

# Internet Hotspot Gateway Products

*WiFi Hotspots made easy  
so you can provide a  
better Internet service for  
your guests and visitors*



## A Guide to the Operation of Guest Internet Products

Version 2.4 Software



Manual Revision 2.4



## FCC STATEMENT

### ***Class A Digital Device***

*This equipment complies with Part 15 of the FCC rules. Operation is subject to the following conditions.*

- 1. The device may not cause harmful interference.*
- 2. This device must accept any interference received, including interference that may cause undesired operation.*

### ***Federal Communications Commission Notice***

*This equipment complies 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.*

*The equipment can radiate radio frequency energy. If not installed and used in accordance with the instructions in this manual, it may cause harmful interference to radio, television or telecommunications reception, which can be determined by turning the equipment off and on. The user is encouraged to try and correct the interference by one or more of the following measures.*

- Reorient or relocate the receiving antenna*
- Increase the distance between the equipment and the receiver*
- Power the equipment via a different electrical circuit from that which the receiver is connected*
- Consult the dealer who installed the equipment, or an experienced radio frequency technician*

### ***Modifications***

*The FCC requires that no changes or modifications may be made to this device that are not expressly approved by Guest Internet Solutions. Any unauthorized changes may void the users authority to operate the equipment.*



# Contents

	page
Preface	5
<b>1 INTRODUCTION</b>	<b>6</b>
Provide a Public Internet Hotspot Service for your Guests and Visitors	
Provide Managed Internet Access or Controlled Internet Access	
Using Social Media (Facebook) Login to know who your Users are	
<b>2 PRODUCT FEATURES</b>	<b>18</b>
Features of Guest Internet Gateway Products	
Tabulated summary of features	
<b>3 PRODUCT INFORMATION</b>	<b>25</b>
Current Products	
Your Gateway Product Package Contents	
GIS-K1 Gateway	
GIS-R2 Gateway	
GIS-R3 Gateway	
GIS-R4 Gateway	
GIS-R5 Gateway	
GIS-R6 Gateway	
GIS-R8 Gateway	
GIS-R10 Gateway	
GIS-R20 Gateway	
GIS-R40 Gateway	
GIS-TP1 Ticket Printer	
<b>4 PREPARING YOUR GATEWAY FOR USE</b>	<b>40</b>
Installing the Gateway product in the Computer Network	
Switching the Gateway Product on for the First Time	
Connecting Your Computer Browser to a Guest Internet Product	
The Quick Start Wizard: Get Your Gateway Working Quickly	
Check the Internet Connection	
Set the Time Zone and Password	
Enter Your Business Information for the Login Page	
Select Disclaimer or Code Access	
Completing the process	
<b>5 USING YOUR GATEWAY</b>	<b>53</b>
Operating the Guest Internet Gateway Unit	
Second Login for Access Code Generation and Management	
<b>6 STATUS FUNCTIONS</b>	<b>62</b>
System Information	
Connected Users	
Usage Reports	



	<b>Billing Reports</b>	
<b>7</b>	<b>MANAGEMENT FUNCTIONS</b>	<b>67</b>
	Manage Codes	
	Hotspot Availability	
	Change Password	
	Reboot System	
<b>8</b>	<b>ADVANCED SETTINGS</b>	<b>79</b>
	Login Settings	
	Login Messages	
	Credit Card / PayPal	
	Edit Disclaimer	
	Time Zone	
	Email Settings	
	Content Filter	
	Dynamic DNS	
	Bandwidth Control	
	Network Interfaces	
	Wireless Settings: for the GIS-K1 only	
	WAN Settings: GIS-R10 and GIS-R20 only	
	LAN Settings: GIS-R10 and GIS-R20 only	
	Firewall	
	Port Forwarding	
	Monitoring / Alerting	
	Hostname	
	Allowed IP List	
	Allowed MAC List	
	Blocked MAC List	
	Ticket Printer Setup	
	Upgrade Firmware	
	Backup and Restore	
<b>9</b>	<b>RESET THE PRODUCT CONFIGURATION</b>	<b>147</b>
	Set to Factory Defaults	
<b>10</b>	<b>PROGRAMMERS REFERENCE</b>	<b>150</b>
	Access Code Request API for PoS/PMS Systems	
<b>11</b>	<b>LINUX DISTRIBUTION</b>	<b>155</b>





## Preface

We work very hard to ensure that our customers get the product features that they need. We always value feedback from our customers regarding new features that they would like to have in future versions. If you have a request for a new feature then please contact us at: [info@guest-internet.com](mailto:info@guest-internet.com) with your suggestions.

### TAKE CARE WHEN USING WIRELESS ROUTERS WITH GUEST INTERNET GATEWAYS

Please be aware that wireless routers will prevent your WiFi hotspot working correctly if the wireless router is not configured properly. Please avoid using a wireless router unless you are familiar with configuring the wireless router as a bridge mode access point

All GIS gateway products authenticate users by issuing an IP address to each user, and recording the MAC address of each users computer. The GIS gateway requires a wireless access point to be connected for WiFi access. If a wireless router is used to connect users then the login and authentication process will become intermittent. DO NOT use a wireless router such as the Linksys WRT-54G unless you are familiar with the procedure to disable the NAT'ing service. A wireless router, such as the Linksys WRT-54G, can be used if (a) the WAN port of the router is left disconnected, and (b) the router DHCP service is disabled.

Always install the GIS gateway together with a wireless access point configured in bridge mode (default mode) to the GIS gateway LAN port. Wireless routers intended for residential use have a limited range and area of coverage due to low RF power output. We recommend installing high power, long range commercial grade access points with GIS gateway products, such as those manufactured by Engenius and Ubiquiti.

### UPGRADING EARLIER FIRMWARE

#### Upgrades are always free:

Guest Internet products can be upgraded to the latest firmware specification free of charge. Please see our website support page to request a firmware update. Install the upgrade file using the firmware upgrade feature shown in the menu. When the upgrade has been initiated leave the unit powered up for 10 minutes before using it or powering it down. This time is required to store the new firmware in the product memory.

### NEW GATEWAY FEATURES FOR CURRENT PRODUCT MODELS

#### Social media login

##### 'Social WiFi'

The user login process can optionally use the guests social media account (Facebook) to login to the public hotspot. This login procedure can provide the hotspot owner with the guests profile information is the guest authorizes access. In addition the guest is presented with the opportunity to 'like' the hotspot owners social media website.

#### Access codes with download volume limits

Access codes can now be generated with a limit on the volume of bytes that can be downloaded in addition to the time limits set on the codes as with previous versions. This feature has been added for customers that have ISP's who add additional charges for monthly data volumes.

### FUTURE GATEWAY FEATURES

#### Cloud Management for remote management of multiple devices:

The gateway firmware can be upgraded to become a managed node in the Guest Internet cloud based management and accounting system. Guest Internet will offer a server that includes: central management of devices and groups of devices, central failure monitoring of devices, comprehensive reporting that includes usage and billing for both devices and groups, global access codes, and credit card reporting. The cloud management system is suitable for a multi-device, multi-site network. The cloud service is free to manage one device. An annual fee is paid for the cloud service that will manage 2 to 99 devices..



# 1: INTRODUCTION

## Provide a Public Internet Hotspot Service for your Guests and Visitors

Many restaurants, bars, hotels and motels offer free wireless Internet for guests, or charge guests for the Internet service. Guests and travelers make reservations based on Internet availability because they have gadgets that use wireless Internet: iPhones®, iPod Touch®, laptop computers, and Blackberries®

Guest Internet (GIS) products provide an easy and economical solution for any restaurant or lodging business that wants to begin offering Internet for guests, or wants to upgrade an existing system.

Restaurant and lodging businesses that already provide Internet for guests can install GIS products to improve their Internet service quality and increase returns.

- GIS low cost products are tough, reliable and very simple to install and can be used in many different applications
- You can brand your Internet service with the easy to use wizard
- Use your guest Internet service to advertise your special offers and promote your website
- You can control Internet access to prevent guests abusing the service
- Choose to provide free Internet or charge guests for your Internet service

Many locations can benefit by providing Internet services to the public. Business benefits include improved sales, more return customers, and increased walk-in customers.

- Restaurant
- Coffee bar
- Public library
- Truck stop
- Motel
- RV park
- Visitor center
- Public park
- University
- Student dorms
- Marina
- Church
- Trade show
- Event reception
- Fashion show
- Train station
- Music concert
- Theater
- Golf club
- Casino
- Sports club
- Gymnasium
- Bookstore
- Beach kiosk
- Hospital
- Airport
- Shopping mall
- Hotel
- Resort
- Multi-tenant condo

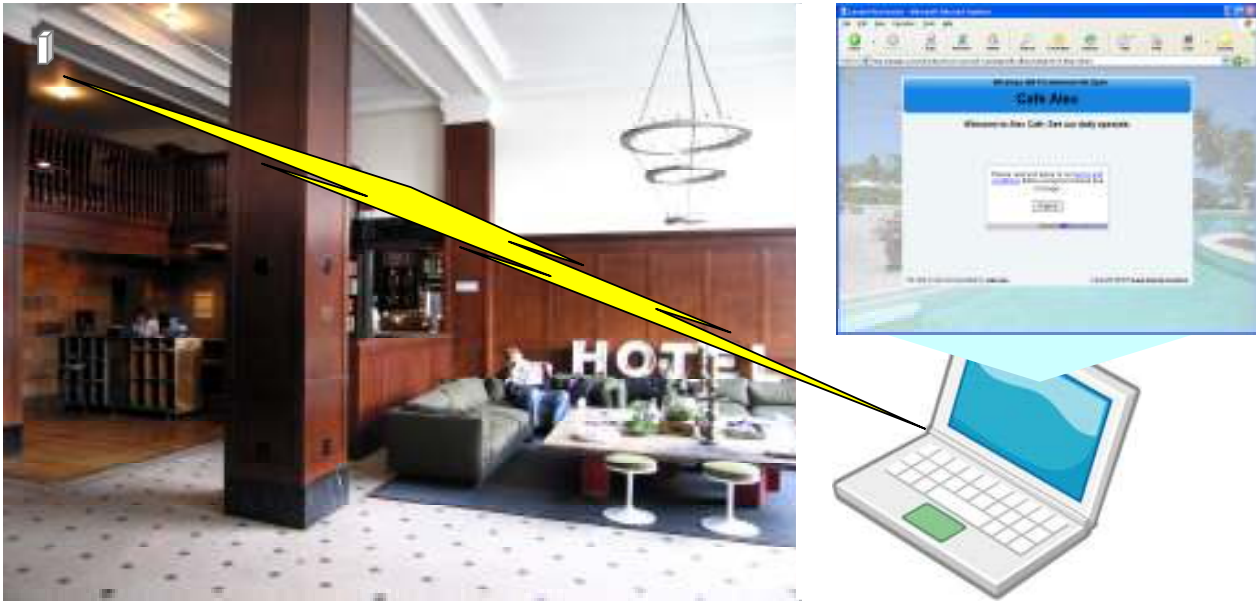
Internet access can be offered for free or can be charged for by selling access codes. Advertising can also generate revenue for both free and charged Internet access. Free controlled access can be provided where authorized customers are provided with access codes. The duration of access codes is selected when they are generated.



Guest Internet gateway products are very robust and reliable as they are manufactured to commercial grade standards. Wireless access points can be connected to the gateway to provide WiFi wireless Internet. Any type of WiFi enabled device can receive the signal: including PC laptops, MAC computers, netbook computers, iPhones™, and Blackberries™.

Guest Internet products have a 'login page' that requires the user to agree to the terms and conditions, and possibly pay a fee for an access code. The business owner decides if Internet will be free or if guests will pay for the service.

## Login Display



The login page is very important for the business providing the Internet service as it has several essential features:

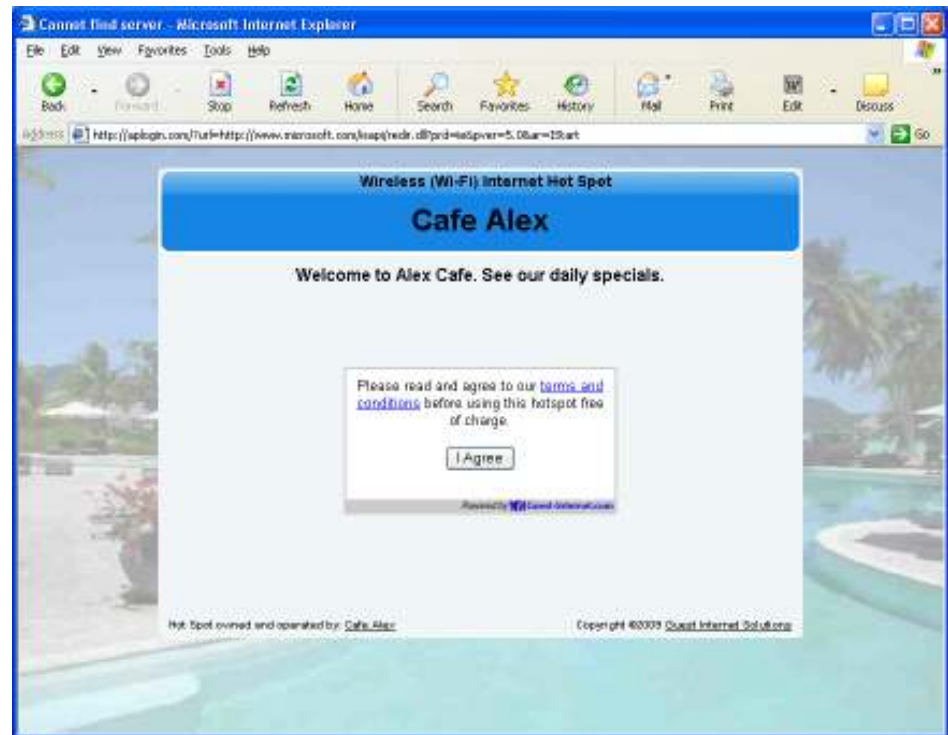
- Brand the Internet service
- Provide the business contact information for guests
- Encourage the guest to go to the business Web site
- Guests must agree to a disclaimer, so the business avoids liability
- Advertise products or services provided by the business
- Control who uses the Internet with access codes
- Charge for Internet access by selling access codes

This manual explains how to install a Guest Internet gateway product and create a custom login page ready for guests to access the Internet. The only decision you have to make is if you will provide free Internet or charge for the service.

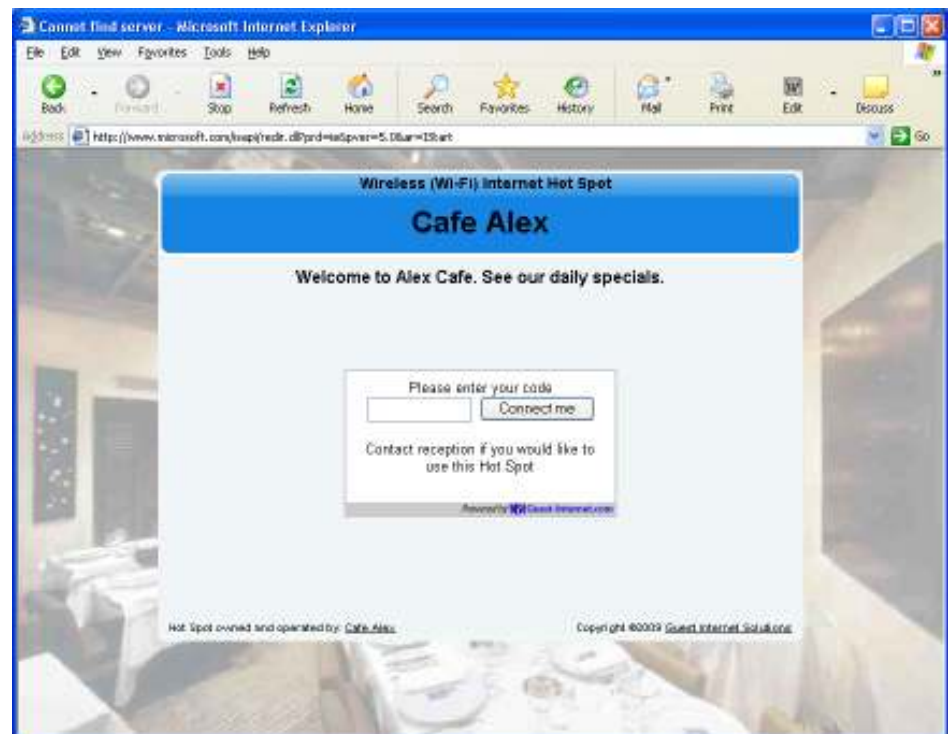
Two login page examples are shown below. The first is an example of unlimited access where the user has to click on a button agreeing to the terms and conditions. The second example shows controlled access: the user has to enter an access code that has been generated using the code management admin page



**Login Page Example: the user has to accept the terms and conditions**



**Login Page Example: in addition to accepting the terms and conditions, the user has to enter an access code provided by the business owner**





## Provide Managed Internet Access (with the social media login option) or Controlled Internet Access

Before installing the Guest Internet router product you must decide if you want to provide unlimited Internet for your guests or if you want to control the access your guests have to Internet services.

Both unlimited access and controlled access show the guests your login page when their computer browser opens. Both options also require guests to click on a disclaimer button accepting the terms and conditions of use. You can edit and change our standard disclaimer document. The disclaimer is important to protect you if your guests download copyrighted files or illegal content.

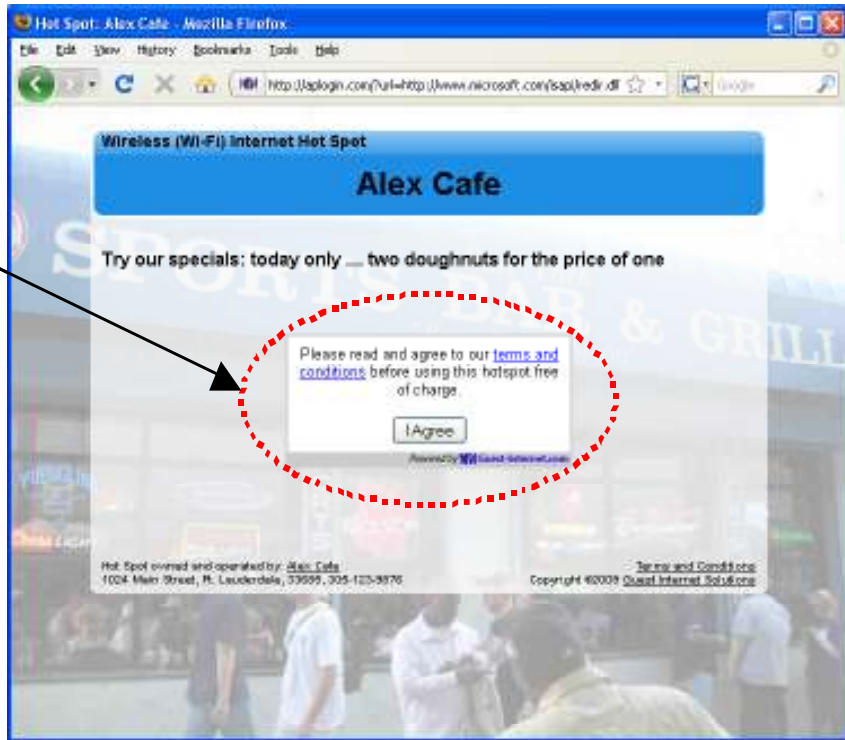
Controlled access also adds the requirement that the guest must enter an access code. You generate the access codes using the Guest Internet gateway product and you determine who gets access codes and who does not. If you wish you can charge your guests for access codes. Please read later sections describing access code generation.

### Unlimited Internet Access

When unlimited Internet access has been selected during the configuration wizard setup process the guest tries to access the Internet but sees the custom login page in the browser. The custom login page provides business contact information that may be useful for the guest. A box is shown on the page that requires the guest to click on a button that says "I agree to the terms and conditions of use". The guest can read the terms and conditions of use document. The terms and conditions of use document can be modified to include local laws (see the later section).

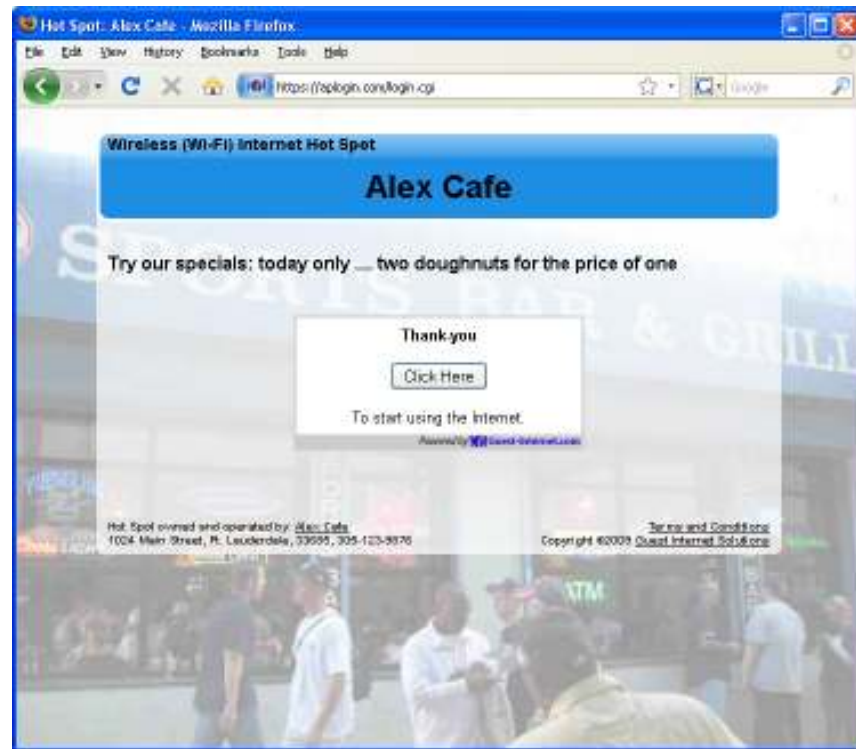
Login Box

Click on 'I agree' to disclaimer



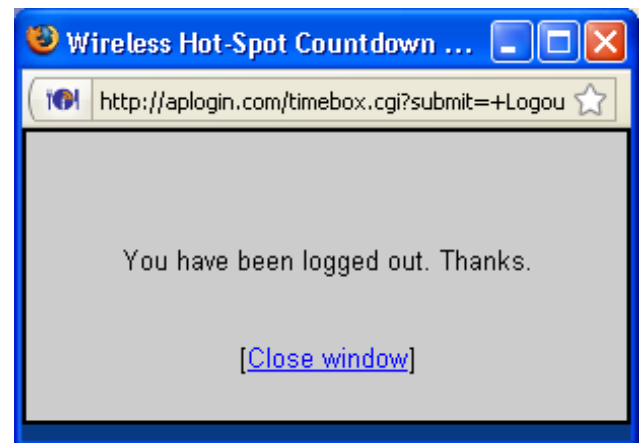
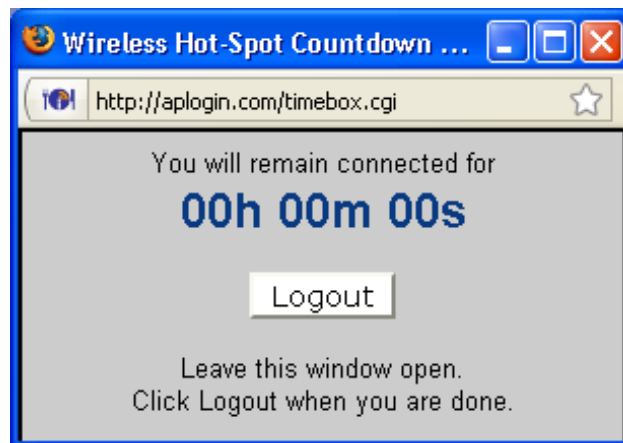
When the guest has clicked on the button then a second page is shown with a button that says click to access the Internet. When this button is clicked the guest has access to the Internet. The web page that the guest initially requested (the guests home page) is also shown. The figure below shows the screen that the guest sees when the 'I agree..' button is clicked





In addition to the browser showing the Web page that was originally requested, a small window will open that provides a button for the guest to log out of the Internet service.

The figure below on the left shows the window that the guest sees when the 'Click here' button is clicked. When the guest has finished using the Internet and clicks on the 'Logout' button then the window changes to that shown on the right.



If the guest closes the window showing the remaining time then this information can be accessed once more by opening a new browser window and typing the URL:

**http://aplogin.com**

The time that remains for the guest's access code is shown on the screen.



There is also an alternative to uncontrolled access called open access. In this mode the login page is not displayed, however all controls are applied to the user, including content filtering, speed control, P2P blocking and other firewall rules. Open mode is ideal for a condominium or rental community where a login page is not required, however access controls are necessary.

There is an option of uncontrolled access where information can be requested from the user before the user is permitted to access the Internet. Three data fields can be specified, where the fields might be name, phone number and email address. The email option is configured to send the information that is collected to the hotspot owner. Note that there is no verification of the information provided by the user.

## Controlled Internet Access

When controlled Internet access has been selected during the configuration wizard setup then the login process requires the guest to enter an access code.

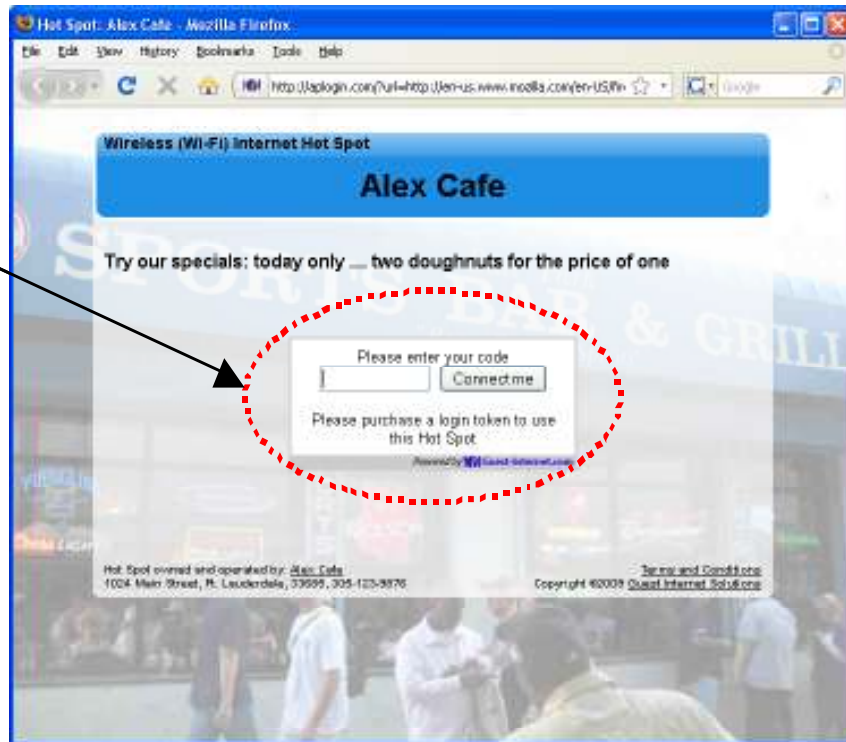
When the guest opens a computer browser to access the Internet the custom login page will be shown in the browser window. The box shown on the page requires the guest to enter an access code and then click on a button that says, "I agree to the terms and conditions of use".

Access codes are generated within the Guest Internet gateway unit for use with only that unit: see later sections describing how this is done. Each access code has a fixed duration, determined when the code is generated. When the time expires the code cannot be reused.

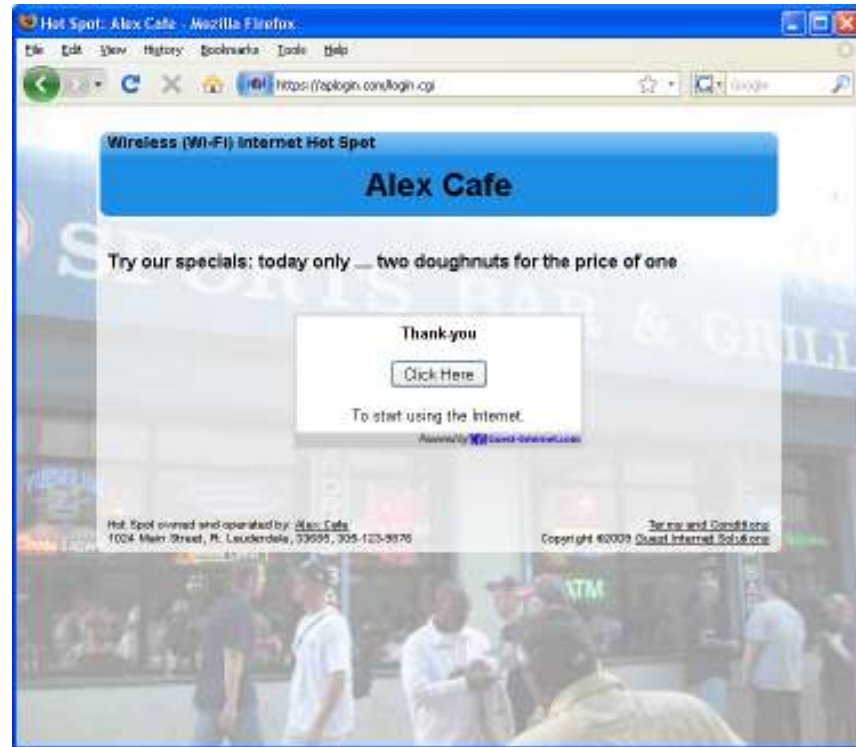
The login screen that the guest will see is shown below.

### Login Box

Enter access code then click on 'I agree' to disclaimer

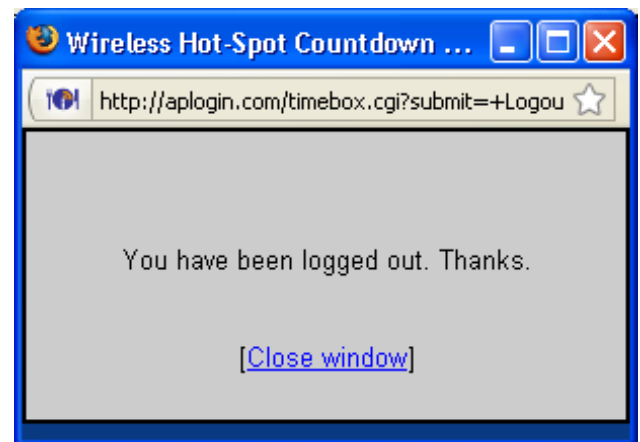
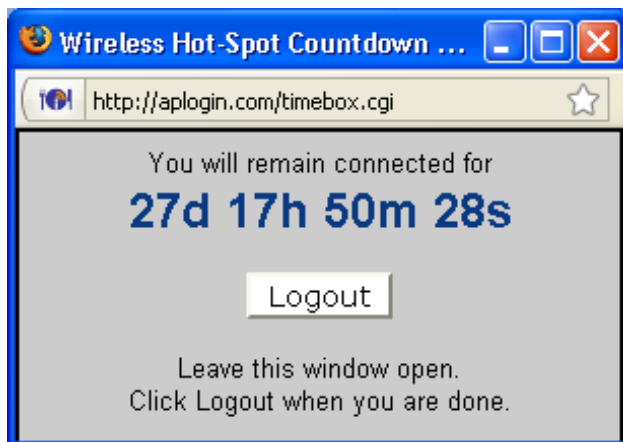


When the guest has typed in the access code and clicked on the button then a second page is shown with a button that says click to access the Internet. When this button is clicked the guest has access to the Internet. The web page that the guest initially requested (the guests home page) is also shown. The figure below shows the screen that the guest sees when the 'Connect me' button is clicked.



In addition to the browser showing the Web page that was originally requested, a small window will open that provides a button for the guest to log out of the Internet service.

The figure below on the left shows the window that the guest sees when the 'Click here' button is clicked. When the guest has finished using the Internet and clicks on the 'Logout' button then the window changes to that shown on the right.



If the guest closes the window showing the remaining time then this information can be accessed once more by opening a new browser window and typing the URL:





## <http://aplogin.com>

The time that remains for the guest's access code is shown on the screen.

Controlled Internet access requires the guest to type an access code into the login page box. You will generate the access codes using the managed code feature. You can access the managed code feature by logging in to the gateway product as the administrator;

## <http://aplogin.com/admin>

The screen will request you type in a username (**admin**) and the password that you will enter during the wizard setup process.

When you are logged in the select 'manage codes' shown in the menu on the left side of the screen.

You can generate codes that are valid from 30 minutes to 180 days and also unlimited time codes. You can generate single user or multi-user codes. Only one guest can use a single user codes and the code cannot be passed from one guest to another. Many guests can use multi-user codes simultaneously.

You decide who can access your Internet service by giving codes only to guests that you authorize. You can also sell codes to guests and provide wireless Internet as a paid service.

Some examples are included here to illustrate how codes can be used

1. Restaurant: Prevent guests at the restaurant next door using your Internet service by creating a one-day multi-user code that you can give to your guests when they ask for Internet access. Create a different multi-user code each day.
2. Hotel: Free Internet for guests; generate a unique code to give to each guest for the length of the stay. However if a visitor using the conference room wants to use the Internet then charge for a code (e.g. \$10/day).
3. Coffee bar: charge guests for Internet, each day download access codes and print onto adhesive labels.

Use your Internet service as a tool to attract customers. For example, if your competitor is charging for Internet then offer free Internet.

Take care how you offer Internet service for guests. For example a coffee bar that offers free unlimited Internet might find that guests are occupying tables to use the Internet and not buying coffee or food. This problem can be easily solved using Guest Internet gateway products. Give 30-minute free codes at the checkout, and state that codes are given only with a purchase. The guest will be blocked from the Internet after the 30-minute code expires and the only way for the guest to continue using the Internet is to make a second purchase.

### **Using Social Media (Facebook) Login to Know who your Users are:**

Social Wifi helps your guests to grow your business by telling their friends how great you are. Your guests use your Internet Hotspot and tell you how they are via social media. You can also give them an opportunity to 'like' your social media web page.

Improve sales: Social WiFi is great marketing. You provide a high speed wireless Internet service for your customers and they thank you by telling their friends about your business via social networking.

Low cost: Guest Internet products offer great price/performance. Install social WiFi for as little as \$99. There are no additional fees to pay - unlike other Social WiFi vendors. This small investment can pay you back within a few days.



Easy to use: No technical skills are required. If you can use a computer then you can get the benefits of social WiFi. Set up your social media business page then connect the GIS product to your DSL/cable router. Configuration takes five minutes using the simple setup wizard. Get customer 'likes' plus powerful analytical reports.

Analytical Reports: Social media traffic analysis is at your fingertips via the Guest Internet Gateway.

## What is Social Media?

Social media is regularly used by over a billion people worldwide to maintain contact with friends and family, and share information about people, places and events with friends. Social media is a collection of websites that permit people to post information for their relatives and friends quickly and easily. The top ten social media websites are listed below, the most important social media sites are Facebook, Twitter and Google plus+.

- #1 - Facebook; 800,000,000 - Estimated Unique Monthly Visitors.
- #2 - Twitter; 250,000,000 - Estimated Unique Monthly Visitors .
- #3 - LinkedIn; 200,000,000 - Estimated Unique Monthly Visitors .
- #4 - Google plus+; 150,000,000 - Estimated Unique Monthly Visitors .
- #5 - Pinterest; 140,500,000 - Estimated Unique Monthly Visitors.
- #6 - Tumblr; 125,000,000 - Estimated Unique Monthly Visitors .
- #7 - Flickr; 67,000,000 - Estimated Unique Monthly Visitors .
- #8 - VK (similar to Facebook); 65,400,000 - Estimated Unique Monthly Visitors.
- #9 - Instagram; 50,000,000 - Estimated Unique Monthly Visitors .
- #10 - Myspace; 26,500,000 - Estimated Unique Monthly Visitors .

Each social media website requires a login procedure with username and password. A smartphone that is used to access the social media website can access via either the 3G/4G network or using a WiFi network. A WiFi is much faster than the 3G/4g network. Most tablets must access a WiFi Hotspot in order to connect to the Internet. Many businesses that have visitors or guests also provide a WiFi Hotspot Internet service. By adding a Social WiFi Gateway and use the guests social media login to authorize access to the Internet via the WiFi hotspot, then the business can begin building a social relationship with the guest. This concept is called Social WiFi.

## From Social Media to Social WiFi

The visitors and guests of many businesses are anonymous. Restaurants and retail stores for example do not know who their visitors and guests are. Businesses can employ social media as a tool to begin to build a relationship with with anonymous customers. A one-to-one relationship with the customer permits the business to generate more sales per customer through several methods. This includes encouraging the customer to return to the business frequently, and to persuade the customer to tell friends about the business. Building a special relationship with the customer requires the business to give the customer advantages that anonymous customers don't have. These advantages include discounts when purchasing products and services, and advance information about new products and services before anonymous customers know about them. Although the profit per sale to this special customer is reduced, the revenue per customer is greatly increased, which more than offsets the lower profit per sale. In addition, business that have a one-to-one relationship with customers are much more valuable than businesses that have only anonymous customers. The one-to-one customer relationship also promotes faster business growth, which further increases the value of the business. Social WiFi is one of the best tools available to enable businesses to begin marketing using social media.



## Social WiFi data

The proposition of Social WiFi is that your business provides an Internet WiFi Hotspot for guests to use with smart-phones and tablets and in return you ask your guests to 'like' your social media website and possibly comment on your business via the guests social media web page. If your guest gives authorization then you can collect some information about the guest that is provided by the social media website. The guest is encouraged to use your WiFi Hotspot because you provide a much faster download speed than the 3G/4G wireless network. Your guest will click on his/her social media website icon (e.g. facebook) to get access to the Internet. Before connecting the guest to the Internet one or more questions are asked of the guest

- Will you click the 'like' button to add 'likes' to the business social media page?
- Will you allow the the business to post a comment on your social media page?
- Will you allow the business to collect some information about you?
- Will you allow the business to send you special offers and information?

By interacting with the guest by asking the questions listed above, the guest ceases to be an anonymous customer, and becomes a 'friend' who can receive special offers and can tell friends and relatives about your business. A one-to-one marketing channel is established with each guest who provides social media information.

## Nurture the relationship with each guest

The people who decided to establish a connection with your business via social media are special, each one represents income for your business and so you must take steps to make them feel special. Here are some suggestions that you might try to strengthen the relationship with each guest.

- Send each guest a daily/weekly/monthly discount voucher to encourage returns
- Give guests a referral discount for each new guest that they send to you
- Encourage guests to post blog articles which will improve your website SEO rating
- Offer special deals for groups to encourage guests to network your business

Social media is a very powerful marketing tool and Social WiFi is the ideal method to access the power of social media marketing.

## Social WiFi Gateway

The Social WiFi Gateway is a tool that permits the business to offer a high-speed WiFi Hotspot Internet service with the user providing his or her social media links to get Internet access. The deal is good for the Internet user, he or she can decline to provide any information and still get Internet access - the terms and conditions of social media websites prohibit the business obliging the user to provide social media information in exchange for Internet access. However it is not desirable to coerce users to provide social media information, it is much better to provide the user with benefits and advantages that can only be obtained using social media as a tool. Examples of this are sending the user special discounts via social media, or advising the user of a product availability before other customers, via social media. The Social Wifi gateway has a list of features that benefit the business owner, some are listed below.

- Wifi Hotspot welcome page that advertises the business
- Display format that is suitable for smartphones and tablets
- Description of the social media benefits for the user



- Social media website login options
- Requests for different interaction levels with each user
- Logging of user information, sent to the business owner via email
- Extensive reporting for analysis of usage and social media interactions
- PCI compliance permits using the same Internet connection as business computers
- Control over the bandwidth available to each user
- Protection from viruses on the users computer, smartphone or tablet
- Website content filtering when the WiFi service must be family friendly
- Very easy for the business owner to install and use
- Remote access for management of the equipment
- Network diagnostic and alarm features to locate network problems

### **Social WiFi Data analysis**

While many Social WiFi providers charge a monthly fee to provide each business owner with a comprehensive report about social media data gathering using the Social WiFi Hotspot, Guest Internet does not charge you a cent or penny for this service. When you purchase the GIS Social WiFi gateway the product software has built in features that generate tables and charts from data logged during operation. The data files can be downloaded to your computer for long term analysis using spreadsheet or other software that can read CSV files. Data analysis is presented in five different formats. as listed below.

#### **Email of user social media data.**

Email transmission is an optional feature for use when the Social WiFi hotspot owner needs immediate notification of login events. Data collected at each login is sent via email to the designated email account, Gmail is the default email service supported on all GIS gateway products.

#### **Connected users table.**

Connected user data is tabulated and accessed via the administrator login. The data includes user information and the network usage. The table can be downloaded in CSV format for additional analysis. The last 10,000 data entries are logged so the file should be downloaded periodically when long term data analysis is required.

#### **Internet use graph.**

A graphical display that shows network data use for the WiFi Hotspot. Use this graph to verify that the Internet backhaul bandwidth is sufficient for the number of users who are using the WiFi Hotspot service.

#### **IPs vs. logged users graph.**

The IPs issues vs. logged user graph compares the number of smartphone and tablet devices within range of the WiFi Hotspot vs. the number of users that are actually logged into the WiFi Hotspot. This valuable information tells the business owner that additional advertising of the WiFi Hotspot service is required when the logged users is small compared to the devices in the proximity of the WiFi Hotspot.

#### **Media type login graph.**

The media type login graph shows a comparison between the login options chosen by the users. Each user has several login options, including login without providing information, login and like the business social media page. login and agree to a comment sent to the users social media page, and finally user authorization to provide some personal information to the business.



## **How Social WiFi can benefit your business**

Your guests can easily recommend your business to their friends: Each time that your guests connect to the Internet using the GIS Social WiFi Gateway they are invited to click a button which will place a recommendation of your business on their social page.

Your social media website visits rapidly increase with guest clicks: When your guests connect to the Internet using your GIS Social WiFi Gateway they are asked to 'like' your business social media page, which is the fastest way to add 'likes' to your social media page.

You get access to information that helps you improve your business sales: You can get your guests social media analytical data directly from the GIS Social WiFi Gateway. There is no need to pay for expensive 3rd party services to get the analysis of your guests social media use, saving you a lot of money.

Increase the tie-in's between your website and others to improve SEO: Improving Search Engine Optimization (SEO) means that your website gets a higher ranking on search engines like Google. Social WiFi can establish thousands of links between your business website and social media pages.

## **IT Installers: Provide a Social WiFi service for your business customers**

Help business owners without computer skills get the benefits of Social WiFi: Many business owners understand the benefits that social networking can provide to their businesses. However most don't have the skills to create a social media website and analyze the data to make it work. This is an opportunity for you.

Sell your analytical services with the advantages of recurring revenue: Your business may provide website development, SEO or business marketing for your clients. Now you can add social media services to your portfolio using the GIS Social WiFi Gateway as a tool to analyze your clients social media performance.

GIS Social WiFi Gateways are managed remotely directly by you: By installing a GIS Social WiFi Gateway at your clients site you can provide ongoing reports and analysis of your clients business social networking performance. You can access your clients data directly from the GIS Social WiFi gateway, and package the data in daily and weekly reports.

There are no additional charges for you to operate a GIS Social WiFi gateway: The great advantage of providing social media services for your clients using GIS Social WiFi Gateway products is that there are no service charges - unlike our competitors. When you purchase and install the GIS Social WiFi Gateway it provides all the data analysis that you need.

Integrate your back-office data analysis tools: If your business includes social media marketing then you will have already developed a suite of back-office analytical tools that generate data for your customers. These same tools can load data from any GIS Social WiFi Gateway for further analysis.

Product branding is available for quantity buyers: Resell products with your branding with a minimum five-piece quantity order of any model. Product branding includes labeling the enclosure with your logo and model number, and adding your logo and model number to the product firmware.



## 2: PRODUCT FEATURES

### Features of Guest Internet Gateway Products

When any business provides an Internet service for guests, visitors and customers, it is very important to prevent abuse of the services, otherwise bad things can happen;

People are using your Internet service without your consent.

A free service can become a headache if users start complaining about the poor performance of the Internet service.

Users start surfing inappropriate websites in public areas.

The DSL or Cable service provider can threaten to disconnect the service because users are sharing files illegally.

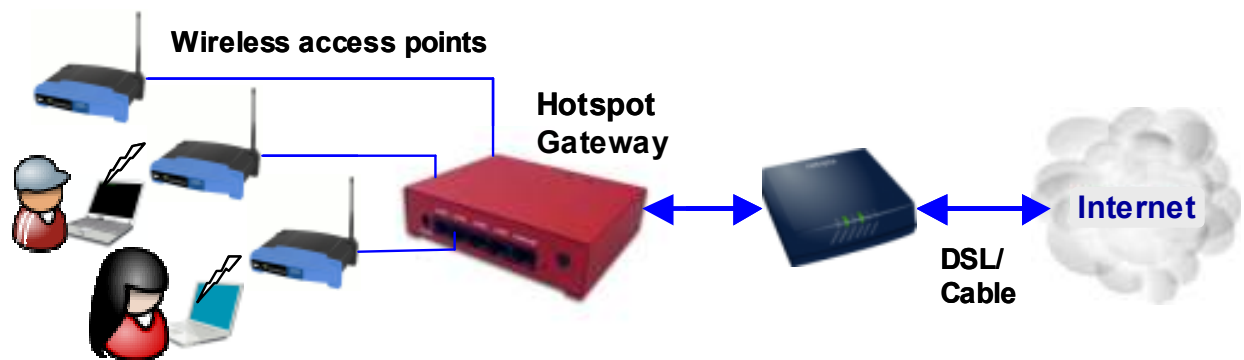
A free service starts costing the business a significant amount of money as the use is far greater than expected

The Hotspot gateway give you control of the Internet service that you provide for your guests, visitors and customers. You can prevent unauthorized use, and prevent any authorized user abusing the service.

The Hotspot gateway is installed in your network between the wireless access point, and the DSL or Cable router. See the diagram below. All communications between your users and the Internet flows through the Hotspot Gateway. The gateway allows Internet access for authorized users, and blocks people not authorized. The gateway also controls how users access the Internet. You choose how your users will access the internet by choosing to set the features described in this manual.

The gateway is very easy to setup and use. A setup Wizard will be displayed on your computer the first time that you connect your computer to the gateway. Simply follow the steps described in the Quick Start Guide that is shipped with the product.

### Connecting the Hotspot Gateway



### Choosing the Right Hotspot Gateway

Guest Internet manufactures a range of Hotspot gateways that provide different levels of performance and features. The gateway performance is specified as the number of users that can use the Hotspot simultaneously. This is called the maximum number of concurrent users. The maximum number of concurrent users can only be reached when the Internet connection has a minimum speed. The maximum number of concurrent users is also reduced when several users are downloading large files such as video or music files. The following summary (next page) lists the Guest Internet products, and the parameters for each product.



## Login Page

The login page is the most important feature of the Hotspot gateway. All Guest Internet gateways provide three levels of login page customization;

Twelve pre-prepared login pages are contained in the gateway, choose one of the twelve login pages when answering the setup Wizard questions.

Any photo or design background can be uploaded in a JPG format and displayed as part of your login page. Combine a photo of your business and include your logo using Photoshop® to create a custom login page.

Design and program your login page using HTML. This procedure takes longer but gives the best results. Create a login page that looks like your website and then create a 'Walled Garden' to make sure that your users are familiar with your website.

## Social media login

Social Wifi hotspot login using the customers social media account (Facebook). With user authorization the hotspot owner can access the customer profile and add 'likes' to the hotspot owners social media web page.

## Disclaimer Text and Editor

When any user connects to the Internet they have to click a button and agree to the terms and conditions of use. This is very important and protects the service provider from possible legal action at a later date.

A standard disclaimer text is installed that is appropriate for US laws. A disclaimer editor permits the text to be modified so that additional requirements can be added, or the text can be translated to a different language.

## Access Codes

The login page can be setup so that the user only has to click on a button to agree with the terms and conditions, however there is no control over who can access the Internet.

Alternatively the gateway can be setup in the controlled access mode. Users can be authorized to access the Internet by generating access codes and giving one to each user. Access codes can have a time duration from 30 minutes to 180 days and can also be unlimited. An access code can also be terminated at any time.

Access codes ensure that only authorized users get access to the Internet.

## Reports of Usage

The Hotspot use can be monitored at all times by checking the usage report. This report shows the number of users connected (obtained IP addresses) and authenticated (entered a valid access code). The MAC address of each user is shown and the bytes each user has transferred has shown. Any users abusing the Hotspot service can be easily seen. A check box is provided to include the users MAC address in the blocked MAC list, thereby preventing the user accessing the Internet.

## Timer/Calendar for Availability

Many Hotspots are available 24x7 in businesses such as hotels. However the Hotspot in a dental office should only be available during business hours e.g. 9AM to 5PM). A 7-day timer /calendar is provided to set availability of the Hotspot in 1 hour increments. Outside the time that the Hotspot is activated the user will get a login screen with the message 'Hotspot not available'.

## Content Filter

The content filter blocks access to websites that are not suitable for a public environment. Content filtering services are provided by **OpenDNS** who have a basic free service and a range of paid services when advanced content filtering rules are required.

## Bandwidth Control

All gateway products provide an overall bandwidth control where download and upload speeds are set independently. In addition each access code can have a download and upload speed associated that will override the overall bandwidth setting.

This feature enables tiered use of the Hotspot. A basic free low speed service can be provided, and augmented with a paid service where the bandwidth is much higher. Typical applications for such a service are student accommodation and motels.

## Firewall

GIS gateway products include a firewall that stops users on the public network (DMZ) accessing computers in the business network behind the gateway. This feature permits the public network and business network to share one DSL or Cable circuit.

The GIS-K1 also includes a second firewall that protects business computers (such as PoS





terminals) from access via the Internet.

## Remote Management

All gateway products can be managed from a remote location, provided that the network DSL or Cable service has a fixed IP, and that the DSL/Cable router has a port forwarding feature to provide access to the Hotspot gateway.

In the case where the DSL or Cable service has a dynamic IP allocation the Hotspot gateway can be accessed remotely using the **DynDNS** service. The Hotspot gateway has a DynDNS agent installed to permit the network IP address to be located via the DynDNS server. A free test account is provided by DynDNS, and the monthly account fee is very low.

## Remote access to Wireless Devices via Port Forwarding

The Hotspot gateway port-forwarding feature allows access to devices from outside the network (wireless access points) that are connected in the public network (gateway LAN ports). This feature can be used in conjunction with the monitoring and alerting feature to provide complete remote management and support for the Hotspot network.

## Monitoring and Alerting

It is very important that a Hotspot operator find out that a wireless network has problems before the users do to avoid stressful calls and complaints. All our Hotspot gateways can monitor LAN attached devices, such as wireless access points, for failure. The failure warning is sent out via email to the owner or operator of the network. The installer can use an existing email SMTP service to send the message. In many cases however the network provider who offers the email service is not the one that the gateway is connected to.

All our gateway products have an agent for the **SMTP2go** service that permits an email to be sent out from any network. The SMTP2go service has a very low monthly charge and the benefits of this service far outweigh the small cost.

## Allowed and Blocked IP and MAC Addresses

When any computer connected to the public network must access the Internet without requiring the login page then the device MAC address is included in the MAC bypass table.

Web sites that must be seen by users without login can have their IP addresses or URL's included in the IP bypass table. This feature permits a walled garden login when implemented in conjunction with the custom login page feature.

When users abuse the Hotspot service then their computer MAC addresses can be blocked. Look in the usage report table and identify users who are causing a lot of traffic. Then click on the block MAC address to block that user from the Internet.

## Network Port Configurations

The LAN port configuration is set permanently as a DHCP server. The reason for this is that IP addresses must be allocated to users as the IP's are used to authenticate each user. Other LAN port parameters can all be modified. The DHCP start and end addresses are used to set the limit for the maximum number of users.

The WAN port can be either a DHCP client or can have a fixed IP. When the content filter is activated the WAN DNS settings are replaced with those of OpenDNS.

## Backup and Restore the Configuration

The product configuration can be saved in a backup file. If the product is replaced or configuration changes are made but previous settings are required then the configuration file can be restored.

The configuration file of any gateway model can be restored on any other gateway model. All gateway models use an identical file structure.

## Upgrade Firmware

Firmware upgrades are released periodically for all gateway products. The upgrades include new features that have been requested by customers. We also work on product performance improvements. Firmware upgrades are free for our customers. There will never be a charge for the latest firmware.

## Tabulated Summary of Features







The tables on the following pages summarize the features provided with each product model, grouped as:

- Performance**
- Access control**
- Management**
- Security**
- Billing**
- Benefits**
- Social WiFi**











## Performance







Performance	GIS-K1	GIS-R2	GIS-R3	GIS-R4	GIS-R5	GIS-R6	GIS-R10	GIS-R20	GIS-R40
 Recommended maximum number of concurrent users (no limit is imposed)	50	50	100	150	100	200	250	500	1000
 Maximum throughput (bits/second between the LAN and WAN ports)	20 Mb/s	20 Mb/s	30 Mb/s	30 Mb/s	30 Mb/s	40 Mb/s	2x45 Mb/s	2x100 Mb/s	4x100 Mb/s
 Access code database size, maximum number of entries, recycled when codes expire	10,000	10,000	10,000	10,000	10,000	10,000	10,000	10,000	10,000
 Robust commercial grade equipment suitable for any business environment	✓	✓	✓	✓	✓	✓	✓	✓	✓
 LCD status display showing time, users, and system error messages					✓	✓	✓	✓	✓
 Built-in WiFi Wireless providing an area of coverage of 2000 sq ft	✓								

## Access Control







Access Control	GIS-K1	GIS-R2	GIS-R3	GIS-R4	GIS-R5	GIS-R6	GIS-R10	GIS-R20	GIS-R40
 Login page: library or custom login page with disclaimer editor	✓	✓	✓	✓	✓	✓	✓	✓	✓
 Access control: generate pass codes with many duration and control options	✓	✓	✓	✓	✓	✓	✓	✓	✓
 7-day timer-calendar which limits Internet access to business opening hours	✓	✓	✓	✓	✓	✓	✓	✓	✓
 Connected, authenticated and blocked user status information	✓	✓	✓	✓	✓	✓	✓	✓	✓
 Content filter: adult website blocking for a family friendly service	✓	✓	✓	✓	✓	✓	✓	✓	✓
 Speed control: prevent data hogs consuming your bandwidth	✓	✓	✓	✓	✓	✓	✓	✓	✓






## Management

Management		GIS-K1	GIS-R2	GIS-R3	GIS-R4	GIS-R5	GIS-R6	GIS-R10	GIS-R20	GIS-R40
	Remote access allows management of the gateway from anywhere in the world	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Data logging permits tracking of Internet use with report downloads	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Log hotspot user information, archive via email to comply with laws and regulations	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Management of network devices remotely via port forwarding (# of devices)	25	25	25	25	25	25	250	250	250
	Failure monitoring: receive an email alert if a wireless AP fails (# of devices)	25	25	25	25	25	25	250	250	250
	Backup and restore: save the configuration data for configuration recovery	✓	✓	✓	✓	✓	✓	✓	✓	✓







## Security

Security		GIS-K1	GIS-R2	GIS-R3	GIS-R4	GIS-R5	GIS-R6	GIS-R10	GIS-R20	GIS-R40
	PCI compliant firewall: protects your business computers from data theft	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Virus and Trojan blocking which eliminates network performance problems	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Block illegal P2P downloads to avoid Internet service disconnection lawsuits	✓		✓	✓	✓	✓	✓	✓	✓
	Block websites so hotels can prevent loss of income such as pay-per-view	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Track individual network usage and ban / restore abusive users	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Increase reliability with multi-WAN load balance and fail-over					✓		✓	✓	✓

## Billing

Billing		GIS-K1	GIS-R2	GIS-R3	GIS-R4	GIS-R5	GIS-R6	GIS-R10	GIS-R20	GIS-R40
	Hotspot credit card billing via PayPal with no Guest Internet commission to pay	✓		✓	✓	✓	✓	✓	✓	✓
	Credit card charge reporting via spreadsheet download and email announcement	✓		✓	✓	✓	✓	✓	✓	✓
	Subscription service via a custom website that interfaces with the API	✓	✓	✓	✓	✓	✓	✓	✓	✓

## Benefits

Benefits		GIS-K1	GIS-R2	GIS-R3	GIS-R4	GIS-R5	GIS-R6	GIS-R10	GIS-R20	GIS-R40
	Setup wizard: plug and play, very easy to install and operate	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Free lifetime firmware upgrades for all models	✓	✓	✓	✓	✓	✓	✓	✓	✓
	1-year gateway product warranty for defects of manufacture	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Free technical support with a knowledgeable engineer via the trouble ticket system	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Integration with property management systems and point of sale terminals	✓	✓	✓	✓	✓	✓	✓	✓	✓
	System expansion peripherals: access code Ethernet ticket printer	✓	✓	✓	✓	✓	✓	✓	✓	✓

All Guest Internet products include a feature for Social WiFi login.

### Hotspot login via social media account: Social WiFi




Social WiFi permits the Hotspot user to log onto the network using his or her social media account (Facebook).

When the user gives authorization, the Hotspot owner can download the users social media profile and save via email. The user is also given the opportunity to 'like' the Hotspot owners social media web page.

The user can bypass the social media request and begin using the Internet if desired. The terms and conditions of social media usage do not permit the Hotspot owner to oblige the user to login using his or her social media account in order to get Internet access.



## Social WiFi

Social WiFi Hotspot		GIS-K1	GIS-R2	GIS-R3	GIS-R4	GIS-R5	GIS-R6	GIS-R10	GIS-R20	GIS-R40
	Social media login using the customers Facebook account	✓	✓	✓	✓	✓	✓	✓	✓	✓
	With user authorization, fetch the user profile and save via email	✓	✓	✓	✓	✓	✓	✓	✓	✓
	User opportunity to 'like' the hotspot owners Facebook web page	✓	✓	✓	✓	✓	✓	✓	✓	✓

## Integrated Solution

Guest Internet is committed to providing customers with an integrated product solution and we work with partners to achieve this goal.

Partners provide us with value-added channels and with additional functionality that we don't provide. Currently we have four functionality partners.

**SMTP2go:** Additional SMTP services for the gateway mail server

**OpenDNS:** Content filtering using their DNS service

**DynDNS:** Remote access service when the gateway network has a dynamic IP

**PayPal:** Payment services for the credit card billing feature

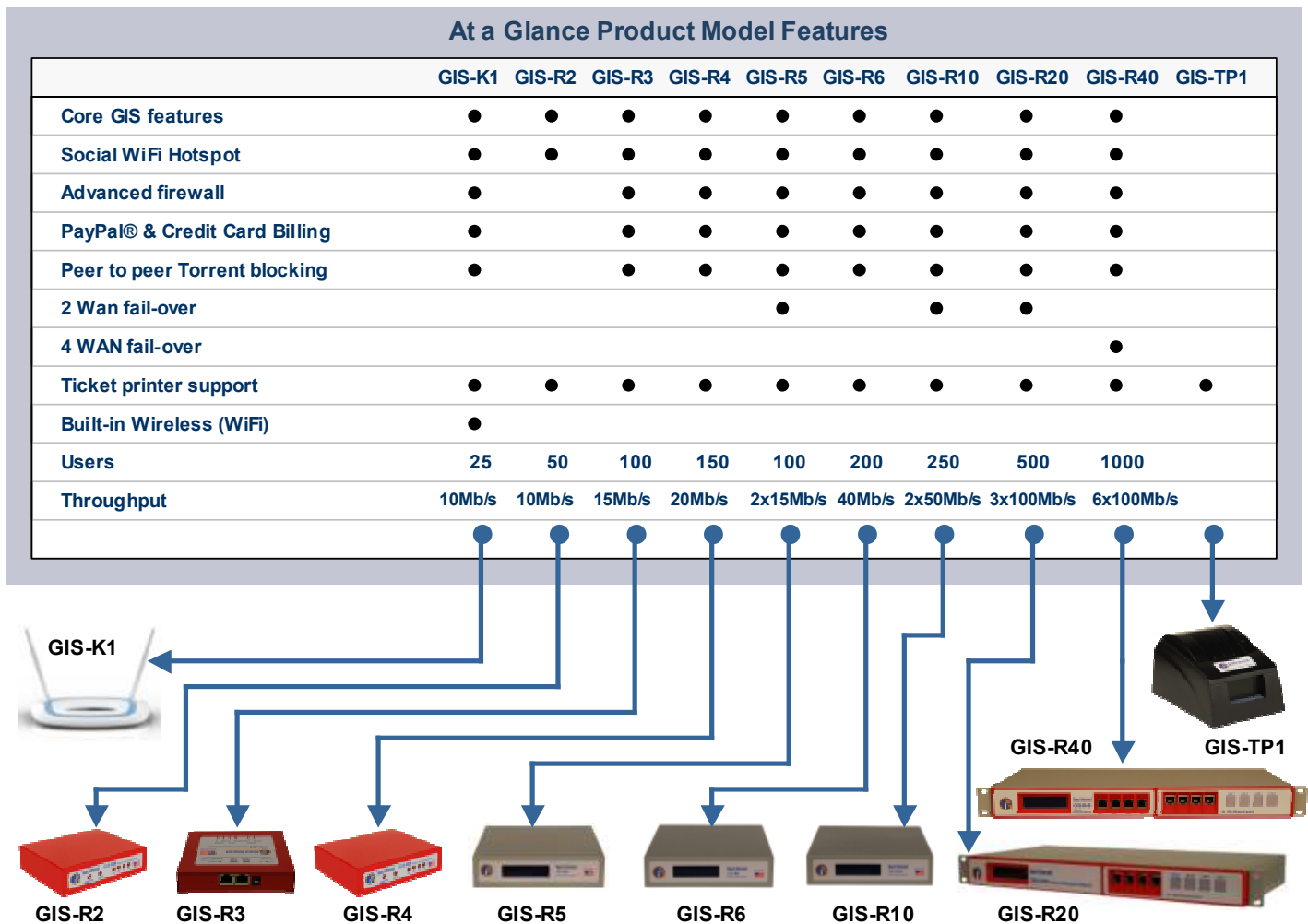
### 3: PRODUCT INFORMATION

#### Current Products

The Guest Internet product range extends performance from 25 users who can access the Internet concurrently, up to 500 concurrent users.

The product range includes two wireless products suitable for installation in coffee bars and small restaurants, for 25 and 50 users, and is being expanded from 10 to 1000 users. The range also includes seven gateway models for 50 to 1000 users. The gateway models are installed together with wireless access points and all compatible with products from all manufacturers. Finally the product lineup includes an access code ticket printer then can be connected to any of the gateway models.

The current product lineup is shown in the figure below:



Guest Internet constantly incorporates the latest technology advances into the range of gateway products. For this reason product specifications will change from time to time, ensuring that you get the best performance for your budget.

Firmware upgrades are always free for the lifetime of the product.



## Your Guest Internet Gateway Product Contents

Your Guest Internet gateway product contains several components that have to be installed and connected to make the system work. Your product package contains the following components.

- Quick start guide (Please read this document before operating your GIS product)
- Gateway unit
- Ethernet cable
- Power supply



When you receive your Guest Internet product, first verify that you received the items listed above.

If one of these items is missing then please inform our customer support immediately; contact information is provided on our website.

This manual is downloaded from our Web site to ensure that you always get the latest version. See the manual download URL on the rapid start guide card or copy this link:

**<http://www.guest-internet.com/manual>**

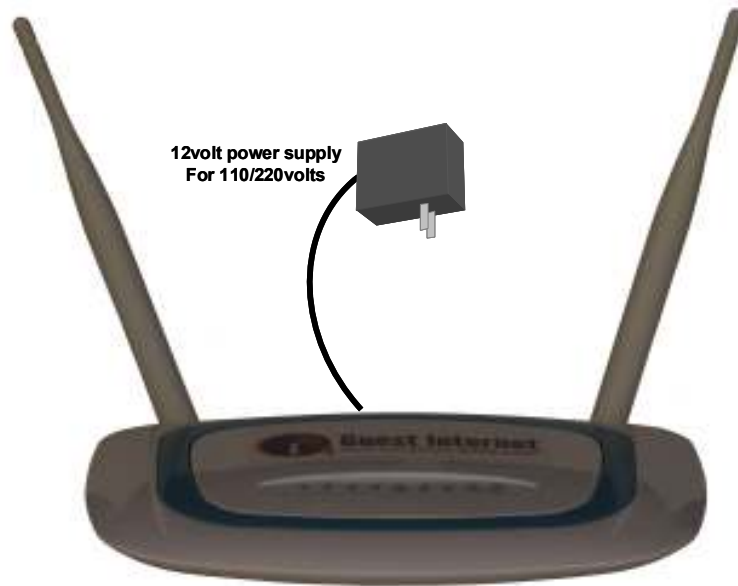
## GIS-K1 Gateway

The GIS-K1 is a wireless hotspot gateway for up to 25 concurrent users; this means that the unit can have wired computers connected directly to it (Internet kiosks, business center computers, etc), and can have wireless access points connected to it. Each wireless access point can provide a wireless, or WiFi connection for laptop computer users who are within range of the wireless transmission. The GIS-K1 has all the features of the GIS-R4, including social media login, peer to peer (P2P) blocking and credit card billing, for up to 25 users. The GIS-K1 gateway product is shown below.

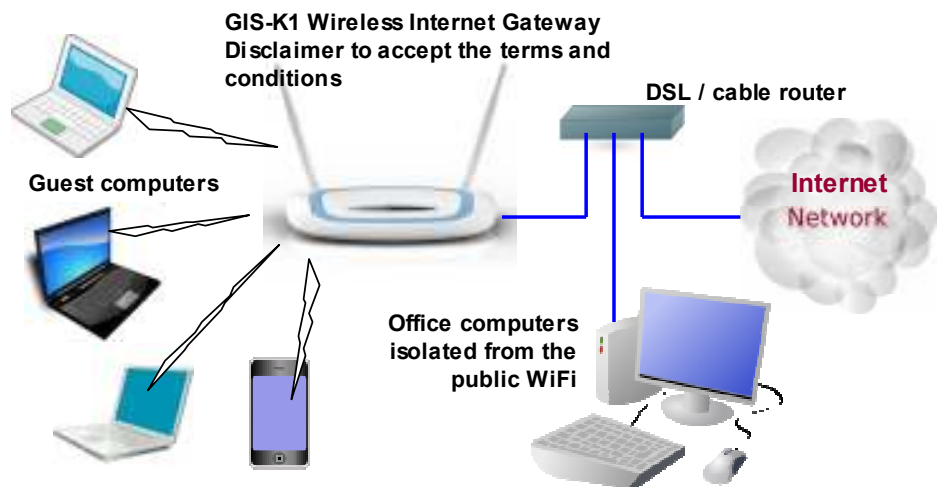
**GIS-K1: The wireless gateway has five Ethernet connectors. One is for the Internet or WAN, and is connected to the DSL router. The other connectors are the LAN ports. These ports can have any network device or computer connected.**

**The LAN ports can also be optionally configured to extend the hotspot network by adding wireless access points.**

**If more LAN ports are required then a switch can be connected to one of the LAN ports.**



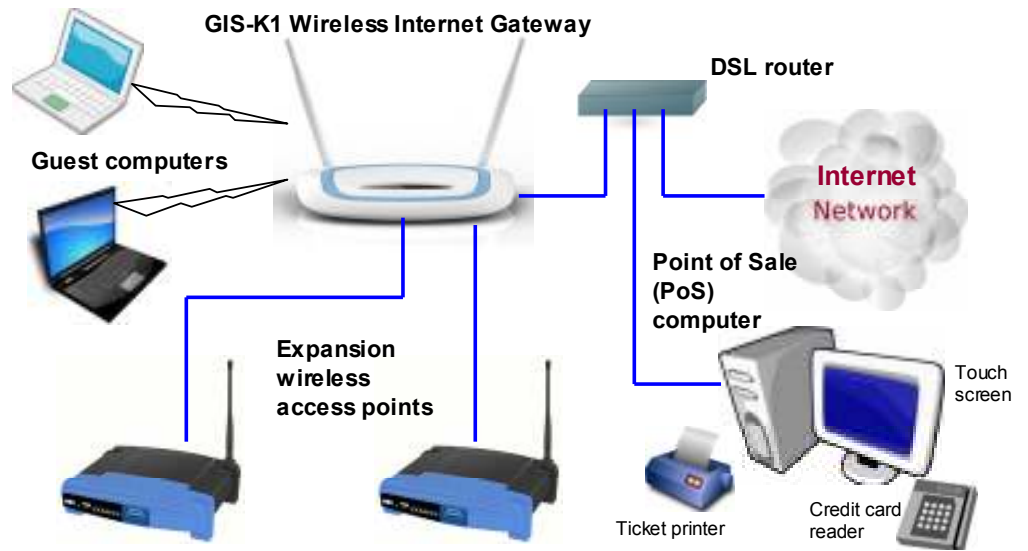
**The GIS-K1 is shown with guest laptop computers, tablets and smart-phones connecting wirelessly**



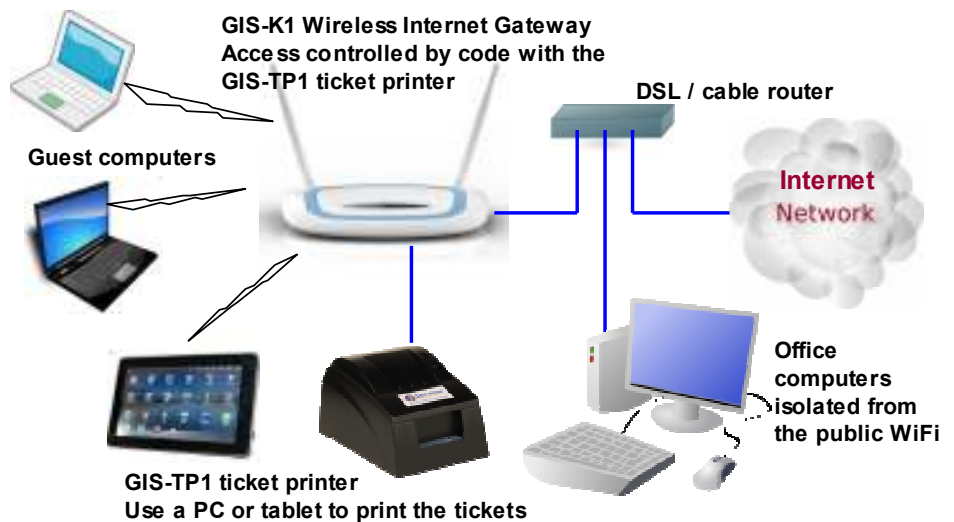
The internal wireless access point can be expanded by connecting additional wireless access points to the LAN port via a switch.



The GIS-K1 is shown with additional wireless access points connected to the LAN ports that will extend the wireless hot spot network. Each LAN port is firewalled to prevent public hotspot users hacking into business computers that are connected to the same DSL/cable circuit



The GIS-K1 is shown with the GIS-TP1 ticket printer what will permit printing of access codes. A tablet computer connects to the GIS-K1 via wireless to control ticket printing





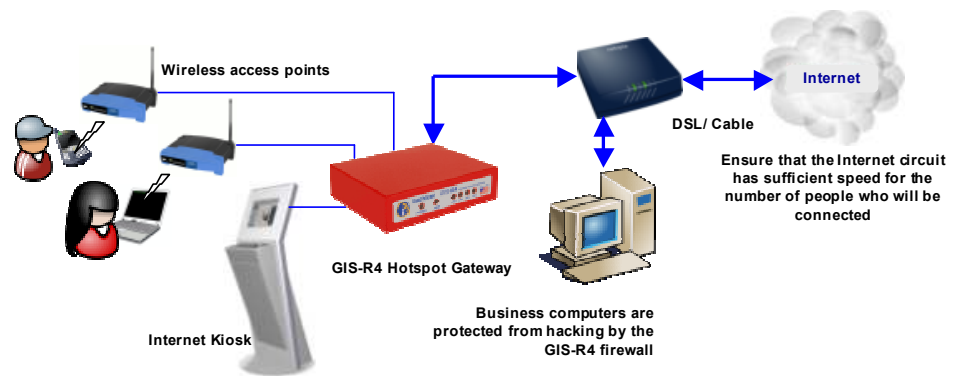
## GIS-R2 Gateway

The GIS-R2 is a hotspot gateway for up to 50 concurrent users; this means that the unit can have wired computers connected directly to it (Internet kiosks, business center computers, etc), and can have wireless access points connected to it. Each wireless access point can provide a wireless, or WiFi connection for laptop computer users who are within range of the wireless transmission. WiFi enabled devices include notebook computers, MAC™ computers, iPhones™, iPods™, and Blackberries™. The GIS-R2 has many of the features of other GIS gateway products, however credit card billing and peer to peer (Torrent) blocking are not included. The GIS-R2 gateway product is shown below.

**The GIS-R2 gateway has five Ethernet connectors. One is labeled Internet and is connected to the DSL/cable/T1 router. The other four connectors are labeled LAN to LAN4. A computer can be connected to the LAN ports directly or via a wireless access point. If more LAN ports are required then a switch can be connected. There is also a power plug for the 12 volt connector, and a reset button to reset the unit to factory defaults.**



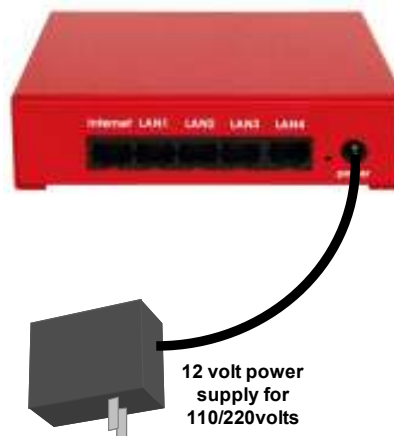
**The GIS-R2 is shown with wireless access points connected via a switch to the LAN port. Business computers connected to the same DSL circuit as the WAN port are protected from hacking by the PCI DSS compliant firewall.**



### GIS-R2 power supply and connections

#### 12 volt power supply

Use only the power supply provided to avoid damage





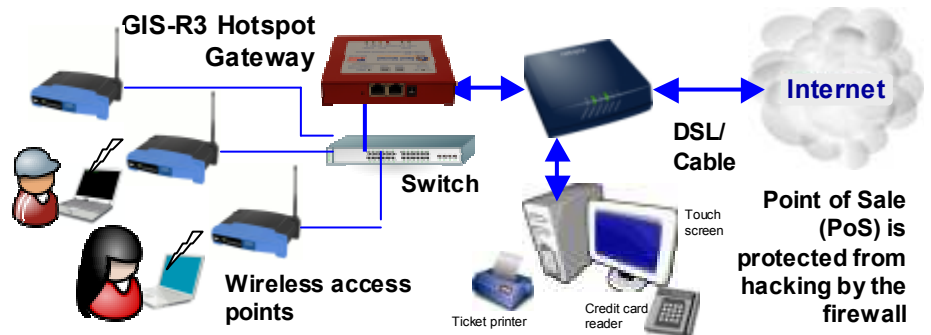
## GIS-R3 Gateway

The GIS-R3 is a hotspot gateway for up to 100 concurrent users; this means that the unit can have wired computers connected directly to it (Internet kiosks, business center computers, etc), and can have wireless access points connected to it. Each wireless access point can provide a wireless, or WiFi connection for laptop computer users who are within range of the wireless transmission. WiFi enabled devices include notebook computers, MAC™ computers, iPhones™, iPods™, and Blackberries™. The GIS-R3 gateway product is shown below.

The GIS-R3 gateway has two Ethernet connectors. One is labeled Internet and is connected to the DSL/cable/T1 router. The second connector is labeled LAN. A switch can be connected to the LAN port to permit several wireless access points to be connected. There is also a power plug for the 12 volt connector, and a reset button to reset the unit to factory defaults.



The GIS-R3 is shown with wireless access points connected via a switch to the LAN port. Business computers connected to the same DSL circuit as the WAN port are protected from hacking by the PCI DSS compliant firewall.



### GIS-R3 power supply and connections

#### 12 volt power supply

Use only the power supply provided to avoid damage



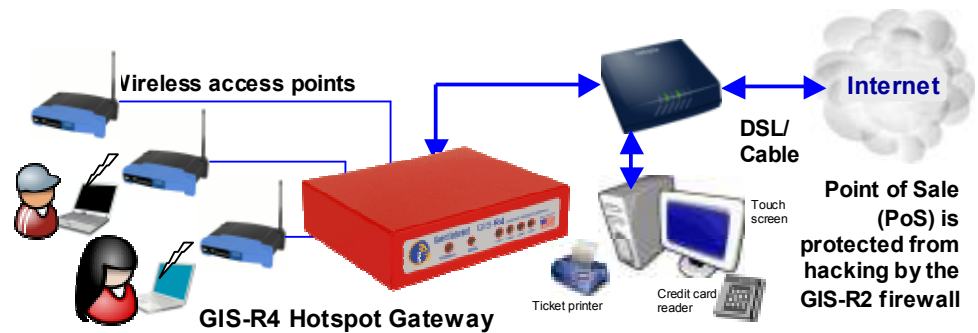
## GIS-R4 Gateway

The GIS-R4 is a hotspot gateway for up to 100 concurrent users; this means that the unit can have wired computers connected directly to it (Internet kiosks, business center computers, etc), and can have wireless access points connected to it. Each wireless access point can provide a wireless, or WiFi connection for laptop computer users who are within range of the wireless transmission. WiFi enabled devices include notebook computers, MAC™ computers, iPhones™, iPods™, and Blackberries™. The GIS-R4 gateway product is shown below.

The GIS-R4 gateway has five Ethernet connectors. One is labeled Internet and is connected to the DSL/cable/T1 router. The other four connectors are labeled LAN to LAN4. A computer can be connected to the LAN ports directly or via a wireless access point. If more LAN ports are required then a switch can be connected. There is also a power plug for the 12 volt connector, and a reset button to reset the unit to factory defaults.



The GIS-R4 is shown with wireless access points connected via a switch to the LAN port. Business computers connected to the same DSL circuit as the WAN port are protected from hacking by the PCI DSS compliant firewall.



### GIS-R4 power supply and connections

#### 12 volt power supply

Use only the power supply provided to avoid damage





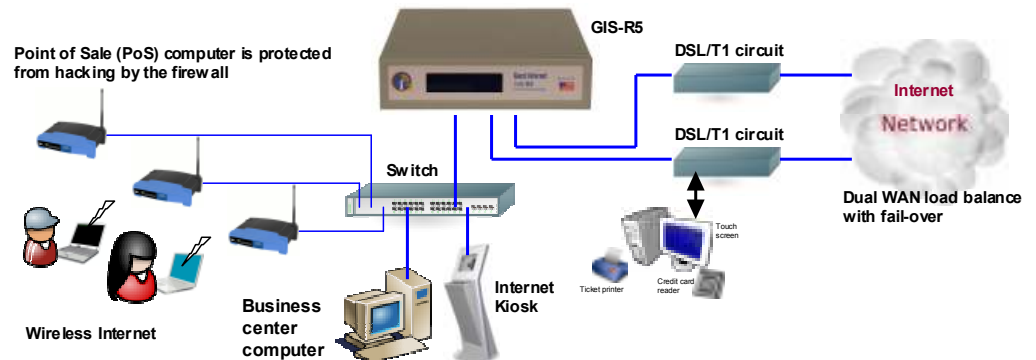
## GIS-R5 Gateway

The GIS-R5 is a dual-WAN hotspot gateway for up to 100 concurrent users; this means that the unit can have wired computers connected directly to it (Internet kiosks, business center computers, etc), and can have wireless access points connected to it. Each wireless access point can provide a wireless, or WiFi connection for laptop computer users who are within range of the wireless transmission. WiFi enabled devices include notebook computers, MAC™ computers, iPhones™, iPods™, and Blackberries™. The GIS-R5 gateway product is shown below.

The GIS-R5 gateway has five Ethernet connectors. Two are labeled WAN1 and WAN 2 for connection to two DSL/cable/T1 routers. Three connectors are labeled LAN1, LAN2 and LAN3. Any network device or computer can be connected to these ports. If more LAN ports are required then a switch can be connected.



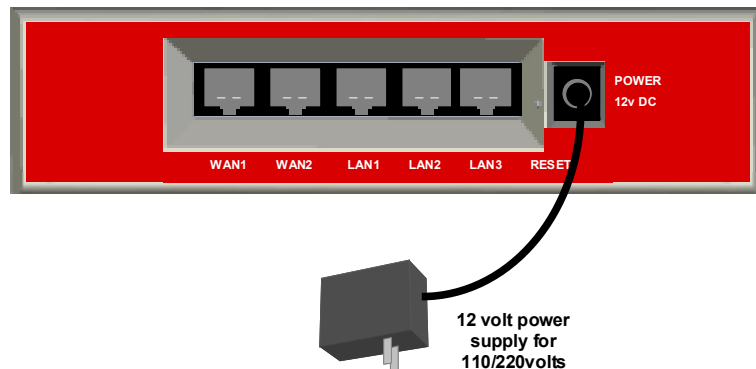
The GIS-R5 is shown with wireless access points, a business center computer and a kiosk are connected to a LAN port via a switch. Business computers connected to the same DSL circuit as the WAN port are protected from hacking by the PCI DSS compliant firewall.



### GIS-R5 power supply and connections

#### 12 volt power supply

Use only the power supply provided to avoid damage





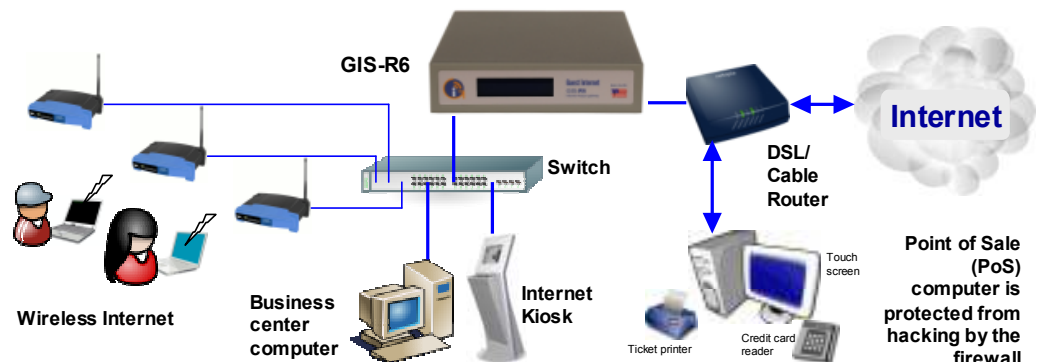
## GIS-R6 Gateway

The GIS-R6 is a hotspot gateway for up to 200 concurrent users; this means that the unit can have wired computers connected directly to it (Internet kiosks, business center computers, etc), and can have wireless access points connected to it. Each wireless access point can provide a wireless, or WiFi connection for laptop computer users who are within range of the wireless transmission. WiFi enabled devices include notebook computers, MAC™ computers, iPhones™, iPods™, and Blackberries™. The GIS-R6+ gateway product is shown below.

The GIS-R6 gateway has two Ethernet connectors. One is labeled Internet and WAN, and is connected to the DSL/cable/T1 router. The connector labeled LAN is connected to computers wireless access points via a switch. If more LAN ports are required then the switch can be expanded.



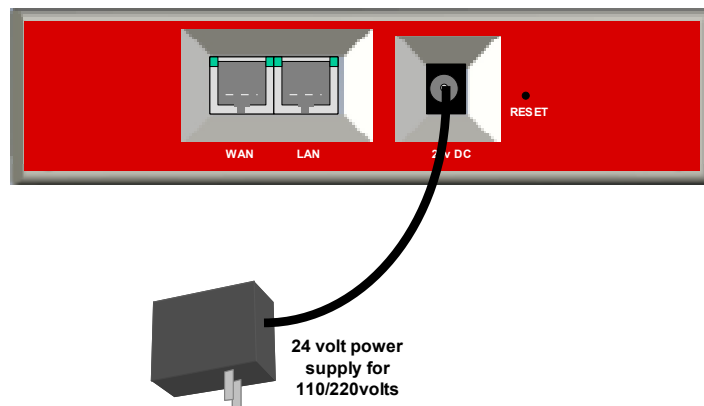
The GIS-R+ is shown with three wireless access points connected via a switch to the LAN ports. Business computers connected to the same DSL circuit as the WAN port are protected from hacking by the PCI DSS compliant firewall.



### GIS-R6 power supply and connections

#### 24 volt power supply

Use only the power supply provided to avoid damage





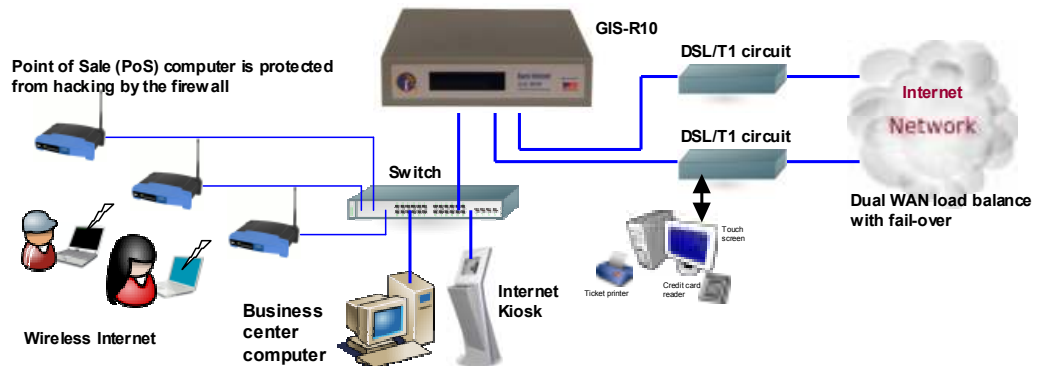
## GIS-R10 Gateway

The GIS-R10 is a hotspot gateway for up to 250 concurrent users; this means that the unit can have wired computers connected directly to it (Internet kiosks, business center computers, etc), and can have wireless access points connected to it. Each wireless access point can provide a wireless, or WiFi connection for laptop computer users who are within range of the wireless transmission. WiFi enabled devices include notebook computers, MAC™ computers, iPhones™, iPods™, and Blackberrys™. The GIS-R10 gateway product is shown below.

**The GIS-R10 gateway has three Ethernet connectors. Two are labeled WAN1 and WAN 2 for connection to two DSL/cable/T1 routers. The connector labeled LAN1 can have computer can be connected directly or via a wireless access point. If more LAN ports are required then a switch can be connected for a maximum of 250 ports.**



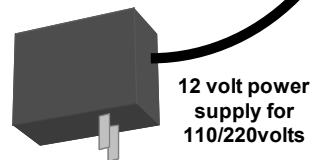
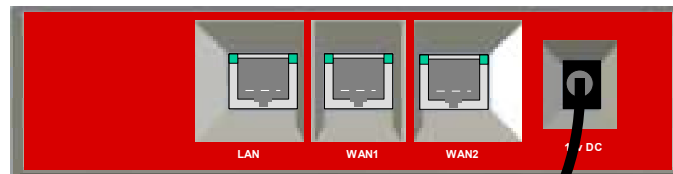
**The GIS-R10 is shown with two wireless access points connected to the LAN port via a switch. The two WAN ports are DSL and Cable circuits. Business computers connected to the same DSL circuit as the WAN ports are protected from hacking by the PCI DSS compliant firewall.**



### GIS-R10 power supply and connections

#### 12 volt power supply

Use only the power supply provided to avoid damage





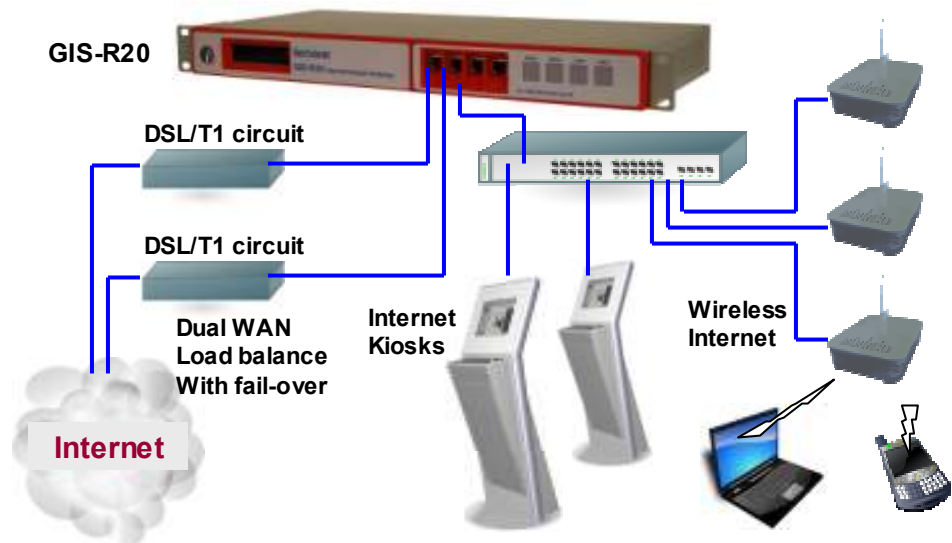
## GIS-R20 Gateway

The GIS-R20 is a hotspot gateway for up to 500 concurrent users; this means that the unit can have wired computers connected directly to it (Internet kiosks, business center computers, etc), and can have wireless access points connected to it. Each wireless access point can provide a wireless, or WiFi connection for laptop computer users who are within range of the wireless transmission. WiFi enabled devices include notebook computers, MAC™ computers, iPhones™, iPods™, and Blackberries™. The GIS-R20 gateway product is shown below.

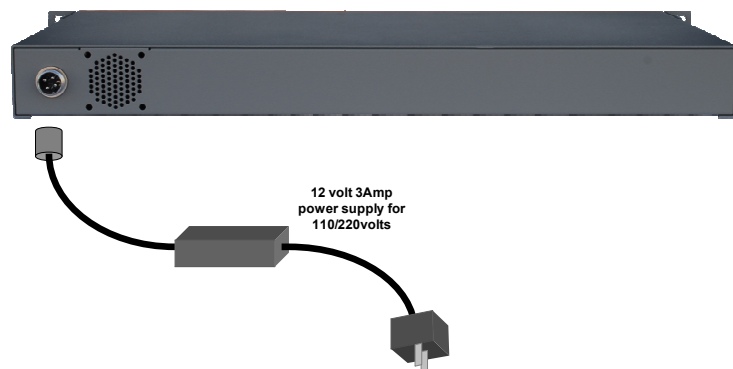
The GIS-R20 gateway has four Gbit Ethernet connectors. Two ports are configured for WAN connections. Two ports are configured for LAN connections with independent and isolated subnets. Any network device or computer can be connected to the LAN ports. If more LAN ports are required then a switch can be connected.



The GIS-R20 is shown with wireless access points and Internet kiosks connected via a switch to one of the LAN ports. The two WAN ports provide load balancing and fail-over for redundant operation. Business computers connected to the same DSL circuit as the WAN ports are protected from hacking by the PCI DSS compliant firewall.



**GIS-R20 power connector**  
**12 volt supply**  
 4-pin power connector  
 12 volts, 3amps  
 Use only the power supply provided to avoid damage



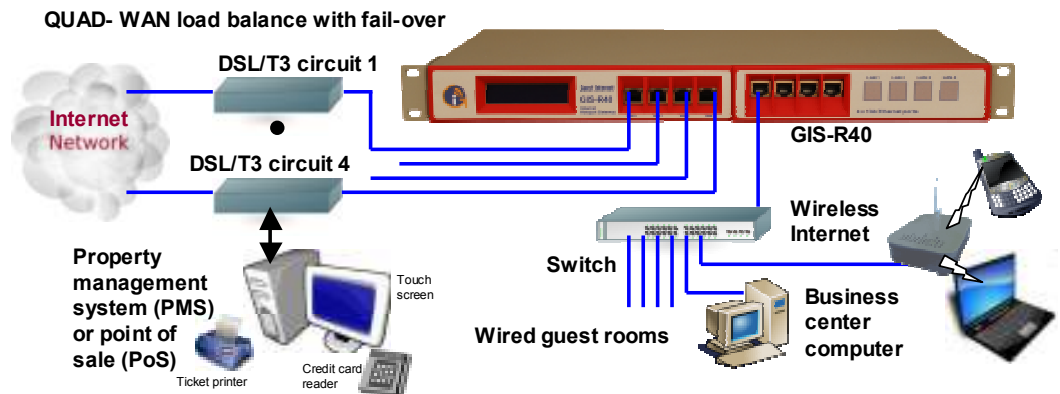


## GIS-R40 Gateway

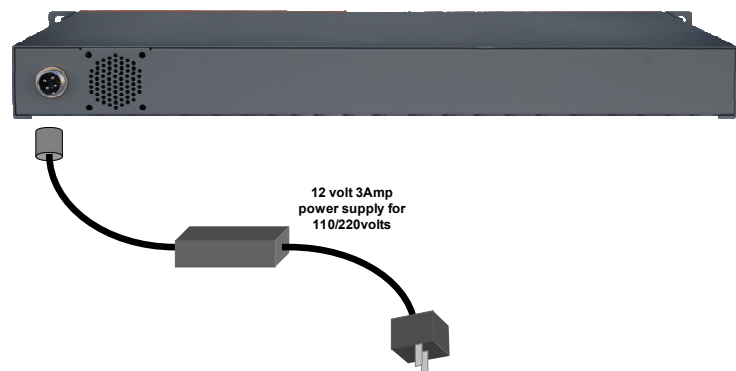
The GIS-R40 is a dual-core hotspot gateway for up to 1000 concurrent users; this means that the unit can have wired computers connected directly to it (Internet kiosks, business center computers, etc), and can have wireless access points connected to it. Each wireless access point can provide a wireless, or WiFi connection for laptop computer users who are within range of the wireless transmission. WiFi enabled devices include notebook computers, MAC™ computers, iPhones™, iPods™, and Blackberries™. The GIS-R40 gateway product is shown below.

**The GIS-R40 gateway has eight Ethernet connectors, Four connectors are Gbit and for connectors are 100Mb. Up to 6 ports are configured for WAN connections. Two or more ports are configured for LAN connections with independent and isolated subnets. Any network device or computer can be connected to the LAN ports. If more LAN ports are required then a switch can be connected.**

**The GIS-R40 is shown with wireless access points and Internet kiosks connected via a switch to one of the LAN ports. The two WAN ports provide load balancing and fail-over for redundant operation. Business computers connected to the same DSL circuit as the WAN ports are protected from hacking by the PCI DSS compliant firewall.**



**GIS-R40 power connector**  
**12 volt supply**  
**4-pin power connector**  
**12 volts, 3amps**  
**Use only the power supply provided to avoid damage**





## GIS-TP1 Ticket Printer

Many Internet WiFi Hotspots are configured so that the user has to type an access code to be connected to the Internet. This procedure prevents unauthorized users from getting Internet access. Guest Internet gateways have a page to generate access codes which can be downloaded to a spreadsheet and printed on labels. GIS gateways also have an application program interface (API) that allows point of sale (PoS) systems to request an access code and print the code on the PoS ticket printer. The GIS-TP1 provides an alternative to print access codes on demand when the user requests a code. This greatly simplifies the management of access codes as it is no longer necessary to generate a large number of codes and then print codes using a computer. A hotel reception desk or concierge can now print access codes for guests. A coffee bar can print access codes for guests when purchases are made. Codes are printed using the touch screen of a tablet computer. This can be a low cost Android tablet with a 7inch display screen, or an Apple iPad tablet. Ten access codes can be pre-configured and appear as buttons on the screen of the tablet computer.

Like all Guest Internet gateway products, the ticket printer is very easy to install and operate. The ticket printer should be connected to a LAN port of the GIS gateway using a switch. Wireless access points will also be connected to the GIS gateway using the same switch. Next, the ticket printer is configured using the GIS administrator page to select up to ten access code durations as ticket options. A new login password is also created for the tablet computer login. Finally, the tablet computer wireless should be connected to the GIS gateway via the wireless access point. Open the browser and use the ticket printer login. The ticket select buttons are then displayed on the screen.

### GIS-TP1 access code ticket printer

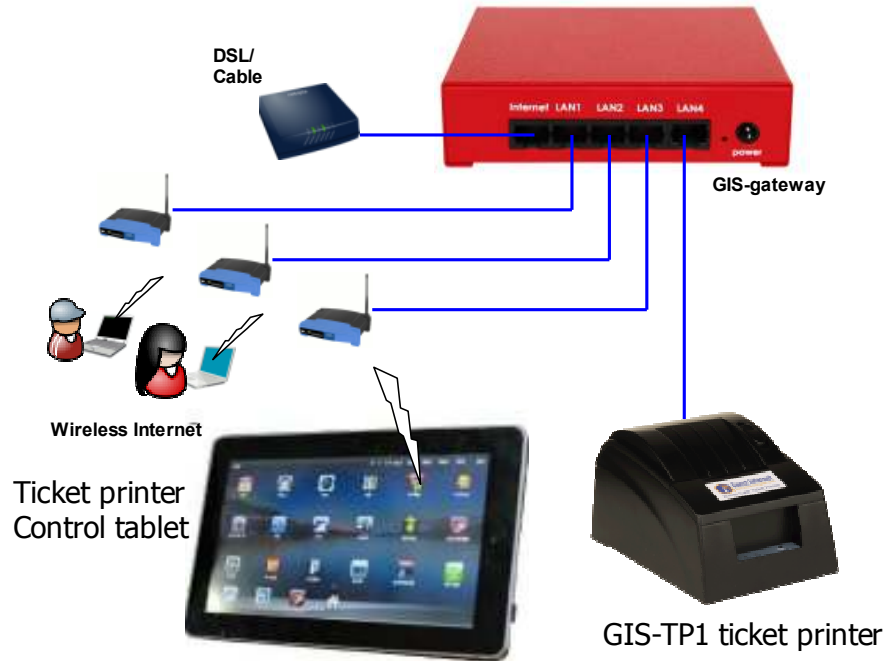


The GIS-TP1 ticket printer uses 58mm thermal paper that can be obtained from any office supplies store. 58mm thermal paper is used by point of sale thermal printers.

The GIS-TP1 ticket printer has an Ethernet connection that must be connected to a LAN port of the gateway, either directly or via a switch. The GIS-TP1 cannot be connected to the WAN port of the gateway.

The GIS-TP1 is connected to the gateway as shown in the figure below. A separate tablet computer is required to control ticket printing.

### GIS-TP1 network connection



### GIS-TP1 power connector

**12 volt 3amps power supply**

**Use only the power supply provided to avoid damage**

**Connect the Ethernet data cable as shown**

The power and data connections of the GIS-TP1 are underneath the unit to the rear.

Use only the 12 volt, 3 amp power supply provided with the unit.

A power on/off switch is located at the rear of the printer.

**Power Ethernet**



The GIS-TP1 is shipped together with the following accessories

- Power supply, 12 volts, 3Amps
- Ethernet cable
- Quick start guide

## 4: PREPARING YOUR GATEWAY FOR USE

### Installing the Gateway Product in a Computer Network

When the GIS-gateway has been configured it can be installed in the business network. Configuration changes may be necessary for the GIS-gateway to provide all the desired features required for the business network.

Several different network configurations are possible when installing the GIS- gateway. It is important to recognize that restrictions are placed on the network design if the network has any computer point-of-sale terminal that is used to process credit card information.

The **Payment Card Industry Data Security Standard (PCI DSS)** requires all businesses to ensure that credit card information is protected, by preventing unauthorized access via the network, using one or more firewall products.

Network designs have two points of entry for hackers who try to steal credit card information from point of sale computers. The first point of entry is through the Internet connection. The outbound Internet connection is required to process credit card information. However the inbound direction has to be blocked to prevent hackers using the internet to access the point of sale computers.

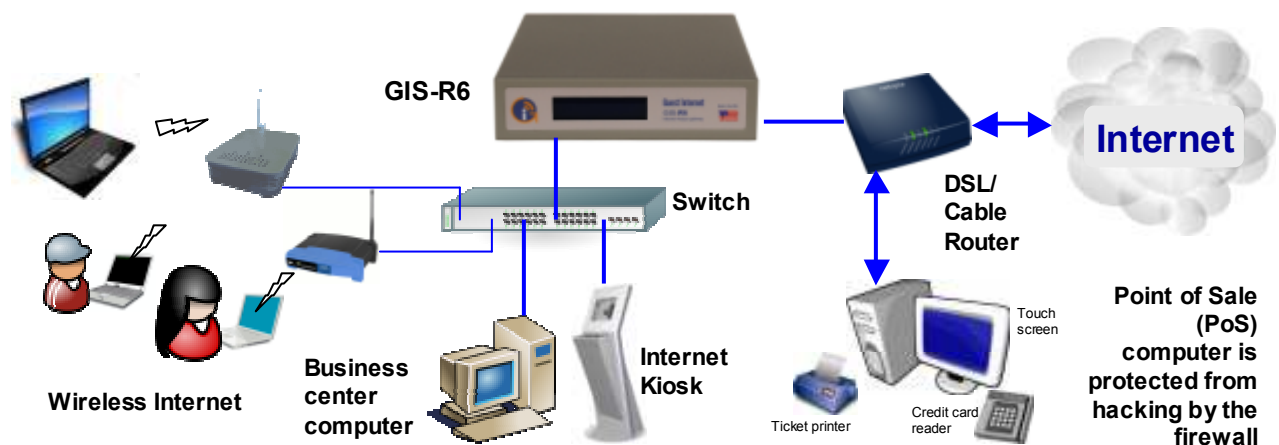
The second point of entry is through any wireless access point that is provided for guests and visitors to get Internet access. The PCI DSS standards recommend that two separate Internet circuits should be used: one for the point of sale system, and one for the public guest Internet network.

One Internet circuit can be used when firewall devices are installed to protect the point of sale system from attack. A firewall however is only as good as the person who configures the firewall. It is necessary to take great care when writing the firewall rules to ensure that no path exists for a possible attacker.

PCI DSS compliant network configurations are shown in the following figures. Additional information about PCI DSS recommendations can be found at this URL.

[https://www.pcisecuritystandards.org/security\\_standards/pci\\_dss\\_download\\_agreement.html](https://www.pcisecuritystandards.org/security_standards/pci_dss_download_agreement.html)

The gateway connected to a DSL router to provide Internet access for guests





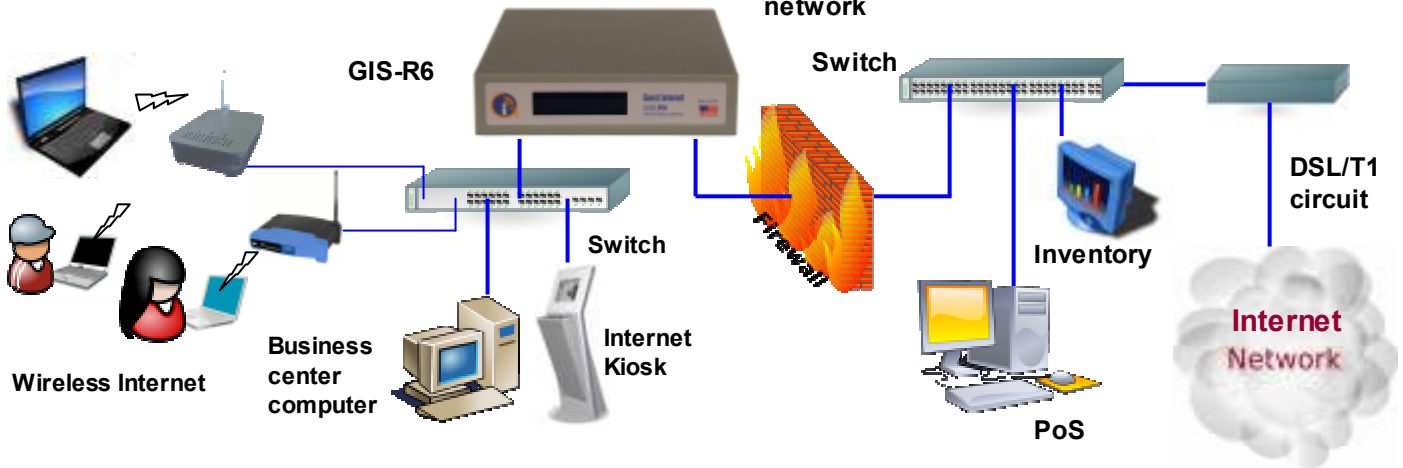
The next figure shows the GIS-gateway connected to a business network that has an Internet connection via DSL or T1. The GIS-gateway firewall blocks access of public network DMZ (de-militarized zone) users to the business network computers for PCI DSS compliance.

## Gateway Firewall Details

Public network (DMZ): wireless hotspot, kiosks, business center

Public user access is blocked to the business network that includes a point of sale terminal

Set private IP range 192.168.xx.xx 172.16.xx.xx or 10.xx.xx.xx to prevent access from the public network

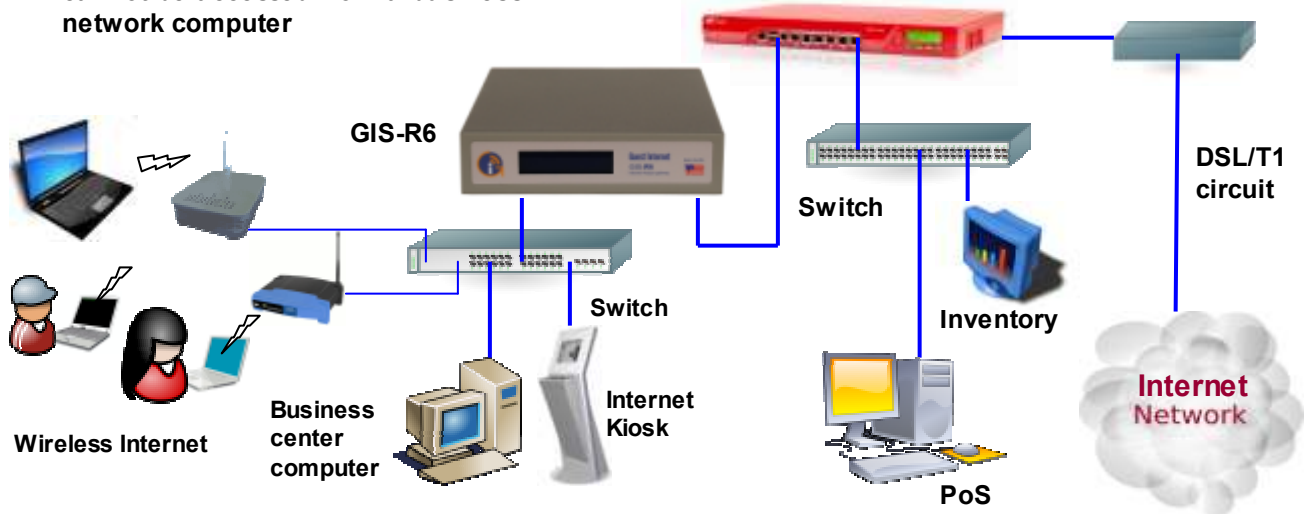


The next figure shows a business network with full PCI-DSS compliance: a single firewall isolates the business network and public network (DMZ). With this configuration it is possible for one of the business computers to generate and manage access codes using the GIS-gateway providing that the computer has been authorized to do so within the firewall.

## Gateway Connected via a Firewall

Public network (DMZ): The gateway cannot be accessed from a business network computer

Firewall: isolates the public and private networks. Protects the private network from attack via the Internet





The GIS K1+/K3 wireless gateway devices are configured differently to the GIS-R-series gateway devices. Configuration changes may be necessary for the GIS-K1+/K3 to provide all the desired features required for the business network.

Several different network configurations are possible when installing the GIS-K1+/K3. It is important to recognize that restrictions are placed on the network design if the network has any computer point-of-sale terminal that is used to process credit card information.

The **Payment Card Industry Data Security Standard (PCI DSS)** requires all businesses to ensure that credit card information is protected, by preventing unauthorized access via the network, using one or more firewall products.

Network designs have two points of entry for hackers who try to steal credit card information from point of sale computers. The first point of entry is through the Internet connection. The outbound Internet connection is required to process credit card information. However the inbound direction has to be blocked to prevent hackers using the internet to access the point of sale computers.

The second point of entry is through any wireless access point that is provided for guests and visitors to get Internet access. The PCI DSS standards recommend that two separate Internet circuits should be used: one for the point of sale system, and one for the public guest Internet network.

One Internet circuit can be used when firewall devices are installed to protect the point of sale system from attack. A firewall however is only as good as the person who configures the firewall. It is necessary to take great care when writing the firewall rules to ensure that no path exists for a possible attacker.

PCI DSS compliant network configurations are shown in the following figures. Additional information about PCI DSS recommendations can be found at this URL.

**[https://www.pcisecuritystandards.org/security\\_standards/pci\\_dss\\_download\\_agreement.html](https://www.pcisecuritystandards.org/security_standards/pci_dss_download_agreement.html)**

All GIS hotspot gateway products have identical PCI DSS compliant firewalls.

## Switching the Gateway Product on for the First Time

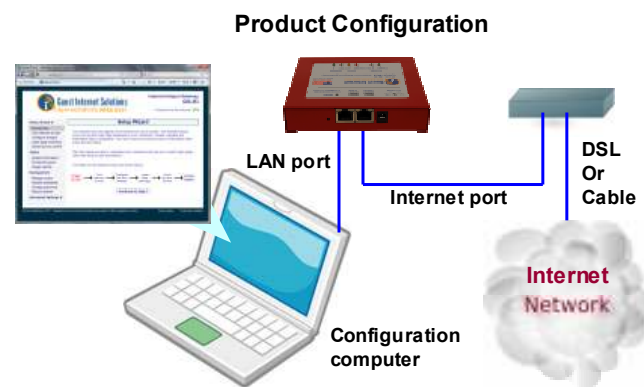
The GIS-gateway must be configured before it can be used. The product has a very easy to use Wizard which speeds through the configuration process. Configuration takes around five minutes.

The GIS-gateway must be connected as shown in the diagram at the bottom of this page. The INTERNET port must be connected to the Internet via the DSL router. The GIS-gateway cannot be configured without Internet access. The computer Ethernet cable is connected to any LAN port

When the GIS-gateway is connected as shown in the diagram the power supply should be connected. Check the power on LED is lit on the front of the enclosure, or the LCD display is lit on some models. The WAN link LED indicates that the Internet port is connected to the DSL router, on models with the LCD display a message indicated this connection.

Next switch on the computer. When the computer has booted up then open the browser. If the browser gives a message that the Internet is not available then check the Ethernet cable and connectors between the GIS-gateway LAN port and the computers Ethernet connector.

Connect your computer to the gateway product LAN port

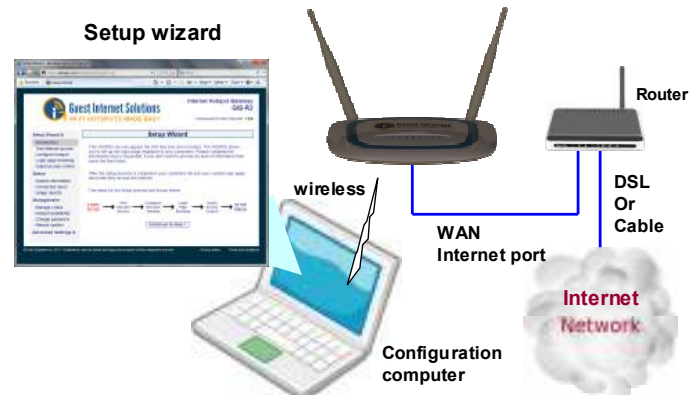


The GIS-K1 must be connected as shown in the diagram on the following page. The GIS-K1 INTERNET port must be connected to the Internet via the DSL/Cable/T1 router. The GIS-K1 cannot be configured without Internet access. The computer wireless network interface is connected to network name: **Hotspot**

When the GIS-K1 is connected as shown in the diagram the power supply should be connected. Check power on LED is lit above the enclosure. A LED indicates power is connected and a LED indicates that the Internet port is connected to the DSL router.

Next open the computer browser. If the browser gives a message that the Internet is not available then check the wireless connection between the GIS-K1 and the computer.

Connect your computer using the wireless interface. Look for the network name (SSID): **Hotspot** and connect



With the Guest Internet gateway connected as shown, proceed to the Wizard configuration process.





## Connecting Your Computer Browser to the Guest Internet Product

When your computer is connected to the GIS-gateway (previous section) then you can start the configuration and set up process using your computer browser. The set up process can be done with any type of browser.

When a browser opens it is usually directed to go to the home page. This is the page you always see when the browser opens.

When you open your browser your home page will change, instead of your usual home page you will see the Guest Internet setup wizard.

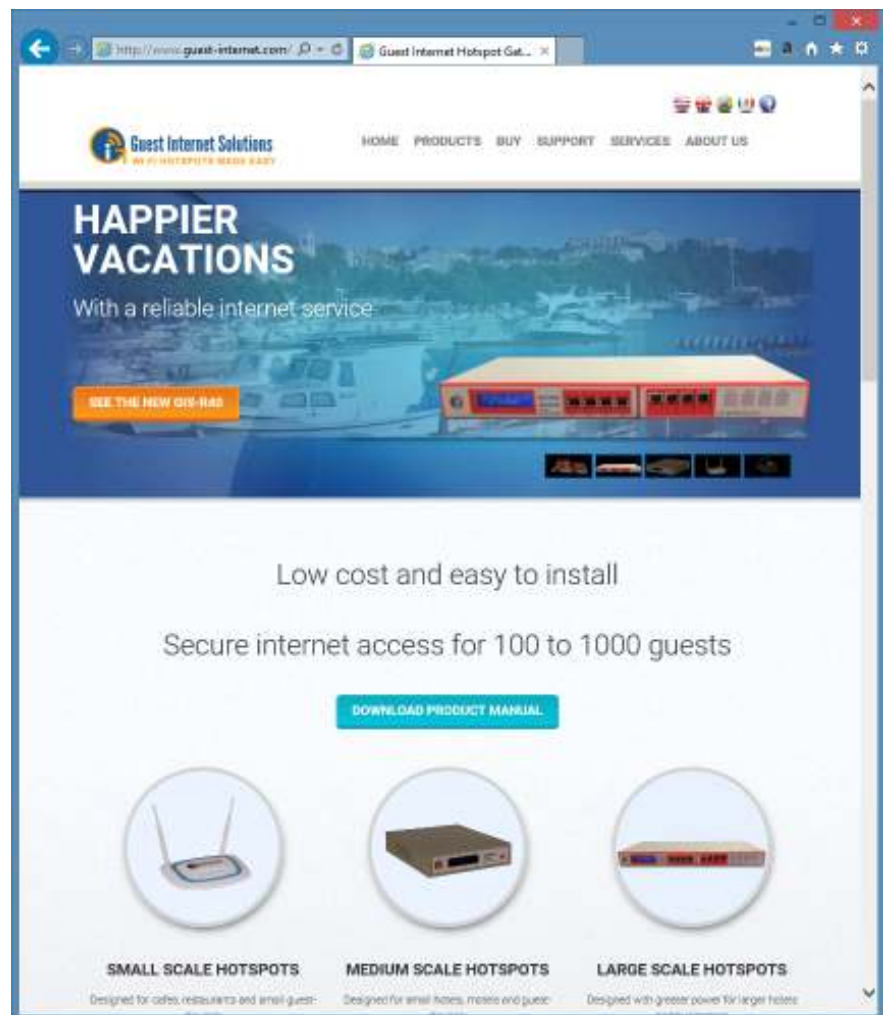
If you did not have a home page set in your browser you should type the following into the URL address line.

**<http://aplogin.com>**

The setup wizard will appear only the first time you power up the device. When the Guest Internet product has been configured then the configuration wizard is no longer shown. It is replaced by a login page, which was generated by the setup wizard.

**When the browser window opens it will go to the home page URL  
If the Setup Wizard is not displayed then type the website name:**

**[www.aplogin.com](http://www.aplogin.com)**







## The Quick Start Wizard: Get Your Gateway Working Quickly

The first time that you connect to your Guest Internet gateway product you should see the page shown below displayed in your Internet browser window.

The screen shows that there are five steps to complete the setup process. Each step is a page that requires some information to be typed in or an option selected.

Please read through this manual first before setting up your Guest Internet product.



The purpose of the setup wizard is twofold

- (a) Verify that the gateway is connecting to the Internet
- (b) Configure the login page that your guests will see when they try to connect to the Internet

During the wizard set up process you will be requested to enter information about your business that will be shown to guests on the login page. It is always good to present your website address, email address and telephone number for guests to note or save on their computers. All information is optional: if you don't type it in it will not be shown on the login screen.

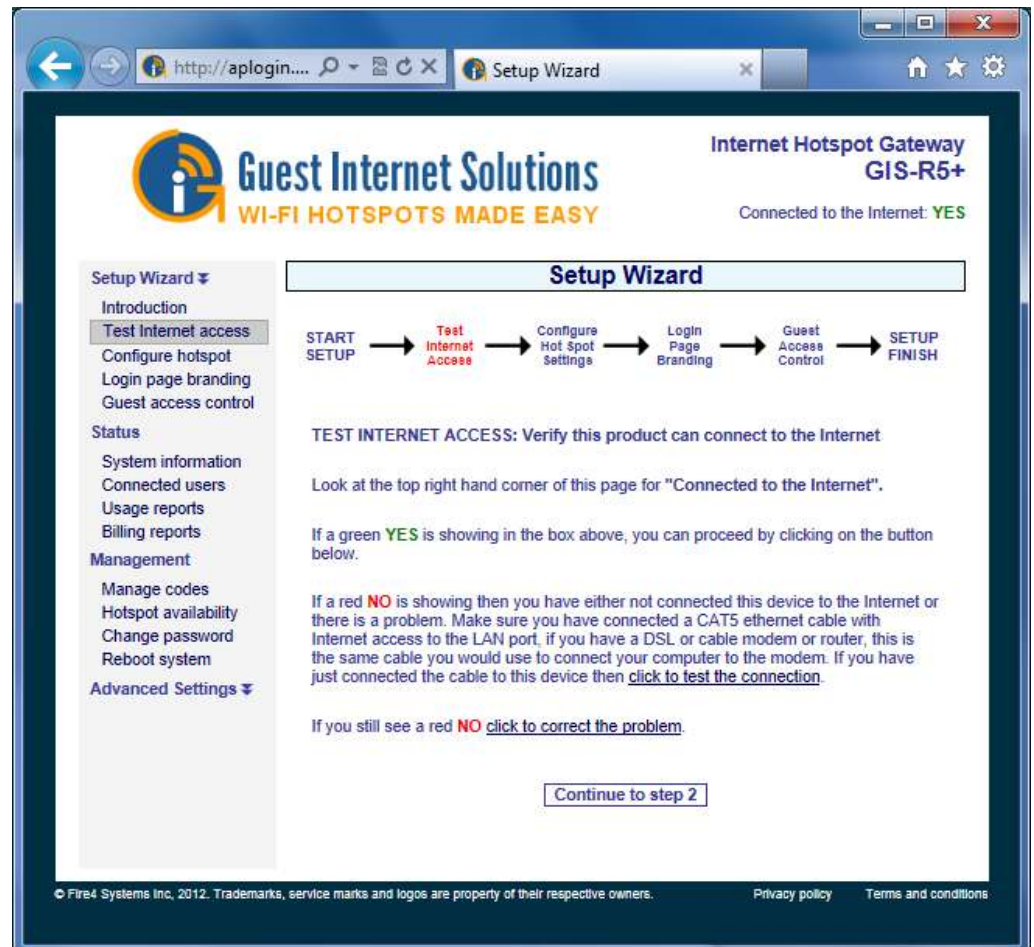
In addition to your business information you can also type in an advertising message. The message could tell guests about a special offer, or provide information essential for guests. You can also log in at any time to change the advertising message.



## Check the Internet Connection

The TEST INTERNET ACCESS setup page verifies that your Guest Internet gateway product is connected to the Internet. The setup process cannot be completed unless the product is connected to the Internet.

Look on the top right hand corner of the browser window. You will see a green YES or a red NO. If you have a green YES then your product is connected to the Internet and you can proceed to the next page by clicking on the button 'Continue to Step 2'.



If you see a red NO then you have a connection problem.

First verify that your DSL modem provides a good Internet connection by connecting a computer to the DSL modem using an Ethernet cable.

Verify that the Guest Internet product is connected to the DSL router (check that the blue LED is lit) and then click on 'click to test the internet connection'.

If the Internet status still shows a red NO then click on 'click to correct this problem'.

Verify that your DSL modem is a 'DHCP server'. You may need help from an IT or network person to answer this question. Click on the link 'click to attempt an IP address' shown on the following page.

You may have a shared T1 service in which case you will have to configure your Guest Internet product with a 'fixed IP address'. You can click on **Advanced Settings** and then click on **Network Interfaces** to set a fixed IP address. This procedure is explained later in this manual. Your T1 service provider will tell you what IP address should be configured.



Internet Hotspot Gateway  
GIS-R5+  
Connected to the Internet: YES

### Setup Wizard

START SETUP → **Test Internet Access** → Configure Hot Spot Settings → Login Page Branding → Guest Access Control → SETUP FINISH

**TEST INTERNET ACCESS:** Verify this product can connect to the Internet

Look at the top right hand corner of this page for "Connected to the Internet".

If a green YES is showing in the box above, you can proceed by clicking on the button below.

If a red NO is showing then you have either not connected this device to the Internet or there is a problem. Make sure you have connected a CAT5 ethernet cable with Internet access to the LAN port, if you have a DSL or cable modem or router, this is the same cable you would use to connect your computer to the modem. If you have just connected the cable to this device then [click to test the connection](#).

If you still see a red NO [click to correct the problem](#).

You may need technical help for this step from your network or DSL provider.

This product is set as a "DHCP client". Check with your DSL or network provider to confirm that the router you have is a "DHCP server".

If your provider tells you that devices have to be configured with a "fixed IP address" then you will need to ask what IP access you should use. The IP address is four groups of three digits and will look like this example 192.168.90.3. Use the button on the right to set the IP address you were given by your DSL or network provider.

If you are sure that you are using DHCP then [click to attempt to get an IP address](#).

© Fire4 Systems Inc, 2012. Trademarks, service marks and logos are property of their respective owners. [Privacy policy](#) [Terms and conditions](#)

If you still have a red NO after trying the steps described above then you will have to call a network specialist to help you. You can contact a network specialist by calling local IT companies. You may also find a network specialist by calling your high speed Internet service provider.

It is likely that your DSL router or cable modem has a firewall that is preventing the GIS-gateway connecting to the Internet. You should look at your DSL router configuration to 'enable NAT'ing devices'.

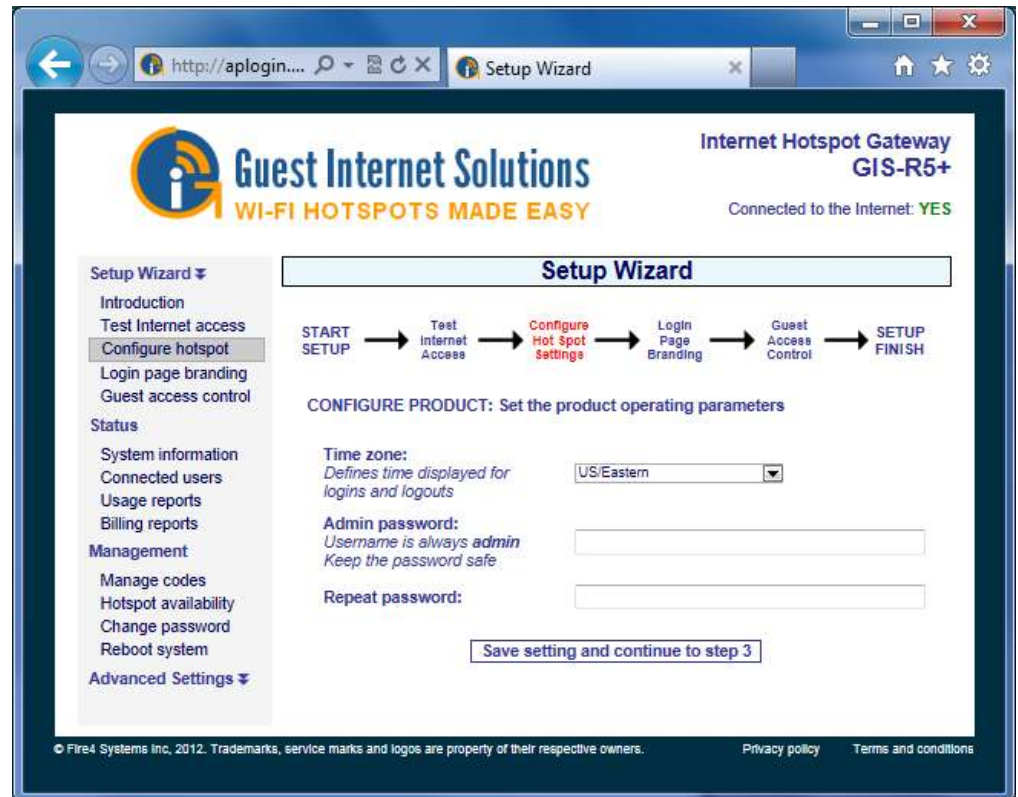
Unfortunately our support line cannot help you with this problem because an on-site inspection is required. The network specialist will visit your premises to diagnose and correct the problem.

Configuration of the Hotspot gateway cannot be completed until a connection to the Internet is obtained. Connect the gateway to an alternative DSL or cable service to complete the configuration process.



## Set the Time Zone and Password

When your Guest Internet product has a good connection to the Internet and you have clicked on the link to proceed to page 2, then you will see the page shown below.



The GIS-gateway synchronizes with Internet time and date to time access codes and provide the data and time for the usage log. It is necessary to first select the time zone for the gateway. Click on the arrow at the right of the box to see the drop down menu. Select your time zone from this list. The default time zone is US eastern time.

The GIS-gateway has no default administrator password. The administrator access password must be entered in the box. Guest Internet products can only be operated when a unique password has been entered, following the recommendations of the Payment Card Industry Data Security Standard (PCI - DSS). Create a 'strong' password using the following rules:

- The password should be at least 8 characters

- Don't use words that are in the dictionary

- Include capital letters, numbers and punctuation marks in the password

The GIS-K1 and GIS-K3 wireless gateways have an additional box to set the hotspot name (SSID) that is broadcast wirelessly. The default name is HOT SPOT. A name should be selected that can be recognized by users (e.g. Coffee Bar Hotspot).

See the screen on the following page.





When you have completed this screen click on the button to proceed to step 3.



## Enter Your Business Information for the Login Page

The next step in the setup process is the creation of the login page. Your guests will see this page when they connect to your Internet service. Your guests have to click on the disclaimer or enter a code to access the Internet.

The first option you select is the category that describes your venue. This selection determines the login page background image. The information you type into the boxes will be displayed on your login page. It is important that you provide guests with the information they need to email to friends or make a return reservation. In addition to your business information you can also type in an advertising message so that you can promote a product or service. You may not want your guests to see all the information listed on this page. Type in only the business information that you want your guests to see on your custom login page. Ignore the boxes where you do not wish to provide the information. When you have completed this screen click on the button to proceed to step 4.



## Select Disclaimer or Code Access

The next step is to select the type of access control you require. You have two options.

1. Unlimited access: The guest sees the login page and has to click on the disclaimer button to get Internet access.
2. Controlled Access: The guest has to type in an access code. The code is generated using the MANAGE CODES menu option and can be given or sold to the guest.

The choice you make here is determined by the way that you want to offer your Internet service for your guests. See the earlier section that explains this choice.

It is also necessary to type a message that tells your customer how to proceed to get Internet access. For example, you may wish to give access codes at the point of sale. In this case the message should read; "Speak to the cashier to get your access code".

Internet Hotspot Gateway  
GIS-R5+  
Connected to the Internet: YES

### Setup Wizard

START SETUP → Test Internet Access → Configure Hot Spot Settings → Login Page Branding → **Guest Access Control** → SETUP FINISH

**GUEST ACCESS CONTROL: Choose unlimited or controlled Internet access**

Unlimited access requires the user to accept your terms and conditions, Controlled access requires the user to enter an access code. You can also collect email addresses, this can be set up later from the Advanced Settings menu.

Unlimited access  
 Controlled access

**Login instructions:**

Instructions to be displayed to the customers, eg:  
*Collect free login token from cashier or  
Please use our free service*

Enter a login token to use this Hot Spot

[Save setting and finish wizard](#)

© Fire4 Systems Inc. 2012. Trademarks, service marks and logos are property of their respective owners. [Privacy policy](#) [Terms and conditions](#)

When completed click on the save settings and finish button

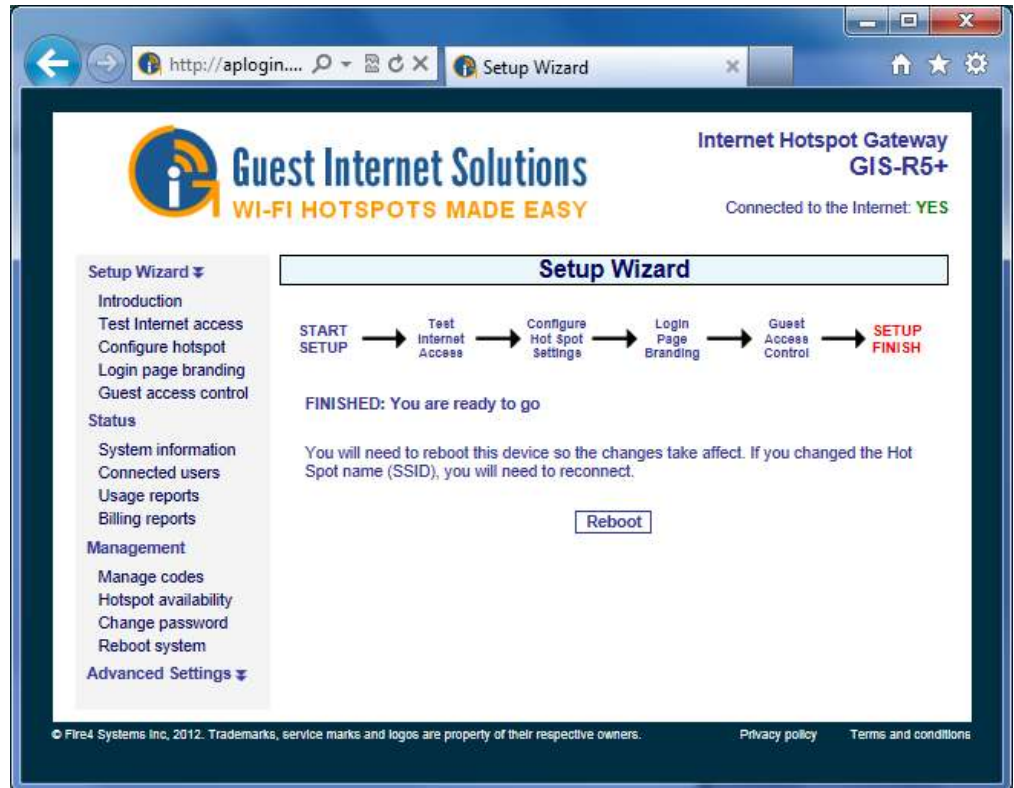




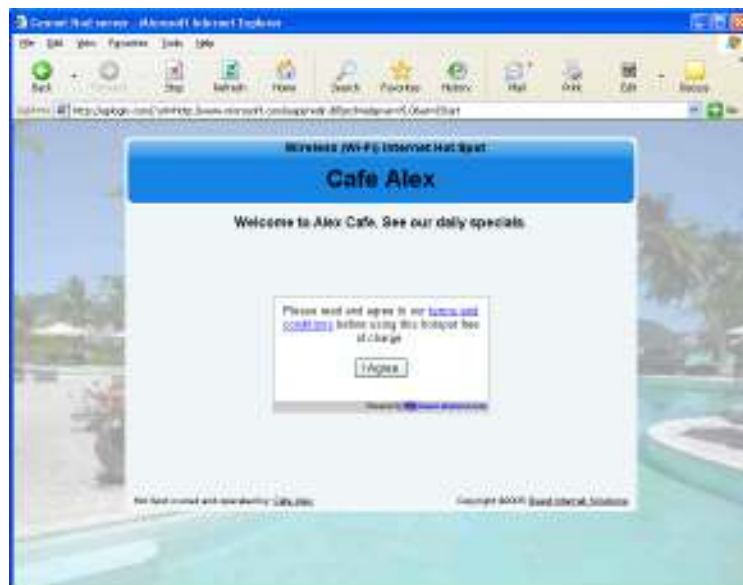
## Completing the process

The final step in the setup process is to restart or reboot the Guest Internet gateway unit. This step will restart the gateway unit with all the parameters that were entered during the setup process.

Click on the Reboot button shown on the screen below.



The Guest Internet gateway unit will take approximately three minutes before it begins functioning again. Now open your browser and you will see the login page that you created. Your login page will be similar to the display shown here.





## 5: USING YOUR GATEWAY

### Operating the Guest Internet Gateway Unit

When the setup wizard procedure has been completed it should not be necessary to make any configuration changes. If the access mode was set to CONTROLLED ACCESS then it will be necessary to log in to the device periodically to generate and download access codes.

The Guest Internet gateway unit has many features that you may wish to take advantage of by accessing the unit as the administrator. The password that you entered during the wizard setup process will be required to login as the administrator so keep a note of that password in a safe place, and don't share it with others, unless you are authorizing someone to administrate the product. You can also set a different password for a dedicated page that is used to generate and administrate access codes.

When you log in as administrator you will see a menu on the left side of the page. The menu is divided into four sections for convenience.

- SETUP WIZARD: by clicking on this menu option any information provided during the setup process can be changed.
- STATUS: this page shows the status of the product. This information will be useful for an IT technician.
- MANAGEMENT: These functions are used to administer your Internet service, you may use the **manage codes** page frequently if you are providing guests with codes.
- ADVANCED SETTINGS: These settings permit you to change technical parameters of your product. Changes in these parameters should not be required unless you have specific network requirements. For example your IT technician may have to set a fixed IP address.

This manual has a description of each page and how it can be configured.

#### Important Note

**Some of the advanced settings can disrupt normal operation of the Guest Internet gateway if changed without care. In extreme cases you may get 'locked out' of the device due to changes that you made. You can also get 'locked out' if you forget your password.**

**If you are 'locked out' then there is a procedure to reset the unit to factory defaults. This procedure is described later in this manual. All Guest Internet products have a label on the product that explains how to reset the unit to factory defaults.**

**Once set to factory defaults you will have to follow the setup wizard procedure to configure the product again for your requirements.**

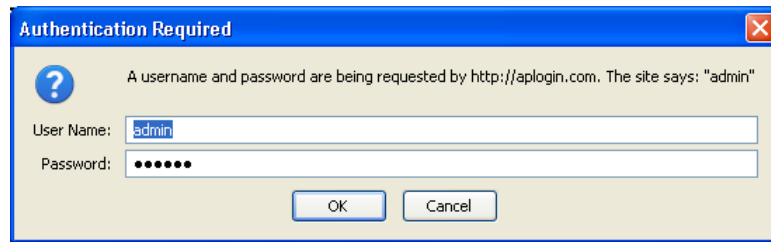
The Guest Internet gateway is configured using any type of computer. The notebook computer can be connected directly to the GIS-gateway unit using an Ethernet cable, or connected wirelessly through an access point connected to one of the LAN ports.

After powering the Guest Internet product allow 2 minutes for the unit to perform internal test routines before beginning the configuration process.

The computer's browser is used to configure the Guest Internet product. Open the browser and type the URL:

**<http://aplogin.com/admin>**

A box will open requesting the user name and password.



The username and password are:

Username = **admin**

Password = **(password set during the Wizard setup process)**

When the password has been accepted then the **Status: System Information** page will open (following section). The computer is now logged in as the administrator of the Guest Internet GIS-gateway.

Remember the password as it is required each time you wish to login as administrator. If you forget your password then you will have to reset the GIS-gateway to factory defaults and start the configuration process anew.

## Second Login for Access Code Generation and Management

All GIS gateway products have a special graphic user interface specifically to generate access codes that are given to guests for Internet access. The user interface has been optimized for display on a 7inch tablet permitting the tablet to be located at the point of sale, and be operated like a PoS screen. The user interface can also be displayed on larger and small tablets, and with both desktop and laptop computers. The access code generation display is also excellent for use with smart-phones. When the ticket printer is activated the display is used to print access codes onto tickets, as a self-contained PoS. Access codes can be generated and managed using the administrator login:

**<http://aplogin.com/admin>**

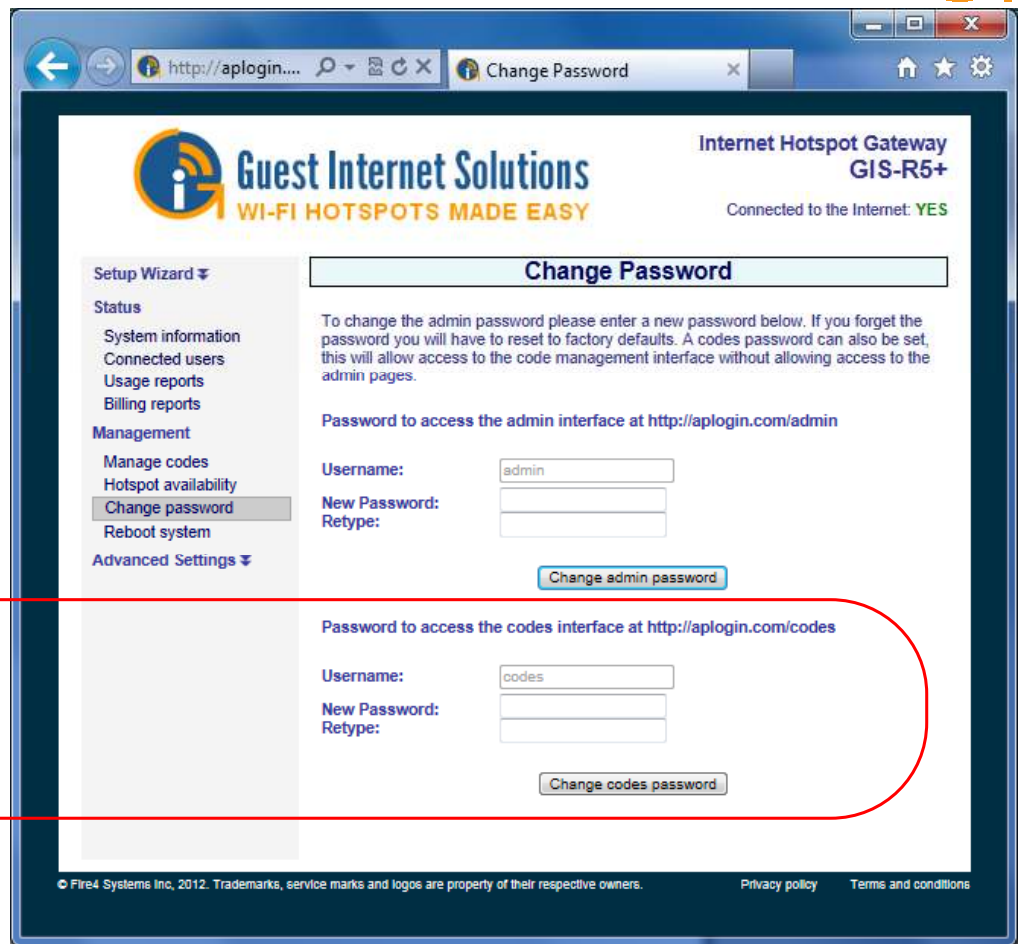
The administrator login gives access to all the features of the GIS- gateway. In many cases it is desirable to give someone the permission to generate and manage access codes, but not permit that person to have access to all the configuration parameters. A page that permits only the generation and management of codes can be accessed using the URL:

**<http://aplogin.com/codes>**

A username and password is requested when this URL is typed in and so the code administration page password must be created before this feature can be used. First login as administrator and click on the *change password* menu entry to create the password for the access code management page. See the screen below.



Change password screen:  
a second password is  
required for the access  
code generation and  
management page



If your Guest Internet gateway has been configured for the controlled access mode then you will use the **Manage Codes** feature frequently. This page is used to generate codes in several different formats and to cancel codes. It is also used to list outstanding codes. Codes can also be printer using the optional ticket printer GIS-TP1.

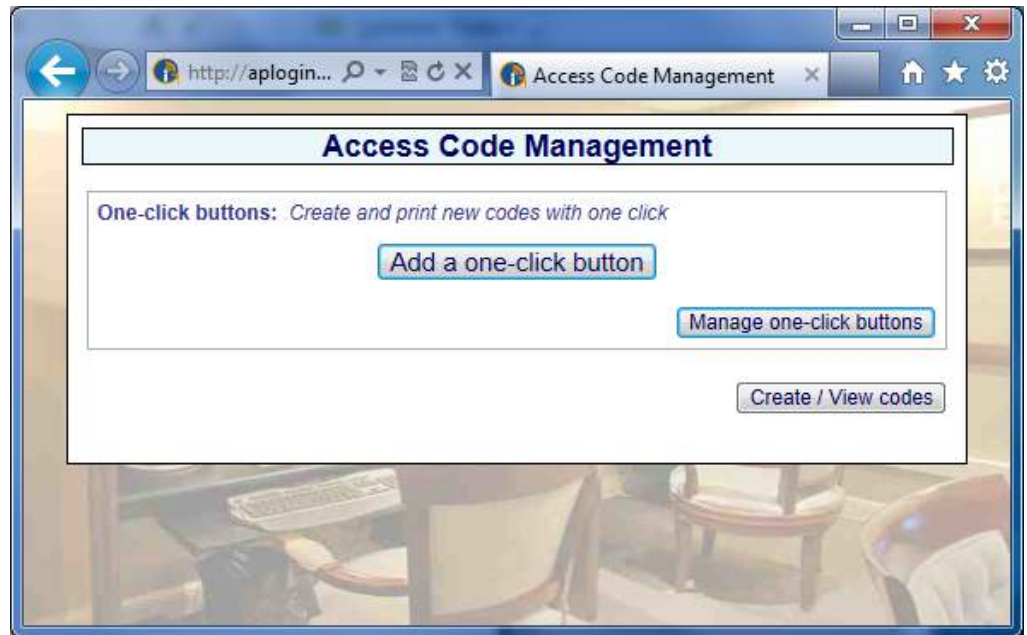
Now login to open the access code generation and management page typing in the URL:

**<http://aplogin.com/codes>**

The username for the code generation and management page is always *codes*. The password that was configured for the code generation and management page should be typed into the box shown below. Click on the button OK to see the access code management page as shown in the figure below.



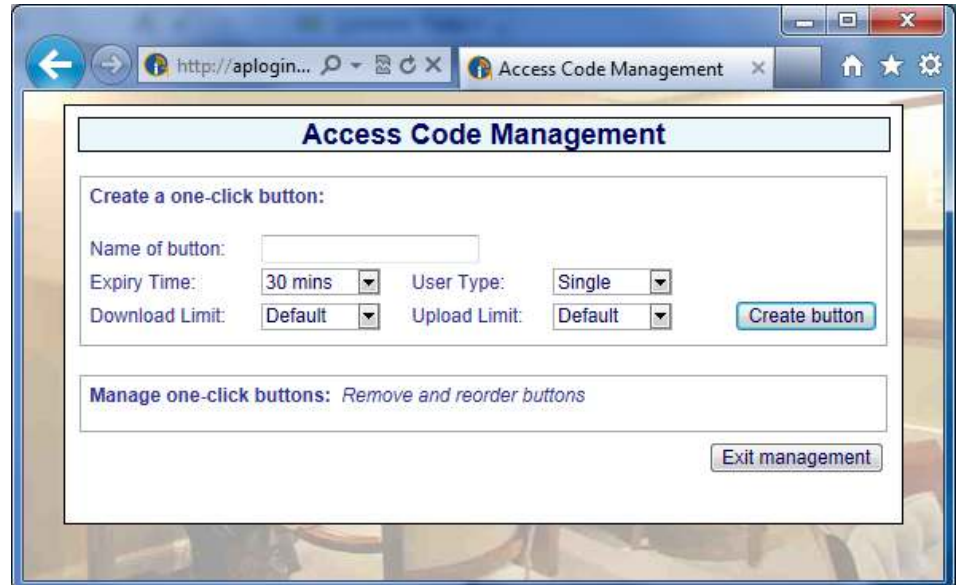
## Access code management page



The ticket printer screen is designed to be easy to use, similar in operation to a point of sale (PoS) display. It is necessary to first create buttons that are used to generate access codes. Up to ten buttons can be added to the display. The button can be touched on a tablet display, or clicked with a mouse on a desktop or laptop computer, to generate the access code. The buttons also work with a smart phone touch display.

Click on the 'add a one-click button' to add a button to the display. The screen that is shown on the following page will be displayed.

## Add one-click button page



First type the name of the button that will be shown on the display subsequently. This could refer to the access time, e.g. two-hours, or the type of user, e.g. conference-guest. The code duration can be selected from 30 minutes to 180 days using the drop down menu. One of two codes types can be selected

- **Single:** Only one guest can use this code. The code runs to completion after login. The duration of the code is selected by the time option.
- **Multi-User:** Many guests can use this code concurrently for Internet access. The

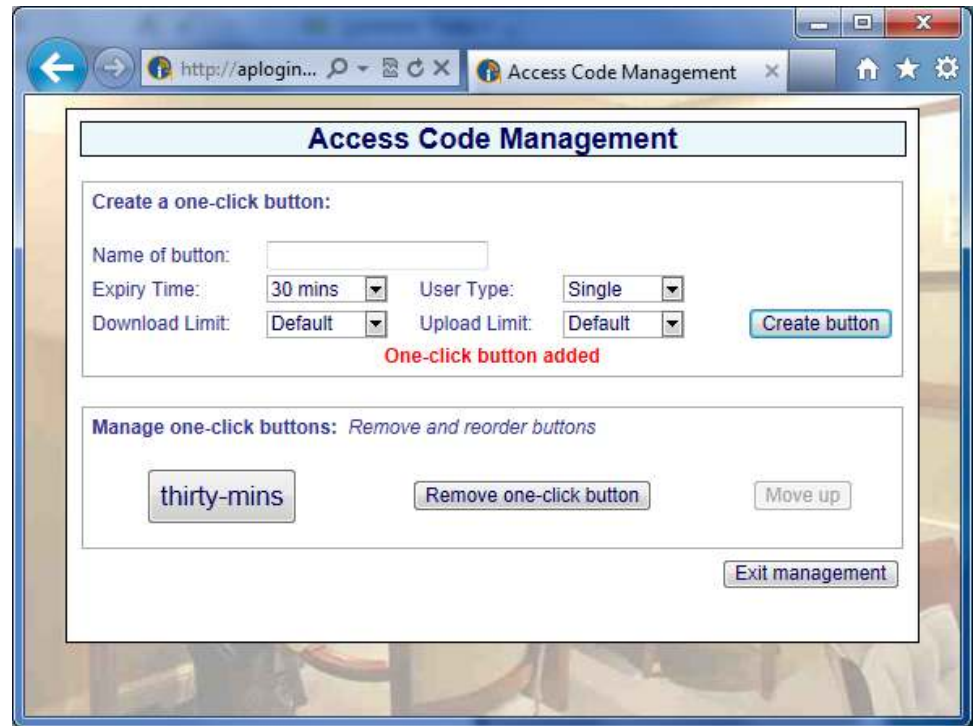




timer starts the first time that the code is used by any user, and the code expires after the duration set for the code. Subsequent users will therefore have less time available for the code.

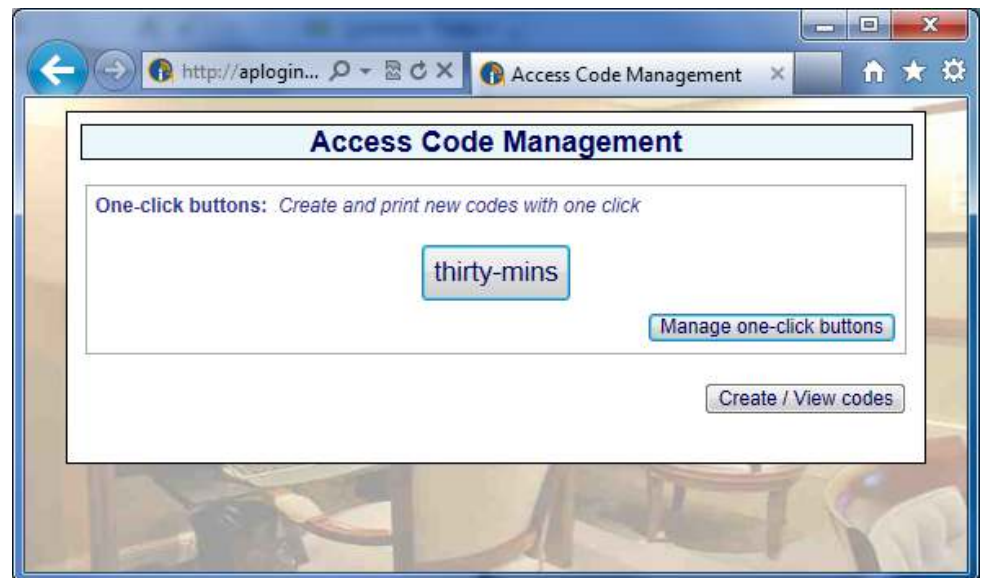
The download and upload speed limits can also be specified for the code using the drop down menu. When the 'create button' is clicked the following screen is displayed.

Button added page



Click the 'exit management' button to see the display with button that is used to generate access codes.

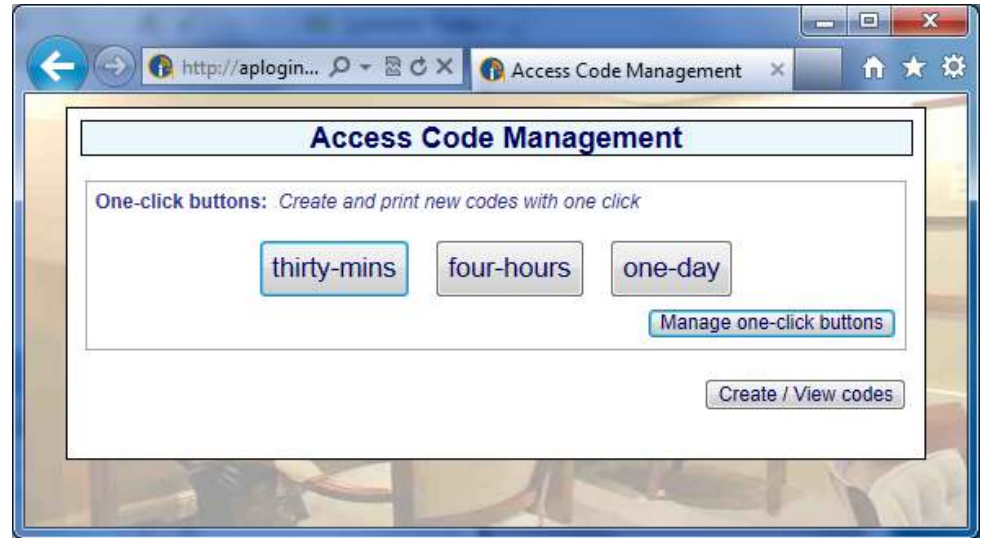
Access code generation page



Two more buttons have been added to the display shown below. A maximum of ten buttons can be added to the display.

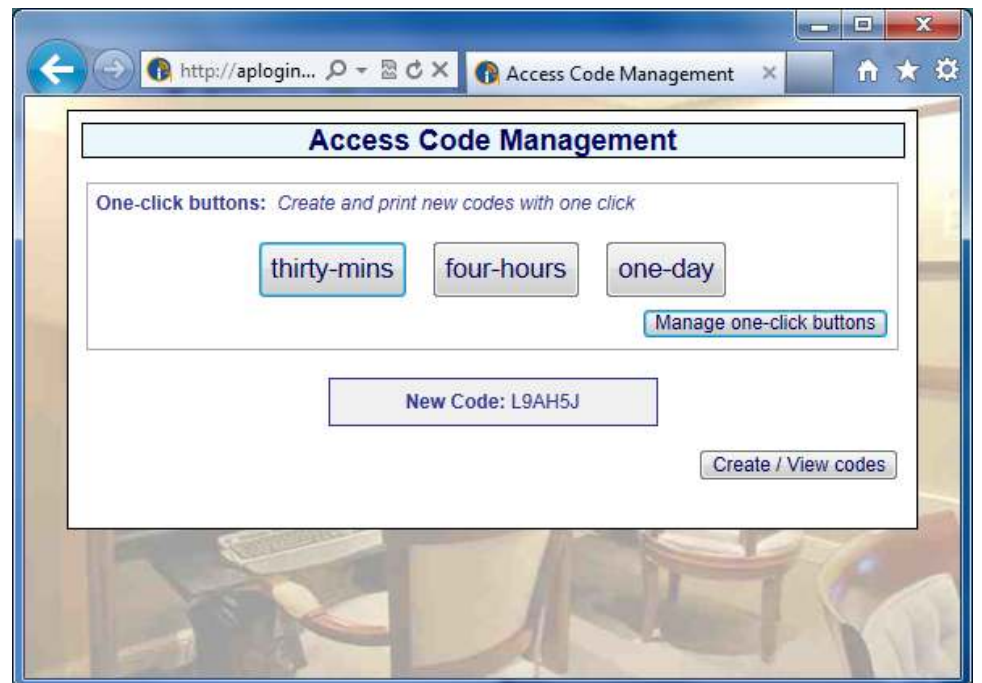


**Access code generation page showing three buttons**



When any button is clicked the access code that has been generated is shown on the display. See the figure on the following page.

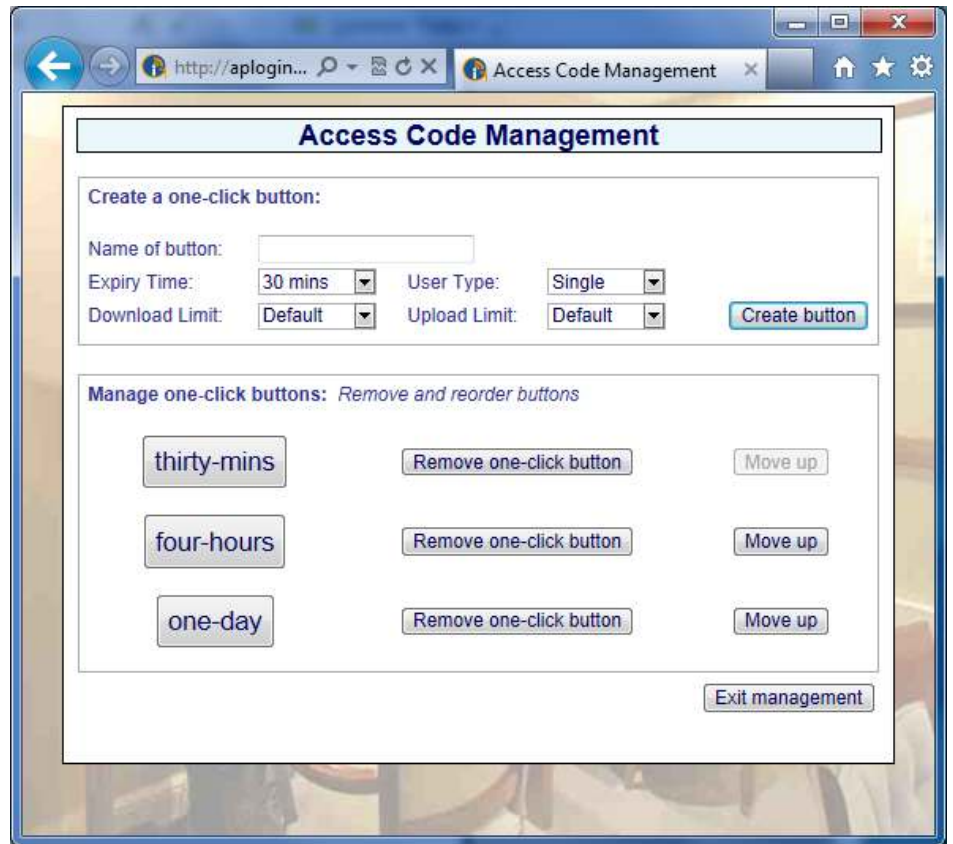
**Access code generated**



Buttons can be removed, and new buttons created at any time by clicking on 'manage one-click buttons'. When clicked the screen shown on the following page is displayed. Any button can be removed by clicking on 'remove one-click button'. New buttons can be added by following the procedure describer above. Click on 'exit management' when finished.

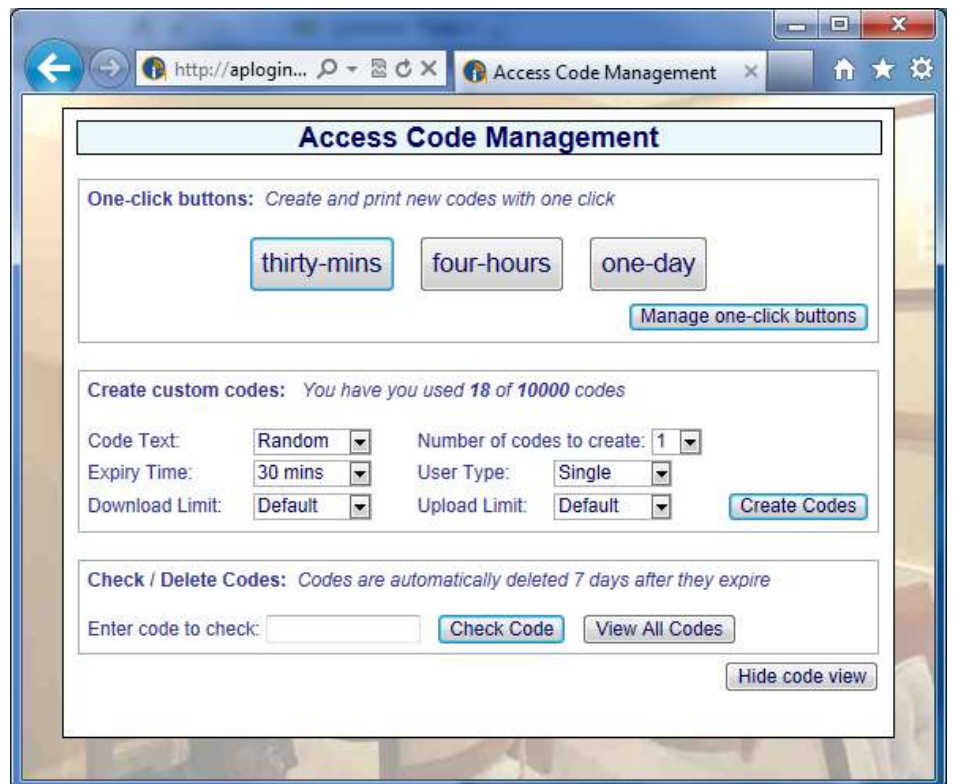


### Manage buttons page



The access code management page also has a 'create/view codes' option. See the figure above. The create/view codes display is shown on the following page.

### Create/view codes page





The create/view codes page provides two features. The first is the option to create custom codes. The screen below shows a custom code that has been generated.

## Create new custom code

**Access Code Management**

One-click buttons: *Create and print new codes with one click*

thirty-mins four-hours one-day

Manage one-click buttons

Create custom codes: *You have you used 10 of 10000 codes*

Code Text: Random Number of codes to create: 1

Expiry Time: 30 mins User Type: Single

Download Limit: Default Upload Limit: Default Create Codes

New Codes:

#	Code	Time	Type	Down	Up
1	W284GW	30 mins	single user	default	default

Check / Delete Codes: *Codes are automatically deleted 7 days after they expire*

Enter code to check:  Check Code View All Codes

Hide code view

This option is used when several of codes are required as the number of codes can be specified. As an alternative, one code can be generated with a name that can be specified in the code text box, rather than use the random codes generated by the buttons. As with the button, the code duration, user type, and download /upload limits are specified. Click the 'create codes' button to generate the access codes.

Access codes can also be verified by typing the code into the 'code to check' box. Click the 'check code' button to see the access code characteristics.

Click the 'view all codes' button to display a list of all access that have been generated, and have not expired. This display is shown in the figure below. This display can be used to delete any code or codes by checking the boxes and clicking the 'delete checked codes' button.



### View all codes page

**Access Code Management**

One-click buttons: *Create and print new codes with one click*

thirty-mins    four-hours    one-day

Manage one-click buttons

Create custom codes: *You have you used 9 of 10000 codes*

Code Text: Random    Number of codes to create: 1  
 Expiry Time: 30 mins    User Type: Single  
 Download Limit: Default    Upload Limit: Default    Create Codes

Check / Delete Codes: *Codes are automatically deleted 7 days after they expire*

Enter code to check:    Check Code    View All Codes

<input type="checkbox"/>	Code	Time	Type	Used	Time Left	Down kbit/s	Up kbit/s	Download Used	Upload Used
<input type="checkbox"/>	0BXH45	30 mins	single	NO	30 mins	*	*	0	0
<input type="checkbox"/>	0T0W1F	30 mins	single	NO	30 mins	*	*	0	0
<input type="checkbox"/>	20EY1E	30 mins	single	NO	30 mins	*	*	0	0
<input type="checkbox"/>	4LL5DH	2 hours	single	NO	2 hours	*	*	0	0
<input type="checkbox"/>	7158TB	30 mins	single	NO	30 mins	*	*	0	0
<input type="checkbox"/>	9F6KRE	2 hours	single	NO	2 hours	*	*	0	0
<input type="checkbox"/>	C6KQYQ	30 mins	single	NO	30 mins	*	*	0	0
<input type="checkbox"/>	D57XCC	30 mins	single	NO	30 mins	*	*	0	0
<input type="checkbox"/>	W2W31K	30 mins	single	NO	30 mins	*	*	0	0

Delete checked codes

\* Default bandwidth limit (kbit/s)

Hide code view

Available access codes are shown in the list of generated codes. When the time of a code has expired it remains in the list for seven days before automatic deletion. An expired code can be removed from the list by clicking in the box to the left of the code then clicking the 'Delete checked codes' button and multiple codes can also be deleted. When codes are removed from the list new codes can be generated. The list of codes can be downloaded in a CSV format and copied into a spreadsheet for analysis.

The type of code that is generated will depend on your business and the type of Internet service that you want to offer your guests.

For example, if you own a coffee bar and want to provide free Internet then give your guests a 30-minute access code but only with a purchase. This will avoid Internet users filling your tables and not buying your products. If the guest wants to continue to access the Internet after 30 minutes then he or she has to make a second purchase to get a new code.



In summary, you have to select the parameters for each code or block of codes according to the needs of your business.

The access code parameters that can be configured are:

- Number of codes
- Duration of each code (30 minutes to 180 days)
- Type of code (single user or multi-user)
- Download speed limit (in Kbytes/second)
- Upload speed limit (in Kbytes/second)

The screens on the previous pages showed the generation of the access code where the name was composed of random numbers and letters. An easily remembered name can also be typed in to use as the access code. Note that if the code is easy to recognize then unauthorized users will also discover the code and get access to the Internet. The custom access code name must not include spaces. If it desired to separate two words then the underscore character can be used. The code name is limited to nine characters maximum.

Guests and visitors who have been given codes for Internet access may complain that the code cannot be used or the time was too short. Any access code can be verified. First type the code into the 'Enter codes to check box', and then click on the **Check code** button. The current status of the code will be shown. This feature is especially important if you are selling codes and have to address customer complaints regarding the Internet service.





## 5: STATUS FUNCTIONS

### System Information

On completion of the administrators login process the system information screen is displayed (shown below). The information displayed shows;

- **Product model** (required for firmware upgrades)
- **Firmware version** (required for firmware upgrades)
- **Serial number** (required for firmware upgrades)
- Verification that the device is connected to the Internet
- Current date and time and timezone
- Authenticated users and codes used
- WAN and LAN port network configurations
- Status of firewall, content filter, remote access and Dynamic DNS
- Information text box for configuration notes

### System Information Display

The screenshot shows the 'System Information' page of the Guest Internet Solutions web interface. The page is titled 'System Information' and displays various system details. On the left, there is a 'Setup Wizard' menu with options like 'System information', 'Connected users', 'Usage reports', 'Billing reports', 'Management', and 'Advanced Settings'. The main content area shows the following information:

- Uptime:** 23h 00m 13s
- Hostname:** aplogin.com
- Date / time:** 06/18/15 09:08:17 AM [\[Reset\]](#)
- Timezone:** US/Eastern
- Firmware version:** 2.4.4.1a
- Serial Number:** 4562dda6

A promotional banner for a 'NEW login code ticket printer available' is displayed, with the text: 'Print login codes for hotspot users with the click of a button. Find out more about the new Point-of-Sale style ticket printer.'

Below the banner, the following status information is shown:

- Hotspot enabled:** YES [\[View Schedule\]](#)
- Authenticated users:** 0
- Codes used:** 0

Network configuration details include:

- WAN IP address:** 10.1.10.70 (dhcp)
- WAN MAC address:** 04:F0:21:10:5F:95
- LAN IP address:** 192.168.96.1
- LAN DHCP range:** 192.168.96.10 - 192.168.111.254

Security and access settings are listed as:

- Firewall:** Enabled
- Content filter:** Disabled
- Remote access:** Disabled
- Dynamic DNS:** Disabled

At the bottom, there is a 'Notes: (Private information about this device)' section with a text area and a 'Save' button. The footer of the page contains copyright information: '© Fire4 Systems Inc, 2015. Trademarks, service marks and logos are property of their respective owners.' and links for 'Privacy policy' and 'Terms and conditions'.





Four main menu topics are shown, and each main menu has several configuration pages:

- Setup Wizard
- Status (includes this system information page)
- Management
- Advanced settings

The management menu is used to manage the product for day-to-day use. Click on the down arrow to expand the Setup Wizard and the Advanced settings.

## Connected Users

Clicking on the **Connected Users** menu will show the page seen in the figure below.

There are two boxes, Authenticated users and Connected users. Connected users lists all the computers that are connected to the gateway unit: they have requested and obtained an IP address. The authenticated users box shows all the guests that have provided a valid access code (controlled access mode) or clicked on the disclaimer agreement button (unlimited access mode). Information about connected clients is shown: MAC address, IP address allocated by the gateway unit, time that remains on the code, bytes out (use of the network) and the access code used.

## Connected Clients Menu Page

The screenshot displays the 'Connected Users' page of the Guest Internet Solutions web interface. The page is titled 'Internet Hotspot Gateway GIS-R3' and indicates 'Connected to the Internet: YES'. The main content area is titled 'Connected Users' and contains the following sections:

- Authenticated users (logged in):** A table with columns: Mac address, OS/Browser, Time left, Bytes In / Out, Code. The table shows 'No users connected'.
- Connected users (using the gateway):** A table with columns: Mac Address, IP Address, Blocked IP, Blocked MAC, Allowed MAC. The table shows one entry: Mac Address 80:c1:6e:45:07:b7, IP Address 192.168.98.10, Blocked IP No, Blocked MAC No, Allowed MAC No.
- IP addresses issued:** A table with columns: Mac Address, IP Address, Host Name, Lease Expiry Time. The table shows one entry: Mac Address 80:c1:6e:45:07:b7, IP Address 192.168.98.10, Host Name jb-HP, Lease Expiry Time 21:58:04.

The sidebar on the left contains navigation links for Setup Wizard, Status, Management, and Advanced Settings. The page footer includes copyright information for Fire4 Systems Inc. 2015 and links for Privacy policy and Terms and conditions.



Clicking on the blue 'X' in the right hand column will disconnect that authenticated user.

Clicking on the red 'X' in the right hand column will disconnect that user, and include the users computer MAC address in the blocked MAC list, preventing the user accessing the Internet.

## Usage Report

Clicking on **Usage reports** will display the page shown below. The last 10,000 entries are stored and displayed on this page. The number of users per day is shown on the top time-varying graph that can extend up to 28 days. The graph below shows the login times during the previous 24 hour period, and an indication below the graph shows the number of new guests vs. returning guests, and the devices used for access.

The data table had seven parameters for each entry: Login time, MAC address, Access code used, Time connected, Downloaded data volume, Uploaded data volume, Logout reasons (listed on the next page). The usage data can be downloaded in a CSV format and loaded into a spreadsheet program such as Excel for further analysis.

### Usage Reports Menu Page

The screenshot displays the 'Usage Reports' page in a web browser. The browser address bar shows 'http://aplogin.com/adr' and the page title is 'Usage Reports'. The page header includes the 'Guest Internet Solutions' logo and 'Internet Hotspot Gateway GIS-R3'. A sidebar menu on the left contains the following items: Setup Wizard, Status (System information, Connected users, Usage reports, Billing reports), Management (Manage codes, Hotspot availability, Change password, Reboot system), and Advanced Settings. The main content area features a 'Usage Reports' section with a dropdown menu set to 'last 28 days'. Below this are two empty bar charts: 'Login times' and 'New vs returning guests'. At the bottom of the page, there is a form to 'Deliver daily report to email address' with an 'Update' button. A table at the bottom has columns: Login, MAC, OS/Browser, Code, Usage, Down, Up, Logout. The footer contains copyright information for Fire4 Systems Inc, 2015, and links for Privacy policy and Terms and conditions.



**Logout reasons:**

-	Unknown logout reason
<b>User</b>	User logged out (logout button)
<b>Time Up</b>	Login time expired
<b>Inactivity</b>	User disconnected from the network or turned computer off
<b>Forced</b>	User was logged out by admin on connected users page or settings were changed
<b>Banned</b>	User was banned by admin from connected users page
<b>Disabled</b>	Hotspot entered disabled mode (see hotspot availability schedule)
<b>Banned/P2P</b>	User was blocked for using Peer-to-peer software
<b>Duplicate</b>	There was a duplicate MAC address or IP address on the network
<b>Reboot</b>	The hotspot was rebooted
<b>Over limit</b>	User exceeded upload or download data limit







## 6: MANAGEMENT FUNCTIONS

### Manage Codes

If your Guest Internet gateway has been configured for the controlled access mode then you can login as **admin** to use the **Manage Codes** menu page or login as **codes** to use the Manage Codes page (previous section). This page is used to generate codes in several different formats and to cancel codes. It is also used to list outstanding codes. Codes can be downloaded in a CSV format (comma separated value) and then used by popular word processors such as MS WORD™ to print the codes onto Avery peel-off labels. When the Manage Codes menu option is selected the page shown below appears. The upper part of the box is used to generate codes; the lower part of the box is used to manage codes. Up to 10,000 access codes can be generated. As codes are used they are deleted from the database and more codes can be generated. The code duration can be selected from 30 minutes to 180 days. Code usage can be selected as follows

- **One to five guests:** Specify one to five guests who can use this code. The code runs to completion after the first login. The duration of the code is selected by the length option.
- **Multi-User:** Many guests can use this code concurrently for the duration set for the code. Note that the counter starts the first time that the code is used by any user, and the code expires after the duration set for the code. Subsequent users will therefore have less time available than the time set for the code.

The screen below shows the access code setting options. The code can have random or user specified text. In addition to expiration time and number of users, the code can have up and down speed limits set, and also up and down byte count limits.

Access code generation and management page, the access code type is random: a random name will be generated

Internet Hotspot Gateway  
GIS-R3  
Connected to the Internet: YES

### Access Code Management

Create codes: You have you used 0 of 10000 codes

Code Text:  Number of codes to create:

Expiry Time:  Usage:

Down Speed:  Up Speed:

Down Limit:  Up Limit:

Usage: Code can be shared by the number of selected users. Code expires at pre-set time after code was first used.

Speed: Guests using this code will be throttled (limited) to the speeds selected. Default set on [bandwidth control](#) page.

Limit: Data usage will be limited to values selected. Guests sharing codes will also share the limit. Default set on [bandwidth](#) page.

You can also use <http://aplogin.com/codes/> to manage codes, [set a password](#).  
[Import codes](#) from a CSV file, all existing codes will be replaced.

Check / Delete Codes: Codes are automatically deleted 7 days after they expire

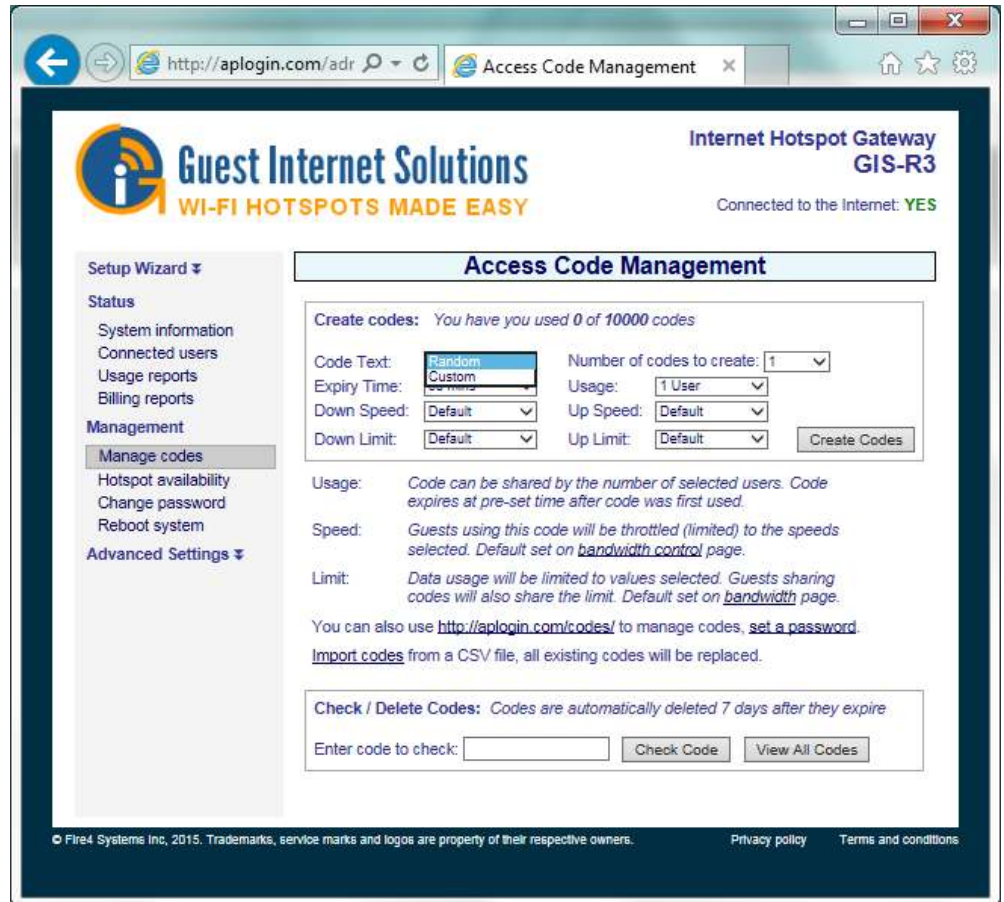
Enter code to check:

© Fire4 Systems Inc, 2015. Trademarks, service marks and logos are property of their respective owners. [Privacy policy](#) [Terms and conditions](#)



Two buttons at the bottom of the screen are **Check Code** and **View all Codes**. A code that has been given to a guest can be checked for validity. This is important if you are selling codes to guests. Type the code into the box then click on the Check Code button. A report will be shown of the remaining time for that code. Clicking the View all Codes button will display all codes that have been generated and show the status of each. The procedure to generate an access code is shown in the sequence of screens below.

**Access code generation and management page:**  
Select the type of access code, random or custom



The access code can be a randomly generated sequence of eight characters, or can be a custom name of up to 9 characters (letters and numbers).

If random is selected then the box to the right permits the number of codes to be selected, up to a maximum of 10,000. If custom is selected then only one code is generated, and the box to the right permits the characters to be typed for the custom code. A name up to 9 digits can be entered, letters and numbers, spaces are not allowed. An example for a custom access code is 'cityhotel'. Only one code can be generated with this name.





For random code type,  
select the number of  
codes to create

Internet Hotspot Gateway  
GIS-R3  
Connected to the Internet: YES

### Access Code Management

Create codes: You have you used 0 of 10000 codes

Code Text: Random Number of codes to create: 1  
 Expiry Time: 30 mins Usage: 1 User  
 Down Speed: Default Up Speed: Default  
 Down Limit: Default Up Limit: Default

Usage: Code can be shared by the number of selected users. Code expires at pre-set time after code was first used.

Speed: Guests using this code will be throttled (limited) to the speeds selected. Default set on [bandwidth control](#) page.

Limit: Data usage will be limited to values selected. Guests sharing codes will also share the limit. Default set on [bandwidth](#) page.

You can also use <http://aplogin.com/codes/> to manage codes, [set a password](#).  
[Import codes](#) from a CSV file, all existing codes will be replaced.

Check / Delete Codes: Codes are automatically deleted 7 days after they expire

Enter code to check:

© Fire4 Systems Inc, 2015. Trademarks, service marks and logos are property of their respective owners. Privacy policy Terms and conditions

Select the duration of the  
code(s) from 30 minutes  
to 180 days, or a custom  
time, or unlimited

Internet Hotspot Gateway  
GIS-R3  
Connected to the Internet: YES

### Access Code Management

Create codes: You have you used 0 of 10000 codes

Code Text: Random Number of codes to create: 1  
 Expiry Time: 30 mins Usage: 1 User  
 Down Speed: Default Up Speed: Default  
 Down Limit: Default Up Limit: Default

Usage: Code can be shared by the number of selected users. Code expires at pre-set time after code was first used.

Speed: Guests using this code will be throttled (limited) to the speeds selected. Default set on [bandwidth control](#) page.

Limit: Data usage will be limited to values selected. Guests sharing codes will also share the limit. Default set on [bandwidth](#) page.

You can also use <http://aplogin.com/codes/> to manage codes, [set a password](#).  
[Import codes](#) from a CSV file, all existing codes will be replaced.

Check / Delete Codes: Codes are automatically deleted 7 days after they expire

Enter code to check:

© Fire4 Systems Inc, 2015. Trademarks, service marks and logos are property of their respective owners. Privacy policy Terms and conditions



Select the type of code(s): single user, two to five users, or multi-user

**Internet Hotspot Gateway GIS-R3**  
Connected to the Internet: **YES**

### Access Code Management

Create codes: You have you used 0 of 10000 codes

Code Text:  Number of codes to create:

Expiry Time:  Usage: **1 User**

Down Speed:  Up Speed:

Down Limit:  Up Limit:

**Create Codes**

Usage: Code can be shared by the number of selected users. Code expires at pre-set time after code was first used.

Speed: Guests using this code will be throttled (limited) to the speeds selected. Default set on [bandwidth control](#) page.

Limit: Data usage will be limited to values selected. Guests sharing codes will also share the limit. Default set on [bandwidth](#) page.

You can also use <http://aplogin.com/codes/> to manage codes, [set a password](#), [Import codes](#) from a CSV file, all existing codes will be replaced.

Check / Delete Codes: Codes are automatically deleted 7 days after they expire

Enter code to check:  **Check Code** **View All Codes**

© Fire4 Systems Inc, 2015. Trademarks, service marks and logos are property of their respective owners. [Privacy policy](#) [Terms and conditions](#)

Select download speed limit for the code(s) (in Kbytes/second). If the speed you want is not in the drop-down menu then select custom and type in the speed in Kbits/sec.

**Internet Hotspot Gateway GIS-R3**  
Connected to the Internet: **YES**

### Access Code Management

Create codes: You have you used 0 of 10000 codes

Code Text:  Number of codes to create:

Expiry Time:  Usage:

Down Speed: **Default** Up Speed:

Down Limit:  Up Limit:

**Create Codes**

Usage: Code can be shared by the number of selected users. Code expires at pre-set time after code was first used.

Speed: Guests using this code will be throttled (limited) to the speeds selected. Default set on [bandwidth control](#) page.

Limit: Data usage will be limited to values selected. Guests sharing codes will also share the limit. Default set on [bandwidth](#) page.

You can also use <http://aplogin.com/codes/> to manage codes, [set a password](#), [Import codes](#) from a CSV file, all existing codes will be replaced.

Check / Delete Codes: Codes are automatically deleted 7 days after they expire

Enter code to check:  **Check Code** **View All Codes**

© Fire4 Systems Inc, 2015. Trademarks, service marks and logos are property of their respective owners. [Privacy policy](#) [Terms and conditions](#)





Select upload speed limit for the code(s) (in Kbytes/second). If the speed you want is not in the drop-down menu then select custom and type in the speed in Kbits/sec.

The screenshot shows the 'Access Code Management' page for 'Internet Hotspot Gateway GIS-R3'. The 'Up Speed' dropdown menu is open, displaying various speed options in kbit/s. The 'Create Codes' section includes fields for Code Text, Expiry Time, Down Speed, Down Limit, Number of codes to create, Usage, and Up Speed. A 'Create Codes' button is visible. The page footer contains copyright information for Fire4 Systems Inc. and links to Privacy policy and Terms and conditions.

Select download byte limit for the code(s) (in Mbytes). If the byte limit required is not in the drop-down menu then select custom and type in the download limit in Mbytes. The default is unlimited. This feature is included for hotspot operators who are charged per Mbyte by their ISP's.

The screenshot shows the 'Access Code Management' page for 'Internet Hotspot Gateway GIS-R3'. The 'Down Limit' dropdown menu is open, displaying various byte limit options in MB and GB. The 'Create Codes' section includes fields for Code Text, Expiry Time, Down Speed, Down Limit, Number of codes to create, Usage, and Up Speed. A 'Create Codes' button is visible. The page footer contains copyright information for Fire4 Systems Inc. and links to Privacy policy and Terms and conditions.



Select upload byte limit for the code(s) (in Mbytes). If the byte limit required is not in the drop-down menu then select custom and type in the download limit in Mbytes. This feature is included for hotspot operators who are charged per Mbyte by their ISP's.

The screenshot shows the 'Access Code Management' page. The 'Create codes' section is active, showing 'You have you used 0 of 10000 codes'. The 'Up Limit' dropdown menu is open, displaying options: Default, 16 MB, 32 MB, 64 MB, 128 MB, 256 MB, 512 MB, 1024 MB (1 GB), 2048 MB (2 GB), Custom, and Unlimited. The 'Create Codes' button is visible.

The screen shows the generation of a 30 minute access code with a random name.

The screenshot shows the 'Access Code Management' page after creating a code. The 'Create codes' section now shows 'You have you used 1 of 10000 codes'. Below it, a table titled 'New Codes' displays the generated code details.

#	Code	Time	Users	Down Speed	Up Speed	Down Limit	Up Limit
1	JHF2TR	30 mins	1	default	default	default	default

A 'Download CSV file' button is located below the table. The 'Check / Delete Codes' section is also visible at the bottom.



List all access codes generated. The access code list shows the code, the duration of the code, the code type, if used, the time remaining, and the download/upload maximum speeds set for the code. Check the box then click on 'delete checked codes' to delete the codes and increase the number of codes that can be generated.

Internet Hotspot Gateway  
GIS-R3  
Connected to the Internet: YES

### Access Code Management

Create codes: *You have you used 1 of 10000 codes*

Code Text:  Number of codes to create:

Expiry Time:  Usage:

Down Speed:  Up Speed:

Down Limit:  Up Limit:

Check / Delete Codes: *Codes are automatically deleted 7 days after they expire*

Enter code to check:

<input type="checkbox"/>	Code	Time	Users	Used	Time Left	Down kbit/s	Up kbit/s	Down MB	Up MB	Down Used	Up Used
<input type="checkbox"/>	JHP2TR	30 mins	1	NO	30 mins	-	-	-	-	0	0

\* Default bandwidth limit (kbit/s)

© Fire4 Systems Inc, 2015. Trademarks, service marks and logos are property of their respective owners. [Privacy policy](#) [Terms and conditions](#)

Up to a maximum of 10,000 codes can be shown in the list of generated codes. When the time of a code has expired it remains in the list for seven days before automatic deletion. An expired code can be removed from the list by checking the box to the left of the code and clicking on the 'Delete checked codes' button. When codes are removed from the list new codes can be generated.

The list of codes can be downloaded in a CSV format and copied into a spreadsheet for analysis.

The type of code that is generated will depend on the Internet hotspot service being offered to guests.



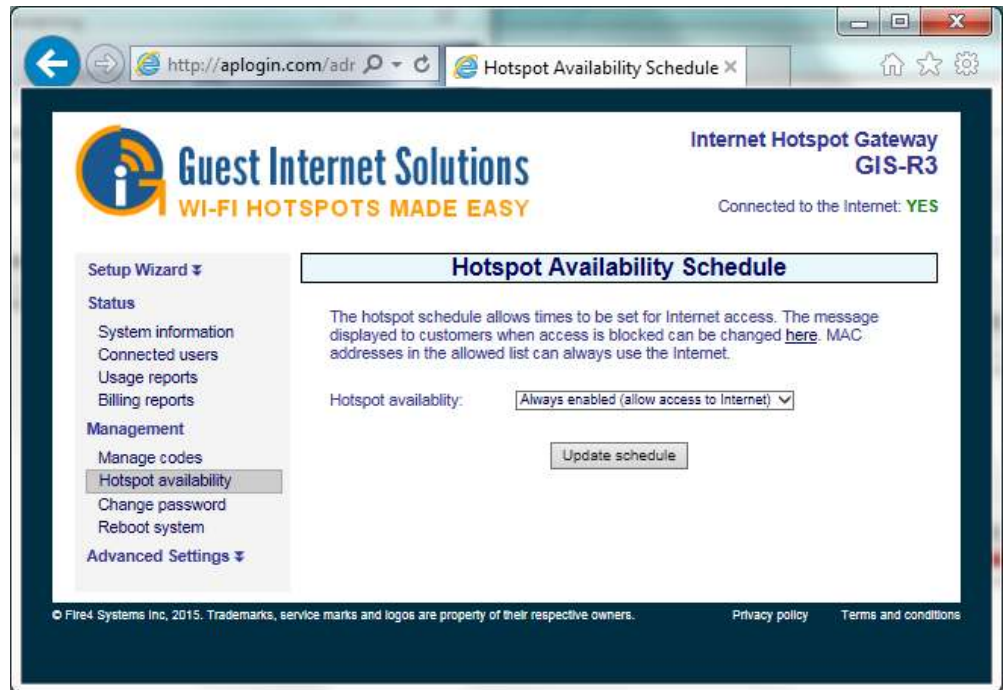


## Hotspot Availability

Hotspot availability permits the gateway to be enabled or disabled during a weekly cycle. Clicking on the **Hotspot availability** menu opens the default page, which shows always enabled.

Click on the right hand arrow to see the drop down menu.

Default Hotspot availability screen, always enabled



If 'schedule access' is selected from the drop-down menu then the selection table is displayed (shown on the following page).

The Hotspot can be enabled or disabled in increments of 1-hour, during a 7-day period.

Each hourly selection box is checked for enabled when the table is first opened. Uncheck the boxes when the Hotspot service should not be provided.

For example, to configure availability for a dental office where the hours of operation are 9AM to 5PM, Monday to Friday, uncheck the boxes as follows. First uncheck all boxes 12AM to 8AM, Monday to Friday. Next uncheck all boxes 5PM to 11PM Monday to Friday. Finally uncheck all boxes for Saturday and Sunday.

At the times when the Hotspot has been disabled, the login screen will display the message "this hotspot is not available". The message that is displayed can be changed, see the Login messages menu page.





### Hotspot availability selection table

Internet Hotspot Gateway GIS-R3  
Connected to the Internet: YES

## Hotspot Availability Schedule

The hotspot schedule allows times to be set for Internet access. The message displayed to customers when access is blocked can be changed [here](#). MAC addresses in the allowed list can always use the Internet.

Hotspot availability:

ALL / NONE	Sun	Mon	Tue	Wed	Thu	Fri	Sat
12 am	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
01 am	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
02 am	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
03 am	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
04 am	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
05 am	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
06 am	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
07 am	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
08 am	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
09 am	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
10 am	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
11 am	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
12 pm	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
01 pm	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
02 pm	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
03 pm	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
04 pm	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
05 pm	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
06 pm	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
07 pm	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
08 pm	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
09 pm	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
10 pm	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
11 pm	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Ticked boxes indicated the hotspot is enabled

© Fire4 Systems Inc, 2015. Trademarks, service marks and logos are property of their respective owners. [Privacy policy](#) [Terms and conditions](#)

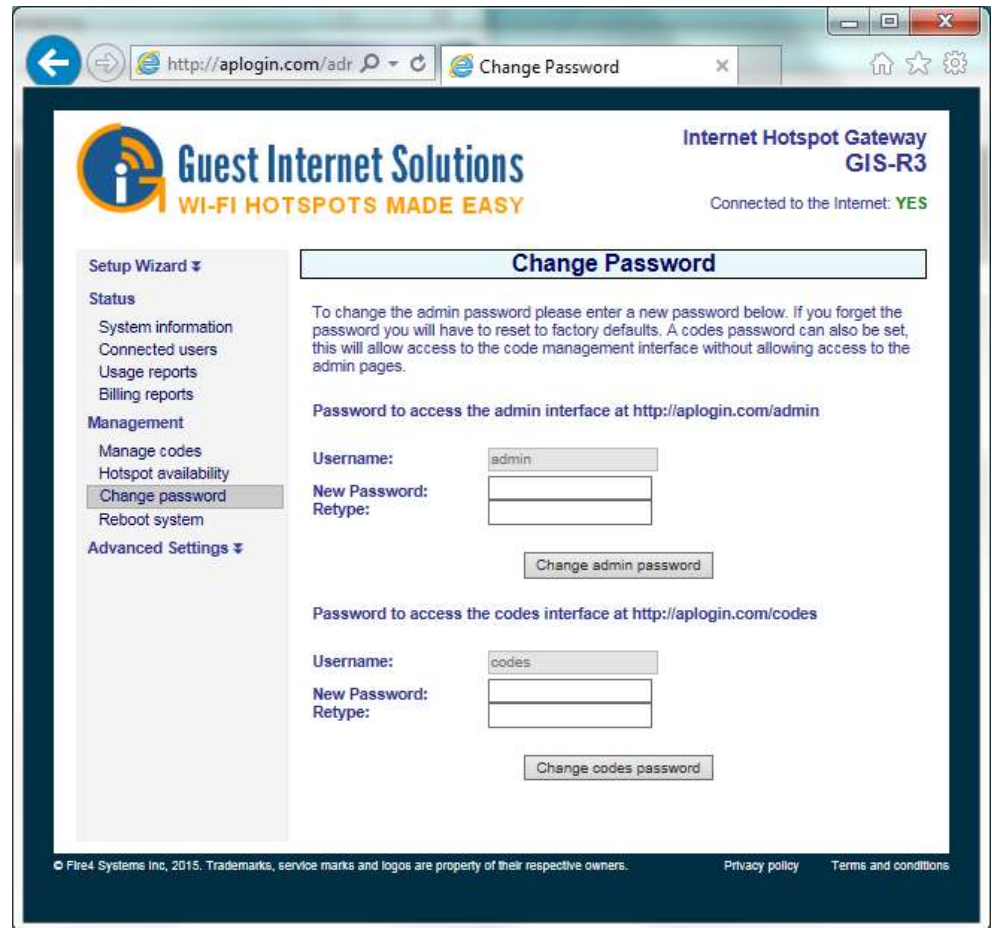


## Change Password

During the wizard setup procedure a password must be typed in for the administrator login. The **Change Password** menu option is used to change the password at any time after the initial setup procedure.

The change password menu page is shown in the figure below.

### Change Password Menu Page



Two passwords are required. The first is the **admin** password that is used to access the Admin pages: this password was entered during the Wizard setup process.

The second is the **codes** password is required for login to the Codes page (see previous sections). The codes page is used to create and administer access codes, however there is no access to other administration pages. The codes page is also used when the ticket printer GIS-TP1 is used with the gateway.

Always make a note of your passwords and keep in a safe place: if the admin password is lost then the Guest Internet gateway will have to be reset to factory defaults and you will have to configure the device again.



## Reboot System

The reboot system function restarts the device. Some functions may require the device to be rebooted before the changes take effect.

To reboot the device select **Reboot System** from the menu. The screen will show the page in the figure below.

### Reboot Menu Page



Click on the **Reboot** button to restart the device.

The firmware is reloaded and all interface ports are initialized using the data stored in the configuration file. The reboot procedure will be required after uploading a login page, for example. Each command will indicate if the unit should be rebooted on completion of the command so that the command takes effect.

When the device has been rebooted there will be a pause of approximately three minutes before it becomes functional again. This process is the same as cycling the power to the device.

The reboot page also has a drop down menu for 'set auto reboot'. The drop down menu permits a time to be selected to reboot the device each day (see the next page).

The auto-reboot should be selected for a time of day when no one will be using the hotspot, for example 3AM.

The auto reboot is very useful to release resources allocated by users. For example, IP's will be allocated and will only expire after the termination of the IP lease time. The auto reboot forces the release of IP leases to free up resources for new users. This feature is very useful for a hotel environment.



### Auto Reboot time selection

Internet Hotspot Gateway  
GIS-R3  
Connected to the Internet: YES

## Reboot

Click the button below to reboot, you'll be told when the reboot is complete.

The system can be set to automatically reboot at any time of the day, to set up an auto reboot simply select the time.

Set auto reboot:

- 12 am
- 1 am
- 2 am
- 3 am
- 4 am
- 5 am
- 6 am
- 7 am
- 8 am
- 9 am
- 10 am
- 11 am
- 12 pm
- 1 pm
- 2 pm
- 3 pm
- 4 pm
- 5 pm
- 6 pm
- 7 pm
- 8 pm
- 9 pm
- 10 pm
- 11 pm

© Fire4 Systems Inc, 2015. Trademarks, service marks and logos are the property of their respective owners. [Privacy policy](#) [Terms and conditions](#)

## 8: ADVANCED SETTINGS

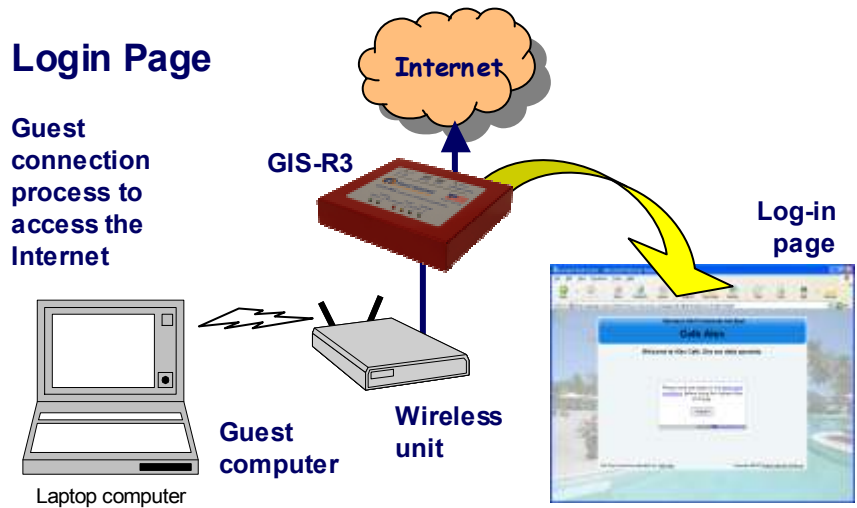
### Login Settings

The login page is a mechanism to present the Internet user with a browser page with authorization request box (sometimes called the splash page) when the user attempts to access a Web site.

When with login page is displayed on the users computer an access code can be entered if the unit is configured for controlled access. The login page also has an unlimited access mode where no access code is required to connect to the Internet, however the user has to agree to the terms and conditions of use. The user can click on a link to read the terms and conditions. This procedure offers legal protection to business owners who offer Internet hotspot access for their customers.

The unlimited access mode also has a timer that determines how long users are permitted access to the Internet: this is a feature for coffee bars that want to avoid becoming free office space.

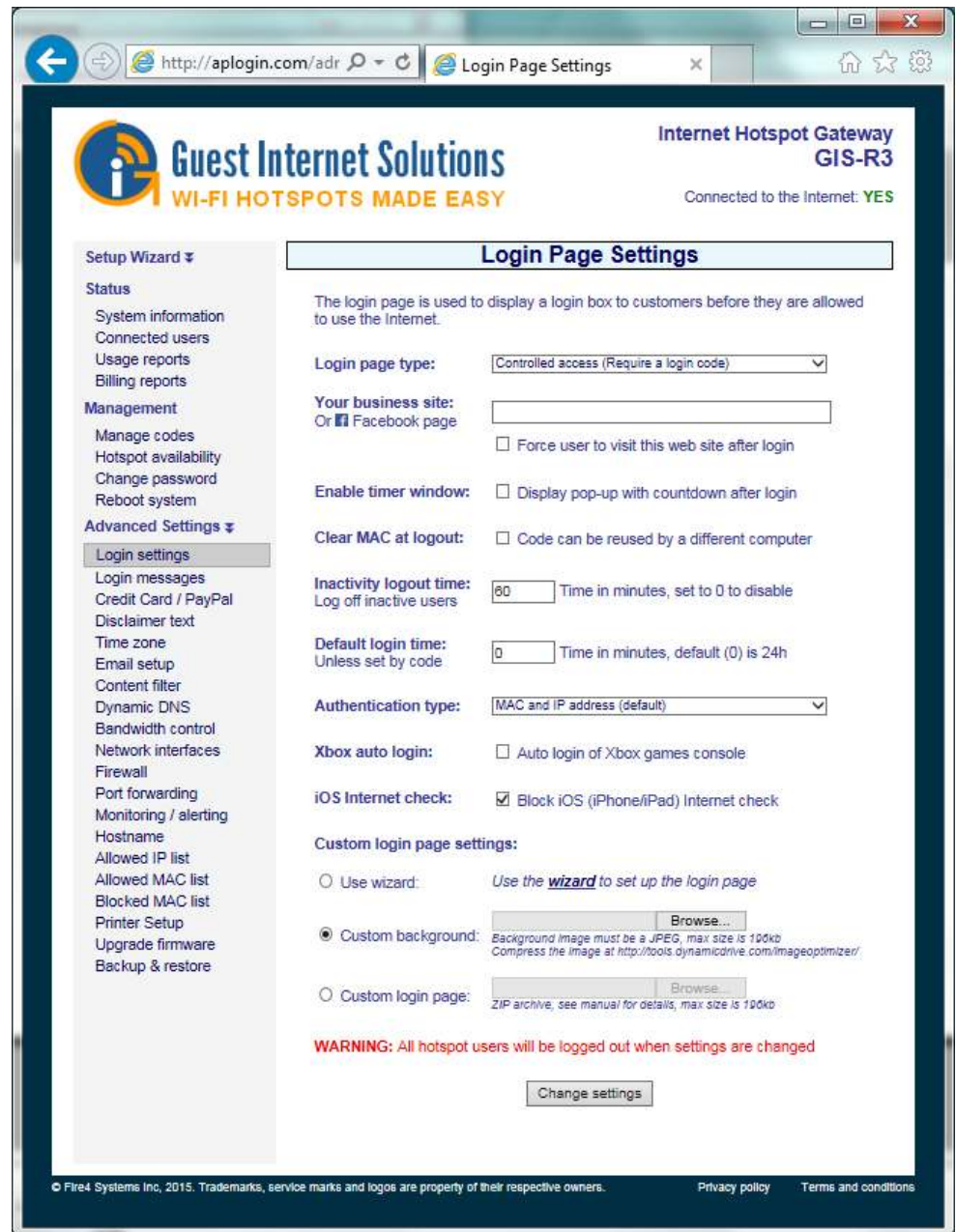
When the user opens a browser it will attempt to access the home page URL before showing the login page. When the user has completed the login process then the browser window shows the users home page. The login page is customized during the wizard setup process. The login page process is illustrated in the diagram below.



The login page design is selected during the wizard setup process. A custom login page can also be created and uploaded to the gateway. If you require help to prepare a custom login page then please email for additional information at: [info@guest-internet.com](mailto:info@guest-internet.com) as we have partners who can prepare custom login pages.

The login box displays the business owner's information that was entered during the wizard setup process. This information includes the business name, the business address, telephone number, email and website. The business website address is displayed as a link that the user can click on to see the business web page. The user can see the business web page without logging in. However the user cannot navigate away from the business web site until the login process is completed. When the login page menu entry is clicked then the page shown below will be seen in the browser window.





**Login page Menu Page Display: Controlled access is selected**

Several configuration parameters can be modified: the function of each is explained below.

- **Login page type:** The drop down menu has four options, two of which were available for selection during the wizard setup process.

**Controlled access:** shows the login page, the user has to type an access code to connect to the Internet. If credit card billing is configured then controlled access must always be selected to display the payment button.

**Registered access:** displays a request for the user to type three parameters that permit access to the Internet. The user has to provide the data requested before proceeding to the login page. The three parameters are usually name, email address and phone number. The information typed by the user is sent to the hotspot owner by email. Although the field format is verified (e.g. emails have <name>@<name> it is not possible to verify the validity of the data entered. The hotspot owner must provide an incentive to the user to type his/her information correctly. For example a restaurant can offer to send a discount voucher via email.





**Social media access:** permits the user to connect to the Internet by providing a valid Facebook login. The user is asked to authorize providing his/her Facebook profile to the hotspot operator, and on agreement the information is sent to the hotspot operator via email. The user can also be requested to 'like' the hotspot operators Facebook home page. The user can decline both requests and is then connected to the Internet for a specific period of time. Access to the Internet is not a condition of the user providing personal information.

**Unlimited access:** shows the login page, the user has to click on the disclaimer button accepting the terms and conditions.

**Open access:** permits all users to connect directly to the Internet without the login page. All firewall restrictions apply (e.g. download speed control applies). This access more is suitable for residential condominiums where a login page is not required, however firewall rules are required.

When controlled access is selected then the screen is displayed as shown on the previous page. When other options are chosen (e.g. Registered access or Social media access) then additional information is required. The following pages show any additional information required for the following login page types:

- Registered access
- Social media access
- Unlimited access
- Open access

## Registered access additional data fields

When the registered access login page is selected then more settings are displayed in a red box. Registered access data collection permits three data fields to be specified, and has the option to check the format of the data entered (there is not validity checking however). In addition to collecting the three data fields, two boxes can be checked to collect the users computer MAC address and the users web browser type. The collected information is sent to the email provided in the field below (Email sending must be configured on a different page of the menu) and the email subject can be entered to permit email readers direct the emails to a different folder. Finally a field is available for programmers who wish to write the collected data directly to a server database. Implementation of this option required the hotspot operator to program a server application that will listen for information packages and store them in a database. Note that the email settings page has to be configured before the registered access login page settings. The registered access login page settings are as follows:

- **Custom data field 1:** A label is given to this field and displayed for the user on the login page, and example for the field is 'name'.
- **Custom data field 2:** A label is given to this field and displayed for the user on the login page, and example for the field is 'email'.
- **Custom data field 3:** A label is given to this field and displayed for the user on the login page, and example for the field is 'telephone'.
- **Collect MAC address:** when the box is checked the MAC address of the users computer is recorded and included with the email containing the user-entered information.
- **Collect browser type:** when the box is checked the browser type of the users computer is recorded and included with the email containing the user-entered information.
- **Send to email:** the email address to which the information is to be sent (the email configuration settings must be completed first to specify how the email will be sent via SMTP).
- **Email subject:** type the subject line of the email that is sent to identify which gateway the message was sent from.
- **HTTP post to URL (PROGRAMMERS ONLY):** The collected information can be sent to a server, however programming skills are required to write software for the server that will receive the message and format the data.
- The registered access login page settings are shown in the figure below.



**Login page Menu Page Display: Registered access is selected, the red box shows the information that is required in addition for this mode of access**

Internet Hotspot Gateway GIS-R3  
Connected to the Internet: YES

### Login Page Settings

The login page is used to display a login box to customers before they are allowed to use the Internet.

Login page type: **Registered access (Collect Email address)**

**Registered access data collection:**

Up to 3 custom fields of data can be collected from your guest, you could for example ask for their name, email address and age. The data collected will be sent to the designated email address every time a guest logs in. You should publish a privacy policy so guests know how their data will be used.

Custom data field 1:

Custom data field 2:

Custom data field 3:

Collect MAC address:  Record guest's MAC address

Collect browser type:  Record guest's web browser type

Send data to email:   
Your email address: [Email must set up and tested on email page.](#)

Email subject:   
e.g. Data collected from Joe's Burger Bar Hotspot

HTTP post to URL:   
**Programmers only** URL to post to: (<https://myserver.com/post.php>)

Your business site:   
Or  Facebook page  Force user to visit this web site after login

Enable timer window:  Display pop-up with countdown after login

Clear MAC at logout:  Code can be reused by a different computer

Inactivity logout time:  Time in minutes, set to 0 to disable  
Log off inactive users

Default login time:  Time in minutes, default (0) is 24h  
Unless set by code

Authentication type:

Xbox auto login:  Auto login of Xbox games console

iOS Internet check:  Block iOS (iPhone/iPad) Internet check

**Custom login page settings:**

Use wizard: Use the **wizard** to set up the login page

Custom background:   
Background image must be a JPEG, max size is 100kb  
Compress the image at <http://tools.dynamicdrive.com/imageoptimizer/>

Custom login page:   
ZIP archive, see manual for details, max size is 100kb

**WARNING: All hotspot users will be logged out when settings are changed**

© Fire4 Systems Inc. 2015. Trademarks, service marks and logos are property of their respective owners. [Privacy policy](#) [Terms and conditions](#)



**Login page Menu Page Display: Social media access is selected, the red box shows the information that is required in addition for this mode of access**

Internet Hotspot Gateway  
GIS-R3  
Connected to the Internet: YES

### Login Page Settings

The login page is used to display a login box to customers before they are allowed to use the Internet.

Login page type: **Social Media access (Using Facebook)**

**Social Media access:**

Allow guests to log in to the hotspot using their social media account. Facebook users will be asked to "Like" your page and share with friends. Guests will see your updates on their Facebook page.

You will need a Facebook page to set up access using Facebook: [A Facebook page can be created](#) using your personal Facebook account.

Facebook Page:

Facebook Check: **No** Guest has 5 mins to click Like or lose access  
Check Like was clicked

Offer email login option for guests without social media accounts

Your business site:   
Or Facebook page  Force user to visit this web site after login

Enable timer window:  Display pop-up with countdown after login

Clear MAC at logout:  Code can be reused by a different computer

Inactivity logout time:  Time in minutes, set to 0 to disable  
Log off inactive users

Default login time:  Time in minutes, default (0) is 24h  
Unless set by code

Authentication type: **MAC and IP address (default)**

Xbox auto login:  Auto login of Xbox games console

iOS Internet check:  Block iOS (iPhone/iPad) Internet check

**Custom login page settings:**

Use wizard: Use the **wizard** to set up the login page

Custom background:    
Background image must be a JPEG, max size is 100kb

Use wizard: Use the **wizard** to set up the login page

Custom background:    
Background image must be a JPEG, max size is 100kb  
Compress the image at <http://tools.dynamicdrive.com/imageoptimizer/>

Custom login page:    
ZIP archive, see manual for details, max size is 100kb

**WARNING: All hotspot users will be logged out when settings are changed**

© Fire4 Systems Inc, 2015. Trademarks, service marks and logos are property of their respective owners. [Privacy policy](#) [Terms and conditions](#)



Login page Menu Page  
Display: Unlimited access  
is selected

Internet Hotspot Gateway  
GIS-R3  
Connected to the Internet: YES

### Login Page Settings

The login page is used to display a login box to customers before they are allowed to use the Internet.

**Login page type:**  
Controlled access (Require a login code)  
Registered access (Collect Email address)  
Social Media access (Using Facebook)  
**Unlimited access (Agree to disclaimer)**  
Open access (No login page)

**Your business site:**  
Or  Facebook page

Force user to visit this web site after login

**Enable timer window:**  Display pop-up with countdown after login

**Clear MAC at logout:**  Code can be reused by a different computer

**Inactivity logout time:** 60 Time in minutes, set to 0 to disable  
Log off inactive users

**Default login time:** 0 Time in minutes, default (0) is 24h  
Unless set by code

**Authentication type:** MAC and IP address (default)

**Xbox auto login:**  Auto login of Xbox games console

**iOS Internet check:**  Block iOS (iPhone/iPad) Internet check

**Custom login page settings:**

Use wizard: Use the **wizard** to set up the login page

Custom background:   
Background image must be a JPEG, max size is 100kb  
Compress the image at <http://tools.dynamicdrive.com/imageoptimizer/>

Custom login page:   
ZIP archive, see manual for details, max size is 100kb

**WARNING:** All hotspot users will be logged out when settings are changed

© Fire4 Systems Inc, 2015. Trademarks, service marks and logos are property of their respective owners. [Privacy policy](#) [Terms and conditions](#)





Login page Menu Page Display: Open access is selected

The screenshot shows the 'Login Page Settings' page for an Internet Hotspot Gateway GIS-R3. The page is titled 'Guest Internet Solutions WI-FI HOTSPOTS MADE EASY'. The left sidebar contains a navigation menu with categories: Setup Wizard, Status, Management, and Advanced Settings. The 'Login settings' option is selected under Advanced Settings. The main content area is titled 'Login Page Settings' and contains the following configuration options:

- The login page is used to use the Internet:** A dropdown menu with options: Controlled access (Require a login code), Registered access (Collect Email address), Social Media access (Using Facebook), Unlimited access (Agree to disclaimer), and **Open access (No login page)** (selected).
- Login page type:** A dropdown menu with the same options as above.
- Your business site:** A text input field.
- Or Facebook page:** A checkbox.
- Force user to visit this web site after login:** A checkbox.
- Enable timer window:** A checkbox.
- Display pop-up with countdown after login:** A checkbox.
- Clear MAC at logout:** A checkbox.
- Code can be reused by a different computer:** A checkbox.
- Inactivity logout time:** A text input field with '60' and the label 'Time in minutes, set to 0 to disable'.
- Log off inactive users:** A checkbox.
- Default login time:** A text input field with '0' and the label 'Time in minutes, default (0) is 24h'.
- Unless set by code:** A checkbox.
- Authentication type:** A dropdown menu with 'MAC and IP address (default)' selected.
- Xbox auto login:** A checkbox.
- Auto login of Xbox games console:** A checkbox.
- iOS Internet check:** A checkbox with 'Block iOS (iPhone/iPad) Internet check' checked.
- Custom login page settings:**
  - Use wizard:** A radio button with the text 'Use the wizard to set up the login page'.
  - Custom background:** A radio button with a 'Browse...' button and the text 'Background image must be a JPEG, max size is 100kb. Compress the image at http://tools.dynamicdrive.com/imageoptimizer/'.
  - Custom login page:** A radio button with a 'Browse...' button and the text 'ZIP archive, see manual for details, max size is 100kb'.

A red warning message states: 'WARNING: All hotspot users will be logged out when settings are changed'. A 'Change settings' button is located at the bottom of the settings area.

© Fire4 Systems Inc, 2015. Trademarks, service marks and logos are property of their respective owners. Privacy policy Terms and conditions



## Social media access additional data fields

The Social media access requires the hotspot operator to create a Facebook page for the hotspot business. When the guest opens the login page a request will be made to connect to the Internet using the users Facebook login. The users login information is not visible to the GIS gateway, but is communicated directly to the Facebook website. The user will be asked to share his/her profile information and can decline. If the user agrees then the profile information will be sent to the hotspot operator via email. This feature requires the email feature to be configured (see the separate menu page). The users can optionally also 'like' the hotspot operators Facebook page. If the user declines then a nominal 5 minutes of Internet access is provided. A checkbox can activate an optional login mechanism for users who do not have a social media account.

## Interactive configuration parameters

The remaining parameters that are required for the login page configuration are listed below.

- **Business Web site or Facebook page:** This is the Web site URL of the business providing Internet service. This website URL can become the *landing page* (substituting the users home page) by checking the box below to force visit to this website. When Social media login is selected this box should contain the URL of the business Facebook page
- **Force the user to visit this website after login:** checking this box will replace the users browser home page with the URL of the page explained in the previous section.
- **Enable Timer window:** checking this box will enable the pop-up timer window that the user sees after completion of the login process.
- **Clear MAC at logout:** By default an access code can only be used with one computer. By checking this box the access code can be used on many computers, tablets and smart-phones sequentially, but not concurrently.
- **Inactivity logout time:** This is a timer (shown in minutes, the default is 5 minutes) after which a user will be logged out when the user has stopped using the Internet. This feature releases resources so that more people can use the Internet service. Note that most computers have tasks that constantly connect to the Internet even when the computer is not being used. The inactivity logout time will therefore be effective when the computer is put into sleep mode (laptop screen closed) or switched off.
- **Default login time:** This timer is normally set to zero: zero means it is inactive. The timer is in minutes. This timer is used with the unlimited access and registered access modes, and will disconnect the user after the time specified. This feature is useful for a restaurant or coffee bar that prefers not to give codes for Internet access, but wants to limit the time that each user has access to the Internet, before having to login again.
- **Authentication type:** When computers are authenticated the default method is to associate both the IP address and the MAC address of the computer with the access code. In some cases it is desired to authenticate the user by IP address only (a) when it is desired to permit the user to use one access code with several devices (not simultaneously), and (b) when a wireless distribution network has been configured for guest access, however WDS is not activated for point to point links for whatever reason (in this case the MAC address is the wireless access point, not the users computer).
- **XBox auto login:** Standard configuration Xbox gaming products do not have a browser and therefore cannot log in to the network like a computer can. Checking this box will permit Xbox products to be detected and allow them to bypass the login page and connect directly to the Internet. The firewall rules apply to the Xbox however.
- **iOS Internet check:** Apple portable devices (phones and tablets) use the iOS operating system. iOS attempts to connect to the Internet when in range of a wireless network. Checking this box will block iOS access to the Internet.





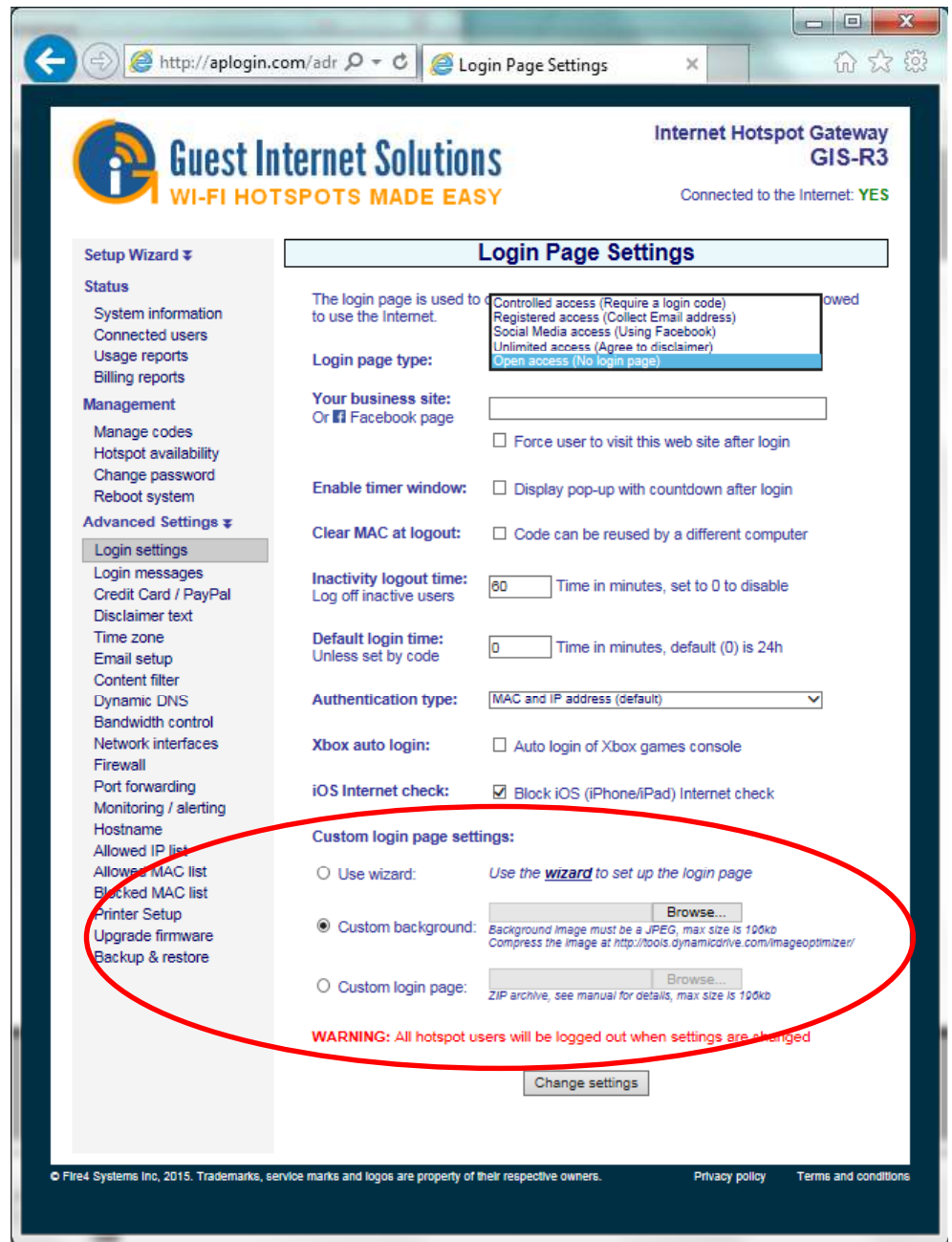
## Custom login page settings

There are three custom login page options available:

- The wizard selects 1 of 12 backgrounds during the setup process
- A custom JPG background can be uploaded
- A custom login page can be programmed using HTML

Additional details explaining the login page configurations are provided in the following sections.

Select the login page background, and the installation of a custom programmed login page





## Using the wizard login page

The wizard login page setup has 12 background options suitable for different businesses. A thumbnail picture of each login screen was shown during the wizard setup process.

- Restaurant
- Coffee bar
- Sports bar
- Hotel
- Resort lobby area
- Marina
- Motel
- Conference center
- Resort pool area
- Business center
- Church
- Library

The login page background can be changed at any time by logging in to the unit as admin and then clicking on the setup wizard menu option. Select the 'login page branding' option and then select the desired background.

Finally save the selection by clicking on 'save setting and continue to step 4' and then on 'save settings and finish'.

## Login page custom background

A login page custom background can be created in JPG format and uploaded using this feature. The image size should not exceed 196KB, however it should be made as small as possible so that the login page loads quickly for the user. The background image will be placed behind the login information box and the image contrast will be reduced to highlight the information box. The image can be a composite photo plus logo prepared using software such as Photoshop.

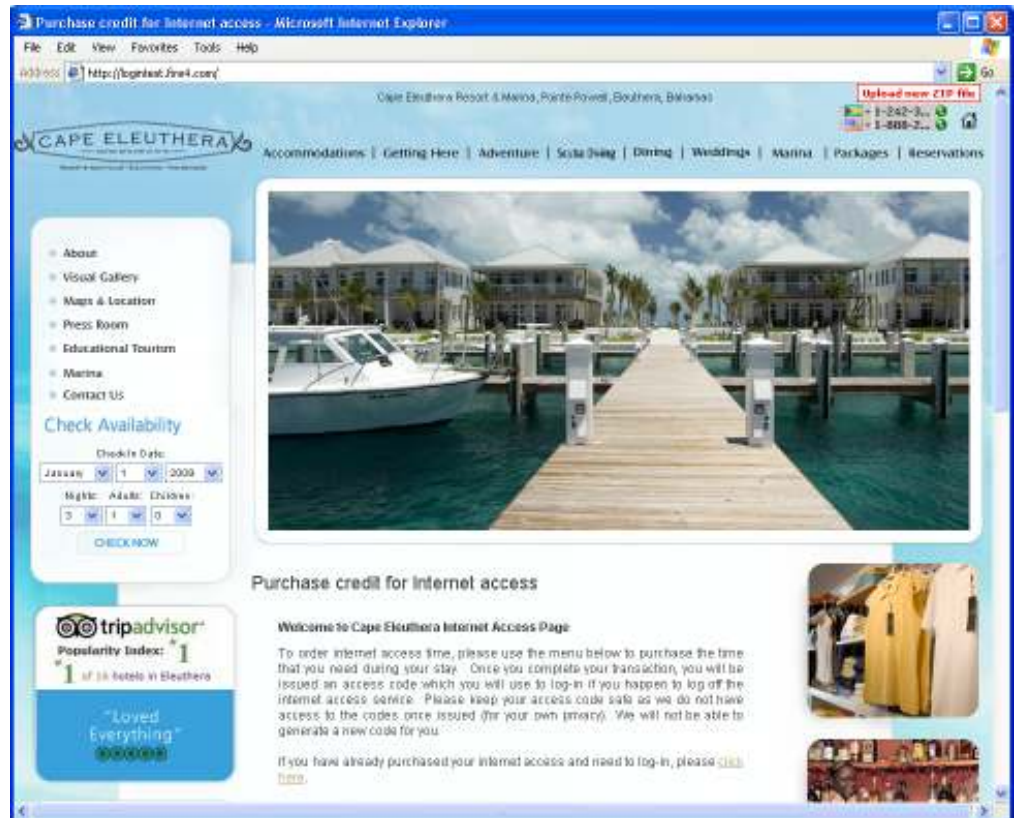
## Custom login page

A custom login page can be created using HTML code and uploaded to the Guest Internet gateway. Login page sample designs can be downloaded from the Guest Internet website at:

<http://www.guest-internet.com/loginpages>

A custom design log in page can include advertising banners. When the login page design has been prepared it can be tested using our simulator before installation. An example of a customized login page with banner advertising is shown below.

## Custom Login Page Example





The only requirement to create a login page is knowledge of programming using HTML code and Javascript. The completed program is saved as a ZIP archive (e.g. using WinZip, not the MAC zip). The login page can be customized with a logo, a corporate identity, and information about the hotspot or public Internet service.

The login page file size cannot exceed 196KB. However try to keep the file size below 50KB so that it loads quickly for the user. If your product firmware is older than 2.1r\_b14 please email technical support ([info@guest-internet.com](mailto:info@guest-internet.com)) requesting a new firmware installation. The login page is uploaded to the gateway as a single zip file, this zip file needs to contain a file called '**login.html**' (all lower case, be careful not to call the file Login.html). The login.html file must include the text shown below to locate the login box on the page.

```
'<!--LOGIN-->'
```

Login page examples can be seen in the sample login.html file which can be downloaded from

**<http://www.guest-internet.com/loginpages>**

The zip file can contain images, flash files, HTML files etc. The zip file can contain any number of directories and files; the files will be uncompressed by the gateway during initialization. The directory structure in the zip file will be maintained when the files are unzipped. The file **login.html** works as the index page; any HTML pages linked to, or from, login.html can also be seen when using the gateway.

We provide a login page zip file simulator for testing new login pages. In order to test your **login.zip** file we have a server application that will emulate a gateway. If you upload your **login.zip** to this application first then you'll get feedback about any issues. To access the application go to:

**<http://logintest.guest-internet.com/>**

User: **test** Pass: **logintest**

When you log in you will see a red box in the top right hand corner, click on this box and you will be able to upload your **login.zip** file for test. If there is a problem with your zip file the simulator will tell you, otherwise it will display the page with the login box.

When your login page has been tested you can login to the gateway admin page, click on ADVANCED SETTINGS and then click on LOGIN SETTINGS. The last option in the list is CUSTOM LOGIN PAGE. Use this option to upload your zip file.

## Creating a 'Walled Garden' login page

A custom login page can be part of a business website, with menu tabs that link to the website. All URL's used on the website must be entered into the gateway URL table. The user can navigate between the login page and the business website. However if the user tries to navigate away to another web site then the login box will be shown. This type of login page is called a 'walled garden'

An example of a 'walled garden' login page is included with the zipped file downloaded at

**<http://www.guest-internet.com/loginpages>**

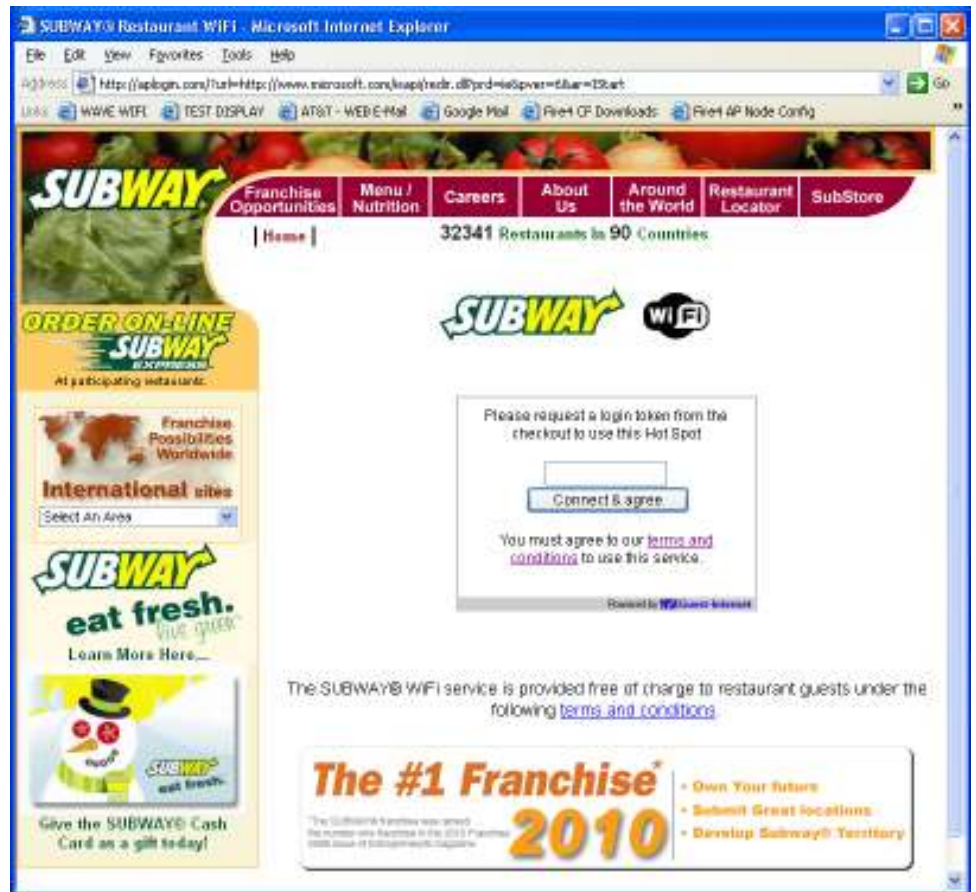
You will see two files, called **subway.zip** and **subway.txt**. Subway.zip is upoaded to the gateway as described above. Subway.txt contains a series of URL's that must be typed into the Allowed IP Address Table (see later section).

The subway.zip file is small as it uses graphic files from the company website. The menu tabs on the login page are linked to the company website. The user can navigate between the login page and the company website without having to login to the Internet: providing an access code or agreeing to the terms and conditions. However when the user tries to access any other website then the login box is presented on the screen.

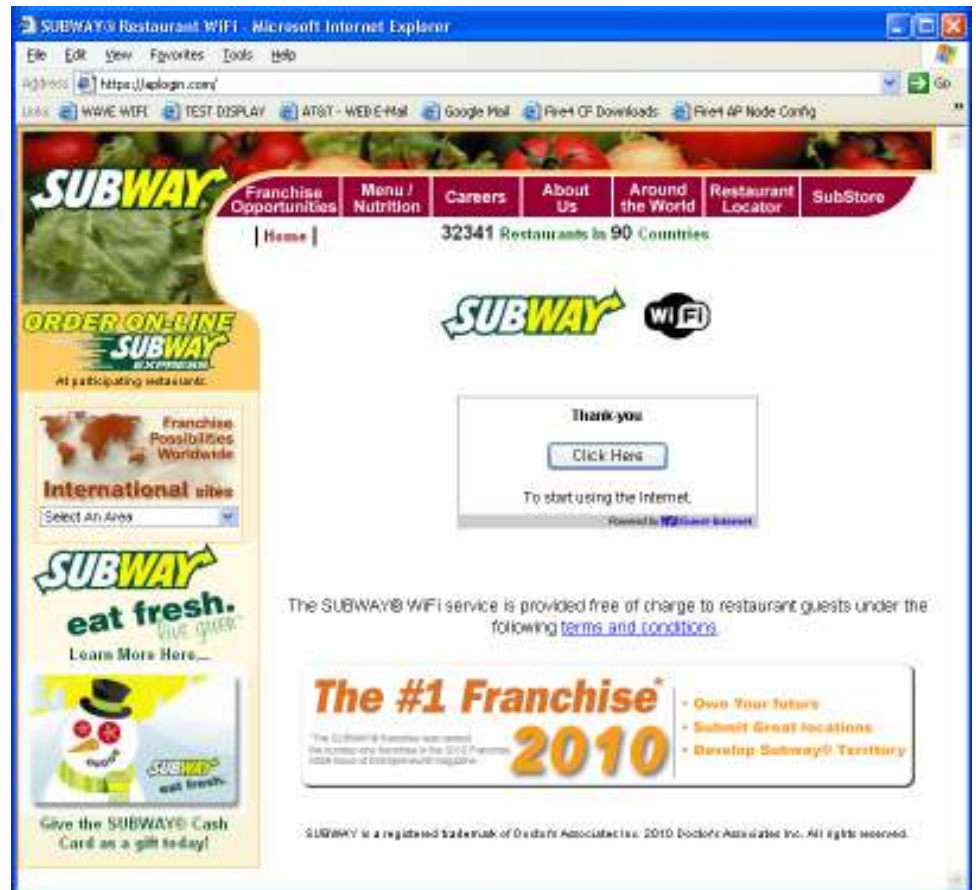
The user is able to navigate all pages in the company website because all the URL's required for this are included in the Allowed IP Address Table. This is called a 'Walled Garden'. The Walled garden login page is shown in the figure on the next page.



'Walled Garden' login page



Internet access granted page



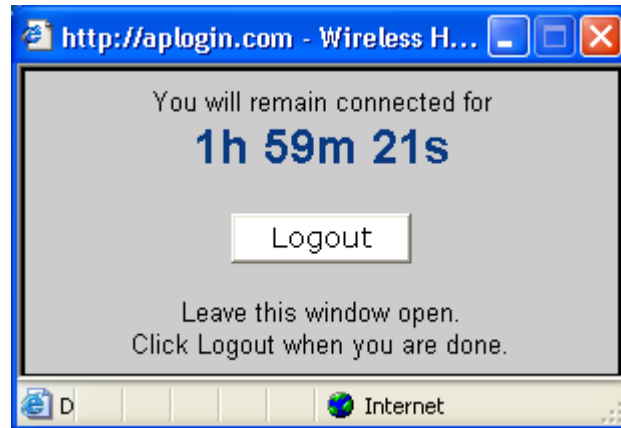




When the user types the access code and clicks on the 'connect and agree' button then the 'thank you' page appears, informing the user that the login was successful, and requesting the user to click a button to connect to the Internet.

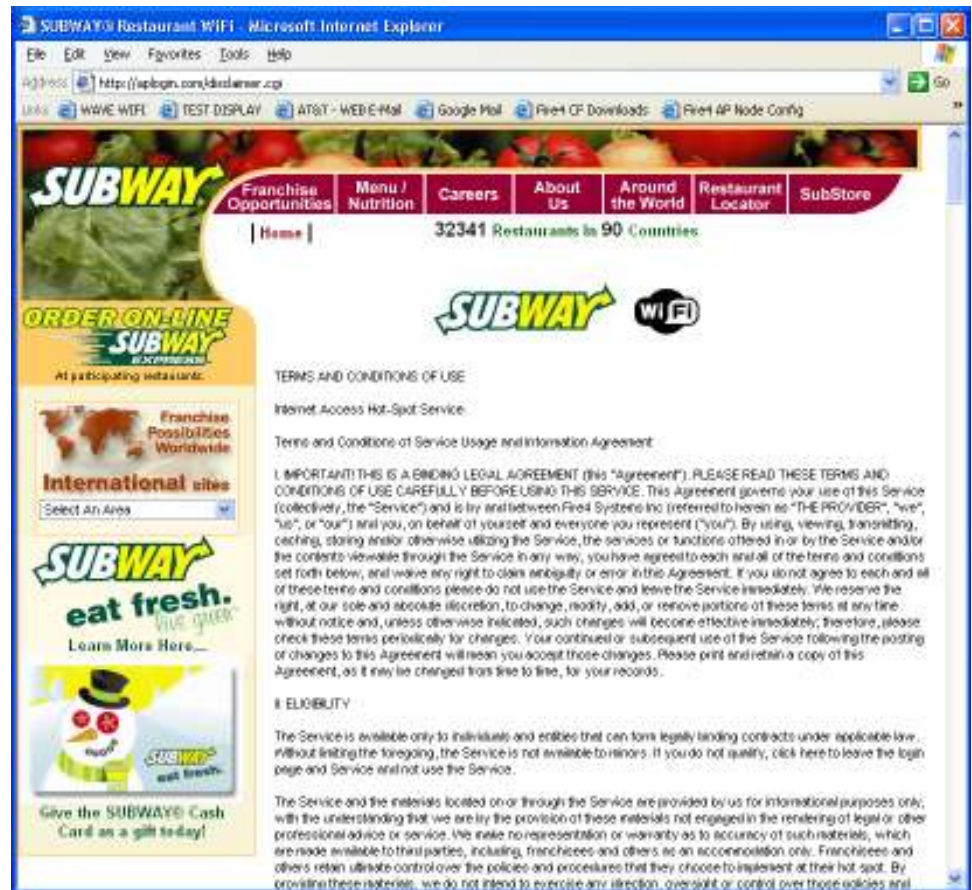
When the button is clicked to access the Internet the users Web page appears (or the landing page if set). In addition a small optional window opens (if the 'enable timer window' box is checked) indicating the time that the user has been given to access the Internet. The window also has a link to permit the user to disconnect from the Internet. This window is disabled by default. This pop-up window may cause problems with portable devices that use the iOS and Android operating systems.

### Countdown timer display



### Terms and conditions page

If the user clicks the login page link to the terms and conditions then the information appears as shown on the pages below. This information can be modified using the disclaimer editor (see the menu).

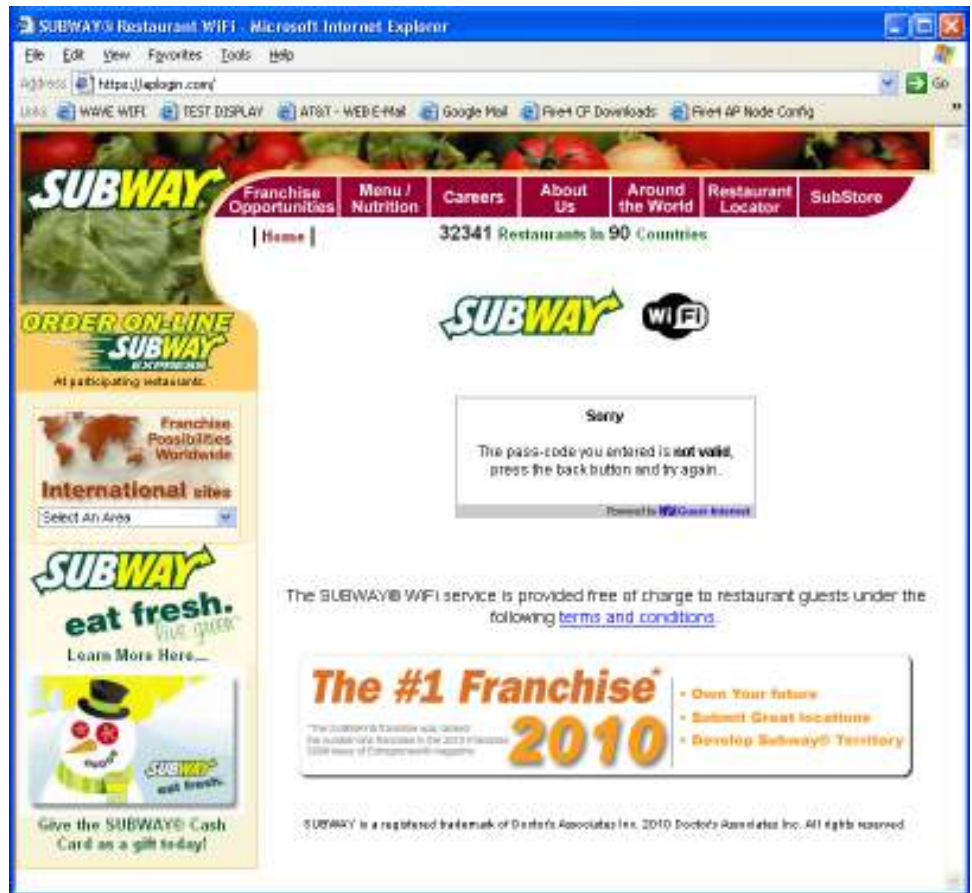






## Login code error message

If the user enters the wrong login code then a message is shown in the login box





## Login Messages

All messages displayed on the login pages can be modified. This is very useful if the hotspot is being setup in a non-English speaking country permitting interaction with the users to be in the native language.

### Login page message editor

The screenshot shows the 'Login Page Messages' configuration page in the Guest Internet Solutions web interface. The page is titled 'Login Page Messages' and is part of the 'Internet Hotspot Gateway GIS-R5+' system. The interface includes a navigation menu on the left with options like 'Setup Wizard', 'Status', 'Management', and 'Login settings'. The main content area is divided into two sections for configuring messages. The top section contains fields for 'Access Message' (Displayed at login, Login button text, Terms of usage text, Hotspot disabled), 'Login Message' (Use Internet button, Use Internet text), 'Logout Message' (When login expires, Logout button text), 'Timer Message' (Timer window text, Timer window logout), and 'Logout Message' (Text after logout, Close timer window). The bottom section contains 'Error Message' fields for 'When no Internet access' and 'Login code in use/expired'. A 'Change settings' button is located at the bottom of the configuration area. The footer of the page includes copyright information for Fire4 Systems Inc. and links to privacy policy and terms and conditions.



There are a total of 19 messages that can be modified. The messages are as follows:

- **Access message 1:** When the controlled access mode is selected this message is displayed in the login box shown on the login page. The default message reads, "Enter a login token to use this hotspot".
- **Access message 2:** This message appears on the button in the login box. The default message reads, "Connect and agree".
- **Access message 3:** When the unlimited access mode is selected this message is displayed in the login box. The default message reads, "You must agree to our terms and conditions (highlighted) to use this service".
- **Access message 4:** When the hotspot availability mode is enabled this message is displayed in the login box when the hotspot is inactive. The default message reads, "Sorry this hotspot is not enabled. Please try later".
- **Login message 1:** This message is displayed on the button in the box when the access code has been successfully entered. The default message reads, "Click here". The button is used to open the timer box.
- **Login message 2:** This message is displayed in the box below the button when the access code has been successfully entered. The default message reads, "to start using the Internet"
- **Logout message 1:** This message is displayed in the timer box when the access code time has expired. The default message reads, "Sorry, the time is up. Please purchase more time (highlighted) to continue".
- **Logout message 2:** This message is located inside the button of the timer box. The default message reads, "Logout".
- **Timer message 1:** This message is shown at the top of the timer box. The default message reads, "You will remain connected for". The time countdown is shown below.
- **Timer message 2:** This message is shown in the lower part of the timer box. The default message reads, "Leave this window open. (newline) Click logout when you are done".
- **Logout message 3:** This message is shown in the timer box after logout. The default message reads, "You have been logged out. Thanks".
- **Logout message 4:** This message is shown at the bottom of the timer box after logout. The default message reads, "Close window (highlighted)".
- **Error message 1:** The message "Sorry no Internet access, (newline) Please try later" is displayed in the login box when the Internet connector does not have a connection to the Internet.
- **Error message 2:** The message "Sorry you have been blocked, (newline) Please speak to a member of staff" is displayed in the login box when the user has been blocked due to a violation.
- **Error message 3:** The message "Sorry you have been blocked for using file sharing software, (newline) Please speak to a member of staff" is displayed in the login box when the user has been blocked due to the use of file sharing software.
- **Error message 4:** The message "There is a problem with this hotspot" is displayed in the login box when an operational error has been detected.
- **Error message 5:** The message "The passcode you entered is not valid, (newline) press the back button and try again" is displayed in the login box when the access code is not valid.
- **Error message 6:** The message "The passcode you entered is in use, (newline) Please get a new passcode" is displayed in the login box when the access code is used.
- **Error message 7:** The message "The passcode you entered has expired, (newline) Please get a new passcode" is displayed when the access code expired.



## Credit Card / PayPal (Function not available with the GIS-R2)

The credit card billing feature allows an Internet hotspot operator to sell Internet access by charging the customer's credit card. The feature requires the hotspot operator to have a valid business account with PayPal™ which is used to charge credit cards. A personal PayPal™ account cannot be used to charge credit cards. PayPal™ will require the hotspot operator to provide valid business information, including a business bank account, in order to open a PayPal™ business account.

When PayPal™ is used to charge for Internet access, users can pay with their PayPal account or a credit card. Users do not need a PayPal account to pay with a credit card.

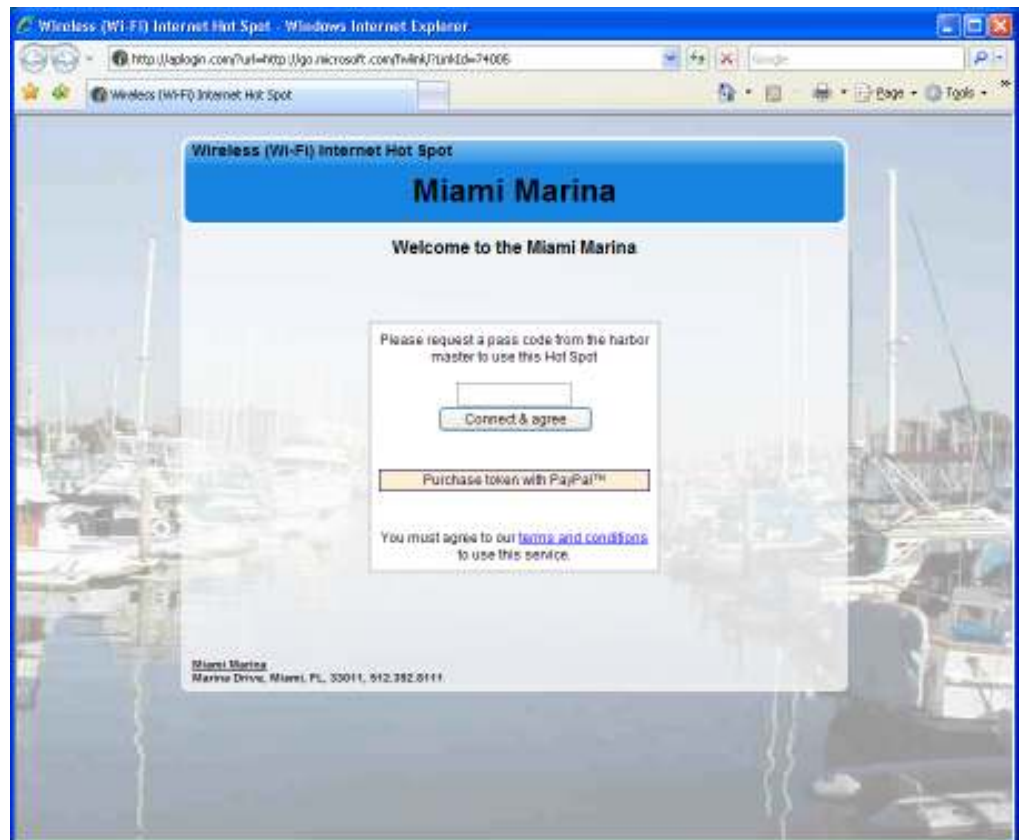
In order to comply with PCI DSS (Payment Card Industry Data Security Standards) directives, GIS products do not store any part of the credit card information provided by the user. A log is maintained that has a transaction ID. When the hotspot operator needs additional information it is necessary to log into the PayPal™ business account and use the transaction ID to obtain additional information about the transaction.

Guest Internet Solutions does not make any additional charge for credit card processing. The GIS gateway functions identically to a Point of Sale (PoS) terminal. Credit card charges are the sole responsibility of the hotspot operator, who is referred to as the 'merchant' in all transactions.

The credit card billing feature is not available on all product models. Currently it is available with the GIS-K3, GIS-R3 to GIS-R20 products.

When the credit card billing feature is activated the login page is modified to include an additional button 'purchase token with PayPal™' as shown on the screen below.

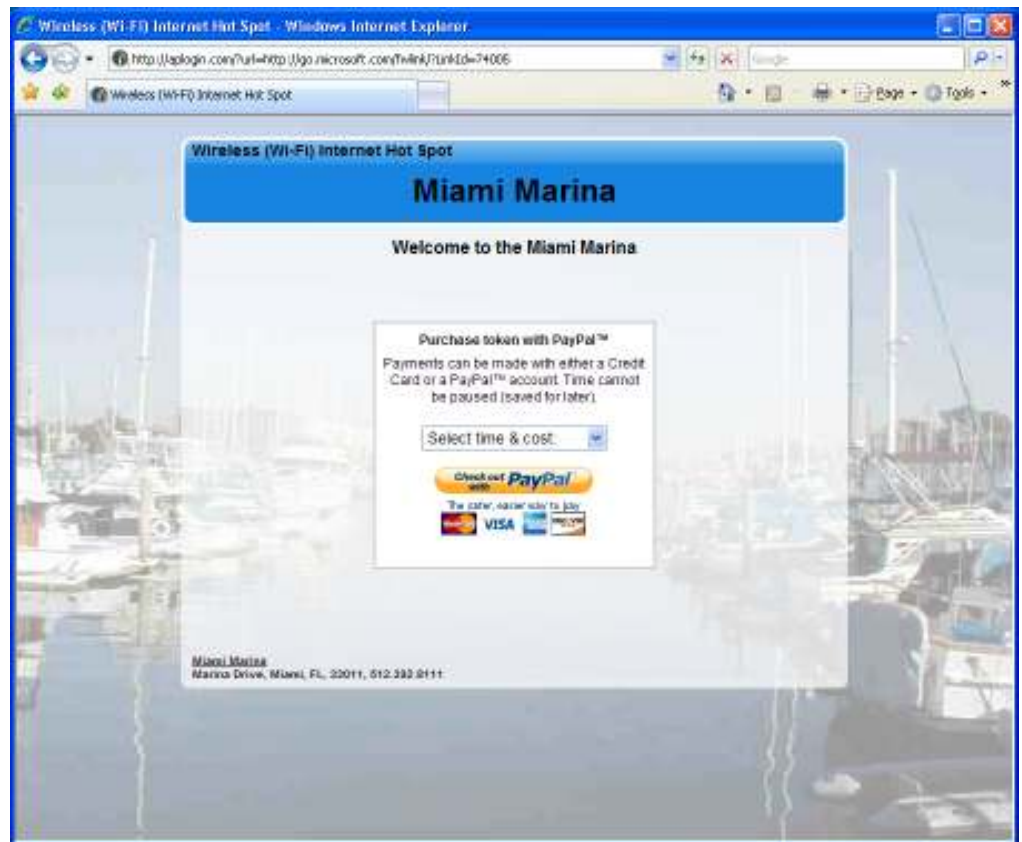
The login page has credit card billing activated. The additional button shows 'Purchase token with PayPal™'



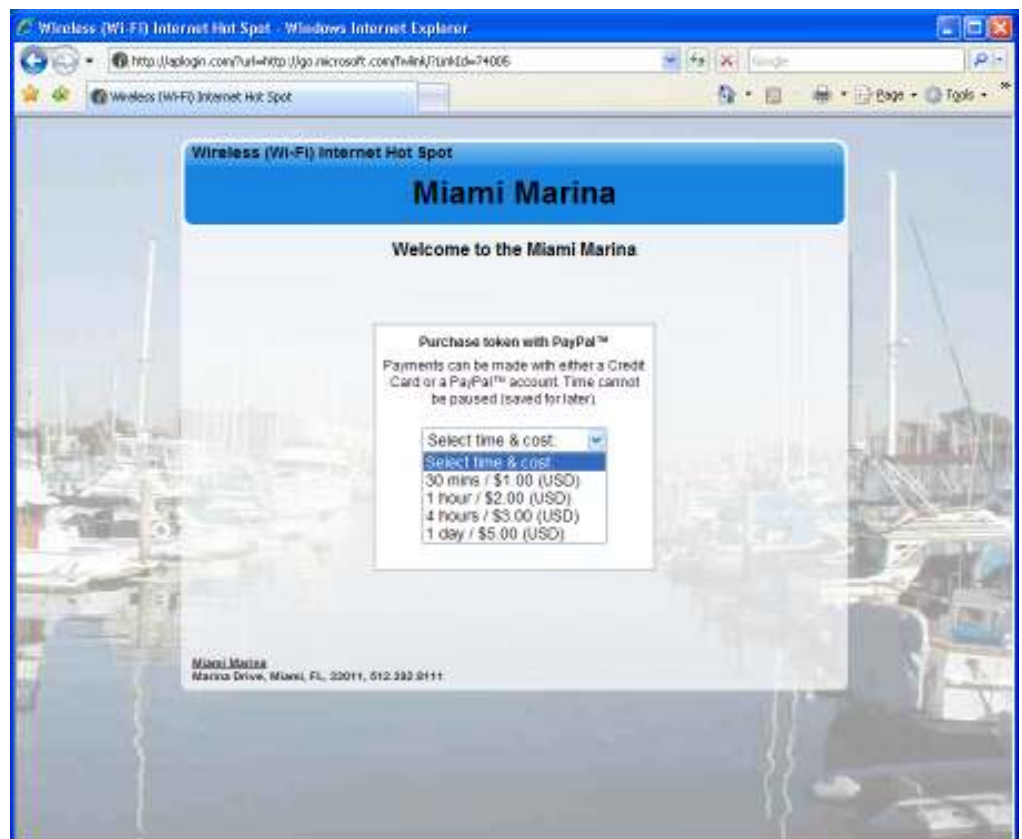




When the PayPal™ button is clicked a drop down menu is shown to select the time and cost of the Internet access. After the selection is made then the PayPal™ button is clicked



The login page drop down menu showing the Internet access options that have been configured







After the selection is made then the 'Check out with PayPal™' button is clicked. The user then sees the merchants payment page on the PayPal™ web site. Payment can be made using a credit card as shown below.

PayPal™ website credit card payment page

**Your order summary**

Description	Amount
WiFi hotspot -> 20 TEST UNIT ->	\$0.50
Item description: 20 units of Intern...	
Item price: \$0.50	
Quantity: 1	
<b>Item total</b>	<b>\$0.50</b>
	<b>Total \$0.58 USD</b>

**Choose a way to pay**  
PayPal securely processes payments for Fire4 Systems, Inc.

**Have a PayPal account?**  
Log in to your account to pay

**Pay with Bill Me Later, Debit or Credit Card**  
Pay with your debit or credit card, or with Bill Me Later

Country: United States

Bill Me Later, a PayPal service  
 Get 6 month financing on purchases of \$198 or more  
 Credit Card

Card number: \_\_\_\_\_

Payment Types:

Expiration date: mm / yy  
\_\_\_\_ / \_\_\_\_

CSC  
What is this? \_\_\_\_\_

First name: \_\_\_\_\_

Last name: \_\_\_\_\_

Address line 1: \_\_\_\_\_

Address line 2 (optional): \_\_\_\_\_

City/State: \_\_\_\_\_

ZIP code: \_\_\_\_\_

Telephone: 555-555-1234  
\_\_\_\_\_-\_\_\_\_-\_\_\_\_

Email: \_\_\_\_\_

Save your information with PayPal. [What?](#)  
(Optional)

**Review and Continue**

Payments processed by **PayPal**

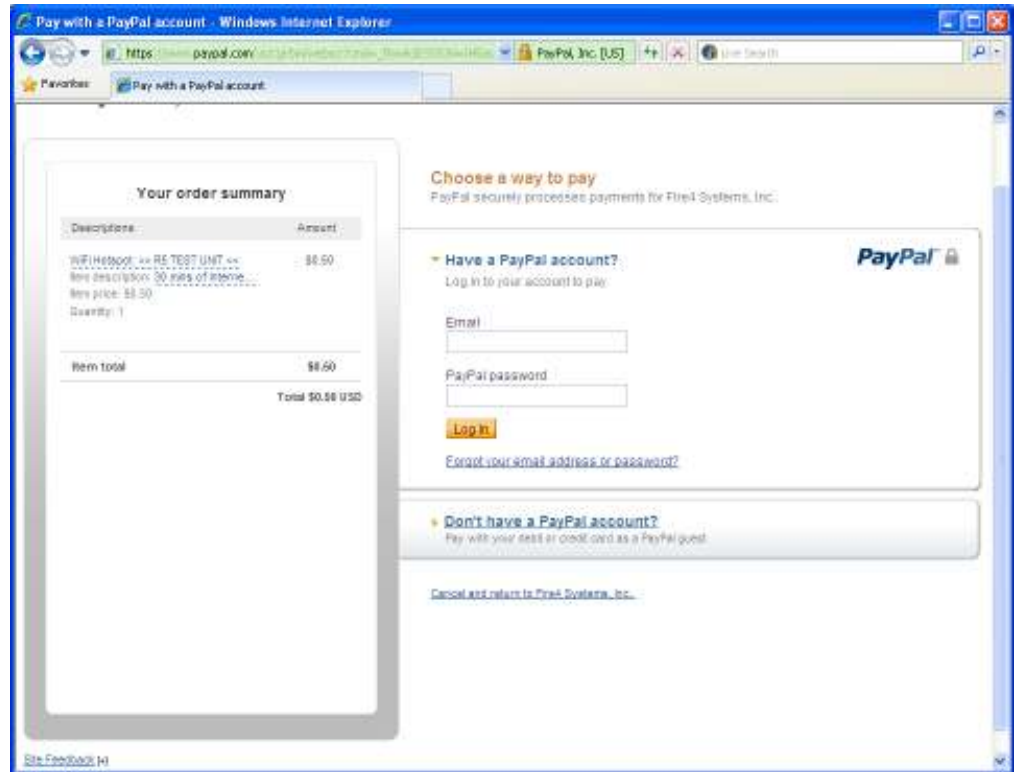
[Go back and return to Fire4 Systems, Inc.](#)

Site Feedback (0)  
PayPal. The safer, easier way to pay. For more information, read our [User Agreement](#) and [Privacy Policy](#).



Payment can also be made with a PayPal account. See the screen below.

**PayPal™ website  
payment using a PayPal™  
account**



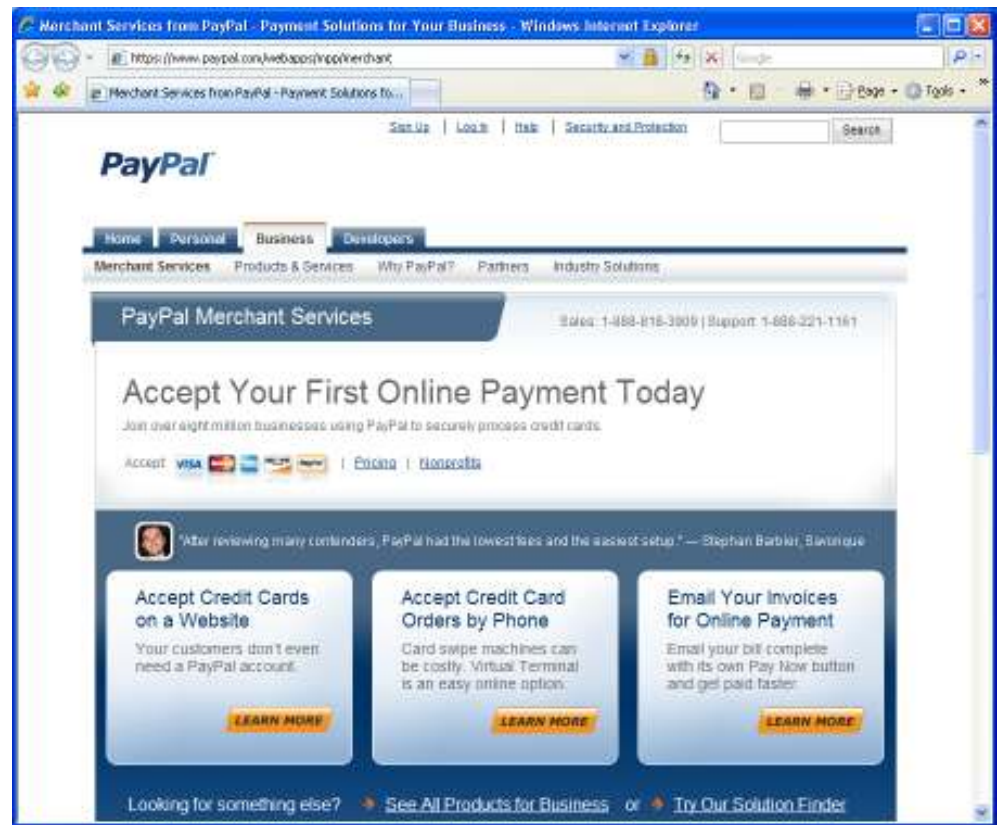
When the payment is completed then the GIS gateway displays an access code (token) for the user to note. A confirmation email is also sent by the GIS gateway to the users email address. A copy of the transaction information is also sent to the hotspot owners email address.

In the case where PayPal™ declines the transaction then the user is informed of the reason. The hotspot owner can also optionally have a message sent with information about the declined transaction.

In order to set up credit card payments the GIS customer (hotspot owner) must go to the PayPal™ website and open a PayPal™ Business account then obtain the API credentials. There is no cost to open a business account but PayPal will charge a commission on every transaction. The PayPal™ screen that is used to create a PayPal™ business account is shown on the next page.



PayPal™ website introductory page



To create an API signature with your PayPal Business account:

- Log in to PayPal, then click Profile under My Account.
- Click My selling tools.
- Click API Access.
- Click Request API Credentials.
- Check Request API signature and click Agree and Submit.

A hotspot owner name and email address must be configured for PayPal credit card billing to work. The email must be configured and tested via the Email setup page before the PayPal™ credit card processing is configured.

Go to the email setup menu page first before continuing with the billing setup





## PayPal™ credit card billing setup page

Check the box shown to enable PayPal™ payments via credit card

The screenshot shows the 'Credit Card and PayPal Payments' setup page. The sidebar menu on the left includes 'Setup Wizard', 'Status', 'Management', and 'Advanced Settings'. The 'Credit Card / PayPal' option is selected. The main content area contains the following text:

**Credit Card and PayPal Payments**

PayPal can be used to charge for Internet access. Users can pay with their PayPal account or a credit card, users do not need a PayPal account to use a credit card.

In order to set up credit card payments you must open a PayPal Business account and obtain some API credentials. There is no cost to open a business account but PayPal will charge a commission on every transaction.

Click to open a [PayPal Business](#) account and see transaction charges.

To create an API signature with your PayPal Business account:

1. Log in to PayPal, then click Profile under My Account.
2. Click My selling tools.
3. Click API Access.
4. Click Request API Credentials.
5. Check Request API signature and click Agree and Submit.

A hotspot owner name, email address and SMTP server must be set up if you want to receive customer and payment details, please set this up via the [Email setup](#) page. Customer details are not stored on this device.

Enable PayPal payments:

PayPal Business account and API settings: *Provided by PayPal*

PayPal API Username:

PayPal API Password:

PayPal API Signature:

**Payment settings:**

Time:	Cost: \$	0.00
Time:	Cost: \$	0.00
Time:	Cost: \$	0.00
Time:	Cost: \$	0.00
Time:	Cost: \$	0.00
Time:	Cost: \$	0.00
Time:	Cost: \$	0.00
Time:	Cost: \$	0.00
Time:	Cost: \$	0.00
Time:	Cost: \$	0.00

*Select the times and costs to offer to customers*

*All payments in US Dollars (USD)*

*A receipt and login code will be emailed to the customer after login*

Type of code:  Multi user codes can be shared

Purchase Prompt: (HTML may be used)

When the PayPal™ business account has been authorized then it is necessary to obtain three account parameters to copy to the boxes shown previously.

- **PayPal™ API Username**
- **PayPal™ API Password**
- **PayPal™ API Signature**

The next step is to enter up to ten time/cost parameters using the drop down menu. These are the Internet access packages that will be offered to users. The example shown on the previous page has six options that users can select. The boxes below the payment settings are the messages shown on the users computer screen to indicate success or failure of the purchase.



## PayPal™ credit card billing setup page (continuation)

be emailed to the customer after login

Time: [dropdown] Cost: \$ 0.00

Time: [dropdown] Cost: \$ 0.00

Type of code: [Single user] Multi user codes can be shared

Created after payment

Purchase Prompt: [Purchase token with PayPal&trade;]

Purchase Message: [Payments can be made with either a Credit Card or a PayPalstrade;]

Cancel Message: [The purchase has been cancelled, you have not been billed.]

Double Bill Message: [A login code purchased with your account less than an hour ago has]

Success Message: [Thank you, your account has been billed. A confirmation email has]

Login Message: [Log in using code]

Cust Email Subject: [Confirmation of Hotspot payment using PayPal]

Customer Email: [Thank you for using our hotspot. Your login code is: %c Details of payment: Value: %v]

Owner Email Subject: [Confirmation of Hotspot payment using PayPal]

Owner Email: [A payment has been made using PayPal, the details are as follows: Hotspot ID: %h Customer Name: %n Customer Email: %e]

Receive Error Emails:  With details of transaction & payment issues

Email settings must be updated before emails can be delivered

WARNING: All hotspot users will be logged out when settings are changed

[Change settings](#)

The PayPal name and the PayPal logo are registered trademarks of PayPal, Inc

© Fire4 Systems Inc, 2012. Trademarks, service marks and logos are property of their respective owners. [Privacy policy](#) [Terms and conditions](#)

Six boxes shown on the screen above have the messages that are sent to the purchasers email address, and also to the hotspot owners email address. The parameters included in the respective emails are shown.

These messages can be translated to other languages, or elaborated. It would be unwise however to change the meaning of these messages.

Two message boxes at the bottom of the page show the format of the messages sent to the customer (hotspot user) and to the hotspot owner (merchant). Take care if changing these messages.





There is a final check box called 'receive error emails'. When a transaction does not complete then it is not necessary to receive a message about this in most cases. However the hotspot owner might wish to be notified when an error condition occurs, for example if the credit card is declined. The purchaser will also receive an email notification.

Once in operation, the hotspot billing system will be the 'PoS' of a business, such as an Internet café. The hotspot owner will wish to produce accounts of the daily operations. A complete transaction record is provided by the PayPal™ business account, and the information can be downloaded and imported into popular accounting programs such as Quickbooks™.

The GIS gateway also stores a report summary, described earlier in the section: Status Functions: Billing Reports. An example of a billing report is shown on the following page. This report can be downloaded in CSV (comma separated value) format and loaded into a spreadsheet program such as Excel™.

Credit card billing report page

**Internet Hotspot Gateway GIS-R6**  
Connected to the Internet: **YES**

**PayPal™ Billing Reports**

**\$2.00** Today (so far)    **\$1.99** Yesterday    **\$18.89** This month (so far)    **\$0.00** Last month

[Download report as CSV file](#)

Date / Time	Value	Code	Transaction ID	First Login
09/28/2011 07:21	0.99	PTKYM4	5PT038063K0005-4EJ	Not Used
09/28/2011 07:26	0.99	JWY7BD	2P8243541J8510013	Not Used
09/28/2011 07:37	1.99	BFFLLW	3384000000000000000	Not Used
09/28/2011 08:15	1.00	BGLH7H	0VY379826LD9400000	Not Used
09/28/2011 08:20	0.99	WALZ5B	1E100000UR0630000	30/08/2011 10:56
09/28/2011 08:27	1.99	7FQMLD	5MC02255V67740000	Not Used
09/28/2011 08:29	0.99	MXCGWC	4B907117P9040842Y	Not Used
09/28/2011 08:31	1.00	WUJW68	08D61955UP000402K	Not Used
09/28/2011 08:35	0.99	BJHJTC	9X0000015E350700L	Not Used
09/28/2011 08:37	1.99	QNP41N	1285837857964713J	29/08/2011 11:11
09/28/2011 08:38	0.99	3B5ACW	79D52885C557500U	29/08/2011 09:33
09/28/2011 12:05	0.99	LN32HC	5SH7E244A1-603041	29/08/2011 12:04
09/28/2011 05:15			Error 1115: Missing Parameter PaymentAction: Required parameter missing	
09/28/2011 05:15			Error 1115: Missing Parameter PaymentAction: Required parameter missing	
09/28/2011 05:15			Error 1115: Missing Parameter PaymentAction: Required parameter missing	
09/28/2011 05:15			Error 1115: Missing Parameter PaymentAction: Required parameter missing	
09/28/2011 05:15			Error 1115: Missing Parameter PaymentAction: Required parameter missing	
09/28/2011 05:15			Error 10: couldn't connect to host	
09/28/2011 05:15			Error 10: couldn't connect to host	
09/28/2011 05:15			Error 10410: Invalid token (invalid token)	
09/28/2011 05:15	0.99	AADAPL	BLU05000C70031-000	29/08/2011 05:15
09/28/2011 05:15			Error 10002: Security error Security header is not valid	
09/28/2011 05:15	1.99	DW85YC	4E168964UG841542X	30/08/2011 05:57
09/28/2011 06:03	1.00	33373Q	9PC534713K746114E	30/08/2011 06:03
09/28/2011 06:06	1.00	CSG3PC	444872556K441233Z	Not Used
09/28/2011 05:15			Error 10404: Transaction refused because of an invalid argument. See additional	

© Free4 Systems, Inc. 2011. Trademarks, service marks, and logos are property of their respective owners. [Privacy policy](#) [Terms and conditions](#)

A summary of transactions for the current day, previous day, current month and previous month are presented at the top of the page.

The table rows itemize each transaction. The transaction ID code refers to the code generated by the PayPal™ business account. The transaction ID permits the PayPal™ record to be located.

No credit card information is stored on the GIS gateway to comply with the Payment Card Industry Data Security Standards (PCI DSS) requirements.



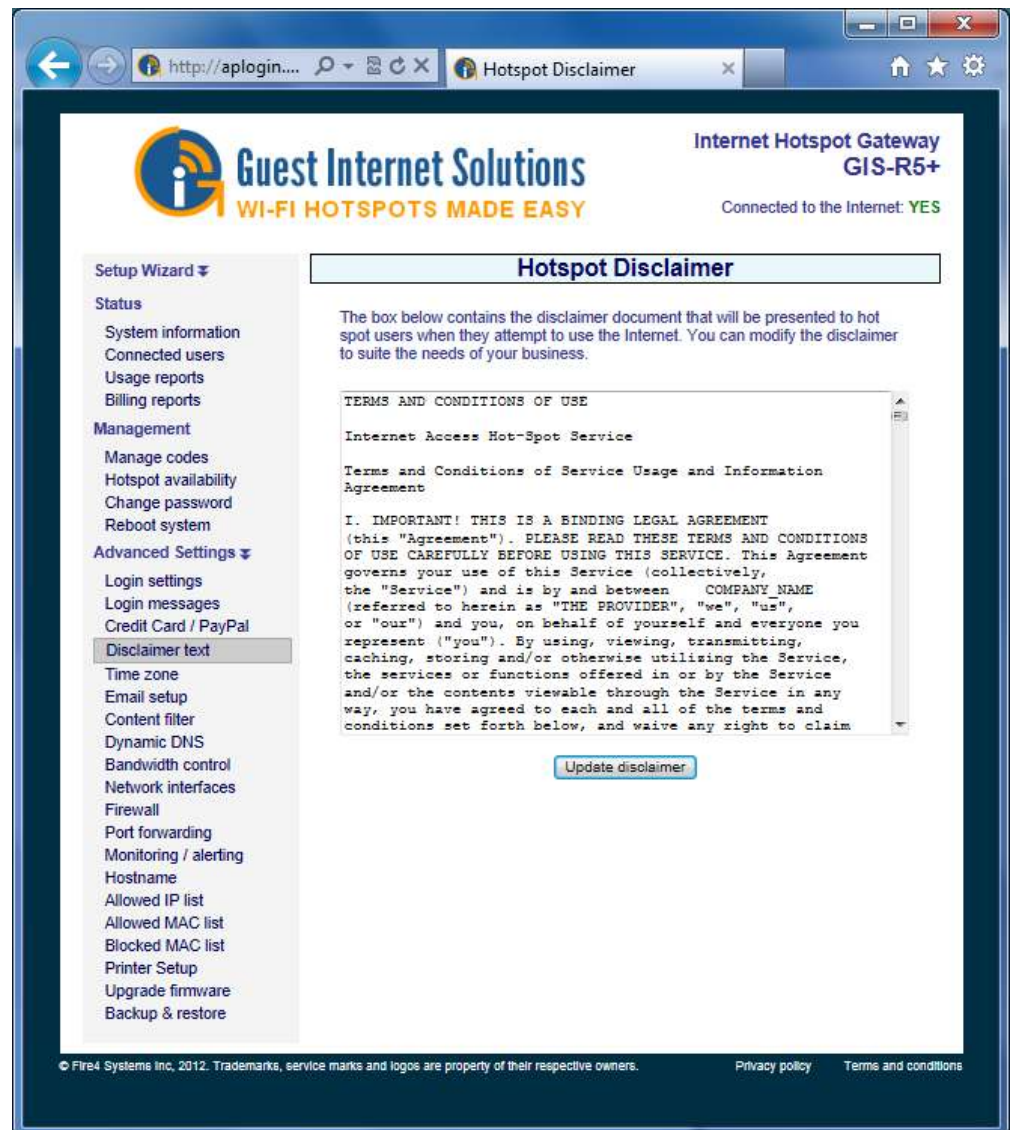
## Edit Disclaimer

When the guest connects to the Internet service he or she has to agree to the terms and conditions of use before being permitted to access the Internet.

The terms and conditions of use is a document contained within the Guest Internet unit that was drafted by a legal team to remove liability from the Internet service provider in the case that the guest is using the network for illegal purposes, such as downloading copyrighted material. The disclaimer is based on Federal laws, however each state, county and municipality can also draft laws regarding the use of the Internet. Customers outside the United States may require a completely different document.

By clicking on the **Disclaimer text** menu option an editing window opens that permits any part of the disclaimer document to be modified. The company name has already been set to the name of your business entered during the wizard setup process. Additional clauses can also be added to the document.

## Change Disclaimer menu



If you have any concerns about liability issues in your area, then please consult a specialized attorney who will help you to modify the disclaimer document, or draft a new one.

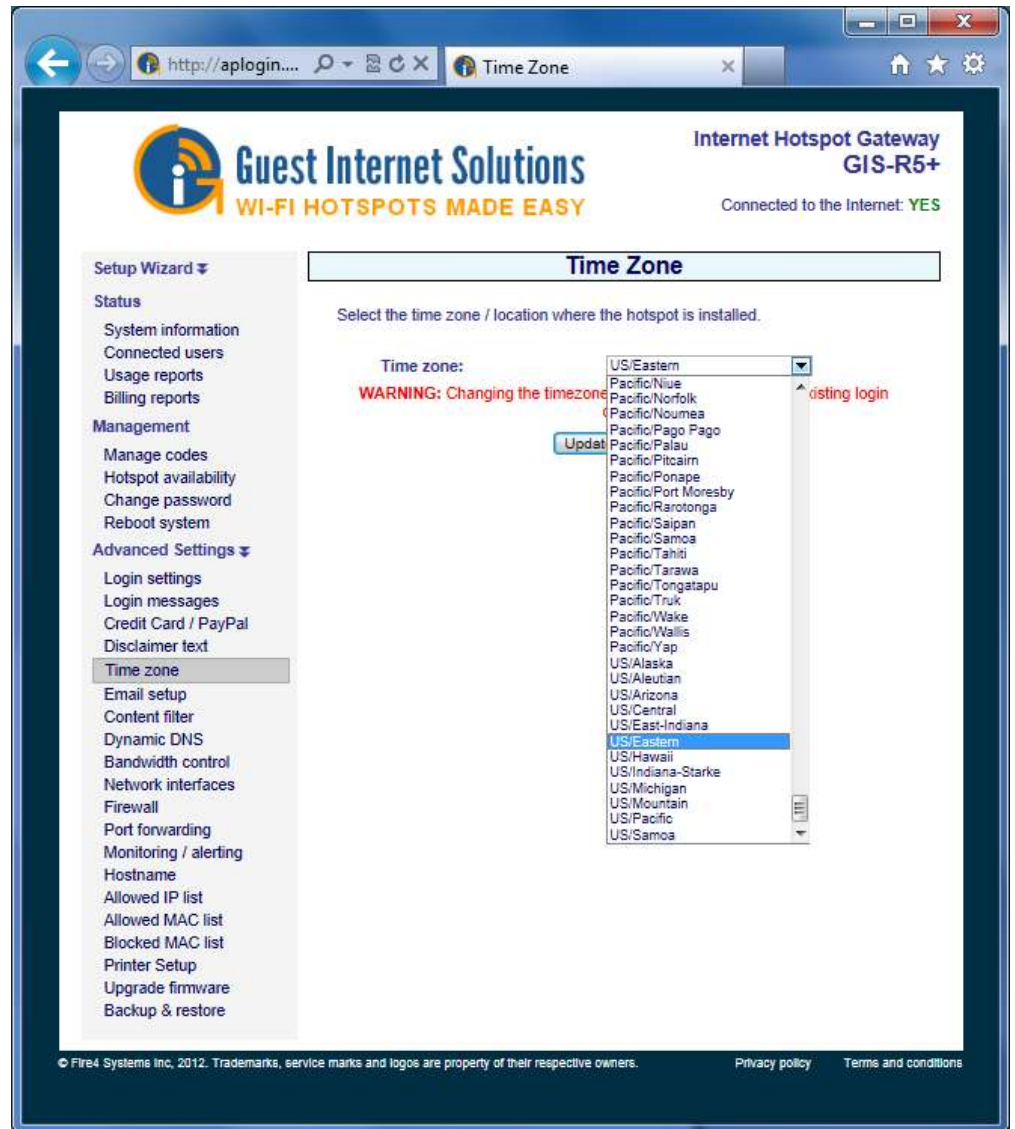


## Time Zone

The correct time zone is selected during the setup wizard. However if the gateway is moved to a different location then the time zone can be changed.

A drop down menu is used to select the correct time zone.

### Set time zone menu



Click on the correct time zone in the list to set the gateway time zone.



## Email Settings

Gateway features that require email transmission include device monitoring and credit card billing. The **Email settings** page must be configured before the email features can be used. The settings that are configured are:

- SMTP server name**
- SMTP server port number**
- SMTP username (usually not required)**
- SMTP password**
- Use SSL encryption (yes/no)**
- Hotspot owner name**
- Hotspot owner email**

### Set email menu

Internet Hotspot Gateway  
GIS-R3  
Connected to the Internet: **YES**

### Email Setup

Email setup is not necessary for the operation of the hotspot, emails are however sent from the hotspot when payment are made by credit card, when monitoring/alerting is enabled or when login notifications have been requested.

**SMTP Server:** Provided by ISP (eg mail.bellsouth.net)

**SMTP Server Port:**  (Usually 25)

**SMTP Username:** (Usually not required)

**SMTP Password:** (Usually not required)


**Use SSL Encryption:**  (Usually not required)

**Hotspot owner name:** Will appear in emails

**Hotspot owner email:** Valid email address

**Send Test Email: Check SMTP server and connectivity**

**Send to Email address:**

 Google's Gmail can be used to relay emails from this gateway. To use Gmail you will need a Gmail account. Set the **SMTP Server** to smtp.gmail.com, the **SMTP Server Port** to 587, provide your Gmail Username and Password and select **Use SSL Encryption**.

© Fire4 Systems Inc, 2015. Trademarks, service marks and logos are property of their respective owners. [Privacy policy](#) [Terms and conditions](#)

The email test feature should be used to verify that the SMTP server will transmit the email. When it is not possible to use the SMTP server of the Hotspot owner's email account then use a Gmail account to send them email.



## Content Filter

*Web content filtering* is available on GIS gateway and wireless products. Content filtering ensures that Internet surfing is family friendly. Any attempt to access sites that have undesirable content (e.g. adult sites) for viewing in public places such as hotel lobbies, libraries or schools is blocked; providing the web sites are being viewed using domain names rather than IP addresses.

Guest Internet Solutions partners with a 3<sup>rd</sup> party content filtering service, *OpenDNS*, who maintains a current list of web sites to block. *OpenDNS* has three types of accounts. A summary of the *OpenDNS* features with each type of account is shown on the following page.

- BASIC: free account
- DELUXE: \$9.95/year for households, \$5/user for businesses
- ENTERPRISE: \$2000/year for businesses

The difference between the BASIC and DELUXE/ENTERPRISE accounts is the depth and breadth of the content filtering. The BASIC account provides an excellent service and will ensure that no one is viewing adult content material in a public area. For schools and businesses where it is desirable to have comprehensive filtering then a DELUXE or ENTERPRISE account will provide excellent results and is well worth the small cost of the service. The DELUXE and ENTERPRISE accounts will block staff access to personal email and web sites such as Ebay and Facebook, avoiding loss of productivity.

For more information please go to the OpenDNS Website:

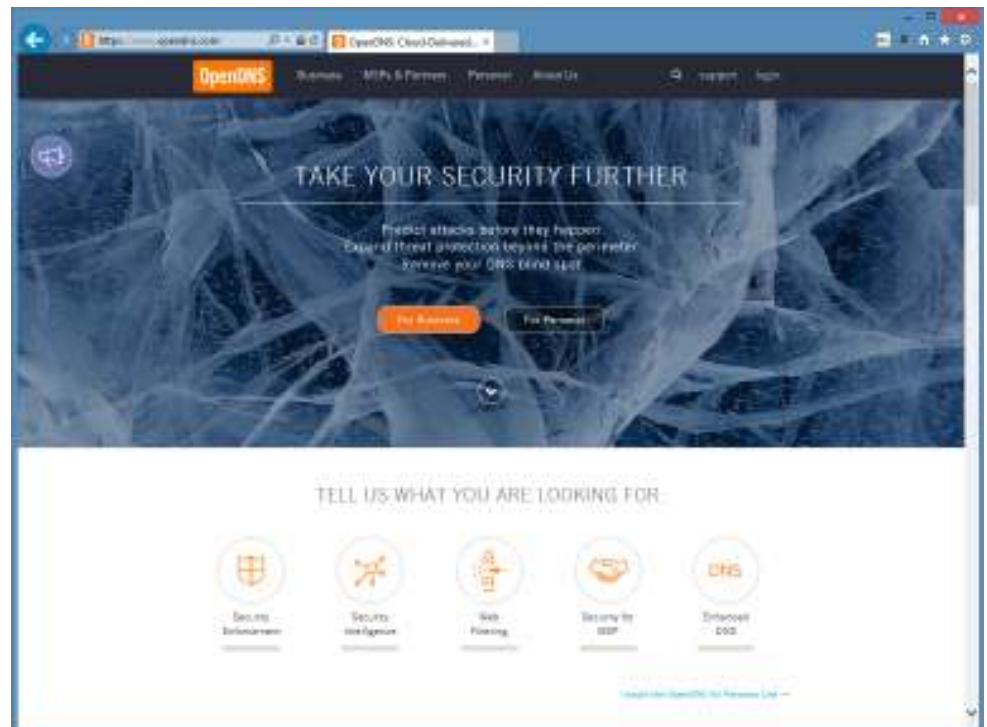
**<http://www.opendns.com/>**

Before the GIS content filtering service can be used an account must be created with ***OpenDNS*** at the website:

**<http://www.opendns.com/start/>**

Select the type of account desired. A free account can be created initially and then upgraded later according to the filtering requirements. Click on 'Sign Up' for a basic account and complete the information requested on the screen;

**The OpenDNS Website:  
select the type of account  
required and proceed to  
registration.**





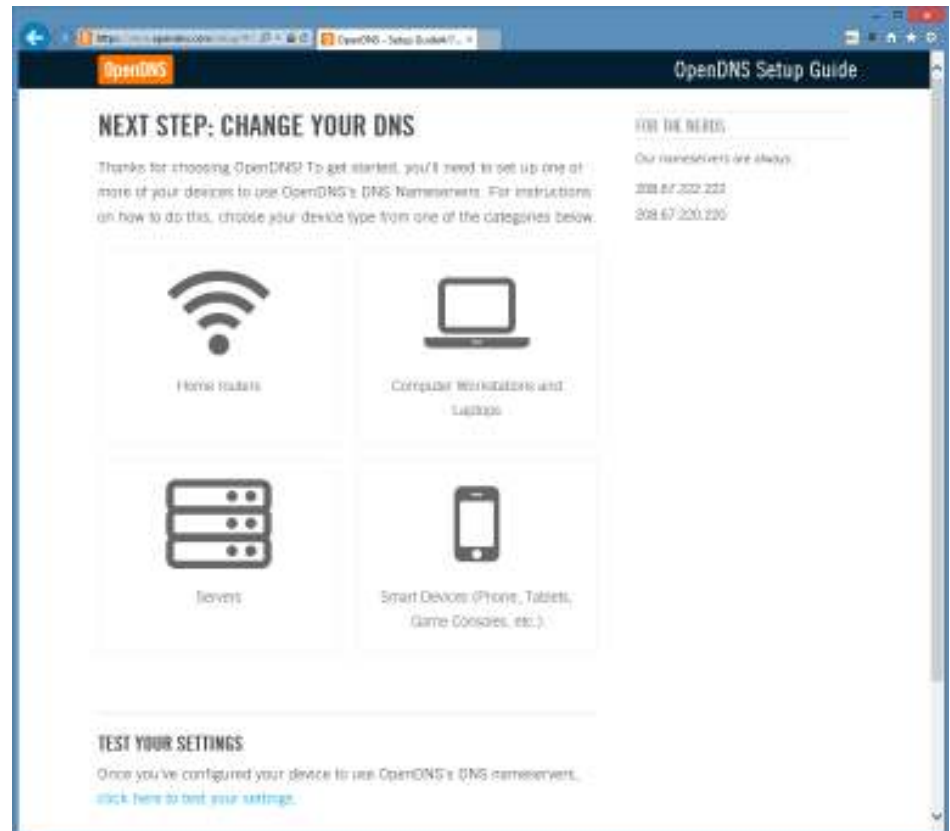


Provide your email address and password. This email and password will be required by the GIS product to use your content filtering account. Select the options 'where did you hear...' and 'where will you use...' to complete the account registration process. Finally click on CONTINUE.

**The OpenDNS account registration. Complete the information requested then click on Continue**



**The next page requests you to change the DNS address on your computer or router and test the settings. This step is not necessary with GIS gateway products as the DNS addresses are already installed in the equipment.**



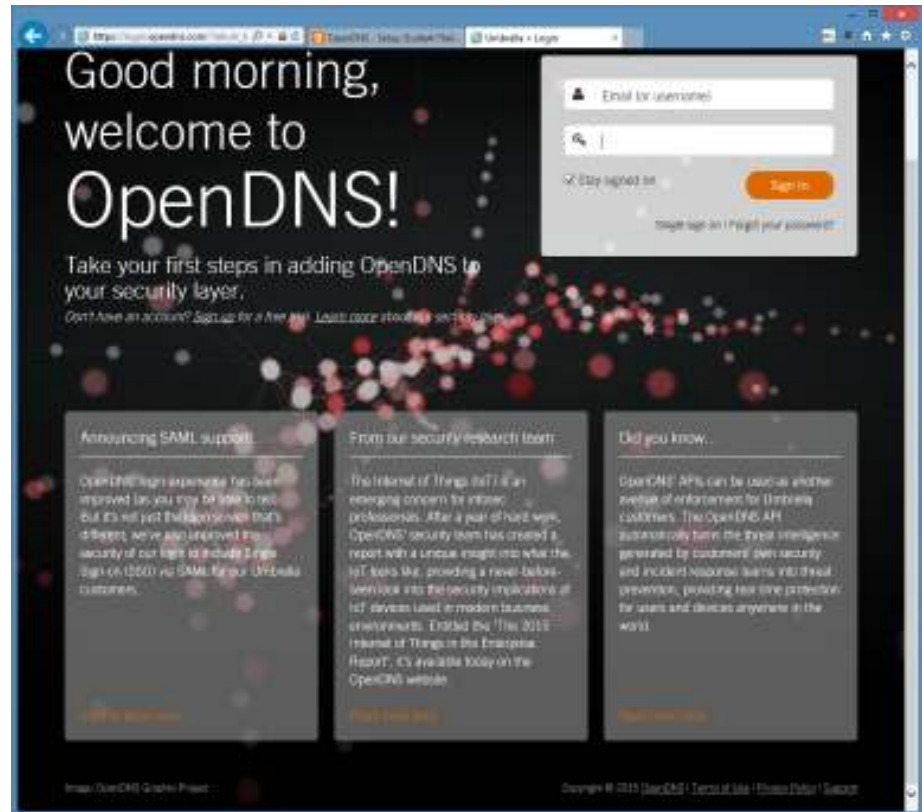


Go back to the Open DNS home page at:

**<http://www.opendns.com/>**

Click on **sign in** (top right of screen) to see the screen shown below. Login using your email address and password.

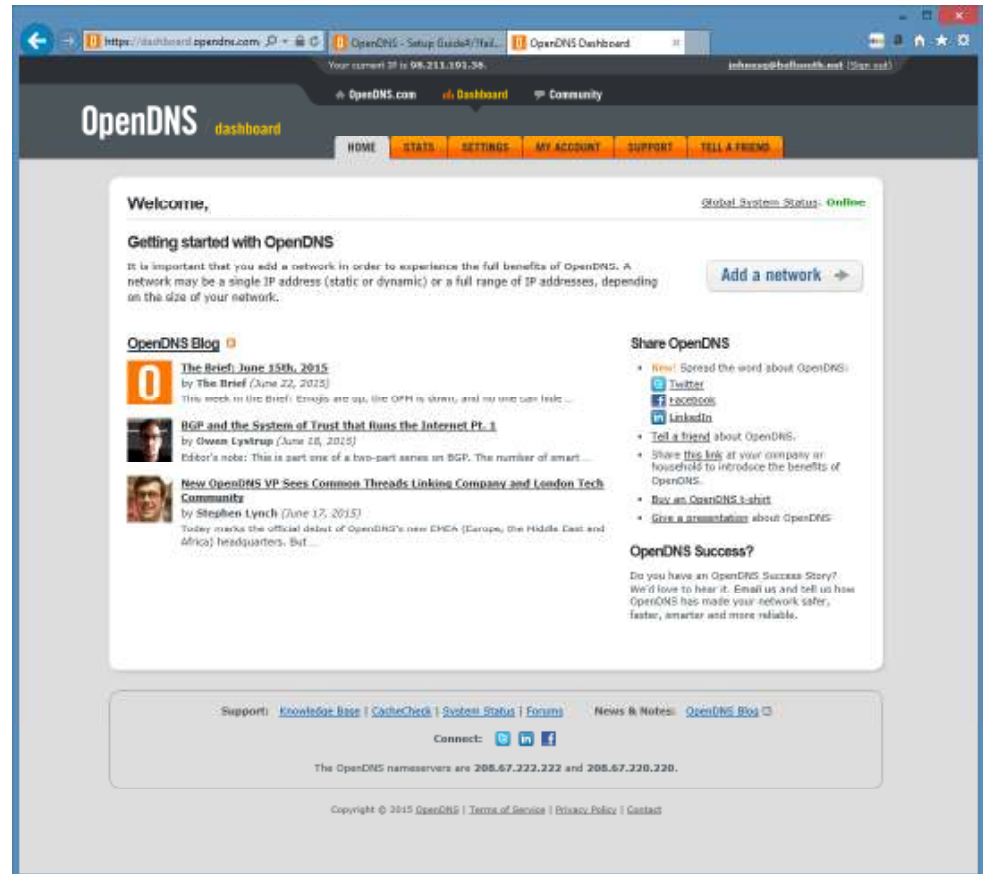
## Open DNS account login



After login you will see the OpenDNS ***Dashboard*** home page (see overleaf). Information must now be provided to begin using the OpenDNS content filtering service.

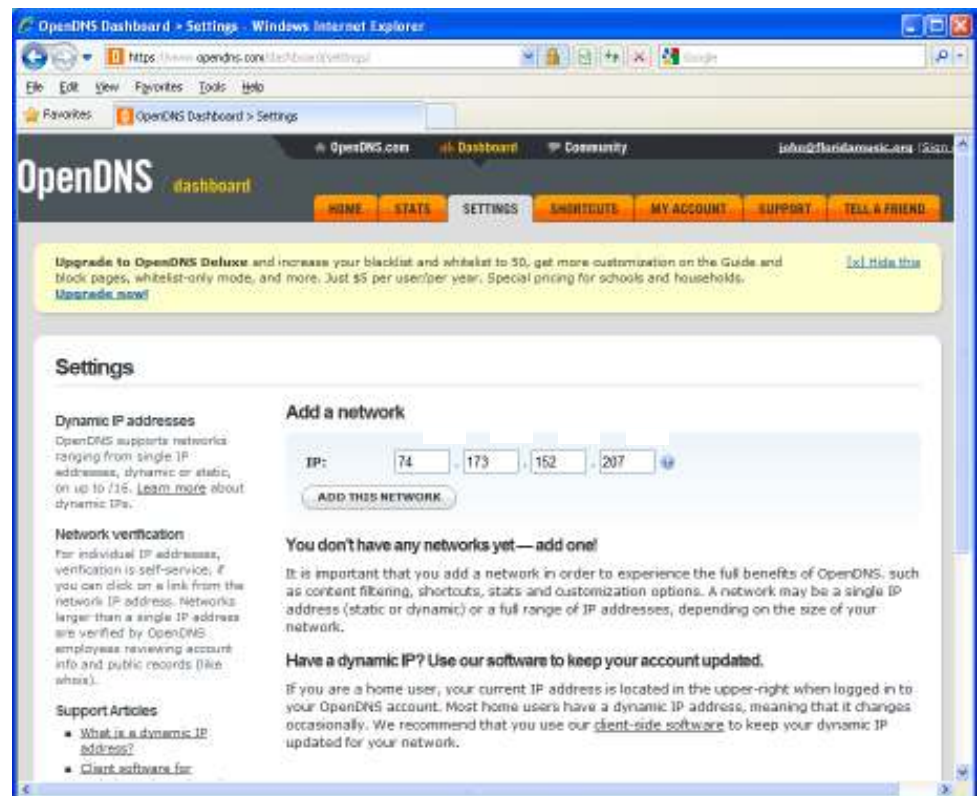


## Open DNS *dashboard* home page



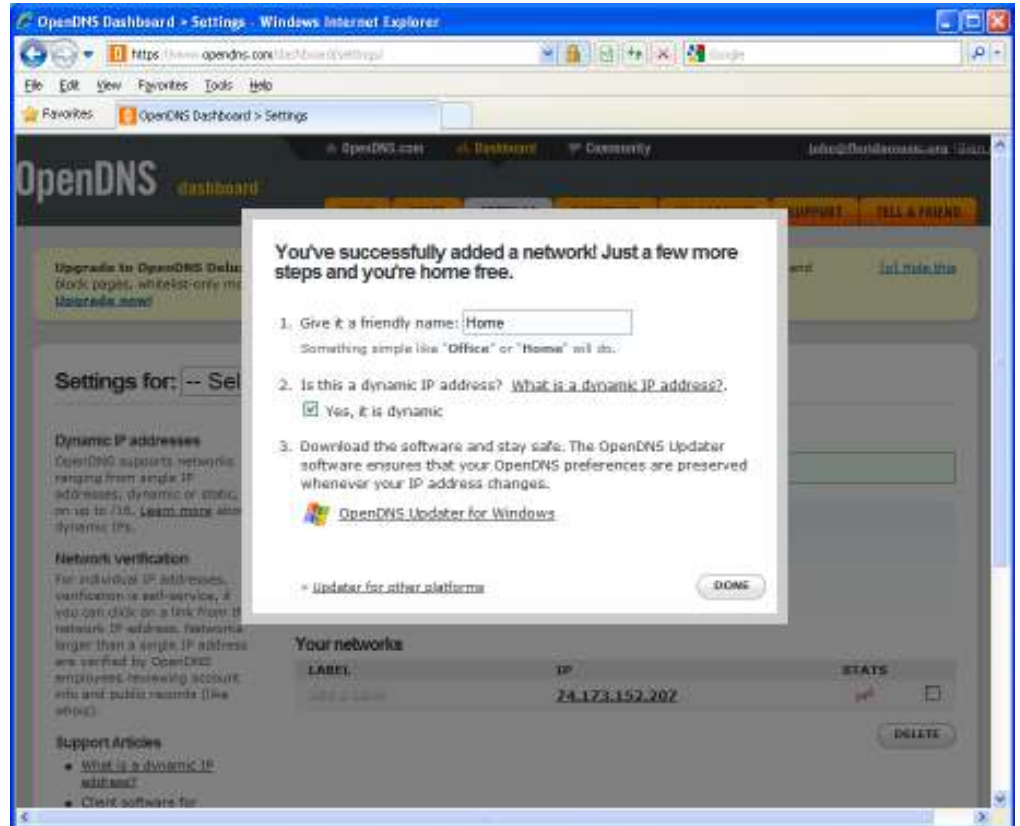
Click on the link 'Add a network'; you will see the IP address of your network.

Your network IP address must be added to you're your OpenDNS account as OpenDNS will filter all traffic from this IP address.

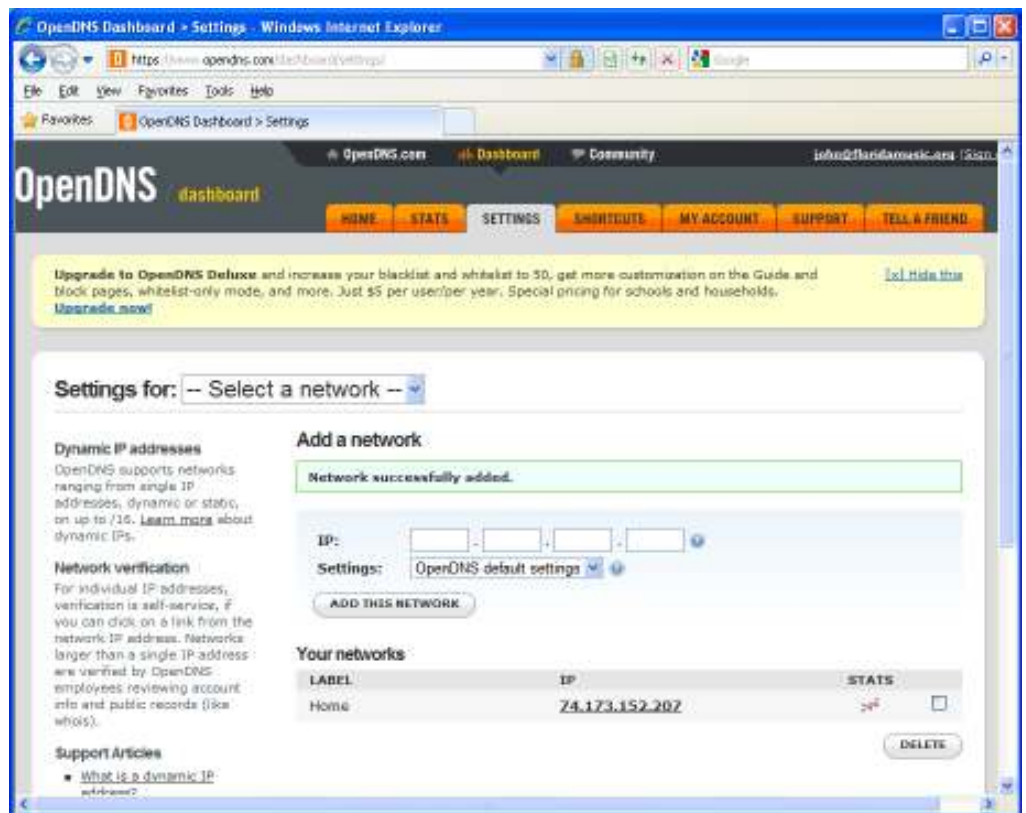




Click on the button 'Add this network', and then provide a name for the network as shown below. Check the dynamic address box for DSL or cable modem. T1 connections will be static. Finally click on the DONE button.



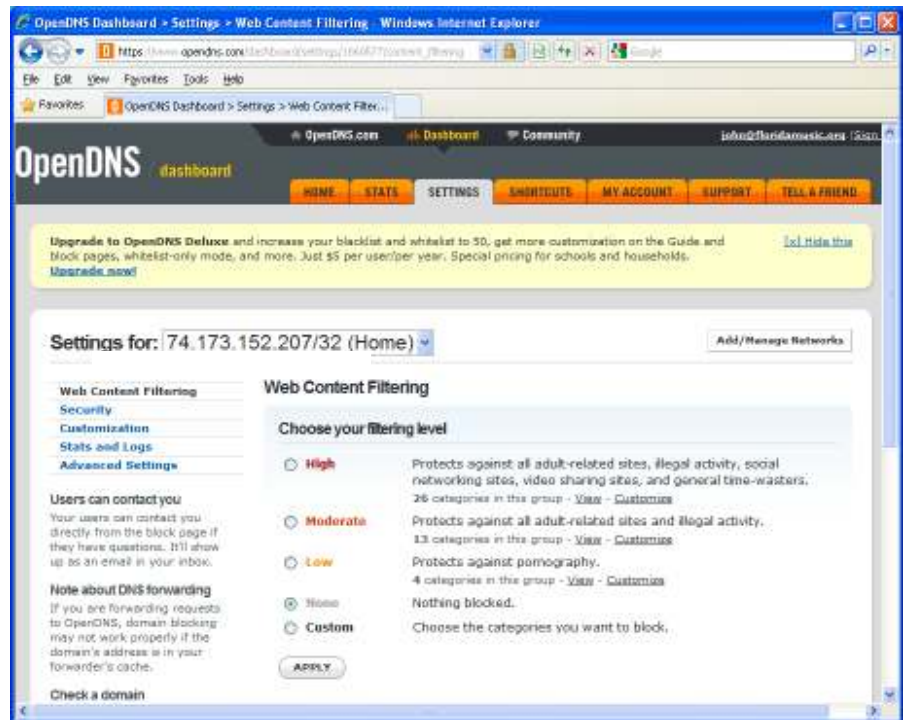
Next you will see a page showing your IP address, click on this as it is a link to the configuration page.



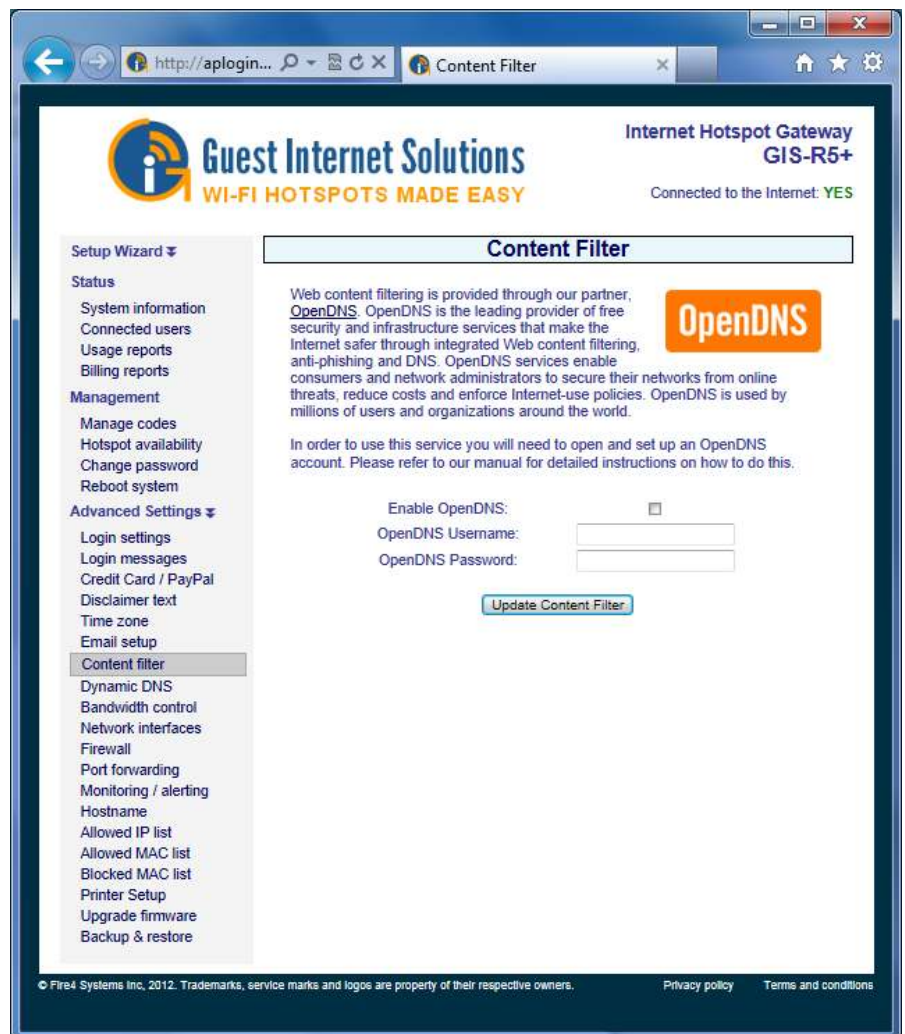




Next you have to select your content filtering level: you will see that content filtering is not active until you make your selection. Make your selection, high, moderate, low, depending on the level of content filtering you require. Finally click on the APPLY button.



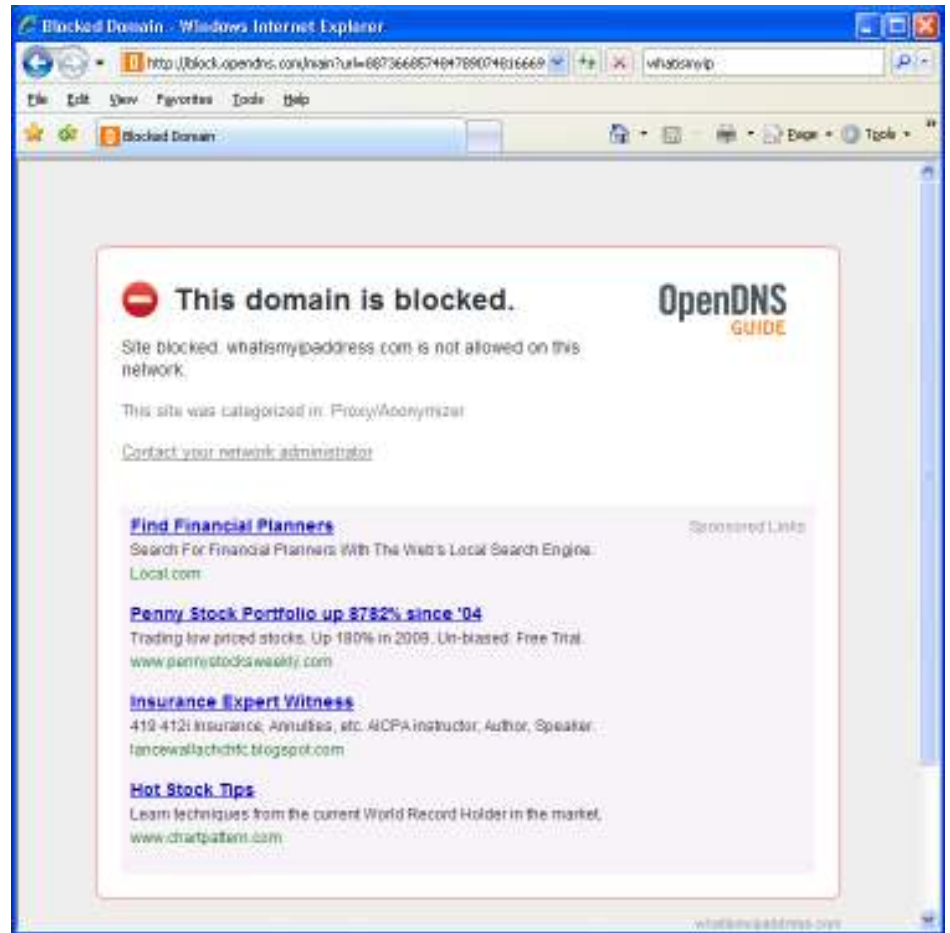
One final step remains. You must now login to the GIS product as ADMIN and select content filtering in the menu. The page you will see is shown here. Check the box to enable OpenDNS then enter your OpenDNS username and password. Finally click the 'Update content filter' button.



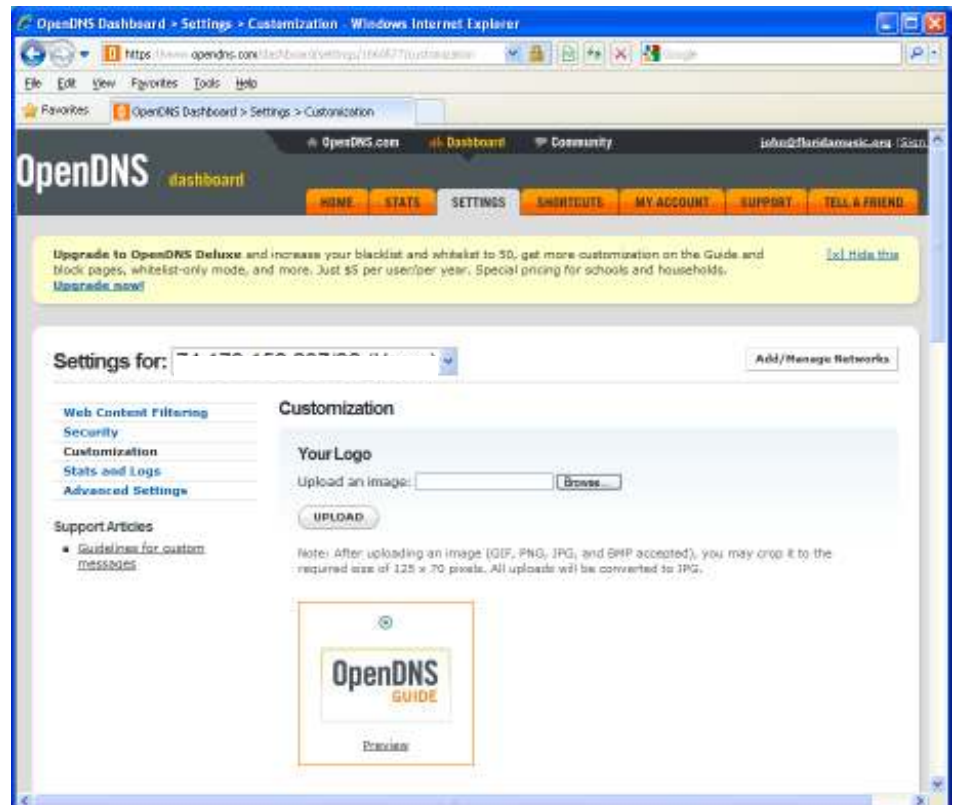




Any attempt to access a blocked site will give the page shown here.

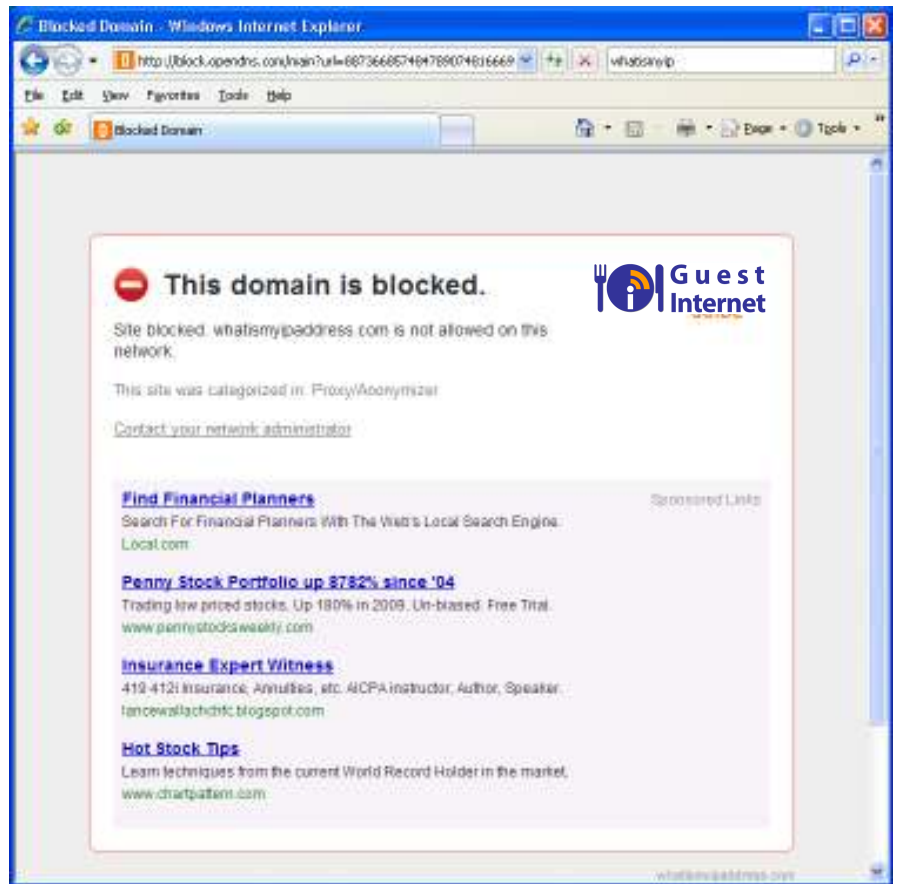


There is a configuration step that makes your content filter look professional. You can upload your business logo to the OpenDNS page shown above to personalize it for your users and guests. Click on the 'customization' message shown and upload your business logo.

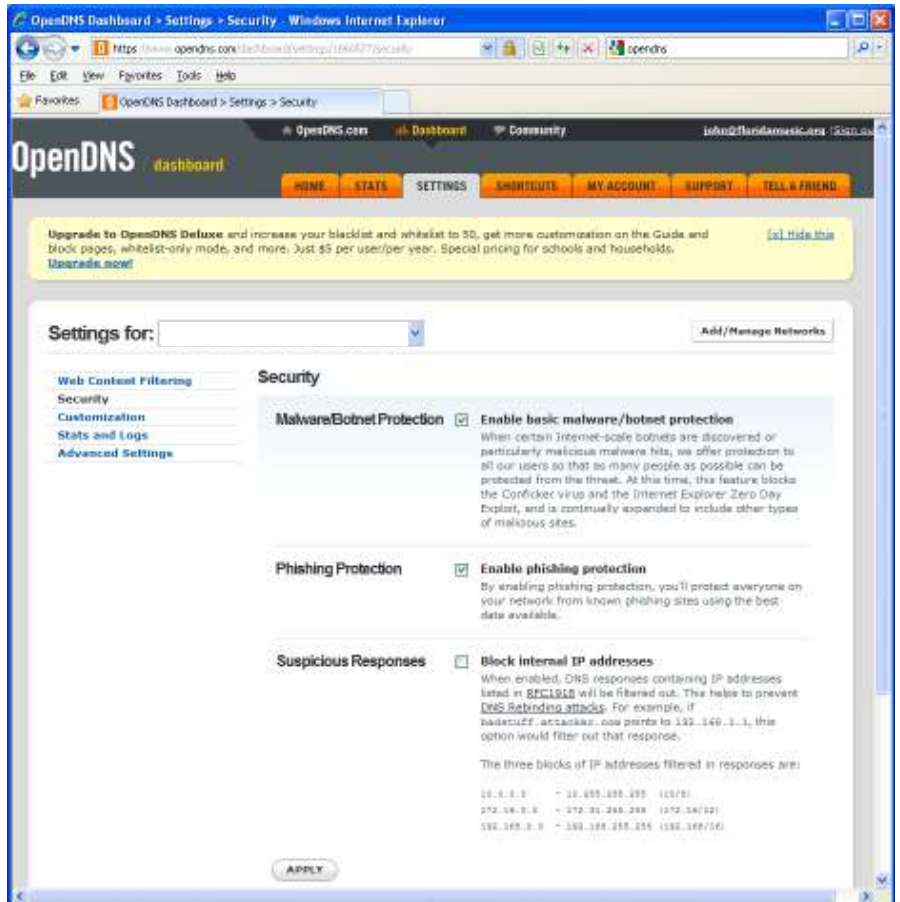




After customization your guests and users will see the page shown when they try to see blocked web sites.



Finally, you can complete your OpenDNS account information. Select the menu options SETTINGS as shown. Some settings have already been entered. Select the menu options on the left side of the screen to complete the remaining settings.





## Dynamic DNS

The Dynamic DNS is used to access the gateway remotely when the DSL or Cable Internet service has a dynamic IP address setting. The gateway is located using the services of DynDNS (<http://www.dyndns.com/>).

The **Dynamic DNS** setting requires a hostname account with DynDNS. When the box is checked to enable the DynDNS agent the DynDNS hostname, username and password must be entered.

Subsequently, the DSL or cable router can be located using the hostname URL which is resolved to an IP using the DynDNS server.

### Dynamic DNS configuration page

The screenshot shows a web browser window with the URL <http://aplogin...> and a tab titled "Dynamic DNS Update". The page header includes the "Guest Internet Solutions" logo with the tagline "WI-FI HOTSPOTS MADE EASY" and the text "Internet Hotspot Gateway GIS-R5+ Connected to the Internet: YES".

The main content area is titled "Dynamic DNS Update" and contains the following text:

Dynamic DNS is provided through our partner, [DynDNS.com](http://www.dyndns.com). DynDNS allows you to set up a hostname like *example.dyndns.org* which can be used to connect to the GIS device for remote management and monitoring.

In order to use this service you will need to open and set up a DynDNS account. Please refer to our manual for instructions on how to do this.

Below the text are three input fields:

- Enable DynDNS:
- DynDNS Hostname:
- DynDNS Username:
- DynDNS Password:

An "Update DynDNS settings" button is located below the input fields.

The left sidebar contains a "Setup Wizard" menu with the following items:

- Status
  - System information
  - Connected users
  - Usage reports
  - Billing reports
- Management
  - Manage codes
  - Hotspot availability
  - Change password
  - Reboot system
- Advanced Settings
  - Login settings
  - Login messages
  - Credit Card / PayPal
  - Disclaimer text
  - Time zone
  - Email setup
  - Content filter
  - Dynamic DNS**
  - Bandwidth control
  - Network interfaces
  - Firewall
  - Port forwarding
  - Monitoring / alerting
  - Hostname
  - Allowed IP list
  - Allowed MAC list
  - Blocked MAC list
  - Printer Setup
  - Upgrade firmware
  - Backup & restore

At the bottom of the page, there is a footer with the text: "© Fire4 Systems Inc, 2012. Trademarks, service marks and logos are property of their respective owners." and links for "Privacy policy" and "Terms and conditions".

To access the gateway remotely, the DSL or Cable router must have port forwarding enabled with a port number allocated to the GIS gateway. The port number allocated may be appended to the hostname URL to access the gateway.



## Bandwidth Control

Bandwidth control is very important for a public Internet hotspot. Many users simply want to check emails, or flight times and such browser-based applications consume little bandwidth.

However some users have applications that require a very large Internet bandwidth: such as peer-to-peer applications, sometimes-called file sharing applications (Bittorrent, Limewire, etc.), or large file downloads (music MP3's, videos). The bandwidth control prevents users with large bandwidth applications from slowing users who have low bandwidth applications by setting a maximum download and upload speed limit. Both upload and download speed limits are required because DSL is asynchronous (ADSL): the download speed available is much faster than the upload speed. Setting a very slow upload speed (32Kb/sec) is hardly noticeable by most users, however this speed slows file-sharing applications, which try to use the maximum upload speed available.

Both download and upload speeds are set by clicking on each dropdown menu and selecting the desired speeds. When the speeds have been selected then click on Change Settings for the new speeds to take effect.

### Bandwidth control page

The screenshot shows the 'Bandwidth Control' page in a web browser. The browser address bar shows 'http://aplogin.com/adr'. The page header includes the 'Guest Internet Solutions' logo and 'Internet Hotspot Gateway GIS-R3'. The main content area is titled 'Bandwidth Control' and contains the following sections:

- Default speed limits:** Download speed: Unlimited, Upload speed: Unlimited.
- Default data limits for login session:** Download limit: Unlimited, Upload limit: Unlimited.

At the bottom of the main content area is a 'Change settings' button. The footer of the page contains copyright information: '© Fire4 Systems Inc, 2015. Trademarks, service marks and logos are property of their respective owners.' and links for 'Privacy policy' and 'Terms and conditions'.





If upload and download speed settings have been selected with the access codes, then those speed settings will override the bandwidth settings on this page. This permits a slow free Internet service to be provided, while a charge can be made for a fast Internet service.

Similarly, if upload and download byte limits have been selected with the access codes, then those speed settings will override the bandwidth settings on this page.

### Setting the download and upload speed limits



The default data limits can be set for each user session. This sets a limit on the maximum number of bytes that can be downloaded and uploaded in one user session. This feature is very useful for hotspot operators who are charged for data volume by the ISP, such as the case where the backhaul circuit is a 4G wireless network.

Click on the drop-down menu bars to select the download and upload limits. Note that the limits set here will be overridden by any limits that are associated with the access code that the user enters to initiate the session.

When the settings have been selected click on the update settings button.

Bandwidth usage depends on the type of data traffic that the Hotspot users are sending and receiving over the network. Contact your broadband service provider for additional information about data charges and limits.





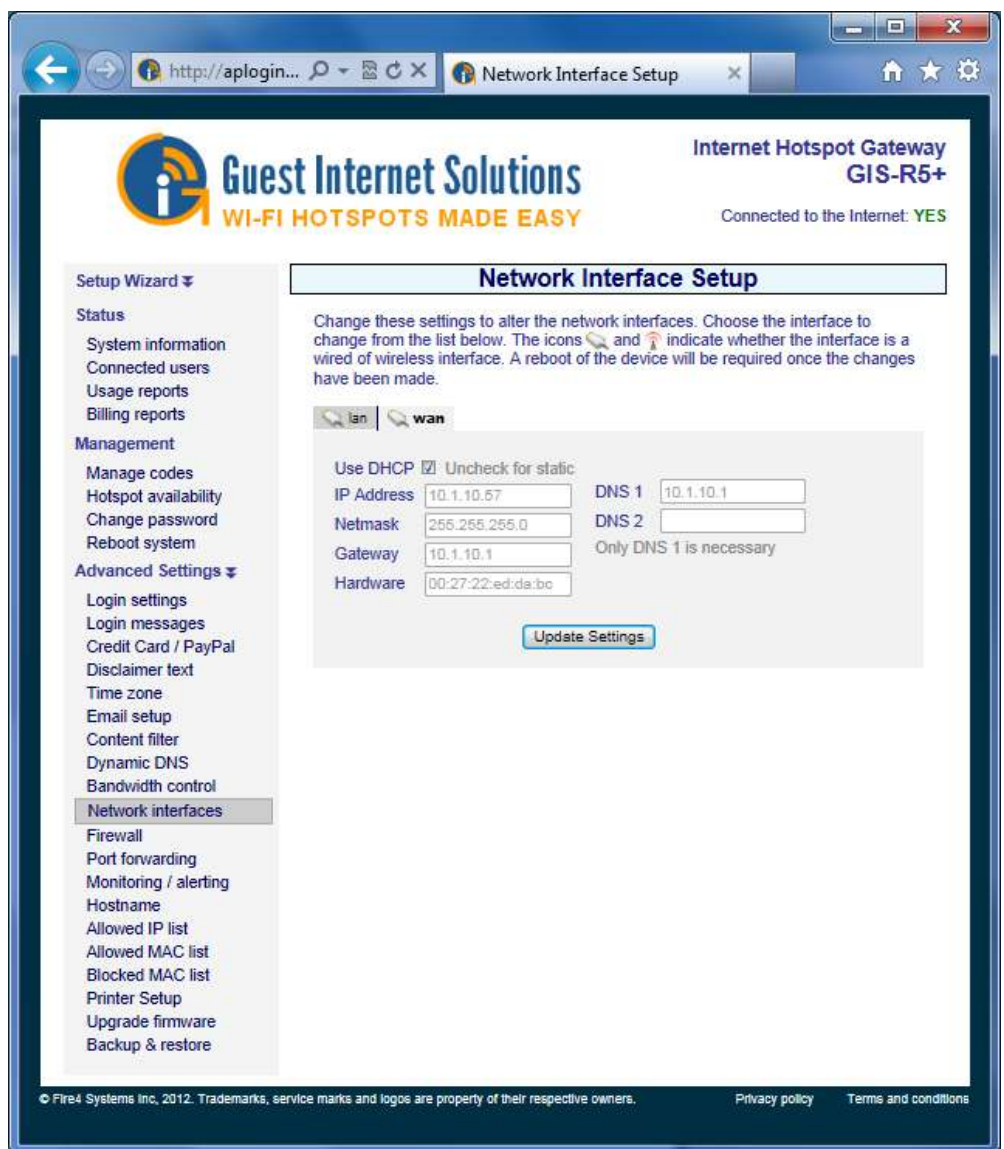
## Network Interfaces

Most network designs follow simple rules: the Internet router is a 'DHCP server' and all computers are 'DHCP clients'. Some networks however require special configurations. A T1 internet connection may require that all computers and network devices be configured with 'fixed IP addresses'. The **Network Interfaces** menu option is selected to change the device configuration for non-standard networks.

When configuring the Guest Internet product for a non-standard network configuration, the help of a network specialist may be required, as there are many configuration options. One mistake may prevent the Guest Internet product from functioning correctly. In the worst case a configuration mistake might prevent you from communicating with the Guest Internet products and you will be locked out. In this case the only course of action is to reset factory defaults and start again. If you are locked out then go to the later section of this manual.

Open the **network interfaces** page by clicking in the Network Interfaces menu line. The network interfaces page is shown below. This page may have opened during the wizard set up process if the Guest Internet unit had to be configured with a fixed IP address.

Network Interface Menu Page showing the WAN tab.

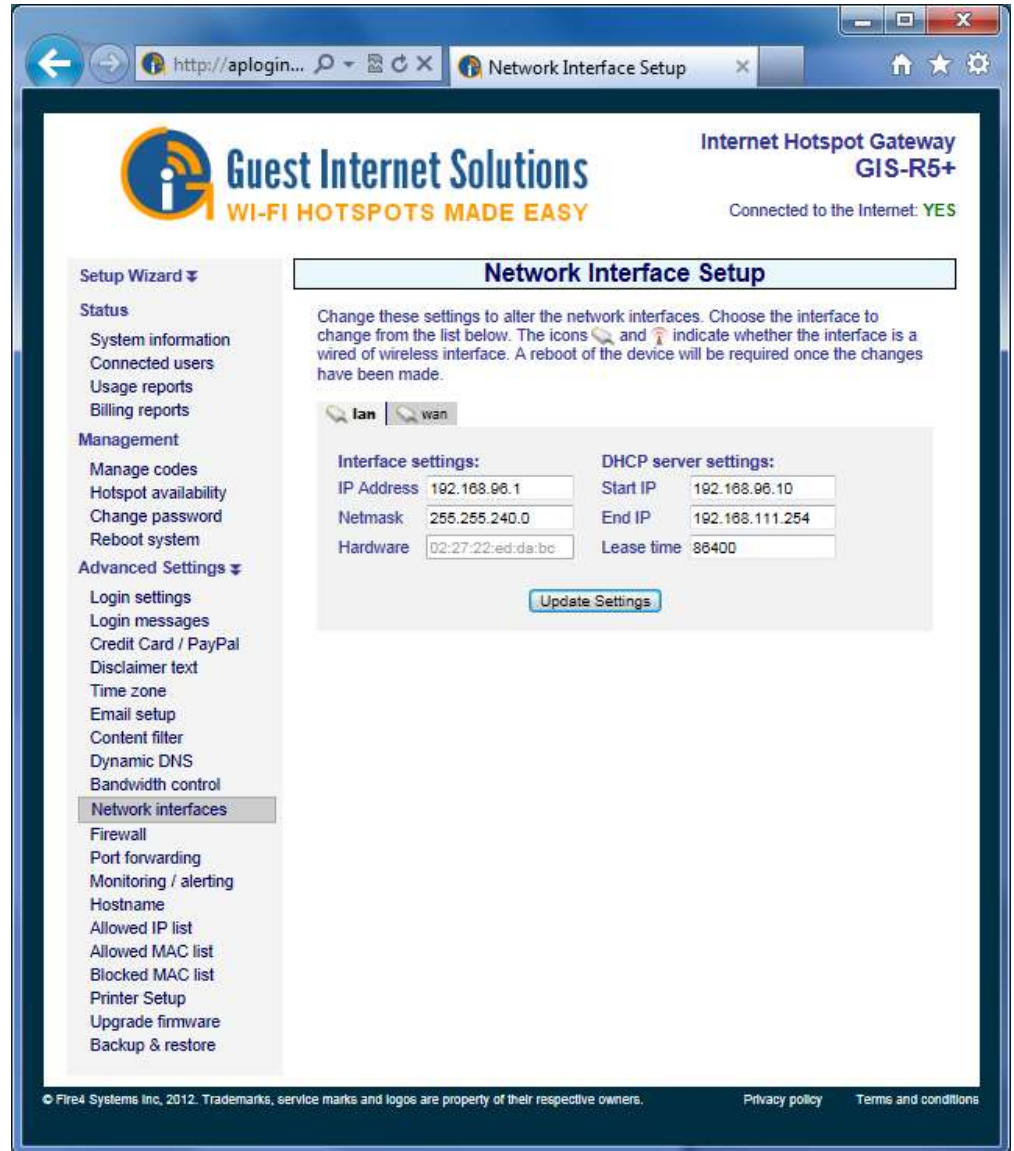




The screen view on the previous page shows the WAN tab (Wide Area Network). These settings are for the gateway unit Internet port. The DHCP box checked for default configuration. In this case the DSL router or cable modem provides the IP address for the gateway. When the gateway is used with a T1 circuit it may require setting the unit to a fixed IP. In this case the Use DHCP box is unchecked and the three IP addresses shown must be typed in manually: IP Address, Netmask and Gateway.

Clicking the LAN tab (Local Area Network) shows the settings used for the LAN ports on the gateway. The LAN ports are always a DHCP server and provide IP addresses for devices connected to the LAN ports. Computers connected to wireless access points request an IP address from the gateway LAN ports.

**Network Interface Menu  
Page showing the LAN  
tab.**



The LAN Network Interfaces configuration permits you to set parameters that will improve the service for your guests. For example you can set a limit on the number of guests that can connect to the gateway unit simultaneously. The procedure is described below.

Click on the LAN tab (network interface). You will see the IP range start and IP range end. The IP range is set for a maximum of 240 users connected (see the last digits of the IP addresses,  $250 - 10 = 230$ ). Obviously this number is higher than a DSL line can support. A good value to limit the number of guests is between 20 for a standard DSL line and 50



for a very fast DSL line. You can set the maximum number of users to 25, for example, by changing the last 3 digits of the IP range end, from 240 to 35. The number of users is determined by subtracting the IP range start from the IP range end (in this case  $35 - 10 = 25$  users).

When any change has been made to the network settings then click the update settings button so the changes take effect. Please consult a network specialist if you require any special network information for your gateway installation.

Products with a wireless interface (GIS-K1) have three tabs on the network Interface page:

- WLAN: the wireless interface
- WAN: the Ethernet port that connects to the Internet via the DSL router
- LAN: The Ethernet ports that are fire-walled for PoS computers

Note that the LAN interface shown for the GIS-K1 is a fire-walled switch that can be used to connect back-office and point of sale computers to protect them from hackers.

**Network Interface Menu Page for the GIS-K1 showing the WLAN (wireless) tab with network settings. This page is not available on gateway products (GIS-R2 to GIS-R40)**



The screen above shows the WLAN (Wireless local area network) IP settings. This interface is always a DHCP server.

The WAN (wide area network) configuration is identical to other gateway products. The WAN interface can be configured as a DHCP client, or with a fixed IP address. The LAN (local area network) IP settings are configured as a DHCP server. Care should be taken if the LAN IP address is modified: the isolating firewall is valid only for the private address ranges 192.168.x.x, 172.16.x.x and 10.x.x.x. The firewall will not function for other IP (public) address ranges if selected using this page.



## Wireless Settings for the GIS-K1 product only

Products that have a wireless interface (GIS-K1+, GIS-K3) also have an additional menu page for wireless settings. There are two configuration options:

- Name (SSID)
- Channel

The menu page is shown below.

### Wireless Settings Menu (ONLY for the GIS-K1 products).



The Name (SSID) (Service Set Identifier) is the name that is broadcast by the wireless transmission. Any laptop computer within range of the transmission will detect and show the SSID of the K1+ and K3 units.

The channel can be selected to avoid conflict with adjacent transmitters if there is more than one hotspot at a location. It will be necessary to use laptop identification software, such as NETSTUMBLER to identify the channel number of adjacent transmissions.





## WAN Settings (GIS-R5, R10, R20 and R40 only)

The GIS-R5, R10, and R20 products have dual port WAN interfaces. The GIS-R40 has a quad-WAN interface. Multiple WAN connections permit these products to balance loads over two Internet backhaul circuits to increase the throughput and permit more users to be connected simultaneously. In addition the dual WAN has a fail-over feature: when one of the WAN backhaul circuits fails then all traffic is routed through the functional circuit.

The WAN settings page shows two WAN circuits. Each circuit can be configured independently as a DHCP client, or with a static IP address.

Note that both WAN circuits are configured by default to have the same DNS address, in this case the Google public DNS servers are installed. It is necessary to have identical DNS server address for both backhaul circuits to avoid DNS problems with client computers.

The respective configuration pages are shown below.

### GIS-R5, R10, R20 and R40 WAN1 Configuration







## GIS-R5, R10, R20 and R40 WAN2 Configuration



The GIS-R5, R10 and R20 can have the WAN ports configured for either dual WAN or single WAN. The default is dual-WAN. When the configuration is changed from dual to single WAN the WAN2 port becomes a LAN port. The GIS-R40 default configuration is four WAN ports, however the WAN port configurations can be changed also.



## LAN Settings (GIS-R5, R10, R20 and R40 only)

The GIS-R5, R10, R20 and R40 products have dual port (quad-port on the GIS-R40) WAN interfaces. Two WAN connections permit these products to balance loads over two Internet backhaul circuits to increase the throughput and permit more users to be connected simultaneously. In addition the dual WAN has a fail-over feature: when one of the WAN backhaul circuits fails then all traffic is routed through the functional circuit.

The LAN settings differ between the two models. The GIS-RR5 has three Ethernet ports that can be configured for any IP address range. The GIS-R10 has a single Ethernet port that can be configured for any IP address range. The GIS-R20 has two Ethernet ports that can be configured independently for applications where multiple isolated subnets are required. The GIS-R40 has four Ethernet ports that can be configured independently for applications where multiple isolated subnets are required.

The respective configuration pages are shown below.

### GIS-R10 LAN1 Configuration



When the GIS-R10 WAN configuration is changed from dual to single then the WAN2 port becomes the LAN1 port1, and LAN1 changes to LAN2.



## GIS-R5, R20 and R40 LAN port Configuration



The GIS-20 has two LAN ports in the default settings. If the WAN ports are reconfigured from dual to single WAN then the GIS-R20 has one WAN port.

The GIS-R40 has four WAN ports in the default settings.



## Firewall

The gateway has a firewall that provides four features: remote management, blocking private IP address ranges, blocking of virus DoS attacks, and blocking of peer-2-peer file sharing.

The first feature permits administrator login access via the Internet port to allow remote management of the gateway by opening the HTTP/HTTPS port. By clicking the box to activate Internet port access the admin login is available on the Internet port by typing a fixed IP address into the browser. The gateway can be administered from anywhere on the Internet providing that the business network has a fixed IP address and the business router has port forwarding. Port forwarding is required from a device that owns the public facing IP address to a device that has a private (NAT) IP address. If the GIS device gets a public IP then no port forwarding is required, if it gets an IP address in the range 192.168.X.X, 172.16.X.X, or 10.X.X.X then packets need to be forwarded for TCP port 80/HTTP (and 443 for HTTPS/SSL) on the public facing device to the GIS unit.

### Firewall Menu Page

The screenshot shows a web browser window with the URL <http://aplogin.com/adr>. The page title is "Firewall" and the browser tab is "Firewall". The main content area is titled "Internet Hotspot Gateway GIS-R3" and shows "Connected to the Internet: YES". The "Firewall" section is active, displaying the following settings:

- Allow remote management:**  (unchecked)
- Select management port:** 80
- Block private IP ranges:**  (checked)
- Block DoS attacks:**  (checked)
- Block P2P file sharing:**  (unchecked)
- Select block time:** 5 mins

A red warning message states: "WARNING: All hotspot users will be logged out when settings are changed". A "Change settings" button is located at the bottom right of the configuration area.

© Fire4 Systems Inc, 2015. Trademarks, service marks and logos are property of their respective owners. Privacy policy Terms and conditions



The second feature prevents public Internet users accessing business computers in the network that the Internet (WAN) port is connected to. This option is selected by default to ensure compliance with the recommendations of PCI DSS

[https://www.pcisecuritystandards.org/security\\_standards/pci\\_dss\\_download\\_agreement.html](https://www.pcisecuritystandards.org/security_standards/pci_dss_download_agreement.html)

The third feature blocks any computer infected with has a software virus or Trojan that is sending out a packet stream as part of a DoS (denial of service) attack. If the computer is permitted to connect to the Internet then the service will become very slow for all users. Therefore the default setting is to block infected computers.

The fourth feature when selected blocks any computer that has active torrent file sharing software. Many businesses that offer a public Internet service subsequently receive notifications of illegal sharing of copyrighted material. The business must cease of face penalties. A hotel is venerable to legal action because the management cannot know if a guest has file sharing installed on his or her computer. By activating the P2P (peer to peer) blocking service the business can prevent any computer with P2P software from connecting to the Internet. A drop down menu permits the offending computer to be blocked for a period of time, or permanently. We recommend that permanent blocking should be selected as a malicious user who is reconnected can use an encrypted service to share files, and encrypted communications cannot be detected.

## Allow remote management

A computer is connected to one of the LAN ports to configure the Guest Internet gateway. Connecting a computer to the gateway Internet port and checking the Allow Remote Management box can also be used to configure the gateway. When connecting to the Internet port the Hostname URL cannot be used: The IP address of the Internet port has to be used. If remote management is used frequently then it is necessary to set the Internet port to a fixed IP address: the DHCP address configuration may cause the IP address to change when the gateway is rebooted.

The management port number must also be specified. It is usual to use port 80 (HTTP) however any port can be used.

The gateway can also be managed outside the network via the Internet by enabling port forwarding on the DSL or T1 router. It will then be necessary for the telecom provider to give a fixed IP for the network so that it can be accessed remotely, or deploy the dynamic DNS feature. The procedure to access the gateway remotely is as follows:

Determine whether you are using static public IP address or DHCP

1) If using static public IP address:

- a) Set the WAN IP address of the GIS-R unit to the static IP address given to you by your Internet provider (e.g. 91.122.50.70 )
- b) On the firewall page check the remote access box
- c) Select a port number (8600 for example)
- d) To access the GIS-R unit remotely use the static public IP address of the Internet provider plus the port number:

Using the example enter the IP/port into your browser when connected remotely:  
91.122.50.70:8600

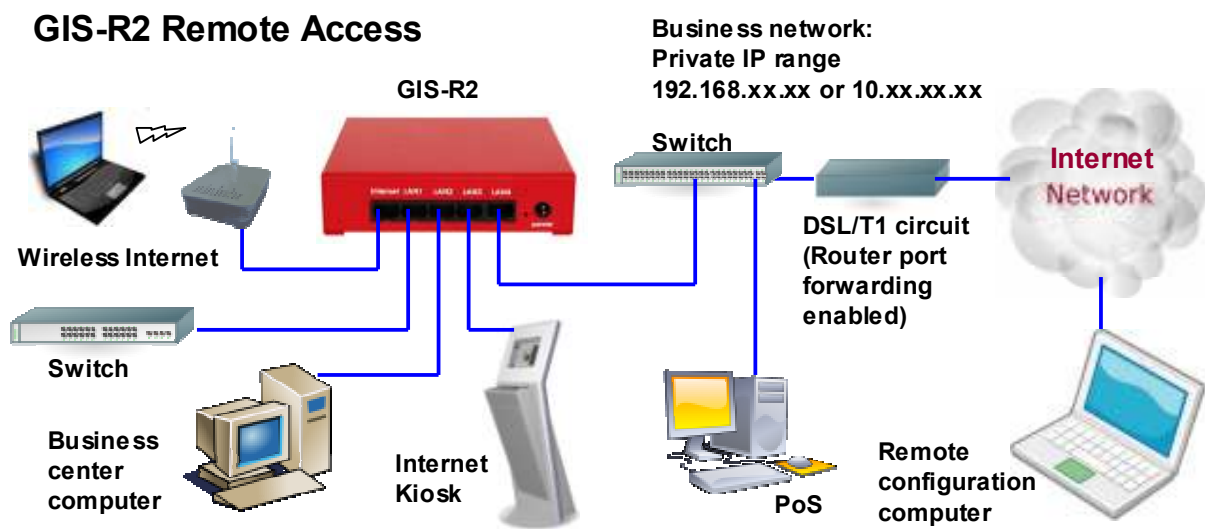
2) if using DHCP:

- a) find the LAN IP address range of the Internet provider router's subnet





- b) find the LAN dynamic range of the Internet provider router's subnet
- c) pick an IP address in the Internet provider router's subnet, out of the LAN DHCP range
- d) set the WAN IP address of the GIS-R unit to the chosen static IP address. If the LAN DHCP range is 192.168.1.10 – 192.168.1.254 choose an IP address between 192.168.1.2 and 192.168.1.9, for example: 192.168.1.5
- e) on the firewall page (Advanced Settings) of the GIS-R unit check the remote access box
- f) select a port number between 8502 and 8600
- g) set a port forwarding rule in your Internet provider router  
for example:  
application port range protocol ip address  
name public private  
GIS-R 9050 8505 TCP/UDP 192.168.1.5
- h) find the WAN IP address of the Internet provider router, for example: 98.211.180.90
- i) to access the GIS-R unit remotely use the WAN IP address of the Internet provider router plus the public port number: for example: 98.211.180.90:9050

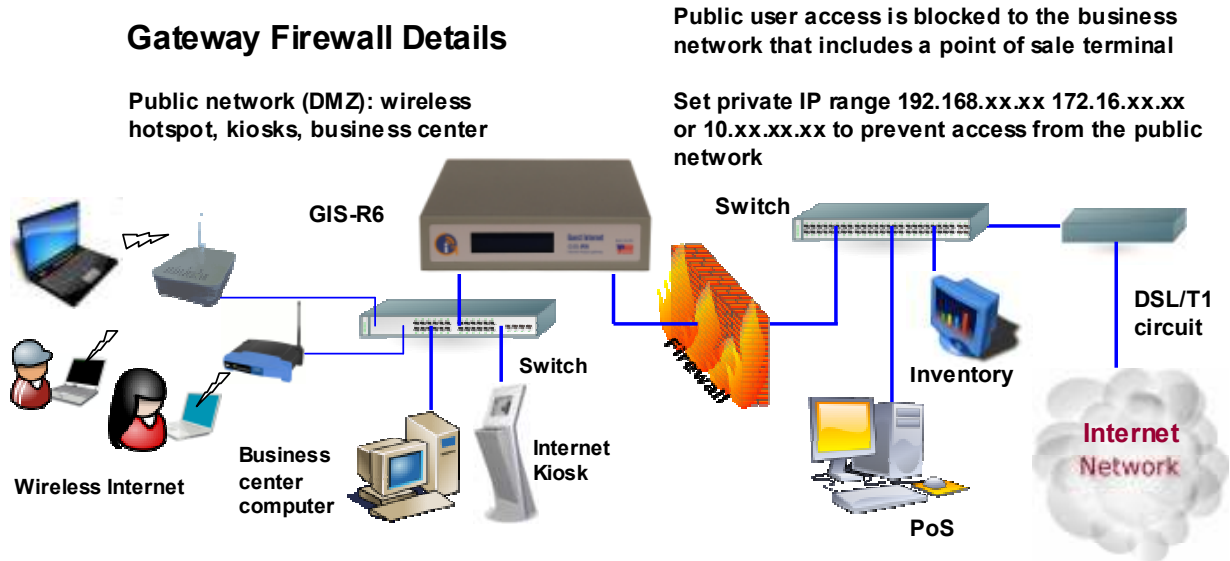


### Block private IP ranges

The Guest Internet gateway has a firewall that is designed to protect computers connected to the Internet port network from public users connected to the gateway LAN ports. The firewall provides compliance with the PCI DSS requirements for data security. The business network is connected as shown in the diagram on the following page.



## Gateway Firewall Details



Checking the box to block private IP ranges activates the gateway firewall. When activated the firewall 'drops' or discards all data IP packets that are sent by public users to the three private IP address ranges:

**192.168.xx.xx    172.16.xx.xx    10.xx.xx.xx**

The firewall is effective when the business network is configured for one of the three private IP ranges listed above.

A hacker can connect to the public network, however any attempt to discover or connect to computers in the business network requires the transmission of IP packets that have the business network IP range as the destination address. Any such IP packets are not forwarded from the LAN port to the Internet WAN port and so do not reach their intended destination.

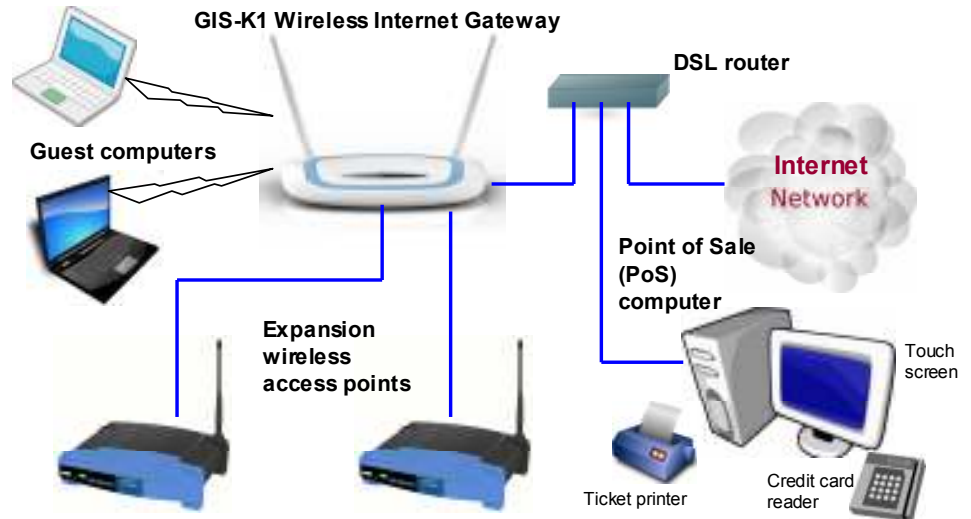
Note that full PCI DSS compliance also requires a second firewall located between the DSL router and the business network to prevent computers being hacked from the Internet.

The configuration of the firewall in the GIS-K1 product is identical to the GIS-R-series gateway products.

The Guest Internet GIS-K1 gateway default setting has a firewall configuration that is designed to protect business computers connected to the same network as the Internet port. Public users connected to the gateway LAN ports cannot access any computer or device on the WAN side of the gateway. The firewall provides compliance with full PCI DSS requirements for data security, blocking attacks from both the public wireless network and from the Internet. The business network is connected as shown in the first diagram on the following page.

The GIS-K1 permits expansion of the wireless network by adding wireless access points. This mode is compatible with non-wireless gateway products. This configuration is shown in the second diagram on the following page.

**GIS-K1 LAN port extending the public network by connecting additional wireless access points. Computers connected to the same DSL circuit as the GIS-K1 are protected from hackers by the GIS-K1 firewall.**



### Block DoS attacks

Many personal computers are infected with viruses or worms that are programmed to conduct a Denial of Service attack (DoS) on a network server. The purpose of the DoS attack is to stop a server communicating with users for a period of time. The perpetrators of a DoS attack have to program millions of computers to repeatedly access a web site in order to stop the website working. For this reason the DoS attack code is distributed as a virus. The computer owners do not realize that their computer is infected, only that it appears to be "running slow".

DoS attacks are programmed for malicious reasons, for retribution, or illegal gain. The perpetrators have high technical skills but they are not smart enough to understand that they can get a well paid job with those skills.

When a computer infected with a DoS virus is connected to the public network then it will consume all the available bandwidth and cause the hotspot service to be very slow for all other users. The GIS gateway can detect a DoS attack and block that computers access to the Internet, ensuring that all other users have a normal Internet service.

This option is active by default. Do not disable unless you are prepared to deal with users complaining of very slow Internet access.

### Block P2P file sharing

Many younger Internet users share music and video files through Internet file sharing services that communicate using variants of the Torrent protocol. One such service that was closed down temporarily is 'Pirate Bay'. When the files being transferred are not authorized by the copyright holder of the information, then the transfer of information is illegal, as specified by the Digital Millennium Copyright Act (DMCA).

Copyright holders have set up server farms to download the material they own and during this process they log the IP address that provided the file element. A Torrent client is also a server, files can be downloaded but are also uploaded to others without the knowledge of the computer owner.

When the copyright owner has the IP address then a communication is sent to the ISP who owns the block of IP addresses, of which the offending IP address is part. The ISP has an agreement to issue a 'DNCA Takedown' notice to the IP users, advising that the service will be terminated if illegal file transfers are not stopped. If illegal file transfers continue then the ISP has an obligation to terminate service to the offending customer.



Most hotels have received 'DMNCA Takedown' notices and have an obligation to respond and to terminate illegal activity. The common option is to install a firewall that will block file sharing.

Gust Internet products incorporate a firewall filter that blocks Torrent communications to prevent transfer of files illegally. When this feature is activated, any computer that has Torrent software installed will be blocked from accessing the internet. A drop down menu permits the computer to be blocked for a minimum of five minutes, up to a permanent block.

Hotels are recommended to activate this feature to avoid any risk of Internet service termination due to a guest having a computer with Torrent software installed.



## Port Forwarding

Port forwarding permits a computer on the WAN side of the gateway to connect to a device on the LAN side of the gateway. Port forwarding is very useful for remote configuration of wireless access points.

Port forwarding can be configured for up to 25 devices (up to 250 on the R10/R20/R40). The port forwarding configuration page requires four parameters for each device.

**The first field is the port number assigned for the device.**

**The second field is the destination IP (fixed) of the LAN side device.**

**The third field is the port number used to access the device (usually port 80 however most devices permit this to be changed).**

**The fourth field is for comments used to identify the device.**

A static WAN port setting is required to access forwarded devices.

### Port Forwarding Menu Page



### IMPORTANT NOTE:

**The LAN side device fixed IP must be in the same subnet as the LAN DHCP range, however the subnet DHCP range must be modified so that the device fixed IP's are outside the DHCP range.**

Each device connected to a LAN port is addressed by:

**http:// < IP of WAN port> : < assigned port number>**





## Monitoring / Alerting

The purpose of the monitoring and alerting feature is to advise the Hotspot owner that a wireless access point or other device connected to the LAN port has failed. The GIS gateway can be set to periodically 'ping' each device in the device list. If a device does not respond then a second attempt is made to 'ping' the device. If the device does not respond after two attempts then a message is sent out using the previously configured email. The email message has a subject line and content derived from the device name entered when configuring monitoring and alerting as follows:

*Subject: Compex WPP54g on the GIS-R2 is DOWN*

*Device 'Compex WPP54g on the GIS-R2' with MAC address '00-80-48-50-93-3a' attached to Hotspot ID 5f7d7d45 stopped responding at 2011-05-28 16:19:51 EDT*

A similar message is also sent out if the device comes back on line.

The **monitoring and alerting** configuration screen is shown below.

### Monitoring and Alerting Menu Page

Monitoring and Alerting - Windows Internet Explorer  
 http://aplogin.com/admin/monitor.asp

Guest Internet Solutions  
 WI-FI HOTSPOTS MADE EASY

Internet Hotspot Gateway  
 GIS-R2  
 Connected to the Internet: YES

Monitoring and Alerting

Monitoring can be set up for Access Points or other devices like switches and CCTV cameras connected to this hotspot. If a device fails or recovers from a failure an alert will be emailed to the address below. Devices being monitored must have fixed IPs. It is not necessary for the device to have an IP address assigned by this hotspot.

Email address to send alert to:

MAC Address	IP Address	Interface	Device Name
00-02-6f-55-06-80	192.168.90.12	lan	Benao 2610 LAN port [X]
00-80-48-50-93-3a	192.168.90.11	lan	Compex WPP54G LA [X]
		lan	[X]
		lan	[X]
		lan	[X]
		lan	[X]
		lan	[X]
		lan	[X]
		lan	[X]
		lan	[X]

Change settings

© Fin4 Systems Inc. 2011. Trademarks, service marks and logos are property of their respective owners. Privacy policy Terms and conditions



Information has to be provided for three fields, and there is also a drop down tab to select the port that the device is connected to.

**MAC address**

The MAC address is provided for the device Ethernet port. Not that wireless access points usually have two MAC addresses, one for the Ethernet port and one for the wireless port.

**IP address**

The IP address is a static address that is configured in the device for access to the administration pages. This is set to a default by each manufacturer but is programmable.

Note that the IP address must be in the same subnet as the Ethernet port to which it is attached. However if the Ethernet port is a DHCP server then the DHCP range must be modified to ensure that no IP address can be issued which is the same as the device.

**Interface selector**

Select the Ethernet interface that the device will be connected to, (LAN, WAN, etc).

**Device name**

Type a text string that describes the device (and the location of the device if necessary). This text string will be sent via email if the device does not respond.



## Hostname

The hostname is a special URL or Web address that is used by Guest Internet products for the login page and to access the configuration pages. The default hostname is:

**aplogin.com**

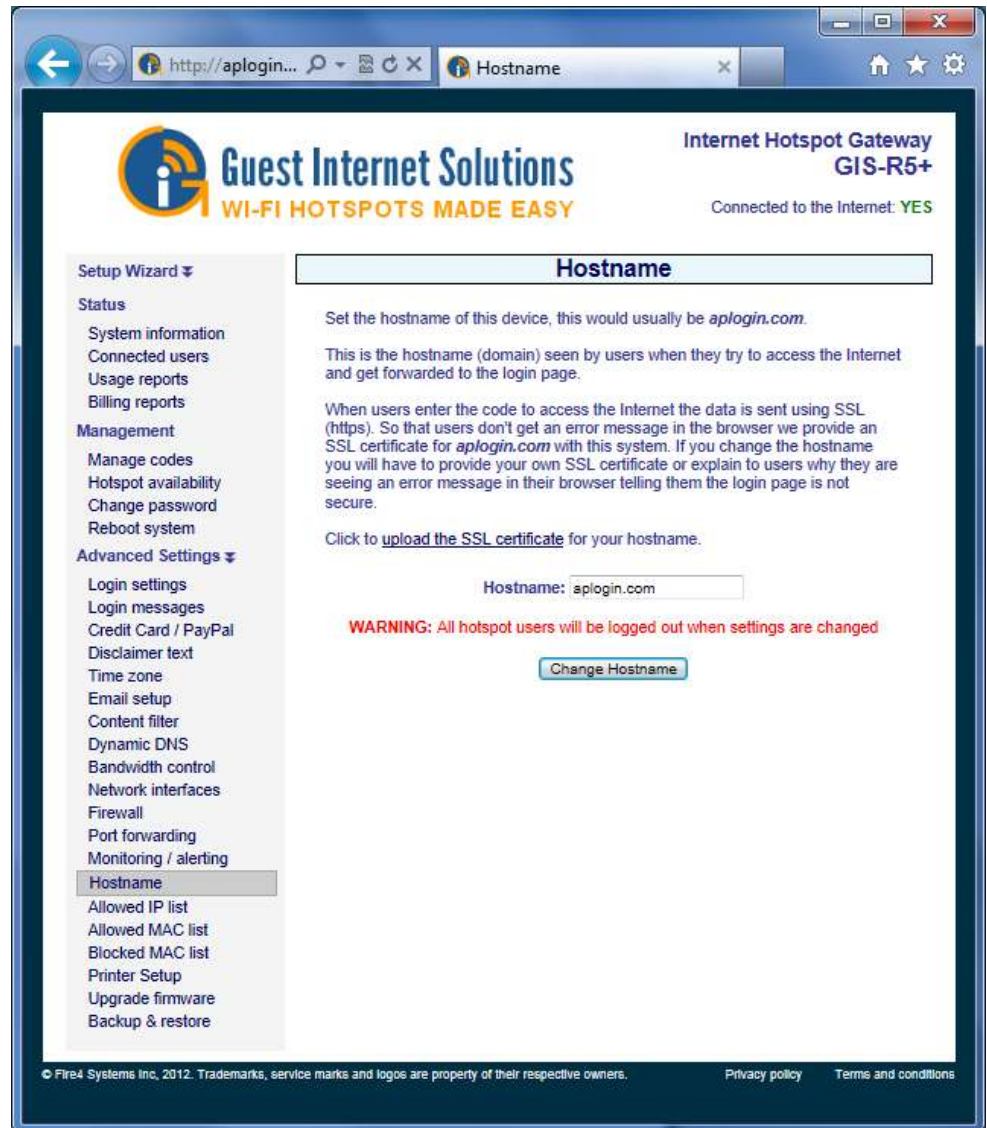
Therefore to access the configuration pages in a browser enter the URL in the address line as:

**http://aplogin.com/admin**

The username is **admin**; the password was entered during the wizard setup.

When the Hostname menu entry is clicked the page shown below appears in the browser window.

### Node Hostname Menu Page



The hostname can be changed, however the URL for the new name must be purchased and be a valid Internet URL. When the hostname has been changed click on the change hostname button. The hostname is changed only for special applications. Changing the hostname is not recommended for normal use. A valid SSL certificate must be purchased for the URL that has been purchased, and uploaded to the SSL certificate menu.

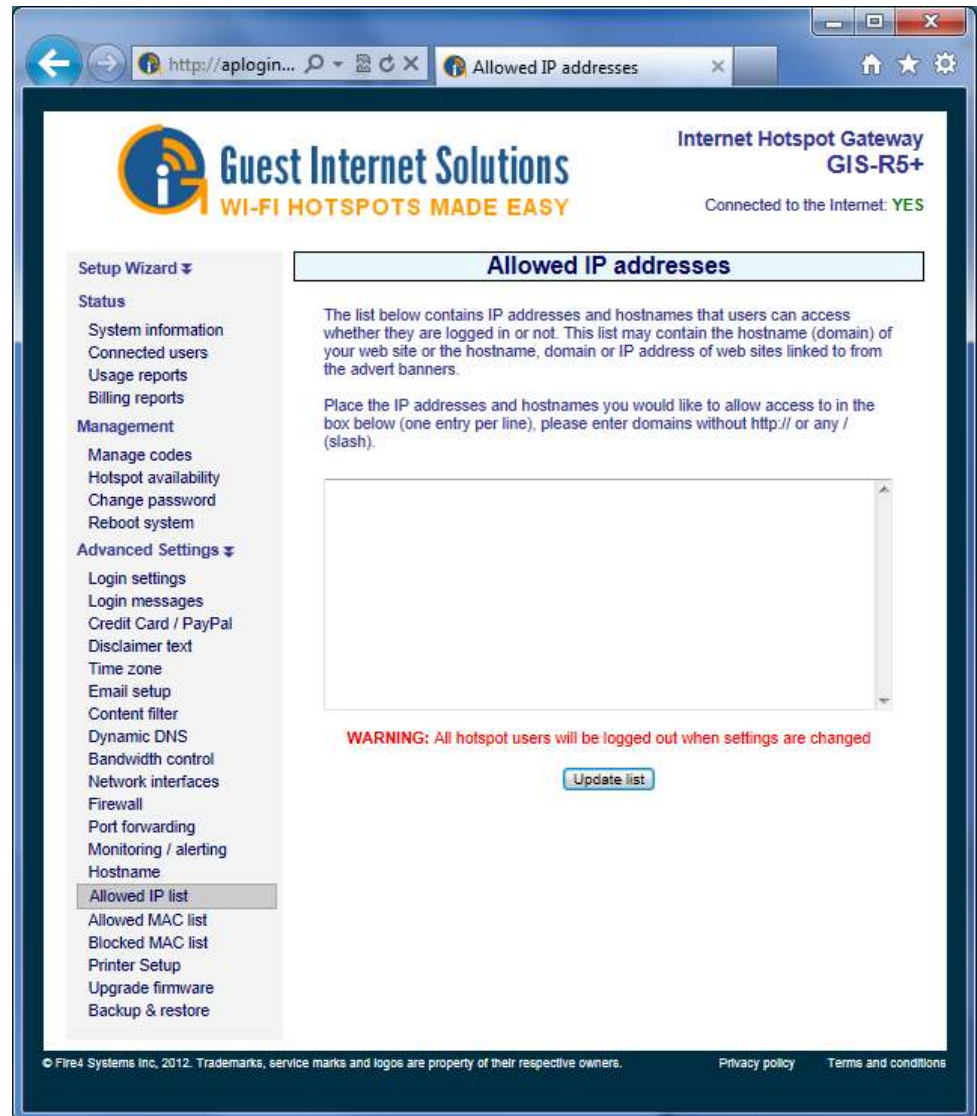


## Allowed IP List

Allowed IP addresses permit your guests to access websites without completing the login page process. If you entered the address of your business Web site during the wizard setup process you will see that your website address is already included in this table. You can add other Web site addresses that you want your guests to access directly without logging in.

For example. The Guest Internet product may be installed in a hotel and the hotel charges for Internet access. If however the hotel wishes to give guests free access to airline websites then the URL's of the airlines are entered in this window. Click on the **Allowed IP** **addr** menu tab to see the table of allowed IP addresses shown in the figure below.

### Allowed IP Addresses page



Type in the URL or IP address that you wish to allow guests to access without logging in. There is no limit to the number of IP addresses /URL's that can be entered. Finally click on update list to make the IP active.

The Allowed IP Addresses table is used to construct a 'walled garden' login page. See the Login page section for more information about creating a Walled Garden login page.

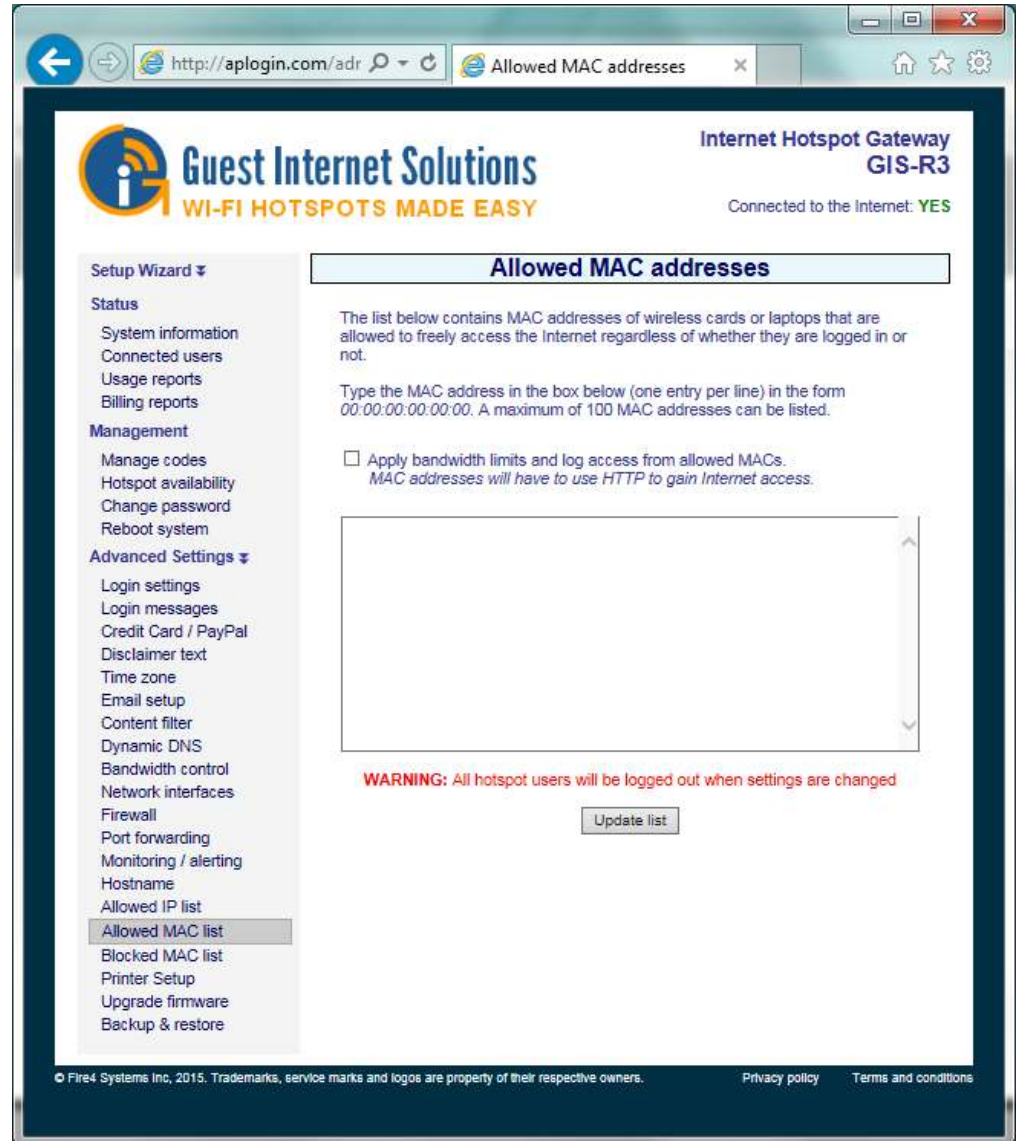


## Allowed MAC List

Allowed MAC addresses permit you to configure the Guest Internet unit so that specific computers can bypass the login process. These computers can be your business computers, or a laptop computer used for network maintenance.

Click on the **Allowed MAC list** menu line and you will see the screen shown below.

**Table of Allowed MAC Addresses Meun Page**



The MAC address of your computer will be noted on a label with the FCC ID number. The MAC address is a sequence of six 2-digit alphanumeric codes separated by a colon. There is no limit to the number of MAC addresses that can be entered. A typical MAC address might look like this:

**00:2C:0D:55:A3:1E**

Type the MAC address into the table and click the update list button to permit each computer to access the Internet, bypassing the login screen. The 'apply bandwidth limits' box should be checked if it is desired to apply the firewall rules to the bypassed user.





## Blocked MAC List

Any user can be prevented from using the Internet Hotspot by including the MAC address of that users computer on the blocked MAC address list.

A computer is blocked using the usage report page (see previous section). Select the user by access code or MAC address and click on the 'block user' button. That users computer MAC address is then included in the list below. A user might be blocked for trying to use P2P software.

The blocked MAC address screen is shown below.

### Table of Blocked MAC Addresses Menu Page

The screenshot shows the 'Blocked MAC addresses' page in the Guest Internet Solutions web interface. The page title is 'Blocked MAC addresses'. Below the title, there is a message: 'This list contains MAC addresses of users blocked from this hotspot. Click  to remove a user from the list and allow them to use the hotspot.' Below this message is a table with two columns: 'Blocked MAC Address' and 'Remove'. The table contains one row with the MAC address '80:C1:6E:45:07:B7' and a 'Remove' button with a red 'X' icon.

Blocked MAC Address	Remove
80:C1:6E:45:07:B7	<input type="checkbox"/>

The users computer can be removed from the blocked MAC list by clicking on the remove button shown on the screen above.

## Ticket Printer Setup

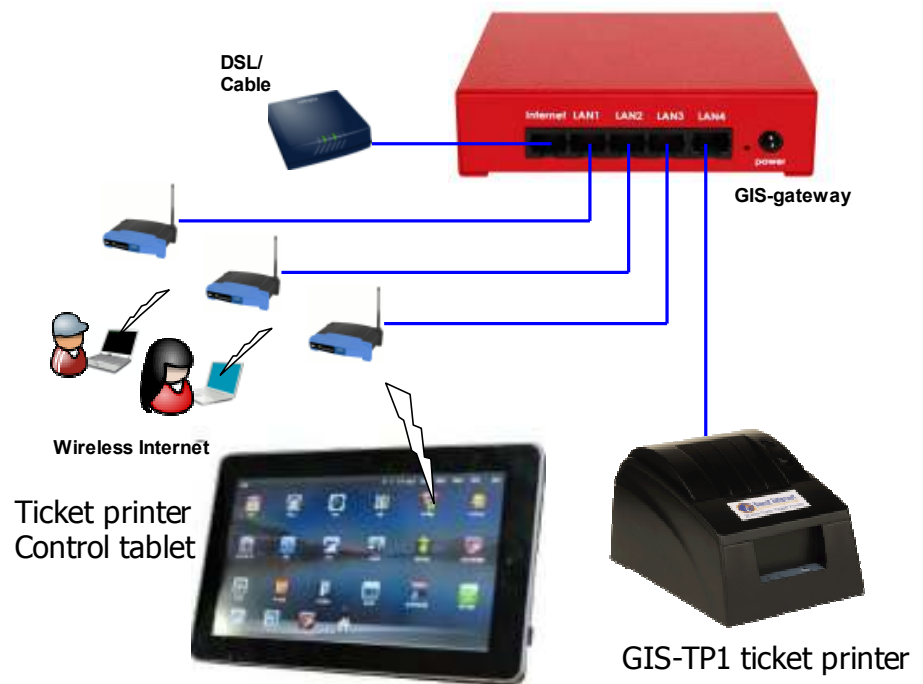
The ticket printer GIS-TP1 is used to print access codes for a point of sale station in Internet Cafes or for user businesses, such as a hotel concierge desk, or a trade show management desk.

The GIS-TP1 connects to the gateway LAN port via an Ethernet cable connected to a switch. The printer uses standard 58mm thermal paper widely available for point of sale terminals.

The GIS-TP1 ticket printer can be operated using a personal computer or laptop. The better solution is to use a tablet computer because the printer operation interface is designed for a touch screen display. Any type of tablet can be used: both iPAD's and Android tablets work very well. The setup cost can be minimized by using a sub \$100 Android tablet with a 7inch display.

The connection of the GIS-TP1 ticket printer is shown below.

## Ticket Printer Network Configuration



The GIS-TP1 combined with a tablet computer makes a very convenient point of sale register for businesses such as Internet cafes. The ticket printer scripts are configurable and so the printed ticket is also the customers purchase receipt.

Up to ten ticket printer buttons can be configured for the tablet display. Each button represents the duration of an access code, and can also represent the cost of the ticket. The tablet display is operated in an identical manner to any point of sale terminal. The customer requests Internet access for a specific duration, the operator touches the display button that corresponds to the Internet access that was requested. The operator can charge the customer before giving the ticket, or give the ticket without charging when the Internet is offered as a free service.

To use the GIS-TP1 ticket printer, the printer is first connected to the gateway LAN port via a switch and powered up. Next the printer is activated using the printer setup menu display, shown on the following page.



## Ticket Printer Setup Page

Internet Hotspot Gateway  
GIS-R5+  
Connected to the Internet: YES

### Printer Setup

The GIS-TP1 ticket printer can be used to print code tokens for guests. The settings below are used to enable the printer and change the printer settings.

Printer Status:  Enabled

Test Printer:

Business Name:

Ticket Header:   
Text will appear above the code.  
Max 100 characters.

Ticket Footer:   
Text will appear at the bottom of the ticket.  
Max 100 characters.

Show Time on Ticket:  Print time until expiry of code on ticket

© Fire4 Systems Inc. 2012. Trademarks, service marks and logos are property of their respective owners. [Privacy policy](#) [Terms and conditions](#)

When the configuration page is first opened the printer status will be shown as disabled. First click on the printer status enable button to enable printing via the printer. Next type the messages that will be displayed on the ticket: the business name, the ticket header text that is printed before the access code, and finally the ticket footer text which is printed below the access code. In addition a check box selects the option to print the duration of the access code.

When the printer configuration is complete click the update settings button. Note that only one printer can be connected to each gateway. The gateway is now ready to communicate with the printer, however the **codes** display must be configured to initiate ticket printing.

Ticket printing is controlled using a computer. The ticket printer screens have been designed for use with a tablet computer touch screen. Use an iPad or Android tablet, the display can be small (e.g. 7 inches) or large (e.g. 10 inches). The tablet computer is convenient to install together with a point of sale terminal.

The ticket printer screens can also be operated using a laptop or desktop computer by clicking the buttons with a mouse.

First ensure that a CODES password has been set in the previous section: **Management Functions: Change Password.**

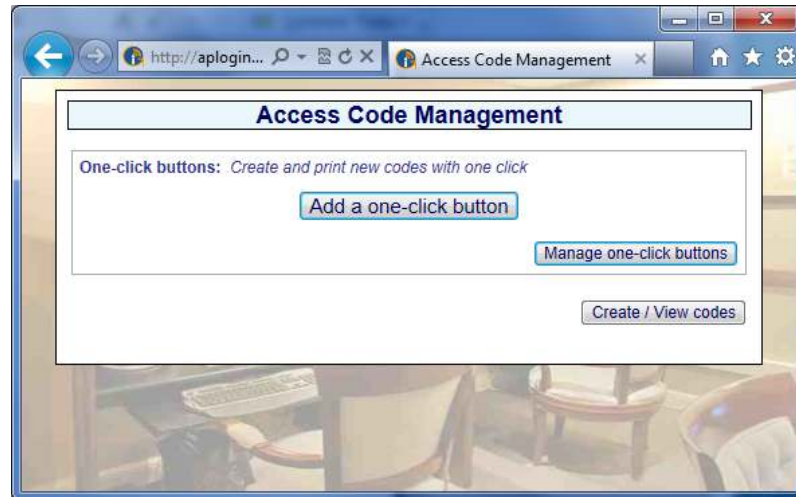
Using the tablet computer, connect to the wireless access point that is connected to the gateway LAN port. When the tablet is connected then open the browser, instead of the home page, the login page will be displayed. Now type the following into the browser URL line.

**aplogin.com/codes**

A box will open requesting the username and password. The username is **codes**, the password was set previously using the **Management Functions: Change Password.**

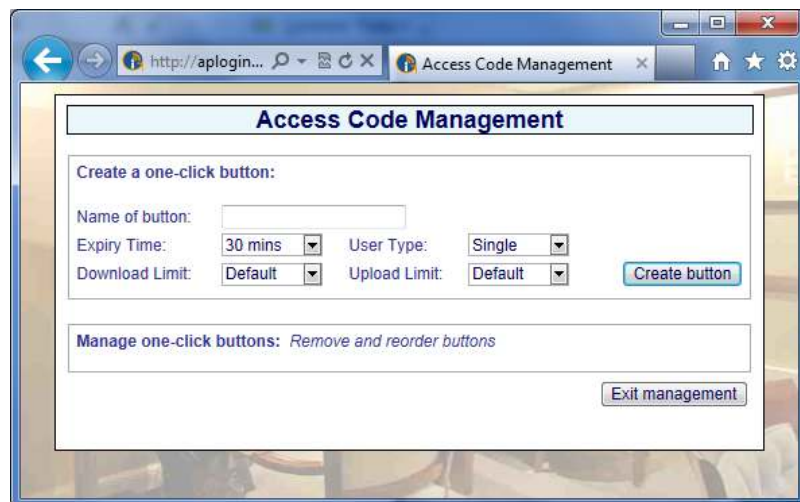
When the login process has been completed the display will show the screen below.

### Codes screen setup



Up to ten **One-click** buttons can be added to the display to control the printer. Each one-click button initiates printing of an access code with the specific duration associated with the one-click button. Click the button 'add a one click button'. The screen shown below will be displayed.

### One-click button setup





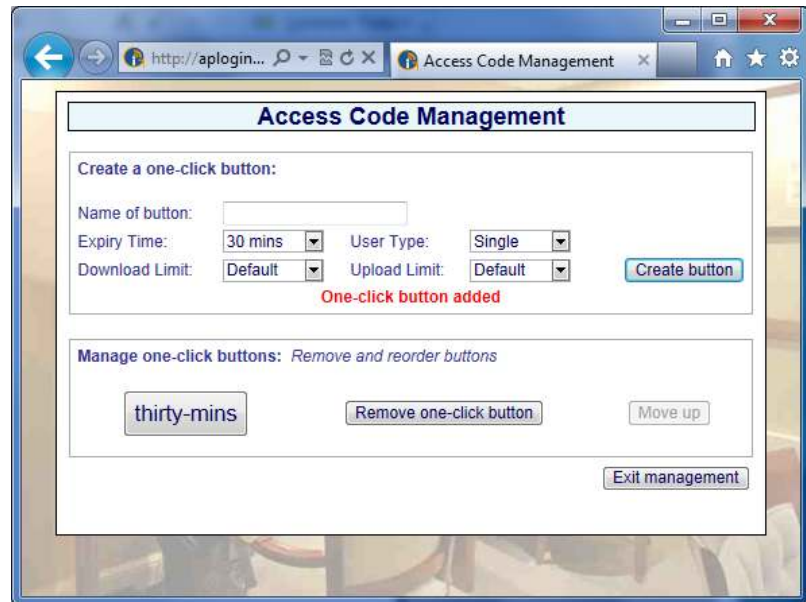
Parameters have to be set to configure the button. The first parameter is very important as this name is what the operator will see on the display. An example is shown.

Name of button: **1 hour for \$5.00**

The text **'1 hour for \$5.00'** will be displayed on the button. This will tell the operator that when a customer requests a 1-hour code this button should be touched, and the customer should be charged \$5.00.

The remaining button parameters can now be selected. Because the message says '1-hour' then click the expiry time drop down menu and select 1 hour. Then select user type as single, and set a download and upload limit if required. Finally click on **create button**. The button that has been created is now shown on the display, and can be seen in the example below.

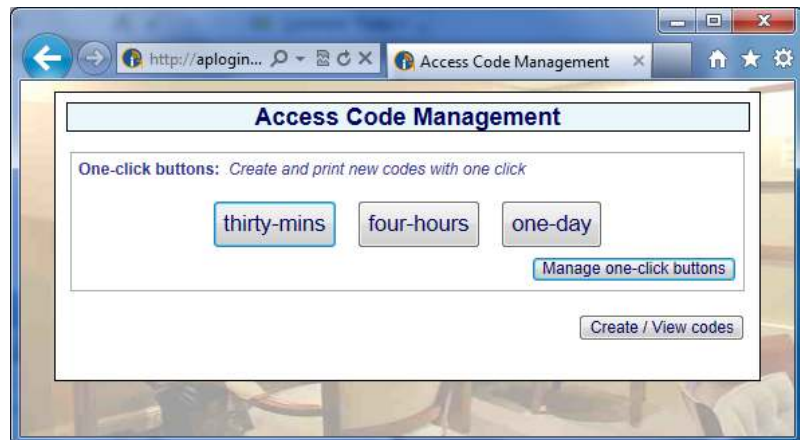
**One-click button created**



More buttons can be added with up to ten buttons maximum, for example **'1-day for \$10'**, and **'1-week for \$25'**.

Now exit the management screen to see the operators screen. The screen shown below has had three buttons created.

**Operators screen with three buttons created**

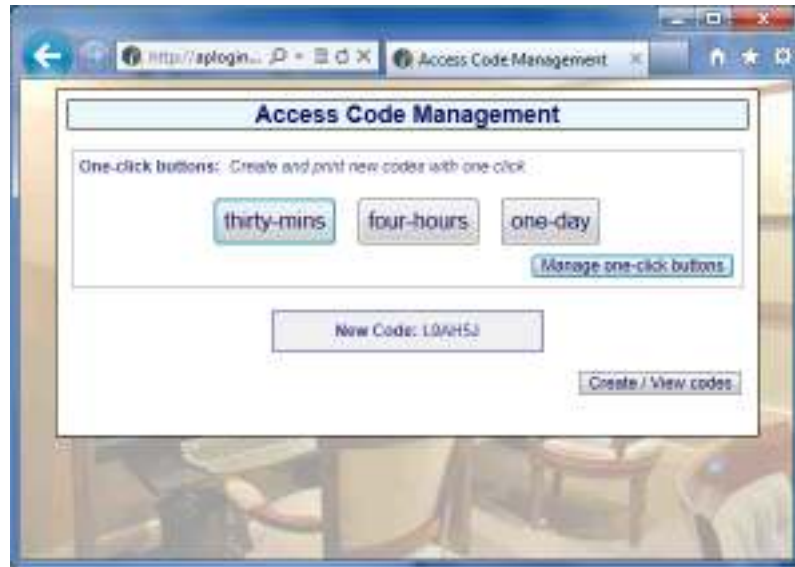






Click on a button to display the access code and send the code to the printer. The screen shown below will be seen.

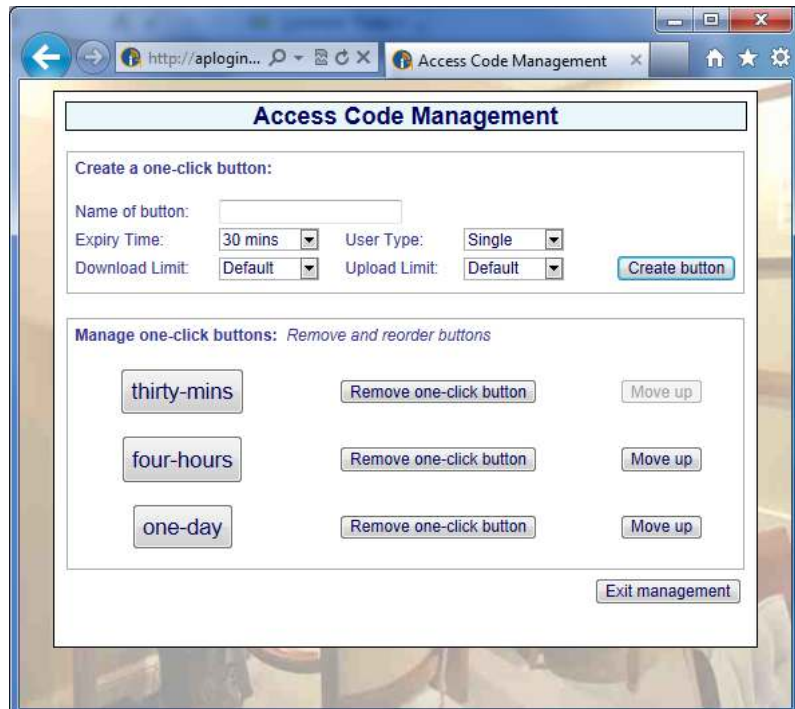
**Access code generated by clicking the one-click buttons**



Buttons can be modified or deleted at any time by clicking on **manage one-click buttons**.

When this button is clicked the screen shown below is displayed.

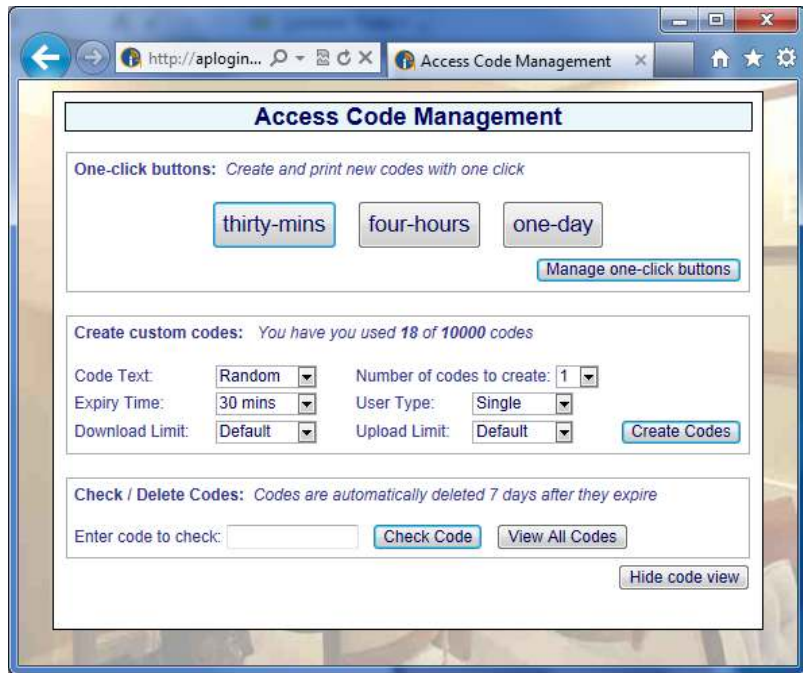
**Manage one-click buttons, edit or delete**



The operator's display also has a button '**create/view codes**'. When this button is clicked the screen shown on the following page is displayed.



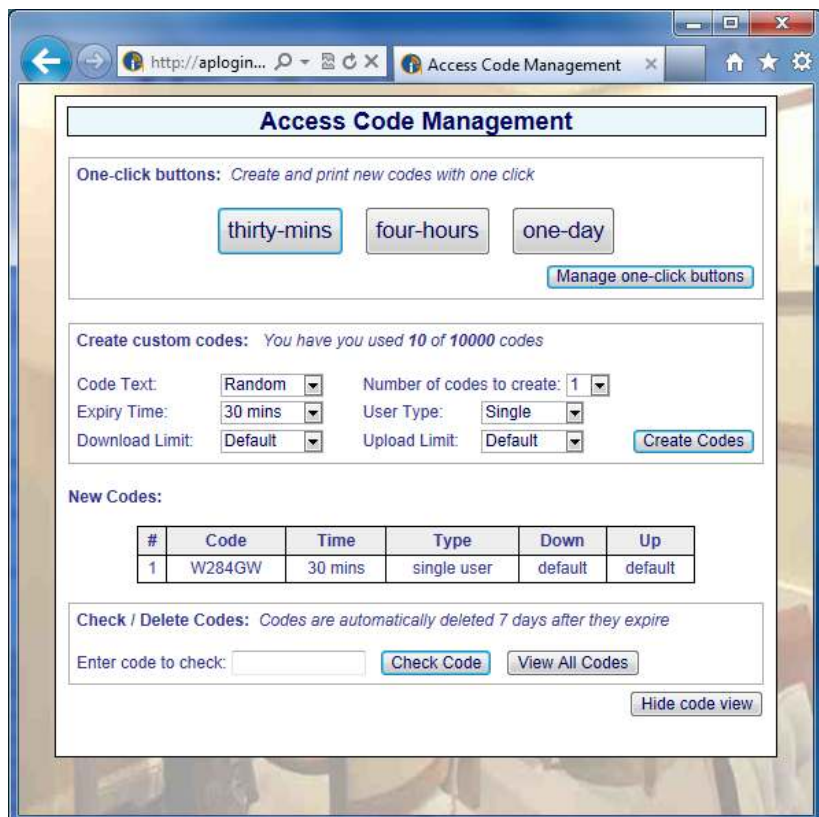
### Create/view codes display



A code that has been generated and given to a user can be checked to verify the time remaining for the code. Type the code in the box 'enter code to check' then click the check code button.

A custom code requires the selection of random text or custom text. If a random code is selected then select the number of codes to be printed. Select the expiry time, user type, and download / upload limits. Click the **create codes** button to generate the custom code as shown in the screen below.

### Custom code generation display





All access codes can be viewed by clicking the **view all codes** button. When this button is clicked a screen similar to the one shown below will be displayed.

**View all codes display**

**Access Code Management**

One-click buttons: *Create and print new codes with one click*

thirty-mins   four-hours   one-day

Manage one-click buttons

Create custom codes: *You have you used 9 of 10000 codes*

Code Text: Random   Number of codes to create: 1  
 Expiry Time: 30 mins   User Type: Single  
 Download Limit: Default   Upload Limit: Default   Create Codes

Check / Delete Codes: *Codes are automatically deleted 7 days after they expire*

Enter code to check:   Check Code   View All Codes

<input type="checkbox"/>	Code	Time	Type	Used	Time Left	Down kbit/s	Up kbit/s	Download Used	Upload Used
<input type="checkbox"/>	0BXH45	30 mins	single	NO	30 mins	*	*	0	0
<input type="checkbox"/>	0T0W1F	30 mins	single	NO	30 mins	*	*	0	0
<input type="checkbox"/>	20EY1E	30 mins	single	NO	30 mins	*	*	0	0
<input type="checkbox"/>	4LL5DH	2 hours	single	NO	2 hours	*	*	0	0
<input type="checkbox"/>	7158TB	30 mins	single	NO	30 mins	*	*	0	0
<input type="checkbox"/>	9F6KRE	2 hours	single	NO	2 hours	*	*	0	0
<input type="checkbox"/>	C6KQYQ	30 mins	single	NO	30 mins	*	*	0	0
<input type="checkbox"/>	D57XCC	30 mins	single	NO	30 mins	*	*	0	0
<input type="checkbox"/>	W2W31K	30 mins	single	NO	30 mins	*	*	0	0

Delete checked codes

\* Default bandwidth limit (kbit/s)

Hide code view

When the code is sent to the printer the code is printer in receipt format. The figure below shows the ticket that is printed onto the thermal paper.



**Rob's Cafe**

Thank you for visiting Rob's Café.  
Your code for Internet access is:

**1D 0H 0M**

**AGL5TX**

Please visit us again soon and try our delicious home baked pastries



## Upgrade Firmware

The Guest Internet product firmware can be upgraded by loading the firmware file from the computer used for the upgrade process. Firmware upgrades will be announced through the Guest Internet newsletter as they become available.

Remember that each Guest Internet product has a unique firmware file. Ensure that you are downloading the correct firmware file for your product.

When the firmware file has been loaded from the computer then click on the **Upgrade Firmware** menu link. You will see the page shown below.

### Upgrade Firmware Menu Page



Click on browse to find the correct upgrade file that you downloaded from the Guest Internet web site onto your computer. When the file is located, click on the file then click on the Upgrade Firmware button.

The upgrade process will take approximately 15 minutes. Do not disconnect power to the gateway during this process or the program storage memory may be corrupted.

A message will indicate when the upgrade process is complete and then the unit will reboot to work with the new firmware.

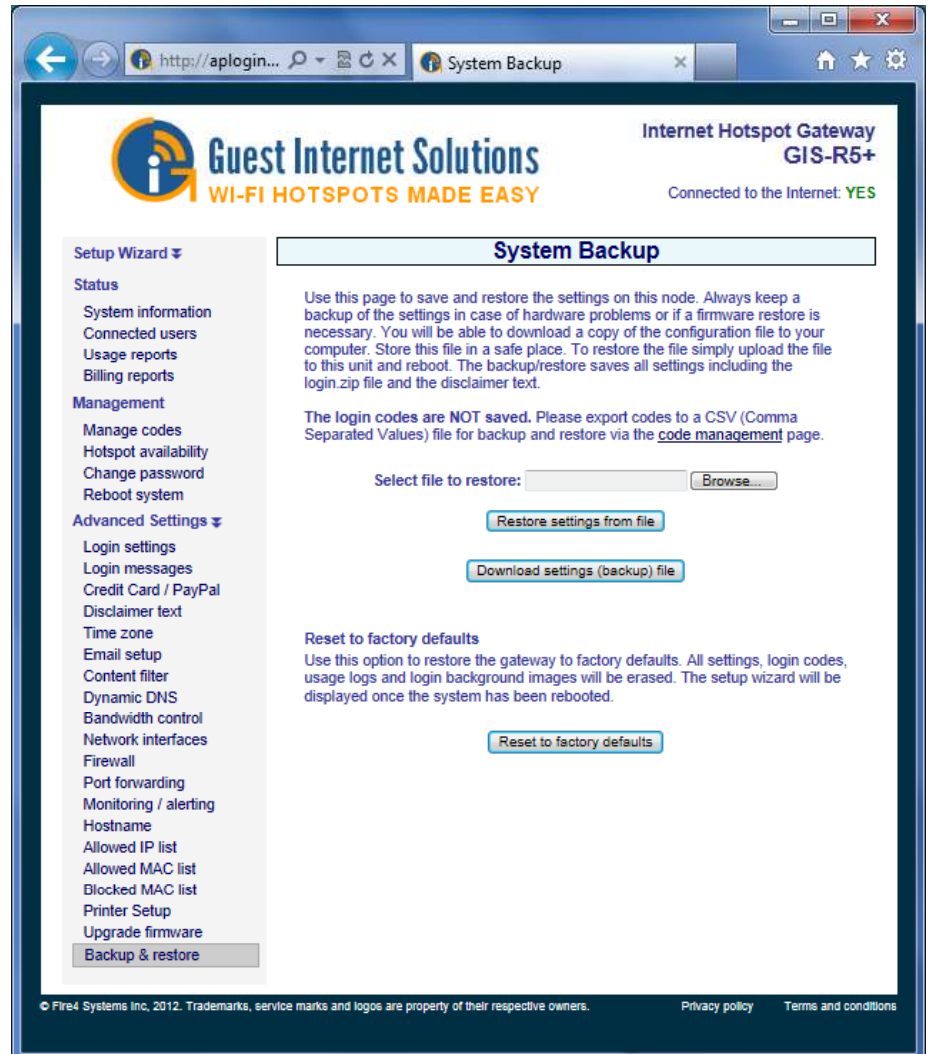




## Backup and Restore

All configuration parameters that have been set on a gateway unit are stored in a file in memory. The configuration file can be downloaded to a computer and saved for backup purposes. This page also permits the configuration backup file to be uploaded into the gateway to restore a previous configuration setting.

### Configuration backup/restore menu page



The backup file contains the following information

- All configuration settings
- The login page zip file (if uploaded)
- The modified terms and conditions text

Configuration settings backup and restore has two important applications. The first is to save the configuration file each time that the gateway configuration is changed. If some problem occurs with a configuration change then the previous configuration can be restored. The second application is for installers who are putting many similar configured gateways in a restaurant or hotel chain. One gateway is configured for the application and then the configuration file is saved. The configuration file is restored into all other gateways to be installed at different locations, thus speeding the installation process.

This screen also has a button that can be used to reset the unit to factory defaults. The function of this button is identical to the reset button on the rear of the enclosure. After the button is clicked all settings will be erased and the unit will restart with the wizard page.



## 9: RESET THE PRODUCT CONFIGURATION

### Reset the Product Configuration to Factory Defaults

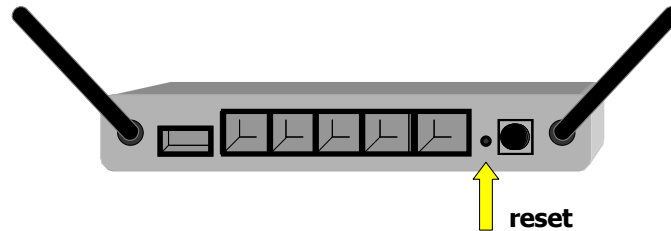
It is possible to get locked out of the Guest Internet gateway product, by forgetting the password or by incorrectly changing one of the IP addresses shown on the network configuration page.

This section describes procedures to reset all product parameters to factory defaults so that the product can be accessed once more. After this procedure however the product will have to be reconfigured. Upon restart the wizard screen will appear.

Reset to defaults as follows:

1. Power up the gateway unit and locate the hole in the enclosure for the reset button (shown in the diagram).
2. Using a paper clip, push the reset button (a click will be felt) and hold down for 10 seconds, after which the factory defaults will be restored.

The GIS-K1 gateways have a hole in the enclosure as shown with the reset button behind it



GIS-R2 gateway has a reset button in the rear of enclosure



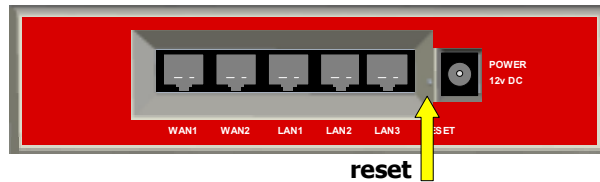
GIS-R3 gateway has a hole in the enclosure with the reset button behind it



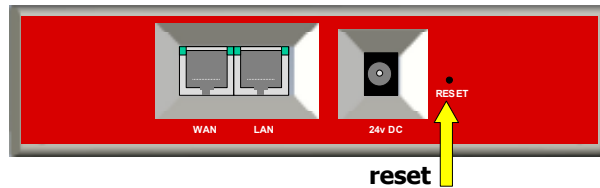
**GIS-R4 gateway has a reset button in the rear of enclosure**



**GIS-R5 gateway has a hole in the enclosure with the reset button behind it**

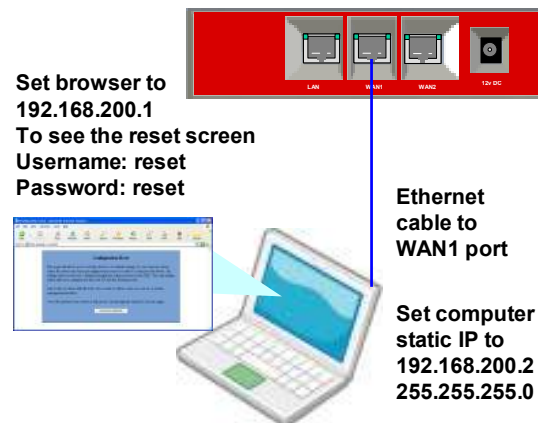


**GIS-R6 gateway has a hole in the enclosure with the reset button behind it**

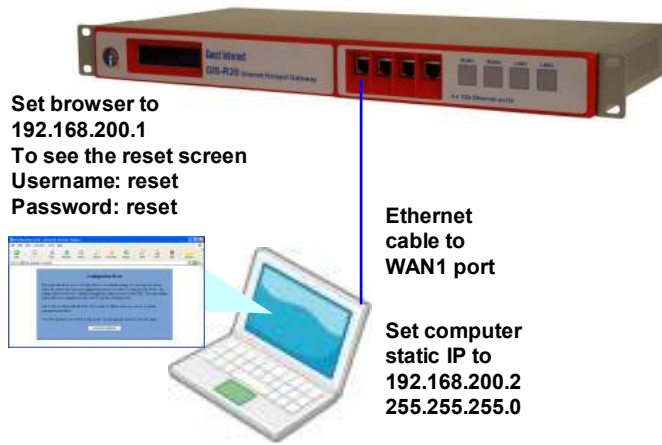


The GIS-R10, GIS-R20 and GIS-R40 products do not have a reset button. These products are reset to the factory default configuration using a computer connected to the primary WAN port of the device. The computer Ethernet port is set to an IP of 192.168.200.2. The browser is then opened at an IP address of: 192.168.200.1.

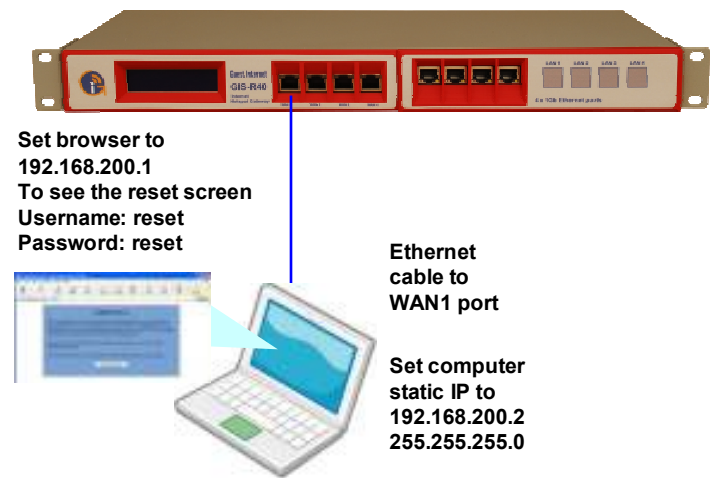
**GIS-R10 gateway connection to reset to factory defaults**



### GIS-R20 gateway connection to reset to factory defaults



### GIS-R40 gateway connection to reset to factory defaults



A box will open requesting a username and password. The username is **reset** and the password is **reset**. Click on enter and the screen shown below will appear.

### Reset Factor Defaults Screen



Click on the **Reset to defaults** button and then wait two minutes. Finally, switch the product power off then on and proceed to reconfigure the product using the wizard as described in an earlier section.

## 10: PROGRAMMERS REFERENCE

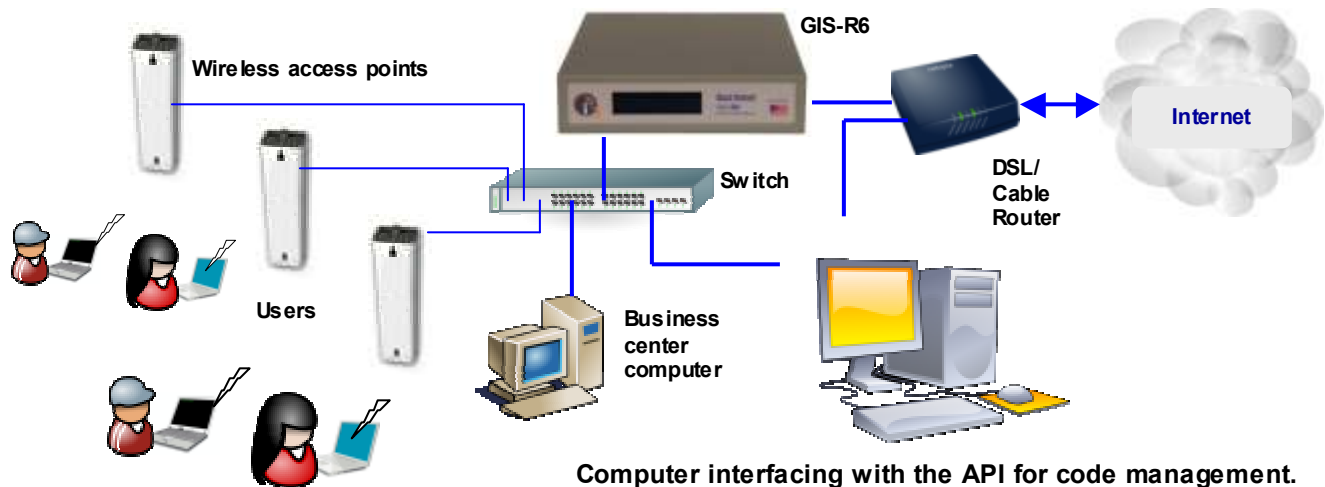
### Access Code Request API for PoS and PMS Systems

This section describes implementation of PoS access code requests using the Guest Internet firmware API

The access code request API is implemented in GIS firmware so that PoS vendors can include a screen button that prints a hotspot access code on the ticket printer for sale to guests. The access code request API is implemented in all GIS firmware versions and is available to PoS vendors and other systems integrators upon request. In order to implement the API the network configuration must be made as shown below.

#### API Implementation with the GIS-gateway

The GIS firmware includes a firewall from the DMZ to the private network to ensure compliance of the PCI-DSS recommendations. The firewall prevents any DMZ public access to the private subnet, which protects sensitive information stored in PoS computers. The GIS-gateway has four LAN ports to connect DMZ devices.



**Computer interfacing with the API for code management. The computer can be connected to the LAN side or the WAN side (with remote access activated) of the gateway.**

#### Access Code Request API Criteria:

Any computer can make an API request, however the API request must include the password for CODES (not the password for ADMIN).

A computer in the DMZ can make a request directly to the gateway. A computer in the private network can make a request only after the remote access box in the firewall menu has been checked.

The API has three separate functions

- Generate one or more codes (up to the limit permitted by the gateway)
- List access codes available on the gateway with status of each
- Delete codes and remove from the database



## Guest Internet Login Code API

Any computer or other system capable of performing HTTP communications can control the login codes on the GIS R and K units remotely. The programmer must have the password for the CODES login in order to perform API commands.

The access code API has been designed to allow systems such as POS (Point-of-Sale) to automatically manage code generation, removal and testing. Hotspot administrators wishing to control codes from a web browser should not use the API, instead they should use the web user interface at <http://aplogin.com/codes>.

Access to the API is controlled via a username and password. The username is always set to 'codes'; the password can be changed via the password page in the web management interface. There is no default password.

The API is designed for programmers and systems integrators who understand HTTP communications; how to form queries and how to parse responses from a web server. A hotel or restaurant wishing to implement the GIS API on their PoS system should seek advice from the PoS supplier before deciding to use the feature: there will be some cost associated with implementing the API calls in the PoS software.

### Creating codes

Codes can be added to the system via a single HTTP call, the URL to use is:

<http://aplogin.com/codes/makecode.cgi>

The IP of the GIS device can also be used instead of the *hostname*

Parameters to pass are shown in the following table:

Parameter	Values	Optional	Comments
num	Number of codes to create	no	Argument must be included in the call. The maximum number of codes is limited by the codes available on the gateway (see error messages)
time	Time in minutes	no	Argument must be included in the call.
type	Type of code: n = normal / single user m = multi-user	no	Argument must be included in the call.
download	Download limit (kbps)	Yes	Argument is optional and is not necessary for the call
upload	Upload limit (kbps)	Yes	Argument is optional and is not necessary for the call

An example call would be:

<http://aplogin.com/codes/makecode.cgi?num=1&time=30&type=n>

This would create a normal, single user code with a 30 minute duration.

The API call will either return a new code which is ready to use or an error; the possible errors are listed below:

- ERROR: Invalid parameters
- ERROR: You can't create more than XX codes
- ERROR: Code type not valid
- ERROR: Code time not valid
- ERROR: Code upload limit not valid
- ERROR: Code download limit not valid





If not logged in to the device, the password should be passed as an argument:

<http://codes:password@aplogin.com/codes/makecode.cgi>

The programmer can provide the password with each call to ensure that the call can be completed in the event that power has been cycled on the GIS device or on the PoS.

### Deleting codes

Codes can be deleted from the system via a single HTTP call, the URL to use is:

<http://aplogin.com/codes/deletetcode.cgi>

Parameters to pass include:

Parameter	Values	Optional	Comments
code	Code to be deleted	no	Argument must be included in the call.

An example call would be:

<http://aplogin.com/codes/deletetcode.cgi?code=876DTW>

This would remove the code 876DTW if it exists on the system.

The API call will either return OK or an error; the possible errors are listed below:

- ERROR: Invalid parameters
- ERROR: Code does not exist
- ERROR: Unable to delete code

### Viewing codes

Codes cannot be tested individually but a call can be made to list all of the codes on the system, it is then up to the software making the API call to parse the data returned and present it in the format required for the user or make any search or tests required on a code.

A list of codes can be obtained from the system via a single HTTP call, the URL to use is:

<http://aplogin.com/codes/showcode.cgi>

There are no parameters to pass for this API call.

The API call will either return a list of codes or an error message, the list of codes are presented in a tab (\t) delimited format with a header row. An example output is shown on the following page:



CODE	TIME	TYPE	USED	LEFT	DOWN	UP
113DRW	2	n	Yes	Expired	*	*
1AT1AQ	30	t	No	30	*	100
3B0AQ0	2	n	Yes	Expired	*	999
61QG8G	30	t	No	30	*	*
8CWJLE	30	n	No	30	*	*
94KH4E	30	n	No	30	*	*
ARLGH0	30	m	No	30	*	*
BJKBH7	2	n	Yes	Expired	*	*
M47TGF	32	t	No	32	*	999
WY7W0R	2	t	No	2	*	999

The \* (asterisk) in the UP and DOWN limit columns show that no limit has been set and that system wide limits will be imposed on the user.

The error message below will be returned if the clock is not set on the system, without the clock it is not possible to calculate the time remaining:

ERROR: Clock not set

### Creating codes

Codes can be added to the system via a single HTTP call, the URL to use is:

<http://aplogin.com/codes/makecode.cgi>

Password for codes needs to be created first at:

<http://aplogin.com/admin/password.cgi>

If not logged in to the **codes interface at <http://aplogin.com/codes>**, the password should be passed as an argument:

<http://codes:password@aplogin.com/codes/makecode.cgi>

The IP of the GIS device can also be used instead of the hostname.

### Get list of allowed MACs

Type the URL:

<http://aplogin.com/admin/macmanage.cgi?list=allowed>

### Get list of blocked MACs

Type the URL:

<http://aplogin.com/admin/macmanage.cgi?list=blocked>

### Block a MAC

Type the URL:

<http://aplogin.com/admin/macmanage.cgi?mac=00:11:22:33:44:55&action=block>

Where the MAC address is written in the colon separated format as shown



### **Allow a MAC**

Type the URL:

<http://aplogin.com/admin/macmanage.cgi?mac=00:11:22:33:44:55&action=allow>

Where the MAC address is written in the colon separated format as shown

### **Enable remote management**

Remote management can be enabled by substituting [aplogin.com](http://aplogin.com) for the IP address of the gateway.

### **Program Implementation**

The API can be accessed with any programming language or operating system.

Use a web/http client library. Libcurl (<http://curl.haxx.se/libcurl/>) is probably one of the best open source ones. Essentially, only a web client is required to make an HTTP request to the web server on the GIS-gateway. The response will come as plain ASCII and can be parsed in any number of ways.

If a secure connection is required then a library capable of HTTPS as well as an SSL library like openssl is required.

Here is a simple example in C using libcurl:

<http://curl.haxx.se/libcurl/c/simple.html>



## 11: LINUX DISTRIBUTION

All Guest Internet products use the Linux operating system, as part of the software suite included with each product. The Linux operating system is distributed under the GNU (General Public License). Guest Internet Solutions and its parent company Fire4 Systems Inc. abides by all the terms of the GNU. The Linux distribution installed in Guest Internet products is available on a CD. Customers can request a copy of the Linux distribution CD and will be charged \$10 for packing and postage of the CD. For more information, please call 1-800-213-0106.

The software distribution does not include proprietary applications programs developed exclusively for Guest Internet Solutions by Fire4 Systems (UK) Ltd.

### GNU GENERAL PUBLIC LICENSE Version 2, June 1991

*Copyright (C) 1989, 1991 Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA. Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.*

#### Preamble

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

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

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

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

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

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

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

*The precise terms and conditions for copying, distribution and modification follow.*



**GNU GENERAL PUBLIC LICENSE  
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION**

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

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

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

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

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

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

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

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

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

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





a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

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

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

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

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

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

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

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

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed



through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

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

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

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

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

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

#### NO WARRANTY

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

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

END OF TERMS AND CONDITIONS

***This Manual is Copyright © Fire4 Systems, Inc., 2005-2015. All Rights Reserved***

***Guest Internet Solutions is a division of Fire4 Systems Inc.***