PLANET
Networking & Communication

Unified Office Gateway

UMG-2000 / UMG-2200

User's Manual

Copyright

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-2200
Rev: 1.0 (May. 2010)
Part No.: EM-UMG2000_2200_v1.0

Table of Contents

1. Introduction

The PLANET UMG-2000 / UMG-2200 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, and 4 / 8-Port FXO, the UMG-2000 / UMG-2200 allows you to connect to various Internet and telephone carriers.

Via the 4 / 8-Port FXO interface, the UMG-2000 / UMG-2200 provides a feature-rich IP PBX system that supports seamless communications between existing PSTN calls, analog, IP phones and SIP-based endpoints. Branch-to-Branch secured network and call features bring your remote offices together. The UMG-2000 / UMG-2200 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 / UMG-2200 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 and Call Detail Record (CDR), configuration backup and restore, secure remote management capabilities and many more.

1.1 Product Features

IP PBX / VoIP Service

- SIP 2.0 (RFC3261)
- PSTN Support
- Call-Parking, Echo Cancellation
- FXO 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

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
- 3 x RP-SMA Detachable Antenna
- Security: WEP / WPA / WPA2
- SSID
- Wireless 802.1x Authentication

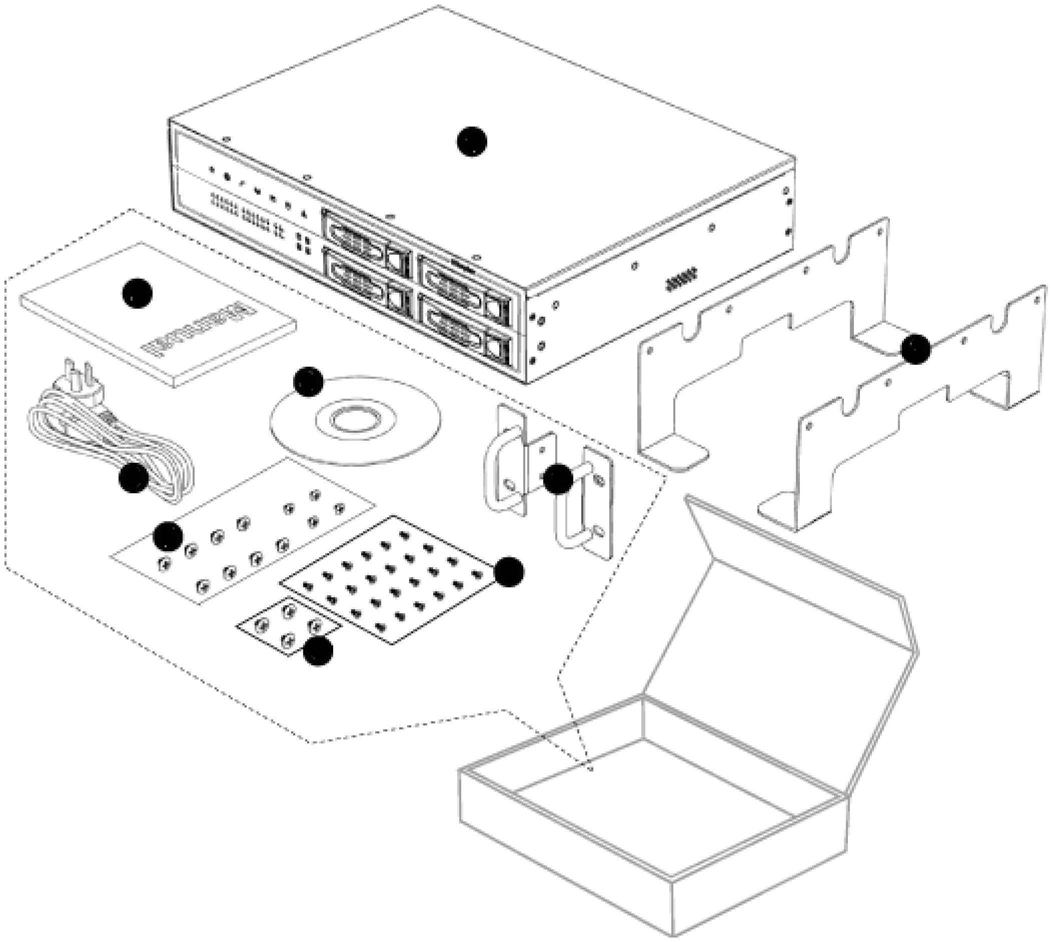
24+2G Switch Service

- IEEE 802.1d Spanning Tree
- IGMP Snooping

1.2 Package Contents

- UMG-2000 / UMG-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.

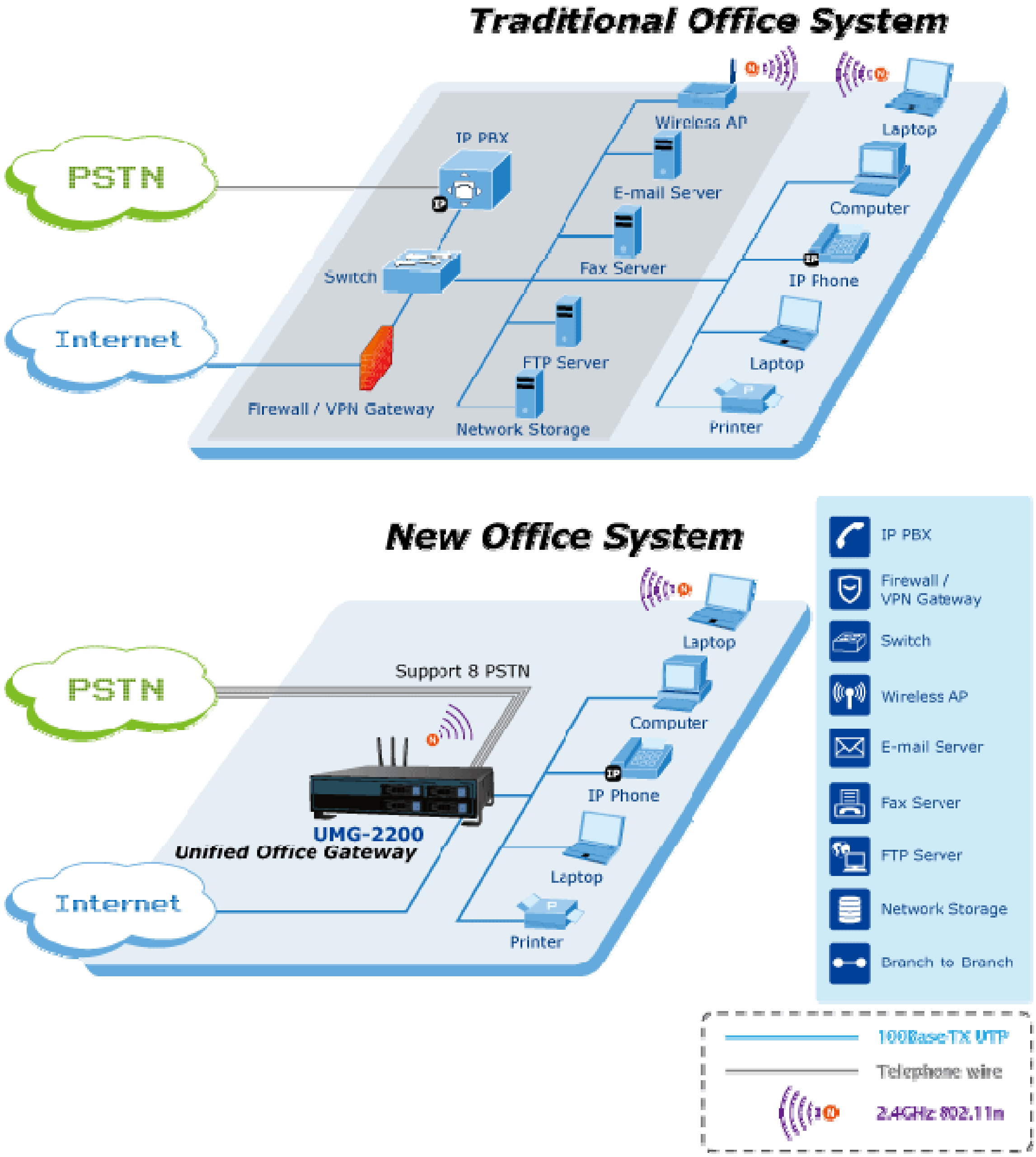


1.3 Application

Highly Integrated IT Services

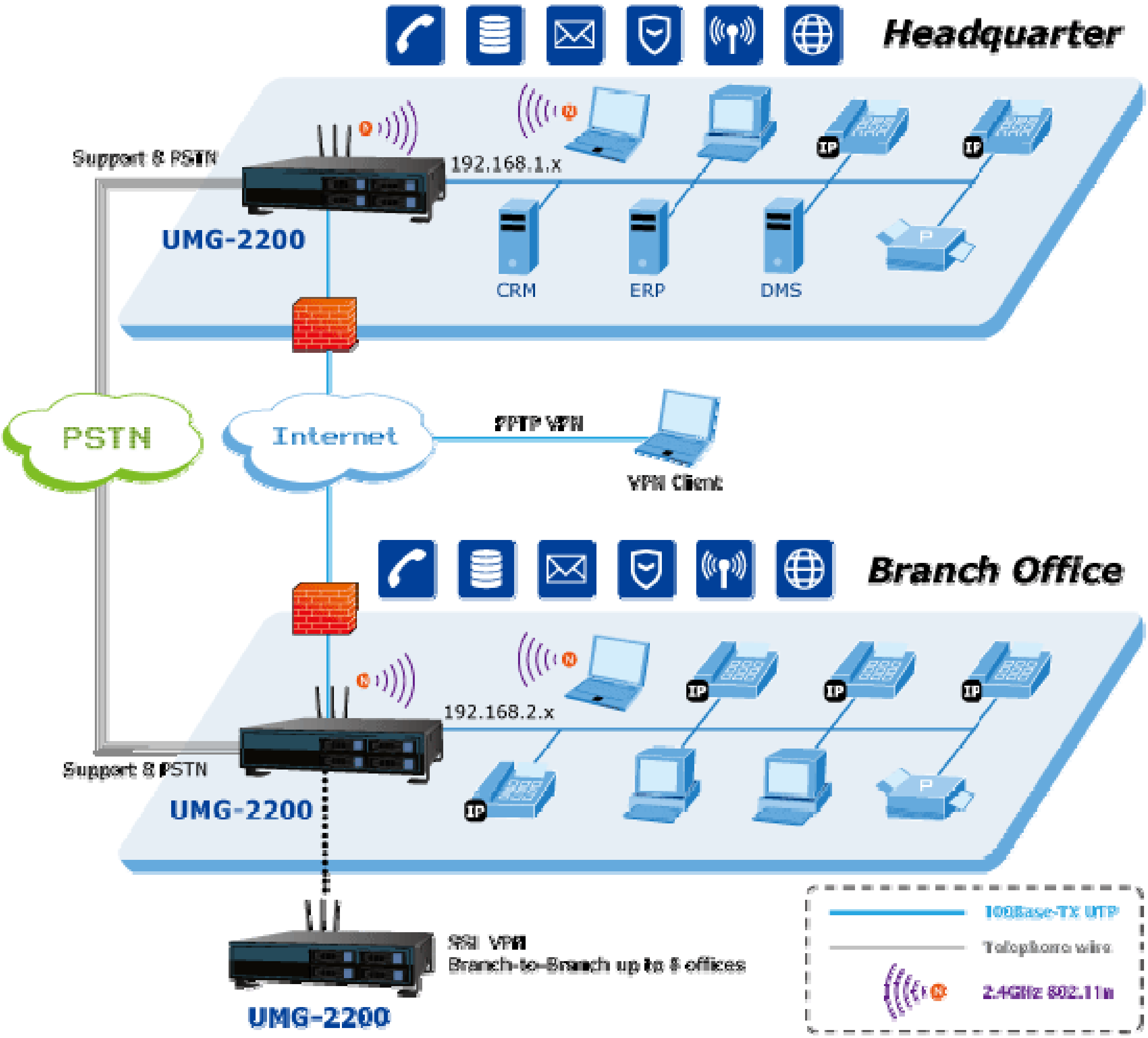
Providing IP PBX / VoIP, Internet Security, E-mail / FAX Server, Switch, Wireless AP, and Network Storage service, the UMG-2000 / UMG-2200 features single point of management to improve IT service ability.

The UMG-2000 / UMG-2200 benefits the SMBs lower cost of ownership, quick and easy deployment, low noise, space saving and energy conservation for better business environment.



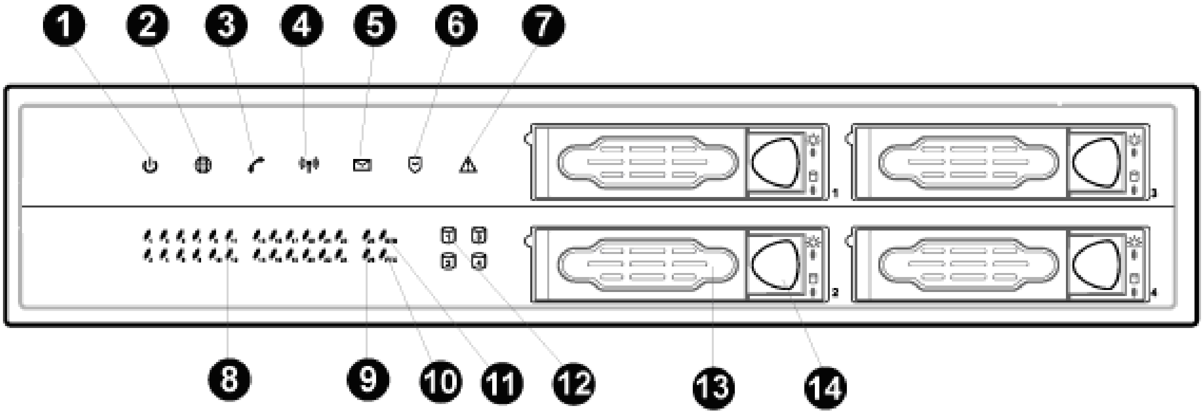
Office Voice and Data Communication

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-2000 / UMG-2200 supports Branch-to-Branch up to 8 offices.



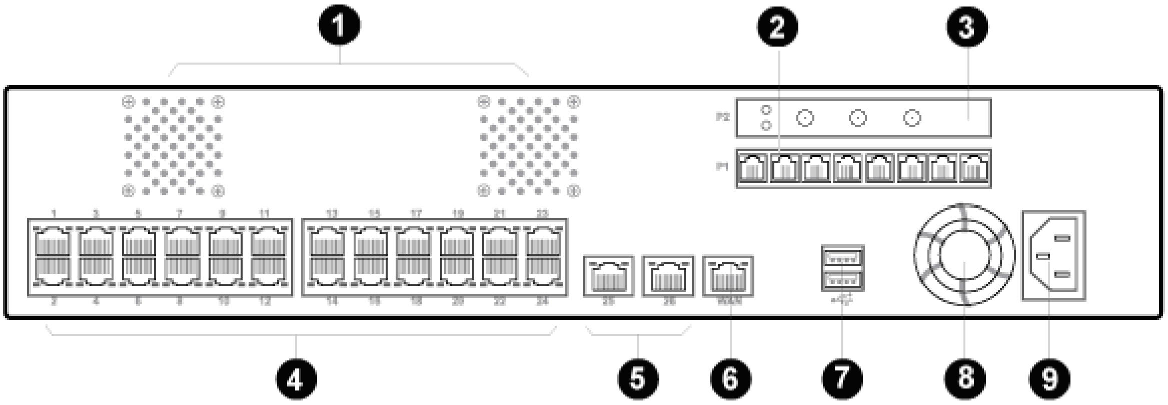
1.4 Outlook

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 hander 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)	**UMG-2000** : 4 x RJ-11 (4 x FXO) **UMG-2200** : 8 x RJ-11 (8 x FXO)
3	Wireless (P2)	1 x 802.11b/g/n Wireless Access Point, 3 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	**UMG-2000: 4 x RJ-11 (4 x FXO)** **UMG-2200: 8 x RJ-11 (8 x FXO)**
Wireless	1 x 802.11b/g/n Wireless Access Point, 3 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 - Call privilege grouping

	- FXO interface for PSTN Inbound/outbound - FXO disconnection tone detection - Caller ID detection - In-band/RFC2833/SIP-INFO DTMF translation - Music on hold (MoH), user upload MoH - Direct line Outbound - User upload IVR
Voicemail	- User PIN - 450 minutes for personal record - E-mail notification - Personal reception on unavailability - Reply call or new call in voicemail menu
E-mail	Protocol - POP3,IMAP,SMTP, Web mail Support accounts - 250 users Email Security - Secured Socket Layer (SSL) Anti-Virus - ClamAV Anti-Spam Junk mail block Mailbox size Limit - 200M/500M/1G/2G/No Limit Attachment - 2M/5M/10M/20M/50M/No Limit Block List - Share/User/Domain security modes Email Backup - Auto-Backup
Network Storage	RAID - RAID 0, RAID 0/1, RAID 5, JBOD Date Sharing - Windows Network Sharing, NFSv3
Security	Network Security - DoS attack Prevention VPN Max. connection - 100 PPTP VPN tunnels - 8 Site-to-Site SSL VPN tunnels VPN pass-through - IPSec, PPTP, L2TP pass-through Internet Security - Domain/Keyword Content Filter, Access Control - IP-MAC Binding
Other Protocol / Function	Protocol - TCP/IP, NAT, DHCP, HTTP, DNS, NTP, HTTPS, CIFS/SMB, NFSv3 LAN - IEEE 802.1d Spanning Tree Internet Access - Static IP, PPPoE, DHCP, PPTP, L2TP DMZ, UPnP, QoS, DDNS Multiple host name
Management	- Web based GUI management - Firmware upgradeable via local

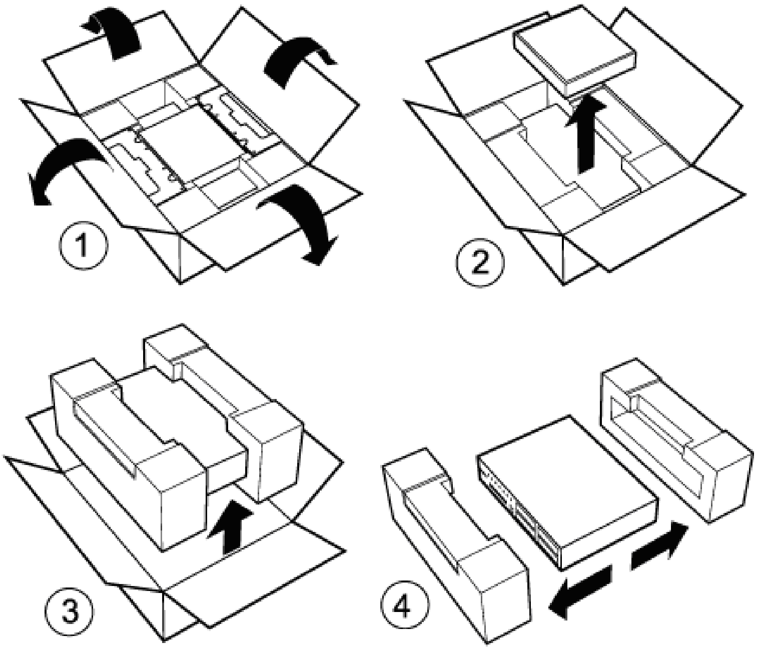
2. Installation

The followings are instructions for setting up the UMG-2000 / UMG-2200. Refer to the illustration and follow the steps install your unified office gateway.

2.1 Hardware Installaion

2.1.1 Unpack the UMG-2000 / UMG-2200

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 / UMG-2200 itself shows damage you should file a damage claim with the carrier to who delivered it. Unpack the UMG-2000 / UMG-2200 as listed below.



2.1.2 Choosing a Setup Location

Decide on a suitable location for the UMG-2000 / UMG-2200 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 / UMG-2200 near a grounded power outlet and pay attention to the following requirements.

- Leave approximately 40cm (16inche) of clearance in front of the UMG-2000 / UMG-2200 to ensure the disk carriers can be unplugged.
- Leave approximately 30cm (12 inch) of clearance in the back of the UMG-2000 / UMG-2200 to allow for sufficient airflow and ease in servicing.

2.1.3 Preparing for Setup

The UMG-2000 / UMG-2200 system was shipped with desk brackets, ear brackets, and mounting screws, so it is possible to install the UMG-2000 / UMG-2200 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 / UMG-2200 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.

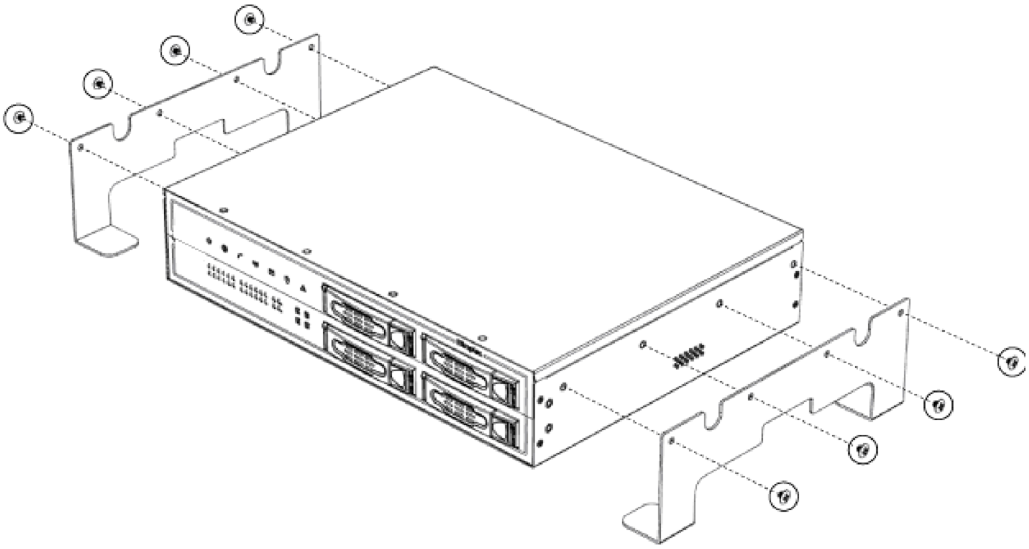
REDUCED AIRFLOW
Consideration should be given to the amount of airflow required for safe operation maybe not compromised for the rack mounting.

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 / UMG-2200.
- The desk brackets have been fixed to the device before packing.
- Place the system to appropriate site.

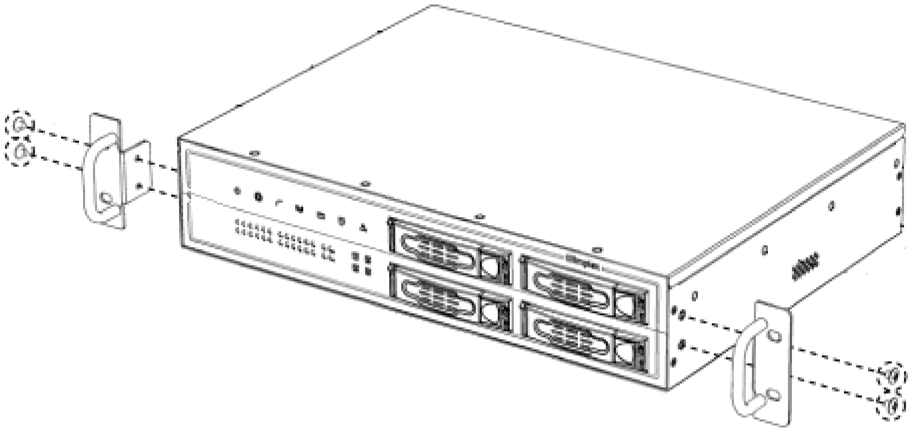


2.1.7 The Rack Mount Installation

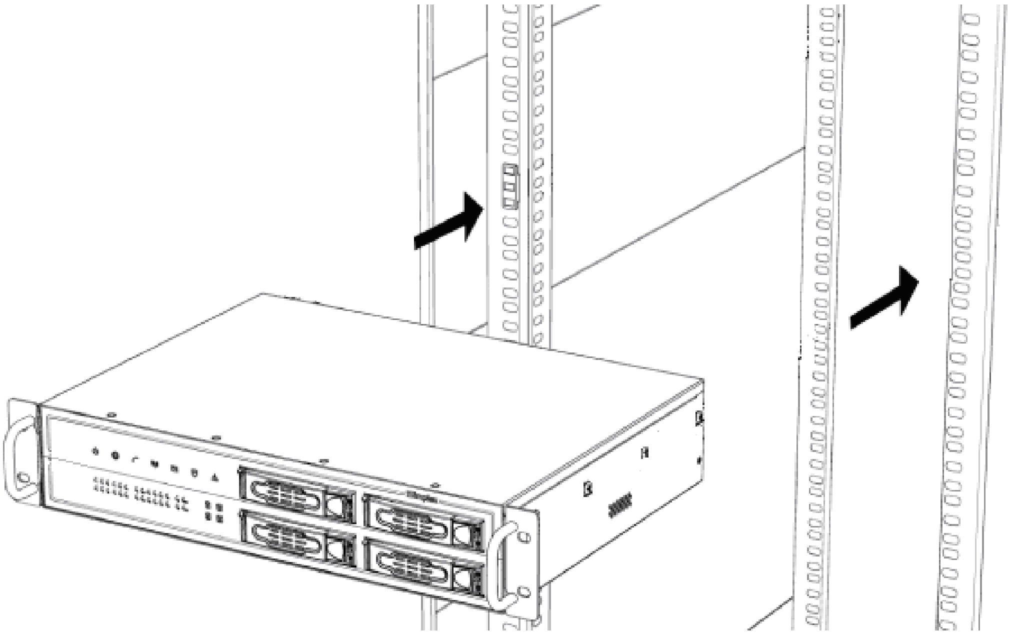
It is strongly recommended to securely fasten the mounting rack to the floor or wall to eliminate any possibility of tipping over the rack. This is especially important if you decide to install several UMG-2000 / UMG-2200 chassis in the top of the rack.

A brief overview of the UMG-2000 / UMG-2200 installation is as follows:

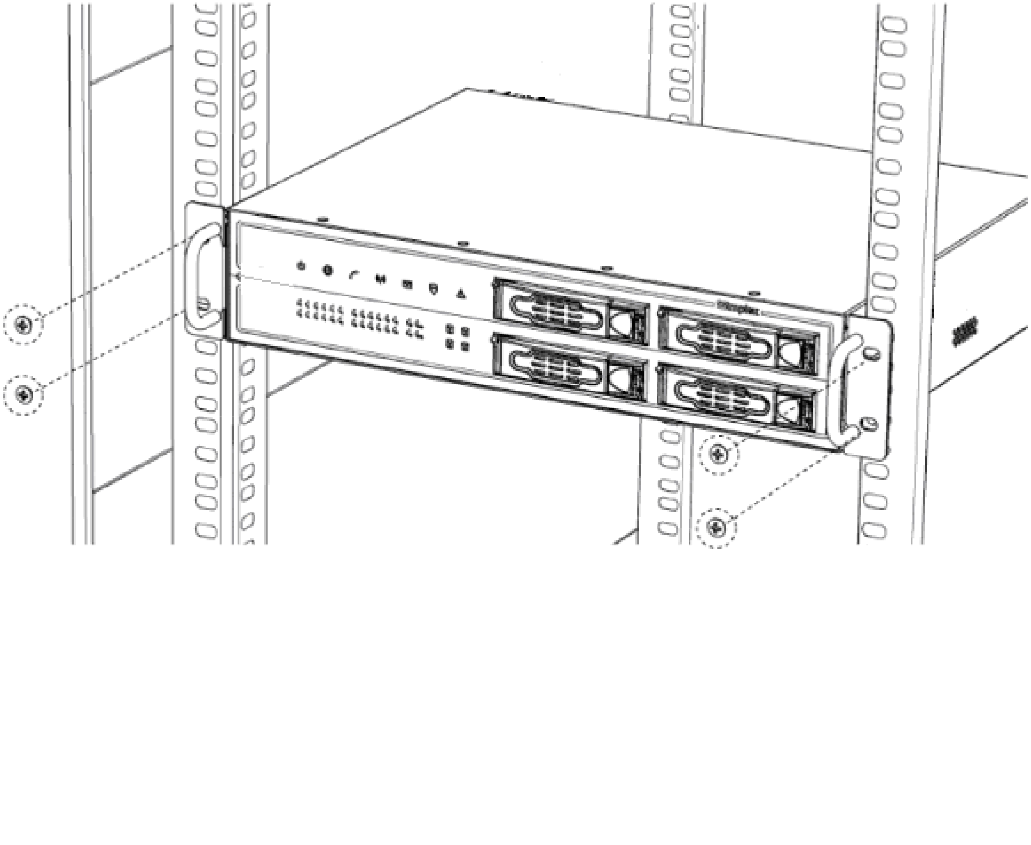
- Select an appropriate site in the rack.
- Unload 4 the plug screws from each side of the server.
- Mount the ear brackets to the server from the each side.



- Mount the server into the rack.



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

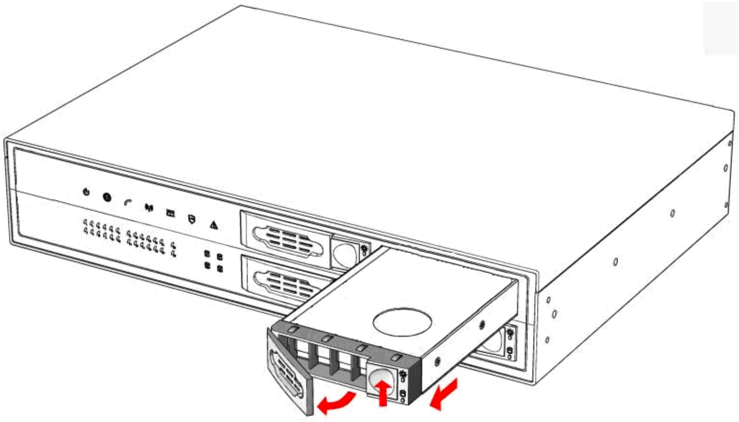


2.1.8 The Hard Disk Installation

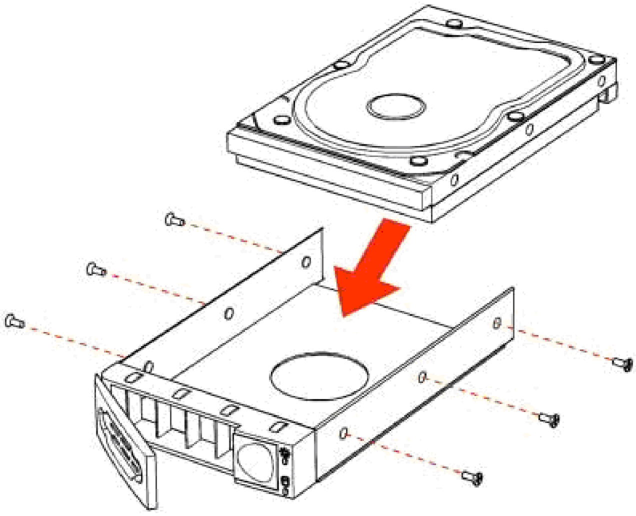
The SATA subsystem supports four hot-swappable hard drives. The SATA drives are inserted to the SATA backplane that provides power and bus termination.

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.

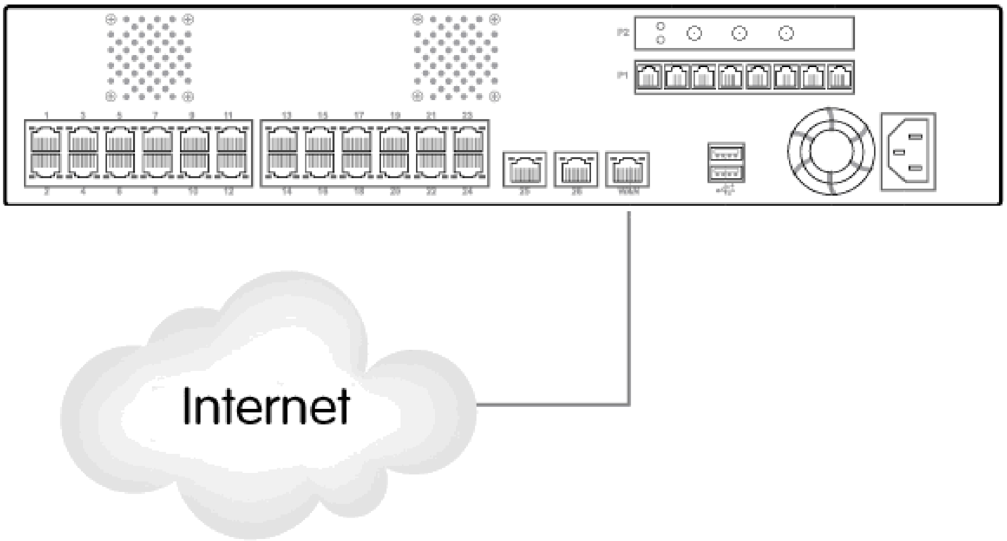


- Press the disk carrier switch to insert the carrier to the disk slot.
- Close the disk carrier lock/switch to lock the carrier.

2.2 Physical Connection

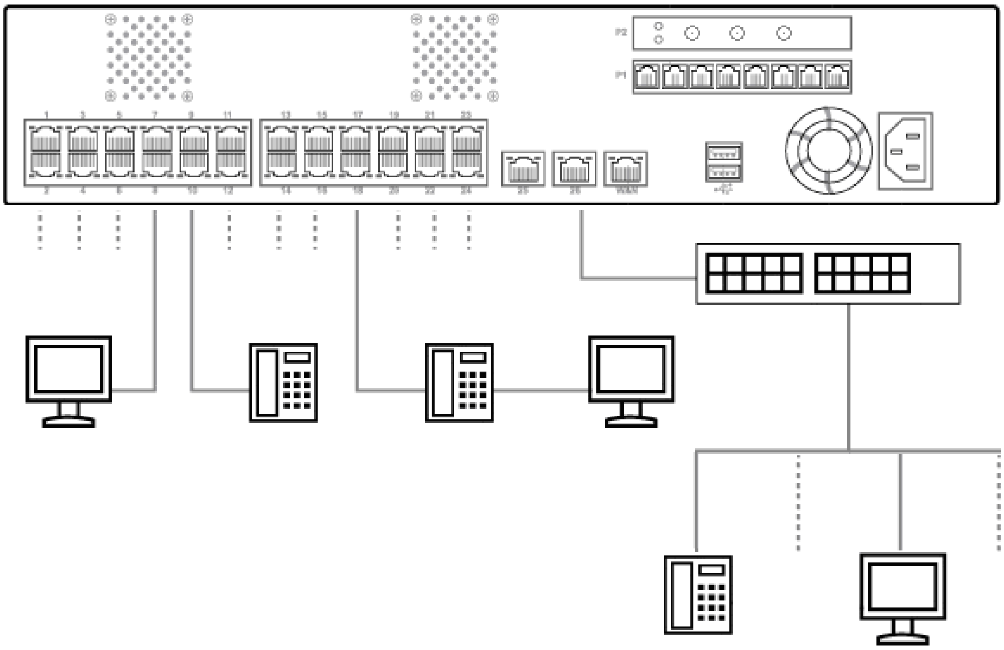
2.2.1 WAN Connection

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



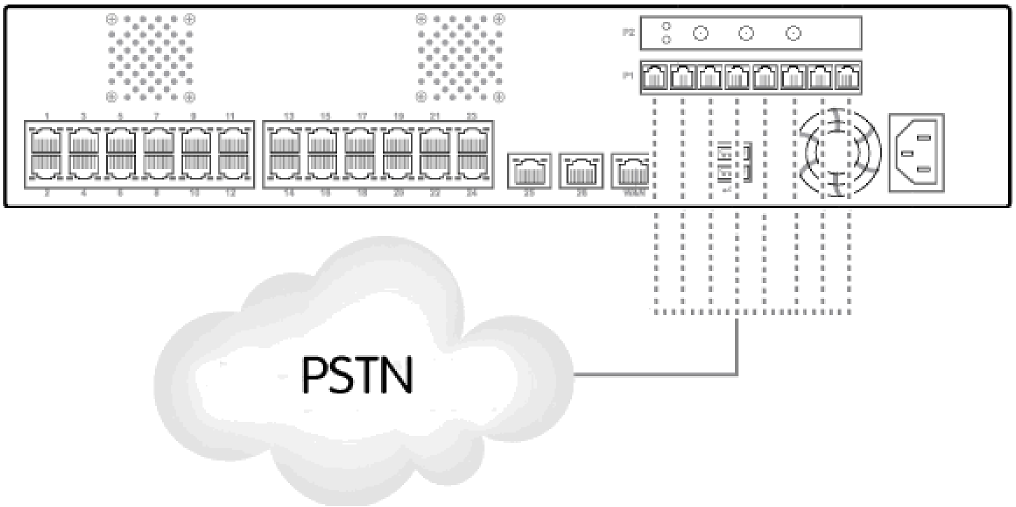
2.2.2 LAN Port Connection

- 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.



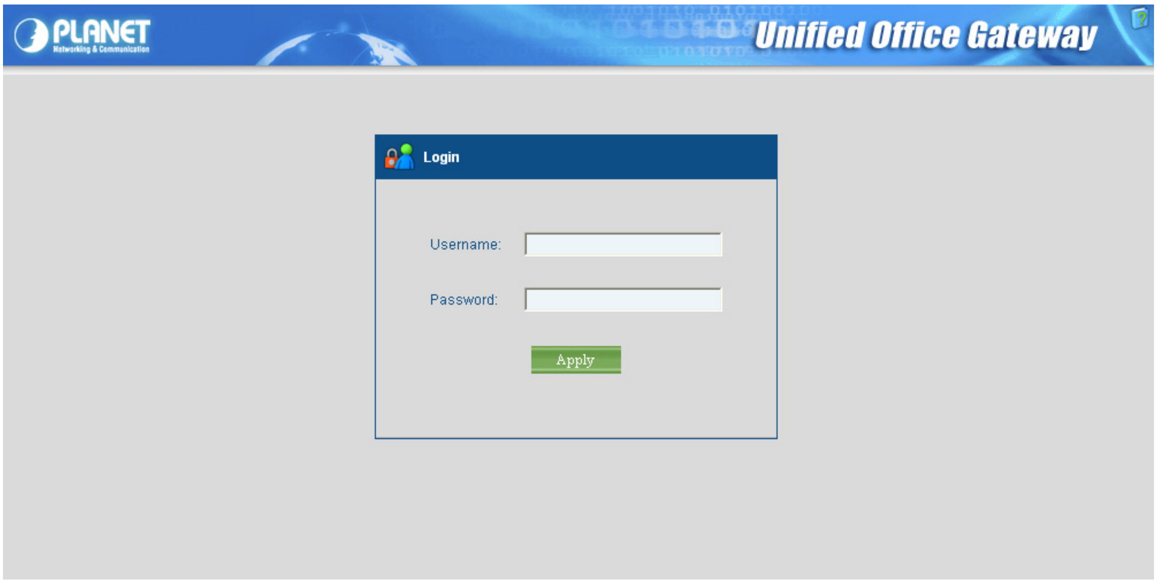
2.3 Quick Setup Wizard

2.3.1 First Time Login

Now that the network connection between your PC and UMG-2000 / UMG-2200 has been established, you must login in order to access PLANET View.

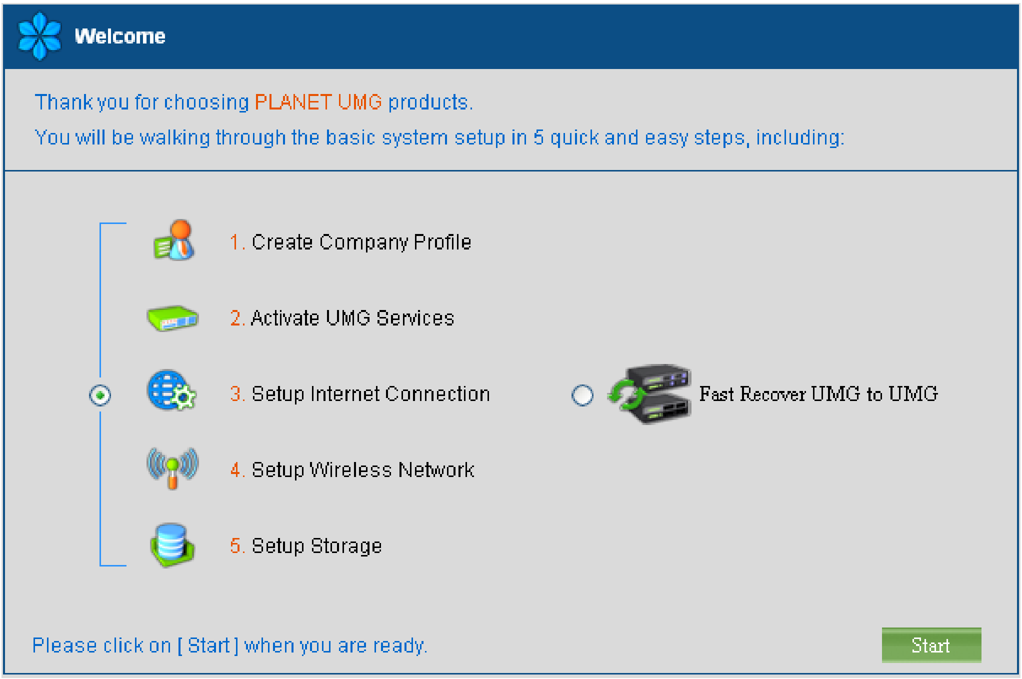
Launch a web browser (for example: IE, Firefox etc.) and type the UMG-2000 / UMG-2200 IP address in the address bar. The default address is **"http://192.168.1.1"**.

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.



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 / UMG-2200 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 / UMG-2200. Check the first radio box and then click the button “Start” to continue.



Welcome

Thank you for choosing PLANET UMG products.

You will be walking through the basic system setup in 5 quick and easy steps, including:

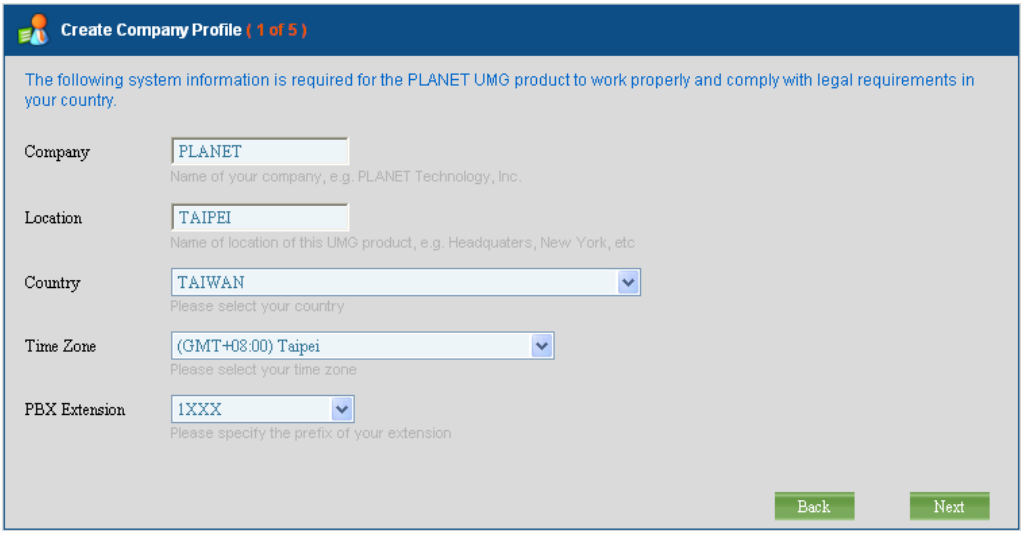
● 1. Create Company Profile
2. Activate UMG Services
3. Setup Internet Connection
4. Setup Wireless Network
5. Setup Storage

○ Fast Recover UMG to UMG

Please click on [Start] when you are ready.

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.



Create Company Profile (1 of 5)

The following system information is required for the PLANET UMG product to work properly and comply with legal requirements in your country.

Company: PLANET
Name of your company, e.g. PLANET Technology, Inc.

Location: TAIPEI
Name of location of this UMG product, e.g. Headquaters, New York, etc

Country: TAIWAN
Please select your country

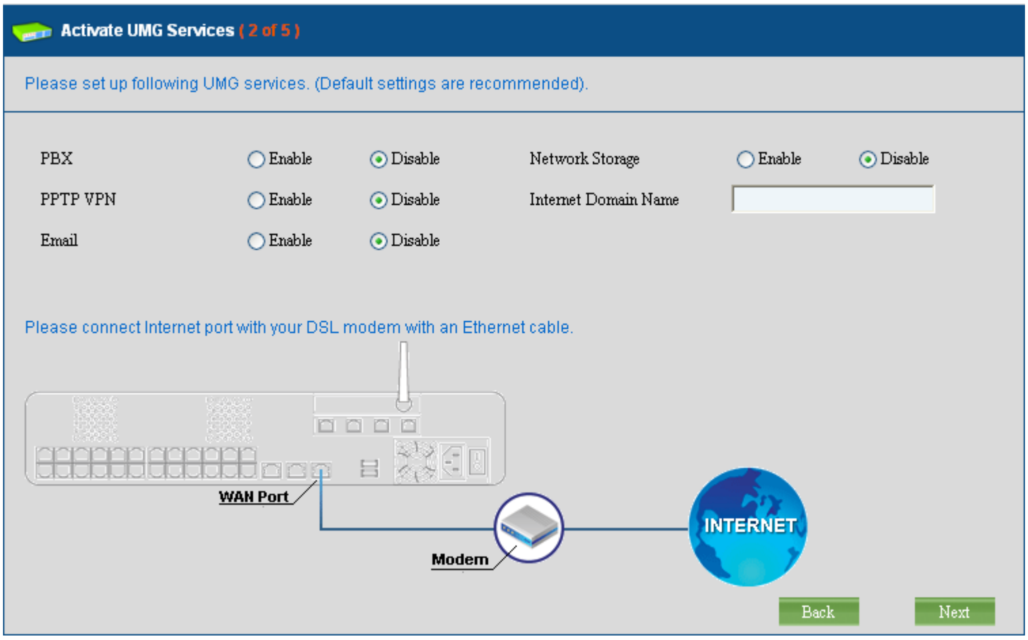
Time Zone: (GMT+08:00) Taipei
Please select your time zone

PBX Extension: 1XXX
Please specify the prefix of your extension

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 / UMG-2200 services

The UMG-2000 / UMG-2200 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.



Activate UMG Services (2 of 5)

Please set up following UMG services. (Default settings are recommended).

PBX ○ Enable ● Disable

PPTP VPN ○ Enable ● Disable

Email ○ Enable ● Disable

Network Storage ○ Enable ● Disable

Internet Domain Name

Please connect Internet port with your DSL modem with an Ethernet cable.

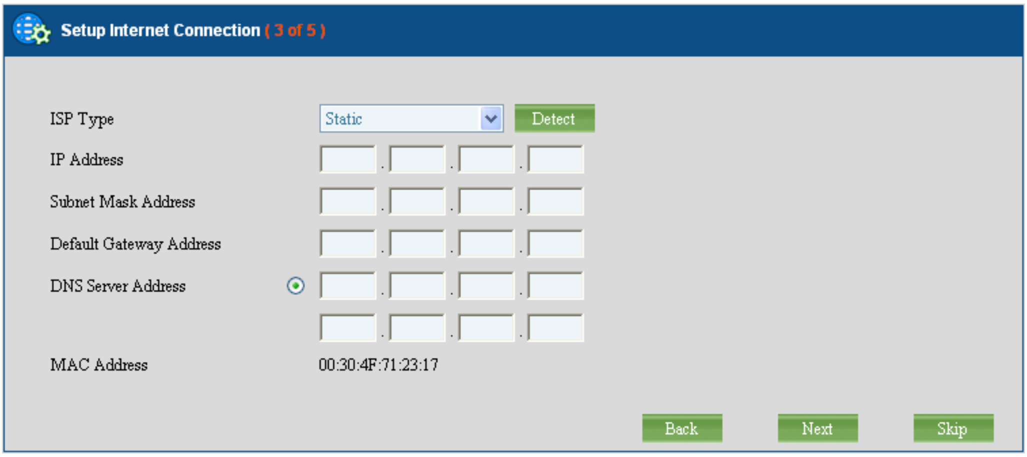
Item	Description
PBX	Enable or disable the IP PBX service.
PPTP VPN	Enable or disable the PPTP VPN service.
Email	Enable or disable the Email service.
Network Storage	Enable or disable the network storage service.
Internet Domain Name	Specify a valid Internet domain for the email server if the email 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 / UMG-2200 to recognize the ISP type automatically.



Setup Internet Connection (3 of 5)

ISP Type: Static

IP Address

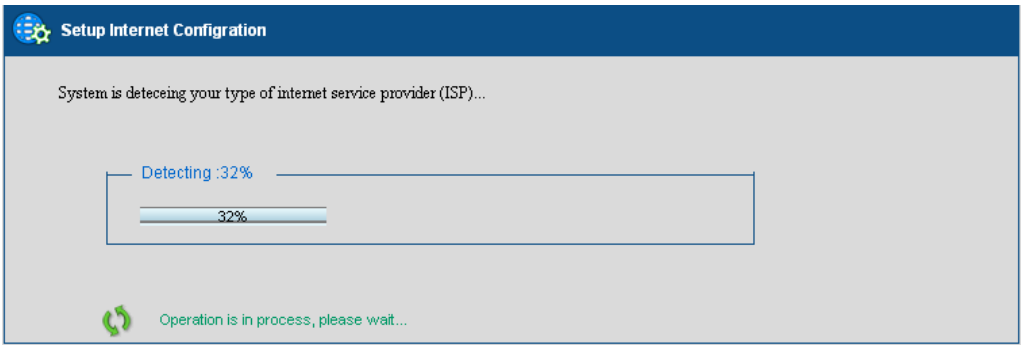
Subnet Mask Address

Default Gateway Address

DNS Server Address ◉

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

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



Setup Internet Configration

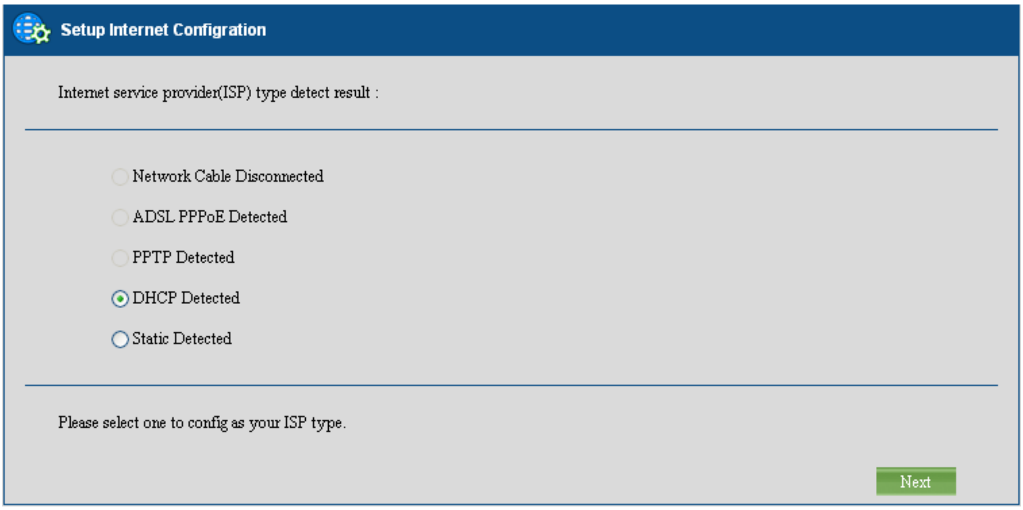
System is deteceing your type of internet service provider (ISP)...

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.



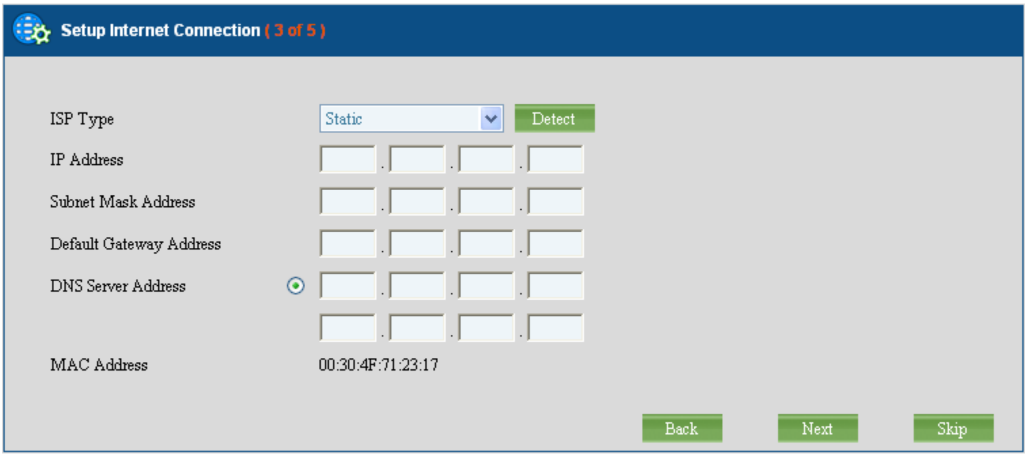
Internet service provider(ISP) type detect result :

○ Network Cable Disconnected
○ ADSL PPPoE Detected
○ PPTP Detected
● DHCP Detected
○ Static Detected

Please select one to config as your ISP type.

MANUAL SETUP INTERNET CONFIURATION: STATIC

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



ISP Type: Static

IP Address

Subnet Mask Address

Default Gateway Address

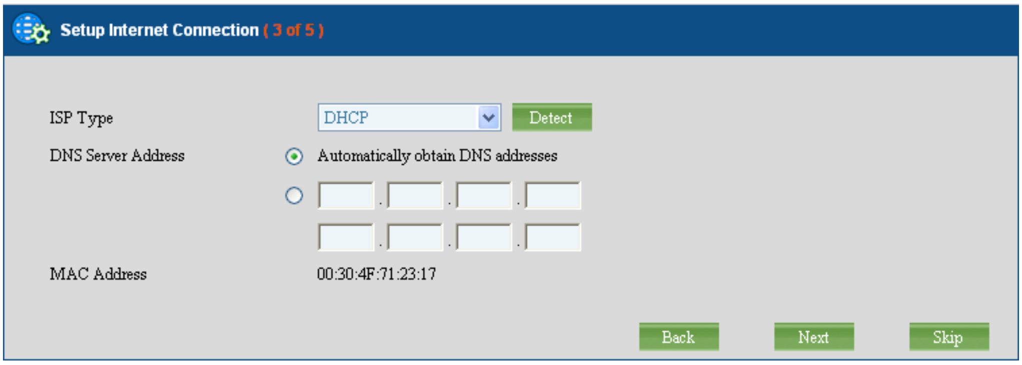
DNS Server Address ●

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

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.



Setup Internet Connection (3 of 5)

ISP Type: DHCP

DNS Server Address: ● Automatically obtain DNS addresses

○ ___ . ___ . ___ . ___

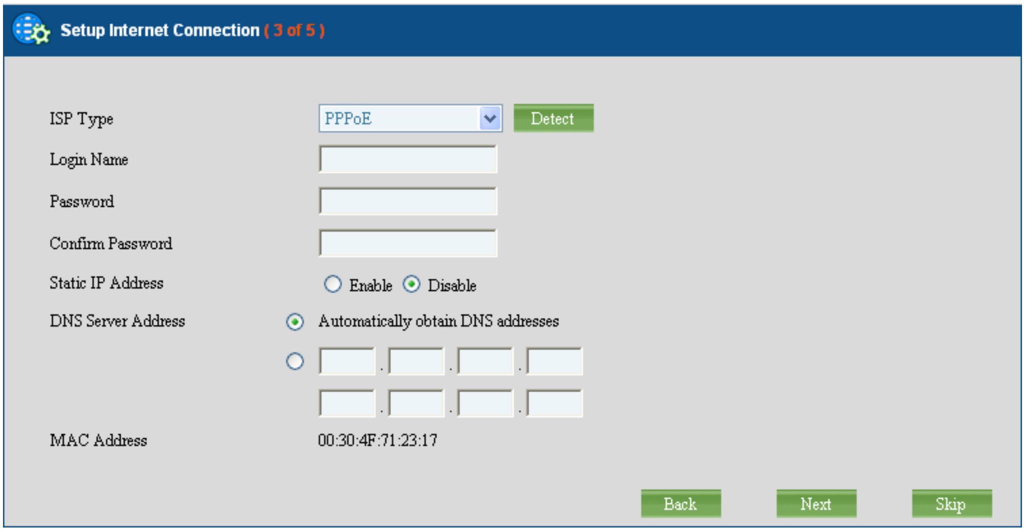
___ . ___ . ___ . ___

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

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.



Setup Internet Connection (3 of 5)

ISP Type: PPPoE

Login Name:

Password:

Confirm Password:

Static IP Address: ○ Enable ● Disable

DNS Server Address: ● Automatically obtain DNS addresses

○ ___ . ___ . ___ . ___

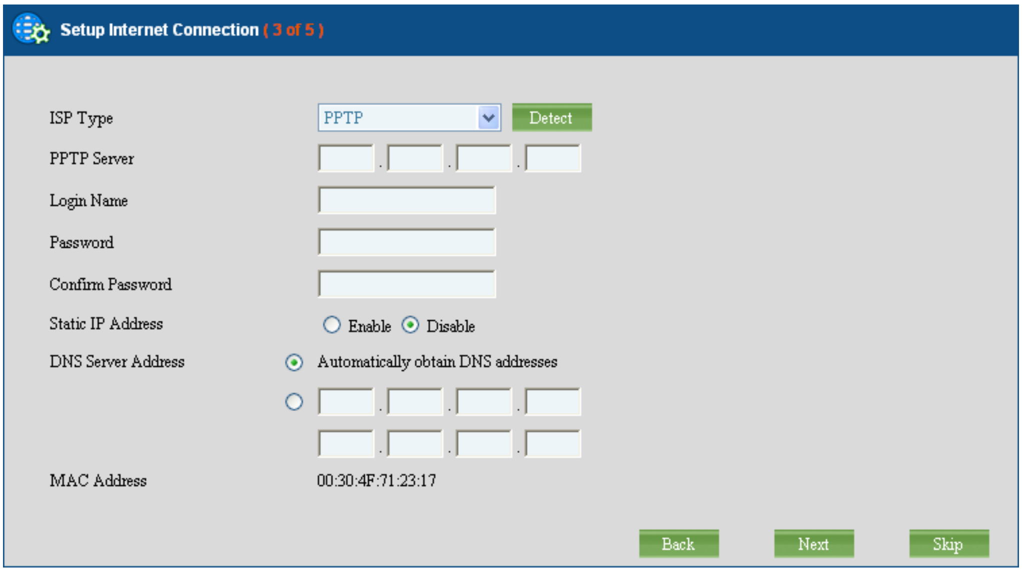
___ . ___ . ___ . ___

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

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.



Setup Internet Connection (3 of 5)

ISP Type: PPTP

PPTP Server: . . .

Login Name:

Password:

Confirm Password:

Static IP Address: ○ Enable ● Disable

DNS Server Address: ● Automatically obtain DNS addresses

○ . . .

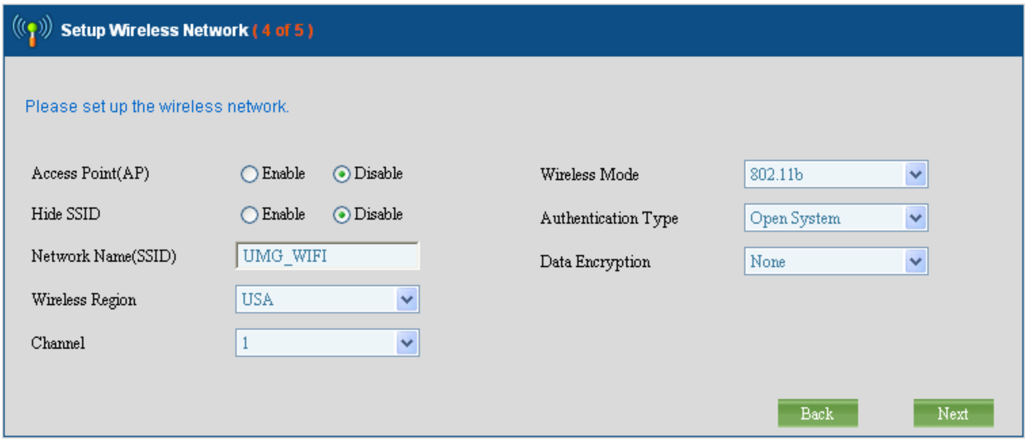
. . .

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

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.



Please set up the wireless network.

Access Point(AP) ○ Enable ● Disable

Hide SSID ○ Enable ● Disable

Network Name(SSID): UMG_WIFI

Wireless Region: USA

Channel: 1

Wireless Mode: 802.11b

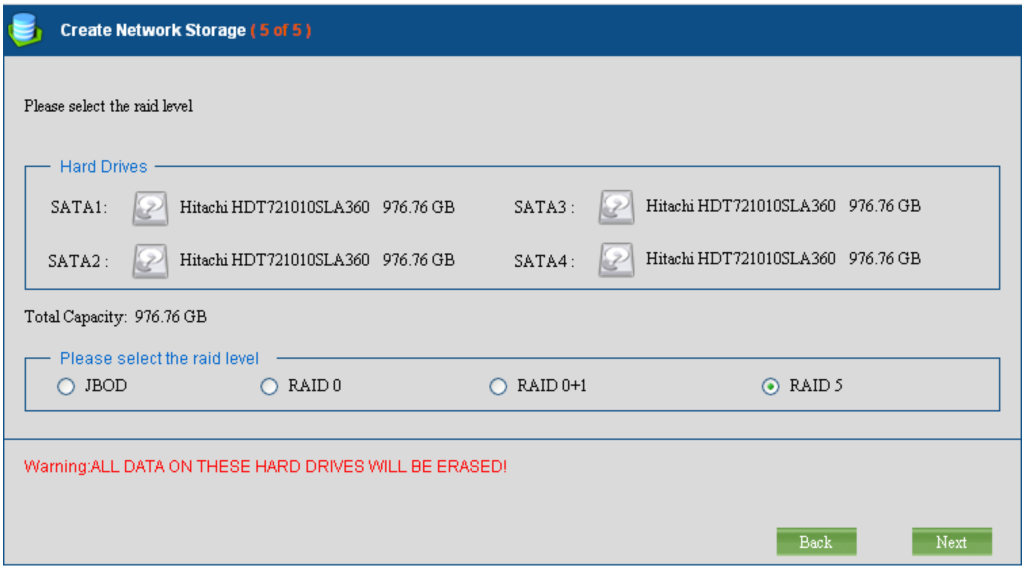
Authentication Type: Open System

Data Encryption: None

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

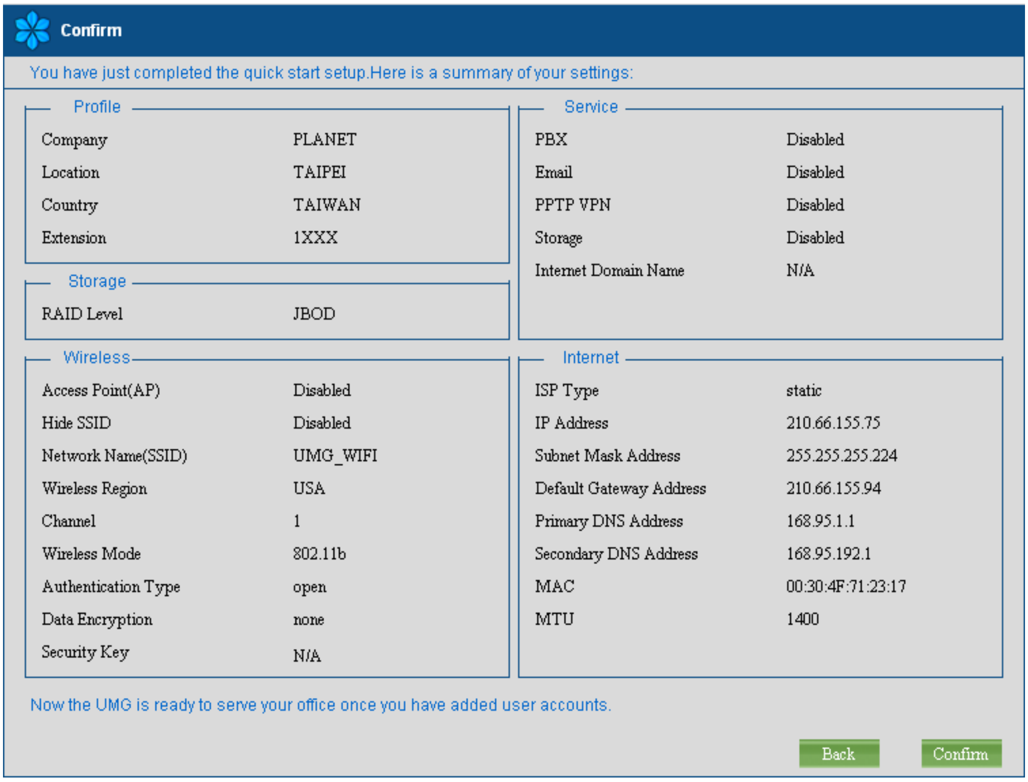
Please select the raid level

○ JBOD ○ RAID 0 ○ RAID 0+1 ● RAID 5

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

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:

Profile

Company	PLANET
Location	TAIPEI
Country	TAIWAN
Extension	1XXX

Service

PBX	Disabled
Email	Disabled
PPTP VPN	Disabled
Storage	Disabled
Internet Domain Name	N/A

Storage

RAID Level	JBOD

Wireless

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

Internet

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

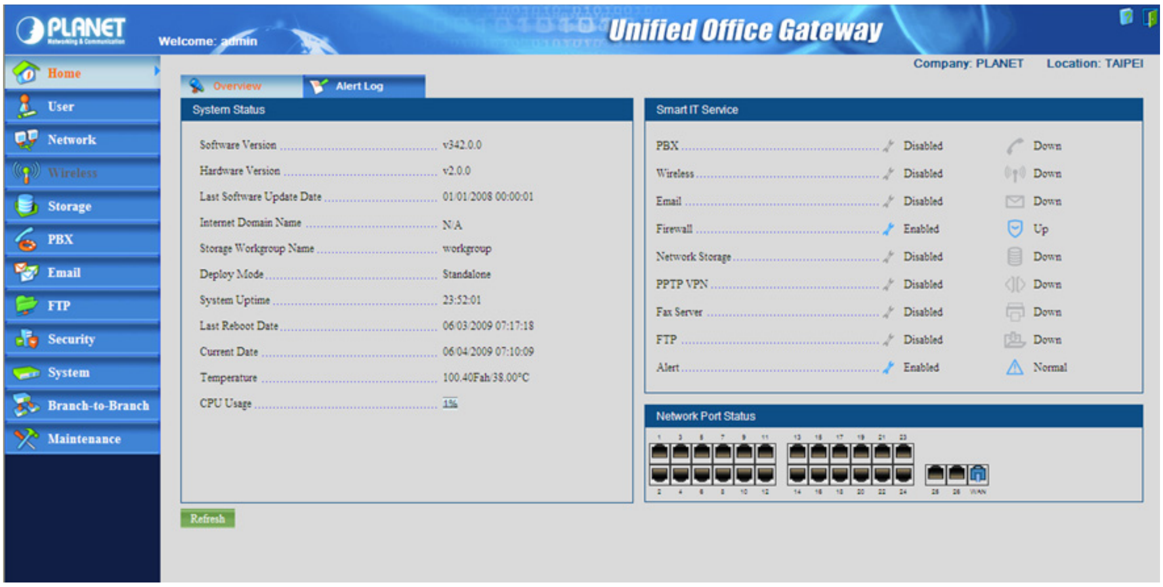
Now the UMG is ready to serve your office once you have added user accounts.

3. Web Management - Home

UMG-2000 / UMG-2200 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 / UMG-2200.

3.1 Overview

The “Overview” screen presents the UMG-2000 / UMG-2200 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.



Welcome: admin

Company: PLANET   Location: TAIPEI

System Status

Software Version	v342.0.0
Hardware Version	v2.0.0
Last Software Update Date	01/01/2008 00:00:01
Internet Domain Name	N/A
Storage Workgroup Name	workgroup
Deploy Mode	Standalone
System Uptime	23:52:01
Last Reboot Date	06/03/2009 07:17:18
Current Date	06/04/2009 07:10:09
Temperature	100.40Fah/38.00°C
CPU Usage	1%

Smart IT Service

PBX	Disabled	Down
Wireless	Disabled	Down
Email	Disabled	Down
Firewall	Enabled	Up
Network Storage	Disabled	Down
PPTP VPN	Disabled	Down
Fax Server	Disabled	Down
FTP	Disabled	Down
Alert	Enabled	Normal

Network Port Status

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 / UMG-2200, 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.

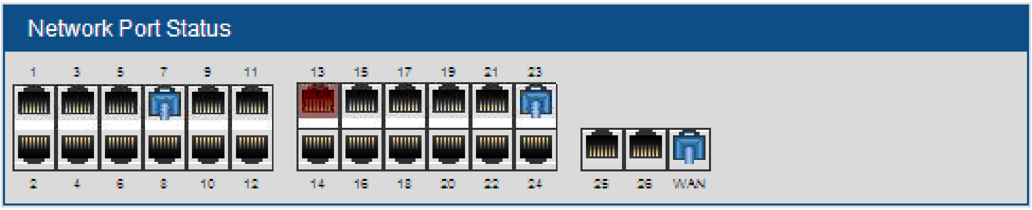
Port 25: Displays the physical link state of the 10/100/1000 Mbps network port, connected or disconnected.

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.

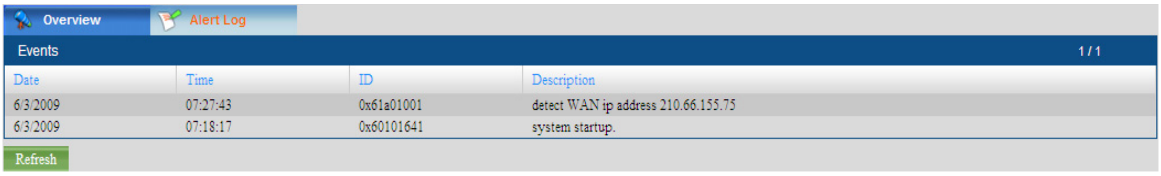
3.2 Spanning Tree Protocol

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 / UMG-2200 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 / UMG-2200 alert log list. If the administrator has assigned the alert email address, the messages will be sent to the added email address.



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.

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

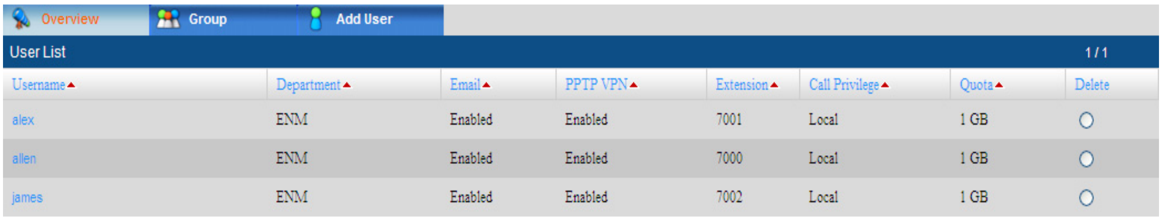
The UMG-2000 / UMG-2200 provides a user based service provisioning with secured access control based on the given privilege.

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.)



User List 1 / 1

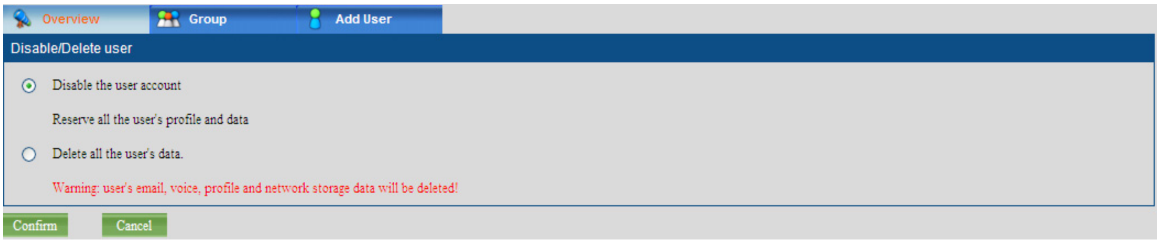
Username▲	Department▲	Email▲	PPTP VPN▲	Extension▲	Call Privilege▲	Quota▲	Delete
alex	ENM	Enabled	Enabled	7001	Local	1 GB	○
allen	ENM	Enabled	Enabled	7000	Local	1 GB	○
james	ENM	Enabled	Enabled	7002	Local	1 GB	○

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.



Disable/Delete user

● Disable the user account

Reserve all the user's profile and data

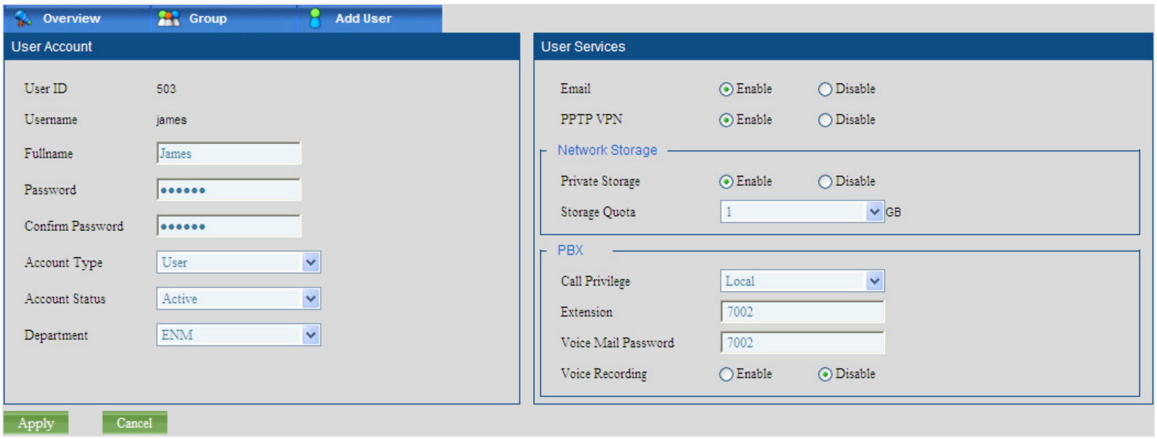
○ Delete all the user's data.

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

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.



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

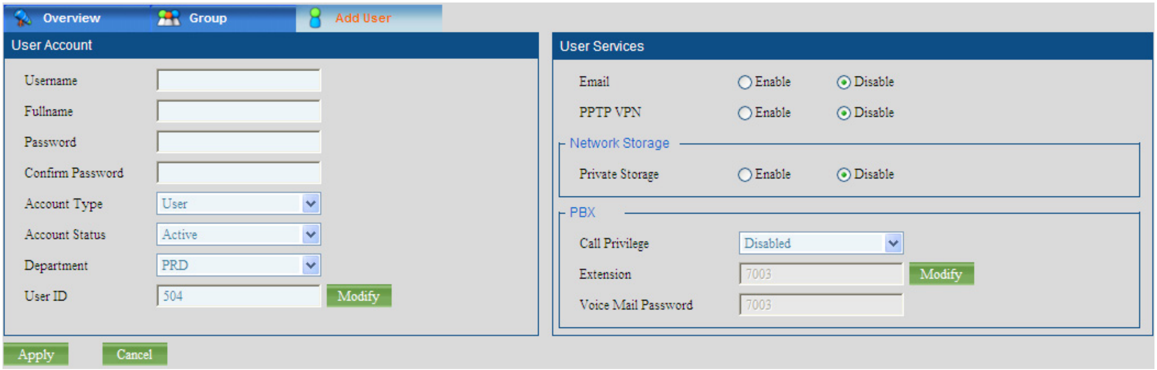
Private Storage	● Enable	○ Disable
Storage Quota	1 GB	

PBX

Call Privilege	Local	
Extension	7002	
Voice Mail Password	7002	
Voice Recording	○ Enable	● Disable

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

Username	
Fullname	
Password	
Confirm Password	
Account Type	User
Account Status	Active
Department	PRD
User ID	504

User Services

Email	○ Enable	● Disable
PPTP VPN	○ Enable	● Disable

Network Storage

Private Storage	○ Enable	● Disable

PBX

Call Privilege	Disabled
Extension	7003
Voice Mail Password	7003

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 / UMG-2200 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.

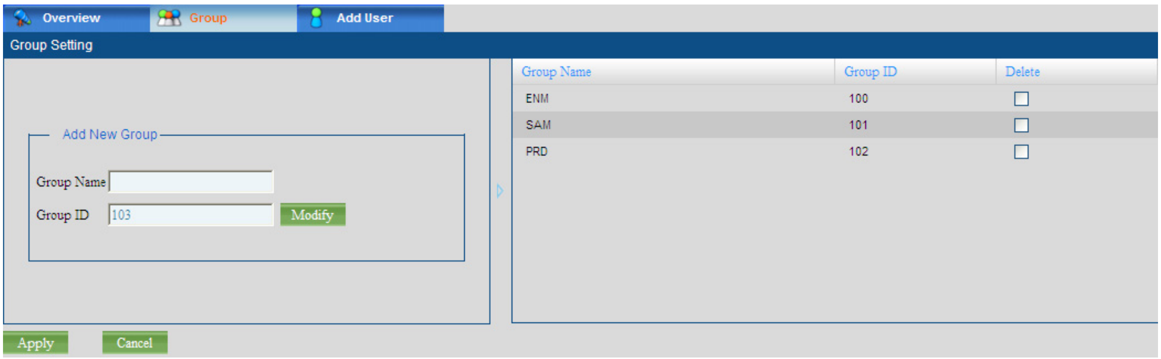
USER SERVICES:

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.



Group Name:
Group ID: 103

Group Name	Group ID	Delete
ENM	100	□
SAM	101	□
PRD	102	□

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

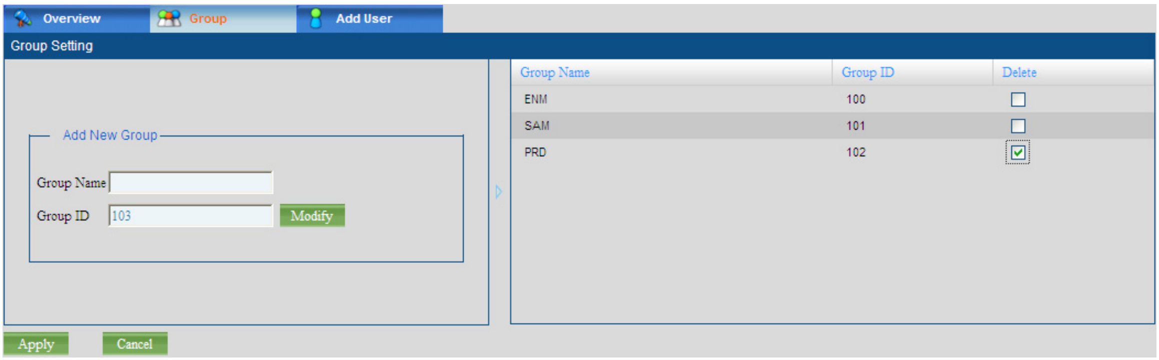
This section lists available group information:

- **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.



Group ID: 103

Group Name	Group ID	Delete
ENM	100	□
SAM	101	□
PRD	102	☑

5. Web Management - Network

The UMG-2000 / UMG-2200 network management suite provides the administrator the ability to co figurate Internet service, Local Area Network services, FTP control services, NTP service and network storage security services.

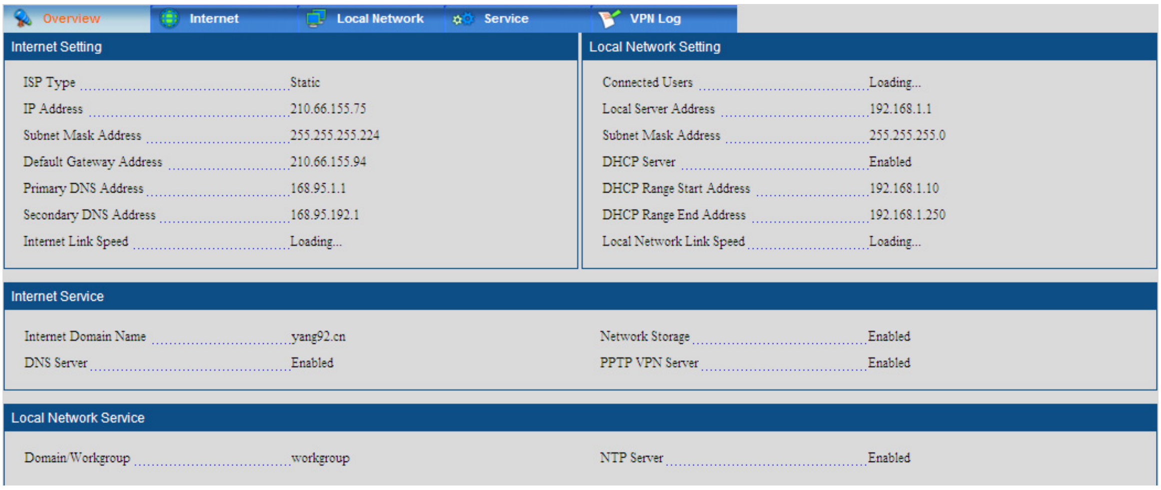
INERNET Configuration
The UMG-2000 / UMG-2200 provides 10/100Mbps WAN ports as the internet interface and supports static IP, DHCP, PPTP and PPPoE as the ISP type. Internet management provides the ability for the administrator to manage the configuration of the Internet interface. The UMG-2000 / UMG-2200 can also works 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 / UMG-2200.

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 / UMG-2200 provides 24x4 10/100 Mbps and 2x10/100/1000 Mbps ports for LAN switching. The UMG-2000 / UMG-2200 also provides the Spanning Tree Protocol (STP) to prevent undesirable loops in the network.

NETWORK SERVICES Configuration
The UMG-2000 / UMG-2200 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

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
Internet Link Speed	Loading...

Local Network Setting

Connected Users	Loading...
Local Server Address	192.168.1.1
Subnet Mask Address	255.255.255.0
DHCP Server	Enabled
DHCP Range Start Address	192.168.1.10
DHCP Range End Address	192.168.1.250
Local Network Link Speed	Loading...

Internet Service

Internet Domain Name	yang92.cn	Network Storage	Enabled
DNS Server	Enabled	PPTP VPN Server	Enabled

Local Network Service

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 / UMG-2200.
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 / UMG-2200.
Local Server Address: Displays the LAN IP address of the UMG-2000 / UMG-2200.
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.

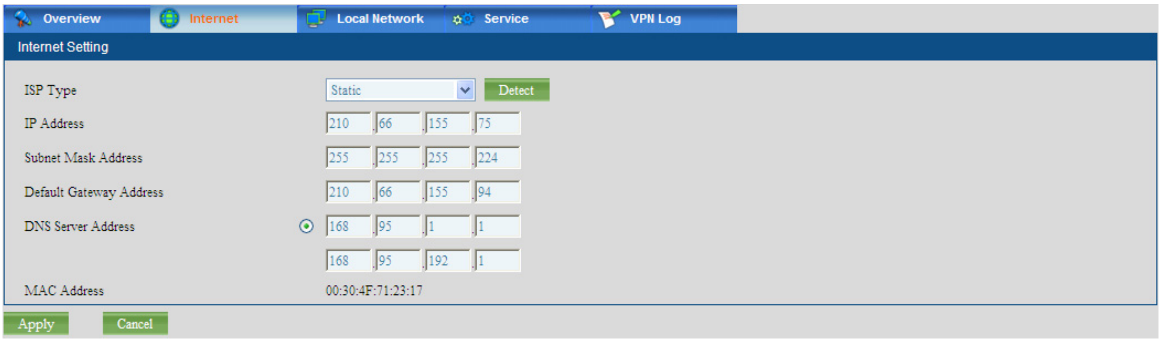
LOCAL NETWORK SERVICES

This section lists the service state of the LAN services:

Domain Controller: Displays whether the UMG-2000 / UMG-2200 is the domain controller.
Domain Work Group: Displays the Windows workgroup that UMG-2000 / UMG-2200 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.

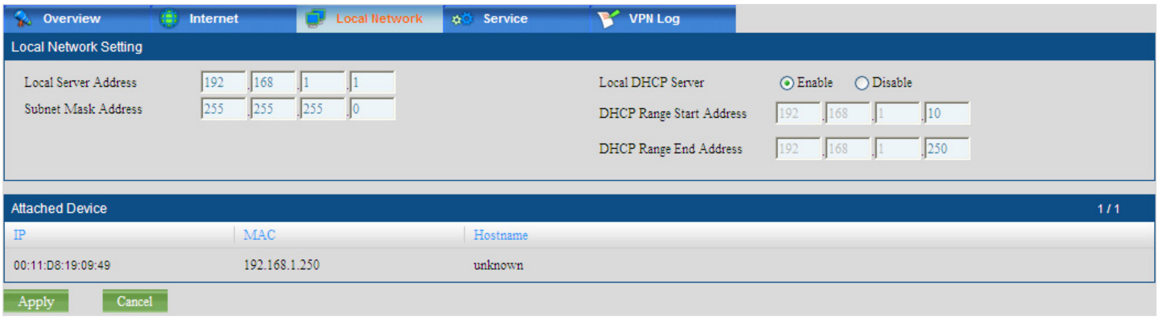


Internet Setting

ISP Type	Static
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
	168 . 95 . 192 . 1
MAC Address	00:30:4F:71:23:17

5.3 Local Network

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



Local Network Setting

Local Server Address	192 . 168 . 1 . 1	Local DHCP Server	● Enable ○ Disable
Subnet Mask Address	255 . 255 . 255 . 0	DHCP Range Start Address	192 . 168 . 1 . 10
		DHCP Range End Address	192 . 168 . 1 . 250

Attached Device 1 / 1

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

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 / UMG-2200

Subnet Mask Address: Specifies the LAN subnet mask address.

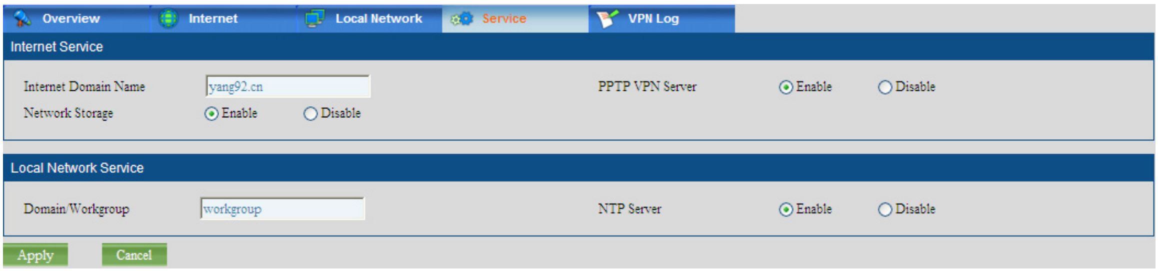
DHCP Server: Specifies the state of the DHCP server, enabled or disabled.

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.



Internet Service

Internet Domain Name: yang92.cn

PPTP VPN Server: ● Enable ○ Disable

Network Storage: ● Enable ○ Disable

Local Network Service

Domain/Workgroup: workgroup

NTP Server: ● Enable ○ Disable

INTERNET SERVICES

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

Internet Domain Name: Specifies the Internet domain name.
PPTP VPN Server: Enables or disables the PPTP VPN service.
Network Storage: Enables or disables the network storage server (SAMBA) service.

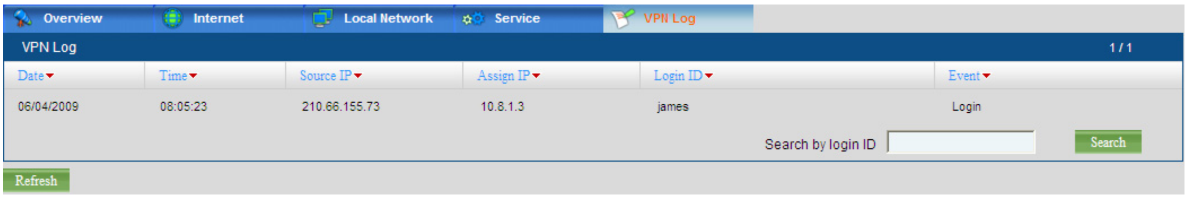
LOCAL NETWORK SERVICES

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

Domain Work Group: Specifies the UMG-2000 / UMG-2200 Windows workgroup.
NTP Server: Enables or disables the NTP service.

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.



VPN Log 1 / 1

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 / UMG-2200 wireless suite integrates the following services: standard access point (AP), multiple layers of wireless security and client blocking.

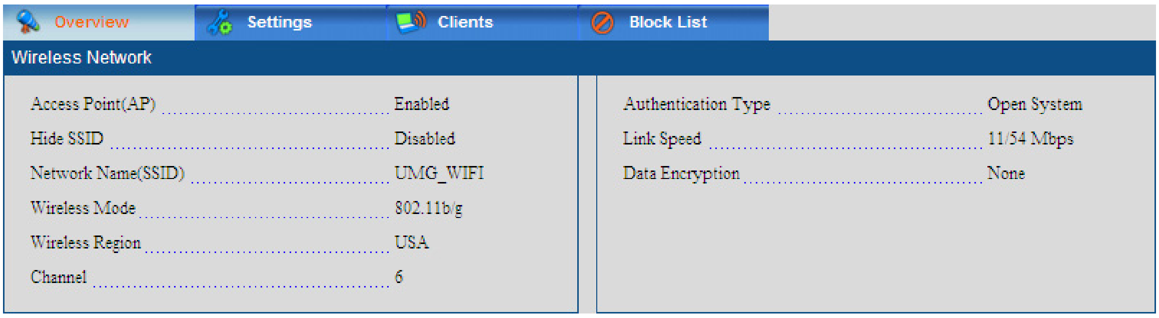
STANDARD WIRELESS ACCESS POINT
The UMG-2000 / UMG-2200 supports three task groups in 802.11 standard working groups: 802.11b/g/n. 802.11b supports data rates up to 11 Mbps, 802.11g supports data rates of at least 20 Mbps and 802.11n supports up to 300Mbps / 2T3R.

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 clock 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

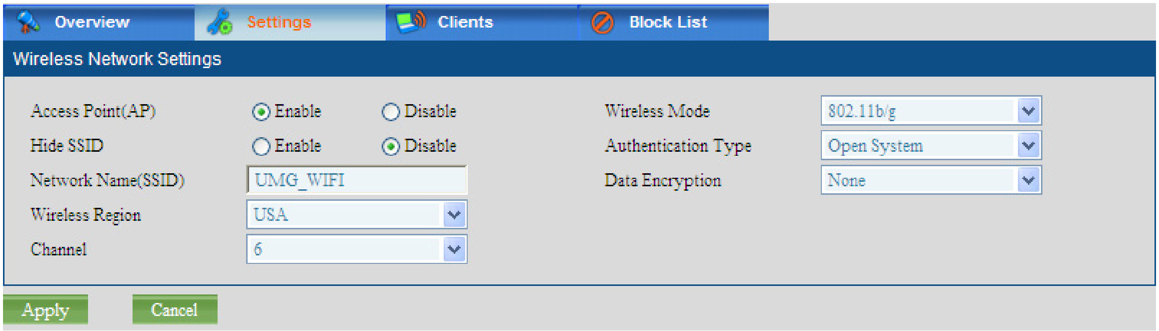
WIRELESS NETWORK

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.



Wireless Network Settings

Access Point(AP)	● Enable	○ Disable	Wireless Mode	802.11b/g
Hide SSID	○ Enable	● Disable	Authentication Type	Open System
Network Name(SSID)	UMG_WIFI		Data Encryption	None
Wireless Region	USA			
Channel	6			

WIRELESS NETWORK

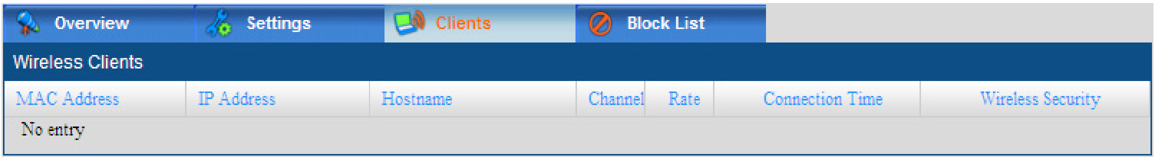
This section lists all the available settings to the wireless Access Point (AP). Service is only accessible when enabled. SSID is visible and can be scanned only when “Hide SSID” is disabled.

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 / UMG-2200 wireless Access Point (AP). Each connected wireless clients information is listed in a tabulated form. The following are the wireless client connection information.



Wireless Clients

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

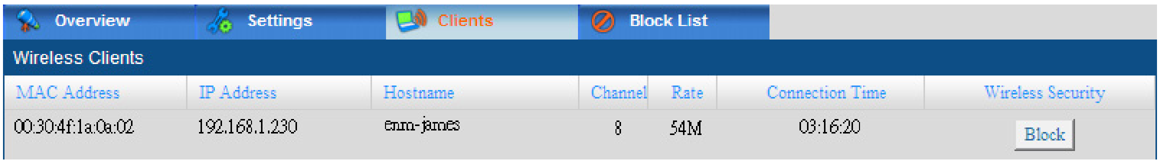
WIRELESS CLIENT

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.

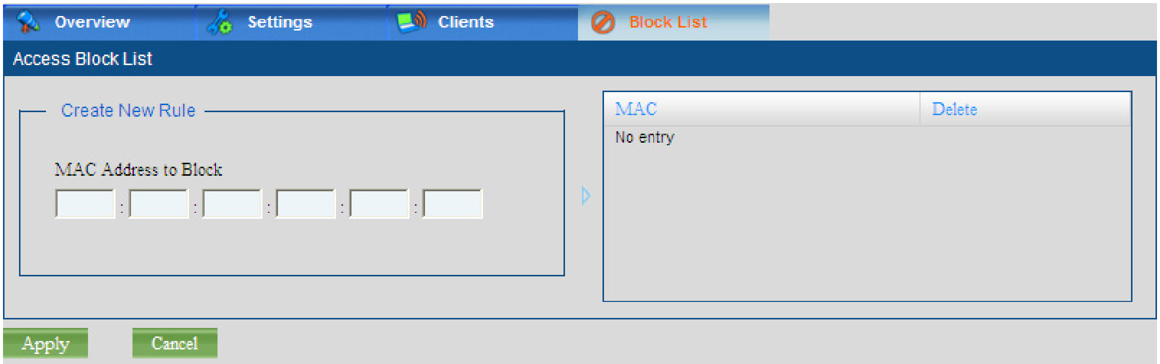


Wireless Clients

MAC Address	IP Address	Hostname	Channel	Rate	Connection Time	Wireless Security
00:30:4f:1a:0a:02	192.168.1.230	enm-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.



No entry

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 / UMG-2200 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 / UMG-2200 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 / UMG-2200 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 / UMG-2200 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

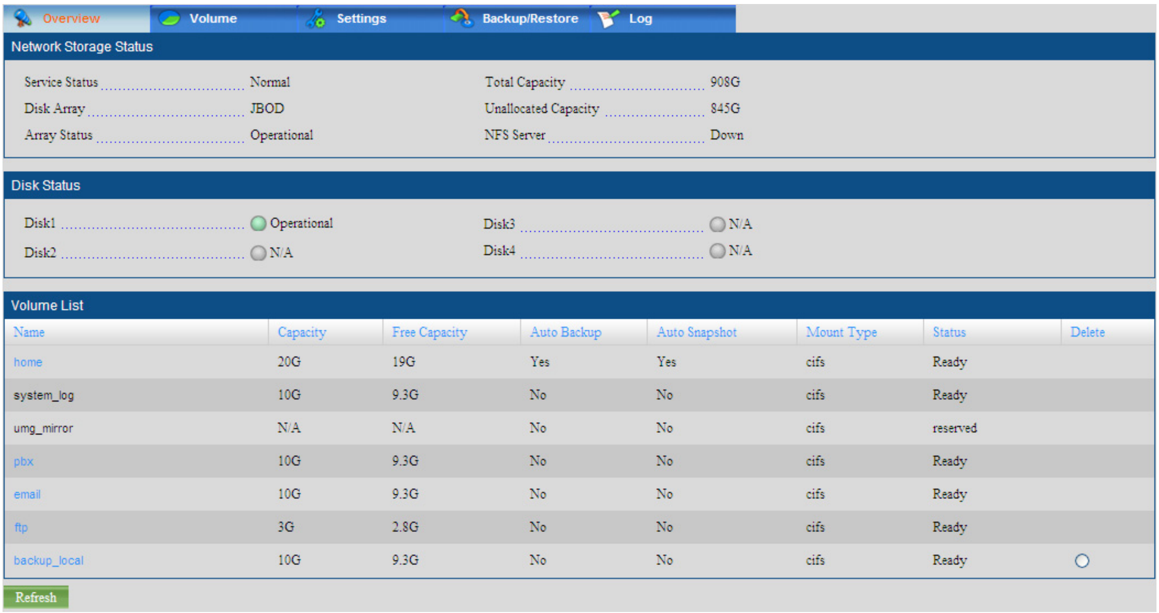
The UMG-2000 / UMG-2200 will automatically backup storage according to the scheduled time. The administrator can also backup the current storage manually. The UMG-2000 / UMG-2200 supports two solutions for backup. One is snapshot and the other is full data copy. Snapshot is an effectual and space-saving 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 / UMG-2200. 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.



Network Storage Status

Service Status .... Normal
Disk Array .... JBOD
Array Status .... Operational
Total Capacity 908G
Unallocated Capacity 845G
NFS Server .... Down

Disk Status

Disk1 .... ● Operational
Disk2 .... ○ N/A
Disk3 .... ○ N/A
Disk4 .... ○ N/A

Volume List

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	
pbx	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	○

NETWORK STORAGE STAUS

This section lists the current status of the storage.

Total Capacity: Displays the total storage size in Gigabyte.
Free Capacity: Displays the available storage size in Gigabyte.
RAID Level: Displays the current storage RAID level: RAID 0, RAID 0+1, or RAID 5.
RAID 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.
NFS Status: Displays the status of the NFS service, up or down.
Disk Status: Displays the status of the 4 disks, good or bad.

DISK STAUS

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.

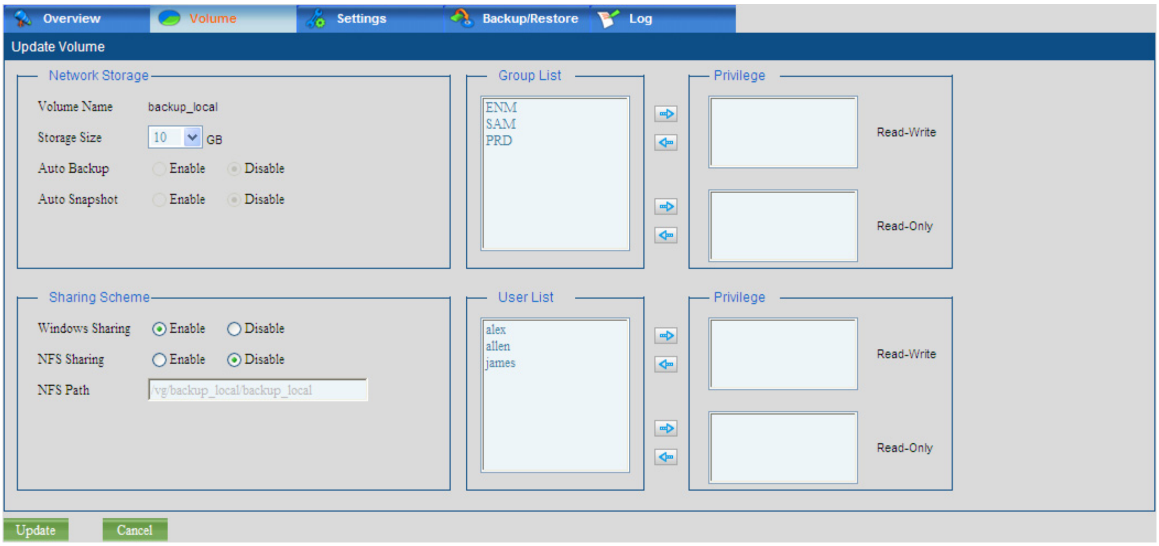
7.2 View a Volume by SMB

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 / UMG-2200 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.



Update Volume

Network Storage

Volume Name backup_local
Storage Size 10 GB
Auto Backup ○ Enable ● Disable
Auto Snapshot ○ Enable ● Disable

Group List
ENM
SAM
PRD

Privilege
Read-Write
Read-Only

Sharing Scheme

Windows Sharing ● Enable ○ Disable
NFS Sharing ○ Enable ● Disable
NFS Path /vg/backup_local/backup_local

User List
alex
allen
james

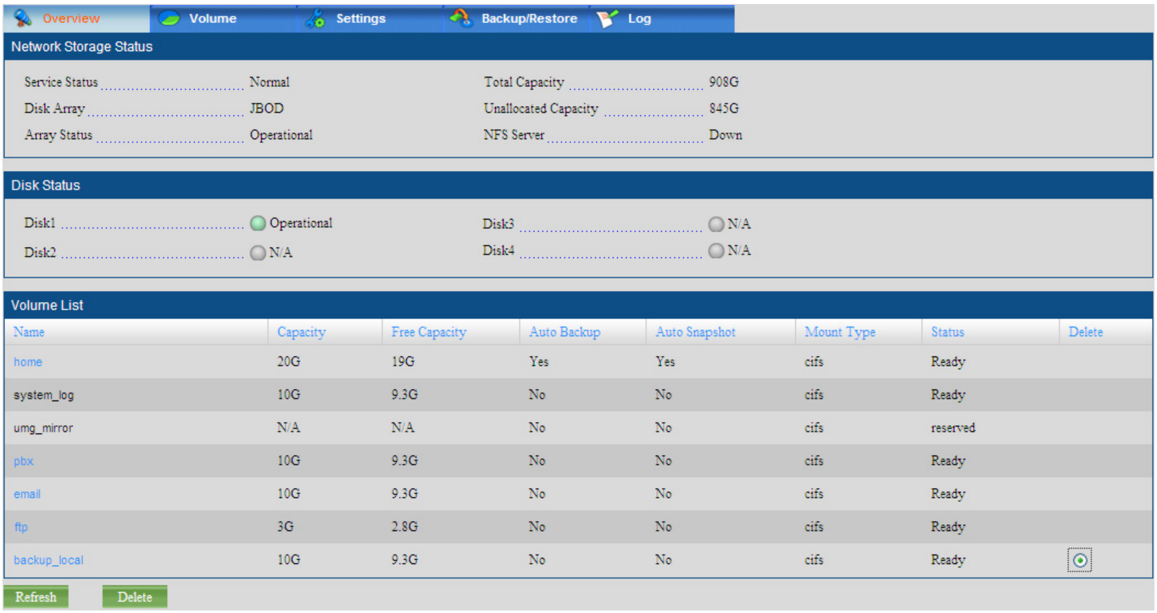
Privilege
Read-Write
Read-Only

Update Cancel

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.



Network Storage Status

Service Status .... Normal
Disk Array .... JBOD
Array Status .... Operational
Total Capacity 908G
Unallocated Capacity 845G
NFS Server .... Down

Disk Status

Disk1 .... ● Operational
Disk2 .... ○ N/A
Disk3 .... ○ N/A
Disk4 .... ○ N/A

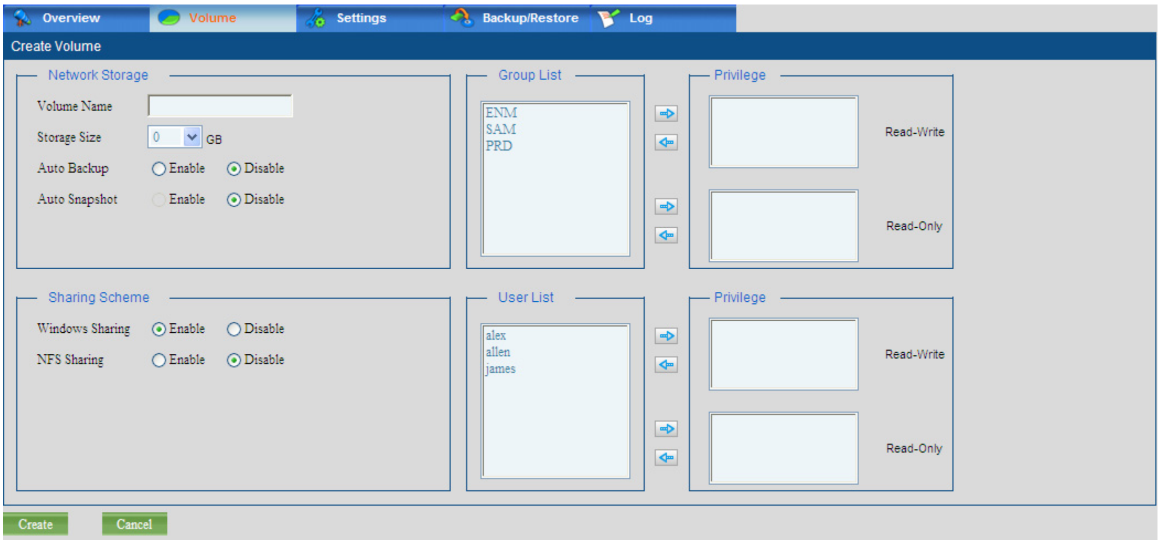
Volume List

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	
pbx	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	●

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.



Network Storage

Volume Name

Storage Size 0 GB

Auto Backup ○ Enable ● Disable

Auto Snapshot ○ Enable ● Disable

Sharing Scheme

Windows Sharing ● Enable ○ Disable

NFS Sharing ○ Enable ● Disable

Group List: ENM, SAM, PRD

Privilege: Read-Write, Read-Only

User List: alex, allen, james

Privilege: Read-Write, Read-Only

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

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: Specifies whether to share this volume to Linux clients by NFS.

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.

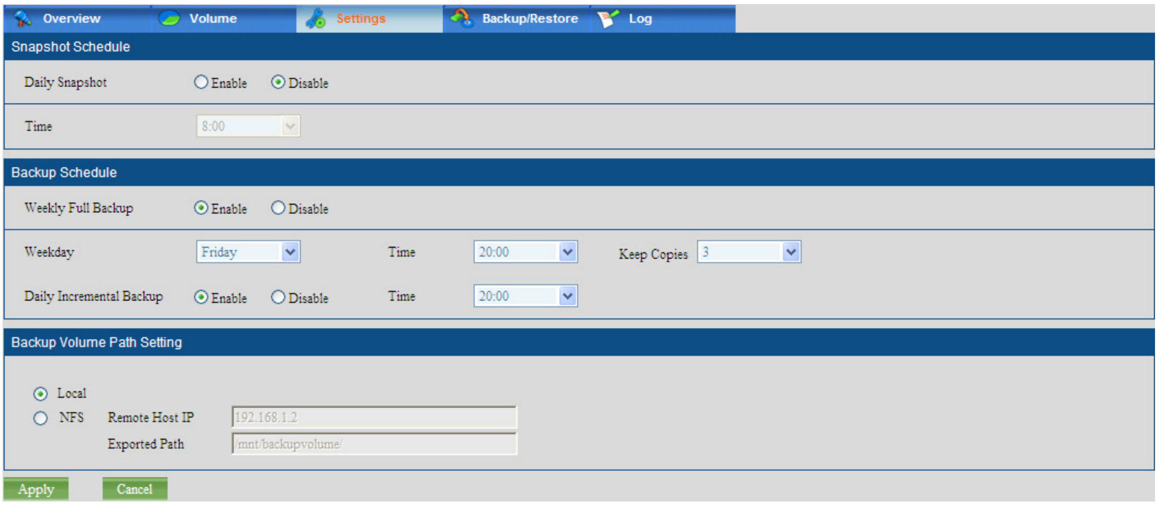
USER LIST

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.



Snapshot Schedule

Daily Snapshot ○ Enable ● Disable

Time 8:00

Backup Schedule

Weekly Full Backup ● Enable ○ Disable

Weekday Friday Time 20:00 Keep Copies 3

Daily Incremental Backup ● Enable ○ Disable Time 20:00

Backup Volume Path Setting

● Local

○ NFS Remote Host IP 192.168.1.2

Exported Path /mnt/backupvolume/

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.
Keep Copies: Specifies the maximum number of the snapshot copies.

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.

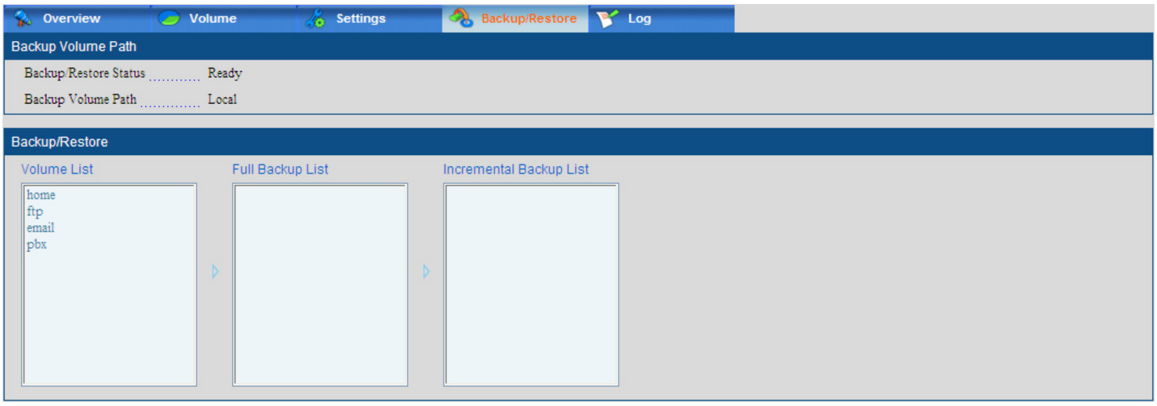
VOLUME BACKUP PATH SETTING

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 Bakcup 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 Volume Path

Backup/Restore Status .... Ready

Backup Volume Path .... Local

Backup/Restore

BACKUP/RESTORE

This section lists all the volumes and the available backup.

Volume List: Displays all the existing volumes in the UMG-2000 / UMG-2200.

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

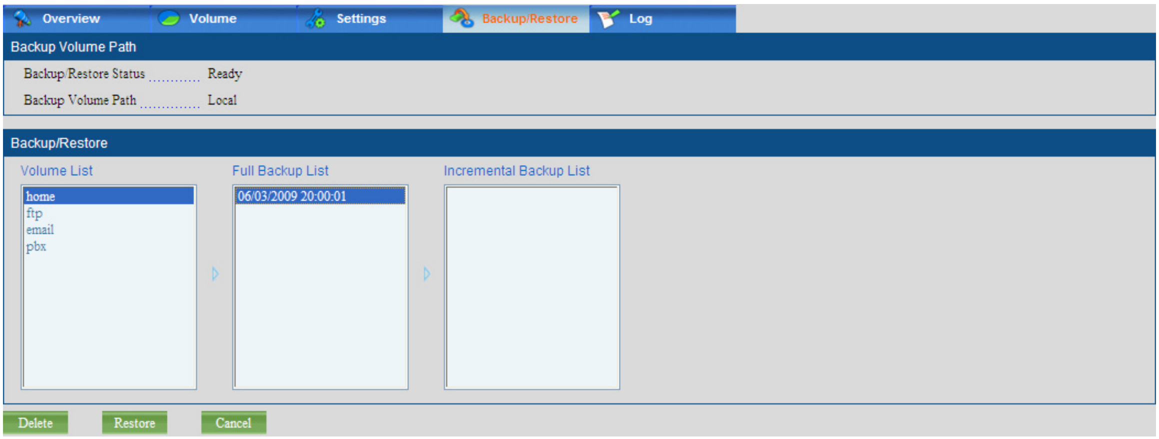
This section lists settings of the backup path.

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.



Backup Volume Path

Backup/Restore Status .... Ready

Backup Volume Path .... Local

Backup/Restore

Volume List: home, ftp, email, pbx

Full Backup List: 06/03/2009 20:00:01

Incremental Backup List

Delete and restore Backup files

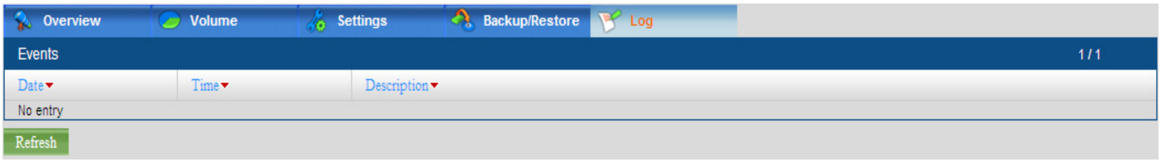
Select a backup file of a volume in the full backup list and then click the “Restore” button to restore the volume to the file. Click the “Delete” button to delete the backup files.

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.



No entry

EVENTS

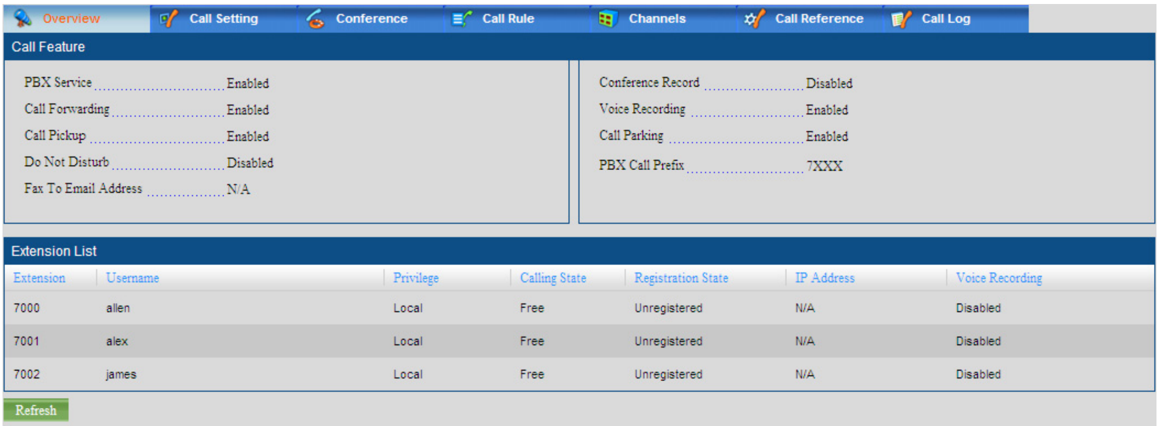
Date: Displays the date of the event.
Time: Displays the time of the event.
Description: Display the detailed description of the event.

8. Web Management - PBX

The UMG-2000 / UMG-2200'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 / UMG-2200 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 / UMG-2200's PBX allows end users to place calls using a network instead of the standard telephone infrastructure. UMG-2000 / UMG-2200'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 / UMG-2200'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 / UMG-2200 IP PBX overview displays the current IP PBX services status.



Call Feature

PBX Service .... Enabled
Call Forwarding .... Enabled
Call Pickup .... Enabled
Do Not Disturb .... Disabled
Fax To Email Address .... N/A

Conference Record .... Disabled
Voice Recording .... Enabled
Call Parking .... Enabled
PBX Call Prefix 7XXX

Extension List

Extension	Username	Privilege	Calling State	Registration State	IP Address	Voice Recording
7000	allen	Local	Free	Unregistered	N/A	Disabled
7001	alex	Local	Free	Unregistered	N/A	Disabled
7002	james	Local	Free	Unregistered	N/A	Disabled

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.

Do Not Disturb: Displays the state of the feature "Do Not Disturb", enabled or disabled.

Call Parking: Displays the state of the feature "Call Parking", enabled or disabled.

Conference Call: Displays the state of the feature "Conference Call", enabled or disabled.

Record Voice: Displays the state of the feature "Record Voice", enabled or disabled.

Operator Number: Displays the current assigned Operator extension Number.

Call Prefix: Displays the call prefix.

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

EXTENSION LIST

This section lists all the extensions with the owner's information in the UMG-2000 / UMG-2200.

Extension: Displays an extension number.

Username: Displays the full name of the specific extension.

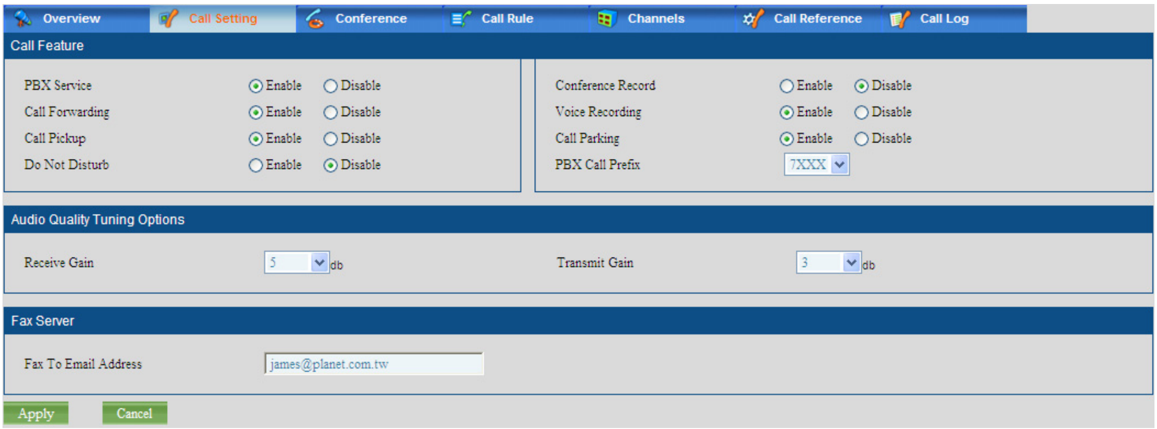
IP Address: Displays the current IP Address of the phone with the specific extension.

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

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

8.2 IP PBX Feature 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.



Call Feature

PBX Service ● Enable ○ Disable
Call Forwarding ● Enable ○ Disable
Call Pickup ● Enable ○ Disable
Do Not Disturb ○ Enable ● Disable
Conference Record ○ Enable ● Disable
Voice Recording ● Enable ○ Disable
Call Parking ● Enable ○ Disable
PBX Call Prefix 7XXX

Audio Quality Tuning Options

Receive Gain 5 db
Transmit Gain 3 db

Fax Server

Fax To Email Address james@planet.com.tw

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 / UMG-2200 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.

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

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.

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

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

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

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.

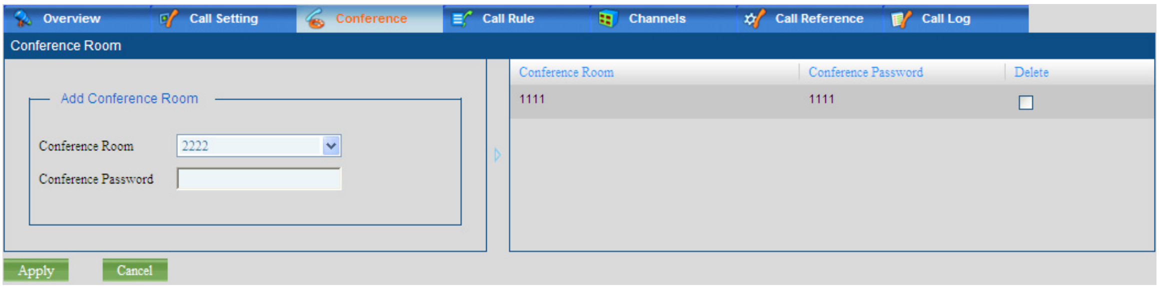
FAX Server

This section set the email address of fax receiver.

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

8.3 IP PBX Conference

Click the “Conference” tab in the “VoIP” screen. The VoIP “Conference” screen appears, allowing the administrator to manage the conference features. The conference setting need select the conference room number and then set the room password.



Conference Room: 2222

Conference Password:

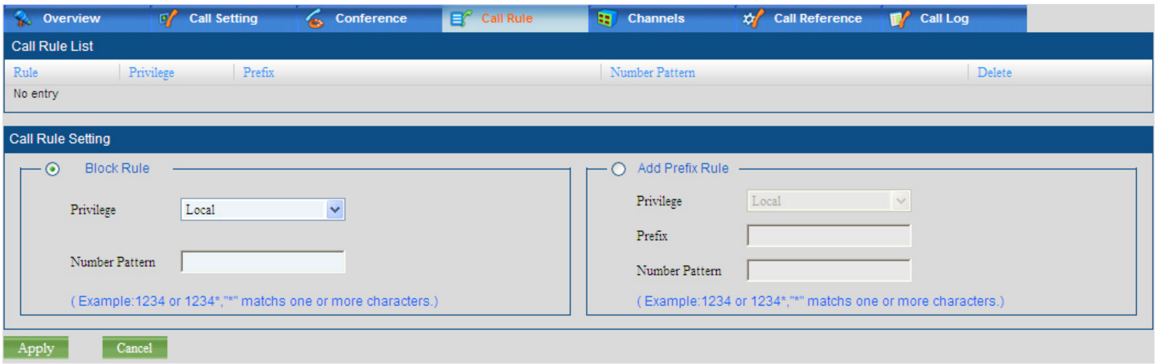
Conference Room	Conference Password	Delete
1111	1111	□

Conference room

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

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.



Call Rule List

Rule	Privilege	Prefix	Number Pattern	Delete
No entry				

Call Rule Setting

● Block Rule

Privilege: Local

Number Pattern:

(Example:1234 or 1234*,"*" matchs one or more characters.)

○ Add Prefix Rule

Privilege: Local

Prefix:

Number Pattern:

(Example:1234 or 1234*,"*" matchs one or more characters.)

CALL RULES 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.

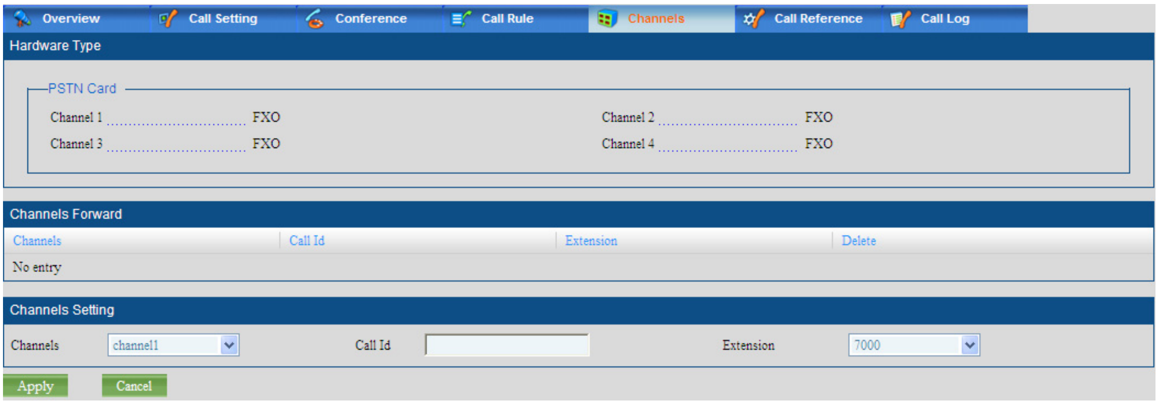
CALL RULES LIST

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.



Hardware Type

PSTN Card

Channel 1	FXO	Channel 2	FXO
Channel 3	FXO	Channel 4	FXO

Channels Forward

Channels	Call Id	Extension	Delete
No entry			

Channels Setting

Channels: channel1 Call Id: Extension: 7000

Hardware Type

This section lists the channels of PSTN Card.

Channel1: Shows channel 1 of PSTN.
Channel2: Shows channel 2 of PSTN.
Channel3: Shows channel 3 of PSTN.
Channel4: Shows channel 4 of PSTN.

Channels Forward

This section lists the settings of the caller ID.

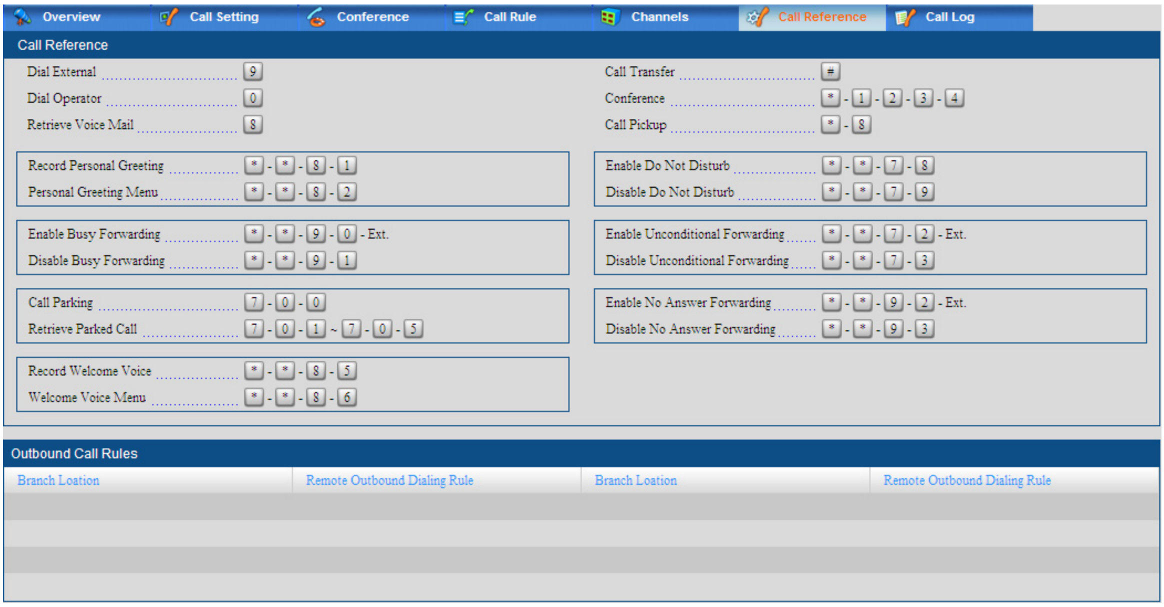
Name: Specifies the call name that will be shown to the call receiver.
Number: Specifies the call number that will be shown to the call receiver.
The administrator can choose a channel as a voice or a data channel by clicking the corresponding “right” button or removing a channel from the existing list 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.

8.6 IP PBX Call Reference

The UMG-2000 / UMG-2200 IP PBX Call Reference displays the guide to help you configure the call features using your telephone.



Call Reference

Dial External	9	Call Transfer	#
Dial Operator	0	Conference	* - 1 - 2 - 3 - 4
Retrieve Voice Mail	8	Call Pickup	* - 8
Record Personal Greeting	* - * - 8 - 1	Enable Do Not Disturb	* - * - 7 - 8
Personal Greeting Menu	* - * - 8 - 2	Disable Do Not Disturb	* - * - 7 - 9
Enable Busy Forwarding	* - * - 9 - 0 - Ext.	Enable Unconditional Forwarding	* - * - 7 - 2 - Ext.
Disable Busy Forwarding	* - * - 9 - 1	Disable Unconditional Forwarding	* - * - 7 - 3
Call Parking	7 - 0 - 0	Enable No Answer Forwarding	* - * - 9 - 2 - Ext.
Retrieve Parked Call	7 - 0 - 1 ~ 7 - 0 - 5	Disable No Answer Forwarding	* - * - 9 - 3
Record Welcome Voice	* - * - 8 - 5		
Welcome Voice Menu	* - * - 8 - 6		

Outbound Call Rules

Branch Loation	Remote Outbound Dialing Rule	Branch Loation	Remote Outbound Dialing Rule

Call Reference

Dial External: Dials 9 and destination number to call the number.
Dial Operator: Dials 0 to call the operator.
Retrieve Voice Mail: Dials 8 to retrieve voice mail.
Record Personal Greeting: Dials **81 to record a personal greeting.
Play Personal Greeting: Dials **82 to play the personal greeting record.
Enable Forward On Busy: Dials **90 and a forward extension the number to enable the forwarding of calls when busy. All your calls will be forwarded to the preselected extension when your line is busy.
Disable Forward On Busy: Dials **91 to disable the forwarding of calls when busy.
Call Parking: Dials 700 when on the line allows the holding of the incoming call and retrieves that call from another telephone line.
Retrieve Parked Call: Dials the number that you have heard when you have parked the former call to retrieve the parked call. It is a number between 701 and 705.
Record Welcome Voice: Dials **85 to retrieve voice mail.
Welcome Voice Menu: Dials **86 to access the Welcome Voice Menu.
Call transfer: Dials # to transfer the incoming call to the other line.
Conference: Dials *1234 to join a call conference.
Call Pickup: Dials *8 and an extension to enable a call pickup. It will allow answering an incoming call to the specific extension from another phone within the same call pick up group.
Disable Do not Disturb: Dials **78 to disable do not disturb.
Enable Do not Disturb: Dials **79 to enable do not disturb. It will prevent ringing when there are incoming calls.

Enable Unconditional Forwarding: Dials **72 and the extension to enable unconditional forwarding. It will allow the redirecting of all your temporary calls to the preselected phone.
Disable Unconditional Forwarding: Dials **73 to disable unconditional forwarding.
Enable No Answer Forwarding: Dials **92 and a forward extension the number to enable No answer forwarding. All your calls will be forwarded to the preselected extension when nobody answers your line.
Disable No Answer Forwarding: Dials **93 to disable No answer forwarding.

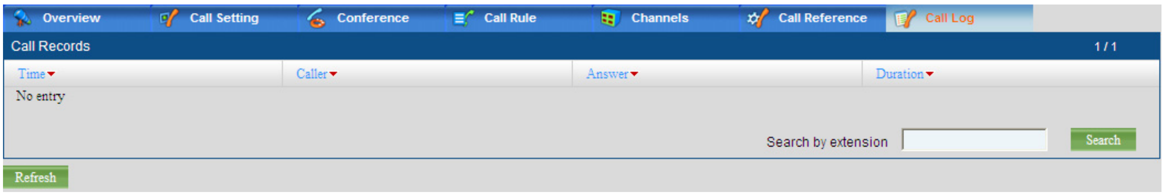
Outbound Call Rules

This section lists the guide to call the remote branches visa VoIP. In the UMG-2000 / UMG-2200 call group, all the extensions can be dialed directly without any long distance charges.

Branch Location: Displays the location of the branch.
Remote Outbound Dialing Rules: Displays the call prefix of the branch. All the extensions belonging to the branch are prefixed with this number.

8.7 IP PBX Call Log

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



Call Records 1 / 1

Time	Caller	Answer	Duration
No entry			

Search by extension

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 / UMG-2200 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 / UMG-2200 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 / UMG-2200 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 / UMG-2200 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

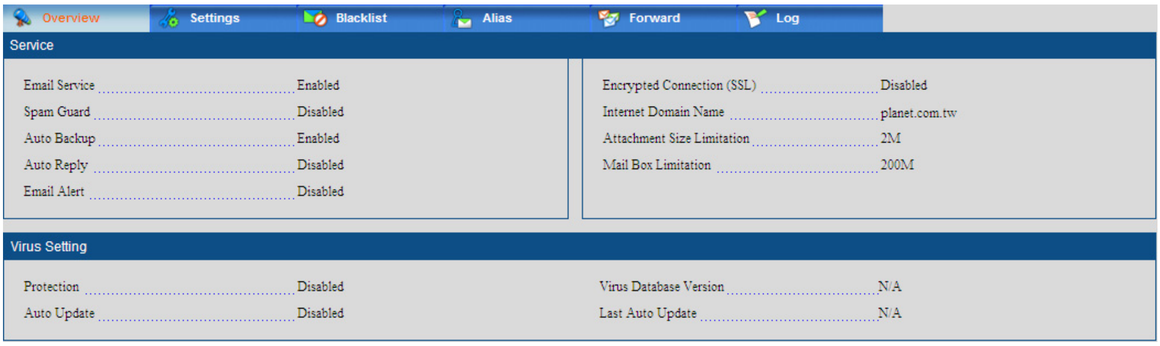
An email server always gathers the reports about the spam and threaten coming from certain addresses. The administrator can add these addresses to the email blacklist so that the email server will filter, reject and drop mails from these addresses.

EMAIL forward

The UMG-2000 / UMG-2200 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:

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.

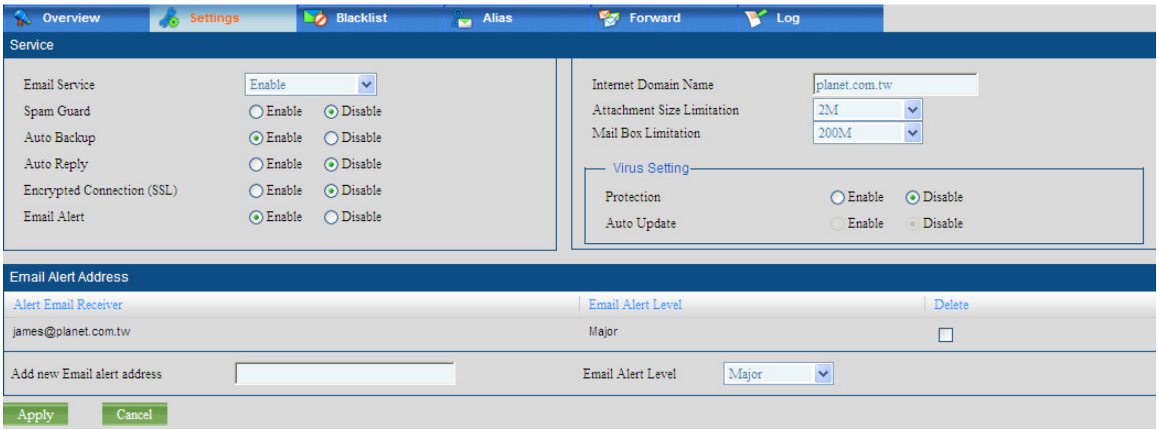
Auto Update: Displays the state of the feature “auto update Email virus database”, enable or disable.

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

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

Virus Setting

Protection	○ Enable ● Disable
Auto Update	○ Enable ● Disable

Email Alert Address

Alert Email Receiver	Email Alert Level	Delete
james@planet.com.tw	Major	□

Add new Email alert address Email Alert Level Major

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 / UMG-2200 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 / UMG-2200 Email when you send or receive Email.
Email Alert: Enables or disables the “Email Alert” feature. Enabling this feature will allow the UMG-2000 / UMG-2200 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.
Mail 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 / UMG-2200 update the email virus database automatically.

ALERT EMAIL ADDRESS

This section lists all the email alert mail addresses that the UMG-2000 / UMG-2200 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

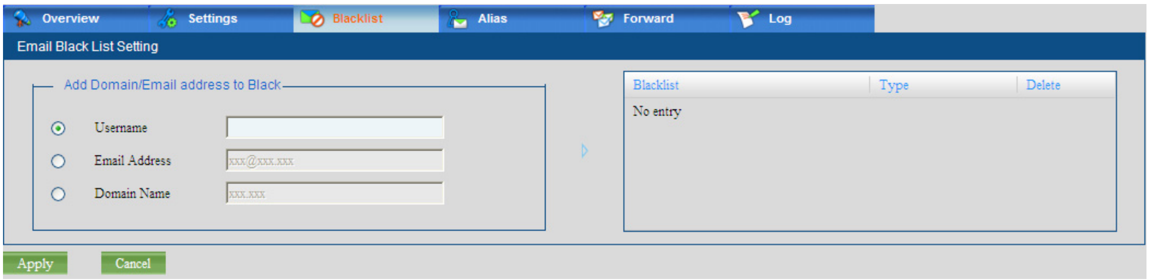
Specify a full Email address and click the “Apply” button to add the email address to the alert list.

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.



Email Black List Setting

Add Domain/Email address to Black

●	Username	
○	Email Address	xxx@xxx.xxx
○	Domain Name	xxx.xxx

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.

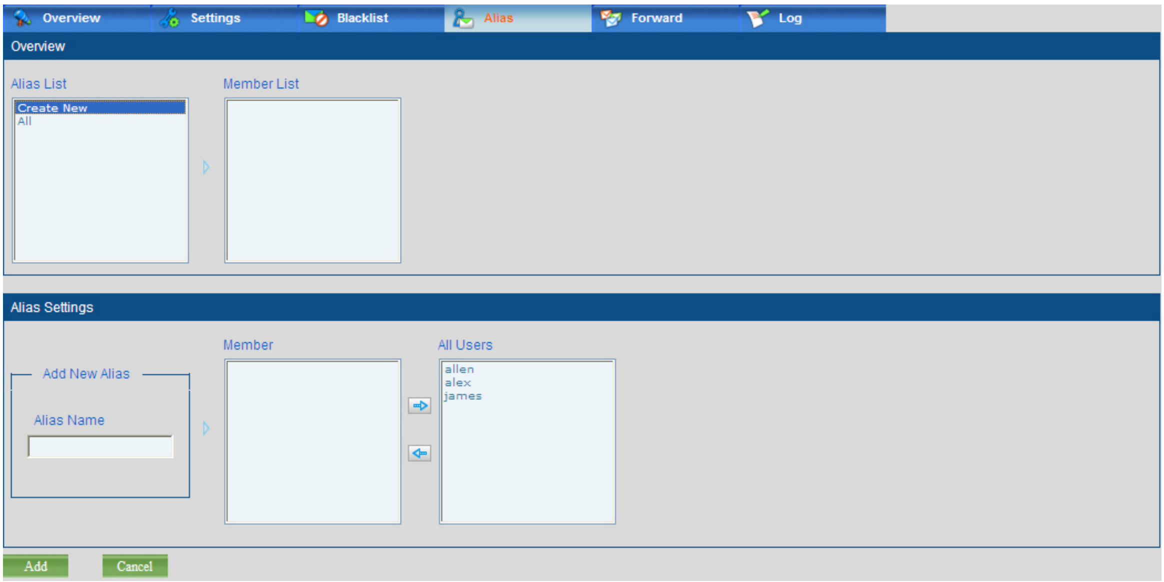
Email Address: Display the type of the black entity, username, email address, or domain name.

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.

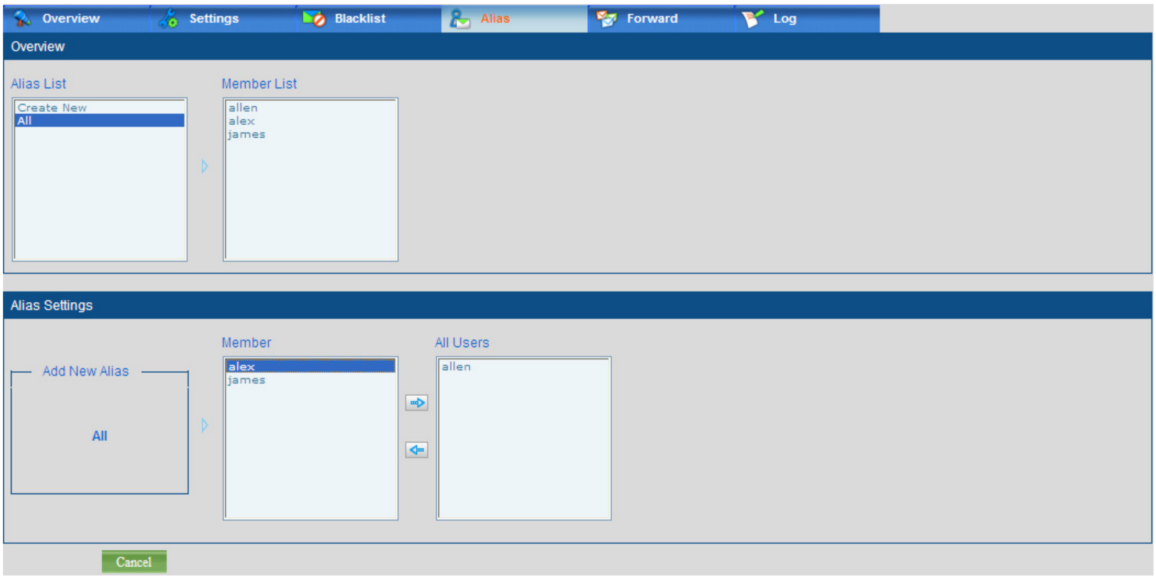
Alias List: Displays all alias names.
Number List: Displays the numbers of an alias.

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.



Overview

Alias List: Create New, All

Member List: allen, alex, james

Alias Settings

Add New Alias: All

Member: alex, james

All Users: allen

DELETING AN EMAIL ALIAS

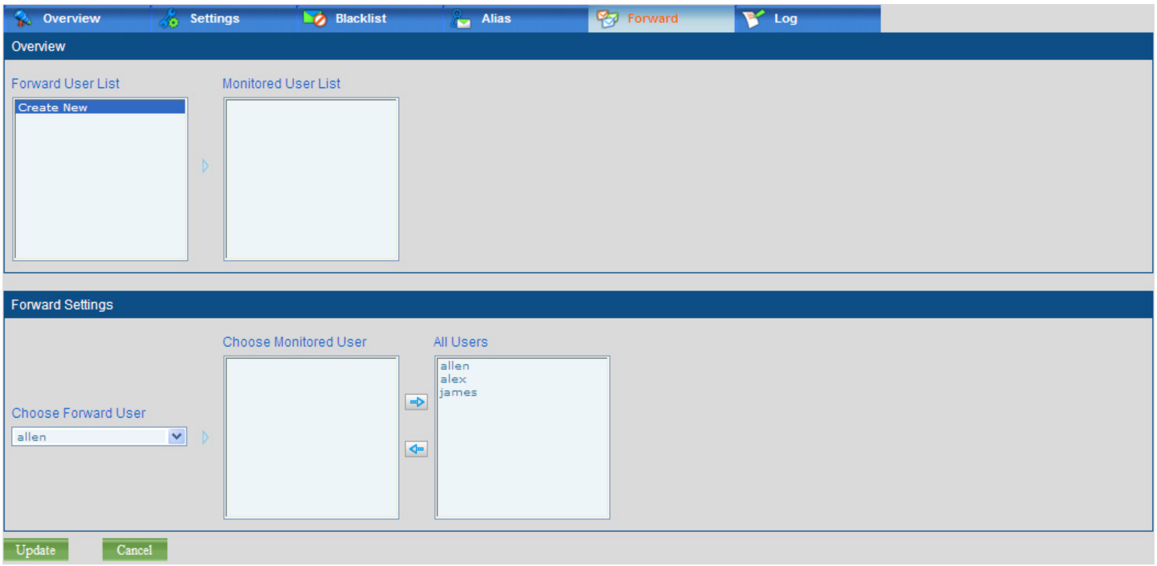
Select an alias from the alias list, and then click the “Delete” button to delete the email alias.

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.



Overview

Forward User List: Create New

Monitored User List

Forward Settings

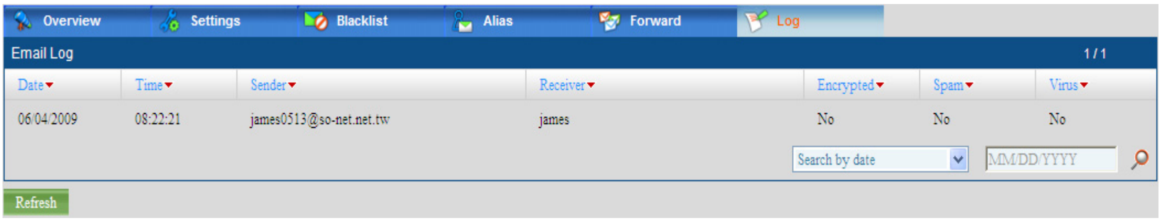
Choose Forward User: allen

Choose Monitored User

All Users: allen, alex, james

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.



Email Log 1 / 1

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

Search by date MM/DD/YYYY

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 / UMG-2200 Email server.
Spam: Displays whether it is a junk mail.
Virus: Displays whether a virus is existing in the mail.

EMAIL LOG SORTING

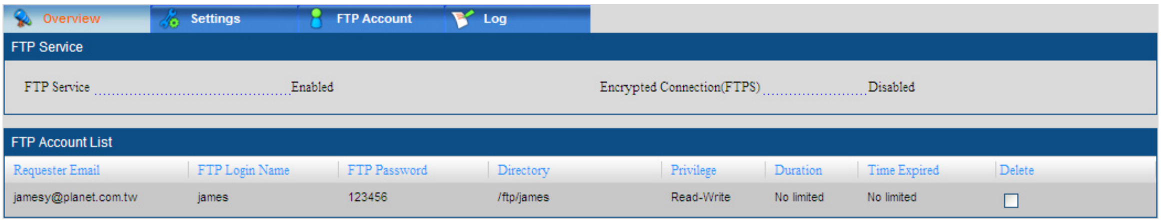
Select “Search by name” or “Search by date” in the drop down menu and specify the key word in the text fill. Then click the “Search” button, and the results will appear.

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 / UMG-2200 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.



FTP Service

FTP Service .... Enabled

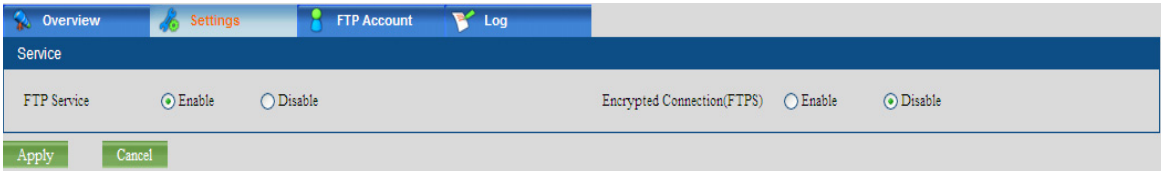
Encrypted Connection(FTPS) .... Disabled

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	□

10.2 FTP Setting

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



Service

FTP Service ● Enable ○ Disable

Encrypted Connection(FTPS) ○ Enable ● Disable

FTP SETTING

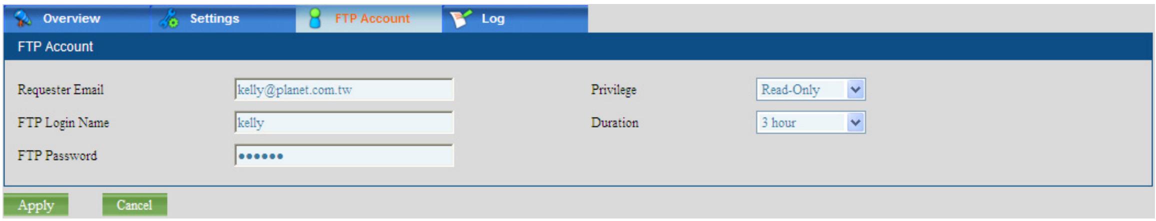
This section lists all the available settings of the FTP service:

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.



FTP Account

Requester Email	kelly@planet.com.tw	Privilege	Read-Only
FTP Login Name	kelly	Duration	3 hour
FTP Password	••••••		

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.

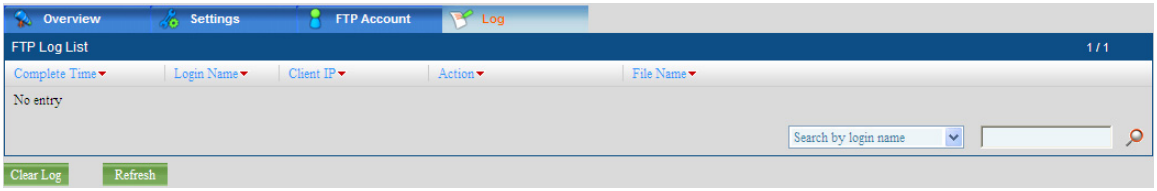
Directory: Specifies the authorized directory of this account.

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 Management - Security

The UMG-2000 / UMG-2200 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

The UMG-2000 / UMG-2200 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.

HTTP CONTENT FILTER

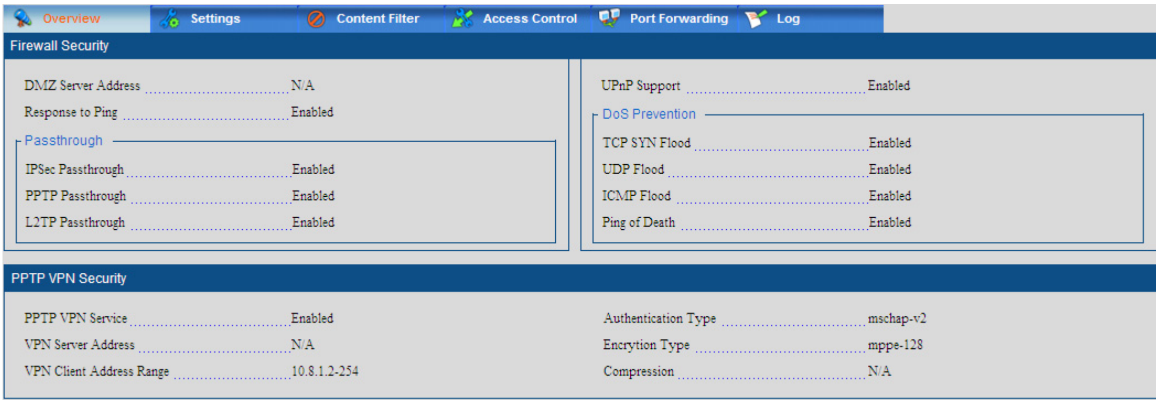
The HTTP content filter is the upper level application aiming to reduce the risk of a HTTP visit by controlling the access to some specific sites and keywords. The administrator can also block certain sites and sensitive keywords to avoid unauthorized HTTP access.

PPTP VPN

PPTP VPN is a secure tunnel for transporting IP traffic using PPP. It is supported by Microsoft dial-up Networking. The UMG-2000 / UMG-2200 provides the PPTP VPN server to build a secure link to the UMG-2000 / UMG-2200 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.

11.1 Security Overview

The page “Security Overview” shows the current security settings.



Firewall Security

DMZ Server Address .... N/A
Response to Ping .... Enabled

Passthrough

IPSec Passthrough .... Enabled
PPTP Passthrough .... Enabled
L2TP Passthrough .... Enabled

UPnP Support .... Enabled

DoS Prevention

TCP SYN Flood .... Enabled
UDP Flood .... Enabled
ICMP Flood .... Enabled
Ping of Death .... 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
Encrytion Type mppe-128
Compression .... N/A

FIREWALL SECURITY
This section lists all the current firewall settings.

SPI Firewall: Displays the state of firewall service, enabled or disabled.
TCP SYN Cookie: Displays the state of the feature “TCP SYN Cookie”, enabled or disabled.
DMZ Server Address: Displays the DMZ host IP address.
UPnP Support: Displays the state of the feature “UPnP Support”, enabled or disabled.
Response to Ping: Displays the state of the feature “Response to Ping”, 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.

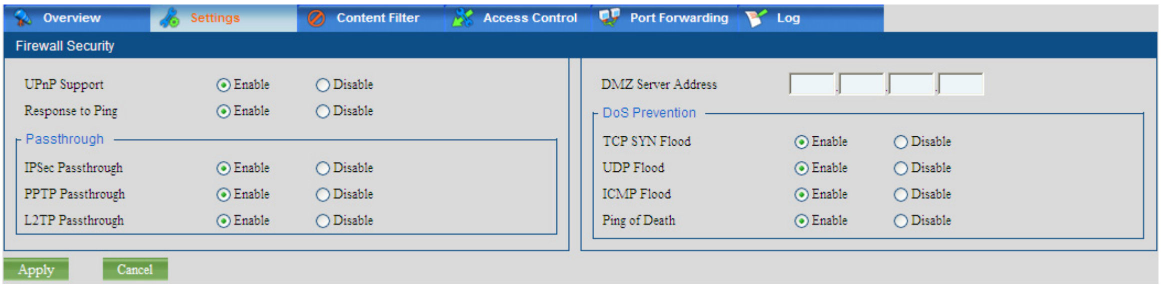
Authentication Type: Displays the authentication method in which the PPTP server authenticates its clients.

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.

11.2 Security Setting

The "Security Setting" page allows the administrator to manage the firewall.



Firewall Security

UPnP Support ● Enable ○ Disable

Response to Ping ● Enable ○ Disable

Passthrough

IPSec Passthrough ● Enable ○ Disable

PPTP Passthrough ● Enable ○ Disable

L2TP Passthrough ● Enable ○ Disable

DMZ Server Address

DoS Prevention

TCP SYN Flood ● Enable ○ Disable

UDP Flood ● Enable ○ Disable

ICMP Flood ● Enable ○ Disable

Ping of Death ● Enable ○ Disable

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 / UMG-2200 respond to the ping request from the Internet.

TCP SYN Cookie: Enables or disables the "TCP SYNC Cookie" feature. Enabling this feature will enable the SYN cookie to protect partial SYN-flood DoS attacks.

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.

PASSTHROUTH

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.

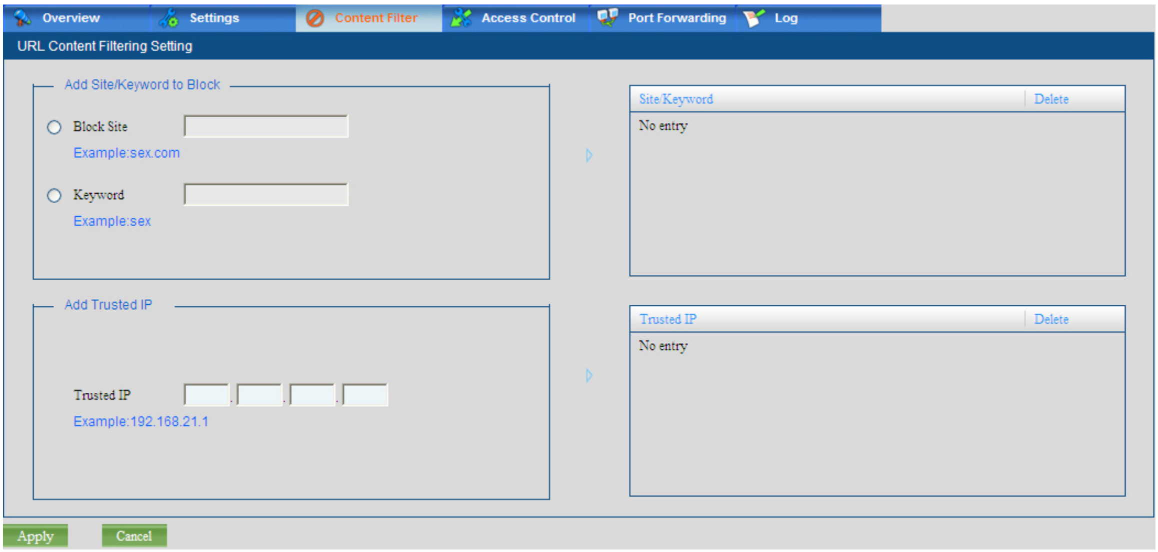
Ping of Death: Enables or disables the "Ping of Death" feature. Enable this feature for protection from a "Ping to Death" attack.

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.

11.3 Content Filter

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



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.

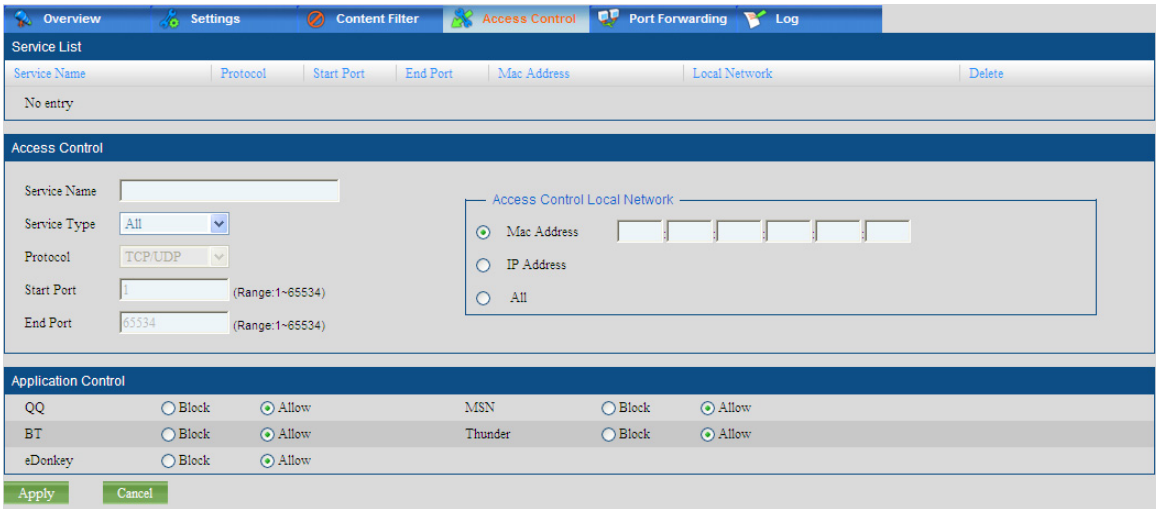
Trusted IP: Specifies the trusted IP address.

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.

11.4 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 List

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

Access Control

Service Name:

Service Type: All

Protocol: TCP/UDP

Start Port: 1 (Range:1~65534)

End Port: 65534 (Range:1~65534)

Access Control Local Network

● Mac Address

○ IP Address

○ All

Application Control

QQ	○ Block	● Allow	MSN	○ Block	● Allow
BT	○ Block	● Allow	Thunder	○ Block	● Allow
eDonkey	○ Block	● 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.

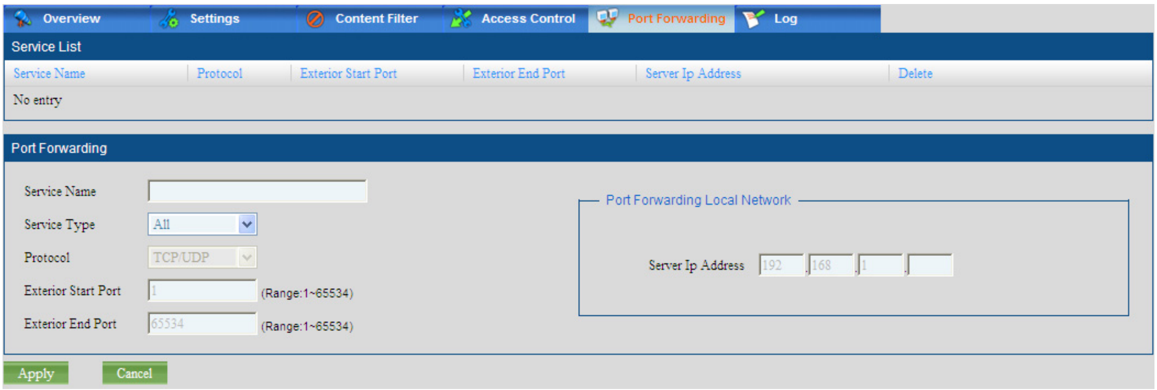
All: Specifies whether or not you want to apply the rules on all PC clients in LAN.

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.

11.5 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.



Service List

Service Name	Protocol	Exterior Start Port	Exterior End Port	Server Ip Address	Delete
No entry					

Port Forwarding

Service Name	
Service Type	All
Protocol	TCP/UDP
Exterior Start Port	1 (Range:1~65534)
Exterior End Port	65534 (Range:1~65534)

Port Forwarding Local Network

Server Ip Address 192 . 168 . 1 .

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.

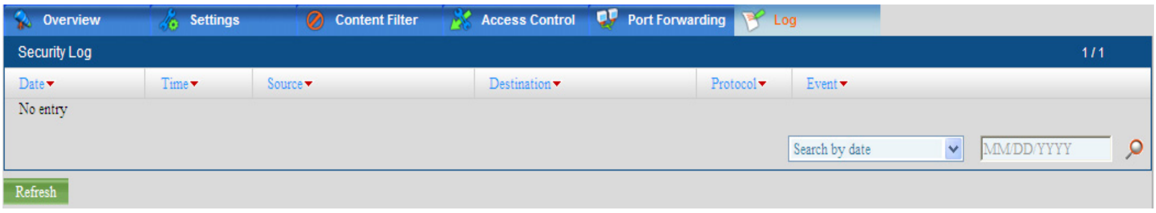
Server IP Address: If you want to apply the rule to a special IP address, check this option.

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.

11.6 Security Log

The “Security Log” page shows the firewall logs.



Security Log 1 / 1

Date	Time	Source	Destination	Protocol	Event
No entry					

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.

12. Web Management - System

The UMG-2000 / UMG-2200 provides system management mechanisms to understand and manage our system. It mainly provides: hardware overview, company profile setup, and system event management.

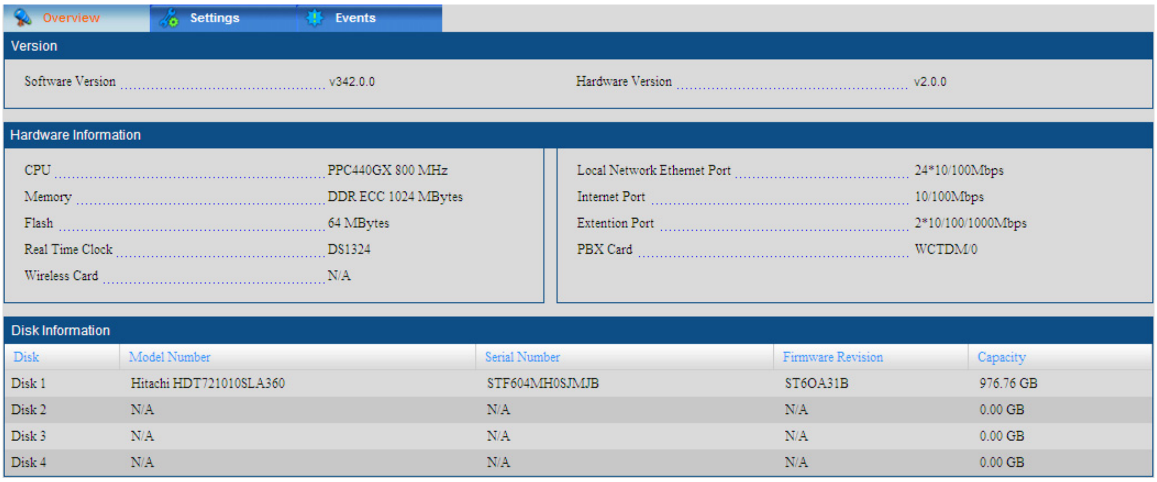
HARDWARE OVERVIEW
The UMG-2000 / UMG-2200 will display all hardware information, including: hardware version, the technical parameter of CPU, Memory, Flash, RTC, Disk etc.

COMPANY PROFILE SETUP
The UMG-2000 / UMG-2200 provides the ability to build and update the profile of the customer's company.

SYSTEM EVENT MANAGEMET
The UMG-2000 / UMG-2200 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.

12.1 System Overview

The system “Overview” screen presents a summary of the UMG-2000 / UMG-2200 system status.



Version

Software Version .... v342.0.0   Hardware Version v2.0.0

Hardware Information

CPU .... PPC440GX 800 MHz
Memory .... DDR ECC 1024 MBytes
Flash .... 64 MBytes
Real Time Clock DS1324
Wireless Card .... N/A

Local Network Ethernet Port 24*10/100Mbps
Internet Port 10/100Mbps
Extention Port 2*10/100/1000Mbps
PBX Card WCTDM/0

Disk Information

Disk	Model Number	Serial Number	Firmware Revision	Capacity
Disk 1	Hitachi HDT721010SLA360	STF604MH0SJMJB	ST6OA31B	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 / UMG-2200.

Hardware Version: Displays the current hardware version of the UMG-2000 / UMG-2200.

HARDWARE INFORMATION

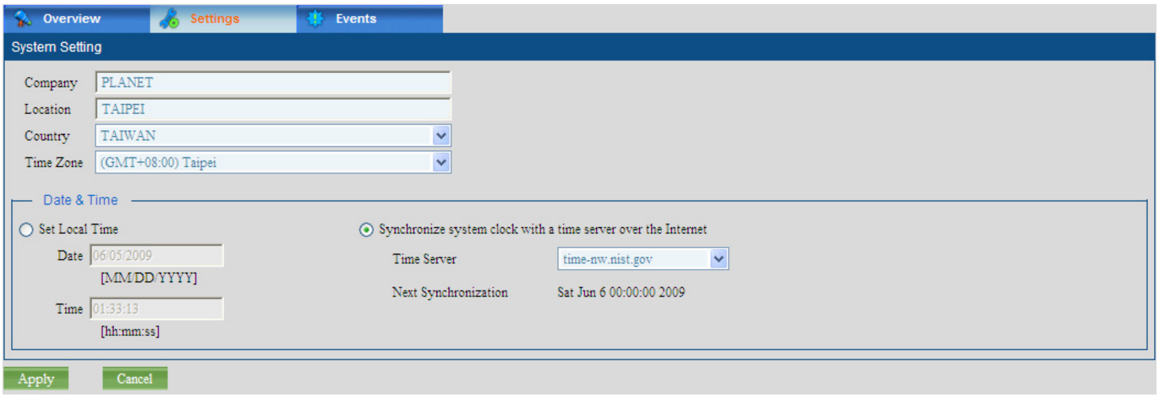
CPU: Displays the CPU information.
Memory: Displays the memory information.
Flash: Displays the flash information.
Real Time Clock (RTC): Displays the RTC information.
Wireless: Displays the information of the wireless adapter.
Local Network Ethernet Port: Displays the information of the switch.
Internet Port: Displays the information of the WAN interface.
Extension Port: Displays the information of the extension ports.
PBX Adapter: Displays the information of VoIP adapter.

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.

12.2 System Setting

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



System Setting

Company	PLANET
Location	TAIPEI
Country	TAIWAN
Time Zone	(GMT+08:00) Taipei

Date & Time

○ Set Local Time

Date 06/05/2009 [MM/DD/YYYY]

Time 01:33:13 [hh:mm:ss]

● Synchronize system clock with a time server over the Internet

Time Server time-nw.nist.gov

Next Synchronization Sat Jun 6 00:00:00 2009

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

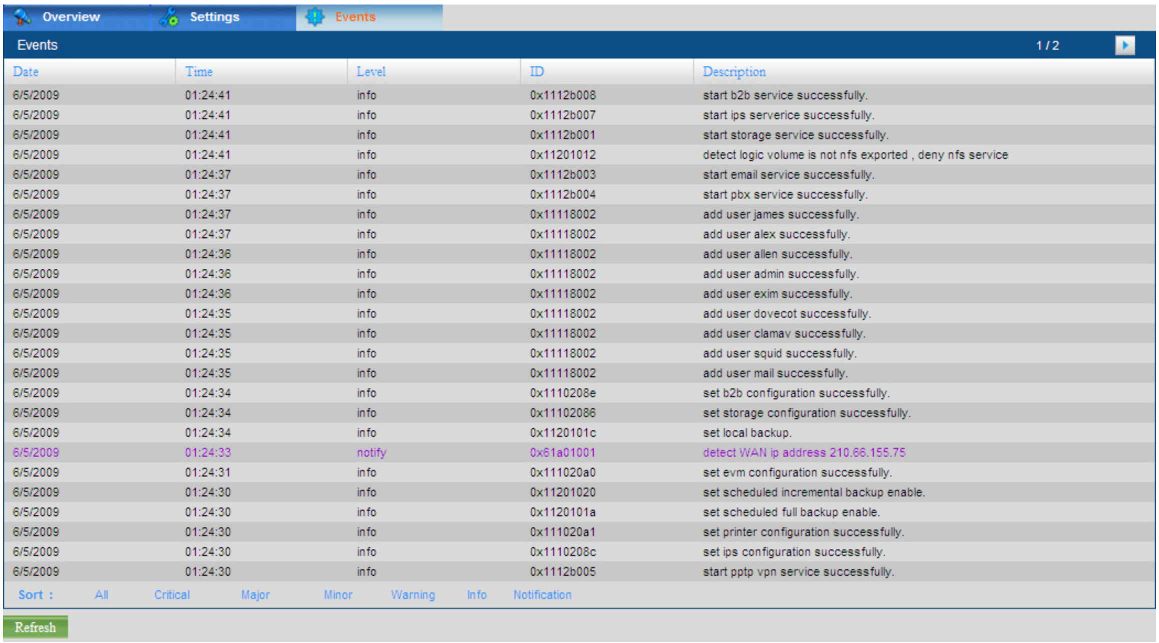
This section allows the administrator to set the local time.

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.

12.3 System Event Log

The UMG-2000 / UMG-2200 system events are classified by its severity which includes Critical, Major, Minor, Notification, Warning, and Informational.

- The Critical event shows that the UMG-2000 / UMG-2200 is in critical, unrecoverable condition and cannot service any more.
- The major event shows that the UMG-2000 / UMG-2200 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 / UMG-2200 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 serverice 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	0x61a01001	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.

13. 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 / UMG-2200 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 / UMG-2200 in this mode will be the master node in this group.

DIVISION
Division is a client or slave mode. The UMG-2000 / UMG-2200 in this mode will be a slave node in the group and can be managed by its headquarter.

13.1 Branch-to-Branch Setup

If you want to setup up Branch-to-Branch, you must connect the UMG-2000 / UMG-2200 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.

13.2 Secruity 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.

13.3 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 / UMG-2200 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 / UMG-2200 joins the UMG-2000 / UMG-2200 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 changes.

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

13.4 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”.

13.5 Shared Services

Some specific services can be shared among different UMG-2000 / UMG-2200 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.

13.6 Global user Profile

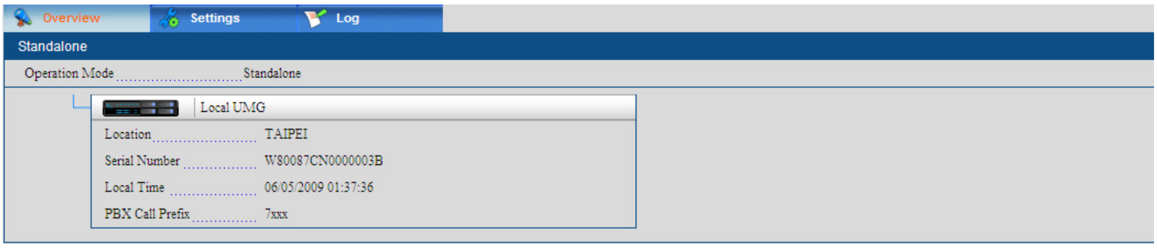
After connection, the profile of the headquarter and its divisions will be synchronized. So far, the contact list synchronization is supported. Anyone who can access the UMG-2000 / UMG-2200 can get the fully detailed contract list which includes all users in the UMG-2000 / UMG-2200 group in user private web administration.

13.7 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).

13.8 Branch-to-Branch Overview

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



Standalone

Operation Mode .... Standalone

Local UMG

Location .... TAIPEI

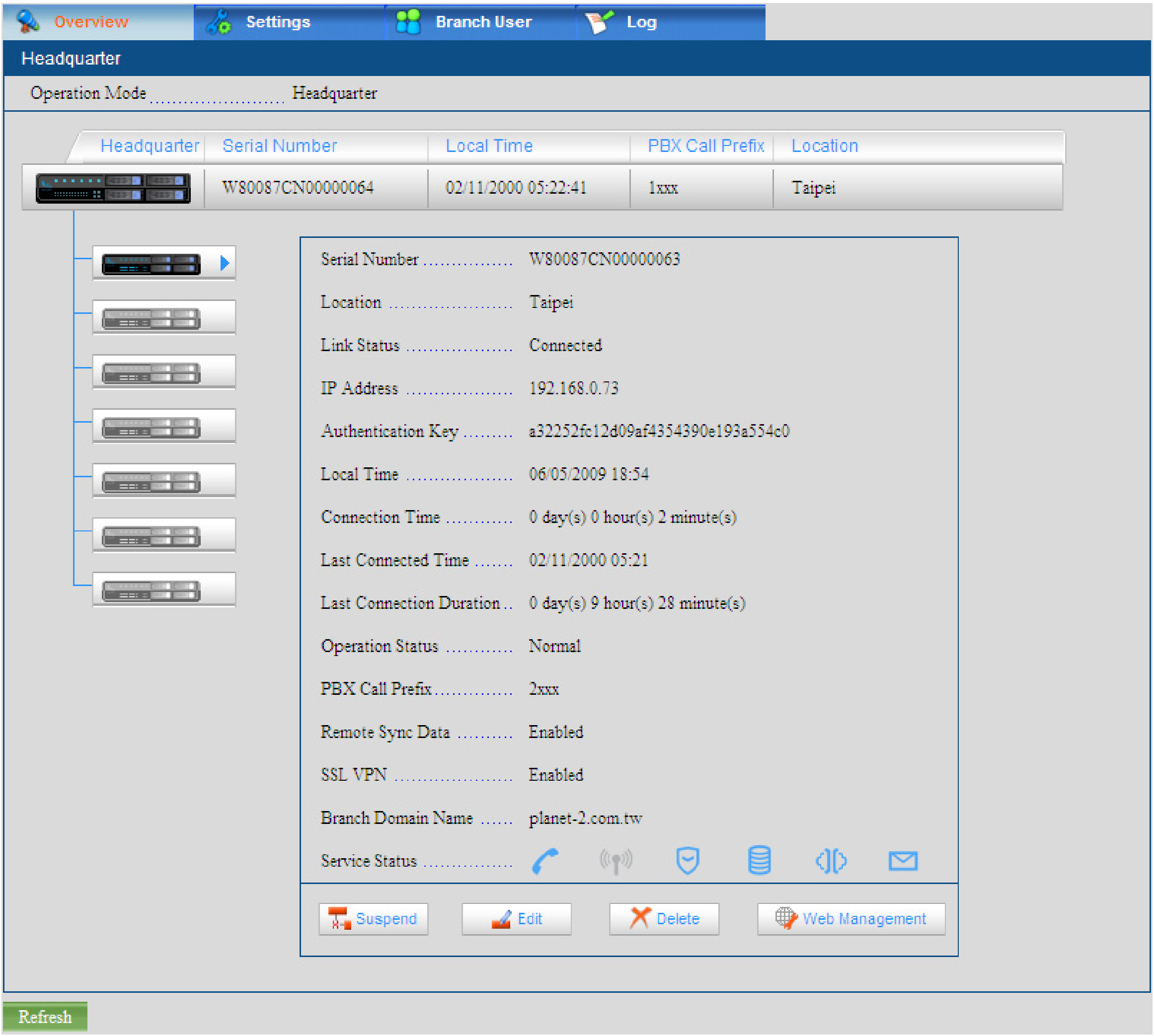
Serial Number W80087CN0000003B

Local Time 06/05/2009 01:37:36

PBX Call Prefix 7xxx

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 .... Headquarter

Headquarter	Serial Number	Local Time	PBX Call Prefix	Location
	W80087CN00000064	02/11/2000 05:22:41	1xxx	Taipei

Serial Number W80087CN00000063

Location .... Taipei

Link Status .... Connected

IP Address 192.168.0.73

Authentication Key a32252fc12d09af4354390e193a554c0

Local Time 06/05/2009 18:54

Connection Time .... 0 day(s) 0 hour(s) 2 minute(s)

Last Connected Time 02/11/2000 05:21

Last Connection Duration .. 0 day(s) 9 hour(s) 28 minute(s)

Operation Status .... Normal

PBX Call Prefix............. 2xxx

Remote Sync Data .... Enabled

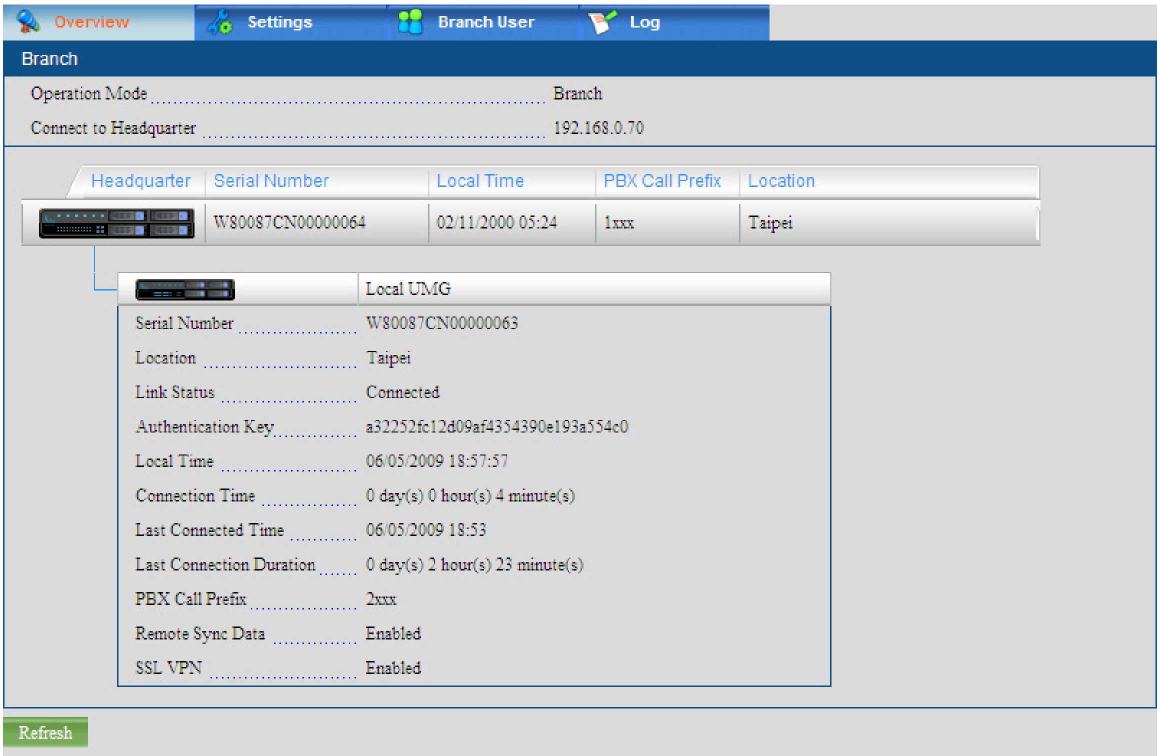
SSL VPN .... Enabled

Branch Domain Name planet-2.com.tw

Service Status ....

HEADQUARTER

Operation mode: Displays the current operation mode
Headquarter Location: Displays the location of the UMG-2000 / UMG-2200.
Headquarter Serial Number: Displays the BTB serial number.
Headquarter Local Time: Displays the local time of the UMG-2000 / UMG-2200.
Headquarter Call Prefix: Displays the call prefix of the UMG-2000 / UMG-2200.
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 / UMG-2200 when and only when connected.



Branch

Operation Mode .... Branch

Connect to Headquarter 192.168.0.70

Headquarter	Serial Number	Local Time	PBX Call Prefix	Location
	W80087CN00000064	02/11/2000 05:24	1xxx	Taipei

Local UMG

Serial Number W80087CN00000063

Location .... Taipei

Link Status .... Connected

Authentication Key a32252fc12d09af4354390e193a554c0

Local Time 06/05/2009 18:57:57

Connection Time .... 0 day(s) 0 hour(s) 4 minute(s)

Last Connected Time 06/05/2009 18:53

Last Connection Duration .... 0 day(s) 2 hour(s) 23 minute(s)

PBX Call Prefix 2xxx

Remote Sync Data .... Enabled

SSL VPN .... Enabled

BRANCH

Operation mode: Displays the current operation mode

Connect to Headquarter: Displays the host/IP address of headquarter UMG-2000 / UMG-2200.

Headquarter Location: Displays the location of the headquarter UMG-2000 / UMG-2200.

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

Headquarter Local Time: Displays the local time of the headquarter UMG-2000 / UMG-2200.

Headquarter Call Prefix: Displays the call prefix of the headquarter UMG-2000 / UMG-2200.

Location: the Displays the location of the UMG-2000 / UMG-2200.

Serial Number: Displays the BTB serial number.

Link Status: Displays the link status of the UMG-2000 / UMG-2200.

Key: Displays the key used to connect to the headquarter UMG-2000 / UMG-2200.

Local Time: Displays the local time of the UMG-2000 / UMG-2200.

Connection Time: Displays the total connection live time of the headquarter UMG-2000 / UMG-2200.

Call Prefix: Displays the call prefix of the UMG-2000 / UMG-2200.

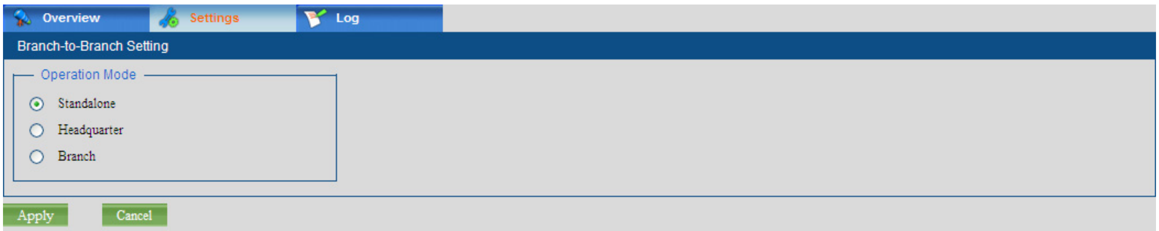
13.9 Delete a Branch

If the mode of your UMG-2000 / UMG-2200 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.

13.10 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.

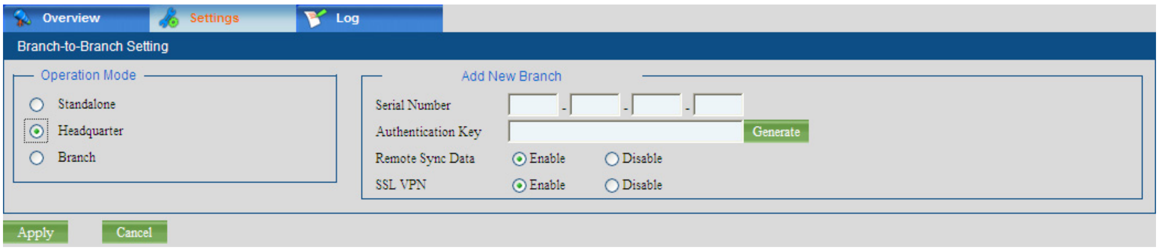


Branch-to-Branch Setting

Operation Mode
● Standalone
○ Headquarter
○ Branch

OPERATION MODE

Standalone: Disables the Branch-to-Branch feature.
Headquarter: Specifies the operation mode to Headquarter.
Division: Specifies the operation mode to Branch.



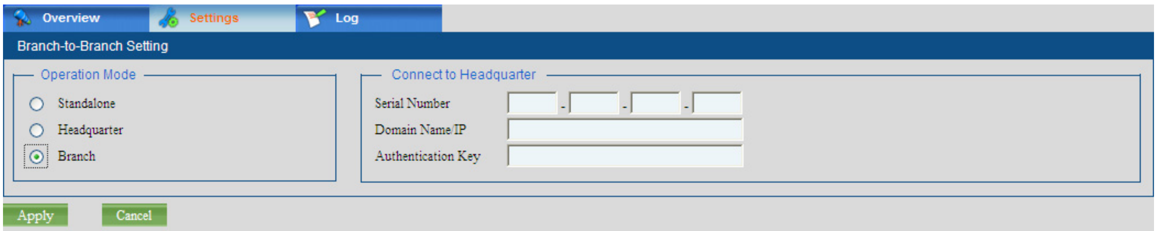
Branch-to-Branch Setting

Operation Mode
○ Standalone
● Headquarter
○ Branch

Add New Branch
Serial Number [ ]-[ ]-[ ]-[ ]
Authentication Key [ ]
Remote Sync Data ● Enable ○ Disable
SSL VPN ● Enable ○ Disable

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 / UMG-2200 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 / UMG-2200 and the branch.



Branch-to-Branch Setting

Operation Mode

○ Standalone
○ Headquarter
● Branch

Connect to Headquarter

Serial Number ____ - ____ - ____ - ____
Domain Name/IP ____
Authentication Key ____

CONNECT TO HEADQUARTER

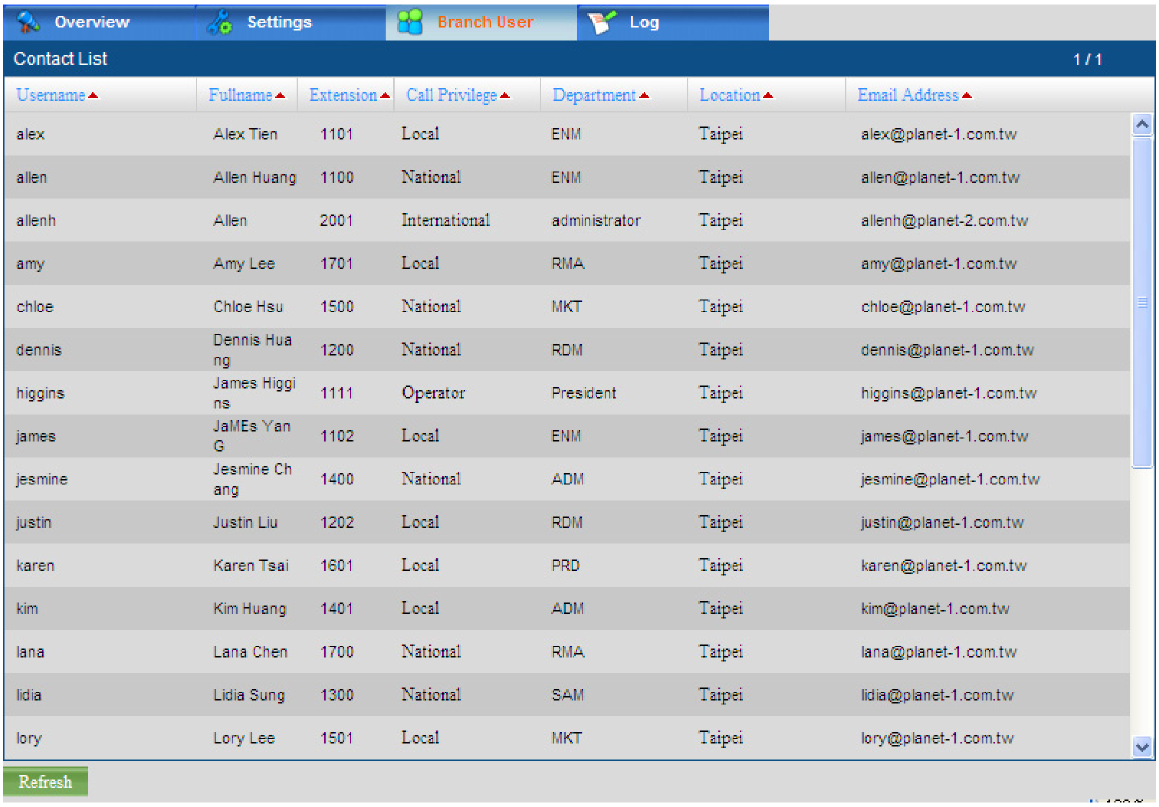
Serial Number: Specifies the BTB serial number of the headquarter you want to connect.

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.

13.11 Branch Users

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

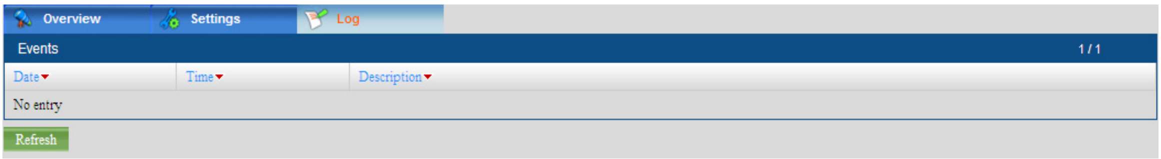


Contact List 1 / 1

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 Hua ng	1200	National	RDM	Taipei	dennis@planet-1.com.tw
higgins	James Higgi ns	1111	Operator	President	Taipei	higgins@planet-1.com.tw
james	JaMEs Yan G	1102	Local	ENM	Taipei	james@planet-1.com.tw
jesmine	Jesmine Ch ang	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

13.12 Branch-to-Branch Log

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



Events 1 / 1

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.

14. Web Management - Maintenance

The UMG-2000 / UMG-2200 maintenance suit includes the following services: configure backup/restore, software update, diagnose, and remote support request.

BACKUP/RESTORE CONFIGURE

The UMG-2000 / UMG-2200 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 / UMG-2200 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

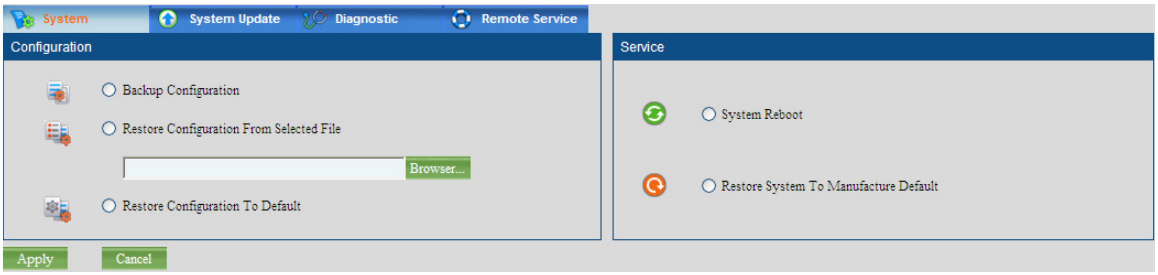
The UMG-2000 / UMG-2200 provides the mechanism of self diagnostic. The diagnostic includes: memory test, Wireless test, PBX test, flash memory test, USB port test, storage RAID testing, Real-time clock test, network test, and LED test. If one or more test fail, please replace the faulty product or contact your product provider.

REMOTE SERVICE

If your UMG-2000 / UMG-2200 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.

14.1 System

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



○ Backup Configuration

○ Restore Configuration From Selected File

○ Restore Configuration To Default

○ System Reboot

○ Restore System To Manufacture Default

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 Configuration To Default: Restores the configuration to default.

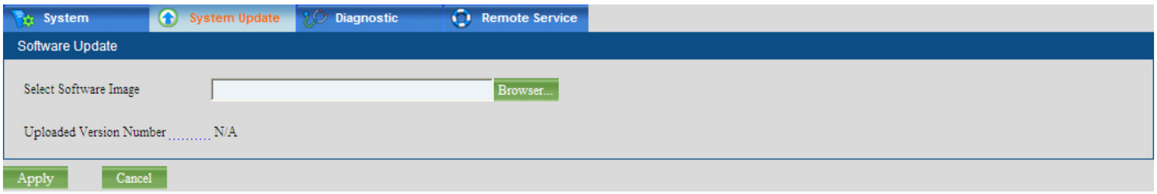
System Reboot: Reboots the UMG-2000 / UMG-2200.

Shut Down: Shuts down the UMG-2000 / UMG-2200.

Restore System To Manufacture Default: Restores the UMG-2000 / UMG-2200 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.

14.2 System Update

The “System Update” page allows the administrator to update the software to the latest version.



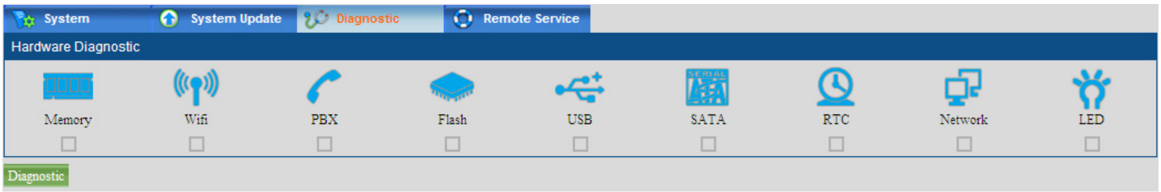
SOFTWARE UPDATE

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.

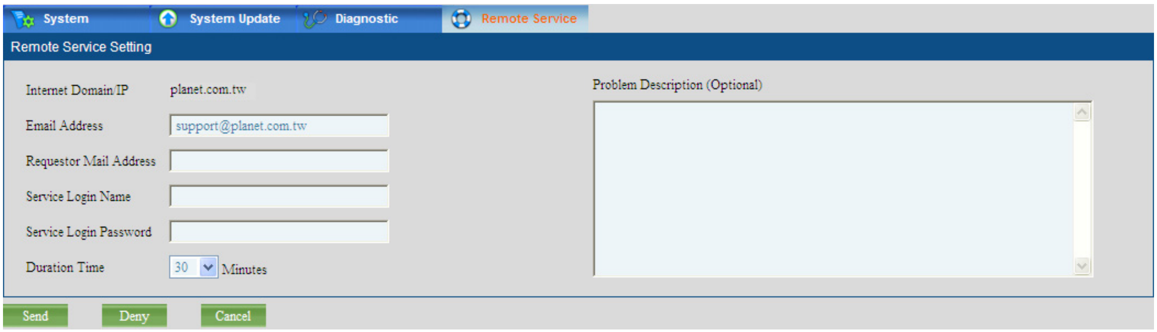
14.3 Diagnose

The page “Diagnose” allows the administrator to test hardware. The diagnostic report will be shown after the testing.



14.4 Remote Service

The page “Remote Service” allows the administrator to report problems and get online help.



Internet Domain/IP	planet.com.tw
Email Address	support@planet.com.tw
Requestor Mail Address	
Service Login Name	
Service Login Password	
Duration Time	30 Minutes

Problem Description (Optional)

Internet Domain/IP: Displays the Host/IP of the UMG-2000 / UMG-2200.
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 / UMG-2200 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 / UMG-2200 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.

15. 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 / UMG-2200 and allows every user to be his own administrator. Once an active user account is added to UMG-2000 / UMG-2200, 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 / UMG-2200 tutorial, etc

UPDATE THE USER PROFILE

The UMG-2000 / UMG-2200 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

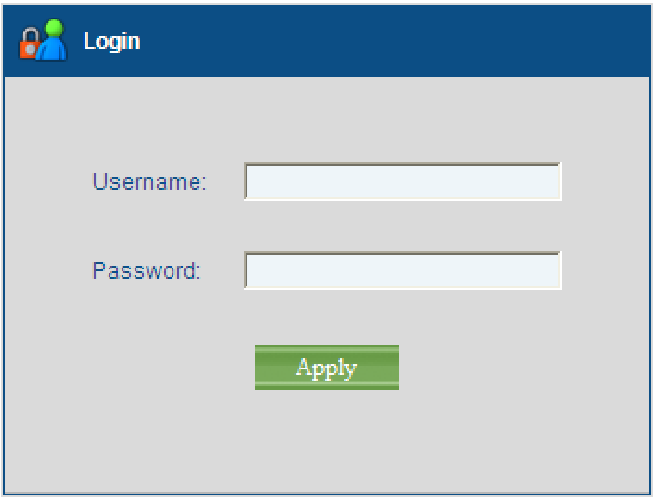
Based on all the user's profiles, a detailed contact list will be presented, including the user's email address and extension. All branch users will be presented here if the feature “Branch to Branch” is enabled. Refer to Section - Profile in One to get further information.

UMG-2000 / UMG-2200 TUTORIAL

The UMG-2000 / UMG-2200 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.

15.1 User Login

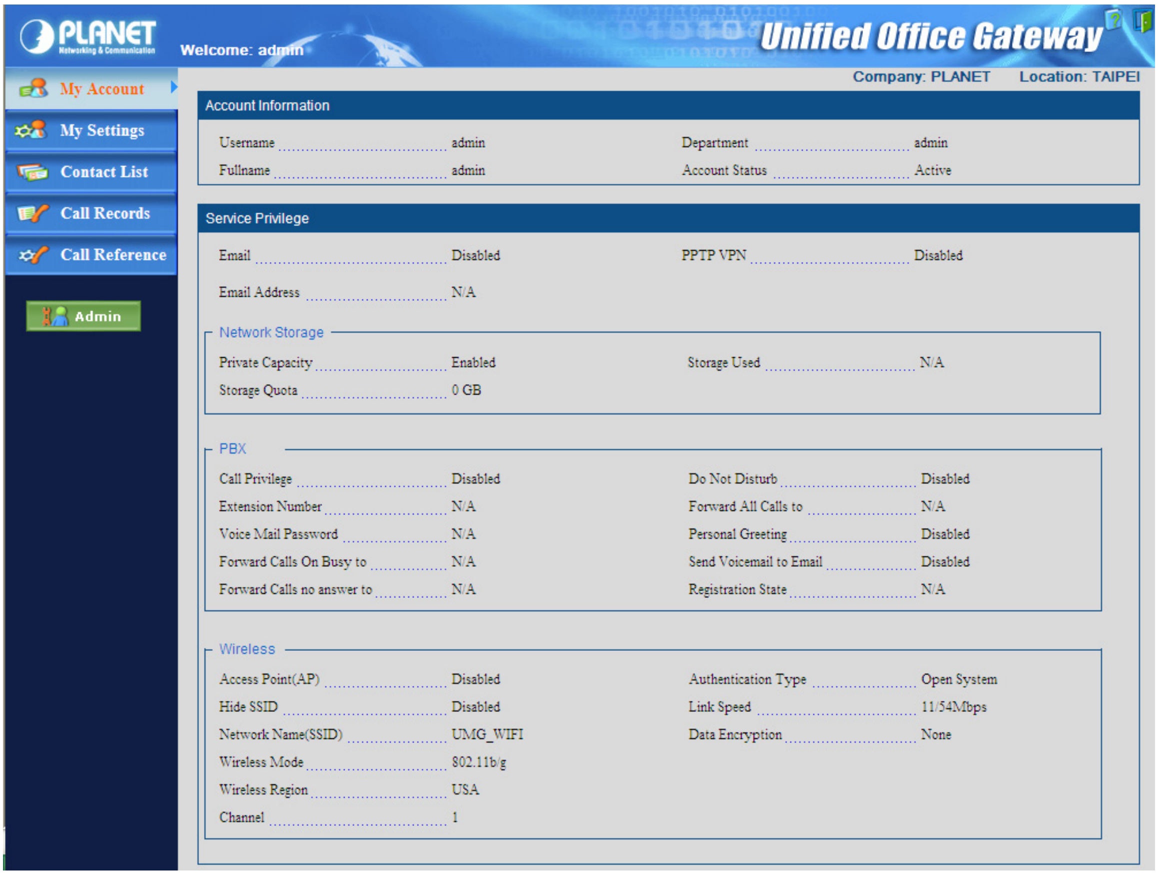
Any user who wants to access the UMG-2000 / UMG-2200 web management must login here. Type an authorized username and password and then login.



Note:
The user login session will be automatically terminated for security reason, If no action is taken in 5 minutes.

15.2 User Home Page

The page “My Account” shows the user profile.



Company: PLANET Location: TAIPEI

Account Information

Username	admin	Department	admin
Fullname	admin	Account Status	Active

Service Privilege

Email	Disabled	PPTP VPN	Disabled
Email Address	N/A		

Network Storage

Private Capacity	Enabled	Storage Used	N/A
Storage Quota	0 GB		

PBX

Call Privilege	Disabled	Do Not Disturb	Disabled
Extension Number	N/A	Forward All Calls to	N/A
Voice Mail Password	N/A	Personal Greeting	Disabled
Forward Calls On Busy to	N/A	Send Voicemail to Email	Disabled
Forward Calls no answer to	N/A	Registration State	N/A

Wireless

Access Point(AP)	Disabled	Authentication Type	Open System
Hide SSID	Disabled	Link Speed	11/54Mbps
Network Name(SSID)	UMG_WIFI	Data Encryption	None
Wireless Mode	802.11b/g		
Wireless Region	USA		
Channel	1		

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.

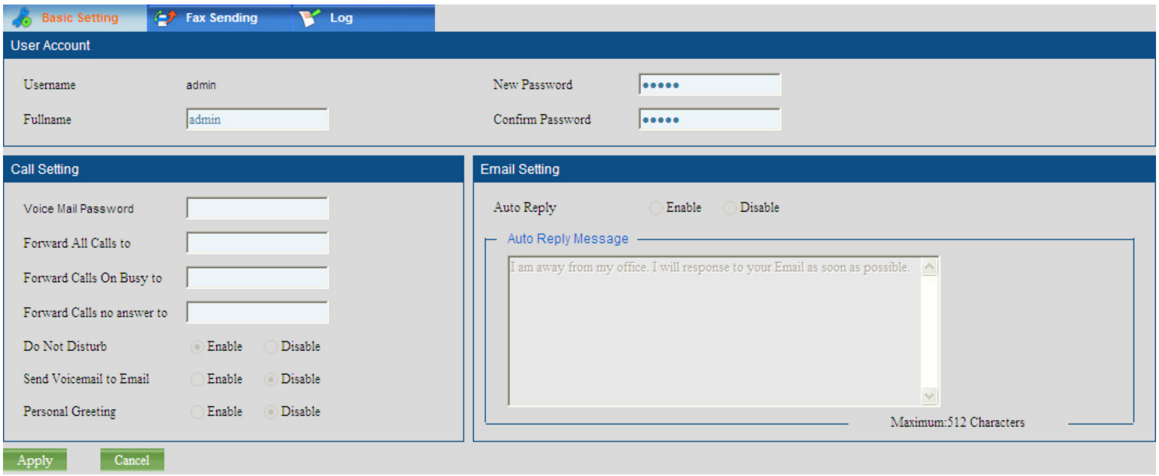
15.3 Access to Administrator

If your account is the administrator, there will be an “Admin” button on the left. Click that button to access the UMG-2000 / UMG-2200 web management.

Note:
Only one system administrator login session is allowed at any time.

15.4 Personal Setting

Users can update the profile in their own way on the “Personal Setting” page.



User Account

Username admin

Fullname admin

New Password •••••

Confirm Password •••••

Call Setting

Voice Mail Password

Forward All Calls to

Forward Calls On Busy to

Forward Calls no answer to

Do Not Disturb ● Enable ○ Disable

Send Voicemail to Email ○ Enable ● Disable

Personal Greeting ○ Enable ● Disable

Email Setting

Auto Reply ○ Enable ○ Disable

Auto Reply Message

I am away from my office. I will response to your Email as soon as possible.

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

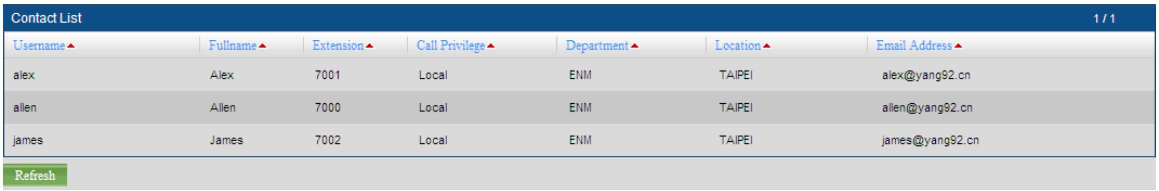
Voice Mail Password: Specifies your voice mail password.
Forward All Call to: Specifies the unconditional forward extension. Fill the text fill only if you would like to forward all your calls to the extension.
Forward Calls on Busy to: Specifies the forward extension. Fill the text fill if you would 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.

15.5 Contract List

All users with their extensions and email addresses in the UMG-2000 / UMG-2200 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

CONTACT LIST

Username: Displays a username.

Full Name: Displays the full name of the user.

Extension: Displays the extension of the user.

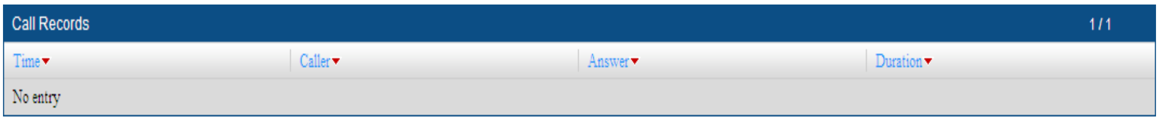
Department: Displays the department/group the user belongs to.

Location: Displays the location of this user.

Email Address: Displays the Email address of the user.

15.6 Personal Call Records

The “Call Records” page shows the call records of the user.



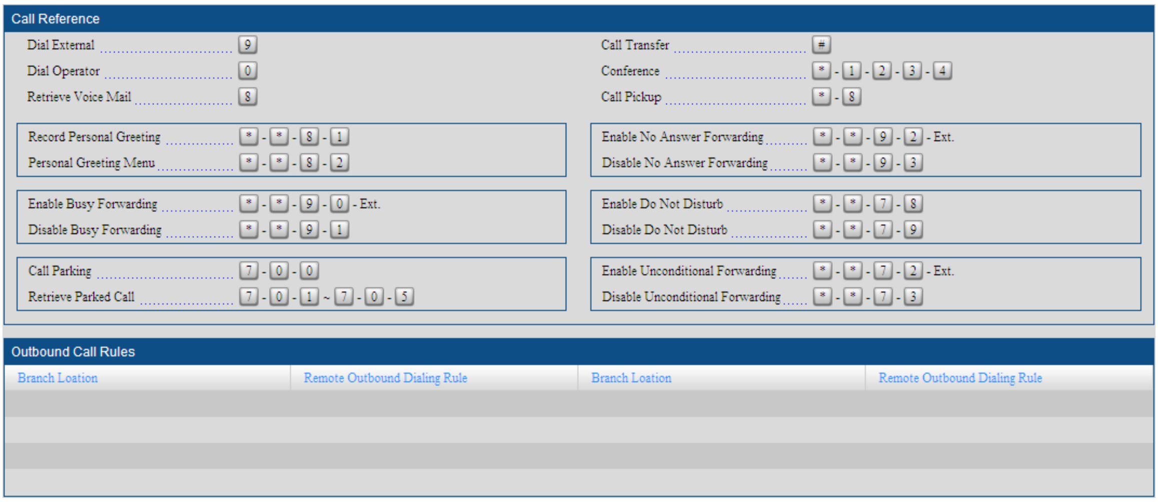
Call Records 1 / 1

Time	Caller	Answer	Duration
No entry			

Please refer to Section - IP PBX Call Records.

15.7 Call Reference

Users can get the call reference from the page “Call Reference”.



Call Reference

Dial External	9	Call Transfer	#
Dial Operator	0	Conference	* - 1 - 2 - 3 - 4
Retrieve Voice Mail	8	Call Pickup	* - 8
Record Personal Greeting	* - * - 8 - 1	Enable No Answer Forwarding	* - * - 9 - 2 - Ext.
Personal Greeting Menu	* - * - 8 - 2	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

Outbound Call Rules

Branch Loation	Remote Outbound Dialing Rule	Branch Loation	Remote Outbound Dialing Rule

Please refer to Section - IP PBX Call Reference.

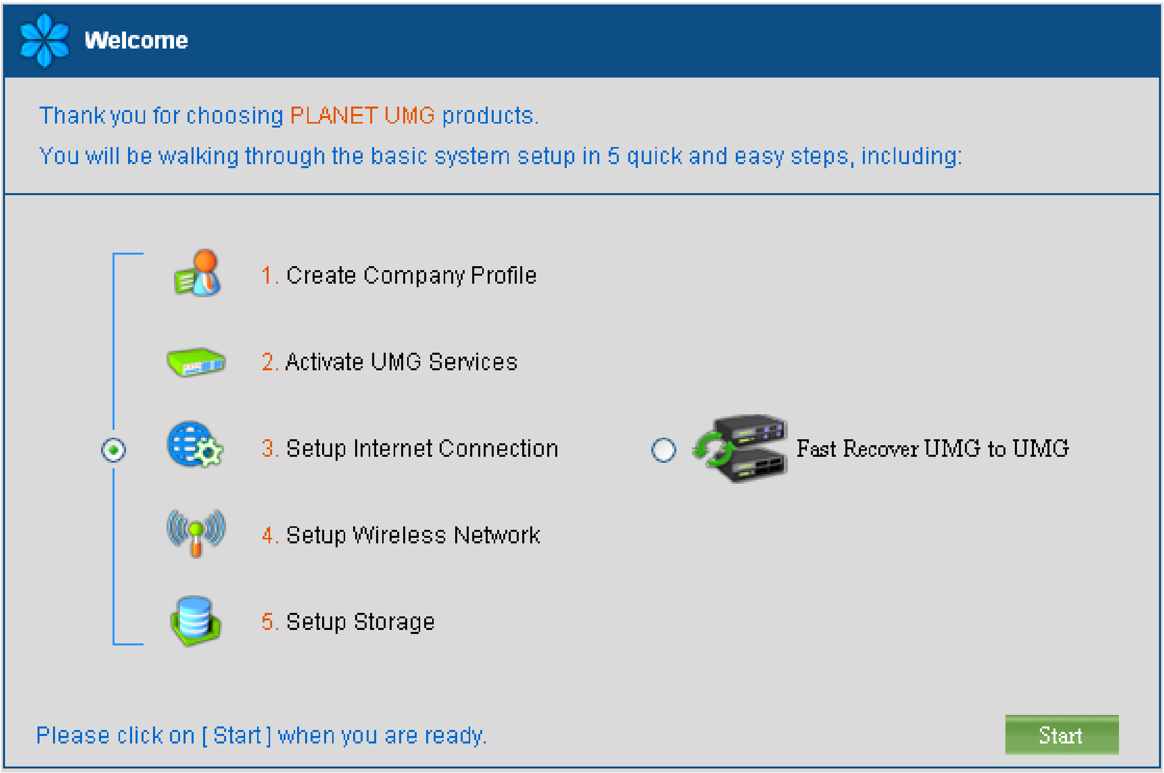
15.8 Logout

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.



Welcome

Thank you for choosing PLANET UMG products.

You will be walking through the basic system setup in 5 quick and easy steps, including:

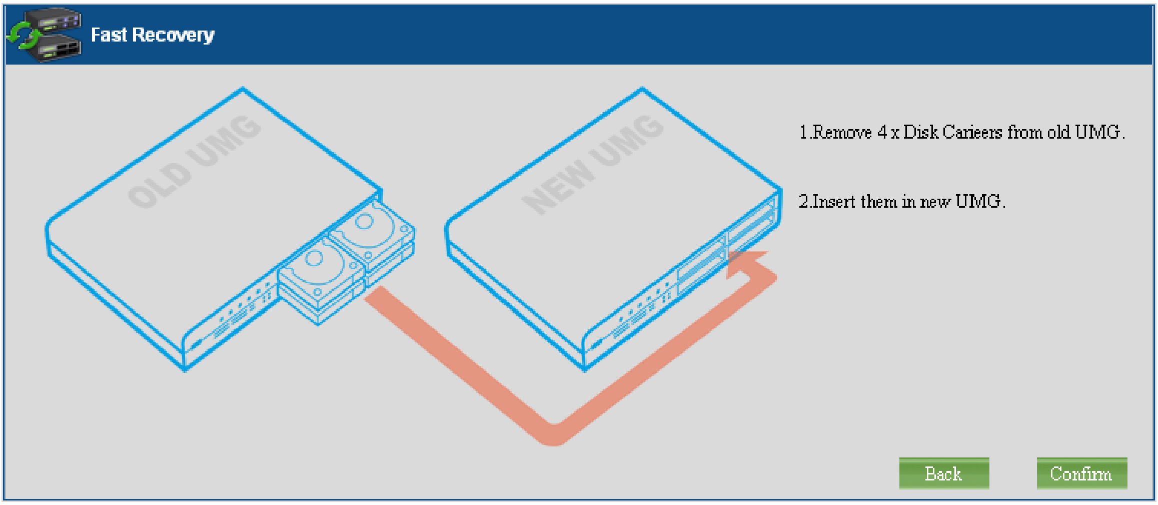
● 1. Create Company Profile
2. Activate UMG Services
3. Setup Internet Connection
4. Setup Wireless Network
5. Setup Storage

○ Fast Recover UMG to UMG

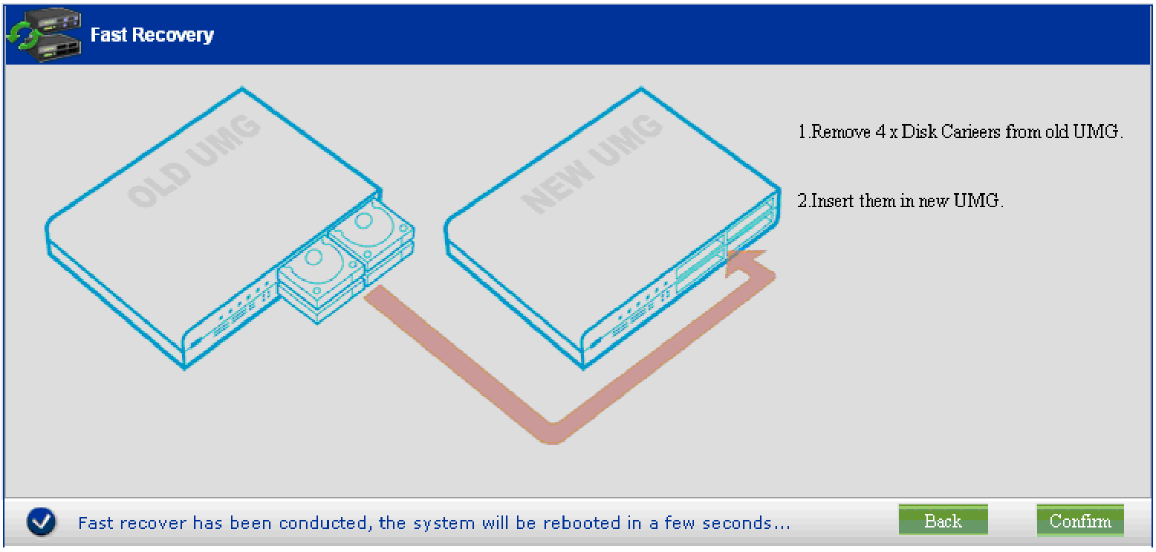
Please click on [Start] when you are ready.

Fast Recovery

Insert the four disks that you removed from the faulty UMG-2000 / UMG-2200 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.


Fast Recovery
OLD UMG
NEW UMG
1.Remove 4 x Disk Carieers from old UMG.
2.Insert them in new UMG.
Back
Confirm

If the following screen appears, it means the fast recovery has completed successfully. Otherwise, check the devices. After the rebuilding, the UMG-2000 / UMG-2200 will reboot automatically. Then the new UMG can serve normally.


Fast Recovery
OLD UMG
NEW UMG
1.Remove 4 x Disk Carieers from old UMG.
2.Insert them in new UMG.
Back
Confirm

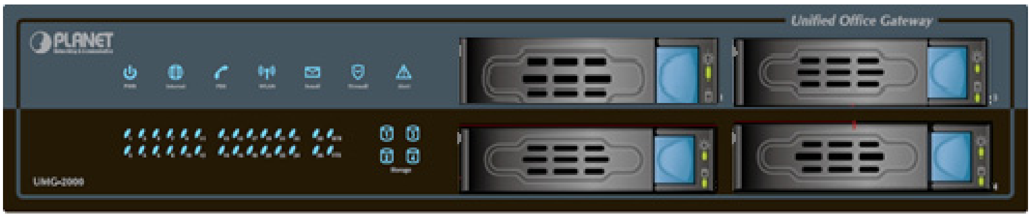
Fast recover has been conducted, the system will be rebooted in a few seconds...

Appendix B - Hard Disk Hot Plug

The UMG-2000 / UMG-2200 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)

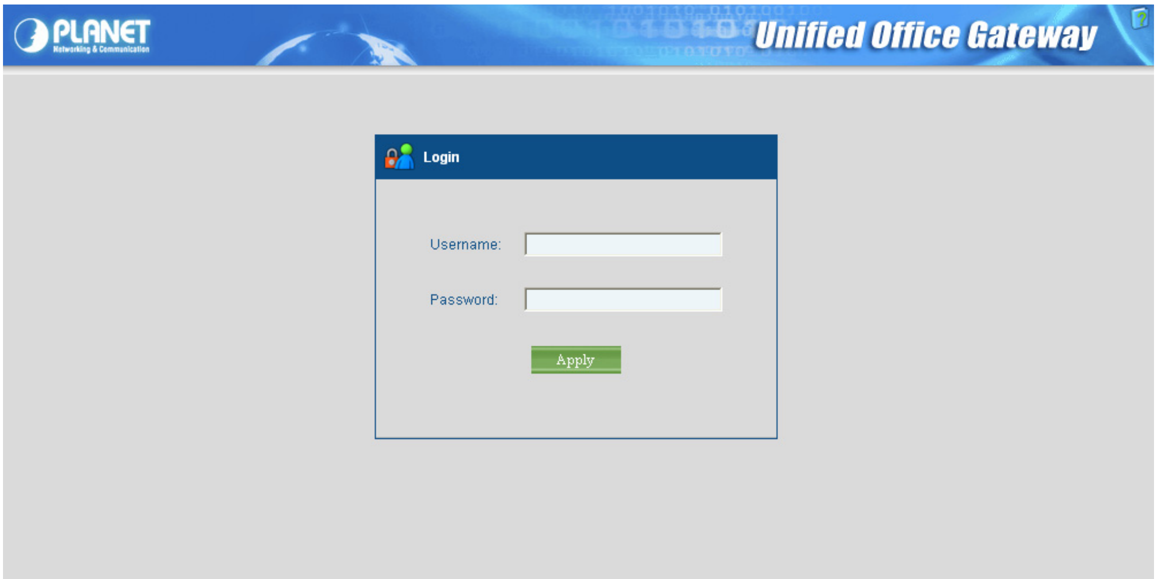
After the alert LED is turned off, you can plug in the new hard disk. Then the alert LED will flash again. Please do not insert or remove any disks while the LED is flashing. After plugging the new devices into the disk bay, the RAID will rebuilt corrupted data automatically. The data repair duration 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 / UMG-2200 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.


PLANET
Networking & Communication
Unified Office Gateway
Login
Username:
Password:
Apply