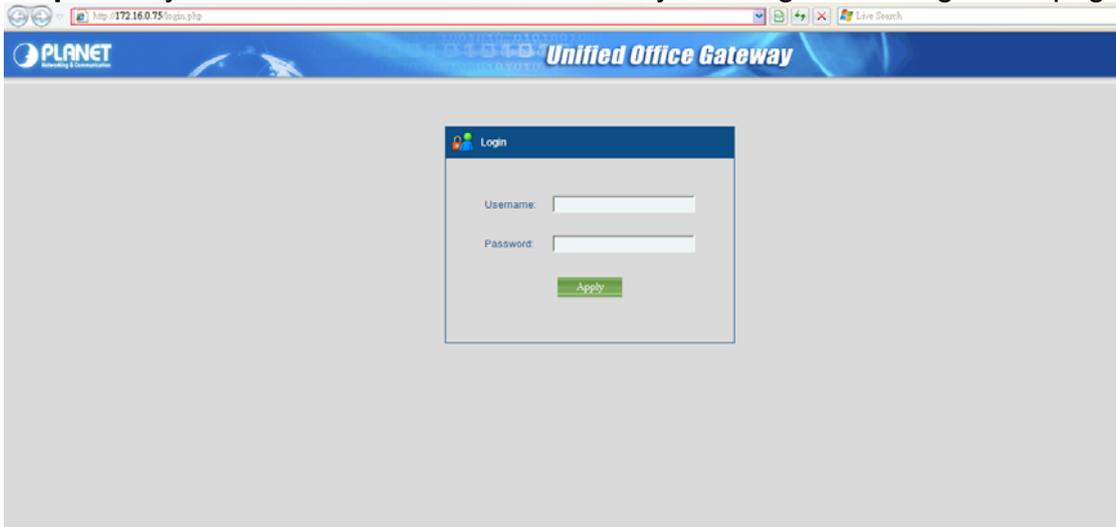
**Step9.** Insert your User name and Password (the same UMG-2000 user account )



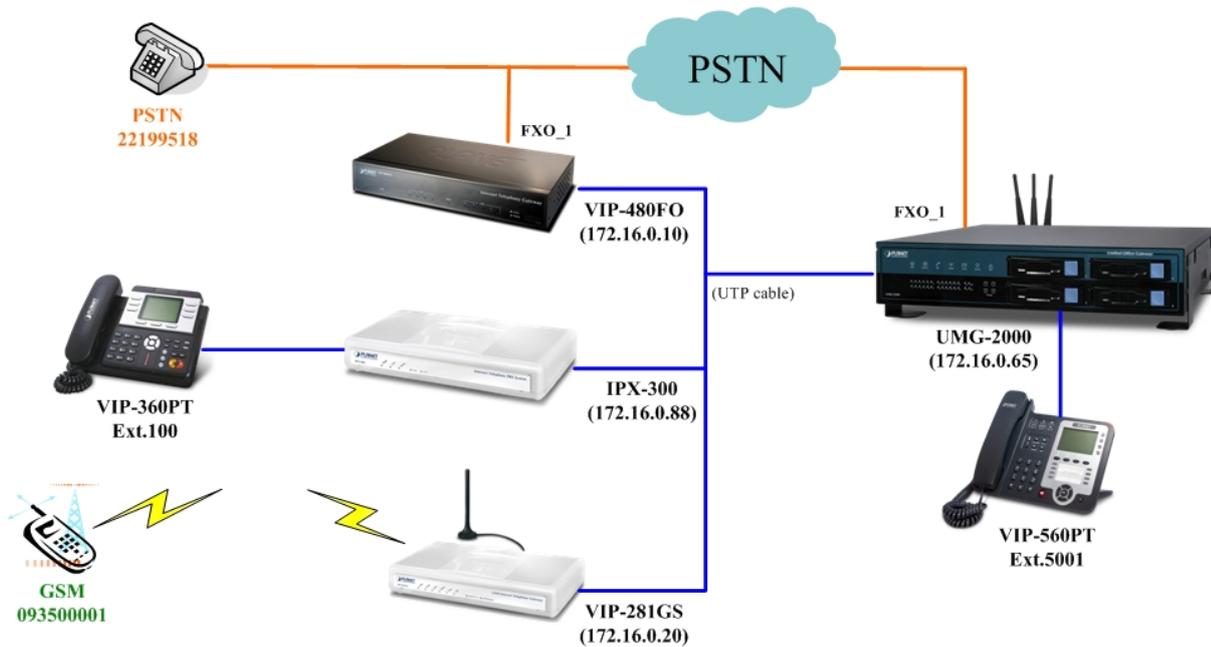
**Step10.** Display connect to UMG-2000 and check it



**Step11.** Key Local IP address in the browser, you can go in management page.



## Case 6\_ How to use LCR function on UMG-2000 Series



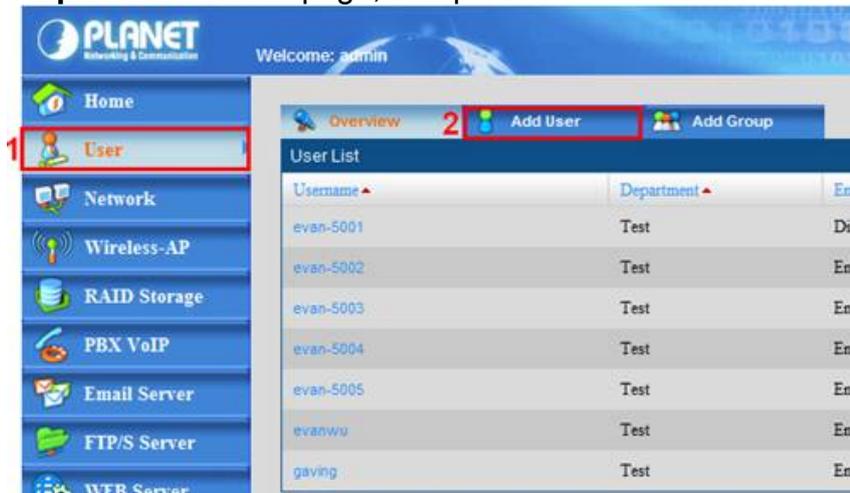
### \*\*\* FW & Utility version List:

UMG-2000: v3.6.81  
 IPX-300: v2.1.9  
 VIP-480FO: v3.0.8  
 VIP-281GS: v3.2.4  
 VIP-360PT: v2.0002  
 VIP-560PT: v2.0.3.2-809

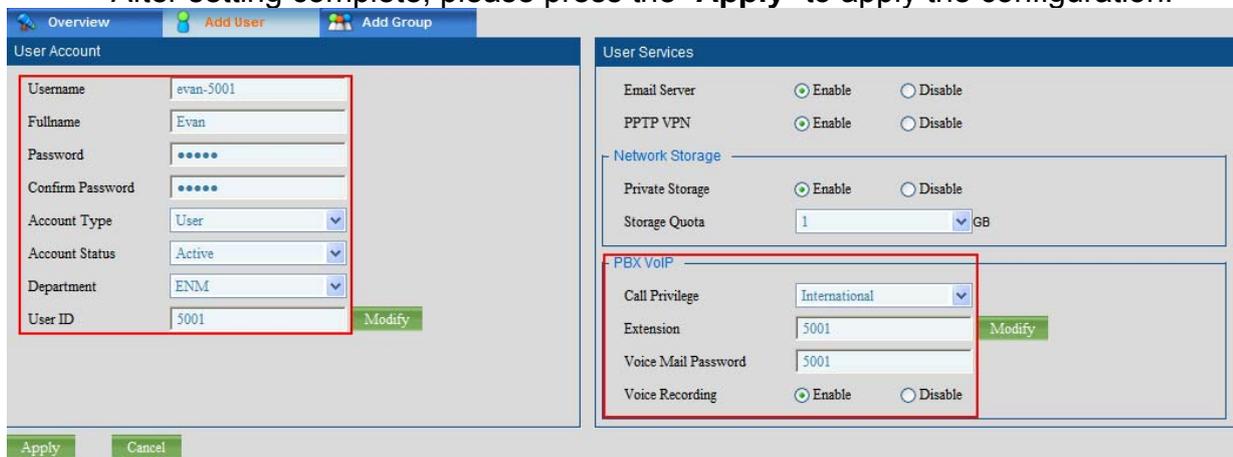
### \*\*\* Create your UMG-2000 user account :

**Step1.** Please login to your UMG-2000 Web-UI, and press the “Admin” button.

**Step2.** Go to “User” page, and press the “Add User” to create the user account.

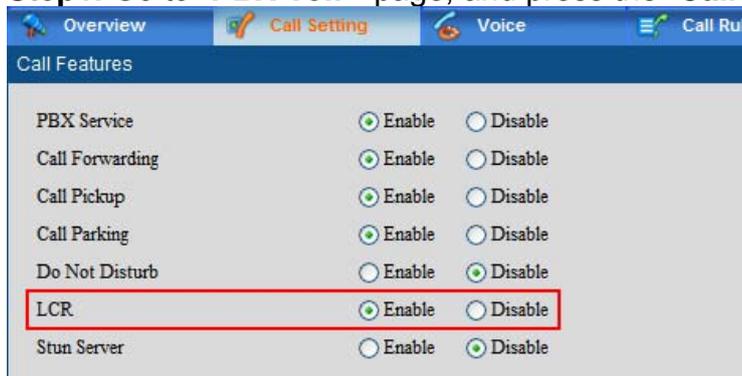


**Step3.** Input the Username, password..., and modify the “Extension” number you want. After setting complete, please press the “Apply” to apply the configuration.



**\*\*\* Enable LCR, create SIP Trunk and setup LCR settings on UMG-2000 :**

**Step1.** Go to “PBX VoIP” page, and press the “Call Setting” to enable LCR function.



**Step2.** To press the “SIP Trunk” to create SIP Trunk for registering with IPX-300.

SIP Trunk Setting	
Outbound Prefix	*1
Trunk/User ID	101
Incoming Number	101
Trunk/User Password	123
Available Time Period	0:00 To 24:00
SIP Register Domain	172.16.0.88 (FQDN)
Registration Required	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
SIP Proxy Domain	172.16.0.88 (FQDN)
SIP Proxy Port	5060
DTMF Mode	rfc2833

**Step3.** To press the “LCR” to setup LCR settings.

Gateway Trunk Setting			
IP Address	Port (1~65535)	Group Name	
	5060		<input type="button" value="Add"/>
172.16.0.10	5060	172.16.0.10:5060	<input type="checkbox"/> Delete
172.16.0.20	5060	172.16.0.20:5060	<input type="checkbox"/> Delete

FXO Trunk Setting			
Group Name	Channels		
	(eg:1,3,5)		<input type="button" value="Add"/>
FXO	1		<input type="checkbox"/> Delete

LCR Trunk Group Setting (LCR Feature must be enabled in call setting)			
Group Name	Prefix Number	Path (FXO/Gateway/SIP Trunk)	
		FXO	<input type="button" value="Add"/>
FXO	61	FXO	<input type="checkbox"/> Delete

LCR Dialing Rules Setting (LCR Feature must be enabled in call setting)					
Prefix Number	Delete Length (0~16)	Add Prefix Number	Path (FXO/Gateway/SIP Trunk)	Secondary Path	
			FXO	N/A	<input type="button" value="Add"/>
71	2		FXO	n/a	<input type="checkbox"/> Delete
72	0		172.16.0.10:5060	n/a	<input type="checkbox"/> Delete
73	0		172.16.0.20:5060	n/a	<input type="checkbox"/> Delete

### Gateway Trunk Setting:

UMG-2000 can make the off-net call either via the external voice gateway. Before you can make the successful call, you have to fill in gateway’s IP address and SIP port.

In this case, we created 172.16.0.10 for FXO Gateway (VIP-480FO), and 172.16.0.20 for GSM Gateway (VIP-281GS).

### FXO Trunk Setting:

You also could determine use which FXO port for outgoing call via LCR function.

In this case, we define channel 1 of FXO module.

### LCR Trunk Group Setting:

When want to make VoIP calls through the above Gateway Trunk, FXO channel or SIP Trunk, the user can use this function to accomplish the 2\_Stage dialing method.

In this case, we created the rule for outgoing call.

Prefix No.61: When dialing the number 61, it will hear the prompt for dialing desired external number. Then this call will go through FXO channel 1.

### LCR Dialing Rules Setting:

This is another way to make VoIP calls through the above Gateway Trunk, FXO channel or SIP Trunk, the user can use this function to accomplish the 1\_Stage dialing method.

In this case, we created the below rules for outgoing call.

Prefix No.71: When dialing the number start by 71, this call will go through FXO channel 1.

Prefix No.72: When dialing the number start by 72, this call will go through VIP-480FO.

Prefix No.73: When dialing the number start by 71, this call will go through VIP-281GS.

Prefix No.8: When dialing the number start by 8, this call will send to IPX-300 and ring up the desired extension.

### \*\*\* Setup Dialing Plan on VIP-480FO and VIP-281GS :

**Step1.** Login to VIP-480FO Web-UI, and go to the “Dialing Plan” page. To add an Incoming Dial Plan.

Incoming Dial Plan: (maximun 50 entries, maximun length of prefix digits is 16 digit, maximun length of number is 20 digit):

Item	Incoming no.	Length of Number	Delete Length	Prefix no.	Destination telephone port	Operation
1	72x	3 ~ 16	2	None	1	
	<input type="text"/>	<input type="text"/> ~ <input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	ADD

**Incoming no.:**72x, when the subscribers of UMG-2000 dial the number start by 72, this call will send to VIP-480FO.

**Length of Number:** 3~16, to define the total number length.

**Delete Length:** 2, to remove 72

**Prefix no.:** None, no add additional digits before the dialing number

**Destination telephone port:** 1, the finial dialing number will send to FXO port1 for outgoing.

**Step2.** Login to VIP-281GS Web-UI, and go to the “Dialing Plan” page. To add an Incoming Dial Plan.

Incoming Dial Plan: (maximun 50 entries, maximun length of prefix digits is 16 digit, maximun length of number is 20 digit):

Item	Incoming no.	Length of Number	Delete Length	Prefix no.	Destination telephone port	Operation
	<input type="text" value="73x"/>	<input type="text" value="3"/> ~ <input type="text" value="16"/>	<input type="text" value="2"/>	<input type="text"/>	<input type="radio"/> FXS <input checked="" type="radio"/> GSM	ADD

**Incoming no.:**73x, when the subscribers of UMG-2000 dial the number start by 73, this call will send to VIP-281GS.

**Length of Number:** 3~16, to define the total number length.

**Delete Length:** 2, to remove 73

**Prefix no.:** None, no add additional digits before the dialing number

**Destination telephone port:** 1, the finial dialing number will send to GSM port for outgoing.

### \*\*\* Create extension on IPX-300 :

**Step1.** Login to IPX-300 Web-UI, and go to the “**IP PBX Setup >> SIP Extension Setup**” page. To add 2 extensions for VIP-360PT and UMG-2000 registrations.

**IP PBX Setup**

- User Extensions Setting**

Add New User Extensions

**Extensions List**      **Extension Max is 100**

User Extension	Password	Caller Id	Action
100	123	100	<input type="button" value="Advance"/> <input type="button" value="Delete"/>
101	123	101	<input type="button" value="Advance"/> <input type="button" value="Delete"/>

**Step2.** To setup the VIP-360PT register to IPX-300 as ext.100, and VIP-560PT register to UMG-2000 as ext.5001.

### \*\*\* Dialing Procedures :

- 1. Call to PSTN via FXO\_1 of UMG-2000**  
Ext.5001 dials 61, hear the prompt for inputting 22199518.
- 2. Call to PSTN via FXO\_1 of UMG-2000**  
Ext.5001 dials 7122199518
- 3. Call to PSTN via VIP-480FO**  
Ext.5001 dials 7222199518
- 4. Call to GSM via VIP-281GS**  
Ext.5001 dials 73093500001
- 5. Call to VIP-360PT via SIP Trunk**  
Ext.5001 dials 8100
- 6. VIP-360PT Call to VIP-560PT**  
Ext.100 dials 101 and hears welcome prompts, then dials 5001.